Asiantuntijalausunto
Asianumero: VN/2558/2026
Päivämäärä: 3.3.2026

Hallintovaliokunta

Liikenne- ja viestintäministeriön kirjallinen lisäselvitys aiheesta: VNS 6/2025 vp Valtioneuvoston selonteko sisäisestä turvallisuudesta

Hallintovaliokunta on 25.2.2026 pyytänyt liikenne- ja viestintäministeriöltä kirjallista lisäselvitystä asiassa: VNS 6/2025 vp Valtioneuvoston selonteko sisäisestä turvallisuudesta.

Selvityspyynnön sisältö

Sisäisen turvallisuuden selonteon mukaan:

”Kyberturvallisuutta vakavasti vaarantavassa tilanteessa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa. Sääntelyn ja tehtävien hajautuminen, erilaiset toimintamallit ja soveltuvien yhteisten tietojärjestelmien puute edellyttävät yhteistoimintaa, jonka perusteet on kuvattu vuoden 2024 kyberturvallisuusstrategiassa ja yhteiskunnan turvallisuusstrategiassa. Kyberuhkien havaitsemista ja torjuntaa tulee jatkossa parantaa muun muassa varmistamalla keskeisten toimijoiden välisen tiedonvaihdon sujuvuus sekä viranomaisten riittävät toimivaltuudet.”

Selonteossa mainitaan toimenpiteinä muun muassa:

- Panostetaan kyberuhkien havaitsemiseen ja torjuntaan sekä niihin liittyvään tiedonvaihtoon turvallisuusviranomaisten välillä. Arvioidaan ja toteutetaan poliisin esitutkintavelvoitteen mahdolliset lainsäädännölliset muutostarpeet paremman tiedonsaannin mahdollistamiseksi kyberuhkien osalta. Varmistetaan lainvalvontaviranomaisten pääsy tietoon kybertoimintaympäristössä ja kehitetään toimivaltuuksia ja työvälineitä verkossa tapahtuvien rikosten torjuntaan.; ja

- Mahdollistetaan Suomen viranomaisille oikeus puuttua sellaisten ulkomailla olevien tietoverkkolaitteiden ja ohjelmistojen toimintaan, joita käytetään Suomen kansallista turvallisuutta vakavasti vaarantavaan kybervakoiluun tai -vaikuttamiseen.

Hallintovaliokunta on pyytänyt selvitystä siitä, **mitkä ovat keskeisimmät lainsäädännön muutostarpeet edellä mainittujen tavoitteiden toteuttamiseksi**. Lisäksi valiokunta on pyytänyt selvitystä siitä, **millä lainsäädännöllisillä toimenpiteillä voidaan vaikuttaa siihen, että esim. Valtorin tietomurron kaltaiset teot voidaan jatkossa nykyistä tehokkaammin estää ja teoista aiheutuvat vahingot minimoida**?

Liikenne- ja viestintäministeriö kiittää hallintovaliokuntaa lausuntopyynnöstä ja lausuu kohteliaimmin seuraavaa.

Asiantuntijalausunto; lisäselvitys

Suomi on maailman kärkeä kyberturvallisuudessa[1]. Kyberturvallisuuden yhteistoimintamalli Suomessa on hajautettu ja vastaa periaatteiltaan kokonaisturvallisuuden yhteistoimintamallia. Yhteistyön perustana ovat lakisääteiset tehtävät, yhteistyösopimukset ja yhteiskunnan turvallisuusstrategia, jonka jokaisessa strategisessa tehtävässä otetaan huomioon kyberturvallisuus. Kyberturvallisuuden yhteistoimintamallissa, jonka ylläpitämisestä liikenne- ja viestintäministeriö yhdessä muiden ministeriöiden kanssa vastaa[2], ja kyberturvallisuusdirektiivin tarkoittamassa kyberkriisitilanteessa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa. Toimivaltaiset viranomaiset, toiminnan yhteensovittaminen sekä tukeminen määritetään tarvittaessa yhteiskunnan kriisijohtamisen mallin mukaisesti. Kyberhäiriötilanteisiin varaudutaan ja niihin reagoidaan tiiviissä yhteistyössä julkisen sektorin, elinkeinoelämän ja kansalaisyhteiskunnan kanssa.

