Suomen Erillisverkot Oy

Lausunto

17.10.2025

Asia: VNS/6/2025

Lausuntopyyntö: Valtioneuvoston selonteko sisäisestä turvallisuudesta

Suomen Erillisverkot Oy:n lausunto

Suomen Erillisverkot Oy kiittää mahdollisuudesta lausua Valtioneuvoston selontekoon sisäisestä turvallisuudesta.

Erillisverkot on valtion kokonaan omistama erityistehtäväyhtiö, joka tuottaa turvallisuusverkon (Tuve) verkko- ja infrastruktuuripalveluja ja kriittisen viestinnän ratkaisuita turvallisuustoimijoille. Erillisverkkojen tehtäväkenttä kattaa mm. viranomaisradioverkon (Virve) sekä kriittisen osan valtion verkkoinfrastruktuuria ja konesaleja. Näin ollen selonteon uhkat ja vaatimukset osuvat suoraan Erillisverkkojen ydintehtäviin: varmistaa toimintakyky poikkeusoloissa, suojata kyberuhilta, ylläpitää riippumatonta kriittistä viestintää ja toimia viranomaiskentän ensivasteen tukena 24/7/365.

Sisäisen turvallisuuden selonteossa todetaan: ”Suomen ulkoinen turvallisuusympäristö on muuttunut perustavanlaatuisesti ja pitkäkestoisesti. Venäjän hyökkäyssota Ukrainaan ja maailman geopoliittinen murrosvaihe heijastuvat voimakkaasti myös Suomen sisäiseen turvallisuuteen ja heikentävät sen ennustettavuutta. Suomen Nato-jäsenyys lisää Suomen ulkoista turvallisuutta. Geopoliittisesti jännittyneessä tilanteessa jäsenyys myös lisää Suomeen kohdistuvaa vihamielistä toimintaa.”

Erillisverkot kiinnittää huomiota erityisesti seikkoihin teknologian ja turvallisuuden symbioosissa sekä sisäisen ja ulkoisen turvallisuuden yhteyden ja viranomaisten yhteistoiminnan varmistamiseen muuttuvassa turvallisuuskentässä:

1. Strateginen rooli ja lainsäädäntö/hallinnointi

    - Yksi perustavanlaatuinen muutos on muutoksen nopeus. Ukrainan sota on osoittanut, että kyky innovoida ja sopeutua nopeasti ja jatkuvasti on välttämätöntä. Viranomaisten käyttämät palvelut eivät nykyisellään kykene kehittymään samassa tahdissa kuin hyökkääjän käyttämien keinojen voidaan olettaa kehittyvän.

    - Viranomaisten yhteisen turvallisuusverkon palveluiden ohjaus-, kehitys- ja hallintamalli sekä hajautunut palvelutuotanto eivät tue asiakaslähtöistä ja riittävän ketterää kehitystä. Palveluiden kehitystä ohjaa tällä hetkellä ensisijaisesti kustannustehokkuus, usein jopa saatavuuden kustannuksella.

- Lainsäädännöllinen rooli on oltava selkeä – myös poikkeusoloissa. Vastuista ja valtuuksista on oltava selkeä, lain tasoinen määrittely kriisi- ja poikkeusoloissa (esim. priorisointi, verkon sulkeminen/eristäminen, yhteydet Puolustusvoimiin ja poliisiin). Tämä vähentää epäselvyyksiä kriisitilanteessa. Tällä hetkellä tilanne on sirpaloitunut.

- Puolustuksen ja kyberturvallisuusorganisaatioiden yhteinen tilannekuva on varmistettava. Tiedonvaihto- ja toimintasuhde on varmistettava Kyberturvallisuuskeskukseen ja Puolustusvoimiin (saatavuus, tilannekuva, häiriöraportointi).

- Toiminnan kehittäminen voi vaatia roolimuutoksia tai -laajennuksia. Tämä voi tarkoittaa mahdollisesti lainsäädännön muutoksia. Tuve-lain ja muiden viranomaisvelvoitteiden tarkastelu ja yhteensovittaminen on välttämätöntä.

- Harjoitustoiminta ja yhteisharjoitusten koordinointi on tärkeää – sisältäen kyber-/häiriötilanteet.

2. Kapasiteetti ja tekniset painotukset

    - Kriittisen viestinnän suojaaminen ja redundanssi (fyysinen ja looginen) on varmistettava.

    - Kyberresilienssi ja toimitusketjun turvallisuus: viranomaisverkkojen laite- ja ohjelmistotoimitusketjun riskit on hallittava (hyväksytyt toimittajat, päivitys- ja haavoittuvuusskenaariot, jne.)

    - Quantum-ready ja salausstrategia: Tulisi laatia tiekartta siirtymisestä kvanttikestäviin salausratkaisuihin pitkällä aikavälillä.

    - Jo vuodesta 2022 kaupalliseen lentoliikenteeseen vaikuttanut satelliittipaikannuksen häirintä alkoi vaikuttaa meriliikenteeseen kevään ja kesän 2024 aikana kasvattaen onnettomuusriskiä entisestään. Satelliittipaikannuksen häirintään on olemassa vastekeinoja, kuten Galileo PRS -palvelut. Erillisverkot nimettiin PRS-palveluoperaattoriksi vuonna 2020, mutta Traficomin vetämä hanke ei ole edennyt aikataulussa. Näihin uhkiin on löydettävissä teknologisia ratkaisuja, mutta niiden hyödyntäminen edellyttää kansallista tahtotilaa ja useiden toimijoiden tiivistä yhteistyötä.

