TRAFICOM Liikenne- ja viestintävirasto
Transport- och kommunikationsverket

Lausunto

Eduskunta
puolustusvaliokunta

PuV@eduskunta.fi

Päiväys/Datum
20.10.2021
Dnro/Dnr
TRAFICOM/474308/03.03.01/2021
Viite/Referens
Puolustusvaliokunta tiistai 26.10.2021 klo 10.30 / VNS 8/2021

Liikenne- ja viestintävirasto Traficomin lausunto puolustusvaliokunnalle puolustusselonteosta (VNS 8/2021 vp)

Liikenne- ja viestintävirasto Traficom kiittää mahdollisuudesta lausua puolustusselontekoa koskevassa asiassa. Traficom katsoo, että puolustusselonteossa on otettu kattavasti huomioon kyberturvallisuuteen liittyvät tulevaisuuden uhkakuvat sekä digitalisaation ja teknologisen kehityksen vaikutukset kybertoimintaympäristöön. Kyberturvallisuusuhkien globaalin ja rajat ylittävän luonteen sekä koko yhteiskuntaa koskevien vaikutusten vuoksi kyberturvallisuusuhkia tulee arvioida laaja-alaisesti ja kokonaisvaltaisesti. Kybertoimintaympäristön uhkia ja niihin liittyviä kansallisia kehittämistoimia tarkastellaan valtioneuvoston periaatepäätöksessä kyberturvallisuuden kehittämisohjelmasta, johon selonteossakin viitataan. Puolustusselonteossa asetettujen tavoitteiden toteutumisen näkökulmasta on tärkeää, että kyberturvallisuuden kehittämisohjelman rahoitus turvataan.

Selonteossa on kattavalla tavalla tunnistettu kyberturvallisuuden toimintakentän viranomaisroolit ja -vastuut sekä tehtävien hoitamiseen liittyvän yhteistyön merkitys. Kuten selonteossa todetaan, kyberturvallisuutta koordinoi Suomessa liikenne- ja viestintäministeriö ja puolustusvoimat vastaa Suomen sotilaallisesta kyberpuolustuksesta osana kansallista kyberturvallisuutta. Liikenne- ja viestintäministeriön hallinnonalalla toimiva Kyberturvallisuuskeskus palvelee kaikkia yhteiskunnan kriittisiä sektoreita ja tekee aktiivisesti yhteistyötä eri viranomaisten kanssa mukaan lukien turvallisuusviranomaisten, kuten puolustusvoimien kanssa. Kyberturvallisuuskeskuksella on keskeinen rooli kyberturvallisuuden kokonaistilannekuvan ylläpitämisessä ja jakamisessa ja vakavien tai laajavaikutteisten kyberuhkien ennaltaehkäisyssä.

Vähemmälle huomiolle selonteossa jää siviiliyhteiskunnan merkitys kyberturvallisuuden ja kybervarautumisen kannalta. Muun muassa eri toimialoille perustetut ISAC-tiedonvaihtoryhmien jäsenet muodostavat laajan kansallisen verkoston, jolla on tärkeä rooli kybervarautumisessa ja häiriötilanteiden hallinnassa. Nykyisessä monimutkaisessa ja verkottuneessa yhteiskunnassa eri toimijoiden välisen yhteistyön merkitys korostuu. Traficom pitää tärkeänä, että nykyisiä verkostomaisia rakenteita ja toimintamalleja, kuten tiivistä yhteistyötä kriittisten toimialojen yritysten kanssa (ISAC-verkostot), hyödynnetään jatkossakin kyberturvallisuuden ylläpitämisessä ja kehittämisessä. Kyberturvallisuuden osaamista ja resursointia tulee kasvattaa yhteiskunnan kaikilla osa-alueilla.

Selonteon mukaan puolustusjärjestelmän kybertilannekuvan parantaminen sekä kyberuhkien estäminen ja torjuminen edellyttävät tiedonvaihdon, toimivaltuuksien ja kansallisten yhteistyörakenteiden kehittämistä viranomaisten välillä. Selonteossa todetaan, että viranomaisyhteistyön kehittämistarpeet on selvitettävä ja määriteltävä muutosten perusteiksi. Myös kyberturvallisuuden kehittämisohjelmassa on asetettu toimenpiteeksi jatkokehittää poikkihallinnollisesti viranomaisten varautumista laajoihin kyberhäiriötilanteisiin. On selvää, että toimintaympäristömme on viime vuosina muuttunut ja kyberturvallisuuden verkostossa toimivilla viranomaisilla on oltava riittävät toimivaltuudet lakisääteisten tehtäviensä hoitamiseksi digitalisoituvassa yhteiskunnassa.

Traficom kiinnittää huomiota siihen, että valtioneuvoston periaatepäätöksessä tietoturvan ja tietosuojan parantamiseksi kriittisillä toimialoilla (VN/3501/2021) linjataan tarvittavat toimenpiteet sen varmistamiseksi, että viranomaisilla on edellytykset valvoa tietoturvan toteutumista ja tehdä sektorirajat ylittävää yhteistyötä. Periaatepäätös pohjautuu pääosin Liikenne- ja viestintäministeriön koordinoiman poikkihallinnollisen valmisteluryhmän loppuraporttiin, jonka mukaan viranomaisten väliselle yhteistyölle tietoturvaloukkaustilanteissa on tarve luoda yhtenäinen säädöspohja. Loppuraportin mukaan viranomaisten yhteistoiminnasta tietoturvaloukkausten ehkäisemisessä ja selvittämisessä sisältäisi säännökset yhteistyöryhmän perustamisesta tietoturvaloukkaustilanteissa, viranomaisten välisestä ennakoivasta ja tapahtumakohtaisesta keskinäisestä tiedonvaihdosta sekä välineistön, tilojen ja henkilöstön tilapäisestä luovuttamista toisen viranomaisen käyttöön.

Traficom katsoo, että selonteossa on otettu kattavasti huomioon myös avaruus- ja satelliittiteknologian merkitys sekä tarve turvata yhteiskunnan kannalta kriittisten avaruusjärjestelmien ja -palveluiden toiminta kaikissa olosuhteissa. Traficom jakaa selonteossa esitetyn käsityksen siitä, puolustusvoimien ja muiden viranomaisten toiminta on yhä enemmän riippuvaista avaruudellisista järjestelmistä. Traficomin vastuulle kuuluva häiriöiltä, häirinnältä ja harhautukselta suojattu PRS-palvelu (Public Regulated Service) pyrkii turvaamaan sijainti- ja aikatiedon saatavuuden ja luotettavuuden viranomaisille ja huoltovarmuuskriittisille toimijoille.