Määräys viestintäverkon kriittisistä osista

Sisällysluettelo

1. Määräyksen tausta ja säädösperusta

Sähköisen viestinnän palveluista annetun lain (917/2014, SVPL) 244 a §:ssä (laissa 1207/2020; HE 98/2020 vp) 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.

SVPL 244 a §:n 6 momentin mukaan Liikenne- ja viestintävirasto (jäljempänä myös Traficom) antaa tarkempia määräyksiä viestintäverkkojen, erityisesti niiden kriittisten osien, teknisestä määrittelystä 244 b §:ssä tarkoitetun verkkoturvallisuuden neuvottelukunnan suositukset huomioiden.

Viestintäverkon osan kriittisyyden arvioinnista voidaan SVPL 244 a §:n 1 momentin soveltamisessa erottaa sen ratkaiseminen, onko painavia perusteita epäillä kansallisen turvallisuuden tai maanpuolustuksen vaarantuvan viestintäverkkolaitteen käytön johdosta. Tämä määräys ei lainkaan koske tuon ns. *vaarantamisedellytyksen* arviointia, sillä 6 momentin mukaan Traficomin määräyksenantovaltuus koskee ainoastaan viestintäverkkojen kriittisten osien teknistä määrittelyä.

EU:n jäsenvaltiot julkaisivat 29. tammikuuta 2020 yhteisen keinovalikoiman turvallisuusriskien hallitsemiseksi ja ratkaisemiseksi. Määräyksellä toteutetaan osaltaan EU:n 5G-verkkojen turvallisuuteen liittyvää yhteisen keinovalikoiman toimenpidettä, joka koskee verkon kriittisten osien suojaamista.

SVPL 244 a §:n 6 momentin lisäksi Liikenne- ja viestintäviraston määräyksenantovaltuus perustuu SVPL 244 §:n 1, 3 ja 12 kohtiin. Pykälän 1 kohdan mukaan Liikenne- ja viestintäviraston määräykset voivat koskea muun ohella tärkeysluokittelua, 3 kohdan mukaan tietoturvallisuutta ja häiriöttömyyttä sekä niiden ylläpitoa, seurantaa ja verkonhallintaa sekä 12 kohdan mukaan teknistä dokumentointia ja tilastointia sekä näihin liittyvien asiakirjojen muotoa ja tietojen säilyttämistä.

2. Asiaan liittyviä muita Liikenne- ja viestintäviraston määräyksiä

Määräys *teletoiminnan tietoturvasta* (määräys 67) määrittelee tietoturvan toteuttamista koskevat vähimmäisvaatimukset. Määräyksellä pyritään siihen, että tietoturvan huomioiminen teleyrityksissä on osa jokapäiväistä toimintaa. Määräyksellä pyritään varmistamaan, että tietoturvatekijät huomioidaan rutiininomaisesti ja tehokkailla prosesseilla osana viestintäverkkojen ja -palvelujen toteutusta.

Määräys *viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista* (määräys 54) asettaa teleyrityksille minimivelvoitteet muun muassa viestintäverkkojen ja -palvelujen toteutuksessa käytettyjen laitteiden tehonsyötön varmistukselle, laitteiden ja yhteyksien varmistamiselle sekä laitteiden fyysiselle suojaamiselle.

Määräyksessä *teletoiminnan häiriötilanteista* (määräys 66) käsitellään erilaisia teletoiminnan häiriötilanteita. Määräys kattaa yhtäältä tilanteet, joissa teleyrityksen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus (*tietoturvahäiriö*), ja

toisaalta tapahtumat, jotka estävät viestintäpalvelun toimivuuden tai häiritsevät sitä olennaisesti (*toimivuushäiriö*). Määräys asettaa velvoitteita teleyrityksille koskien niin tietoturva- kuin toimivuushäiriöiden havaitsemista ja hallintaa kuin niistä ilmoittamista ja tilastointia.

Suositus *teletoiminnan varautumisesta* (suositus 311) antaa teleyrityksille neuvoja lain varautumisvelvoitteiden täyttämiseen. Suositus, joka on osin salassa pidettävä, ei ole yleinen, kaiken kattava varautumis-, jatkuvuus- tai valmiussuunnittelua ja niiden toteuttamista koskeva ohje, vaan siinä on nostettu esiin asiakokonaisuuksia, joita Liikenne- ja viestintävirasto suosittelee teleyrityksiä ottamaan huomioon osana varautumisvelvollisuutta ja olemassa olevia varautumiskäytäntöjä.

Määräys *viestintäverkkojen ja -palvelujen laadusta ja yleispalvelusta* (määräys 58) koskee viestintäverkkojen ja -palvelujen toimintavarmuuden, suorituskyvyn, luotettavuuden ja laadun mittaamista ja varmistamista. Määräyksessä on annettu tähän liittyen yleisiä kaikkiin yleisiin viestintäverkkoihin ja -palveluihin sovellettavia velvoitteita sekä puhelinpalveluja, internetyhteyspalveluja ja televisiopalveluja koskevia erityisvaatimuksia.

Määräys *hätäliikenteen teknisestä toteutuksesta ja varmistamisesta* (määräys 33) sisältää vaatimukset, joilla yleisten viestintäverkkojen osalta varmistetaan hätäpuheluiden ja hätätekstiviestien sekä niihin liittyvän hätäpalvelun kannalta olennaisen informaation siirtyminen viestintäverkoista hätäkeskuksiin. Määräyksen vaatimukset myös varmistavat hätäpuheluille normaaleja puheluja paremmat onnistumismahdollisuudet erilaisissa viestintäverkon ruuhka- ja häiriötilanteissa.

3. Määräyksen tavoite

Määräyksen tavoitteena on määritellä viestintäverkon kriittiset osat. Määräyksessä kuvataan hallituksen esityksen perustelujen sekä liikenne- ja viestintävaliokunnan mietinnön mukaisesti teknisesti verkon kriittiset osat eli ne verkon keskeiset toiminnot ja toimenpiteet, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä.

Määräys ohjaa teleyrityksiä ja sen soveltamisalaan kuuluvia erillisverkkotoimijoita verkkojen suunnittelussa, verkkolaitteiden hankinnassa sekä verkkojen rakentamisessa, ylläpidossa ja hallinnoimisessa. Määräyksellä edistetään kansallista turvallisuutta ja viestintäverkkojen tietoturvaa.

Määräys täsmentää niitä viestintäverkon osia, joihin sähköisen viestinnän palveluista annetun lain 244 a §:n mukainen velvoite olla käyttämättä viestintäverkkolaitetta voi kohdistua. Siten määräys selkeyttää kyseisen pykälän soveltamiskohteita.

4. Muut toteuttamisvaihtoehdot

4.1. Määräyksen soveltamisalaan kuuluvat verkot ja verkkotekniikat

SVPL 244 a §:n soveltamisalaan kuuluvat kaikki yleiset viestintäverkot sekä sellaiset yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden erillisverkot, jotka on liitetty yleiseen viestintäverkkoon.

Määräyksen valmistelussa arvioitiin, mitkä verkot olisi tärkeintä kattaa määräyksellä ensi tilassa, sillä määräyksen soveltamisalan laajentaminen on tarvittaessa myöhemmin mahdollista. Traficom kiinnitti arvioinnissa huomiota verkon osien kriittisyyden

määrittelyn kiireellisyyteen, vaikuttavuuteen ja määrittelystä aiheutuvaan työmäärään.

Määräyksen soveltamisalan kannalta keskeistä on, että niiden verkkojen osalta, joita määräys ei kata, verkon osien kriittisyys määräytyy suoraan lain yleislausekkeen (SVPL 244 a § 1 mom.) nojalla. Toisin sanoen se, että määräys ei määrittelisi tiettyjen verkkojen tai verkkotekniikoiden osalta niiden kriittisiä osia, ei tarkoittaisi, etteikö niidenkin osalta voida tarvittaessa osoittaa kriittiset osat. Voidaankin arvioida, että tekniikaltaan vakiintuneiden ja pitkään käytössä olleiden tekniikoiden osalta verkon omistajalle tai haltijalle on lähtökohtaisesti suhteellisen suoraviivaista arvioida, mitkä ovat verkon kriittiset osat. Viraston määräyksen tuottama lisäarvo taas on suurin tilanteissa, joissa yleislausekkeen soveltaminen voi olla haasteellista, kuten uusien verkkotekniikoiden osalta.

4.1.1. Kaikille viestintäverkoille yhteisten kriittisten osien määrittely

Traficom arvioi tarvetta ja mahdollisuutta määritellä kaikille viestintäverkoille kriittiset osat yhteisesti. Mikäli tällainen määrittely todetaan toteuttamiskelpoiseksi, sen etuna olisi kohtuullisella työmäärällä saavutettavissa oleva selkeyden lisääminen lain yleislausekkeen suoraan soveltamiseen nähden. Toisaalta tällainen määrittely jää välttämättä selvästi yleisemmälle tasolle, kuin mihin on mahdollista päästä verkkoteknologiakohtaisella määrittelyllä. Ottaen huomioon, että määräys helpottaisi tällöin lain soveltamista myös niiden verkkojen osalta, joiden kriittisiä osia ei erikseen määritellä, piti Traficom perusteltuna selvittää tarkasti, onko tällainen määrittely toteuttavissa määräykseltä vaadittavalla täsmällisyydellä. Tässä tapauksessa ei siis tarvittaisi erillistä määrittelyä esimerkiksi kiinteitä verkkoja varten.

Lisäksi yhteisten kriittisten osien määrittely täydentää verkkotekniikkakohtaisia määrittelyjä siten, että niiden kriittisten osien määrittelyssä on mahdollista välttää toistoa. Yhteisten kriittisten osien määrittely täydentää myös aukkoja sellaisten toimintojen osalta, joita ei ole erikseen määritelty niissä teknisissä määrittelyissä, joihin verkkoteknologiakohtaisissa määrittelyissä viitataan.

Määräysvalmistelussa Traficom kuuli näkemyksiä siitä, tulisiko yhteisten kriittisten osien määrittely rajata vain IP-pohjaisiin viestintäverkkoihin. Osa toimijoista katsoi, että piirikytkentäisiä verkkoja ei ole syytä rajata pois soveltamisalasta, koska yhteinen määrittely soveltuu suurelta osalta myös niihin. Osa toimijoista puolestaan katsoi, että IP-pohjaisiin verkkoihin kohdistuva rajaus voi aiheuttaa soveltamisongelmia. Myös Saksassa käytetty määrittelytapa on teknologianeutraali (ks. luku 4.3.1).

Traficom arvioi, että viestintäverkon kriittisten osien määrittely on mahdollista tehdä asianmukaisella tarkkuustasolla niin, että se soveltuu suureen osaan erilaisista viestintäverkoista. Etenkin IP-verkot ovat keskenään monelta kannalta siinä määrin samankaltaisia, että yhteinen yleinen viestintäverkon kriittisten osien määrittely soveltuu niihin varsin hyvin. Määrittelyä ei kuitenkaan rajata vain IP-pohjaisiin pakettikytkentäisiin verkkoihin, koska yhteinen määrittely voidaan laatia teknologianeutraalisti. Sikäli kuin yhteinen viestintäverkon kriittisten osien määrittely ei yksittäistapauksessa olisi sovellettavissa johonkin verkkoon, viestintäverkon kriittiset osat olisi määritettävä suoraan lain määritelmän perusteella, jos niitä koskien ei anneta erillistä määrittelyä. Asiaa käsitellään tarkemmin jäljempänä kriittisten osien määrittelytavan toteutusvaihtojen ja yksityiskohtaisten perustelujen kohdalla.

4.1.2. 2G- ja 3G-verkot

Toisen sukupolven (2G) matkaviestinverkkotekniikkoihin lasketaan vakiintuneesti esimerkiksi GSM-, GPRS- ja EDGE-tekniikat. Kolmannen sukupolven (3G) matkaviestinverkkotekniikoita ovat esimerkiksi UMTS ja HSPA. 2G- ja 3G-verkot hyödyntävät sekä piiri- että pakettikytkentäistä runkoverkkoa. Perinteinen puheliikenne reititetään piirikytkentäiseen verkkoon ja dataliikenne pakettikytkentäiseen verkkoon.

3G-tekniikasta ollaan luopumassa, eikä uusia komponenttihankintoja lähtökohtaisesti tehdä. Komponentteja ei hyödynnettäne laajasti modernimpien sukupolvien palveluissa, eikä tiedossa ole erityisiä kriittisiä käyttötapauksia. 3G-tekniikkaa ei käytetä myöskään erillisverkoissa.

2G-tekniikka saattaa pysyä käytössä hyvinkin pitkään, jolloin komponenttien elinkaaret tulevat täyteen ja niiden uusintatarvetta voi syntyä. Lisäksi 2G-tekniikalla on kriittisiä käyttötapauksia jatkossakin (esim. 2G IoT, hätäliikenne, eCall). Toisaalta teknologian maturiteetti on korkea ja sen monimutkaisuus huomattavasti pienempi kuin uudemmissa sukupolvissa.

Traficom arvioi, että näiden tekniikoiden osalta teleyritykset pystyvät määrittämään viestinverkon kriittiset osat riittävän selvästi määräykseen sisältyvän eri verkoille yhteisten kriittisten osien määrittelyn ja SVPL 244 a §:n yleislausekkeen perusteella. Tämän takia tarvetta yhteisiä kriittisiä osia täsmentävän, teknologiakohtaisen kriittisten osien määrittämiselle ei tältä osin ole.

4.1.3. 4G-verkot ja 5G Non-Standalone -verkot (5G NSA -verkot)

Traficom kiinnitti määräyksen soveltamisalaa arvioidessaan erityistä huomiota matkaviestinverkon 4G- ja 5G-tekniikkoihin. 4G-verkoilla tarkoitetaan tässä LTE-tekniikalla toteutettuja verkkoja.

5G NSA -verkon keskeinen käyttötapaus on tiedonsiirtokapasiteetin kasvattaminen radioverkon osalta. 5G NSA -verkko perustuu 4G-verkon EPC-ytimeen (Evolved Packet Core). 5G NSA -verkoissa ei vielä tapahdu paradigman muutosta verkon olemuksessa, eivätkä 5G-verkon uudet käyttötapaukset kehitysversioista huolimatta laajamittaisesti toteudu. 5G NSA -verkko päivittyy toiminnallisuuksiltaan elinkaarensa aikana 5G Standalone- eli 5G SA -verkoksi, jolloin siihen tullaan soveltamaan kaikilta osin 5G-verkon kriittisten osien määrittelyjä.

Traficom arvioi 4G-verkkojen osalta määräyksen soveltamisalaa. Jos 4G-verkon kriittiset osat määritellään, määräys kattaa ensinnäkin kokonaan LTE-teknologiaan perustuvat 4G-verkot. Toiseksi määräys voisi samalla kattaa myös 5G NSA -verkot niiden LTE-teknologiaan perustuvilta osilta (4G-verkon ydin eli EPC).

Verkon ytimen ja sitä kautta verkon kriittisten osien määrittely on 5G:tä aiemmissa sukupolvissa selväpiirteisempää ilman määräystäkin, mikä sinänsä vähentää erityisen määrittelyn tarvetta. Aiempien verkkojen tekniikka on varsin kypsä ja arkkitehtuuri vakiintunut. Toisaalta tämä tarkoittaa samalla, että kriittisten osien määrittelystä viranomaiselle aiheutuva työmäärä on arvioitavissa kohtuulliseksi. Tällöin ratkaisevaksi muodostuu, onko määrittelyn vaikuttavuus suuri.

4G-verkkoja tullaan näillä näkymin käyttämään laajasti kriittisissä toiminnoissa, kuten uudessa viranomaisviestintäpalvelussa (Virve 2.0) ja kriittisissä erillisverkoissa, mikä puoltaa voimakkaasti niiden kriittisten osien määrittelyä. Lisäksi 4G-verkon elinkaari jatkuu vielä pitkään, sillä 5G-verkot eivät lähiaikoina korvaa LTE-tekniikalla

toteutettua valtakunnallisten matkaviestinverkkojen laajaa peittoaluetta. 4G-verkot tulevat pitkään olemaan erittäin tärkeä osa suomalaisia viestintäverkkoja. Lisäksi on huomattava, että 5G NSA -verkoissa 5G-teknologiaan perustuva radioverkko tukeutuu 4G-verkon ytimeen, eli 4G-teknologia on kriittisessä roolissa myös 5G NSA -verkoissa. On myös huomattava, että 4G- ja 5G-verkkojen välillä on useita rajapintoja yhteentoimivuuden varmistamiseksi (EPC-5GC interworking), ja verkkojen välille voi muodostua keskinäisiä riippuvuuksia.

Kansainvälisenä vertailukohtana voidaan todeta, että Yhdistyneessä kuningaskunnassa on kiinnitetty teleyritysten huomiota 5G-verkkojen ohella 4G-verkkojen erityisen riskialttiisiin osiin.[1]

5G NSA -verkon 5G-komponentit kuuluisivat soveltamisalan kannalta 5G-verkon kriittisten osien määrittelyn piiriin. Esimerkiksi jos 5G-verkon jotkin osat määriteltäisiin kriittisiksi, ne olisivat sitä myös 5G NSA -verkon yhteydessä. Vastaavasti 5G NSA -verkkojen tapauksessa hyödynnettyjen 4G-verkon osien kriittisyyttä voitaisiin arvioida lähtökohtaisesti sen mukaan, mitä 4G-verkon osista määräyksessä määrättäisiin.

Edellä mainituilla perusteilla voidaan arvioida, että sekä 4G-verkkojen että 5G NSA -verkkojen LTE-tekniikkaan perustuvat kriittiset osat on perusteltua täsmentää määräyksessä. 4G- ja 5G-verkkojen kriittisten osien tarkempaa määrittelyä kannatettiin laajasti myös Traficomin määräysvalmistelussa saamissa näkemyksissä.

4.1.4. 5G-teknologiaan perustuvat verkot

Voidaan katsoa, että 5G-teknologian avulla toteutettavat verkot on tärkeää kattaa määräyksellä siltä osin kuin niiden kriittisten osien määrittely on tekniikan kehitykseen nähden mahdollista. Uusi SVPL 244 a § panee esitöiden mukaan täytäntöön EU:n 5G-verkkojen turvallisuuteen liittyvän yhteisen keinovalikoiman toimenpiteen, joka koskee verkon kriittisten osien suojaamista. 5G-verkkojen kriittisten osien määrittely olisi siten uuden säännöksen tavoitteiden kannalta keskeistä.

Uuden sääntelyn soveltamisen helpottamiseksi verkon kriittisten osien täsmentäminen olisi tärkeää nimenomaan 5G-verkkojen osalta. 5G-verkkojen rakentaminen on alkuvaiheissaan, ja lähitulevaisuudessa tehtävät suuret investoinnit määrittävät pitkälle tulevaisuuteen verkon turvallisuutta ja käytettyihin komponentteihin liittyviä riskejä. Siinä missä aiemmissa matkaviestinverkon sukupolvissa verkon ns. ytimen (core) määrittely on ollut suhteellisen suoraviivaista, on ytimen tai verkon muutoin kriittisten osien määrittely 5G-teknologialle tulkinnanvaraisempaa.

5G-verkon yksi keskeinen ero aiempaan nähden on uudelleen suunniteltu palveluväyläpohjainen ja ohjelmistokomponentteihin pohjautuva verkon ydin. Verkon ytimen funktioiden välinen liikenne tapahtuu vakioitua palveluväylää pitkin. Vakioitu palveluväylä mahdollistaa palveluntarjoajien kiinteän integroitumisen 5G-verkon ytimeen. Tämä mahdollistaa verkon mukautumisen siten, että verkko pystytään optimoimaan käyttäjien käyttämiä palveluita varten. Uusien komponenttien lisääminen palveluväylään sitä muuttamatta tulee olemaan mahdollista.

[1] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, kohta 11.a.iii. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.

5G-teknologian avulla toteutettavat uudet, yhteiskunnan ja käyttäjien turvallisuuden kannalta kriittiset toiminnallisuudet muuttavat koko verkon perusolemusta. Aiemmin suurelta osin tiedonsiirtoon ja fyysisiin verkkoelementteihin pohjautunut järjestelmä muuttuu pitkälti tietoa jalostavaksi ohjelmistopohjaiseksi pilvipalveluksi, jossa turvallisuuden varmistamiseksi on määriteltävä riittävät kontrollit. 5G-teknologian avulla tullaan toteuttamaan aikakriittisiä palveluita ja muita palveluita erityisiä käyttötapauksia varten. Aiemmasta poiketen itse verkossa voidaan toteuttaa erityisesti reunalaskentaan perustuvaa tiedonkäsittelyä, joka muuttaa verkon aiemmista verkoista poikkeavaksi.

Yllä todetun perusteella voidaan arvioida, että 5G-verkkojen kriittisten osien määrittely on perusteltua. Määrittelytyössä on kuitenkin varauduttava teknisten määrittelyjen ja teknologian jatkuvaan kehitykseen sekä siihen, että verkkojen tulevat käytännön toteutukset ovat vielä pitkälti täsmentymättömiä. Määrittelytyössä on myös tarpeen arvioida, millä aikajänteellä eri 5G-teknologioita olisi tulevaisuudessa otettavissa käyttöön kaupallisissa verkoissa.

Traficomin erikseen käynnistämässä referenssiarkkitehtuurityössä on tarkoitus määritellä yhteisiä toimintatapoja, prosesseja ja parhaita käytäntöjä, joilla varmistetaan matkaviestinverkkojen, lähinnä 5G-verkkojen, turvallinen käyttöönotto ja verkkojen hallinta. Työtä tehdään yhteistyössä laitevalmistajien ja matkaviestinverkon teleyritysten kanssa.

4.1.5. Matkaviestinverkon tukiasemat

Tukiasemat kokonaisuutena sisältävät tukiasemayksikön sekä päätelaitteiden tietoliikenteen vastaanottamiseen ja lähettämiseen käytettävän antenniyksikön. 4G- ja 5G-teknologioissa tukiasema välittää käyttäjien liikenteen suoraan operaattorin (teleyrityksen tai erillisverkon haltijan eli erillisverkkotoimijan) verkkorajapinnasta muihin tietoverkkoihin. Edellisen sukupolvien teknologioissa liikenne välitetään erillisen tukiasema- tai radioverkko-ohjaimen kautta.

4G- ja 5G-verkkojen tukiasemat toteuttavat osittain vastaavia toiminnallisuuksia (esim. radioresurssien hallinta) kuin aiempien sukupolvien tukiasema- ja radioverkko-ohjaimet (Base Station Controller, BSC 2G:ssä; Radio Network Controller, RNC 3G:ssä). Yksittäisen 4G- tai 5G-tukiaseman tapauksessa nämä siirtyneet toiminnallisuudet vaikuttavat kuitenkin suhteellisen pieneen käyttäjämäärään verrattuna esimerkiksi siihen, että 3G-verkossa yksi RNC saattaa ohjata jopa tuhatta tukiasemaa.

5G-verkon turvallisuusarkkitehtuurin perustana on verkon määrittely ja segmentointi erilaisiin turvallisuusvyöhykkeisiin sekä turvallisuusvyöhykkeiden välisen liikenteen kontrollointi sekä monitorointi. Verkko voidaan määritellä käsittelemään tukiasemaa siihen liittyvien riskien vuoksi luottamukseltaan alhaisemman turvallisuustason komponenttina.

Traficom katsoo, että 5G SA -verkon tukiasemien (gNodeB; myös ng-eNodeB[2]) erityispiirteitä voidaan arvioida vasta tulevaisuudessa, sillä tukiasemien tekninen kehitys on vielä kesken. Tukiasemien arkkitehtuurin määrittely ja käyttötapaukset ovat

[2] ng-eNodeB on Rel-15:ssa määritelty eNodeB, joka toimii yhdessä gNodeB:n kanssa, kun core-verkko on 5GC (3GPP TS 37.340, k. 4.1.3.1 ja 4.1.3.2). Tämä mahdollistaa 5G-coren mahdollistamien uusien toiminnallisuuksien toteuttamisen

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-tukiasemia (gNodeB/en-gNodeB) käytetään myös 4G-verkon ytimeen perustuvissa 5G NSA -verkoissa, jolloin 5G-tukiasemien keskeinen käyttötapaus on radioverkon tiedonsiirtokapasiteetin kasvattaminen. Lähtökohtaisesti 5G-verkon edellä kohdassa 4.1.4. kuvattuja uusia palveluita ei näissä verkoissa toteuteta.

Erillisverkkojen kohdalla yksittäisen tukiaseman merkitys osana verkkoa voi poiketa merkittävästi yleisistä viestintäverkoista. Traficom arvioi, että erillisverkkojen erityispiirteiden takia niiden tukiasemia on arvioitava erillisenä kysymyksenä. Asiaa käsitellään tarkemmin jäljempänä yksityiskohtaisten perustelujen kohdalla.

Tässä määräyksessä ei ole tarkoitus määrätä erikseen 4G- tai 5G-verkon tukiasemien kriittisyyden arvioinnista yleisen teletoiminnan osalta. Näin ollen niiden kriittisyyttä verkon osina olisi tarvittaessa arvioitava suoraan SVPL 244 a §:n 1 momentissa olevan viestintäverkon kriittisten osien määritelmän perusteella. Tukiasemien kriittisyyden arviointiin palataan tarvittaessa määräyksen jälkiseurannassa.

Samasta syystä Traficom arvioi, että on ennenaikaista ottaa kantaa toimintojen kriittisyyteen 5G-verkon mahdollistamien luotettujen Wi-Fi-verkkojen tai kiinteän verkon yhteyksiin perustuvan liitynnän (Wireline Access) osalta, jotka voivat tulevaisuudessa täydentää 5G-tukiasemiin perustuvaa liityntäverkkoa. Näihin liittyviä 3GPP:n määrittämiä toimintoja ovat ainakin Wireline Access Gateway Function (W-AGF) Trusted Non-3GPP Gateway Function (TNGF) ja Trusted WLAN Interworking Function (TWIF). Näiden mahdollisen tulevan käytön laajuutta ja toimintojen toteutusta on ennenaikaista arvioida tässä, joten niiden arviointiin palataan tarvittaessa määräyksen jälkiseurannassa.

4.1.6. Muut viestintäverkkoteknologiat

Traficom arvioi määräyksen valmisteluvaiheessa tarvetta määritellä erikseen eräiden muiden yleisimpien viestintäverkkotekniikoiden kriittiset osat määräyksessä. Edellä on käsitelty kaikille viestintäverkoille yhteisten kriittisten osien määrittelyä, mitä koskevan arvion lopputulos vaikuttaa myös tarpeeseen määritellä yksittäisten verkkotekniikoiden tasolla verkkojen kriittisiä osia.

Traficom arvioi, että joukkoviestintäverkkojen kriittisten osien määrittelylle ei ole erityistä tarvetta. Niiden määrittämisen voidaan arvioida olevan teleyrityksille selväpiirteistä ilman määräyksen tukea. Määrittelytarvetta vähentää osaltaan myös se, ettei joukkoviestintäverkoissa välitetä luottamuksellisia viestejä eikä niissä ole lähtökohtaisesti tarpeen kontrolloida käyttäjien pääsyä verkkoon, vaikka verkkojen toimivuus onkin varsin keskeistä.

(esim. QoS, verkon viipalointi) LTE-radioteknologian avulla. Ks. myös 3GPP TS 36.300, k. 24.1 sekä 3GPP TS 38.300 k. 4.1 ja 4.2.

Valmistelussa arvioitiin myös tarvetta määritellä kiinteiden laajakaistaverkkojen kriittiset osat erityisesti siitä syystä, että niiden komponentteja hyödynnetään myös 5G-verkkojen osalta siirto- ja runkoyhteyksinä. Tukiasemat toimivat liityntäverkon ja alueverkon yhteyksien varassa. 5G-verkkojen toteuttaminen ei kuitenkaan muuta kiinteiden verkkojen roolia mobiiliverkkojen toteuttamisessa kuin mahdollisesti 5G:n päälle siirtyvien entistä kriittisempien palvelujen myötä. Siirtoyhteyksien osalta puhe- ja muu liikenne voidaan salata, millä voidaan vähentää niistä aiheutuvia riskejä. Alue- ja liityntäverkon komponenttien osalta määrittelytarvetta ei arvioida yleisesti olevan, sillä niiden vaikutukset ovat varsin paikallisia. Kiinteän verkon kriittisten komponenttien määrittely voidaan arvioida suhteellisen selväpiirteiseksi myös ilman määräyksen tukea.

