Pääesikunta

Lausunto

29.01.2021 PEJOJÄOS AK AR1835

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

PÄÄESIKUNNAN LAUSUNTO KYBERTURVALLISUUDEN KEHITTÄMISOHJELMASTA

1 JOHDANTO

Puolustusvoimat arvostaa mahdollisuutta lausua kyberturvallisuuden kehittämisohjelmasta. Kehittämisohjelma on ajankohtainen sekä tarpeellinen. Kokonaismaanpuolustuksen sekä valtion toimintakyvyn ja suvereniteetin turvaamiseksi julkishallinnon ja elinkeinoelämän läpileikkaava kehittämisohjelma on välttämätön.

Puolustusvoimat on osallistunut kehittämisohjelman laatimistyöhön eri vaiheissa ja korostanut systemaattisesti erityisesti kansallisen turvallisuuden ja kyberpuolustuksen toimintaedellytysten varmistamisen tärkeyttä myös kyberturvallisuuden kehittämisohjelman toimenpiteiden kautta.

Kyberpuolustus on vuoden 2013 kyberturvallisuusstrategian mukaan poikkihallinnollista moniviranomaistoimintaa. Vuoden 2019 kybertuvallisuusstrategiassa kyberturvallisuuden johtamisen, suunnittelun ja varautumisen keskeisiä kehittämisen osa-alueita olivat kyberpuolustus ja kansallista turvallisuutta vaarantavien kyberuhkien torjunta. Kyberturvallisuuden kehittämisohjelma on siten luonnollinen yhteys tuoda esille myös kansallisen turvallisuuden ja kyberpuolustuksen kehittämistä.

Digitaalisen toimintaympäristön kehitystä sanelevat teknologian kehitys, sen merkitys taloudelle ja yhteiskunnan toiminnan muutokselle. Viime aikoina niin kutsutun kovan turvallisuuden korostuminen kyberympäristössä on kuitenkin haastanut teknologisiin mahdollisuuksiin nojaavaa kehityskulkua. Tämä ilmenee lisääntyneinä kyberuhkina, -vakoiluna ja jopa -iskuina eri toimijoita kohtaan. Muutos on pysyvä eikä sitä voida sivuuttaa missään maassa kansallisen kyberturvallisuuden kehittämisessä. Muuttuneessa digitaalisessa toimintaympäristössä myös kyberpuolustuksella ja kansallisen turvallisuuden näkökulmien huomioimisella on aiempaa korostuneempi merkitys. Ne ovat keskeisiä osa-alueita myös digitaalisen toimintaympäristön luomien uusien mahdollisuuksien varmistamisessa.

TITUKRI-työssä (Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla) laajemmat kybertoimintaympäristöön liittyvät kysymykset mm. kansallisen turvallisuuden ja maanpuolustuksen osa-alueet rajattiin pois ja määritettiin kyberturvallisuuden kehittämisohjelman kuvausvastuulle. Tämä loi selkeää painopistettä TITUKRI-työlle, mutta antoi samalla lisävaatimuksia kyberturvallisuuden kehittämisohjelmalle. Tällä hetkellä kyberturvallisuuden kehittämisohjelmassa on useita suoraan tai välillisesti kansallista turvallisuutta ja kyberpuolustusta tukevia kokonaisuuksia osaamisen kehittämisen, tutkimuksen, yritystoiminnan sekä kyberteollisuuden osa-alueilla. Kuitenkin myös kehittämisohjelman merkittävimmät puutteet ovat kansallisen turvallisuuden ja kyberpuolustuksen kehittämisessä.

2 YLEISTÄ

Kehittämisohjelman lähestyminen on mahdollisuuksia painottava kuten kyberturvallisuusstrategiakin. Lähestymistapa on perusteltu ja ohjelman sisältö noudattaa tätä linjaa. Kyberturvallisuuden kansallisen ratkaisun rakentaminen keskittyy kansallista kilpailukykyä parantaviin talous- ja kauppapoliittisiin, viennin edistämisen toimenpiteisiin. Samanaikaisesti keskeiseksi haasteeksi todettiin osaajapula ja kilpailu osaajista toimijoiden välillä. Yhteistyö, yhteiset rakenteet, jaetut kyvykkyydet ovat vähintäänkin yhtä keskeistä kuin kansallisen pärjäämisen edistäminen. Mahdollistavien toimenpiteiden sekä kasvun ja kansainvälistymisen korostaminen ei saa kuitenkaan rajata kansallista turvallisuutta tai kyberpuolustusta parantavia toimenpiteitä pois kehittämisohjelmasta.

