TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Selvitys 5G:n kyberturvallisuudesta

Yhteenveto

Traficomin julkaisuja
14.05.2019

Sisältö

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISBN 978-952-311-329-9
20/2019

Johdanto

Liikenne- ja viestintävirasto Traficom on syksyn 2018 ja talven 2019 aikana selvittänyt 5G-teknologian mukanaan tuomia muutoksia kyberturvallisuuskentässä. Työn tavoitteena on ollut ymmärtää 5G:n mukanaan tuomaa muutosta viraston toimintakentässä, sekä koko yhteiskunnassa.

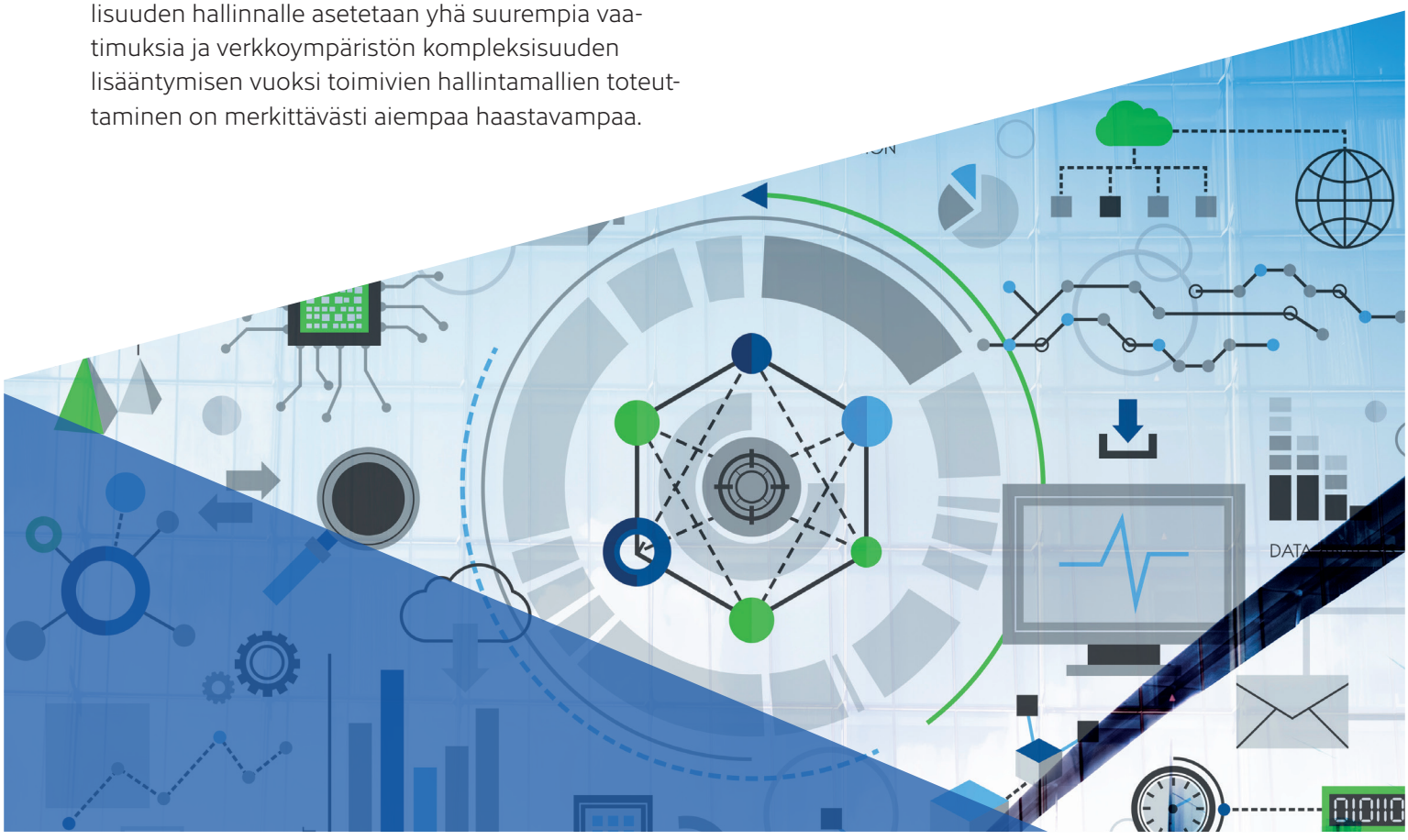
Osana työtä on tunnistettu, että 5G-teknologiaan siirtyminen tuo mukanaan suuremman paradigmamuutoksen kuin yksikään aikaisempi matkaviestinverkkosukupolvi on tuonut. 5G-teknologian uusien ominaisuuksien ja toimintamallien käyttöönotto muuttaa operaattoreiden roolia, se tuo mukanaa paikallisiin tarpeisiin räätälöidyt verkot, saattaa laajentaa viranomaisohjauksen toimintakenttää ja tuo täysin uudenlaisia riskienhallintavaatimuksia 5G:n ominaisuuksia hyödyntäville toimijoille. Verkko muuttuu tiedonsiirtoputkesta yhä enemmän jaetuksi tietojenkäsittelyn ja tietojen tuottamisen alustaksi, jossa verkon reunojen rajat hämärtyvät. Tämä mahdollistaa uusia toiminnallisuuksia ja mahdollisuuksia, joita myös yhteiskunnan kriittisiä toimintoja tarjoavat toimijat tulevat hyödyntämään. Samalla yhä tärkeämmät yhteiskunnan toiminnot tulevat lepäämään 5G-verkkojen varassa.