Kiinteiden langattomien verkkojenosalta Traficom arvioi, että määrittelytarve ei ole akuutti. Wi-Fi-tekniikan (IEEE 802.11 WLAN) avulla toteutetaan pääasiassa paikallisia verkkoja. 5G:ssä ja 4G:ssä mahdollistetaan esimerkiksi muita kuin matkaviestinverkon tekniikoita hyödyntäen tapahtuva liittyminen verkon ytimeen. Tällöin operaattori mahdollistaa esimerkiksi langattoman Wi-Fi-lähiverkon kautta tapahtuvan liittymisen suoraan 5G-palveluihin.[3] Vaikka esimerkiksi Wi-Fi-verkkoja voidaan hyödyntää sisäpeiton parantamiseksi ulkoisen rajapinnan kautta (Non-3GPP Access), ei verkon ytimen tarvitse kuitenkaan luottaa tällaisiin verkkoihin. Wi-Fi-teknologiaa ei myöskään lähtökohtaisesti käytetä kriittisissä verkoissa. Myös LoRa-verkko voi kuulua lain soveltamisalaan, ja sillä voi olla yhteiskunnan toiminnan kannalta tärkeitä käyttötapauksia. Traficom arvioi tässä vaiheessa, ettei määräyksen antaminen erityisesti näitä verkkoja koskien toisi merkittäviä hyötyjä siihen nähden, että niiden kriittisten osien määräytyminen jää joko lain yleislausekkeen varaan tai kaikkia viestintäverkkoja koskevan määrittelyn piiriin (ks. luku 4.1.1).

4.2. Verkkoarkkitehtuuriin, turvallisuusarkkitehtuurin tai tietoturvakontrolleihin liittyvien ratkaisujen vaikutus viestintäverkon osan kriittisyyttä koskevaan määrittelyyn tai arvioon

SVPL 244 a §:n soveltamisen kannalta voidaan pohtia kysymystä siitä, missä vaiheessa sen soveltamista tulisi arvioida verkkoarkkitehtuuriin, turvallisuusarkkitehtuuriin, tietoturvakontrolleihin tai muihin vastaaviin liittyviä ratkaisuja. Pykälän soveltamisen kannalta on erotettava arviot yhtäältä siitä, mikä on viestintäverkon kriittinen osa, ja toisaalta siitä, onko painavia perusteita epäillä kansallisen turvallisuuden tai maanpuolustuksen vaarantuvan viestintäverkkolaitteen käytön johdosta eli täyttääkö verkkolaitteen käyttäminen kyseisessä viestintäverkon osassa SVPL 244 a §:m 1 momentin 1. virkkeessä säädetyn ns. vaarantamisedellytyksen.

On huomattava, että pykälästä ja sen perusteluista ilmenee mahdollisuus, että verkon kriittisessä osassa käytettävää verkkolaitetta koskeva turvallisuuspuute voi tilanteesta riippuen olla mahdollista korjata muutoinkin kuin poistamalla laite verkosta, kuten esimerkiksi päivittämällä se[4]. Tämä viittaa siihen, että ainakin konkreettiset tietoturvakontrollit voisivat tulla parhaiten arvioitavaksi vasta osana vaarantamisedellytystä eivätkä jo siinä vaiheessa, kun arvioidaan, pidetäänkö kyseistä verkon osaa tai siinä käytettävää verkkolaitetta kriittisenä osana verkkoa. Toisaalta olisi ajateltavissa, että ainakin verkkoarkkitehtuuria koskevat seikat voisivat vaikuttaa siten,

[3] Selvitys 5G:n kyberturvallisuudesta. Yhteenveto. Liikenne- ja viestintävirasto. Traficomin julkaisuja 14.05.2019, s. 5.
[4] HE 98/2020 vp, s. 263: "Ennen päätöksen tekemistä Liikenne- ja viestintäviraston olisi kuultava viestintäverkon omistajaa tai muuta haltijaa ja varattava sille mahdollisuus korjata havaitut turvallisuuspuutteet. Tällä pyrittäisiin korostamaan erityisesti suhteellisuusperiaatteen toteutumista valvontatoimissa. Viestintäverkon omistaja tai muu haltija voisi korjata turvallisuuspuutteen esimerkiksi päivittämällä viestintäverkkolaitteen, jos se olisi riittävää tilanteen korjaamiseksi."

että kahden sinänsä samalla tekniikalla toteutetun verkon kriittiset osat eroaisivat joissakin tilanteissa tietyssä määrin toisistaan.

Mikäli arkkitehtuuriin tai tietoturvakontrolleihin liittyviä seikkoja otettaisiin määräyksessä huomioon jo viestintäverkon kriittisiä osia määriteltäessä, lisäisi se merkittävästi määräyksen kompleksisuutta. Se ei myöskään olisi omiaan edistämään määräyksen yhdenmukaista soveltamista eri yritysten taholta ja lisäisi valvonnan tarvetta. Mikäli kuitenkin ilmenee tarkasti rajattavissa oleva tilanne, joissa näillä seikoilla on ratkaiseva merkitys, voisi verkkoarkkitehtuurin tai tietoturvakontrollit huomioiva sääntelytekniikka kuitenkin olla perusteltavissa. Tämän johdosta määräyksessä käytetään lähtökohtaisesti määrittelytapaa, jossa viestintäverkon osien kriittisyyttä ei kytketä mihinkään tiettyihin teleyrityskohtaisiin ratkaisuihin. Sen sijaan Traficom on arvioinut, että näihin seikkoihin perustuva määrittelytapa sopii määräyksen kohtaan 7, jossa määritellään poikkeusmahdollisuus viestintäverkon kriittisiin osiin niiden toimintojen osalta, jotka tukevat verkon reunalla tuotettavia palveluita.

Jossakin määrin edellisestä erillinen kysymys liittyy saman verkkolaitteen käyttöön eri osissa viestintäverkkoa. Tietty konkreettinen verkkolaite voi soveltua käytettäväksi sekä kriittisissä että ei-kriittisissä viestintäverkon osissa.

4.3. Määräyksessä käytettävä viestintäverkon kriittisten osien määrittelytapa

4.3.1. Valittu määrittelytapa

SVPL 244 a §:n esityöt edellyttävät määräykseltä teknistä määrittelyä, joka ottaa huomioon viestintäverkkoja koskevat standardit. Esimerkiksi 3GPP:n määrittelyissä verkkojen osat määritellään tyypillisesti loogisella tasolla eli verkon osien funktioiden tai toiminnallisuuksien perusteella. SVPL 244 a §:n perustelujen (HE 98/2020 vp, s. 264) mukaan verkon kriittisiä osia koskevassa "määräyksessä kuvattaisiin teknisesti pykälässä tarkoitetut ja määritellyt verkon kriittiset osat eli ne toiminnot ja toimenpiteet, joiden avulla verkkoa ja siellä kulkevaa liikennettä keskeisellä tavalla hallitaan. –– Määräyksen teknisissä määrittelyissä olisi huomioitava kansainväliset standardit, joiden perusteella viestintäverkkoja suunnitellaan ja rakennetaan."

Yllä sanotun takia Traficom asetti toteuttamisvaihtoehtoja arvioitaessa ensisijaiseksi vaihtoehdoksi sen, että määräyksessä täsmennetään ne funktiot tai toiminnallisuudet, joita (ainakin) pidetään viestintäverkon kriittisinä osina siltä osin kuin määrittely tehdään verkkoteknologiakohtaisesti. 3GPP:n määrityksiin tukeutuva funktiopohjainen määrittely on valittu myös niissä Traficomin tiedossa olevissa maissa, joissa on pyritty teknisesti täsmentämään 5G- tai 4G-verkkojen kriittisiksi arvioitujen verkkojen osien piiriä, eli Ranskassa ja Yhdistyneessä kuningaskunnassa.[5]

5G-ja 4G-verkon kriittisten osien määrittelyn olisi tällöin oltava erillisiä, koska niiden toimintojen (funktioiden) nimet ja toiminnallisuudet eroavat niiden välillä. Funktiot ovat loogisia useaan sovellukseen hajautettuja eivätkä välttämättä täysin yksikäsitteisesti tosielämän toimintaympäristöstä rajattavia. Määrittelytavasta kuitenkin seuraisi, että kun yksittäisen ohjelmistokomponentin voidaan osoittaa toteuttavan osaksikaan jonkin kriittisen verkon osaksi määritellyn 3GPP-funktion, olisi komponentti katsottava verkon kriittiseksi osaksi, vaikkei se koko funktiota toteuttaisikaan.

[5] Ks. Yhdistyneen kuningaskunnan osalta alaviite 1 ja Ranskan osalta Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000039455672.

Tarkempi määrittely suoraviivaistaa sääntelyn soveltamista yksittäiseen verkkoon ja edistää määrittelyn yhdenmukaista soveltamista eri yrityksissä. Tarkemmassa määrittelyssä on myös mahdollista hyödyntää aiempia ulkomaisia esimerkkejä. Tarkempi määrittely osaltaan myös vähentää niitä viranomaistoiminnan kustannuksia, joita aiheutuisi yrityskohtaisen määrittelyn soveltamisesta ja tulkinnasta täytäntöönpanovaiheessa sekä riskiä siitä, että valvova viranomainen ei pitäisi yrityksen tulkintaa oikeana.

Teknologianeutraaliuteen pyrkivän yhteisten kriittisten osien luettelon osalta määrittely ei voi perustua teknisiin standardeihin, sillä ne ovat teknologiasidonnaisia. Myös EU:n yhteisessä keinovalikoimassa on pyritty määrittelemään verkon osien tärkeyttä niiden toteuttamien toiminnallisuuksien kautta, joskaan ei viittaamalla nimenomaan 3GPP:n määrittämiin 5G-verkon funktioihin.[6] Lisäksi Saksassa ja Yhdistyneessä kuningaskunnassa on pyritty eri tavoin määrittelemään laajasti eri verkkoihin soveltuvia kriittisiä toimintoja, joista Traficom pitää Saksan ratkaisua rakenteeltaan ja sisällöltään varsin käyttökelpoisena vertailukohtana tämän määräyksen kannalta.

Saksassa liittovaltion telealan valvontaviranomainen (Bundesnetzagentur, BNetzA) ja tietoturvaviranomainen (Bundesamt für Sicherheit in der Informationstechnik, BSI) ovat laatineet luonnoksen kriittisistä verkon toiminnoista.[7] Listaa ei luonnoksen mukaan ole tarkoitettu tyhjentäväksi, ja se on teknologianeutraali. Listalla mainitaan käyttäjien hallinta, kryptografiset mekanismit, verkkojen väliset rajapinnat, verkon palvelut, NFV ja MANO sekä virtualisointi, hallinta- ja muut tukijärjestelmät, verkkoliikenteen ohjaus ja lawful interception (telekuuntelu- ja valvonta). Listaa täsmennetään luonnoksessa lyhyesti kohta kohdalta.

Yhdistyneessä kuningaskunnassa taas on kansallisen kyberturvallisuuskeskuksen ohjauskirjeessä kiinnitetty teleyritysten huomiota tiettyihin kaikille verkoille yhteisiin erityisen riskialttiiksi nähtyihin funktioihin.[8] Nämä on ohjauskirjeessä määritelty seuraavasti: "IP Core, Security Functions, Operational Support Systems (OSS), Management and Authentication, Authorisation and Audit (AAA) functions, Virtualisation infrastructure (including Network Function Virtualisation Infrastructure (NFVI)), Orchestrator and controller functions (including Management and Network Orchestration (MANO) and Software Defined Networks (SDN) orchestrators/controllers), Network monitoring and optimization, Interconnection equipment, Internet gateway functions, Lawful Intercept related functions."

4.3.2. Viestintäverkon kriittisten osien määrittelytavan vaihtoehtojen arviointi

Valmisteluvaiheessa pyrittiin tunnistamaan myös muita, edelliselle alakohdalle vaihtoehtoisia tapoja määritellä viestintäverkon kriittiset osat. Julkaistuihin teknisiin määrittelyihin perustuvaan funktiopohjaiseen määrittelyyn liittyy riski siitä, että jos se tehdään suljettuna luettelona, joustamattomuuden takia joitakin kriittisiä kom-

[6] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. Liite 2, s. 39. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.
[7] Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial, luonnos saatavissa: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Listekritische-Funktionen.pdf.
[8] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, kohta 11.a. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks. Ks. myös kohta 12.

ponentteja voi jäädä määrittelyn ulkopuolelle. Tämä voi seurata siitä, että jo määritellyt funktiot eivät kattaisi 3GPP:n määritysten muuttumisen tai uusien toiminnallisuuksien kehittämisen takia kaikkia kriittisiä komponentteja. Tätä riskiä voidaan kuitenkin tarvittaessa pienentää käyttämällä määrittelyssä apuna rinnastuksia, muotoilemalla luettelo ei-tyhjentäväksi, olemalla viittaamatta tiettyihin standardiversioihin ja seuraamalla standardoinnin kehitystä, mikä lisää sääntelyn valvonnasta aiheutuvaa viranomaistyötä.

Funktiopohjainen, tarkka määrittely voikin osoittautua joustamattomaksi siinä tapauksessa, että samojenkin komponenttien kriittisyys osana eri toimijoiden verkkoja olisi tarkemmassa analyysissä katsottava ratkaisevassa määrin vaihtelevan esimerkiksi teleyrityksen valitseman verkko- tai turvallisuusarkkitehtuurin perusteella. 5G-verkkojen tietoturvaan vaikuttavat oleellisesti kutakin verkkoa koskevat toteutuskohtaiset ratkaisut, laitteiden fyysinen suojaus ja reunalaskentaympäristön turvaratkaisut, joita ei ole käsitelty 5G-standardissa.[9] Tarkkaan määrittelyyn tarvitaan myös todennäköisesti muutoksia useammin kuin yleispiirteiseen.

Toisaalta yleispiirteisempi määrittely olisi verkon omistajalle työläämpi soveltaa, koska lopputulos voi riippua sen verkon erityispiirteistä, ja arviota olisi päivitettävä muutosten tapahtuessa. Jos taas määrittely ei merkittävästi riippuisi yksittäisen teleyrityksen ratkaisuista, on valvonta yksinkertaisempaa ja on helpompi varmistaa, että sääntelyä sovelletaan yhdenvertaisesti.

Yleispiirteisempi määrittely voidaan kuitenkin toteuttaa useammalla eri tasolla, ja määrittelyn edut ja haitat riippuvat sen yksityiskohdista.

Ensiksi voidaan nostaa esiin, että Traficomin määräyksissä 54 ja 66 viestintäverkon ja -palvelun komponenttien tärkeys- ja häiriöluokittelu perustuu viestintäpalvelun tyyppiin, käyttäjämäärään ja maantieteellisen vaikutusalueen pinta-alaan. *Palvelun tyyppiin ja käyttäjävaikutuksiin perustuvan määrittelytavan* etuna olisi, ettei itse määräyksessä tarvittaisi tarkalle tekniselle tasolle menevää määrittelyä, joka vanhentuu nopeasti. Mikäli tämä vaihtoehto valittaisiin, täytyisi kuitenkin tarkemmin analysoida, täyttäisikö määrittelytapa määräyksenantovaltuuden vaatimukset; kysymystä arvioidaan jäljempänä tässä kohdassa sekä kohdassa 4.5.

Mahdollisen toimivuus- tai tietoturvahäiriön vaikutuksiin perustuvan määrittelytavan etuna olisi, että sen avulla saataisiin luokiteltua viestintäverkon komponentteja käyttäjävaikutuksen perusteella. Lisäksi määrittelytavan käytöstä on aiempaa kokemusta. Määrittelytavan huonona puolena on, että se ei sovellu ainakaan erillisverkkojen osien kriittisyyden määrittelyyn sellaisenaan, jolloin ne tarvitsisivat omat kriteerinsä. Määrittelytapa ei myöskään huomioi hyvin tilanteita, joissa komponentin kriittisyys perustuu viestinnän luottamuksellisuuden varmistamiseen, eikä tilanteita, joissa toiminnallisuus voi olla hajautettu useisiin laitteisiin, jolloin yksittäisen laitteen käyttäjämäärä saattaa jäädä alle käyttäjämäärään perustuvan rajan. Nykyisissä määräyksissä käytetyt kriteerit eivät siis sellaisenaan sovellu kriittisten komponenttien määrittelyssä käytettäväksi, sillä kriittisten osien määrittelyn tavoitteet ovat erilaiset kuin aiemmissa määräyksissä tehdyllä tärkeysluokittelulla. Onkin epäselvää, mitkä ne käyttäjävaikutuksiin perustuvat kriteerit voisivat olla, joihin perustuen verkon osien kriittisyys voitaisiin määritellä.

[9] Selvitys 5G:n kyberturvallisuudesta. Yhteenveto. Liikenne- ja viestintävirasto. Traficomin julkaisuja 14.5.2019, s. 9.

Käyttäjävaikutuksiin perustuva määrittely olisi periaatteessa sääntelyteknisessä mielessä mahdollista kirjoittaa nykyisissä Traficomin määräyksissä käytetyllä tavalla palvelun tyypin avulla. Tällä tarkoitetaan tässä sitä, että tärkeysluokittelu on kytketty tapahtumiin, jotka estävät esimerkiksi yleisen puhelinpalvelun, internetyhteyspalvelun tai tekstiviestipalvelun toiminnan tietyn suuruiselta käyttäjäjoukolta. Tällaisen määrittelytavan kääntöpuolena on kuitenkin, ettei se välttämättä toisi tarvittavaa selkeyttä viestintäverkon kriittisten osien määrittelyyn, kun määräystä soveltava verkon haltija joutuisi itse ratkaisemaan, millä komponenteilla voisi olla määräyksen edellyttämä käyttäjävaikutus. Traficom arvioi kuitenkin, että viestintäpalvelun tyyppiin perustuva määrittely soveltuisi täydentämään muita määrittelytapoja esimerkiksi 4G- ja 5G-verkon puhepalvelujen (Voice over LTE eli VoLTE ja Voice over New Radio, VoNR / 5G Voice) osalta, sillä määrittelytapaa käyttämällä voidaan välttää tarve määritellä komponentit erikseen määräyksessä; kysymys on matkaviestinverkon IP-multimedia-alijärjestelmän (IP Multimedia Core Network Subsystem, IMS) komponenttien määrittelystä. Tähän palataan jäljempänä yksityiskohtaisten perustelujen kohdalla.

Toisena vaihtoehtona voidaan tuoda esille, että suoria 3GPP:n määrittelemiä verkon ytimen funktioita *abstraktimmalla tasolla* olisi mahdollista kuvata ne toiminnot, joita toteuttavat verkon komponentit olisi katsottava kriittiseksi. Tällä tarkoitetaan määrittelytasoa, joka perustuisi sellaisiin käsitteisiin kuten liikenteen ohjaus ja reititys, käyttäjien tunnistaminen ja valtuuttaminen sekä kryptografisten avainten hallinta. Tällaisen määrittelytavan etuna on pienempi alttius muutostarpeille verrattuna määrittelytapaan, jossa on suoria viittauksia standardeissa tai teknisissä spesifikaatioissa määriteltyihin verkon osiin tai funktioihin. Tämän vastinparina on kuitenkin vähemmän yksiselitteinen soveltaminen käytäntöön. Jos on mahdollista suoraan viitata spesifikaatioissa määriteltyihin funktioihin, tällainen yleisempi taso voisi täydentää tarkkaa luetteloa ja vähentää niitä funktiotason määrittelystä aiheutuvia haittoja, joita on edellä kuvattu. Tällainen hieman yleisempi, verkon toimintoihin pohjautuva määrittely sopii sen sijaan hyvin tilanteeseen, jossa pyritään määrittelemään eri verkoille yhteisesti niiden kriittisiä osia, jolloin tarkemman tason viittaaminen standardeissa määriteltyihin funktioihin ei edes tule kyseeseen verkkojen erojen takia.

Kolmanneksi voidaan tuoda esille vaihtoehto, jossa teleyrityksen tai muun sääntelyn soveltamisalaan kuuluvan verkon omistajan tai haltijan pitäisi *itse tunnistaa ja kuvata*, mitkä verkkonsa komponentit se on todennut sääntelyn nojalla verkkonsa kriittisiksi osiksi. Tarkempi verkon kriittisten osien määrittely jäisi siis kunkin verkon omistajan tai haltijan tehtäväksi sääntelyn asettamien kriteerien pohjalta. Tämä vaihtoehto ottaisi huomioon sen ajateltavissa olevan tulkinnan, jossa arvio verkon osan kriittisyydestä voisi vaihdella riippuen yksittäisen operaattorin valitsemasta verkko- tai turvallisuusarkkitehtuurista tai sen toteuttamista konkreettisista tietoturvakontrolleista. Tällainen vaatimus voisi ensinnäkin kaikissa tapauksissa täydentää määrittelyjä siten, että se voisi edellyttää operaattoria nimenomaisesti tunnistamaan (määräyksen osoittamat) viestintäverkkonsa kriittiset osat ja dokumentoimaan ne. Toisaalta tällainen sääntelytekniikka voi olla osa määrittelymenettelyä, jossa määräyksen yleispiirteisimpien mutta teknisten arviointikriteerien perusteella operaattori määrittelee itse oman verkkonsa kriittiset osat.

Valmistelun aikana arvioitiinkin mahdollisuutta siihen, että Traficom antaisi kriittisten osien määrittelyprosessia koskevan määräyksen. SVPL 244 a §:n 6 momentin määräyksenantovaltuutuksen voisi tulkita tarkoittavan tai ainakin mahdollistavan sen, että viraston määräys koskee määrittelyä eli sitä prosessia, jossa kriittiset osat määritellään. Varsinaisesta määrittelystä oman verkkonsa osalta vastaisi teleyritys tai

erillisverkkotoimija. SVPL 244 a §:n perusteluissa kuitenkin todetaan, että "määräyksessä kuvattaisiin teknisesti pykälässä tarkoitetut ja määritellyt verkon kriittiset osat". Säännöksen tarkoituksena näyttääkin näin ollen olevan, että lähtökohtaisesti Traficom määrittelee viestintäverkon kriittiset osat. Tätä tukee perustelujen mainita siitä, että Traficom arvioisi säännöllisesti sääntelyn nojalla annettujen määräysten päivitystarvetta viestintäverkkoteknologian kehittyessä. SVPL 244 a § ei näin ollen vaikuta yksinään riittävän siihen, että toiminnanharjoittajia osallistettaisiin omien viestintäverkkojensa kriittisten osien määrittelyprosessiin. Toisaalta säännös ei myöskään vaikuta edellyttävän, että viraston antamassa määräyksessä määritellään tyhjentävästi viestintäverkon kriittiset osat.

Valmistelussa arvioitiin myös sitä, että SVPL:n muut säännökset toimisivat perustana viestintäverkon omistajan tai muun haltijan velvollisuudelle osallistua määrittelyprosessiin ja sen dokumentointiin. Uuden 244 a §:n perusteluissa todetaan, että "ehdotettu sääntely täydentäisi lain muita toimenpiteitä ja velvollisuuksia". Näin ollen lain 244 §:ssä olevia viraston yleisempiä määräyksenantovaltuuksia voidaan soveltaa uudessa 244 a §:n 6 momentissa olevan erityisen määräyksenantovaltuuden ohella. Viestintäverkon kriittisten osien määrittelyyn ja dokumentointiin soveltuvat erityisesti 244 §:n 1, 3 ja 12 kohdat, joiden mukaan Liikenne- ja viestintäviraston määräykset voivat koskea mm. tärkeysluokittelua, tietoturvallisuutta ja häiriöttömyyttä sekä niiden ylläpitoa, seurantaa ja verkonhallintaa, sekä teknistä dokumentointia ja tilastointia sekä näihin liittyvien asiakirjojen muotoa ja tietojen säilyttämistä.

Kansainvälisenä vertailukohtana voidaan tuoda esiin *Norjan malli*. Siinä ministeriöt tunnistavat kansallisesta turvallisuudesta annetun lain nojalla omalta toimialaltaan yhteiskunnan perustoiminnot sekä sellaiset merkittävät yritykset, jotka ovat välttämättömiä yhden tai useamman yhteiskunnan perustoiminnon toteuttamisessa. Nämä yritykset tekevät puolustusministeriön antaman yritysturvallisuusmääräyksen nojalla oman toimintansa osalta vahinkoarvioinnin ja toimittavat sen toimialansa ministeriölle. Ministeriö puolestaan luokittelee suojattavan kohteen tai infrastruktuurin yrityksen tekemän vahinkoarvion perusteella sekä ilmoittaa luokittelusta turvallisuusviranomaiselle. Vastuu suojattavien kohteiden ja infrastruktuurin suojelemisesta on yrityksellä.[10]

> Vahinkoarvion tekemiseen velvoittaa yritysturvallisuusmääräys, jossa myös annetaan perusteet arvioinnin tekemiselle. Vahinkoarvion laatimisen sekä sen dokumentoinnin tarkempi ohjeistus on kansallinen turvallisuusviranomaisen laatimassa yrityksille tarkoitetussa käsikirjassa.[11] Käsikirja jaottelee arviointiprosessin neljään eri vaiheeseen, joissa yritys 1) selvittää liiketoimintansa merkityksen yhteiskunnan perustoiminnoille, 2) kartoittaa kohteet ja infrastruktuuri, 3) tekee kohteiden ja infrastruktuurin vahinkoarvioinnin sekä 4) dokumentoi tekemänsä vahinkoarvioinnin.

[10] Lov om nasjonal sikkerhet (sikkerhetsloven; https://lovdata.no/dokument/NL/lov/2018-06-01-24); Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften, 57 §; https://lovdata.no/dokument/LTI/forskrift/2018-12-20-2053). Suojattavalla kohteella tarkoitetaan esim. rakennusta, tilaa, kuljetusvälinettä tai muuta materiaalia tai tällaisen osaa; infrastruktuurilla tarkoitetaan tiloja tai järjestelmiä, ja se sisältää usein kaksi tai useampia komponentteja ja niiden väliset yhteydet.
[11] Nasjonal sikkerhetsmyndiget: Håndbok i skadevurdering. https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-skadevurdering/om-denne-handboken/.

Kutakin arviointiprosessin vaihetta kuvataan käsikirjassa tarkemmin. Esimerkiksi kohdassa 3 ohjeistetaan vaiheittain määrittelemään, millaisia vahingollisia seurauksia kansallisille perustoiminnoille voi aiheutua, mikäli tunnistetut kohteet tai infrastruktuuri altistuvat vauriolle, tuhoutumiselle tai laittomalle haltuunotolle[12].

Norjan mallissa yritysten itsensä tekemä arviointityö on kiinteä ja olennainen osa viranomaisprosessia, jossa yhteiskunnan toiminnan kannalta kriittiset toimijat sekä näiden toiminnan kannalta kriittiset kohteet tunnistetaan, arvioidaan ja luokitellaan. Malli perustuu lakiin, määräykseen sekä prosessia kuvaaviin ohjeisiin ja käsikirjoihin. Määrittelytyössä korostuu vuorovaikutteisuus ja se, että yritykset ovat parhaita asiantuntijoita omien kohteidensa ja niiden haavoittuvuuden arvioimisessa.

Norjan tyyppinen sääntelyratkaisu olisi osittain toteutettavissa Suomessa siten, että viraston määräyksellä annettaisiin ensiksikin kaikille toimijoille yhteiset kriteerit siitä, mitä ainakin on pidettävä kriittisinä osina. Toiseksi toimijoiden voitaisiin edellyttää arvioivan itse, onko niiden verkoissa käytössä sellaisia osia, jotka ovat kriittisiä toimintansa puolesta määräyksen tai jo lain yleissäännöksen (244 a § 1 mom.) nojalla. Toimijan olisi dokumentoitava, mitkä viestintäverkkonsa osat se on määritellyt kriittisiksi. Traficomilla olisi oikeus saada tämä dokumentaatio SVPL 315 §:ssä säädetyn yleisen tiedonsaantioikeutensa nojalla. Traficomin määräyksellä ei kuitenkaan voida asettaa velvoitetta luovuttaa dokumentaatio viranomaiselle säännöllisesti tai ennakollisesti silloin, kun uusia komponentteja otetaan käyttöön, vaan tämä edellyttää viranomaisen pyyntöä.

Voidaan arvioida, että funktiopohjaiselle listaukselle ei löytynyt kokonaan korvaavia vaihtoehtoja haluttaessa määritellä kriittiset osat nimenomaan tietylle verkkoteknologialle. Muut tunnistetut vaihtoehdot eivät olisi yhtä selkeitä eikä niillä saavutettaisi selkeitä etuja funktiopohjaiseen määrittelyyn nähden. Yleisemmän tason määrittely arvioidaan kuitenkin sopivaksi täydentämään verkkotekniikkakohtaista yksityiskohtaista määrittelyä.

4.4. Tukiasemien ja muiden komponenttien hallintajärjestelmät

Tukiasemien hallintajärjestelmällä on mahdollista vaikuttaa käyttäjien verkkoon pääsyyn tai jopa estää se kokonaan sekä tukiasemien välittämään liikenteeseen esimerkiksi hidastamalla sitä. Voidaankin arvioida, että tukiasemien hallintajärjestelmä voi olla viestintäverkon kriittinen osa siinäkin tilanteessa, jossa sen hallitsemaa yksittäistä tukiasemaa itsessään ei katsottaisi viestintäverkon kriittiseksi osaksi. Sama voi koskea muita elementtien hallintajärjestelmiä.

Tyypillisesti tukiasemien laitetoimittaja toimittaa myös niiden hallintajärjestelmän. Rajapinnat radioverkon ja hallintajärjestelmän välillä ovat pääosin suljettuja, vaikka eri laitetoimittajien hallintajärjestelmillä voi olla rajoitetusti mahdollista hallita myös toisen valmistajan tukiasemaelementtejä. Toimialalla on meneillään kehitystä järjestelmien ja niiden rajapintojen avaamiseksi Open RAN -hankkeessa.

Valmistelussa arvioitiin erityisesti tukiasemien hallintajärjestelmän kriittisyyttä ja asianmukaista tapaa määritellä se määräyksessä. Erilaisia arvioituja vaihtoehtoja olivat

[12] Vaiheessa 3 yrityksen on määrä selvittää, (i) millaisia vahingollisia seurauksia kansallisille perustoiminnoille voi aiheutua, mikäli tunnistetut kohteet tai infrastruktuuri katoavat kokonaan tai osittain, (ii) kuinka kauan kohteet tai infrastruktuuri voi olla kokonaan tai osittain poissa käytöstä ennen kun sillä on vaikutusta kansallisille perustoiminnoille, (iii) miten kohteet tai infrastruktuuri voidaan korvata tai palauttaa kohtuullisen ajan kuluessa, sekä (iv) kuinka kohteiden tai infrastruktuurin laiton haltuunotto voi vaikuttaa väestön perusturvallisuuteen.

A) tukiasemien hallintajärjestelmän määrittely sellaisenaan kriittiseksi, B) tapauskohtaista arviointia vaativa hallintajärjestelmän kriittisyyden arviointi ja C) tukiasemien hallintajärjestelmän ei-kriittisyyden kytkeminen tiettyihin kriteereihin.

Vaihtoehto C hylättiin sillä perusteella, että se näyttäisi edellyttävän tarvittavien tietoturvakontrollien ja muiden asiaan vaikuttavien kriteerien määrittämistä määräyksessä ennakolta. Traficom katsoo, ettei tiedossa ole sopivia ennakolta määritettäviä kriteerejä, joilla voitaisiin varmuudella poissulkea järjestelmän kriittisyys. Konkreettisten tietoturvakontrollien merkitys sopii parhaiten arvioitavaksi vasta siinä vaiheessa, kun ratkaistaan, täyttyykö SVPL 244 a §:n 1 momentin ensimmäisessä virkkeessä kuvattu ns. vaarantamisedellytys.

Vaihtoehtoa A ei valittu, koska tukiasemien hallintajärjestelmää ei nähty mahdolliseksi määritellä poikkeuksetta viestintäverkon kriittiseksi osaksi. Määräyksessä on asianmukaista määritellä viestintäverkon kriittisiksi osiksi ainakin ne verkonhallintajärjestelmät, jotka liittyvät viestintäverkon kriittisten osien hallintaan. Hallinnan kohteena olevat komponentit eli tukiasemat eivät olisi välttämättä itsessään viestintäverkon kriittisiä osia, vaan niiden kriittisyyttä olisi arvioitava tarvittaessa suoraan SVPL 244 a §:n 1 momentin määritelmää vasten, koska tässä määräyksessä ei vielä määrätä tukiasemien kriittisyyden arvioinnista. Tämän johdosta tukiasemien hallintajärjestelmien kriittisyyttä silloin, kun tukiasemat eivät olisi kriittisiä, tulisi arvioida erillisin perustein. Tukiasemien hallintajärjestelmän kriittisyyttä koskeva arvio riippuu viime kädessä siitä, täyttääkö se yksittäistapauksessa viestintäverkon kriittisen osan määritelmän. Tähän voivat vaikuttaa tietyn konkreettisen tilanteen erityispiirteet esimerkiksi sen suhteen, kuinka suurta joukkoa tukiasemia kyseinen hallintajärjestelmä ohjaa.

Vaihtoehto B osoittautui näin ollen toteutuskelpoiseksi vaihtoehdoksi. Tällöin muiden kuin viestintäverkon kriittisten osien hallinta- ja valvontajärjestelmät katsottaisiin määräyksen mukaan viestintäverkon kriittiseksi osaksi, kun ne voivat olennaisesti vaikuttaa verkkoon pääsyyn tai verkossa kulkevaan liikenteeseen. Arvion tekeminen aiheuttaa jonkin verran hallinnollista taakkaa teleyrityksille ja erillisverkkotoimijoille, mutta sen vastinparina on, että tukiasemien hallintajärjestelmää voidaan pitää tapauskohtaisesti ei-kriittisenä.

4.5. Matkaviestinverkon puhelinpalvelut

IP-pohjaisissa 4G- ja jatkossa 5G-matkaviestinverkoissa toteutetaan pakettikytkentäinen yleinen puhelinpalvelu verkon ytimen IP-multimedia-alijärjestelmän (IP Multimedia Core Network Subsystem, IMS) avulla. Aiemman sukupolven verkoissa yleinen puhelinpalvelu on piirikytkentäinen.

Traficomin määräyksen valmistelun yhteydessä saamissa näkemyksissä IP-pohjaisia puhelinpalveluja pidettiin pääosin kriittisinä ja katsottiin, että niihin liittyvät viestintäverkon osat tulisi määritellä erikseen kriittisiksi. Puhelinpalvelun saatavuus samoin kuin puheluiden luottamuksellisuus ovat erittäin tärkeitä. Matkaviestinverkon yleisen puhelinpalvelun saatavuuden kannalta voidaan tuoda esille, että toistaiseksi puhelut voidaan normaalisti toteuttaa myös 2G- tai 3G-verkossa. Osa valmisteluun osallistuneista tahoista näkikin 2G- tai 3G-verkon palveluiden turvaavan äänipuhelut toistaiseksi. Traficom katsoo, että IMS Core on silti perusteltua määritellä tarvittavilta osin viestintäverkon kriittiseksi osaksi. Uudemmilla verkkotekniikoilla toteutetuissa puhelinpalveluissa sillä on suuri merkitys viestinnän luottamuksellisuuden kannalta, sillä sen kautta voi olla mahdollisuus päästä käsiksi sekä salaamattomaan puheliiken-

teeseen että käyttäjän sijaintitietoihin. Kaikissa tilanteissa ei myöskään ole mahdollista käyttää piirikytkentäisiä palveluita sen sijasta, joten myös saatavuuden kannalta IMS Core on merkittävä.

Traficom katsoo, että yleisen puhelinpalvelun merkittävyyden takia on perusteltua, että siihen liittyvien IP-pohjaisten toimintojen kriittisyys määritellään erikseen. Piirikytkentäisen puhelinpalvelun toteuttamiseen liittyvien toimintojen ja toimenpiteiden kriittisyyttä arvioitaisiin määräykseen sisältyvän eri verkkojen yhteisten kriittisten osien luettelon sekä tarvittaessa suoraan SVPL 244 a §:n 1 momentin perusteella.

Kuten edellä viestintäverkon kriittisten osien määrittelytapaa koskevassa luvussa 4.3.2 on todettu, viestintäpalvelun tyyppiin perustuva määrittely voi sopia täydentämään muita määrittelytapoja. Tällaista määrittelytapaa käyttämällä voidaan välttää tarve määritellä IMS:n kriittiset komponentit erikseen määräyksessä.

Traficom arvioi, että 3GPP:n määrittelyjen hyödyntäminen on asianmukaista myös IMS Coren osalta, koska se muodostaa yhteisen pohjan eri teleyrityksille. Tällä perusteella hylättiin vaihtoehto, jossa olisi määritelty pelkästään IP-pohjaisen yleisen puhelinpalvelun toteuttamiseen matkaviestinverkossa liittyvät toiminnot kriittisiksi, sillä tämän kaltaiseen määrittelyyn liittyy rajanveto-ongelmia. Traficomin saamissa näkemyksissä kannatettiin IMS:n määrittelyn kohdalla myös 3GPP:n funktiotasolla tapahtuvaa määrittelyä, joskin osa vastaajista koki, että kriittiset osat voidaan määritellä myös kokonaisuutena. Traficom katsoo, että IMS Coren kriittisten toimintojen määrittely yksityiskohtaisesti ja funktiopohjaisesti lisäisi huomattavasti ja tarpeettomasti määräyksen yksityiskohtaisuutta, sillä IP Multimedia Core Network Subsystemin tekniseen määritykseen sisältyy huomattavan monimutkainen toimintojen kokonaisuus. Tämän takia Traficom päätyi ratkaisuun, jossa yhdistetään viestintäpalvelun tyyppiin ja 3GPP:n teknisiin määrittelyihin perustuva määrittelytapa. Tällaisen määrittelytavan arvioidaan silti olevan riittävän selkeästi sovellettavissa teleyrityksissä.

4.6. Kriittiset erillisverkot

SVPL 244 a §:n 2 momentin mukaan "Mitä 1 momentissa säädetään, sovelletaan myös ydinvoimaloiden, satamien, lentokenttien ja vastaavien yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden yleiseen viestintäverkkoon liitettyyn erillisverkkoon". Näihin verkkoihin viitataan termillä "kriittiset erillisverkot" ja kyseisten verkkojen omistajiin tai haltijoihin termillä "erillisverkkotoimija". SVPL 244 a § ei ota kantaa siihen, millä teknologialla kriittinen erillisverkko on toteutettu, vaan kriittinen erillisverkko voi olla kiinteä tai langaton.

4G- ja 5G-verkkoja voidaan toteuttaa paikallisiin tarkoituksiin mukautettuina erillisinä verkkoina. Tällaisia kohteita voivat olla esimerkiksi oppilaitokset, sairaalat, kauppakeskukset, tapahtumakeskukset ja tehtaat. Paikalliset räätälöidyt verkkototeutukset voivat periaatteessa hyödyntää verkoissaan valtakunnallisilta operaattoreilta vuokrattuja tai tähän käyttöön mahdollisesti erikseen osoitettuja taajuuksia tai toimia luvasta vapailla taajuuskaistoilla. Paikallisen toimijan tiloihin ja ympäristöön tuodulla reunalaskennalla voi olla keskeinen rooli erityispalveluiden sisällön ja laskentatoimintojen toteutuksessa.[13]

[13] Selvitys 5G:n kyberturvallisuudesta. Yhteenveto. Liikenne- ja viestintävirasto. Traficomin julkaisuja 14.05.2019, s. 8.

Paikallisia 4G- tai 5G-verkkoja voidaan periaatteessa toteuttaa hyvin erilaisilla malleilla (deployment models) 3GPP:n määritysten mukaisilla arkkitehtuureilla.[14] Näihin verkkoihin voidaan viitata teknisissä määrittelyissä käsitteellä non-public network, NPN. Standalone NPN -tapauksessa verkon funktiot toteutetaan kokonaan paikallisesti. Verkosta voi olla yhteys yleiseen viestintäverkkoon palomuurin lävitse. Lisäksi mahdollisia ovat erilaiset yleisen viestintäverkon ja NPN:n yhdistelmät, joissa jotkin toiminnot toteutetaan paikallisesti ja jotkut yleisessä viestintäverkossa. NPN on tällöin yleisestä viestintäverkosta riippuvainen. Esimerkiksi vain radioverkko voi olla jaettu, mutta myös control plane (ohjausliikenne) voi olla toteutettu yleisen viestintäverkon puolella. Toteutustapoina voidaan käyttää mm. liikenteen ohjaamista paikalliseen dataverkkoon (local breakout), verkon viipalointi tai oma yhteysosoite eli APN (access point name).

Traficom arvioi valmisteluvaiheessa seuraavia vaihtoehtoja:

A) Kriittisille erillisverkoille ei määritellä erikseen niiden kriittisiä osia, vaan ne määräytyvät samojen perusteiden mukaisesti kuten yleisten viestintäverkkojen kohdalla

B) Määritellään kriittisten erillisverkkojen kriittiset osat itsenäisesti

C) Täydennetään yleistä kriittisten osien määrittelyä tarvittaessa kriittisiä erillisverkkoja koskevilla täsmennyksillä.

Vaihtoehto B hylättiin sillä perustella, että se johtaisi tarpeettomasti päällekkäisten määrittelyjen kirjoittamiseen, sillä verkoissa hyödynnetään samoja teknologioita kuin yleisissä viestintäverkoissa. Traficom arvioi, että kriittisten osien piiri ei voi olla ainakaan suppeampi kuin yleisten viestintäverkkojen kohdalla, jolloin tarkemmin arvioitavaksi jäivät vaihtoehdot A ja C.

Traficom arvioi, että määräystä tulee soveltaa lähtökohtaisesti sellaisenaan myös kriittisten erillisverkkojen kriittisten osien määrittelyyn. Yleisten viestintäverkkojen ja erillisverkkojen arkkitehtuurissa tai toiminnallisuuksissa ei arvioida olevan suuria periaatteellisia eroja. Erillisverkkojen ominaispiirteiden takia tukiasemien osalta arvioidaan kuitenkin tarvittavan täydentävää sääntelyä (ks. luku 4.1.5 verkon tukiasemista ja yksityiskohtaisen perustelujen kohta 3). Muita erillisverkkojen kriittisten osien määrittelyyn vaikuttavaa erityistä täsmennystarvetta ei määräyksen valmistelun yhteydessä ilmennyt. Näin ollen päädyttiin vaihtoehtoon C.

4.7. Verkon reunalla tuotettavia palveluita tukevat toiminnot

Reunalaskennan avulla voidaan tuottaa tietojenkäsittelypalveluita 5G-verkon reunalla tilanteissa, joissa edellytetään esimerkiksi hyvin alhaista viivettä. Reunalaskenta mahdollistaa useiden eri palvelukokonaisuuksien toteuttamisen samalla alustalla. Palvelukokonaisuuden voi muodostaa yksi tai useampi työkuorma, jota tuotetaan alustalla virtualisoituna.[15]

[14] Ks. esim. 5G-ACIA: 5G Non-Public Networks for Industrial Scenarios; GSA: Private LTE & 5G Networks Report; ja Ericsson: Critical capabilities for private 5G networks.
[15] Reunalaskentaan liittyviä komponentteja on kuvattu esimerkiksi dokumentissa ENISA Threat Landscape for 5G Networks, k. 3.9.

Reunalaskennan ja verkon ytimen välisten rajapintojen voidaan nähdä olevan erityisen alttiina hyökkäyksille, ja niiden vaikutus koko verkon toimintaan voi olla suuri. Reunalaskennan keskeinen riski on ajoalustan hyväksikäyttö muuhun verkkoon tai toisiin työkuormiin tunkeuduttaessa tai palvelunestohyökkäys muualle verkkoon. Riskien keskeiset toteutumiskeinot voivat olla ohjelmallinen tunkeutuminen toisen työkuorman, internet- tai radiorajapinnan taikka laitteeseen tapahtuvan fyysisen pääsyn kautta.

Reunalaskentaa varten verkon ytimen toimintoja voidaan viedä verkon reunalle tai muutoin lähemmäs verkon käyttäjiä. Reunalaskentaa varten verkon reunalla voidaan toteuttaa verkon ytimen toimintoja, esimerkiksi 5G-verkon UPF-toiminto (User Plane Function) tai sen paikallinen kopio tai muita ytimen toimintoja, jotka on määräyksen kohdassa 6 määritelty oletusarvoisesti verkon kriittisiksi osiksi. Kun käyttäjäliikennettä halutaan ohjata ja purkaa se verkon reunalla reunalaskentaa varten, on UPF toteutettava siellä. Tämä edellyttää rajapintoja verkon varsinaiseen ytimeen. Tämän takia seuraavassa arvioidaan erityisesti UPF:ää ja tuodaan esiin perusteet sille, miksi UPF on oletusarvoisesti viestintäverkon kriittinen osa myös verkon reunalla toteutettuna.

UPF:n keskeinen rooli käyttäjien liikenteen hallinnassa ja monitoroinnissa verkon reunalla tekee sen oletusarvoisesti kriittiseksi toiminteeksi 5G-verkossa myös verkon reunalla. UPF toteuttaa myös muita kriittisiä palveluita, kuten käyttäjien liikenteen ohjaamisen, suodattamisen, monitoroinnin tai sen edelleen reitityksen tarvittaessa paikalliseen dataverkkoon tai internetverkkoon N6-rajapinnan avulla. UPF tuottaa palveluita ja ohjaa liikennettä RAN-verkosta ja muista kuin 3GPP-verkosta tuleville mobiiliverkon käyttäjille. UPF:llä on myös keskeinen rooli käyttäjän liikenteen telekuuntelussa sekä laskutustietojen keräämisessä. UPF voi olla kaikelle dataliikenteelle yleisesti käytössä oleva funktio, sessiokohtainen tai viipalekohtainen. Se voidaan myös toteuttaa reunalaskennan omassa alustassa, johon käyttäjän liikenne ohjataan N6-rajapintaa pitkin.

Yhtäältä UPF päättää käyttäjän liikenteen ohjauksesta, monitoroinnista ja tarvittaessa liikenteen terminoinnista paikalliseen verkkoon tai dataverkkoon, jolloin tärkeää on se, kuinka UPF:n turvallisuus itsessään on varmistettu. UPF:n keskeisiä turvallisuustoimintoja käyttäjän liikenteen kannalta ovat mm. DPI (Deep Packet Inspection), salaustoiminnot sekä telekuuntelun mahdollistaminen verkon reunalla tapahtuvaan liikenteeseen.

Toisaalta UPF vuorovaikuttaa myös verkon ytimen käyttäjäistuntoja hallitsevan Session Management Function (SMF) -toiminnon kanssa, joka on suoraan yhteydessä SBA-palveluväylään, jonka turvallisuus on kriittinen koko verkon turvallisuuden kannalta. UPF vuorovaikuttaa verkon muiden funktioiden kanssa, ja näiden käyttötapaukset voivat vaihdella esimerkiksi sessio-, viipale- tai sovellusperusteisesti. UPF vaatii yhteyden verkon yhteiseen SMF:ään, jotta käyttäjien liikenne voidaan siirtää yhdestä UPF:stä toiseen, jos käyttäjä liikkuu esimerkiksi usean eri maantieteellisesti sijoitetun funktion toteutuksen välillä. Kyse on siis siitä, onko verkon varsinainen ydin suojattavissa verkon ydintoimintojen paikallisilta toteutuksilta.

Koska UPF:n merkitys verkon osana on potentiaalisesti suuri, on määräyksessä asetettava korkea kynnys katsoa se ei-kriittiseksi verkon reunallakin toteutettuna. Arvioon vaikuttavia asioita voivat olla ainakin se, että toiminto palvelee vain tiettyjä käyttäjiä eikä sen kautta tarjota yhteyksiä yleiseen viestintäverkkoon kuten internetiin. Arvioon voi vaikuttaa myös se, miten paikallisten toimintojen resurssipyynnöt

käsitellään ja miten niitä valvotaan sekä se, käsitelläänkö paikallista toimintoa ei-luotettuna ydinverkon tietoturvan kannalta. Traficom on arvioinut seuraavia vaihtoehtoja.

A) UPF ja muut core-funktiot määritellään aina verkon kriittiseksi osaksi eli myös silloin, kun ne palvelevat verkon reunalla tuotettavia palveluita.

Tällaisen määrittelytavan etuna olisi selkeys ja määräyksen yksiselitteinen soveltaminen. On kuitenkin ajateltavissa, että näiden toimintojen määrittely viestintäverkon kriittiseksi osaksi jossain määrin vaikuttaa niiden käyttöönottoon ja teleyritysten päätöksiin käyttämistään laitevalmistajista. Mahdollisten toimittajien määrä esimerkiksi verkon reunalla toteuttavalle UPF-toiminnolle on kuitenkin suuri, sillä ne eivät rajoitu tunnetuimpiin laitevalmistajiin.

Tämä määrittelytapa olisi varmempi suhteessa epävarmuuteen siitä, kuinka merkittäväksi verkon reunalla tapahtuva ohjaus tulee lopulta olemaan 5G-verkossa ja mihin reunalaskentaa tullaan käytännössä käyttämään. On ajateltavissa, että verkon toimintojen siirtyminen reunalle voi muodostua hyvinkin yleiseksi, kun nopea vasteaika ja käytettävissä olevan kapasiteetin optimointi on olennaista, jolloin tämä määrittelytapa varmistaisi sen, että nämä toiminnot eivät jää SVPL 244 a §:n soveltamisen ulkopuolelle.

B) Määritellään poikkeus, jonka mukaan verkon reunalla tuotettavia palveluita tukevat toiminnot eivät ole viestintäverkon kriittisiä osia tietyin ehdoin.

Tämä vaihtoehto edellyttää, että määräykseen laaditaan vähintään yleispiirteiset kriteerit, joilla toiminto voidaan katsoa ei-kriittiseksi. Haasteena vaihtoehdossa on sellaisten kriteerien laatiminen, joilla voidaan varmistua siitä, että toiminto ei täytä viestintäverkon kriittisen osan määritelmää. Konkreettisia keinoja suojausmekanismien toteuttamiseen ei ole mahdollista määrittää etukäteen, vaan se jäisi teleyrityksen osaksi. Tarvittavat suojausmekanismit tulevat myös riippumaan siitä, millä tavoin näitä toimintoja käytetään ja miten tekniikka kehittyy esimerkiksi sen suhteen, miten toimintojen rajapinnat muihin ydinverkon toimintoihin tullaan tulevaisuudessa järjestämään[16]. Tiedossa ei myöskään ole, mahdollistaako nykyinen tekniikan taso riittäviä suojausmekanismeja, jolla tästä voidaan varmistua. Kynnys katsoa suojausmekanismit riittäviksi olisi korkea.

Poikkeuksen määrittelyn kannalta olisi ongelmallista, jos verkkojen kehityksen myötä suurta osaa verkon toiminnoista ei määräykseen tehdyn poikkeuksen johdosta pidemmällä aikavälillä katsottaisikaan viestintäverkon kriittiseksi osaksi. Poikkeuksen määrittelyn riskinä siis on, että ei-kriittiseksi voisi mahdollisesti rajautua suuri osa sellaisista verkon toiminnallisuudesta, jotka tukisivat 5G-verkon uusia käyttötarkoituksia.

Näitä poikkeuksen määrittelyyn liittyviä riskejä vähentää kuitenkin merkittävästi se, että määräyksen ajantasaisuutta tullaan seuraamaan tiiviisti. Jälkiseurannassa tullaan jo lähivuosina tarkastelemaan määräyksen soveltamista sekä tekniikan kehityk-

[16] On esimerkiksi mahdollista, että 5G-verkon teknisten määrittelyjen tulevissa versioissa mahdollistetaan palveluväylän avaaminen käyttäjäliikenteelle ja siten UPF:lle sen sijaan, että se on ytimeen yhteydessä välillisesti käyttäjäistuntoja hallitsevan Session Management Function (SMF) -toiminnon kautta.

sen ja reunalaskennan käytännön toteutuksen vaikutuksia. Tällöin on mahdollista arvioida uudelleen, onko poikkeukselle edelleen perustelut, sekä laajemminkin reunalaskentaan liittyvien toimintojen mahdollista kriittisyyttä.

5. Määräyksen valmistelu

Määräyksen teknisissä määrittelyissä tulee hallituksen esityksen (HE 98/2020 vp) mukaan huomioida kansainväliset standardit, joiden perusteella viestintäverkkoja suunnitellaan ja rakennetaan. Määräyksen valmistelussa on erityisesti tukeuduttu ETSI:n standardeihin ja 3GPP:n teknisiin määrityksiin, jotka on otettu huomioon 4G- ja 5G-verkkojen kriittisten osien määrittelyssä.

Määräys on valmisteltu laaja-alaisessa yhteistyössä toimialan ja eri viranomaistahojen kanssa. Valmisteluun ovat osallistuneet kansalliseen turvallisuuteen ja maanpuolustukseen liittyviä viranomaistehtäviä hoitavat tahot.

5.1. Kuuleminen

Traficom lähetti syyskuussa 2020 kaikille teleyrityksille, keskeisimmille verkkolaitevalmistajille sekä keskeisille viranomaisille kutsun osallistua määräyksen valmisteluun. Valmisteluun osallistuivat määräyksen varhaisesta luonnosvaiheesta lähtien seuraavat tahot joko kommentoimalla tai seuraamalla työskentelyä: DNA, Cinia, Digita, Elisa, Ericsson, FiCom ry, Finnet-liitto ry, FNE-Finland, Huawei, Luoteis-Kuhmon kyläverkko-osuuskunta, Länsilinkki, NDC Networks, Nokia, Suomen Erillisverkot, Telia Finland ja Ålands Telekommunikation sekä Huoltovarmuuskeskus, puolustusministeriö, puolustusvoimat, sisäministeriö, ulkoministeriö ja valtiovarainministeriö. Syys-marraskuun aikana valmisteluun osallistuneille tahoille (valmisteluryhmälle) järjestettiin viisi etäkokousta, minkä lisäksi suuri osa osallistujista vastasi Traficomin laatimiin määräyksen valmistelua tukeviin kirjallisiin kysymyksiin kokousten välillä. Osallistujilla oli mahdollisuus kommentoida Traficomin laatimia luonnoksia määräyksestä ja perustelumuistiosta.

Valmisteluryhmään osallistuneilla oli vielä tilaisuus kommentoida määräyksen ja perustelumuistion luonnoksia 21.1.–3.2.2021 lausuntokierrokselle lähtevien luonnosversioiden viimeistelemiseksi. Seuraavassa kuvataan keskeisimmät kommentit ja niiden perusteella tehdyt tarkennukset.

Eräissä kommenteissa esitettiin, että määräykseen lisättäisiin velvoite luovuttaa dokumentaatio viranomaiselle säännöllisesti tai ennakolta, kun uusia komponentteja otetaan käyttöön. Traficom toteaa, että sillä ei ole toimivaltaa asettaa määräyksellä uusia tiedon luovuttamista koskevia velvoitteita tai tiedonsaantioikeuksia, joten asiassa on sovellettava olemassa olevia asiaa koskevia säännöksiä, joita Traficomin osalta ovat muun muassa SVPL 315 §, 320 §, 244 a §:n 5 momentti ja 244 b §:n 3 momentti. Kommenteissa ehdotettiin myös 4G- ja 5G-tukiasemien määrittelyä aina kriittiseksi, mitä ei toteutettu. Tältä osin viitataan yllä kohdassa 4.1.5 todettuun, jota tarkennettiin palautteen perusteella.

Saatujen kommenttien perusteella täsmennettiin yhtä esimerkkiä, jolla kuvataan viestintäverkon ja -palvelun toiminnalle välttämättömiä, sen toimintaa tukevia infrastruktuuripalveluja (perustelumuistion yksityiskohtaisten perustelujen kohdan 4.2 alakohta 4)). Kyse voi olla esimerkiksi keskitetystä aikapalvelujärjestelmästä, joka välittää ja varmistaa tukiasemien aika- ja vaihesynkronointisignaaleja.

Yhteenliittämiseen liittyvien kriittisten osien määrittelyn osalta pyydettiin täsmentämään, että vastaanottava puoli ei ole vastuussa viestintäverkon kriittisistä osista

(toisen osapuolen osalta). Traficom toteaa tämän johdosta, että SVPL 244 a §:n 1 momentin mukainen kielto käyttää yleisen viestintäverkon kriittisissä osissa verkkolaitetta koskee nimenomaan viestintäverkon (so. kyseisen verkkolaitteen) omistajaa tai muuta haltijaa eli niitä tahoja, joihin velvoite poistaa verkkolaite verkosta voidaan SVPL 244 a §:n 3 momentin perusteella kohdistaa.

Useissa kommenteissa esitettiin, että 2G- ja 3G-verkon tukiasemaohjaimet rajattaisiin niiden tärkeysluokasta riippumatta pois määräyksen 4 kohdan luettelon 1 kohdan i) alakohdan piiristä. Traficom ei pitänyt ehdotusta perusteltuna, jos tukiasemaohjain kuitenkin kuuluisi käyttäjämääränsä tai vaikutusalueensa perusteella tärkeysluokkaan 1 tai 2. Traficom täsmensi kohtaa kuitenkin siten, että tukiasemaohjaimet eivät tule viestintäverkon kriittisiksi osiksi pelkästään sen takia, että ne määritellään määräyksessä 54 automaattisesti vähintään tärkeysluokkaan 2 kuuluviksi. Vaikutusarviota täydennettiin tältä osin.

[Täydennetään lausuntokierroksen toteuttaminen.]

5.2. Lausuntopalaute

[Täydennetään lausuntokierroksen jälkeen.]

6. Arvio määräyksen vaikutuksista

Määräys on uusi. Viestintäverkon kriittisten osien määrittelystä ei ole aiemmin ollut määräystä. Määräys tulee ennalta ohjaamaan teleyrityksiä ja sen soveltamisalaan kuuluvia erillisverkkotoimijoita verkkojen suunnittelussa, verkkolaitteiden hankinnassa sekä verkkojen rakentamisessa, ylläpidossa ja hallinnoimisessa. Määräyksellä edistetään kansallista turvallisuutta ja viestintäverkkojen tietoturvaa. Määräys täsmentää niitä viestintäverkon osia, joihin sähköisen viestinnän palveluista annetun lain 244 a §:n mukainen viestintäverkkolaitteen käyttökielto voi kohdistua. Siten määräys selkeyttää kyseisen pykälän soveltamiskohteita.

Tunnistamis- ja dokumentointivelvollisuus

Yritysvaikutukset. Määräyksen kohtaan 3 ehdotetun viestintäverkon kriittisten osien määrittelyä ja dokumentointia koskevan velvoitteen arvioidaan aiheuttavan sen kohteena oleville teleyrityksille ja erillisverkkotoimijoille jonkin verran taloudellisia kustannuksia näiden määritellessä ja dokumentoidessa verkkojensa kriittisiä osia ja niissä käytettyjä komponentteja. Velvoite kohdistuu yhtäläisesti kaikkiin SVPL 244 a §:n soveltamisalan piiriin kuuluviin teleyrityksiin ja erillisverkkotoimijoihin. Dokumentoinnin edellyttämä työmäärä on pienten ja teknisesti yksinkertaisten verkkojen omistajille tai haltijoille kuitenkin käytännössä vähäisempi kuin suurten ja monimutkaisten verkkojen omistajille tai haltijoille. Tunnistamis- ja dokumentointivelvoitteella voidaan arvioida olevan myös myönteisiä yritysvaikutuksia, sillä velvoite edistää osaltaan uuden sääntelyn noudattamista teleyrityksissä ja erillisverkkotoimijoissa. Näin ollen uuden sääntelyn vaatimukset tulevat todennäköisesti varmemmin huomioiduiksi myös suunniteltaessa muutoksia viestintäverkkoon. Velvoitteen voidaan lisäksi arvioida jossain määrin pienentävän – mutta ei poistavan – riskiä siitä, että toimija joutuisi poistamaan viestintäverkkolaitteen SVPL 244 a §:n nojalla verkostaan. Traficomin määräyksen valmistelun aikana saamissa näkemyksissä ei pääosin kannatettu tunnistamis- ja dokumentointivelvollisuuden rajaamista hallinnollisen taakan vähentämiseksi vain osaan yleisistä viestintäverkoista tai kriittisistä erillisverkoista.

Vaikutukset viranomaisten toimintaan. Tunnistamis- ja dokumentointivelvoitteella arvioidaan olevan merkittäviä myönteisiä vaikutuksia sääntelyn noudattamista valvovan viranomaisen valvontatehtävien toteuttamisen kannalta. Ajantasainen dokumentaatio toimii pohjana sääntelyn noudattamisen valvomiselle sekä tarvittaviin jatkotoimenpiteisiin ryhtymiselle.

Muut yhteiskunnalliset vaikutukset. Tunnistamis- ja dokumentointivelvoitteen arvioidaan osaltaan turvaavan SVPL 244 a §:ssä tarkoitettuja viestintäverkon kriittisiä osia sekä sen myötä uuden sääntelyn tarkoituksen toteutumista ja viestintäverkkojen turvallisuutta.

Eri verkkojen yhteisten kriittisten osien sekä 4G- ja 5G-verkon kriittisten osien määrittely

- Virtualisointi ja verkon virtualisoidut toiminnot

Yritysvaikutukset. Määräyksessä virtualisointi määritellään viestintäverkon kriittiseksi osaksi silloin, kun sitä käytetään viestintäverkon kriittisenä osana pidettävän toiminnon tai toimenpiteen toteuttamiseen. Lisäksi viestintäverkon kriittiseksi osaksi määritellään mikä tahansa toiminto tai toimenpide, kun se toteutetaan viestintäverkon kriittisenä osana pidettävän virtualisoinnin avulla. Määräys ei sinänsä estä toteuttamasta samalla virtualisointialustalla kriittisiä ja lähtökohtaisesti ei-kriittisiä toimintoja, mutta riski SVPL 244 a §:n mukaisesta verkkolaitteen käyttökiellosta voisi kuitenkin johtaa siten, että teleyritys varmuuden vuoksi toteuttaa useita virtualisointialustoja kriittisten ja ei-kriittisten toimintojen erottamiseksi. Teleyrityksen on sääntelyn kannalta kuitenkin mahdollista toteuttaa toiminnot samallakin alustalla, jos se pystyy näin toimiessaan huolehtimaan velvoitteistaan. Viestintäverkon kriittisten osien piiri on pyritty yritysvaikutusten minimoimiseksi rajaamaan välttämättömään, eikä mitä tahansa virtualisointialustaa katsota määräyksen perusteella verkon kriittiseksi osaksi.

- Verkon reunalla tuotettavia palveluita tukevat toiminnot

Yritysvaikutukset. Määräys sisältäisi kriteerit, joiden perusteella 4G-tai 5G-verkon reunalla tuottavia palveluita tukeva verkon ohjaamiseen liittyvä toiminnallisuus, joka sinänsä kuuluu viestintäverkon ydintoimintoihin, voitaisiin katsoa poikkeuksellisesti muuksi kuin viestintäverkon kriittiseksi osaksi. Poikkeus mahdollistaisi sen, että määräystä ei tarpeettomasti sovellettaisi sellaisiin toimintoihin, joiden osalta voidaan varmistua siitä, että toiminnon ei ole katsottava kontrolloivan tai ohjaavan pääsyä verkkoon tai verkon liikennettä. Tällöin SVPL 244 a § ei rajoittaisi teleyrityksen toimintaa tältä osin. Toisaalta teleyritykselle aiheutuisi kustannuksia poikkeuksen osoittamisesta ja sen edellyttämien suojausmekanismien käyttöönotosta. Niiden arvioidaan kuitenkin olevan välttämättömiä, jotta näiden toimintojen katsominen muuksi kuin viestintäverkon kriittiseksi osaksi on mahdollista.

Vaikutukset viranomaisten toimintaan. Jos teleyritys tai erillisverkkotoimija vetoaisi poikkeukseen, Traficomin olisi arvioitava SVPL 244 a §:n soveltamista varten suojausmekanismien riittävyys, mikä voi vaatia huomattavaa asiantuntemusta. Näiden seikkojen selvittely voisi kuitenkin olla välttämätöntä joka tapauksessa osana sitä koskevaa arviota, täyttyykö ns. vaarantamisedellytys teleyrityksen tai erillisverkkotoimijan toteuttamien toimenpiteiden johdosta. Tämän takia ei arvioida, että poikkeuksen olemassaolo lisäisi ratkaisevasti Traficomin työmäärää.

- Radioliityntäverkon osat ja tukiasemien hallintajärjestelmä

Yritysvaikutukset. Traficom pitää ennenaikaisena määritellä tässä määräyksessä sitä, ovatko tukiasemat viestintäverkon kriittisiä osia. Teleyrityksen ja erillisverkkotoimijan olisi itse arvioitava niiden kriittisyyttä suhteessa tekniikan tasoon ja muun muassa tukiasemien toteuttamiin toimintoihin ja toimenpiteisiin nähden. Tästä aiheutuu toimijoille jonkin verran epävarmuutta laitevalintoihin, mitä Traficom ei katso voitavan välttää tässä tilanteessa. Määräyksessä otetaan kuitenkin kantaa tiettyihin tukiasemiin liittyvien verkon osien kriittisyyden arviointiin siitä riippumatta, ovatko tukiasemat itsessään viestintäverkon kriittisiä osia. Näitä ovat hallintajärjestelmät ja tukiasemaohjaimet.

Viestintäverkon hallinta- ja valvontajärjestelmät katsotaan tämän määräyksen mukaan viestintäverkon kriittiseksi osaksi silloinkin, kun ne voivat olennaisesti vaikuttaa verkkoon pääsyyn tai verkossa kulkevaan liikenteeseen, vaikka hallittava elementti itsessään ei olisikaan viestintäverkon kriittinen osa. Tukiasemien hallintajärjestelmä voi olla tällä perusteella viestintäverkon kriittinen osa, vaikka kyseisessä tapauksessa tukiasemia itsessään ei pidettäisikään viestintäverkon kriittisinä osina. Arvion tekeminen osan kriittisyydestä aiheuttaa jonkin verran hallinnollista taakkaa teleyritykselle tai erillisverkkotoimijalle, mutta sen vastinparina on, että tukiasemien hallintajärjestelmää voidaan pitää tapauskohtaisesti ei-kriittisenä.

Koska tukiasemien laitetoimittaja toimittaa tyypillisesti myös niiden hallintajärjestelmän, ei tukiasemien hallintajärjestelmän hankkiminen toiselta toimittajalta tai sellaisen kehittäminen liene tällä hetkellä välttämättä taloudellisteknisesti perusteltua. Tämän takia voidaan arvioida, että tukiasemien hallintajärjestelmän mahdollinen kriittisyys verkon osana voi välillisesti vaikuttaa myös teleyrityksen tai erillisverkkotoimijan verkkonsa tukiasemien osalta tekemiin toimittajavalintoihin. Hallintajärjestelmät voivat kuitenkin mahdollistaa myös toisen valmistajan tukiasemien hallinnan, mutta tällöin toiminnoissa voi olla rajoituksia.

Vaikka tukiasemien hallintajärjestelmä katsottaisiin viestintäverkon kriittiseksi osaksi, voisi teleyritys tästä huolimatta valita viestintäverkkolaitteen, jonka käyttöön voi mahdollisesti liittyä korkeampi riski SVPL 244 a §:n mukaisen käyttökiellon soveltamisesta. Tällöin operaattori voisi pyrkiä osoittamaan, että vaikka verkossa käytetään kyseistä tukiasemien hallintajärjestelmää, jota pidetään viestintäverkon kriittisenä osana, ei kansallinen turvallisuus tai maanpuolustus kuitenkaan vaarannu. Tämän se voi pyrkiä osoittamaan esimerkiksi toteuttamalla lisäkontrolleja tietoturvan varmistamiseksi (ks. kohta 4.3); tällöin hallintaympäristöön voi syntyä eri turvatason segmenttejä, joiden erottelun ja turvallisuuden varmistaminen on keskeistä. Koska SVPL 244 a § perustuu jälkikäteiseen valvontaan, ei operaattorilla olisi mahdollista ennalta kokonaan poistaa riskiä siitä, että tukiasemien hallintajärjestelmään voisi jatkossa kohdistua poistovelvoite. Lisäksi tulee huomata, että tukiasemien hallintajärjestelmä ei kuitenkaan olisi tapauksen erityispiirteistä riippuen välttämättä määräyksen perusteella viestintäverkon kriittinen osa silloin, kun sen ohjaamia tukiasemia itsessään ei pidettäisi viestintäverkon kriittisinä osina.

Toisaalta silloinkin, kun verkon tukiasemia ei pidettäisi viestintäverkon kriittisinä osina, teleyritys voi riskit arvioituaan päätyä ratkaisuun, että tukiasemia ei olisi järkevää hankkia ilman saman toimittajan hallintajärjestelmää, mikäli hallintajärjestelmää pidettäisiin viestintäverkon kriittisenä osana. Tällaiseen ratkaisuun voisi johtaa se, jos taloudellisesti ja toiminnallisesti järkevää toimittajariippumatonta tukiasemaelementtien hallintajärjestelmää ei ole saatavissa tai mahdollista kehittää ja jos tele-

yritys arvioi, että on olemassa liian korkea riski siitä, että hallintajärjestelmään kohdistuisi tukiasemien elinkaaren aikana poistovelvoite ilman täyttä korvausta. Tällaisen arvion lopputuloksena operaattorin mahdollinen tukiasematoimittajakenttä voisi käytännössä supistua, jos se arvioisi, että tukiasemien hallintajärjestelmän toimittajan tulee olla sama kuin tukiasemien. Tällä voisi olla vaikutusta operaattorin neuvotteluasemaan ja laitetoimittajien väliseen kilpailutilanteeseen. Tällaisen vaikutuksen arvioidaan kuitenkin olevan rajallinen suhteessa siihen, että operaattorilla olisi muutoinkin riski siitä, miten itse tukiasemien kriittisyyttä on arvioitava, sillä tässä määräyksessä ei määritellä sitä, ovatko tukiasemat viestintäverkon kriittisiä osia.

2G- ja 3G-verkoissa käytetään erityisiä tukiasema- ja radioverkko-ohjaimia, jotka olisivat tämän määräyksen mukaan viestintäverkon kriittisiä osia ainakin silloin, kun ne kuuluvat käyttäjämäärän tai vaikutusalueen mukaan määräyksen 54 perusteella tärkeysluokkaan 1 tai 2. Traficomin saamien kommenttien mukaan tukiasemat ovat käytännössä riippuvaisia saman valmistajan tukiasemaohjaimista, joskin Traficomin tietojen mukaan niihin liittyy rajapinta, joka voisi mahdollistaa eri valmistajien laitteiden käytön. Tukiasemaohjainten pitämisellä viestintäverkon kriittisinä osina voidaan arvioida olevan samankaltaisia vaikutuksia kuin yllä on arvioitu olevan sillä, jos tukiasemien hallintajärjestelmä on viestintäverkon kriittinen osa, eikä tukiasemia ei ole taloudellisesti ja toiminnallisesti mahdollista käyttää ilman saman valmistajan tukiasemaohjaimia. Samaan tukiasemayksiköön voi olla integroituna eri verkkotekniikat, jolloin integroidun tukiaseman 2G- ja 3G-toiminnallisuutta ei tässä tapauksessa voitaisi käyttää 4G- ja 5G-toiminnallisuuden kuitenkin säilyessä. 3G-tekniikasta ollaan kuitenkin joka tapauksessa luopumassa.

Pidemmällä aikavälillä tukiasemien hallintajärjestelmän tai tukiasemien arviointi viestintäverkon kriittisiksi osiksi voi vaikuttaa radioverkon arkkitehtuurivalintoihin ja johtaa esimerkiksi OpenRAN-ratkaisun käyttöönottoon, jolloin kytkös hallintajärjestelmän ja tukiasemien sekä niiden toimittajien välillä pienenee merkittävästi. Tällöin radioverkon arkkitehtuuri muuttuu laitetoimittajariippumattomaan suuntaan, ja hallintajärjestelmän vaihtaminen voi olla käytännössä helpommin toteutettavissa. Tekniset ratkaisut ovat kuitenkin vielä kehitys- ja kokeiluvaiheessa tätä määräystä annettaessa.

Yksityiskohtaiset perustelut

1. Soveltamisala

Määräyksen 1 kohdan mukaan määräystä sovelletaan yleiseen teletoimintaan sekä sähköisen viestinnän palveluista annetun lain (917/2014, SVPL) 244 a §:n 2 momentissa tarkoitettuihin yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden yleiseen viestintäverkkoon liitettyyn erillisverkkoon.

Määräyksen soveltamisala kattaa kaikki toimijat, joihin SVPL 244 a §:ää sovelletaan eli sekä teleyritykset että erillisverkkotoimijat.

Määräys ei ole tyhjentävä. Määräyksessä viestintäverkon kriittiseksi määriteltyjen viestintäverkon osien lisäksi sovelletaan SVPL 244 a §:ää, joten viestintäverkon kriittiset osat voivat määräytyä myös suoraan sen 1 momentin mukaisen viestintäverkon kriittisten osien määritelmän mukaisesti.

2. Määritelmät

Tässä kohdassa määritellään määräyksessä käytettävät keskeiset käsitteet.

Viestintäverkon kriittinen osa

Viestintäverkon kriittisen osan määritelmä vastaa SVPL 244 a §:n 1 momentissa olevaa määritelmää. Viestintäverkon kriittisenä osana pidetään sen mukaan verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Määritelmästä seuraa, että lähtökohtaisesti jokaisella viestintäverkolla on kyseisen verkon toiminnan kannalta kriittiset osat.

Tulee huomata, että viestintäverkon osan kriittisyyden arvioinnista erillinen kysymys on, täyttääkö tietyn viestintäverkkolaitteen käyttäminen verkon kriittisessä osassa SVPL 244 a §:n 1 momentin mukaisen ns. vaarantamisedellytyksen. Sen täyttyminen edellyttää, että "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". Tämä määräys ei lainkaan koske vaarantamisedellytyksen arviointia, koska Traficomin määräyksenantovaltuus koskee 6 momentin mukaan ainoastaan viestintäverkkojen kriittisten osien teknistä määrittelyä.

Hallituksen esityksessä viestintäverkon kriittisen osan käsitettä täsmennetään seuraavasti (s. 261):

> *Viestintäverkon kriittisenä osana pidettäisiin verkon ydintä, erityisesti sellaisia toimintoja ja toimenpiteitä, joiden avulla verkkoa ja siellä kulkevaa liikennettä keskeisesti ohjataan ja hallitaan. Nykyisessä verkkoteknologiassa kriittistä ydintä on esimerkiksi se osa runkoverkkoa, jossa hallinnoidaan eri käyttäjien pääsyä verkkoon ja ylläpidetään käyttäjien yhteyksien tilaa. Viestintäverkon kriittis[et] 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.*

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. Olennaista viestintäverkon kriittisten osien määrittelyssä olisi arvioida myös sitä, kenellä on tosialliset mahdollisuudet vaikuttaa viestintäverkon osan tai siellä olevan viestintäverkkolaitteen toimintaan ja ominaisuuksiin.

Liikenne- ja viestintävaliokunnan mietinnössä (LiVM 16/2020 vp, s. 16) viestintäverkon kriittisen osan määritelmää on perustuslakivaliokunnan lausunnossa (PeVL 35/2020 vp) edellytetyllä tavalla täsmennetty. Mietinnön mukaan "viestintäverkon kriittisenä osana pidetään vain verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Valiokunnan saaman selvityksen mukaan täsmennys on laadittu eri ministeriöiden välisissä keskusteluissa. Valiokunta on kuitenkin lisännyt muutokseen täsmennyksenä sanan 'keskeisiä' perustuslakivaliokunnan lausunnosta johtuen. Viestintäverkon kriittisillä osilla on keskeinen merkitys verkon toimivuuden, ylläpitämisen sekä viestinnän luottamuksellisuuden ja verkon tietoturvallisuuden kannalta."

Hallituksen esityksessä viestintäverkon kriittisinä osina pidettävistä toiminnoista esitettyjen kannanottojen merkitystä arvioitaessa on siis huomioitava, että kriittisten osien piiriä on valiokuntamietinnön mukaisesti täsmennetty koskemaan verkon hallinnan ja ohjaamisen sijasta *verkkoon pääsyn* kontrollointia tai ohjaamista. Verkkoon pääsyn käsitettä ei kuitenkaan ole rajattu vain hallituksen esityksessä mainittuun käyttäjien verkkoon pääsyyn, vaan viestintäverkon kriittiset osat voivat kontrolloida tai hallita myös muuta verkon toimintoihin ja laitteisiin pääsyä, joka voi perustua esimerkiksi verkkojen yhteenliittämiseen tai verkon ylläpitoon liittyviin hallintayhteyksiin. Lisäksi verkkoon pääsyn kontrolloinnin tai ohjaamisen käsite voi sisältää esimerkiksi viestinnän luottamuksellisuuden ja verkon palveluiden saatavuuden varmistamiseen kytkeytyviä toimintoja edellyttäen, että ne liittyvät myös verkkoon pääsyn kontrollointiin tai ohjaamiseen. Liikenne- ja viestintävaliokunnan mietinnön perusteella voidaan päätellä, että keskeisyyttä ja olennaisuutta lisää se, jos toiminnolla on vaikutuksia verkon toimivuuteen, verkon ylläpitämiseen, viestinnän luottamuksellisuuteen tai verkon tietoturvallisuuteen. Lisäksi on huomattava, että verkossa kulkevan liikenteen kontrollointiin tai ohjaamiseen liittyvät toiminnot on määritelty viestintäverkon kriittiseksi osaksi hallituksen esitystä vastaavasti lukuun ottamatta sitä, että käsite hallinta on korvattu kontrolloinnin käsitteellä.

Kriittinen erillisverkko ja erillisverkkotoimija

SVPL 244 a §:n 2 momentissa ulotetaan pykälän soveltamisala ydinvoimaloiden, satamien, lentokenttien ja vastaavien yhteiskunnan elintärkeiden toimintojen kannalta keskeisten toimijoiden yleiseen viestintäverkkoon liitettyihin erillisverkkoihin. Näihin verkkoihin viitataan määräyksessä käsitteellä kriittinen erillisverkko ja tällaisen verkon omistajaan tai haltijaan käsitteellä erillisverkkotoimija.[17] Jos esimerkiksi mikro-operaattori tarjoaa palveluna kriittisen erillisverkon yhteiskunnan elintärkeiden toimintojen kannalta keskeiselle toimijalle, pidetään mikro-operaattoria tältä osin myös

[17] Esitöiden mukaan (HE 98/2020 vp, s. 262) yhteiskunnan kriittisiä palveluita on tunnistettu muun muassa huoltovarmuudesta annetun lain (1390/1992) 2 §:n nojalla annetussa valtioneuvoston päätöksessä huoltovarmuuden tavoitteista (VNp 1048/2018) sekä osana verkko- ja tietoturvadirektiivin kansallista täytäntöönpanoa (HE 192/2017 vp).

itse yhteiskunnan elintärkeiden toimintojen kannalta keskeisenä toimijana. Määräyksen velvoitteet kohdistuvat siten kriittisen erillisverkon omistajaan tai muuhun haltijaan.

SVPL 244 a §:ää ja määräystä sovelletaan vain *yleiseen viestintäverkkoon liitettyyn* erillisverkkoon. Soveltamisalaan kuuluu siis vain ns. epävarsinainen erillisverkko erotukseksi sellaisesta varsinaisesta erillisverkosta, jota ei ole lainkaan yhteenliitetty yleisen viestintäverkon kanssa ja joka ei siten ole SVPL 244 a §:n soveltamisalan piirissä.[18] SVPL 244 a §:ää ei sovelleta sellaisiin viestintäverkkoihin, jotka eivät ole yleisiä viestintäverkkoja eivätkä myöskään kriittisiä erillisverkkoja, kuten tavanomaisiin kiinteistöjen tai yritysten sisäverkkoihin. Sen sijaan silloin kun viestintäverkkoa käytetään viestintäpalvelujen tarjontaan ennalta rajaamattomalle käyttäjäpiirille eli harjoitetaan yleistä teletoimintaa, sovelletaan SVPL 244 a §:n 1 momenttia ja määräyksen teleyrityksiä koskevia kohtia[19].

Yhteenliittämisellä tarkoitetaan esimerkiksi sitä, että matkaviestinverkon tekniikalla toteutetusta erillisverkosta on yhteys internetiin kiinteän verkon yhteenliittämisen kautta tai mahdollisuus soittaa puheluita erillisverkon ulkopuolelle. SVPL 244 a §:n 2 momentin soveltamisedellytyksenä ei siis ole esimerkiksi mobiiliverkkojen yhteenliittäminen ja verkkovierailumahdollisuus.

Kriittinen erillisverkko voi olla millä tahansa teknologialla toteutettu muu kuin yleinen viestintäverkko. SVPL 244 a §:n perustelujen mukaan 2 momentin soveltamisalan kannalta on olennaista, että kyseinen viestintäverkko toimii yhteiskunnan näkökulmasta siinä määrin kriittisessä ympäristössä, että verkon ydintoimintojen vaarantuminen voisi johtaa kansallisen turvallisuuden tai maanpuolustuksen vaarantumiseen (HE 98/2020 vp, s. 262).

Viestintäverkon tai -palvelun komponentti

Viestintäverkon tai -palvelun komponentilla tarkoitetaan tässä määräyksessä verkkoelementtiä, laitetta tai tietojärjestelmää, joista viestintäverkko tai -palvelu muodostuu tai jota se hyödyntää. Käsitettä käytetään useissa Traficomin määräyksissä. Viestintäverkon tai -palvelun komponentteja ovat esimerkiksi matkaviestinkeskus, tukiasemaohjain, tukiasema, tekstiviestikeskus, laajakaistakeskitin, nimipalvelin, verkon pääsynhallinnasta vastaava palvelin, kytkin, reititin, SIP-sovelluspalvelin, älyverkon komponentti, DVB-T-verkon pää- ja täytelähetin tai DVB-T2-verkon lähetin. Viestintäverkon tai -palvelun komponentilla *ei* tarkoiteta siirtoteitä tai laitteen tai verkkoelementin osia, kuten esimerkiksi matkaviestinkeskuksen prosessoriyksiköitä. Mikäli jokin toiminto (esimerkiksi nimipalvelinohjelmisto) on hajautettu usealle eri laitteelle, katsotaan kukin laite omaksi komponentikseen.

4G-verkko

[18] Erillisverkon käsitettä käytetään SVPL 244 a §:ssä tavalla, joka poikkeaa kumotusta viestintämarkkinalaista (393/2003). Viestintämarkkinalaissa erillisverkolla tarkoitettiin verkkoa, jota ei ole liitetty yhteen yleisen viestintäverkon kanssa (130 §).
[19] Kuten säännöksen perusteluista ilmenee, yleisiä viestintäverkkoja koskevaa SVPL 244 a §:n 1 momenttia sovelletaan myös SVPL:ssä tarkoitettuun viranomaisviestintään liittyvään verkkopalveluun siltä osin kuin sen tarjoamisessa hyödynnetään teleyritysten yleisiä viestintäverkkoja (HE 98/2020 vp, s. 261).

4G-verkolla tarkoitetaan tässä määräyksessä LTE-tekniikalla toteutettua matkaviestinverkkoa (sen ydintä tai radioliityntäverkkoa), joka perustuu 3GPP:n teknisten määritysten mukaiseen EPS- eli Evolved Packet System -arkkitehtuuriin. EPS muodostuu pakettikytkentäiselle liikenteelle optimoiduista verkon ytimestä (Evolved Packet Core, EPC) ja radioliityntäverkosta (Evolved UTRAN eli E-UTRAN)[20].

5G-verkko

5G-verkolla tarkoitetaan tässä määräyksessä viidennen sukupolven tekniikalla toteutettua matkaviestinverkkoa, joka perustuu 3GPP:n teknisten määritysten mukaiseen viidennen sukupolven ydinverkkoon (5GC Fifth Generation Core Network, TS 21.905) tai viidennen sukupolven radioliityntäverkkoon (New Radio, NR, Fifth Generation radio access technology).

5G-verkon käsite sisältää määräyksen soveltamisen kannalta myös 5G Non-Standalone- eli 5G NSA -verkon 5G-sukupolven komponentit, jotka kuuluvat siis määräyksen sisäisen jaottelun kannalta 5G-verkon kriittisten osien määrittelyn alaan. Esimerkiksi jos jossakin 5G-verkon osassa käytetty komponentti on määritelty määräyksessä kriittiseksi, määrittelyä sovelletaan myös tilanteessa, jossa komponenttia käytettäisiin 5G NSA -verkon osana. 5G NSA -verkko päivittyy elinkaarensa aikana 5G Standalone- eli 5G SA -verkoksi, jolloin siihen tullaan soveltamaan kaikilta osin 5G-verkon kriittisten osien määrittelyjä. 5G NSA -verkkoja ei ole tarpeen erikseen määritellä määräyksessä, sillä niissä käytetään 4G- ja 5G-verkkojen toimintoja. 4G-verkon ytimeen eli EPC-verkkoon ei tiettävästi tule 5G NSA:n takia uusia komponentteja tai 3GPP:n määrittämiä funktioita, vaan kehittyneet toiminnallisuudet toteutetaan olemassa olevissa komponenteissa.

Muut määritellyt käsitteet

Muutoin sovelletaan SVPL 3 §:n mukaisia määritelmiä. Pykälässä on määritelty muun muassa teleyritys, viestintäpalvelu, viestintäverkko, viestintäverkkolaite ja yleinen viestintäverkko.

3. Kriittisten osien määrittely ja dokumentointi

3.1. Viestintäverkon kriittisten osien tunnistaminen ja dokumentointi

Kohdan ensimmäisessä alakohdassa velvoitetaan teleyritys ja erillisverkkotoimija tunnistamaan viestintäverkkonsa kriittiset osat ja niissä käyttämänsä viestintäverkon ja -palvelun komponentit. Sen on siis määriteltävä oman verkkonsa osalta, mitkä osat ja niissä käytetyt komponentit se katsoo lain ja määräyksen nojalla kriittisiksi osiksi verkkoa. Lisäksi teleyrityksen ja erillisverkkotoimijan on laadittava ja ylläpidettävä ajantasainen dokumentaatio tunnistamistaan viestintäverkon kriittisistä osista ja niissä käyttämistään viestintäverkon ja -palvelun komponenteista. Dokumentaatiosta tulee ilmetä komponentin valmistaja ja mallinumero tai muu yksilöintitieto. Esimerkiksi virtualisoinnin kohdalla dokumentoitavia olisivat ainakin komponentit, joilla toteutetaan virtualisoinnin fyysinen alusta, virtualisointi-infrastruktuuri, verkon virtualisoidut funktiot ja virtualisoinnin hallinta (vrt. määräyksen 4 kohdan luettelon 11 kohta).

[20] TS 21.905 Vocabulary for 3GPP Specifications: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558.

Määräys edellyttää, että teleyritys ja erillisverkkotoimija ensinnäkin tunnistavat ne konkreettiset verkkolaitteet, joita se käyttää viestintäverkkonsa kriittisissä osissa. Toiseksi kriittiset osat tulisi tunnistaa myös suhteessa verkkoarkkitehtuuriin niin, että yritys tunnistaa ja määrittelee tietyt verkkonsa osat kriittisiksi jo verkkoarkkitehtuurin suunnitteluvaiheessa, jolloin määrittely ohjaisi yritystä huomioimaan SVPL 244 a §:n vaatimukset jo sen suunnitellessa verkkolaitehankintoja. Arviota olisi ylläpidettävä ajantasaisena verkkoarkkitehtuurin, turvallisuusarkkitehtuurin tai laitekannan muutosten yhteydessä ja niihin kohdistuvia muutoksia suunniteltaessa.

Verkon kriittisten osien tunnistaminen ei velvoita teleyritystä tai erillisverkkotoimijaa arvioimaan niiden merkitystä kansalliselle turvallisuudelle. Määräyksen lisäksi toimijan on sovellettava suoraan SVPL 244 a §:n 1 momentin määritelmää, jonka mukaan viestintäverkon kriittisenä osana pidetään verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä.

Velvoitteella pyritään edistämään SVPL 244 a §:n täytäntöönpanoa sekä varmistamaan sen ja määräyksen yhdenmukainen soveltaminen. Ilman kyseisenlaista dokumentointivelvoitetta Traficom ei pystyisi yhtä tehokkaasti valvomaan sitä, miten teleyritykset ja erillisverkkotoimijat soveltavat uutta sääntelyä. Traficom voi valvontatoiminnassaan pyytää kohdan edellyttämän dokumentaation SVPL 315 §:ssä säädetyn yleisen tiedonsaantioikeutensa nojalla.

Teleyrityksen ja erillisverkkotoimijan on arvioitava itsenäisesti viestintäverkkonsa osien kriittisyys määräyksen 3 kohdan mukaisen tunnistamis- ja dokumentointivelvollisuuden nojalla. Viime kädessä Traficom ratkaisee yksittäisen valvonta-asian yhteydessä teleyrityksen tai erillisverkkotoimijan tekemästä itsearviosta riippumatta, onko tiettyä verkon osaa pidettävä kriittisenä.

3.2. Verkon reunalla tuotettavia palveluita tukevien toimintojen kriittisyyttä koskeva arviointi

Kohdan toisessa alakohdassa määrätään, että teleyrityksen ja erillisverkkotoimijan on dokumentoitava perustelut arviolleen, jos se katsoo määräyksen 7 kohdan perusteella, että taulukossa 1 tai 2 (määräyksen kohdissa 5 ja 6) tarkoitettu 4G- tai 5G-verkon toiminto tai toimenpide ei ole sen viestintäverkon kriittinen osa. Määräyksen 7 kohdassa mahdollistetaan se, että muutoin viestintäverkon kriittiseksi osaksi katsottava toiminnallisuus voidaan tietyin edellytyksin katsoa ei-kriittiseksi, kun sillä tuetaan verkon reunalla tuotettavia palveluita ja se on tehokkaasti erotettu viestintäverkon kriittisistä osista.

Dokumentaatiossa tulisi kuvata ne perusteet kuten toteutetut tietoturvakontrollit, joiden perusteella operaattori on päätynyt arvioonsa. Dokumentointivelvollisuus kohdistuisi vain niihin viestintäverkon oletusarvoisesti kriittisiin osiin, jotka on määritelty nimenomaisesti taulukossa 1 tai 2.

3.3. Erillisverkon tukiasemien kriittisyyttä koskeva arviointi

Kohdan kolmannessa alakohdassa asetetaan erillisverkkotoimijalle erityinen velvollisuus laatia ja ylläpitää arvio sitä, onko sen erillisverkon tukiasemia pidettävä viestintäverkon kriittisinä osina. Sen tulee ottaa arviossaan huomioon ainakin erillisverkon maantieteellinen kattavuus, yksittäisen tukiaseman osuus verkon liikenteestä ja tukiaseman toteuttamat toiminnot ja toimenpiteet erillisverkossa. Erikseen mainittujen kriteerien lisäksi on arvioitava mahdolliset muut seikat, joilla on merkitystä ratkaistaessa sitä, kontrolloiko tai ohjaako tukiasema pääsyä verkkoon tai verkossa kulkevaa

liikennettä olennaisella tavalla. Velvoite ylläpitää arviota tarkoittaa, että sen ajantasaisuutta on tarkasteltava ja arviota tarvittaessa muutettava, jos verkossa tai sen käytössä tapahtuu merkittäviä muutoksia.

Traficom pitää perusteltuna asettaa korostettu velvoite tukiasemien osalta erillisverkoille, sillä 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. Traficom ei kuitenkaan ole arvioinut tarpeelliseksi määrittää kaikkien erillisverkkojen tukiasemia aina viestintäverkon kriittiseksi osaksi tai pyrkiä määrittämään sitovia kriteerejä sitä koskevalle arvioinnille.

Alakohdassa asetetaan erillisverkkotoimijalle lisäksi erityinen velvoite dokumentoida, miten se on päätynyt arvioonsa. Velvoite soveltuu myös siinä tapauksessa, että toimija päätyy katsomaan, ettei tukiasema ole sen erillisverkon kriittinen osa.

Erillisverkkotoimijoita koskeva tunnistamis- ja dokumentointivelvoite ei koske tukiasemia tai muita viestintäverkon osia tai niissä käytettyjä viestintäverkon tai -palvelun komponentteja siltä osin kuin niitä käytetään *yleiseen teletoimintaan*. Yleisen viestintäverkon osiin soveltuvat määräyksessä teleyrityksille asetetut velvoitteet.

4. Viestintäverkon kriittiset osat

4.1. Kriittisten osien määrittely

Kohdassa määritellään verkon toiminnallisuudet, joita ainakin on pidettävä viestintäverkon kriittisinä osina. Luettelo ei ole tyhjentävä, vaan sen lisäksi teleyrityksen tai erillisverkkotoimijan on arvioitava, onko sen verkossa kohdassa luettelemattomia viestintäverkon kriittisiä osia. Määräys ei siis rajoita SVPL 244 a §:n 1 momentin mukaisen viestintäverkon kriittisen osan määritelmän suoraa soveltamista. Tämän kohdan luettelo ja määräyksen verkkotekniikkakohtaiset kohdat täydentävät toisiaan.

Luettelo on teknologianeutraali. Kohta koskee periaatteessa kaikkia viestintäverkkoja, kuten esimerkiksi piiri- ja pakettikytkentäisiä matkaviestinverkkoja sekä kiinteitä laajakaistaverkkoja. Luettelo on laadittu ensi sijassa kohdeviestintäverkkoja varten, mutta sitä voidaan soveltuvin osin käyttää myös joukkoviestintäverkon kriittisten osien määrittelyssä. Kohdan mukaan verkon osa on kriittinen, vaikka se toteuttaisi vain osan kriittiseksi määritellystä toiminnallisuudesta. Tästä ja toiminnallisuuteen perustuvasta määrittelytavasta seuraisi, että kun yksittäisen komponentin voidaan osoittaa toteuttavan osaksikaan jonkin kriittisen verkon osaksi määritellyn toiminnallisuuden, olisi komponentti katsottava verkon kriittiseksi osaksi, vaikkei se koko toiminnallisuutta toteuttaisikaan. Yksittäinen ohjelmistokomponentti tai verkkolaite voi toteuttaa myös useamman kuin yhden toiminnallisuuden.

Luettelon laadinnassa on otettu vertailukohtana huomioon vastaavan kaltaiset luettelot, joita on laadittu Saksassa ja Yhdistyneessä kuningaskunnassa (ks. tarkemmin määräyksen yleisperustelujen luku 4.3) Lisäksi EU:n yhteisessä keinovalikoimassa[21] kriittisiksi on kuvattu ydinverkon funktioiden (core network functions) ohella verkon

[21] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. Liite 2, s. 39. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. 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.

funktioiden virtualisoinnin hallinta (NFV management) ja verkon orkestrointi (Management and Network Orchestration, MANO), jotka on sisällytetty myös määräyksen luetteloon. Eräin täsmennyksin luetteloon sisältyvät osaksi myös keinovalikoimassa kriittisyystasolle moderate/high (kohtalainen/korkea) määritellyt muut laskutus-, hallinta- ja tukijärjestelmät kuin MANO, siirto- ja transmissiofunktiot ja verkkojen väliset liityntäpisteet.

4.2. Viestintäverkon kriittiset toiminnallisuudet

1) Loppukäyttäjien liikenteen reititys ja muu kontrollointi tai ohjaaminen

Tämän alakohdan mukaan viestintäverkon kriittisiä osia ovat loppukäyttäjien liikenteen reititykseen ja muuhun kontrollointiin tai ohjaamiseen viestintäverkossa liittyvät keskeiset toiminnot, jotka voivat olennaisesti vaikuttaa viestintäverkossa kulkevaan liikenteeseen. Alakohdassa täsmennetään lisäksi, että viestintäverkon kriittisiä osia ovat tämän perusteella muiden ohella ainakin:

- yleisen viestintäverkon tai -palvelun komponentit, kun ne kuuluvat viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista annetun määräyksen eli määräyksen 54 mukaisiin tärkeysluokkiin 1 tai 2 niiden käyttäjämäärän tai vaikutusalueen mukaan,

- viestintäverkon tai -palvelun komponentit, kun ne muutoin kontrolloivat tai ohjaavat olennaista osaa koko verkon liikenteestä, sekä

- viestintäverkon tai -palvelun komponentit konesaliverkossa, kun ne ovat välttämättömiä viestintäverkon kriittisen osan toiminnan kannalta.

Tämä alakohta kattaa siis keskeiset toiminnot, joilla verkossa huolehditaan loppukäyttäjien liikenteen reitityksestä tai muusta ohjaamisesta verkossa päätelaitteille ja verkkojen välillä. Alakohta sisältää vastaavalta osin myös M2M-liikenteeseen liittyvät toiminnot. Alakohta sisältää myös käyttäjien liikenteen analysointiin kykenevät järjestelmät, joita käytetään haitallisen liikenteen havainnointiin ja jotka voivat osin kuulua myös jäljemmän, tietoturvatoimintoja koskevan kohdan alaan. Tyypillisesti nämä toiminnot toteutetaan matkaviestinverkon ytimessä tai runkoverkossa.

Tämä alakohta kattaa matkaviestinverkoissa etenkin toiminnallisuudet, jotka liittyvät käyttäjäliikenteen (user plane) välittämiseen tai joilla kontrolloidaan verkossa kulkevaa liikennettä ohjausliikenteen avulla (control plane). Alakohdan alaan kuuluu myös osaltaan liikkuvuuden hallinta mobiiliverkoissa (mobility management). Matkaviestinverkoissa myös tekstiviestikeskus (SMSC) ja siihen yhteydessä olevat yhdyskäytävät ohjaavat käyttäjien liikennettä tämän alakohdan tarkoittamalla tavalla.

Alakohtaan sisältyvät myös verkon viipalointiin (network slicing) liittyvät toiminnallisuudet siltä osin kuin ne toteuttavat kohdan mukaisia toimintoja. Verkon viipaloinnilla tarkoitetaan liikenteen jaottelua ja eriyttämistä matkaviestinverkossa haluttujen laatuparametrien takaamiseksi. Verkkoviipale muodostaa loogisen kokonaisuuden (loogisen verkon) yhdessä fyysisessä verkkoinfrastruktuurissa. Verkon viipaleella voi olla yhteisiä ja sille dedikoituja resursseja. Matkaviestinverkossa neljännen ja viidennen sukupolven teknologiat tukevat verkon viipalointia eri laajuuksissa, ja 5G:ssä viipalointiin osallistuvat useat verkon funktiot.

Näillä toiminnoilla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät myös

olennaisesti palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Runkoverkko on keskeinen erityisesti verkon liikenteen ohjaamisen kannalta ja palveluiden saatavuuden kannalta, koska verkon liikenne reitittyy tai välittyy sen kautta. Runkoverkko on samasta syystä keskeinen myös viestinnän luottamuksellisuuden kannalta. Myös alue- ja siirtoverkon komponentit ovat vastaavalla tavalla keskeisiä ollessaan riittävän merkittäviä.

Alakohdassa täsmennetään lisäksi, että yleisen viestintäverkon kriittisiä osia ovat tärkeysluokkiin 1 ja 2 käyttäjämäärän tai vaikutusalueen mukaan kuuluvat viestintäverkon tai -palvelun komponentit, mukaan lukien tämän kriteerin täyttävät reunareitittimet, riippumatta siitä, kuuluvatko ne operaattorin arkkitehtuurissa runko-, alue- vai siirtoverkon osaksi. Tärkeysluokittelusta määrätään tällä hetkellä Viestintäviraston määräyksessä 54 B/2014 M viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista. Määräyksen velvoite tärkeysluokittelusta ei sovellu erillisverkkoihin. Näihin tärkeysluokkiin kuuluvat verkkolaitteet ovat aina viestintäverkon kriittisiä osia, koska ne vaikuttavat niin merkittävään määrään käyttäjiä, että niiden on katsottava aina kontrolloivan tai ohjaavan olennaisesti verkon liikennettä.

Matkaviestinverkon tukiasemaohjaimen tärkeysluokka on määräyksen 54 mukaan aina vähintään 2, mutta tämän määräyksen kannalta ne katsottaisiin viestintäverkon kriittiseksi osaksi vain, jos ne kuuluisivat määräyksen 54 perusteella tärkeysluokkiin 1 tai 2 myös käyttäjämääränsä tai vaikutusalueensa mukaan. Näin ollen niiden kriittisyyden arviointi perustuisi tältä osin samoihin kriteereihin kuin viestintäverkon muidenkin osien.

Lisäksi viestintäverkon kriittisiä osia ovat täsmennyksen mukaisesti muun ohella olennaista osaa koko viestintäverkon liikenteestä ohjaavat komponentit. Tämä soveltuu myös erillisverkkoihin. Tällaisia ovat esimerkiksi runkoverkon keskittävät komponentit. Runkoverkossa voidaan välittää sekä matkaviestinverkon että kiinteän verkon liikennettä. Runkoverkossa välitetään ja ohjataan kaikki tai pääosa tukiasemien ja mobiiliverkon ytimen välisestä tai ytimen sisäisestä taikka kiinteän verkon liikenteestä. Runkoverkolla liitetään alueelliset verkot toisiinsa. Esimerkki tämän alakohdan piiriin kuuluvista verkon osista on operaattorin alueverkot yhdistävä IP/MPLS-verkko. Alakohdan soveltamista ei kuitenkaan ole rajattu runkoverkkoon tai ydinverkkoon, koska näiden määrittely ei ole yksiselitteistä.

Toisen täsmennyksen perusteella tämän alakohdan piiriin kuuluu myös konesaliverkko esimerkiksi silloin, kun sen avulla liitetään konesalissa tuotetut viestintäverkon kriittiset osat kuten mobiiliverkon ytimen keskeiset toiminnot runkoverkkoon.

2) Loppukäyttäjien pääsynhallinta, todentaminen ja valtuutus, verkon resurssien jakaminen loppukäyttäjille ja loppukäyttäjien yhteyksien ja istuntojen hallinta

Tämä alakohta kattaa toiminnot, joilla hallinnoidaan loppukäyttäjien ja siten loppukäyttäjien käyttämien päätelaitteiden pääsyä verkkoon, ylläpidetään käyttäjien istuntoja ja yhteyksien tilaa sekä todennetaan ja valtuutetaan loppukäyttäjät (päätelaitteet) ja huolehditaan verkon resurssien allokoinnista niille. Käyttäjien todentaminen, verkon resurssien jakaminen käyttäjille ja käyttäjäistuntojen hallinta ovat keskeisiä paitsi palvelun saatavuuden myös viestinnän luottamuksellisuuden säilymisen kannalta.

Tämän alakohdan piiriin kuuluvat muun ohella toiminteet, jotka mobiiliverkoissa vastaavat käyttäjän päätelaitteen todennuksesta ja todennuksen välittämisestä verkkojen välillä sekä yhteyksien (bearer) hallinnasta päätelaitteen ja verkon välillä. Kohdan alaan kuuluu myös osaltaan liikkuvuuden hallinta mobiiliverkoissa (mobility management).

Mobiiliverkoissa tämä alakohta kattaa muun ohella osaltaan eri verkoista tulevien yhteyksien todentamisen keskitetyssä komponentissa (Non-3GPP Access) sekä Authentication, Authorisation and Accounting (AAA) -toiminnallisuuden siltä osin kuin se liittyy loppukäyttäjien todentamiseen ja valtuutukseen.

Alakohtaan sisältyy resurssien allokoinnin osalta muun muassa IP-osoitteiden jakaminen käyttäjien päätelaitteille ja käyttäjiä palvelevat DNS-palvelimet, jotka ovat palvelun saatavuuden kannalta keskeisiä.

Alakohtaan sisältyvät myös verkon viipalointiin (network slicing) liittyvät toiminnallisuudet siltä osin kuin ne toteuttavat kohdan mukaisia toimintoja, kuten päätelaitteiden osoittamista verkon viipaleisiin. 5G:ssä viipalointiin osallistuvat useat verkon funktiot. Viipalointiin liittyviä keskeisiä turvallisuusriskejä ovat viipaleiden riittämätön eriyttäminen ja pääsynhallinta, jolloin riskinä on viipaleiden välinen tietovuoto tai viipaleiden jaetun laskentatehon varaaminen.

Näillä toiminnoilla kontrolloidaan ja ohjataan erityisesti käyttäjien pääsyä verkkoon, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät myös olennaisesti verkon liikenteen kontrollointiin, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

3) Viestintäverkon ja -palveluiden toimintojen rekisteröinti, todentaminen ja valtuutus

Tämän alakohdan mukaan viestintäverkon kriittisiä osia ovat verkon sisäisten eri toimintojen rekisteröinti ja keskinäinen todentaminen ja valtuutus. Viestintäverkon kriittisiä osia ovat esimerkiksi erilaiset verkon rekisterit, joilla ylläpidettäisiin tietoja verkon toiminnoista, ja verkon toiminnot, jotka vastaisivat muiden toimintojen valtuuttamisesta (Authentication, Authorisation and Accounting (AAA)).

Näillä toiminnoilla kontrolloidaan ja ohjataan pääsyä verkkoon, kuten verkon eri toimintojen pääsyä verkon muihin toimintoihin, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät myös olennaisesti verkon kontrollointiin, käyttäjien verkkoon pääsyn hallintaan, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

4) Viestintäverkon ja -palvelun toiminnalle välttämättömät, sen toimintaa tukevat infrastruktuuripalvelut

Tämän alakohdan mukaan viestintäverkon kriittisiä osia ovat viestintäverkon ja -palvelun toiminnalle välttämättömät sen toimintaa tukevat infrastruktuuripalvelut. Tällaisia toimintoja ovat muun muassa:

- tietovarastot, jotka pitävät sisällään verkon kriittisten toimintojen tietoja ja käyttäjien tietoja

- verkon komponentteja palvelevat verkon ytimen sisäiset osoitteenmääritys- ja nimipalvelut, kuten DNS- ja DHCP-palvelut

- aikapalvelut, joita hyödynnetään verkon kriittisissä osissa ajan synkronointiin (nämä vaikuttavat muun muassa avaintenhallintaan ja lokitukseen)

- keskitetty aikapalvelujärjestelmä, joka välittää ja varmistaa tukiasemien aika- ja vaihesynkronointisignaalin[22].

Näillä toiminnoilla kontrolloidaan ja ohjataan verkon eri toimintojen pääsyä verkkoon sekä verkossa kulkevaa synkronointiliikennettä, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät myös olennaisesti verkon kontrollointiin, käyttäjien verkkoon pääsyn hallintaan, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

5) Toiminnot, joilla toteutetaan viestintäverkkojen tai -palvelujen väliset rajapinnat mukaan lukien verkkovierailu

Tämän alakohdan mukaan viestintäverkon kriittisiä osia olisivat toiminnot, joilla toteutetaan viestintäverkon tai -palvelun rajapinnat muille viestintäverkoille ja -palveluille. Tällä tarkoitetaan etenkin verkon ytimen ulkoisia rajapintoja, joiden avulla avataan pääsy verkon palveluihin muista verkoista tai palveluista, jotka voivat olla joko teleyrityksen tai erillisverkkotoimijan omia tai toisen toimijan tuottamia.

Viestintäverkon kriittisiä osia olisivat muun ohella myös verkkovierailuun (roaming) liittyvät rajapinnat, joita avataan esimerkiksi IPX-toimijoille ja joilla mahdollistetaan verkkojen väliset yhteydet. Tässä tarkoitetuilla rajapinnoilla voidaan mahdollistaa myös pääsy verkon toiminnallisuuksiin esimerkiksi langattoman lähiverkon kautta. Viestintäverkon kriittiseksi osaksi katsottaisiin myös verkon käyttäjien internetyhdyskäytävä sekä rajapinnat teleyrityksen tai erillisverkkotoimijan sisäisiin muihin järjestelmiin kuten IMS-verkkoon.

Ulkoisten rajapintojen kautta voi olla mahdollista tunkeutua ydinverkon toimintoihin, heikentää verkon toimintaa tai saada luottamuksellisia tietoja verkon toiminnoista ja sen käyttäjistä. Rajapintatoteutuksia on useita erilaisia, ja niiden turvallisuusominaisuudet ovat laajalti standardointityön ulkopuolella.

Näillä toiminnoilla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä sekä palveluiden verkkoon pääsyä, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät myös olennaisesti verkon kontrollointiin, käyttäjien verkkoon pääsyn hallintaan, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

6) Toiminnot, joiden avulla viestintäverkot tai -palvelut yhteenliitetään, kun toiminto voi olennaisesti vaikuttaa viestintäverkkoon pääsyyn tai verkossa kulkevaan liikenteeseen

Tämä alakohta kattaa yhdysliikennepisteet ja suoran yhteenliittämisen muiden verkkojen ja palvelujen kanssa, jolloin liikenne välittyy viestintäverkkojen välillä. IP-runkoverkon lisäksi viestintäverkon ja sen palveluiden toiminnan kannalta keskeisiä ovat

[22] Mukaan lukien ainakin ePRTC (Enhanced Primary Reference Time Clock), T-GM (Telecom Grandmaster) ja atomikello. Sama järjestelmä voi mahdollisesti välittää tukiasemille keskitetysti satelliittipaikannusjärjestelmän kautta saatavan synkronointisignaalin normaalitilanteessa varmistuksen lisäksi. Tällä järjestelmällä ei tarkoiteta signaalin siirtämiseen käytettyjä siirtoverkon komponentteja, jotka ovat tyypillisesti samat kuin muulle tietoliikenteelle ja jotka voivat olla viestintäverkon kriittisiä osia tämän määräyksen muiden kohtien perusteella.

IP-transit ja reitityspisteet muiden operaattoreiden verkkoihin ja internetverkkoon. Yhteenliittämisen olennaista vaikutusta viestintäverkon liikenteeseen arvioitaisiin suhteessa kyseisen liikennelajin liikenteeseen verkossa.

Alakohta sisältää esimerkiksi internetliikenteen yhteenliittämispisteen (IXP) ja mobiilioperaattoreiden yhteenliittämispisteen (DIX). Siirtotie yhdysliikennepisteeseen voi olla osa operaattorin runkoverkkoa, jonka komponentit olisivat alakohdan 1 kriteereillä viestintäverkon kriittisiä osia.

Näillä toiminnoilla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät olennaisesti verkkojen välisen liikenteen ja palveluiden saatavuuteen sekä viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

7) Viestintäverkon, sen toimintojen ja loppukäyttäjien liikenteen salauksen ja avainten keskitetty hallinta

Tämä alakohta kattaa viestintäverkon laitteiden, ohjelmistojen ja käyttäjien salausavainten luomiseen, säilytykseen ja välittämiseen, eheyden varmistamiseen sekä muuhun niiden elinkaareen liittyvät keskitetyt toiminnot. Toimintoa voidaan pitää keskitettynä, vaikka se olisi fyysisesti hajautettu esimerkiksi useampaan laitetilaan. Kohta sisältää myös toiminnot, jotka osallistuvat varmennehierarkiaan ja/tai joilla luodaan ja välitetään avaimia sekä välitetään niiden voimassaolotietoja (CRL eli Certificate Revocation List tai vastaava).