Suomen kyberturvallisuuden kehittämisen tulee perustua uhkien ja nykytilan todenmukaiseen arviointiin. Toimintaympäristön muutos edellyttää sekä ”pehmeän” että ”kovan” kyberturvallisuuden kehittämistä laaja-alaisesti, myös maanpuolustuksellisen osan sisältävää tarkastelua sekä eri osa-alueiden aktiivista yhteensovittamista.

Kehittämisohjelman toimenpidesuunnitelmat ovat merkittäviltä osin passiivilauseita ja tavoitteen tai linjauksen omaisia toteamuksia sen sijaan, että niissä kuvattaisiin konkreettista etenemispolkua kyberturvallisuusstrategian asettamiin tavoitteisiin. Keskeinen osa tavoitteisiin pääsemisen arviointia on kuvattujen toimien mittarien hyvyys. Nyt osa liitteen mittareista on hyvin yleisiä. Liian yleisellä

tasolla olevilla mittareilla on helppo sanoa, että tavoite on saavutettu, vaikka tosiasiallisesti näin ei ole.

Kehittämisohjelma ei ole realistinen ilman selvästi suurempaa rahoitusta. Vaikka niin kutsutut normaalit toimintamenot voivatkin olla resurssillinen ratkaisu niihin kehittämiskohteisiin, joilla muutetaan nykyistä toimintaa uuden malliseksi toiminnaksi, niin toimintamenot eivät riitä ratkaisemaan esimerkiksi yritystoimintaan tai muihin uusiin avauksiin liittyviä merkittäviä kehittämiskohteita. Myös tavoitteisiin, joiden keskeinen resurssi on vapaaehtoinen osallistuminen kunkin omilla resursseilla (erityisesti 3. ja 4. sektori), liittyy merkittäviä riskejä toteutumisen kannalta. Tällöin niiden varaan ei etenkään viranomaisten tulisi laskea, vaikka toiminnan edistäminen onkin tärkeää. Tämän tulisi näkyä tavoitteiden asettelussa.

Kehittämisohjelman todetaan ulottuvan vuoteen 2030 saakka, mutta suurin osa esitetyistä toimenpiteistä ajoittuu vuodelle 2021 tai lähivuosille. Kehittämisohjelman jäsentämiseksi tulisi harkita esimerkiksi vaiheistamista ja vaihekohtaisia strategisia tavoitteita ja vaiheiden suunnittelun aikataulun kuvaamista. Lisäksi kehittämisohjelmassa tulisi esittää selvästi yhteys, miten esitetyillä toimenpidelistauksilla saavutetaan uskottavasti kaikki Suomen kyberturvallisuusstrategian tavoitteet. On hyvä, että kehittämisohjelman linjausten mukaan ohjelman teemoja tullaan jatkossa päivittämään, sillä myös jatkossa on kansallisesti kyettävä vahvemmin linkittämään kyberturvallisuus ja kyberpuolustus sekä sovittamaan saadut kokemukset toiminnan ja suorituskykyjen kehittämiseen. Kyberpuolustus ja kyberturvallisuus ovat toisistaan riippuvaisia.

3 KEHITTÄMISOHJELMA KANSALLISEN TURVALLISUUDEN JA KYBERPUOLUSTUKSEN NÄKÖKULMASTA

3.1 EU:n ja kansallisen kyberturvallisuusstrategian linjausten huomiointi

Vuoden 2019 kyberturvallisuusstrategia painottaa kyberpuolustuksen olevan yksi kyberturvallisuuden kehittämisen painopistealueista. Vastaavasti Euroopan unionin kyberturvallisuusstrategia korostaa kansallisen turvallisuuden ja kyberpuolustuksen merkitystä kyberturvallisuuden tavoitteisiin pääsemiseksi sekä oman toiminnan vapauden takaamiseksi. Kokonaisuudessa korostuu niin kansallisen ja kansainvälisen yhteistoiminnan kuin kansallistenkin kyberkyvykkyyksien kehittämistarpeet. Valitettavasti nämä periaatteet eivät ole täysmääräisesti jalkautuneet kyberturvallisuuden kehittämisohjelmaan.

