Lausuntoyhteenveto – määräys viestintäverkon kriittisistä osista

1 Yleistä

Luonnos Liikenne- ja viestintävirasto Traficomin määräykseksi viestintäverkon kriittisistä osista sekä luonnos määräyksen perustelumuistioksi olivat lausuttavana lausuntopalvelussa 3.3.–23.3.2021. Traficom vastaanotti asiassa 12 lausuntoa. Lausunnon antoivat DNA Oyj, Elisa Oyj, Finnet-liitto ry, Huawei Technologies Oy (Finland) Co. Ltd, Nokia Oyj, puolustusministeriö, sisäministeriö, Suomen Erillisverkot Oy, Telia Finland Oyj, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, ulkoministeriö sekä valtiovarainministeriö. Lausunnot ovat saatavilla lausuntopalvelu.fi:ssä.

Tässä yhteenvedossa kuvataan aihealueittain keskeisimmät lausunnoissa esitetyt huomiot sekä niiden vaikutukset määräyksen jatkovalmisteluun.

2 Viestintäverkon kriittisten osien määrittely ja dokumentointi

Määräysluonnoksen mukainen teleyrityksen ja erillisverkkotoimijan velvollisuus tunnistaa viestintäverkkonsa kriittiset osat ja niissä käyttämänsä viestintäverkon tai -palvelun komponentit sekä laatia ja ylläpitää niitä koskeva ajantasainen dokumentaatio sai lausunnoissa laajasti kannatusta. Sitä pidettiin perusteltuna ja toimivana tapana viestintäverkkolaitekannan arvioinnissa ja osaltaan tietoisuuden lisäämisessä verkon turvaamisesta. Sen ei nähty aiheuttavan merkittävää hallinnollista taakkaa teleyrityksille ja erillisverkkotoimijoille. Myös dokumentaation laatimiselle suunniteltua kuuden kuukauden määräaikaa määräyksen voimaantulosta pidettiin kohtuullisena ja kannatettavana.

Erityisesti teleyritysten sekä näiden edunvalvontajärjestöjen lausunnoissa pidettiin kuitenkin tarpeellisena, että Traficom valvovana viranomaisena antaa ohjeistusta ja mallipohjan dokumentaation laadintaan. Ohjeistuksen ja mallipohja katsottiin sujuvoittavan ja yhdenmukaistavan dokumentaation laadintaa ja hallintaa, mikä on omiaan vähentämään velvoitteesta toimijoille aiheutuvaa hallinnollista taakkaa. Dokumentaation yhdenmukaistamisella nähtiin myös olevan viranomaisvalvontaa helpottava vaikutus. FiCom teki vielä 13.4.2021 yksityiskohtaisemman ehdotuksen dokumentoinnin toteutustavaksi, jossa mainittiin myös mahdollinen perustelujen kirjaaminen kriittisiksi arvioiduille verkon osille. – Traficom tulee järjestämään teleyrityksille ja erillisverkkotoimijoille työpajan dokumentaatiota koskevasta velvoitteesta, ja voi sen perusteella antaa tarkempia ohjeita dokumentaation laatimisesta.

Traficom on täsmentänyt määräyksen yleistä dokumentointivelvoitetta niin, että se vastaa paremmin määräyksen erityisiä dokumentointivelvoitteita. Tämän johdosta dokumentoitava on myös perusteet sille, miksi teleyritys tai erillisverkkotoimija on arvioinut tietyn verkon osan kriittiseksi. Traficom katsoo, että tarkennus ei lisää määräyksen yritysvaikutuksia perustelumuistiossa arvioituun nähden, koska operaattori tekisi tämän arvioinnin joka tapauksessa kriittisten osien tunnistamisvelvoitteensa täyttämiseksi.

Sisäministeriö esitti lausunnossaan, että määräyksessä tulisi asettaa teleyrityksille ja erillisverkkotoimijoille velvoite toimittaa valvovalle viranomaiselle ilman aiheetonta viivettä tiedot tulevista muutoksista viestintäverkon kriittisissä osissa. Traficom toteaa, että asiaa on käsitelty perustelumuistion yleisperustelujen kohdassa 5.1. Traficomilla ei ole toimivaltaa asettaa määräyksellä uusia tiedon luovuttamista koskevia velvoitteita tai tiedonsaantioikeuksia, joten asiassa on sovellettava olemassa olevia säännöksiä. Näitä ovat mm. sähköisen viestinnän palveluista annetun

lain (917/2014, SVPL) 315 §, 320 §, 244 a §:n 5 mom. ja 244 b §:n 3 mom. Voimassa olevien säännösten mukaan Traficomilla on pyynnöstä oikeus saada tehtäviensä hoitamiseksi tarvittavia tietoja valvomiltaan toimijoilta. Uusia tiedon luovuttamista tai saamista koskevia oikeuksia tai velvollisuuksia voidaan asettaa vain eduskuntalailla.

3 Tukiasemaohjaimet ja tärkeysluokittelu

Nokia katsoi lausunnossaan, että määräyksen kohdan 4 luettelon kohdan 1 viittaus määräykseen 54 jättää epäselväksi, onko määräyksen 54 mukaan tukiasemat aina luettu pois tärkeysluokista 1 ja 2 (määräyksen 54 mukainen tärkeysluokka 5) ja tukiasemaohjaimet aina luettu mukaan tärkeysluokkaan 2. Traficom toteaa, että nyt annettavan määräyksen kyseisen virkkeen nojalla viestintäverkon kriittisinä osina pidetään, kuten perustelumuistiostakin ilmenee, tärkeysluokkiin 1 ja 2 kuuluvia komponentteja vain silloin, kun ne kuuluvat niihin käyttäjämääränsä tai vaikutusalueensa perusteella. Tämä tarkoittaa, että esimerkiksi tukiasemaohjainta ei katsota viestintäverkon kriittiseksi osaksi määräyksen 54 mukaisen tärkeysluokittelun nojalla, jos se käyttäjämäärän ja vaikutusalueen perusteella jää kuitenkin tärkeysluokalle 2 määritettyjen rajojen alle. Tämä on siis poikkeus siihen, että tukiasemaohjain on määräyksen 54 soveltamisen kannalta määritelty aina vähintään tärkeysluokkaan 2 kuuluvaksi. Traficom kuitenkin korostaa, että vaikka viestintäverkkolaite ei kuuluisikaan tärkeysluokkiin 1 tai 2, se voi kuitenkin olla viestintäverkon kriittinen osa muulla määräyksen mukaisella perusteella. Luettelon 1 kohdan luetelmat kuvaavat tapauksia, joissa ainakin on kyseessä loppukäyttäjien liikenteen reititykseen ja muuhun kontrollointiin tai ohjaamiseen viestintäverkossa liittyvä viestintäverkon kriittinen osa.

Nokia pohti lausunnossaan määräyksen kohtaa 4 koskien myös, käsitelläänkö kriittisten osien määritelmässä käyttäjämäärän tai vaikutusalueen arvioinnissa vain yksittäisiä toimintoja ja toimenpiteitä (esim. yksittäisiä laitteita) vai huomioidaanko toimintona esim. joukko samanlaisia potentiaalisesti yhdessä toimivia laitteita. – Traficom toteaa, että tulkinta-apuna voidaan käyttää määräyksen 54 B/2014 M perustelumuistion kohtaa 3.7. jossa on todettu muun muassa, että "Mikäli jokin toiminto (esimerkiksi nimipalvelinohjelmisto) on hajautettu usealle eri laitteelle, katsotaan kukin laite omaksi komponentikseen." Tarvittaessa Traficom voi antaa tulkintaohjeita teleyrityksen viestintäverkon tai -palvelun komponenttien tärkeysluokittelusta konkreettisten tulkintapyyntöjen pohjalta.

DNA, FiCom ja Huawei kritisoivat lausunnoissaan sitä, että radioverkko- ja tukiasemaohjaimia määriteltäisiin kriittiseksi viittauksella määräyksen 54 mukaisiin tärkeysluokkiin. Ne katsoivat, että määräystä ei tulisi soveltaa 2G- ja 3G-verkoissa käytettäviin tukiasema- ja radioverkko-ohjaimiin (BSC ja RNC). DNA ja FiCom esittivät, että viestintäverkon kriittisten osien määräyksen kohdan 4 luettelon kohdan 1 luetelmaa i tulisi täsmentää siten, että tärkeysluokittelun perusteella ei katsottaisi viestintäverkon kriittisiksi osiksi 2G- ja 3G- matkaviestinverkon laitteita, kuten tukiasemaohjaimia. FiCom esitti, että tukiasemaohjaimiin sovellettaisiin yksinomaan SVPL 244 a §:n mukaista verkon kriittisten osien määritelmää eikä niitä määriteltäisi kategorisesti kriittisiksi määräyksen 54 mukaan, jolloin tukiasemaohjaimen kriittisyyden määritelmä olisi teleyrityksen itsensä harkittavissa. FiCom esitti 13.4.2021 vielä lisäperusteeksi ehdotukselleen, että mobiiliverkkojen häiriötilanteissa hätäpuhelut ohjautuvat toiseen verkkoon, eikä 2G- ja 3G-verkkojen häiriötilanteissa yhden verkon toimimattomuus uhkaa ihmisten henkeä tai terveyttä. FiCom huomautti, että pelastus-, turvallisuus- ja puolustusviranomaisilla on nykyisin oma erillinen viranomaisverkkonsa, johon ei sovelleta määräystä 54.

Traficom toteaa, että määräyksen kohta 4 on laadittu teknologianeutraaliin muotoon. Traficom katsoo, että 2G- ja 3G-verkoissa käytettäviä komponentteja ei ole

teknisiä perusteita rajata määräyksen soveltamisen ulkopuolelle, jos kyseiset komponentit kuitenkin vaikuttavat esimerkiksi tärkeysluokkansa johdosta niin merkittävään määrään käyttäjiä, että niitä on pidettävä viestintäverkon kriittisinä osina. Traficom toteaa edelleen, että vaikka ehdotettu rajaus tehtäisiin, voisivat tukiasema- ja radioverkko-ohjaimet olla verkon kriittisiä osia esimerkiksi 4 kohdan luettelon 1 kohdan perusteella jo siksi, että ne "voivat olennaisesti vaikuttaa viestintäverkossa kulkevaan liikenteeseen". Traficom katsoo myös, ettei sillä, että hätäpuhelut mahdollisesti ohjautuvat toiseen verkkoon (mikäli kuuluvuutta on), ole teknisesti arvioiden merkitystä sen kannalta, onko tukiasemaohjain tai radioverkko-ohjain sen verkon kriittinen osa, johon se kuuluu. Tämänkaltaisilla seikoilla voi kuitenkin olla merkitystä arvioitaessa SVPL 244 a §:n 1 momentin mukaisesti sitä, että onko painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta säännöksessä tarkoitetulla tavalla (ns. vaarantamisedellytys).

DNA nosti esiin 2G- ja 3G-tukiasemien riippuvuuden saman valmistajan tukiasema- ja radioverkko-ohjaimista ja sen, että tukiasema- tai radioverkko-ohjaimen määrittäminen kriittiseksi tarkoittaisi, että kyseisen teknologian tukiasemat jouduttaisiin vaihtamaan toisen valmistajan laitteisiin. Tämä taas DNA:n mukaan ei ole mahdollista johtuen nykyaikaisten tukiasemien integroidusta arkkitehtuurista, jossa kaikki tukiasemateknologiat (2G/3G/4G/5G) ovat integroituna yhteen fyysiseen yksikköön. Näin ollen DNA:n näkemyksen mukaan lopputuloksena olisi kriittiseksi määritelty tukiasema kaikkien teknologioiden osalta. Myös FiCom toi lausunnossaan esiin nykyaikaisen tukiaseman integroidun arkkitehtuurin ja vetosi siihen, että tukiasema ei itsessään ole kriittinen, joten myöskään 2G- ja 3G-verkkojen laitteiden, kuten tukiasemaohjaimien, ei oletusarvoisesti tulisi olla kriittisiä.

Traficomin käsityksen mukaan 2G- tai 3G-tukiasematoiminnallisuuksien erottaminen integroidusta tukiasemasta on sinänsä teknisesti mahdollista. Näin toimittaessa toisen valmistajan 2G- tai 3G-tukiasema asennettaisiin samaan laitetilaan integroidun tukiaseman rinnalle. Traficom toteaa, että DNA:n esiin tuomaa tilannetta on jo käsitelty määräyksen vaikutusarviossa. Traficom korostaa, että radioverkko- ja tukiasemaohjaimien lukeminen viestintäverkon kriittisiksi osiksi ei sinänsä tarkoita, että kyseisen verkkotekniikan (saman radioverkon) tukiasemat olisivat pelkästään tämän takia verkon kriittisiä osia. Kuten vaikutusarviossa on todettu, tukiasemaohjainten pitämisellä verkon kriittisinä osina voi kuitenkin olla käytännössä vaikutusta myös saman valmistajan tukiasemien käyttöön. Jos tukiasemia ei ole taloudellisesti ja toiminnallisesti mahdollista käyttää ilman saman valmistajan tukiasemaohjaimia, velvoite poistaa viimeksi mainitut verkosta saattaisi tosiasiallisesti johtaa myös saman laitevalmistajan tukiasemien verkosta poistamiseen.

Huawei totesi lausunnossaan, että tukiasemaohjaimella ei estetä loppukäyttäjän pääsyä järjestelmään eikä rajoiteta liikennevirtoja viestintäverkkoon. Huawein lausunnossa tuotiin myös esiin, että 2G- ja 3G-teknologiat ovat olleet käytössä vuosikausia kaikkialla maailmassa, eikä niissä ole havaittu kansallista turvallisuutta tai maanpuolustusta uhkaavia ongelmia. Lausunnossa mainittiin myös 3G-verkkojen elinkaaren päättyminen lähivuosina sekä 2G-verkkojen rajallinen tarve tulevaisuudessa (esim. 2G IoT -ratkaisut).

Traficomin näkemyksen mukaan tukiasema- ja radioverkko-ohjaimet voivat vaikuttaa merkittävällä tavalla loppukäyttäjien verkkoon pääsyyn sekä palveluiden saatavuuteen. Radioverkko- tai tukiasemaohjaimen ollessa poissa käytöstä esimerkiksi palvelunestohyökkäyksen johdosta ei yhdenkään kyseiseen ohjaimeen yhteydessä olevan tukiaseman kautta pääse liittymään verkkoon. Lisäksi 2G- ja 3G-verkot ovat huomattavasti nykyisiä verkkoteknologioita haavoittuvampia, ja esimerkiksi SS7-protokollan väärinkäyttöön perustuvat hyökkäykset kohdistuvat pääosin 2G- ja 3G-teknologioihin. Traficom katsoo, että 3G-verkkojen elinkaaren päättyminen sinänsä vähentää teleyrityksiin kohdistuvia mahdollisia vaikutuksia siitä, että osa kyseisen

verkon osista määritellään kriittisiksi. Traficom toteaa myös, että pitempään käyttöön jäävän 2G-verkon rajalliset käyttötarkoitukset voivat olla seikkoja, jotka voidaan periaatteessa ottaa huomioon siinä SVPL 244 a §:n 1 momentin mukaisessa erillisessä arviossa, että onko painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta säännöksessä tarkoitetulla tavalla.

4 Tukiasemien hallintajärjestelmä

Nokia katsoi lausunnossaan, että perustelumuistion luvun 6 kohdan (Radioliityntäverkon osat ja tukiasemien hallintajärjestelmä) kappaleet 2 ja 4 ovat osittain ristiradassa keskenään. Traficom toteaa, että kyseisissä kappaleissa tarkastellaan tukiasemien hallintajärjestelmän arviointia yksittäistapauksina määräyksen ja SVPL 244 a §:n mukaisten kriteerien ja rakenteen kautta. Kappaleissa käsitellään ensin viestintäverkon osan kriittisyyden arviointia ja sitten siitä erikseen ratkaistavaa kysymystä siitä, täyttääkö tietyn viestintäverkkolaitteen käyttäminen verkon kriittisessä osassa SVPL 244 a §:n 1 momentin mukaisen ns. vaarantamisedellytyksen.

DNA katsoi lausunnossaan, että koska radioverkon hallinnan kriittisyyden arviointi on jätetty tapauskohtaiseksi, tulisi asiassa noudattaa suhteellisuusperiaatetta ja tulkintamahdollisuuksista olisi aina valittava suppein vaihtoehto. Traficom toteaa, että kriittisyyden arviointi tehdään aina asiaa koskevia SVPL:n säännöksiä sekä hallinnon oikeusperiaatteita noudattaen.

5 Kriittisten osien määrittelytapa sekä tukiasemien kriittisyyden määrittely kriittiseksi

5.1 Määräyksenantovaltuuden ala

Sisäministeriö katsoo, että määräyksessä sivuutetaan tarve tunnistaa kansallista turvallisuutta vaarantavat laitteet sekä tarve soveltaa teknistä tietoturvallisuutta laajempaa turvallisuusarviointia. Sisäministeriö pitää tukiasemia olennaisena verkon osana, joka voi johtaa kansallisen turvallisuuden vaarantumiseen. Sisäministeriö katsoo, että mikä tahansa yksittäinenkin osa viestintäverkkoa, joka voi estää turvallisuusviranomaisten aikakriittisen viestinnän välittämisen teleyrityksen viestintäverkossa yhteiskunnan tai käyttäjien turvallisuuden varmistamiseksi, on kriittinen osa viestintäverkkoa. Tukiasemat kontrolloivat verkkoon pääsyä ja voivat viestintäverkkoliikenteen estäessään johtaa kansallisen turvallisuuden vaarantumiseen. Puolustusministeriön lausunnossa määräyksen lähestymistapaa kritisoitiin niin ikään siitä, että kriittiset osat on määritelty hyvin pitkälti teknisen ilmentymän näkökulmasta, kun asiaa olisi arvioitava myös kansallisen turvallisuuden ja maanpuolustuksen näkökulmasta. Puolustusministeriö katsoo myös, että määräysluonnoksessa ei huomioida laitevalmistajariskiä.

Sisäministeriö katsoo lausunnossaan, että jo lain valmisteluvaiheessa on tuotu esille tarve tunnistaa kaikki ne verkon komponentit ja toiminnot, jotka voivat vaarantaa kansallista turvallisuutta ja joiden osalta tämä tekninen määrittely tulisi tehdä. Hallituksen esityksessä (HE 98/2020 vp) todetaan, että "Teknisessä määrittelyssä on keskeistä tunnistaa ne viestintäverkon osat, joissa viestintäverkkolaite voisi tosiasiallisesti johtaa kansallisen turvallisuuden vaarantumiseen ja joissa käytettäviin viestintäverkkolaitteisiin olisi tästä syystä tarpeen soveltaa teknistä tietoturvallisuutta laajempaa turvallisuusarviointia kulloisessakin verkkoteknologian kehitysvaiheessa." Lisäksi liikenne- ja viestintävaliokunta on todennut, että "esityksessä on noudatettu suhteellisuusperiaatetta asianmukaisesti kohdistaen sääntely niihin verkon osiin ja toimintoihin, joissa käytettävät viestintäverkkolaitteet voivat johtaa kansallisen turvallisuuden tai maanpuolustuksen vaarantumiseen" (LiVM 16/2020 vp).

Traficomin käsityksen mukaan lausunnonantajat esittävät, että kriittisten osien määrittelyssä tulisi huomioida laajemmin se, voiko johonkin verkon osaan kohdistuva uhka joissain tilanteissa vaarantaa kansallista turvallisuutta tai maanpuolustusta. Traficom katsoo, että tällä ei voida kuitenkaan perustella viestintäverkon kriittisten osien laajentavaa tulkintaa. Tukiasemien osalta lausuntoja käsitellään tarkemmin jäljempänä. Tämän näkemyksen osalta on aluksi todettava, että viranomaismääräysten antamisessa on kyse siirretyn lainsäädäntövallan käyttämisestä. Kyseessä on poikkeus siihen pääsääntöön, että lainsäädäntövaltaa käyttää eduskunta ja että asetuksia voivat laissa säädetyn valtuuden nojalla tietyissä tapauksissa antaa tasavallan presidentti, valtioneuvosto tai ministeriö (perustuslaki 3 § 1 mom. ja 80 § 1 mom.). Viranomaisen voi lailla valtuuttaa yleisten oikeussääntöjen antamiseen vain määrätyistä asioista, erityisestä syystä ja soveltamisalaltaan tarkasti rajatulla valtuutussäännöksellä (perustuslaki 80 § 2 mom., HE 1/1998, s. 133). Perustuslakivaliokunta on vakiintuneessa lausuntokäytännössään katsonut, että perustuslain 80 §:n 1 ja 2 momentin säännökset rajoittavat suoraan viranomaismääräysten sisältöä samoin kuin valtuussäännösten tulkintaa, ja että määräysten antamiseen valtuuttavia lain säännöksiä on tulkittava supistavasti (esim. PeVL 26/2001 vp, PeVL 48/2001 vp, PeVL 19/2002 vp, PeVL 24/2002 vp, PeVL 17/2003 vp ja PeVL 9/2004 vp). Näin ollen myös tämän määräyksen antamiseen valtuuttavaa säännöstä on tulkittava supistavasti. SVPL 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."

Traficomin näkemyksen mukaan valtuutussäännös mahdollistaa vain viestintäverkon kriittisten osien teknisen määrittelyn SVPL 244 a §:n 1 momentin toisessa virkkeessä vahvistettujen objektiivisten teknisten kriteerien perusteella.[1] Viestintäverkon kriittisenä osana pidetään verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Näin ollen määräyksessä ei ole mahdollista huomioida esimerkiksi laitevalmistajakohtaista riskiprofiilia, viestintäverkon tai sen osan käyttäjiä (esim. viranomainen) taikka kansallisen turvallisuuden ja maanpuolustuksen näkökulmaa. Traficomin näkemyksen mukaan nämä ovat seikkoja, jotka voivat tulla arvioitavaksi mahdollisissa konkreettisissa yksittäistapauksissa ratkaistaessa SVPL 244 a §:n nojalla sitä, onko viestintäverkon omistaja tai haltija velvoitettava poistamaan verkkonsa kriittisestä osasta laite, jonka osalta on painavia perusteita epäillä säännöksen 1 momentissa tarkoitettua kansallisen turvallisuuden tai maanpuolustuksen vaarantumista.

Traficom katsoo, että nyt annettava määräys voi sisältää täsmentävää sääntelyä vain siitä, milloin kriittisen osan määritelmän katsotaan täyttyvän, eikä lainkaan siitä, milloin kansallisen turvallisuuden katsotaan vaarantuvan. Sen arviointi, onko painavia perusteita epäillä, että tietyn viestintäverkkolaitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta, ei kuulu määräykseen. Kriittisen osan määritelmän soveltamisen kannalta ei ole tarpeen eikä määräyksenantovaltuuden kannalta mahdollistakaan ottaa kantaa siihen, missä konkreetissa skenaariossa kansallinen turvallisuus tosiasiassa vaarantuisi, vaan tämä tapahtuisi vasta mahdollista poistovelvoitteen asettamista koskevan yksittäisen asian yhteydessä.

Kun viestintäverkon toiminnot ja toimenpiteet ovat verkon kannalta keskeisiä, ne voivat luonnollisesti vaarantaa myös kansallista turvallisuutta. Kriittisen osan määritelmä ei itsessään edellytä erillistä arviota suhteessa kansalliseen turvallisuuteen. Kriittisen osan määritelmän kannalta ei lähtökohtaisesti ole merkitystä esimerkiksi viestintäverkkolaitteen valmistajalla, vaan arvioitavana ovat viestintäverkkolaitteen toteuttamat toiminnot ja toimenpiteet verkossa. Eri asia on, että kriittisten osien

[1] Kuten myös professori Kaarlo Tuorin perustuslakivaliokunnalle antamassa asiantuntijalausunnossa painotetaan, muita kuin teknisiä määräyksiä ei voida perustuslain 80 §:ään nähden Liikenne- ja viestintäviraston päätöksellä lainkaan antaa.

määrittelyssä on kiinnitetty huomiota HE:n mukaisesti siihen, onko jollakin taholla teleyrityksen lisäksi ylipäänsä mahdollisuuksia vaikuttaa viestintäverkon osan tai siellä olevan viestintäverkkolaitteen toimintaan ja ominaisuuksiin (HE 98/2020). Koska tämä voi toteutua esimerkiksi laitteessa käytetyn ohjelmiston laatimisen tai mahdollisen etähallinnan kautta, tämä näkökohta ei juurikaan voi rajoittaa viestintäverkon kriittisten osien piiriä.

Lisäksi on huomattava, että määräys viestintäverkon kriittisistä osista ei ole ainoa viestintäverkkojen tietoturvallisuutta koskeva määräys. Muita verkkojen turvallisuuden ja toimivuuden takaamiseen tähtääviä Traficomin määräyksiä on esitelty perustelumuistion luvussa 2 (s. 3–4).

5.2 Euroopan unionin suositusten huomioon ottaminen

Puolustusministeriön näkemyksen mukaan määräysluonnoksessa ei ole huomioitu riittävästi Euroopan unionin antamia suosituksia 5G-turvallisuuteen liittyen.

Traficom toteaa, että kuten perustelumuistiossa tuodaan esiin, määräyksellä toteutetaan osaltaan EU:n 5G-verkkojen turvallisuuteen liittyvää yhteisen keinovalikoiman[2] toimenpidettä, joka koskee verkon kriittisten osien suojaamista. Keinovalikoiman huomioimista määräyksen valmistelussa kuvataan mm. perustelumuistion yleisperustelujen luvussa 4.3.1 (Valittu määrittelytapa) sekä yksityiskohtaisten perustelujen luvuissa 4.1 (Kriittisten osien määrittely) ja 6.4 (Kansainvälinen vertailu). Kohdissa arvioidaan määräyksen mukaista verkon kriittisten osien määrittelyä suhteessa keinovalikoimassa kriittisiksi tai sensitiivisiksi kuvattuihin verkon osiin.

Kuten edellä on tuotu esiin, Traficom on sidottu sille annettuun määräyksenantovaltuuteen. Viestintäverkon kriittisten osien määrittely määräyksellä perustuu kansalliseen lakiin sisältyvän viestintäverkon kriittisen osan määritelmän soveltamiseen. EU:n piirissä laadittujen suositusten ja muiden soft law -instrumenttien perusteella ei voida laajentaa kansallisen lain ja tässä erityisesti SVPL:n 244 a §:n 6 momentin määräyksenantovaltuuden sisältävän säännöksen tulkintaa.

5.3 Tukiasemien määrittely verkon kriittisiksi osaksi

Puolustusministeriön näkemyksen mukaan 5G-tukiasemat ovat kriittinen osa viestintäverkkoa. Puolustusministeriö toteaa, että tukiasemien osalta tulee noudattaa varovaisuusperiaatetta niin, että tukiasemat katsottaisiin kriittisiksi, kunnes toisin todistetaan. Puolustusministeriön näkemyksen mukaan tämä on ainoa tapa vastata tässä vaiheessa teknologian kehitykseen, mutta määräysluonnos ei sisällä tällaista ennakoivaa arviointia, vaan Traficom tarkentaa tarvittaessa määräyksen sisältöä teknologian kehittyessä.

Traficom toteaa kohdassa 5.1 määräyksenantovaltuudesta sanotun perusteella, että viestintäverkon kriittisten osien teknisen määrittelyn on perustuslakivaliokunnan käytäntö ja hallinnon oikeusperiaatteet huomioiden oltava oikeasuhtaista ja tarkkarajaista. Tämä tarkoittaa, että tulevien verkkosukupolvien osalta niiden osia ei voida ennakolta määritellä kriittisiksi ilman, että niiden voidaan osoittaa täyttävän viestin-

[2] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. Liite 2, s. 39. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. Ks. myös EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019, k. 2.21. https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

täverkon kriittisen osan määritelmän. Tämä edellyttää tarkempaa tietoa niiden luonteesta ja toiminnasta osana verkkoa. Myös esitöissä lähtökohtana on olemassa olevan tekniikan taso[3].

Sisäministeriö esittää, että 4G- ja 5G-verkkojen tukiasemien osalta tulisi arvioida jo tässä vaiheessa, miten tukiasemissa olevat toiminnot olennaisella tavalla kontrolloivat verkkoon pääsyä. Sisäministeriön näkemyksen mukaan, vaikka kaikkia tukiasemien toimintoja ei vielä voida käyttötarkoitukseltaan määrittää, voidaan gNodeB:n ja eNodeB:n osalta kriittiset toiminnot kuitenkin jo kuvata. Tukiasema on ensimmäinen yhteyskohta, jossa voidaan kontrolloida käyttäjien pääsyä verkkoon ja verkossa pääsyä kulkevaa liikennettä kokonaan tai osittain, minkä takia tukiasemia on pidettävä viestintäverkon kriittisinä osina. Nämä toiminnot liittyvät olennaisesti myös yhteyksien ylläpitoon ja palvelujen saatavuuteen. Vaikka osaa tukiasemien parametreista kontrolloidaankin verkon ytimen puolelta, vaikuttavat ne jo tukiasemassa. Lisäksi tukiasemalla on merkitystä tietoturvan kannalta, mikäli käyttäjien data on salaamattomana tukiasemakomponenteissa.

Sisäministeriö siis esittää, että tukiasemien kriittiset toiminnot olisi jo mahdollista kuvata määräyksessä. Traficom toteaa tämän johdosta aluksi, että määräyksen 4 kohdassa määritellään jo teknologianeutraalisti ne toiminnot ja toimenpiteet verkossa, joita määräyksen mukaan pidettäisiin viestintäverkon kriittisinä osina. Kohta ei ota kantaa siihen, missä osassa verkkoa kyseiset toiminnallisuudet toteutetaan. Mikäli niitä toteutetaan jatkossa tukiasemissa tai muutoin radioverkossa, pidettäisiin niitä määräyksen mukaisesti viestintäverkon kriittisinä osina. Radioverkon osana toimivien tukiasemaohjainten osalta tilannetta onkin käsitelty jo edellä kohdassa 3.

Lisäksi Traficom korostaa, että SVPL 244 a §:n 3 momentissa tarkoitettuihin toimenpiteisiin (verkkolaitteen poistaminen verkon kriittisistä osista) voidaan edellytysten täyttyessä ryhtyä siitä riippumatta, onko viestintäverkon osa määritelty nimenomaan määräyksessä ennakollisesti kriittiseksi. Viestintäverkon kriittiset osat määritellään SVPL:n 244 a §:n 1 momentissa, jonka mukaan viestintäverkon kriittisenä osana pidetään verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Asiaa on käsitelty perustelumuistiossa (s. 9), jossa todetaan, että 4G- tai 5G-verkon tukiasemien kriittisyyttä verkon osina olisi tarvittaessa arvioitava suoraan SVPL 244 a §:n 1 momentissa olevan viestintäverkon kriittisten osien määritelmän perusteella sekä määräyksen eri verkoille yhteisten kriittisten osien teknologianeutraalin määrittelyn perusteella. Määräys ei ole tyhjentävä. Ei siis ole niin, kuten sisäministeriö lausunnossaan esittää, että tukiasemiin voisi kohdistua käyttökielto (tai päätöksellä asetettava poistovelvoite) niiden vaarantaessa kansallista turvallisuutta vain, jos ne olisi määräyksessä määritelty viestintäverkon kriittisiksi osiksi. Traficomin näkemyksen mukaan SVPL 244 a § sekä tähänastinen määräysvalmistelu ohjaavat teleyrityksiä huomioimaan verkon osien mahdollisen kriittisyyden tulevissa laitehankinnoissaan.

Traficom kuitenkin huomauttaa, että sisäministeriön mainitsemat 4G- ja 5G-tukiasemien piirteet koskevat käytännössä suurelta osin myös vanhempia matkaviestinverkkojen sukupolvia.[4] Vaikka uusimpien sukupolvien tukiasemiin sisältyy aiempaa

[3] Tulevien sukupolvien verkkotekniikoiden osalta lain esitöissä (HE 98/2020 vp, s. 261) mainitaan, että "Myös 5G-verkkojen osalta on mahdollista erottaa verkon kriittiset osat, vaikkakin 5G-verkon rakenne on aikaisempia verkkosukupolvia monimutkaisempi. Tulevaisuuden verkkosukupolvissa, kuten 5G-verkoissa ja 6G-verkoissa, kriittiset osat tulisi määritellä sen hetkisen teknologisen kehityksen mukaisesti."

[4] Esitöissä (HE 98/2020 vp, s. 261) todetaan, että viestintäverkon kriittisenä osana pidettäisiin verkon ydintä, ja että nykyisessä verkkoteknologiassa kriittistä ydintä on esimerkiksi se osa runkoverkkoa, jossa hallinnoidaan eri käyttäjien pääsyä verkkoon ja ylläpidetään käyttäjien yhteyksien tilaa. Viestintäverkon kriittisten osat varmistavat palveluiden saatavuuden ja viestinnän luottamuksellisuuden. Viestintäverkon kriittisiin osiin kuuluvat myös ne verkon osat, joissa varmistetaan koko viestintäverkon tietoturva. Nykyisten verkkojen osalta nämä toimet ja toimenpiteet on toteutettu runkoverkossa.

enemmän toiminnallisuuksia, käyttäjien verkkoon pääsyn pystyy estämään yksittäisessä tukiasemassa myös aiemmissa sukupolvissa. Myös 2G- ja 3G-tukiasemat ovat verkon ensimmäisiä yhteyskohtia, joissa voidaan kontrolloida käyttäjän pääsyä verkkoon ja myös estää se. 2G- ja 3G- tukiasemat (kuten myös 4G-tukiasema) ovat vastuussa kaiken käyttäjäliikenteen lähettämisestä ja vastaanottamisesta radiorajapinnassa ja näin ollen vastaavat myös käyttäjien verkkoon pääsystä. Esimerkiksi integroidun tukiaseman tapauksessa, jos tukiasemaa on mahdollista hallita ohjelmallisesti ja tätä kautta estää käyttäjien pääsy verkkoon, koskee tämä lähtökohtaisesti yhtä lailla kaikkien eri sukupolvien tekniikoita. Kuten perustelumuistiossa on todettu (s. 8), aiempien sukupolvien tukiasema- ja radioverkko-ohjaimiin verrattuna yksittäisen 4G- tai 5G-tukiaseman toiminnallisuudet vaikuttavat kuitenkin suhteellisen pieneen käyttäjämäärään.

Traficom toteaa määräyksen perustelumuistiossa (yleisperustelujen kohta 4.1.5 ja 6), että 5G-verkkojen osalta on ennenaikaista määritellä sitä, ovatko tukiasemat viestintäverkon kriittisiä osia.[5] Jälkiseurannassa voidaan tarvittaessa selvittää, onko tarpeen määrätä tukiasemien kriittisyyden arvioimisesta tarkemmin. Määräyksen perustelumuistiossa todetaan (luku 4.1.5), että: "5G SA -verkon tukiasemien (gNodeB; myös ng-eNodeB) erityispiirteitä voidaan arvioida vasta tulevaisuudessa, sillä tukiasemien tekninen kehitys on vielä kesken. Tukiasemien arkkitehtuurin määrittely ja käyttötapaukset ovat vielä tärkeiltä osin kehitysvaiheessa. Tukiasemaan voi siirtyä päätöksentekoa, laskentatehoa ja älyä sisältäviä toiminteita tai verkon ytimen komponentteja. Nämä seikat olisi erityisesti huomioitava tukiaseman kriittisyyttä koskevassa arvioinnissa. On vasta kehittymässä, millaiseksi tukiaseman komponenttien arkkitehtuuri muodostuu, ja miten komponentteja tai funktioita voidaan jaotella ja virtualisoida (vrt. Open RAN). Samoin verkon viipaloinnin (slicing) sekä reunalaskennan kehitys ja käyttötarkoitus ovat vielä muotoutumassa, joten olisi ennenaikaista antaa sääntelyä asiasta ainakaan yleisten viestintäverkkojen osalta."

5G-verkkojen keskeisiä piirteitä uusien palvelujen mahdollistamiseksi ovat matkaviestinverkon korkeat datanopeudet, suuri kapasiteetti, mahdollisimman viiveetön toiminta ja luotettavuus. Näiden tekijöiden saavuttamiseksi radioverkon toiminnallisuuksia on laajennettu ja lisätty sen autonomiaa suhteessa runkoverkon keskitettyihin verkkoelementteihin. Tulevien verkkosukupolvien odotetaan tarjoavan uuden edistysaskeleen suorituskyvyssä kohti terabitin kapasiteettia ja millisekunnin vasteaikoja, joita uudet kriittiset sovellukset kuten reaaliaikainen automaatio tai laajennettu todellisuus tarvitsevat. Seuraavassa kuvataan perustelumuistiota yksityiskohtaisemmin asioita, jotka ainakin voivat tulevaisuudessa vaikuttaa tukiasemien kriittisyyttä koskevaan arviointiin, mutta joihin liittyy huomattavaa epävarmuutta. Näitä muutoksia voidaan arvioida osana määräyksen jälkiseurantaa.

Suuri epävarmuutta aiheuttava kokonaisuus on mahdolliset kehityskulut, jotka liittyvät tukiaseman toiminnallisuuksien kehittymiseen sekä niiden virtualisointiin, erotteluun ja keskittämiseen. Näillä voi olla vaikutusta siihen, miten tukiasemien ja niihin läheisesti liittyvien toiminnallisuuksien kriittisyyttä tullaan arvioimaan. Niitä kehitetään mm. osana 3GGP Release 17:aa, jossa ollaan tiettävästi tuomassa uusia ominaisuuksia ja lisäksi tekemässä mahdollisia muutoksia verkon arkkitehtuuriin (esim. palveluväylään liittymisessä). Kehityskulkuja kuvataan tiiviisti seuraavaksi.

Merkittävä tekijä 5G-tukiaseman kriittisyyden arvioinnissa tulee olemaan tukiaseman keskusyksikön eli CU:n (Central Unit) virtualisointi ja keskittäminen. CU tulee mahdollisesti ohjaamaan hyvinkin suurta määrää hajautettuja yksiköitä eli DU:ita (Distributed Unit). Yksi mahdollinen toteutus saattaisi olla, että yksittäisen CU:n oh-

[5] Tukiasemien lisäksi näin todetaan myös 5G-verkon mahdollistamien luotettujen Wi-Fi-verkkojen tai kiinteän verkon yhteyksiin perustuvan liitynnän (Wireline Access) osalta, jotka voivat tulevaisuudessa täydentää 5G-tukiasemiin perustuvaa liityntäverkkoa.

jauksen piirissä voisi olla esimerkiksi kokonainen kaupunki. Tällaisessa toteutuksessa CU:n ja DU:n suhdetta voisi yksinkertaistetusti verrata saman tyyppiseen jakoon, joka 2G:n ja 3G:n tapauksissa on tukiasemien sekä radioverkko- ja tukiasemaohjainten välillä.

Tukiaseman toiminnallisuuksien jakautuminen CU:n, DU:n ja radioyksikön välillä on vielä ratkaisematta, ja on mahdollista, että toteutukset tulevat vaihtelemaan laitevalmistajien kesken. Esimerkiksi Ericsson on tunnistanut useita mahdollisia erilaisia toteutustapoja ja kehityskulkuja, miten CU:n ja DU:n toiminnallisuuksia tai niiden osia voidaan jatkossa toteuttaa keskitetysti tai hajautetusti.[6] CU:n ja DU:n välisen F1-rajapinnan turvallisuusvaatimukset on määritelty 3GPP:n teknisessä määrityksessä TS 33.501, ja vaatimusten toteutustapa on pääosin laitevalmistajan päätettävissä.[7] Myös OpenRAN:in yleistyminen saattaa vaikuttaa siihen, miten toiminnallisuudet tulevat jakautumaan eri yksiköiden/3GGP:n funktioiden välillä.

CU:n ja DU:n toiminnallisuuksien jakautuminen sekä keskitetyn ja virtualisoidun arkkitehtuurin muotoutuminen on myös suurelta osin riippuvainen verkon ja tukiaseman käyttötarkoituksesta. Esimerkiksi loppukäyttäjän tarvitessa luotettavaa lyhytviiveistä palvelua tulee prosessoinnin painotus olla hajautettuna lähelle verkon reunaa. Toisaalta taas ei-aikakriittisten peruspalvelujen tapauksessa toiminnallisuus voi olla hyvinkin vahvasti keskitetty yhteen sijaintiin.

Myös radioyksikön rooli on muuttumassa. Yleistymässä ovat massive-MIMO-radiot, joissa samaan yksikköön on integroitu radiotoiminnallisuuksien lisäksi myös antennit. Tällaisella beamforming-teknologiaa hyödyntävällä toteutuksella mahdollistetaan muun muassa käyttäjän sijaintiin perustuva radiorajapinnan optimaalinen käyttö. Mahdollista on, että osa DU:n toiminnallisuuksista voitaisiin myös toteuttaa tällaisessa integroidussa radioyksikössä. Verkon turvallisuuden kannalta haasteita voi tuoda se, jos yksiköiden välinen kommunikaatio muuttuu täysin IP-pohjaiseksi. Tämä tulee luonnollisesti ottaa huomioon tarkasteltaessa verkon funktioiden kriittisyyttä.

Luotettava pieniviiveinen kommunikaatio eli URLLC (Ultra-reliable low-latency communication) on yksi 5G:n peruspilareista, ja sen mahdollistamiseksi verkon ytimen funktioita täytyy hajauttaa lähemmäs verkon reunaa ja loppukäyttäjiä. Tällöin esimerkiksi UPF-funktion tulisi sijaita mahdollisimman lähellä verkon reunaa eli todennäköisesti CU-yksikön läheisyydessä. – UPF-funktio on jo määritelty määräyksessä oletusarvoisesti viestintäverkon kriittiseksi osaksi, johon kuitenkin kohdistuu poikkeusmahdollisuus määräyksen 7 kohdan perusteella verkon reunalla tuotettavia palveluita tukevan toiminnon osalta.

Korkeammilla mmWave-taajuuskaistoilla 5G-tukiasemien kantama on vain satoja metrejä, jolloin ketjutettu runkoliityntäyhteys käyttäen IAB-ominaisuutta (Integrated Access and Backhaul) saattaa tulla laajaan käyttöön.[8] Tiheää 5G-verkkoa rakennettaessa kyseinen ominaisuus mahdollistaa useiden DU-yksiköiden langattoman ketjuttamisen ja vähentää näin kiinteiden kuituyhteyksien tarvetta. Ainakin CU:n ja ketjussa ensimmäisenä olevan donor-DU:n kriittisyys tulee tämän myötä arvioitavaksi.

Sisäministeriö katsoo myös, että määräyksen mukaista erillisverkkoja koskevaa tukiaseman kriittisyyttä koskevaa arviointivelvoitetta tulisi soveltaa myös yleisten

[6] Tech Unveiled Ericsson Cloud RAN, October 2020, https://www.ericsson.com/4af677/assets/local/ran/doc/tech-unveiled-cloudran-ebook.pdf, s. 18-19.
[7] Security architecture and procedures for 5G System, 3GPP TS 33.501 version 15.2.0 Release 15, https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf.
[8] Integrated access and backhaul: Why it is essential for mmWave deployments, 13.11.2020, https://www.nokia.com/blog/integrated-access-and-backhaul-why-it-is-essential-for-mmwave-deployments/. 3GPP Release 16 määrittelee toiminnallisuuden.

viestintäverkkojen tukiasemiin, koska niitä käytetään muutaman vuoden päästä ihmishenkien ja ympäristön pelastamiseen. Erillisverkkojen tukiasemien käyttötapaukset voivat merkitykseltään olla jopa vähäisempiä kuin yleisen viestintäverkon tukiasemien huomioiden viranomaisten viestiliikenteen merkitys ihmishenkien pelastamisessa tai omaisuuden turvaamisessa. Sisäministeriö kritisoi sitä, että erillisverkkojen tukiasemien osalta tunnistetaan jo nyt palveluiden merkittävyys käyttäjilleen, mutta viranomaisten viestiliikenteen osalta tätä ei määräysluonnoksessa tehdä.

Traficom toteaa, että määräyksen perustelumuistion yksityiskohtaisten perustelujen kohdassa 3.3 perustellaan erityistä tunnistamis- ja dokumentointivelvoitetta tukiasemien osalta erillisverkoille sillä, että niissä verkko ja sen tukiasemat voivat palvella pientä aluetta, palvelu voi olla hyvin merkittävä käyttäjilleen ja tukiaseman toimintoja voinee olla useammin samalla alustalla verkon ytimen toimintojen kanssa. Tästä erillisenä asiana kuvataan kohdan alussa, mitä seikkoja tukiaseman kriittisyyttä koskevassa arviossa olisi huomioitava.

5.4 Tärkeysluokittelun ja käyttäjämäärän ja vaikutusalueen käyttäminen kriittisyyden määrittelyssä

Sisäministeriö katsoo, että käyttäjämäärän ja vaikutusalueen käyttäminen kriittisten osien määrittelyssä ei vastaa määräyksen tarkoitusta tai tavoitetta. Näitä ei voida lausunnon mukaan yksistään pitää määrittävänä tekijänä huomioiden, että tulevaisuudessa yksi tukiasema saattaa toimia yhteiskunnan turvallisuuden kannalta merkittävän moniviranomaisoperaation ainoana viesti- ja palveluyhteysväylänä tai esimerkiksi terroritekoon liittyvän pelastusoperaation tilannekuvan välityspisteenä. Sisäministeriö toteaa, että yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten, valtion ylimmän johdon ja kriittisen infrastruktuurin toimijoiden viestinnän tietoturvallisuuden vaarantuminen voi uhata vakavasti kansallista turvallisuutta tai sotilaallista maanpuolustusta, ja että näiden yhteiskunnallisesti tärkeiden tahojen toiminta edellyttää, että viestintäverkkojen avulla siirretyn tiedon tietoturvallisuus tulee olla suojattuna sen kaikilla eri osa-alueilla (eheys, luottamuksellisuus ja saatavuus) läpi koko viestintäverkon. Käyttäjämäärän perusteella esimerkiksi ihmisten ympäristön ja omaisuuden turvallisuudesta huolehtivien viranomaisten viestiliikenne ei ole niin merkittävää, että se Traficomin nyt käyttämien määritelmien mukaan olisi kriittistä tai että tämän viestiliikenteen varmistamiseen käytettävät tukiasemalaitteet kuuluisivat viestintäverkon kriittisiin osiin.

Traficom toteaa ensinnäkin, että käyttäjämäärä ja vaikutusalue mainitaan määräyksessä kriteereinä vain yhdessä kohdassa, jossa määrätään viittaamalla määräykseen 54, että mitkä ainakin ovat sellaisia liikenteen reititykseen ja muuhun kontrollointiin tai ohjaamiseen viestintäverkossa liittyvät keskeiset toiminnot, joita on pidettävä viestintäverkon kriittisinä osina. Nämä kriteerit ja tärkeysluokitteluun viittaaminen eivät millään tavoin rajoita muulla perusteella kriittisinä pidettävien verkon osien alaa.

Traficom toteaa toiseksi, että edellä kohdassa 5.1 sanotun perusteella sen määräyksenantovaltuus ei mahdollista erilaisten käyttäjäryhmien huomioimista sen määrittelyssä, mikä on viestintäverkon kriittinen osa. SVPL 244 a §:n nojalla viestintäverkon kriittiset osat määräytyvät teknisin kriteerein sen mukaan, onko kyseessä verkon keskeinen toiminto ja toimenpide, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Vaikka tietyssä yleisessä viestintäverkossa tarjottaisiin viranomaisviestintään liittyviin verkkopalvelua, sääntelyä sovelletaan tällaiseen verkkoon samoin kuten mihin tahansa yleiseen viestintäverkkoon. Tämä periaate ilmenee Traficomin käsityksen mukaan myös esitöistä, kun niissä todetaan, että ehdotettavaa (yleisiin viestintäverkkoihin kohdistuvaa) säännöstä sovellettaisiin myös viranomaisviestintään liittyviin verkkopalveluihin siltä

osin kuin näiden palveluiden tarjoamisessa hyödynnetään teleyritysten yleisiä viestintäverkkoja (HE 98/2020 vp).

6 Kriittiset erillisverkot ja turvallisuusverkkotoiminta

Valtiovarainministeriön näkemyksen mukaan SVPL 244 a §:n 2 momentissa olevan erillisverkon määritelmän perusteella jää pykälätasolla epäselväksi, voidaanko turvallisuusverkon tulkita olevan siinä ja määräyksessä tarkoitettu kriittinen erillisverkko. Valtiovarainministeriön näkemyksen mukaan SVPL 3 §:n 39 a kohdassa määritelty viranomaisverkko eikä siten myöskään turvallisuusverkko ole lain 244 a §:ssä ja määräysluonnoksessa tarkoitettu erillisverkko, eikä määräystä näin ollen tule soveltaa viranomaisverkkoihin, mukaan lukien turvallisuusverkkotoimintaan. Valtiovarainministeriö tunnistaa myös tarpeen edelleen selkeyttää sähköisen viestinnän palveluista annetun lain 244 a §:n 2 momenttia tältä osin.

Suomen Erillisverkot Oy (ERVE) toteaa lausunnossaan, että tarve viestintäverkon kriittisiä osia koskevalle määräykselle on Virve 2.0 -palveluiden käyttöönoton myötä entisestään korostunut. ERVE:n näkökulmasta olisi tärkeää selkeyttää eri lainsäädännöistä muodostuvaa mahdollista päällekkäistä ohjausta, sillä julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015, TUVE-laki) 14.1 § mukaan valtiovarainministeriö vastaa turvallisuusverkkotoiminnan yleishallinnollisesta, strategisesta, taloudellisesta ja tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjauksesta ja valvonnasta. ERVE katsoo, että määräystä ei tule soveltaa TUVE-lain tarkoittamaan turvallisuusverkkoon.

Traficom toteaa, että määräyksessä ei oteta kantaa siihen, missä määrin SVPL 244 a §:n sovelletaan viranomaisverkkoihin tai viranomaisviestintään liittyvään viestintäpalveluun kriittisinä erillisverkkoina, vaan tältä osin on kyse SVPL 244 a §:n 2 momentin tulkinnasta. Tulkintakysymykseen otetaan tarvittaessa kantaa erikseen.

Puolustusministeriön lausunnossa esitetään, että määräyksen valmistelussa tulisi ottaa huomioon, ettei SVPL:n valmistelussa ole huomioitu mikro-operaattoritoimintaa riittävästi. Samoja turvallisuuskriteeristöjä tulisi soveltaa niin mikro-operaattorien kuin isompien operaattorien toimintaan. – Traficom toteaa tämän osalta, että valmisteltava määräys koskee yhtäläisesti kaikenkokoisia teleyrityksiä ja SVPL 244 a § 2 momentissa tarkoitettuja ns. erillisverkkotoimijoita. SVPL 244 a §:n 2 momentti määrittelee, mihin erillisverkkoihin sääntelyä sovelletaan.

7 Verkon reunalla tuotettavia palveluita tukevat toiminnot

Lausunnonantajilla ei pääosin ollut huomautettavaa määräyksen verkon reunalla tuotettavia palveluita tukevia toimintoja koskevaan kohtaan. Tarkentavia kommentteja esittivät kuitenkin Nokia ja sisäministeriö.

Nokia katsoi, että määräyksessä oletetaan käytettävissä olevien suojauskeinojen riittävän määritellyn suojaustason saavuttamiseksi mutta on epäselvää, onko tavoitellun kaltainen kattava suojaus mahdollista normaalein suojauskeinoin, jos toiminto sisältää tarkoituksellisesti pahantahtoisia toiminnallisuuksia.

Traficom toteaa, että määräys edellyttää, että viestintäverkon kriittiset osat on suojattu toiminnallisuuden niihin mahdollisesti kohdistamalta haitalliselta liikenteeltä toteuttamalla verkossa tarvittavat luotettavat suojausmekanismit. Määräyksessä tai sen perusteluissa ei ole mahdollista määrittää niitä mekanismeja, joilla tästä voitaisiin käytännössä varmistua, eikä Traficom määritä niitä ennalta. Teleyrityksen tai erillisverkkotoimijan on määritettävä riittävät toimenpiteet, ja poikkeukseen vetoavalla on selvitysvelvollisuus suojaustoimenpiteiden riittävyydestä. Jos riittäviä suojaustoimenpiteitä ei ole osoitettavissa tai voida käytännössä toteuttaa, ei poikkeukseen tällöin voida vedota.

Traficom korostaa, että reunalaskennan ja reunan palveluita tuottavien tai ohjaavien komponenttien tietoturvallisuuden varmistaminen on olennaisen tärkeää, jos komponenteilla on pääsy tai mahdollisuus ohjata muun verkon liikennettä. Kyseisten komponenttien kattava (riskiperustainen) suojaaminen myös fyysisiltä tunkeutumisilta on erityisen tärkeää.

Sisäministeriö esitti, että poikkeuksen soveltamisen edellytykseksi tulisi lisätä, että "toiminnallisuus ei mahdollista sellaista pääsyä viestintäverkkojen tietoliikenteeseen, joka mahdollistaisi viestiliikenteen luottamuksellisuuden vaarantumisen tai tunkeutumisen syvemmälle viestintäverkkoihin".

Traficomin käsityksen mukaan sisäministeriön ehdotuksella pyritään saavuttamaan korkea varmuus siitä, että toiminnolla ei ole kykyä ohjata muuta verkkoa ja että tämä varmistetaan riittävillä kontrolleilla. Traficom katsoo, että määräyksen velvoitteet kuitenkin kattavat jo asiallisesti ehdotetun lisäyksen. Traficom on kuitenkin tehnyt tarkentavia kirjauksia perustelumuistioon. Ensinnäkin määräyksen 7 kohdan 1 alakohdan luetelma 1 edellyttää, että verkon muuhun tietoliikenteeseen ei pitäisi olla suoraan pääsyä, koska se edellyttää, että sitä ei ohjata toiminnolle eli sen kautta ei välitetä viestintäverkossa muuta liikennettä kuin mikä liittyy verkon reunalla tarjottavan muun kuin viestintäpalvelun toteuttamiseen. Luetelma 2 taas edellyttää luotettavien suojausmekanismien toteuttamista. Toinen alakohta kuvaa tarkemmin, mitä suojaustoimenpiteiltä toiminnallisesti edellytetään. Suojaustoimenpiteillä tulee varmistaa, että muuhun liikenteeseen ei päästä käsiksi myöskään välillisesti tunkeutumalla verkon ytimeen tai toisiin verkon funktioihin ja alustoihin taikka uudelleenohjaamalla liikennettä oikeudettomasti. Lisäksi, kuten perusteluissa mainitaan, suojausmekanismeilla tulee tunnistaa ja käsitellä myös esimerkiksi palvelunestohyökkäykset, jotka voisivat vaarantaa muun verkon palveluiden saatavuuden, vaikka ne eivät voisikaan johtaa luottamuksellisuuden vaarantumiseen tai tunkeutumiseen verkkoon.

Traficom ei ole toteuttanut Huawein ehdotusta lisätä määräykseen kohta, jonka nojalla viestintäverkon kriittiseksi osaksi ei katsottaisi sellaista osaa, jonka osalta teleyritys voi tietoturvakontrollien tai muiden vastaavien järjestelyiden avulla varmistua siitä, ettei kolmansilla osapuolilla ole mahdollisuutta vaikuttaa verkon tai palveluiden toimintaan kyseisen toiminnon tai toimenpiteen kautta. Traficomin näkemyksen mukaan viestintäverkon osaa ei voida todeta SVPL 244 a §:n mukaiseen määritelmään nähden ei-kriittiseksi pelkästään sillä perusteella, onko ulkopuolisella taholla hallintayhteys tai muu vaikutusmahdollisuus verkon osan kautta.

Voidaan arvioida, että verkon reunalla tapahtuvan laskennan ja palvelutuotannon sekä niiden tarvitsemien rajapintojen kehitys tulee muuttamaan verkon tarvitsemaa turvallisuusarkkitehtuuria. 3GGP Release 17 tuonee verkon arkkitehtuuriin muutoksia, jotka yhtäältä entisestään korostavat suojaustoimenpiteiden merkitystä ja toisaalta luovat haasteita niiden toteuttamiselle. Näitä muutoksia tullaan arvioimaan osana määräyksen jälkiseurantaa.