Alakohta koskee paitsi käyttäjien ja verkon välistä myös verkon komponenttien ja funktioiden välistä todentamista ja salausta.

Alakohta kattaa erityisesti seuraavat alueet: verkon tukiasemien ja verkon ytimen välisen liikenteen salaukset (mukaan lukien tukiasemien langattomat siirtoyhteydet), runkoverkon komponenttien käyttämät salaukset ja verkon ytimessä olevien funktioiden salaukset. Se sisältää myös viestintäverkon kriittisten osien käyttämien tietovarastojen salauksen. Alakohta ei kata esimerkiksi käyttäjän ja tukiaseman välistä radioliikenteen salausta radiorajapinnassa.

Näillä toiminnoilla kontrolloidaan ja ohjataan verkossa kulkevaa käyttäjäliikennettä sekä käyttäjien verkkoon pääsyä, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät olennaisesti viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

8) Viestintäverkon kriittisiin osiin vaikuttavat tietoturvatoiminnot

Alakohta kattaa toiminnot, joiden tehtävä on valvoa, ohjata, rajoittaa tai suodattaa verkon liikennettä tai käsitellä viestintäverkon kriittisiin osiin liittyvien järjestelmien lokitietoja. Alakohta kattaa myös toiminnot, joiden tehtävä on hallita ja valvoa verkon ylläpitoon tai hallintaan liittyviä toimenpiteitä.

Tietoturvatoiminnot suojaavat esimerkiksi ydinverkkoa radioverkon suunnasta ja ulkopuolisista verkoista tulevilta uhilta mutta myös ydinverkon funktioita sen sisäisiltä uhilta. Tietoturvatoiminnot, kuten palvelimissa olevat tietoturvaohjelmistot, mahdollistavat kriittisten järjestelmien alustojen tai niiden käyttöjärjestelmien ohjaamisen. Alakohta kattaa myös tietoturvatoiminnot, jotka kohdistuvat muihinkin viestintäverkon kriittisiin osiin kuten hallintayhteyksiin.

Tässä alakohdassa tarkoitettu verkon ydintä suojaava tietoturvafunktio voi olla toteutettu verkkoarkkitehtuurin kannalta myös ydinverkon ulkopuolella. Alakohta sisältää myös muut viestintäverkon kriittisiksi osiksi määriteltyihin toimintoihin kuten hallintajärjestelmiin vaikuttavat tietoturvatoiminnot.

Tietoturvatoiminnot erottelevat verkon eri turvallisuusvyöhykkeet ja verkkosegmentit sekä suodattavat ja valvovat tietoliikennettä niiden välillä. Näitä ovat muun muassa:

- verkon ytimen ja siirtoverkon sekä radioverkon väliset segmentit ja
- OSS- ja BSS-järjestelmien keskinäiset rajapinnat ja niiden rajapinnat viestintäverkkoon sekä
- edellisten välisen tai niiden sisäisen liikenteen valvontaan ja kontrollointiin tarkoitetut toiminteet, kuten palomuurit, tunneloidun liikenteen operaattorin verkon eri turvavyöhykkeiden (security domain) välillä terminoivat Security Gatewayt ja reunayhdyskäytävät (Border Gateway), joita käytetään yhden operaattorin eri verkkojen tai eri operaattorien verkkojen välisen liikenteen kontrollointiin ja ohjaamiseen.

Tietoturvatoiminnot voivat olla myös verkon virtualisoituja toiminteita (NVF), jotka tuottavat verkon palveluita ja ohjelmistoja virtuaalisesti. Ne voivat jakaa saman alustan muiden vastaavien ohjelmistojen kanssa.

Alakohdan alaan kuuluvat myös tietoturvatoiminnot, joiden tehtävä on ohjata ja välittää verkon palveluita ulkopuolisiin verkkoihin kuten roaming-verkkoihin tai muihin matkapuhelinverkon ulkopuolisiin verkkoihin. Esimerkkeinä voidaan mainita Diameter Edge Agent ja 5G-verkon osalta SEPP-yhdyskäytävä, joka toimii välittäjänä eri operaattorien verkkojen välisen liikenteen ja palvelujen toteuttamisessa ja jonka tehtäviin kuuluu verkon ytimen palveluiden viestinnän suojaaminen operaattorien välisen yhdysverkon suuntaan. Muita esimerkkejä tietoturvatoiminnoista, jotka voivat olla myös virtualisoituja, ovat verkon tietoturvaohjelmistot kuten palomuurit, liikenteen suodatusohjelmistot tai verkkoinfrastruktuurissa käytettävät tukiohjelmistot kuten DHCP- tai DNS-palvelut.

Näillä toiminnoilla kontrolloidaan ja ohjataan verkon sisäistä liikennettä sekä verkkoon pääsyä, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät olennaisesti viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

9) Verkonhallinta- ja verkonvalvontajärjestelmät ja eräät muut laskutus-, tuki- ja taustajärjestelmät

Tämän alakohdan mukaan viestintäverkon kriittisiä osia ovat yhtäältä verkonhallinta- ja verkonvalvontajärjestelmät, kun ne liittyvät joko suoraan viestintäverkon kriittisten osien hallintaan tai valvontaan taikka kun ne voivat muutoin olennaisesti vaikuttaa verkkoon pääsyyn tai verkossa kulkevaan liikenteeseen. Toisaalta viestintäverkon kriittisiä osia ovat myös muut tuki- ja taustajärjestelmät, jotka voivat olennaisesti vaikuttaa viestintäverkkoon pääsyyn tai verkossa kulkevaan liikenteeseen.

Verkonhallinta- ja verkonvalvontajärjestelmät ovat viestintäverkon kriittisiä osia siis ensinnäkin silloin, kun ne liittyvät muulla perusteella viestintäverkon kriittiseksi osaksi katsottavan toiminnon hallintaan tai valvontaan. Toiseksi tässä tarkoitetut toiminnot ovat viestintäverkon kriittisiä osia silloin, kun ne muutoin voivat olennaisesti

vaikuttaa viestintäverkkoon pääsyyn tai siellä kulkevaan liikenteeseen esimerkiksi hallittavien elementtien määrän johdosta, vaikka esimerkiksi yksittäinen hallittava elementti ei olisikaan viestintäverkon kriittinen osa. Esimerkiksi tukiasemien hallintajärjestelmä voi olla viestintäverkon kriittinen osa tällä perusteella siinäkin tilanteessa, jossa yksittäistä tukiasemaa itsessään ei katsottaisi viestintäverkon kriittiseksi osaksi, koska tukiasemien hallintajärjestelmällä voi vaikuttaa käyttäjien verkkoon pääsyyn tai jopa estää se kokonaan sekä tukiasemien välittämään liikenteeseen esimerkiksi hidastamalla sitä.

Verkonhallinta- ja verkonvalvontajärjestelmillä tarkoitetaan tässä ohjelmistoja, laitteita tai rajapintoja, joiden avulla operoidaan, ylläpidetään tai muutoin hallitaan ja valvotaan viestintäverkon eri resursseja kuten tukiasemia, tietoturvajärjestelmiä, verkkolaitteita ja verkon ylläpitoon tarkoitettuja ohjelmistoja.

Verkonhallinta- ja verkonvalvontajärjestelmiä ovat esimerkiksi ns. OSS-järjestelmät (Operations Support Systems) ja MANO- (Management and Orchestration) järjestelmät sekä niiden käyttämät rajapinnat BSS-järjestelmiin (Business Support Systems). OSS- ja BSS-järjestelmät voivat olla yhteydessä toisiinsa verkkoarkkitehtuurista riippuen palveluväylän avulla, joka tällöin muodostaa kriittisenä osana pidettävän rajapinnan. Myös verkon optimointiin ja ohjaukseen käytetyt automaattiset järjestelmät voivat kuulua tämän alakohdan piiriin yllä mainituilla edellytyksillä kokonaan tai osittain. Tällaisia ovat esimerkiksi verkon suorituskyvystä tietoa keräävät järjestelmät, jotka ohjaavat verkkoa esimerkiksi toimittamalla verkkoa ohjaavaa analysoitua tietoa takaisin verkon funktioille. Tämä alakohta kattaa myös esimerkiksi IPAM-järjestelmät, joilla hallitaan osoitteenmääritystä verkossa sekä Liikenne- ja viestintäviraston määräyksen 66A 4.2 §:ssä tarkoitetut järjestelmät viestintäverkon tai -palvelun valvontatietojen vastaanottamiseen ja analysointiin.

MANO-toiminteisiin kuuluvat ohjelmisto-ohjatun verkon mm. NFV-orkestrointia tuottavat komponentit. Niiden päätehtäviin kuuluu ohjata, määritellä ja yhdenmukaistaa verkkokomponenttien välisiä yhteyksiä ohjelmisto-ohjatuissa verkoissa. Tämän alakohdan mukaiset toiminnot kattavat myös VIM- ja VNF-toiminteet, joiden tehtävänä on hallita verkon virtuaalista infrastruktuuria alustoineen ja sen käyttämiä palvelukomponentteja. Myös verkon viipaloinnin hallinta sisältyisi tähän kohtaan. Myös ohjelmisto-ohjatut verkot (Software Defined Networking, SDN) kuuluu tähän alakohtaan. SDN:llä tarkoitetaan verkkotoimintojen virtualisointia ja niiden siirtämistä yhdenmukaiselle ohjaustasolle, jossa verkon ominaisuuksia voidaan hallita ohjelmistorajapintojen kautta. Esimerkiksi 5G-verkkojen osalta hallintaa voidaan automatisoida ja hallita ohjelmallisesti ja dynaamisesti muuttuvien tarpeiden mukaisesti.

Muiden laskutus-, tuki- ja taustajärjestelmien (mm. BSS) osalta alakohta kattaa järjestelmät, joilla voidaan olennaisesti vaikuttaa viestintäverkkoon pääsyyn tai verkossa kulkevaan liikenteeseen esimeriksi palveluiden saatavuuden osalta. Esimerkiksi liittymien provisiointiin vaikuttavilla järjestelmillä voi olla mahdollista väärinkäytöksen tai ohjelmistovirheen takia sulkea kerralla suuri määrä liittymiä pois verkosta.

Laskutusjärjestelmällä tarkoitetaan tässä sekä verkon ytimen veloituksen tekniseen toteuttamiseen liittyviä toimintoja että ytimen ulkopuolista laskutusta tukevaa järjestelmää. Vaikka verkko voi toimia ilmankin laskutusjärjestelmää, laskutusta voidaan pitää viestintäverkon kriittisenä osana, jos se voi vaikuttaa olennaisesti palvelujen saatavuuteen tai viestinnän luottamuksellisuuteen. Laskutusjärjestelmän toiminnot voidaan tyypillisesti jakaa online- ja offline-toimintoihin. Matkaviestinverkkojen osalta verkon laskutuksen hallinta ja arkkitehtuuri on määritelty 3GPP:n teknisessä

määrityksessä 32.240. Laskutusjärjestelmä voi vaikuttaa palvelun saatavuuteen online-laskutuksen tapauksessa siten, että järjestelmä voi estää reaaliaikaisesti käyttäjän pääsyn verkkoon tai sen palveluihin toteuttamalla kiintiönhallintapalvelun (quota management), jolloin se myöntää tai evää käyttäjiltä pääsyn palveluun aika- tai datapohjaisesti. Laskutusjärjestelmä kerää ja käsittelee laskutustietoja, jotka voivat sisältää luottamuksellista viestintää kuvaavia tietoja esimerkiksi viestinnän osapuolista. Laskutusjärjestelmä mahdollistaa pääsyn verkossa käsiteltyihin välitystietoihin, mikä voi vaarantaa viestinnän luottamuksellisuuden.

Näillä toiminnoilla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä sekä verkkoon pääsyä, minkä takia niitä on pidettävä viestintäverkon kriittisinä osina. Toiminnot liittyvät olennaisesti verkon ohjaukseen ja kontrollointiin, käyttäjien verkkoon pääsyn hallintaan sekä palveluiden saatavuuden ja viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen. Laskutusjärjestelmään kuuluvilla toiminnoilla voidaan kontrolloida ja ohjata verkkoon pääsyä, minkä takia niitä voidaan pitää viestintäverkon kriittisenä osana. Toiminnot liittyvät olennaisesti verkon liikenteen kontrollointiin sekä palveluiden saatavuuden varmistamiseen, mutta myös viestinnän luottamuksellisuuteen.

10) Telekuuntelun tai televalvonnan toteuttaminen

Tämän alakohdan mukaan viestintäverkon kriittisiä osia olisivat lawful interception-eli LI-toiminnallisuudet. Tämä alakohta koskee sekä erikseen LI:tä varten hankittuja komponentteja että muitakin verkon komponentteja, jotka suoraan liittyvät LI-toiminteen toteuttamiseen. 3GPP:n teknisissä spesifikaatioissa on määritelty funktioita, jotka toteuttavat LI-toiminnallisuuksia.

Tämä alakohta sisältää ne SVPL 243.1 §:n 16 kohdan ja SVPL 245 §:n edellyttämät viestintäverkon ja -palvelun tekniset apuvälineet ja ominaisuudet, joilla teleyritys varmistaa telekuuntelun ja televalvonnan teknisten ja toiminnallisten vaatimusten toteutumisen (ks. HE 221/2013 vp, s. 183-184 ja 187).

Näiden toiminnallisuuksien oikea toiminta on viestinnän luottamuksellisena säilymisen kannalta keskeistä. Toimenpiteestä riippuen ne liittyvät osaltaan ainakin liikenteen ohjaamiseen (telekuuntelutietojen tallentaminen), käyttäjien pääsyn hallintaan (televalvontaan kuuluva mahdollisuus osoitteen tai laitteen käytön tilapäiseen estämiseen, pakkokeinolaki (806/2011) 10:6 §) tai muuhun verkkoon pääsyyn (pääsy televalvonta- ja telekuuntelutietoihin).

11) Virtualisointi silloin, kun sitä käytetään viestintäverkon kriittisenä osana pidettävän toiminnon tai toimenpiteen toteuttamiseen

Tässä alakohdassa määritellään virtualisointi viestintäverkon kriittiseksi osaksi silloin, kun virtualisoidaan viestintäverkon kriittisiin osiin kuuluvia toiminnallisuuksia. Tällöin virtualisointialusta (virtualisointi-infrastruktuuri ja sen fyysinen alusta) hallitsee komponentteja, jotka puolestaan kontrolloivat ja ohjaavat verkkoa ja siellä kulkevaa liikennettä, ja on siksi viestintäverkon kriittinen osa. Virtualisoidussa viestintäverkossa verkon toiminnot ovat riippuvaisia virtualisointialustasta ja sen hallinta- ja orkestrointijärjestelmistä.

Ne viestintäverkon kriittiset osat, joiden virtualisointia kohta koskee, on pitkälti määritelty tämän määräyksen muissa kohdissa. Koska määräys ei ole tyhjentävä, viestintäverkon kriittisiä osia voivat SVPL 244 a §:n nojalla olla myös muut kuin tässä määräyksessä erikseen määritellyt viestintäverkon kriittiset osat. Määräyksen 3 kohdassa

velvoitetaan teleyritys tai erillisverkkotoimija tunnistamaan viestintäverkkonsa kriittiset osat. Virtualisointia koskeva kohta tarkoittaisi siis lähtökohtaisesti sitä, että teleyrityksen tunnistamien viestintäverkon kriittisten osien virtualisointi olisi myös viestintäverkon kriittinen osa.

Alakohdassa ei määritellä virtualisointia kriittiseksi sellaisenaan. Siinä tilanteessa, kun virtualisoidaan vain muita kuin viestintäverkon kriittisiksi osiksi katsottavia toimintoja ja toimenpiteitä, ei virtualisointiakaan pidettäisi viestintäverkon kriittisenä osana.

5G-verkon ydin perustuu virtualisoituihin palveluihin, joita voidaan tuottaa tyypillistä IT-infrastruktuuria muistuttavissa ympäristöissä, mutta myös aiempien verkkosukupolvien verkkotoimintoja voidaan virtualisoida. 5G-verkossa itse verkkotoiminnot ovat virtualisoitavissa, verkot ohjattavissa ohjelmistoilla ja verkon kapasiteetti jaettavissa virtuaalisiin viipaleisiin erilaisten tarpeiden mukaisesti. Verkkotoimintojen virtualisoinnilla (Network Function Virtualization, NFV) tarkoitetaan 5G-verkkotoimintojen toteuttamista ohjelmallisesti perinteisten verkkolaitteiden sijaan. Virtualisointialustat ovat jaettavissa useiden funktioiden tai ohjelmistojen kesken. Alustojen turvallisuus muodostuu kriittiseksi tekijäksi koko verkon tietoturvan varmistamisessa.[23] Virtualisointialustalla voidaan toteuttaa yksi tai useampi verkon toiminto.

Alakohdan mukaisin kriteerein viestintäverkon kriittisiä osia voisivat olla 5G-verkoissa ainakin verkon virtualisoidut funktiot (Virtual Network Functions, VNF), verkon funktioiden virtualisointi-infrastuktuuri (NFV Infrastructure, NFVI), virtualisoitujen funktioiden ja virtualisoinnin hallinta ja orkestrointi sekä virtualisoinnin fyysinen alusta. Virtualisoitujen funktioiden ja virtualisoinnin hallinta toteutetaan MANO-järjestelmällä, johon sisältyvät ainakin NFV Orchestrator (NFVO, vastaa mm. resurssien orkestroinnista VIM:ien välillä), VNF Manager (VNFM, joka vastaa VNF-instanssien hallinnasta) ja Virtualised Infrastructure Manager (VIM, joka ohjaa virtualisointi-infrastuktuurin (NFVI) toimintaa).[24]

12) Viestintäverkon kriittisenä osana pidettävän virtualisoinnin avulla toteutetut toiminnallisuudet

Tämän alakohdan perusteella viestintäviraston kriittisenä osana pidetään muutakin kuin yllä mainittua tai muuten viestintäverkon kriittiseksi osaksi katsottavaa toimintoa tai toimenpidettä, kun se toteutetaan edellä kohdassa 11 tarkoitetun viestintäverkon kriittisenä osana pidettävän virtualisoinnin avulla. Edellisessä alakohdassa määritellään itse virtualisointi viestintäverkon kriittiseksi osaksi tietyissä tilanteissa. Silloin kun virtualisointi katsotaan viestintäverkon kriittiseksi osaksi, määritellään tässä alakohdassa muukin samassa virtualisointiympäristössä toteutettu toiminnallisuus viestintäverkon kriittiseksi osaksi.

Kun virtualisoidut toiminnot jakavat resursseja, aiheutuu siitä tietoturvariskejä ja riippuvuuksia virtualisoitujen toimintojen välille, ja toimintojen voi olla mahdollista vaikuttaa muihin virtualisoituihin toimintoihin. Pääsy alustaan virtualisoidusta toiminnosta vaarantaisi muut toiminnot. Tästä syystä kaikkia samalla kriittisellä virtualisointialustalla toteutettuja toimintoja on perusteltua pitää verkon kriittisisinä osina ja katsoa, että niitä käytetään tällöin viestintäverkon kriittisessä osassa, vaikka jotkin

[23] Virtualisoinnin tietoturvauhista ks. esim. 3GPP TR 33.848 V0.5.0 (2019-11). Study on Security Impacts of Virtualisation. https://www.3gpp.org/DynaReport/33848.htm.
[24] Ks. virtualisoinnista 5G-verkossa ENISA Threat Landscape for 5G Networks, k. 3.7.

niistä erillisellä alustalla toteutettuna eivät olisikaan viestintäverkon kriittisiä osia. Esimerkiksi jos tukiaseman keskusyksikkö (Central Unit, CU) ei muutoin olisi viestintäverkon kriittinen osa, mutta se virtualisoitaisiin samalla alustalla kuin viestintäverkon kriittisinä osina pidettäviä ytimen toimintoja, katsottaisiin myös CU viestintäverkon kriittiseksi osaksi tämän alakohdan perusteella.

Tämä alakohta ei sinänsä estä toteuttamasta samalla alustalla kriittisiä ja muutoin ei-kriittisiä toimintoja, vaan samalla virtualisointialustalla toteuttaminen ainoastaan tuo muutoin ei-kriittisenä pidettävät virtualisoidut toiminnot 244 a §:n soveltamisen piiriin. Teleyrityksen on mahdollista toteuttaa toiminnot samalla alustalla, jos se pystyy näin toimiessaan silti huolehtimaan muun sääntelyn mukaisista velvoitteistaan.

13) Keskeiset toiminnot ja toimenpiteet, joilla mahdollistetaan pääsy viestintäverkossa käsiteltäviin liittymän tai päätelaitteen maantieteellistä sijaintia koskeviin tietoihin tai jotka mahdollistavat sijainnin selvittämisen viestintäverkon avulla

Liittymän tai päätelaitteen ja sitä kautta käyttäjän maantieteellisen sijainnin paljastavat tiedot (paikkatiedot) ovat potentiaalinen väärinkäytön kohde, ja ne voivat altistaa käyttäjiä jopa fyysisille uhille. Kyse voi olla välitystiedoista, joita normaalisti käsitellään viestinnän välittämiseen ja jotka samalla ilmaisevat käyttäjän sijainnin tietyllä tarkkuudella, tai sijaintitiedoista, joita käsitellään muuhun kuin viestinnän välittämiseen. Paikantamiseen liittyvät palvelut/komponentit verkossa eivät aina liity suoraan viestinnän välittämiseen, vaan niitä voidaan käyttää ns. lisäarvopalveluihin, eivätkä siten välttämättä kaikilta osin kuulu edellisten alakohtien piiriin. Välitystiedon, sijaintitiedon ja lisäarvopalvelun käsitteet on määritelty SVPL 3 §:ssä.

Alakohdan mukaan viestintäverkon kriittisiä osia olisivat ensinnäkin toiminnot ja toimenpiteet, jotka mahdollistavat pääsyn viestintäverkossa käsiteltäviin liittymän tai päätelaitteen maantieteellistä sijaintia koskeviin tietoihin, kuten sinne tallentuneisiin välitys- tai sijaintitietoihin. Näillä toiminnoilla voidaan katsoa kontrolloitavan tai ohjattavan verkkoon pääsyä, joten niitä on pidettävä viestintäverkon kriittisinä osina. Toiseksi viestintäverkon kriittisiä osia olisivat toiminnot ja toimenpiteet, jotka mahdollistavat liittymän tai päätelaitteen maantieteellisen sijainnin selvittämisen. Sijainnin selvittämisen voidaan katsoa perustuvan verkon ja sen liikenteen kontrollointiin.

Alakohdan tarkoittamia toimintoja olisivat esimerkiksi:

- Gateway Mobile Location Centre (GMLC), joka tukee sijaintiin perustuvien palvelujen tarjoamista ja jonka avulla mahdollistetaan tietoihin oikeutetuille toiminnoille tai ulkopuolisille palveluntarjoajille, kuten käyttäjän suostumuksen perusteella tietoja käsittelevälle lisäarvopalvelun tarjoajalle, kyselyjen tekeminen käyttäjän sijainnista ja pääsy sijaintia koskeviin tietoihin (3GPP TS 23.273, Rel. 16)

- Enhanced Serving Mobile Location Center (E-SMLC), joka tukee päätelaitteen sijainnin selvittämistä LTE-verkossa (3GPP TS 23.271)

- Location Management Function (LMF), joka tukee päätelaitteen sijainnin selvittämistä 5G-verkossa (3GPP TS 23.273).

Yllä mainittuja toimintoja hyödynnetään esimerkiksi hätäpaikannuksessa.[25] Sijaintia koskevien verkon palvelujen toteuttamiseen osallistuvat lisäksi useat muut toiminnot, jotka on määritelty kriittiseksi joko edellä olevissa alakohdissa tai jäljempänä tämän määräyksen muissa kohdissa.

5. 4G-verkon kriittiset osat

5.1. 4G-verkon kriittisten osien määrittely

Kohdassa määritellään ne verkon toiminnallisuudet, jotka ainakin ovat 4G-verkon kriittisiä osia, viittaamalla 3rd Generation Partnership Projectin (3GPP) teknisen määrityksen TS 23.002 mukaisiin verkon ytimen toiminnallisuuksiin. Kohdan ensimmäinen alakohta on suurelta osin luonteeltaan selkeyttävä siten, että siinä tuodaan esiin se lähtökohta, että ytimen toiminnallisuudet ovat viestintäverkon kriittisiä osia.

Ensimmäisessä alakohdassa määrätään, että viestintäverkon kriittisiä osia ovat 4G-verkon ytimen toimintojen ja toimenpiteiden osalta 3GPP:n teknisen määrityksen TS 23.002 kohdan 4.1.1, 4.1.4 ja 4.1.5 mukaiset pakettikytkentäiset toiminnallisuudet siltä osin kuin ne kontrolloivat tai ohjaavat olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Näin ollen kaikki mainittuihin kohtiin sisältyvät toiminnallisuudet eivät kuitenkaan ehdottomasti ole viestintäverkon kriittisiä osia. Ensimmäiseen alakohdan täsmennyksellä "pakettikytkentäiset" on tarkoitus rajata pois lueteltuihin kohtiin sisältyvät piirikytkentäiset toiminnallisuudet[26]. Toiminnallisuudet on voitu kohdassa tarkoitetulla tavalla määritellä teknisessä määrityksessä 23.002 myös viittaamalla siinä toisiin 3GPP:n määrityksiin.

Kohdan toisessa alakohdassa puolestaan määritellään ne 4G-verkon toiminnallisuudet, joita ainakin on pidettävä viestintäverkon kriittisinä osina. Määräyksen taulukossa 1 mainittujen toiminnallisuuksien osalta tarkempi analyysi viestintäverkon osan kriittisyydestä ei olisi tarpeen, vaan ne olisi katsottava oletusarvoisesti viestintäverkon kriittisiksi osiksi. Määräyksen 7 kohta sisältää kuitenkin tätä koskevan poikkeusmahdollisuuden. Määräyksen 7 kohdassa mahdollistetaan se, että muutoin viestintäverkon kriittiseksi osaksi katsottava toiminnallisuus voidaan tietyin edellytyksin katsoa ei-kriittiseksi, kun sillä tuetaan verkon reunalla tuotettavia palveluita ja on toteutettu mekanismit viestintäverkon kriittisten osien suojaamiseksi.

Ensimmäinen alakohta ja toisessa alakohdassa viitattu taulukko kriittisistä osista eivät ole miltään osin tyhjentäviä, vaan lisäksi teleyrityksen tai erillisverkkotoimijan on arvioitava, onko sen verkossa taulukossa mainittujen lisäksi muita kriittisiä osia. Luettelon rinnalla olisi siis sovellettava paitsi määräyksen 4 kohdan mukaista kaikille verkoille yhteistä kriittisten osien määrittelyä myös SVPL 244 a §:n 1 momentin mukaista viestintäverkon kriittisen osan määritelmää sellaisenaan.