Suomella on kansainvälisellä tasollakin poikkeuksellinen kyky havainnoida, ennakoida, reagoida ja toipua erilaisista kyberpoikkeamista tai niiden uhista yhteiskunnan kaikilla tasoilla. Kansallinen kyberturvallisuus ja kyberuhkien torjunta rakentuu pitkälti viranomaisten ja yksityisen sektorin väliselle luottamukselliselle yhteistyölle. Eri toimialoilta vapaaehtoisesti saatu tieto kyberuhkista ja -poikkeamista muodostaa tärkeän perustan kansalliselle kyberturvallisuuden tilannekuvalle ja kyberhäiriötilanteiden tilanneymmärrykselle. Suomessa on myös ainutlaatuinen vapaaehtoisuuteen perustuva luottamusverkosto, jossa jaetaan tietoa kyberturvallisuudesta sekä kyberpoikkeamista ja -uhkista. Yhteistyötä yksityisen sektorin kanssa tehdään myös kansainvälisesti, ja tietoa kyberpoikkeamista saadaan myös kansainvälisten luottamusverkostojen kautta. Yhteiskunnan toimijoiden mahdollisuudet ja kyvykkyydet vastata kyberuhkiin ja -poikkeamiin on varmistettava kaikissa olosuhteissa. Yhteiskunnan häiriöttömän toimivuuden edellytyksenä on, että organisaatioilla on kyky palautua kyberhäiriöistä ja -hyökkäyksistä nopeasti ja palauttaa järjestelmät ripeästi ja turvallisesti takaisin käyttöön.

Kyberturvallisuuspoikkeamiin reagoiminen ja niiden tutkiminen perustuu tällä hetkellä selkeisiin eri viranomaisten lakisääteisiin tehtäviin ja toimivaltoihin sekä viranomaisten väliseen kattavaan yhteistyöhön, jota viime vuosien aikana on kehitetty. Yhteistoimintaa ja tiedonvaihtoa on kehitetty niin strategisella tasolla valtioneuvostotasoisen tilannekuvan ja tiedonvaihdon parantamiseksi kuin myös operatiivisella tasolla toimivaltaisten viranomaisten yhteistyön ja tiedonvaihdon varmistamiseksi erityisesti poikkeamatilanteissa. Valtioneuvoston turvallisuusjohtamisen toimintamallin kehittämishankkeessa onkin todettu, että viimevuosina tehdyt kehitystoimenpiteet kyberturvallisuuden rakenteisiin, uudessa kyberturvallisuusstrategiassa linjatut kehittämistoimenpiteet ja yhteiskunnan turvallisuusstrategian mukainen kyberturvallisuuden yhteistoimintamallin ylläpitäminen luovat jatkumon kyberturvallisuuden pitkäjänteiselle kehittämiselle osana turvallisuusjohtamisen yleistä kehittämistä[3].

[1] ITU Global cybersecurity index; Suomi sai (kahden muun maan lisäksi) 100/100 pistettä
[2] Yhteiskunnan turvallisuusstrategia, Strategiset tehtävät, tehtävä 35: Kyberturvallisuuden yhteistoimintamallin ylläpitäminen
[3] Valtioneuvoston turvallisuusjohtamisen toimintamallin kehittämishankkeen loppuraportti; Valtioneuvoston julkaisuja 2026:4

Toimivaltuudet ja tiedonvaihdon kehittäminen

Liikenne- ja viestintäministeriö pitää tärkeänä, että viranomaisilla on asianmukaiset ja tehokkaat toimivaltuudet yhteiskunnan turvallisuuteen liittyvien tehtävien hoitamiseksi ja siten sisäisen turvallisuuden selonteon toimenpiteet vievät eteenpäin kyberturvallisuuden kehitystyötä.

Liikenne- ja viestintäministeriö katsoo, että on tärkeää kehittää sääntelyä viranomaisten välisen sujuvan tiedonvaihdon ja siten toimivan yhteistyön varmistamiseksi. Julkaisussa Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa[4] eli ns. SM/PLM-hankkeessa todettiin, että ”Tiedonvaihtoon liittyvä lainsäädäntö vaatii selkeyttämistä, koska voimassa olevan lainsäädännön ei voida katsoa mahdollistavan riittävää tiedonvaihtoa useiden kyberuhkien torjunnan kannalta keskeisten viranomaisten välillä riittävän laajasti”. Liikenne- ja viestintäministeriö pitääkin tärkeänä, että kyseisen selvityksen tiedonvaihtoa koskevia ehdotuksia viedään tulevaisuudessa eteenpäin soveltuvissa hankkeissa.

Sisäisen turvallisuuden selonteossa mainittujen toimenpiteiden osalta liikenne- ja viestintäministeriö haluaa kiinnittää huomiota, että mainitut lainsäädäntöhankkeet valmistellaan sisäministeriön ja puolustusministeriön toimesta ja liikenne- ja viestintäministeriö osallistuu niihin tarpeen vaatimassa laajuudessa kyberturvallisuuden yhteistoimintamallin ja oman hallinnonalansa näkökulmasta.

Pääministeri Petteri Orpon hallitusohjelma sisältää useita kirjauksia, joiden tavoitteena on varmistaa sujuva tietojenvaihto viranomaisten välillä. Hallitusohjelman yhtenä tavoitteena on poistaa rikostorjuntaan kytkeytyviä tietojenvaihdon esteitä. Viranomaisten väliseen tietojenvaihtoon liittyvien hankkeiden edistymistä seurataan oikeusministeriön asettamassa koordinaatioryhmässä, joka tukee ministeriöiden lainsäädäntöhankkeita viranomaisten välisen tietojenvaihdon sujuvoittamiseksi rikosten ehkäisemisen tehostamiseksi.

Liikenne- ja viestintäministeriö on todennut käynnissä oleviin hankkeisiin liittyen, että esimerkiksi rikosoikeudellisiin menettelyihin tai todisteiden hankintaan liittyvien tehtävien tulisi säilyä pääasiassa lainvalvontaviranomaisten tehtävinä, eikä niitä tulisi esittää Liikenne- ja viestintävirastolle. Koska digitalisaatio on laajasti yhteiskunnan eri sektoreita koskettava megatrendi, tulisi myös kaikkien viranomaisten kyetä reagoimaan digitalisaatiokehitykseen ja päivittää osaamistaan muutoksen edellyttämällä tavalla. On tärkeää, että myös lainvalvontaviranomaisten ja rikosoikeudellisista menettelyistä vastaavien viranomaisten tulee kehittää ja päivittää digialan ja sen sääntelyn tuntemusta tehtäviään vastaavalla tavalla.

Liikenne- ja viestintäministeriö korostaa, että digitalisoituvassa maailmassa digitaalisten palveluiden ja infrastruktuurin turvallisuudella on erittäin kriittinen merkitys koko yhteiskunnan toiminnan kannalta. Nykyinen lainsäädäntö velvoittaa suomalaisia yhteisöjä huolehtimaan korkeatasoisesta tietoturvasta, jolloin palveluntarjoajien tulee ryhtyä riittäviin toimenpiteisiin esimerkiksi ulkopuolisten oikeudettoman pääsyn estämiseksi. Liikenne- ja viestintäministeriö pitääkin tärkeänä, että niin käynnissä olevissa kuin myös tulevissa lainsäädäntöhankkeissa varmistetaan, että toimivaltuudet ovat välttämättömiä, tehokkaita ja oikeasuhtaisia suhteessa tavoiteltavaan päämäärään eikä niillä aiheuteta sähköisen viestinnän tai laajemminkin digitaalisten palveluiden tietoturvan heikentymistä ja siten vaaranneta yhteiskunnan turvallisuutta.

[4] Valtioneuvoston julkaisuja 2023:1

Liikenne- ja viestintäministeriö on mm. lausunnossaan ehdotuksesta sotilastiedustelusta annetun lain muuttamisesta ja siihen liittyviksi laeiksi huomioinut, että valmistelussa tulee huomioida, että esitettävän sääntelyn ei tule vaikuttaa viestinnän välittäjien ja tietoyhteiskunnan palvelun tarjoajien normaaleihin toimenpiteisiin esimerkiksi kyberturvallisuuslain (124/2025) mukaisen riskienhallinnan ja poikkeamisen ilmoittamisen osalta. Lisäksi sähköisen viestinnän palveluista annetussa laissa (917/2014) säädetään viestinnän välittäjän velvollisuudesta huolehtia tietoturvasta (247 §). Myös kyberturvallisuuslain soveltamisalaan kuuluvilla tahoilla on velvollisuus toteuttaa riskienhallintatoimenpiteitä (9 §). Lisäksi EU:n yleinen tietosuoja-asetus (EU) 2016/679 velvoittaa toimijoita huolehtimaan tietoturvan tasosta. Palveluntarjoajien tulee toteuttaa toimia tietoturvasta huolehtimiseksi rangaistuksen uhalla, joka esimerkiksi yleisen tietosuoja-asetuksen tapauksessa tarkoittaa merkittävän taloudellisen sanktion uhkaa. Lisäksi palveluntarjoajien tulee raportoida havaitsemistaan poikkeamista viranomaisille. Liikenne- ja viestintäministeriö on lisäksi pitänyt keskeisenä, että lainsäädäntötoimenpiteillä ei aiheuteta sähköisen viestinnän tai muiden digitaalisten palveluiden tarjoajille sellaisia turvallisuuteen liittyviä riskejä, joihin palveluntarjoajat eivät kykene riittävällä tavalla vastaamaan. Esimerkiksi tietojärjestelmään asennettavalla ohjelmalla voi olla suomalaiselle tiedusteluviranomaiselle keskeinen merkitys. Liikenne- ja viestintäministeriö pitää kuitenkin tärkeänä, etteivät tällaiset toimenpiteet johda sellaiseen palvelun tietoturvan heikkenemiseen, joka mahdollistaisi myös muille ulkopuolisille toimijoille tietojärjestelmien hyväksikäytön tai luvattoman pääsyn järjestelmään.

Liikenne- ja viestintäministeriön hallinnonalan hankkeet

Kyberturvallisuuden tason parantamiseksi on liikenne- ja viestintäministeriön hallinnonalalla jo toteutettu seuraavia keskeisiä laki- ja strategiahankkeita. On tärkeää, että näiden laajojen kyberturvallisuutta edistävien hankkeiden toimeenpanoa edistetään tavoitteiden saavuttamiseksi.

Kyberturvallisuuslaki

Kyberturvallisuusdirektiivin (NIS 2 -direktiivi) tavoitteena on ollut vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa useiden yhteiskunnan toiminnan kannalta kriittisten toimialojen osalta. EU:n kyberturvallisuudirektiivi on toimeenpantu 8.4.2025 voimaan tulleella kyberturvallisuuslailla (124/2025). Soveltamisalaan kuuluvien toimijoiden tulee arvioida ja hallita riskejä, joita kohdistuu niiden käyttämien viestintäverkojen ja tietojärjestelmien turvallisuuteen. Toimijoiden on lisäksi ilmoitettava merkittävistä poikkeamista viestintäverkoissa ja tietojärjestelmissä. Kyberturvallisuuslain soveltamisala kattaa toimijoita esimerkiksi liikenne-, energia- ja terveydenhuoltoaloilla sekä digitaalisen infrastruktuurin palveluntarjoajia. Laki koskee myös esimerkiksi elintarvikealaa, eräitä tuotteita valmistavaa teollisuutta, kemianteollisuutta, jätehuoltoa ja postipalveluita.

Kyberturvallisuuslain kansallinen toimeenpano on käynnissä ja lain myötä vahvistetaan merkittävästi yhteiskunnan kyberturvallisuutta ja poikkeamiin varautumista. Yhteiskunnan kriisinkestävyyttä ja kansallista turvallisuuttta vahvistaa lisäksi 1.7.2025 voimaan astunut laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (CER-laki). Kyberturvallisuuslakia sovelletaan myös yhteisöihin, jotka määritetään tulevaisuudessa kriittisiksi toimijoiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla. Toimijoille on tärkeää antaa aikaa lakien toimeenpanoon.

Tuotteiden ja palvelujen kyberturvallisuus

EU-sääntelyllä tullaan parantamaan tuotteiden ja palveluiden kyberturvallisuutta. EU:n kyberkestävyysasetus[5] asettaa kyberturvallisuutta koskevat vähimmäisvaatimukset tuotteille ja ohjelmistoille, jotka ovat yhdistettävissä internetiin tai toiseen laitteeseen. Asetus koskee myös ohjelmistoja sekä kuluttajakäyttöön tarkoitettuja tuotteita. Asetuksen velvoitteet soveltuvat tuotteisiin, jotka on asetettu saataville markkinoilla EU:ssa.

Kyberkestävyysasetuksen arvioidaan parantavan yhteiskunnan kokonaisturvallisuutta, kun käytössä ja markkinoilla on aikaisempaa tietoturvallisempia laitteita ja ohjelmistoja. Asetuksen kansallista toimeenpanoa koskeva lakiesitys on parhaillaan eduskunnan käsittelyssä.

Suomen kyberturvallisuusstrategia 2024–2035

Suomen kyberturvallisuusstrategia on uudistettu tällä hallituskaudella ja sen tavoitteena on, että kyberturvallisuus on erottamaton osa Suomen kokonaisturvallisuutta. Kyberturvallisuusstrategian toimeenpanosuunnitelma valmistui vuoden 2024 lopulla ja siinä määritellään kehittämistoimet tavoitteiden saavuttamiseksi.

Yksi kyberturvallisuusstrategian ja sen toimeenpanosuunnitelman neljästä pilarista on *Yhteistoiminta: ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”*, joka sisältää kehittämistoimenpiteitä yhteistoiminnan ja tiedonvaihdon parantamiseksi.

Kyberturvallisuusstrategian toimenpiteitä edistämällä on mahdollista parantaa yhteiskunnan kyberturvallisuutta ja erityisesti mm. kansallista havainnointikykyä.

Kyberturvallisuuden resurssien vaikutus kyberturvallisuuteen

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on Suomen kyberturvallisuuden kivijalka; se auttaa kaikkia yhteiskunnan toimijoita huolehtimaan tietoturvastaan.

Kyberhyökkäyksiä ja -poikkeamia ennaltaehkäistään keräämällä tietoa sekä havainnoimalla uhkia ja haavoittuvuuksia, joita hyödyntämällä valtiolliset toimijat ja rikolliset tyypillisesti murtautuvat tietojärjestelmiin ja sähköisiin palveluihin. Kokonaisturvallisuuden varmistamiseksi Kyberturvallisuuskeskuksella tulee säilyttää kykyä havainnoida, torjua ja reagoida yhteiskunnan turvallisuutta uhkaaviin kyberuhkiin. Tässä oleellisessa osassa on vakavien tietoturvaloukkauksien havainnointijärjestelmä HAVARO, jonka kehittäminen nykyisiin kyberuhkiin vastaamiseksi edellyttäisi merkittävää lisäresursointia.

Kyberuhkien oikea-aikainen ja tehokas torjunta edellyttää riittävää viranomaisten resursointia. Muuttunut turvallisuustilanne, virastoihin kohdistuvat tuottavuustoimenpiteet sekä uudet lakisääteiset tehtävät edellyttävät Kyberturvallisuuskeskuksen riittävän rahoituksen varmistamista ja toiminnan turvaamista.

Liikenne- ja viestintävaliokunta on jo kyberturvallisuuslain muuttamista koskevassa mietinnössään (LiVM 12/2025 vp HE 27/2025 vp) kiinnittänyt huomiota Liikenne- ja viestintävirastolle uusista tehtävistä aiheutuviin määrärahatarpeisiin. Liikenne- ja viestintävaliokunta on tuolloin korostanut aikaisemmin lausumansa mukaisesti riittävien resurssien osoittamisen tärkeyttä kansallisen

[5] (EU) 2024/2847, Cyber Resilience Act (CRA),

kokonaisturvallisuuden kannalta keskeisten tehtävien turvaamiseksi ja katsonut, että nykyisessä taloustilanteessa viranomaistoimintojen priorisointi on tärkeää. Valiokunta on pitänyt tärkeänä, että viranomaisresurssien riittävyyttä tarkkaillaan kansallisen kokonaisturvallisuuden turvaamiseksi.

Liikenne- ja viestintävaliokunta on lisäksi useissa lausunnoissaan kantanut huolta Liikenne- ja viestintäviraston Traficomin ja Kyberturvallisuuskeskuksen riittävästä resursoinnista. Huoli on nostettu esiin mm. lausunnossa vuoden 2026 talousarvioesityksestä (LiVL 16/2025 vp — HE 99/2025) sekä lausunnossa sisäisen turvallisuuden selonteosta (LiVL 17/2025 vp VNS 6/2025 vp). Liikenne- ja viestintävaliokunta on tuonut esiin, että viraston toimintaan kohdistuvat säästötoimet vaikuttavat myös Kyberturvallisuuskeskuksen resursseihin ja kantanut huolta siitä, että taloudelliset sopeutustoimet voivat osaltaan vaikuttaa kansallisen kyberturvallisuuden tasoon.

Lausunnossaan LiVL 2/2026 vp – HE 175/2025 vp, hallituksen esityksestä eduskunnalle sähköisen todisteiden esittämismääräystä ja säilyttämismääräystä koskevaksi lainsäädännöksi, liikenne- ja viestintävaliokunta totesi Traficomin taloustilanteen osalta sen, että jo pidempään jatkuneen kehityksen seurauksena virasto on joutunut — ja joutuu jatkossakin — priorisoimaan tehtäviään voimakkaasti. Traficomin Kyberturvallisuuskeskuksen toiminnassa tämä näkyy muun muassa pidempinä vasteaikoina yhteiskunnan eri toimijoiden ja kansalaisten suuntaan.

Myös Valtiontalouden tarkastusvirasto (VTV) on suosittanut, että LVM:n ja VM:n tulisi pyrkiä varmistamaan vaaditut resurssit kyberturvallisuusstrategian toimenpiteille. Lisäksi Onnettomuustutkintakeskus (OTKES) on Helsingin kaupungin tietomurtotapauksen tutkintaselostuksessa suosittanut, että VM:n tulisi yhdessä LVM:n kanssa varmistaa riittävät kyvykkyydet julkisen hallinnon tietoturvapuutteiden havaitsemiseksi.

Liikenne- ja viestintäministeriö on esittänyt vuosien 2027–2030 julkisen talouden suunnitelmaan yhteensä noin 31 miljoonan euron lisäystä kokonaisturvallisuutta vahvistaviin kyberturvallisuustoimiin ja 7,1 miljoonaa euroa kasvua tukeviin toimiin. Esitetyillä lisäresursseilla olisi mahdollista ylläpitää kyberturvallisuuden nykyinen taso.

Lopuksi

Liikenne- ja viestintäministeriö pitää tärkeänä, että sisäisen turvallisuuden selonteon hankeita sekä tiedonvaihdon ja kyberturvallisuuden yhteistoiminnan kehittämistä jatketaan. Lisäksi on ensiarvoisen tärkeää, että toteutetaan Suomen kyberturvallisuusstrategian toimenpanosuunnitelman mukaiset toimenpiteet ja edistetään kyberturvallisuuslain sekä kyberkestävyyssetuksen kansallista toimeenpanoa varmistamalla riittävät resurssit kokonaisturvallisuutta vahvistaviin kyberturvallisuustoimiin.

Viranomaisten yhteistoiminnalla, yhteiskunnan riittävällä varautumisella, kyvykkyksien kehittämisellä ja riittävällä resursoinnilla voidaan parhaiten vaikuttaa siihen, että esim. Valtorin tietomurron kaltaiset teot voidaan jatkossa nykyistä tehokkaammin estää ja teoista aiheutuvat vahingot minimoida.