**Liikenne- ja viestintävaliokunta**
LiV@eduskunta.fi

Viite
Liikenne- ja viestintävaliokunnan asiantuntijapyyntö asiassa VNS 6/2025 vp

# Kyberturvallisuuskeskuksen asiantuntijalausunto valtioneuvoston sisäisen turvallisuuden selonteosta VNS 6/2025 vp

Liikenne- ja viestintävaliokunta on pyytänyt Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen asiantuntijalausuntoa valtioneuvoston sisäisen turvallisuuden selonteosta (VNS 6/2025 vp). Tässä lausunnossa selontekoa tarkastellaan yksinomaan Kyberturvallisuuskeskuksen tehtävien kannalta merkityksellisiltä osin ja Liikenne- ja viestintäviraston muiden tehtävien osalta erikseen myöhemmin annettavassa asiantuntijalausunnossa. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus muun ohella tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Se ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Lisäksi Kyberturvallisuuskeskus huolehtii viestintätoimialan varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin, edistää ja valvoo sähköisen viestinnän toimintavarmuutta sekä tukee toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin. (Laki Liikenne- ja viestintävirastosta 3 §). Kyberturvallisuuskeskus kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan kunnioittavasti seuraavaa:

## Tietoturvallisuus ja viestinnän luottamuksellisuus

Selonteossa esitetään toimenpiteinä ja linjauksina lainsäädännön ja toimivaltuuksien kehittämisen osalta mm. vakavan rikollisuuden ja hybridivaikuttamisen torjuminen sekä tiedustelun kehittäminen vastaamaan muuttuneen turvallisuus- ja kybertoimintaympäristön vaatimuksia (s. 20). Tähän liittyy mm. tiedustelulainsäädännön toimivaltuuksien kehittäminen, ja rikostiedustelusääntelyn uudistaminen. Kyberturvallisuuskeskus kiinnittää huomiota siihen, että lainvalvontaviranomaisten tiedonsaantioikeuksia laajentavia lainsäädäntötoimia tehdään lisääntyvällä tahdilla, jolloin kokonaisuutena tarkasteltaessa nämä muutokset saattavat vaikuttaa hyvinkin merkittävästi yksityisyyteen ja viestinnän luottamuksellisuuteen. Kyberturvallisuuskeskus katsoo, että laajennettaessa viranomaisten tiedonsaantioikeuksia, erityisesti telepakkokeinojen ja muiden salaisten pakkokeinojen avulla, on punnittava tarkasti muutosten perusoikeusvaikutuksia ottaen huomioon myös muiden tiedonsaantioikeuksien kumulatiivinen vaikutus[1].

[1] Tämän lisäksi on otettava huomioon unionin oikeudesta seuraavat rajoitteet säilytysvelvollisuuden piiriin kuuluvien välitystietojen käytölle. Esimerkiksi kansallisen turvallisuuden varmistamiseksi voidaan oikeuttaa laajempi välitystietojen säilytysvelvollisuus, mutta näitä tietoja ei voida välttämättä käyttää

Kyberturvallisuuskeskus painottaa sen tärkeyttä, että toimenpiteillä, joilla pyritään varmistamaan lainvalvontaviranomaisten pääsy tietoon kybertoimintaympäristössä, ei vaikuttaisi haitallisesti yleiseen tietoturvallisuuden tasoon. On keskeistä, ettei toimenpiteillä heikennetä päätelaitteiden tai viestintä- ja tietojärjestelmien turvallisuutta eikä rajoiteta toimivien ja tehokkaiden salausratkaisujen laajamittaista käyttöä. Salausta tai muita tietoturvaratkaisuja ei voida heikentää vain kotimaan turvallisuusviranomaisten tarpeita varten. Salauksen heikentäminen huonontaa tietojärjestelmien turvallisuutta yleisesti ja mahdollistaa siten myös pahantahtoisille toimijoille aiempaa helpommin erilaiset väärinkäytökset. Esimerkiksi erilaiset takaportit voisivat olla myös ulkopuolisten valtiollisten toimijoiden ja rikollisten tahojen hyödynnettävissä. Nämä vaikutukset olisivat kielteisiä myös sisäisen turvallisuuden kannalta. Tietoturvan tason heikentämisellä on myös suoria vaikutuksia luottamuksellisen viestin suojan ja muiden perusoikeuksien toteutumiseen. Kasvanut alttius tietomurroille myös heikentäisi yritysten mahdollisuuksia suojata liikesalaisuuksia.