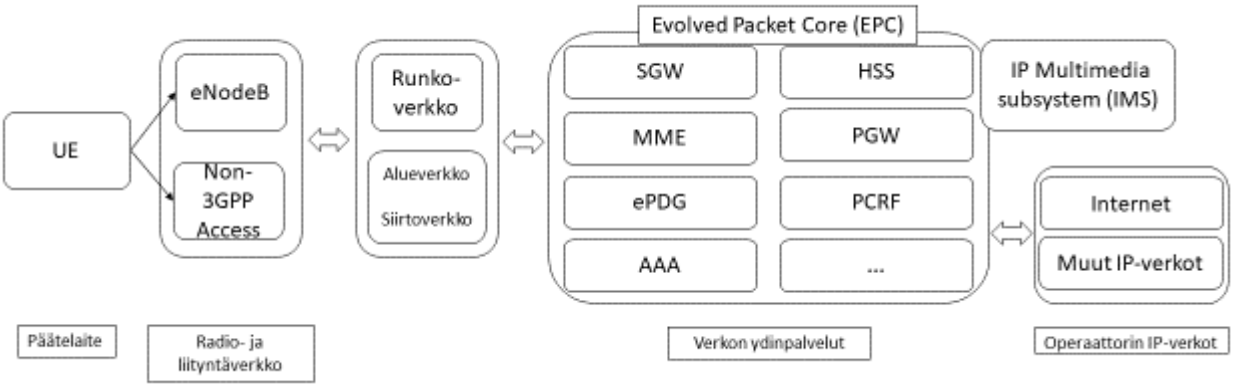
3GPP:n määritysten mukaiset funktiot (toiminnallisuudet) ovat loogisia ja useaan sovellukseen hajautettuja. Kohdan mukaan verkon osa olisi kriittinen, vaikka se toteuttaisi vain osan kriittiseksi määritellystä toiminnallisuudesta. Tästä ja toiminnallisuuteen perustuvasta määrittelytavasta seuraisi, että kun yksittäisen ohjelmistokomponentin voidaan osoittaa toteuttavan osaksikaan jonkin verkon kriittiseksi osaksi määritellyn toiminnallisuuden, olisi komponentti katsottava verkon kriittiseksi osaksi,

[25] Network Induced Location Request (NI-LR). https://itectec.com/spec/6-10-procedures-dedicated-to-support-regulatory-services/.
[26] Kuten tekstiviestin toimittamiseen tukiasemille tai tukiasemilta tekstiviestikeskukselle liittyvät SMS-GMSC (SMS Gateway MSC) ja SMS Interworking MSC (SMS-IWMSC).

vaikkei se koko toiminnallisuutta toteuttaisikaan. Yksittäinen ohjelmistokomponentti tai verkkolaite voi toteuttaa myös useamman kuin yhden toiminnallisuuden.

Selvänä olisi pidettävä, että 5G NSA -verkkojen tapauksessa hyödynnettyjen 4G-verkon osien kriittisyyttä arvioitaisiin lähtökohtaisesti sen mukaan, mitä 4G-verkon osista määräyksessä määrätään. 5G NSA -verkko perustuu 4G-verkon EPC-ytimeen. Tämän määräyksen kannalta 4G-verkon kriittisten osien luettelo koskee siis myös 5G NSA -verkon hyödyntämiä 4G-verkon toimintoja.

Kuvassa 1 on kuvattu yleisellä tasolla LTE-teknologiaan perustuvan viestintäverkon arkkitehtuuri yleisellä tasolla. Kuvassa mainittua IP Multimedia Subsystemiä käsitellään määräyksen kohdassa 8. Kaikki seuraavassa kuvatut toiminnallisuudet sijoittuvat osaksi kuvan mukaisia verkon ydinpalveluita.



Kuva 1 Esimerkki 4G-verkon arkkitehtuurista yleisellä tasolla

Määräyksen luettelon 1 laadinnassa on otettu vertailukohtana huomioon vastaavan kaltainen luettelo, joka on laadittu Yhdistyneessä kuningaskunnassa. Yhdistyneessä kuningaskunnassa on kansallisen kyberturvallisuuskeskuksen ohjauskirjeessä kiinnitetty teleyritysten huomiota 5G-verkkojen ohella tiettyihin 4G-verkkojen sekä kaikille verkoille yhteisiin erityisen riskialttiiksi nähtyihin funktioihin.[27]

5.2. 4G-verkon kriittisiä toiminnallisuuksia

Home Subscriber Server (HSS)

Home Subscriber Server (HSS) on keskustietokanta, joka sisältää tiedot käyttäjän istuntojen ja yhteyksien käsittelemiseksi LTE-teknologiaan perustuvassa viestintäverkossa. Matkaviestinverkossa voi olla yksi tai useampia keskustietokantoja riippuen verkon käyttäjämäärästä ja arkkitehtuurista.

[27] NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, kohta 11.a. 28.1.2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks. Ks. myös kohta 12. Nämä funktiot ovat 4G:n osalta seuraavat: "mobile core functions, including Home Subscriber Server (HSS), Packet Gateway (PGW), Policy and Charging Rules Function (PCRF) and, in some cases, the Mobility Management Entity (MME) and Serving Gateway (SGW)."

HSS vastaa käyttäjien pääsynhallinnasta, käyttäjien tunnistamisesta, käyttäjäprofiilista sekä liikkuvuuden hallinnasta (esimerkiksi tarjoamalla tiedon käyttäjää palvelevasta MME:stä). HSS vastaa myös avainten hallinnasta sekä käyttäjän ja viestintäverkon todentamisvektoreiden luomisesta. HSS:llä on myös rooli telekuuntelun tai televalvonnan toteuttamisessa (Lawful Interception- eli LI-toiminnallisuuksissa).

HSS sisältää 3GPP:n teknisten määrittelyjen mukaan nykyisin kotirekisterin (HLR, Home Location Register) ja tunnistuskeskuksen (AuC, Authentication Centre) toiminnallisuudet.[28]

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien pääsyä verkkoon, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti viestintäverkon ja sen liikenteen ohjaukseen ja hallintaan, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Equipment Identity Register (EIR)

EIR eli laitetunnusrekisteri on matkaviestinverkon tietokanta, johon tallennetaan kansainvälisiä matkaviestimien laitetunnuksia (IMEI) ja joka sisältää tiedot matkaviestimien käytön luvallisuudesta. EIR:n mustalle listalle asetettujen päätelaitteiden normaali käyttö viestintäverkossa on estetty.

Tällä toiminnolla kontrolloidaan käyttäjien verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy luvattomien laitteiden käytön estämiseen verkossa ja sitä kautta olennaisesti verkon palveluiden saatavuuden varmistamiseen.

Subscription Locator Function (SLF)

SLF välittää verkon funktioille (AAA, AS, I-CSCF) käyttäjädatan sisältävän keskustietokannan (HSS) nimen, kun niitä on matkaviestinverkossa useampi kuin yksi.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien pääsyä verkon palveluihin, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy olennaisesti myös viestintäverkon ja sen liikenteen ohjaukseen ja hallintaan, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Mobile Management Entity (MME)

MME (liikkuvuudenhallintayksikkö) on vastuussa päätelaitteiden ohjausliikenteen terminoinnista, päätelaitteiden rekisteröinnistä ja yhteyksien hallinnasta sekä liikkuvuuden hallinnasta. Sillä on myös rooli verkkovierailussa. MME toteuttaa myös LI-toiminnallisuuksia.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien pääsyä verkkoon, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti viestintäverkon ja sen liikenteen ohjaukseen ja hallintaan, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

[28] 3GPP TS 23.002, k. 4.1.1.1.1–4.1.1.1.2.

Serving Gateway (SGW)

SGW (palveleva yhdyskäytävä) vastaa käyttäjätason liikenteen reitittämisestä ja hallinnasta tukiasemien ja PDN-GW:n välillä. MME ohjaa SGW:tä kanssa uusien yhteyksien luomiseksi ja olemassa olevien muokkaamiseksi päätelaitteen ja verkon välillä. SGW toteuttaa myös LI-toiminnallisuuksia.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy olennaisesti myös viestintäverkon yhteyksien ylläpitoon sekä palveluiden saatavuuden ja viestinnän luottamuksellisuuden varmistamiseen.

Packet Data Network Gateway (PDN GW)

PDN-GW (pakettikytkentäisen verkon yhdyskäytävä) on rajapintatoiminto operaattorin sisäisen IP-verkon ja ulkoisen IP-verkon välissä. PDW-GW vastaa IP-osoitteiden jakamisesta päätelaitteille. Se myös valvoo käyttöpolitiikkaa. PDN-GW:llä tehdään myös liikenteen suodatusta ja analyysiä, jonka perusteella voidaan toteuttaa laskutusta sekä kontrolloida liikennettä. PDN-GW toteuttaa myös LI-toiminnallisuuksia.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy olennaisesti myös viestintäverkon yhteyksien ylläpitoon sekä palveluiden saatavuuden ja viestinnän luottamuksellisuuden varmistamiseen.

Evolved Packet Data Gateway (ePDG)

ePDG:n avulla toteutetaan matkaviestinverkon ulkopuolisten (non-3GPP-access) käyttäjien yhteys reitittämällä liikennettä PDN-GW:n ja käyttäjän välillä. EPDG:llä toteutetaan yleisesti VoWiFi-palvelu (Voice over WiFi, langattoman lähiverkon avulla toteutettava puhelupalvelu).

ePDG aktivoi käyttäjän ja ePDG:n välisen avaintenvaihdon sekä perustaa IPSec-tunnelin turvamaan rajapinnalla tapahtuvan viestinnän. ePDG myös toteuttaa IPSec-tunnelin todentamisen ja valtuutuksen. ePDG toteuttaa myös LI-toiminnallisuuksia.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy olennaisesti myös viestintäverkon yhteyksien ylläpitoon sekä palveluiden saatavuuden ja viestinnän luottamuksellisuuden varmistamiseen.

3GPP AAA Server ja 3GPP AAA Proxy

AAA-palvelin (server) vastaa matkaviestinverkon ulkopuolisten (non-3GPP-access) käyttäjien todentamisesta, valtuutuksesta ja liikkuvuuden hallinnasta sekä sisältää tarvittavat käyttäjätiedot pääsynhallinnan toteuttamiseksi. AAA-välityspalvelin (proxy) tarjoaa vastaavat palvelut verkkovierailutilanteessa. AAA-välityspalvelin myös tarvittaessa valitsee käyttäjän istuntoa palvelevan yhdyskäytävän.

AAA-palvelin liittyy erityisesti VoWifi-palvelun toteutukseen. AAA toteuttaa myös LI-toiminnallisuuksia.

Tällä toiminnolla kontrolloidaan käyttäjien pääsyä verkkoon, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy olennaisesti myös viestinnän luottamuksellisuuteen, viestintäverkon ja sen liikenteen ohjaukseen ja hallintaan sekä yhteyksien ylläpitoon.

Access Network Discovery and Selection Function (ANDSF)

ANDSF vastaa käyttäjän liikenteen ohjauksesta matkaviestinverkon ja matkaviestinverkon ulkopuolisten (non-3GPP-access) verkkojen kuten WLAN-verkon välillä jakaen tietoja liikenteen reititykseen ja päätelaitteen liikkuvuuteen. Toteutustavasta riippuen tiedot joko noudetaan ANDSF-palvelimelta tai palvelin jakelee ne kohdelaitteille.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien verkossa kulkevaa liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy olennaisesti myös käyttäjien verkkoon pääsyyn ja verkon palveluiden saatavuuteen.

Policy and Charging Rules Function (PCRF)

PCRF toimii käyttäjien yhteyksien käyttöpolitiikan ja laskutuksen ohjauspisteenä. PCRF varmistaa, että käyttäjätason liikenne on käyttäjäprofiilin mukaista. PCRF:llä on keskeinen rooli käyttäjille tarjottujen yhteyksien palvelun laadun, laskutuksen ja VoLTE-puhepalvelun ja verkkovierailun ohjaamisessa.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien liikennettä ja verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti yhteyksien ylläpitoon sekä palveluiden saatavuuden varmistamiseen.

6. 5G-verkon kriittiset osat

6.1. 5G-verkon piirteitä ja sen arkkitehtuuri

5G-verkon ydin käsittää tietyt ydintoiminnot verkossa, joita ilman verkko ei pysty toimimaan tai tuottamaan tiettyjä kriittisiä palveluita verkolle. Se käsittää myös rajapinnat ulkopuolisiin järjestelmiin ja verkkoihin, reunaverkkoon ja ulkopuolisiin ns. IPX- ja dataverkon toimintoihin. Verkon ytimessä tehdään päätökset käyttäjän verkkoon pääsystä ja liikenteen ohjauksesta sekä määritellään, ohjataanko tieto käsiteltäväksi paikallisesti verkossa lähellä käyttäjää. Verkon ytimessä tehdään myös verkon tarvitsemaan infrastruktuuriin ja sen alustoihin liittyviä ohjauksia, päätöksiä ja verkon toimivuuden varmistamista.

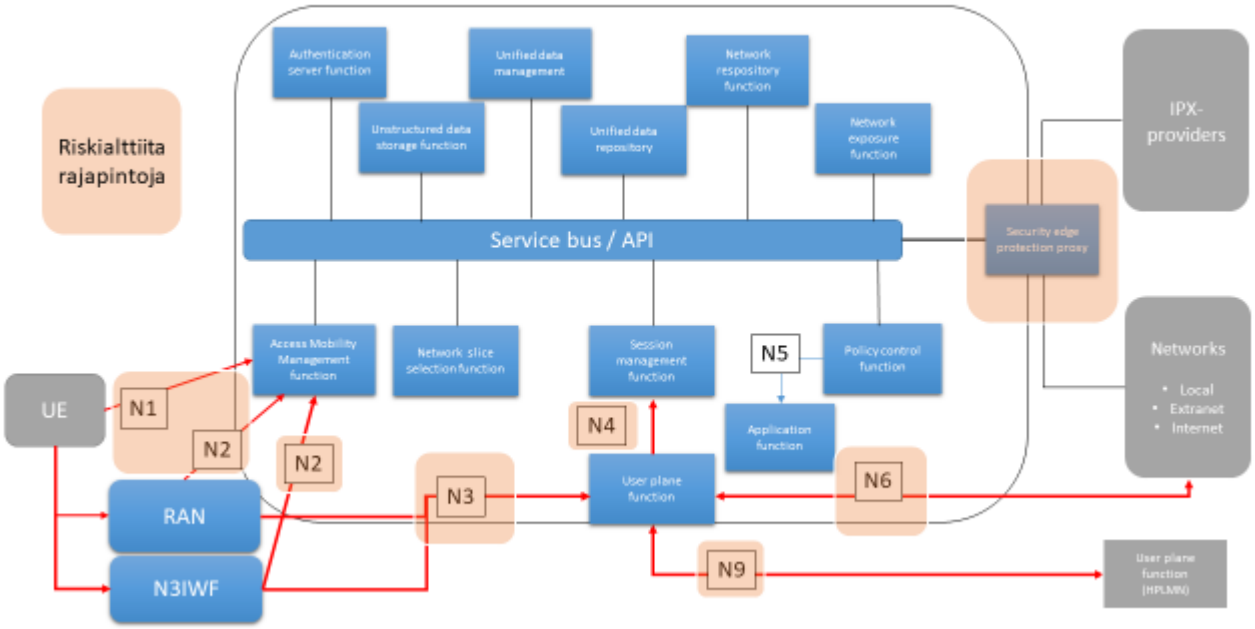
5G-verkon ydin perustuu palveluväylään ja ohjelmistokomponentteihin. Verkon ytimessä alusta ja verkon ohjelmistopohjaiset komponentit on eroteltu toisistaan, ja ne voidaan rakentaa toisistaan riippumatta. Useat funktiot tai ohjelmistot voivat jakaa alustan. Alustojen turvallisuus on kriittinen tekijä koko verkon tietoturvan varmistamisessa. Verkon ytimen funktioiden riskeihin kuuluvat ulkoiset rajapinnat, joiden kautta voidaan pyrkiä vaikuttamaan tai tunkeutumaan verkon ytimen ohjelmistoihin, sekä verkon ytimen sisällä tapahtuva poikittainen liikenne. 5G-palveluarkkitehtuurissa vakioidut palveluväylät mahdollistavat palveluntarjoajien kiinteän integroitumisen 5G-ytimen tärkeisiin väyliin. Tämä mahdollistaa verkon mukautumisen siten, että verkko pystytään optimoimaan käyttäjien käyttämiä palveluita varten.

5G-verkon toimintaa ohjaavia komponentteja käsitellään verkon funktioina, jotka voivat koostua useasta eri ohjelmistosta tai ns. konteista, jotka tarjoavat vakioidun ja valmiin ajoympäristön tarvittaville ohjelmistolle. Verkon ytimen funktioiden välinen liikenne tapahtuu vakioitua palveluväylää pitkin. Verkon ydin tarjoaa myös rajapinnat, joiden avulla mahdollistetaan käyttäjien verkkovierailut (roaming) toisten operaattoreiden verkkoon sekä liikenne muihin tietoverkkoihin kuten internetiin tai organisaatioiden sisäverkkoihin.

5G-verkoissa virtualisointi lisääntyy ja tulee olemaan tärkeässä roolissa, ja virtuaaliympäristöt muuttuvat huomattavasti dynaamisemmiksi. Virtualisointia voidaan käyttää myös jo 4G-teknologioissa ja IMS-alijärjestelmässä. Alustaratkaisuissa voidaan siirtyä pilvipohjaisiin virtualisointiratkaisuihin tietoliikennealustoissa ja palvelinalustoissa. Verkon eri komponentit kuten tukiasemien ohjelmistot ja verkon ytimen toiminnallisuudet voidaan tuottaa virtualisoitujen alustojen avulla.

5G-verkon ytimeen voidaan laskea kuuluvaksi verkon tukiasemiin yhteydessä olevat komponentit, jotka huolehtivat liikenteen ohjauksesta ja reitityksestä, käyttäjien tunnistamisesta, valtuuttamisesta sekä salausavainten hallinnasta ja jakamisesta. Ytimeen kuuluvat lisäksi teleyrityksen mobiiliverkon yhteenliittämisrajapinnat muiden toimijoiden verkkoihin. Näitä vastaavia funktioita 3GPP:n mukaisessa määrittelyssä ovat ainakin UPF, AMF ja SEPP sekä näihin komponentteihin yhteydessä olevat palvelupohjaisen arkkitehtuurin komponentit. 5G-verkon keskeiset funktiot 3GPP:n arkkitehtuurin mukaan on esitetty kuvassa 2.

5G-verkon pääasialliset turvallisuusalueet voidaan yleisesti ottaen jakaa kahteen eri tasoon: yhtäältä verkon ytimeen ja sen rajapintoihin sekä toisaalta reunaverkkoon. Reunaverkko käsittää verkon siirtoyhteydet niiden toteutustavasta riippumatta, tukiasemat ja mahdollisesti reunalaskennan komponentit. Verkon ytimen ja verkon reunan erottelu ei ole yksiselitteistä, mutta niiden välisen rajan voidaan katsoa muodostuvan yhtäältä päätelaitteiden ja tukiaseman kontrolliyhteyden (control plane) ja verkon välisistä N1- ja N2-rajapinnoista sekä toisaalta tukiaseman ja verkon välisen datayhteyden (user plane) N3-rajapinnasta. Rajapinnat N32 ja N6 erottavat verkon IPX- ja datapohjaisesta verkosta ja N9-rajapinta vierailuverkosta.



Kuva 2 5G-ydinverkon keskeiset toiminnot ja rajapinnat

6.2. 5G-verkon kriittisten osien määrittely

Kohdassa määritellään ne verkon toiminnallisuudet, jotka ainakin ovat 5G-verkon kriittisiä osia, viittaamalla 3GPP:n teknisen määrityksen TS 23.501 mukaisiin verkon ytimen toimintoihin. Kohdan ensimmäinen alakohta on suurelta osin luonteeltaan selkeyttävä siten, että siinä tuodaan esiin se lähtökohta, että ytimen toiminnallisuudet ovat viestintäverkon kriittisiä osia.

Ensimmäisessä alakohdassa määrätään, että viestintäverkon kriittisiä osia ovat 5G-verkon ytimen toiminnallisuudet sellaisena kuin ne on määritelty 3GPP:n teknisen määrityksen 23.501 kohdassa 6.2 siltä osin kuin ne kontrolloivat tai ohjaavat olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Näin ollen kaikki mainittuihin kohtiin sisältyvät toiminnallisuudet eivät kuitenkaan ehdottomasti ole viestintäverkon kriittisiä osia. Toiminnallisuudet on voitu kohdassa tarkoitetulla tavalla määritellä teknisessä määrityksessä 23.501 myös viittaamalla siinä toisiin 3GPP:n määrityksiin.

Kohdan toisessa alakohdassa puolestaan määritellään ne 5G-verkon toiminnallisuudet, joita ainakin on pidettävä viestintäverkon kriittisinä osina. Määräyksen taulukossa 2 mainittujen toiminnallisuuksien osalta tarkempi analyysi viestintäverkon osan kriittisyydestä ei olisi tarpeen, vaan ne olisi katsottava oletusarvoisesti viestintäverkon kriittisiksi osiksi. Määräyksen 7 kohta sisältää kuitenkin tätä koskevan poikkeusmahdollisuuden. Määräyksen 7 kohdassa mahdollistetaan se, että muutoin viestintäverkon kriittiseksi osaksi katsottava toiminnallisuus voidaan tietyin edellytyksin katsoa ei-kriittiseksi, kun sillä tuetaan verkon reunalla tuotettavia palveluita ja on toteutettu mekanismit viestintäverkon kriittisten osien suojaamiseksi.

3GPP:n määritysten mukaiset funktiot (toiminnallisuudet) ovat loogisia ja useaan sovellukseen hajautettuja. Kohdan mukaan verkon osa olisi kriittinen, vaikka se toteuttaisi vain osan kriittiseksi määritellystä toiminnallisuudesta. Tästä ja toiminnallisuuteen perustuvasta määrittelytavasta seuraisi, että kun yksittäisen ohjelmistokomponentin voidaan osoittaa toteuttavan osaksikaan jonkin viestintäverkon kriittiseksi osaksi määritellyn toiminnallisuuden, olisi komponentti katsottava verkon kriittiseksi osaksi, vaikkei se koko toiminnallisuutta toteuttaisikaan. Yksittäinen ohjelmistokomponentti tai verkkolaite voi toteuttaa myös useamman kuin yhden toiminnallisuuden.

5G NSA -verkon 5G-komponentit kuuluvat määräyksen eri kohtien soveltamisalan kannalta 5G-verkon kriittisten osien määrittelyn piiriin. Esimerkiksi jos 5G-verkon jokin osa määritellään kriittiseksi, osa on kriittinen myös 5G NSA -verkon yhteydessä käytettynä. Vastaavasti 5G NSA -verkkojen tapauksessa hyödynnettyjen 4G-verkon osien kriittisyyttä arvioitaisiin lähtökohtaisesti sen mukaan, mitä 4G-verkon osista määräyksessä määrättään.

Pääosa kohdassa määritellyistä funktioista rajautuu ydinverkon alueelle siinäkin tapauksessa, että ydinverkko ymmärretään edellä kohdassa 6.1 kuvatulla tavalla siksi verkon osaksi, joka voidaan erottaa sen tiettyjen rajapintojen perusteella reunaverkosta. Poikkeus tästä on Non-3GPP InterWorking Function (N3IWF), joka mahdollistaa WLAN:in kautta tapahtuvan liitynnän 5G-verkkoon.

Ensimmäinen alakohta ja toisessa alakohdassa viitattu taulukko kriittisistä osista eivät ole miltään osin tyhjentäviä, vaan lisäksi teleyrityksen tai erillisverkkotoimijan on arvioitava, onko sen verkossa taulukossa mainittujen lisäksi muita kriittisiä osia. Luettelon rinnalla on siis sovellettava paitsi määräyksen 4 kohdan mukaista kaikille ver-

koille yhteistä kriittisten osien määrittelyä myös SVPL 244 a §:n 1 momentin viestintäverkon kriittisen osan määritelmää sellaisenaan. Koska taulukko ei ole tyhjentävä, mahdolliset muut tulevaisuudessa määriteltävät funktiot, jotka toteuttaisivat samankaltaisen kriittisen toiminnallisuuden, voisivat olla joko määräyksen kohdan 4 tai SVPL 244 a §:n 1 momentin määritelmän nojalla viestintäverkon kriittisiä osia.

6.3. 5G-verkon kriittisiä toiminnallisuuksia

Access and Mobility Management Function (AMF)

AMF on vastuussa liityntäverkon ja käyttäjien ohjausliikenteen terminoinnista, radioverkon tukiasemien ja päätelaitteiden yhteyksistä ja rekisteröinnistä ydinverkkoon sekä liikkuvuuden hallinnasta.

AMF toimii avainasemassa verkon viipaloinnissa ja tarjoaa päätelaitteelle pääsyn kaikkiin sille tarjottuihin viipaleisiin. AMF:n vastaa myös matkaviestinverkon ulkopuolisten yhteyksien (non-3GPP-access, esim. WLAN) luomisesta ja hallinnasta. AMF:llä on myös rooli telekuuntelun tai televalvonnan toteuttamisessa (lawful interception- eli LI-toiminnallisuuksissa).

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien pääsyä verkkoon, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti verkon liikenteen kontrollointiin, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

User Plane Function (UPF)

UPF vastaa käyttäjäliikenteen reitittämisestä, ohjaamisesta ja hallinnasta samaan tapaan kuin SGW/PGW 4G-verkoissa. UPF voidaan toteuttaa verkossa hajautetusti ja paikallisesti esimerkiksi reunalaskennan (MEC) yhteydessä[29]. UPF:n vastuulle kuuluu myös käyttäjäliikenteen palvelun laadun (QoS) hallinta sekä erityisesti URLLC:n kannalta olennainen sessioiden ja palveluiden jatkuvuuden ylläpitäminen. UPF toteuttaa myös LI-toiminnallisuuksia.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti yhteyksien ylläpitoon sekä palveluiden saatavuuden ja viestinnän luottamuksellisuuden varmistamiseen.

Policy Control Function (PCF)

PCF vastaa liikenteen ohjaamisesta ja pääsynhallintapolitiikan toteuttamisesta. Toiminto hyödyntää käyttäjien liikenteen ohjaukseen liittyviä parametreja mm. UDR-rekisteristä. PCF:llä on keskeinen rooli verkon palveluiden laadun ja laskutuksen ohjauksessa. PCF:ssä on tuki verkon viipaloinnille, liikkuvuuskäytännöille (mobility policies) ja verkkovierailulle.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien liikennettä ja verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy

[29] MEC in 5G networks. First edition – June 2018, ETSI White Paper No. 28, s. 8. Saatavissa: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf.

myös olennaisesti yhteyksien ylläpitoon sekä palveluiden saatavuuden varmistamiseen.

Authentication Server Function (AUSF)

AUSF vastaa käyttäjien päätelaitteiden todentamiseen liittyvistä palveluista ja toiminnallisuuksista verkossa ja tarjoaa yhteisen todentamisviitekehyksen sekä 3GPP- että muille kuin 3GPP-yhteyksille. AUSF toteuttaa 5G:n osalta osittain samankaltaisia toiminnallisuuksia kuin HSS 4G:ssä.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien liikennettä ja verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Unified Data Management (UDM)

UDM vastaa käyttäjien tunnistamisesta, pääsynhallinnasta, liittymien hallinnasta, käyttäjärekistereistä sekä salausavainten luomisesta ja hallinnasta. UDM ylläpitää tilaajatietojen hallintatoimintoja, kuten 5G-tilaajien määrittely ja poistaminen, SIM-korttien vaihtaminen, MSISDN-numeroiden muuttaminen sekä tilaustietojen muuttaminen ja kysely. UDM toteuttaa 5G:n osalta osittain samankaltaisia toiminnallisuuksia kuin HSS 4G:ssä. UDM toteuttaa myös LI-toiminnallisuuksia.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien pääsyä verkon palveluihin, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti viestintäverkon ja sen liikenteen kontrollointiin, yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Application Function (AF)

AF tukee reitityspäätösten tekemistä verkossa käyttäjien käyttämien sovellusten perusteella. AF käyttää hyväksi NEF-funktioon määriteltyjä tietoja ja voi olla NEF:in välityksellä vuorovaikutuksessa ydinverkon kanssa. Verkon eri toiminnot voivat toimia AF:n roolissa. Esimerkiksi IMS-palveluiden toteuttamiseen liittyvä P-CSCF voi ottaa AF:n roolin.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä ja verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti yhteyksien ylläpitoon sekä palveluiden saatavuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Network Exposure Function (NEF) ja Intermediate NEF (I-NEF)

NEF mahdollistaa 5G-ydinverkon toiminnallisuuksien tarjoamisen kolmannen osapuolen toimijoille ja ulkoisille sovelluksille. NEF vastaa verkon palveluiden mainostamisesta esim. 3GPP-verkkoihin, verkon ulkopuolisten sovellustietojen välittämisestä mobiiliverkkoon ja palveluväylän sisäisistä ohjauksista.

NEF mahdollistaa AF:n turvallisen kommunikoinnin verkon kanssa. Se voi myös tallentaa UDR:ään muilta funktioilta saamaansa tietoa. I-NEF toimii NEF:inä verkkovierailutilanteessa.

