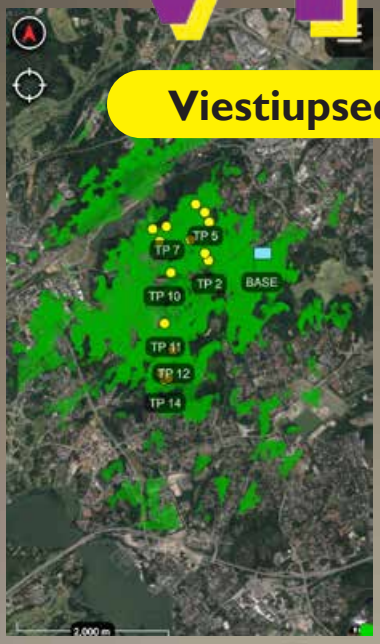
Viestimies

Viestiupseeriyhdistyksen julkaisu 78. vsk Numero 4 Talvi 2023



www.viestiupseeriyhdistys.fi

www.combitech.fi

Viestimies-lehti

Päätoimittaja
Pasi Puhakka
p 050 5290003
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Hanna Liitola
p 040 5930675
henkilotoimittaja@viestiupseeriyhdistys.fi

Toiminnanjohtaja
Harri Reini
p 040 514 2497
toiminnanjohtaja@viestiupseeriyhdistys.fi

Toimituskunta
Vähätiitto Jarmo (pj)
Blomqvist Reima
Holma Harri
Hyvärinen Pertti
Isomäki Pekka
Mikkonen Mauri
Nyqvist Antti
Suokko Harri
Tunkkari Antti
Wirman Kari
Yli-Äyhö Janne

Toimituksen osoite:
Päivölänrinne 7 A 1
04220 Kerava

www.viestiupseeriyhdistys.fi/viestimies
Pankkitili FI21 5780 5520 0177 44
Vuosikerta 35 €

Tilaukset ja osoitteenmuutokset
Harri Reini
p 040 514 2497
toiminnanjohtaja@viestiupseeriyhdistys.fi

Ilmoitusmyynti
Juha Halminen
p. 050 59 22722
juha.halminen@mediaosasto.fi

Painopaikka
Newprint Oy, Raisio
p 010 231 2600

ISSN 0357-2153

Kansikuva.

Tässä numerossa

Seuraavan numeron aineistopäivä on 26.1.2024. Lehti ilmestyy viikolla 10.

Uusi normaali

Vuosi 2023 on viime metreillään ja paljon ehti kalenterivuoden aikana tapahtua Suomelle, Euroopalle ja globaalille yhteisölle ennen kokemattomia asioita. Suomi osana pohjoista ulottuvuutta, Eurooppaa ja trans-atlanttista yhteisöä on saanut kokea sekä yhteenkuuluvuuden hyvät että huonot puolet. Vuoden aikana tapahtunut Nato-liittoutuminen lienee ollut jokaista suomalaista ainakin jollakin tasolla keskusteluttanut merkkitapaus. Liittymisen aikaansaamat seurannaisvaikutukset ovat moninaiset ja kokonaisuus on vasta hahmottumassa. Kaiken positiivisen tekemisen mukanaan tuoma on kuitenkin saanut varjoja ylleen viimeisimpien kehityskulkujen myötä.

Monimuotovaikuttaminen – olkoonkin sitten tahallisesti tai tahattomasti aiheutettua – on noussut vääjäämättä osaksi turvallisuusympäristömme nykytilaa. Nykytilasta johtuen Tasavallan presidentin toistamat toteamukset liittoutumisen riskienarvioinnista tulee ottaa vakavasti. Ylipäällikön pitkin syksyä esittämät kehotukset ”suomalaisille varautua kaikenlaisiin ilkeyksiin” ohjatkoon ajatuksiamme myös johtamisjärjestelmäalalla.

Kehotuksessa on velvoittava sävy kaikille viranomaistoimijoille sekä toimintaansa vakavasti suhtautuville organisaatioille. Velvoite on otettava huomioon nyt ja tulevaisuudessa, sillä ainoa pysyvä olotila turvallisuusympäristössämme on jatkuva muutos. Muutos taas on hallittava jatkuvalla riskienarvioinnilla. Osoituksena siitä, miten riskienarvioinnista huolimatta turvallisuusuhkat voivat joskus yllättää oli johtamisjärjestelmäalaan läheisesti vaikuttanut Balticconnector kaasuputken ja Elisa valokaapelin -casesta syntynyt turvallisuuspoikkeama.

Onneksemme kyse ei ole vain pelkästä uhkakuvien lisääntymisestä pohjoisella alueella. Ruotsille pikkuhiljaa avautuva Nato-jäsenyys tulee ottaa mahdollisuutena vaikuttaa kokonaisturvallisuuteemme positiivisena lisänä. Edellä mainitun kaltaisten tietoliikenneinfrastruktuuriin vaikuttamisten vastatoimia voitanee yhä tiivistyvässä yhteistyössä kehittää Euroopan yhteisön, Nato-kumppaneiden, tulevan Nato-kumppanimme Ruotsin sekä muun bilateraalisen yhteistyön kautta. Yhdessä tekemisessä todella on voimaa ja taloudellisia hyötynäkökulmia.

Edellä mainitsemani ylipäällikön kehotus toimii suorana ohjenuorana myös Puolustusvoimien johtamisjärjestelmäalalle. Entistä tarkemmin, kovan turvallisuuden viranomaisena, Puolustusvoimien johtamisjärjestelmäalan on tutkailtava mahdolliset tulevaisuuskuvat ja varauduttava ennakoimaan ja torjumaan uhkat johtamisjärjestelmiämme vastaan. Jälleen kerran läntisen yhteisön ja Naton voimavarojen hyödyntäminen avaavat uudella tavalla mahdollisuuksia kehittää Puolustusvoimien johtamisjärjestelmäalan toimintaa ja teknistä suorituskykyä. Tätä ajatusta vasten ylipäällikön kehotus kannattaa kääntää positiiviseen tulokulmaan johtamisjärjestelmien ja johtamisen tuen järjestämisen osalta. Asetelman voisi muotoilla vaikkapa seuraavasti ”koettakaa kuvitella kaikki mahdolliset hyvyydet hyödynnettäväksi”.

Nuo kaikki hyödynnettävät hyvyydet koko laajuudessaan tulevat pitämään sisällään yhä enenevissä määrin kaupallisten toimijoiden ratkaisuja, teknologioita ja yhteistyötä lisäten diversiteettiä johtamisjärjestelmäalan ratkaisukentässä. Perinteisistä ratkaisumalleista poikkeavien, innovatiivisten ratkaisuiden etsiminen, huomioiminen ja arvostaminen voivat avata aivan uudenlaisia kehityskulkuja monimutkaisten haasteiden ja riskien hallitsemiseksi. Mahdollisesti monimutkaistuvat ja kerrostuvat ratkaisut edellyttävät varmasti uudenlaista osaamista, mutta samalla ehkäisevät yksittäisten vaikutuskeinojen lamauttavaa vaikusta kohteena olevalle johtamisen suorituskyvylle.

Tämän kertaiseen lehteen on koostettu muutamia innovatiivisia esimerkkejä eri teknologioiden hyödynnettävyydestä sotilaallisessa toimintaympäristössä. Kirjoittajat ovat oman alansa huippuosaajia ja tuovat esiin uusien teknologioiden hyödyntämismahdollisuuksia taktisella ja operatiivisella sekä osin myös strategisella tasolla joukkojen tilannetietoisuuden lisäämiseksi ja johtamisen työvälineinä. Nousevien teknologioiden marssi on käynnissä. Varmistakaamme Puolustusjärjestelmän sisältä käsin, että meillä on innovatiiviseen ajatteluun positiivinen ja kannustava ote johtamisen ketjussamme ylhäältä alas saakka. Kannustamalla ja positiivisesti ajattelemalla saamme hyödynnettyä kaikki ne hyvyydet, joita ympärillämme on saavutettavissa. Mutta huomatkaa, että pelkkä sisältä käsin toteutettu innovointi ei tänä päivänä riitä, ja vain yhdessä tekemällä saavutetaan kustannustehokas malli suorituskykyjen rakentamiseksi. Verkottuminen yhteisöjen, yritysten, tutkimusmaailman ja lukemattomien muiden toimijoiden kanssa kantaa innovoinnissa sataprosenttisen varmasti pidemmälle kuin omassa pienessä nurkkakunnassa pohdiskelu.

Muutos lienee sana, joka kuvaa jatkuvuutta, uutta normaalia, globaalia, Eurooppalaista sekä Suomessa vallitsevaa kokonaisturvallisuuden tilannetta. Muutos kuvaa myös Viestimies -lehden toimituksen tilaa päätoimittajan vaihtuessa uuteen vuoteen käännyttäessä. Kiitän omalta osaltani toimituskuntaa, Viestiupseeriyhdistystä, yritys- ja tutkimusmaailman verkostoja, asialleen omistautuneita kirjoittajia, lukijakuntaamme sekä kaikkia toimintaan osallistuneita verkostoja ja henkilöitä lehtemme eteen tehdystä erinomaisesta työstä. Samalla haluan toivottaa uuden päätoimittaja Kimmo Kaipaisen tervetulleeksi katkeamattomaan ketjuumme sekä onnea ja menestystä sinulle Kimmo perinteikkään aselajilehtemme toimittamiseen.

Näillä sanoilla toivotan rauhaisaa joulunalusaikaa lehtemme lukijoille ja yhteistyökumppaneille sekä uutta normaalia vuodelle 2024,

Päätoimittaja

Pasi Puhakka

WE ARMOR IT.™

Letters. Words. Codes. Coordinates. Orders.

Every moment vital information is transmitted around us and at risk. Enter MilDef. We create rugged IT solutions for the harshest conditions and most challenging environments, which prevent your information from being interrupted, intercepted or disrupted.

Put simply; we armor your IT, when and where the stakes are the highest.

MILDEF

Kohti 2030-lukua

Kulunut vuosi on ollut tuntemamme suomalaisen historian valossa poikkeuksellinen. Venäjän hyökkäyssota Ukrainassa, Suomen liittyminen Natoon, Lähi-Idän tilanteen eskaloituminen, turvallisuustilanteen muuttuminen Ruotsissa, yhteiskuntaamme vaikuttaneet merikaapelien katkeamiset, kaasuputken vaurioituminen, runsaat palvelunestohyökkäykset kalasteluviesteineen ja informaatioympäristössä tapahtuva jatkuva haastaminen muutamia toimia mainitakseni. Näin tarkasteltuna kaikki maanpuolustuksen eri sektoreilla toimineet ovat uskoakseni saaneet osansa ja tehdyllä varautumisella ja valmistautumisella on ollut merkitystä.

Merkityksellisyys korostuu monessakin mielessä. Yksi ehkäpä herättelevin tapa on tarkastella Venäjä hyökkäyssodan vaikutuksia Ukrainassa. Moni asia on napakan operaatioturvallisuuden johdosta vielä karkeiden arvioiden varassa. Ukrainalaiseen viestintään nojautuen voidaan kuitenkin todeta, että pääosa Venäjän ohjusiskuista on kohdistettu kriittiseen infraan ja teleoperaattoreiden kohteisiin ja pieni osa suoraan asevoimien kohteisiin. Venäjä kykenee myös koordinoimaan offensiivisia kyberoperaatioita ohjusiskujen kanssa. Näillä toimilla vaikutetaan yhtäältä yhteiskunnan tarvitsemaan jokapäiväiseen energiatarpeeseen, tiedonkulkuun ja muihin perusrakenteisiin sekä toisaalta maanpuolustuksen viimeiseen puolustuslinjaan, maanpuolustustahtoon. Asevoimiin kohdistuva vaikutus on silti huomattava, vaikka vaikutus olisi välillinen. Keskinäisriippuvuuden ollessa erittäin merkittävää, tarvitsemme yhteistyötä ja riittävää kommunikaatiota sekä toisten tukemista resurssiemme rajoissa.

Edellä kuvattuun vastatessa on Puolustusvoimilla ja sen kanssa suorituskykyä rakentavalla ja valmiutta ylläpitävällä johtamisjärjestelmäalan verkostolla oltava riittävä kyky turvallisuusympäristön muutoksiin. Niihin vastataksemme pyrimme Puolustusvoimissa saamaan johtamisjärjestelmäalan kehityksen nopeammaksi siten, että meillä olisi samanaikainen kyky toimeenpanna lukuisia välittömästi, kvartaalissa ja vuodessa-kahdessa toteutettavia muutosprojekteja ja hankkeita. Toiminnan tehostaminen on toinen päätavoite. Sitä tuetaan esimerkiksi konkreettisten suorituskykytavoitteiden seurannalla ja sitä kautta

toteutettavalla johtamisella, hallinto ja muiden marginaalien keventämisellä, puristamalla läpimenoaikoja lyhyemmäksi, asiakaspalvelun kehittämisellä ja monilla muilla toimenpiteillä. Kehitykselle ja muulle toiminnalle asetettavien tavoteiden saavuttaminen perustuu kykyyn kehittää toimintatapaa, organisaatiota ja organisaatiokulttuuria sekä erityisesti varmistaa muutoksen toteuttamisessa ja tavoitteiden saavuttamisessa tarvittava osaaminen. Osaamisen kehittämistä ja uutta osaamista tarvitaan jo pelkästään toiminnan ja teknologian muutoksesta johtuen.

Kaikilla edellä mainituilla toimilla on kyettävä tukemaan Puolustusvoimien toimintaa ja erityisesti operatiivisia tehtäviä nykyistä paremmin. Muutamia jo pidempään ohjenuorana olleita perustavoitteita ovat ensinnäkin kyvykkyys, jossa vastustajan toimintaa voidaan ennakoida sensorijärjestelmien informaatioon tukeutuen ja maali voidaan havaita sekä identifioida useammalla sensorilla lavetista riippumatta. Toiseksi tulitehtävä voidaan koordinoida kaikkien kantaman piirissä olevien asejärjestelmien kesken ja vaikutuksen arviointi kyetään tekemään useamman havainnon perusteella. Lisäksi automatisoitu maalittamis- ja tulenkäyttöprosessi toimii erittäin pienellä viipeellä ja samalla operatiivistaktisen, multi-domain tilannekuvan ja erityisesti maalitilannekuvan viive on mahdollisimman pieni.

Viiteryhmämaihin verrattuna meidän ei tarvitse hävetä, päinvastoin. Meillä on osaavaa henkilöstöä, hyvässä kunnossa olevat asevoimat ja erinomainen kansallinen narratiivi, mutta nykyinen toiminnan taso vaatii silti kehittymistä kohti 2030-lukua. Osaamista haastavien tavoitteiden saavuttaminen edellyttää Puolustusvoimien, yritysten, asevelvollisten ja vapaaehtoisten yhteistyön edelleen kehittämistä, jonka yhtenä toimena tulisi rakentaa kotimaista sovelluskehityksen verkostoa ja ottaa suorituskykyloikka ohjelmistopohjaisuuden ja datan käytön mahdollistamaan suorituskykyyn.

Kiitän kaikkia Viestimieslehden lukijoita ja laajaa verkostoamme kuluneesta vuodesta. Marssi jatkuu ja toivotan sitkeyttä sekä turvallista uutta vuotta 2024.

Johtamisjärjestelmäpäällikkö

Prikaatikenraali

Jarmo Vähätiitto

Patria

Kun kaiken on pakko toimia.

Patria tarjoaa huippuluokan suorituskykyä

Patria on moderni ja kansainvälinen puolustus- ja teknologiayritys, jonka kokemus ulottuu yli 100 vuoden päähän. Järkevästi käytetyt resurssit, innovatiiviset ratkaisut ja älykkäät järjestelmät varmistavat, että voimme tarjota asiakkaillemme suorituskykyä, johon voi luottaa kaikissa olosuhteissa. Patrian tarjooma on NATO-yhteensopivaa.

Patrian laaja tarjooma on jaettu kolmeen päähaaraan, jotka ovat **Through Life Capability**, **Protected Mobility and Defence Systems** ja **Battlefield and Critical Systems**.

Toimimme asiakkaidemme kanssa yhteistyössä tuotteidemme koko elinkaaren ajan, jotta tuotteiden hyöty saadaan varmasti maksimoitua. Rakennamme kumppanuuksia, jotka toimivat myös kriittisissä olosuhteissa.

Tatu Tahkokallio on koulutukseltaan sähkötekniikan DI ja toimii Maavoimien tutkimuskeskuksen johtavana tutkijana virkapaikkanaan Hamina.

TEKSTI: TATU TAHKOKALLIO, ERIKOISTUTKIJA, MAAVOIMIEN TUTKIMUSKESKUS

Meshtastic-monihyppyverkko – mahdollisuus paikallispuolustukselle?

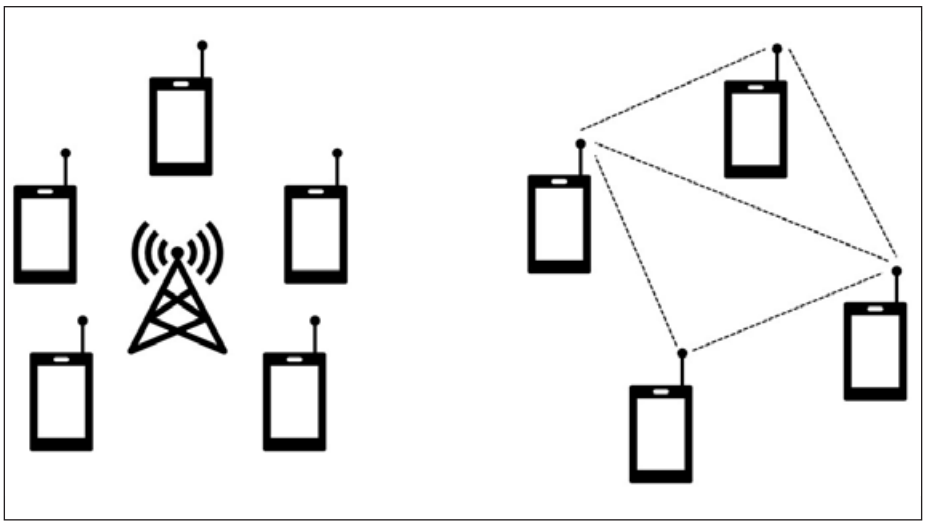
Avoin lähdekoodi ja yhteisöllinen ohjelmistokehitys käynnistivät 1990-luvulla liikkeen, joka tuottaa jatkuvasti uusia ohjelmistoinnovaatioita siviilitarpeisiin. Eräs tällainen on Meshtastic-monihyppyverkko, jota kehitetään avoimen lähdekoodin periaattein ja joka perustuu LoRa-radioihin. Tämä artikkeli tarkastelee Meshtastic-verkkoon liittyvää tekniikkaa ja verkon soveltuvuutta paikallispuolustuksen tarpeisiin. Havainnot perustuvat kesän ja alkusyksyn 2023 aikana kirjoittajan harrastuspohjalta tekemiin kenttäkokeisiin.

LoRa ja LoRaWAN

LoRa eli Long Range on pitkän kantaman hajaspektrimodulointiin perustuva radioteknologia. Teknologia määrittelee langattomassa LPWAN-tiedonsiirrossa (Low Power Wide Area Network) käytettävän datan modulointitekniikan ja pakettirakenteet. LoRa-teknologian juuret ovat Ranskassa, jossa se kehitettiin alun perin esineiden Internetiä varten (IoT, Internet of Things). Teknologian alkuperäisiä suunnittelutavoitteita olivat kyky toimia pattereiden varassa, alhainen virrankulutus ja maantieteellinen kattavuus. Nykyään LoRa-radiopiirejä kehittää ja valmistaa Semtech Corporation, joka osti teknologiaan liittyvät immateriaalioikeudet vuonna 2012 ja patentoi ne vuonna 2014.

Vuonna 2015 perustettiin komponentti ja laitevalmistajien LoRa-allianssi, jonka päätehtävänä on standardoida ja edistää LoRaWAN päätelaitteiden ja verkkoratkaisujen käyttöönottoa ja leviämistä. LoRaWAN eroaa monihyppyverkoista siten, että se perustuu tähtitopologiaan, jossa päätelaitteet kommunikoivat keskenään yhdyskäytävän (tukiaseman) ja verkkopalvelimen kautta. Monihyppyeli MESH-verkoissa päätelaitteita kutsutaan solmuiksi (engl. nodes) ja tiedonsiirto näiden välillä tapahtuu suoraan ilman erillisiä tukiasemia.

LoRa-teknologiaa hyödyntävät radiot toimivat maailmanlaajuisesti ns. lupavapailla ISM-taajuuksilla (Industrial, Scientific, Medical). Euroopassa LoRa-verkot käyttävät taajuuksia 433 MHz ja 868 MHz. ISM-taajuuksilla käytettävät kanavajakoperusteet vaihtelevat maittain. Euroopassa käytetään 125 kHz ja 250 kHz levyisiä kanavia. Kapeiden taajuuskaistojen lisäksi rajoittavana tekijänä on ns. toimintasuhde (engl. duty cycle), joka määrittää yhden tunnin aikana käytettävän enimmäislähetysajan. Euroopassa toimintasuhteeksi on määrätty ≤10%, jolloin lähetin saa olla ”ilmassa” korkeintaan 6 minuuttia tunnissa. Toimintasuhteen noudattamista valvoo radiotaajuuksista vastaava regulaattori, Suomessa Traficom sekä käytetty LoRa-ohjelmisto. Meshtasticin tapauksessa käyttäjä voi halutessaan kytkeä toimintasuhderajoitteen pois päältä.



LoRaWAN- tähtiverkko vs. monihyppyverkko.

Meshtastic

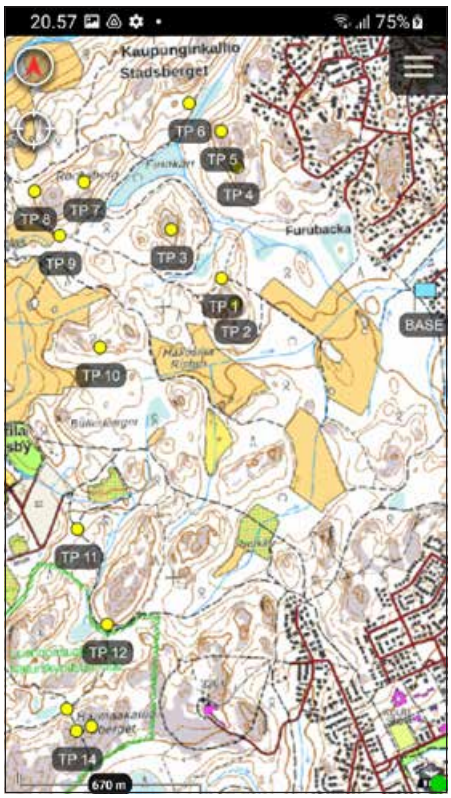
Meshtastic-projekti käynnistyi vuonna 2020 pienen kehittäjäyhteisön siivittämänä. Harrasteprojektin tavoitteena oli luoda halpojen LoRa-radioiden avulla pitkät yhteysvälit mahdollistava käyttäjien myötä laajeneva verkko. Toteutettavan ratkaisun tuli mahdollistaa mm. käyttäjien sijaintitiedon ja etäisyyden välittämisen, salattu pikaviestinnän keskustelukanavilla ja toiselle solulle tarkoitetun viestien edelleen lähetyksen. Ohjelmiston kehittäminen ja lisensointi päätettiin toteuttaa avoimen lähdekoodin periaatteita noudattaen.

Nykyään Meshtastic on pitkälle tuotteistettu ja sillä on maailmanlaajuinen ja aktiivinen käyttäjä- ja kehittäjäyhteisö. Ratkaisu on helppo ottaa käyttöön www.meshtastic.org sivustolta löytyvän ohjeistuksen avulla. Ohjelmoinnista kiinnostuneille Meshtastic-lähdekoodit löytyvät GitHub-verkkopalvelusta (www.github.com/meshtastic), josta löytyy LoRa-firmware-ohjelmistojen lisäksi ratkaisua tukevat mobiilisovellukset ja laajennusosat. Kehittäjien ja käyttäjien välisenä keskustelufoorumina toimii Discord-yhteisöpalvelu. Yhteisöllinen toimintamalli näytti kyntensä kesällä, kun allekirjoittanut tarvitsi erääseen ohjelmiston lisäosaan pikaisesti korjausta. Usealla eri aikavyöhykkeillä toimiva kehittäjäyhteisö koodasi ja testasi vaihtoehtoisen ohjelmistokomponentin erittäin nopeasti ja ammattitaitoisesti.

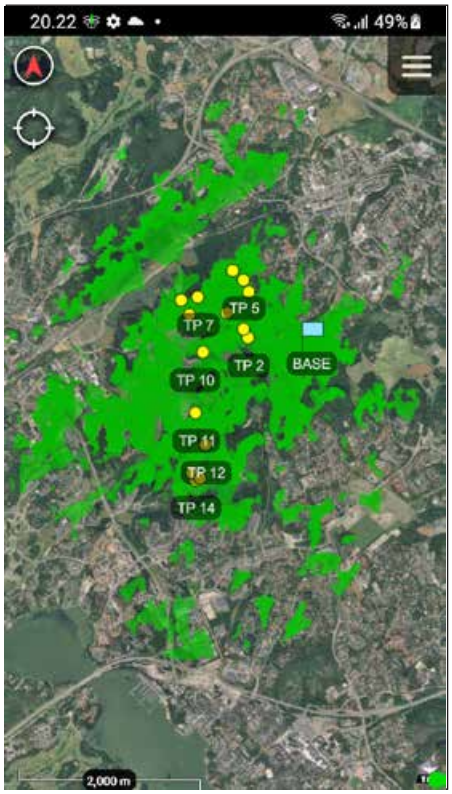
Kenttäkoe

Kenttäkokeen alkuperäisenä ja ensisijaisena tarkoituksena oli testata kahdella eri taajuudella toimivien LoRa-radioiden kuuluvuutta maastossa. Kenttätestit tehtiin kahtena eri viikonloppuna heinä-syyskuun välisenä aikana, joista ensimmäisessä oli käytössä vain korkeamman taajuuden radiot. Tässä esitetyt tulokset perustuvat lähinnä jälkimmäisen viikonlopun testeihin.

Testausalueena toimi Espoon Kaupunginkallion lähimaasto. Alueelta valittiin viisitoista testauspistettä ja lähtöpisteeseen sijoitettiin tukikohtaradio, jota vasten testit suoritettiin. Testipisteet kierrettiin numerojärjestyksessä. Testipisteisiin ei sijoitettu kiinteitä radioita, vaan testejä tehtiin liikkuvalla tilaajalla. Poikkeuksena oli testipiste kolme, johon jätettiin erillinen tukiasemaradio. Paikka valikoitui sillä perusteella, että aiemmat yhteyskokeilut ko. sijainnin länsi–luoteispuoleisesta maastosta olivat järjestäen epäonnistuneet.



Kenttäkoealue, testipisteet (TP 1 – 15) ja kiinteä tukikohta (BASE)



Monihyppyverkon teoreettinen kokonaispeitto.

Testilaitteisto

Yksittäisen Meshtastic-päätelaitteen ytimenä on elektroniikkapiiri, joka sisältää mikroprosessorin (ESP32 tai nRF52), LoRa-radiokomponentin, lyhyen kantaman Wifi- ja/tai Bluetooth-radion ja mahdollisen GPS-vastaanottimen. Päätelaitteeseen tarvitaan myös akku, antenni ja mielellään jonkinlainen kotelointiratkaisu ja näyttö. Valmiita piirejä voi ostaa suoraan Internetistä, mutta mikään ei estä ostamasta komponentteja erikseen ja rakentamasta piiriä itse. Päätelaitteen ohjelmistoksi ladataan Meshtastic-firmware.

Testilaitteisto koostui kiinalaisista LiLyGo LoRa-radioista ja näihin erikseen hankituista antenneista. Radiot olivat mallia T-Echo (868 MHz) ja T-Beam (433 MHz), joille valmistaja ilmoittaa maksimilähetystehoiksi +22 dBm ja +14 dBm vastaavasti. T-Echo radioita oli käytössä kaksi kappaletta ja T-Beam malleja kolme. Antenneina käytettiin ulkokäyttöön suunniteltuja taipuisia Taoglas Meteor ympärisäteileviä monopoliantenneja. Antennien maksimivahvistukset keskitaajuudella ovat valmistajan mukaan 2,82 dBi (868 MHz) ja 0,46 dBi (433 MHz). T-Echo päätelaitteet ovat valmiiksi tehtaalla koteloituja mutta T-Beam -radiot piti itse koteloida kirjaston 3D-tulostimen avulla.

Kenttäkokeessa käytettiin MediumFast -kanavaprofiilia. Profiili on Meshtastic-projektin määrittelemä ja suunniteltu keskipitkille yhteysväleillä nopeaa tiedonsiirtoa varten. Tämän päivän Internet-surffaajalle LoRa-verkon ”nopeus” voi tosin olla pienoinen yllätys. Käytetyn kanavaprofiilin 250 kHz levyisellä kanavalla saavutettava maksiminopeus on 2,2 kbs, kun linkkibudjetti on 143 dB (oletuksena 17 dBm lähetysteho ja 0 dBm antennivahvistus). Teoreettinen maksiminopeus LoRa-radioille on Meshtastic-sivuston mukaan 500 kHz kanavaleveydellä jopa 37,50 kbps!

Tukikohdan kiinteä ja testaajan liikkuva radio olivat molemmat liitetty Bluetooth-yhteydellä Android-älypuhelimiin, joihin oli asennettu Meshtastic-päätelaitesovellus. Sovelluksen avulla tehtiin varsinaiset yhteyskokeilut siten, että kustakin testipisteestä lähetettiin LoRa-verkkoon pikaviesti. Viesti oli tekstisisältöinen, esim. ”T433-TP-11”, jossa välittyi käytetty taajuus/radio ja lähettävän testipisteen numero. Testin onnistuminen voitiin todentaa lähetyspäässä pian lähettämisen jälkeen, koska Meshtastic-sovellus ilmoittaa graafisen ikonin avulla viestin perillemenosta tai sen epäonnistumisesta.

LoRa-radioiden peitto

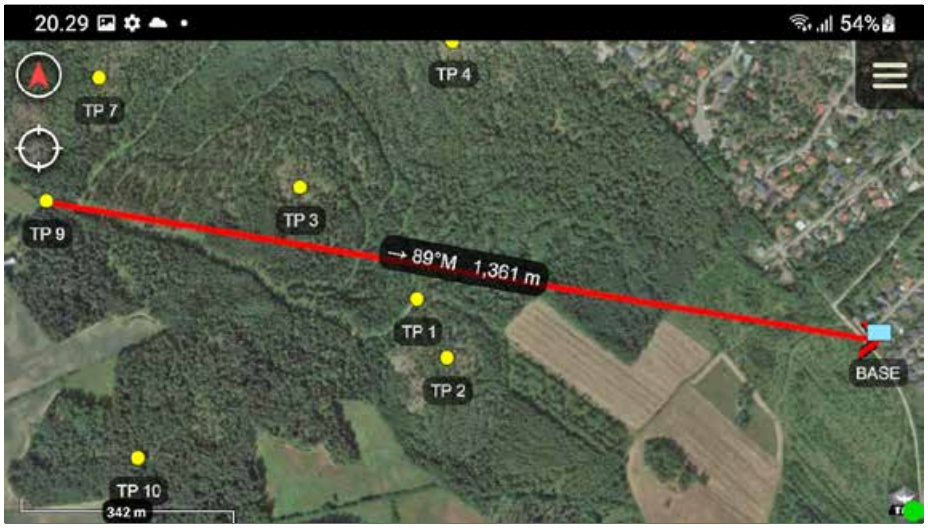
Testialueen maasto vaihteli paljon. Korkeimmalla sijaitsi testipiste 8, joka oli GPS-tietojen mukaan 51,7 metriä meriveden keskipinnan yläpuolella. Korkeusero matalimman (TP 11) ja korkeimman testipisteen välillä oli peräti 32,6 metriä. Muilta osin maasto sisälsi varsin laajoja ja paikoitellen jyrkkiäkin kallioita, havumetsää ja peltoaukeita.

LoRa-radioiden kuuluvuutta ennustettiin Soothsayer-työkalun ilmaisversiolla, joka mahdollisti testipistekohtaisten peittoalueiden mallintamisen. Peittoalueet laskettiin GPU-laskentaa hyödyntävällä Line-of-Sight (LOS) radiomallilla, jossa radion antenni oletettiin 2 metrin korkeuteen. Ilmaisversio laski peittomallit CloudRF-pilvipalvelussa, joka palautti peittoaluekuvat 2 km säderajoitteen kera. Oletettavat kuuluvuus- ja peittoalueet työkalu maalasi karttaan vihreinä.

Sijoittamalla yksittäisten testipisteiden peittoaluekuvat päällekkäin oli mahdollista tarkastella teoreettista kokonaispeittoaluetta monihyppyverkolle, jonka kuhunkin testipisteeseen olisi sijoitettu kiinteä LoRa-radio.

Testitulokset

Testipisteiden ja tukikohdan väliset yhteysvälit erosivat paljonkin toisistaan. Toisissa maa oli kalliota, toisissa kosteikkoa ja/tai peltoa. Paikoitellen puusto oli harvaa tai harvennettua ja paikoitellen



Yhteysväli TP 9 – tukikohta (BASE).

Peittoalue pisteestä TP 9.

hoitamatonta havumetsää. Oletettavissa oli hyvinkin erilaisia testituloksia.

Yksittäisistä yhteysväleistä saatavia havaintoja saattoi arvuutella jo ennalta, koska käytössä oli kesällä tehtyjen 868 MHz testien tulokset sekä kullekin testipisteelle erikseen luotu peittoaluemalli. Lopulliset testitulokset vahvistivat ennakkokäsityksiä onnistumisen todennäköisyyksistä. Yleensä yhteys toimi, jos peittoaluemalli ennusti jännevälille vihreää kaistaletta tai jos vastaanottoalue ja sen välitön läheisyys lähettimen suuntaan olivat vihreitä. Poikkeuksen muodostivat pisteet TP1, TP3 ja TP4.

Yhteyskokeilut pisteestä TP1 epäonnistuivat molemmilla taajuuksilla, vaikka kyseinen piste oli vain 748 metrin päässä tukikohdasta. Epäonnistumisen syytä voi vain arvailla, mutta yhtenä tekijänä saattoi olla jännevälillä sijainnut tiheähkö havumetsä. Yhteyskokeilut pisteistä TP3 ja TP4 vaikuttivat alun alkaen haastavilta. Ne kuitenkin onnistuivat 433 MHz taajuudella mutta eivät 868 MHz taajuudella. Aiemmin kesällä tehty onnistunut yhteyskoe pisteestä neljä osoitti myös, miten antennivalinnalla voi olla merkitystä kuuluvuuteen. Tällöin käytössä oli dipoliantenni nyt käytetyn monopoliantennin sijasta.

Pisteille TP5 ja TP6 sekä TP9 – TP11 luotujen peittoaluemallien perusteella oli oletettavissa, etteivät suorat yhteydet näistä tulisi onnistumaan. Tämä tuli toteen näytetyksi 868 MHz taajuudella,

jolla ko. pisteistä tehdyt yhteyskokeilut epäonnistuivat kaikki. Koska peittokuvien mukaan kaikista pisteistä on yhteydet pisteeseen TP3, oli oletettavissa, että yhteyskokeilut 433 MHz taajuudella voisivat onnistua yhden hypyn avulla. Näin myös kävi ja tilannetta havainnollistaa hyvin oheiset peittoaluekuvat pisteille TP9 ja TP3. Yhdistämällä peittoaluekuvat voi kuvitella lähes yhtenäisen peittoalueen TP9 – tukikohta (BASE) väliselle jännevälille.

Muut epäonnistuneet yhteyskokeilut noudattivat poikkeuksetta joko aiemmin tehtyjä havaintoja tai peittoaluemalleja.

Peittoalue pisteestä TP 3.

Rajapyykki, 2 km

Pisimmät onnistuneet yhteydet kenttäkoealueen haasteellisessa maastossa saatiin testipisteestä 15, jonka etäisyys tukikohtaan oli tasan 2 km linnuntietä. Testipiste sijaitsi korkealla kallion laella noin 47 metrin korkeudessa ja jännevälille sijoittui yhtä lailla kalliota, metsää kuin peltoaukeitakin. Yhteyskokeilut tästä pisteestä onnistuivat molemmilla taajuuksilla.

Testipisteen osalta oli myös merkille pantavaa, ettei sen välittömässä läheisyydessä sijaitsevat yleisradioantennimastot ja niihin kiinnitetyt eri taajuusalueilla toimivat antenniryhmät tuntuneet häiritsevän LoRa-yhteyksiä lainkaan. Näin siitäkin huolimatta, että ko. mastoissa sijaitsee tiettävästi myös Digitan hallinnoiman LoRaWAN-verkon antenneja.

Monihyppyverkko paikallispuolustuksessa

Soveltuuko Meshtastic-ohjelmistolla ja LoRa-radioilla varustettu monihyppyverkko paikallispuolustukseen? Kysymys on mielenkiintoinen, eikä vähiten siksi, että yhden LoRa-radion kokonaiskustannus jää alle sadan euron ja toisaalta siksi, että radiot voidaan liittää arjen välineillä toimivan johtamisjärjestelmän tiedonsiirtoverkoksi.

Paikallispuolustuksen tärkeimmäksi johtamispalveluksi on useassa yhteydessä todettu puhe. Valitettavasti testatuilla alle GHz-taajuuksilla toimivilla radiolla IP-pohjaisen puhepalvelun toteutus on käytännössä mahdotonta. Lähitulevaisuudessa uudet 2,4 GHz LoRa-radiot voivat silti muuttaa tilannetta. Korkeampi taajuusalue ja laajempi tiedonsiirtokaista tuovat lisää nopeutta, mutta samalla yhteysvälit lyhenevät.

Rajoitteista huolimatta kapeakaistaiset LoRa-radiot soveltuvat mainiosti esimerkiksi tulikomentojen, pikaviestien ja tiedusteluhavaintojen välittämiseen. Siis samoihin käyttötapauksiin, joihin viestimiehet jo aikaa sitten opettelivat käyttämään sanomalaitteita. Erona vanhaan, uudet teknologiat tavallaan modernisoivat sanomaverkkoa, kun radiotiellä sovelletaan häiriöitä kestävää aaltomuotoa ja sanomien monitie-eteneminen mahdollistetaan monihyppyprotokollalla. Lisäetuna on käytännön yhteensopivuus nykyaikaisten sotilasstandardien kanssa. Esimerkiksi Meshtastic-monihyppyverkko voidaan liittää tilannekuvasovellukseen, jolloin verkon kautta voidaan siirtää MIL-STD-6090 mukaisia Cursor-on-Target (CoT) -tilannekuvamerkkejä.

Monen paikallispuolustajan haasteena voi olla laaja vastuualue. Tämä kasvattaa todennäköisyyttä ja tarvetta saarekkeiselle toimintakyvylle. Monihyppyverkko tarjoaa joukolle helpon ratkaisun, kun viestiverkkoa ei tarvitse erikseen rakentaa vaan sen automaattiset solmut kulkevat viestimiesten olkapäillä. Lisäksi monihyppyverkon ameebamainen topologia seuraa joukon liikettä ja ylläpitää johtamisyhteyksiä myös tilanteissa, joissa verkkoon kohdistuu muutospaineita. Esimerkiksi yksittäisen solmun sammuminen, katveeseen joutuminen, rikkoutuminen tai tuhoutuminen ei lamaannuta koko verkkoa, koska viestit hakeutuvat vastaanottajilleen useita eri reittejä pitkin.

Paikallisesti operoiva joukko ei ole immuuni riskeille, jotka uhkaavat tietoturvaa ja operaatioturvallisuutta. Kaikki viestiliikenne, jopa peitteinen, tulee tämän vuoksi mahdollisuuksien mukaan aina salata. Meshtastic-protokolla salaa hyötykuorman joko AES 128 tai 256 bittisellä salausavaimella, joka voidaan määrittää jokaiselle Meshtastic-kanavalle erikseen. Koska salausavaimet tallennetaan yksittäisiin solmuihin, LoRa-radion joutuminen vääriin käsiin saa tässäkin verkossa aikaan tietoturvapoikkeaman ja pakottaa vaihtamaan salausavaimia.

Lopuksi

Kenttäkoe oli monella tapaa innostava ja opettavainen kokemus. Syvällinen tutustuminen kaupalliseen LoRa-teknologiaan ja yhteisöllisesti kehitettyyn Meshtastic-monihyppyverkkoon toi esille näiden mahdollisuudet ja rajat. Vaikka testattujen teknologioiden sidos on vahva, mikään ei estä monihyppyverkon sovittamista jonkun toisen radioteknologian päälle. Sotilaallisesta näkökulmasta monihyppyverkko MANET-verkkona on ehdottomasti mahdollisuus ja siksi kokeilun arvoinen.

Siviilikäyttöön suunnitellulta ja testatulta ratkaisulta ei tietenkään odotettu taiste-

lunkestävyyttä. Silti käytettyjen elektroniikkapiirien ja niille ladottujen komponenttien laadusta saattoi olla montaa mieltä. Lisäksi muovikoteloinnit olivat vahvistamattomia ja lataukseen tarvittavat mikro-USB -liittimet kenttäkäytössä hankalia ja epäluotettavia.

Tiedonsiirto Meshtastic-verkossa toimi hyvin, kun solmuja oli vähän eikä verkkoa kuormitettu monilla yhtäaikaisilla viesteillä. Jatkoa ajatellen olisi mielenkiintoista selvittää, miten laajempi verkko vaikuttaa yksittäisten radioiden virrankulutukseen.

Yhteenvetona voi todeta, että monihyppyverkko tarjoaa mielenkiintoisia mahdollisuuksia paikallispuolustukselle ja kustannustehokkaan radioratkaisun reserviläisten vapaa-ajan harjoitteluun. Radioita voi käyttää sellaisenaan tai joko älypuhelimen tai tietokoneen avulla. Liittämällä monihyppyverkko osaksi tilannekuvajärjestelmää laajentaa käyttömahdollisuuksia entisestään.

Peittomalli pisimmällä onnistuneella yhteysvälillä.

TESTIPISTE	433 MHZ	868 MHZ
TUKIKOHTA	OK	OK
TP 1	NOK	NOK
TP 2	OK	OK
TP 3	OK	NOK
TP 4	OK	NOK
TP 5	OK	NOK
TP 6	OK	NOK
TP 7	OK	OK
TP 8	OK	OK
TP 9	OK	NOK
TP 10	OK	NOK
TP 11	OK	NOK
TP 12	NOK	NOK
TP 13	NOK	NOK
TP 14	NOK	NOK
TP 15	OK	OK

Yhteyskokeilujen tulokset eri taajuuksilla.

Komentaja Saima Ratasvuori Palvelee Pääesikunnan johtamisjärjestelmäosastolla Johtamisjärjestelmäpalvelut sektorilla. Kirjoittaja on valmistellut viime vuosina esikuntien harjoituksiin sotapelien johtamisjärjestelmäosuuksia.

TEKSTI: SAIMA RATASVUORI

Johtamisjärjestelmäalan sotapeli esikuntaharjoituksessa

Sotapelaaminen on hyvä tapa testata joukon osaamista ja suunnitelmien toteuttamiseen liittyviä haasteita. Johtamisjärjestelmäalan sotapelaamisella kyetään oman toimialan lisäksi tukemaan muita toimialoja ja kokonaisia organisaatioita harjaantumaan poikkeavissa tilanteissa toimimiseen.

Tässä artikkelissa käsitellään johtamisjärjestelmätoimialan sotapelaamista isossa esikuntaharjoituksessa. Tarkoituksena on avata millaisia mahdollisuuksia sotapelaamisen kehys antaa johtamisjärjestelmätoimialan laajalle harjoituttamiselle esikuntaharjoituksissa ja millä vaihtoehdoilla toimialan omaa harjaantumista voidaan tukea sotapelillä. Artikkeli keskittyy nimenomaan perinteisen johtamisjärjestelmäalan sotapelaamiseen. Vaikka kyber on johtamisjärjestelmäalan johdossa, esikunnalle suunnitellussa sotapelissä näiden pelaaminen kannattaa erottaa kahdeksi erilliseksi kokonaisuudeksi. Nämä kaksi kokonaisuutta tekevät kuitenkin paljon yhteistyötä ja miettivät jo suunnitteluvaiheessa omien toimintojensa vaikutukset. Kyber-pelillä voi olla omia erillisiä tavoitteitaan, joista voi tulla vaikutuksia johtamisjärjestelmälle. Kyber-pelistä osana esikuntaharjoituksia voisi kirjoittaa oman artikkelinsa.

Esikuntaharjoitukset

Nykypäivän esikunnissa lähes kaikki taistelijat käyttävät erilaisia johtamisjärjestelmäalan tuottamia palveluita ja tiedonsiirtoyhteyksiä. Toisin sanoen johtamisjärjestelmät ovat olennainen osa sotilaallista toimintaa sekä operatiivisissa että hallinnollisissa tehtävissä. Johtamisjärjestelmät auttavat sotilasjohtajia reagoimaan muuttuviin tilanteisiin, koordinoimaan joukkojen liikkeitä ja tekemään päätöksiä. Johtamisjärjestelmätoimiala mahdollistaa esimerkiksi nopeamman suojatun tiedonsiirron kautta saatavan paremman tilannekuvan ja nopeamman vaikuttamisen.

Esikuntaharjoitukset ovat sotilaallisia harjoituksia, jotka keskittyvät sotilasjohtajien ja esikunnan henkilöstön valmisteluun ja toimintaan erilaissa skenaarioissa. Esikuntaharjoitukset ovat tärkeitä sotilasorganisaatioille, sillä ne auttavat varautumaan mahdollisiin todellisiin tilanteisiin ja parantavat yhteistyötä eri osastojen välillä. Harjoitusten avulla pystytään myös testaamaan ja arvioimaan esikunnan reagointi- ja suorituskykyä erilaisissa skenaarioissa. Harjoituksien tarkoituksena on kehittää päätöksentekokykyä, viestintätaitoja ja yhteistoimintaa. Esikuntaharjoituksessa osallistujat voivat simulaatioiden ja skenaarioiden avulla käydä läpi erilaisia tilanteita, joita heidän tehtävissään voisi poikkeusoloissa esiintyä. Harjoitus voi olla karttapohjainen, tietokonesimulaatioon perustuva tai fyysinen toimintaharjoitus, jossa osallistujat käyttävät erilaisia viestintä- ja suunnitteluvälineitä.

Yleistä sotapelaamisesta

Sotapelaamisen juuret ovat kaukana antiikin ajassa, jolloin jo kehiteltiin erilaisia strategisia lautapelejä sotilaskonfliktien simuloimiseen. Yhtä lailla keskiajalla käytettiin ritarien koulutuksessa strategista ajattelua kehittäviä pelejä. Nykypäivän sotilaille tutumpi tapa sotapelaamisesta kehittyi Preussin valtakunnan aikana. Sotapelaamisella voidaan mallintaa sekä vihollisen että oman joukon toimintaa. Taisteluiden ja operaatioiden simuloiminen tai mallintaminen maaston, olosuhteiden tai sään osalta ovat usein olleet keskeisiä osa-alueita sotapelejä suunnitellessa. Sotapelaamisen kautta voidaan havainnollistaa kokonaistilannetta kaikille osallistujille.

Sotapelaaminen on yksi tapa testata operatiivisten suunnitelmien toimivuutta. Sotapelaamisen kautta voidaan myös nostaa esiin joitakin tunnistettuja haasteita ja mallintaa niiden vaikutusta toimintaan. Parhaimmillaan sotapelaaminen voi tuoda esiin esimerkiksi taktisia puutteita suunnitelmissa, jolloin suunnitelmia voidaan parantaa sotapelistä saaduilla opeilla. Sotapelaamisen kautta on mahdollista tunnistaa syy - seuraus suhteita. Erilaisten skenaarioiden harjoitteleminen auttaa tunnistamaan: miksi jotainkin tapahtui, miten tehdyt päätökset vaikuttivat tapahtumiin ja miten tapahtumat olisi mahdollisesti voitu välttää. Jos sotapelaamisen jälkeen kyetään arvioimaan tapahtumia uudestaan ja käymään niiden pohjalta keskustelua, sekä tarvittaessa tekemään operatiivisiin suunnitelmiin tai esikunnan toimintaohjeisiin muutoksia, on sotapelaaminen onnistunut tavoitteessaan.

Jojä-alan sotapelaaminen

Miten sotapelaaminen voidaan tuoda johtamisjärjestelmäalan toimintaan, kun osa operaatioista ja niiden tukemisesta tapahtuu tietoverkoissa, tietokoneiden näytöillä ja tulevaisuudessa opetetun tekoälyn tukemana? Johtamisjärjestelmäalalla sotapelaamista voidaan toteuttaa usealla eri tavalla, myös toimialan sisällä. Johtamisjärjestelmäalalla on jo käytössään erilaisia simulointiin soveltuvia työkaluja, joilla voidaan laskea esimerkiksi radioasemien optimaalista sijoittelua tai testata häirintälähetteiden vaikutusta suunniteltuun verkon rakenteeseen. Yhtä lailla voidaan tarkastella johtamisjärjestelmäalan joukkojen liikkeeseen ja tehtävien suorittamiseen kuluvaa aikaa simuloimalla joukkojen liikkeitä erilaisten karttaan sidottujen ohjelmistojen avulla. Näiden tapojen yhdistäminenkin on joskus tarpeen, ellei jopa välttämätöntä. Nämä ovat hyvin lähellä sitä mitä ylempänä kuvattiin yleisesti sotapelaamisesta maaston ja olosuhteiden huomioon ottamisena, sekä taktiikan suunnittelussa.

Johtamisjärjestelmäalan sotapelaamista voidaan käyttää hyödyksi myös esikuntien harjoituksissa laajemminkin. Johtamisjärjestelmän sotapelaaminen esikuntaharjoituksessa ei tulisi rajoittua vain johtamisjärjestelmäalan omaan sisäiseen toimintaan, vaan laajat vaikutukset tulisi kyetä harjoituttamaan myös muilla harjoitukseen osallistujilla. Kuten artikkelin alussa todettiin johtamisjärjestelmäala mahdollistaa lähes jokaisen esikuntaan sijoitetun taistelijan työskentelyn. Jotta esikunnan taistelijoille kyetään varmistamaan toiminnan edellytykset, tapahtuu johtamisjärjestelmätoimialalla lukuisia sisäisiä toimenpiteitä, joiden toteuttaminen on suunniteltu toimialan omassa operatiivisessa suunnittelussa.

Osallistuminen muiden toimialojen peleihin

Johtamisjärjestelmäalan tapahtumilla on vaikutusta muidenkin toimialojen peleihin ja toisinpäin. Joillain toimialoilla voi olla sellaisia tavoitteita harjoitukselle, joiden saavuttamisessa johtamisjärjestelmäala pystyy tukemaan. Ison esikunnan harjoituksessa eri peliryhmien tuleekin olla alusta asti keskusteluyhteydessä, jotta syötteet saadaan kulkemaan oikeaa reittiä ja vaikuttamaan halutulla tavalla koko esikunnan toimintaan. Muiden toimialojen pelien suunnittelussa voi nousta esille asioita, jotka vaikuttavat sekä johtamisjärjestelmätoimialan peliin että toimialan harjoitettavan joukon toimintaan. Esimerkkejä tämän kaltaisista pelitapahtumista voisivat olla logistiikan kuvaamat haasteet tuotteiden tai palveluiden saatavuudessa, turvallisuusalan kuvaamat tuhotyöt kriittisissä yrityksissä tai yhteiskuntapelin kuvaamat laajat häiriöt yhteiskunnan toiminnan kannalta kriittisissä järjestelmissä, kuten sähkönjakelussa.

Pyrkimys olemaan osa isompaa kokonaisuutta

Johtamisjärjestelmä- ja kybersotapeleillä on mahdollista harjoituttaa myös muita esikunnan osia tunnistamaan johtamisjärjestelmän vaikutuksia omaan toimintaan. Samalla opitaan ymmärtämään oman toiminnan vaikutuksia johtamisjärjestelmäalan toimintaan. Johtamisjärjestelmätoimialan ei tule esikuntien harjoituksissa eristäytyä pelaamaan omaa peliään, vaan osallistua muiden toimintaan, tuoda oman toimialan pelin syötteiden vaikutukset mukaan päätöksentekoon ja huomioida operatiivisen päätöksenteon vaikutukset omassa toiminnassaan. Osana isompaa kokonaisuutta voidaan myöskin johtamisjärjestelmäalan pelille suunniteltuja syötteitä tarjota esimerkiksi harjoitukseen luodun media-kehyksen kautta toimialalle kokonaiskuvan muodostamista varten.

Esikuntaharjoituksen sotapelin valmistelut

Sotapelaaminen vaatii suuren määrän valmistelua ja taustatyötä. Huolellinen valmistelu on edellytys onnistuneen pelin ja sitä kautta saatavan hyvän oppimiskokemuksen saavuttamiseksi. Osana valmistelua tulee myös tunnistaa riittävä harjoiteltavien asioiden määrä, jotta pelin syötteillä ei tukita organisaation toimintaa.

Johtamisjärjestelmäpelin suunnittelussa lähdetään liikkeelle harjoituksen yleisistä tavoitteista, joita täydennetään toimialan omilla tavoitteilla. Harjoituksen tavoitteet ja harjoituksen kohteena oleva harjoitusorganisaatio (training audience) määrittelevät isot linjat myös johtamisjärjestelmäpelin toteutukselle. Harjoituksen päätapahtumien alle rakennettavilla tapahtumakorteilla luodaan pelin yleiskulku yhdessä muiden toimialojen pelivalmistelijoiden kanssa.

Toimialan omat tavoitteet antaa toimialan johto. Toimialan tavoitteilla pyritään, oman toimialan harjoituttamisen lisäksi, tukemaan harjoituksen isojen tavoitteiden saavuttamista. Asiaa valmistellaan yhdessä ja valmistelijoilla on mahdollisuus nostaa esiin kohtia, jotka on tunnistettu erillistä tarkastelua vaativiksi esimerkiksi edellisissä harjoituksissa, operatiivisen suunnittelun yhteydessä tai uuden suorituskyvyn käyttöönoton yhteydessä. Tämä ei tarkoita, että pelin tulisi valmistella vain tilanteita, joissa tietää joukon pärjäävän, vaan on myös uskallettava ottaa esiin hankalampiakin asioita. Sotapelin suunnittelussa on lähdettävä liikkeelle olemassa olevilla suorituskyvyillä, eikä ratkaista tilanteita mahdollisesti tulevilla suorituskyvyillä tai organisaatioilla. Pelin valmisteluissa on mietittävä, mitä kaikkia osapuolia johtamisjärjestelmäpelissä on oltava edustettuna, jotta harjoituskohteena oleva esikunta saa riittävän tilannekuvan muodostettua. Mitkä alajohtoportaat ja sidosryhmät pelataan, mitä tietoja harjoitettava organisaatio tarvitsee peliltä voidakseen tehdä tilannearvion ja siihen liittyviä päätöksiä.

Pelin suunnittelussa voidaan hyödyntää aika-tila-joukot jakoa. Aika-ulottuvuuden arviointiin vaikuttaa keskeisesti harjoitettavien joukkojen ja johtamistasojen johtamisen aikaulottuvuus. Minkä johtamistason esikuntaa harjoitetaan, mikä on kyseisen johtamistason aikajänne 1-3 vrk, 14 vrk, 1kk vai vuosi? Isojen esikuntien, kuten Pääesikunnan ja Puolustushaaraesikuntien, ollessa harjoitettavana joukkona syötteiden tulisi tarjota mahdollisuuksia toimintaan sekä operaatiokeskuksen välittömille toimille että suunnitteluosien viikkojen ja kuukausien päähän ulottuvalle toiminnalle.

Tila-ulottuvuutta voidaan johtamisjärjestelmäpelissä tarkastella useammasta näkökulmasta. Käytössä oleva fyysinen tila, esimerkiksi oman valtion alue tai vihollisen valtaaman alueen vaikutus toimintaan. Tilana voidaan tarkastella myös johtamisjärjestelmäalan keskeistä toimintaympäristöä tietoverkkoja ja siellä olevia palveluita, sekä tässä ympäristössä olevaa tilaa tehdä operaatioita.

Johtamisjärjestelmätoimialan joukkojen osalta kyse ei ole vain taistelukentällä osana prikaateja ja pataljoonia sotivista toimialan joukkoista. Logistiikkalaitoksen, Järjestelmäkeskuksen ja Puolustusvoimien johtamisjärjestelmäkeskuksen ja Palvelukeskuksen toiminta tulee ottaa aktiivisesti mukaan pelin suunnitteluvaiheessa. Näiden joukkojen toiminta on tiivistä erilaisissa työryhmissä jo jokapäiväisessä työarjessa. Sotapelaamisen tulisi kyetä tarvittaessa antamaan syötteitä, jotka käynnistäisivät kyseisten normaaliolojen toimintojen toteuttami-

sen myös poikkeusoloissa. Jos kyseisten työryhmien asiantuntijat eivät osallistu harjoitukseen olisi valmisteluvaiheessa hyvä suunnitella erilaisten työryhmien esityksiä valmiiksi, jotta niitä voidaan tarjota päätöksentekijöille sopivissa kohdissa tukemaan päätöksentekoa tietoon perustuen.

Toimialan tuntemus

Johtamisjärjestelmä alan sotapelaamisen valmisteluissa tulisi kiinnittää huomiota harjoituksen tavoitteiden lisäksi peliorganisaation muodostamiseen. Organisaation tulisi koostua monipuolisesti toimialaa ja eri puolustushaaroja edustavista yhteistyökykyisistä ihmisistä. Valmisteluihin tulisi osallistua tietoliikenteen, palveluiden tuottamisen ja puolustushaarojen toiminnan tuntevia ihmisiä, joilla on riittävä pääsy valmistelussa tarvittavaan tietoon. Mitä isommasta harjoitusesikunnasta on kyse, sitä laajempi myös peliorganisaation osaamisen on oltava. Tämä mahdollistaa syötteisiin riittävän tarkan sisällön, eli paremman laadun. Syötteiden hyvä laatu parantaa harjoitusorganisaation mahdollisuuksia harjaantua tehtävien kautta oman operatiivisen suunnitelman kehittämisessä ja omassa toiminnassaan.

Valmisteluvaiheessa on myös tunnettava toimiala ja harjoituksen kohteena oleva organisaatio riittävän hyvin, jotta kyetään viemään syötteet oikeisiin tapahtumakortteihin. Kaiken tiedon ei tarvitse tulla johtamisjärjestelmäpeliltä suoraan toimialan käyttöön, vaan tietoa ja syötteitä voidaan tarjota myös yhteistyössä muiden kanssa. Johtamisjärjestelmäalan syötteitä voidaan antaa esimerkiksi tiedustelun, turvallisuuden, puolustushaarojen, sidosryhmien, median tai logistiikan pelin kautta. Tämä mahdollistaa tapahtumakortin tapahtumien kasvattamisen ja harjoitusorganisaation muiden osien kouluttamisen siitä, mitkä asiat saattaisivat kiinnostaa johtamisjärjestelmätoimialaa.

Peliorganisaation tulisi myös harjoituksen aikana olla riittävän vahva ja verkostoitunut kyetäkseen edistämään toimialan harjoituksen tavoitteiden saavuttamista. Nykyiset kollaboraatioon tarkoitetut työkalut mahdollistavat monipaikkaisen toiminnan. Johtamisjärjestelmäpelin tulee olla samaan aikaan yhteydessä sekä peliorganisaation että hajallaan toimivien harjoitukseen osallistuvien esikuntiin ja niiden alapeleihin.

Harjoituksen aikana peliorganisaation on hyvä olla kuulolla myös erilaisissa toimialan kokouksissa, jotta kyetään seuraamaan syötteiden vaikutusta. Pelin tulee kyetä toimimaan vuorovaikutteisesti, eli reagoimaan harjoitettavan organisaation toimintaan. Toisinaan jotain syötettä tulee jatkaa uusilla syötteillä, jos ensimmäinen ei aiheuta haluttua toimintaa, toisinaan muokkaamaan suunniteltuja syötteitä, jos toimialan toiminta antaa siihen aihetta. Yksinkertaisimmillaan tämä tarkoittaa esimerkiksi suunnitellun järjestelmän käyttökatkon ja varamenetelmien päättymisajankohdan muuttamista operatiivisen johdon käskyjen mukaisesti pelisuunnitelmasta poikkeavalla tavalla.

Tapahtumat ja syötteet

Tämän artikkelin kuvaamat tilanteet on rakennettu mallilla, jossa harjoituksen tavoitteiden kautta harjoitukselle on valittu muutama päätapahtuma, joiden alle

suunnitellaan tapahtumakortit. Tapahtumakorteille laitetaan kyseiseen tapahtumakorttiin liittyvät syötteet, joilla ohjataan harjoituksen kohteena olevan organisaation toimintaa. Lähtökohtaisesti johtamisjärjestelmä alan syötteet löytyvät samoilta tapahtumakorteilta muiden toimialojen syötteiden kanssa. Vain erillistapauksissa toimialat voivat laatia omia tapahtumakortteja. Tällä yhteisellä valmistelulla varmistetaan sekä sotapelin tilanteiden kehittyminen harjoituksen tavoitteiden suuntaisesti että toimialojen riittävä yhteistyö ja pelikuvausten, ja niiden aikauttamisen, eheys. (Tähän kuva 1)

Kuvassa 1 on esitettynä organisatorisesti malli sotapelin rakentamisesta kahdessa esimerkki tapahtumassa: vihollisen hyökkäyksessä ja yhteiskunnan laaja-alaisista häiriöistä. Päätapahtuman ollessa vihollisen hyökkäys, yksi tapahtumakortti voi käsitellä hyökkäykseen liittyvää tiedustelua ja seuraava tapahtumakortti käsittelee hyökkäykseen liittyvää tuli-iskua kaukovaikutteisilla aseilla ja kolmas maahyökkäyksen etenemistä. Kyseisten tapahtumakorttien syötteet kuvaavat harjoitusorganisaatiolle meneviä tietoja kyseiseistä tapahtumista. Syötteillä, esimerkiksi lisäämällä niitä tai tarjoamalla niiden kautta tarkempaa tietoa, myös ohjataan harjoitusorganisaatiota kohti oikeanlaisia toimenpiteitä. Peliorganisaatio siis rakentaa oman tilanteensa ylhäältä alaspäin, kun taas harjoituksen kohteena olevan organisaation pitäisi saamiensa syötteiden pohjalta kyetä muodostamaan kokonaiskuva tapahtumista, eli edetä alhaalta ylöspäin.

Seuraavaksi esitellään kaksi erilaista tapahtumakorttia: Yhteiskunnan laaja-alaiset häiriöt, jotka johtavat varamenetelmien käyttöön, sekä tuli-isku.

Yhteiskunnan laaja-alaiset häiriöt

Yhteiskunnan laajalaiset häiriöt tarjoavat johtamisjärjestelmäalalle paljon mahdollisuuksia antaa syötteitä, sekä nopeaa tilanteen ratkaisemista vaativiin tilanteisiin tai pitemmän ajan suunnittelun haastamiseksi. Nopeammin ratkaistaviksi asioiksi voidaan syötteillä rakentaa tilanne, jossa koko harjoitettava esikunta joutuu siirtymään nopeasti erilaisten varamenetelmien käyttöön tietojärjestelmien tai tiedonsiirtoväylien osalta. Teknisiin varamenetelmiin kuuluu tietojen ja järjestelmien käytettävyyden varmistaminen esimerkiksi varmuuskopioinnilla, tietokantojen hajauttamisella. Tiedonsiirtoyhteyksien vaihtoehtoiset reitit ja mahdollisuudet tukevat erilaisten varamenetelmien käyttöä esikunnan toiminnassa.

Varamenetelmien tarkoitus on varmistaa toiminnan jatkuvuus ongelmien ja häiriöiden aikana. Muita kuin teknisiä varamenetelmiä ovat esimerkiksi sekä henkilöstön että organisaatioiden sijaisuusjärjestelyt ja esikuntien fyysinen hajauttaminen eri fyysisiin sijainteihin päätöksenteko prosessin jatkuvuuden varmistamiseksi. Lisäksi viestintäsuunnitelmat, joilla määritellään miten poikkeustilanteessa tärkeää tietoa ja päätöksiä jaetaan esikunnan sisällä ja ulkopuolisille organisaatioille ovat tärkeä osa varamenetelmiä.

Varamenetelmiin siirtyminen voidaan sotapelissä toteuttaa kahdella tavalla: yllättäen tai hallitusti. Ensimmäinen tapa toteuttaa varamenetelmiin siirtyminen on niin sanottu ”pikatilanne”, jossa jokin ohjelma tai palvelu lakkaa toimimasta yllättäen. Yllättävän tilanteen onnistunut harjoituttaminen vaatii organisaation valmistautumista ja on peliryhmälle vaikeammin hallittavissa oleva tilanne.

Toinen tapa varamenetelmiin siirtymisen pelaamiselle on niin sanottu ”hallittu huoltokatko”. Johtamisjärjestelmätoimialalle aiheutetaan syötteillä tilanne, jossa joudutaan esittämään tarvetta palvelun tai järjestelyn ”huoltokatkoille”. Syynä voi olla teknisen vian korjaaminen tai alustojen päivittäminen haavoittuvuuden takia. Sotapelaamisella voidaan katkon pituus kuvata riittäväksi, jotta erilaisten prosessien suorittaminen varamenetelmillä tulee ajankohtaiseksi. ”Huoltokatkojen” kautta tehtävä teknisen vian korjaaminen käynnistää myös toimialan sisäisen pelin, jos sille on tarvetta ja kyseiset asiantuntijat osallistuvat harjoitukseen. Tällöin samalla tapahtumalla harjoitetaan suurta joukkoa esikunnissa varamenetelmien osalta, sekä pienempää joukkoa toimialalla oman tehtävänsä tekemisessä.

Riippumatta varamenetelmiin siirtymisen syystä esikunnassa on ratkaistava samanlaisia asioita. Esikuntatyössä varamenetelmiin siirtyminen tarkoittaa jonkin toisen palvelun käyttöä, siirtymistä manuaalisiin menetelmiin tai asioiden odottamaan jättämistä. Esikunnalle varamenetelmiin siirtyminen tarkoittaa päätöksenteko- ja käskytysprosessin harjoittelua: Kuka saa päättää varamenetelmiin siirtymisestä? Miten niiden aikana toimitaan ja miten siirrytään takaisin päämenetelmään? Nämä päätökset eivät pääsääntöisesti ole johtamisjärjestelmäalan yksin tekemiä päätöksiä, vaan toimialan esityksestä päätökset ja käskyttämisen tekee operatiivinen johto. Laajamittaisissa häiriöiden kuvaamisen etuna on, että lähes jokainen toimiala ja puolustushaarat joutuvat miettimään, miten heidän omistamansa palvelut ja yhteydet tuotetaan varamenetelmien aikana.

Tuli-iskut

Toinen esimerkki pelitapahtumasta on tuli-isku kriittisiin kohteisiin. Valmisteluvaiheessa toimialojen pelillä on mahdollista esittää tuli-iskujen kohteita vihollisen pelistä vastaavalle taholle. Riippumatta siitä, hyväksytäänkö oman toimialan esitykset kohteiksi, on seuraava vaihe peliryhmällä samanlainen. Kun kohteet ovat selvillä, peliryhmän on selvitettävä itselleen niiden mahdolliset vaikutukset oman toimialan osalta. Useissa valituissa kohteissa on usein johtamisjärjestelmätoimialan kannalta vähintään kyseisen kohteen tarvitsemat yhteydet ja toisinaan myös muualle jatkavia yhteyksiä. Vaikutuksien selvittämisen jälkeen voidaan suunnitella toimialan sisäiset kuvaukset ja tilanteen elättäminen. Tuli-iskusta ensimmäiset syötteet lähtevät liikkeelle samanaikaisesti muiden toimialojen ensimmäisten syötteiden kanssa.

Tuli-iskun ensimmäisiä syötteitä ovat esimerkiksi operatiivisen järjestelmäkeskuksen ilmoitukset verkosta pudonneista viestiasemista. Samaan aikaan tulisi lähteä myös muille toimialoille vastaavia ilmoituksia, esimerkiksi tietyn alueen tutkakuvan katoamisesta. Näiden syötteiden tulisi aiheuttaa pelin harjoituskohteena olevassa organisaatiossa tarpeen tehdä analyysi iskun vaikutuksista omaan toimintaan ja informoida vaikutuksista myös muita toimialoja. Jos peli huomaa, ettei analyysi käynnisty, syötteitä voidaan lisätä ja varautua antamaan niitä myös muille toimialoille. Tuli-iskun jälkeistä intensiteettiä säädellään harjoituskohteena olevan joukon toiminnan mukaisesti. Mahdollisen korjaus tai uudelleen reitityssuunnitelman mukaisia tekoja kuvataan syötteillä tehdyksi, kun asioilla olisi realistinen mahdollisuus edetä ja harjoitettavan joukon tekemät päätökset ja antamat käskyt mahdollistavat asioiden etenemisen. Tämä vaatii peliorganisaatiolta harjoitusorganisaation suunnitelmien ja käskyjen seuraamista, jotta tilanteen eteenpäin vieminen voidaan tehdä harjoitettavan joukon suunnitelmien, hyvien tai huonojen, mukaisesti.

Pitkän aikavälin suunnitteluun vaikuttavat tapahtumat

Usein harjoituksien esikunnissa keskitytään lähes koko henkilöstön voimin rea-

goimaan välittömiin tapahtumiin, joihin on olemassa valmiita ratkaisumalleja. Näin tapahtuu riippumatta siitä, mikä on kyseisen esikunnan virallinen suunnittelujänne. Syötteet, joiden tulisi vaikuttaa analyysiin pidempi aikaisesta toiminnasta jäävät vähemmälle huomiolle. Inhimillisesti ajatellen tämä on ymmärrettävää, sillä ne eivät ehdi vaikuttamaan tapahtumiin niiden 5 - 10 päivän aikana, jonka harjoitus kestää.

Toisaalta nykyiset sodat eivät ole vaikuttaneet kovin nopeilta vaan ovat venyneet pitemmiksi, jolloin myös pitkän ajan suunnittelua tulee harjoitella. Pitemmän ajan suunnitteluun vaikuttavilla syötteillä pyritään sotapeleissä tukemaan suunnittelua, jossa mietitään vaihtoehtoisia skenaarioita ja kyetään tunnistamaan niiden toteutumiseen vaikuttavia asioita. Haastavinta on rakentaa syötteitä, joiden pitäisi asettaa haasteita toimialan pitkän aikavälin suunnittelulle. Yhtenä vaihtoehtona on kuvata toimitusketjuun, tuotteita toimittaviin yrityksiin tai tuotteiden maahan pääsyyn haasteita, joiden vaikutukset eivät ole välittömiä, mutta tulevat vaikuttamaan viikkojen tai kuukausien viiveellä toimintaan. Edellä mainituilla tuli-iskuilla voi olla myös tiedonsiirtoverkkoa tai johtamispaikkoja laajempia seurauksia, jos ne kohdistuvat toimintojen kannalta kriittisiin kohteisiin, joita ei ole siirretty väistötiloihin tai joiden siirtäminen on haastavaa. Näiden syötteiden on tarkoitus tarjota suunnitteluosille mahdollisuuksia analysoida tapahtumien vaikutuksia pitemmällä aikajänteellä.

Lopuksi

Artikkelissa käsiteltiin yleisellä tasolla johtamisjärjestelmäalan sotapelaamisen ulottamista harjoituksissa laajemman joukon käyttöön sekä johtamisjärjestelmäalan pelin sisällyttämistä osaksi yleistä pelitoimintaa eristäytymisen sijasta. Yhdessä tekemällä sotapeleistä saadaan harjoitettavalle organisaatiolle mielenkiintoisia tapahtumia testata osaamistaan ja valmistautua mahdollisiin haasteisiin. Vaikka sotapelaamisen suunnittelu ja pelin läpivieminen on työlästä, se on myös peliorganisaatiolle opettavaista. Hyvä henkisessä peliryhmässä erialojen osaajat kykenevät tukemaan toisiaan. Usein peliryhmässä oppii omastakin toimialasta uusia näkökulmia, joiden hyödyntäminen on mahdollista myös kyseisen harjoituksen jälkeen omissa työtehtävissä.

Millog

Hyvää Joulunaikaa

& TURVALLISTA UUTTA VUOTTA

YHDESSÄ PAREMPI JA
TURVALLINEN TULEVAISUUS

MILLOG.FI

TEKSTI: SEPPO SIMOLA

Viestijoukkojen väreissä oli aluksi 12 koulutushaaramerkkiä

Suuntaradioasentajan merkki oli käytössä vain pari vuotta

Koulutushaaramerkit tulivat osaksi varusmiesten lomapukua itsenäisyyspäivänä 1949. Viestiaselajin kannalta kiinnostavin vaihe oli ajanjakso vuoteen 1962 saakka. Silloin viestin violetti-keltaisissa väreissä ehti olla pitkälti toista kymmentä erilaista koulutushaaramerkkiä. Lisäksi viestiin viittaavia koulutushaaramerkkejä oli muissakin aselajeissa kunkin aselajin omissa väreissä.

Koulutushaaramerkkien käyttöönotosta käskettiin 10.11.1949 päivätyllä Puolustusvoimain pääesikunnan käskylehdellä numero 10. Puolustusvoimain komentaja oli hyväksynyt merkit käyttöön otettaviksi jo saman vuoden helmikuussa.

Merkin joutui ostamaan

Merkkien myynti sotilaskodeissa aloitettiin joulukuun alussa 1949, ja itsenäisyyspäivänä merkit jo koristivat monien niihin oikeutettujen varusmiesten vasenta hihaa. Merkit eivät olleet jakotavaraa, vaan niiden hinta oli 55 silloista markkaa. Todennäköisesti kaikki merkkiin oikeutetut eivät sellaista koskaan lunastaneet. Suomen Kuvalehden irtonumero maksoi tuolloin 35 markkaa ja Sotamiehen taskukirja 30 markkaa, joten aivan halpa merkki ei ollut.

Merkkiä käyttöön otettaessa sen paikaksi määrättiin vasen hiha tulitikun mitta alaspäin olkapoletin saumasta. Täten merkki oli aluksi selvästi ylempänä kuin vaikka 1970-luvun varusmiehillä, jotka ompelivat merkin olkavarren puoliväliin lomapuvun vasempaan hihaan. Nykyisen maastopuvun vasemmassa hihassa on valmiina tarranauha, johon mahtuu Suomen lipun ja joukko-osastotunnuksen ohella myös koulutushaaramerkki. Tarrakiinnitteiset merkit ovat tilankäyttösyistä selvästi edeltäjiään pienempiä.

Aselajivärit ilmenivät koulutushaaramerkissä

Koulutushaaramerkkejä käyttöön otettaessa perusperiaatteena oli, että aselajiväri käy ilmi myös koulutushaaramerkistä. Esimerkiksi viestijoukoissa palvelleen moottoriajoneuvon kuljettajan koulutushaaramerkki – siivetty ohjauspyörä – oli violetti-keltaisissa viestin väreissä.

Marraskuun 1949 käskylehden luettelossa viestijoukkojen väreissä olivat seuraavat suoraan viestijoukkojen tehtäviin viittaavat koulutushaaramerkit: puhelinmies, radiomies, lennätinmies, puhelinmekaanikko ja radiomekaanikko.

Näiden ohella viestin väreissä oli myös lääkintämies, kengitysseppä, eläinlääkintämies, moottoriajoneuvonkuljettaja, ajomies, kirjuri ja talousmies. Näitä osaajiahan tarvittiin sotaväessä aselajiin katsomatta. Viestin väreissä oli alkujaan kaksitoista koulutushaaramerkkiä.

Kuva-1 (Seppo Simola):Ylinnä on vuosina 1957–1962 käytössä ollut keskusmiehen merkki. Suuntaradioasentajan merkki (alhaalla vasemmalla) oli käytössä vain vuosina 1960–1962, joten se lienee yksi lyhytaikaisimmista merkeistä. Puhelinasentajan merkki (alhaalla oikealla) kuului alkuperäiseen merkkivalikoimaan ja se poistui vuoden 1962 suuressa karsinnassa.

Yleisimpiä koulutushaaramerkkejä – vaikkapa lääkintämiehiä, autonkuljettajia ja talousmiehiä – oli enimmillään kymmenessä eri aselajivärissä. Vastaavasti oli monia merkkejä, joita esiintyi vain yhdessä värissä.

Kromipainosta kudontaan

Merkit valmistettiin aluksi kromipainomenetelmällä. Kuvasymboleja oli alussa kuutisen kymmentä ja aselajiväriyhdistelmiä yksitoista. Eri variaatiot huomioon ottaen merkkien kokonaismäärä oli 142. Kuvasymbolin sisältänyt aselajivärinen merkki kiinnitettiin tehtaalla kauluslaatan reunuksen värisellä 3 mm paksulla ompeleella sarkapohjalle. Vanhimman merkkiversion tunnistaa helpoiten juuri sarkapohjasta. Alkuperäinen versio oli käytössä vain viisi vuotta.

Vuonna 1954 merkkejä alettiin valmistaa kutomalla, mutta merkit säilyivät kuva- ja värisymboliikaltaan entisellään. Viisikymmenluvulla kuvasymbolien määrä jopa lisääntyi, ja uusia merkkejä tuli myös viestijoukoille.

Kuva-2 (Seppo Simola):Aluksi viestijoukkojen väreissä oli myös lääkintämiehen ja eläinlääkintämiehen merkki. Mallin m/49 merkit tunnistaa sarkapohjasta.

Viestiaselajiin tuli uusia merkkejä 1950 ja 60-luvuilla

Vanha viestimiehen merkki, jonka symbolina oli kalevalainen salama ja puhelimen kuuloke ristissä, annettiin marraskuussa 1957 jalkaväen ja tykistön käyttöön. Viestijoukkojen puhelinmiehet saivat tuolloin uuden merkin, jonka symbolin muodostivat puhelinjohto, eriste ja puhelimen kuuloke. Nykyinen viestimiehen merkki oli aluksi radiomiehen merkki.

Keskusmiehetkin saivat samalla kertaa oman merkkinsä, jonka symbolina oli kaksi kalevalaisten käsien yhdistämää puhelimen kuuloketta. Suuntaradioasentajat saivat oman merkkinsä vuonna 1960. Symbolin muodosti hammasratas, jonka päällä oli suuntaradionuoli. Suuntaradiota ryhdyttiin sittemmin kutsumaan linkiksi. Linkkiyhteyksiä tarvittiin tyypillisesti prikaatien sisällä sekä niistä armeijakuntaan etäisyyksien ollessa 20–50 km. Jalkaväkiprikaatin viestikomppaniaan kuului linkkijoukkue.

Viestin uudet merkit 50-luvun lopulta ja 60-luvun alusta jäivät lyhytaikaisiksi, koska vuoden 1962 suuri karsinta vei ne. Lieneekö suuntaradioasentajan merkki Suomen lyhytikäisin koulutushaaramerkki vain parin vuoden voimassaoloajallaan?

Viestimiesten merkkejä muissa aselajeissa

Viestimiehiä tarvittiin monissa muissakin aselajeissa kuin viestijoukoissa. Edellä kerrotun mukaisesti koulutushaaramerkit olivat aluksi aselajikohtaisia. Niinpä panssarijoukoilla oli käytössä panssarivaunun viestittäjän merkki (panssarivaunun symboli päällikkeenään ylöspäin iskevä salama). Merkin värimaailma oli aselajin mukaan musta-harmaa.

Ilmasähköttäjän merkki noudatti puolestaan ilmavoimien merkkien sini-mustaa värimaailmaa kuva-aiheen ollessa vaalea. Kuva-aiheena oli pystyasennossa oleva siivetty kalevalainen salama. Nämäkin merkit vei mennessään vuoden 1962 suuri karsinta. Tosin tehtävätkin poistuivat ennen pitkää, koska T-54 ja T-55 -panssarikaluston myötä vaunuradion operointi siirtyi vaununjohtajalle, eikä moderneissa lentokoneissakaan tarvittu erillistä sähköttäjää.

Panssarijoukkojen väreissä oli aluksi myös puhelinmies ja radiomies. Jalkaväellä ja jääkärijoukoilla oli viestiin viittaavina merkkeinä edellisten ohella myös puhelinmekaanikon sekä radiomekaanikon merkki. Kranaatinheittimistöllä oli lisäksi oma viestimiehen merkki, jonka kuvasymboli muodostui putoavasta kranaatista päällikkeenään kalevalainen salama.

Epäsuora tuli tarvitsee viestimiehiä

Muukin epäsuora tuli kuin kranaatinheittimistö tarvitsi luonnollisesti viestiyhteyksiä, joten puhelinmiehen ja radiomiehen merkki löytyi sekä kenttätykistön että rannikkotykistön väreissä. Ilmatorjunta käytti merkkien m/49 ja m/54 voimassa ollessa vielä kenttätykistön puna-mustia aselajivärejä.

Viestimies löytyy myös pioneerijoukkojen väreissä, mutta rajavartioston väreissä ei viestimiesten koulutushaaramerkkejä ollut. Ilmavoimilla puolestaan oli muutama viestiaselajiin tai elektroniseen sodankäyntiin viittaava merkki. Näitä olivat aiemmin mainitun ilmasähköttäjän ohella tutkamies ja radiosähköttäjä. Tutkamiehen merkki esiintyi myös rannikkotykistön väreissä.

Vuonna 1962 karsittiin merkkejä

Vuonna 1962 karsittiin rajusti kuvasymbolien määrää ja samalla merkeistä katosivat vaihtelevat aselajivärit. Siirryttiin oletusaselajiväreihin, eli esimerkiksi moottoriajoneuvonkuljettajien merkki oli kuljettajan aselajiin katsomatta jatkossa aina huollon väreissä eli sinipohjainen ja harmaalla reunustettu.

Seuraava isompi uudistus merkkeihin tuli maastopuvun m/91 myötä. Värimaailma ja kuvasymbolit pysyivät ennallaan, mutta merkkien koko pieneni selvästi kun siirryttiin yhä käytössä oleviin tarrapohjaisiin merkkeihin. Samalla joidenkin merkkien alaosassa ollut ilmeisesti laakeriseppelettä symboloinut kaksoisreunus poistui. Merkkien valmistusta jatkettiin kutomalla, mutta nyt merkit ommeltiin tehtaalla tarrapohjiin, kun m/62 merkit liimattiin kudonnan jälkeen taustakankaalle.

Kulutushaaramerkit kertovat sotaväen historiaa

Suomen sotaväki oli koulutushaaramerkkien käyttöön oton aikaan vielä oleellisesti hevosvetoinen. Niinpä viestijoukkojen väreissä oli koulutushaaramerkki

Kuva-3 (Seppo Simola): Nykyisin viestimiehen merkkinä tunnetun merkin alkuperäinen merkitys oli radiomies ja sitä valmistettiin useissa eri aselajiväreissä. Merkit ovat vasemmalta lukien ilmavoimien, viestijoukkojen ja jääkärijoukkojen väreissä.

Kuva-4 (Seppo Simola):Viestin ammattimiehille oli käyttöä monissa aselajeissa. Merkit ovat vasemmalta lukien: kranaatinheittimen viestimies (jalkaväki), puhelinmies (kenttätykistö) ja radiomekaanikko (ilmavoimat).

niin ajomiehelle, kengityssepälle kuin eläinlääkintämiehellekin. Kenttätykistöllä puolestaan oli ratsurin merkki. Ratsurit ohjasivat tykkivaljakkoa vasemmanpuoleisten valjakkohevosten selässä istuen.

Hevosvetoisuudesta luovuttaessa poistuivat myös hevosiin viittaavat koulutushaaramerkit. Puolustusvoimien teknistyminen sekä uudet sodankäyntitavat puolestaan toivat – ja tuovat yhä – uusia koulutushaaramerkkejä.

1970-luvun uutuuksia oli esimerkiksi panssarijääkärin merkki, jonka kuva-aiheena on BTR-60 miehistönkuljetusvaunu päällikkeenään rynnäkkökivääri. Samoihin aikoihin myös ohjusampujat saivat oman merkkinsä.

Kybervarusmiehen merkki on uusin

Uusin koulutushaaramerkki on vuonna 2023 vahvistettu kybervarusmiehen merkki, joka on viestijoukkojen violetti-keltaisissa väreissä. Merkissä viestimiehen koulutushaaramerkin toinen salama

on korvattu avaimella. Merkkiä saa kantaa puvussa vain varuskunta-alueella.

Toinen varsin uusi elektroniseen sodankäyntiin viittaava merkki on ELSO-miehen merkki. Se on panssarijoukkojen musta-harmaissa väreissä. Sodankäyntitapojen muutokseen liittyy myös kaupunkijääkärin merkki, joka on yksi 2000-luvun uutuuksista.

Muitakin erikoismiehiä kuin elektronisen sodankäynnin osaajia on alettu nostaa esiin. Oman merkkinsä ovat saaneet niin laskuvarjojääkärit, rannikkojääkärit kuin valmiusjoukkosotilaatkin. Viimeksi mainittua merkkiä uusin koulutushaaramerkkikuvasto ei tosin tunne.

Kanto-oikeus piti ansaita

Koulutushaaramerkkien aamunkoitossa joukko-osaston komentaja myönsi merkin käyttöoikeuden perusyksikön päällikön esityksestä, eli merkin saanti ei suinkaan ollut automaatio. Useamman ehdon piti täyttyä, jotta päällikkö saattoi kanto-oikeutta esittää. Merkillä oli alkuun varsin vahvasti palkitsemisesineen luonne. Kanto-oikeuden saaneiden nimet jopa julkaistiin joukko-osaston päiväkäskyssä.

Upseerikokelaille merkki tuli automaattisesti samoin aliupseerikurssin ensimmäisen jakson hyväksytysti suorittaneille. Kesällä 1950 merkkeihin oikeutettuihin lisättiin upseerioppilaat, ja kesästä 1952 alkaen merkkejä voitiin myöntää myös B-miehille.

Merkin saattoi saada varusmies, joka oli saavuttanut koulutustavoitteet, jotka piti hallita varusmiesajan puolessa välissä. Tavoitteiden hallinnan piti olla todettu jatkuvan tarkkailun tai tarvittaessa sopivan kokeen avulla.

Miehistötehtävissä palvelevat saattoivat saada merkin aikaisintaan palvelusaikansa puolessa välissä. Merkki tuli myöntää vähintään 25 %:lle kunkin koulutushaaran vahvuudesta. Normaalitapauksessa merkin sai 75 % koulutushaaran varusmiehistä. Jos suoritukset kaikkinensa olivat hyviä, niin poikkeustapauksessa jopa kaikki saman koulutushaaran taistelijat saattoivat merkin saada.

Palkitsemisvälineestä yleismerkiksi

Palkitsemisvälineen rooli himmeni vähitellen, ja jo vuonna 1962 merkki annettiin kaikille varusmiehille, joiden palvelusajasta puolet oli takana. Aliupseerioppilaat saivat merkkinsä puolikurssivaiheessa. Ilmeisesti jo vuonna 1965 merkki useimmiten annettiin heti sotilasvalan jälkeen eli alokasajan päätyttyä.

Nykyisin koulutushaaramerkkiä aletaan kantaa yleensä peruskoulutuskauden jälkeen. Erikoisjoukot ovat asia erikseen. Esimerkiksi laskuvarjojääkärit saavat merkin joukkokoulutusvaiheessa laskuvarjojääkärin tasokokeen perusteella.

Periaatteena oli aluksi yksi merkki per henkilö vaikka olisi palvellut useammassa koulutushaarassa. Normia on myöhemmin lievennetty, koska silloin tällöin näkee vanhoissa tj-kravateissa ja muissa inttimuistoesineissä kaksikin koulutushaaramerkkiä. Vain yhtä kerrallaan saa tietenkin kantaa.

Radioviestittäjän merkki

Erityisesti viestiaselajiin liittyy myös yksi varusmiesten suoritusmerkki. Ampuma- ja kuntomerkki ovat laajalti tunnettuja ja ne koristavat monen varusmiehen lomapuvun rinnusta, mutta radioviestittäjän merkki on varsin harvinainen.

Ajatus radioviestittäjän merkistä juontaa jo 1930-luvulle. Sotilasradiosähköttäjän valioluokan merkki otettiin lopulta käyttöön juuri jatkosodan kynnyksellä. Merkki muuttui kolmiluokkaiseksi vuonna 1951. Kolmen vuoden kuluttua siitä tuli viisiluokkainen sisältäen luokat I-III sekä mestari- ja suurmestariluokan. Samalla merkin nimi muuttui radioviestittäjän merkiksi.

Merkin kantopaikka on muista kunto- ja taitomerkeistä poiketen oikeanpuoleisen rintataskun keskellä. Varusmiehillä paikka on vapaana, mutta suurin osa kantahenkilökunnasta kantaa tuolla paikalla jatkokoulutuksen merkkiä. Kunto- ja taitomerkkien perinteinen paikkahan on oikean rintataskun yläpuolella.

Radioviestittäjän merkki on nykyään mahdollista ansaita luokissa I-III muiden muassa Kainuun prikaatiin kuuluvassa Pohjois-Suomen viestipataljoonassa.

Seppo Simola

Kaikki lisätiedot tässä artikkelissa käsiteltyihin asioihin sekä muut kiinnostavat tiedot ovat erittäin tervetulleita samoin kuin aiheeseen liittyvät merkit. Allekirjoittaneen yhteystiedot saa lehden toimituksesta.

Lähteitä:

Kari K. Laurla: Sotilasheraldiikka – Liput, merkit, tunnukset (2003)

Kari K. Laurla: Koulutushaaramerkki (moniste)

Janne Mäkitalo: Puolustusvoimien kurssi- ja suoritusmerkit (1995)

Puolustusvoimain pääesikunnan käskylehti n:o 10 1949

Sotilaan käsikirja 2022

Kuva-5 (Seppo Simola): Monien koulutushaaramerkkien ohella viestitoimintaan liittyi myös yksi suoritusmerkki eli radioviestittäjän merkki. Vasemmalla on I luokan ja oikealla III luokan merkki.

Kuva-6 (Viestimies-lehti): Vuonna 2023 vahvistettu kybervarusmiehen merkki on uusin tulokas koulutushaaramerkkirintamalla. Sitä saa kantaa vain varuskunta-alueella.

Kapteeni (res.) Seppo Simola tutkii, kerää ja tallentaa kokoelmaansa suomalaista sotilasperinnettä, kuten kauluslaattoja, arvomerkkejä ja muita sotilaspuvun tunnuksia sekä sotilaspukuja. Simola on kirjoittanut artikkeleja ja kirja-arvosteluja etenkin sotilasalan lehtiin jatkuvasti vuodesta 2008 alkaen.

Jarkko Pellikka, Program Director, Nokia Mobile Networks

Jari Collin, Adjunct Professor, Aalto University ja CTO, Telia Finland

Jyrki Penttinen, Technology Manager, GSMA North America

Teollinen 5G ja yksityisverkot

Matkaviestinnän viidennen sukupolven käyttöönotto edistyy vauhdilla. 4G:n ja 5G:n yhdistelmäverkkojen (NSA, non-standalone) yleistyessä myös itsenäiset 5G-verkot (SA, standalone) ovat saaneet vahvasti jalansijaa. 5G:n hyödyt alkavat siten näkyä konkreettisesti kuluttajille samoin kuin yrityksille ja teollisille käyttäjäryhmille nopeampien datayhteyksien lisäksi myös uusina digitaalisina palveluina. Samalla 5G alkaa profiloitua yhä selkeämmin alueilla, jotka hyötyvät sen uudesta verkkoarkkitehtuurista ja kehittyneistä toiminnoista, päivitetystä tietoturvasta ja mahdollisuudesta palvella uusia kohderyhmiä kuten yritysasiakkaita joustavammin kuin aiemmat järjestelmien sukupolvet. 5G mahdollistaa samalla uudistettuja järjestelmäarkkitehtuurimalleja yksityisverkkojen käyttöönottoon, ja ne voivat soveltua erityisen hyvin teollisuuden reaaliajassa tapahtuvaan dataliikenteen ja -laskennan tarpeisiin varmistaen tietoturvalliset palvelut. Uusia 5G-yksityisverkkomalleja voidaan soveltaa myös maanpuolustuksen nopeasti muuttuviin tilanteisiin.

Taustaa

5G:n käyttö on yleistynyt Suomessa vahvasti, joskin maailmanlaajuisesti 4G edustaa suosituinta matkaviestinnän sukupolvea vielä lähivuosien ajan. GSMA:n Mobile Economy 2023 -raportin päivitettyjen ennusteiden mukaan 5G-käyttäjien lukumäärä ylittää 4G-tilaajapohjan vuoden 2028 aikana, ja vuonna 2030, 5G-tilaajien suhteellinen lukumäärä muihin sukupolviin nähden on jo 54% verrattuna 4G-, 3G- ja 2G-verkkojen vastaaviin suhteellisiin arvoihin 36%, 8% ja 1%.

Samalla, kun 5G:n käytön kasvu jatkuu tasaisesti ja sen suhteellinen käyttö nousee tällä vuosikymmenellä noin viiden prosenttiyksikön verran vuositasolla, 5G-sovelluksia, jotka perustuvat uuden sukupolven toimintoihin ja suorituskykyyn, kehitetään kiihtyvän tahtiin. Matkaviestintäpalveluiden tilaajat toki hyötyvät 5G:n korkeammista datanopeuksista, mutta on nähtävissä, että 5G voi palvella erityisen tehokkaasti yritysmaailmaa ja teollisuutta. Esimerkiksi tuotantolaitokset ja tehtaat ovat erityisen mielenkiintoisessa asemassa langattomien kytkentäpalveluiden laajentuessa kattamaan matkaviestintäpalveluita aiempien Wi-Fi- ja muiden ei-solukkoverkkopohjaisten järjestelmien rinnalle.

Yhtenä esimerkkinä 5G:n hyödyistä yritysmaailmassa on sen mahdollistama alhaisempi viive (latency) sekä korkeampi luotettavuus (reliability). Nykyiset 3GPP-spesifikaatiot, Release 17:n jo ollessa valmis, mahdollistavat teoreettisen viivearvon 1 ms sekä luotettavuuden 99.9999 %. Nämä parannukset näkyvät myös käytännössä siten, että verrattuna aiempaan 4G-suorituskykyyn, 5G-verkot tarjoavat keskimäärin nopeampia datayhteyksiä ja vasteaikoja niillä radioverkon palvelualueilla, joissa uuden sukupolven toiminnot ovat tarjolla. Toinen tärkeä seikka on 5G:n ehostettu tietoturvallisuus, jota voidaan hyödyntää esimerkiksi korkean suojaustason 5G-pohjaisissa yksityisverkoissa.

5G:n erilaiset käyttötarkoitukset eri toimialoilla eli vertikaaleilla vaatii verkkosuunnittelussa teollisuuden käyttöympäristöjen dataliikennöintitarpeiden entistä tarkempaa ymmärtämistä ja huomioonottamista. Tämä ei ole välttämättä yksinkertaista, sillä operaattorit ovat tottuneet matkaviestintätilaajakeskeisiin suunnittelukriteereihin. Uusien, potenti-

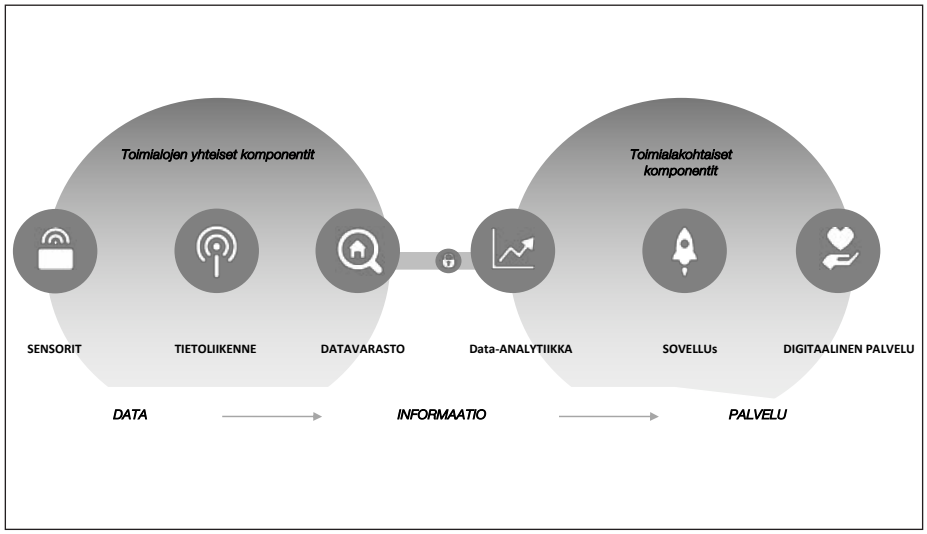
aalisten vertikaalien tietoliikenteelle asettamat vaatimukset voivat erota merkittävästi yksityis- ja yrityskäyttäjien data- ja puhepalveluiden profiileista. Esimerkkinä, öljy- ja kaasuteollisuudessa on tärkeää ottaa huomioon kriittiset prosessit sekä ennakoida ja minimoida tapaturmien mahdollisuus, mikä vaatii erityisen luotettavaa sensoriverkkoa ja jatkuvaa, korkean luotettavuuden valvontayhteyttä.

Teollisen 5G-ratkaisun tärkein arvo syntyy, kun data muutetaan reaaliajassa merkitykselliseksi tiedoksi ja digitaalisiksi palveluiksi. 5G-teknologian avulla voidaan tätä parantaa infrastruktuurin kaikissa osissa, vaikka sen uudet ydinominaisuudet keskittyvätkin tietoliikenteeseen. Kuten kuva 1 koostaa, yleisiä komponentteja, jotka ovat yhteisiä eri toimialoilla, ovat sensorit, tietoliikenne ja datan varastointi. Nämä osakokonaisuudet ovat jo hyvin standardoituja. Suurin asiakasarvo syntyy kuitenkin data-analytiikasta, sovelluksista ja digitaalisista palveluista, jotka puolestaan ovat toimialakohtaisia ja räätälöityjä. Näille osille ei ole olemassa standardia tai yhteistä ratkaisua. Siksi niiden käyttöönotto voi usein vaatia ylimääräistä järjestelmäintegraatiotyötä.

Suomessa on tätä aihepiiriä pohdittu Aalto yliopiston koordinoimassa tutkimusohjelmassa ”5G innovaatiot teollisuuden digitalisaation kiihdyttämiseksi”. Ohjelma on hiljattain koostanut tutkimusraportteja aliprojekteista, joissa yhteistyökumppanit tutkivat ja testasivat teollisen 5G:n käytettävyyttä omissa erikoisympäristöissään. Ohjelmassa käsitellyt teemat ja tulokset on koostettu pian julkaistavaan kirjaan ”5G Innovations for Industry Transformation – Data Driven Use Cases”. Tämä artikkeli valottaa tutkimuksen avainlöydöksiä.

Tutkimus käsitteli teollisuuden digitaalista murrosta ja datavetoisia digitaalisia palveluja, joiden hyödyntämistä ja käyttöönottoa voidaan kiihdyttää 5G-teknologian avulla. Tutkimus on tehty tulosten ja käytännön kokemusten perusteella siitä, miten uutta mobiiliteknologiaa voidaan hyödyntää teollisuuden digitaalisessa murroksessa.

Tutkimuksen tavoitteena oli kuvata datavetoisia teollisuuden käyttötapauksia, jotka hyödyntävät 5G-teknologiaa asiakasarvon, tuottavuuden ja kestävän kehityksen edistämiseksi valituissa teollisissa ekosysteemeissä. Tutkimuksessa on ollut mukana viisi eri toimialaa: kaivos-, metsä-, rakennus/hissi-, televiestintä- ja öljynjalostusteollisuus, joista jokaisessa on alan edelläkävijä case-yritys.



Teollisen 5G:n osa-alueet ja digitaalisten palveluinnovaatioiden synnyttäminen.

Tutkimuksen näkökulmana on teollisuusyritys, joka etsii uusia liiketoimintamahdollisuuksia teollisen 5G:n avulla. Oppien ja parhaiden käytäntöjen jakaminen eri toimialojen välillä on olennainen osa tuloksia.

5G:n standardointi

5G standalone

Uuden sukupolven ”täysverinen” versio on 5G standalone (SA) eli kokonaisuudessaan 5G-spesifikaattioihin perustuva erillinen verkkoratkaisu. Siinä, kun 5G:n ensimmäinen käyttöönottovaihe, NSA (non-standalone), on sisältänyt tyypillisesti yhdistelmän 4G-komponentteja (4G- ja 5G-tukiasemia joko 4G- tai 5G-kytkentäverkkoon liitettyinä), 5G SA on puhtaasti 5G-tukiasemiin ja 5G-kytkentäverkkoon pohjautuva ratkaisu. 5G SA toki voidaan liittää aiempiin 4G-verkkoihin siten, että esimerkiksi 5G-radion palvelukatveessa yhteysvastuun vaihto onnistuu olemassa olevaan verkkotekniikkaan, mutta verrattuna 5G NSA -ratkaisuihin, 5G SA mahdollistaa täyden yhdistelmän uuden sukupolven hyödyistä ml. korkeimmat mahdolliset datanopeudet sekä uudet 5G-verkkopalvelut.

5G-pohjaiset yksityisverkot

Yritysten ja teollisuuden yksityisverkko on perusteltu monesta näkökulmasta. Esimerkkinä, yritys voi käsitellä luottamuksellista tietoa, jota ei halua paljastettavan oman sisäisen verkon ulkopuolelle siitä huolimatta, että tieto voidaan suojata koko reitillä sovellustasolla ja taltioida esimerkiksi kolmannen osapuolen pilveen vaikkapa julkiseen ja yksityiseen avainpariin perustuvilla salausmenetelmillä. Toinen mahdollinen syy sisäisen verkon tarpeeseen saattaa olla yrityksen toive hallita verkkoratkaisua itsenäisesti, jolloin sen ylläpito ja päivitys ovat riippumattomia ulkopuolisista toimijoista. Kolmantena esimerkkinä, mikäli yritys käyttää omia (pilvi)palvelimia fyysisesti lähellä toimitilojaan ja oman yritysverkon kautta, on niiden resursseihin mahdollista kytkeytyä hyvin nopeasti.

Perinteisesti, yritysten ja teollisuuden sisäinen verkko voidaan toteuttaa lukuisilla tekniikoilla, joista esimerkkinä on Wi-Fi-pohjainen tai muu pienitehoisista langattomista kytkentäpisteistä koostuva rajoitetun alueen verkko. Sisäisiä yritysverkkoja on myös toteutettu jo NMT:n ajoista lähtien operaattoripalveluna määrittämällä osa julkisen matkaviestintäverkon kapasiteetista yrityksen käyttöön esimerkiksi luomalla rajattuja käyttäjäryhmiä.

4G:n ja 5G:n myötä 3GPP on luonut myös uusia verkkoarkkitehtuurimalleja, joka toteuttavat yritysverkkojen tarpeita erityisen hyvin, ml. tietoturva sekä entistä optimaalisempi verkkoelementtien ja -resurssien jako. 5G on saanut erityisaseman tässä kehityksessä, ja lopputuloksena 3GPP-spesifikaatiot mahdollistavat uusia teknistaloudellisesti tehokkaita malleja.

3GPP:n spesifikaatiosarja Release 16 niputtaa yksityisverkkomallit kategoriaan “ei-julkinen verkko” (NPN, non-public network). Kuvan 2 mukaisesti yksityis-

verkko voi olla täysin eristetty (SNPN, standalone NPN), tai jaettu yrityksen ja operaattorin kesken (PNI-NPN, public network integrated NPN).

3GPP-spesifikaatiot mahdollistavat uudet menetelmät luomaan yksityisverkkoja myös teollisen IoT:n tarpeisiin (IIoT, industrial Internet of things), esimerkiksi matkaviestintäjärjestelmän liitynnän aikasensitiivisiin verkkoihin (TSN, time sensitive network), sekä muihin kuin 3GPP:n määrittämiin verkkoihin kuten paikallisverkkoihin (LAN, local area network). Julkaisusarja Release 17 ja sen jälkeiset versiot kehittävät tätä aihealuetta edelleen.

3GPP:n määrittäessä teknisen perustan yksityisverkkojen tukeen matkaviestintäjärjestelmien kautta, myös monet teollisuuden foorumit täydentävät niiden käyttöönoton ohjeistusta. Esimerkkinä näistä toimijoista on 5G-ACIA (5G Alliance for Connected Industries and Automation), joka on koostanut teollisen IoT:n käyttöönottovaihtoehtoja perustuen 5G NPN -arkkitehtuurimalleihin. Toinen merkittävä toimija on matkaviestintäoperaattoreiden edustukseen keskittynyt GSMA (GSM Association), joka on tuottaa ohjeita NPN-verkkojen teknisiin ja tuotannollisiin näkökohtiin. Esimerkkinä, GSMA:n Pohjois-Amerikan verkkoryhmä (NANG, North America Network Group) työstää parhaillaan teknistä ohjeistusta 3GPP-yksitysverkkomalleja evaluoimalla.

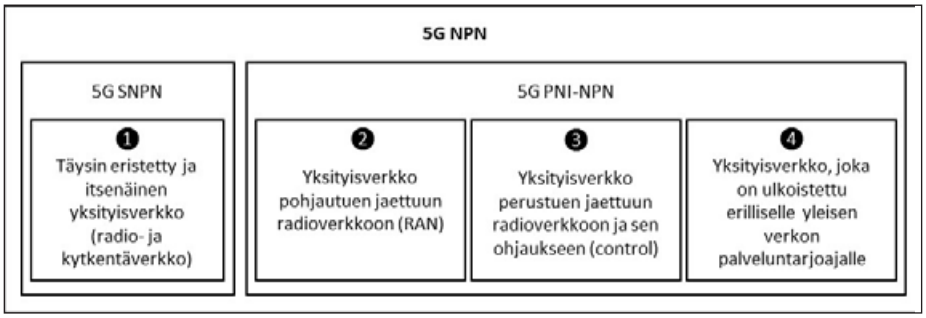
3GPP määrittää NPN-perustan teknisissä spesifikaatioissa TS 23.251 (verkkoresurssien jaon arkkitehtuuri ja toiminnallisuus), TS 22.104 (vertikaalisovellusten ohjaus- ja palvelunäkökulmat) ja TS 23.501 (5G:n järjestelmäarkkitehtuuri).

Yksityisverkkojen käyttöönotto teollisessa ympäristössä

Teollinen 5G-verkkoratkaisu voidaan toteuttaa monella tavalla, kuten yksityisenä 5G-verkkona, virtuaalisena 5G-yksityisverkkona ja 5G-verkkoviipaleena (network slice). Kuva 3 koostaa kuvassa 2 esitettyjen neljän ratkaisun arkkitehtuurimallien periaatteet. Kuvassa olevat 5G-kytkentäverkon (5GC, 5G core) avainverkkotoiminnot (network function, NF) ovat seuraavat:

UPF: datatason toiminto (user plane function) datan reititykseen 5G-verkon ja ulkopuolisten komponenttien välillä.

UDM: datanhallintatoiminto (unified data management) esimerkiksi käyttäjän profiilien taltiointiin ja hallintaan.



3GPP:n määrittämät 5G-yksityisverkkojen kategoriat.

5G-verkko voidaan kytkeä UPF-komponentin kautta esimerkiksi dataverkkoon (DN, data network), reunalaskentapilveen (MEC, multi-access edge computing), tai Wi-Fi-pääsypisteisiin. On huomattava, että yksityiskohtaisessa 5G-kytkentäverkossa on joukko muitakin verkkotoimintoja, mutta tässä esitetyt ovat oleelliset yksityisverkkojen omistajuuden ja hallinnan jaon kannalta. Toisin sanoen, yritys voi hallita koko 5G-verkkoaan mukaan lukien tilaajalaitteet (UE, user equipment), 5G-tukiasemat (gNB, next generation nodeB) ja 5G-kytkentäverkko, tukeutua täysin ulkoistettuun palveluun verkkopaloittelun kautta, tai toteuttaa jaetun radioverkon strategian. Kullakin mallilla on hyötynsä ja heikkoutensa, ja valinta tapahtuu arvottamalla toteutuksen kokonaiskustannukset (verkon rakennus ja operointi), tietoturvallisuus, saavutettava laatu (ml. datanopeus, viive), muiden näkökulmien ohella.

Yksityinen 5G-verkko

Yksityinen, eristetty 5G-verkko, eli SNPN (standalone non-public network), on 5G-teknologiaan perustuva langaton verkko, joka on omistettu tietylle teollisuusyritykselle valitussa fyysisessä paikassa. Pääsy verkkoon on rajoitettu ennalta määritetyille käyttäjille yrityksen palomuuriasetuksissa. Verkkoinfrastruktuurin omistaa, hallinnoi ja ylläpitää yritys itse. Eristettyjen yksityisverkkojen avulla teollisuusyritykset voivat hallita verkkoresurssejaan ja turvallisuuttaan, jolloin ne voivat mukauttaa verkkojaan omien erityisvaatimustensa mukaan. 5G-tekniikka tarjoaa verkon omistajalle aiempiin sukupolviin nähden parempia turvaominaisuuksia, sillä 3GPP on uusinut tietoturva-arkkitehtuurin uudelle tasolle.

Omaan yksityiseen 5G-verkkoonsa investoivat teollisuusyritykset pitävät täyttä hallitsevuutta pakollisena vaatimuksena ml. maksimaalinen liiketoiminnan jatkuvuus, turvallisuus, minimaalinen viive sekä verkon hallinnan kaikinpuolinen joustavuus kyseisessä toimipaikassa. Tämän ansiosta suurta kaistanleveyttä ja pientä viivettä vaativat teolliset sovellukset voivat toimia saumattomasti. Yksityisverkko mahdollistaa verkkoarkkitehtuurin räätälöinnin ja uusien palveluiden nopean käyttöönoton tarpeen mukaan.

Yksityisverkon suorituskykyedut takaavat luotettavat ja nopeat yhteydet käyttäjille ja laitteille varmistaen, että kriittiset tiedot voidaan siirtää nopeasti ja turvallisesti. Yksityiset 5G-verkot voivat tarjota käyttäjille pienemmän viiveen kuin julkiset 5G-verkot, koska käyttäjätietojen laskenta tapahtuu paikan päällä. Tämä on tärkeää reaaliaikaisia vastauksia vaativissa teollisen Internetin sovelluksissa, kuten autonomisissa ajoneuvoissa ja prosessiautomaatiossa.

Käyttötutkimukset vahvistavat teollisuusyritysten kasvavan kiinnostuksen 5G-yksityisverkkoihin, ja uusien verkkojen käyttöönotto todennäköisesti yleistyy lähivuosina. Tällä hetkellä pelkästään Saksassa on jo yli 320 yksityistä verkkoa, jotka käyttävät 5G-teknologiaa.

Virtuaalinen 5G-yksityisverkko

Kevyempi tapa hyödyntää yksityisverkkojen hyötyjä on ns. virtuaalinen 5G-yksityisverkko eli alueellisesti eristetty verkkokapasiteetti julkisesta verkosta tietylle teollisuusyritykselle ja/tai -alueella. Tämä suljetun käyttäjäryhmän luonti hyödyntää julkista 5G-verkkoa ja sen reunalaskentamahdollisuuksia teollisuuslaitoksen läheisyydessä. Näin varmistetaan, että teollisuusyrityksellä on suhteellisen matalaviiveinen vasteaika sekä riittävän suuri verkkokapasiteetti. Toinen tärkeä näkökohta on se, että teollisuuslaitoksen ja liikkuvan reunan välillä on vain turvattuja yhteyksiä ja tietoja ei siirretä julkisen Internetin kautta. Suurin osa turvallisuusvaatimuksista voidaan hallita tällä järjestelyllä.

Virtuaalinen 5G-yksityisverkko on suojattu ja salattu yhteys, jonka avulla käyttäjät voivat käyttää yksityistä verkkoa julkisen verkon kautta. Se luo yksityisen verkon käyttämällä salaus- ja tunnelointiprotokollia luodakseen suojatun yhteyden kahden pisteen välille, jolloin käyttäjät voivat muodostaa yhteyden etäverkkoon turvallisesti ja nimettömästi. Oma verkkokapasiteetti on varattu yrityksille, joilla ei ole suuria investointeja omaan paikalliseen privaattiverkkoon teollisuusalueella. Latenssia voidaan pitää paljon pienempänä kuin normaaleissa julkisissa verkoissa, koska laskenta tapahtuu mobiilireunalla, joka sijaitsee sivuston läheisyydessä.

Virtuaaliset 5G-yksityisverkot ovat turvallinen ja kustannustehokas menetelmä, joka mahdollistaa suljetut yhteydet edullisemmin, kuin omaan yksityisverkon infrastruktuuriin investoimalla. Tämä lähestymistapa sopii teollisuusyrityksille, jotka pitävät turvallisuutta ja matalaa latenssia ratkaisevina tekijöinä, mutta joiden vaatimukset eivät estä julkisen 5G-verkon mobiilireunaominaisuuksien hyödyntämistä.

5G-verkkoviipale

Kustannustehokas ja yksinkertainen tapa hankkia rajallisia 5G-privaattiverkkovalmiuksia on verkon viipalointi (network slicing), joka on uusi kyvykkyys 5G-teknologiassa. Sen avulla operaattorin tietty verkkoviipale tai eristetty kapasiteetti voidaan varata yritykselle halutussa paikassa ja määritetyksi ajaksi. Tämä on tehokas ja joustava tapa varata kapasiteettia julkisen 5G-verkon kautta. Verkon viipalointi on osa verkkoarkkitehtuuria, joka mahdollistaa virtualisoitujen ja autonomisten loogisten verkkojen yhteiskäytön saman fyysisen verkkoinfrastruktuurin sisällä. Kukin operaattorin verkkoviipale näyttää käyttäjilleen omana eristettynä päästä päähän -verkkona, joka on räätälöity täyttämään sitä käyttävän sovelluksen erityisvaatimukset. Julkisen verkon viipalointi ei kuitenkaan takaa erityisiä viive- ja turvallisuusvaatimuksia, koska niiden palvelutasot riippuvat julkisen 5G-verkon asetuksista.

Verkkoviipaloinnin avulla yksittäisen operaattorin matkaviestintäverkko voidaan siis jakaa useisiin loogisiin verkkoihin, joilla on omat resurssit ja ominaisuudet, ja jotka voidaan räätälöidä vastaamaan eri sovellusten ja palveluiden erityisvaatimuksia. Jokaisella komponentilla on omat ainutlaatuiset ominaisuutensa, kuten kaistanleveys, viive ja suojaustasot, jotka voidaan mukauttaa tietyn palvelun tai sovelluksen tarpeiden mukaan.

Verkon viipalointi on joustava ja tehokas tapa tukea monenlaisia, eri vertikaalien käyttökohteita. Sen avulla viestintäpalvelujen tarjoajat voivat kohdistaa resursseja dynaamisesti vastaamaan eri palveluiden, sovellusten ja käyttäjien vaatimuksia reaaliajassa kysynnän muuttuessa. Esimerkiksi verkkoviipale voidaan luoda dynaamisesti teollisuusyritykselle, joka tarvitsee tehokkaan ja omistautuneen verkon liiketoiminnan kannalta kriittisille sovelluksille tietyssä toimipaikassaan tai toimipaikoissaan. Tämä uusi verkko-ominaisuus mahdollistaa paremman palvelun laadun ja taatun verkon suorituskyvyn.

Tämä lähestymistapa sopii teollisuusyrityksille, jotka pitävät verkon kapasiteettia ratkaisevana tekijänä langattoman verkon tarpeidensa täyttämisessä. 5G-palvelutason parantuessa tietyille teollisuuslaitoksille aiheutuu kuitenkin lisäkustannuksia, jotka on otettava huomioon eri lähestymistapoja vertailtaessa. Lisäksi verkon viipaloinnin toteuttamisessa on tärkeää huomioida turvallisuuden periaatteet, kuten “älä koskaan luota, varmista aina”, monikerroksinen tietoturva sekä järjestelmien uudet salausteknologiat, joihin kaikkiin yksityisten verkkojen viipalointi antaa käyttäjilleen hyvät mahdollisuudet.

Käyttöönoton esteet

Teollisen 5G:n käyttöönotto ei ole suoraviivaista, koska se on sidoksissa moniin teollisiin prosesseihin ja järjestelmäalueisiin. Teollinen 5G koskettaa myös prosessien ja järjestelmien integrointia tuotannon automaatiojärjestelmien ja muun IT:n välillä. Perinteisesti teollisuudessa käsitellään operaatioteknologiota (OT) ja IT-järjestelmiä kahtena erillisenä alueena, pitäen erilliset teknologiapinot, protokollat, standardit, hallinta ja organisaatioyksiköt. Vanhojen prosessien ja työkalujen modernisointi voi johtaa melkoiseen monimutkaisuuteen, viivästyksiin toteutuksessa ja kustannusten nousuun. Kyberturvallisuusriskit ja riittämättömät taidot voivat myös muodostua täytäntöönpanon pullonkaulaksi.

Teollisuusalojen näkökohtia

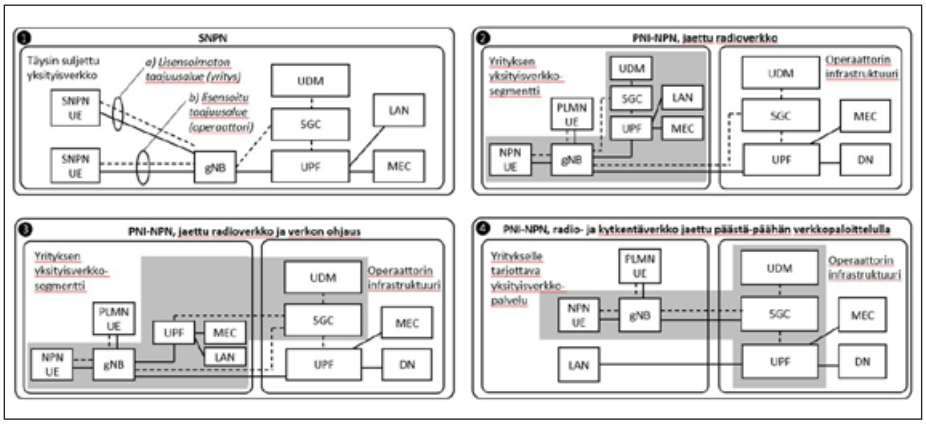
Kaivosteollisuus: Case Sandvik

Tämä tapaustutkimus edustaa kaivosteollisuutta, jossa digitalisaatio etenee vauhdilla kaivoksissa ympäri maailmaa. Autonomisten ajoneuvojen langaton etäohjaus on jo todellisuutta, mutta ekosysteemi ei vielä välttämättä tiedosta, mitä hyötyjä ja uusia mahdollisuuksia 5G-teknologia voi mahdollistaa langattomien ratkaisujen rakentamisessa, käytössä ja ylläpidossa kaivosalueilla sekä maan alla että maan päällä.

Yksityiskohtaisten mittaustulosten pohjalta voidaan todeta, että 5G mahdollistaa selkeitä parannuksia tiedonsiirron luettavuuteen, kapasiteettiin ja viansietoisuuteen Wi-Fi teknologiaan verrattuna. Perinteisesti matkapuhelinverkot on suunniteltu ja rakennettu optimoimaan matkaviestinten vastaanottosuunnan downlink-kapasiteettia. Kaivosympäristössä toimittaessa maan alla matkaviestinten lähetyssuunnan uplink-suorituskyky on kuitenkin tärkeämpää, koska koneet, ajoneuvot ja IoT-sovellukset lähettävät reaaliaikaista tietoa maan alta maanpäälliseen valvomoon. Tässä 5G tarjoaa merkittävän parannuksen aikaisempiin teknologioihin verrattuna. Toinen tärkeä osa-alue on yhteyksien luotettavuudessa, jolla tarkoittaa keskeytyksetöntä kaivostoimintaa ilman häiriöitä: korkea siirtonopeutta voidaan hyödyntää täysimääräisesti ja automatisoidut koneet toimivat keskeytyksettä.

Uudet 5G-sovellukset tehostavat reaaliaikaisia datayhteyksiä ja videosovellusten käyttöönottoa kaivoksissa. 5G-verkko ei yksin nopeuta digitalisaatiota, vaan päätelaitteiden ja sovellusten kehitys on tulevaisuudessa ratkaisevassa roolissa. Turvallisten 5G-laskenta-alustojen kyvykkyyksien parempi hyödyntäminen

luo mahdollisuuksia rakentaa integroituja operointiteknologioiden (OT) ja informaatioteknologioiden (IT) ratkaisuja, jotka perustuvat mobiiliin reunalaskentaan (edge computing) perinteisillä rajapinnoilla. Yhtenäinen, tietoturvallinen verkko- ja laskentakapasiteetti muodostaa data-alustan kaivosteollisuuden digitalisaation seuraaville vaiheille, ja 5G avaa täysin uusia tapoja parantaa turvallisuutta vaarallisessa työympäristössä esimerkiksi mahdollistamalla reaaliaikaisen tilannekuvan muodostamisen video- ja audio-dataa hyödyntämällä.



Kuva 3. 3GPP-pohjaisten 5G-yksityisverkkojen arkkitehtuuri. Harmaalla merkitty alue esittää niitä verkkotoimintoja, jotka voidaan tarjota verkkopaloittelulla.

Metsäteollisuus: Case Metsä Group

Tapaustutkimus edustaa metsäteollisuutta, jossa prosessiautomaation jatkuva tuottavuuden parantaminen on kilpailukykyisen tuotanto- ja turvallisuustoiminnan ytimessä. Metsä Group edustaa suomalaista metsäteollisuutta, ja tapaustutkimus keskittyi 5G:n mahdollisuuksiin ja esteisiin tuottavuuden parantamisessa nykyaikaisessa biotuotetehtaan toiminnassa. Keskeinen kysymys 5G:n soveltamisessa on, miten tehostaa biotuotetehtaan toimintaa tuotannossa, kunnossapidossa ja turvallisuudessa.

5G mahdollistaa koko tehdasalueella langattoman, reaaliajassa tapahtuvan videoanalytiikan hyödyntämisen aivan uudella tasolla. Sen avulla voidaan muuttaa metsäteollisuuden tuotantoprosesseja entistä digitaalisemmiksi, turvallisemmiksi ja saavuttaa uusia tuottavuusparannuksia uusien automaatiokäyttötapausten kautta. Uusien teknologien käyttöönotto ei ole mikään suoraviivainen asia, vaan siihen liittyy käytännön esteitä, jotka pitää tunnistaa ja poistaa ennen kuin uusia mahdollisuuksia voidaan täysimääräisesti hyödyntää. Tapaustutkimuksessa tunnistetut esteet analysoitiin ja arvioitiin uusien käyttötapausten valossa.

Rakennusteollisuus: Case Kone

Tämä tapaustutkimus edustaa maailmanlaajuista hissiteollisuutta, ja case-yhtiö on Kone, yksi maailman johtavista hissiteknologiayrityksistä. Tutkimus keskittyy rakennusten, erityisesti korkeiden kerrostalojen rakennusvaiheeseen, jonka aikana älykkäät hissit voivat tarjota rakentamisen ekosysteemille yhteisen digitaalisen alustan työmaalogistiikan optimoimiseksi. Rakennusalan tunnettu tuottavuuden pysähtyneisyyden ongelma on saanut yritykset etsimään uusia innovatiivisia tapoja hyödyntää digitalisaatiota ja uusimpia teknologioita, kuten 5G:tä ja reunalaskentaa. Keskeinen kysymys on ymmärtää, miten rakentamisen ekosysteemin toimijoille voidaan tarjota joustavasti yhteinen, reaaliaikainen data-alusta rakennustyömaihin liittyvälle logistiikkatiedolle.

Standardi API-ratkaisuihin pohjautuva reaaliaikaisen tiedon jakaminen toimijoiden välillä voi parantaa merkittävästi materiaali- ja ihmisvirtoja rakennusvaiheessa. Videokameroiden käyttö hissivaunuissa ja -auloissa käytön seuraamiseksi laajentaisi käyttötapausta. Hissikuilukameroita voidaan käyttää myös hissien kunnon seurantaan rakennusvaiheissa.

Tällä periaatteella esimerkiksi videovalvontajärjestelmiä ja niiden kuvamateriaalia voitaisiin käyttää yhtenä tietolähteenä hissiliikenteen priorisoinnissa, ja reaaliaikaisen materiaalin hyödyntäminen analytiikassa auttaisi ymmärtämään ihmisvirtaa osana suurempaa kuvaa. Olemassa olevien lähteiden analysointi yhdistettynä mobiiliin reunalaskentaan olisi tässä ympäristössä järkevää, ja 5G-teknologian suorituskyky olisi hyödyksi monissa käyttötapauksissa varmistaen mm. luotettavan yhteyden etätukikeskukseen korjausta ja huoltoa silmällä pitäen.

Eräs malli voisi olla, että sovelluskehitys tapahtuisi julkisessa AWS-pilvessä konttiratkaisuna, ja sen jakelu voitaisiin toteuttaa automaattisesti lähimpään mobiilireunaan sivuston käyttäjille. Tämä järjestely varmistaisi nopean kehityksen sovellusliittymien avulla ja maksimoisi sovellusten suorituskyvyn, ml. vaadittava alhainen viive ja riittävän suuri kapasiteetti.

Tietoliikenneteollisuus: Case Telia Finland

Tämä tapaustutkimus edustaa televiestintäalaa, jossa energiankulutus kasvaa jatkuvasti siirretyn tiedon määrän kasvaessa. Tapaustutkimuksessa selvitetään 5G- ja 4G-verkkojen energiatehokkuutta ja niiden vertailua tutkitaan verkkodata-analyysin avulla. Toimialan yksi suurimmista haasteista on varmistaa, että 4G/5G-radioverkkojen kuluttama energia ei kasva datavirtojen tahdissa. Tutkimus sivuaa kysymystä, miten eri järjestelmäkomponenteista saatavaa reaaliaikaista dataa voidaan hyödyntää 5G-verkon, reunalaskennan ja asiakkaiden teollisten prosessien energiatehokkuuden parantamisessa.

Mobiiliverkoissa jatkuvasti kasvussa oleva tietomäärä luo suuren muutoshaasteen televiestintäalalle, johon 5G energiatehokkuusparannukset tarjoavat ratkaisuja. Ne voidaan jakaa kahteen osa-alueeseen: energiatehokkuuden parantamiseen laitteiden tehokkuutta parantamalla ja reaaliaikaisen datan hyödyntämiseen verkon optimoinnissa. Tutkimusdata osoittaa, että 5G teknologia mahdollistaa merkittävät parannukset molemmissa luokissa.

Kun dataa siirtyy tukiaseman läpi tietyn kynnyksen yli, 5G on paljon energiate-

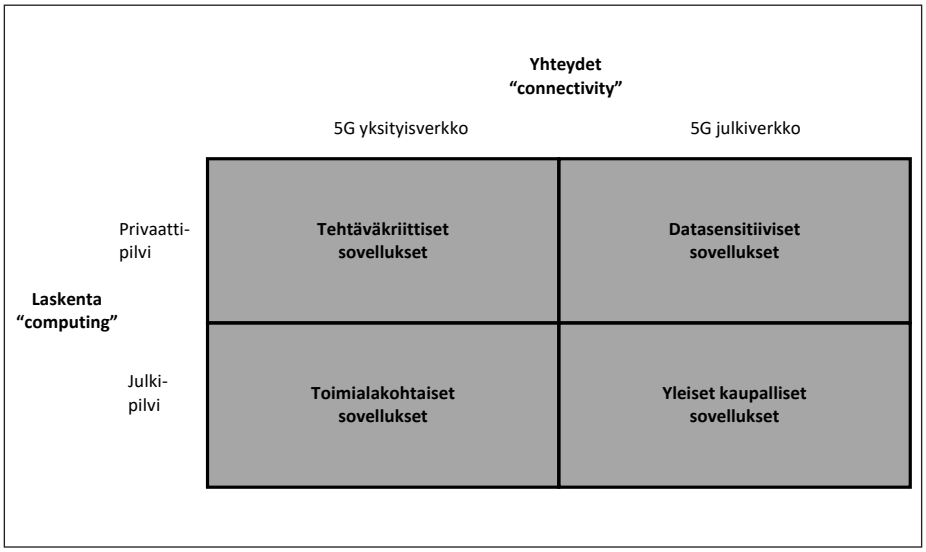
hokkaampi kuin 4G. Teollisuusympäristöissä tämä raja ylittyy helposti, kun teollisen 5G:n sovellukset siirtävät jatkuvaa videokuvaa verkon yli. Reunalaskenta tarjoaa merkittäviä parannuksia energiatehokkuuteen teollisissa sovelluksissa, joita ei voida siirtää julkiseen pilveen viiveen ja tietoturvarajoitusten vuoksi. Dataohjatuilla koneoppimisalgoritmeilla on iso potentiaali verkon suunnittelussa sekä suorituskyvyn että energiatehokkuuden parantamiseksi.

5G, reunalaskenta ja datavetoinen lähestymistapa energiatehokkuuteen ovat olennaista toimialan energiatehokkuuteen ja vastuullisuuteen liittyen. Ympäristövaikutukset minimoivat 5G liittymätyypit tulevat tulevaisuudessa olemaan vastuullisuustietoisille asiakkaille tapa pienentää oman toimintansa hiilijalanjälkeä. Televiestintäalan kaikki 5G teknologian mahdollistamat positiiviset ympäristövaikutukset ovat vielä tunnistamatta ja työ siltä osin jatkuu, kun uutta empiiristä tutkimusaineistoa saadaan kerättyä ja analysoitua.

Öljy- ja kaasuteollisuus: Case Neste

Tämä tapaustutkimus edustaa öljy- ja kaasuteollisuutta, jolle on ominaista pitkän aikavälin kestävyystavoitteet kohti hiilivapaata tuotantoa. Kohdeyhtiö Neste on myös keskellä suurta uudistusta: siirtymää fossiilisesta öljystä uusiutuviin ja kiertotalouden ratkaisuihin. Digitalisaatio nähdään tärkeänä työkaluna teollisten prosessien uudistamisessa laajalla öljynjalostamoalueella, jossa miehittämättömiä ilma-aluksia, eli drooneja, voidaan hyödyntää putkistojen, laitosten ja infrastruktuurin valvonnassa ja videoanalytiikkaratkaisuissa niin ympäristöystävällisyyden, turvallisuuden kuin tuotantotehokkuuden lisäämiseksi. Teräväpiirtovideon reaaliaikainen suoratoisto yhdistettynä havaitsemisanalytiikkaan voi auttaa energiantoimittajia tunnistamaan riskit ja alkavat viat – kuten vuotavan putken. 5G-teknologia mahdollistaa lyhyt viiveisen langattoman viestinnän ja analytiikan uudelle tasolle.

Porvoon öljynjalostamolla toteutetun haastattelututkimuksen pohjalta tunnistettiin käyttötapauksia, joissa 5G-kytketyt droonit mahdollistavat uusia toimintatapoja jalostamon turvallisuuden, vastuullisuuden ja tehokkuuden parantamiseksi. Kameroilla ja antureilla varustettuja drooneja voidaan käyttää putkistojen, säiliöiden ja tornien tarkastamiseen,



Teolliset sovellukset vaativat erilaisia toteutusratkaisuja.

mikä tehostaa ajankäyttöä ja vähentää työntekijöiden tarvetta suorittaa vaarallisia tehtäviä. Niitä voidaan käyttää jalostamoiden valvontaan ja mahdollisten tietoturvaloukkausten tunnistamiseen. Niitä voidaan käyttää myös päästöjen ja muiden ympäristötekijöiden tarkkailuun. Drooneista voidaan tehdä jalostamosta 3D-karttoja, joita voidaan käyttää huoltojen ja korjausten suunnitteluun. Kerätyt tiedot voivat auttaa tunnistamaan huomiota vaativat alueet ja priorisoimaan korjaukset. Niitä voidaan käyttää myös pienten osien ja työkalujen toimittamiseen jalostamon työntekijöille. Tämä voi säästää aikaa ja lisätä tehokkuutta erityisesti suurissa ja monimutkaisissa jalostamoissa. Droonien käyttö voi siten parantaa merkittävästi jalostamojen turvallisuutta, tehokkuutta ja ympäristövaatimusten noudattamista.

On kuitenkin huomattava, että droonien käyttö on erittäin säänneltyä, ja lainsäädäntöä kehitetään edelleen. Säännöissä ja määräyksissä on harmaa alue, sillä multikopterityyppiset droonit ovat kehittyneet teknisesti nopeammin kuin niihin liittyvä lainsäädäntö, mutta kuilun umpeen kuromiseksi on tehty paljon työtä. Sen vuoksi sekä miehittämättömien ilma-alusten valmistajien että käyttäjien olisi otettava huomioon näiden lainsäädäntötoimenpiteiden odotetut vaikutukset.

5G:n soveltuvuus maanpuolustukseen

5G-ominaisuuksien käyttöönoton yleistyttyä käytännössä jo pikkuhiljaa teollisessa yritysmaailmassa, on 5G:n hyötyjä mahdollista arvioida myös muilla käyttöalueilla kuten maanpuolustuksen eri toiminnoissa. 5G-yksityisverkot toteutettuna uusien arkkitehtuurimallien mukaisesti voivat tarjota varsin käyttökelpoisen ympäristön nopeasti muuttuviin erityistilanteiden tarpeisiin parantamalla esimerkiksi operaatioiden koordinoinnin tehokkuutta ja päätöksenteon laatua kattavamman sekä reaaliaikaisen tilannekuvan avulla. Nykyaikainen 5G-yksityisverkko tarjoaa tarvittavan kapasiteetin hyödyntää ja tukea kenttäolosuhteissa tapahtuvaa henkilöstön ja logistiikan johtamista videoviestinnän ja muiden data-intensiivisten sovellusten avulla. Sen avulla voi suorittaa sotilas-, rajavalvonta- ja luonnonkatastrofeihin liittyviä operaatioita entistä tehokkaammin ja synkronoidummin.

5G-yksityisverkon luominen esimerkiksi verkkopaloitteluna – joko täysin erillisenä toteutuksena, jaettuna verkkoinfrastruktuurina paikallistoimijoiden ja maanpuolustuksen toimijoiden kanssa, tai täysin ulkoistettuna – voi tarjota erityisen merkittäviä hyötyjä esimerkiksi droonien käyttöön jatkuvasti muuttuvan tilannekuvan vaatiessa dynaamista verkon kapasiteettia. Tällainen erityisverkko voidaan toteuttaa esimerkiksi liikkuvien tukiasemien kautta, jotka tarjoavat radiopeittoaluetta suljetuille käyttäjäryhmille joko ajoneuvoihin asennettuina tai drooneihin kiinnitettyinä.

3GPP on myös määrittänyt ensimmäiset mallit 5G:n satelliittikomponentille, joka voi perustua satelliitin toistimeen tai satelliittiin asennettuun 5G-tukiasemaan. 3GPP tarkentaa Release 17:ssä esitettyjä konsepteja, joten 5G:n verkkoarkkitehtuurien kehittyessä, lähitulevaisuuudessa on mahdollista tukeutua siten myös käytännössä 5G-satelliittikomponenttiin varmentavana komponenttina.

Päätelmät

5G-teknologia on paljon muutakin kuin uuden sukupolven langaton tietoliikenneratkaisu. Se tarjoaa teollisuusyrityksille avoimen ja luotettavan digitaalisen alustan kiihdyttää operatiivisia reaaliaikaiseen dataan pohjautuvia uusia innovaatioita ja liiketoimintamalleja koko teollisessa ekosysteemissä. Tämä tietoturvallinen data-alusta perustuu globaalin standardin mukaiseen pilvipohjaiseen teknologiaan, joka pystyy joustavasti yhdistämään verkkoyhteydet (connectivity) ja laskennan (computing) erilaisia teollisia käyttötapauksia ja sovelluksia varten kaikkialla maailmassa. Kuten tapaustutkimuksemme osoittavat uudet 5G-ominaisuudet on suunniteltu vastaamaan erilaisten teollisten vertikaalien hyvin vaihteleviin tarpeisiin hyödyntäen privaatti- ja julkiratkaisuja – sekä verkkoyhteyksien että laskennan osalta. Erilaisiin käyttökohteisiin liittyviä sovelluksia voidaan toteuttaa usealla eri tavalla perustuen sovellusten käyttötarkoitukseen ja -ympäristöön.

Kuvassa 3 tiivistää, kuinka erilaiset sovellusalueet voidaan toteuttaa verkkoyhteyksien (kapasiteetti, nopeus ja viive) ja laskennan (datan sijainti, suvereniteetti, kybertuvallisuus) yhdistelmänä.

Eri sovelluksilla on erilaiset datan suojaus- ja yksityisyystasot sekä erilaiset vaatimukset verkon viiveen, kapasiteetin ja liiketoiminnan jatkuvuuden osalta. Siksi erilliset sovellukset pitää voida toteuttaa useilla eri tavoilla. Missiolle kriittiset sovellukset muodostavat perustan automatisoiduille teollisille prosesseille, joiden luotettavuus, jatkuvuus ja tietoturva pitää turvata rajoittamalla niihin pääsy privaattiverkkoyhteyksillä ja privaatilla pilviratkaisulla. Toinen luokka ovat datalle herkät sovellukset, jotka käsittelevät liiketoiminnan ja yksityisyyden kannalta arkaluonteisia tietoja ja joita pitää hallita vain privaattipilvipalveluissa, joilla ei ole pääsyä Internetiin tai Internetistä. Langattomat verkkoyhteydet voivat kuitenkin perustua julkiseen 5G-matkapuhelinverkkoon, koska siellä on luotettava kansallinen datasiirto ilman yhteyttä Internetiin. Julkiset pilvet soveltuvat joihinkin ei-kriittisiin teollisuusspesifisiin sovelluksiin, jotka toimivat yksityisverkossa teollisuusalueella. Nämä sovellukset on ensisijaisesti suunniteltu jakamaan dataa alan ekosysteemissä, ja siksi ne toteutetaan julkisessa pilvessä. Lopuksi, kaupallisia perussovelluksia, joita käytetään yleisesti ja laajasti eri paikoista, voidaan käyttää turvallisesti julkisten pilvien ja verkkojen kautta. On siis tärkeää hallita näitä eri käyttötarkoituksia kullekin sovellukselle ja pitää tietojen laadun elementit hyvässä kunnossa.

Tässä esitetyt esimerkkitutkimukset myös osoittavat, että hyvin suunniteltu ja koordinoitu yhteistyö toimialan ekosysteemissä on avainasemassa uusien teknologiakyvykkyyksien hyödyntämisessä. Teollisuuden digitaalisen murroksen mukanaan tuomat haasteet ovat monimutkaisia ja kyseenalaistavat perinteiset tavat johtaa ussien innovaatioiden käyttöönottoa. Teollinen 5G avaa toimialan ekosysteemeille mahdollisuudet synnyttää yhdessä uusia datavetoisia palveluinnovaatiota ja alustatalouteen pohjautuvia liiketoimintamalleja. Muutokset tulisi toteuttaa osana digitaalista transformaatiota ja siksi pyrimme tarjoamaan käytännön oppeja ja ohjeita, miten 5G-teknologiaa voidaan hyödyntää käytännössä.

Lopuksi tiedämme, että tutkimuksen tulokset tarjoavat vain pienen lisäyksen olemassa olevaan tietoon ja monet kysymykset jäävät vastaamatta. Siksi tarvitaan lisää ponnisteluja, tutkimusta ja ekosysteemiyhteistyötä, jotta teollisen 5G:n koko potentiaali voidaan hyödyntää.

Artikkelin kirjoittajat

TkT Jari Collin on vuodesta 2013 lähtien toiminut Aalto yliopistossa osa-aikaisena Adjunct Professorina pääalanaan yrityksen tietojärjestelmät ja palveluverkostot. Yliopistomaailmassa hän on viime vuosina ollut mukana teollisuuden digitalisaatio- ja 5G/6G- tutkimuksessa. Collinin varsinainen päätyö on Telialla, jossa hän toimii Telia Finland Oy:n teknologiajohtajana ja Infrastruktuuri -yksikön vetäjänä.

KTT Jarkko Pellikka johtaa Nokian teollisen 5G- ja reunalaskennan ratkaisuja kehittäviä ohjelmia. Molemmat ohjelmat tähtäävät tuottavuuden ja turvallisuuden kehittämiseen eri toimialoilla yhdessä yli 200 ekosysteemikumppanin kanssa. Hän on työskennellyt yli 20 vuotta teollisuuden automaation ja telealan liiketoiminnan kehittämisen sekä tutkimus- ja kehitysohjelmien vastuullisena johtajana. Hänen kokemuksiaan innovaatioiden johtamisesta ja kaupallistamisesta, liiketoimintamalleista ja uusien liiketoimintamahdollisuuksien kehittämisestä on julkaistu useissa tieteellisissä julkaisuissa ja kirjoissa.

TkT, ins-ltn (res) Jyrki Penttinen on toiminut telealalla vuodesta 1994 Suomessa, Espanjassa, Meksikossa ja Yhdysvalloissa. Penttinen työskentelee nykyään konsulttina Pohjois-Amerikassa pääaiheenaan 5G ja luennoi televiestintäteknologioista kansainvälisillä areenoilla. Penttisen julkaisuihin voi perehtyä blogissaan www.5g-simplified.com.

Lisätietoa artikkelissa esitetystä pian julkaistavasta kirjasta löytyy osoitteesta: https://www.whsmith.co.uk/products/5g-innovations-for-industry-transformation-datadriven-use-cases/jari-collin/jarkko-pellikka/hardback/9781394181483.html

TEXT: SILKE HOLTMANSS

Secure Usage of 5G in Military Scenarios

5G is being taken up by many industrial players and the defense sector also realised the opportunities 5G can bring. Often 5G is considered in combination with satellite communication to offer seamless communication to all defense entities and for a wide range of scenarios. The North Atlantic Treaty Organization (NATO) considers 5G and 6G as a "priority area" and an "emerging and disruptive technology" [1].

The NATO Communication and Information Agency (NCI) has identified four key areas for usage of 5G in defense scenarios [2]:

1. Deployable Communications and Information Systems (CIS) for expeditionary operations;

2. Tactical operations;

3. Maritime operations;

4. Static communication

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) identified in addition the usage and risks of 5G for military movements [3].

Many defense system vendors started prototyping usage of 5G for those scenarios. There activities on 5G enabled drones [4], unmanned ground vehicles [5], local networks [6], maritime communication [7], aircrafts [10], TETRA replacement [8], space [9], maintenance [11] and many more.

Having been working in industrial research for many years I understand the huge difference between a proof of concept and a final product. Typically, a proof of concept is created to explore the potential of a certain technology and evaluate its possibilities and usage areas. Security is rarely on the agenda for a prototype, but when moving towards a 5G defense product, it becomes the security elephant in the room.

Articles and announcements for 5G usage in military scenarios are often accompanied by a note of caution or some questions about the resilience and security of the system. After all, 5G is an open standard with APIs for sharing and not a secret proprietary technology. The defense sector is aware of the general security challenges related to usage of 5G and attempts are made to improve the situation. For example, funding is provided for a challenge created by NATO Defence Innovation Accelerator for the North Atlantic (DIANA) to foster innovation and startups to create a security industry that ensures the security of the new emerging and disruptive technologies [12].

While in the past many of the protocols and applications used for communication were proprietary and vendor specific 5G is a public standardized technology. Also, many scenarios involve the usage of public mobile networks e.g., to extend the coverage or to reduce costs. This is a major difference compared to previous communication technology approaches in the defense sector. 5G and telecommunication technology are still very specific technologies and expertise is rare, therefore many defense companies team up with mobile operators or vendors for their development [13], [14], [15].

The threats are also very specific and while in the past the concerns were mostly about radio jamming and interconnection spying attacks, the attack scenarios are now much more complex and diverse.

Each usage scenario has its own attack and risk profile. The risks depend on many factors, here are some:

- Interconnection with other systems (e.g., satellite, public networks, partner networks)

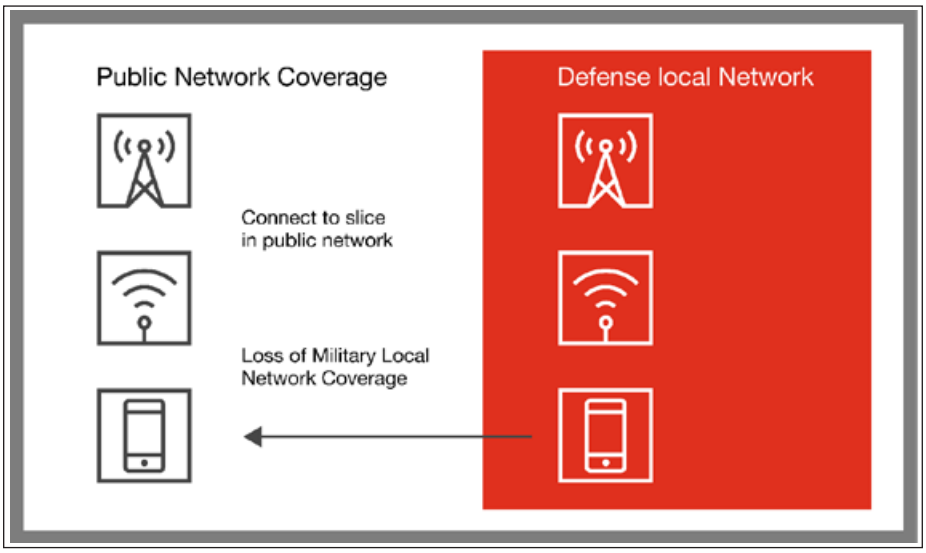
- Cloud usage

- Radio interception / jamming

- Legacy technology usage

- API security

- Supply chain (including Open Source)



Public Network Usage for Coverage Extension.

- Operations, configurations and maintenance

To understand the risks for the defense sector one needs to understand how actually 5G is used in a specific defense scenario. In this article, we will look at a coverage extension scenario. There are many other scenarios e.g., local troops using 5G direct communication, then the local hub uses satellite communication to the headquarter, which uses its own 5G private network [17].

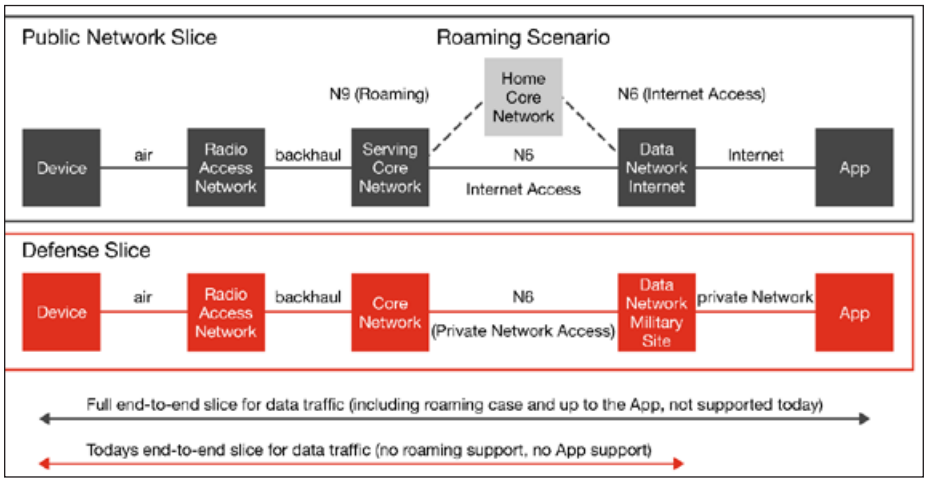
Coverage Extension – TETRA Replacement

In this scenario we assume that the defense entity uses a slice in a public network. The defense entity may want to extend its coverage e.g., outside of the base or it might be fully relying on the public 5G network.

A network slice is an end-to-end logical network that provides specific services for a user group. It is realized through virtualization and Software Defined Network (SDN). In laymen's term one can think of a "software based mini-network" that in most cases sits on the same hardware as the "normal public network". Let's assume our defense entity has a local base where it uses its own 5G local network when the devices are in range. For exercises and coverage extension they utilize their slice in the public network.

There are different ways to slice a network (e.g., Radio Access Network (RAN) slicing, core slicing, transport network slicing, user plane slicing) each one provides its own benefits and challenges in terms of security and management. We assume that the network architecture may look like this:

In the public network the defense entity utilizes their dedicated network functions which are basically dedicated containers for the different network functions and RAN elements. Other users and user groups of the public network utilize their own dedicated network function and RAN elements. All those network functions are managed by the MANO (Network Function Virtualization Management and Orchestration). MANO is a telecommunication term, the large cloud providers have features which are of course called differently but performing the same management functionalities. Cloud providers may offer the MANO functionality as a service to mobile operators. The underlying infrastructure i.e., hardware, storage, computing in our scenario is shared between the defense entity and the public users.



End-to-end slicing for user data traffic.

In our scenario, we have a military site, which is covered by a private defense network. When a defense entity user is on site, he uses the private defense network. When he is in a public network and enters the defense entities local site, he connects into the local site. If he is leaving the site and loses the coverage of the private local defense network, he connects to the slice in the public network.

This implies that there is a connection between the public and the local defense network. If this is a normal roaming connection, then the local defense network is also "reachable" by other operators on the interconnection link. This approach would enable the potential to attackers in the roaming network to reach the military network and launch attacks. This is not the most secure approach; therefore a direct connection is seen as a better approach. If our defense entity user is in the public network, he uses there a specific slice as in the figure above. He then connects to the local defense network through a direct N6 interface between the public network and the local defense network. That way the defense user can reach his specific applications, even if he is out of coverage of the local defense network.

While 5G is widely deployed in city areas, we can safely assume, that operators will have a close eye on the return of investment and that legacy generation base station and core network element continue to exist for quite some time to come. Those legacy elements are not designed to support slicing. If no special measures are taken "all users will be equal", that means any user management action e.g., finding the location of a person or redirecting traffic does not require special privileges compared to normal user management [16].

Based on this architecture, we can deduct the following attack vectors:

- Attack from underlying cloud infrastructure and traffic management (MANO and SDN)

- Breakout of container isolations and entering the defense slice

- Attack on shared resources like memory or computing

- Attack coming from compromised hardware

- Attack coming from the interconnection link to the local site network

- Attack coming from the interconnection link to the public operator

- Attacks on the radio interface

- Attacks using vulnerabilities in legacy infrastructure

- Attacks based on insufficient software configuration and authorization

The range of required countermeasures is wide for 5G networks, the European

Agency for Cybersecurity (ENISA) has published a 5G Security Control Matrix [24], [25], which can used as a tool by experts to customize the security also for private networks e.g., on-site defense network.

The above scenario only represents a small part of the potential usage scenarios and the required countermeasures to provide the 5G usage in the defense sector with a robust security. Each scenario has its own specific requirements which also need to be aligned with defense specific requirements and the potential capabilities of the public operators.

Security requirements may cover items like:

- RAN slicing (with special security measures if O-RAN is used e.g., usage of Packet Data Convergence Protocol (PDCP) and N2/N3 security)

- dedicated core network functions, if e.g., a UDR/UDM is shared, then fine grained authorization and authentication is required

- Direct connection between public operator and private local network (no roaming network usage)

- Certified in-country cloud center

- Additional slice specific authentication support

- Data

- Transport network slicing support

- Zero Trust Architecture (ZTA) usage for security management of a network slice

This is only a snapshot of some potential security requirements, there are many more details [18] which require attention and need to be specified for a sensitive usage scenario like defense.

Summary

Defense may utilize 5G in many different ways and each scenario has its own specific security requirements. Many defense scenarios will utilize public networks for their purpose and use slicing technology. There are many details which need to be analyzed to describe the security demands of a slicing for defense purposes. Slicing and slicing security still evolves and improves: IETF standardization activities e.g., for transport, optical and routing support for slicing [20], GSMA improves slice templates and slice roaming, O-RAN security still evolves [19], MEF is active on SDWAN slicing, TM-Forum works on network slice management, and the market studies other options then modem chip in the phone for support of slicing. These activities and their latest market adoptions need to be studied for each usage scenario and impact the agreement and approach a military usage scenario can take on security.

Other defense scenarios may use 3rd Generation Partnership Project (3GPP) direct communication in combination with satellite communication. Here many activities are ongoing e.g., by the European Union Agency for Cybersecurity (ENISA), to improve the resilience and security of the communication systems. The latest European Union activity to improve the resilience in the update of the Network and Information Systems Directive (called NIS2 directive) covers also the space sector. The member states have to implement the NIS2 directive till October 2024 and then we will also see further improvements of space security for communication networks.

References:

[1] North Atlantic Treaty Organization (NATO), “Emerging and disruptive technologies”, 2023, https://www.nato.int/cps/en/natohq/topics_184303.htm#policy

[2] NATO Communications and Information Agency (NCI) Agency, “NATO tech Agency explores the potential of 5G for the Alliance”, 2021 https://www.ncia.nato.int/about-us/newsroom/nato-tech-agency-explores-the-potential-of-5g-for-the-alliance.html

[3] NATO Cooperative Cyber Defence Centre of Excellence, Veeli Oeselg, Rokas Šalaševičius, Hendrik Ploom, Andreas Palm, Alar Kuusik, Tony Lawrence, Kadri Peeters, “Research Report Military Movement Risks From 5G Networks”, 2020, https://ccdcoe.org/library/publications/research-report-military-movement-risks-from-5g-networks/

[4] Lockheed Martin, “Lockheed Martin, Verizon Demonstrate 5G-Powered ISR Capabilities For Department Of Defense”, 2022, https://news.lockheedmartin.com/2022-09-28-Lockheed-Martin-Verizon-demonstrate-5G-powered-ISR-Capabilities-for-Department-of-Defense

[5] Patria Group, “Protected Mobility and Defence Systems - Autonomous Systems”, 2022, https://www.patriagroup.com/products-and-services/protected-mobility-and-defence-systems/autonomous-systems

[6] DefenseOne, “The US Navy Is Testing 5G For Future Forward Operating Bases”, 2022, https://www.defenseone.com/technology/2022/07/navy-testing-5g-future-forward-operating-bases/375164/

[7] AT&T, “Lockheed Martin, AT&T Demonstrate 5G High Speed Transfer of Black Hawk Data to 5G.MIL® Pilot Network”, 2022, https://about.att.com/story/2022/5g-lockheed-martin.html

[8] Tekniikkatalous, “Virve hyppää 5G aikaan viranomaisten Laajakaistaisen mobiiliverkon käyttöönotto alkaa”, 2022, https://www.tekniikkatalous.fi/uutiset/virve-hyppaa-5g-aikaan-viranomaisten-laajakaistaisen-mobiiliverkon-kayttoonotto-alkaa-2022/a3f260b0-0129-40f0-8d45-b284ce0b6951

[9] European Union, European Defence Fund, “5G Communications for Peacekeeping And Defense (5G COMPAD)”, 2021, https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_5G%20COMPAD.pdf

[10] Avionics – International, “Lockheed Martin and Intel Demonstrate 5G Capabilities For Military Aircraft Use”, 2022, https://www.aviationtoday.com/2022/12/02/lockheed-martin-intel-demonstrate-5g-capabilities-military-aircraft-use/

[11] Avionics – International, “Boeing Aims to Use 5G for Aircraft Maintenance Improvements”, 2023, https://www.aviationtoday.com/2023/08/16/boeing-aims-to-use-5g-for-aircraft-maintenance-improvements/

[12] North Atlantic Treaty Organization (NATO), “NATO’s innovation accelerator becomes operational and launches first challenges“, 2023, https://www.nato.int/cps/en/natohq/news_215792.htm

[13] Lockheed Martin, “5G.MIL® Unified Network Solutions for All-Domain Operations”, https://www.lockheedmartin.com/en-us/products/5G.html

[14] NPS The Sea Land Air Military Research Initiative, ”Launch of Secure Maritime 5G“, 2022, https://nps.edu/web/slamr/-/secure-maritime-5g-ribbon-cutting

[15] Technexus, “Telenor to deploy private 5G network for the Norwegian Defense forces”, 2022, https://tecknexus.com/5gusecase/telenor-to-deploy-private-5g-network-for-the-norwegian-defense-forces/

[16] ENEA AdaptiveMobile Security, Silke Holtmanns, Cathal McDaid, White Paper “5G Network Slicing Security in 5G Core Networks”, 2021, https://www.enea.com/insights/white-paper-slicing-security-in-5g/

[17] NATO Communications and Information Agency (NCI) Agency, Luis Bastos; Germano Capela; Alper Koprulu; Gerard Elzinga, “Potential of 5G technologies for military application”, 2020, https://ieeexplore.ieee.org/document/9486402

[18] National Security Agency (NSA) and Cybersecurity & Infrastructures Security Agency (CISA), “5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance”, 2023, https://www.cisa.gov/news-events/alerts/2023/07/17/nsa-cisa-release-guidance-security-considera-

tions-5g-network-slicing

[19] PricewaterHouse (PwC) Finland, Silke Holtmanns, “Open RAN Security – Still some way to go”, 2023, https://www.pwc.fi/en/publications/open-ran-security-still-some-way-to-go.html

[20] Internet Engineering Task Force (IETF), Mohamed Boucadair, “An Overview of IETF Network Slicing Efforts“, 2023, https://datatracker.ietf.org/doc/draft-boucadair-teas-ietf-slicing-overview/

[21] MEF, “SD-WAN and 5G with Network Slicing”, https://www.mef.net/poc/sd-wan-with-5g-network-slicing/

[22] TMForum, https://inform.tmforum.org/topics/network-slicing

[23] European Union Agency for Cybersecurity (ENISA), “Securing the Seas and the Skys”, 2023, https://www.enisa.europa.eu/news/securing-the-seas-and-the-skies

[24] PricewaterHouse (PwC) Finland, Silke Holtmanns, “Using the 5G security control matrix for telecommunication risk management”, 2023, https://www.pwc.fi/en/publications/using-the-5g-security-control-matrix-for-telecommunication-risk-management.html

[25] European Union Agency for Cybersecurity (ENISA),”5G Security Control Matrix”, 2023, https://www.enisa.europa.eu/publications/5g-security-controls-matrix

Personal Information

Dr. Silke Holtmanns

Telecommunication Security Expert

PwC, Finland (Helsinki)

Silke.Holtmanns@pwc.com

Nationalities: Finnish, German

Certified Information Systems Security Professional (CISSP)

Certified Cloud Security Professional (CCSP)

Silke is a world leading expert on 5G security. Silke has 23 years of telecommunication security experience and worked with Ericsson, Nokia, AdaptiveMobile Security, and ENEA. During her career, she covered the whole range of telecommunication security e.g., embedded secure elements, SIM/UICC and remote provisioning, O-RAN/RAN security, core network security interconnection security (SS7, diameter, 5G), MEC/edge security, NFV and MANO security, hyperscaler/cloud usage for 5G in different deployment and hosting models, and highly sensitive application requirements. In addition, she has hands-on experience on threat analysis of nation states against mobile operators and is one of the original creators of the MITRE for Mobile Networks (now hosted under MITRE FIGHT).

She worked in security research, where she presented new attack to telecommunication networks e.g. at NATO conference, Blackhat and DefCon. She discovered in 2021 the first 5G slicing vulnerability. She was working in GSMA and 3GPP security for many years. She was editor of 11 technical mobile security specifications. She was member of the Panel of Experts of GSMA which evaluates new threats and vulnerabilities and gives guidance to their members on impact, needed actions and severity. She is member of the European Union Agency for Cybersecurity (ENISA) Advisory Group. Nowadays, she is assisting governments, mobile operators, defense and critical infrastructure providers to improve their 5G security.

Marko Höyhtyä työskentelee tutkimusprofessorina Teknologian Tutkimuskeskus VTT:llä ja hänellä on dosentuuri niin Maanpuolustuskorkeakoulussa kuin Oulun yliopistossa.

Heikki Rantanen työskentelee erikoistutkijana Puolustusvoimien Tutkimuslaitoksella tutkimusalueena myös 5G/6G-verkot.

TEKSTI: MARKO HÖYHTYÄ JA HEIKKI RANTANEN

5G NTN ja 6G – luotettavaa viestintäkykyä kaikkialle?

Maanpäällinen 5G-verkko tarjoaa huomattavasti aikaisempia mobiiliverkkoja korkeampaa suorituskykyä. Suomessa ja monissa kehittyneissä maissa valtaosa ihmisistä on jo hyvien 5G-yhteyksien varassa. Verkon kapasiteettia on rakennettu vahvasti urbaanialueille ja ratkaisuja on kehitetty tukemaan kriittisiä käyttäjiä mm. viranomaistoiminnassa ja tehdasympäristöissä. Verkkojen rakentaminen on keskittynyt sinne, missä ihmisiä on paljon ja monilla etäisillä alueilla hyviä 5G-yhteyksiä ei ole tarjolla. Kuten edellisessä numerossa jo kuvasimme, on 5G-kehityspolulla tulossa ratkaisuja laajaan maantieteelliseen kattavuuteen 5G:n satelliittilaajennuksen eli 5G NTN (Non-Terrestrial Networking) avulla. Luonnollisesti tällainen kyvykkyys herättää suurta sotilaallista mielenkiintoa. Tässä artikkelissa tarkastelemme 5G NTN:n käyttöä osana sotilaallisia viestintäverkkoja ja kerromme nykyisin kehitteillä olevista matalan kiertoradan satelliittiviestintäjärjestelmistä. Lopuksi analysoimme vielä mitä kyvykkyyksiä 6G tuo niin viestinnän, ympäristön seurannan kuin paikannuksen näkökulmasta.

Kriittisen sotilasviestinnän vaatimukset

Nykyaikaisessa sodankäynnissä korostuvat erilaiset digitaaliset järjestelmät, joita käytetään verkottuneen tilannekuvan muodostamiseen, tehokkaaseen kaukovaikuttamiseen sekä reaaliaikaiseen viestintään. Taistelukentällä on käytössä suuri määrä erilaisia radiotaajuuksilla toimivia laitteita sisältäen niin ajoneuvoihin integroidut radiot, kannettavat laitteet kuin tutkatkin. Näitä laitteita on joukoilla käytössä niin maalla, merellä kuin ilmassa. Lisäksi erilaiset avaruusjärjestelmät tukevat joukkojen toimintaa maanpäällä tarjoten niin tiedustelutietoa, paikannuskyvykkyyttä kuin tietoliikenneyhteyksiä kaikkialle.

Sotilasviestintäjärjestelmän päävaatimukset ovat: 1) Aina saatavilla ole yhteys sijainnista riippumatta. 2) Erittäin luotettavat ja turvalliset yhteydet, jotka resilientisti yhdistävät kaikki taistelukentän elementit. 3) Eri joukkojen ja verkottuneiden asejärjestelmien yhteistoiminnan välisen viestinnän ja toiminnan mahdollistaminen. Koska joukot toimivat usein etäisillä alueilla ja kaukana toisistaan, tarvitaan resilienssin ja toiminnan takaamiseksi muitakin yhteyksiä kuin maanpäällisiä verkkoja. Droneja voidaan käyttää dynaamisesti väliaikaisiin yhteyksiin, mutta pidempiaikaista toimintaa varten avainasemassa ovat korkeammalta yhteyksiä tarjoavat järjestelmät kuten HAPS (High Altitude Pseudo Satellites) ja varsinaiset satelliittijärjestelmät. Etenkin jälkimmäiset mahdollistavat yhteydet missä tahansa toimittaessa.

Matalan kiertoradan satelliitit: Olemassa olevat ja kehitteillä olevat järjestämät

Maata kiertää avaruudessa tällä hetkellä 10 000 satelliittia ja määrä on nopeassa kasvussa. Vuosittain laukaistaan yli 1000 satelliittia kiertoradalle. Suurimpana ajurina tässä ovat suureksi estimoidut laajakaistamarkkinat ja Internet-yhteyksien tarjonta syrjäisille alueille sekä erilaiset laitteiden Internetin (IoT, Internet of Things) ratkaisut. Koska useat sovellukset vaativat kapasiteetin lisäksi myös matalia viiveitä, dominoivat matalien kiertoratojen (LEO, Low Earth Orbit) järjestelmät tällä hetkellä kehittyviä markkinoita. Lisäksi LEO-järjestelmät tarjoavat peittoa myös pohjoisille alueille.

Tällä hetkellä tärkeimmät LEO-järjestelmät Suomen kannalta ovat seuraavat: **Starlink** on suurin koskaan rakennettu avaruusjärjestelmä. Satelliitteja on kiertoradalla noin 5000 kappaletta reilun 500 km korkeudella ja se tarjoaa laajakaistayhteyksiä globaalisti. Päätelaite yhdistää käyttäjän satelliittiin ja toimii reitittimenä, johon voidaan kytkeytyä esim. kännykällä. VTT:n mittaukset ovat osoittaneet, että pohjoisessa Suomessakin voidaan päästä 60 Mbps uplink-nopeuk-

siin (päätelaitteelta satelliitin suuntaan) sekä yliE200 Mbps downlink-nopeuksiin (satelliitista päätelaitteeseen). Kuvassa 1 on esillä mittausjärjestelmä, jossa Starlink-terminaalilla lähetettiin verkottuneen turvallisuuden ajoneuvoviestintää. **OneWeb** on samankaltainen järjestelmä, jossa on vajaa 600 LEO-satelliittia 1200 km korkeudessa. Päätelaitteen toimintaperiaate on sama ja peittoalue taas ulottuu korkeammalle pohjoiseen polaaristen ratojen takia. VTT-mittauksissa suorituskyky pohjoisessa Suomessa on ollut parhaimmillaan noin 20 Mbps uplink- ja 100 Mbps downlinkin suuntaan. Lisäksi Suomessa toimii hyvin **Iridium**, joka on 66 satelliitin konstellaatio ratakorkeudella 780 km. Päätelaitteet ovat kädessä pidettäviä puheyhteyksiin ja matalan tiedonsiirtonopeuden datayhteyksiin (< 0.5 Mbps) soveltuvia laitteita. Näiden lisäksi olemme mitanneet **Viasat**in korkean kiertoradan GEO-satelliittia, joka operoi 36 000 kilometrin korkeudessa päiväntasaajan päällä. Etelä-Suomessa pienellä lautasantennilla on saatu 10 Mbps uplink ja 50 Mbps nopeuksia, mutta pohjoisessa yhteyttä ei välttämättä ole aina saatu pystyyn lainkaan. Mitä pohjoisemmaksi mennään, sitä haastavampi se on GEO-yhteyksien kannalta.

Edellä mainittujen lisäksi kehitellään aktiivisesti muita suuria megakonstellaatioita, joissa on satoja tai jopa tuhansia satelliitteja. Merkittävimpiä näistä ovat Amazonin kehittämä Kuiper, jossa tavoitteena yli 3000 LEO-satelliitin järjestelmä ja nopeat laajakaistayhteydet sekä Eurooppaan kehitteillä oleva IRIS2. Jälkimmäinen on Euroopan oma satelliittijärjestelmä, jonka on tarkoitus olla operatiivisessa käytössä vielä tämän vuosikymmenen aikana. Se tarjoaa luotettavia yhteyksiä niin siviileille kuin turvallisuuskriittisille toimijoille. Nykyisessä geopoliittisessa tilanteessa tämä tuo myös huoltovarmuutta Eurooppaan ja kilpailijan amerikkalaisten järjestelmille. Julkisten tietojen mukaan tavoitteena on monikerrosverkko, jossa yhdistetään GEO-satelliitit, n. 200 satelliitin LEO-konstellaatio sekä maanpäällinen 5G-verkko yhteen. Tämän noin 6 miljardin euron kokonaisuuden rahoittavat Euroopan avaruusjärjestö ESA, Euroopan komissio sekä yksityiset toimijat. Kiinalaisilla on myös omat suunnitelmansa jopa 13 000 satelliitin järjestelmistä.

5G NTN-teknologian kehitys

5G NTN on sateenvarjotermi, joka sisältää 5G-teknologian käytön niin avaruudessa kuin ilmassa toimivilta alustoilta. Suurimpana mielenkiinnon kohteena ovat tällä hetkellä matalan kiertoradan satelliitit ja niihin liittyvä kehitystyö. Maanpäällisiin verkkoihin verrattuna pitää satelliittipohjaisissa 5G-yhteyksissä huomioida erittäin suuri satelliitin nopeus (yli 7 km/s), joka aiheuttaa Doppler-siirtymää signaaliin sekä pitkät etäisyydet ja edellä mainittujen tekijöiden aiheuttama viivevaihtelu. Aika- ja Doppler-kompensaatiota voidaan tehdä joko tukiaseman päässä eli arkkitehtuurin mukaan satelliitissa tai maa-asemassa, johon on integroituna tukiasematoiminnallisuudet – tai sitten suoraan päätelaitteessa hyödyntäen tarkkaa paikkatietoa ja laskien rataparametrien ja oman sijainnin perusteella tarvittava kompensointi. Tämä mahdollistaa sitten muiden protokollien käytön kuten maanpäällisissä 5G-järjestelmissä.

Starlink-terminaali autonomisen ajoneuvon katolla.

Pääarkkitehtuurivaihtoehdot loppukäyttäjän näkökulmasta ovat joko suorat yhteydet satelliittiin tai sitten reititys tukiaseman kautta (ks. Kuva 2), jolloin satelliitilla voidaan toteuttaa esim. paikallisen verkon tukiaseman ja core-verkon välinen runkoliityntä (bakchaul). Tukiasema voidaan tuoda toiminta-alueelle repussa tai ajoneuvoon integroituna eli luodaan paikallinen 5G-verkko tai taktinen kupla ja erillisellä satelliittiantennilla toteutetaan yhteys tukiasemasta satelliittiin. Suorat yhteydet voivat tulevaisuudessa toimia kaikkiin standardin mukaisiin älypuhelimiin ilman tarvetta investoida erilliseen satelliittivastaanottimeen. Ensimmäiset onnistuneet demonstraatiot on jo toteutettu AST SpaceMobile-järjestelmällä, jossa myös Nokia on mukana. Syyskuun 8. päivä 2023 soitettiin puhelu Samsungin S22 älypuhelimella Havaijilta suoraan Blue Walker 3 -satelliitin kautta. Lisäksi on todennettu samalla järjestelmällä yli 10 Mbps datanopeudet kädessä pidettävään laitteeseen. Yhteyden mahdollistajana on 64 neliömetrin kokoinen vaiheistettu ryhmäantenni satelliitissa. Sillä saadaan aikaan voimakas vahvistus ja näin päätelaitteen antenni voi olla jopa ympärisäteilevä.

Viestimies-lehden edellisen numeron 5G NTN-artikkelissa kerroimme, että mobiilijärjestelmien standardisoinnista vastaavan 3GPP:n terminologiassa 5G NTN sisältää satelliittialustaisten toteutusten lisäksi myös HAPS (High Altitude Platform System) -alustaiset 5G järjestelmät. HAPS-alustana voivat toimia joko ilmalaivat tai tyypillisesti suuren siipipinta-alan dronet. Aiemmin testattiin myös ilmapalloja (kuten Google projekti LOON), mutta ne osoittautuivat hankalasti hallittaviksi. AALTO HAPS -yrityksen ZEPHYR käyttää kiinteäsiipisessä dronessa aurinkokennoja energialähteenä, kun taas Stratospheric Platform Ltd (SPL) käyttää vetyä. On muistettava, että aurinkokennojen tehokkuus päiväntasaajalla on huomattavasti parempi kuin

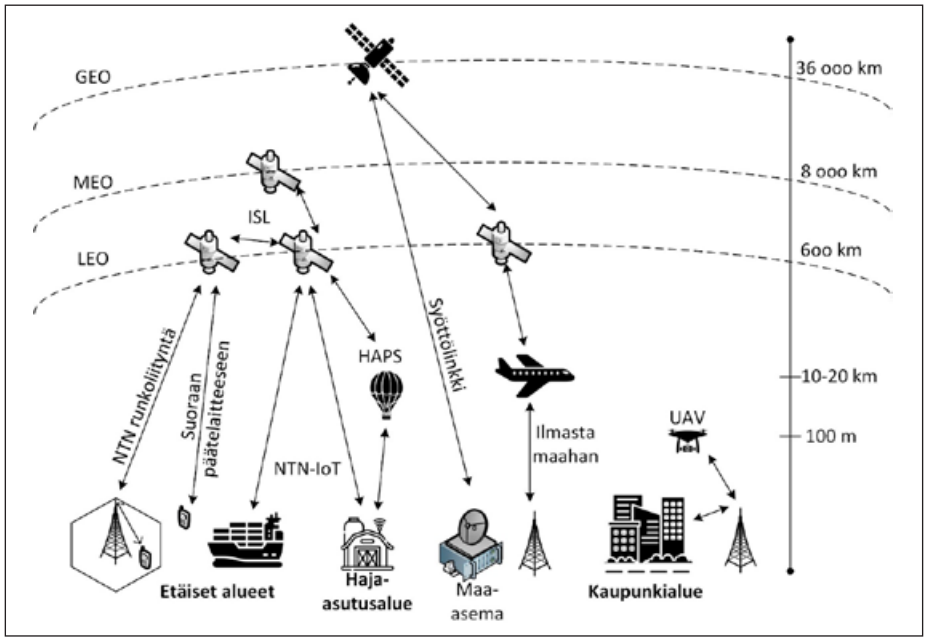
meillä Suomessa. Kuvassa 3 on esillä erilaisia HAPS-alustoja.

HAPSin englanninkielisessä nimessä sana ’System’ korvautuu usein sanalla ’Station’ tai kaksi viimeistä sanaa yhdistelmällä ’Pseudo Satellite’. Viimeinen vaihtoehto on hyvin kuvaava, koska HAPSia kutsutaan myös köyhän miehen satelliitiksi – sillä saavutetaan usean kymmenen kilometrin peittoalue murto-osalla satelliitin hintaan verrattuna. Kun 5G-tukiasema sijoitetaan LEO-satelliitin sijasta HAPS-alustalle, saavutetaan myös useita etuja hinnan lisäksi. Viive satelliittijärjestelmiin verrattuna on huomattavan pieni, suuruusluokaltaan sama maanpäällisten järjestelmien kanssa eikä itse asiassa muokkauksia 5G-teknologiaan tarvita samalla tavalla kuin satelliitissa. 5G HAPS-järjestelmällä voidaan lyhyellä varotusajalla kasvattaa verkon kapasiteettia sekä peittoa. Lisäksi järjestelmän päivitys ja huolto on helppoa. On esitetty arvioita, että vetykäyttöinen 5G HAPS drone voisi olla ilmassa viikon ilman uudelleentankkausta. Toisaalta satelliiteilla taas saadaan pysyvämpi peitto ja yhteys aikaan jopa globaalisti.

5G HAPS drone sijoitetaan tyypillisesti noin 20 km korkeudelle koska siellä ilmavirtaukset ovat pienimmillään ja ollaan turvallisesti reittilentojen yläpuolella. Tällä korkeudella saavutetaan noin 600 km radiohorisontti, mutta koska 5G NTN satelliittijärjestelmien tavoin HAPS käyttää monikeila-antenneja, käytännössä solun halkaisija on luokkaa 10–70 km. Monikeila-antenni on helppo sijoittaa kiinteäsiipisen dronen siiven alapinnalle. Se voi koostua tuhansista antennielementeistä ja sillä voidaan toteuttaa useita satoja erillisiä antennikeiloja sisältävä solukkoverkko.

Vielä muutama vuosi sitten 5G HAPS-asian edistämistä haittasi teollisuuden, operaattoreiden ja muiden potentiaalisten HAPS-toimijoiden järjestäytymättömyys. Nyt tilanne on toinen. Tällä hetkellä on olemassa organisaatio nimeltä HAPS Alliance, johon kuluu televiestintä-, teknologia- ja ilmailualan yrityksiä, mutta myös tutkimuslaitoksia. Sen tavoitteena on edistää HAPS-teknologiaa ja sitä käyttäviä tietoliikenneratkaisuja 5G- ja 6G-standardisoinnissa.

Euroopassa viime vuonna käynnistyi EDF (European Defense Fund) -ohjelman alaisuudessa EUROHAPS tutkimus, jossa keskitytään erityisesti HAPS alustan hyödyntämiseen Euroopan asevoimien hyödyksi. Tietoliikenteen lisäksi tutkiaan HAPS-alustan soveltuvuutta ISR (Intelligence, Surveillance and Reconnaissance) -käyttöön eli tiedusteluun



NTN-teknologian arkkitehtuurivaihtoehtoja, laitteiden tyypillisiä korkeuksia sekä sovelluksia.

eri teknologioilla kuten 3D LIDARia käyttäen. Testeissä käytetään erilaisia alustoja, joita tutkittiin aiemmin eurooppalaisessa EHAAP (European High Atmosphere Airship Platforms) tutkimuksessa.

Vuoden 2023 kevään suuressa Barcelonan Mobile World Congress (MWC) -näyttelyssä katosta roikkui luonnollisessa koossa ZEPHYR näyttelytilan yläpuolella ja useat toimijat kuten British Telecom ja Deutsche Telekom esittelivät, kuinka HAPSin avulla voidaan korvata jopa satoja tukiasemia.

5G ja NTN-ratkaisut MIL-yhteisöissä

Käytännössä kaikki maailman sotavoimat hyödyntävät toiminnassaan kaupallisten satelliittijärjestelmien palveluita ja mobiiliverkkoteknologioita. MIL-yhteisössä tehdään aiheen parissa myös aktiivista tutkimustyötä.

NATO IST-187 työryhmä: Työryhmän yksi pääteemoista on Extreme long range coverage, joka kattaa niin satelliittien, HAPSien kuin matalammallakin lentävien dronejen käytön pitkän kantaman viestinnässä. IST-187 arvioi 5G-tekniikan hyödyntämistä sekä teknisestä että suorituskyvyllisestä näkökulmasta ja näitä vasten analysoi millaista uutta suorituskykyä 5G voisi tuoda taistelukentälle. Työryhmässä on osallistujia niin teollisuudesta kuin myös siviili- ja sotilastutkimusorganisaatiosta. Työryhmätyön lisäksi NATO rahoittaa tutkimushankkeita, joissa perehdytään erityisesti 5G NTN:n tuomiin sotilaallisiin mahdollisuuksiin niin sotilaiden kuin koneiden näkökulmasta.

NATO DIANAn innovaatio- ja testikeskukset:

Suomi on VTT:n aloitteesta ehdottanut kahden DIANA-keskuksen rakentamista Suomeen ja näissä olisi tavoitteena kehittää mm. erittäin turvallista kaikkialla toimivaa viestintäteknologiaa. Puolustusministeriö on hyväksynyt VTT:n esityksen ja toimittanut ehdotuksen Naton Diana-aloitteen sihteeristölle heinäkuussa 2023. Testikeskusten avulla voitaisiin sitoa paremmin NATOn toimintoja Suomeen ja vauhdittaa kotimaista puolustusteollisuutta.

Havainnekuvia erilaisista HAPS-alustoista: Thales Alenia Stratobus, Aalto Hapsin Zephyr sekä Stratospheric Platformin kiinteäsiipinen drone.

EDF 5G COMPAD -hanke: 5G COMPAD on eurooppalainen EDF-rahoituksella tehtävä tutkimus, jossa on yli 20 osallistujaa eurooppalaisista teollisuusyrityksistä ja tutkimusorganisaatioista. Tärkeimpänä tehtävänä on selvittää, millaista suorituskykyä voidaan saavuttaa suuren datansiirtokapasiteetin standardoidulla 5G-järjestelmällä, kun se integroidaan osaksi taktista järjestelmää. Tutkimus tuottaa teknisen ratkaisun verkkojen liittämiseksi yhteen ja se todennetaan demonstraatiolla.

Suomi on ollut kautta vuosikymmenien merkittävässä roolissa mobiilijärjestelmien eri sukupolvien kehittämisessä. On siis luonnollista, että edellä kuvattuihin EU- ja NATO- foorumeilla tehtäviin tutkimuksiin on Suomesta osallistuvia yrityksiä ja tutkimuslaitoksia kuten Nokia, Bittium, VTT ja Oulun Yliopisto.

Mitä uutta 6G voi tuoda tullessaan?

Jokainen viestintäverkkojen sukupolvi tuo tullessaan uusia mielenkiintoisia ominaisuuksia, joita voidaan hyödyntää niin siviili- kuin sotilasviestinnässä. 6G-verkkojen osalta ei vielä tiedetä varmasti mitä se tulee sisältämään, sillä varsinainen standardoidun järjestelmän spesifikaatio valmistuu vasta tulevina vuosina. Operatiivisen 6G-järjestelmän odotetaan olevan valmiina 2030 mennessä.

Nykyisen käsityksen mukaan 6G tulee muuttamaan verkkoja merkittävästi:

5G:hen asti verkot on suunniteltu ja optimoitu horisontaalisesti eli ne toimivat hyvin maanpinnalla ja sen läheisyydessä. 5G NTN on lähinnä jälkikäteen lisätty palikka kokonaisuuteen. 6G:n suunnittelussa vertikaalidimensio on alusta asti mukana ja koko verkkoarkkitehtuuri on kolmeulotteinen. Tämä mahdollistaa luotettavat yhteydet ja suorituskyvyt kaikkialle, myös ei-maanpäällisiin järjestelmiin.

Samalla verkolla voidaan toteuttaa viestinnän lisäksi tarkkaa 3D-paikannusta ja ympäristön monitorointia käyttäen hyödyksi tietoliikennesignaaleja. Näin voidaan verkolla tukea lukemattomia eri sovelluksia kuten autonomista ajamista ja radioiden käyttämistä tutkana. Avaruuspuolella voidaan tehdä avaruusympäristön seurantaa käyttämällä hyväksi muista satelliiteista tai avaruusromusta tapahtuneita tietoliikennesignaalien heijastuksia.

Esimerkkinä kansallisesta kehityksestä artikkelin teemassa voidaan mainita VTT:n koordinoima 6G-SatMTC-hanke, jossa toisena tutkimusosapuolena on Oulun yliopisto. Projektissa kehitetään integroituja verkkoratkaisuja kriittisille käyttäjille kuten viranomaisille, etäisiin kaivoksiin ja merenkulkuun tavoitteena tilanne, jossa voidaan saumattomasti käyttää niin mobiiliverkkoa kuin satelliittiverkkoa niiden saatavuuden, kapasiteetin ja käyttäjätarpeiden mukaan missä tahansa globaalisti toimittaessa. Työssä ovat ohjaavassa roolissa mukana mm. Erillisverkot, Nokia ja Keysight. Erityisenä huomion kohteena ovat yhteydet ja viranomaisten yhteistoiminta suurten metsäpalojen yhteydessä ja miten voidaan taata pelastushenkilöstön turvallisuus sekä luotettava tilannekuva niin paikallisesti kuin operaatiota etänä ohjaavalle johtokeskukselle.

Yhteenveto

Avaruusjärjestelmät ovat pitkään olleet tärkeä osa sotilastoimintaa. Tulevaisuudessa niiden rooli voi kasvaa vielä merkittävästi ja osana tätä kehityspolkua ovat kaupalliset ratkaisut. Vaikkakin tällä hetkellä erilaiset proprietary-ratkaisut kasvavat vauhdilla ja tarjoavat varsin hyvää suorituskykyä Suomessakin, ovat erityisesti standardoidut ratkaisut suuren mielenkiinnon kohteena. 5G- ja 6G-teknologia voivat tuoda suorat satelliittiyhteydet myös kädessä pidettäviin laitteisiin kuten älypuhelimiin, jolloin viestintää voidaan tehdä sekä maanpäällisessä verkossa että satelliittien välityksellä. Lisäksi HAPS-ratkaisut ovat lupaava vaihtoehto suurten peittoalueiden viestintään tarjoten matalaviiveisen vaihtoehdon etäisille alueille. Teknologiakehitystä tehdään aktiivisesti niin kansainvälisillä sotilasfoorumeilla kuin kansallisissa hankkeissakin.

Standardoidut ratkaisut mahdollistavat kaikkein kustannustehokkaimmat ja usein myös suorituskykyisimmät järjestelmät kun tutkimusyhteisöt kilvan tarjoavat omia ratkaisujaan standardisointiorganisaatioiden kuten 3GPP käyttöön. Mobiilijärjestelmien tapauksessa teknisen kehitys on vielä hyvin hallittua ja tehokasta, kun esimerkiksi 5G tapauksessa järjestelmäspesifikaatio päivittyy useamman kerran järjestelmän elinkaaren aikana. Päivitys ei välttämättä aina vaadi laitteiden uusintaa vaan se voidaan tehdä ohjelmistollisesti. Ei olekaan siis yllätys, että sotilasyhteisöt pyrkivät tänä päivänä vaikuttamaan 3GPP standardisointiin esimerkiksi tietoturvan ja viranomaisille tarjottavan palvelunlaadun osalta.

TEKSTI: HANNU MUIKKU

Tietoturva tämän päivän tietoliikenneverkoissa

Yhteiskunta on vaikeuksissa, jos tietoliikenneverkot – ja verkkojen varassa toimivat järjestelmät – eivät toimi. Tietoturvauhkat haastavat verkkojen suunnittelua ja toteutusta, kun palveluiden tulisi olla aina turvallisesti saatavilla. Millaisiin osa-alueisiin ja teknologioihin kannattaa kiinnittää huomiota juuri nyt?

Artikkeli on osa sarjaa, jossa tarkastellaan nousevien teknologioiden hyödyntämistä vaativissa, korkean turvatason IT-ympäristöissä.

Mitä enemmän yhteiskunnan ja yritysten palveluita sähköistetään, automatisoidaan ja siirretään tietojärjestelmien varaan, sitä enemmän kasvaa tietoliikenneverkkojen kriittisyys. Häiriöt näkyvät jokapäiväisten rutiinien sujumisessa välittömästi. On siis tärkeää kiinnittää entistä enemmän huomiota siihen, että palvelut ovat saatavilla, vaikka poikkeustilanteet koettelisivat verkkojen kestävyyttä.

Käyn seuraavaksi läpi tietoliikenneverkkoihin kohdistuvia uhkia. Sen jälkeen teen katsauksen tärkeimpiin toimintatapoihin ja teknologioihin, joilla tietoverkkojen, ja sitä kautta myös -järjestelmien, turvallisuutta vahvistetaan.

Välimatkat palvelimille ovat pidentyneet

Tietoliikenneverkoista on viime vuosina tullut entistä luotettavampia, ja niiden siirtokapasiteetti on kasvanut. Aiemmin palveluita tuotettiin lähellä olevilla palvelimilla, mutta teknisen kehityksen myötä yhä useammat organisaatiot ovat siirtyneet käyttämään keskitettyjä konesaleja ja julkisia pilvipalveluita.

Silloinkin, kun järjestelmä nojaa perinteiseen konesalimalliin, on järkevää hajauttaa kriittistä dataa useisiin eri konesaleihin. Näin varmistetaan palveluiden jatkuvuutta ja varaudutaan poikkeustilanteisiin. Tyypillisesti ainakin korkean käyttövarmuuden järjestelmien edusta- ja taustajärjestelmät toimivat eri osoitteissa. Konesalien välissä on silloin tarve siirtää luottamuksellista dataa suurinakin määrinä, ja se täytyy pystyä salaamaan vahvoilla keinoilla. Palveluiden jatkuvuuden turvaamiseksi palveluiden dataa hajautetaan useisiin konesaleihin.

Julkipilvipalveluiden hyödyntäminen vie palvelimet kauemmas omien silmien ulottuvilta, mutta ei poista tarvetta datan fyysiselle säilyttämiselle. Pilvipalveluntarjoajan konesalit sijaitsevat esimerkiksi Saksassa tai Alankomaissa, joista tiedon on kuljettava moitteettomasti käyttäjän päätelaitteelle ja takaisin.

Julkipilvipalveluiden varaan voi tänä päivänä rakentaa korkean turvatason järjestelmiä, jos vain organisaation omat vaatimukset datan sijainnista sen sallivat. Julkipilvialustoille siirtyykin entistä kriittisempiä palveluita, jotka vaikuttavat tavallisten kansalaisen arkipäiviin. Samalla käyttöön saadaan edistyksellisiä, tietoturvaa vahvistavia ominaisuuksia. Toisaalta tiedonsiirtomatkojen kasvaessa entistä pidemmät verkko-osuudet ovat alttiita fyysisille häiriöille.

Katkennut kaapeli ja muut fyysisen maailman riskit

Tietoliikenneverkko muodostuu toisiinsa kytketyistä tietoliikennelaitteista. Niiden fyysinen suojaaminen alkaa luvattomien tunkeutumisten estämisestä. Keskeisimmät laitteet ja järjestelmät sijoitetaan esimerkiksi murtosuojattuihin ja kulkuvalvottuihin tiloihin.

Valtaosa datasta liikkuu fyysisiä kaapeleita pitkin. Ja kaikkeen, mikä on fyysistä, liittyy aina tahattoman tai tahallisen rikkoutumisen vaara.

Jotta kriittisen tärkeiden sovellusten toiminta voi jatkua luotettavasti ilman katkoja, on niihin kytkeytyvien tietoliikenneverkkojen oltava riittävän vahvasti varmennettuja. Pelkkä laitekohtainen varmennus ei riitä, vaan vikatilanteessa liikenne pitää pystyä reitittämään kokonaan vaihtoehtoisille reiteille.

Sitä mukaa kun tietoliikenneverkkojen kriittisyys on lisääntynyt, on syntynyt myös kysyntää vaihtoehtoisille maantieteellisille reiteille. Näitä toteutetaankin jatkuvasti lisää. Uudet reitit parantavat tietoverkkojen vikasietoisuutta ja niiden päällä tuotettavien palveluiden saatavuutta.

Laitteiden suojaaminen ja yhteyksien varmistaminen on vasta alkusoittoa tietoliikenneyhteyksien turvaamiselle. Palveluiden luotettavuus syntyy myös siitä, että tietoverkkojen kuljettama viestiliikenne on oikeellista ja eheää. Tietoon saa päästä käsiksi vain sellainen henkilö tai laite, jolla on siihen lupa. Näihin haasteisiin tartutaan myös muilla kuin fyysisen maailman suojauksen keinoilla.

Uhkana salakuuntelu ja tiedon muuntelu

Iso osa päivittäin käyttämistämme palveluista on tehty siten, että ne näkyvät julkisessa internetissä ja ovat siellä kenen tahansa käytettävissä. Tämä tekee niistä alttiita monenlaisille tietoturvauhkille. Toisaalta juuri jatkuvasti kehittyvät hyökkäystaktiikat kirittävät myös suojautumistapojen kehittymistä.

Niitä periaatteita ja tekniikoita, joilla suojataan internetin päällä toimivia palveluita, voidaan hyödyntää myös suljetuissa ja turvallisuuskriittisissä verkoissa. Jos verkko on täysin suljettu ja data sijaitsee omilla palvelimilla, kaikkia saatavilla olevia suojautumisteknologioita ei voida täysipainoisesti käyttää. Se johtuu siitä, että monet uudet, tietoturvaa tietoliikenneverkkoihin tuottavat teknologiat tarvitsevat ratkaisuja, jotka toimivat nimenomaan internetin kautta keskitetyiltä pilvialustoilta käsin.

Tällaisia moderneja, pilvipohjaisia ratkaisuja voivat olla esimerkiksi erilaiset tietoturvatapahtumien analysointiin liittyvät työkalut, jotka seuraavat jatkuvasti globaalia verkkoliikennettä ja tekevät sen perusteella riskiarvioita sekä globaaliin että asiakaskohtaiseen liikenteeseen liittyen.

Ei ole yhtä oikeaa vastausta siihen, miten rakennetaan turvallinen ja tehokas tietoliikenneyhteyksien ja -palveluiden kokonaisuus järjestelmien ja sovellusten ympärille. Se riippuu muun muassa organisaation vaatimuksista ja järjestelmän kriittisyyden tasosta.

Korkean vaatimustason järjestelmissä, joissa halutaan hyödyntää modernia teknologiaa, voi julkipilviresursseja hyödyntää esimerkiksi jatkuvasti valvottujen, omaan yritysverkkoon kytkettyjen internetistä erotettujen tietoliikenneyhteyksien kautta.

Järkeviä toteutustapoja saattaa olla myös useita yhtä aikaa, päällekkäin ja limittäin. Monimutkaisissa järjestelmäympäristöissä tietoliikenneasiantuntijoilta vaaditaan entistä parempaa kykyä tunnistaa, millaisia periaatteita erilaisiin tietoverkkoihin tulisi soveltaa.

Segmentointi turvallisuustasojen perusteella

Segmentointi on turvallisuustasoiltaan erilaisten verkkojen erottelua toisistaan tietoliikennetekniikoiden avulla. Segmentointi voi tähdätä esimerkiksi siihen, että kaikki tietyn tasoiset laitteet tai käyttäjät liitetään samaan verkkoon, jossa ne voivat turvallisesti liikennöidä keskenään.

Julkisin verkko, jossa päätelaitteet ja käyttäjät voivat liikennöidä, on internet. Erilaiset turvallisuuskriittiset verkot voivat puolestaan olla erittäin tarkasti suojattuja fyysiseltä tasolta lähtien: niihin pääsy on rajattu ainoastaan tarkkaan määritellyille päätelaitteille ja käyttäjille.

Segmentointia voi tehdä sekä fyysisellä että loogisella tasolla. Fyysinen verkon eriyttäminen tarkoittaa sitä, että tiettyä käyttötarkoitusta varten tehdään oma verkko. Siihen liitetyt verkkolaitteet palvelevat ainoastaan kyseistä käyttötarkoitusta. Niiden väliset yhteydet on toteutettu erillään muista, esimerkiksi omilla fyysisillä valokuiduilla. Loogisessa verkkoerittelyssä fyysinen verkko voidaan virtualisoida, eli yhden fyysisen verkon päälle voidaan toteuttaa useampia virtuaalisia verkkoja.

Otetaan esimerkki yritysmaailmasta, jossa tietoverkot segmentoidaan liiketoiminnallisista tarpeista lähtien:

- Yritysverkko erotetaan internetistä erilliseksi verkoksi. Internetin ja yritysverkon välinen liikenne ei ole enää suoraan mahdollista, ja yleensä välissä on tietoturvakomponentti, kuten palomuuri, jonka kautta yritysverkon ja internetin välistä liikennettä voidaan kontrolloida ja suodattaa.

- Yrityksen sisäverkossa voi olla omat segmenttinsä eli virtuaaliset verkkonsa esimerkiksi toimisto-, tuotanto-, kiinteistöautomaatio- ja vierailijaverkoille. Näiden toisistaan erotettujen verkkojen välillä ei ole lähtökohtaisesti yhteyttä, ellei sitä erikseen sallita suoraan reitittämällä tai tietoturvallisemmin palomuurin kautta.

- Vastaavasti yrityksen omien palvelimien tai erilaisista pilvipalvelualustoista hankittujen palvelimien tuottamat palvelut on yleensä erotettu muista verkoista ja niille pääsyä suodatetaan palomuureilla.

Huomio hallittuihin yhdyskäytäviin

Kriittiset operatiiviset järjestelmät on siis eriytetty yleensä omiin, fyysisesti eroteltuihin verkkoihinsa. Niistä voi toteuttaa hallittuja, tietoturvallisia yhdyskäytäviä muihin tuotantoon liittyviin verkkoihin, sen mukaan mistä tai mihin tieto on tarpeen saada liikkumaan.

Näistä operatiivisten verkkojen kokonaisuuksista sekä niihin liitetyistä päätelaitteista ja järjestelmistä käytetään nimitystä OT-verkot (Operational Technology). Suunnittelussa ja toteutuksessa voidaan käyttää viitekehyksenä esimerkiksi Purdue-arkkitehtuuria. Se antaa valmiin viitekehyksen useamman tasoiselle hierarkialle, jotta tuotantoverkkojen segmentointia ja eri segmenttien välistä liikennöintiä on selkeämpää suunnitella ja toteuttaa.

Viranomaisympäristöissä huomio kiinnittyy tarkkaan määriteltyihin turvallisuusluokkiin. Jokaisen verkkototeutuksen ja tietoliikennelaitteen tulee olla noudattaa kyseiselle ympäristölle määritellyn turvallisuusluokan kriteerejä. Verkkojen välille voidaan tällöinkin rakentaa luotettavia turvallisuusluokitukset täyttäviä yhdyskäytäväratkaisuja. Niiden ansiosta tieto liikkuu turvallisesti eri turvaluokkiin kuuluvien ympäristöjen välillä.

Palomuurien teknologia kehittyy

Palomuurit kontrolloivat ja suodattavat eri verkkosegmenttien välistä liikennettä. Palomuurin toimintaperiaate on yksinkertainen: muurille määritetään säännöstö, jonka perusteella liikenteen kulku estetään tai liikennettä päästetään läpi.

Nykyaikaiset palomuurit tarjoavat uusia ominaisuuksia liikenteen seurantaan ja niiden kautta kulkevan haitallisen liikenteen tunnistamiseen ja estämiseen.

Perinteinen palomuuri, joka sallii protokollatasolla liikennöinnin web-palvelimelle, ei ota kantaa siihen, onko liikenne verkkopalvelun toiminnalle haitallista vai ei. Kun palomuurissa otetaan käyttöön esimerkiksi tunkeutumisen havainnoinnin ja estämisen ominaisuus, se pystyy tunnistamaan web-palvelimelle tehtäviä tunkeutumisyrityksiä ja estämään ne. Näin verkkopalvelu pysyy varmemmin saatavilla sen todellisille käyttäjille. Nykyaikaiset palomuurit tukevat hyvin myös erilaisten haittaohjelmien suodatuksia.

VPN-tunneli turvaa etäkäyttöä

Monipaikkainen työ asettaa omat haasteensa tietoliikenneyhteyksille. Miten päästä käsiksi organisaation luottamuksellisiin palveluihin ja dataan kotoa tai kesämökiltä? Tänä päivänä erilaisiin internetistä erotettuihin verkkoihin tehtävät tietoturvalliset etäkäyttöratkaisut ovat

hyvin yleisiä. Erilaisia VPN-etäkäyttöratkaisuja (Virtual Private Network) käytetään esimerkiksi silloin, kun julkisesta internetistä halutaan tehdä tietoturvallinen yhteys yrityksen sisäverkkoon.

VPN-ohjelmisto asennetaan luotetulle päätelaitteelle. Sen jälkeen se ottaa yhteyden internetin ja yrityksen sisäverkon välissä olevaan, VPN-yhteyksiä terminoivaan laitteeseen. Päätelaite todennetaan oikeaksi esimerkiksi siihen asennetun tietoturvasertifikaatin avulla.

Kun VPN-yhteys on muodostettu, päätelaitteen ohjelmiston ja terminoivan laitteen välille muodostetaan salattu tunneli. Se tarjoaa turvallisen ja suojatun pääsyn sisäverkon palveluihin.

Tunneleiden kautta tuleva liikenne reititetään tavallisesti vielä palomuurin kautta, ja sitä täydennetään tarvittaessa myös muilla tietoturvakontrolleilla.

NAC-teknologia ei tyydy pelkkään tunnistamiseen

Kun uusi laite liittyy nykyaikaiseen lähiverkkoon langattoman WLAN-aseman tai kytkimen kautta, sen pääsyoikeudet voidaan halutessa todentaa automaattisesti. Todentamisen voi toteuttaa esimerkiksi laitteelle asennettavalla tietoturvasertifikaatilla. Jos verkkoon liittyvä laite ei täytä sille asetettuja vaatimuksia, niin sen sen pääsy verkkoon estetään. Jos laite tunnistetaan luvalliseksi, on tarkistusprosessi loppukäyttäjälle käytännössä näkymätön.

Verkkoon liittyvien käyttäjien – siis ihmisten – käyttöoikeudet voi puolestaan todentaa esimerkiksi käyttäjätunnuksen, varmennekortin, monivaiheisen tunnistautumisen tai näiden yhdistelmän avulla.

Tietoverkkoihin liittymistä voidaan hallinnoida myös politiikkapohjaisesti. Silloin tarvitaan verkon pääsynhallintaan kehitettyä NAC-teknologiaa (Network Access Control). Tässä teknologiassa verkkoon liittyvää päätelaitetta tai käyttäjää ei ainoastaan tunnisteta, vaan päätelaitteelle tehdään erilaisia tietoturvapolitiikan mukaisia tietoturvatarkastuksia. Onko liittyvän laitteen virustorjunta ajan tasalla? Käyttääkö laite vaadittua käyttöjärjestelmää?

Jos laite ei läpäise tietoturvapolitiikan kaikkia ehtoja, sille voidaan antaa rajoitettu pääsy verkkoon, jotta käyttäjä pääsee päivittämään esimerkiksi virustorjunnan ajan tasalle. Kun vaatimukset on täytetty, laite voidaan todeta luotettavaksi, ja se pääsee liikennöimään verkkoon normaalisti.

Zero Trust -malli olettaa kaikki laitteet epäluotettaviksi

Uusi malli palveluihin pääsyn kontrolloinnissa on niin sanottu Zero Trust -ajattelutapa. Se on kehitetty vastaamaan tyypilliseen tämän päivän haasteeseen: yritykset käyttävät pilvipohjaisia, nopeasti muuttuvia palveluita, joita käyttäjien on päästävä käyttämään sijainnista riippumatta ja tietoturvan vaarantumatta.

Malli lähtee siitä olettamuksesta, että kaikki käyttäjät ja päätelaitteet ovat epäluotettavia. Siksi käyttäjän täytyy todentaa henkilöllisyytensä vahvalla tunnistuksella. Palveluihin pääsyä todennetaan jatkuvasti, ja myös päästämisen riskejä arvioidaan jatkuvasti.

SD-WAN -verkot vahvistavat tietoturvaa toimipisteiden välillä

Tämän päivän yritysverkoissa uudet, toimipisteitä, konesaleja ja pilvipalveluita yhdistävät tietoliikenneverkkojen toteutukset tehdään pääasiassa SD-WAN -tekniikalla (Software Defined Wide Area Network).

Se tekee toimipisteiden, konesalien ja pilvipalveluiden välisestä liikennöinnistä tietoturvallista, sillä kaikki liikenne verkon reunalaitteiden ja -pisteiden välillä salataan.

Keskitetty järjestelmä hallinnoi yhteyksien salaukseen tarvittavia avaimia ja huolehtii salauksen käytännön toteutuksesta, joten SD-WAN -ratkaisun hallinta on helppoa.

SD-WAN -ratkaisuissa tietoliikenteen siirtotienä eli ns. underlay -verkkona voidaan käyttää mitä tahansa IP-liikennettä (Internet Protocol) reitittävää verkkoa. Siirtotien tehtävänä on yhdistää SD-WAN -verkon pisteet toisiinsa ja mahdollistaa niiden pisteiden välille salatun SD-WAN -verkkotason muodostaminen. Käytännössä siirtotie voi siis olla esimerkiksi internet tai tietoliikenneoperattoreiden MPLS- tai mobiiliverkkojen päällä toteutettu yhteyspalvelu. Jos halutaan, ettei SD-WAN -verkon liikenne kulje julkisessa internetverkossa, niin silloin siirtotienä voidaan käyttää esimerkiksi MPLS-pohjaisia virtuaalisia VPN-verkkoja, jolloin toteutuksien tietoturva paranee. Usein kriittiset SD-WAN -yhteydet toteutetaan erillisessä MPLS-verkon päälle tehdyssä virtuaalisessa VPN-verkossa, mutta niitä saatetaan varmistaa mobiili- ja internetverkkojen kautta.

SD-WAN -tekniikan reunalaitteissa voi olla myös muita tietoturvaominaisuuksia. Tällöin puhutaan UTM-laitteista (Unified Threat Management). SD-WAN -tekniikalla tehtävän yhteyksien salauksen ja reitityksen optimoinnin lisäksi UTM-laitteista voi löytyä esimerkiksi palomuuri, tunkeutumisen havainnointi ja esto, virusten sekä haittaohjelmien tunnistus ja suodatus, web-liikenteen suodatus sekä ominaisuuksia arkaluonteisen tai luottamuksellisen datan siirron estämiseen.

DDoS-pesurit torjuvat hajautettuja palvelunestohyökkäyksiä

Hajautettujen palvelunestohyökkäysten (DDoS, Distributed Denial of Service) toimintamalli on yksinkertaistettuna tämä: Hyökkääjä masinoi bot-verkon kuormittamaan tiettyä palvelua, kuten verkkopankkia, yhtäaikaisesti useista eri lähteistä tulevalla haittaliikenteellä. Jos tilanteeseen ei ole varauduttu ennalta, tiedonsiirtoverkot tai kohteena olevien järjestelmien prosessointikapasiteetti tukkeutuvat niin, että palvelun normaali käyttö estyy. Palvelunestohyökkäyksillä hyökkääjä pyrkii siis vaikuttamaan tietoverkossa näkyvän palvelun saatavuuteen.

Koska hajautetussa palvelunestohyökkäyksessä haitallisen liikenteen lähteitä voi olla lukuisia ja ne voivat vaihdella, on mahdotonta suodattaa hyökkäykset yksittäisiä hyökkäyksen lähdeosoitteita estämällä. Tällaisten hyökkäyksen estämiseen on kehitetty esimerkiksi niin sanotuksi DDoS-pesuriratkaisuiksi kutsuttuja teknologioita. Ne seuraavat jatkuvasti suojattavan verkon ja palveluiden liikennettä ja tunnistavat siitä hyökkäysyrityksiä. Tunnistamisen jälkeen hyökkäyksen kohteena olevaan palvelimeen kohdistuva liikenne ohjataan erilliselle pesurille, joka suodattaa haitallisen liikenteen pois normaalin liikenteen seasta. Näin saadaan hyökkäystilanteessa palvelu näkymään ja toimimaan normaalisti.

Volymetriset eli korkeaan tietoliikenteen määrään perustuvat palvelunestohyökkäykset saattavat aiheuttaa ongelmia myös muille palveluille, joita tuotetaan samoista verkkosegmenteistä kuin hyökkäyksen varsinaisena kohteena olevaa palvelua. Silloin torjunta saattaa vaatia muitakin mekanismeja, kuten hyökkäävän liikennetyypin määrän rajoitusta (rate-limit). Haitallista liikennettä voidaan ohjata myös niin sanottuun mustaan aukkoon eli tuhota sitä. Lisäksi voidaan käyttää geo-blokkausta, eli liikenne palveluun sallitaan vaikkapa vain Suomesta,

jolloin muualta maailmasta tuleva liikenne tuhotaan.

Kvanttiteknologia muuttaa tulevaisuutta

Tulevaisuudesta kiinnostuneiden katseet ovat tällä hetkellä kvanttitietokoneissa. Kehittyvä laskentateho pystyy todennäköisesti murtamaan nykyisin käytetyt salausalgoritmit kohtuullisessa ajassa. Siksi parhaillaan kehitetään uudenlaisia salausalgoritmeja, joilla salattuun tietoon kvanttitietokoneillakaan ei päästäisi helposti käsiksi. Toinen esimerkki kvanttiteknologian sovelluskohteista on tietoliikenteen salauksessa tarvittavien salausavainten vaihto: sitä voidaan tehdä kvanttiteknologiaan pohjautuen esimerkiksi valokuidun yli turvallisesti siten, että avainten vaihtamiseen liittyvän tiedonsiirron salakuuntelu ei onnistu paljastumatta.

Tulevaisuudessakin tietoliikenneverkkojen tietoturva koostuu monesta osasta, kuten fyysisten riskien torjumisesta, järjestelmiin tunkeutumisen estämisestä sekä laittoman salakuuntelun ja tiedon muuntamisen ehkäisemisestä. Mukana on myös entistä enemmän analytiikkaa, millä saadaan tunnistettua eri tietoverkoissa olevien tietoturvakomponenttien keräämien tietojen perusteella haitallinen toiminta ja liikenne. Valvontajärjestelmien tuottamien hälytysten ja niiden reagointiin liittyvien prosessien on oltava myös kunnossa.

Teknologiat kehittyvät ja vaihtuvat toisiin, mutta jatkossakin vahvat, korkean käytettävyyden tietoliikenneverkot rakennetaan yhdistelemällä useita eri teknisiä ratkaisuja ja toimintamalleja.

Hannu Muikku johtaa Cinialla noin 70 tietoliikenneasiantuntijan palvelutuotantoyksikköä. Hänen tiiminsä vastaa vaativien tietoverkkototeutusten ja niihin kytkeytyvien palveluiden suunnittelusta, operoinnista ja valvonnasta.

Tietoliikenneverkkojen tietoturva

- Hyödynnetään useita teknologioita eri käyttötarkoituksiin

- Teknologiat valitaan suojattavan ympäristön ja datan mukaan

- Monet nykyaikaisista teknologioista ovat jollakin tavalla sidoksissa julkipilveen, joten käyttäminen kriittisissä erillisverkoissa vaatii tapauskohtaista tarkastelua, osa pilviratkaisuista on käytettävissä myös suljetuissa ympäristöissä

- Tietoturva ei ole ainoastaan suojaavaa teknologiaa, vaan myös arkkitehtuuria, tiedon keräämistä, analysointia ja hyödyntämistä, valvonta- ja reagointikykyä sekä toimintamalleja eli prosesseja.

Maanpuolustuksen Viestisäätiön kannatusyhdistys kiittää seuraavia yhteistyökumppaneita vuodesta 2023:

Aerial Oy, Bitwise Oy, Cojot Oy, Conlog Group Oy
Kaisanet Oy, Loihde Oyj, Milcon Oy, Millog Oy, Nixu Oy
Vaisala Oyj, Ålands Telefonandelslag

Viestisäätiön kannatusyhdistys esittää parhaimmat kiitokset myös lukuisille yksityisille henkilöille, jotka ovat osallistuneet keräykseen v. 2023.

Toivotamme Rauhallista Joulua ja Onnellista Vuotta 2024!

Reima Blomqvist
Puheenjohtaja

Kirsi Salo
Sihteeri

Satelliitit muuttavat sotilasviestiverkkoa

Joukot saavat haltuunsa tiedustelutuloksia, jotka kiidätetään taistelukentällä sijaitsevaan esikuntaan. Materiaali käsitellään ja lajitellaan nopeasti. Muutamia tunteja myöhemmin valokopiot tärkeimmistä ainaistoista ovat Pentagonin tutkittavana. Täydennyspyyntö laaditaan USA:n lentotukikohdassa Euroopassa. Muutamia tunteja myöhemmin paperisota on siirtynyt USA:n puolelle. Puolustusministeriön virkamies ottaa puhelun saadakseen välittömät tilannetiedot taistelukentältä maapallon toiselta puolen. Samanaikaisesti annetaan toisia kanavia käyttäen käskyjä maanosasta toiseen ja ilmakuljetusjoukkojen komentopaikka pitää yhteyksiä tukikohtansa esikuntaan.

Kaikki nämä ovat nykypäivän yhteyksiä tapahtuen satelliitin välityksellä. Yhteysmahdollisuudet ovat äärettömät ja voidaan sanoa satelliittiyhteyksien lopettaneen romantiikan sotilaallisilta operaatioilta. Sotilasviestiverkko on kehittymässä nopeasti ja satelliitti on nykyään vain kiertoradallaan oleva toistoasema – tehokas, taloudellinen, tarkkuustyönä valmistettu horisontin laajentaja.

Satelliitin olemassaolon merkityksen toteaa muistelemalla aiempia hitaita, epävarmoja, katkoksille alttiita ja kalliita viestiyhteyksiä. Ionosfäärietenemiseen perustuvien HF-yhteyksien haittana on niiden ennustettavuus, joten vihollinen tietää milloin kaukoyhteydet ovat käytettävissämme. Merenalaiset kaapelit ovat käyttökelpoisia, mutta kalliita, haavoittuvia eivätkä omaa liikkuvuutta ja määrä on vähäinen. Mikroaaltolinkkien käyttömahdollisuuksia rajoittavat asemapaikalle asetettavat vaatimukset; tarvitaan monia kalliita releasemia eivätkä valtameren takaiset yhteydet ole mahdollisia. Ennen satelliitteja sotilasyhteyksien saanti niin taistelukentällä kuin merelläkin oli aina epävarmaa. Sanoman viestitys saattoi vaatia tunteja, vuorokausia jopa viikkoja. Liikkuvien yhteyksien saanti horisontin taakse oli epäluotettavaa.

Nykyaikainen sotilasviestiyhteysjärjestelmä kehittyy jatkuvasti samalla kun kustannukset kanavaa kohden laskevat. Uusimpiin satelliittireleasemiin käytetyllä rahalla saataisiin yhä vähemmän kanavia käytettynä kaapeleihin, mikroaaltolinkkeihin ja korkealaatuisiin HF-yhteyksiin. Jo pelkästään tämän seikan perusteella on satelliittiyhteysjärjestelmä paras sijoitus. Sotilaiden ei kuitenkaan pidä viestiyhteysjärjestelmissään turvautua yksinomaan satelliittijärjestelmään. Nykyisillä järjestelmillä on ehdottomasti rajoituksensa. Ne kykenevät palvelemaa ainoastaan korkeimman prioriteetin liikkuvia käyttäjiä.

Maavoimilla, laivastolla ja taktisilla ilmavoimilla on kullakin omat vaatimuksensa. UHF- alueen valinta johtuu ensisijaisesti antennien suuntausongelmasta. UHF- kanavien erittäin runsas käyttö kiihdyttää teknisten ratkaisujen etsimistä korkeammilta, vähäisemmässä käytössä olevilta taajuuksilta. Ilmeinen lähiaikojen sotilaallinen vaatimus kohdistuu yleisjoukkojen viestiyhteyssatelliitteihin. Strategiset käyttäjät tarvitsevat omiin toimintaolosuhteisiinsa soveltuvan haavoittumattoman yhteysverkon. Pitkäaikaiset satelliittijärjestelmät yhdessä esim. suunnittelun ELF-järjestelmän (sukelluksissa oleviin sukellusveneisiin yhteyttä pitävä järjestelmä) kanssa saattavat mahdollistaa näiden vaatimusten toteuttamisen. Järjestelmä ehkä saataisiin aikaan muutamalla erittäin korkealla olevalla geosynkronisella satelliitilla, useilla alempana olevilla satelliiteilla, napojen kautta kulkevilla elliptisillä radoilla olevilla satelliiteilla tai jollakin näiden yhdistelmillä.

Tulevaisuuden vaatimukset voidaan ennustaa. Tullaan tarvitsemaan yhä suurempia kaistanleveyksiä yhteyksien muuttuessa digitaalisiksi ja aikajakoon perustuviksi. Lopuksi tulevat satelliittiyhteydet siirtymään optiselle taajuusalueelle. Satelliittien väliset laser-yhteydet tulevat väistämättä käyttöön. Tulevaisuuden järjestelmissä säteilytehon on oltava suurempi ja taajuuksien samanaikainen käyttö on oltava mahdollista. Suunnattavat kapeakeilaiset antennit ovat tähän ilmeisin ja tehokkain ratkaisu, joka samalla rajoittaa häiriöitä.

Tutkimus- ja kehittämisbudjettien rajoittamisella voidaan ainoastaan hidastaa liikkuva satelliittijärjestelmän käyttöönottoa, sillä sellaisen tulo on väistämätön. Tullessaan tällaiset satelliitit muodostavat pääosan yhteysjärjestelmästä eivätkä ole enää pelkkiä radiohorisontin laajentajia.

Artikkelin kirjoittaja: Veli-Matti Pesola

Heidi Helwe työskentelee kyberturvallisuuskonsulttina IBM:n konsultointipalveluissa. Kirjoittajan erikoisosaamista on organisaatioiden tietoturvaheikkouksien ja haavoittuvuuksien tunnistaminen, sekä korjaavien toimenpiteiden suunnittelu ja jalkauttaminen liiketoiminnan tarpeet huomioiden.

Sami Serpola toimii Suomen IBM:n tietoturvateknologia yksikössä ja työskentelee läheisesti tekoälyä hyödyntävien analytiikka-, tutkinta- ja tietoturvateknologioiden parissa. Kirjoittajalla on reilun 25 vuoden kokemus informaatioympäristöön rakennettavien järjestelmien kehittämisestä, arkkitehtuurisuunnittelusta, analytiikasta sekä teknologian hyödyntämisestä yritysten ja organisaatioiden liiketoiminnassa.

TEKSTI: HEIDI HELWE JA SAMI SERPOLA

Henrin vesittynyt viikonloppu

Tietoturvahyökkäys voi johtaa huomaamattomasta alusta ennennäkemättömän nopeaan eskalaatioon ja vaarantaa pahimmassa tapauksessa koko kriittisen infrastruktuurin. Tekoäly lisää uusia mahdollisuuksia sekä kyberturvauhkien torjuntaan että niiden toteuttamiseen. Mitä tapahtuu, jos esimerkiksi vesilaitos joutuu vihamielisen kyberhyökkäyksen kohteeksi?

Vesilaitoksen tietoturva-alihankkija Henri sai perjantai-iltana, juuri ennen viikonloppua, puhelun tutusta numerosta. Soittaja oli hänen yhteyshenkilönsä Timppa. Timppa kyseli, miten edellisen viikonlopun kalareissu oli mennyt ja kertoi sitten Henrille kriittisestä tietoturvahaavoittuvuudesta, joka koski juuri heidän vesilaitoksensa käytössä olevaa laitetta. Haavoittuvuus oli sen verran kriittinen, että sitä hyödyntämällä voisi IoT-laitteen etäyhteyden avulla manipuloida vesilaitteiden säätöjä. Tämä taas aiheuttaisi ongelmia koko vedenjakeluverkostoon. Vaikka puhelun yhteys oli hieman huono, sai Henri kaiken keskeisimmän tiedon ylös.

Henri ymmärsi heti, että kyseessä on haavoittuvuus, joka tulisi korjata välittömästi. Timppa itse oli jo lähtenyt työpaikalta, joten hän pyysi Henriä avaaman etäyhteyden IoT-laitteeseen, jotta tarvittava korjauspäivitys voitaisiin haavoittuvuuden poistamiseksi tehdä. Henri ei nähnyt tässä mitään ongelmaa. Puhelu tuli luotettavasta numerosta tutulla äänellä. Tämän lisäksi Henri muisti, että vesilaitoksen tämän vuoden tietoturvan kehityskohteena oli teknisten laitteiden tehdasasetusten koventaminen. Muiden uudistusprojektien vuoksi laitteiden koventamista oli siirretty usein kvartaalista seuraavaan. Tästäkin syystä oli tärkeää reagoida kriittisiin päivityksiin.

Itse päivitys asentui hyvin helposti, eikä mitään ongelmia havaittu. Henri oli valmis viikonlopun viettoon. Tunnollisena miehenä hän kuitenkin halusi vielä tiedottaa muita vesilaitoksia ja toimijoita uudesta haavoittuvuudesta IoT-laitteessa. Henri julkaisi huoltovarmuuslaitoksen infosivuilla kehotuksen päivittää haavoittuvuuteen korjaus.
Ne toimijat, jotka näkivät ilmoituksen ja halusivat päivittää IoT-laitteen viimeisimmän version hyödynsivät hakuselainta. Hakukoneen ensimmäiset osumat ohjasivat luotettavan näköisille sivuille, joista viimeisin päivitys oli ladattavissa.

Sosiaalinen media vuotaa kyberrikollisille

Henri ei tiennyt, että puhelu, jonka hän vastaanotti Timpalta, oli tekoälyä hyödyntämällä toteutettu yhteydenotto, jossa puhelun soittajan ääni saatiin kuulostamaan tutulta Timpalta. Henri ja Timppa oli kyetty profiloimaan tekoälyn avulla keskeisiksi henkilöiksi vedenjakeluprosessissa ja he olivat olleet jo pitkään hyökkäyksen ja tietoturvaurkinnan kohteena. Heistä oli tehty kattava selvitys sosiaalisen median tilien perusteella. LinkedInin kautta oli saatu tietää IoT-laitteista, joita Henri toimittaa, ja myös yhteys vesilaitokseen oli helposti löydettävissä. Henri oli lisäksi julkaissut paljon kuvia yhteisistä juhlista ja tapahtumista eri alustoille. Tämä oli alkuosa

tapahtumaketjua, joka aiheutti alueen vesilaitoksille, tehtaille ja asukkaille laajaa vahinkoa.

IoT-laitteen päivityksen yhteydessä haittaohjelma asentui vesilaitokselle ja loi asennuksen yhteydessä takaportin etäyhteyden mahdollistamiseksi. IoT-laitteessa oli nyt avoin portti hyökkääjille. Tunnin kuluessa hyökkääjillä oli yhteys laitoksen verkossa oleviin muihin laitteisiin. Hyökkääjät olivat myös päässeet hallintakoneisiin käsiksi, ehkä jopa liian helposti, olihan koventamissuunnitelmaa lykätty jo kolme kertaa.

Hyökkääjäryhmällä oli paljon tietoa laitoksen työntekijöistä, myös heidän käyttämistänsä etäyhteysohjelmista. He tiesivät, millä käyttäjänimillä kirjaudutaan ja hyökkääjillä oli tiedossaan työntekijöiden mahdollisia salasanoja. Työntekijät olivat noudattaneet vesilaitoksen salasanapoliitiikkaa, paitsi sitä, jossa mainitaan, että salasanaa ei saisi käyttää muissa palveluissa. Moni oli laiminlyönyt tämän ja käyttänyt samaa laitoksen salasanaa muissa käyttämissään palveluissa kuten Facebookissa ja LinkedInissä. Muutama näistä palveluista oli kärsinyt tietoturvaloukkauksesta, jonka yhteydessä kaikki käyttäjätiedot ja salasanat olivat vuotaneet. Hyökkääjät kykenivät yksinkertaisella metodilla koostamaan vesilaitoksen pääkäyttäjätunnukset vuotaneista tiedoista, joilla voitiin toteuttaa pääsy vesilaitoksen kriittisiin järjestelmiin.

Tietoverkko valuu vesijohtoverkostoon

Tapahtumien edetessä terveyskeskusten päivystykseen alkoi hakeutua ihmisiä huimaus- ja pahoinvointioireiden vuoksi. Vesilaitokselle on tullut myös ilmoituksia kloorin mausta juomavedessä. Vaikka vesilaitos saa usein tämäntapaisia ilmoituksia, on ilmoitusten määrä huolestuttavan suuri. Vesilaitos teki vedelle tarkastusmittaukset ja havaitsi, että veden lipeän ja kloorin pituisuudet ylittävät sallitut raja-arvot hälyttävin lukemin. Vesilaitos tiedotti terveysviranomaisia ja vesi asetetaan käyttökieltoon. Myös muiden kaupunkien päivystykseen alkoi hakeutumaan potilaita yllättävien pahoinvointioireiden vuoksi.

Hakkerit olivat manipuloineet kloorin ja lipeän syöttöarvoja ja suurentaneet niitä. Arvoja ylittävää ylisyöttöä oli tapahtunut jo yli kolme tuntia. Määrät olivat terveydelle haitallisia ja tämä alkaa näkymään asukkaiden pahoinvointioireina. Henri sai puhelun palata pikaisesti vesilaitokselle, lisäksi sisäinen tietoturvaloukkauksiin erikoistunut tiimi kutsutaan paikalle selvittämään asiaa. Vielä tässä vaiheessa vesilaitos ei ollut tietoinen hakkereista, jotka ovat heidän järjestelmissään. Henri lähti ajamaan vesilaitokselle mökkinsä pihalta, jonne hän saapui vain muutama minuutti aiemmin.

Sumutus onnistuu lokitietojen poistolla

Pian vesilaitoksella huomattiin, että tilanteen korjaaminen ei olekaan niin helppoa. Kriittisten järjestelmien pääkäyttäjien tunnukset eivät enää toimi. Hyökkääjät, jotka saivat laajat oikeudet järjestelmiin, olivat tehneet mahdottomaksi pääkäyttäjien kirjautumisen järjestelmiin. Useiden yritysten jälkeen yksi vesilaitoksen käyttäjistä pääsi onnistuneesti kirjautumaan järjestelmiin. Vesilaitoksen tärkein tehtävä oli selvittää, mitä on tapahtunut ja tehdä tilannearvio.

Lokitiedoissa havaittiin epäselvyyksiä, aikaleimoissa ja tapahtumissa on epäjohdonmukaisuuksia sekä selviä tapahtumia puuttui. Tässä kohtaa tietoturvaloukkauksiin erikoistunut tiimi teki johtopäätöksen, että heillä on laajempi hyökkäys meneillään. Selvisi, että suuria määriä lokitietoja kriittisien järjestelmien toiminnoista oli poistettu. Erityisen hälyttävää oli huomata lokitietojen puutteellisuus kriittisten järjestelmien osalta. Lokitietojen poistaminen on yleistä moniosaisessa hyökkäyksessä. Tällä pyritään vaikeuttamaan hyökkäyksen kohteena olevan organisaation mahdollisuutta havaita itse hyökkäystä, tilannekuva-arvion muodostamista, sekä kyvykkyyttä vastata hyökkäykseen.

Pian viranomaiset saivat ilmoituksen jätevesipuhdistamossa tapahtuneesta kemikaalivuodosta. Kemikaalivuodot ovat yleensä erittäin harvinaisia automatisoidun annostelun vuoksi, mutta hyökkääjät olivat myös onnistuneet saamaan pääsyn jätevesipuhdistamon valvontalaitteisiin. He manipuloivat automaatioannostelun arvoja räikeän vaarallisiin lukemiin, mikä mahdollisti kemikaalivuodon. Laitoksella aloitettiin hätätoimet vedenjakelun estämiseksi, virheellisten puhdistusarvojen korjaamiseksi sekä kriisiviestinnän toteuttamiseksi.

Useat vedenjakelulaitokset asettivat vetensä käyttökieltoon. Vahinkojen laajuutta tutkiessaan viranomaiset totesivat mahdolliseksi, että kyseessä on kohdistettu hyökkäys vedenjakelulaitoksiin, koska on hyvin epätodennäköistä, että samanaikaisesti useissa vedenjakelulaitoksissa ympäri maata ilmenisi näin paljon samankaltaisia poikkeustilanteita. Viranomaiset käynnistivät vahinkojen rajaamistoimenpiteet ja määräsivät vahinkojen torjuntaryhmän selvittämään mahdollisia yhteyksiä. Sairaaloiden päivystykset olivat jo ehtineet ruuhkautua potilaista, jotka olivat juoneet juomavettä ennen vedenkäyttökiellon julistamista.

Oppikirjahyökkäys vesitti tietoturvan

Useat maan vesilaitokset ja heidän henkilöstönsä olivat olleet hakkereiden tarkkailun alaisena viimeiset kahdeksan kuukautta. Laitoksista ja heidän henkilöstöstään oli kerätty dataa, jonka perusteella tiedettiin, mitä työrooleja kullakin on ja kenen tunnuksilla olisi tuloksellis-

ta toteuttaa järjestelmien manipuloinnit. Hakkerit saivat kartoituksessaan tietoonsa tekniset laitteet sekä ohjelmistot, joita vedenjakelulaitokset käyttivät. Heidän tiedoissaan oli laitteiden tehdasasetukset ja haavoittuvuudet, joita voisi hyödyntää, jos laitteita ei oltu kovennettu.

Kaikki alkoi perjantaisesta tekoälyn avulla toteutetusta puhelusta alihankkijalla työskentelevälle Henrille. Hakkereiden tarkoitus ei ollut alun perin hyökätä niin moneen vedenjakelupisteeseen kerralla, mutta ilokseen he huomasivat, että kolme muutakin laitosta latasi haittaohjelman, jossa takaportti oli. Muut vedenjakelulaitokset olivat ladanneet tuon saman ”Kriittisen päivityksen”, koska luotettu ja alalla hyvin tunnettu alihankkija Henri oli näin kehottanut. Koska hyökkääjät olivat suunnitellusti kokoontuneet testaamaan hyökkäystä, oli heillä resursseja toteuttaa useita iskuja kerralla.

Hyökkäyksen takana oli toisen valtion tukema hakkeriryhmä, jonka tarkoituksena oli testata mahdollisuutta aiheuttaa kriittisten infrastruktuurin toimijoille haittaa sekä kerätä hyökkäyksen edetessä mahdollisimman paljon teknistä tietoa vedenjakelulaitoksen teknologiasta, verkoista sekä ohjelmistoista. Motiivina oli kartoittaa ja testata, kuinka mahdollisen sodan aikana voitaisiin luoda kriisitilanteita maan kriittisiin toimijoihin ja aiheuttaa mahdollisimman paljon vahinkoa ja häiriötä. Kyberiskujen tunnistaminen on tärkeä osa ennakointia ja pidäke muiden operaatioiden etenemiselle.

Uhkamallinnus ja ennakointi avainasemassa

On tärkeää tunnistaa oman organisaation tietoturvan taso ja saada ymmärrys tärkeimmistä kehitystoimenpiteistä. Usein organisaatioissa on ongelmana liian suuri määrä kehitystoimenpiteitä, joita ei ole järkevästi priorisoitu. Uhkamallinnuksen avulla pyritään tunnistamaan mahdolliset infrastruktuurin, järjestelmien ja sovelluksien haavoittuvuudet, jotka ovat mahdollisia uhkia organisaatiolle. Uhkamallinnus on erittäin tärkeää, koska sen avulla saadut tulokset antavat organisaatiolle hyvän näkymän myös tarvittaviin kehitystoimenpiteisiin. Useasti organisaatiossa ei kuitenkaan huomata uhkia, joissa työntekijä tahallisesti toteuttaa haitallisia toimenpiteitä. On kuitenkin tärkeää käydä lävitse tämäkin skenaario asiantuntijoiden kanssa, jotka tietävät mahdollisuudet väärinkäytöksille.

Useissa hyökkäyksissä on tunnetusti hyödynnetty vuotaneita tai kaapattuja työntekijän tunnuksia. Kun uhkamallinnuksessa uhat ja mahdolliset skenaariot on kartoitettu, tulee seuraavaksi päättää suojaavista tietoturvakontrolleista, joilla voidaan estää uhkien toteutuminen sekä minimoida riskit. Myöskin it-infrastruktuurin, tietoverkkojen, järjestelmien ja sovellusten tekniset testaukset näihin perehtyneillä asiantuntijoilla auttavat tunnistamaan organisaation haavoittuvuudet ja uhat.

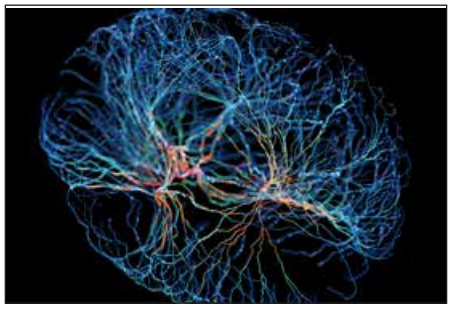
Uhkamallinnuksella ja teknisellä testauksella saadaan tehokkaasti tunnistettua tietoturvan heikkoudet, jolloin voidaan suunnitella keskitetysti tietoturvakontrollit ja oikea teknologia pienentämään kyberrikollisten hyökkäysvektoria. Valitettavasti liiankin monessa organisaatiossa tietoturvan kehittäminen on rajoittunut vain tietoturvakartoituksesta saatuihin kehitystoimenpiteisiin, jolloin organisaatiolta puuttuu ajantasainen tieto haavoittuvuuksista ja mahdollista uhista.

Tekoälyn käyttö lisää uhkia ja mahdollisuuksia

Hyökkääjät kykenevät hyödyntämään tekoälyä monin eri keinoin. Tekoälyllä voidaan tehostaa erilaisten hyökkäysskenaarioiden ideointia sekä toteuttaa kerätyn tiedon analysointia entistä tehokkaammin. Kuten edeltävässä fiktiivisessä vesilaitos-tarinassa voidaan tekoäly valjastaa hyökkäyksessä imitoimaan henkilöä ja siten manipuloida toinen osapuoli tekemään haluttuja toimenpiteitä.

Uhkamallinnuksen avulla kyetään tunnistamaan ne operatiivisen toiminnan keskeiset kohdat, joihin on syytä keskittyä. Tietoturvaprosessien tiedostaminen, harjoittelu ja hallitseminen ovat tärkeimpiä toimia tietoturvallisen toiminnan kannalta, erityisesti kriittisten järjestelmien ja operaatioiden ympärillä.

Tekniikkana vahvennettu tunnistautuminen on hyvä toimintatapa, jolla kyetään varmistamaan henkilön identiteetti, mutta tämän hyödyntäminen puhelinkeskustelussa voi olla haasteellista käytännössä – onhan tietoturva jatkuvaa tasapainottelua käyttömukavuuden ja tietoturvaprosessien välillä. Tarinan Henrin olisi pitänyt soittaa takaisin Timpalle ja varmistaa, että puhelu ja IoT-ohjelmiston päivitys-



pyyntö oli tullut häneltä ja siten Henri olisi kyennyt varmistamaan puhelun aitouden.

Edellä kuvattu hyökkäys lähti leviämään inhimillisen erehdyksen kautta, joka johti vakavaan tietoturvamurtoon. Nykyisen teknologian on kyettävä suojaamaan It-ympäristöä vastaavanlaisissa kriittisissä operaatioissa, mikäli mahdollinen tietoturvamurto tai -murron yritys tapahtuu.

Pitkäkestoiset ja monimutkaiset hyökkäykset toteutetaan hyvin organisoidusti ja usein näiden takana on joko vahvasti valtiovallan tukema ja rahoittama ryhmä tai suoraan tietty valtio. Suuret kansainväliset tietoturvayhtiöt keräävät, analysoivat ja koostavat malleja erityyppisistä APT (Advanced Persistent Threat) hyökkäyksistä ja yksilöivät näihin kohdistuvia erityispiirteitä sekä jakavat tätä koostettua tietoa omassa ekosysteemissään yrityksille, organisaatioille ja tietoturvaan erikoistuneille palvelun tarjoajille.

Mikäli tällainen tieto olisi ollut hyödynnettävissä vesilaitoksen tietoturvakeskuksessa ja valvontajärjestelmät olisivat kyenneet analysoimaan kerättyä tietoa, olisi vesilaitos kyennyt tunnistamaan selkeitä viitteitä siitä, että tietyt aiemmin lähetetyt kalasteluviestit vesilaitosta kohtaan sekä muut mahdolliset hyökkäystä valmistelevat toimet ovat yhteydessä isompaan kokonaisuuteen ja liittyvät mahdollisesti tiettyyn APT-hyökkäykseen. Tekoälyn avulla nämä ulkoisesti toisistaan irralliset uhkatapahtumat olisi kyetty kuvaamaan esim. MITRE ATT&CK -viitekehyksen mukaisesti ja siten tietoturvaan erikoistunut valvontajärjestelmä olisi kyennyt ohjaamaan havainnot tehtäviksi toimenpiteiksi joko automaattisesti tai tietoturva-asiantuntijoiden suoritettaviksi.

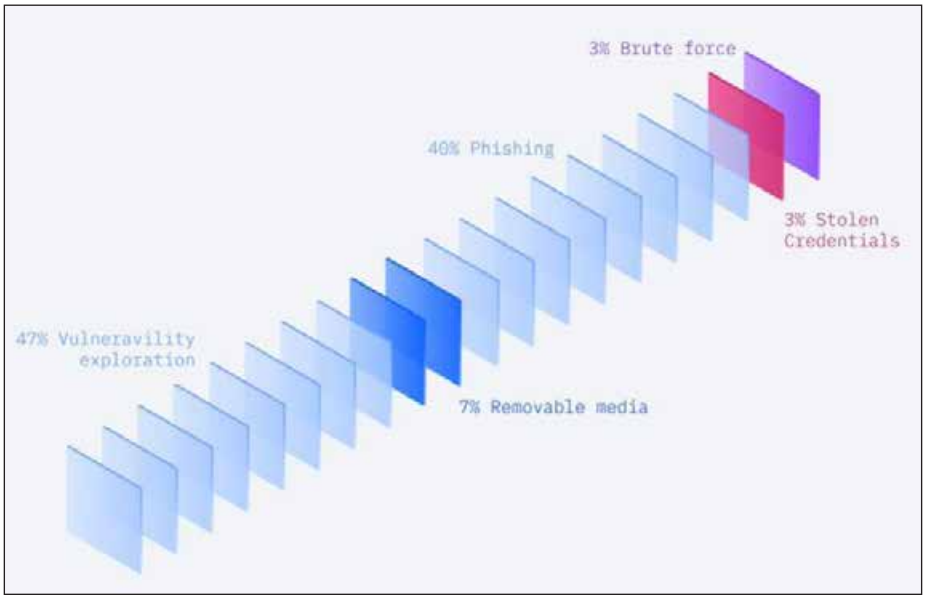
Valmiit tietoturvaan rakennetut kyvykkyydet, valmiit ohjeistukset ja pelikirjojen pohjat sekä sääntömääritykset, joita nykyaikaiset tietoturvajärjestelmät tarjoavat, voidaan hyödyntää niin uhkamallinnuksen määrittelyssä ja suunnittelussa kuin itse operatiivisessa tietoturvavalvonnassa. Näillä jo valmiiksi toteutetuilla ratkaisuilla tietoturvakäytäntöjen ja toimintojen jalkauttaminen organisaatioon on aiempaa nopeampaa ja mutkattomampaa.

Tekoäly tehostaa riskien analysointia

Älykkäiden tekoälyä hyödyntävien tietoturvajärjestelmien sisäänrakennetut analysointimallit sekä niihin liitetyt prosessit kykenevät yhdistämään useista eri tietoturvajärjestelmistä ja lähteistä saatavaa laitteiden loki- ja verkkoliikenteen tietoa sekä ympäristön historiatietoa keskenään ja koostamaan siitä ketjutettua uhkahavaintotietoa ja siten yksilöimään mahdollisia APT-hyökkäyksiä. Tietoturvaan keskittyneiden yritysten valmiiden analyysitietojen liittäminen ja peilaaminen osana yrityksen uhkahavainnointia nostaa myös esille ympäristöön kohdistuvia ulkoisia sekä sisäisiä uhkia ja niiden mahdollisia vaikutuksia.

Tekoälyyn pohjautuvilla teknisillä sovellutuksilla, jotka kykenevät käsittelemään ulkopuolisen uhka-analyysin sisältöä asiakkaan omasta ympäristöstä kerättyyn uhkatietoon peilaten säästetään paljon aikaa uhkatilanteiden analysoinnissa sekä haittojen minimoinnissa. Älykkäät tietoturvajärjestelmät kykenevät keräämään mm. vesilaitoksessa käytettävien laitteiden ominaisuuksista ja niiden käyttäytymisestä tietoa, jonka avulla jokaiselle laitteelle muodostetaan laitteelle ominainen käyttäytymisprofiili.

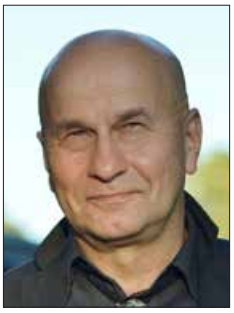
Profiloinnin avulla tietojärjestelmät kykenevät ilmoittamaan myös mikäli uusia ja/tai tunnistamattomia laitteita on ilmaantunut valvottavaan ympäristöön tai olemassa olevien laitteiden käyttäytyminen aiemmasta on muuttunut. Ympäristössä olevien laitteiden käyttäytymisen yhdistäminen loki- ja verkkoliikenteestä saatavaan tietoon, määriteltyihin tietoturvatointatapoihin liittyvät ristiriidat (esim. lokitietojen manipulointi tai poistaminen), luotettavasta lähteestä saatavan uhkanäkymätiedon ja tämän tietokokonaisuuden analysointi tekoälyn avulla mahdollistaa ns. hiljaisten signaalien havainnoinnin. Nämä hiljaiset signaalit ja niistä muodostetut tapahtumaketjut olisivat herättäneet hälytyksen myös vesilaitoksen IoT-laitteen toiminnan muutoksesta normaaliin käyttäytymiseen verrattuna.



Nykyaikaiset tekoälyllä varustetut tietoturvajärjestelmät hyödyntävät analysoinnissa myös henkilöön liitettyjä ominaisuuksia käyttäytymisen profilointiin. Vesilaitoksessa työskentelevien ja pääkäyttäjätunnuksia hyödyntävien henkilöiden profiilitiedot kyetään yhdistämään valvottavaan ja korreloitavaan kokonaisuuteen aivan kuten valvottavat laitteet, jolloin tietoturvakeskuksen valvontajärjestelmä kykenee tunnistamaan henkilö- ja käyttäjäprofiilissa tapahtuneet muutokset, mm. tietyn pääkäyttäjän luoman etäyhteyden avaamisen ulkoisesta verkosta.

Viimeisimpänä uudistuksena älykkäisiin valvontajärjestelmiin on toteutettu ns. riskipohjainen reagointi, jonka avulla jokainen hälytys ja ketjutettu uhkatieto kyetään peilaamaan suoraan valvottaviin operatiivisiin liiketoimintaprosesseihin. Tällä tavoin tietoturva-analyytikot kykenevät nopeasti reagoimaan ja suorittamaan toimenpiteitä, joilla kyetään varmistamaan operatiivinen toiminta uhkahavainnoista huolimatta.

Vesilaitosta kohtaan osoitettua kyberhyökkäystä ei voida havaita ajoissa tai toteuttaa tarpeeksi nopeasti korjaavia toimenpiteitä, mikäli valvonta pohjautuu perinteisiin tunnistettuihin IOC (Indicators of Compromise) -haavoittuvuuksien havainnointiin ja pelkästään lokitettua tietoa lähettäviin uhkatietolähteisiin. Nykyisten tietoturvajärjestelmien on kyettävä mukautumaan hyvin monitasoisiin, pitkäkestoisiin ja ennalta arvaamattomiin hyökkäyksiin, jotka toteutetaan joko epäsuorasti (toimitusketjujen kautta) tai suoraan yrityksen digitaaliseen ympäristöön. Tämä reaaliajassa tapahtuva uhkavalvonta saavutetaan vain tekoälyä hyödyntävillä, käyttäytymistä analysoivilla ja riskitasoa mittaavilla järjestelmillä, jotka kykenevät tuottamaan pitkälle analysoitua uhkatietoa analyytikoiden avuksi ja päätösten tueksi.



Kirjoittaja on 67-vuotias pappa, insinöörimajuri evp ja Kaakkois-Suomen Viestikillan kunnia-puheenjohtaja.

TEKSTI: TAPIO TEITTINEN, KUVAT: JUHA PELTOMÄKI, JOUKO HUTTUNEN JA TAPIO TEITTINEN

Viestimiespäivät 2023 Mikkelissä

19.-20.8. kutsui neljän sodan Päämaja-kaupunki Mikkeli viestimiehiä ja -naisia Viestimiespäiville Mikkeliin. Lauantaina toimittiin Riuttalan leirikeskuksessa ja sunnuntaina Vanhalla varuskunta-alueella.

Paikalle olivat saapuneet Kaakkois-Suomen Viestikillan väen lisäksi edustajia Uudenmaan Viestikillasta, Varsinais-Suomen Viestikillasta, Pohjanmaan Viestikillasta, Pirkanmaan Viestikillasta, Kymen Viestikillasta, Etelä-Hämeen Viestikillasta, Päijät-Hämeen Viestikillasta, Ilmavoimien Viestikillasta ja lisksi muutama toistaiseksi kiltoihin kuulumaton maanpuolustushenkinen radioamatöörikin. Tette ja Heikki Huttunen ottivat osallistujien ilmoittautumiset vastaan ja jakelivat majoitukseen avaimet. Ilmoittautumisen jälkeen pääsivät matkalaiset kahvipöydän ääreen.

Tilaisuuden aluksi muistutti liiton puheenjohtaja Jukka-Pekka Virtanen Viestimiespäivien pitkästä historiasta joka alkoi jo 1964 Riihimäellä, jolloin paikalla oli jopa Suomen television kuvausryhmä. Tuolloin mukana oli vielä runsaasti viestijoukkojen sotaveteraaneja. Aselajin johto oli tuolloin ja myöhemminkin mukana tukemassa tapahtumaa. Riihimäki säilyi pääosin kokoontumispaikkana aina vuoteen 1989 asti jolloin killat muodostivat liitto-organisaation ja päiviä aloitettiin kierrättämään eri alueellisten kiltojen järjestämänä. Liiton puheenjohtaja arvosti sitä, että Pääesikunnan johtamisjärjestelmäpäällikkö lupautui suojelemaan tapahtumaa.
Viestimiespäivissä on puheenjohtajan mukaan ennen muuta kysymys maanpuolustushenkisten ystävien kohtamaamisesta - yhdessä olemisesta. Näin jatkamme omalla vuorollamme 60-luvulta alkanutta, lähes katkeamatonta, perinnettä, jossa vahvistamme koko viestiaselajin vapaaehtoiskentän yhteishenkeä.

Kaakkois-Suomen Viestikillan puheenjohtaja Martti Susitaival toivotti kenraalin ja osanottajat tervetulleiksi tapahtumaan ja kertoi lyhyesti tapahtuman järjestelyistä.

Pääesikunnan johtamisjärjestelmäpäällikkö, prikaatikenraali Jarmo Vähätiitto kertoi johtamisjärjestelmäalan ja viestiaselajin ajankohtaisia asioita tietotekniikkaan ja koulutukseen liittyen. Johtamisjärjestelmäala ylläpitää ja kehittää useita eri tietoturvatasoa olevia tietojärjestelmiä. Toiminnassa seurataan tarkasti turvallisuusympäristön muutoksia ja havaintoja mm Ukrainan tapahtumista. Koulutuksessa kyber- ja ICT-asiat ovat vahvasti esillä. Esitelmän päätteeksi kenraali avasi virallisesti vuoden 2023 Viestimiespäivät.

Heti kenraalin jälkeen estraadille asettui Jussi Saarinen, joka kertoi maanpuolustusjärjestöjen Drone-hankeen taustoista, nykytilasta ja tulevaisuuden näkymistä. Hankkeen tavoitteena on aktivoida reserviläisten VAPEPA toimintaa, kehittää maakunnan varautumista ja houkutella uusia toimijoita maanpuolustustyöhön. Hankkeen taustalla on eri maanpuolustusjärjestöjen lisäksi MPK ja eri viranomaisia alueelta sekä maa- ja metsätalouden järjestöjä ja mm sähköyhtiöitä. Varainhankintaa varten on perustettu yleishyödyllinen osakeyhtiö ja sen alle kaupallista toimintaa mahdollistava osakeyhtiö ”Saimaan Dronepalvelu Oy”. Hankeessa on jo kasassa lentokalustoa ja johtamisopaikka-ajoneuvo tietoliikennejärjestelyineen. Hankkeen organisaatioon kuuluu lennätyskoulutuksen saaneita henkilöitä, tohtoreita, väitöskirjatutkijoita, diplomi-insinöörejä, ammattilentäjiä, meteorologi jne. Kaakkois-Suomen Viestikilta tukee hanketta ja sen jäseniä on hankkeen johdossa. Jussi Saarisen esityksen jälkeen siirryttiin ulos seuraamaan drone-lennokin toimintaa Jesse Tolvasen lennättämänä. Jouni Hautamäki esitteli johtokeskusauton tietotekniikkaa ja radiokalustoa. Tämä kokonaisuus kiinnosti osallistujia niin, että heitä oli patisteltava lounaalle.

Herkullisen Paukkulan emännän valmistaman lounaan jälkeen alkoi odotettu “Herrasmieskilpailu” (nimeä on ehkäpä

Drone lähdössä.

syytä päivittää, koska mukana oli jo useita rouviakin). Tällä kertaa tuo perinnenimi oli vielä käytössä.

Kilpailussa oli kaksi useampiosaista tietokilpailukysymystä koskien viestin historiaa ja tietoliikennetekniikkaa, Seppo Kiiski ja Esko Pitkänen hoitivat rastia jossa piti heittää antennipainoa 10 metrin päässä olevan merkin luo, yhdellä rastilla piti selvittää 20- 40-luvuilta olleiden esineiden nimiä tai käyttötarkoitusta, noita laitteita tutkittiin lähes purkamalla ne osiin. Yhdellä rastilla etsittiin kaukana näkyvän rakennuksen katon korkeutta merenpinnasta, yhdellä rastilla ammuttiin Jussi Saarinen opastamana eko-aseella (kolme koelaukausta sallittiin) ja Martti Susitaival pyöritti kenttäpuhelinyhteyden rakentamisrastia. Matkapuhelimet olivat kovassa käytössä kun Wikipediasta ja muista lähteistä yritettiin löytää vastauksia tehtäviin, vaan eipä netistä juuri ollut apua. Sen sijaan Kaakkois-Suomen Viestikillan julkaisemista kirjoista ”Viestisotaa Rukajärvellä” ja ”Ylijohdon viestiverkot Suomen sodissa 1918-1945” olisi ollut apua.

Majoitusrakennuksen läheisyyteen oli kiltamme hallituksen jäsen Vesa Kauppinen pystyttänyt kauko-ohjattavan radioamatööriaseman autoon ja tapahtuman osanottajilla oli mahdollisuus tutustua aseman järjestelyihin. Moni käytti tarjottua tilaisuutta hyväkseen.

Saunomisen jälkeen syötiin herkullinen päivällinen ja näin kiltalaiset pääsivät jatkamaan ravittuina kohti illan viettoa.

Saunomisen aikana oli kisan pääjärjestelijällä Tapio Teittisellä haastava tehtävä laittaa lähinnä kahden hengen joukkueina toimineet osallistujat paremmuusjärjestykseen. Kisa oli tiukka ja pisteet olivat lähellä toisiaan. Monella ryhmällä oli sama pistemäärä. Tuolloin ratakaisevaksi tekijäksi piti laittaa puhelinrastilla käytetty aika ja eräässä tapauksessa parempi ampumatulos. Tulosjärjestys kuitenkin syntyi. Kisan voittivat yhdellä pisteellä seuraavaan joukkueeseen Taina ja Jukka-Pekka Virtanen. Onneksi olkoon! Tähän pitää vielä mainita, että Pellervo Pekkola ampui viidellä laukauksella tuloksen 48 ja ryhmä Jari Kallonen ja Paavo Rintapää ampuivat keskiarvon 47 pistettä.
Paljon oli kisan päätyttyä "parran pärinää" ja jossittelua, mutta tuomaristo oli tiukkana eikä pisteitä puheilla herunut.

Palkintojen jaon jälkeen saliin saapasteli puhkiammuttua kypärää kantava, kaikki sodat käynyt, hahmo hyräellen vanhaa viestimiesten laulua. Tuo hahmo oli Pellervo Pekkola ja hän "muisteli" uransa varrelle sattuneita tai muuten kuulleita hauskoja tapahtumia. Osa oli K18-aineistoa, mutta naurut kelpasivat.

Illan ohjelma jatkui Filmi- ja videokuvaajien liiton SM-kisassa dokumenttisarjassa hopealla palkitun "Päämajan viestikeskus Lokki"-filmin esityksellä. Tämän jälkeen kutsui makkaranpaisto ja virvoitusjuomien nauttiminen hyvässä seurassa.

Seuraavana päivänä aamupalan jälkeen osallistujat suuntasivat Mikkelin Vanhalle kasarmialueelle jossa Jalkaväkimuseon museoasistentti Riikka Sinokki esitteli elävöittävien tarinoiden höystämänä museon eri osastoja. Kaakkois-Suomen Viestikillan ja Mikkelin seudun radioamatöörien yhdessä rakentaman radiohuoneen ja puhelinkeskusnäyttelyn esitteli killan puheenjohtaja Martti Susitaival.

Tapahtuma päättyi lounaaseen Mikkelin Upseerikerholla. Ennen ruokailua Esko Pitkänen, Heikki Huttunen ja Tapio Teittinen saivat liiton puheenjohtajan jakamat liiton kultaiset ansiomerkit. Martti Susitaival, Seppo Kiiski ja Pellervo Pekkola olivat saaneet vastaavat merkit jo liiton 60-vuotisjuhlassa 5.3.2023 Riihimäellä. Liiton kunniapuheenjohtaja Seppo Uro totesi, että tällaiset ne Viestimiespäivien pitääkin olla, näistä voisi tehdä oikein standardin.

Viestimiespäivien osanottajia Jv-museon portailla.

Taina ja Jukka-Pekka Virtanen.

Martti Susitaival valvoo kun Seppo Uro ja Jukka-Pekka Pelttari laittavat puhelinyhteyttä kuntoon.

Säät olivat suosineet tapahtumaa ja osanottajat läksivät ilmeisen tyytyväisinä kotimatkalle.

Vuoden 2023 Viestiupseeri - Insinöörikapteeniluutnantti Sami Nikkanen

Vuoden 2023 viestiupseeriksi valittiin Merivoimien esikunnan johtamisjärjestelmäosastolla tietoliikenneinsinöörinä palveleva insinöörikapteeniluutnantti Sami Nikkanen. Nikkanen on kotoisin Porista, mutta asuu nykyisin Turun seudulla Ruskolla. Hän on valmistunut tietotekniikan diplomi-insinööriksi Tampereen Teknillisen Yliopiston Porin yksiköstä vuonna 2010 pääaineenaan ohjelmistotuotanto. Sami on työskennellyt ennen Puolustusvoimia Turun telakalla tietohallintoalalla tietoliikenteen-, puhepalveluiden ja tietoturvan parissa vuosina 2007–2016.

Varusmiespalveluksen Nikkanen suoritti Porin prikaatissa vuonna 2002 ja teki aikanaan toimintavalmiussitoumuksen sotilaallisiin kriisinhallintatehtäviin. Niin sanottu ”krihakortti” ei kuitenkaan koskaan konkretisoitunut, mutta sen sijaan hän kävi muutaman vuoden Kriisinhallintakeskuksen (CMC Finland) kansainvälisen pelastustoiminnan kursseilla ja harjoituksissa pitkin Eurooppaa sekä parissa operaatiossa Filippiineillä ja Nepalissa päivätyön ohessa.

Sami oli jo pitkään ollut kiinnostunut ja seurannut Puolustusvoimien toimintaa, kunnes hänen ystävänsä vinkkasi kesällä 2016 työpaikasta Merivoimissa. Hän haki tehtävää ja meni työhaastatteluun sillä ajatuksella, että kuulisi vähän, mitä Merivoimissa puuhataan. Ennen haastattelua hän luki vanhoja Rannikonpuolustaja-lehtiä ja Turun Laivastoaseman 50-vuotis julkaisun vuodelta 1989 sekä soitti kaikki tutut ja puolitut läpi hankkiakseen taustatietoja. Mutta vasta Cooperin-testin ja haastattelun jälkeen hänelle alkoi selvitä, mistä tässä työssä saattaisi olla kyse. Ennen ensimmäistä työpäivää ainoat tosiasialliset kokemukset Puolustusvoimista olivat olleet vain varusmiespalvelus sekä yksittäinen ”Aseet ja välineet” kertausharjoitus, joista aika oli jo kullannut muistot.

Nikkanen aloitti Merivoimien tietotekniikkakeskuksessa järjestelmäpäällikkönä vuonna 2016 ja koordinoi merikaapeli- ja turvalaitetöitä Merivoimien toiminta-alueella. Sodanajan johtajakurssin hän suoritti RUK:ssa Haminassa uransa alkuvuosina ja sieltä tarttui hyvää oppia muun muassa jääkärijoukkueen manöövereistä. Vuonna 2019 Nikkanen haki ja tuli valituksi nykyiseen tehtäväänsä tietoliikenneinsinööriksi Merivoimien esikunnan johtamisjärjestelmäosaston viesti- ja tietoliikennesektorille. Tehtävässä hän koordinoi Merivoimien taktisen datalinkin käyttöä ja toimii erilaisissa hankkeissa JOJÄ-suunnittelijana. Natojäsenyyden myötä Nikkanen on päässyt lisäksi osallistumaan muun muassa työryhmään, joka määrittelee Nato-alusten johtamisjärjestelmien vaatimuksia.

Sami on viihtynyt Puolustusvoimissa erinomaisesti ja vanha, vähän kulunut sanonta, ettei kahta samanlaista päivää ole, pitää hänen mielestään täysin paikkansa. Työtä vauhdittaa aito uteliaisuus ja kiinnostus Puolustusvoimien toimintaa kohtaan. Nikkasen kokemuksen mukaan työssä on paljon samoja elementtejä kuin siviilipuolellakin, mutta Puolustusvoimien niin kutsuttu ”liiketoimintamalli” eroaa yritysmaailman vastaavasta. Tuloksellisuuden mittaaminen on jossain määrin erilaista ja veronmaksajien rahoilla toimittaessa on syytä pitää tehtävä kirkkaana mielessä. Positiivisena yllätyksenä Nikkaselle tulivat aikanaan joustavat etätyökäytännöt ja moni perusasia, kuten TUVE-koneet ja työpaikkaruokailu. Puolustusvoimat eroaa siviiliyrityksestä myös siinä, että moni asia on kirjattu määräykseksi tai ohjeeksi, mikä on lähtökohtaisesti hyvä asia, vaikka joskus voisi vähemmälläkin ”normeerauksella” pärjätä.

Insinöörikapteeniluutnantti Sami Nikkanen kuvassa keskellä. Vasemmalla VUY:n puheenjohtaja Pertti Hyvärinen ja oikealla viestitarkastaja eversti Antti Tunkkari.

Seitsemän vuoden työuransa aikana puolustusvoimissa Sami on omasta mielestään ehtinyt jo vaikka ja mihin, siitä huolimatta, että on vasta virkauransa alussa. Tähänastiset parhaimmat muistot ovat Merivoimien toimintaympäristöstä, jossa on saanut toimia meren, saarten ja alusten parissa. Joskus olo on tuntunut jopa vähän epätodelliselta, että voiko tällaistakin tehdä päivätyökseen ja siitä maksetaan vielä palkkaa. Myös kansainvälisestä toiminnasta on paljon hyviä muistoja. Niissä yhteyksissä on päässyt tutustumaan sekä puolustusvoimien että muiden maiden johtamisjärjestelmätoimialan tekijöihin ja sitä myötä saanut kokemusta JOINT-toiminnasta.

Vaikka työ on mukavaa, on se myös haasteellista. Tähänastisista tehtävistä haastavimpana Nikkanen mainitsee merivoimien FMN CIAV-toiminnan aloittamisen ulkomailla. Ensimmäisessä KV-kokouksessa ihan kaikki oli uutta alkaen

paikanpäälle pääsemisestä aina kokouksessa vilahteleviin akronyymeihin, joista vain osan uskalsi googlettaa. Ylipäänsä työn haastavuus liittyy Nikkasen mielestä siihen, miten PV:n niukoilla resursseilla saadaan kehitettyä ”hyvä idea” jonkinlaiseen tuotantoon tai pysyvään tilaan. Toisaalta siinä piilee Samin mukaan myös suomalaisen tekemisen taika, jossa kekseliäisyydellä saadaan pikkurahallakin priimaa verrattuna moniin isoihin valtioihin. Kiinnostavimmat työtehtävät ovatkin liittyneet jonkinlaiseen prosessikehittämiseen, jossa pienillä yksinkertaisilla asioilla on pystytty kasvattamaan toiminnan laatua tai nopeutta.

Vapaa-ajallaan Sami harrastaa sähkömaastopyöräilyä ja alamäkipyöräilyä, vaikka hän toteaakin, että harrastustoiminta on selkeästi nuoruusvuosien turbomoottoripyörien virittelystä taantunut näin keski-iän kynnyksen lähestyessä.

Valinta vuoden viestiupseeriksi oli Samille todellinen yllätys ja veti mielen nöyräksi. Hän kokee, ettei ehkä koskaan ole saanut näin merkittävää palautetta omasta työstään. Tunnustuksen myötä hän on myös pohtinut, miten voisi jakaa muille omia hyviä käytäntöjä ja siten tuoda koko organisaatiolle lisäarvoa.

Viestimieslehden toimitus onnittelee insinöörikapteeniluutnantti Sami Nikkasta valinnasta vuoden 2023 viestiupseeriksi!

TEKSTI: JUHA PELTOMÄKI

A.R. Saarmaa -seminaari 22.9.2023

”Uudet toimintaympäristöt osana paikallispuolustuksen johtamisjärjestelmää – haasteet ja mahdollisuudet!”

Viestikiltojen liitto järjesti paikallispuolustuksen johtamista ja viestitoimintaa käsittelevän A.R. Saarmaa -seminaarin 22.9.2022 klo 12.00–16.00. Tilaisuuden järjestelyt toteutettiin yhteistoiminnassa puolustusvoimien, Viestiupseeriyhdistyksen ja Maanpuolustuskoulutusyhdistyksen (MPK) kanssa. Tilaisuuden keskuspaikkana toimi Riihimäellä Viestikoulun luokka Saarmaa. Seminaarin puheenjohtajana toimi Viestikiltojen liiton koulutuspäällikkö, everstiluutnantti Juha Peltomäki.

Tilaisuuteen osallistui 17 paikkakunnalta yhteensä runsaat 250 henkilöä, joka on ennätys seminaarin historiassa. Suurin osanottajamäärä oli Riihimäellä. Paikkakunnat liitettiin seminaariin PV:n joukko-osastojen ja aluetoimistojen kautta TUVE-videoneuvottelupalvelun välityksellä.

Seminaarin agenda on perinteisesti muodostunut kolmesta kokonaisuudesta: edeltävän seminaarin jatkumo, saatu palaute ja ajankohtaisuus. Tämän vuoden teemaksi valikoitui “Uudet toimintaympäristöt osana paikallispuolustuksen johtamisjärjestelmää – haasteet ja mahdollisuudet!”

Seminaarin tavoite oli syventää luennoin ja case-tarkasteluin osallistujien tietoutta paikallispuolustuksen johtamisesta ja johtamisen tukemisesta, kyberpuolustuksesta ja arjen välineiden käytöstä niin kansallisesti kuin Ukrainan sodan havaintojen perusteella.

Seminaarin kohderyhmänä oli paikallispataljoonaan sijoitetut johtajat ja viestihenkilöstö, paikallispuolustuksen kehittämiseen osallistuva henkilöstö, viesti- ja johtamisjärjestelmäalan vapaaehtoisten maanpuolustusjärjestöjen jäsenet, maanpuolustuskoulutusyhdistyksen henkilöstö ja kurssilaiset sekä MPK:n jäsenjärjestöjen jäsenet.

Saarmaa-seminaari 2023 juliste.

Aikaisemmin saadun palautteen perusteella päädyttiin jakamaan julkinen materiaali halukkaille. Materiaalin jako toteutettiin tiedostojakona sähköpostiosoitteisiin perustuen. Materiaalipyyntöjä tuli noin 40 kpl. Mikäli olet halukas saamaan seminaarin julkisen materiaalin, niin vielä ehtii. Lähetä pyyntö osoitteeseen juha.peltomaki@mil.fi.

Koska materiaali on jaettavissa, niin tämänkertainen Saarmaa-seminaarin artikkeli on merkittävästi tiiviimpi ja rakenteeltaan aikaisemmista poikkeava.

Avaus – ”tsiigaa avaruuden ikkunaa”

Seminaarin avasi Viestikiltojen liiton puheenjohtaja, Jukka-Pekka Virtanen. Hän toivotti osallistujat tervetulleiksi kertoen seminaarin historiasta sekä esitellen seminaarin ohjelman.

” Herra kenraali, arvoisat maanpuolustuksen ystävät, hyvät viestimiehet ja -naiset

Tervetuloa seitsemänteen valtakunnalliseen A.R. Saarmaa –seminaariin, joka on samalla Viestikiltojen Liiton 60-vuotisjuhlaseminaari. Tällä kertaa seminaariin osallistuu ennätyksellisesti noin 250 henkilöä, 17 eri paikkakunnalla ympäri Suomen.

Seminaarin teemaksi on valikoitunut ”Uudet toimintaympäristöt osana paikallispuolustuksen johtamisjärjestelmää – haasteet ja mahdollisuudet?” Samalla kun kuulija on tempaistu edellisissä seminaareissa perinteisistä maa-, meri- ja ilmapuolustusympäristöistä yhä vahvemmin kyberulottuvuuteen, vie tämän kertainen seminaari meidän J Karjalaisen sanoin ”tsiigaa avaruuden ikkunaa”.

”Vuoden 2023 seminaarin pääteeksi on vuorossa eräs merkittävimmistä Viestikiltojen Liiton juhlavuoden projekteista, jonka päätepistettä monet meistä ovat kovasti odottaneet - eikä allekirjoittanut ollenkaan vähiten. Julkaisemme valtakunnallisesti liiton 60-vuotisesta toiminnasta kertovan juhlakirjan ja käynnistämme sen jaon lämpimäiskappaleilla maakuntia myöten.

Hyvät naiset ja herrat, näillä aloitussanoilla olemme valmiit aloittamaan vuoden 2023 valtakunnallisen A.R. Saarmaa –seminaarin.”

Ohjelma – monipuolisesti kaikilla lentokorkeuksilla

Pääesikunnan johtamisjärjestelmäpäällikkö, prikaatikenraali Jarmo Vähätiitto käsitteli esityksessään kansainvälistä turvallisuustilanne, liittoutumisen ja kansainvälistymisen merkitystä Puolustusvoimille. Kansainvälisyys merkitsee sekä tukea että velvoitteita. Muita esille tulleita asioita olivat mm. kyberin henkilöstötavoitteiden saavuttaminen, käynnissä olevan johtamisjärjestelmätoimialan kehittäminen (JOHKE) sekä ajatuksia kybervarusmieskoulutuksen mallin laajentamisesta ICT-varusmiehiin.

Seminaariesitysten sisältö oli poikkeuksetta korkea ja mielenkiinnon kohteet jakautuivat aikaisempaa enemmän, mikä on hyvä asia. Jokaisesta esityksestä olisi erittäin haastava puristaa muutamaan lauseeseen keskeisin sanoma, joten en edes yritä sitä tehdä. Sen sijaan laitan esityksistä muutamia kuvia, jotka toimikoon ”houkuttimena” tilaamaan materiaali, ja erityisesti osallistumaan vuoden 2024 seminaariin.

Viestikiltojen liiton puheenjohtaja, Jukka-Pekka Virtanen, avaamassa Saarmaa-seminaaria.

Saarmaa-seminaari 2023 – palautteella on merkitystä, palaute vaikuttaa.

Palautteen kerääminen toteutettiin sähköisellä järjestelmällä (kyselynetti). Saadun palautteen määrä (32 kpl) mahdollistaa entistä paremmin seminaarin jatkokehittämisen. Kasvava palautteen määrä kertoo myös siitä, että mobiililaitteilla toteutettava kysely on toimiva tapa palautteen keräämiseksi ja analysoimiseksi, vaikka kehitettävää siitäkin löytyy. Palautepalvelut tarjoavat varsin monipuoliset ja helppokäyttöiset toiminnallisuudet. Saatu palaute oli monipuolista ja rakentavaa. Perustellut kehittämisajatukset ja uudet aihepiirit tullaan huomioimaan vuoden 2024 Saarmaa-seminaarin valmistelussa, kuten myös palautteen keräämisestä saatu palaute.

Saadun palautteen perusteella osallistujajoukko oli varsin tyytyväinen päivän antiin: ”Kuinka todennäköisesti suosittelisit seminaaria ystävällesi?” vastauskeskiarvo oli 9.44 (asteikko 1-10), joka on 0.3 edeltävää vuotta parempi – ollen kaikkien aikojen paras.

Palautteen perusteella mielenkiintoisimmat esitykset olivat Mikko Laineen ”Perustamisen hallintaohjelma.” sekä Jesse Tolvasen ”Kaupalliset dronet – nykyaikaisen sodankäynnin uusi normaali?” Eniten uutta tietoa tarjosi Jouni Salmen ja Mikko Kyllösen esitys ”Kognitiivinen ja laajakaistainen HF-ohjelmistoradio.”

12:00	Seminaarin avaus ja järjestelyt	VKL PJ
12:05		Jukka-Pekka Virtanen
12:10	Johtamisjärjestelmäalan ajankohtaiset asiat	PEJOJÄPÄÄL
12:30	Aluetoimisto paikallispuolustuksen kehittäjänä	Markku Salo, Pirkanmaan aluetoimisto
12:35	- Perustamisen hallintaohjelma	Mikko Laine
12:40	- Datapohjainen tiedustelu, tietovirrat ja tiedonkäsittely	Mikko Hakola
12:45	- Kenttäradioiden keskinäishäiriön vaimennus	Taneli Riihonen
13:20	Kognitiivinen ja laajakaistainen HF-ohjelmistoradio.	Mikko Kyllönen
13:45	Kahvitauko	
14:10	Kaupalliset dronet – nykyaikaisen sodankäynnin uusi normaali?	Jesse Tolvanen
14:45	Satelliittitietojärjestelmät PV:n käytössä.	Arto Hokkanen
14:50	Satelliittien käyttö Ukrainan sodassa - hybridinäkökulma.	Sari Uusipaavalniemi
15:20	MPK:n HF-koulutusohjelman kokemuksia PAPU 2/23.	Mikko Laakkonen
15:35	Vapaaehtoinen maanpuolustus, MPK	MPK:n koulutuspäällikkö (SOTVA)
15:40	- Varaviestiverkko, Kyber erikoiskurssi, ELSU-ohjelma	Juha Niemi
15:45	Vapaaehtoinen maanpuolustus, Viestikilta	VKL:n koulutuspäällikkö
15:50		Juha Peltomäki
15:55	Päätös	Seminaarin puheenjohtaja
16:00	Juhlakirjan julkaiseminen ja palkitsemiset	VKL PJ
16:30		Jukka-Pekka Virtanen

Saarmaa-seminaari 2022 agenda.

Koostekuva esityksistä.

Seminaarin sisältöön oltiin varsin tyytyväisiä. Kehittämistoiveet liittyivät lähinnä esitysteknisiin asioihin, kuten käsitteiden avaaminen, ”fonttikoko” ja ruuhkaiset diat. Äänentoistoa tulee kehittää käyttämällä päämikrofoneja. Lisäksi kaivattiin videokuvaa esiintyjistä. Ensikertaa käytössä ollut sähköinen ilmoittautumismenettely toimi hyvin.

Esitykset olivat korkealaatuisia ja tilaisuudelle asetetut tavoitteet saavutettiin hyvin. Järjestävä organisaatio esittää parhaimmat kiitokset tilaisuuden esiintyjille ja osallistujille.

Ensi vuonna tilaisuus järjestetään 20.9.2024 pääpaikkana Riihimäki. Aihepiiri muodostunee perinteiseen tapaan paikallispuolustuksen ympärille. Monesta tämänkertaisesta aiheesta toivottiin ”jatko-osaa”. Uusina aiheina mainittiin mm. 5G datakuplat, puolustusvoimien JOJÄ – HF – ELSO -koulutus tänä päivänä, varaviestiverkko, kyber, tekoäly sotilaskäytössä, Ukrainan kokemukset sekä NATO:n johtamisjärjestelmät. Aika näyttää kuinka em. aiheet kyetään sovittamaan seuraavan seminaarin agendaan ja turvallisuusluokkaan. Jotakin edellä mainitun suuntaista on valmisteilla.

Tervetuloa A.R. Saarmaa -seminaariin 2024.

Taukokeskustelu oli erittäin vilkasta. Riihimäellä oli nähtävillä mm. KNL CNHF-radio sekä droneja.

Juhlakirja: ”Kipinä kantaa – Viestikiltojen Liitto 60 vuotta”.

Saarmaa-seminaari päätteeksi julkaistiin Viestikiltojen Liiton 60-vuotisjuhlakirja – ”Kipinä kantaa – Viestikiltojen Liitto 60 vuotta”. Tilaisuudessa jaettiin ensimmäiset kappaleet kirjasta ja palkittiin kirjan kirjoittamiseen osallistuneita henkilöitä. Juhlakirjasta on 50 numeroitua kappaletta. Juhlakirjan ensimmäiset kappaleet myönnettiin seuraavasti: 1 - VKL, 2 - Toimitusjohtaja Martti Rusi, 3 - Eversti SeppoUro.

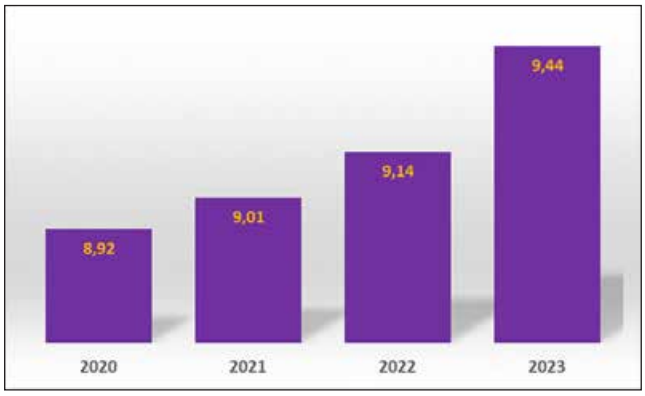
Alla on otteita juhlakirjan esipuheesta, joka on kirjoittanut Viestikiltojen liitto ry:n puheenjohtaja, Jukka-Pekka Virtanen.

”Viestikilta ry perustettiin Riihimäellä 3.3.1963 viestiaselajin pääkillaksi. Vuoden 1989 organisaatiomuutoksessa se sai nimekseen Viestikiltojen Liitto ry. Vuonna 2023 Viestikiltojen liitto täytti kunniakkaat 60 vuotta. Juhlavuoden lähestyessä herätteli liiton kunniapuheenjohtaja Seppo Uro liittohallitusta ajatuksella päivittää vuonna 1998 julkaistu 35-vuotishistoriikki. Päätös syntyi varsin nopeasti ja asiaa ryhdyttiin edistämään suunnitelman laatimisella ja projektiryhmän perustamisella.

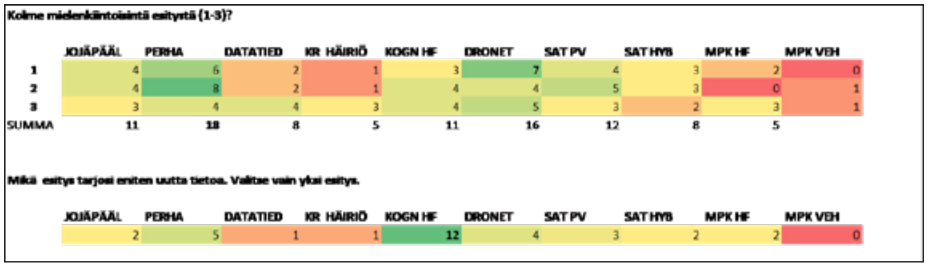
Päätettiin tehdä perinteisestä historiikista poiketen artikkelikokoelmaa muistuttava juhlakirja, joka olisi ulkoasultaan kevyempi, sisältäisi paljon kuvia ja irtautuisi tarvittaessa kronologisesta kerronnasta.

Kirjan nimestä järjestettiin kilpailu, joka tuotti toinen toistaan parempia nimiehdotuksia. Liittohallituksen päätöksellä voittajaksi valittiin ”Kipinä kantaa – Viestikiltojen Liitto 60 vuotta”. Nimessä yhdistyy hienolla tavalla historia, perinteet, toiminta, tekniikka ja maanpuolustushenki. Suomen Puolustusvoimiin jääkäreiden mukaan Saksasta tullutta salamaa tai kipinää muistuttavaa nuolta käytetään viestiaselajin ja erityisesti radioalan merkkinä.

Kipinä antaa toiminnalle henkisen alun sytyttäen soihdun, joka roihuaa voimakkaana ja valaisee tietä. Kipinän sytyttämä liekki roihuaa sydämissämme sitouttaen meitä aselajin tunnuslauseen jaloon velvoitteeseen: ”Viesti vain perille vietynä ratkaisee.” Tahtotila, joka on ollut ja olkoon myös tulevaisuudessa toiminnan kantavana ajatuksena. Viesti on vietävä perille vastoinkäymisistä huolimatta.”



Palautekeskiarvot 2020–2023.



Kolme mielenkiintoisinta esitystä (1-3)?

	JOJÄPÄÄL	PERHA	DATATIED	KR HÄIRIÖ	KOGN HF	DRONET	SAT PV	SAT HYB	MPK HF	MPK VEH
1	4	6	2	1	3	7	4	3	2	0
2	4	8	2	1	4	4	5	3	0	1
3	3	4	4	3	4	5	3	2	3	1
SUMMA	11	18	8	5	11	16	12	8	5	

Mikä esitys tarjosi eniten uutta tietoa. Valitse vain yksi esitys.

JOJÄPÄÄL	PERHA	DATATIED	KR HÄIRIÖ	KOGN HF	DRONET	SAT PV	SAT HYB	MPK HF	MPK VEH
2	5	1	1	12	4	3	2	2	0

Saarmaa-seminaari 2023 palautekooste.

Jukka-Pekka Virtanen esittelee juhlajulkaisua.

Viestiupseeriyhdistys järjestää seminaarin 13. - 14.2.2024

”INFORMAATIOYHTEISKUNNAN TURVALLISUUS NYKYISESSÄ MAAILMANTILANTEESSA”

Seminaarissa käsitellään informaatioyhteiskunnan turvallisuusympäristössä tapahtuneita muutoksia ja arvioidaan niiden vaikutuksia muun muassa NATO-jäsenyyden kannalta.
Seminaari on tarkoitettu organisaatioiden tietoverkkojen resilienssistä, suunnittelusta, ratkaisuista ja tietoturvallisuudesta vastaaville.
Puhujiksi ovat alustavasti lupautuneet kenr evp, kansanedustaja **Jarmo Lindberg** Suomen NATO-integraatiosta eduskunnan työssä, tutkimusjohtaja **Mikko Hyppönen** tekoälyn turvallisuudesta (WithSecure), professori **Marko Höyhtyä** satelliittikommunikaatiosta (VTT), professori **Jouko Vankka** sotilasteknologian kehityksestä (MPKK) ja prikaatikenraali **Jarmo Vähätiitto** NATO-jäsenyyden mahdollisuuksista johtamisjärjestelmäalalla (PE).
13.2. iltapäivän tilaisuus on Digia Oy:n isännöimänä pääkaupunkiseudulla ja ilta- sekä 14.2. ohjelma risteilynä Helsinki – Tallinna - Helsinki m/s Victoria I:llä.
Seminaarin hinta 800,00 €, jäseniltä 650,00 €. Hinta sisältää seminaariohjelman, majoituksen yhden hengen hytissä, ohjelmaan merkityt ateriat ja kahvit. Viestiupseeriyhdistys laskuttaa seminaarin tammikuussa 2024.

Sitovat ilmoittautumiset 9.1.2024 mennessä yhdistyksen kotisivuilla www.viestiupseeriyhdistys.fi (suositeltavin tapa) tai seminaari@viestiupseeriyhdistys.fi. Paikkoja on rajoitetusti.

Oikeus muutoksiin pidätetään.
Lisätietoja antavat: Harri Reini, puh. 040 514 2497 tai seminaari(at)viestiupseeriyhdistys.fi tai
Jaakko Wallenius 050 525 0138 tai jaakko.wallenius(at)elisa.fi

Seminaarin alustava ohjelma, jota päivitetään verkkosivuilla.

Tiistai 13.2.2024

Aloitus	Digia Oy Seminaaritila pääkaupunkiseudulla
11.00–12.00	Ilmoittautuminen ja tulokahvi
12.00–12.15	Tervetuloa! Viestiupseeriyhdistyksen puheenjohtaja Pertti Hyvärinen Digia Oy Digian edustaja

1. Jakso: Suomen NATO-jäsenyyden vaikutuksia

12.15–12.45	Turvallisuusympäristön muutos NATOn jäsenenä, PLM
12.50–13.20	Suomen NATO-integraatio eduskunnan työssä, kenr evp, kansanedustaja Jarmo Lindberg, Eduskunta
13.30–14.00	NATO-jäsenyyden mahdollisuudet johtamisjärjestelmäalalla, prkenr Jarmo Vähätiitto, PE
14.00–14.30	TAUKO, kahvi

2. Jakso: Ajankohtaista digitaalisesta turvallisuudesta

14.30–15.00	Ajankohtaista kyberturvallisuudesta, Stefan Lee, LVM
15.10–15.40	Merellisen kriittisen infran suojaaminen ja haasteet, Tuomas Seppälä, HVK
15.50–16.20	Tekoälyn turvallisuus, Mikko Hyppönen, WithSecure
16.45	Siirtyminen laivalle linja-autokuljetuksella, Länsiterminaali 2
18.00	Lähtöselvitys kiinni
18.35	Laiva lähtee
20.30 –	Illallinen Grill House

Keskiviikko 14.2.2024

07.00 -	Meriaamiainen, Grande Buffet

3. Jakso: Estonian perspective

09.00–10.10	Critical infrastructure protection in Estonia
10.10–10.40	Tauko, kahvit

4. Jakso: Kyberturvallisuus, informaatiovaikuttaminen ja turvallista viranomaisviestintää

10.40–11.10	Kansainvälinen turvallisuustilanne ja kyberturvallisuus, Kauto Huopio, Traficom
11.10–11.40	Informaatiovaikuttamisohjelma, Antti Sillanpää, HVK
11.45–12.15	VIRVE2 – turvallista laajakaistaista viranomaisviestintää, liiketoimintajohtaja Jarmo Vinkvist, Suomen Erillisverkot Oy
12.15–12.45	Tauko, kahvit
12.30	Laiva lähtee

5. Jakso: Tekniikan hyödyntäminen operaatioissa ja kriittisillä käyttäjillä

12.45–13.15	Sotilastekniikan kehitysnäkymät, professori Jouko Vankka, MPKK
13.20–13.50	Droonien taktinen käyttö, Ville Nousiainen, MAASK
13.50–14.30	Satellite communications for critical users, Marko Höyhtyä, VTT
14.30 – 14.40	Seminaarin päättäminen, puheenjohtaja Pertti Hyvärinen
14.30	Lounas, Grande Buffet
16.00	Laiva saapuu Helsinkiin

Yhteydet maastoon Nestorin tuotteilla

Nestor Cablesin valikoimasta löytyvät vaativaan kenttäkäyttöön soveltuvat valokaapelit väliaikaisten verkkojen rakentamiseen. Kaapelit ovat saatavilla erilaisilla liitinvaihtoehdoilla, ja niiden lisäksi valikoimassa ovat myös asennuslaitteistot sekä huolto-tarvikkeet. Kenttäkaapelituotteita voidaan hyödyntää myös erilaisissa siviilitapahtumissa.

nestor cables

www.nestorcables.fi
info@nestorcables.fi
Puh. 020 791 2770

Mittarikuja 5,
90620 Oulu
PL 276, 90101 Oulu