## Kyberturvallisuuden tilannekuva ja viranomaisten roolit

Kyberturvallisuuskeskuksen yksi keskeisimpiä tehtäviä on tuottaa kansallista kyberturvallisuuden tilannekuvaa. Tilannekuvaa muodostetaan niin kansallisista kuin kansainvälisistä verkostoista tulevalla tiedolla. Tieto voi olla yksittäinen tekninen uhkatieto tai muu ei-tekninen tieto, joka on oleellinen tilannekuvan muodostamiselle. Kybermaailman poikkeamat tapahtuvat harvoin omassa tyhjiössä vaan ne linkittyvät yhä enenevissä määrin reaalimaailman tapahtumiin ja trendeihin. Tästä esimerkkinä on valtiollisten toimijoiden ja rikollisten toimijoiden rajapinnan hämärtyminen, sillä molemmat toimijat käyttävät samoja menetelmiä, mutta niiden tavoitteet voivat erota toisistaan.

Kyberturvallisuuskeskus on rakentanut yli 20 vuoden ajan luottamuksellisia suhteita yksityiseen sektoriin ja huoltovarmuuskriittisiin organisaatioihin, jotka omistavat vähintään 90% Suomen verkkoinfrastruktuurista. Suomen kriittisen infrastruktuurin organisaatiot ovat se eturintama, johon uhkat kohdistuvat. Kyberturvallisuuskeskuksen rooli kansallisen tilannekuvan muodostamisessa on erittäin tärkeä, koska Kyberturvallisuuskeskuksella on muihin turvallisuusviranomaisiin verrattuna suorempi ja välittömämpi yhteys näihin toimijoihin.

Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, jolla on laaja kansallinen ja kansainvälinen verkosto. Nämä verkostot jakavat tilannekuvatietoa tietoturvapoikkeamista ja siten Kyberturvallisuuskeskus saa usein ensitiedon myös vakavammista tietoturvapoikkeamista, joiden taustalla on todennäköisesti valtiollista toimintaa. Tätä tietoa jaetaan muille turvallisuusviranomaisille, joilla on toimivalta asian selvittämisessä. Kyberturvallisuuskeskuksen rooli ensitiedon vastaanottajana ja avun tarjoajana on keskeinen, kun puhutaan kyberturvallisuudesta ja sen tilannekuvasta.

---

vakavankaan rikollisuuden torjuntaan (ks. esim. asia C-140/20, *Commissioner of An Garda Síochána*, tuomio 5.4.2022, EU:C:2022:258, kohdat 59-64 viittauksineen).

Selonteon Toimenpiteet ja linjaukset -osiossa todetaan, että yhtenä kehityskohteena panostetaan kyberuhkien havaitsemiseen ja torjuntaan sekä niihin liittyvään tiedonvaihtoon turvallisuusviranomaisten välillä. Kyberturvallisuuskeskuksen rooli yhtenä kansallisena turvallisuusviranomaisena olisi syytä tunnistaa, kun kyse on kyberuhkien havaitsemisesta ja torjunnasta. Kirjausta itsessään pidetään kannatettavana.

Selonteossa mainitaan Venäjän ja Kiinan olevan Suomelle merkittävimpiä vakoilun ja valtiollisen vaikuttamisen uhkia, ja kerrotaan molempien toteuttavan Suomeen kohdistuvaa tiedonhankintaansa kyberympäristössä. Silti raportissa nostetaan ainoastaan Venäjä-tuntemuksen kehittäminen, ylläpito ja tähän liittyvä riittävä resursointi erikseen esiin. Kyberturvallisuuskeskus katsoo, että myös Kiina-tuntemuksen kehittäminen, ylläpito ja siihen liittyvä resursointi voisi olla syytä nostaa selvemmin esiin.

Kyberturvallisuuskeskus pitää tarkoituksenmukaisena, että jatkossa Suomen viranomaisilla olisi oikeus puuttua sellaisten ulkomailla olevien tietoverkkolaitteiden ja ohjelmistojen toimintaan, joita käytetään Suomen kansallista turvallisuutta vakavasti vaarantavaan kybervakoiluun tai -vaikuttamiseen.

Osana toimenpiteitä ja linjauksia olisi tärkeää myös varmistaa resurssit toiminnalle, jotta työhön osallistuvat viranomaiset voivat torjua vakavaa rikollisuutta ja hybridivaikuttamista sekä kehittää tiedustelua vastaamaan muuttuneen turvallisuus- ja kyberympäristön vaatimuksia.

