FiCom ry | Elina Ussa
17.10.2025

FiComin lausunto Valtioneuvoston selontekoon sisäisestä turvallisuudesta (VNS 6/2025 vp)

Selonteko kuvaa sisäisen turvallisuuden toimintaympäristön muutoksia hyvin, mutta digitaalista viestintäinfrastruktuuria – kuten kiinteitä ja mobiiliverkkoja, merikaapeleita, konesaleja ja kyberturvaoperaatioita – käsitellään liian yleisesti. Koska poliisi, rajaturva, hätäkeskukset, ensihoito ja teollisuus nojaavat kaikki viestintäverkkoihin, on verkkojen toimintavarmuus yhtä kuin sisäinen turvallisuus. Tätä yhteyttä ja sen merkitystä on korostettava selonteossa: **viestintäverkot muodostavat sisäisen turvallisuuden kriittisimmän kerroksen.**

1. **Merikaapelit ja varareitit:** Suomenlahden ja Ahvenanmaan riskit on mainittu, mutta tarvitaan konkreettinen ohjelma, jossa on huomioitu kartoitus, valvonta, varareitit, toipumissuunnitelmat sekä viranomaisten ja operaattoreiden välisen yhteistyön pysyvät menettelyt. Tämä on myös CER-direktiivin hengen mukaista.

2. **GNSS-häirinnän vastatoimet ja paikannuksen, navigoinnin ja ajanmäärityksen PNT-varajärjestelmät:** Häirintä on selonteonkin mukaan lisääntynyt, joten varajärjestelmä, esim. useisiin eri signaali- ja mittauslähteisiin perustuva järjestelmä ja toimivaltuudet häiriötilanteissa on kirjattava selontekoon selkeästi.

3. **Verkkohuijausten estämiseen ”vihreä kaista”:** Tarvitaan lainsäädännöllinen oikeusperusta, joka sallii viranomaisten, pankkien ja teleoperaattoreiden reaaliaikaisen tiedonvaihdon ja estotoimet huijausten torjumiseksi ilman byrokratiaa. Lainsäädännössä on huomioitava sekä reaaliaikaiset estot että verkon ohjausliikenteeseen liittyvä tiedonvaihto teleoperaattoreiden ja viranomaisten välillä.

4. **EU-sääntelyn päällekkäisyyksien purku:** EU-lainsäädännön, kuten CER-asetuksen (kriittiset toimijat), NIS2-direktiivin (kyberturvallisuus) ja DORA-asetuksen (rahoitussektorin ICT-resilienssi), toimeenpanossa on vältettävä päällekkäisiä auditointeja ja raportointivaatimuksia. Yksi yhtenäinen riskiarvio ja kontrollikehikko, jota voidaan soveltaa eri säädösten vaatimuksiin, on riittävä. Moninkertaiset auditoinnit vievät resursseja pois varsinaisesta työstä – järjestelmien varmistamisesta, valvonnasta ja korjaamisesta – ja kohdistavat ne raportointiin. EU-tason tavoitteet voidaan saavuttaa ilman kansallista ylisääntelyä.

5. **TUUTTI-hanke:** Liikenne- ja viestintäministeriön hankkeen jatkuvuus ja toimeenpano on varmistettava. TUUTTI linjaa verkkojen turvallisuuden ja varautumisen vuoteen 2037 saakka – selontekoon tarvitaan suora kytkentä hankkeen tuleviin toimenpiteisiin.

6. **Kyberasiantuntijoiden turvallisuusselvitykset:** Hitaat, maakohtaiset turvallisuusselvitykset hidastavat kyberturvallisuuden varautumista. Yritysten on voitava hyödyntää nopeasti samassa yhtiössä eri maissa jo toimivia, kertaalleen turvallisuusselvityksen läpikäyneitä kyberasiantuntijoita.

   FiCom esittää, että henkilöturvallisuusselvitykset yhdenmukaistetaan ensin Pohjoismaissa ja myöhemmin EU-tasolla, jotta kriittisen infrastruktuurin tuki voidaan varmistaa ilman hallinnollista viivettä.

7. **Sähköriippuvuus ja investointikyky:** Valtion pitäisi kompensoida teleyritysten ja konesalien investointeja varautumiseen. Digitaalisen infran oma sähköveroluokka (tai teollisuusveroluokitus) lisäisi resursseja varavoiman, hajautuksen ja resilienssin kehittämiseen.

8. **Avaruuspohjaiset palvelut ja häiriönsietokyky:** Selontekoon tulisi sisällyttää oma luku, joka käsittelee PNT- ja viestintäpalveluja, kuten satelliittiviestintää, ajastusta, varayhteyksiä ja kansallista priorisointimallia. Satelliittiviestinnän rooli viranomaisviestinnän varajärjestelmänä on määriteltävä selkeästi, ja häiriötilanteita varten on otettava käyttöön priorisointimalli, joka varmistaa yhteyksien toimivuuden kriittisissä tilanteissa.

9. **Droonihyökkäysten torjunta kriittisen infrastruktuurin ympärillä:** Infrayhtiöille on luotava selkeät virka-apukanavat ja ilmoitusmenettelyt droonihyökkäysten varalta. EU-tasolla valmistellaan yhteistä droonimuuria, joten Suomelle on tärkeää laatia oma kansallinen toimeenpanosuunnitelma, jotta se ei jää kehityksestä jälkeen.

Selonteko etenee oikeaan suuntaan – mutta digikerros tarvitsee lisää painoarvoa. Vahvistamalla kaapeleita, verkkoja, varajärjestelmiä ja julkisen sekä yksityisen sektorin yhteistyötä Suomi voi parantaa turvallisuutta kustannustehokkaasti. Turvallisuus ei synny asetuksilla, vaan toimivilla ja luotettavilla verkoilla.

Elina Ussa
toimitusjohtaja
FiCom ry