Riskienhallinnallisesti tämä tarkoittaa siirtymistä ympäristöön, jossa haavoittuvuuksien ja tietoturvallisuuden hallinnalle asetetaan yhä suurempia vaatimuksia ja verkkoympäristön kompleksisuuden lisääntymisen vuoksi toimivien hallintamallien toteuttaminen on merkittävästi aiempaa haastavampaa. Verkkojen toimittajiin ja näiden tietoturvallisuuskontrolleihin on kyettävä luottamaan ja niitä on pystyttävä tarkastelemaan ja mittaamaan. Riskejä on myös hallittava erilaisia riippuvuuksia hajauttamalla.

Viidennen sukupolven matkaviestinteknologian verkkojen rakentamisen vaatimat investoinnit tuovat mahdollisesti mukanaan uudenlaisia yhteisomistusmalleja julkisen ja yksityisen sektorin toimijoiden välillä. Nykyistä korkeampien taajuusalueiden käyttöönoton myötä tukiasemainfrastruktuurin tiheys kasvaa ja tiivistä vuoropuhelua tullaan tarvitsemaan verkon rakentamisen, verkon ylläpidon ja kuntainfrastruktuurin ylläpidon ympärillä.

Samalla 5G muuttaa palveluntuotantokenttää lähemmäs perinteisille IT-alan kansainvälisille suuryrityksille tuttua toimintakenttää ja saattaa tehdä markkinoille saapumisen näille toimijoille entistä houkuttelevammaksi.

Muutos aiemmista verkkosukupolvista kohti 5G-maailmaa tulee vaatimaan tiedon aktiivista jakamista, viranomaisohjauksen rajojen uudelleentarkastelua ja yhä laajempaa vuoropuhelua eri toimijoiden välillä sekä lopulta myös uudenlaisia viranomaismääräyksiä. Kansainvälisesti oman haasteensa 5G:n tietoturvamaisemaan tuovat myös maakohtaiset ja EU-laajuiset suositukset, lait ja säädökset.



1 5G:n tuomat keskeiset uudistukset

5G-teknologiaan ja -palveluihin liittyy runsaasti odotuksia, jotka liittyvät entisestään tehostuvaan langattomaan suorituskykyyn ja uudenlaisiin palveluihin. Tulevaisuudessa kaikki laitteet voivat olla jatkuvasti yhteydessä toisiinsa sekä internetiin nopeilla matalaviiveisillä yhteyksillä.

Suurimman muutoksen teknologian odotetaan tuovan aloilla, joilla se mahdollistaa täysin uudet palvelut ja käyttötapaukset sekä fyysisten prosessien digitalisoitumisen. Näitä ovat esimerkiksi teollisuuden, terveydenhuollon sekä liikenteen ja logistiikan sovellutukset. 5G-teknologia eri kehitysversioineen tuleekin olemaan digitaalisen yhteiskunnan perusrakenteita.

5G ei tule olemaan yksi homogeeninen verkko, vaan verkkoja tulee olemaan useita ja ne tulevat rakentumaan eri taajuusalueille, joilla on erilaiset ominaisuudet ja reunaehdot. Näin ollen tulevaisuudessa tullaan näkemään suorituskyvyltään ja käyttötarkoitukseltaan hyvin monenlaisia 5G-verkkoja. 5G-teknologian keskeisiksi taajuusalueiksi on Euroopassa tunnistettu erityisesti taajuusalueet 700 MHz, 3400–3800 MHz ja 26 GHz. 5G-järjestelmille on esitetty myös muita gigahertsiluokan taajuusalueita ja globaalisti niistä tullaan päättämään vuoden 2019 lopulla järjestettävässä maailman radiokonferenssissa (WRC-19).

Ensimmäiset kaupalliset 5G-toteutukset nähdään Suomessa oletettavasti vuoden 2019 aikana ja ne pohjautuvat vuoden 2018 lopulla huutokaupatulle 3,5 GHz taajuuskaistalle. Ensi vaiheen kaupalliset toteutukset keskittynevät alkuvaiheessa ensisijaisesti entistä nopeamman langattoman laajakaistan tarjoamiseen. 5G:n mahdollistamia uusia palveluita ja teknologian täysimittaisia hyötyjä tullaan näkemään vasta hieman myöhemmin, kun korkeiden taajuusalueiden käyttöön liittyvät päätökset on tehty, kaikki 5G-teknologian toiminnallisuudet sekä niitä tukevat päätelaitteet ovat laajamittaisesti saatavilla ja 5G-verkkoja on toteutettu riittävän kattavasti.

	2018	2019	2020	2021 >
Teknologian standardisointi	Ensimmäinen vaihe valmis (Release 15, entistä nopeampi laajakaista eMBB)	Toinen vaihe valmis (Release 16, uudet toiminnallisuudet mm. URLLC, mMTC)	5G:n tekniset määritykset valmistuvat	5G:n kehitystyö jatkuu
5G:n taajuudet Suomessa	3,5 GHz taajuusalueen huutokauppa	3,5 GHz taajuusalueen toimilupakausi alkaa Korkeampien taajuusalueiden kansainväliset taajuuspäätökset WRC-19:ssa lokakuussa	26 GHz taajuusalueen käyttöoikeuksien myöntäminen alkaa	Muita korkeita millimetrialueen taajuuksia otetaan 5G-käyttöön
Kaupalliset toteutukset Suomessa	Esikaupallisia testiverkkoja valmiina	Ensimmäiset 3,5 GHz -toteutukset hyödyntäen LTE:n verkkoydintä Päätelaitteita alkaa olla saatavilla	Todennäköisesti ensimmäiset 26 GHz- toteutukset Päätelaitesaatavuus paranee	Innovatiiviset 5G-palvelut, jotka hyödyntävät uutta verkkoarkkitehtuuria, viipalointia ja reunalaskentaa
EU:n 5G-tavoitteet	Jäsenmaissa on ensimmäisiä esikaupallisia verkkoja		Jäsenmaissa on vähintään yksi kaupunki, jossa rakennettu täysin kaupallinen 5G-verkko	Jäsenmaissa on kaikki kaupunkialueet ja niiden väliset liikennöintiväylät katettu katkeamattomalla 5G-peitolla vuoteen 2025 mennessä

Taulukko 1: Suuntaa-antava aikataulu 5G:n vaiheittaisesta toteutumisesta Suomessa.