## Suomelle kriittisen infrastruktuurin suojaaminen

Selonteossa todetaan, että Suomenlahdella viime vuosina tapahtuneet kriittisen infrastruktuurin vauriot voivat vaikuttaa yhteiskunnan elintärkeiden toimintojen toimivuuteen (s. 16). Viestintäverkkojen- ja palvelujen toimivuus on välttämätöntä yhteiskunnan elintärkeille toiminnoille. Niin viranomaiset, kriittiset yksityisen sektorin toimijat kuin myös tavalliset kansalaiset hyödyntävät jokapäiväisessä toiminnassaan digitaalisia palveluita, joiden jatkuvuus on kyettävä mahdollisimman hyvin varmistamaan normaaliolojen häiriötilanteissa sekä valmiuslain mukaisissa poikkeusoloissa. Yleisten viestintäverkkojen ja -palvelujen eli teletoiminnan toimintavarmuudesta ja varautumisesta huolehtiminen on ollut osa toimijoita koskevaa lainsäädäntöä ja viranomaisohjausta ja -valvontaa jo 1990-luvulta lähtien. Tällä ja Kyberturvallisuuskeskuksen jatkuvasti tekemällä teleyritysyhteistyöllä on ollut merkittävä vaikutus siihen, että mm. merikaapelikatkoksista on ollut tuskin lainkaan näkyviä vaikutuksia teleyritysten asiakkaille. Vaikka viestintäverkkojen toimintavarmuus Suomessa on korkealla tasolla, voidaan vastaavanlaisten vaurioiden mahdollisia vaikutuksia vähentää kehittämällä edelleen kansainvälisten yhteyksien varmistuksia, eli esimerkiksi lisäämällä maantieteellisesti hajautettuja maa- ja merikaapeliyhteyksiä.

Kyberturvallisuuskeskus pitää kannatettavana panostusta kriittisen infrastruktuurin kohteiden suojaamiseen CER-direktiivin toimeenpanon edellyttämällä tasolla ja sitä, että arvioidaan merialueilla olevan kriittisen

infrastruktuurin ylläpidon ja suojaamisen haasteet sekä näiden edellyttämä lainsäädännöllinen, valvonnallinen ja teknologinen vaste (s. 22). Merikaapeleiden valvonnallisen ja teknologisen vasteen osalta kansallinen ja kansainvälinen yhteystyö on tärkeää. On myös keskeistä, että kansallisten viranomaisten vastuut ovat selkeät.

Kuten selonteossa todetaan, kriittisen infrastruktuurin suojaaminen edellyttää ajantasaista lainsäädäntöä (s. 17). Selonteossa mainitun CER-direktiivin tavoitteena on yhteiskunnan kriittisten palvelujen häiriönsietokyvyn parantaminen ja direktiivin kansallisella toimeenpanolla pyritään mm. kriittisten palvelujen häiriönsietokyvyn parantamiseen. Lisäksi NIS 2 -direktiivin tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa useiden yhteiskunnan toiminnan kannalta kriittisten toimialojen osalta. Kansallisesti NIS 2 -direktiivi on pantu täytäntöön 8.4.2025 voimaan tulleella Kyberturvallisuuslailla, jossa mm. osoitetaan yhteiskunnan kriittisille toimialoille kyberturvallisuutta vahvistavia riskienhallintavelvoitteita ja raportointivelvoite merkittävistä poikkeamista.

Yleiseen teletoimintaan käytettävien merikaapelien suojaamista koskevista vaatimuksista säädetään sähköisen viestinnän palveluista annetussa laissa (viestintäpalvelulaki), jonka mukaan yleiset viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä mm. siten, että ne kestävät normaalit odotettavissa olevat ilmastolliset, mekaaniset ja sähkömagneettiset ja muut ulkoiset häiriöt ja niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt voidaan havaita. Lisäksi Liikenne- ja viestintävirasto on antanut useita määräyksiä teletoiminnan tietoturvaan ja varmistamiseen liittyen sekä teleyrityksille suosituksen varautumisesta.

Lisäksi Kyberturvallisuuskeskus pitää kannatettavana vaaratiedottamisen ja väestön varoittamisjärjestelmän kehittämistä vastaamaan turvallisuusympäristön muutosta ja järjestelmien toimivuuden varmistamista myös poikkeusoloissa (s. 24). Kyberturvallisuuskeskus valvoo viestintäpalvelulaissa säädettyjä vaaratiedotteiden välittämistä koskevia velvollisuuksia, joiden mukaan mm. laissa vaaratiedotteiden välittämiseen velvoitettujen on huolehdittava siitä, että vaaratiedote voidaan välittää myös normaaliolojen häiriötilanteissa ja valmiuslaissa tarkoitetuissa poikkeusoloissa. Vaaratiedottaminen perustuu monikanavaisuuteen, ja matkaviestinverkkojen kautta välitettävät tiedotteet ovat nyky-yhteiskunnassa yhä tärkeämpiä. Myös satelliittipohjainen järjestelmä voisi olla tulevaisuudessa yksi ratkaisu vaaratiedotteiden välittämiseen.

Jutta Sarvilinna
lakimies

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus