1. PEJOJÄOS:n lausunto AQ9902/4.6.2020/TL IV (PUOLUSTUSVOIMIEN LAUSUNTO PUOLUSTUSMINISTERIÖN HALLINNONALAN 5G LINJAUSTEN VALMISTELUUN)

PÄÄESIKUNNAN ASIANTUNTIJAN KUULEMINEN HALLITUKSEN ESITYKSEEN HE 98/2020

1 Yleistä

Muistio perustuu viitteen mukaiseen PEJOJÄOS:n lausuntoon PLM:n hallinnonalan 5G linjausten valmistelussa. Lausunnossa keskestä on riskiarvio, joka huomioi mobiiliverkkojen käyttötapaukset nykytilanteessa sekä 5G-teknologian käyttöönoton myötä syntyvät uudet riskit.

Toisessa alaluvussa tiivistyy keskeiset riskit 5G -teknologian käyttöön ottoon liittyen. Alaluvussa esitetään vaatimuksia puolustusvoimille, viranomaisten väliselle yhteistoiminnalle ja lainsäädännölle. Kolmannessa alaluvussa arvioidaan hallituksen esityksen mahdollistama lainsäädännön tuki riskien hallintaan. Kokonaisuutena voidaan todeta, että hallituksen esitys vastaa hyvin tunnistettuihin vaatimuksiin eikä hallituksen esitykseen ole tarve esittää muutoksia.

2 5G -teknologian käyttöönottoon liittyvä riskien hallinta

2.1 5G -teknologian käyttöön liittyvät riskit

Maanpuolustuksen kannalta keskeisimpänä riskinä nähdään valtiollisen toimijan tiedustelu ja vihamielinen vaikuttaminen laitetoimittajien ja toimitusketjujen kautta. 5G-teknologian käyttöönoton myötä toimittajaverkostot monimutkaistuvat. Kaikissa laitteissa, mukaan lukien verkkolaitteet siirrytään ohjelmistopohjaisuuteen (SDN), mikä lisää suorituskykyä mutta samalla tuo uusia riskejä. Ohjelmistopäivitysten ja muutosten tahti tulee arvion mukaan kiihtymään. Tiedon määrä ja muutosnopeus ei mahdollista riskien hallintaa pelkästään teknisesti.

5G-teknologian käyttöönoton myötä mobiiliratkaisujen määrä lisääntyy kasvattaen hyökkäyspinta-alaa kybertiedusteluun ja kybervaikuttamiseen. Verkkojen hallinnan ja konfiguraatiovirheiden, puutteellisen pääsynhallinnan ja heikkolaatuisen tai kirjavan laitekannan aiheuttamat riskit lisääntyvät. Näiden riskien toteutuminen saattaisi aiheuttaa häiriöitä palveluiden saatavuuteen ja samalla niitä voi hyödyntää

vihamielinen valtiollinen toimija. Verkon reunoilla näitä haavoittuvuuksia voivat hyödyntää myös rikolliset toimijat, jonka seurauksena riskit ovat todennäköisesti vähäisiä, mutta kuitenkin kiusallisia.

2.2 Vaikutukset puolustusvoimissa

Operatiivisissa johtamisjärjestelmissä ja tiedustelun erillisjärjestelmissä ei käytetä mobiiliratkaisuja, mutta tulevaisuudessa voi olla vaikeaa saada päätelaitteita ja verkkolaitteita, joihin ei ole valmiiksi integroituna mobiiliratkaisuja.

Arvion mukaan puolustusvoimien alemman suojaustason verkoissa tullaan käyttämään langattomia 5G-ratkaisuja. Esimerkkeinä tästä ovat turvallisuus- ja kiinteistönvalvontajärjestelmät, arjen ratkaisut ja varuskuntien langattomat ratkaisut (mikro-operointi). 5G käyttöönotto lisää suorituskykyä uusien käyttötapausten, langattomuuden, helppokäyttöisyyden ja kustannustehokkuuden vuoksi, mutta samalla lisää kuitenkin hyökkäyspinta-alaa vihamielisen valtion tiedustelulle ja vaikuttamiselle.

