Lausunto

09.08.2024 Tulli/2024/00418-2

Asia: VN/36693/2023

# Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

## Lausunnonantajan lausunto

**Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään**

Tulli kiittää liikenne- ja viestintäministeriötä mahdollisuudesta lausua valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuusstrategiaksi 2024-2035.

Tulli pitää kyberturvallisuusstrategian uudistamista tärkeänä toimenpiteenä muuttuneessa toimintaympäristössä osana kansallista kokonaisturvallisuuden kehittämistä. Tulli pitää lausuttavana olevaa kyberturvallisuusstrategiaa kokonaisuutena kattavana ja laadukkaana. Strategia kuvaa hyvin toimintaympäristön muutosta, nykytilaa sekä tulevaisuuden suuntalinjoja. Toimeenpanosuunnitelman laadinnan yhteydessä pyydetään huomioimaan se, että toimenpiteet olisivat mahdollisimman yksiselitteisiä sekä toimeenpanon edellyttämät resursointitarpeet otetaan huomioon jo valmisteluvaiheessa.

Logistiikan huomiointi strategiassa:

Johdannossa (s. 8) on tuotu esille se, että kyberturvallisuus ja siihen liittyvät toimet osaltaan liittyvät kansallisen turvallisuuden ja samalla huoltovarmuuden turvaamiseen.

Toimintaympäristön muutoksen yhteydessä (s. 11) on huomioitu hyvin keskinäisriippuvuuksien tuntemus ja se, että kybertoiminta kohdistuu yhä laajemmin myös yrityselämään. Strategiassa onkin todettu asianmukaisesti, että elinkeinoelämällä on merkittävä rooli kansallisen kyberturvallisuuden varmistamisessa (s. 16). Logistiikan sektorilla voidaan edelleen todeta, että kansallinen ja kansainvälinen logistiikka nojaa pitkälti yksityissektorin toiminteiden varaan. Vastaavasti strategiassa on muutoin infrastruktuurin osalta tuotu esiin se, että elinkeinoelämä omistaa merkittävän osan Suomen kriittisestä infrastruktuurista ja vastaa sen kyberturvallisuuden varmistamisesta (s. 41). Tämä korostaa yksityisen ja julkisen sektorin vuoropuhelun tärkeyttä ja merkittävyyttä.

Logistiikkaa ei sellaisenaan mainita osana NATO työtä (s. 12), mutta näkemyksemme mukaan liittokunnan infrastruktuurin kehittäminen ja vahvistaminen edellyttävät loogisesti samalla tavalla mm. tavaran liikkumiseen liittyvän logistisen infrastruktuurin kehittämistä.

Strategiassa nostetaan huomiona esille (s. 26), että ”keskeistä on varmistaa elintärkeiden toimintojen, kriittisen infrastruktuurin, tietovarantojen, julkisten palveluiden sekä huoltovarmuuskriittisten toimijoiden toimivuus ja häiriönsietokyky”.

Logistiikka sellaisenaan on asianmukaisella tavalla huomioitu toimintaympäristön kuvauksen yhteydessä sikäli, kun strategiassa kuvataan toimitusketjujen turvallisuuden korostumista (s. 14).

Palvelu- ja toimitusketjujen pidentyminen ja monimutkaistuminen on nostettu esille, samoin logistiikan ja infrastruktuurin keskinäisriippuvuus. Strategian mukaan ”yhteiskunnan toimintakyvyn kannalta kriittisten toimijoiden täytyykin varmistaa, että myös niiden palveluntuottajat ja toimitusketjut ovat kyberturvallisia”. Tämä loogisesti tukee myös sitä, että jatkossa viranomaistoiminteita turvatessa ja kehitettäessä tulee turvata logistiikan ja huoltovarmuuden kannalta keskeisten viranomaistoimijoiden, kuten myös Tullin, kyvykkyys.

Yhtenä olennaisena osana on yksityisen sektorin kanssa tehtävä yhteistyö. Tämä on huomioitu strategiassa (s. 21), jossa todetaan kyberturvallisuuden ekosysteemin käsittävän kokonaisuutta kattaen laajalti niin julkishallinnon kuin yksityisen sektorin toimijat.

Vastaavasti palveluiden priorisointi nostetaan strategiassa esille (s. 27) ja tähän liittyen toimeenpanosuunnitelman yhteydessä tulee kriittisesti ja priorisoiden käydä eri valtionhallinnon toiminteita ja turvattavia palveluita läpi. Mikäli logistiikan aluetta halutaan jatkossa turvata osana kokonaisturvallisuuden (ml. kyberturvallisuus) tuotantoa, tulee Tullin palveluiden turvaaminen priorisoida riittävällä tavalla.

Viranomaisen toimintakyvyn varmistaminen:

Haasteena vähenevien viranomaisresurssien ja lisääntyvän sääntelyn maailmassa on Tullilla jatkossa se, miten kyetään turvaamaan riittävä osaaminen, jotta se voi yhtenä turvallisuusviranomaisena olla tukemassa kansalliselle turvallisuudelle ja huoltovarmuudelle olennaista kyberturvallisuutta. Samaan aikaan on tunnustettava strategiassa esille nostettu tosiseikka (s. 15), että julkisen sektorin kilpailukyky työnantajana on jäämässä yksityisen sektorin varjoon.

Viranomaisten toimintakykyä on jatkossakin vahvistettava kyberturvallisuuden alueella, jotta elinkeinoelämä voi luottaa viranomaisten toimintakykyyn ja toimintavarmuuteen – tämä koskee myös logistiikkaa ja tullisektoria. Luottamus liittyy myös siihen, että viranomaiset kykenevät turvaamaan kaikille toimijoille tasapuoliset toimintaedellytykset ja palvelut yhdenvertaisesti. Luottamusyhteiskunnan ylläpitäminen (s. 17) edellyttää tasaista ja laadukasta viranomaistoimintaa.

Luottamusta voidaan lisätä yhteistoiminnalla mm. harjoitusten kautta (s. 29) ja yksityisen sektorin kanssa tehtävä yhteistyö (public private partner, PPP) onkin nostettu yhdeksi strategiseksi tavoitteeksi. Kriittistä tässä yhteydessä on huomata se, että samaan aikaan kun PPP-yhteistyöllä voidaan tukea luottamusyhteiskunnan toteuttamista, voidaan tätä kautta yhteiskunnan toimin PPP:n avulla vahvistaa myös erityisesti viranomaisten kyvykkyyttä kohdata kyberuhkia, jos yksityisen sektorin erityisosaamista voidaan käyttää viranomaistoiminnan kehittämisessä. Tämä edellyttää jatkotoimia toimeenpanosuunnitelman yhteydessä.

Yksi osa toimintakyvyn rakentamista on keskeisten kyberturvallisuutta ylläpitävien viranomaisten koordinoima tilannekuva (s. 19), jota tulee aktiivisesti välittää valtionhallinnossa erityisesti turvallisuusviranomaisille (ml. Tulli) ja muille kriittisille keskusvirastoille. Jatkossa strategian

toimeenpanossa tuleekin tukea entistä vahvemmin tiedonvaihtoa ja yhteisten toimintamallien hyödyntämistä.

Tämä onkin nostettu yhdeksi kansallisen kyberturvallisuuden tavoitetilaksi (s. 21). Edelleen strategiassa todetaan (s. 33), että juuri ”yhteinen tilanneymmärrys mahdollistaa viranomaisten, yritysten ja yhteisöjen välisen tehokkaan ja luotettavan yhteistoiminnan kybertoimintaympäristössä”.

Rikostorjuntatoimenpiteiden hyödyntäminen osana kyberpuolustusta ja attribuutiota on tuotu strategiassa esille (s. 39). Tätä tulee edelleen jatkokehittää toimeenpanosuunnitelman yhteydessä. Tavoitetilana tulee varmasti olla kokonaismaanpuolustus ja ”whole of society” –mallin mukaisen vasteen kehittäminen.

Riittävä toimintamallien kehittäminen ja tiedonjako osana viranomaiskyvykkyyden kehittämistä on omiaan tukemaan ennakoivaa kybervarautumista. Strategian mukaisesti (s. 43) lienee suositeltavaa, että kyberkestävyyden indikaattorit myös laajennetaan kattamaan ennakoiva kybervarautumistyö. Parhaiden käytänteiden tunnistaminen, hyödyntäminen ja jakaminen osana strategian toimeenpanoa (s. 41) on varsin kannatettava jatkotoimi.

Strategiset kehittämisehdotukset

Strategiset kehittämisehdotukset (s. 44) pitävät sisällään edellä esille nostetut viranomaistoiminnan yhteistoiminnan ja kyvykkyyden seurannan ja kehittämisen sekä kyberrikollisuuden torjunnan. Lisäksi yksityisen sektorin kanssa tehtävä yhteistyö on tuotu hyvin esiin strategian kehittämisehdotuksissa.

Tullin kannalta olennainen logistiikkasektorin turvaaminen ja/tai kehittäminen ei ole sellaisenaan kirjattu kehittämisehdotuksissa.

Strategiaan tulisi kirjata maininnan kybersietoisuuden kehittämisestä eli siitä, että kybersietoisuuden kehittäminen kriittisen infrastruktuurin ja huoltovarmuuden, yhteiskunnan kannalta elintärkeiden toimintojen (ml. logistiikka) sekä julkisten palveluiden osalta on erillisen tarkastelun kohteena.

Lahti Toni
Tulli.fi