1.1 Parempi langaton suorituskyky ja uudet käyttötapaukset

Siinä missä 2G-, 3G- ja 4G-teknologioiden datapalveluiden kehityksessä on ollut pääasiassa kyse nopeammista yhteyksistä, 5G-teknologia on perusteiltaan suurempi muutos. 5G-keskustelussa onkin tunnistettavissa kaksi erilaista lähestymistapaa. Ensimmäinen koskee uuden radioteknologian mahdollistamia uusia langattoman viestinnän nopeusluokkia ja aiempaa matalampia viiveitä. Tämä ajattelu on luonnollista historiallisessa langattoman viestinnän kehityksen viitekehyksessä. Se ei ole kuitenkaan kovin kiinnostava turvallisuusnäkökulmasta, sillä turvallisuutta koskevat muutokset koskevat lähinnä radiorajapinnan suojausta.

Toinen lähestymistapa on palvelulähtöinen ja keskittyy kysymykseen siitä, mitä palveluinnovaatioita langattoman viestinnän teknologioilla on mahdollista toteuttaa ja miten tämä muuttaa käsitystämme siitä, mikä on ylipäänsä mahdollista uuden teknologian sovellutuksilla. 5G-teknologian keskeisiin lupauksiin kuuluu esimerkiksi esineiden internetin (IoT, Internet of Things) nykyistä laajempien palvelumallien tukeminen. Tässä huomio siirtyy siihen, miten viestintäverkot tukevat sitä hyödyntäviä innovatiivisia uusia palveluita nykyistä paremmin. Esimerkiksi liikenteen, teollisuuden ja logistiikan uudenlaiset mobiiliverkkoa hyödyntävät palvelut kytkeytyvät tähän keskusteluun.

5G-teknologiamääritykset jakautuvat kolmeen osaan, jotka tukevat erilaisia käyttötapauksia:

Huippunopea langaton laajakaista (enhanced Mobile Broadband, eMBB).
Yhteysnopeudeltaan jopa kymmeniä Gbit/s tarjoavat langattomat yhteydet yrityksille, kotitalouksiin ja liikkuville käyttäjille. Ensivaiheessa toteutukset mahdollista myös hyödyntäen nykyistä televerkkojen infrastruktuuria päivittämällä radioverkon osat.

Luotettava lyhyen viiveen kommunikaatio (Ultra Reliable Low Latency Communications, URLLC).
Mahdollistaa erittäin pieniviiveiset langattomat yhteydet korkeaa luotettavuutta ja liki reaaliaikaisuutta vaativiin käyttötapauksiin kuten automaatioon ja etäohjaukseen. Lähelle sijoitettu reunalaskenta tukee sovelluksia. Käyttötapauksissa tarvitaan 5G-verkkoydin yhteysviiveiden minimoimiseksi.

Massiivinen koneiden välinen kommunikaatio (massive Machine Type Communications, mMTC).
Tukee mm. IoT-peruskäyttötapauksia, joissa vaaditaan suurta energiatehokkuutta ja toimintakykyä jopa kymmeneksi vuodeksi ja kytkettyjä laitteita on erittäin paljon.

Erilaiset käyttötapaukset voivat yhdistyä toisiaan tukevilla tavoilla. Esimerkiksi ajoneuvoverkko (Vehicle-to-anything, V2X) edellyttää edistyneissä käyttötapauksissa pieniä viiveitä ja luotettavaa viestinvälitystä. 5G-teknologiaa on suunniteltu käytettäväksi perinteisen maanpäällisen verkkototeutuksen lisäksi myös ajoneuvojen keskinäisessä sekä ajoneuvojen ja infrastruktuurin välisessä viestinnässä.

Viihdepalvelujen osalta ajoneuvoihin 5G:n välityksellä toimitettu suoratoistovideo vaatii nopeaa laajakaistayhteyttä, mutta toteutuvilla yhteysviiveillä ei välttämättä ainakaan alkuvaiheessa ole keskeistä merkitystä. Viiveiden merkitys voi korostua myöhemmissä käyttösovelluksissa, kuten lisätyn todellisuuden sovelluksissa. Yleisesti ottaen erilaisten 5G-verkkoon pohjautuvien uusien palveluiden kaupallinen saatavuus ja aikataulut vaihtelevat myös alueellisesti 5G-verkkojen saatavuuden mukaan.

5G-määrityksiin kuuluu myös mahdollisuus liittää 3GPP:n työn ulkopuolisia verkkoteknologioita 5G-ydinverkkoon. Tällöin operaattori mahdollistaa esimerkiksi langattoman lähiverkon (IEEE 802.11 WLAN, Wi-Fi) kautta tapahtuvan liittymisen suoraan 5G-palveluihin. Tämä on kustannustehokas ratkaisu palvelujen tuomiseksi esimerkiksi toimistokiinteistöihin ja tiiviisiin asuinrakennuksiin, joihin korkeilla

taajuuksilla toimivat 5G-ulkotukiasemat eivät pysty tarjoamaan riittävän voimakasta signaalia.

Tällainen toissijainen verkkoteknologia ei kuitenkaan välttämättä mahdollista optimaalisella tavalla kaikkia 5G:n toiminnallisuuksia, kuten suurta luotettavuutta, erittäin lyhyttä viivettä tai erittäin suurta yhteysnopeutta. Se voi silti tarjota riittävän suorituskykyisen yhteyden esimerkiksi joidenkin laajakaista- tai IoT-palvelujen tarjoamiselle.

1.2 Palveluihin pohjautuva arkkitehtuuri

Uudenlaiset mobiiliverkon palvelut tarvitsevat toteutuakseen uudenlaisen operaattorin ydinverkon (core network) arkkitehtuurin, joka skaalautuu käyttötarpeiden mukaisesti. Tämän ajatuksen tueksi 5G-teknologiamäärityksiin kuuluu Service-Based Architecture (SBA) -määritys[1], joka kuvaa millaisia palveluita televerkon arkkitehtuuriin kuuluu sekä miten palvelut rekisteröityvät ja liittyvät toisiinsa.

Standardi määrittää 18 erilaista palvelua, jotka kuuluvat 5G-järjestelmäarkkitehtuuriin. Palvelut huolehtivat esimerkiksi siitä, miten verkkoon liitettävät laitteet tunnistetaan ja että oikeat palvelut ovat päätelaitteiden käytettävissä. Verkon palveluiden tehtävien ja rajapintojen määrittely on 3GPP:n standardisoinnin olennainen sisältö.

Palveluiden rajapintojen toiminta perustuu seuraaviin web-teknologioihin:

HTTP/2-tiedonsiirtoprotokolla, joka on merkittävä uudistus internetin perusprotokollaan. Huomioitavaa on se, että vaikka HTTP/2-protokollan määritykseen ei sisälly vaatimusta tietoliikenteen salaamisesta TLS:ää käyttäen, 5G-määrityksissä sitä tulee käyttää ydinverkon komponenttien välillä, mikäli riittävää turvallisuutta ei toteuteta muutoin[2]. Muu keino voi olla esimerkiksi fyysinen turvallisuus.

JSON on vakioitu tiedostomuoto attribuuttiarvo-parien ja muiden sarjoitettavissa olevien (serialization) tietojen välittämiseen. Sen hyötyjä esimerkiksi XML-muotoon nähden on tiivis esitysmuoto, joka tarkoittaa aiempaa tehokkaampaa ja nopeampaa tietojen välitystä. Lisäksi JSON on laajasti käytössä web-teknologioissa ja toimii hyvin HTTP:n kanssa.

REST on yleisesti käytössä oleva rajapintojen suunnitteluperiaate. 3GPP on noudattanut tätä periaatetta sen varmistamiseksi, että arkkitehtuurin rajapinnat ovat riippumattomia itse palveluiden teknologiavalinnoista, kuten prosessoreista, käyttöjärjestelmistä ja ohjelmointikielistä. Tämän lisäksi yhdenkään palvelun ei tarvitse ylläpitää tietoa muiden palveluiden tilasta.

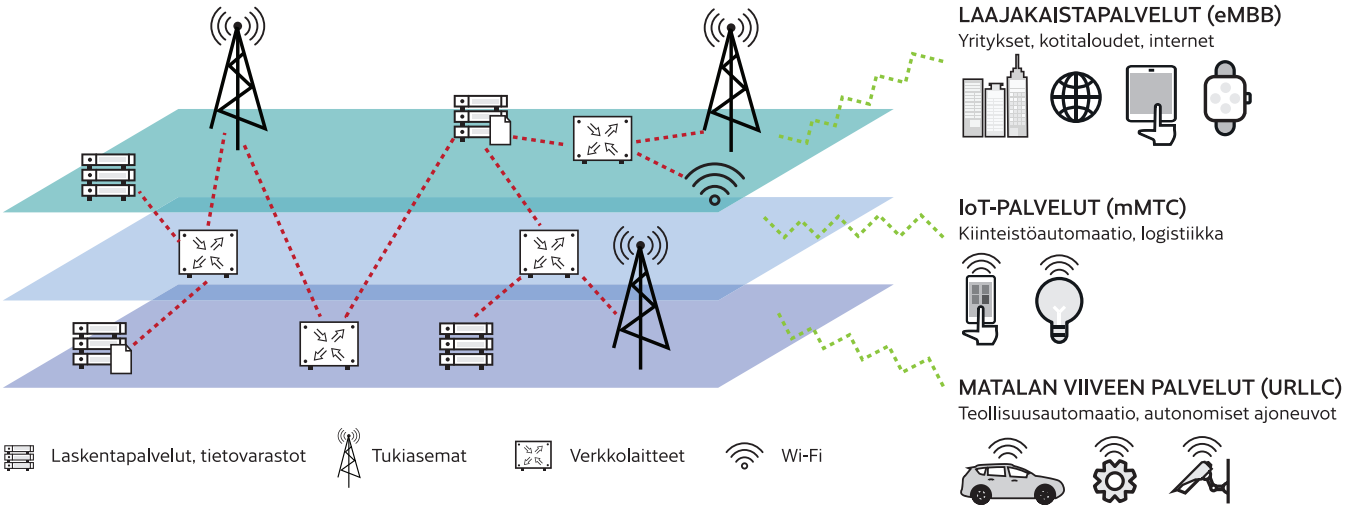
Edellä kuvattuja teknologioita käytetään operaattorin hallinnassa olevien palveluiden rajapinnoissa ja Network Exposure Function -rajapinnoissa (NEF), jotka avaavat operaattorin verkon toimintoja kolmansille palveluita tarjoaville osapuolille[3].

Verkkoja toteuttavien valmistajien ja operaattorien näkökulmasta palveluihin perustuva arkkitehtuuri avaa mielenkiintoisia mahdollisuuksia. Enää televerkon toiminnot eivät perustu kalliisiin, muuttumattomiin ja pitkäikäisiin koneisiin, vaan palvelurajapintoja toteuttaviin sovelluksiin, joita on mahdollista kehittää ja integroida nykyajan liiketoiminnan edellyttämällä kehitysnopeudella. Eri valmistajat voivat toteuttaa ratkaisujaan yhdistelemällä eri palveluita, jolloin markkinoille syntyy innovatiivisia tuotekokonaisuuksia. Vastaavasti operaattorit voivat yhdistää kaupallisia ja myös avoimen lähdekoodin toteutuksia parhaaksi katsomallaan tavalla.

[1] 3GPP 23.501, System Architecture for the 5G System

[2] 3GPP 33.501, Security architecture and procedures for 5G System

[3] Georg Mayer, RESTful APIs for the 5G Service Based Architecture – https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_617.pdf



Kuva 1: Kapasiteetin ja infrastruktuurin virtualisoinnilla voidaan tuottaa palveluviipaleita erilaisiin toisistaan poikkeaviin käyttötarpeisiin.

1.3 Dynaaminen kapasiteetin hallinta

Keskeinen 5G:n piirre ja edellä kuvattujen innovatiivisten käyttötapausten mahdollistaja on ajatus modernista arkkitehtuurista, jonka toiminnot ja kapasiteetti ovat mukautettavissa joustavasti kulloistenkin palveluiden ja käyttömäärien tarpeisiin. Joustavuus varmistaa, että tehdyt investoinnit viestintäverkon infrastruktuuriin ovat tehokkaassa käytössä ja loppukäyttäjien palvelukokemus on paras mahdollinen. Keskeiset keinot tämän saavuttamiseksi ovat virtualisointi ja ohjelmistopohjainen verkon ohjaus.

5G:ssa virtualisointi ulottuu useille eri tahoille. Palveluihin pohjautuvassa arkkitehtuurissa palvelukomponentit ovat virtualisoitavissa ohjelmistoilla. 5G-toteutuksissa myös itse verkkotoiminnot ovat virtualisoitavissa, verkot ohjattavissa ohjelmistoilla ja verkon kapasiteetti jaettavissa virtuaalisiin viipaleisiin erilaisten tarpeiden mukaisesti. Lisäksi virtualisointia hyödynnetään myös reunalaskennan eri toteutuksissa.

Verkkotoimintojen virtualisoinnilla (Network Function Virtualization, NFV) tarkoitetaan 5G-verkkotoimintojen toteuttamista ohjelmallisesti perinteisten verkkolaitteiden sijaan. Tällöin operaattorit voivat toteuttaa erilaisia toimintoja, kuten nimipalveluja, sovelluspalomuureja ja liikenteen salausta virtuaalikoneissa, joita voidaan skaalata dynaamisesti verkossa käyttö- ja asiakastarpeiden mukaisesti.

Ohjelmisto-ohjatuilla verkoilla (Software Defined Networking, SDN) tarkoitetaan verkkotoimintojen virtualisointia ja niiden siirtämistä yhdenmukaiselle ohjaustasolle, jossa verkon ominaisuuksia voidaan hallita ohjelmistorajapintojen kautta. Tällöin 5G-verkkojen hallintaa voidaan automatisoida ja hallita ohjelmallisesti ja dynaamisesti muuttuvien tarpeiden mukaisesti. Tämä mahdollistaa helpomman verkon hallinnan, paremman kustannustehokkuuden sekä uusien palveluiden innovoinnin ja rakentamisen yhtenäisten rajapintojen päälle.

SDN ja NFV toimivat mahdollistajana verkon viipaloinnille (Network Slicing), jolla tarkoitetaan usean loogisen 5G-verkon toteuttamista yhden fyysisen verkkoinfrastruktuurin päälle. Tämä mahdollistaa edellä kuvattuja käyttötarpeita, jotka vaativat verkolta tiettyjä palvelutason toimintatakuita esimerkiksi viiveiden ja nopeuden muodossa.

Esimerkiksi laajakaistakäyttäjät, älykäs liikenne, teollisuus, logistiikka ja pelastusviranomaiset tarvitsevat erilaisia ominaisuuksia ja palvelutason takuita verkolta. Kukin viipale on loogisesti eriytetty muista samalla alustalla toimivista viipaleista ja voi toteuttaa alustasta riippumattoman arkkitehtuuriltaan, toiminta-alueeltaan, ominaisuuksiltaan ja teknologioiltaan erillisen 5G-verkon.

5G-palvelut tarvitsevat yhteyksien lisäksi muitakin tukipalveluita. Siksi 5G-teknologiamurrokseen liitetään tyypillisesti myös Multi-access Edge Computing -reunalaskentastandardi (MEC, tunnettiin aiemmin nimellä Mobile Edge Computing), jota osaltaan standardisoidaan Euroopan telealan standardisoimisjärjestö ETSI:n piirissä[4].

Reunalaskennan sovellutuksia on odotettavissa alueilla, joita on mahdollista optimoida tuomalla laskentakapasiteettia ja sisällön datan välivarastoja verkossa lähelle käyttäjiä silloin, kun niitä tarvitaan muun muassa reaaliaikaisen ohjaamisen tai automaation mahdollistamiseksi. Käytännössä tämä tarkoittaa sitä, että operaattorin verkkoon tuodaan palveluntuottajien laatimia ohjelmistoja eli työkuormia (workload).

