Muistio: kommentti HE 98/2020 sähköisen viestinnän palveluista

Ericsson kiittää Liikenne- ja viestintävaliokuntaa mahdollisuudesta lausua sähköisen viestinnän palveluista annetun lain muuttamisesta HE 98/2020. Asiantuntijuutemme koskee erityisesti verkkoturvallisuutta ja siten meidän lausuntomme keskittyy erityisesti 5G-vekkojen kyberturvallisuuteen.

Tausta

Esityksen tavoitteet ovat moninaiset liittyen niin kuluttajan asemaan, viestintäverkkojen turvallisuuteen, viestintäverkkoinvestointeihin ja palveluiden saatavuuteen. Samalla sillä pannaan täytäntöön EU-lainsäädäntöä[1]. Erityisen oleellinen verkkojen turvallisuuden kannalta on niin sanottu EU 5G Toolbox[2], eli jäsenvaltioiden yhteinen keinovalikoima koskien viestintäverkkojen kriittisten osien suojaamista, johon Suomikin on sitoutunut[3], [4].

EU-jäsenmaiden tekemien kansallisten riskiarvioiden lisäksi EU:n yhteisen keinovalikoiman sisältöön vaikuttivat myös Enisan uhkakuvaraportti 5G:stä[5], sekä BERECin 5G:n turvallisuutta pohtiva työryhmä. Poliittisella tasolla tähän on sitouduttu, kuten neuvoston päätöksessä 1.-2.10.2020 todetaan[6], [7], [8].

---

[1] 11.6.2020, LVM:n tiedote: https://www.lvm.fi/-/sahkoisen-viestinnan-lainsaadanto-uudistuu-1209109

[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_123

[3] Euroopan neuvoston kokous 22.3.2019; https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/en/pdf

[4] Euroopan komission yhteinen lähestymistapa; https://ec.europa.eu/commission/news/common-eu-approach-security-5g-networks-2019-mar-26_en

[5] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[6] Liikenne-, televiestintä- ja energianeuvoston (TTE council) tapaaminen 3.11.2019; https://www.consilium.europa.eu/media/41595/st14517-en19.pdf

[7] Neuvoston päätelmät Euroopan digitaalisen tulevaisuuden rakentamisesta (9.6.2020); https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf

[8] Euroopan neuvoston kokous 1.-2.10.2020; https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf

Edellämainittujen lisäksi Euroopan talous- ja sosiaalikomitea antoi lausunnon 18.9.2020[9] liittyen EU:n yhteisen keinovalikoiman täytäntöönpanoon.

Kaikkien EU:n jäsenvaltioiden sitoutuminen yhdessä laadittuihin suosituksiin vähentää kansallisen tason pirstoutumista. Suomen ja muiden jäsenmaiden mahdolliset poikkeamat yhteisestä rintamasta saattavat haitata Euroopan sisämarkkinoita, ja saattavat altistaa Suomen hajanaiseen turvallisuuslähtökohtaan suhteessa muihin, kokonaisvaltaisemmin yhteisiä keinovalikoimia noudattaviin EU-jäsenmaihin.

Suomessa lain valmisteluvaiheessa turvallisuuteen liittyvistä kysymyksistä käytiin runsaasti keskustelua ja aiheeseen kiinnitettiin huomiota useiden eri tahojen lausunnoissa[10]. Eri ministeriöiden, ja myös sidosryhmien, välillä oli erimielisyyttä siitä, paneeko ehdotettu lainsäädäntö riittävällä tavalla täytäntöön EU:n jäsenmaiden yhteisen keinovalikoiman mukaiset toimenpiteet, joilla suojataan 5G-verkkoja yhteisessä riskiarviossa tunnistettuja riskejä vastaan (ks. Alla oleva taulukko). 24.7.2020 julkaistun välitilannekatsauksen[11] mukaan EU:n yhteisen keinovalikoiman täytäntöönpanossa tunnistettiin vielä puutteita.

[9] https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/secure-5g-deployment-eu-toolbox

[10] Hankesivu VN, lausunnot helmikuu 2020: https://valtioneuvosto.fi/hanke?tunnus=LVM004:00/2019

[11] Katso sivut 7-8 in https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

(source: the EU coordinated risk assessment report)

I - Risk scenarios related to insufficient security measures	**R1-**Misconfiguration of networks **R2-**Lack of access controls
II - Risk scenarios related to 5G supply chain	**R3-**Low product quality **R4-**Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis
III - Risk scenarios related to *modus operandi* of main threat actors	**R5-** State interference through 5G supply chain **R6-** Exploitation of 5G networks by organised crime or organised crime group targeting end-users
IV - Risk scenarios related to interdependencies between 5G networks and other critical systems	**R7-** Significant disruption of critical infrastructures or services **R8**-Massive failure of networks due to interruption of electricity supply or other support systems
V - Risk scenarios related to end user devices	**R9**-Exploitation of IoT (Internet of Things), handsets or smart devices

Kuva 1: Kooste EU:n jäsenmaiden yhdessä tunnistamista 5G:tä koskevista riskeistä[12].

