Verkkoturvallisuuden neuvottelukunnan suositus
Asianumero: VN/15573/2022
Päivämäärä: 16.6.2025

Verkkoturvallisuuden neuvottelukunnan suositus viestintäverkkojen kriittisten osien määräyksestä

Tausta

EU:ssa laadittiin vuonna 2019 yhteinen riskiarviointi 5G-verkkojen turvallisuudesta. Riskiarvioinnin pohjalta EU:ssa laadittiin yhteiset suositukset 5G-verkkojen turvallisuuden vahvistamiseksi jäsenvaltioissa. Suositukset jakaantuvat strategisiin ja teknisiin suosituksiin. Strategisiin suosituksiin lukeutuu viranomaisten toimivaltuuksien vahvistaminen, monitoimittajastrategian soveltaminen sekä verkon kriittisten osien tunnistaminen. Teknisiin suosituksiin lukeutuu yleiset tietoturvavaatimukset sekä EU-sertifiointikehykset.

Viestintäverkkojen turvallisuudesta säännellään Suomessa tiukasti. Sähköisen viestinnän palveluista annettu laki sisältää säännöksiä viestintäverkkojen turvallisuudesta suunnittelusta ylläpitoon. Lisäksi sähköisen viestinnän palveluista annetun lain 244 a §:ssä säädetään viestintäverkon kriittisissä osissa käytettävistä laitteista. Pykälän 1 momentin mukaan viestintäverkkolaitetta ei saa käyttää yleisen viestintäverkon kriittisissä osissa, jos on painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta siten, että käytöllä mahdollistettaisiin ulkomainen tiedustelutoiminta tai toiminta, jolla häirittäisiin, lamautettaisiin tai muuten vahingollisella tavalla vaikutettaisiin Suomen tärkeisiin etuihin, yhteiskunnan perustoimintoihin tai kansanvaltaiseen yhteiskuntajärjestykseen. Viestintäverkon kriittisenä osana pidetään momentin mukaan verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä.

Viestintäverkon kriittisenä osana pidetään momentin mukaan verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Lain 244 a §:n 6 momentin mukaan Liikenne- ja viestintävirasto antaa tarkempia määräyksiä viestintäverkkojen, erityisesti niiden kriittisten osien, teknisestä määrittelystä 244 b §:ssä tarkoitetun verkkoturvallisuuden neuvottelukunnan suositukset huomioiden.

Sähköisen viestinnän palveluista annetun lain 244 b §:ssä säädetään verkkoturvallisuuden neuvottelukunnasta. Neuvottelukunnan tehtävänä on toimia toimivaltaisten viranomaisten päätöksenteon tukena. Se seuraa viestintäverkkojen ja -teknologian kehittymistä ja verkkoturvallisuutta koskevan lainsäädännön soveltamiskäytäntöä. Neuvottelukunta käsittelee ja esittää suosituksia viestintäverkkojen ja -teknologian kehittymisestä ja viestintäverkkojen kriittisten osien määrittelystä, kansallisen turvallisuuden edistämisestä ja suojaamisesta viestintäverkoissa, erityisesti niiden kriittisissä osissa, toimenpiteistä niiden riskien torjumiseksi, jotka vaikuttavat viestintäverkkojen turvallisuuteen ja kansallisen turvallisuuden toteutumiseen, sekä lainsäädännön muuttamiseksi verkkoturvallisuuden parantamiseksi. Neuvottelukunnassa ovat edustettuina liikenne- ja viestintäministeriön, sisäasiainhallinnon, puolustushallinnon, ulkoasiainhallinnon, työ- ja elinkeinoministeriön ja muiden viestintäverkkojen turvallisuuden kannalta keskeisten hallinnonalojen edustajat sekä keskeisten teleyritysten edustajat ja edunvalvojat.

Liikenne- ja viestintävirasto antaa erilaisia teknisiä määräyksiä viestintäverkkojen osalta. Liikenne- ja viestintäviraston 20.5.2021 antamassa määräyksessä määritellään teknisesti viestintäverkkojen kriittiset osat. Määräystä sovelletaan yleiseen teletoimintaan sekä sähköisen viestinnän palveluista annetun lain 244 a §:n 2 momentissa tarkoitettuihin yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden yleiseen viestintäverkkoon liitettyyn erillisverkkoon.