Kun sovelluksen ohjelmisto ja datan käsittely toimii operaattorin verkossa mahdollisimman lähellä päätelaitteita, saadaan uuden radiotekniikan tarjoamat edut muun muassa lyhyen viiveen osalta hyödynnettyä kokonaisvaltaisesti. Työkuormat voivat koostua useista moduuleista ja ne voivat tarpeen mukaan hakea lisää moduuleita myös verkon kautta.

Reunalaskennan käyttötapauksia ovat esimerkiksi:

- IoT-laitteiden toiminnan mahdollistaminen ja integraatiot valmistajan omiin pilvialustoihin: MEC-työkuorma voi tarjota IoT-laitteille serverless-rajapintoja (Function as a Service, FaaS) tietojen keräämistä, toimittamista tai käsittelyä varten. Tällöin itse laitteet voidaan toteuttaa aiempaa edullisemmin. Esimerkiksi kiinteistöautomaatiojärjestelmä tai kiinteistöturvallisuuden järjestelmä voi jatkossa toimia ilman paikallista palvelinta tai yhdyskäytävää, kun 5G-automaatiolaitteiden toimintojen ohjaus ja valvonta on toteutettu MEC-työkuormassa.
- Fyysiseen paikkaan sidottu tietojen käsittely: Yhdistelemällä reunalaskentaa ja verkon viipalointia on mahdollista toteuttaa tietojenkäsittelyn sovellutuksia, joiden toiminnan tai pääsynhallinnan edellytyksenä on sijainti ennalta määrätyssä paikassa. Esimerkiksi sairaanhoidon henkilöstölle voidaan toteuttaa pääsy potilasaineistoon siten, että päätelaitteen yhteydet tähän tietoon estyvät, kun laite poistuu sairaalan alueelta.
- Tuotanto- ja teollisuusympäristöissä voidaan hyödyntää reunalaskentakapasiteettia, jolloin prosessien digitaaliseen ohjaamiseen ja automatisointiin tarvittavat pienet viiveet saadaan toteutumaan dynaamisessa langattomassa verkossa. Tämä mahdollistaa joustavan automaatioympäristön ja verkon räätälöinnin tarpeiden muuttuessa sekä verkossa liikkuvan ja siinä kerätyn datan pysymisen yrityksen omassa hallinnassa.

1.4 Mikro-operaattorit

Valtakunnallisten operaattorien toteutusten lisäksi 5G-verkkoja nähdään oletettavasti myös paikallisiin tarkoituksiin mukautettuina erillisinä toteutuksina. Konseptista käytetään myös nimeä mikro-operaattori. Näiden toteutusten kantava idea on paikallisen mukautetun verkkoratkaisun rakentaminen ja operointi erityiskohteissa. Tällaisia kohteita voivat olla esimerkiksi oppilaitokset, sairaalat, kauppakeskukset, tapahtumakeskukset ja tehtaat[5].

Paikalliset räätälöidyt verkkototeutukset voisivat hyödyntää verkoissaan valtakunnallisilta operaattoreilta vuokrattuja tai tähän käyttöön mahdollisesti erikseen osoitettuja taajuuksia tai toimia luvasta vapailla taajuuskaistoilla. Paikallisesti räätälöityjen verkkojen haltijat voivat toteuttaa palveluita valtakunnallista operaattoria rajatummin ja siten mahdollisesti myös edullisemmin. Näin mahdollistuvat myös sellaiset toteutukset, jotka eivät ole valtakunnallisten operaattorien kannalta kaupallisesti riittävän houkuttelevia. Paikallisen toimijan tiloihin ja ympäristöön tuodulla reunalaskennalla on monessa tapauksessa keskeinen rooli erityispalveluiden sisällön ja laskentatoimintojen toteutuksessa. Paikallisten verkkojen palvelu- ja toteutusmallit ovat kuitenkin vielä tutkimuksen ja kokeilujen alainen alue.

[4] ETSI, Multi-access Edge Computing – https://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing5

[5] P. Ahokangas et al., "Future micro operators business models in 5G" – https://pdfs.semanticscholar.org/dcee/f733cc64ee1a4f29d0dbdc46d9abea4e1908.pdf

2 5G:n kyberturvallisuudesta

Jokaisen uuden teknologian kohdalla on tarkoituksenmukaista arvioida tietoturvallisuus- ja tietosuojavaikutukset. Erityisen tärkeää arviointi on 5G:n kaltaisen teknologian kohdalla, joka on 2020-luvun digitaalisen yhteiskuntamme perusrakenteita. Mihin tämän teknologian turvallisuus perustuu ja millaisia kyberturvallisuuden uhkakuvia voimme tunnistaa nykyisillä tiedoilla?

5G-teknologian tietoturvallisuus on saanut osakseen enemmän huomiota kuin minkään aiemman verkkosukupolven. 5G-standardi määrittelee koko joukon parannuksia viestinnän turvallisuuden ja käyttäjien tietosuojan parantamiseksi. Kuluttajan näkökulmasta tilanne siis paranee. Parannuksista huolimatta on vaikea etukäteen arvioida, kuinka paljon aiempaa paremmin uuden sukupolven viestintäalusta kykenee suojaamaan tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Tämä johtuu olennaisesti seuraavista seikoista:

Operaattorien 5G-verkkoytimet perustuvat uudenlaiseen arkkitehtuuriajatukseen ja protokolliin, joissa palveluntuottajilla on pääsy aiempaa lähemmäs ydinverkkojen (core-verkkojen) toimintoja. Tämä on tarpeen, jotta 5G-palvelulupaukset esimerkiksi matalista viiveistä voidaan kaikilta osin lunastaa. Tästä johtuen verkon ytimen ja reunan välinen ero hämärtyy ja tarvittavat integraatiorajapinnat ovat turvallisuuden kannalta kriittisiä, koska ne ulottuvat lähelle verkon ydintä.