Tällä toiminnolla kontrolloidaan käyttäjien pääsyä verkon toimintoihin, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti

yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Network Repository Function (NRF)

NRF vastaa verkon palveluiden saatavuudesta, rekisteröinnistä ja valtuuttamisesta. NRF ylläpitää verkon palveluiden ja komponenttien luetteloa ja tarjoaa näin rekisteröinti- ja hakutoiminnallisuuksia, ja mahdollistaa muiden verkon funktioiden ja -palveluiden keskinäisen saatavuuden ja kommunikoinnin. Kaikki 5G-verkon funktiot vuorovaikuttavat NRF:n kanssa.

Tällä toiminnolla kontrolloidaan pääsyä verkon resursseihin ja palveluihin ylläpitämällä ja välittämällä tietoa niistä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti palveluiden saatavuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Network Slice Selection Function (NSSF)

NSSF vastaa verkon viipalointiin liittyvistä palveluista ja määrittelyistä sekä ohjaa ja kontrolloi AMF-funktioita. NSSF määrittää päätelaitetta palvelevan AMF:n ja päättää päätelaitteelle sallitut ja tarjottavat verkkoviipaleet.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä ja käyttäjien verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Network Slice Specific Authentication and Authorization Function (NSSAAF)

NSSAAF vastaa viipalekohtaisesta todentamisesta ja valtuutuksesta yhdessä AAA-palvelimen ja AAA-välityspalvelimen kanssa.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Session Management Function (SMF)

SMF:ään on yhdistetty istunnonhallinnan ohjausliikenteen toiminnot. SMF vastaa muun muassa verkkokäytäntöjen mukaisten istuntojen hallinnasta, IP-osoitteiden allokoinnista sekä ohjaa UPF-toiminnallisuutta sessiokohtaisesti. SMF toteuttaa myös LI-toiminnallisuuksia.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Security Edge Protection Proxy (SEPP)

SEPP on välityspalvelin, joka tukee verkon topologian piilottamista sekä viestien suodattamista ja valvontaa matkaviestinverkkojen välisillä ohjausliikennerajapinnoilla. SEPP toimii luotettavana pääsynhallintafunktiona muihin tietoverkkoihin (esimerkiksi IPX-verkkoihin verkkovierailun tapauksessa).

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä ja verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Unstructured Data Storage Function (UDSF)

UDSF on valinnainen funktio, jota muut verkon funktiot voivat käyttää rakenteettoman tiedon tallentamiseen ja hakemiseen. Tällaista tietoa voivat olla esimerkiksi funktion yhteyksiin, istuntoihin tai tilaan liittyvät tiedot. UDSF voi olla funktiokohtainen tai funktiot voivat käyttää yhteistä jaettua UDSF:ää.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Unified Data Repository (UDR)

UDR on tietovarasto, joka pystyy tallentamaan ja hakemaan muun muassa tilaajatietoja UDM:ltä, käytäntöihin liittyvää dataa PCF:ltä sekä rakenteellista dataa ja sovellustietoja NEF:iltä. Verkossa voi olla useita UDR-funktioita, ja UDR voi palvella joko yksittäistä verkon funktiota tai verkon funktioiden joukkoa. UDR voi olla myös integroituna yksittäiseen verkon funktioon.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

UE radio Capability Management Function (UCMF)

UCMF tallentaa ja säilyttää päätelaitteiden laitetunnuskohtaisia radiokyvykkyystietoja, jotka ovat joko viestintäverkon tai päätelaitevalmistajan määrittämiä. Tällaisia radiokyvykkyystietoja ovat muun muassa tiedot tuetuista radioteknologioista ja taajuuskaistoista sekä muista radioverkko-ominaisuuksista. UCMF kommunikoi AMF:n kanssa toimittamalla sille näitä tietoja. UCMF voi toimia myös 4G-verkossa, jolloin se kommunikoi MME:n kanssa.

UCMF:n sisältämät tiedot eivät sinänsä ole arkaluonteisia, mutta ne ohjaavat verkon toimintaa. UCMF:n tietojen manipuloinnin uhkana on ns. downgrade attack, jota voidaan kuitenkin rajoittaa verkon toteutuksella.

Tällä toiminnolla kontrolloidaan ja ohjataan verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti palveluiden saatavuuden varmistamiseen.

Non-3GPP InterWorking Function (N3IWF)

N3IWF mahdollistaa langattoman lähiverkon (WLAN) kautta tapahtuvan pääsyn 5G-ydinverkkoon. N3IWF tukee IPsec-tunnelin muodostamista päätelaitteen kanssa ja valtuuttaa käyttäjän pääsyn 5G-ydinverkkoon. IPSec-tunneli sekä N2- ja N3-rajapinnat eli käyttäjä- ja ohjausliikenne terminoidaan N3IWF:ssä.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä ja verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

5G-Equipment Identity Register (5G-EIR)

5G-EIR eli laitetunnusrekisteri on matkaviestinverkon tietokanta, johon tallennetaan kansainvälisiä matkaviestimien laitetunnuksia (IMEI) ja joka sisältää tiedot matkaviestimien käytön luvallisuudesta. 5G-EIR:n mustalle listalle asetettujen päätelaitteiden normaali käyttö viestintäverkossa on estetty.

Tällä toiminnolla kontrolloidaan ja ohjataan käyttäjien verkkoon pääsyä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti palveluiden saatavuuden varmistamiseen.

Service Communication Proxy (SCP)

SCP toimii 5G-verkossa tärkeässä roolissa välittäen ja reitittäen viestejä muille verkon funktioille. SCP:n tehtäviin kuuluu myös muun muassa topologian yksinkertaistaminen, kuormantasaus ja -jakaminen, ylikuormituksen käsittely ja viestiparametrien harmonisointi integroinnin helpottamiseksi usean laitetoimittajan ympäristöissä.

Tällä toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti yhteyksien ylläpitoon sekä palveluiden saatavuuden, viestinnän luottamuksellisuuden ja koko viestintäverkon tietoturvan varmistamiseen.

Network Data Analytics Function (NWDAF)

NWDAF:ää ei kuitenkaan pidetä viestintäverkon kriittisenä osana sen viestintäverkkoon hajautetun toiminnallisuuden osalta siltä osin kuin se ei kontrolloi tai ohjaa olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä.

NWDAF käyttää hyväkseen koneoppimista keräten verkon funktioilta verkkokohtaista dataa sekä toimittaen reaaliaikaisesti analysoitua dataa takaisin funktioille. Lisäksi NWDAF tuottaa ennustavaa analyysia, jolla tuetaan 5G-verkon ennakoivaa hallintaa. NWDAF:n keräämän datan perusteella voidaan tehdä esimerkiksi automaattista verkkoinfrastruktuurin skaalausta, verkkoviipaleiden valintaa tai pääsyn- ja liikkuvuudenhallintaa.

NWDAF on viestintäverkon kriittinen osa siltä osin kuin se kontrolloi tai ohjaa olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. NWDAF toteutettaneen verkossa hajautetusti, jolloin analytiikkadataa voidaan hyödyntää reaaliaikaisesti myös verkon reunalla.

Keskitetty toiminnallisuus on hajautetussa toteutuksessakin aina viestintäverkon kriittinen osa. Kun toteutus on ei-hajautettu eli verkossa on pelkästään yksi tai useampi keskitetty NWDAF, niin toiminto on aina kriittinen. Tällöin toiminnolla kontrolloidaan ja ohjataan verkossa kulkevaa liikennettä olennaisella tavalla, minkä takia sitä on pidettävä viestintäverkon kriittisenä osana. Toiminto liittyy myös olennaisesti palveluiden saatavuuden varmistamiseen.

NWDAF:n toteutus on vielä suurilta osin avoinna, ja mahdollisten toteutusvaihtoehtojen kirjo on laaja[30]. Näin ollen ei voida yksiselitteisesti sulkea pois verkon reunalla sijaitsevia hajautettuja NWDAF-toimintoja, vaan niiden kriittisyys määräytyy toteutustavan ja yksittäisen toiminnon olennaisuuden mukaan. Hajautuksen toteutuksesta riippuen verkon reunalla toteutettua yksittäistä NWDAF:ään kuuluvaa toiminnallisuutta ei välttämättä pidetä viestintäverkon kriittisenä osana. Tämä on mahdollista siltä osin kuin se ei kontrolloi tai ohjaa olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä, kuten esimerkiksi silloin, kun se vaikuttaa vain vähäiseen määrään käyttäjiä tai tukiasemia.

6.4. Kansainvälinen vertailu

3GPP:n määrityksiin tukeutuva funktiopohjainen määrittely on valittu myös niissä Traficomin tiedossa olevissa maissa, joissa on pyritty teknisesti täsmentämään 5G-verkkojen kriittisiksi arvioitujen verkkojen osien piiriä, eli Ranskassa ja Yhdistyneessä kuningaskunnassa. Ranskan ja UK:n tarkoittamat funktiot on pääosin määritelty 3rd Generation Partnership Projectin (3GPP) teknisessä määrityksessä TS 23.501.

EU:n yhteisessä keinovalikoimassa kriittiseksi on kuvattu ydinverkon funktiot (core network functions) kokonaisuutena.[31] Yhdistyneessä kuningaskunnassa puolestaan on kansallisen kyberturvallisuusviranomaisen ohjauskirjeessä kiinnitetty teleyritysten huomiota 5G-verkkojen osalta erityisen riskialttiiksi nähtyihin funktioihin. Nämä on määritelty ei-tyhjentävästi niin, että ne kattavat kaikki 3GPP TS 23.501:ssä määritellyt 5G-verkon ytimen toiminnallisuudet. Nämä seikat sinänsä puoltavat tämän kohdan ensimmäiseen alakohtaan sisältyvää lähtökohtaa siitä, että verkon ytimen toiminnallisuuksia pidetään yleisesti viestintäverkon kriittisinä osina.

Ranskassa taas on määräyksessä määritelty lupavaatimuksen piiriin ohjelmistot ja laitteistot, joilla toteutetaan viidennen sukupolven matkaviestinverkoissa päätelaitteiden todennus, radioresurssien allokointi ja sähköisen viestinnän reititys niiden välillä tai kolmansien osapuolien verkkoihin, sekä ohjelmistot ja laitteistot, jotka säätelevät näiden verkkojen turvallisuutta, eheyttä tai saatavuutta. Määräyksessä täsmennetään tämän tarkoittavan 5G-verkon ytimen osalta seuraavia 3GPP:n määritysten mukaisia funktioita:[32] Access and Mobility management Function (AMF); Authentication Server Function (AUSF); User Plane Function (UPF); Session Management Function (SMF); Policy Control Function (PCF); Network Slice Selection Function (NSSF); Network Repository Function (NRF); Network Exposure Function (NEF); Unified Data Management (UDM); Security Edge Protection Proxy (SEPP). Kaikki mainitut määritellään myös tässä Traficomin määräyksessä viestintäverkon kriittiseksi osaksi.

Verrattuna Yhdistyneen kuningaskunnan luetteloon, joka kattaa laajasti kaikki 3GPP:n määrittämät 5G-ydinverkon toiminnallisuudet, tähän määräykseen eivät ai-

[30] Mahdollisia NWDAF:in toteutustapoja on käsitelty teknisessä selonteossa 3GPP TR 23.700-91, Study on enablers for network automation for the 5G System (5GS); Phase 2 (Release 17).
[31] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. Liite 2, s. 39. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. 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.
[32] Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000039455672. Lisäksi määräys kattaa tukiaseman, New Radio Base Station (en-gNodeB ja gNodeB). Ks. tukiasemista tämän perustelumuistion yleisperustelujen kohta 4.1.5.

nakaan ensi vaiheessa sisälly Wireline Access Gateway Function (W-AGF) sekä Trusted Non-3GPP Gateway Function (TNGF) ja Trusted WLAN Interworking Function (TWIF). Tätä ratkaisua on perusteltu kohdan 4.1.5 lopussa. Mikäli teleyritys tai erillisverkkotoimija ottaa näitä toiminallisuuksia käyttöön, sen tulee arvioida toimintojen kriittisyyttä suoraan SVPL 244 a §:n 1 momentin ja määräyksen 4 kohdan perusteella.

7. Verkon reunalla tuotettavia palveluita tukevat toiminnot

Tässä kohdassa määritellään poikkeus, jota voidaan soveltaa verkon reunalla tapahtuvaa verkon ohjausta palvelevien toimintojen kriittisyyden arvioinnissa. Kohdan tarkoituksena on mahdollistaa verkon ydintoimintojen paikallisten toteutusten katsominen muuksi kuin viestintäverkon kriittiseksi osaksi, jos teleyritys tai erillisverkkotoimija voi osoittaa poikkeuksen edellytysten täyttyvän.

Tämän kohdan mukaan viestintäverkon kriittisenä osana ei pidetä edellä taulukossa 1 tai 2 tarkoitettua 4G- tai 5G-verkon toimintoa ja toimenpidettä, jos kohdan mukaiset edellytykset täyttyvät. Poikkeuksen soveltamisen edellytyksenä on, että:

- toiminto tukea pääasiassa muiden palveluiden kuin viestintäpalveluiden tarjoamista verkon reunalla
- toiminnallisuus vaikuttaa vain vähäiseen määrään loppukäyttäjiä, päätelaitteita tai tukiasemia
- toiminnallisuuden avulla ei välitetä muuta liikennettä (eli liikennettä, joka ei liity kyseisen verkon reunalla toteutetun palvelun tarjoamiseen)
- viestintäverkon kriittiset osat on suojattu toiminnallisuuden niihin mahdollisesti kohdistamalta haitalliselta liikenteeltä toteuttamalla verkossa tarvittavat luotettavat suojausmekanismit.

Koska määräyksen mukaan tässä tarkoitetut verkon toiminnot olisivat oletusarvoisesti viestintäverkon kriittisiä osia, olisi poikkeukseen vetoavalla teleyrityksellä tai erillisverkkotoimijalla selvitysvelvollisuus poikkeuksen edellytysten täyttymisestä. Määräyksen 3 kohdassa edellytettäisiin arvion ja sen perustana olevien suojausmekanismien dokumentoimista.

Kohdan mukainen poikkeusmahdollisuus kohdistuisi vain määräyksen taulukoissa 1 ja 2 määriteltyjen 4G- ja 5G-verkon kriittisiin toimintoihin. Se ei siis mahdollistaisi määräyksen kohdan 4 luettelossa eri verkoille yhteisesti määritellyistä viestintäverkon kriittisistä osista poikkeamista. Näin ollen esimerkiksi telekuuntelun ja televalvonnan toteuttaminen olisi toimintona poikkeuksetta viestintäverkon kriittinen osa.

Poikkeus voisi tulla sovellettavaksi eri tilanteissa, joissa halutaan tuottaa palveluita lähellä käyttäjää. Tällaisia olisivat ainakin operaattorin toteuttama reunalaskenta, jolla tarkoitetaan tässä yhteydessä Multi-Access Edge Computingia (MEC), sekä local breakoutia, jossa 5G-verkon liikennettä ohjataan esimerkiksi teleyrityksen asiakasyrityksen omaan sisäverkkoon suoraan verkon reunalla. Näitä tilanteita varten verkon reunalla voidaan toteuttaa esimerkiksi paikallinen UPF tai muita verkon ytimen funktioita. Poikkeuksessa on kyse edellytyksistä, joilla toiminnon (esim. määräyksen mukaan oletusarvoisesti viestintäverkon kriittisenä osana pidettävän UPF:n) kriittisyyttä voidaan arvioida toisin, jos se toteutetaan alueellisesti hajautetusti varsinaisen ydinverkon ulkopuolella.

Kohdassa edellytettäisiin ensiksi, että toiminnon tulee tukea pääasiassa muiden palveluiden kuin viestintäpalveluiden tarjoamista verkon reunalla. Tukemisella tarkoitettaisiin sitä, että toiminnon tulee liittyä esimerkiksi MEC-toteutukseen tai local breakoutiin perustuvan palvelun toteuttamiseen niin, että toiminto ei kuulu varsinaisen ydinverkon toimintoihin eikä siis toimi verkon eri funktioille yhteisenä toimintona. Reunalla tarjottavassa palvelussa tulisi olla kyseessä muu kuin viestintäpalvelu eli esimerkiksi tehtaan ohjaus, teleyrityksen asiakasyrityksen liiketoimintaa palvelevat toiminnot tai muut sellaiset toiminnot, jotka eivät ole viestintäpalveluita ja joita käyttää tietty käyttäjäryhmä eivätkä kaikki teleyrityksen matkaviestinverkon käyttäjät yleisesti. Kriteerinä olisi, että kyseessä on lähellä käyttäjää tuotettava palvelu, mutta itse verkon ydintoiminnon ei tarvitse olla toteutettu fyysisesti reunalaskennan yhteydessä, kunhan se on toteutettu nimenomaan sitä varten eikä siis toimi verkon varsinaisen ytimen osana. Se voisi sijaita siten esimerkiksi liityntäverkossa tai siirtoverkon solmupisteessä.

Toiseksi toiminnallisuus saisi vaikuttaa vain vähäiseen määrään loppukäyttäjiä, päätelaitteita tai tukiasemia. Se ei siten voisi SVPL 244 a §:n 1 momentin tarkoittamalla tavalla ohjata olennaisella tavalla verkon liikennettä, johon myös seuraava edellytys liittyy.

Kolmanneksi edellytetään, että toiminnallisuuden avulla ei välitetä muuta liikennettä, eli liikennettä joka ei liity kyseisen verkon reunalla toteuttavan, muun kuin viestintäpalvelun tarjoamiseen. Tällöin on esimerkiksi kyse tilanteesta, jossa poikkeuksen piiriin tuleva UPF ohjaa vain sellaista käyttäjäliikennettä, jota käsitellään verkon reunalla tarjottavaa palvelua varten. Mikäli käyttäjällä olisi lisäksi pääsy verkon muihin palveluihin, ei poikkeus olisi mahdollinen, ellei niitä toteutettaisi eri UPF:n avulla. Käytännössä tämä voisi tarkoittaa, että niille olisi määritelty oma PDU-istunto, joita palvelevat eri UPF:t. Toteutustavasta riippuen voi olla mahdollista, että yksi käyttäjää palveleva UPF ohjaa liikennettä eteenpäin eri UPF:lle ja eri dataverkkoihin (yhden PDU-istunnon toteutus, 3GPP TS 23.501, kuva 4.2.3-4), jolloin poikkeusta ei voisi soveltaa.

Neljänneksi edellytetään, että viestintäverkon kriittiset osat on suojattu toiminnallisuuden niihin mahdollisesti kohdistamalta haitalliselta liikenteeltä toteuttamalla verkossa tarvittavat luotettavat suojausmekanismit. Näillä suojausmekanismeilla tulee tunnistaa ja käsitellä haitallinen liikenne kuten palvelunestohyökkäykset ja luvattomat pääsy-yritykset sekä varmistaa, että liikenteen oikeudeton uudelleenohjaus ei ole mahdollista. Suojausmekanismeilla tulee siis varmistaa, että verkon reunalla tuotettavia palveluita tukeva toiminnallisuus ei voi kontrolloida tai ohjata olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä.

Näitä suojausmekanismeja olisi mahdollista toteuttaa esimerkiksi palomuurin ja verkon segmentoinnin avulla sekä valmiudella kytkeä toiminto irti verkosta. Niillä tulisi varmistaa, että verkon reunalla tuotettavia palveluita tukeva toiminto ei pysty verkon varsinaiseen ytimeen olevasta rajapinnastaan huolimatta vaikuttamaan siihen tai muihin UPF-toimintoihin haitallisella tavalla. Määräyksessä ei ole mahdollista määrittää niitä mekanismeja, joilla tästä voitaisiin käytännössä varmistua. Teleyrityksen tai erillisverkkotoimijan toteuttamien tietoturvakontrollien ja muiden toimenpiteiden tehokkuus arvioitaisiin kokonaisuutena. Niillä olisi voitava poistaa vaara siitä, että reunalla sijaitsevan toiminnon avulla syntyisi pääsy muuhun verkkoon tai voitaisiin ohjata muun verkon (varsinaisen ytimen) toimintaa olennaisella tavalla. Olennaisuutta arvioitaessa kiinnitettäisiin huomiota siihen, onko toiminnolla mahdollista vaikuttaa muuhunkin kuin vain esimerkiksi kyseisessä reunalaskentapalvelussa käsiteltäviin tietoihin. Suojausmekanismeilta ei kuitenkaan edellytetä verkon reunalla tuotettavia

palveluita tukevan toiminnon täydellistä eristämistä, koska tämän ei arvioida olevan mahdollista verkon ohjaamisen kannalta.

8. IP-pohjaiset puhelinpalvelut matkaviestinverkossa

Kohta täydentää muita määräyksen kohtia. Kohdan mukaan viestintäverkon kriittisiä osia ovat 3GPP:n teknisen määrityksen 23.228 mukaisen IP-multimedia-alijärjestelmän (IP Multimedia Core Network Subsystem, IMS) määritelmään kuuluvat viestintäverkon toiminnot ja toimenpiteet, joilla toteutetaan IP-pohjainen yleinen puhelinpalvelu.

Kohdassa määritellään viestintäverkon kriittiseksi osaksi (IMS) Core siltä osin kuin sillä toteutetaan IP-pohjainen yleinen puhelinpalvelu.[33] IP-pohjaisissa 4G- ja jatkossa 5G-matkaviestinverkoissa toteutetaan yleinen puhepalvelu IMS:n avulla. Sitä käytetään myös muiden multimediapalvelujen toteuttamiseen IP-pohjaisissa matkaviestinverkoissa. IMS Coren funktiot ovat yhteydessä rajapintojen avulla 4G- tai 5G-verkkoon, ja niitä voidaan pitää osana verkon ydintä.

SVPL 3 §:n mukaan yleisellä puhelinpalvelulla tarkoitetaan viestintäpalvelua, jonka avulla voidaan soittaa ja vastaanottaa kotimaan- ja ulkomaanpuheluja kansallisessa tai kansainvälisessä numerointisuunnitelmassa olevan numeron avulla.

Tämän kohdan perusteella IMS Coren kriittisiä toiminnallisuuksia voisivat olla esimerkiksi Call Session Control Function (CSCF), Subscription Locator Function (SLF), Breakout Gateway Control Function (BGCF) ja Media Gateway Control Function (MGCF).

IMS Coreen perustuvia, matkaviestinverkoissa tarjottavia puhelinpalveluita ovat ainakin VoLTE ja VoWifi 4G-verkossa. Kohta ei edellytä, että nimenomaan 4G-tai 5G-radioverkkoa hyödynnetään puhelinpalvelussa, vaan päätelaite voi käyttää myös esimerkiksi WiFi-yhteyttä, kunhan kyse on teleyrityksen tarjoamasta yleisestä puhelinpalvelusta.

IP-pohjaisten matkaviestinverkkojen välityksellä on mahdollista toteuttaa myös muita puhepalveluja, jotka eivät perustu IMS Coren toimintoihin. Tässä määräyksen kohdassa ei määrätä noista muista palveluista, joihin liittyvien toimintojen mahdollista kriittisyyttä olisi tarvittaessa arvioitava muilla perusteilla.

Määräyksen voimaantulo ja siirtymäaika

Määräys tulee voimaan x päivänä xkuuta 2021 ja on voimassa toistaiseksi. [*Määräyksen on tarkoitus tulla voimaan mahdollisimman pian.*]

Määräyksen 3 kohdan mukaiseen tunnistamis- ja dokumentointivelvollisuuteen liittyy kuuden kuukauden siirtymäaika, jonka kuluessa kohdan edellyttämä dokumentaatio on laadittava. Määräyksen 3 kohta edellyttää, että teleyritykset ja erillisverkkotoimijat tunnistavat viestintäverkkonsa kriittiset osat ja niissä käytetyt komponentit ja dokumentoivat arvionsa. Viestintäverkon kriittisten osien ja niissä käytettyjen komponenttien huolelliselle dokumentoinnille on välttämätöntä varata riittävä siirtymäaika. Velvollisuus edellyttää etenkin suurimpien teleyritysten kohdalla varsin huomattavan verkkolaitekannan arviointia, ja se koskee teleyritysten ja erillisverkkotoimijoiden

[33] IMS Core Reference Architecture, 3GPP TS 23.228.

kaikkia verkkoja niiden tekniikasta riippumatta. Velvollisuuden täyttäminen voi dokumentoinnin toteuttamistavasta riippuen edellyttää myös työtä tietojärjestelmien kehittämiseksi. Siirtymäaika koskee vain dokumentointia.

Jälkiseuranta

Liikenne- ja viestintävirasto tulee arvioimaan säännöllisesti määräyksen päivitystarvetta. Arviointityössä otetaan huomioon mahdolliset tulevat verkkoturvallisuuden neuvottelukunnan suositukset, viestintäverkkoteknologian kehitys ja verkkojen toteutukset. Jälkiseurannassa voidaan tarvittaessa selvittää, onko tarpeen määrätä tukiasemien tai 5G-verkon mahdollistamien luotettujen Wi-Fi-verkkojen tai kiinteän verkon yhteyksiin perustuvan liitynnän mahdollistavien toimintojen kriittisyyden arvioimisesta tarkemmin (ks. luku 4.1.5). Lisäksi voidaan seurata, miten määräystä ja erityisesti sen 7 kohdan mukaista poikkeusmahdollisuutta on sovellettu.

Viitteet

Kotimaiset viranomaislähteet

HE 98/2020 vp. Hallituksen esitys eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi

Selvitys 5G:n kyberturvallisuudesta. Yhteenveto. Liikenne- ja viestintävirasto. Traficomin julkaisuja 14.05.2019. https://www.traficom.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-julkaisi-selvityksen-5gn-kyberturvallisuudesta

Liikenne- ja viestintävaliokunnan mietintö LiVM 16/2020 vp — HE 98/2020 vp

Perustuslakivaliokunnan lausunto PeVL 35/2020 vp — HE 98/2020 vp

Euroopan unionin julkaisut

Cybersecurity of 5G networks EU Toolbox of risk mitigating measures. CG Publication 01/2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

EU coordinated risk assessment of the cybersecurity of 5G networks. Report. 9 October 2019. https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

ENISA Threat Landscape for 5G Networks. Updated threat assessment for the fifth generation of mobile telecommunications networks (5G). December 2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

Ulkomaiset viranomaislähteet

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn. Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial. Luonnos 29.4.2020. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/ListekritischeFunktionen.pdf

NCSC advice on the use of equipment from high risk vendors in UK telecoms networks. 28.1.2020, päivitetty 14.7.2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks

Nasjonal sikkerhetsmyndighet: Håndbok i skadevurdering. https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-skadevurdering/om-denne-handboken/

Muut

3GPP TS 21.905. Vocabulary for 3GPP Specifications. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558

3GPP TS 23.002. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network architecture (Release 16)

3GPP TS 23.228. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 16)

3GPP TS 23.273. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 5G System (5GS) Location Services (LCS); Stage 2 (Release 16)

3GPP TS 23.501. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects System architecture for the 5G System (5GS); Stage 2 (Release 16)

3GPP TR 33.848 V0.5.0 (2019-11). Study on Security Impacts of Virtualisation. https://www.3gpp.org/DynaReport/33848.htm.

3GPP TS 36.300. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 15)

3GPP TS 38.300. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2 (Release 15)

5G-ACIA: 5G Non-Public Networks for Industrial Scenarios. White Paper. July 2019. 5G Alliance for Connected Industries and Automation. https://www.5g-acia.org/publications/5g-non-public-networks-for-industrial-scenarios-white-paper/

GSA: Private LTE & 5G Networks Report. February 2020. Global mobile Suppliers Association. https://gsacom.com/paper/private-lte-5g-networks-report-february-2020/

Ericsson: Critical capabilities for private 5G networks. Ericsson White Paper. December 2019. https://www.ericsson.com/en/reports-and-papers/white-papers/private-5g-networks

Ericsson: 5G migration strategy from EPS to 5G system. 24 February, 2020. https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/migration-from-eps-to-5gs