Liikenne- ja viestintävirasto Traficom on asettanut 23.1.2025 viestintäverkon kriittisten osien määräystä koskevan hankkeen, jonka tavoitteena on ajantasaistaa 20.5.2021 voimaan tullut määräys. Hankkeessa tarkastellaan viestintäverkkojen kriittisten osien rajauksia viestintäteknologioiden kehittymisen ja erityisesti matkaviestinverkkojen 5G-verkkoteknologian kehittyminen, huomioiden sen keskeinen yhteiskunnallinen rooli.

Hankepäätöksen mukaisesti määräyksen päivittäminen edistää hallitusohjelman tavoitetta kyberturvallisuuden vahvistamisesta parantamalla viestintäverkkojen ja -palvelujen tietoturvaa muuttuneessa turvallisuusympäristössä. Määräyksellä edistetään kansallista turvallisuutta ja viestintäverkkojen tietoturvaa. Määräys täsmentää niitä viestintäverkon osia, joihin sähköisen viestinnän palveluista annetun lain 244 a § mukaiset toimenpiteet (verkkolaitteen poistaminen verkosta) voisivat kohdistua. Päivitetty määräys on tarkoitus julkaista syksyllä 2025.

Viestintäverkkoteknologian kehityksen ja toimintaympäristön muutoksen vaikutukset viestintäverkkojen turvallisuuteen

Viestintäverkot ovat erottamaton osa yhteiskunnan kriittistä infrastruktuuria. Viestintäverkkojen teknologinen kehitys ja uudet toiminnallisuudet muuttavat viestintäverkot yhä monimutkaisemmaksi kokonaisuudeksi. 5G-verkot mahdollistavat laajasti yhteiskunnan eri toimintojen tehostamisen ja kehittämisen. Viestintäverkoilla on samalla entistä keskeisempi merkitys yhteiskunnan resilienssin ja kansallisen turvallisuuden kannalta, mikä edellyttää riskienhallintaa, varautumista ja laaja-alaista yhteistyötä. Viestintäverkon osien kriittisyyttä ja kriittisyyttä koskevia muutoksia on syytä tarkastella monimutkaistuvan viestintäteknologisen kehityksen ympäristössä. Digitalisoitunut yhteiskunta, kyberuhkien lisääntyminen sekä muuttuva geopoliittinen tilanne ovat korostaneet tarvetta tarkastella viestintäverkkoteknologian turvallista kehitystä entistä tiiviimmin. Suomen uudistetussa kyberturvallisuusstrategiassa kuvataan kattavasti toimintaympäristön muutosta.

Viestintäverkkojen turvallisuuteen liittyvä toimintaympäristö on muuttunut olennaisesti. EU:ssa on viime vuosina annettu lukuisia kyberturvallisuutta vahvistavia säädöksiä, kuten NIS2-direktiivi ja kyberkestävyyssäädös, jotka sisältävät lukuisia velvoitteita kyberturvallisuuden vahvistamiseksi. Näiden ohella komissiossa kiinnitetään myös entistä tarkempaa huomiota 5G-verkkojen turvallisuuteen. Komissio julkaisi vuonna 2023 5G-verkkojen turvallisuutta koskevan tiedonannon, jonka mukaan jäsenvaltioiden toimenpiteet 5G-verkkojen kriittisten osien suojaamiseksi tulisi ulottaa myös radioliityntäverkkoon (RAN, Radio Access Network). Radioliityntäverkko on tunnistettu kriittiseksi lukuisissa jäsenvaltioissa, kuten Ruotsissa, Liettuassa, Portugalissa, Espanjassa ja Kroatiassa. Osassa jäsenvaltioista ei puolestaan ole saatavilla luotettavaa julkista tietoa radioliityntäverkon tunnistamisesta kriittiseksi. Jäsenvaltioilla on erilaisia lähestymistapoja verkon kriittisten osien määrittelyssä.

Samaan aikaan geopoliittinen toimintaympäristö muuttuu entistä nopeammin. Toimintaympäristön muutos EU:ssa ja kansainvälisesti lisää viestintäverkkojen turvallisuuden ja toimintavarmuuden merkitystä kansallisesti. Verkkoturvallisuuden neuvottelukunta on osaltaan kiinnittänyt työssään tähän huomiota. Turvallisuusnäkökulmat tulee huomioida seuraavien verkkosukupolvien kehitystyössä ja tulevaisuudessa tehtävissä hankinnoissa alusta alkaen. Suomessa tähän varaudutaan jo etupainotteisesti, kun

verkkoturvallisuuden neuvottelukunta on arvioinut 6G-verkkoturvallisuuskysymyksiä yhteistyössä 6G-työryhmän kanssa. Tunnistetut turvallisuusnäkökohdat huomioidaan tulevassa 6G-tiekartassa.

Turvallisuusympäristön muutos edellyttää monipuolisia toimenpiteitä, niin strategisia, operatiivisia, organisatorisia kuin teknisiä toimia. Toimintaympäristön muutosten myötä viestintäverkkojen turvallisuuden varmistaminen edellyttää ennakoivaa varautumista, pitkäjänteistä kehitystyötä ja yhteistyötä yli sektorirajojen. Suomen on tärkeää säilyttää asemansa edelläkävijänä turvallisten viestintäverkkojen kehityksessä ja sektorit ylittävässä yhteistyössä, erityisesti siirryttäessä kohti 6G-aikakautta. Viestintäverkkoteknologian kehitys etenee nopeasti, ja siirtymä seuraaviin verkkosukupolviin edellyttää ennakoivaa varautumista sekä uusien teknologisten ratkaisujen ja turvallisuusnäkökulmien huomioon ottamista jo nyt. Pitkän aikavälin tarkastelun ohella huomiota tulee kiinnittää 5G-verkkojen nykyiseen toteutukseen ja kehitykseen. Ennakoivalla varautumisella ja turvallisuusnäkökulmien päivittämisellä on myös keskeinen vaikutus yleisen oikeusvarmuuden kannalta.

Verkkoturvallisuuden neuvottelukunnan suositus

Edellä esitetyn pohjalta neuvottelukunta katsoo, että viestintäverkon osien kriittisyyden arvioinnissa on tarpeen huomioida ennakoivasti viestintäverkkojen merkityksen kasvu koko yhteiskunnalle, viestintäverkkoteknologioiden kehityssuunta sekä toimintaympäristön muutokset. Arvioinnissa tulisi lisäksi kiinnittää huomiota EU:n linjauksiin ja suosituksiin sekä yleiseen kansainväliseen kehitykseen.

Viestintäverkon kriittisten osien määräystä koskevassa hankkeessa ja päivitettävässä määräyksessä on olennaista huomioida edellä mainitut seikat. Voimassa olevaan, 20.5.2021 julkaistuun määräykseen eivät sisälly tietyt 5G-verkon osat, kuten esimerkiksi radioliityntäverkko. Päivitystyössä tulisi arvioida tarvetta laajentaa verkon kriittisten osien määräystä soveltuvin osin myös sellaisiin 5G-verkon osiin, joita voimassa oleva määräys ei kata. Tätä laajentamista puoltaisivat yleinen viestintäverkkoteknologioiden kehitys, viestintäverkkojen merkityksen kasvu yhteiskunnan eri toiminnoille sekä kansallisen turvallisuuden varmistaminen kehittyneimmissä viestintäverkoissa.

Neuvottelukunta pitää tärkeänä, että viestintäverkkojen kriittisyyden arvioinnissa huomioidaan viestintäverkkoihin tehtävien investointien ennakoitavuus ja oikeusvarmuus sekä kansainväliset standardit, joihin viestintäverkkojen rakentaminen perustuu. Tämän vuoksi päivitystyössä on suositeltavaa arvioida mahdollisten siirtymäaikojen tarvetta, kuitenkin elinkaarien tarkastelu ja määräyksen tavoitteet huomioiden.