5G-teknologian käyttöönottoon liittyvä riskitaso pysyy arvion mukaan samana kuin nykyisissä mobiilijärjestelmissä vuoteen 2025 saakka. Tämän jälkeen käyttöön otetaan 5G-standalone verkonhallinta, joka nostaa riskitasoa erityisesti verkonhallintamekanismien osalta.

Puolustusvoimien kumppanit ja palveluita tuottavat toimittajat tulevat arvion mukaan käyttämään 5G-teknologiaa. 5G käyttöönotto parantaa palveluiden laatua, saatavuutta ja kapasiteettia, mikä tehostaa toimintaa ja pienentää saatavuuteen ja kapasiteettiin liittyviä riskejä. 5G käyttöönotto lisää kuitenkin hyökkäyspinta-alaa ja monimutkaistaa toimittajaverkostoja lisäten riskiä vihamielisen valtion tiedustelulle ja vaikuttamiselle.

Arvion mukaan mobiiliratkaisujen käyttö (5G, IoT) lisääntyy puolustusvoimien päivittäisten toimintojen ja logistiikan automatisoinnissa. 5G-teknologian mahdollisuudet houkuttelevat käyttämään teknologiaa uusien hyötyjen, langattomuuden, helppokäyttöisyyden ja kustannustehokkuuden vuoksi. Henkilöstön omien IoT -laitteiden käyttö tulee lisääntymään mm. päätelaitteiden, älykellojen, terveys- ja liikuntasovellusten, älyvaatteiden ja älyautojen myötä. Tämä lisää kuitenkin hyökkäyspinta-alaa ja riskiä vihamielisen valtion tiedustelulle ja vaikuttamiselle.

2.3 Riskien hallinta

Korkean riskitason toimittajat ja heikkolaatuiset tai epästandardinmukaiset laitteet on kyettävä tunnistamaan ja rajaamaan pois operatiivisten järjestelmien, tiedustelun järjestelmien, verkon valvonnan ja hallinnan, verkkojen ytimen sekä turvallisuus- ja kiinteistönvalvontajärjestelmien rakentamisesta ja

ylläpidosta. Tämä edellyttää puolustusvoimilta kykyä arvioida toimittajiin ja laitteisiin liittyvä riskitaso ja testata hankittava teknologia ja laitteet, tarvittaessa yhteistoiminnassa muiden viranomaisten ja kumppaneiden kanssa. Lisäksi tämä edellyttää lainsäädäntöön perustuvaa mahdollisuutta rajata korkean riskitason toimittajat ja laitteet pois rakentamisesta ja ylläpidosta.

Puolustusvoimien verkkojen valvonta ja hallinta, mukaan lukien paikalliset omat 5G verkot (mikro-operointi), on kyettävä pitämään omassa hallinnassa. Verkon valvonta ja hallinta on toimittava Suomen maaperällä olevista toimipaikoista, vaikka tietoliikenneyhteydet olisivat tilapäisesti poikki rajojen ulkopuolelle. Myös kumppaneiden ja muiden palvelutoimittajien verkon valvonta ja hallinta tulisi pitää Suomen maaperällä olevissa toimipaikoissa ja niiden on toimittava, vaikka tietoliikenneyhteydet olisivat tilapäisesti poikki valtion rajojen ulkopuolelle.

Puolustusvoimilla on oltava toimivaltuudet ja kyky valvoa omaa kyberympäristöä kumppaneiden ja muiden palvelutoimittajien verkkojen rajapintoihin asti. Kumppaneilla ja muilla palveluntoimittajilla on oltava kyky valvoa omat verkkonsa ja osallistuttava aktiivisesti kyberpoikkeamien hallintaan yhteistoiminnassa puolustusvoimien kanssa.

Puolustusvoimilla ja kumppaneilla on oltava kyky testata, rakentaa ja ylläpitää luotettavasti ratkaisut, joilla erotellaan verkkojen kriittiset osat, tehtäväkriittiset ja korkean suojaustason järjestelmät tietoturvallisesti. Tarvittaessa puolustusvoimien ja kumppaneiden verkkojen on nopeasti ja yksinkertaisesti mahdollistettava haitallisten ulkoyhteyksien valikoiva katkaisu.

Päivittäisen toiminnan mobiiliratkaisujen (IoT, 5G) hallinta edellyttää erityisesti toimintatapojen sääntelyä puolustusvoimien sisäisillä normeilla. Mobiiliratkaisuille on oltava varamenetelmiä niin, ettei toiminta lamaudu laajoista palveluiden tai sähkönjakelun häiriöistä. Toiminnassa on kyettävä erottelemaan korkean suojaustason ympäristöt ja tiedot päivittäisen toiminnan IoT:sta.

3 Arvio hallituksen esityksestä eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi

Kokonaisuutena hallituksen esitys huomioi hyvin kansallisen turvallisuuden ja maanpuolustuksen tarpeet. Seuraavassa on tiivistelmä maanpuolustuksen kannalta keskeisistä lain kohdista.

(11§, 16§, 17§ ja 18§) Toimilupien säätelyssä on arvioitu hyvin mahdolliset riskit ja se mahdollistaa toimijoiden riskiprofiloinnin sekä korkeariskisten laitevalmistajien ja –toimittajien poissulkeminen tai näiden toimijoiden laitteiden käytön rajoittaminen yhteiskunnan elintärkeän toiminnan, kansallisen turvallisuuden ja maanpuolustuksen kannalta keskeisistä kohteista.

(39§) Puolustusvoimien tai Rajavartiolaitoksen radiolähettimien ja –järjestelmien kannalta ehdotettu radiolupamenettely voidaan arvioida toimivaksi eikä se muuttaisi tilannetta nykyisestä tai velvoittaisi hakemaan taajuuksien käyttöoikeuksia nykyistä laajemmin. Ehdotettu muutos ei aiheuttaisi myöskään muutoksia puolustusvoimien ja Rajavartiolaitoksen radiolähettimien tietoturvallisuuteen, mikä mahdollistaa salassa pidettävien järjestelmätietojen suojaamisen.

(229§) Esitys huomioi maanpuolustuksen tarpeet sisällyttäessään maanpuolustuksen yleiseen turvallisuuteen ja mahdollistaessaan tarvittaessa rajoituksia pienalueen langattomina liityntäpisteinä toimivien matkaviestinverkon tukiasemien sijoittamiseen.

(244§) Liikenne- ja viestintäviraston oikeus antaa määräyksiä viestintäpalveluiden laadusta, varmentamisesta, suojaamisesta, tietoturvallisuudesta, seurannasta ja verkonhallinnasta tukee hyvin maanpuolustuksen tarpeita. Tällä varmistetaan puolustusvoimien käyttämien muiden operaattoreiden verkkojen turvallisuus.

(244a§) Verkkolaitteiden sääntely verkon kriittisissä osissa huomioi kansallisen turvallisuuden ja maanpuolustuksen tarpeet. Kriittiset osat ovat määritelty riittävän laajasti. Sääntely mahdollistaa arvion mukaan riittävän viranomaisvalvonnan, jolla pystyttäisiin puuttumaan viestintäverkkojen kriittisissä osissa oleviin kansallista turvallisuutta tai maanpuolustusta vaarantaviin viestintäverkkolaitteisiin.

(244b§) Valtioneuvoston asettama verkkoturvallisuuden neuvottelukunta mahdollistaa hyvin teknologian kehittymiseen liittyvien muutosten, epävarmuustekijöiden ja riskien arvioinnin ja torjumisen kansallisen turvallisuuden ja maanpuolustuksen näkökulmasta.

(275§) Vaatimus viipymättömästä häiriöilmoittamisesta Liikenne- ja viestintävirastolle mahdollistaa nopean tilannekuvan välittymisen puolustusvoimille. Tämä mahdollistaa palveluiden toimivuuteen, tietoturvallisuuteen ja kyberturvallisuuteen liittyviin riskeihin vastaamisen ja näin tukee maanpuolustusta.

(283§) Vaatimus huolehtia Valmiuslain 60§ mukaisesti viestintäverkon kriittisen järjestelmän Suomeen palauttamisen edellytyksistä tukee hyvin maanpuolustusta. Kriittiset viestintäverkon järjestelmät, ohjaus, ylläpito ja hallinta sekä viipymättömyys ovat keskeisiä ja hyviä vaatimuksia.

Suunnittelusektorin johtaja
Everstiluutnantti Ilkka Vaara