Ydinverkkojen arkkitehtuuri muuttuu virtualisoiduksi ja alkaa siten muistuttaa teknologioiltaan tyypillisiä IT-alustainfrastruktuureja. Turvallisuusnäkökulmasta tämä voi tarkoittaa, että viestintäinfrastruktuurin suojattava pinta-ala kasvaa. Operaattorien tietoturvaprosessien, kuten ydinverkon haavoittuvuudenhallinan, muutoksenhallinnan ja turvallisuusvalvonnan on oltava korkeatasoisia turvallisuusriskien välttämiseksi.

5G-palvelumallit perustuvat verkon loogiseen viipalointiin ja virtualisointiin erilaisia käyttötapauksia varten. Kukin viipale sisältää erilaisia palveluominaisuuksia. Aiemmista teknologioista laskennan ja verkon virtualisoinnin alueilta tiedetään, että turvallisuusrajojen ylläpitäminen jaetuissa resursseissa on vaikeampaa kuin fyysisesti eriytetyissä ympäristöissä. IoT-palveluviipaleet voivat koostua 2020-luvulla suuresta määrästä erilaisia matalan suojaustason laitteita. Tällöin on mahdollista, että hyökkääjä voi hyödyntää esimerkiksi näiden laitteiden tietoturvapuutteita kohdistaessaan hyökkäyksiä kriittisempiin palveluviipaleisiin.

Standardi määrittelee mahdollisuuden käyttää hyviä salaus- ja tunnistusratkaisuja arkkitehtuurin eri osissa operaattorin ydinverkon, operaattorien välisen liikenteen sekä päätelaitteen viestinnän suojaamiseksi. On kuitenkin epäselvää, miten suojausmahdollisuuksia sovelletaan käytännön toteutuksissa. Päätelaitteiden yhteensopivuusvaatimukset mahdollistavat myös toiminnan aiempien sukupolvien verkkojen kanssa. Lisäksi operaattorien välisen viestinnän suojaaminen vaatii avaimenhallintainfrastruktuureja, jotka ovat samalla mahdollisia ongelmanlähteitä infrastruktuurien luotettavalle toiminnalle ja vaativat tasapainoilua kustannuksien kanssa.

5G-standardi ei määrittele kokonaistietoturvallisuusarkkitehtuuria 5G-verkoille. 5G-verkkojen tietoturvaan vaikuttavat oleellisesti myös toteutuskohtaiset ratkaisut, laitteiden fyysinen suojaus ja reunalaskentaympäristön turvaratkaisut, joita ei ole käsitelty 5G-standardissa.

Turvallisuusnäkökulmien vaikutukset eri käyttäjätahoille vaihtelevat.

Yksittäisten henkilöiden näkökulmasta henkilökohtaisten tietojen käsittely operaattorin verkossa ja kolmannen osapuolen palveluissa lisääntyy 5G:n yleistyessä. Palvelumallien kehittyessä selviää tarkemmin, miten näitä tietoja hyödynnetään palveluiden tuotannossa. Viestinnän luottamuksellisuuden suojaamiseen henkilökäyttäjien on jatkossakin suositeltavaa käyttää päästä-päähän salaavia viestintäsovelluksia, etenkin verkkovierailutilanteissa.

Yritysten ja muiden käyttäjäorganisaatioiden näkökulmasta avainkysymys on se, miten luotettavasti uudet infrastruktuurit tukevat heidän käyttötapauksiaan sekä suojaavat käytännössä suljetun ympäristön suojaustasoa vaativien palvelutoteutusten luottamuksellisuutta ja eheyttä. Jos saatavaan palvelutasoon tai tietojen eheyteen aiheutuu häiriöitä, voivat vaikutukset kriittisiin liiketoimintaprosesseihin olla merkittäviä. Tietojen luottamuksellisuuden menettäminen voi johtaa myös kilpailuedun menetykseen. 5G:n varhaisten omaksujien pitää olla tietoisia hyödyistä, riskeistä ja mahdollisuuksista rajoittaa riskejä erilaisilla kompensoivilla teknisillä ja hallinnollisilla menetelmillä.

Yhteiskunnan näkökulmasta etäkäyttöratkaisujen, kuten etäterveydenhuollon, reunalaskennan sovellusten, kuten kodin energiankulutuksen hallinnan, sekä autonomisen logistiikan ja liikenteen toimintojen tulee pysyä luotettavina. Operaattorin haavoittuvuuksien hallinta tulee entistä tärkeämmäksi ja verkon ydinkomponenttien toimittajan tietoturvallisuusprosesseihin kohdistuu suuria odotuksia. Keinot 5G-ympäristöä käyttävien palveluiden riskienhallinnan tukemiseen ovat keskeinen osa jatkuvuuden varmistamista. Samoin 5G-infrastruktuurin fyysinen turvaaminen nousee keskeiseksi alueeksi.