Suomen asema muihin jäsenmaihin suhteutettuna

Tärkeä kysymys lainsäädännön osalta on siis se, toteuttaako Suomi kaikki suunnitellut, yllä mainittuja riskejä hallitsevat toimenpiteet 5G-verkkojen loppukäyttäjien suojelemiseksi niin, että Suomi on tulevaisuudessakin Euroopan tietoturvallisuuden kärkimaita pirstaloimatta sisämarkkinoita.

Vain kokonaisvaltaisella yhteisen keinovalikoiman täytäntöönpanolla on mahdollista hallita 5G-verkkojen tunnistettuja turvallisuusriskejä. Epätäydellinen tai valikoiva täytäntöönpano jättää tunnistettuja riskejä hallitsematta. EU-maiden yhteinen keinovalikoima on suunniteltu kokonaisuutena, joka vain kokonaisuudessaan implementoituna hallitsee riskiarviossa tunnistetut riskit.

Nykyinen, hallituksen esittämä 5G:tä koskevan lain ja siihen liittyvä perustelumuistion muotoilu, jättävät avoimeksi erityisesti verkkojen kehitykseen liittyviä näkökulmia. Kriittiset osat, jotka voivat periaatteessa avata ovia valtiollisille operaatioille tai muille vaikuttamisyrityksille, ovat teknisten laitteiden lisäksi entistä useammin ohjelmistoja, järjestelmäpäivityksiä ja muita ei-fyysisiä verkon osia. Kriittiset osat eivät välttämättä ole eriytettyinä ei-kriittisistä osista, eikä niitä voi keskittää ehdotetun lainsäädännön mukaisesti pelkästään ydinverkon laitteisiin edes nykyään, mutta varsinkaan tulevaisuudessa. Esimerkiksi radiopääsyverkon ja ydinverkon osien erottaminen

[12] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

toisistaan fyysisellä ja ohjelmistotasolla on hankalaa. Muotoilujen tulisikin siten tunnistaa tämä muutos verkkoarkkitehtuurissa jo nykyaikaa vastaavaksi, mutta ennen kaikkea tulevaa kehitystä silmällä pitäen[13].

Suomessa olisi siten syytä käydä perusteellinen keskustelu aiheesta erityisesti koskien esityksen 5G:tä koskevia osia, ja arvioida seurataanko Suomessa esitetyssä ratkaisussa täysimääräisesti EU-jäsenmaiden yhteisiä määritelmiä ja yhdessä sovittuja toimenpiteitä 5G-verkkojen suojaamiseksi.

Taustaa Ericssonista:

Ericsson on yksi johtavista tieto- ja viestintäteknologian (ICT) tarjoajista verkko-operaattoreille.

Mahdollistamme asiakkaidemme menestyksen verkottuneessa maailmassa tuottamalla teknologiaa ja palveluita, joita on helppo ottaa käyttöön ja skaalata teleoperaattorin tarpeen mukaisesti.

Laaja tuotevalikoimamme kattaa verkot, digitaaliset palvelut, operointipalvelut ja kehittyvän liiketoiminnan 5G- ja IoT-alustoilla. Tutkimus ja kehitys (T & K) on liiketoimintamme ytimessä noin 24 000 työntekijällämme. 54 000 myönnetyllä patentillamme olemme yksi vahvimmista alamme toimijoista.

Suomessa Ericsson työllistää yli 800 ammattilaista, joista suurin osa työskentelee Kirkkonummella. Ericsson toimii läheisessä yhteistyössä paikallisten teleoperaattoreiden kanssa digitalisaation edistämiseksi maassamme. Lisäksi Suomen Ericsson panostaa tutkimukseen ja kehitykseen erityisesti verkkoturvallisuuden, esineiden internetin, pilvi- ja 5G-teknologian alueilla.

[13] 7.5.2020 Sisäministeriön muistio SM2014368: https://api.hankeikkuna.fi/asiakirjat/f4a8e63a-5c4f-4c82-a778-dbed38de6595/d721accd-c567-4b07-bbb3-1efd5a0f191c/LAUSUNTO_20200617072106.PDF