    - Avaruutta voidaan hyödyntää tilannekuvan muodostamiseen, turvallisiin viestintäyhteyksiin sekä aika-, paikka- ja navigaatiopalveluihin. Sisäisen turvallisuuden viranomaisten havainnointi- ja vastatoimintakykyä muun muassa droonien osalta tuleekin edelleen kehittää.

    - Satelliittiviestintäyhteyksien hyödyntämisessä on huomioitava Pohjois-Suomen kriittinen merkitys ja siellä käytettävissä olevat palvelut. On tärkeää, että Govsatcom-hanke, jossa toteutetaan IRISS – eurooppalainen satelliittiratkaisu – etenee siten, että palvelukyky ulottuu riittävänä myös pohjoiseen. Tämä edellyttää aktiivista vaikuttamista hankkeessa ja EU-tason päätöksenteossa laajemminkin.

    - Drooneihin liittyvän havainnointikyvyn tarve on yhteinen kaikille turvallisuuspalveluita käyttäville hallinnonaloille. Tämän vuoksi tilannekuva, jonka avulla drooniuhkiin voidaan varautua, tulee rakentaa viranomaisten yhteiseksi. Näin viranomaiset voivat jakaa yhtenäisen tilannekuvan ja koordinoida vastatoimet tehokkaasti.

    - Uhkiin vastaaminen edellyttää parempaa tilannekuvaa. Tämä voidaan muodostaa vain analytiikan avulla, mikä puolestaan vaatii merkittävästi sähköä ja jäähdytystä.

Valtion hallinnassa ei ole riittävästi kohteita, joissa yhdistyvät fyysinen suojaus ja laskentatehon vaatima jäähdytyskyvykkyys. Hajautunut toimijakenttä ei paranna tätä tilannetta.

- Tilannekuva- ja häiriöilmoituspalvelu viranomaisille — Erillisverkot voi laajentaa rooliaan tarjoten keskitetyn (mutta roolitellun) viestintäkanavan tilannekuvan jakamiseen viranomaisten välillä.

Yhteenvetona Erillisverkot toteaa:

- Sisäisen turvallisuuden ja ulkoisen turvallisuuden korrelaatio jää selonteossa hiukan taka-alalle. Sisäinen turvallisuus on käytännössä kuitenkin ulkoisen turvallisuuden “etulinja” arjessa. Kun ulkoisen turvallisuuden vaatimukset kasvavat, sisäisen turvallisuuden rahoitus ja toimivaltuudet nousevat strategiseksi puolustustekijäksi, ei pelkäksi palvelutasokysymykseksi.

- Turvallisuusympäristö on muuttunut merkittävästi: ulkoiset uhkat ja hybridivaikuttaminen näkyvät yhä vahvemmin sisäisessä turvallisuudessa. Hybridiuhat, kyberhyökkäykset, valtiollinen vakoilu, informaatiovaikuttaminen ja uhkat kriittiselle infrastruktuurille korostuvat. Tämä lisää tarvetta kriisinkestävälle ja luotettavalle viestinnälle.

- Selonteko korostaa viranomaisten resurssien vahvistamista, kykyä vastata sekä arjen häiriöihin että vakaviin uhkiin ja poikkeusoloihin. Erityistä huomiota tulee kiinnittää kriittisten palvelujen ylläpidolle ja poikkeusolojen toimintakyvylle. Näihin vaatimuksiin kykeneviä toimijoita on niukasti.

- Selonteko painottaa viranomaisten yhteistyötä sekä kyber- ja kriisivalmiuksien yhdistämistä (koko hallinnon lähestymistapa). Myös harjoittelun, ennakoinnin ja kriittisten toimitusketjujen luotettavuuden merkitys korostuu. Kriisitilanteessa toiminnan on perustuttava koeteltuihin toimintatapoihin ja välineisiin. Viranomaisilla on oltava parhaat välineet käytössä. Viranomaisverkko, turvallisuusverkko ovat näitä välineitä.

- Turvallista ja toimintavarmaa teknologiaa ei tunnisteta selonteossa sellaisenaan. Erillisverkkojen näkemyksen mukaan kehittynyt ja kaikkien turvallisuustoimijoiden käytössä oleva teknologia on sisäisen turvallisuuden elimellinen osa ja kyvykkyys. Teknologia on selonteossa toki mukana (kyber, häirintä, droonit yms.), mutta ei selkeänä yhteentoimivana ”ekosysteeminä”, joka kattaisi viranomaisviestinnän, tilannekuvan, varoitus- ja hälytysjärjestelmät, kriittisen datan jakamisen ja varautumisen.

Selonteko 2025 korostaa, että Suomi tarvitsee turvallisen ja kriisinkestävän viranomaisviestinnän. Erillisverkot on valmis vastuuseen iskunkestävänä kriittisen viestinnän kumppanina kaikkina aikoina.

Kunnioittavasti,
Timo Lehtimäki
Toimitusjohtaja
Suomen Erillisverkot Oy