EU:n kyberstrategian kansallisen toimeenpanon tulisi olla pitkälti kyberturvallisuuden kehittämisohjelman vastuulla. EU:n strategiasta kansalliseen kyberturvallisuuden kehittämisohjelmaan päätyneet kirjaukset jäävät tällä hetkellä kokonaisuutena vaisuiksi ja periaatteellisiksi, esimerkiksi viranomaisten yhteistoimintaa velvoittavan julkilausuman osalta: “Several communities, composed of networks, EU institutions, bodies and agencies, as well as

Member State authorities, are responsible for preventing, discouraging, deterring and responding to cyber threat, using their respective instruments and initiatives. These communities include: (i) NIS authorities, such as CSIRTs, and disaster response; (ii) law enforcement and judicial authorities; (iii) cyber diplomacy; and (iv) cyber defence.”

EU:n kyberstrategia korostaa kaiken tasoisen (tiedustelu, tilannekuva, vaste, pidäke) yhteistoiminnan laajentamista. Se lähestyy kyberturvallisuuden haasteita toimenpidelähtöisesti sekä osin rakenteistamalla (esim. organisointi) niiden toteuttamisen. Kansallisen ohjelman toimenpiteet ovat geneerisesti kyvykkyyttä lisääviä eikä toimijoiden yhteistyörakenteille ole kuvattu kehittäviä toimenpiteitä. Puolustusvoimat esittää, että kyberturvallisuuden kehittämisohjelmassa tulee huomioida Euroopan unionin kyberturvallisuusstrategian periaatteet nykyistä paremmin osana kansallisen kyberkyvykkyyden kehittämistä.

Kyberturvallisuusstrategiassa 2019 todetaan EU:n linjausten mukaisesti "Kybertoimintaympäristöä suojataan kasvattamalla kynnystä erityyppisiin kyberhyökkäyksiin muun muassa parantamalla kyberhyökkäysten havainnointi- ja attribuutiokykyä sekä kykyä vastatoimiin. Vastatoimet voivat koostua esimerkiksi lainvalvontatoimista, diplomaattisista toimenpiteistä tai aktiivisista kybervastatoimista. Vastatoimien kehittämisessä otetaan huomioon EU:n vahvan kyberpuolustuksen kehittämisen linjaukset. Kyberrikollisuuden torjuntaan osallistutaan EU:n puitteissa oikeus- ja lainvalvontaviranomaisten kansainvälisellä yhteistyöllä sekä osallistumalla kansainvälisen oikeuden ja sopimusten kehittämiseen." Kehittämisohjelmasta ei kuitenkaan löydy toimenpiteitä tämän strategisen tavoitteen saavuttamiseksi. Valtioneuvoston hyväksymän vuoden 2019 kyberturvallisuusstrategian toimeenpanemiseksi Puolustusvoimat esittää kyseisen keskeisen strategisen tavoitteen saavuttamiseksi vaadittavien kehittämistoimenpiteiden lisäämistä kehittämisohjelmaan kansallisten kyvykkyyksien kehittämiseksi.

3.2 Tehokkaat kansalliset kyberturvakyvykkyydet

Puolustusvoimien näkökulmasta kehittämisohjelman pääteema on "Tehokkaat kansalliset kyberturvallisuuskyvykkyydet".

Kyberturvallisuusstrategiassa korostetaan jokaisen toimijan vastuuta kyberturvallisuuden toteuttamiseksi. Lähtökohtana hyvä ja tällöin jokaisen viranomaisen ja yhteiskunnan toimijan tulee olla selvillä lakisääteisten ja muiden velvoitteiden muuttamisesta organisaation tehtäviksi ja toiminnaksi. Tavoitteessa onnistuminen edellyttäisi laaja-alaisesti sen selvittämistä, mitkä yhteiskunnan toiminnan kannalta tärkeät kybertoimintaympäristön toimenpiteet ja vastuut ovat kunnossa, mitkä jäävät tekemättä ja missä on päällekkäisyyttä, joka ei ole tarkoituksen mukaista. Puolustusvoimat esittää, että tämän tulisi olla osa kansallisen kyberkyvykkyyden kehittämistä.

"Tehokkaat kansalliset kyberturvallisuuskyvykkyydet" -teema kulminoituu kyberpuolustuksen näkökulmasta yhteen toimeenpanosuunnitelman kohtaan 8.1, "Arvioidaan viranomaisten toimintaedellytykset nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa ottaen huomioon uhkaympäristön jatkuva kehittyminen sekä käynnistetään tarvittavat toimet". Tämä tehtävä sisältää Puolustusvoimien näkökulmasta kyberturvallisuuden edistämisen rinnalla kyberpuolustuksen edellyttämien toimenpiteiden edistämisen, ennakoivan ja aktiivisen kyberpuolustuksen sekä kyberympäristön suvereniteettia tukevan toiminnan kehittämisen. Keskeisenä osana sitä tulee olla vuoden 2013 kyberturvallisuusstrategian linjausten loppuun saattaminen, jossa Puolustusvoimille ja keskeisille turvallisuusviranomaisille luodaan maanpuolustuksen-, virka-avun-, aluevalvonta- sekä kriisinhallintatehtävien toteuttamiseksi tarpeelliset toimivaltuudet, osaaminen ja riittävät tiedonsaantioikeudet.

Tämä edellyttää kokonaisvaltaista toimivaltuustarkastelua ja sen myötä käynnistettävä säädösvalmistelua. Puolustusvoimat esittää säädösvalmistelun kirjaamista konkreettisena toimena osaksi kohdan 8.1 toimenpiteitä. Lainsäädäntö on keskeinen valtion työkalua ohjauksen ja myös mahdollistamisen näkökulmasta. Koska merkittävät säädösmuutostarpeet liittyvät kansalliseen kyberpuolustuksen kehittämiseen, on luonnollista, että työtä lähtee vetämään nyt kirjatusti Puolustusministeriö. Kokonaisuus on rinnastettavissa vähintään tiedustelulainsäädännön laajuuteen. Säädösvalmistelu voidaan toteuttaa myös vaiheittain siten, että ennen varsinaista lainsäädäntöhanketta laaditaan esiselvitys lainsäädännön kehittämistarpeista, kuten tiedustelulainsäädännön kehittämisessä meneteltiin.

Puolustusvoimat vastaa uskottavan puolustuskyvyn luomisesta. Osana uskottavaa puolustuskykyä Puolustusvoimien täytyy voida itsenäisesti hoitaa kriittisimmät kyberpuolustuksen tehtävät ja luoda niihin kyvykkyydet. Puolustusvoimat ei voi olla täysin riippuvainen muiden valtionhallinnon toimijoiden tai muiden sektorien kyvyistä tuottaa palveluita tai tuotteita Puolustusvoimien operatiiviseen toimintaan sen enempää normaali- kuin poikkeusoloissa. Tämän vuoksi ohjelmassa esitetty keskittyminen yritystoimintaan ja teollisuuteen ei saa tarkoittaa kyberkyvykkyyden ja -resurssien ulkoistamista. Lisäksi Puolustusvoimien on oltava mukana etenkin salaustuotteiden suunnittelussa ja kehittämisessä. Puolustusvoimissa on asiaan liittyvää tietotaitoa sekä Puolustusvoimat on valtionhallinnossa merkittävä salaustuotteiden loppukäyttäjä ja asiakas.

Kansallisen salaustuote- ja kryptokyvykkyyden edistäminen on tärkeä kokonaisuus kyberomavaraisuuden edistämisessä. Myös kryptostrategiatyön vakiinnuttaminen on kannatettavaa. Kansallinen kryptostrategiatyö ja muutenkin kansallisen krypto-osaamisen kehittäminen tulisi rakentaa Puolustusvoimien fasilitoiman strategiatyön ja Puolustusvoimissa kehitettävän kansallisen kryptolaboratorion osaamisen pohjalle.

Puolustusvoimat on jo vuosia rakentanut Kyberturvallisuusstrategia 2013 linjausten mukaista kryptokyvykkyyttä, joka tulisi päällekkäisyyksienkin välttämiseksi hyödyntää myös AQUA-kyvykkyyden saavuttamiseksi. AQUA-kyvykkyyden saavuttamiseksi on oleellisempaa panostaa tietyille osa-alueille keskitetysti kuin laajoille osa-alueille ohuesti. Ohjelmassa mainittu tavoite AQUA-statuksesta on hyvä. Sen rakentaminen käytössä olevilla resursseilla ei kuitenkaan vaikuta

mahdolliselta. Kansainvälisen vertailun perusteella tiedetään, että kyseinen AQUA-statuksen saavuttaminen vaatii useita salaustuoteasiantuntijoita ja kryptologeja, sekä vähintään useiden vuosien mittaista määrätietoista kehittämistä toteutuakseen. Tarvittavan osaamispoolin ja kyvykkyyden saavuttamiseksi Puolustusvoimat on valmis osallistumaan työhön. Puolustusvoimien tulee olla mukana nimettynä toimijana AQUA-kyvykkyyden (toimenpide 12.2) saavuttamisen osalta.

3.3 Huippuluokan osaaminen

Maanpuolustuksen kuuluessa kaikille, myös kyberpuolustus kuuluu kaikille. Yleinen kybertaitojen kasvattaminen sekä kyberturvallisuuden koulutusjärjestelmän kehittäminen ovat kokonaisuuksia, joiden kautta myös kyberpuolustus saa osaamista ja kykyä niin päivittäiseen etulinjaan kansalaisten parantuneen osaamisen kautta kuin kyberpuolustuksen huippuammattilaisiksi palkattuna henkilökuntana tai asevelvollisina.

Asevelvolliset ovat kyberpuolustuksen keskeisin suorituskyky, jota tullaan hyödyntämään aikaisempaa laajemmin myös operatiivisissa tehtävissä. Siten he ovat merkittävässä roolissa myös kansallisessa kyberturvallisuudessa. Kyberalan asevelvolliset työskentelevät tyypillisesti myös siviilitehtävässään kyberalalla valtakunnallisina huippuosaajina. Kyberosaamisen kehittäminen sekä siviili- että maanpuolustustehtävässä tukevat siten vahvasti toisiaan. Puolustusvoimat näkee, että osana yhteiskunnan kyberturvallisuuden huippuosaamisen kehittämistä tulee huomioida myös asevelvollisuuden aikana joko varusmiehenä tai reserviläisenä hankitun kokemuksen luomat mahdollisuudet nykyistä laajemmin. Tämä tulisi kirjata kehittämisohjelmaa vähintään yhdeksi mittariksi.

Myös kyberpuolustukselle on tärkeää kannustaa naisia kyberalalle. Näin ollen puolustusvoimienkin tulisi mukana yhtenä toimijan edistämässä asiaa myös kehittämisohjelman kirjauksessa (toimenpide 1.4) Vastaavasti kansalaisten kyberturvallisuustietoisuuden lisääminen (toimenpide 1.6) on kyberpuolustuksenkin näkökulmasta tärkeä kokonaisuus, jota Puolustusvoimat pystyy mm. asevelvollisten koulutuksen kautta edistämään. Yhteinen ponnistus edellyttää osallistumista toimijana viestintäsuunnitelman laatimiseen.

3.4 Vahva kotimainen kyberturvateollisuus

Tutkimustoiminnan yhteistyön ja koordinoinnin kehittäminen tukee niin kansallisen osaamisen kuin myös yritystoiminnan kehittämistä. Tutkimustoiminnassa tulee huomioida osaamisen kehittämisen ja yritystoiminnan tukemisen lisäksi myös eri viranomaisten tarpeet kansallisen turvallisuuden, maanpuolustuksen tai jonkin muun turvallisuuden alan spesifien ja tiedon jatkohyödynnettävyyden kannalta rajatumpien tutkimusaiheiden edistämiseen. Tutkimustoiminnan tulee edistää myös kriittisten osa-alueiden kyberomavaraisuuden kehittymistä.

Kotimaisen kyberturvallisuuden yritystoiminnan merkitys valtion huoltovarmuuteen sekä kriisinsietokykyyn on merkittävä. Yritystoiminnan tukeminen on kriittistä kotimaisen huoltovarmuuden, mutta myös puolustusjärjestelmän sotilas- ja siviilikomponentin suorituskyvyn varmistamisen näkökulmasta. Huoltovarmuusnäkökulman lisäksi erityisesti kansallisesti kriittisten osa-alueiden kyberomavaraisuuden edistäminen tulisi ottaa ponnekkaammin myös kyberturvallisuuden kehittämiskohteeksi oli sitten kyseessä huoltovarmuuskriittiset arvoketjut, yhteiskunnalle kriittiset tietovarannot, -palvelut tai -järjestelmät. Osana tätä prosessia (toimenpide 12.3) on kansallisen turvallisuuden näkökulmasta kriittisten kyberturvallisuusyritysten tunnistaminen ja turvaaminen kansallisessa omistuksessa. Puolustushallinnon tulee ehdottomasti olla mukana tässä työssä maanpuolustuksen tarpeiden näkökulmasta. Puolustusvoimilla on jo nyt merkittäviä kumppanuussopimuksia kansallisiin kyberturvallisuuden yrityksiin tai muuten merkittävää ja kriittistä yhteistoimintaa yrityskentän kanssa. Tätä tuntemusta tulisi hyödyntää.

Kehittämisohjelmassa tulisi pyrkiä kuvaamaan nykyistä selkeämmin ekosysteemi ja sen tavoitteet. Nykyisessä muodossaan asia jää yleiselle tasolle ja varsinaista konkretiaa on hankala löytää. Kehittämisohjelman ekosysteemiä tulisi lähteä rakentamaan kansallisen tason kyberturvallisuuden ja kyberpuolustuksen moottorin kautta, missä vaativa konkreettinen kehittäminen ja tavoitteet lähtisivät rakentamaan osaamista ja yritystoimintaa geneerisiä toiveita paremmin. Huomion arvoista on, että tämä kokonaisuuden käynnistäminen on valtionhallinnon omissa käsissä ja rahallista resurssia käytettävissä olemassa olevien hankkeidenkin kautta. Sen suuntaaminen kotimaisen kyberteollisuuden kehittämiseen saattaa nimenomaan edellyttää kansallisen turvallisuuden ja maanpuolustuksen lähtöisyyttä (PUTU-laki).

3.5 Kiinteä yhteistyö

Kyberturvallisuuden harjoitustoiminnan kehittäminen sekä viranomaisten kyberalan osaamisen ylläpitämisen ja kehittämisen mahdollistaminen on kannatettavaa. Tämä edellyttää kuitenkin, että osaamisen kehittämisessä ja harjoitustoiminnassa huomioidaan kunkin kyberviranomaisen erityistarpeet ja että harjoittelua suoritetaan eri valmiustilojen skenaarioissa niiden erityistarpeet huomioiden. Harjoitustoiminnassa on tärkeää myös ennakkoluulottomasti kokeilla uusia toimintatapoja ja vastuita, vaikka sen hetkinen lainsäädäntö ei niitä vielä tunnistaisi. Tämä tukee myös kyberturvallisuuden kehittämisohjelman välitarkasteluita ja päivittämistä kehityskauden aikana sekä seuraavan strategian laadintaa. Kokeilun ja kehittämisen tulisi olla myös valtionhallinnon harjoitustoiminnan kulmakivistä. Viranomaisten harjoitustoiminnan kehittäminen tukee myös operatiivisen yhteistoiminnan tavoitteisiin pääsemistä, mutta se ei kuitenkaan yksi riitä vaadittavalle suorituskykytasolle pääsemiseksi.

Kehittämisohjelmassa ei ole kuvattu toimenpiteitä, joilla riittävällä tasolla parannettaisiin reagointikykyä nopeisiin kansallista turvallisuutta uhkaaviin tilannekehityksiin. Eri viranomaisten välinen yhteistyö ja koordinaatio sopivat hyvin pitkäjänteiseen kehittämiseen, mutta riittävän nopeaa reagointikykyä näillä toimilla ei saavuteta. Eri puolille valtionhallintoa toteutettavat

tilannekuvat eri kyberturvallisuuden näkökulmista ja viranomaiskoordinaatio eivät riitä keinoiksi vastata kansallista turvallisuutta koskeviin uhkiin. Toiminnassa on kyettävä jo normaalioloissa ilman poikkeusolojen lisätoimivaltuuksia toteuttamaan viranomaisten välittömästi aktivoituvaa, dynaamista, reaaliaikaista, korkean turvallisuusluokan, eri viranomaisten toimivaltuuksia nopeasti hyödyntävää yhteistoimintaa. Suomeen kohdistuvan kyberhyökkäyksen pikatilanteessa rakenteet, ratkaisut ja toimivaltuudet on oltava valmiina.

Yhteistoiminnan nopeusvaatimukset tulee suhteuttaa uhkatoimijoihin, jotka kykenevät muuttamaan toimintaansa huomattavan nopeasti. Hitaat viranomaisten väliset koordinointimekanismit ja osittain puutteellisesti yhteensopivat tietojärjestelmät eivät mahdollista riittävää reagointinopeutta. Tämä edellyttää operatiivisen yhteystoiminnan kehittämistä nykyisen yhteistyöpohjaisen toiminnan syventämiseksi. On huomioitava, että jatkuva operatiivinen yhteistoiminta on eri asia kuin laajojen häiriöiden ja poikkeamien hallinta, joka on tapauskohtaista toimintaa. Molempia kokonaisuuksia tulee kehittää. Puolustusvoimat esittää, että operatiivisen viranomaisyhteistoiminnan kehittäminen tulee lisätä kehittämistoimenpiteeksi lukuun 4 "Kiinteä yhteistyö".

Ulkoministeriö julkaisi Suomen kansalliset näkemykset kansainvälisen lainsäädännön soveltamista kyberympäristössä. Osana kohdan 4 tai 8.1 työtä ja myös edellä mainittua säädöstyötä, on luotava kansalliset toimintatavat, prosessit ja kyvyt (ml. resurssit) Suomen suvereniteetin turvaamiseksi myös kyberympäristössä sekä yhteistoimintamekanismit tuettaessa esimerkiksi kumppanimaiden attribuutiota tai vastatoimia.

4 LOPUKSI

Kehittämisohjelman johdannossa viitataan Haukka- ja Digitaalinen turvallisuus 2030 -ohjelmiin. Näiden lisäksi parhaillaan on käynnissä nk. TITUKRI-työryhmä. Kehittämisohjelman laatimisen vaiheissa kansallisen kyberturvallisuuden joidenkin osakokonaisuuksien pohdittiin tulevan käsitellyiksi näissä muissa ohjelmissa. On hyvä, että kansallista kyberturvallisuutta käsitellään ja rahoitetaan eri viranomaisten ohjelmissa, mutta vaarana on kokonaisnäkemyksen häviäminen ja mahdollisten katveiden syntyminen. Koska kyberturvallisuuden kehittämisohjelma toteuttaa nimenomaan kansallisen kyberturvallisuusstrategian, sen olisi syytä analysoida tarkemmin koko kansallisen kehittämisen kokonaisuus.

Lausunnolla olevan kyberturvallisuuden kehittämisohjelman tavoitteet ovat sinänsä kannatettavia. Se ei tällä hetkellä ole sellainen kokonaisvaltainen kansallisen kyberturvallisuusstrategian kehittämisohjelma, kuten kyberturvallisuusstrategioiden (2013/2019/EU) pohjilta voisi olettaa. Kehittämisohjelman tulisi sisältää kansallisen turvallisuuden ja kyberpuolustuksen kriittisiä ja laajoja kehittämistarpeita. Puolustusvoimat esittää, että kehittämisohjelmaa kehitetään vastaamaan näitä tarpeita.

Ottaen huomioon, että kehittämisohjelman aikajänne on vuoteen 2030 saakka, kansallisen turvallisuuden ja kyberpuolustuksen osakokonaisuuksien kehittämisen päälinjojen puutteet ohjelman lähtökohtatavoitteissa voi johtaa viiveisiin. Koska kyseessä on isoja kokonaisuuksia, joiden kehittäminen jo yksin säädöspohjan osalta on mittava ja pitkäkestoinen projekti, olisi ensiarvoisen tärkeää saada työ käyntiin välittömästi. Toimintaympäristön nopean muutos sekä oman ymmärryksen lisääntymien toimintaympäristöstä edellyttää myös kyberturvallisuusstrategian ajantasaisuutta. Puolustusvoimat esittää, että seuraava kyberturvallisuusstrategia työ aloitetaan viimeistään 2020-luvun puolivälissä.

Tässä lausunnossa esitetyillä muutoksilla Puolustusvoimien kehittämisohjelma tukee parhaiten myös kyberturvallisuuden kehittämisohjelman toimeenpanoa.

Rusila Tuomo
Pääesikunta