Ulkopoliittinen instituutti

Lausunto

08.08.2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Ulkopoliittisen instituutin lausunto Suomen kyberturvallisuusstrategiasta 2024-2035

Ulkopoliittinen instituutti kiittää tilaisuudesta antaa lausunto.

Intro

Kyberturvallisuuden poikkileikkaavuus koko yhteiskunnan ja taloustoiminnan poikkileikkaavana teemana on huomioitu raportissa ensiarvoisen hyvin. Konkreettisissa tavoitteissa on kuitenkin vielä kehittämisen varaa erityisesti kaikkein vakavimpiin uhkiin varautumisen osalta. Suomen kokonaisturvallisuusmalli tarjoaa hyvän lähtökohdan rakentaa Suomen kybertuvallisuutta, mutta erityisesti merkittävissä häiriöissä normaalitilan edellyttämisen nopeus ja tehokkuus riippuu vastuunjaon selkeydestä, ja siitä ovatko resurssit ja vastuut yhteismitallisia.

1) Vahvempi painoarvo vakavimmille uhkille ja häiriöille

Kokonaisturvallisuus tarjoaa erinomaisen perustan strategialle, mutta hajauttaminen ei sovi kaikkeen. Kokonaisturvallisuusmallin vahvuus on laajojen kokonaisuuksien koordinoimisessa ja itsenäisen toimintakyvyn tukemisessa mikä mahdollistaa tehokkaan reagoinnin poikkeuksellisen laajaan uhkakirjoon. Strategia kaipaisi vahvempaa painotusta kaikkein vakavimpiin uhkiin varautumiseen ja tehokkaaseen reagoimiseen vaadittavien kyvykkyyksien luomiseen. Tällaisia ovat esimerkiksi laajamittaisten kyberhyökkäyksien, kansainvälisten viestiliikennekatkosten, (esimerkiksi Petyan kaltaisten) massatuhoon suunniteltujen haittaohjelmien hallitsemattoman leviämisen, ja sotaan valmistelevien tai sodanaikaisten suuroperaatioiden tuhojen kaltaiset uhkat.

2) Kyberpuolustuksen roolia on syytä korostaa

Kyberpuolustuskyvykkyys ja siihen oleellisesti kuuluva uskottavan vastaiskukyvykkyyden luoma pelotevaikutus on osa kansallisen kyberturvallisuuden kokonaisuutta. Kyberpuolustuksen valmiusjoukot myös nopeuttavat normaaliaikaan palaamista vakavan hyökkäyksen jäljiltä. Kyberpuolustuksesta onkin tullut keskeinen osa uskottavaa puolustusta ja kasvavissa määrin yhteiskunnan sodanajan toimintakyvyn jatkuvuuden mahdollistaja ja siksi puolustusvoimien alaiseen kyberpuolustuskyvykkyyteen tulee strategisesti panostaa muutenkin kuin doktriinin kehittämisen avulla.

3) Viimekäden vastuita ja komentoketjuja tulee selkeyttää

Koordinaatio- ja vastuuketjujen selkeyttäminen on keskeinen osa kokonaiskyberturvallisuuden tehostamista. Erityisesti vakavien hyökkäysten ja häiriötilanteiden tapauksissa turvallisuuden ylläpitäminen ja normaalitilan palauttaminen on usein sitä helpompaa mitä nopeammin häiriöihin kyetään reagoimaan mikä puolestaan usein riippuu vastuunjaon selkeydestä, mikä puolestaan edellyttää myös viimekäden päätäntävallan keskittämistä. Kyseisen vastuun keskittäminen voidaan hyvin tehdä myös puolustusvoimien ulkopuolisen organisaation käsiin, mutta realiteetti on että puolustusvoimat on tällä hetkellä ainoa entiteetti jolla on organisatoriset (koordinaatio) ja kyberosaamiskyvykkyydet vastuun kantamiseen verrattain pienin panostuksin.

4) Teknologisen huoltovarmuuden ja kyberturvallisuuden yhteyttä tulisi selkeyttää

Tiedonsiirtojärjestelmät virastojen, toimistojen, ja tuotantolaitosten tietokoneista autoihin ja kaupoissa myytäviin laitteisiin ovat kaikki kyberturvallisuuden ja kyberpuolustuksen toimintakenttää. Niiden kunto, ajantasaisuus ja toimintaperiaatteet määrittävät lattian ja katon Suomen kyberturvallisuudelle. Tästä johtuen järjestelmien ylläpidosta ja päivittämisestä vastaavien tahojen, kuten runkoverkon infrastruktuurista vastaavien yritysten ja huoltovarmuuskeskuksen, sekä kyberturvallisuudesta ja kyberpuolustuksesta vastaavien tahojen välistä yhteistyötä olisi hyvä strategiatasolla tiivistää.

5) Strategista pääomasijoitustoimintaa tulisi kehittää

Erityisesti huipputeknologian alalla syntyy joskus kohtalokkaitakin viiveitä, kun uuden tuotteen kehittäjät joutuvat odottamaan valmistuslaitteiden kehittymistä tilanteessa, jossa valmistuslaitteiden valmistajat eivät tiedä uuden tarpeen olemassaolosta, koska siitä viestiminen riskeeraisi kriittisen tiedon vuotamisen. Valtiolla on luontainen rooli luottamuksellisen yhteistyön fasilitoimisessa, mutta myös strategisella sijoittamisella voidaan strategisesti täyttää edellä mainitun kaltaisia tuotantoketjujen aukkoja. Erityisesti voittoa tavoittelemattoman strategisen sijoitusrahoitustoiminnan kehittämistä tulisi strategisesti tavoitella, joko perustamalla uusi strateginen pääomasijoitusrahasto, tai ohjaamalla Sitraa takaisin siihen suuntaan.

6) Julkisia hankintoja tulisi hyödyntää työkaluna

Myös julkiset hankinnat ovat osa kyberturvallisuuden työkalupakkia. Esimerkiksi tilaamalla tuotteen sijasta ratkaisuja ongelmiin ja tekemällä suunnitelma hankinnan koko elinkaaren muokkaus-

(koodaus-) osaamisen varmistamiseksi hankinta itsessään tukee kyberturvallisuutta. Sen sijaan omavaraisuus- ja datan lokalisaatiopyrkimykset todennäköisesti johtavat tavoitteiden vastaiseen kehitykseen.

Markus Holmgren

Tutkija, digitaalinen suurvaltapolitiikka

markus.holmgren@fiia.fi

+358 50 473 9748

Holmgren Markus
Ulkopoliittinen instituutti