3 Muutokset Liikenne- ja viestintäviraston toimintakentässä

Yhteiskunnallisesta näkökulmasta on syytä arvioida sitä, tarvitaanko 5G-tekniikkaan tukeutuvien ympäristöjen kyberturvallisuuden varmistamiseen uudenlaista viranomaisohjausta ja viranomaismääräystyötä. Tämän selvityksen havaintojen perusteella tällainen ohjaus voisi koskea esimerkiksi verkon käyttäjiä koskevien tietojen keräämistä ja käsittelyä sekä palvelutason varmistamista palveluille, joissa toteutuneet riskit voivat haitata digitaalisen yhteiskunnan yleisestä turvallisuutta. Tällaisia sovellutusalueita voisivat olla esimerkiksi terveydenhuolto, teollisuusautomaatio, älyliikenne ja viranomaisten käyttämät palvelut.

Samaan aikaan 5G on vahva paradigmamuutos uuteen suuntaan. Matkapuhelinverkkojen tietoturvallisuus on perinteisesti luottanut ainakin osittain siihen, että verkkoelementit ja palvelut eivät ole suoraan yhteydessä internetiin eikä tietoa ole käsitelty suoraan matkapuhelinverkkojen sisällä. 5G:n myötä tämä osittain muuttuu ja tuo uusia tietoturvallisuuden hallinnan vaatimuksia verkkojen ylläpitäjille. Ympäristö muuttuu kärjistetysti dataa kuljettavasta tiedonsiirtoputkesta tietoa kerääväksi ja sitä jalostavaksi monimuotoiseksi pilvipalveluksi, jossa turvallisuuden pitää olla varmistettuna loppukäyttäjältä aina verkon ytimeen ja palvelinkeskuksiin asti. Samassa ohjelmistot tulevat entistä vahvemmin keskiöön ja tarjoavat palveluita myös edellisen sukupolven matkaviestinverkoille.

Käyttäjille, yrityksille ja muulle yhteiskunnalle tarjottujen palvelu-rajapintojen ja jaetun infrastruktuurin turvallisuus muodostuu kriittiseksi osaksi kokonaisturvallisuutta. Tällöin operaattorien verkon tietoturvallisuusmallien on lähennyttävä suurien yhteiskunnan kriittisiä palveluita tuottavien virtuaaliohjelmistoihin ja teknologiaan perustuvien palvelinkeskusympäristöjen vaatimuksia. Samoin keskeinen kysymys tulee olemaan, että pitääkö kaikki halukkaat toimijat hyväksyä jaettujen palveluiden asiakkaiksi ja miten varmistetaan, että mahdolliset haitalliset toimijat eivät kykene aiheuttamaan haittaa samassa ympäristössä toimiville kriittisille toiminnoille ja kuinka estetään riskien leviäminen osapuolelta toiselle.

Samalla kun tietoja käsittelevät palvelut voivat sijaita jo lähimmässä tukiasemassa, tulee 5G-verkkojen tukiasemien fyysinen suojaus entistä merkityksellisemmäksi. Tukiasematiheyden kasvaessa ja vaihtelevien sijoituspaikkojen myötä fyysisen suojauksen merkitys korostuu.

5G:n myötä myös uusia toimijoita saapuu markkinoille. Eräs ratkaistavista kysymyksistä kuuluu, että pitääkö 5G:n ympärille rakentuvia määräyksiä valmisteltaessa huomioida uudenlaisten toimijoiden aiheuttamat riskit. Samaan aikaan 5G:n merkitys yhteiskunnalle kasvaa, sillä yhä suurempi osa yhteiskunnalle tärkeistä toiminnoista tulee käyttämään 5G-teknologian päällä tuotettuja palveluita. Tällöin verkon toimittajaan ja sen tietoturvallisuusprosesseihin on kyettävä luottamaan. Yksi tapa hallita tätä riskiä on hajauttaa 5G-palvelutuotannossa käytettävien ohjelmistojen ja laitteistojen toimittajia siten, että yksi toimittaja ei toimita kaikkia verkkoja ja sen komponentteja.

Edellä mainituista syistä on tärkeää rakentaa malleja, joilla 5G-palveluntarjoajien riskinottohalukkuus saadaan jatkuvasti pidettyä lähellä 5G-asiakaskunnan ja yhteiskunnan riskinottohalukkuutta. Tässä työssä EU:n, kansallisten viranomaisten ja operaattoreiden välisellä yhteistyöllä keskeinen rooli.

Traficom seuraa aktiivisesti EU-tasoista 5G:hen liittyvää työtä ja varmistaa, että Suomeen syntyvät 5G-toteutukset tulevat vastaamaan tietoturvallisuudeltaan sellaista tasoa, että digitaalisen yhteiskunnan kriittisiä toimintoja sekä sen tarvitsemia uusia palveluja voidaan rakentaa niiden varaan.

4 Yhteenveto

5G-teknologiaan siirtyminen tuo mukanaan suuremman paradigmamuutoksen kuin yksikään aikaisempi matkaviestinverkkosukupolvi on tuonut. 5G-verkot tulevat tulevaisuudessa olemaan digitaalisen yhteiskuntamme perusrakenteita. Riskienhallinnallisesti tämä tarkoittaa siirtymistä ympäristöön, jossa haavoittuvuuksien ja tietoturvallisuuden hallinnalle asetetaan yhä suurempia vaatimuksia ja verkkoympäristön kompleksisuuden lisääntymisen vuoksi toimivien hallintamallien toteuttaminen on merkittävästi aiempaa haastavampaa.

Muutos aiemmista verkkosukupolvista kohti 5G-maailmaa tulee vaatimaan tiedon aktiivista jakamista, viranomaisohjauksen rajojen uudelleentarkastelua ja yhä laajempaa vuoropuhelua eri toimijoiden välillä sekä lopulta myös uudenlaisia viranomaismääräyksiä.

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000
traficom.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus