Viestimies

Viestiupseeriyhdistyksen julkaisu 79. vsk Numero 1 Kevät 2024

www.viestiupseeriyhdistys.fi

SA-Kuva

COMBITECH

Kovaa softaa

Nopeampaa päätöksentekoa
suorituskykyisillä ohjelmistoilla.

Combitech Finland

www.combitech.fi

Viestimies-lehti

Päätoimittaja
Kimmo Kaipainen
p 040 7222646
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
Puhakka Pasi
Pellikka Jarkko
Hyvärinen Pertti
Isomäki Pekka
Koski Harri
Nyqvist Antti
Sipilä Olli
Suokko Harri
Tunkkari Antti
Wirman Kari

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. SA-kuva ja Tatu Tahkokallio

Tässä numerossa

Viestiupseeriyhdistys ry:n julkaisema viesti-, johtamisjärjestelmä- ja ICT-alojen sekä kyberturvallisuuden päättäjien ja asiantuntijoiden lehti.

Mukana lehdessä
–
Mukana päätöksiä tehdessä!

Seuraavan numeron aineistopäivä on 26.4.2024. Lehti ilmestyy viikolla 22.

Muutoksen tuulet ja uusi normaali

Tervetuloa vuoden 2024 ensimmäisen Viestimies-lehden pariin. Käsissäsi on jälleen tuhti paketti mielenkiintoista luettavaa. Tämä numero on samalla ensimmäinen päätoimittajuuteni aikana painosta tullut lehti. Tartun tehtävään Pasi Puhakan ja edeltävien päätoimittajien jättämän erinomaisen perinnön kanssa. Iso kiitos Pasille lehden eteen tehdystä laadukkaasta työstä! Moni tänä vuonna nähtävä muutos on tunnistettu jo Pasin päätoimittajuuden aikana.

Vuoden 2024 aikana pyrimme tuomaan lehteen hallitusti uutta ilmettä. Ensimmäinen jo tässä numerossa näkyvä muutos on lehden painossa käytettävän paperin vaihtaminen. Toivottavasti muutos parantaa luettavuutta myös sinun mielestäsi. Toinen merkittävä kevään aikana otettava askel on lehden digitaalisen version muuttaminen pdf-julkaisusta näköisjulkaisuksi. Näköislehtenä julkaiseminen mahdollistaa aiempaa paremmin esimerkiksi yksittäisten artikkeleiden jakamisen sosiaalisessa mediassa tai vaikkapa tekstiin sisällytettyjen linkkien avaamisen.

Vuoden 2024 aikana tulemme käsittelemään ajankohtaisia asioita teemoitelluissa numeroissa. Käsissäsi oleva vuoden ensimmäinen lehti käsittelee uutta teknologiaa ja sen hyödyntämistä eri muodoissaan. Vuoden toisen lehden ilmestyessä kesäkuun alussa on NATO jäsenyytemme ratifioinnista kulunut jo yli vuosi. Toisessa numerossa käsittelyn kohteena onkin NATO ja se millaisia muutoksia jäsenyytemme on toimialalla aiheuttanut. Tämän lehden ilmestyessä sota Ukrainassa on jatkunut jo 10 vuotta. Venäjän laajamittainen hyökkäyskin on kestänyt jo 2 vuotta. Vuoden kolmannessa numerossa teemana onkin ”Uhka”.

Tässä numerossa lanseeraamme lukijoillemme kirjoituskilpailun, ja vuoden neljännessä numerossa näemme toivottavasti runsain mitoin kirjoituskilpailun tuloksia. Ajatus kirjoituskilpailusta ei ole täysin uusi. Kokeneempien mukaan Viestimies-lehdessä järjestettiin kirjoituskilpailu jo 1980-luvulla. Onkin mielenkiintoista nähdä miten Viestimies-lehden lukijakunta ja aktiiviset Puolustusvoimien henkilökuntaan kuuluvat sekä reserviläiset tarttuvat haasteeseen. Kirjoita sinäkin visiosi ”Tulevaisuuden digitaalisesta taistelukentästä”!

Tätä kirjoittaessani lehdissä on uutisoitu palvelunestohyökkäysten kohdistumisesta ennätysmäärään suomalaisia yrityksiä. Laaja-alaisen vaikuttamisen kohteena eläminen on valitettavasti yhteiskunnallemme uusi normaali. Laaja-alaisen vaikuttamisen käsite on muuten määritelty vuonna 2021 julkaistussa valtioneuvoston puolustusselonteossa ja vuonna 2022 julkaistussa ajankohtaisselonteossa turvallisuusympäristön muutoksesta. Laaja-alainen vaikuttaminen pitää sisällään hybridivaikuttamisen, mutta sisältää myös sotilaallisen voiman käytön mahdollisuuden.

Viestimies-lehden lisäksi uutta seurattavaa ja tutustuttavaa julkaistaan jatkuvasti. NATO ja Ukraina julkaisivat joulukuussa 2023 yhteisen koonnoksen käynnissä olevan sodan opeista. Laajaan dokumenttiin on koottu 25 sodasta johdettua oppituntia. Erityisesti Lesson 8: Russian Information operations, Lesson 23: Cybersecurity and Defence Lessons Learned, Lesson 24: National Level Cybersecurity in Ukraine – Key Principles, sekä Lesson 25: Key Principles of Ensuring Cybersecurity and Cyber Defence in the Military Sphere tarjoavat tämän lehden lukijakunnalle mittavissa määrin tutustuttavaa. Löydät julkaisun seuraavasta osoitteesta: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/12/pdf/231208-RusWar-Ukraine-Lessons-Curriculum.pdf

Kansallista valmiuttamme ylläpidetään ja kehitetään jatkuvasti harjoittelun kautta. Esimerkiksi Tieto24-harjoituksen toimeenpano on tämän numeron ilmestyessä alkanut ja ensimmäinen koulutustilaisuus toteutetaan maaliskuun aikana. Tieto-harjoitus on Suomen suurin yritysten ja viranomaisten yhteistoiminta ja tiedonvaihtoharjoitus laajojen hybridi-, kyber- ja informaatiohäiriöiden varalta. Harjoituksen organisoinnista vastaa Huoltovarmuusorganisaation digipooli yhteistyössä Huoltovarmuuskeskuksen, Traficomin Kyberturvallisuuskeskuksen, Poliisin ja Puolustusvoimien kanssa. Erityishuomion kohteena on tällä kertaa Energiasektori ja sen tuontiriippuvuudet. Palaamme tähänkin aiheeseen Viestimies-lehden sivuilla myöhemmin tänä vuonna.

Muistathan myös, että laadukkaat kirjoitukset sopivat lehteen jatkossakin. Lähetä siis viestiä osoitteeseen viestimies@viestiupseeriyhdistys.fi jos sinulla on mielessäsi lehteen sopiva aihe tai innokas kirjoittaja. Samalla muistutan yliopistokentässä tai ammattikorkeakouluissa työskenteleviä siitä, että Viestimies-lehti on Opetus- ja kulttuuriministeriön julkaisupisteisiin oikeuttava D-luokan ammattiyhteisölle suunnattu julkaisu. Tarkasta siis oppilaitoksesi ohjeistus ja muista ilmoittaa meillä julkaistu artikkelisi työnantajasi kautta julkaisurekisteriin, jos säädetyt ehdot täyttyvät. Näkisinkin mielelläni jatkossa lehtemme sivuilla enenevissä määrin ammattikorkeakoulujen ja yliopistojen asiantuntijoiden katsauksia tutkimuksensa kohteista.

Ilolla totean myös, että käsissäsi olevan lehden myötä saamme luettavaksemme ensimmäisen ”Telealan uutisia” -palstan. Jyrki Penttinen pitää meidät jatkossa kiinni alan ajankohtaisessa kehityksessä antaen meille näköalapaikan jatkuvasti muuttuvaan ja kehittyvään kenttään.

Mukavaa kevättä ja antoisia lukuhetkiä tämänkin vuosikerran parissa!

Päätoimittaja
Kimmo Kaipainen

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

Tahto ja kyky

Arvoisat Viestiupseeriyhdistyksen jäsenet sekä muut Viestimies-lehden lukijat! Haluan kiittää teitä edellisen vuoden osallistumisistanne yhdistyksen toimintaan eri muodoin niin seminaareissa, kokouksissamme kuin lehden aktiivisina kirjoittajina ja lukijoina. Vahva, osaava ja yhtenäinen vapaaehtoinen maanpuolustuskenttä on keskeinen osa Suomen puolustusjärjestelmää myös liittoutuneena maana. Annetaan siis toimintamme, tahtomme ja kykymme, näkyä ja kuulua mahdollisimman laajasti. Korkea maanpuolustustahto lähettää selkeän, sotilaallisia aggressioita ennalta ehkäisevän viestin jokaiseen ilmansuuntaan.

Tätä lukiessanne yhdistyksen digitaalisen turvallisuuden seminaari on jo pidetty. Olen ylpeä siitä, että yhdistyksemme vahva brändi mahdollistaa sekä korkeatasoisten puhujien että runsaslukuisen osallistujamäärän saamiseen tilaisuuteemme. Nämä seminaarit vahvistavat jäsenistömme sekä sidosryhmiemme välistä yhteenkuuluvuutta ja keskinäistä tuntemista, samalla kun luonnollisesti ammatillinen tiedonvaihto tehostuu. Verkottunut ja toisensa tunteva reservimme, niin henkilö- kuin yritystasolla, on vahva signaali Viestiupseeriyhdistyksen roolista korkean maanpuolustustahdon ylläpidossa.

Korkeatasoisten seminaarien lisäksi saan olla ylpeä myös yhdistyksemme Viestimies-lehdestä. Kiitän yhdistyksen hallituksen puolesta edellistä päätoimittajaa, everstiluutnantti Pasi Puhakkaa, lehden korkeatasoisen toimituksellisen linjan ylläpitämisestä. Samalla toivotan uuden päätoimittajan, majuri Kimmo Kaipaisen, mukaan hienoon joukkoomme. Jo ensimmäisissä yhteisissä keskusteluissamme on Kimmo tuonut esille ajatuksiansa lehden toiminnan kehittämisestä, jotka kaikki ovat omaan korvaani kuulostaneet kannatettavilta. Jätän niiden tarkemman esittelyn päätoimittajalle.

Viestiupseeriyhdistyksen perinteiset jäsenmatkat ovat olleet tauolla jo vuosia. Syynä varmaan ovat olleet niin Korona-pandemian vuodet kuin myös se to-

siasia, että aika monet jäsenet jo työnsä puolesta saavat – tai joutuvat – matkustamaan aivan riittävästi. Yhdistyksen hallituksen ja jäsenistön kanssa käydyissä keskusteluissa on kuitenkin noussut esille Nato-jäsenyytemme mahdollistama ovien avautuminen aiemmin meiltä suljettuina olleisiin kohteisiin. Uskon tähän myös itse. Alustavasti syys-lokakuulle suunnitellun matkan valmistelu käynnistyy kevätkaudella ja siitä viestitään yhdistyksen eri kanavissa vielä näillä lumilla.

Alkaneen vuoden 2024 Viestiupseeriyhdistyksen toiminta pitää sisällään myös jotain uutta. Tulemme yhdessä Puolustusvoimien sekä muiden sidosryhmiemme kanssa selvittämään, voisivatko yhdistyksen työelämässään kokeneemmat jäsenet jollain tavoin olla tukena vasta uraansa aloittaville tai aloittaneille. Tämä koskisi sekä sotilas- että siviilitehtävissä palvelevia ja palvelleilta. Ajatuksena on ollut malli, jossa Viestiupseeriyhdistys saattaisi yhteen omia kokemuksiaan jakamaan valmiit sekä näitä kokemuksia kuulemaan haluavat henkilöt. Tämän tyyppiseen toimintaan aloite on tullut kentältä. Selvitämme tarpeet ja mahdollisuudet tarkemmin ja viestimme niistä vuoden toisella puoliskolla.

Yhtenä, sanoisin henkiin herätettävänä, toimintamuotona suunnitelmissa on lisätä yhteistoimintaa Puolustusvoimien kanssa aselajin perinteisiin liittyvässä toiminnassa. Toiminnan muodot ja määrä selvitetään tarkemmin, mutta jo tätä kirjoitettaessa on sovittu aselajin vuosipäivän tilaisuuteen Karjalan prikaatissa 1.3.2024 sisällytettävästä Viestiupseeriyhdistyksen roolista. Perinteiden vaalimiseen liittyvistä näkökohdista ja esityksistä kuulisin mielelläni myös jäsenistön, niin kokeneimpien kuin nuorempienkin, ehdotuksia.

Toivotan kaikille terveyttä, menestystä ja rauhaa vuodelle 2024!

Pertti Hyvärinen
Viestiupseeriyhdistyksen puheenjohtaja

Millainen on tulevaisuuden digitaalinen taistelukenttä?

Uuden teknologian vaikutukset usein yliarvioidaan lyhyellä aikavälillä ja aliarvioidaan pitkällä aikavälillä. Sotilaallisessa toiminnassa uusi teknologia tai teknologialle annettu uusi käyttötarkoitus ei yksin riitä. Todellinen suorituskyky muodostuu käyttöperiaatteiden, teknologian, osaamisen ja toimintaa varten muodostettujen organisaatioiden yhteistoimintana. Kehittämisen pohjalla on kuitenkin aina uusi innovaatio.

Millainen tulevaisuuden digitaalinen taistelukenttä on sinun näkemyksesi mukaan?

Kirjoita näkemyksesi maksimissaan 1000 sanan esseehen. Voit kuvailla esseessäsi yksittäisen mielestäsi mullistavan teknologian käyttömahdollisuuksia ja periaatteita. Voit kuvata teknologista kehitystä sitoen sen sotilaalliseen maanpuolustukseen. Voit maalata isolla pensselillä tulevaisuuden digitaalista taistelukenttää. Voit käsitellä informaatio- tai kybersodankäyntiä, tai voit kuvata viesti- tai johtamisjärjestelmien kehitystä. Sana on vapaa – innovoi!

Lähetä esseesi yhteystietojesi kanssa elokuun 15. päivään mennessä osoitteeseen viestimies@viestiupseeriyhdistys.fi otsikolla ”Kirjoituskilpailu 2024”.

Toimituskunta valitsee parhaat esseet, jotka palkitaan ja julkaistaan Viestimies-lehden numerossa 4/24.

Kirjoittaja eversti Jarkko Karsikas palvelee pääesikunnan johtamisjärjestelmäosastolla tällä hetkellä projektin johtajana, ja aloittaa apulaisosastopäällikkönä (Kyber) 1.3.2024 alkaen.

TEKSTI: JARKKO KARSIKAS

JOHKE – johtamisjärjestelmäalan toiminnan ja rakenteiden kehittäminen

Tammikuussa 2024 puhuminen Puolustusvoimista, muutoksesta ja turvallisuuspolitiikasta on jopa suurelle yleisölle arkipäivää. Turvallisuuspoliittisen ympäristön muutos, Nato ja Suomen rooli liittoutuneena valtiona ovat meille jo normaalilta tuntuvia asioita, joten tämän kokonaisuuden keskellä yhden toimialan sisäinen muutos tuntuu helposti pieneltä ja yksinkertaisesti toteutettavalta asialta. Asian keskeinen haaste kuitenkin on, että tämä pieni muutos tunkeutuu lukuisten johtamisjärjestelmäalan työntekijöiden päivittäiseen työhön ja vaikuttaa työn tekemiseen. Tämän artikkelin tarkoituksena onkin valottaa hiukan johtamisjärjestelmäalan muutosta isojen muutosten ohessa.

Taustaa

Johtamisjärjestelmäalan toiminnan ja rakenteiden kehittäminen – kuten niin monet muutkin muutosohjelmat – käynnistettiin perustamalla muutostarpeita selvittävä työryhmä. Tuon työn taustatekijöinä toimi polku 2000-luvun alkupuolen tietohallinnon rationalisoinnista (TIERA) aina puolustusvoimauudistukseen saakka. Kumulatiivinen muutos yhdistettynä teknologian uudistumiseen oli jälleen haastamassa meitä. Eikä maailmantilanne helpottanut asiaa. Koko 2020-luvun alkuhan oli ollut todella poikkeuksellinen ja kriisien täyttämä. Covid -virus jylläsi, Suomi oli poikkeustilassa ja kansalaisten työn tekemistä muutettiin muun muassa määräämällä ihmiset etätyöhön. Sitten Venäjä aloitti Ukrainan jo jäätyneeksi tuomitun kriisin kiristämisen. Näiden muutosten keskellä johtamisjärjestelmäalan johto kamppaili suorituskyvyn kehittämisen, toiminnallisten haasteiden ja teknologian kehityksen kanssa. Jotain oli tehtävä.

Vuoden 2021 lopulla Pääesikunnan johtamisjärjestelmäpäällikkö käynnisti selvitystyön toimialan haasteiden kartoittamiseksi sekä niiden pohjalta muodostettavan tulevaisuusstrategian laatimiseksi. Työ pääsi hyvin käyntiin ja pidetyt työpajasarjat tuottivat näkymää toimialan kohtaamiin haasteisiin sekä etenkin mahdolliseen muutosstrategiaan ja sen kulmakertoimeen. Ensimmäisen vaiheen isoin valintahan liittyy tavoiteltavan muutoksen kokoon ja vaikuttavuuteen. Pohdinnan ollessa lähes loppusuoralla 24.2.2022 Venäjän laajamittainen hyökkäys Ukrainaan kuitenkin keskeytti työn sekä valmistelun hetkeksi Puolustusvoimien huomion siirtyessä täysipäiväisesti puolustuskyvyn nostamiseen.

Saavuttaessa syksyyn 2022 Puolustusvoimien sisäinen tilanne oli rauhoittunut jonkin verran. Työtä oli kaikilla valtavasti ja Naton jäsenyyteen liittyvät selvitykset sekä ennakkovalmistelut olivat käynnissä. Ukrainan tilanne oli kuitenkin konkreettisesti osoittanut tietoteknisen ketteryyden, kybersuojan ja innovatiivisen toiminnan merkityksen koko puolustusjärjestelmälle. Vaikka olimme selviytyneet tähän saakka muun muassa varustautumisen käynnistämisen haasteista hyvin, olivat haasteet tietojärjestelmien kehittämisessä sekä käyttöönotossa selkeästi asia, johon tulisi hakea ratkaisua. Samalla tulisi ratkaista tarpeita, jotka liittyivät erilaisen saatavilla olevan datan hyödyntämiseen, tekoälyn nopeaan kehittymiseen sekä erilaisten prosessien digitalisointiin.

Johtamisjärjestelmäkonsepti strategiakartalla, versio 2022.

Johtamisjärjestelmäalan muutoksen valmistelu

Lokakuussa 2022 käynnistettiin muutosprosessin esiselvitys ja valmistelu. Tavoitteena oli luoda lähtökohtaperusteet muutosprosessille sekä hahmottaa tavoiteltavan muutoksen suuruusluokka. Jo perusteiden luominen osoittautui erittäin haastavaksi. Työn aikataulu oli kunnianhimoinen, eikä työryhmätyöskentelyn tilannetta helpottanut samaan aikaan tapahtuva muu puolustusvoimallinen valmistelu. Esiselvitys päättyikin perusteiltaan varsin sekavaan tilanteeseen, jossa pääesikunnan tasolla tehtävistä toimenpiteistä päästiin kohtuulliseen yhteisymmärrykseen, mutta toimialan keskeisimpien toimijoiden (Puolustusvoimien johtamisjärjestelmäkeskus ja Järjestelmäkeskus) rooli jäi isosti auki. Muutoksen laajuuden osalta todettiin, ettei sitä uloteta puolustushaaroihin. Puolustusvoimien palvelukeskuksessa muutos ulottuisi vain palvelupistetoimintaan. Tausta-ajatuksena oli muutoksen kapselointi hallittavaksi kokonaisuudeksi, vaikka kokonaisvaltaisemmallekin lähestymiselle todettiin olevan selkeää tarvetta. Tällä päästiin kuitenkin liikkeelle.

Muutoksen käynnistämiseksi luotiin johtamisjärjestelmäkonseptia sekä sen tiivistelmänä strategiakarttaa. Kartta on sinällään hyvin yleisluontoinen, mutta siihen on koitettu nostaa keskeisimmät havaitut asiat. Jälkeenpäin tarkasteltuna kuvassa 1 esitetty strategiakartta on hyvin kuvaava, mutta yleisluontoisena se ei vielä riittävästi pureutunut ongelmiin yksityiskohtaisesti. Konseptin voidaan kuitenkin jälkeenpäin tarkasteltuna todeta olleen varsin osuva. Juuri sen kuvaamia asioita on siis ratkottu.

JOHKE-ohjelma 2023-2024

Varsinainen johtamisjärjestelmäalan toiminnan ja rakenteiden kehittämisen -projekti eli JOHKE-ohjelma perustettiin PEJOJÄPÄÄLL käskyllä 1.3.2023 ja allekirjoittanut nimettiin projektin johtajaksi. Projektilla ja sen tavoitteilla oli jo tässä vaiheessa Puolustusvoimien johdon hyväksyntä. Projektimaisella työskentelyllä ja varsin tiiviillä projektiryhmällä oli tavoitteena ennen kaikkea isossa kuvassa muutoksen käynnistäminen sekä siihen liittyvien haastavien organisoinnin päätösten aikaansaaminen. Kuvaava ensimmäisen vaiheen julistus oli huhtikuussa 2023 pidetyssä tiedotustilaisuudessa esitetty projektin tavoite: ”JOHKE:n tavoitteena on kehittää johtamisjärjestelmätoimialan johtamis- ja toimintakykyä sekä muutoskyvykkyyttä vastaamaan tulevaisuuden haasteisiin”. Tämän tavoitejulistuksen kautta tarkoituksena oli myös korostaa käynnistettävän muutoksen kestoa ja laajuutta. Muutos siis saatetaan liikkeelle, mutta lopputilannetta ei vielä ehkä kyetä täysin näkemään.

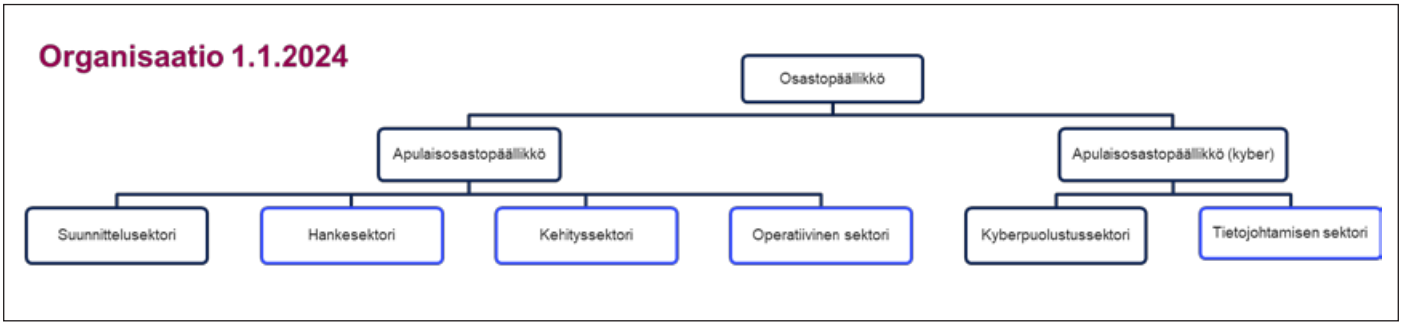
Kokonaismuutoksen ensimmäinen askel suunniteltiin toteutettavaksi kolmessa vaiheessa:

1.) Perusteiden määrittäminen, toimialan toimintamallin suunnittelu ja PE muutoksen suunnittelu kesään 2023 mennessä.

2.) PVJJK:n, JÄRJK:n ja PVPALVK:n muutoksen suunnittelu sekä PE muutoksen käynnistäminen 2023 loppuun mennessä.

3.) PVJJK:n, JÄRJK:n ja PVPALVK:n muutoksen käynnistäminen, koko toimialan toimintamallin uudistaminen sekä muutoksen seuraavien vaiheiden suunnittelu vuoden 2024 aikana.

Tässä vaiheessa muutos on siis koskettanut ennen kaikkea pääesikuntaa. Pääesikunnan johtamisjärjestelmäosasto aloitti uudella organisaatiolla 1.1.2024. Sisäistä rakennetta muokattiin teknologiajakoisesta toiminnalliseen. Samalla PEJOJÄOS otti vastaan tiedonhallinnan sekä toiminnanohjauksen vastuita. Esimerkiksi PVERP 2.0 ja PVASIA hankekokonaisuudet sekä niitä valmisteleva henkilöstö siirtyi osastolle. Johtamisjärjestelmäosastolla on siis tänä päivänä vastuullaan ”lattiasta kattoon” kaikki tietoon, tietojärjestelmiin ja tietoliikenteeseen liittyvä mukaan lukien tieto- ja kyberturvallisuus. Tämän kokonaisuuden tietenkin kruunaa taistelukyky kyberympäristössä.



PEJOJÄOS organisaatio 1.1.2024 alkaen.

JOHKE-ohjelman vaiheistus tavoitteineen on tähän saakka pitänyt varsin hyvin. Myös yksityiskohtaisempia vaiheille asetettuja tavoitteita on saavutettu etenkin jälkeenpäin tarkasteltuna varsin hyvin. Ohjelma etenee tällä hetkellä vaiheessa 3. ja muutoksen ensimmäisen askeleen jalanjälki alkaa hahmottua. Vielä on liian aikaista arvioida lopputilannetta, mutta oppeja matkan varrella on tullut rutkasti. Siitä lisää seuraavassa.

Muutosmatkalla opittua

Olen koonnut tähän omia havaintoja muutoksesta. Näiden havaintojen kirkastajina itselleni ovat toimineet kollegat ja asiantuntijat. Välillä ahdistavakin muutoksen tekeminen on kirkastanut hyvän työskentelyilmapiirin merkitystä ja avoimen kommunikaation välttämättömyyttä. Tässä kaiken teknologisen hurjastelun keskellä keskeisimmät opit ovat kuitenkin kaikkialla muualla kuin teknisissä asioissa.

Ihminen

Ensimmäinen ja keskeisin oppi muutosmatkalla on ollut, että muutoksen ytimessä ovat ihmiset. Muutokselle voidaan määritellä hienoja ja mahtavia tavoitteita, mutta jokaisen ihmisen pitää ymmärtää mistä on kysymys. Tätä taustaa vasten kannattaa aina tarkastella tehtyjä suunnitelmia ja valmisteluja. Jos ihmisten roolia muutoksessa ei ole huomioitu, ei muutoksella ole onnistumisen edellytyksiä.

Muutos on matka.

Matkan vaiheet ovat ihmisille yksilöllisiä, mutta kaikki vaiheet ovat jo tulleet tutuiksi. Matka alkaa yleensä liian nopeasti ja aiheuttaa sekaannusta sekä epävarmuutta. Epävarmuus ja epäselvyys purkautuu helpoimmin vihana, jonka kohde saattaa vaihdella. Matkan tarkoituksen selkiytyminen mahdollistaa eteenpäinmenon ja vähittäisen matkan hyväksynnän. Hyväksyntä muuttuu parhaimmassa tapauksessa innostukseksi uudesta sekä uuden luomiseen. Koko matkan tekeminen vaatii hyvää johtamista ja kommunikaatiota. Ihmiset matkustavat myös eri vauhtia, joten samassa organisaatiossa on todennäköisesti kaikissa vaiheissa olevia matkustajia. Ei ole helppoa matkustajilla tai esimiehillä näissä tilanteissa.

Osallistaminen

Muutosmatkaa helpottaa merkittävästi osallistaminen. Viisaus on organisaatioissa usein syvällä, aivan tekijöillä saakka. Johto näkee tästä viisaudesta oman jäävuoren huippunsa, ja työntekijät oman kokonaisuutensa. Ihmiset sitoutuvat muutoksiin, joita he kokevat olevansa itse luomassa. Pienessä ryhmässä muodostetut tavoitteet ja niiden jalkauttaminen ei sitouta ihmisiä. Tavoitteita ei koeta omaksi tai välttämättä edes ymmärretä niiden sisältöä ja perusteita. Ulkoa saneltu muutos koetaan siis jonkun muun asiaksi.

Osaaminen

Muutoksen tekeminen on myös suuresti yksilöiden osaamista. Muutosjohtaminen, muutosviestintä, toiminnallinen kehittäminen, uusien toimintatapojen ja työkalujen käyttöönotto vaativat kaikki etenkin esihenkilöiltä valmentavaa otetta. Muutos on isosti osaamisasia! Muutoksen on myös oltava hyvin konkreettista ja ponnistettava pienistä asioista kohti isompia. Esimerkiksi kokouskäytäntöjen kehittäminen, uusien työkalujen hyödyntäminen ja uuden toiminnan valmentaminen ihmisille on välttämätöntä, jos muutoksesta halutaan saada pysyvää. Isossa organisaatiossa kaikki tämä vaatii melkoista panostamista osaamiseen ja sen kehittämiseen. Ja kuten kaikessa toiminnassa, hyvät valmentajat selviävät millä tahansa joukkueella mistä vain.

Lopuksi

Johtamisjärjestelmäalan toiminnan ja rakenteiden kehittäminen, JOHKE, on siis edellä kuvatun mukaisesti moniulotteinen kokonaisuus. Kehittämistä voidaan tarkastella organisointina, toimintamallin kehittämisenä, osaamisen kasvattamisena tai vaikka prosessityönä. Kaikki näkökulmat ovat oikeita, mutta kokonaistavoitteen näkökulmasta ne ovat vain osa kokonaisuutta. Muutoksen ydintä on päivän päätteeksi sotakoneen toiminnan varmistaminen ja maanpuolustusvalmius. Meillä pitää olla jatkuva valmius vastata osaltamme Suomen puolustuksesta. Tämän tavoitteen eteen me kaikki Puolustusvoimissa työskentelemme.

JOHKE-ohjelma päättyy erillisenä toimintona 1.3.2024. Vuosi on ollut monivaiheinen, moniulotteinen ja tarjonnut runsaasti tilaisuuksia oppia uutta. Haluan osoittaa ison kiitoksen matkan varrella tukeneille ja muutosta tehneille henkilöille. On ollut kunnia tehdä työtä kanssanne!

TEKSTI: SAIMA RATASVUORI, KUVAT: TATU TAHKOKALLIO

Quo vadis – PVARKI?

Kirjoittaja komentaja Saima Ratasvuori on toiminut useammassa tehtävässä PVARKI kokonaisuuden parissa niin joukko-osastossa, puolustushaaraesikunnassa kuin Pääesikunnassakin. Lisäksi hän on johtanut yhden tutkimushankkeen aiheeseen liittyen ja valmistellut PVARKI-normin sisältöä ja sen jalkauttamista Pääesikunnassa.

Ukrainan vuonna 2014 alkanut sota ja sen viimeisimmät vuodet ovat osoittaneet, että mobiililaitteet, kuten älypuhelimet ja tabletit, ovat siirtyneet arkipäiväiseen käyttöön myös sotilaskäytössä. Taistelukentällä nämä laitteet tarjoavat sotilaille nopean ja tehokkaan tavan viestiä, koordinoida toimintaa ja ylläpitää tilannekuvaa. Reaaliaikainen tiedonsiirto on nyt kriittinen osa joukkojen menestyksekästä toimintaa, ja mobiililaitteet ovat olleet osa tätä murrosta. Reaaliaikainen tiedonsiirto mahdollistaa myös informaation kulkemisen nopeammin taistelukentältä tiedotusvälineille ja erilaisille foorumeille. Samalla informaation siirtyminen ympäröivästä maailmasta taistelukentälle on nopeutunut, jolloin sotilaiden altistuminen erilaisille informaatio-operaatioille on mahdollista.

Tässä artikkelissa tarkastellaan Puolustusvoimallista PVARKI-kokonaisuutta. PVARKI-kattotermillä tarkoitetaan tavoitetilassa Puolustusvoimien arjen kokonaisuutta, joka koostuu saatavilla olevista palveluista, ohjelmista, ratkaisuista, laitteista, välineistä ja teknologioista, sekä niiden käyttöön liittyvästä ohjeistuksesta, innovointitoiminnasta, kehittämisestä ja käytöstä. PVARKI sisältää myös puolustusvoimallisesti kaikille tarjottavia arjen ratkaisuja, joiden jakelu toteutetaan keskitetysti, sekä käyttötapauskuvauksia ja ratkaisumalleja eri tilanteisiin.

”Quo vadis” on latinaa ja tarkoittaa suomeksi ”Minne menet”. Lausetta käytetään usein viittaamaan tilanteeseen, jossa henkilö joutuu pohtimaan tulevaisuuttaan tai suuntaansa elämässä. PVARKI-kokonaisuuden osalta kyse on sen miettimisestä, miten saadaan olemassa olevilla resursseilla uhkaa vastaavasti hyödynnettyä kokonaisuuteen kuuluvia mahdollisuuksia. Miten nykytilanteeseen on päästy ja mihin suuntaan ollaan menossa?

Unde venis – Mistä tulet?

Puolustusvoimissa on jo Ukrainan sodan alkuvaiheista alkaen perehdytty mahdollisuuteen hyödyntää reserviläisten omia päätelaitteita ja operaattoreiden tietoliikenneverkkoja. Vuonna 2016 julkaistussa PUOLUSTUSVOIMIEN JOHTAMISEN TUEN KONSEPTI 2030 -dokumentissa esitettiin uutena lähestymistapana Arjen järjestelmät. Tavoitteena oli hyödyntää jokapäiväisessä käytössä olevia toimintamalleja ja välineitä Puolustusvoimien johtamisen tukemiseen. Tavoitteena oli, ettei järjestelmiä tule edes pyrkiä muokkaamaan sotavarusteiksi, vaan niiden käyttö on sovitettava toiminnallisella tasolla osaksi johtamisen tukea. Järjestelmillä nähtiin mahdollisuuksia vastata kasvaviin vaatimuksiin yllätyksellisyydestä, kattavuudesta ja yhteistyökyvystä. Konseptissa ajateltiin arjen järjestelmien tiedon suojaustason olevan matala. Tiedon suojaustason mataluus ja riippuvuus ympäröivästä infrastruktuurista on tiedostettava riskinä operaatioturvallisuudelle. Konseptissa nähtiin riskien vähentämiseen voitavan vaikuttaa käyttö- ja toimintaperiaatteilla.

Konseptin julkaisun jälkeen Puolustusvoimissa on toteutettu kaksi tutkimushanketta PVARKI-kokonaisuuteen liittyen. Useiden opinnäytetöiden lisäksi Puolustusvoimallisissa tutkimushankkeissa on toteutettu kaksi kokonaisuutta aiheeseen liittyen. Ensimmäisessä lähestyttiin asiaa Arjen verkostojen ja sovellusten kehittämisen kautta. Toisessa painopisteessä oli tietoturvallisuuden lisääminen TLIV käyttö rajoitettu -vaatimusten kautta. Tavoitteena oli löytää sekä uhkamallityöpajojen että auditointivaatimusten kautta ratkaisuja, joilla yksittäisissä joukoissa voitaisiin parantaa arjen välineiden hallintaa ja mahdollistaa TLIV-vaatimusten kaltainen ratkaisu.

Lähivuosina on myös koottu PVARKI-toimintaan liittyvää materiaalia Puolustusvoimien henkilökuntaan kuuluvien yhteiseen Sharepoint-työtilaan. Työtilasta löytyy muun muassa ohjeita PVARKI-asioiden huomioimiseen osana operatiivista suunnittelua. Tarjolla on koulutuspaketit Paikka- ja olosuhdepalvelun käytöstä, operatiivisen suunnitteluprosessin eri vaiheissa huomioitavista asioista, sekä taulukko, jolla voi pyrkiä ennakoimaan toiminnan kustannuksia joukko-osastossa. Operaatioturvallisuuden yksinkertaisimmat lisäosat ovat joukoille tarjottuja kysymyslistoja, joiden avulla pitäisi pystyä välttämään isoimmat karikot Arjen ratkaisuiden käyttämisessä. Useissa joukkoyksiköissä PVARKI onkin muodostunut osaksi johtamisen tuen kokonaisuutta. Käyttöön on myös otettu reserviläisten koodaamia ohjelmistoja, samalla hyödyntäen jo valmiina olevaa tarjontaa erilaisista sovelluksista. Lisäksi on toteutettu yksi laajempi osallistavan asevelvollisuuden ”koodausprojekti”, jossa kokeiltiin vaihtoehtoisia tapoja toteut-

taa vapaaehtoista osallistumista ja saatiin Puolustusvoimille oppia tämän kaltaisesta toiminnasta. Bonuksena mainittakoon tänä vuonna ensimmäistä kertaa Maanpuolustuksen Aloitesäätiön stipendeille noussut reserviläisen kehittämä ohjelmistosovellus.

Ubi es – Missä olet?

Vuonna 2022 Puolustusvoimissa julkaistiin PV ARKI -NORMI – ARJEN JOHTAMISJÄRJESTELMIEN KEHITTÄMINEN JA KÄYTTÖ PUOLUSTUSVOIMISSA. Normi määrittelee toiminnan hyvin pitkälti edellä mainitun konseptin hengessä. *”Arjen välineillä, ratkaisuilla ja järjestelmillä tuetaan ja täydennetään Puolustusvoimien johtamisjärjestelmäkokonaisuutta… Puolustusvoimien joukkojen käyttämät arjen välineet, ratkaisut ja järjestelmät, muodostavat toiminnallisia kokonaisuuksia, joiden on tarkoitus jatkuvasti uudistua loppukäyttäjän operatiivisten vaatimuksien mukaisesti. Arjen ratkaisut eivät ole teknologisia kokonaisuuksia, eivätkä ne lukittaudu yksittäisiin teknologisiin ratkaisuihin.”* Normin ensisijainen tarkoitus on mahdollistaa Arjen välineiden käytön suunnittelu ja harjoittelu joukkoyksiköissä. Päätösvalta käyttämisestä tai käyttämättä jättämisestä on annettu joukkoyksikön komentajalle. Tämä mahdollistaa paikallisten ratkaisujen ketterän käyttämisen ja kehittämisen keskusjohtoisen toiminnan sijasta. Konseptin kirjoitusvuoden (2016) ja tavoitetilan (2030) puolivälin tienoilla olemme siis kyenneet saamaan muutoksen kulttuurissa. Aikaisemmin lähtökohtaisesti kiellettiin kaikki matkapuhelimiin tai muihin ratkaisuihin liittyvä toiminta. Nykyään Arjen ratkaisut ovat osa johtamisen kokonaisuutta ja niiden merkitys myös mahdollisuutena sekä johtamiselle että myös viestinnälle ja informaatiovaikuttamiselle tunnistetaan myös johtamisjärjestelmätoimialan ulkopuolella.

Paljon on saatu aikaiseksi. Toiminnassa on ollut yksi merkittävä kulttuurillinen ero verrattuna perinteisempään Puolustusvoimien ICT-toimintaan. PVARKI kokonaisuutta on rakennettu alhaalta ylöspäin. Asioita lähdettiin kokeilemaan kentällä konseptin hengessä. Asiat kasvoivat alhaalta ylöspäin ja normin kirjoittamisen aikoihin (2022) kokemusta erilaisista ratkaisuista oli jo useammasta

joukosta. Normi kirjoitettiin ohjaamaan toimintaa Konseptin hengessä huomioiden ne kokemukset, joita erilaisissa tutkimuksissa ja kenttäkokeissa, sekä joukkojen omissa harjoituksissa oli syntynyt. Tavoitteena on normin mukaisesti enemmänkin koordinoida kuin kontrolloida toimintaa johtoesikunnista.

Maastoruokailua vai Ruotsinlaivan Buffetia

Jos käytetään kaikille tuttuja ruokaan liittyviä vertauksia, voidaan operatiivisten johtamisjärjestelmien ja PVARKI-kokonaisuuden erot tiivistää vaihtoehdoiksi maastoruokailun ja ruotsinlaivan buffetin välille, ei hinnan, vaan tarjolla olevien vaihtoehtojen näkökulmasta. Operatiiviset järjestelmät ovat toteutukseltaan maastoruokailun ”pönttöjen” kaltaisia. Joku valmistaa ne jossain, ne toimitaan tilauksen mukaisesti sovittuun paikkaan sovitun kokoisena, tai ne ovat noudettavissa jostain. Sisältö on listan mukainen tai ainakin keittopäivänä on joko herne- tai kanakeittoa. Yleensä lämpimänä nautittu ruoka täyttää ruokailijoiden vatsat, kunhan ovat muistaneet ottaa ruokaa sääntöjen mukaisesti, ”pönttö per pönttö, viiden metrin välit, lakki päästä ja pakki oikein päin käteen jne.” Toisin sanoen käyttäjältä ei tässä mallissa vaadita juurikaan ajattelua, vaan se on ulkoistettu jonnekin muualle. Esikunnissa ja joukoissa käytetään niitä johtamisjärjestelmäkokonaisuuksia, joihin ”keskuskeittiö” on miettinyt tarjoiluehdotuksen valmiiksi. PVARKI mahdollisuudet taas muistuttavat enemmänkin Ruotsinlaivan buffetin tarjontaa. Tarjolla on kaikenlaista kalapöydästä lämpimien ruokien kautta pehmiskoneelle, puhumattakaan juomatarjoiluista. Buffetissa toimiminen vaatii sekä tietoa siitä mitä haluaa syödä että osaamista liikkua erilaisten tarjoilupöytien välillä.

Vuosien aikana syntyneen kokemuksen perusteella joukkoyksiköiden PVARKI tekemisen voisi jakaa karkeasti kolmeen osaan. Ensimmäisenä ovat ne, jotka saattaisivat kelpuuttaa PVARKI ratkaisun, jos se tarjoiltaisiin maastoruokailun kaltaisesti valmiiksi ajateltuna ja perille asti toimitettuna. Tosiasiallisesti heillä ei ole aikaa eikä resursseja miettiä asiaa yhtään tämän pitemmälle. Toisessa kategoriassa ovat ne, jotka käyttäisivät Arjen ratkaisuja mielellään, mutta vain jos ne tarjoillaan maastoruokailun kaltaisesti. Äärimmilleen vietynä toisen kategorian joukot pystyisivät venyttämään ajattelunsa henkilöstöruokailun kaltaisiin olosuhteisiin, joissa tarjolla olisi pari harkittua vaihtoehtoa erikseen valituille organisaatioille. Kolmannen kategorian muodostavat joukot, jotka sujuvasti liikkuvat buffetissa tietäen mitä haluavat syödä ja mistä vaihtoehdot löytyvät, lisäksi ne osaavat parhaimmillaan pyytää henkilökunnalta uusia tuotteita tarjolle. Kolmannen kategorian joukoissa PVARKI on ymmärrettävästi jo osa operatiivista toimintaa. Parhaimmissa joukoissa on onnistuttu kehittämään startup henkinen kulttuuri.

Näissä joukoissa henkilökunnan tukemana reserviläiset kehittävät omaa osaamistaan, innovoivat uusia ratkaisuja ja osallistuvat aktiivisesti ”buffetin” tuotteiden ja toimintatapojen kehittämiseen.

Kolmannen kategorian yksiköiden, esimerkkeinä Pirkanmaan ja Etelä-Savon aluetoimistot, toiminnassa on toteutunut hyvin edellä mainitun konseptin tavoitteet kulttuurin muuttamisesta ja arjen järjestelmien hyödyntämisestä. Näissä joukoissa ei ole jääty odottamaan ylemmän johtoportaan toimittamaa valmista ”pönttöä” tai organisaatiouudistusta, vaan on lähdetty hyödyntämään Normin mahdollisuuksia laajasti. Kun toimintakulttuuri ja vapaaehtoisten osallistuminen ovat hyvällä tasolla, on helpompi säädellä toimintaa ja tekniikkaa operaatioturvallisuuden vaatimusten mukaisesti ja jäännösriskejä pienentäen.

Kaikki edellä kuvatut tavat suhtautua asiaan ovat yhtä oikein. Joukkojen tuleekin käyttää PVARKI-normin mahdollisuuksia operatiivisen tarpeen ja oman osaamisensa mukaisesti. Vaikka normi mahdollistaa reserviläisten käytön Arjen järjestelmien ylläpidossa, eroja alueiden ja joukkojen välillä löytyy. Erot erilaisten lähestymistapojen välille syntyvät tarkasteltaessa, kuka saa eniten toiminnallista hyötyä Arjen ratkaisuista ja kenen järjestelmään pystytään tekemään muutoksia paikallisesti nopeassakin aikataulussa.

Solum certum est nihil esse certi

”Varmaa on vain se, ettei mikään ole varmaa.” Tähän lauseeseen tiivistyy se, mikä on sotilaalle vaikeaa PVARKI kokonaisuuden ajattelussa. Sotilas opetetaan hallitsemaan omien ajatustensa lisäksi kaikkea mikä liittyy hänen johdettavakseen uskottuun joukkoon. Sotilaiden koulutukseen liittyy yllättävän paljon kontrollin korostamista johtamisessa, ja vähemmän hallitun riskin koordinoinnin opettamista. Tämän takia on luontevaa, että sotilas vie joukkonsa ennemmin maastoruokailuun kuin buffettiin. Ensimmäinen on tuttu ympäristö ja lähes kaikki on valvottavissa. Helppoa ja riskitöntä, sekä sotilaalle tuttua. Maastoruokailuun liittyy lisäksi useita jonkun muun hoitamia kontrolleja, jolloin jäännösriskit pienenevät, mutta niin saattaa pienentyä ruokailun hyötykin. Jos sotilaan johtamalla joukolla ei ole pakkeja, eikä ruokapönttöjen yhteydessä toimitettu lautasia, voi hyvin kontrolloidusta ruokailusta olla joukon toimintakyvylle erittäin vähän iloa. Toisin sanoen, sotilaan tulisi ymmärtää oman joukkonsa tarpeet ja uskaltaa ratkaista niitä tarpeellisilla tavoilla.

PVARKI kokonaisuuden tarjoama buffet on niin laaja, että useampaa sotilasta pelottaa. Kokonaisuuteen liittyvän epävarmuuden sietäminen vaatii ajattelutavan muuttamista. Kun joukko on buffetin sisäänkäynnin luona, joutuu sotilas miettimään: Osaako joukko syödä oikeita ruokia? Mitä jos ne huutelevat vieraisiin pöytiin? Miten voin varmistua kaiken menevän millilleen oikein? Todennäköisesti kaikki edellä mainitut tapahtumat käyvät jossain mittakaavassa toteen, mutta lopputuloksena saattaa olla hyvin syönyt ja toimintakykyisempi joukko. Todennäköisesti onnistunein tulos saavutetaan, kun joukko ohjeistetaan ennen buffettiin ryntäämistä, mutta jokaista suupalaa ei yritetä vahtia. Tarvittaessa joukon on myös tiedettävä, miten buffetista poistutaan. Erilaisten joukkojen tulisi siis osata hyödyntää laaja PVARKI tarjonta, mutta tarvittaessa toimia myös ilman valittua ratkaisua, jos jotain yllättävää tapahtuu.

Quo vadis – Mihin menet?

Toistaiseksi lähestyminen PVARKI kokonaisuuteen on ollut usein tekniikka edellä kulkemista. Tämä on nähtävissä niin tutkimusohjelmissa kuin kenttäkokeissakin. Buffet esimerkkiä hyödyntäen voisi sanoa, että on keskitytty laittamaan katkaravut, paistisiivut ja jälkiruoka oikeassa järjestyksessä lautaselle. Taustalla lienee toimintaa johtavan toimialan luontaiset taipumukset. Johtamisjärjestelmäalalla usein ollaan teknisesti suuntautuneita ja nähdään asiat hyvin teknisestä näkökulmasta. Alussa toiminnalle ei ollut juuri vaihtoehtoja, sillä kulttuurillinen muutos kaiken matkapuhelimiin liittyvän kieltämisen sijasta mahdollisuuksien etsimiseen ei ollut vielä alkanut. Toisaalta monimutkaisen tekniseltä kuulostava ratkaisuehdotus ja sotilaiden vahva kontrollihakuisuus on myös jonkin verran rajoittanut joukkojen rohkeutta hyödyntää Arjen ratkaisuja osana omaa johtamisjärjestelmäänsä.

Edeltävien vuosien aikana, ennen kaikkea maailmalla olleiden kriisien tukemana, kulttuurillinen muutos toiminnan osalta on käynnistynyt. Arjen ratkaisujen mahdollisuudet ja riskit tunnistetaan aikaisempaa paremmin. Nyt Konseptin tavoitetilan puolivälissä olisikin hyvä hetki miettiä mihin suuntaan PVARKI kokonaisuutta seuraavina vuosina kehitetään.

Erilaisissa keskusteluissa on esiin noussut muutamia vaihtoehtoja: toimintaan painottuva, yhtenäisen järjestelmän rakentamiseen tähtäävä ja normin suunnassa jatkava. Ensinnäkin voidaan panostaa vahvasti toiminnan ohjaamiseen, eli arjen välineiden viestitaktiikan kehittämiseen. Opetettaisiin joukkoja tunnistamaan omalta alueelta ja omaan toimintaan sitoen, että missä arjen välineitä voidaan käyttää, mitä sovelluksia ja verkkoja käytetään, miten käytetään ja kuka käyttää. Tärkeänä taustamateriaalina kysymyksiin vastaamiseen tulisi olla tiedustelun ja operaatioturvallisuuden kanssa yhdessä tuotettu aineisto, jonka pohjalta ymmärrys esimerkiksi puhelimien näkyvyydestä voidaan ulottaa riittävän laajalle. Samalla tulisi kouluttaa riskien vähentämistä toiminnalla ja ehkä jopa sotilaiden hallittua riskin sietämistä, jotta tehtävät saadaan täytettyä. Toisaalta voidaan panostaa yhtenäisen PVARKI teknisen ja toiminnallisen ratkaisun tuottamiseen kaikille joukoille. Kyseistä Puolustusvoimallista ratkaisua johdettaisiin ja ylläpidettäisiin samoin kuin muitakin Puolustusvoimien johtamisjärjestelmiä. Kolmas vaihtoehto on jatkaa normin määrittämässä suunnassa, jossa ei tavoitella kaikille yhteistä järjestelmää, mutta tuotetaan Puolustusvoimallisesti joitakin toimintaa tukevia elementtejä.

Edellä kuvatuista vaihtoehdoista ensimmäinen on toteutettava todennäköisesti tehtävästä valinnasta riippumatta. Tiedustelun ja operatiivisen toimialan kanssa on luotava riittävä operaation vaiheeseen soveltuva ohjeistus toiminnan tukemiseksi. Ukrainasta saatujen kokemuksien valossa etenkin tähän toiminnalliseen puoleen tulee panostaa. Mobiililaitteita käyttävien joukkojen sekä toimintaa suunnittelevien tulee ymmärtää toiminnan näkyvyys esimerkiksi signaalitiedustelussa. Tätä voidaan myös hyödyntää toisin päin. Jos halutaan jonkin joukon pysyvän paremmin piilossa, ohjataan jokin toinen joukko näkymään enemmän. Toiminnalliseen ohjaukseen kuuluu myös informaatio-operaatioiden näkökulma, sekä omien sotilaiden suojaaminen vastustajan operaatioilta että

heidän mahdollinen osallistumisensa omaan informaatiotoimintaan ja viestintään. Tästä saatiin hyviä esimerkkejä Ukrainasta keväältä 2022, jolloin paikallisjoukot täyttivät erilaiset ulkoiset informaatiokanavat, operatiivisten joukkojen jäädessä yleisen huomion osalta hieman katveeseen.

Toinen kuvatuista vaihtoehdoista, eli kaikille yhteinen ratkaisu tuntuisi sotilaista varmasti mukavimmalta ja helpoimmalta. Kontrolli ennen koordinaatiota on tuttu tapa ajatella. Samoin kaiken ylläpidon, tekemisen ja riskien ulkoistaminen jollekin muulle. Toisen vaihtoehdon haasteena on sen ristiriitaisuus konseptin ja normin kanssa. Kaikille yhteisen toimintatavan ja teknisen ratkaisun myötä menetettäisiin se yllätys momentti, joka PVARKI kokonaisuudella on yritetty konseptista asti rakentaa. Yhtenäisen järjestelmän ongelmat, olivat ne kyberin tai tekniikan aiheuttamia, vaikuttaisivat heti kaikkiin käyttäjiin. Toinen vaihtoehto saattaisi myös kasvattaa PVARKI kokonaisuuden ylläpitokuluja ja rajoittaa mahdollisuuksia hyödyntää uusia teknologian ratkaisuja.

Kolmas kuvattu vaihtoehto on kompromissi, jossa toiminnan vapaus ja hyvät toimintatavat tai tekniset ratkaisut pyritään yhdistämään ja skaalamaan myös muiden käyttöön. Kolmannessa vaihtoehdossa Puolustusvoimissa on tehtävä sekä teknistä rakentamista että ylläpitoa. Tämä lisää toisessa vaihtoehdossa tunnistettuja riskejä ylläpidon kallistumisesta ja teknologisen kehityksen hyödyntämisen rajoitteista. Toisaalta kolmas vaihtoehto antaa mahdollisuuden jonkinasteiseen kontrolliin toiminnan osalta.

Lähdettiin Puolustusvoimallisesti PVARKI kokonaisuuden osalta lähivuosina mihin tahansa suuntaan, johtamisjärjestelmäalalla on aina vain yksi tavoite. Viesti vain perille vietynä ratkaisee – Denuntiatio solum traslata valet.

Leo Heng Reaktor

Jarmo Puputti XD Solutions

TEKSTI: LEO HENG, JARMO PUPUTTI

Siiloista yhtenäiseen tilannekuvaan

Monitoimintaympäristöisten operaatioiden haasteet

Kattavan ja ajantasaisen tilannekuvan muodostaminen on keskeinen haaste nykyaikaisella moniulotteisella ja nopeasti muuttuvalla taistelukentällä. Tilannekuvan muodostaminen muuttuu entistä vaikeammaksi, kun puhutaan laajemmasta taistelutilasta. Taistelutilan käsite pitää sisällään varsinaisen taistelukentän ja sotilaallisten toimijoiden lisäksi ympäristön, sääolot, siviili-infrastruktuurin, sekä alueella toimivat siviilit ja muut sotilaallisesti merkityksselliset ryhmittymät.

Sotilaallisen toiminnan suunnittelu ja ohjaaminen tällaisessa tilassa vaatii totuttua laajemman katsantokannan. Perinteisten maa-, meri- ja ilmatoimintaympäristöjen rinnalle alkaakin vakiintua avaruus-, kyber- ja informaatioympäristöt, tosin kahden jälkimmäisen määrittely herättää edelleen keskustelua. Hyvänä nyrkkisääntönä voi todeta, että toiminta kyberympäristössä vaikuttaa teknologiaan, laitteisiin ja verkkoihin sekä määritelmästä riippuen myös sähkömagneettiseen spektriin. Toiminta informaatioympäristössä taas vaikuttaa ihmisten mieliin ja sydämiin. Kun maa-, meri-, ilma- ja avaruusympäristöillä on omat toisistaan erilliset fyysiset ulottuvuutensa, kyber- ja informaatioympäristöt ovat läsnä kaikkialla fyysisessä tilassa.

Nato on ottanut käyttöön käsitteen Multi-Domain Operations (MDO), monitoimintaympäristöoperaatiot, kuvaamaan suunnitelmallista toimintaa, jossa yhdistetään liittouman sotilaallisen voiman käyttö, jäsenvaltioiden ministeriöiden, laitosten ja muiden hallinnollisten elimien toiminta sekä ulkopuolisten sidosryhmien, kuten esimerkiksi tutkimuslaitosten ja yksityisyritysten panos. Kun potentiaalinen vastustaja toimii länsimaissa hybridiuhkakäsitteellä kuvatulla toimintatavalla hyödyntäen kaikkia käytössään olevia keinoja, myös vastatoimet vaativat laaja-alaisuutta.

Kokonaiskäsityksen muodostaminen näin laajasta ja monimutkaisesta toimintakentästä vaatii sekä yhteistyötä eri toimijoiden välisessä tiedon jakamisessa että teknologisia ratkaisuja. Tällä hetkellä käytössä oleva teknologia tarjoaa edellytykset nopealle tilannekuvan muodostamiseen käytettävän tiedon välitykselle, mutta jaettava tiedon määrä edellyttää käytössä olevan tiedonsiirtokapasiteetin kasvattamista ja tiedon eheydestä ja oikea-aikaisuudesta huolehtimista. Lisäksi tiedon omistajuus, tiedon alkuperä ja luotettavuus sekä sen edelleen jakelu tarvitsijoille aiheuttavat lisäkysymyksiä. Tietomassa saattaa myös muodostua niin valtavaksi, ettei pelkästään sen välittäminen riitä, vaan tiedon analysointia tulee automatisoida. Kokonaiskuvan muodostaminen päätöksenteon tueksi toteutuu parhaiten hyödyntämällä tekoälyn mahdollistamia teknologisia kyvykkyyksiä.

MDO-ympäristö on syntytavaltaan, rakenteeltaan ja omistajuudeltaan niin monimutkainen, ettei sitä voida suunnitella tai määritellä etukäteen keskitetysti. Tämän takia on oleellista keskittyä helpon integroitavuuden edistämiseen esimerkiksi kansainvälisten standardien hyödyntämisellä, rajapintoja rakentamalla ja erillisten tiedonkäsittely-ympäristöjen (esimerkiksi eri turvaluokkien ympäristöt) yhdistämistä tukevilla teknisillä ratkaisuilla.

Nopeudesta ylivoimaa

Perinteisesti eri organisaatioiden hallinnoimat erilliset ympäristöt ovat olleet omia siilojaan, jotka toimivat osin hyvin itsenäisesti, ja keräävät dataa omiin käyttötarkoituksiinsa. Erillisten siilojen väliin jää helposti tiedonkulun katveita. Tämän seurauksena yhteisoperaatioiden johtaminen, jossa puolustushaarat ylittävä suunnittelu ja operatiivinen johtaminen ovat erillisiä prosesseja, on haasteen edessä.

Datan käsittelyn kyvykkyyteen pitää panostaa. Mitä nopeampi ketju tiedonsiirrossa on, ja mitä nopeammin tieto on jalostettu kenttäkelpoiseksi, sitä parempi asema on mahdollista saavuttaa. Aiemmin jokainen siilo on kerännyt ja jalostanut dataa itsenäisesti melko pitkälle ennen ylemmälle johtoportaalle toimittamista. Asiakirjoja, dokumentteja ja sähköposteja on laadittu ja jaeltu vakiintuneen prosessin mukaisesti, ja pahimmassa tapauksessa oleellinen tieto on saattanut vanheta jo matkan aikana. Lisäksi tiedon jalostaminen erilliseksi tuotteeksi, joka jaellaan esimerkiksi sähköpostitse tai tallennetaan verkkolevylle, yleensä tarkoittaa sitä, ettei tuotetusta asiakirjasta pysty suoraan palaamaan lähtötietoihin. Kertaalleen jaeltu tuote ei myöskään päivity automaattisesti tilanteen kehittyessä. Näin organisaatio ei aina tiedä, mihin jokin käsitys perustuu, eikä sitä, mikä on ajantasaisin versio jostain tiedosta.

Operatiivinen keskus tarvitsee tiedon nopeasti, ja sen välittäminen alajohtoportaisiin ja sitä kautta myös viimeiselle taistelijalle on avainasemassa modernissa, nopeatempoisessa sodankäynnissä. Erityisen haasteellista on saada eri siiloissa

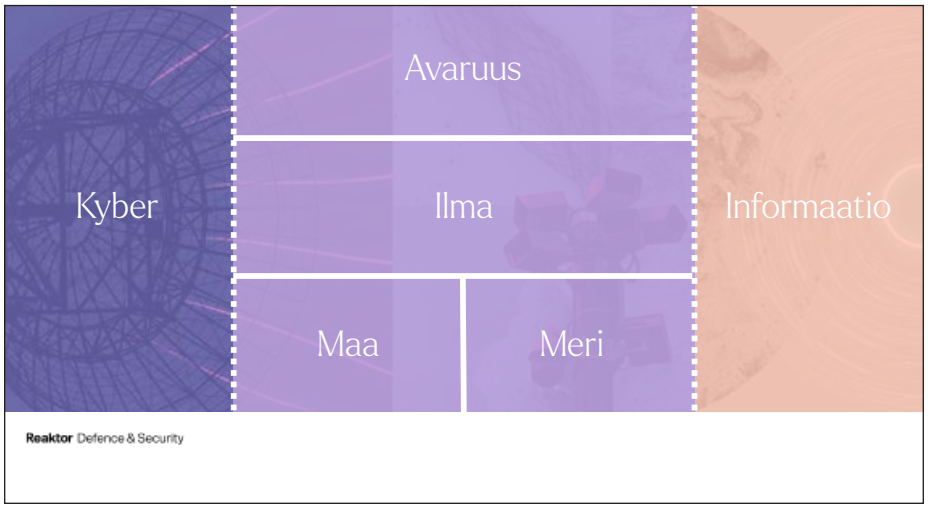
olevat sensorit, ja kineettiseen vaikuttamiseen kykenevät yksiköt toimimaan koordinoidusti ja ilman byrokraattisten komentoketjujen muodostamaa hitautta. Jos tämä haaste kyetään ratkaisemaan, syklisen päätöksenteon silmukka OODA Loop (Observation-Orientation-Decision-Action) nopeutuu, mutta myös samaan aikaan laajenee, kun päätöksenteossa pystytään hyödyntämään tietoa uusista lähteistä.

Tiedon määrä kasvaa väistämättä, ja dataa saadaan yhä enemmän eri lähteistä. Perinteinen ajattelu tiedon kohtaamisesta hyvin korkealla organisaatiossa on murroksessa. Moderni teknologia, sensorit, ja avoimen tiedon lähteet tarjoavat nopeasti analysoitavaa tietoa, jota on mahdollista hyödyntää eri tasoilla.

Viestinnän on oltava nopeaa, asioiden esittäminen ymmärrettävästi pitää olla toimivaa, ja teknisessä toteutuksessa tulee hyödyntää tekoälyä ihmisen tukena. Jos aiemmin tilannekuva on muodostettu vuorokausitasolla, nyt on syytä tavoitella paljon pienempää viivettä tai tietyissä tilanteissa jopa reaaliaikaisuutta.

Tämä haaste herättää kuitenkin paljon lisäkysymyksiä. Millä kaikilla eri sensoreilla pystytään keräämään hyödyllistä tietoa ja mikä tieto yleensäkään on hyödyllistä? Mitä tietoa kannattaa siirtää eteenpäin ja miten se siirretään? Mitä tietoa organisaatiossa jo on? Mitä tietoa tarvitaan sen lisäksi? Miten se saadaan parhaiten kerättyä? Miten käytössä olevat valtavat tietomassat saadaan jalostettua hyödynnettävään muotoon? Miten kerätty tieto tukee päätöksentekoa? Mikä on paras päätös tilanteessa ja miten se on parasta panna toimeen? Miten tieto toimenpiteistä saadaan siirrettyä turvallisesti yksittäiselle taistelijalle uloimmalle luodolle, viimeisimpään poteroon tai korkeimmalle mäenharjalle? Mikä on tehtyjen toimenpiteiden seuraus? Sama sykli alkaa alusta.

Jokaiseen yllä olevista kysymyksistä on paljon erilaisia vastauksia, joista osa liittyy ihmisen tai organisaatioiden toimintatapoihin ja osa on ratkaistavissa teknologialla. Keskeistä parhaan mahdollisen lopputuloksen kannalta on sovittaa nämä kaksi eri puolta yhteen. Teknologian tulee vastata käyttäjän tarpeeseen ja tukea organisaatiota sen tavoitteen saavuttamisessa. Perinteisissä tiedonsiirtoteknologioissa ja tietojärjestelmissä ollaan jo pitkällä,



Toimintaympäristöt: Taistelukentän näkökulmasta keskiössä on meri ja maa, ylempänä ilma ja ylimpänä avaruus, sivuilta fyysisen ympäristön poikkileikkaavina kyber- ja informaatioulottuvuudet. Kybervaikuttaminen kohdentuu teknologiaan ja teknisiin ratkaisuihin, informaatiovaikuttaminen ihmisten mieliin ja sydämiin.

mutta tekoälyn tarjoamia lupauksia vasta kokeillaan. Tekoälyavusteiset järjestelmät tulevat olemaan merkittävä sekä yksilön että organisaation nopeutta ja sitä kautta suorituskykyä lisäävä tekijä. Ihmisen ja koneen yhteistoiminnan suunnittelu ja optimoiminen (human-machine teaming) on tässä keskeisessä roolissa. Tekoäly tulee olemaan monelle meistä työkaveri.

Yhteistyötä yli organisaatiorajojen

Naton MDO-konseptin mukaan liittouman ulkopuoliset sidosryhmät ovat merkittävässä osassa innovaatioiden luomisessa, teknologian hyödyntämisessä ja sotilaallisten kyvykkyyksien kehittämisessä. Sidosryhmiin kuuluvat akateemiset tutkimuslaitokset, yksityinen sektori ja kansainväliset kumppanit, joista monilla on pitkäaikaiset yhteistyösuhteet Naton jäsenmaiden kanssa.

Monitoimintaympäristössä siviiliyritysten korkean teknologian ratkaisut toimivat tärkeänä osana tulevan suorituskyvyn suunnittelussa. Digitaaliset ratkaisut, signaalitekniikka, älykkäät antennit ja langattoman tiedonsiirron kehittyminen luovat uudenlaisia mahdollisuuksia. Digitalisaation tuoma ohjelmoitavuus muodostaa uudenlaisen, monitasoisen suorituskykykokonaisuuden, jossa ohjelmistojen nopea kehitys, ylläpito ja käytettävyys tulee pitää ajantasaisena. Nopeatempoisen ja teknistyvän taistelukentän ongelmanratkaisu vaatii murroksellisen teknologian hyödyntämistä samalla, kun käyttäjän on osattava hyödyntää kehittyviä järjestelmiä ja laitteita.

Teknologian mahdollistama tuottavuusloikka saavutetaan ketteryydellä ja uusilla toimintamalleilla saman vanhan jatkamisen sijaan. Tässä asevoimien tukena on korkean teknologian yrityskenttä. Yksityissektorin teknologiaratkaisut sekä etenkin syvän teknologian innovaatiot tarjoavat tähän hyviä pilotteja.

Uudet toimintaympäristöt vaativat myös uudenlaista osaamista. Perinteiseen järjestelmäkehitykseen koulutetut henkilöt pyrkivät soveltamaan uutta teknologiaa aiemmin opittujen toimintamallien pohjalta. Puolustusvoimat on tehokas koulutusorganisaatio ja osaamisen kehittäminen on huippuluokkaa, mutta kilpailu teknologiaosaajista on kovaa ja yksityisen sektorin houkutus vahva. Suunnitelmallinen osaamisen kehittäminen, jakaminen ja siirtäminen yhdessä kumppaniyritysten kanssa toteutettavissa projekteissa on tärkeä askel kohti tulevaisuutta. Haasteisiin on vaikea vastata yksin.

Suomalainen Digital Defence Ecosystem (DDE) on luotu toiminaan yhteistyöverkostona tässä haasteessa. Ekosysteemin jäsenistö koostuu lähes 30 korkean teknologian siviiliyrityksestä ja tutkimuslai-

toksesta. Ajatuksena on yhdistää siviiliyritysten ketteryys ja huipputeknologia, puolustustarviketeollisuuden alan syvä tuntemus sekä tutkimusorganisaatioiden osaaminen.

Suomi on eturintamassa kehittämässä useita Naton ja EU:n kriittisiksi määrittämiä teknologioita, kuten 5G/6G kommunikaatiota, autonomisia järjestelmiä, tekoälyä, kvanttilaskentaa ja uutta avaruusteknologiaa. Yhteiskunnan eri tasot osallistuvat kokonaismaanpuolustukseen, mikä on jopa muissa NATO-maissa poikkeuksellista. Suomen puolustusrakenteet, teknologiaosaaminen ja niiden hyödyntäminen ovat varmistaneet vahvan aseman myös liittouman jäsenenä myllertävässä maailmantilanteessa. Ekosysteemin jäsenten tehtävänä on myös huolehtia osaltaan teknologiaosaamisen huoltovarmuudesta ja kansainvälisestä kilpailukyvystä Suomessa.

Teknologia kehittyy ja moniulotteinen toimintaympäristö laajenee kiihtyvällä vauhdilla. Teknologiayrityksissä piilee syvän asiantuntemuksen lisäksi vahva maanpuolustustahto ja ketterän kehittämisen malli. Yhteistyöstä löytyy ratkaisu tulevaisuuden teknologiahaasteisiin.

Esittelyssä DDE:n jäsenyritys

Reaktor on yksi DDE:n perustajayrityksistä. Yrityksen ydintoimintaa on suunnitella ja kehittää uudenlaisia digitaalisia ratkaisuja ja auttaa asiakasorganisaatiotaan yhdistämään eri teknologiat tehokkaimmalla tavalla. Reaktor on Suomessa perustettu, kuudessa maassa ja kolmella mantereella toimiva teknologiakonsulttiyritys, joka suunnittelee ja toteuttaa digitaalisia tuotteita ja palveluita.

Reaktorin puolustus- ja turvallisuusliiketoiminta keskittyy luomaan kansallisesta turvallisuudesta vastaaville viranomaisille kilpailuetua toteuttamalla ratkaisuja, jotka mahdollistavat datan käsittelyn nopeammin ja tehokkaammin. Kun oikea tieto on oikeassa paikassa oikeaan aikaan, se antaa etulyöntiaseman päätöksenteossa ja toimenpiteiden toteuttamisessa. Yrityksen tarjoamat ratkaisut keskittyvät datan keräämisen, varastoinnin, käsittelyn, analysoinnin ja jakelun tehostamiseen sekä asiakasorganisaatioiden suorituskyvyn kasvattamiseen tekoälyä hyödyntämällä.

Kuva © iStockPhoto.

Reaktor on ollut mukana luomassa puolustushallinnon tekoälystrategiaa ja toimii tällä hetkellä toimittajana useissa puolustusvoimien keskeisiä suorituskykyjä toteuttavissa tietojärjestelmäprojekteissa.

Reaktor tarjoaa sekä räätälöityjä ohjelmistoprojektitoteutuksia että valmiita tuotteita. Tuotevalikoima sisältää kansainvälisesti yhteensopivan informaatiofuusioratkaisun tilanneymmärryksen rakentamiseen, erillisissä ympäristöissä sijaitsevien tietojärjestelmien välisen integraation mahdollistavan Cross-Domain API Guard (CDG) -yhdyskäytäväratkaisun sekä data lake -ratkaisun, joka tuo skaalautuvan pilviteknologian hyödyt ja kyvyn ajaa tekoälyhyötykuormia suljetussa ympäristössä omilla palvelimilla toteutettuun korkean turvallisuuden tietoallastoteutukseen.

Lisätietoja www.reaktor.com/defsec

Kirjoittajat:

Leo Heng

Leo Heng työskentelee Reaktorin puolustus- ja turvallisuusliiketoiminnasta vastaavana strategiajohtajana. Hänen taustansa on käyttäjäkeskeisessä suunnittelussa, mutta viime aikoina hän on keskittynyt siihen, miten globaali turvallisuustilanne vaikuttaa suomalaisen yhteiskunnan kokonaisturvallisuuteen ja mikä rooli teknologialla on tässä kehityksessä. Leo pyrkii ymmärtämään eri kansallisen turvallisuuden organisaatioiden tarpeita ja tukemaan näitä tehtävässään onnistumisessa.

Jarmo Puputti

Jarmo Puputin johtama XD Solutions toimii Digital Defence Ecosystemsin koordinaattorina. Jarmon yli 30-vuotiseen uraan on kuulunut rauhanturvatehtävät Lähi-Idässä, autonomisten työkoneiden ja modernien asejärjestelmien kehitystä, laajojen kehitysohjelmien johtamista, kansainvälisten liiketoimintojen kehittämistä sekä liiketoimintojen turn-around haasteita. Jarmo on toiminut liiketoiminnan johtotehtävissä mm. Patriassa, Nokian Renkailla ja Raisiossa.

Lyhyesti Ekosysteemistä

Digital Defence Ecosystem luo merkittävää uutta liiketoimintaa suomalaiseen puolustus- ja turvallisuussektoriin yhdistämällä puolustus-, turvallisuus- ja siviiliteknologioiden eturivin yritykset ja tutkimuslaitokset. DDE osallistuu aktiivisesti EU:n ja NATO:n uusimpiin puolustusteollisuuden aloitteisiin, kansallisiin veturihankkeisiin ja verkottuu kansainvälisesti. Ekosysteemiä koordinoi XD Solutions.

www.digitaldefence.fi

DDE:n jäseniä ovat: Bittium, Elfys, Elomatic, Epec, GIM Robotics, Insta, Jyväskylän yliopisto, Kelluu, KuvaSpace, Loihde, Mevea, Millog, Modirum, Nokia, Radientum, Reaktor, ReOrbit, Saab Finland, Savox, Senop, Solita, Tampereen yliopisto, Unikie, VTT, Wirepas

Reaktor) DIGITAL DEFENCE ECOSYSTEM

TEKSTI: JYRKI PENTTINEN, USA

Open RAN

Vaikka mobiiliverkkojen arkkitehtuurit ovat kehittyneet merkittävästi vuosikymmenten saatossa, niiden radio- ja kytkentäverkkojen periaatteet ovat pysyneet samoina. Matkaviestintäoperaattorit hallinnoivat joukkoa verkkoelementtejä ja niiden laitteistoja sekä ohjelmistoja, joista kullakin on määritetyt toimintonsa. Verkkotoimintojen virtualisointi on tullut mahdolliseksi erityisesti viidennen sukupolven (5G) matkaviestintäjärjestelmien palvelupohjaisen arkkitehtuurimallin ansiosta. Samalla vakiintuneet ja uudet standardointielimet päivittävät perinteisiä malleja. Operaattoreilla on siten pikkuhiljaa aiempaa paremmat mahdollisuudet suunnitella ja ottaa käyttöön myös modernisoituja, avoimen radioverkon (Open RAN) mukaisia ratkaisuja.

Taustaa

Radioverkko on langattomien järjestelmien kriittisin ja haastavin osa siksi, että radiorajapinnan signaalien ja häiriöiden tasoa sekä kapasiteettivaatimuksia on usein vaikeaa ennakoida. Radiolinkkibudjetin ja radioverkon kuormitussimulaatioiden avulla operaattorit voivat arvioida peittoalueiden kokoa ja tyypillisiä datanopeuksia perustuen radioaaltojen etenemisvaimennuksiin, signaali-häiriötasoihin ja yhteyksien laatuun, mutta tuntemattomat tekijät, kuten dynaamiset, ennalta-arvaamattomat käyttökeskittymät voivat vaikuttaa arvioituun radioyhteyden laatuun.

Verkkojen uudet toiminnot, kuten radioverkon toimintojen hajauttaminen antennielementtien, tukiasemalaitteiston, ja radioverkon ohjausyksiköiden välillä, parantavat radioverkkojen suorituskykyä, koska ne voivat sopeutua optimaalisemmin vaihteleviin tilanteisiin tarjotun kapasiteetin ja saavutettavissa olevan suorituskyvyn suhteen. Erityisesti radioverkon toimintojen jako keskitettyihin ja jaettuihin radioverkon yksiköihin voivat tarjota mahdollisuuden prosessoida tukiasemien toimintoja kauempana itse tukiasemalaitteistosta, ja verkko voi siten jakaa vaadittavaa kapasiteettia tarpeen mukaisesti eri alueilla tasapainotellen eri tukiasemien tarjoamaa liikennettä esimerkiksi pilvessä prosessoituna.

Ei pelkästään dynaamisen luonteensa vuoksi, mutta radioverkko on haasteellinen myös siksi, että radioverkkoarkkitehtuurit ja niiden rajapinnat edustavat tyypillisesti varsin suljettua verkkoinfrastruktuuria. Siksi ”perinteisen” verkkoratkaisun yksittäisen radiosegmentin toimintoja on ollut vaikeaa, ellei mahdotonta, prosessoida eri laitevalmistajien kesken.

Vuosien suunnittelun tuloksena avoimen radioverkon konsepti (Open RAN) on tullut vähitellen mahdolliseksi, erityisesti 5G-järjestelmän käyttöönoton yhteydessä. Esimerkiksi O-RAN Alliance (lyhennettynä O-RAN), joka on yksi tärkeimmistä Open RAN -konseptin kehittäjistä, on jo tuottanut konkreettisia määrityksiä, jotka täydentävät 3GPP:n määrityksiä abstraktoimalla radioverkon rajapintoja.[1] Määritykset sisältävät edistyneitä käyttöönottovaihtoehtoja ja mahdollistavat uusien toimijoiden liitynnän ekosysteemiin siten, että kukin voi tarjota vaihtoehtoisia tai rinnakkaisia radioverkon toimintoja yksittäisen radioverkon sisällä. Nimenomaan tämä ekosysteemin avoimuus on yksi Open RAN -konseptin hyötyjä, ja on odotettavissa, että eri toimijoiden mukanaan tuoma toimintojen tarjonta vaikuttaa myös positiivisesti verkkoelementtien ja verkkojen käytön hintoihin.

Open RAN:n kehitys

3GPP on luonut alustan avoimen radioverkon kehitykselle mahdollistamalla radioverkkojen toiminnallisen jaon perustuen radioyksikköön (radio unit, RU), jaettuun yksikköön (distributed unit, DU) ja keskitettyyn yksikköön (centralized unit, CU). 3GPP:n määrittelyt ovat joustavia ja toimivat perustana radioverkon merkinantoon, kapasiteetin jakoon ja prosessointiin siten, että osa tukiaseman toiminnoista voidaan suorittaa muualla, kuten reunapilvessä (edge cloud).

Vaikka 3GPP on spesifioinut em. radioverkon toiminnallisen jaottelun, kyseiset radiojärjestelmien sisäiset rajapinnat ovat pysyneet vielä käytännössä laitevalmistajakohtaisina ja 3GPP:n jakomalli ei siten mahdollista vielä sellaisenaan avaamaan markkinoita yksittäisen radioverkon monitoimittajaympäristölle. Eri tahot ovat siksi jatkaneet avoimemman konseptin kehitystä, ihanneratkaisun ollessa eri radiokomponenttien toimittajien tarjoamien ratkaisuiden automaattinen yhteen liittäminen. Vaikka tällainen ”plug and play” -periaate on haasteellista saavuttaa täysin automaattisesti käytännössä, ja jonkin asteen integrointi on edelleen tarpeen, eri toimittajien ratkaisujen sisällyttäminen yksittäisiin RAN-alueisiin on tulossa todellisuudeksi.

3GPP spesifioi kevyen radiotoiminnallisuuksien jakomallin jo 4G-järjestelmiin, ja on tarkentanut jaottelua edelleen 5G:n myötä. 3GPP tarjoaa siten mahdollisuu-

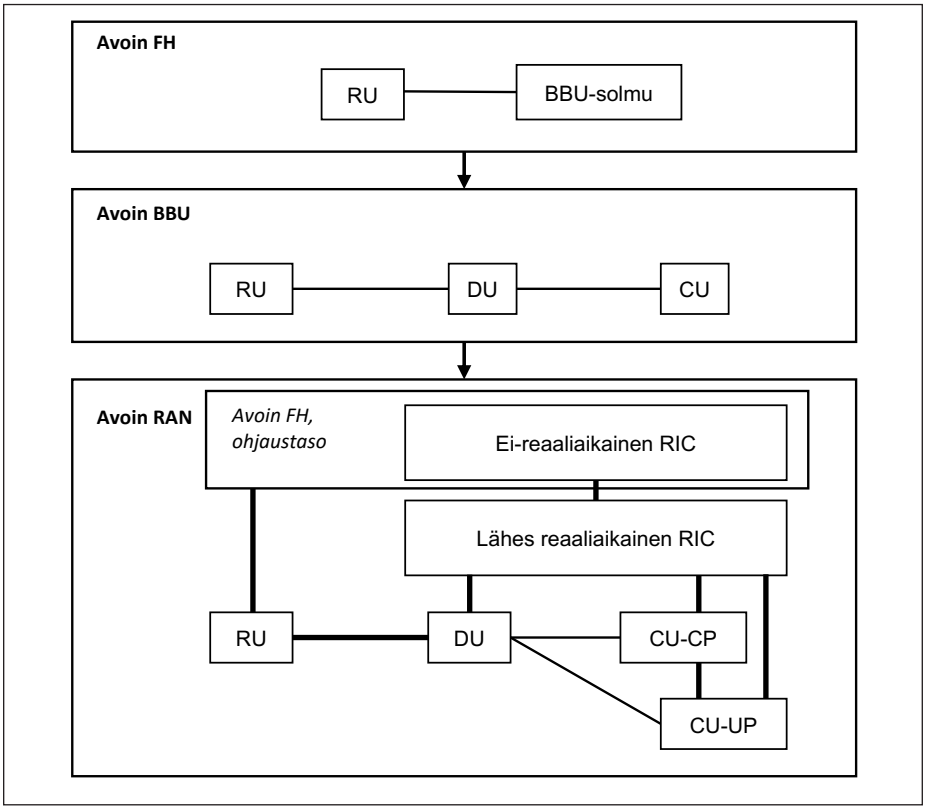
den 5G-tukiasemien (gNB ja sen antennijärjestelmän variantit) CU:n ja DU:n toimintojen jakoon yhteismitallisen F1-rajapinnan kautta. CU voidaan jakaa edelleen hallintatasoon (CU control plane, CU-CP) ja käyttäjätasoon (CU user plane, CU-UP) E1-rajapinnan kautta.

Tällä hetkellä tärkeimmät toimijat, jotka täydentävät 3GPP-standardeja entistä avoimemmilla rajapinnoilla, ovat O-RAN Alliance (O-RAN) ja Telecom Infra Project (TIP). Niiden lisäksi Open RAN -konseptin kehitykseen osallistuu myös monia muita toimijoita, kuten Open Networking Foundation (ONF) ja Open RAN Policy Coalition.

O-RAN on sitoutunut kehittämään radioverkkoja perustuen verkkojen älykkyyteen ja avoimuuteen. Sen tavoitteena on edistää matkaviestintäverkkojen innovatiivista, monitoimittajien välistä, yhteensopivaa ja itsenäistä RAN-ekosysteemiä, jonka hyötynä olisivat alhaisemmat kustannukset, kehittynyt suorituskyky ja aiempaa joustavampi toiminta. O-RAN -arkkitehtuuri perustuu virtuaalisen radioverkon avoimien rajapintojen laitteistoille ja pilvelle, joka käyttää tekoälyä radioverkon ohjaukseen. O-RAN määritykset täydentävät 3GPP:n 4G- ja 5G-spesifikaatioita mahdollistaen valittujen RAN-rajapintojen yhteensopivuuden useiden toimittajien kesken.

Käytännössä O-RAN keskittyy laajentamaan 3GPP:n uuden radiorajapinnan (new radio, NR) option 7.2 jakomallia hajauttamalla tukiaseman toiminnot yksityiskohtaisemmin RU:n, CU:n ja DU:n välillä. Lisäksi O-RAN määrittelee liityntänän radioverkon älykkään ohjainyksikön (RAN Intelligent Controller, RIC) kanssa, joka kattaa toiminnot lähes reaaliaikaisen RIC-toiminnallisuuteen (near-real-time RIC, nRT-RIC) että ei-reaaliaikaisen RIC-toiminnallisuuteen (non-RT RIC), mukaan lukien niiden ohjaus- ja yhteysperiaatteet (control, policy).

Myös Telecom Infra Project (TIP) edistää osaltaan O-RAN-konseptia.[2] TIP on maailmanlaajuinen yhteisö yrityksiä ja organisaatioita, jotka kehittävät yhteensopivia infrastruktuuriratkaisuja. TIP:n tavoitteena on edistää globaalin internetin käytettävyyttä riittävällä laadulla sekä edistää kuluttaja- ja kaupallisia etuja sekä talouskasvua.



Kuva 1. Open RAN -verkkojen käyttöönottovaiheet. Korostetut viivat edustavat O-RAN:n määrittämiä avoimia rajapintoja.

TIP perustettiin vuonna 2016 helpottamaan yhteistyötä yritysten, kuten palveluntarjoajien, teknologiakumppaneiden ja järjestelmäintegraattoreiden kesken. Hanke kehittää ja ottaa käyttöön avoimia, hajautettuja ja standardipohjaisia ratkaisuja. TIP perustaa työnsä O-RAN Alliancen määrityksiin ja edistää O-RAN -hankkeita keskittyen testauksen näkökulmiin, ja mahdollistaa keskusteluja operaattoreiden, toimittajien ja järjestelmäintegraattoreiden kesken RAN -monitoimittajien yhteensopivien tuotteiden ja ratkaisuiden käyttöönottoon. TIP:n OpenRAN -ohjelma tukee hajautettujen ja yhteensopivien 2G, 3G, 4G ja 5G RAN -ratkaisujen kehittämistä palveluntarjoajien vaatimuksiin perustuen. TIP OpenRAN:n tavoitteena on siten mahdollistaa ekosysteemi seuraavan sukupolven RAN:n rakentamiseen yhteistyössä muiden alan organisaatioiden kanssa, mukaan lukien GSMA, ONF ja O-RAN Alliance.

Open Networking Foundation (ONF) osallistuu matkaverkkojen projekteihin ja luo avoimen lähdekoodin ratkaisuja nopeasti kehittyvällä mobiili-infrastruktuurialalla. Yksi ONF:n alueista on SD-RAN, joka täydentää O-RAN:n arkkitehtuurin ja rajapintojen määrityksiä rakentamalla ja kokeilemalla O-RAN -yhteensopivia avoimen lähdekoodin komponentteja matkapuhelinverkkoihin.[3]

ONF:n SD-RAN kehittää nRT-RIC:ia ja joukon esimerkkipohjaisia verkkosovelluksia (xApp) RAN:n hallintaan. Kyseinen RIC on pilvipohjainen ja perustuu useisiin ONF:n alustoihin, mukaan lukien ONOS SDN -ohjain. SD-RAN:n nRT-RIC:n arkkitehtuuri hyödyntää O-RANin arkkitehtuuria. SD-RAN seuraa myös O-RAN-määritysten kehitystä, ja SD-RAN-projekti luo uusia toiminnallisuuksia ja laajennuksia sekä keskustelee kokemuksistaan O-RAN Alliancen kanssa, mikä osaltaan auttaa edistämään O-RAN -määrityksiä.

Open RAN Policy Coalition on yritysten muodostama ryhmä, jonka tavoitteena on edistää käyttöperiaatteita liittyen avoimiin ja yhteensopiviin RAN-ratkaisuihin. Ryhmä edistää samalla kehittyneiden langattomien verkkojen, kuten 5G:n innovatiivisia ratkaisuja ja edistää kilpailua.[4].

Open RAN Alliancen verkkojen käyttöönotto

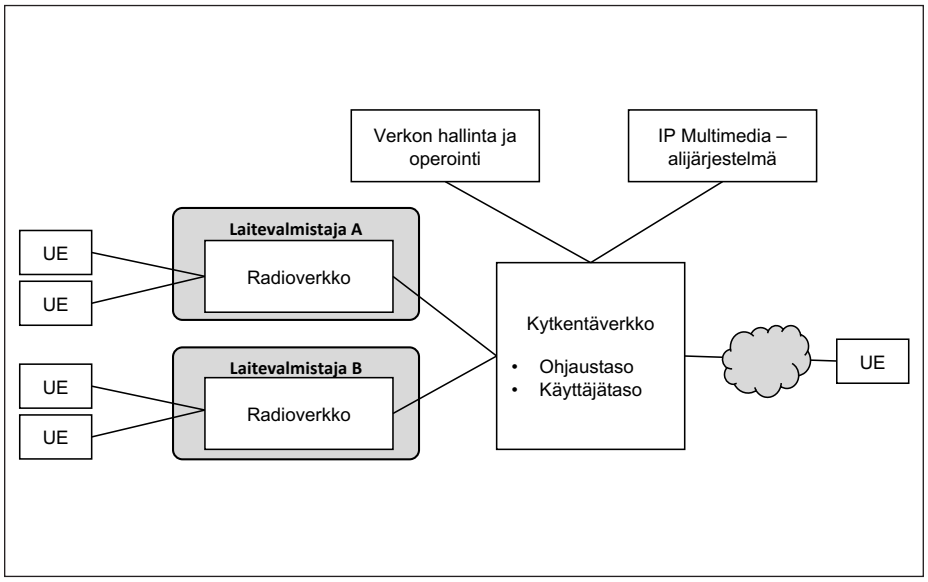
Open RAN Alliancen määrittämien verkkojen käyttöönotto voidaan esittää kuvan 1 vaiheiden kautta.[5] Kuvan termeistä FH (Fronthaul), eli ”etuyhteysväli” tarkoittaa verkon osiota tukiasemien ja tukiaseman radiosignaalien prosessointiyksikön (BBU, baseband unit) välillä, jonka rajapinta perustuu tyypillisesti Common Public Radio Interface (CPRI) -ratkaisuun, tai sen kehittyneeseen versioon evolved CPRI (eCPRI). BBU on puolestaan komponentti, joka huolehtii moduloimattoman (eli radiorajapinnan alkuperäisen) radiosignaalin välityksestä.

Käyttöönottovaiheiden keskeiset näkökohdat ovat seuraavat, perustuen lähteisiin [6] ja [7]:

Avoin FH (vaihe 1): Tässä mallissa tukiaseman BBU on yhdistetty RU:hun suljettuihin erillislaitteistoihin perustuen. Tämä vaihe tarjoaa avoimen rajapinnan RU:n ja DU:n välille ja kattaa FH:n rajapinnan, joka koskee RAN:n jako-optiota 7.2x. Avoimen FH:n käytännön toimintaan osallistuvien toimittajien on tuettava sitä RU:n ja DU:n välillä.

Avoin BBU (vaihe 2): Tässä mallissa RU on yhdistetty DU:hun, joka puolestaan on yhteydessä CU:hun kaupallisesti saatavilla oleviin laitteisiin (commercial off-the-shelf, COTS) perustuen. Tämä skenaario kuvaa askelta kohti avoimia rajapintoja ja laajentaa avoimen FH:n mallia avaamalla F1-rajapinnan DU:n ja CU:n välille 3GPP RAN -mallin korkeamman tason jakomallin mukaisesti. Jotta todellinen yhteensopivuus saavutettaisiin CU:n ja DU:n toimittajien kesken, niiden on tuettava avointa standardia. Tämä skenaario auttaa myös kehittämään aiemmin käytettyä erillislaitteiston lähestymistapaa sallimalla COTS:n käyttö DU:lle ja CU:lle.

Avoin, älykäs ja ohjelmoitava ympäristö (vaihe 3): Tässä mallissa RU on yhdistetty DU:hun, joka on puolestaan yhteydessä RIC:n, CU-CP:n ja CU-UP:n kanssa perustuen COTS- ja pilvilaitteistoon. Tämä skenaario laajentaa CU:n hajauttamista siten, että se jakautuu erillisiin käyttäjä- ja hallintatasoihin (UP ja CP). RIC on olennainen tässä skenaariossa, jotta siinä voidaan prosessoida reaaliaikaisia analyysejä, itseoptimointikonsepteja ja radioresurssien hallinnan sovelluksia siten, että CU ja RIC sijaitsevat fyysisesti reunapilvessä.



Kuva 2. Matkaviestinnän järjestelmätason arkkitehtuuri, joka sisältää päätelaitteen sekä radio- ja kytkentäverkon. Perinteisten radioverkkosegmenttien toteutus on ollut käytännössä mahdollista perustuen ainoastaan yksittäisiin laitevalmistajien komponentteihin, sillä niiden väliset rajapinnat ovat tyypillisesti laitevalmistajakohtaisia.

Avoimien hallintaliittymien kehittäminen kaikkien toimintaan osallistuvien komponenttien välillä on olennainen osa O-RAN-konseptia käytännössä. Kuvassa 1 esitettyjen rajapintojen lisäksi O-RAN:n FH:n hallintataso (management, M) yhdistää näin ollen O-RAN-yksiköt ja COTS-laitteiston (O-Cloud).

O-RAN -konsepti mahdollistaa uusien sidosryhmien liiketoiminnan siten, että kukin osapuoli voi kehittää tuotteita avoimien rajapintojen yhteensopivan merkinnannon ansiosta ja pohjautuen virtuaaliseen RAN-arkkitehtuurin.

Vaatimukset

Open RAN:n näkökulmina on mahdollistaa entistä laajempi toimijoiden kilpailu, edistää innovaatioita ja mahdollistaa uusia palvelumalleja. Open RAN pyrkii hyödyntämään keinoälytekniikoita mahdollistaakseen RAN:n uusia käyttökohteita (use case). Open RAN -konseptin konkretisoitumisen myötä uusia palveluita voidaan ottaa käyttöön aiempaa lyhyemmässä ajassa ja entistä kustannustehokkaammin.

Open RAN -konsepti perustuu neljään perustavaan periaatteeseen: avoimuus, virtualisointi, älykkyys ja ohjelmoitavuus.

Avoimuus: Open RAN -järjestelmän eri solmujen ja toimintojen välisten rajapintojen on oltava avoimia, jotta usean toimittajan toimintojen yhteensopivuus olisi käytännössä mahdollista. Tämä pätee niin toimintojen testaukseen kuin varsinaiseen verkkojen operointiin.

Virtualisointi: Ohjelmistoa pitää voida suorittaa pilvessä, ja sen sijaan, että operaattori käyttäisi tiettyjen verkkotoimittajien omia laitteistoja, Open RAN mahdollistaa toiminnot kaupallisesti saatavilla olevalla COTS-laitteistolla.

Älykkyys: RAN voi käyttää tekoälyä (AI) ja koneoppimista (ML), ja RAN:n optimointi voidaan suorittaa kolmannen osapuolen toimesta sen sijaan, että se rajoittuisi tiettyihin laite- tai verkkotoimittajien palveluihin.

Ohjelmoitavuus: RAN:n optimointi ja toiminta voidaan määrittää ja ottaa käyttöön tiettyjen käyttöönotto- ja suorituskykyvaatimusten mukaisesti sovellusohjelmointirajapintojen (application programming interface, API) avulla, jotka mahdollistavat operaattorin verkkojen ohjelmallisen määrityksen.

Arkkitehtuuri

Matkaviestintäjärjestelmä koostuu kolmesta pääkomponentista, jotka yhdessä mahdollistavat tietojen siirron kahden päätelaitteen välillä, joista ainakin toi-

nen käyttää langatonta teknologiaa osana viestintäreittiä. Kuva 2 selventää periaatetta.

Kuten kuvassa 2 esitetään, nämä kolme elementtiä ovat käyttäjälaitteet (user equipment, UE), radioverkko (radio access network, RAN) ja kytkentäverkko (core network, CN). Matkaviestintäjärjestelmä mahdollistaa sekä täysin itsenäisen viestinnän kahden saman matkaviestintäjärjestelmän UE:n välillä, että viestinnän UE:n ja ulkoisen verkon, kuten matkaviestintäverkon (public land mobile network, PLMN) tai ulkoisen dataverkon, kuten Internetin välillä.

Käyttäjälaitteet

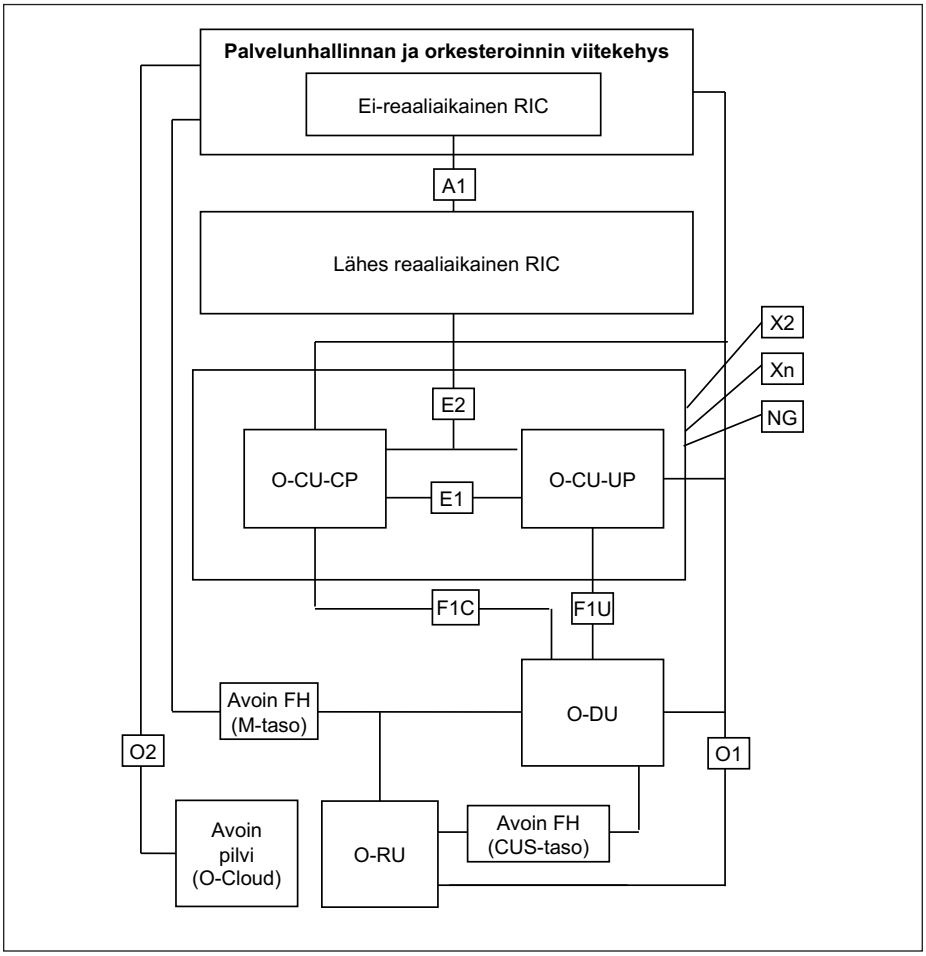
Alkuaikojen matkaviestintälaitteiden toiminnot rajoittuivat puhe-, teksti-, ja datapalveluihin. Sittemmin matkaviestinten tyyppejä on toteutettu monesta näkökulmasta, ml. perus- ja älypuhelimet, datapohjaiset, ja laitteiden väliseen ja esineiden Internetin liikennöintiin tarkoitetut mallit. Käyttäjälaitteita, jotka tukevat koneviestintää, ovat esimerkiksi anturit, teollisuusrobotit, lennokit ja autot.

Radiopääsyverkko

Matkajärjestelmän kahden päätelaitteen välinen langaton viestintä mahdollistetaan radioverkkojen avulla. Ne ovat vastuussa datan siirtämisestä radiotaajuuksilla mahdollistaen samalla käyttäjälaitteen tavoittamisen liikkuessaan.

Kytkentäverkko

Kytkentäverkko yhdistää radioverkon solmut keskenään ja vastaa viestinnän hallinnasta käyttäjälaitteen ja ulkoisten verkkojen, kuten Internetin, julkisen puhelinverkon tai toisen matkaviestinverkon välillä. Ydinverkon toiminnallisuus matkaviestinviestinnän järjestelmässä voidaan jakaa istunnonhallintaan ja liikkuvuuden hallintaan. Istunnonhallinta kattaa toiminnot, joilla pidetään käyttäjän tilaajatiedot ajan tasalla, jaetaan palvelun toimittamiseen tarvittavat resurssit, todennetaan käyttäjät, turvataan heidän viestintänsä ja kerätään tietoa laskutusta varten. Liikkuvuuden hallinta on joukko toimenpiteitä, jotka varmistavat, että käyttäjät pysyvät yhteydessä siirtyessään yhdestä RAN:n osasta toiseen. Ydinverkko on yhteydessä myös toiminta- ja ylläpitojärjestelmän (operations and administrations management, OAM) sekä mahdollisesti puhepalvelun mahdollistavan IP-multimediajärjestelmän (IP Multimedia Subsystem, IMS) kanssa.



Kuva 3. Open RAN Alliancen märittämä Open RAN -arkkitehtuuri.

RAN-komponentit

RAN koostuu joukosta solmuja eli tukiasemia. 5G:ssä niiden termi on gNodeB, ja 4G:ssä eNodeB. Ne ovat järjestelmiä, jotka lähettävät ja vastaanottavat radiosignaaleja valituilla taajuusalueilla. Toisin kuin aiemmissa sukupolvissa, neljännen ja viidennen sukupolven solmut voivat olla yhteydessä kytkentäverkon lisäksi myös suoraan toistensa kanssa standardoidulla liitännällä.

Tukiasemat koostuvat antennijärjestelmästä (ml. masto, antennit ja kauko-ohjattava radiomoduuli, radio remote head, RRH), sekä kantataajuusyksiköstä (baseband unit, BBU).

RRH vastaa radioaalloilta antennijärjestelmän kautta lähetetyistä tai vastaanotetuista radiosignaaleista. Uplink-suunnassa eli tukiaseman vastaanotettujen radiosignaalien osalta radiolaitteen rooli on muuntaa analogiset signaalit muotoon, joka voidaan käsitellä digitaalisen signaalinkäsittelyn tekniikoilla. Downlink-suunnassa eli tukiasemalta lähetettävien radiosignaalien osalta radiolaitteen tehtävänä on muuntaa digitaalinen signaali antennijärjestelmälle sopivaksi analogiseksi syötteeksi.

BBU:n tehtävänä on valmistella verkon lähettämä datavirta alalinkin suuntaan ja muuntaa ilmateitse vastaanotetut ja RRH:n digitoimat radiosignaalit sopivaksi datavirraksi. Yhteyttä BBU:n ja kytkentäverkon välillä kutsutaan termillä backend (”takaliikenne”), kun taas BBU:n ja radioliitäntäyksikön välistä rajapintaa kutsutaan termillä frontend (”etuliikenne”).

Open RAN -konseptin arkkitehtuuri

Avoimen radioverkon konsepti liittyy nimenomaan radioverkkosegmenttiin, optimoiden niiden toimintaa määrittämällä sen sisäisten rajapintojen toimintaa eriyttämällä eri protokollatasojen toimintoja fyysisesti, ja määrittämällä niiden väliset rajapinnat yhteismitallisiksi.

Kuva 3 esittää O-RAN -arkkitehtuurin periaatteen. On huomattavaa, että Open RAN -arkkitehtuurissa on monia 3GPP:n vuosijulkaisun 15 mukaisia komponentteja ja rajapintoja. Itse asiassa O-RAN -arkkitehtuurin perusta on kyseisen 3GPP-julkaisun jakomalli, ja kuvasta on siten mahdollista tunnistaa 5G-tukiaseman (gNodeB) kolme tuttua elementtiä: CU, DU ja RU.

Koska O-RAN Alliancella on tarkempi määritelmä siitä, mihin komponenttiin kukin radioverkon toiminnallisuus kuuluu, O-RAN on nimittänyt komponentit uudelleen muotoon O-CU, O-DU ja O-RU, joista kirjain O kuvastaa avoimuutta (open). O-RAN Alliance on myös lisännyt uusia verkkoelementtejä ja liittymiä RAN-arkkitehtuuriinsa, joilla ei ole vastinetta 3GPP:ssä.

Turvallisuusnäkökohdat

O-RAN-konsepti mahdollistaa uusien toimijoiden verkkoon liittymisen sen palvelujen tarjoamiseen. Konsepti on melko uusi, joten vaikka hyvänä aikomuksena on laajentaa RAN-ekosysteemiä, sillä voi olla myös haittavaikutuksia turvallisuuden näkökulmasta. Periaatteessa laajennettu avoimuus voi myös avata uusia hyökkäysvektoreita, joita ei ole tunnettu aiemmin.

Open RAN -verkkoihin liittyvät monet samankaltaiset turvallisuusriskit, jotka on tunnettu aikaisemmissa verkoissa. Näiden yleisten turvallisuusriskien lisäksi Open RAN:n käyttöönoton myötä voi ilmetä myös täysin uusia tai korostuneempia riskejä. Nämä haavoittuvuudet voivat liittyä esimerkiksi tekoälyn (AI) ja koneoppimisen (ML) sekä pilviturvallisuusriskien osalta.

O-RAN:n työryhmän 11 tekniset määritykset esittävät turvallisuusvaatimuksia osana näiden uusien riskien lieventämistä. Silti O-RAN:n kehityksessä on järkevää toteuttaa jatkuvaa seurantaa, ja uusista haavoittuvuuksista tiedottaminen sidosryhmien kesken voi myös olla avainasemassa verkkojen turvaamisessa.

Kuten lähteessä [12] todetaan, operaattorit tekevät yhteistyötä kansallisten viranomaisten kanssa jakamalla tietoa Open RAN:n turvallisuudesta, toteutuksesta ja hallinnasta. Tekniikan kehittyessä operaattorit ovat myös pyytäneet sisällyttämään Open RAN:n osaksi GSMA:n Security Assurance Scheme (NESAS) -ohjelmaa sekä Euroopan unionin kyberturvallisuusviraston (ENISA) sertifiointiohjelmaa. Lähde [12] osoittaa myös esimerkiksi, että Deutsche Telekom, Orange, TIM, Telefónica ja Vodafone ovat sitoutuneet soveltamaan O-RAN Alliancen ja 3GPP:n turvallisuusmäärityksissä määriteltyjä pakollisia ohjausmekanismeja, mukaan lukien toimitusketjun hallinta.

Tässä ympäristössä avainasemassa olisi, että ekosysteemi soveltaa nollaluotettavuuden (zero trust) lähestymistapaa siten, että kaikki asiaankuuluvat toimittajat sitoutuvat standardien ja O-RAN Alliancen määrityksiin. On myös tärkeää sisällyttää turvallisuusnäkökohtiin kansallisten viranomaisten vaatimukset, jotta toimittajien riskiprofiilit voidaan arvioida asianmukaisesti.

On huomattavaa, että esimerkiksi Telecom Infra Projectin resurssit eivät keskity turvallisuusnäkökohtiin, vaan viittaavat O-RAN Alliancen turvallisuusspesifikaatioihin. O-RAN Alliancen tietoturvallisuusryhmä Security Work Group (WG11) on siten avainasemassa. Se on julkaissut maaliskuussa 2023 turvallisuuden hallintamekanismit valituille rajapinnoille.

O-RAN:n tietoturvallisuusmääritykset

Open RAN:n turvallisuus on äärimmäisen tärkeää maailmanlaajuisesti ja ekosysteemin sidosryhmille. Riittävän turvallisuustason periaatteen tulisi soveltua Open RAN -järjestelmiin jo ennen kaupallisen käyttöönoton alkamista. O-RAN Alliancen Security Focus Group (SFG) määrittelee turvallisuusarkkitehtuurin tavoitteenaan helpottaa yhteisten turvallisuusstandardien soveltuvuutta O-RAN-järjestelmiin.

Käytännön käyttötapauskohtaiset skenaariot on otettava huomioon mahdollisten uhkien kannalta. On ilmeistä, että radioyksiköiden ja taajuusalueiden portfolio voi vaihdella verkkojen välillä, mutta 4G- ja 5G-suunnitteluperiaatteet ovat edelleen yhtä sovellettavissa. Lisäksi on otettava huomioon verkkojen yhteentoiminnot 2G- ja/tai 3G-verkkolaitteiden kanssa, mukaan lukien turvallisuusohjaukset uhkien torjumiseksi vanhemmissa tekniikoissa.

O-RAN Alliancen mukaan RAN-järjestelmien hyökkäyspinta laajenee avoimien ja pilvipohjaisten arkkitehtuurien käytön seurauksena. Samanaikaisesti käytettyjen avointen rajapintojen avoimuuden ansiosta mahdollisten haavoittuvuuksien ja vikojen seuranta tulee helpommaksi.

Tämä avoin ympäristö on hyödyllinen myös kilpailun lisääntymisen muodossa, kun erilaiset O-RAN-laitteiden ja ratkaisujen toimittajat voivat tarjota ja toteuttaa vahvistetun turvallisuuden, jotta operaattorit voivat arvioida ja valita heidän vaatimuksiinsa parhaiten soveltuvat. EU:n 5G Toolbox tuo lisäapua turvallisuussuositusten huomioimiseksi.[13]

O-RAN Alliancen SFG tarkastelee Open RAN -järjestelmän riskejä ISO 27005 riskianalyysimenetelmän perusteella ja soveltaa Zero-Trust-arkkitehtuuria National Institute of Standards and Technologyn (NIST) periaatteiden mukaisesti. [14] O-RAN Alliance julkaisi alustavat tietoturvallisuuden testispesifikaatiot maaliskuussa 2022.

SFG-työ konkretisoituu neljään turvallisuusmääritykseen. Nämä toimivat rakennuspalikoina O-RAN-turvallisuusarkkitehtuurissa. Alkuperäiset SFG-määritykset ovat peräisin vuodelta 2021 ja ne ovat saatavilla O-RAN Alliancen verkkosivustolla osoitteessa https://www.o-ran.org/specifications.

O-RAN Alliancen turvallisuuteen liittyvät dokumentit sisältävät esimerkiksi seuraavat aiheet:

1) O-RAN turvallisuusvaatimukset ja turvallisuusprotokollamääritykset.

2) O-RAN turvallisuusuhkamallinnus ja korjaustoimenpiteiden analyysi.

3) Tutkimus avoimen pilven turvallisuudesta ja turvallisuudesta sovelluksen

elinkaaren hallintaan, turvallisuudesta tietuehallintaan ja turvallisuudesta palvelunhallintaan ja orkestrointiin ja turvallisuudesta jaetulle O-RU:lle.

4) Tutkimus turvallisuudesta kattaen lähellä reaaliaikaista olevaa ja ei-reaaliaikaista RIC:ä sekä xApp:it.

5) O-RAN turvallisuustestimäärityksset.

Päätelmät

Avoimen radioverkon konsepti on jo pitkälle kehittynyt, ja esimerkiksi Open RAN Alliancen määrittelyt kattavat järjestelmän käyttöönottoon tarvittavat näkökohdat jo varsin yksityiskohtaisesti. Avoimien radioverkkojen laajamittainen rakennus on kuitenkin vielä käytännössä jokseenkin alkuvaiheessa.

Avoimen radioverkon hyötynä on aiempaa parempi radioverkkojen sisäisten rajapintojen yhteensopivuus eri toimijoiden kesken, mikä voi laajentaa merkittävästi uusien ja jo markkinoilla olevien ratkaisutarjoajien tuotevalikoimaa. Operaattoreilla on siten mahdollisuus sisällyttää useita radioverkkokomponenttien toimittajia samaan radioverkkosegmenttiin, millä voi olla positiivinen vaikutus myös verkon rakennus- ja operointikustannuksiin.

Avoimen radioverkkokonseptin myötä avautuu samalla erityisen mielenkiintoinen mahdollisuus toteuttaa eräänlaisia kevyitä verkkoja nopeassa aikataulussa tukeutuen perustoimintoihin, useiden komponenttivalmistajien ratkaisuihin, verkkotoimintojen prosessointiin pilvipalveluissa sekä COTS-komponentteihin. Tällainen perusverkko voi olla hyödyksi esimerkiksi pienten operaattoreiden suoraviivaisessa 5G-palvelualueiden laajennuksessa samoin kuin maanpuolustuksen tarpeisiin dynaamisesti muuttuvissa kenttäolosuhteissa.

Haittapuolena, avoimen radioverkkokonseptin myötä saattaa avautua myös täysin uusia, vielä tuntemattomia hyökkäysvektoreita. Ekosysteemin on järkevää varautua niihin laajentamalla yhteistyötä tutkimuksen ja kehityksen kautta sekö jakamalla tietoa luotettavien foorumeiden kautta todetuista riskeistä ja niiden torjuntamenetelmistä.

Lähteet

[1] Open RAN Alliance, “Open RAN Alliance”. https://www.o-ran.org/

[2] Telecom Infra Project, “Telecom Infra Project: Who we are”: https://telecominfraproject.com/who-we-are/

[3] Open Networking Foundation, “ONF Mission”: https://opennetworking.org/

[4] Open RAN Policy Coalition, “Mission”: https://www.openranpolicy.org/

[5] O-RAN Alliance, “O-RAN specifications”: https://www.o-ran.org/specifications

[6] NTT DOCOMO, “5G Open RAN Ecosystem Whitepaper” 2021.

[11] Techplayon, “Open RAN (O-RAN) Reference Architecture”. Techplayon, 28.10. 2018. http://www.techplayon.com/open-ran-o-ran-reference-architecture/

[12] Open RAN Policy Coalition, “Open RAN security in 5G”. Open RAN Policy Coalition, 2021. https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf.

[13] EU, “EU-wide coordinated risk assessment of 5G networks security”. European Union, 19.10.2019. https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[14] Federal Office for Information Security (BSI), “Open RAN Risk Analysis”. Federal Office for Information Security (BSI), 21.2. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf?__blob=publicationFile&v=7.

Artikkelin kirjoittaja

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

Lisätietoa artikkelissa esitetystä pian julkaistavasta Open RAN Explained -kirjasta löytyy osoitteesta: https://www.amazon.com/-/es/Jyrki-T-J-Penttinen/dp/1119847044

TEKSTI: SAMI BORÉN

Henkilökohtainen hyökkäyspinta-ala on koko organisaation riski

Miksi olisit kyberrikollisille kiinnostava kohde? Mitä tietoa sinusta tai läheisistäsi näkyy verkossa ulospäin, ja miksi sillä on merkitystä? Kyberrikolliset käyttävät pitkälle vietyjä taktiikoita, kun he pyrkivät pääsemään kiinni arvokkaaseen tietoon. Vaakalaudalla voi olla yritys- ja jopa valtiotason data.

Artikkeli päättää sarjan, jossa tarkastellaan tietoturvaa moderneissa IT-ympäristöissä. Tämä osa keskittyy kyberrikollisten vaikuttamiskeinoihin organisaatioissa ja niiden palveluketjuissa. Sarjan aiemmissa osissa näkökulmina ovat olleet tekoälyn mahdollisuudet turvallisuuskriittisissä ympäristöissä sekä tietoturva tämän päivän tietoliikenneverkoissa.

Kyberrikollisuuden uhkamaisema on muuttunut merkittävästi pelkästään viime vuoden aikana, ja muutos on nopeaa. Ala on ammattimaistunut selvästi. Jos ennen puhuttiin yksittäisistä, pahantahtoisista hakkereista tai hakkeriryhmistä, muistuttaa rikollisten järjestäytymisen tapa nyt mitä tahansa yritystoimintaa.

Kilpajuoksu hyvän ja pahan välillä on kovaa. Tietoturvan vahvistaminen edellyttää teknologioita ja reaaliaikaista valvontaa, mutta ne eivät yksin riitä muodostamaan aukotonta suojaa. Siksi on olennaista ymmärtää, millaisia riskejä liittyy tietoon, jota itse annamme itsestämme tai organisaatioistamme ulospäin, tiedostamatta tai tarkoituksella.

Palveluihin erikoistuneita ammattirikollisia

Moni tämän päivän kyberrikollisista toimii palveluntuottajina. Heillä ei ole välttämättä omaa intressiä aiheuttaa haittaa kohteelle, vaan hyökkäyksiä tehtaillaan laittomana liiketoimintana.

Osa toteuttaa tilauksesta "*Ransomware as a Service*" -palveluita, eli myy kenelle tahansa kiinnostuneelle palvelua, jossa kohteen järjestelmiin asennetaan dataa kaappaavia tai kryptaavia kiristyshaittaohjelmia. Palvelumalli tekee tietoturvarikosten toteuttamisesta huomattavan helppoa. Ransomwaren lisääntyminen näkyykin tilastoissa.

Osa kyberrikollisista keskittyy hankkimaan pääsytietoja, kuten käyttäjätunnuksia ja salasanoja, ja myy niitä sen jälkeen eteenpäin (*initial access brokers*).

Osa hakkereista on erikoistunut tekoälyn hyödyntämiseen ja deepfake-palveluihin. Kyberhyökkäystä suunnitteleva voi ostaa palveluna esimerkiksi uskottavan oloisia keskusteluja käyvän AI-botin, joka vakuuttaa kohdehenkilön niin, että tämä päätyy klikkaamaan haitallista linkkiä. Keinotekoisilla, todellista henkilöä muistuttavilla videoilla on äänessä esimerkiksi yrityksen "toimitusjohtaja", joka antaa valheellisia "ohjeita" alaisilleen.

Maailmassa, jossa tietoturvahyökkäyksen voi ostaa helposti palveluna, ei haitan aiheuttamiseen tarvita enää omaa, pitkälle vietyä tietoteknistä osaamista. Riittää, että palvelun ostajalla on motiivi päästä kiinni kohdeorganisaation dataan.

Datan kaappaamiseen ja kiristämiseen tähtäävät hyökkäykset yleistyneet erittäin jyrkästi

Globaalit uhkatiedusteluraportit kertovat, että vuonna 2023 ransomware- eli kiristyshaittaohjelmiin liittyvien hyökkäysten määrä kasvoi jopa 55,5 % edelliseen vuoteen verrattuna.

Ennätysmäinen kasvu yllätti kokeneetkin tietoturva-asiantuntijat, mutta kehityskululle on selitys. Kuten edellä kuvattiin, ransomware-hyökkäyksiä on yhtäkkiä helppo hankkia palveluna, ja se on suhteellisen edullista.

Haitan aiheuttamisen takana voi olla useita erilaisia motiiveja. Jos kiristäjä saa haltuunsa suuria määriä liiketoimintakriittistä dataa, lunnaat voivat tuoda rikolliselle suuria taloudellisia voittoja.

Toinen motiivi liittyy poliittisiin tai eettisiin mielenilmauksiin. Aktivisteista tulee hacktivisteja. Jos aktivistiryhmä kokoontui aiemmin yrityksen pääkonttorille osoittamaan mieltä, nyt viestin tehostamiseksi saatetaan ostaa digitaalinen hyökkäys yritystä kohtaan. Tämän tyyppisten hyökkäysten arvioidaan lisääntyvän tulevaisuudessa.

Oma lukunsa on valtiollinen vaikuttaminen ja kybervakoilu. Suomessa seurataan tällä hetkellä tarkasti varsinkin Venäjän hallintoon yhdistettyjä uhkatoimijoita, mutta merkittäviä ryhmiä liittyy myös muun muassa Kiinan ja Pohjois-Korean hallintoihin.

Vuonna 2023 Venäjän valtioon kytkeytyvä hakkeriryhmä APT29 lähetti Ukrainassa

toimiville diplomaateille BMW-autojen myynti-ilmoitukseksi naamioituja viestejä. Ilmoituksen sisältämän linkin klikkaaminen johti haittaohjelman latautumiseen. Ilmoitukset olivat samankaltaisia, joita autoaan myyvä puolalainen diplomaatti oli lähettänyt kollegoilleen muutamaa viikkoa aiemmin. Hyökkäys kohdistui ainakin 22 lähetystöön Kiovassa. Niissä työskenteli muun muassa Yhdysvaltojen, Kanadan, Turkin, Alankomaiden, Tanskan ja Viron valtioiden diplomaatteja. Lähde: Unit 42

Maailman valtioiden välillä on jonkin verran eroja kyberrikollisten kyvykkyydessä. Yleisesti ottaen voi kuitenkin todeta, että osaavia ammattilaisia on tällä hetkellä joka mantereella. Esimerkiksi Etelä-Amerikasta käsin tehdään tällä hetkellä paljon hyökkäyksiä. Osa hakkereista määrätään tehtäviin valtiolliselta taholta, toisia taas saattaa houkutella rikolliselle uralle yksinkertaisesti lupaus paremmasta elintasosta.

Tietojenkalastelun kohdehenkilöt ovat tarkasti valikoituja

Ransomware-hyökkäyksissä rikollisen tavoitteena on tietyn organisaation datan haltuun saaminen. Joko dataa on tarkoitus varastaa omiin tarkoituksiin tai kiristystä varten, tai se halutaan kryptata käyttökelvottomaksi haitantekomielessä.

Kiristyshaittaohjelman asentamiseen ei aina tarvita teknologista haavoittuvuutta, jonka kautta järjestelmiin ujuttauduttaisiin luvatta. Sen sijaan yleinen taktiikka on kalastella pääsytietoja organisaation avainhenkilöiltä.

Tarkkaan kohdennetuissa phishing-hyökkäyksissä, joissa on tarkoitus saada haltuun tietyn organisaation dataa, myös kohdehenkilöt on usein valikoitu hyvin tarkasti.

Mikä sitten tekee yksittäisestä henkilöstä mielenkiintoisen kohteen? Kiinnostavia avainhenkilöitä on rikollisten silmissä paljon:

C-level- eli johtoryhmätason päättäjillä on laajasti valtaa. Finanssiosaston takana on organisaation rahaliikenne. Erikoisalueiden asiantuntijoilla on hallussaan kriittisen tärkeää tietoa. IT-vastuuhenkilöillä on laajat pääsyoikeudet järjestelmiin.

Venäjänkielinen ransomware-ryhmä BlackCat/ALPHV ilmoitti joulukuussa 2023 kohdistaneensa kyberhyökkäyksen yhdysvaltalaiseen Ultra Intelligence and Communicationsiin. Kyseessä on yksityinen kyberturva-alan yritys – ei suoraan valtiollinen taho – mutta sen asiakaskuntaan kuuluu valtion virastoja ja muita Yhdysvaltain kriittisen infrastruktuurin kannalta tärkeitä toimijoita. Ultra Intelligence and Communicationsin kaltaisille organisaatioille on tärkeää varautua hyökkäyksiin ennalta niin, että haitat jäävät mahdollisimman pieniksi. Lähde: The Cyber Express

Suomessa ollaan vielä melko sinisilmäisiä riskien suhteen sekä organisaatioiden että yksilöiden tasolla. Moni ei pidä omaa henkilökohtaista hyökkäyspinta-alaansa (*attack surface*) riittävän kiinnostavana, eikä tunnista, mitä kaikkea kriittistä tietoa oman työroolin hoitamiseen liittyy.

Organisaation datan ajatellaan olevan turvassa Suomen syrjäisen sijainnin vuoksi tai siksi, että muita, houkuttelevampia kohteita hakkereille kyllä riittää. Mediapuhe huoltovarmuuden kannalta keskeisten alojen kriittisestä infrastruktuurista voi johtaa harhaan, jos se yksinkertaistuu mielikuvissa vain energiasektorin tai maanpuolustuksen asiaksi. Oman liiketoimintadatan arvoa ei usein nähdä samoin.

Näitä ajatuksia pitäisi kyseenalaistaa vahvasti. “Kriittisyys” on aina suhteellinen termi. Lähtökohtaisesti kaikki suojausten ja salasanojen taakse suljettu infra ja data on kriittistä millä tahansa toimialalla. Omalla datalla on merkitystä niin yhden hengen mikroyritykselle kuin suurille valtakunnallisille tai globaaleille toimijoille. Pahimmassa tapauksessa vakava ransomware-hyökkäys riittää kaatamaan koko liiketoiminnan ja vaikuttaa myös toimitusketjun muihin osiin.

Rikollisten on helppo löytää henkilökohtaisia tietoja kohteen vakuuttamiseen

Usein ihmiselle tulee yllätyksenä, miten paljon hänestä löytyy tietoa, jonka rikolliset voivat kääntää hyödykseen. Huomaamme tämän, kun teemme hyökkäyspinta-alan kartoituksia yritysten avainhenkilöistä. Tulokset saattavat säikäyttää sellaisenkin henkilön, joka käyttää esimerkiksi sosiaalista mediaa vapaa-ajallaan hyvin rajatusti, tai ajattelee piiloutuneensa anonyymien nimimerkkien taakse.

Huijaukseen haksahtamisen perusidea on yksinkertainen: rikollinen on pystynyt tekemään valesivustosta tai tietopyynnöstä riittävän uskottavan. Se onnistuu vain, jos hyökkääjä arvaa riittävän oikein, millaisilta sidosryhmiltä – kuten tuttavilta tai tavarantoimittajilta – kohdehenkilö saattaisi samaan aikaan saada yhteydenottoja töissä tai vapaa-ajalla.

Jo pelkkä LinkedIn-tili antaa uhkatoimijoille paljon informaatiota, kuten nimiä lähipiiristä ja linkityksiä muihin sosiaalisen median palveluihin. Johtolankojen kautta voi edelleen selvittää, millä alueella kohdehenkilö tai hänen puolisonsa ulkoilevat vapaa-ajallaan ja mitä heidän lapsensa harrastavat. Julkisista rekistereistä saattaa löytyä tieto esimerkiksi taloyhtiön hallitukseen kuulumisesta.

Sosiaalisessa mediassa kiertää tälläkin hetkellä haasteita, joissa kysytään ikää, lemmikin nimeä, syntymävuotta ja monenlaisia mieltymyksiä. Viranomaiset varoittavat näihin osallistumisesta painokkaasti. Jos haluaa pienentää henkilökohtaista hyökkäyspinta-alaansa eli ulospäin näkyvien tietojen määrää, ei riitä, että ohittaa itse tällaiset haastesisällöt. Perheenjäsenet, ystävät tai muut läheiset saattavat kertoa erehdyksessä auliisti tietoja, jotka kertovat myös kyberrikollisten tähtäimessä olevasta avainhenkilöstä.

Kerättyjen tietojen perusteella rikolliset voivat lähettää vastaanottajalle uskottavia, oikean näköisillä tiedoilla täydennettyjä linkkejä vaikkapa “urheiluseuran ilmoittautumisjärjestelmään” tai “taloyhtiön asiakirjojen hoitamiseen”. Mitä luotettavammalta yhteydenottaja tuntuu, sitä helpommin pienet kömpelyydet linkin URL-kentässä tai kirjoitusasussa jäävät huomaamatta.

Henkilökohtainen hyökkäyspinta-ala tarkoittaa kaikkea sitä, mikä yksilöstä näkyy ulospäin avoimesti verkossa. Pinta-alaa

ei voi kutistaa olemattomiin, mutta sen laajuudesta ja siihen liittyvistä riskeistä on hyvä olla tietoinen. Silloin yhteydenottoihin osaa suhtautua suuremmalla varauksella.

Vastaavasti organisaation hyökkäyspinta-ala tarkoittaa kaikkea organisaatiosta julkisesti saatavilla olevaa tietoa. Näitä kahta ei voi tämän päivän maailmassa erottaa toisistaan. Yksi väärä klikkaus riittää avaamaan aukon, jolla ransomware-ohjelmaa levittävä rikollinen voi päästä kiinni yhteisiin järjestelmiin.

Yleisiä väärinkäsityksiä, jotka luovat valheellista turvallisuuden tunnetta:

"Ei minun takanani ole kriittistä dataa." Oman organisaatiosi toiminnan jatkuvuuden kannalta takanasi oleva data on aina kriittistä. Saatat olla myös osa huoltovarmuuden kannalta kriittisiä palveluketjuja.

"Olen todella varovainen, enkä kerro vapaa-ajastani mitään somessa." Rikolliset löytävät onnistuneen phishing-kampanjan taustatiedoksi yllättävän paljon materiaalia pelkästään julkisista lähteistä tai LinkedIn-profiilista. He kykenevät yhdistämään kokonaiskuvaansa myös tietoja, joita läheisesi jakavat verkossa itsestään.

"Meillä on käytössä markkinoiden parhaat antivirustyökalut ja palomuurit." Aina työkaluja ei ole konfiguroitu toimimaan organisaatiota parhaiten palvelevalla tavalla. Ne eivät esimerkiksi kerää lokitietoja.

"Olemme iso organisaatio, joten järjestelmämme ovat hyvin suojattuja." Pienemmissä organisaatioissa suojautumisen taso saattaa olla jopa parempi kuin suurissa, joissa käytössä on paljon legacy-teknologiaa. Vuosien varrella kyberuhkiin varautumiseksi on jouduttu rakentamaan vippaskonsteja, jotka saattavat avata hyökkäyspinta-alaa näkyviin yllättävistä paikoista.

"Meillä on käytössä SOC-palvelu eli kyberturvallisuutta valvotaan reaaliaikaisesti." Kiristyshaittaohjelmia asentavat rikolliset toimivat entistä nopeammin. Aiemmin järjestelmissä saatettiin lymyillä hetki ennen ohjelman asentamista, nyt data pyritään kryptaamaan tai kaappaamaan mahdollisimman nopeasti. Reaaliaikaisen valvonnan lisäksi tarvitaan uhkien kartoittamista ja proaktiivista ennakointia.

"Omat ympäristömme on auditoitu perusteellisesti, ja satsaamme paljon tietoturvaan sekä henkilöstön kouluttamiseen." Palveluketjuhyökkäysten yleistyminen lisää painetta kyberturvan ennakoivaan vahvistamiseen koko toimittajaverkoston kanssa.

Riski ei tarkoita samaa kuin haavoittuvuus

Organisaation hyökkäyspinta-ala kattaa yksilön pinta-alan tavoin kaikki asiat, jotka ovat ulospäin näkyviä ja kenen tahansa löydettävissä. Ne voivat olla ip-osoitteita, avoimia portteja tai kirjautumisikkunoita.

Osa näistä on tietoisesti julkisessa verkossa näkyviä, mutta osan pitäisi olla salattuja ja näkyvissä ainoastaan tietyille käyttäjille yrityksen omassa verkossa. Ennakoivassa hyökkäyspinta-alan monitoroinnissa huomataan, jos tällaisia tietoja on epähuomiossa jäänyt näkyviin.

Tässä kohtaa on tärkeää huomata, että kyse ei ole välttämättä haavoittuvuudesta. Sovellukset ja laitteet voivat olla päivitysten puolesta kunnossa, eikä rikollinen löydä takaportteja tietomurron tekoon. Siitä huolimatta puhutaan hyökkäyspinta-alaa kasvattavista riskeistä.

Esimerkki riskistä, joka ei ole haavoittuvuus: Pilvisiirtymähankkeessa siirretään olemassaolevia resursseja on-premises -palvelimilta pilveen. Konfigurointivirheen vuoksi intranetin kirjautumisikkuna on jäänyt näkyviin julkiseen internetiin, vaikka sen olisi tarkoitus näkyä vain yrityksen lähiverkossa toimiville. Jos rikolliset paikantavat tällaisen kirjautumisikkunan, he pystyvät ostamaan verkosta kalasteltuja käyttäjätunnuksia ja pommittamaan kirjautumisikkunaa näillä.

Haavoittuvuuksien seuraaminen on todella tärkeää, kun halutaan suojata yritysten ja yhteiskunnan kannalta kriittistä dataa ja infrastruktuuria. Riittää, että yksinkertaisista tietoliikennelaitteista löytyy heikko kohta, ja kriittiset järjestelmät ovat vaarassa. Näin tapahtui esimerkiksi Tanskassa vuonna 2023, kun kaikkiaan 22 energiayhtiötä joutui hakkeriryhmän hyökkäyksen kohteeksi palomuureista löytyneen haavoittuvuuden vuoksi (lähde: The Record).

Lisäksi tarvitaan kuitenkin jatkuvaa hyökkäyspinta-alan monitorointia. Näin pystytään puuttumaan hyvissä ajoin myös riskeihin, jotka eivät johdu suoraan haavoittuvuuksista.

Palveluketjuissa mahdollisuuksia useille eri hyökkäystyypeille

Palveluketjuhyökkäys on kyberhyökkäyksen muoto, jossa rikollinen yrittää päästä kohdeorganisaation dataan kiinni kumppanien, kuten tavarantoimittajien, verkoston kautta.

Tämän riskin tunnistaminen on erityisen tärkeää huoltovarmuuskriittisen tai kansallisen turvallisuuden parissa työskenteleville tahoille, kuten maanpuolustusorganisaatioille. Talon omat asiantuntijat saattavat olla tietoturva-asioissa erittäin valveutuneita, mutta satojen tai jopa tuhansien sidosryhmien verkostoa on vaikeampaa kontrolloida.

Palveluketjuihin kohdistuvat hyökkäykset voidaan jakaa kolmeen tyyppiin:

1) Rikollinen uhkatoimija varastaa toimittajalta dataa, jonka avulla on mahdollista räätälöidä entistä vaarallisempi hyökkäys alkuperäistä kohdeorganisaatiota vastaan. Esimerkiksi insinööritoimistolta varastetaan suunnitelmia, jotka on tehty puolustushallinnon tilauksesta.

2) Uhkatoimija hyödyntää kohdeorganisaation ja tämän toimittajakumppanin välistä, luotettavana pidettyä kanavaa sivusuuntaisesti.

3) Uhkatoimija löytää toimittajaketjun asiointikanavista tai integraatioista haavoittuvuuden tai riskialttiin kohdan, ja hyökkää kohdeorganisaation järjestelmiin sen kautta (ns. *watering hole attack*). Ilman riittäviä suojauksia ulkopuolinen, pahantahtoinen toimija voi esimerkiksi identifioida halutun organisaation liikenteen IP-osoitteiden mukaan ja kerätä tietoa kohdeorganisaation toiminnasta ja tätä kautta on myös mahdollista tarjota saastutettuja tiedostoja kohdeorganisaatiolle.

Vuonna 2023 suuri insinööritoimisto Black&McDonald joutui ransomware-hyökkäyksen kohteeksi. Yritys on toiminut sopimuskumppanina sekä Kanadan puolustusvoimille että kriittisen infrastruktuurin liikenne- ja energiayhtiöille Torontossa ja Ontariossa. Hyökkääjä ei päässyt käsiksi Kanadan puolustusvoimien järjestelmiin, mutta Black&McDonaldin asiakasprojekteja ja niihin liittyviä suunnitelmia voi hyvällä syyllä pitää itsessään kriittisen tärkeänä datana, joka ei saisi vuotaa rikollisille. (Lähde: The Record)

Kyberrikollisten teknologiat ja taktiikat kehittyvät ripeästi. EU:n NIS2-direktiivi edellyttää, että tietyt, huoltovarmuuden kannalta kriittiset organisaatiot ovat entistä paremmin perillä toimitusketjujensa kyberturvallisuudesta. Paine toimitusketjujen tietoturvan entistä huolellisempaan auditointiin kasvaa useista suunnista yhtä aikaa.

Rikolliset toimivat nopeammin kuin ennen

Aika, jonka uhkatoimijat viettävät kohdeympäristöissään, on lyhentynyt selvästi. Aiemmin rikolliset lymyilivät järjestelmissä tyypillisesti jonkin aikaa ennen kuin asensivat ransomware-ohjelman ja kaappasivat tai kryptasivat datan. Nyt tämä *"dwell time"* on pienentynyt merkittävästi.

Kriittisenä pidetyn infrastruktuurin ja datan suojaamiseen käytetään usein SOC-palvelua (*Security Operations Center*), jonka toimintaperiaate on perinteisesti tämä: IT-ympäristöjä seurataan reaaliajassa, ja havaittuihin poikkeamiin ja haitantekoon isketään nopeasti vastatoimilla. Mutta sitä mukaa kun rikollisten kohdeympäristöissä viettämä aika lyhenee, tulee proaktiivisista palveluista ja poikkeamien ennaltaehkäisystä – jo ennen kuin omissa ympäristöissä tapahtuu jotakin – jatkuvasti tärkeämpiä liiketoiminnan turvaamisessa ja kansallisen turvallisuuden vahvistamisessa.

Uhkaympäristön tarkkailuun kannattaa ehdottomasti sisällyttää ajatus jatkuvasta, ennakoivasta riskien havainnoinnista. Pelkkä haavoittuvuuksien monitorointi ja tietoturva-aukkojen sulkeminen ei riitä.

Nopeasti muuttuvassa uhkamaisemassa henkilökohtaisten, organisaatiotason ja toimitusketjujen hyökkäyspinta-alojen tunteminen ja riskien ennakointi tulee päivä päivältä tärkeämmäksi.

Sami Borén toimii uhkatiedustelupäällikkönä Cinialla. Hän toimii palveluomistajana digitaalisen riskin ja uhkatiedustelun palvelussa, joka tuottaa proaktiivista monitorointia, tiedustelua ja analyysiä organisaatioiden ja niiden avainhenkilöihin liittyviin uhkiin liittyen, sekä yksityisen että julkisen sektorin organisaatioiden käyttöön. Aiemmin Borén on työskennellyt 17 vuotta viranomaistehtävissä, joista pääosa tiedustelu- ja analyysitehtävissä.

TEKSTI: JANI ISOHANNI

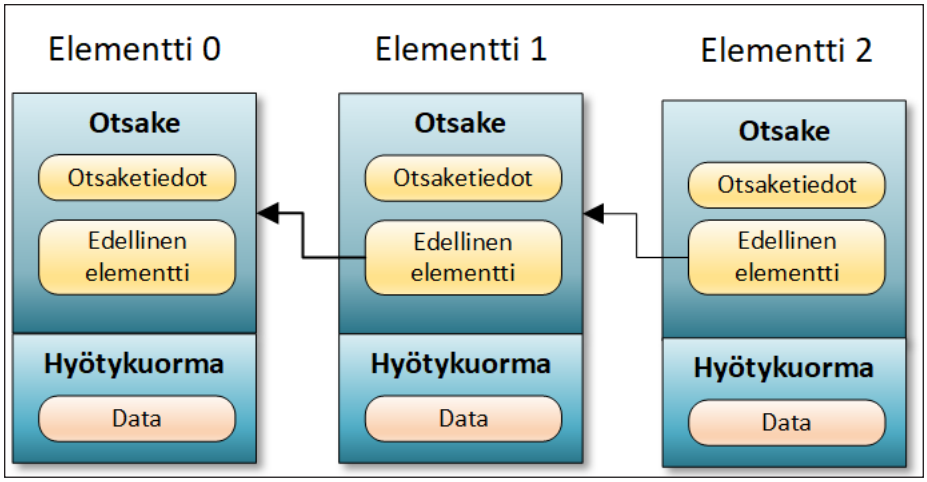
Lohkoketjut

Jani Isohanni toimii Digian Defence-liiketoiminnan pääarkkitehtina. Hänellä on pitkä kokemus ohjelmistoliiketoiminnasta, kokonaisarkkitehtuurista ja tutkimustyöstä. Isohanni on koulutukseltaan tekniikan lisensiaatti.

Lokakuun 31. päivä 2008 Satoshi Nakamoto julkaisi ns. white paper:n otsikolla ”Bitcoin: A Peer-to-Peer Electronic Cash System”. Julkaisussa kuvailtiin kryptovaluutta Bitcoinin perusarkkitehtuuri, ja jo tammikuun 9. päivä 2009 Nakamoto julkaisi ensimmäisen version Bitcoin-ohjelmistosta. Bitcoin alkoi hiljalleen syntyä ja on sittemmin tullut maailmankuuluksi paitsi massaa keränneenä virtuaalivaluuttana, niin myös siinä esitellyn lohkoketjuarkkitehtuurin takia, olkoonkin, että termi ”lohkoketju” jalkautui vasta myöhemmin.

Lohkoketju on teknologiana herättänyt paljon mielenkiintoa ja sille etsitäänkin uusia sovellutuskohteita aktiivisesti. Lohkoketjut sisältävät paljon monimutkaisia algoritmeja ja ne ovat varsin hienostuneita monessakin mielessä. Niitä voi kuitenkin tarkastella arkkitehtuurillisina rakennuspalikoina siinä kuin muitakin teknologioita, kunhan asiaa tarkastelee sopivalla abstraktiotasolla.

Tässä artikkelissa esitellään lohkoketjut ylätasolla, verrataan niitä perinteisiin relaatiotietokantoihin ja sivutaan lyhyesti potentiaalisia käyttökohteita sotilaallisessa kontekstissa.



Linkitetty lista. Esimerkissä on piirretty otsake (”header”) ja data-alue erikseen.

Lohkoketjun rakenne

Alkujaan lohkoketju on luotu digitaalisen valuutan tarpeisiin. Ideana on ollut luoda mahdollisimman avoin ja luotettava kirjanpito. Kun kirjanpito aloitetaan, on se luonnollisesti tyhjä. Siihen luodaan tilejä ja tileille saldo. Jokainen muutos on transaktio ja kirjanpidossa on tärkeää tallentaa paitsi tilin saldot ja omistajat, niin myös jokainen transaktio eli esimerkiksi rahatapahtuma tai vaikkapa uuden tilin luonti. Jokainen haluaa nähdä tilin saldon lisäksi, mitä tilillä on tapahtunut. Erityisesti on tärkeää voida tallentaa tapahtumahistoria niin, ettei sitä voida muuttaa jälkikäteen. Lohkoketju vastaa varsinkin tähän tarpeeseen.

Tiedon tallentamisen näkökulmasta lohkoketjua voi ajatella yksinkertaisena listarakenteena. Yksi ensimmäisiä tietorakenteita, joihin ohjelmistokehittäjä törmää, on linkitetty lista. Linkitetty lista on lista elementtejä tai tietueita, jossa säilytetään dataa, joitain tarpeellisia otsaketietoja ja linkki seuraavaan ja/tai edelliseen elementtiin. Yksinkertainen esimerkki tällaisesta listasta on kuvassa 1.

Listarakenteeseen on helppo lisätä elementtejä aiempien väliin luomalla uusi elementti ja määrittämällä viittaukset ympäröivien elementtien kanssa uusiksi. Vastaavasti on helppo muokata datan arvoja ja muita tietoja.

Kuten todettiin, lohkoketjuissa tavoite on tallentaa transaktioita eli muutoksia luotettavalla tavalla. Halutaan siis ratkaisu, jossa tehtyjen transaktioiden muuttaminen jälkikäteen olisi mahdotonta. Tavoitteeseen päästään hieman linkitettyä listaa vastaavalla tietorakenteella, jossa on hyödynnetty kryptografisia algoritmeja. *Kryptografinen tiivistefunktio* (”cryptographic hash function”) on algoritmi, joka ottaa syötteen ja palauttaa syötteestä lasketun tiivisteluvun (”tiiviste”, toisinaan myös ”hash value” tai pelkkä ”hash”), joka on yksikäsitteinen.

Tiivistealgoritmien toteutustapoja on useita ja niitä käytetään laajalti erilaisissa tietoturvatoteutuksissa. Yleisiä vaatimuksia tällaisille algoritmeille ovat muun muassa seuraavat:

- Palauttaa aina yhtä pitkän luvun (pääsääntöisesti – tästä on jotain poikkeuksia).

- Pienikin muute syötteessä muuttaa tulostetta huomattavasti. Tämä osaltaan varmistaa, ettei tiivisteen rakenteesta voi

käytännössä tehdä halutunlaista syötettä muokkaamalla.

- Algoritmi ei ole siinä mielessä kääntyvä, että ei ole käytännössä mahdollista luoda annettua tiivistettä vastaavaa syötettä, koska se vaatisi valtavasti laskentatehoa.

- Tiiviste edustaa syötettä siinä määrin, ettei ole käytännössä mahdollista, että toinenkin sovellutuksen syöte johtaisi samaan tiivisteeseen.

Koska tiivistefunktio tuottaa määrämittaisen vastauksen, on matemaattisesti mahdollista, etteivät kaikki vaatimukset täyty. Käytännössä vaatimuksiin kuitenkin päästään riittävän hyvin.

Yksi yleisesti käytetty tiivistealgoritmi on SHA-256, joka tuottaa aina 256 bittisen tiivisteen, joka yleensä koodataan edelleen 64 merkin heksadesimaaliluvuksi (merkkijono, jossa jokainen merkki on numero 0-9 tai kirjain a-f). Esimerkiksi merkkijonon ”1” SHA-256 algoritmin laskema tiiviste on

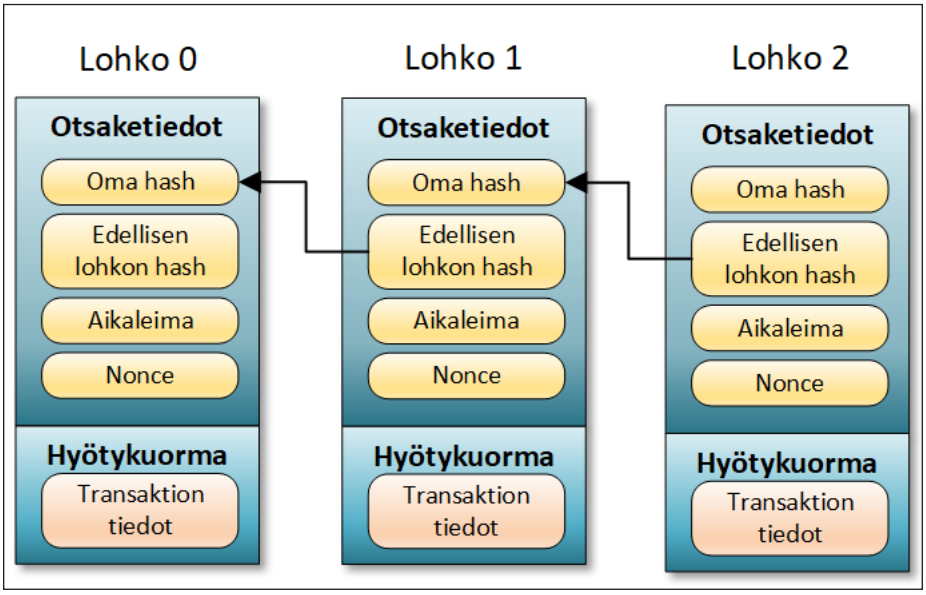
”0x6b86b273ff34fce19d6b804eff5a-3f5747ada4eaa22f1d49c01e52ddb-7875b4b”.

Tässä on hyvä huomata, että mistä tahansa äärellisesti syötteestä tulee siis yhtä pitkä tiivisteluku kuin edellä pelkästään yhdestä merkistä ”1” tuli.

Tiivistefunktion avulla voidaan muokata linkitettyä listaa sellaiseksi, että minkä tahansa elementin muuttaminen vaikuttaisi myös muihin lohkoihin. Kuva 2 sisältää esimerkin siitä minkälainen rakenne voisi olla.

Kutsutaan näitä uusia listan elementtejä lohkoiksi. Lisäsimme jokaiseen lohkoon aikaleiman, mikä on sinänsä kontekstissa looginen vaatimus. Nonce on kertaalleen käytettävä luku (”number once”), joka liittyy konsensualgoritmiin, johon palataan kohta. Lohkoketjuissa lohkot sisältävät yleensä useampia transaktioita ja niihin liittyviä tarkistussummia. Yksi yleinen tapa on muodostaa lohkon sisältämistä transaktioista ns. Merkel-puu ja tallentaa puun juuri lohkon data-alueelle.

Oleellinen muutos pelkkään listarakenteeseen on tiivistearvojen kentät. Toinen tiivistearvo on lohkon itsensä tiiviste ja toinen edellisen lohkon tiiviste. Jos esimerkiksi lohkon 8 sisältöä muutetaan, niin kyseisen lohkon tiivistearvo muuttuu. Nyt voidaan siis tarkistaa seuraavasta lohkosta 9, mikä lohkon 8 arvo pitäisi olla ja sitä kautta voidaan huomata, jos muutoksia on tehty. Jos siis muutamme jotain aiempaa ketjun lohkoa, niin sen tiivisteluku muuttuisi, joten myös seuraavan lohkon sisältämä tiivisteluku muuttuisi, jolloin myös kyseistä lohkoa seuraavan lohkon tiivisteluku muuttuu. Näin muutos propagoituu jokaiseen myöhempään lohkoon. Näin voidaan osaltaan luoda logiikka, miten transaktioketjun eheyden voi tarkistaa.



Lohkoketjurakenteen hahmotelma.

Infrastruktuuri

Edellä esiteltiin tietorakenne, jonka eheys on helppo tarkistaa. Mutta mikä estää muuttamasta aiempia tietoja ja yksinkertaisesti laskemasta uusia arvoja? Tämä ongelma nousee esiin tapauksessa, jossa koko tietovaranto olisi yhden tahon käsissä ja siten muutettavissa. Esimerkiksi perinteiset tietokannat ovat tällaisia. Yksi lohkoketjun ratkaiseva ero tietokantoihin on kuitenkin siinä, että se on hajautettu paitsi useille palvelimille, niin myös eri toimijoille. Ketjusta on siten tallennettu kopiot useille eri tahojen hallinnoimille palvelimille ja palvelinten ohjelmistot sopivat aina keskenään, minkälainen lohko ketjuun voidaan ylipäätään lisätä, mikä lohko lisätään ketjuun seuraavaksi ja lopulta verkosto määrittelee, mikä ketju on kelvollinen.

Hajauttamalla lohkoketju ja erityisesti kirjoituslogiikka useille eri tahojen hallinnoimille palvelimille, joissa jokaisessa on kopio ketjusta, voidaan luoda infrastruktuuri, joka valvoo ketjun eheyttä ilman keskitettyä auktoriteettia. Kun joku verkostossa haluaa lisätä uuden lohkon ketjuun, pitää verkoston hyväksyä muutos. Näin mikään yksittäinen taho ei voi määrittää uuden transaktion tekemistä ja tallentamista, vaan pelkästään ehdottaa sitä ja lopulta enemmistö palvelimista päättää, hyväksytäänkö lisäys.

Jotta yhteinen näkemys eli konsensus voidaan muodostaa, tarvitaan konsensusalgoritmi (”consensus algorithm”). Algoritmeja on monenlaisia erilaisiin käyttötarkoituksiin. Yksi yleisesti käytetyistä on Proof-of-Work tai lyhyemmin PoW, jossa lohkon lisäämistä esittävän pitää esittää todiste, että hän on käyttänyt laskentatehoa lohkon eteen. Käytännössä tämä tapahtuu asettamalla uuden lohkon tiivisteelle jokin vaatimus.

Esimerkiksi voidaan vaatia, että tiiviste alkaa kolmella nollalla eli on muotoa ”0x000…”. Kuten edellä todettiin, tiivistealgoritmien ominaisuuksien takia on käytännössä mahdotonta valita sellainen syöte, jolla vaatimus täytetään. Toisaalta lohkon tietosisältöhän on kiinnitetty, koska haluamme tallentaa juuri tietyn tiedon. Täten jäljelle jää ainoastaan vaihtoehto, jossa lohkon nonce-arvoa nostetaan yhdellä ja tiiviste lasketaan aina uusiksi, kunnes saadaan lohko, jonka tiiviste täyttää vaaditun ehdon. Tätä kutsutaan louhimiseksi. Kun lisättävälle lohkolle on saatu haluttu tiivistearvo, lohko lähetetään verkon hyväksyttäväksi. Koska tiivis-

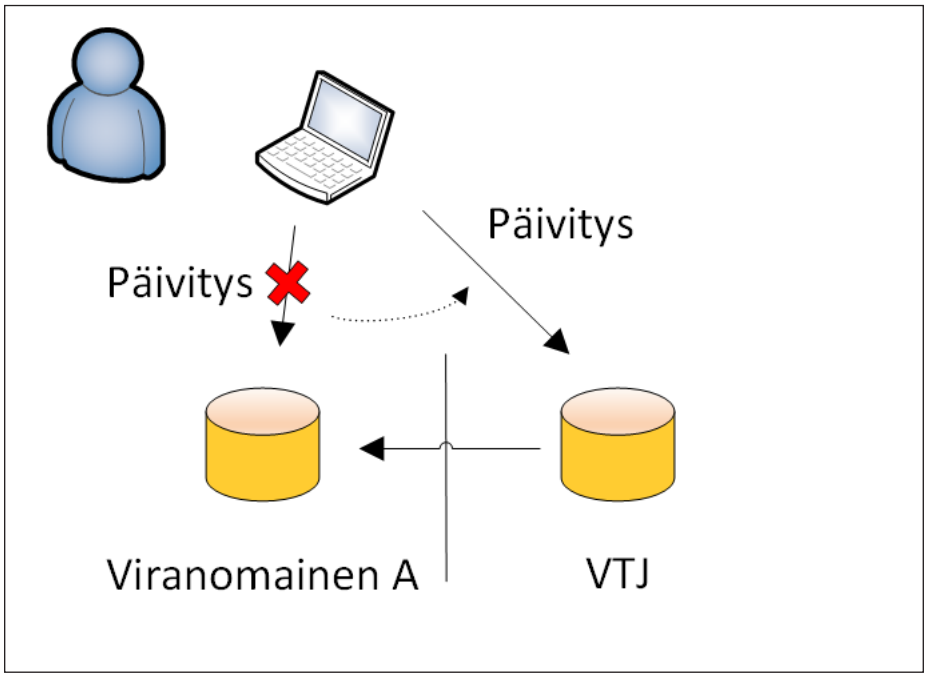
te sinänsä varmistaa vain lohkon kelvollisuuden eikä koko ketjun kelvollisuutta, on verkostossa vielä muita algoritmeja, jotka varmentavat varsinaisen lisäämisen.

Esimerkiksi voidaan tulla tilanteeseen, jossa kaksi palvelinta syöttää verkkoon eri lohkot, jotka täyttävät sinänsä vaaditut ehdot ja osa verkostosta hyväksyy toisen lohkon ja osa toisen. Tällöin ollaan tilanteessa, jossa onkin kaksi eri versiota lohkoketjusta. Jos nyt joku osapuoli haluaa lisätä vielä uuden lohkon, voi sen lisätä vain toiseen olemassa olevista ketjuista ja lisäys tapahtuu siihen ketjuun, jota lisääjä pitää oikeana (tai jonka lisääjä näkee sillä hetkellä).

Tällaisia tilanteita tulee, koska koko palvelininfrastruktuuri ei voi validoida jokaista syötettyä lohkoa yhdessä transaktiossa ihan teknisistä syistä (kyseessä olisi valtava hajautettu transaktio). Tilanne ratkaistaan verkostossa niin, että ketju, johon on käytetty eniten laskentatehoa, preferoidaan ja lyhyempi lopulta hylätään. Jos esimerkiksi lohkoketju hajaantuu ensin kahteen osaan, joissa on vain yksi lohko eroa, niin jossain vaiheessa joku käyttäjä lisää uuden lohkon toiseen näistä ketjuista. Kun huomataan, että kaksi eri mittaista ketjua on olemassa, niin lyhyempi sivuutetaan ja pidemmästä otetaan ”oikea versio”.

On siis mahdollista, että vaikka halutaan lisätä täysin kelvollinen lohko, niin verkosto sen hylkää ja hylkäys voi jopa tapahtua kohtalaisella viipeellä. Tällöin laskenta pitää aloittaa alusta, koska lisäys tapahtuukin muuttuneeseen ketjuun jolloin edellisen blokin tiiviste on muuttunut ja on siis löydettävä uusi nonce-arvo. Tämä toteutus vaatii runsaanlaisesti laskentatehoa ja PoW-algoritmia onkin kritisoitu energiatuhlariksi.

Oleellista ratkaisussa on, että lohkoketjun infrastruktuuri on usealla riippumattomalla käyttäjällä ja ohjelmiston toimintalogiikka on rakennettu sellaiseksi, että sen ohittaminen huijaustarkoituksessa on melkeinpä mahdotonta. Kun verkosto on luonut ja tallentanut yhteisesti hyväksytyn lohkoketjun alun, niin sen muuttaminen ei ole käytännössä mahdollista. Näiden lisäksi kokonaisuus sisältää myös muita algoritmeja esimerkiksi käyttäjän tunnistamiseksi. Lohkoketjuarkkitehtuureja on myös hyvin erilaisia erilaisiin käyttötarkoituksiin.



Käyttäjä ei voi päivittää rekisteritietojaan suoraan asiointiviranomaisen tietovarantoon vaan hänet ohjataan keskitettyyn palveluun.

Lohkoketju vs. tietokanta

Perinteinen relaatiotietokanta on suunniteltu täyttämään ns. ACID-ehdot.

- Atomicity – jokainen operaatio tapahtuu (onnistuu tai epäonnistuu) yhtenä transaktiona eli kokonaisuutena.

- Consistency – tietovarannolla on eheä tila joka hetkellä. Tämä tarkoittaa, että jokainen transaktio voi muuttaa tilaa vain niin, että eheys säilyy.

- Isolation – Jokainen transaktio tapahtuu eristetysti muista transaktioista. Vaatimus varmistaa rinnakkaiset transaktiot turvallisesti.

- Durability – Kestävyys. Jokainen kirjoitus tallentuu niin, että vikatilanteesta voidaan toipua eheään tilaan.

Näillä varmistetaan, että kantaan tehtävät transaktiot ovat nopeita, konsistentteja ja tallentuvat varmasti. Kannat yleisesti myös tukevat CRUD-operaatioita (create, read, update, delete), eli tietueiden luomista, lukemista, päivittämistä ja poistamista. Käytännön toteutuksena relaatiotietokannat ovat nykyään äärimmäisen nopeita ja vikasietoisia.

Lohkoketju on perusarkkitehtuuriltaan ja suunnittelufilosofialtaan erilainen. Uuden lohkon lisääminen voi kestää toteutuksesta riippuen pitkäänkin ja se ei aina edes välttämättä onnistu. Kuten todettiin, vanhoja tietoja ei voida muuttaa ja vanhojen tietojen hakeminen ketjusta ei ole yleensä nopeaa, koska kokonaisuutta ei ole suunniteltu siihen. Toisaalta ketjun tiedot on tallennettu laajaan infrastruktuurin ja esimerkiksi varsinaiselle varmuuskopiolle ei ole sinänsä tarvetta. Lohkoketjuissa tiedot ovat kaikkien saatavilla vaikka yksittäinen palvelin tai jopa verkkosegmentti vikaantuisi.

Esimerkki väestörekisteri

No mitä lohkoketjulla sitten voisi tehdä? Uusien teknologioiden hyötyjen ymmärtäminen vie aina tovin ja vaatii kollektiivista pohtimista ja yhteisen näkemyksen luomista, sekä vaikeimpana aina nykyisyyden ja nykyisten ajatustapojen haastamista. Otetaan esimerkkitietovarannoksi väestötietojärjestelmä ja pohditaan, mitä etuja lohkoketju voisi sen toteutukseen ja käyttöön tuoda.

Suomessa väestörekisteri on tallennettu keskitettyyn väestötietojärjestelmään, jota

ylläpitää DVV ja osa kunnista. Monet viranomaiset käyttävät rekisterin tietoja erilaisten rajapintojen kautta ja erinäisissä käyttötapauksissa rekisteristä voidaan tallentaa tarpeellisia tietoja myös viranomaisten eri järjestelmiin, eli myös rinnakkaisia (osa)kopioita voi olla.

Nykyisellään kansalaiset päivittävät esimerkiksi osoitetietonsa suoraan DVV:n järjestelmään (katso kuva 3). Monilla viranomaisilla on omissa kanavissaan ohjeistus tehdä osoitepäivitys DVV:lle, josta he saavat päivitetyn tiedon käyttöönsä. Tällä varmistetaan, että on yksi keskitetty totuus tiedoista. Muussa tapauksessa tiedot jäisivät kulloisenkin viranomaisen omiin järjestelmiin ja niiden vieminen keskitettyyn kantaan vaatisi omat pohdintansa. Kokonaisuutena prosessi on sinänsä toimiva, mutta siinä on myös kehittämisen paikkoja.

- Organisaatioiden paikalliset kopiot ovat aina vanhentuneita. Tietojen virkistysfrekvenssi on monesti vähintään päivän.

- Käyttäjien on mentävä DVV:n palveluun päivittämään tietoja.

- Kun virkistetään paikallinen kopio, ei siinä yleensä tule historiatietoa.

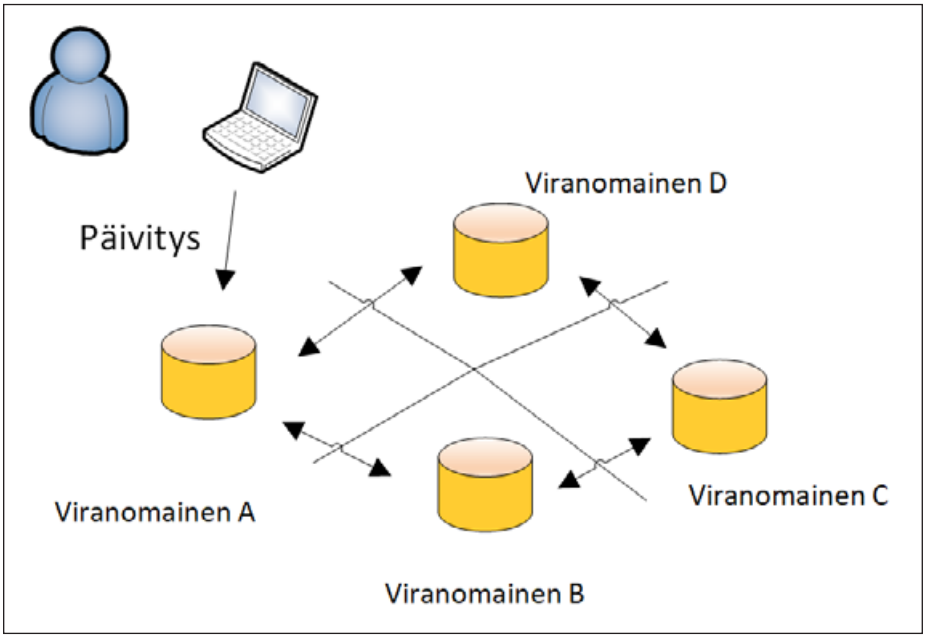
- Lähtökohtaisesti keskustietovarannon tietoturva määrittelee myös muiden palveluiden tietoturvan, koska jos keskustietovaranto murretaan ja tiedot sotketaan, korruptoitunut tieto välittyy myös muualle.

Väestörekisteriä voisi ajatella toteutettavan valittujen viranomaisten yhteisenä, suljettuna lohkoketjuarkkitehtuurina. Tällaisessa mallissa jokainen viranomainen voisi ottaa osoitteenmuutoksen käyttäjältä vastaan ja tallentaa sen lohkoketjuun. Tieto välittyisi suoraan kaikille viranomaisille ja kaikilla olisi ajantasainen osoitteisto käytössä. Tässä myös syntyisi ratkaisu, jossa viranomaiset voisivat valvoa toisiaan – jos tiedoissa huomataan huomiota herättäviä poikkeamia, voidaan nähdä, mistä ne tulevat ja historiatiedoista voidaan haluttaessa palata myös taaksepäin yhteisellä päätöksellä.

Kiteytettynä etuja olisi siis.

- Ajantasainen tieto on kaikkien saatavilla.

- Jokainen viranomainen voi ottaa muutoksia vastaan. Saavutetaan parempi käyttäjäkokemus loppukäyttäjälle.



Lohkoketjuarkkitehtuurissa käyttäjä päivittää tietonsa asiointiviranomaisen järjestelmään, josta muutos kirjautuu automaattisesti muille verkoston viranomaisille.

- Historiatieto on kaikkien näkyvillä ja käytettävissä.

- Poikkeavat kirjoitukset jäävät herkemmin kiinni, koska valvovia organisaatioita on useampia.

Käytännön toteutuksena tässä toki olisi monta selvitettävää asiaa lainsäädännöstä ja vastuujaoista lähtien. Esimerkissä on kuitenkin nähtävissä, miten vanhasta ajattelutavasta luopuminen toisi erinäisiä etuja nykyiseen kokonaisuuteen. Nykyään monesti vanhaksi koettu keskuskonemainen ajattelutapa tuo mukanaan rajoitteita, joihin on totuttu ja joita ei välttämättä aina edes tiedosteta ilman ulkopuolisen tahon näkemyksiä.

Lopuksi

Nakamoton työ on osoittautunut paitsi teknisesti erittäin oivaltavaksi, niin myös yhteiskunnallisesti poikkeuksellisen merkittäväksi. Bitcoin on toiminut virtuaalivaluuttojen esikuvana ja esitetty ohjelmistoarkkitehtuuri on mahdollistanut valtavasti uusia, innovatiivisia käyttötapauksia.

Tarinassa on myös poikkeuksellista mystiikkaa liittyen Nakamoton hahmoon. Hän osallistui Bitcoinin kehittämiseen aktiivisesti sen alkuaikoina, mutta luopui roolistaan 2010 puolivälin aikoihin. Nakamotolla arvioidaan olevan noin miljoona bitcoinia omistuksessaan, joiden yhteisarvo on enimmillään ollut kymmeniä miljardeja dollareita. Tiettävästi tuota valtavaa pääomaa ei kuitenkaan ole käytetty ollenkaan. Tarinasta tekee mystisen myös se, että tänä päivänäkään ei tiedetä, kuka Satoshi Nakamoto on. Ei edes tiedetä, onko hän oikea ihminen vai jopa jonkin ryhmän pseudonyymi. Koko teknologian on siis laittanut alulle myyttinen multimiljardööritaho, josta ei tiedetä juuri mitään. Lohkoketjujen mahdollistama ”julkinen anonymiteetti” on siis ainakin tältä osin toteutunut täydellisesti.

Kirjoittaja toimii Viestikiltojen Liitto ry:n puheenjohtajana.

TEKSTI: TERO PALOKANGAS

KUVAT: JUHA PELTOMÄKI JA JUKKA-PEKKA VIRTANEN

Viestikiltojen Liiton katse tulevaisuudessa

Viestikiltojen Liitto juhli kunniakasta 60-vuotista taivaltaan vuonna 2023. Merkittävä saavutus oli ”Kipinä kantaa” -juhlakirjan julkaiseminen, jolla samalla paketoitiin liiton tämän hetkinen toiminta ja saavutukset. Vaikka elämmekin tällä hetkellä maanpuolustuksen ”kulta-aikaa”, on samalla kilpailu ihmisten vapaa-ajasta käynyt vuosi vuodelta tiukemmaksi. Vapaaehtoisen maanpuolustuksen toimijoiden tuleekin omalta osaltaan kyetä vastaamaan asetettuun haasteeseen. Toiminnan on oltava monipuolista, ja kyettävä tarjoamaan jäsenistölle merkityksellistä sisältöä, jota muualta ei ole saatavissa. Viestikiltojen Liitto onkin käynnistänyt strategiatyönsä, jolla pyritään vastaamaan kysymykseen mitä yhdistys haluaa olla vuonna 2030 osana vapaaehtoisen maanpuolustuksen kokonaiskenttää ja -tarjontaa.

Viestikiltojen Liiton järjestämät viestimiespäivät ovat erinomainen tilaisuus koko toimialan eri toimijoiden väliselle verkostoitumiselle. Kuvia vuoden 2023 elokuun viestimiespäiviltä, jotka ansiokkaasti järjesti Kaakkois-Suomen Viestikilta Mikkelissä.

Kipinä on kantanut

Viestikiltojen Liitossa on kuuden vuosikymmenen ajan tehty pyyteetöntä työtä vapaaehtoisen maanpuolustuksen eteen. Toiminnan kulmakivinä ovat toimineet muun muassa viestihistorian vaaliminen ja museotoiminta sekä moninainen ja monipuolinen koulutustoiminta. Historian vaalimista toteutetaan jatkossakin osana Museo Militarian toimintaa, jossa lähiaikoina onkin edessä pitkään valmisteltu perusnäyttelyn uudistaminen. Koulutustoiminnan osalta merkittävä saavutus viime vuosina on ollut toiminnan sitominen entistä tiukemmin osaksi MPK:n hallinnoimaa sotilaallisia valmiuksia tukevaa vapaaehtoista koulutusjärjestelmää. Merkittävä toimintamuoto myös liiton rahoituksen näkökulmasta on ollut viestiristien jakaminen ansioituneille tahoille saatujen esitysten perusteella kaksi kertaa vuodessa. Viestiristejä tullaan jatkossakin jakamaan perinteisen tyyliin. Hyviä ja perusteltuja anomuksia siis laatimaan.

Viestikiltojen Liitto on viime vuosina järjestänyt myös ajankohtaisseminaareja, niin verkossa kuin lähitoteutuksinakin. Syyskaudella 2024 onkin taas odotettavissa mielenkiintoinen ajankohtaiswebinaari sekä jo perinteeksi muodostunut A.R. Saarmaa -seminaari 20. syyskuuta. Vuosittain on myös järjestetty perinteisiä viestimiespäiviä, jotka on tarkoitettu kaikille viestiaselajin ja johtamisjärjestelmätoimialan parissa toimiville tahoille. Toiveissa olisi saada tähän lämminhenkiseen ja ajassa elävään tapahtumaan entistäkin enemmän osallistujia myös viestikiltakentän ulkopuolelta. Laittakaapa siis

24.–25. elokuuta kalenteriin, sillä silloin viestimiespäiviä vietetään Etelä-Hämeen alueella. Tarkempi paikka selviää suunnittelun edetessä. Vuoden Viestikilta -kilpailun ja Kotirata-ammuntojen toteutusta jatketaan hyväksi todetuilla uusilla säännöillä. Edellä mainittujen lisäksi Viestikiltojen Liitto jatkaa kaikkia muitakin hyväksi havaittuja toimintamuotojaan jatkossakin, niitä samalla jatkuvan parantamisen hengessä kehittäen.

Eräs perinteiden vaalimiseen liittyvä merkittävä kokonaisuus on viestijoukkojen vuosipäivän 5.3. profiilin kohottaminen. Perinteessähän pääsi kiistämättä käymään pieni notkahdus Puolustusvoimien uudistuksen jälkeen, kun perinteitä päätoimisesti vaalinut Viestirykmentti lakkautettiin vuoden 2015 alussa. Viestikiltojen Liitto on kyseistä päivää senkin jälkeen pyrkinyt asianmukaisesti juhlistamaan, esimerkkinä viime vuonna toteutetut liiton 60-vuotisjuhlallisuudet, jotka samalla toimivat viestijoukkojen vuosipäivän juhlana. Nyt Puolustusvoimissa on Pääesikunnan johtamisjärjestelmäpäällikön johdolla päätetty lähteä nostamaan viestijoukkojen vuosipäiväperinnetilaisuuden profiilia ansaitsemaansa arvoon, yhdessä toimialan vapaaehtoisten toimijoiden kanssa. 1.3. Vekaranjärvellä toteutetaankin taas pitkästä aikaa valtakunnallinen viestijoukkojen vuosipäivä yhdessä Puolustusvoimien, Viestikiltojen Liiton ja Viestiupseeriyhdistyksen kesken.

Viestikiltojen Liiton olemassaolon tärkein tehtävä jatkossakin on alueellisten viestikiltojen toiminnan tukeminen ja mahdollistaminen. Tavoitteena on varmistaa jokaisen viestikillan toimintakyky, jonka eteen liiton hallitus tulee jatkossakin ponnistelemaan. Viestikiltojen jäsenmäärät on saatu viimeisten vuosien aikana vakiinnutettua, mutta mihinkään varsinaiseen yleisöryntäykseen uusien jäsenten osalta ei ole päästy. Viestikiltojen toiminnan aktiviteeteissa on edelleen myös merkittäviä eroja. Osa on kyennyt ylläpitämään ja kehittämään monipuolista toimintaa. Osalla viestikilloista toiminta lepää edelleen ikääntyvien kiltaveljien ja siskojen varassa. Viestikiltatoiminnan elinvoimaisuuden tukemiseen tarvitaan jatkossa kaikkia: alueellisten kiltojen omaa vastuukantoa sekä liiton ja myös Puolustusvoimien tukea. Vaikka vapaaehtoisen maanpuolustuksen tuleekin tukea maanpuolustusta, tarvitsevat viestikillat toimintansa tueksi vastavuoroisesti myös Puolustusvoimia. Viime vuosina muun muassa varuskuntaverkon harventuessa

Viestikiltojen liitto jatkoi A.R. Saarmaan päivään liitettyä ajankohtaisseminaariperinnettä, jonka jälleen kerran asiantuntevasti johti liiton varapuheenjohtaja ja koulutuspäällikkö Juha Peltomäki. Samassa yhteydessä julkaistiin liiton 60-vuotisjuhlakirja ”Kipinä kantaa”.

Viestikiltojen Liiton hallituksen kokous ja puheenjohtajaseminaari lokakuussa 2023. Vaikka verkkokokoukset ovat liittohallituksen pääkokoontumistapa, on lähikokouksilla edelleen oma tärkeä merkityksensä.

on perinteinen tuki valitettavasti vähentynyt, tietyillä alueilla jopa tyystin loppunut. Toivoisinkin meitä virkapukuisia suhtautumaan positiivisesti vapaaehtoisten toimijoiden tukipyyntöihin, ja jopa tukea aktiivisesti tarjoamaan. Se ei ole keneltäkään pois, pikemminkin päinvastoin.

Tulevaisuus haastaa

Viime vuosien turvallisuusympäristöön liittyvät tapahtumat ovat nostaneet kansalaisten maanpuolustustahtoa ja samalla vapaaehtoisen maanpuolustuksen eri toimintamuotojen suosiota. Tässä on samalla merkittävä mahdollisuus viestikilloille kehittää toimintaansa ja saada kipeästi kaipaamiaan uusia jäseniä rekrytoitua mukaan toimintaan. Viestikilloilla on tarve saada toimintaansa mukaan etenkin, monen muun vertaisjärjestön tapaan, nuoria sekä myös naispuolisia jäseniä. Jäsenrakenteen elinvoimaisuushan taas mahdollistetaan monipuolisella ja mielenkiintoisella toiminnalla, jonka itsestään pitäisi motivoida ihmisiä hakeutumaan viestikiltojen jäseniksi.

Koulutustoiminta on nähdäkseni jatkossakin se ”veturi”, jolla viestikiltojen kiinnostavuus ja samalla merkitys koko maanpuolustukselle taataan. Meidän tulee laajentaa aselajin ja toimialan vapaaehtoista koulutustarjontaa nyt muun muassa hyväksi havaituista HF- ja Arjen välineiden -koulutuspaketeista kohti monipuolisempia ja nykyaikaisia kokonaisuuksia. Yhden mahdollisuuden tähän nähdäkseni tuo Puolustusvoimissa käynnissä oleva asevelvollisten koulutuksen monipuolistaminen, josta esimerkkinä toimialalla rakennetaan parhaillaan erityistä ICT-varusmieskoulutusjärjestelmää. Taustalla kehittämisessä on muun muassa Ukrainassa saadut hyvät kokemukset erityisosaamista omaavien toimijoiden valjastamisessa toimimaan maanpuolustuksen tarkoitusperien hyväksi, puhutaan siis eräänlaisesta ”joukkoistamisesta”. Siinä esimerkiksi paikallispuolustuksen eri käyttötarkoituksiin koulutettavien ICT-alan asevelvollisten osalta on alueellisilla viestikilloilla merkittävä mahdollisuus toimintansa monipuolistamiseen ja sitä kautta aktiivisten jäsenten rekrytoimiseen.

Liiton toimintasuunnitelman mukaisesti tänä vuonna käynnistetään strategian laatiminen vuotta 2030 silmällä pitäen.

Liiton syyskokouksessa marraskuussa 2023 päätettiin muun muassa puheenjohtajan tehtävien siirtymisestä vuoden 2024 alussa Jukka-Pekka Virtaselta Tero Palokankaalle. Samassa yhteydessä paljastettiin VP10 muistolaatta, joka on sijoitettu Helsingin Postitalon seinään. Tilaisuutta kunnioitti Puolustusvoimien johdon edustajana sotatalouspäällikkö kenraaliluutnantti Mikko Heiskanen.

Haluamme yhdessä yhteistyötahojemme kanssa miettiä mitä Viestikiltojen Liitto ja se alueelliset viestikillat haluavat tulevaisuudessa tehdä osana kokonaismaanpuolustusta. Yksi strategiaan liittyvä selvitystehtävä on toimialan vapaaehtoisjärjestöjen kokonaiskattaus ja roolitus. Olen henkilökohtaisesti sitä mieltä, että meillä olisi tarve ja samalla aito mahdollisuus tarkastella jälleen kerran muun muassa Viestikiltojen Liiton, alueellisten viestikiltojen sekä muiden toimialan vapaaehtoistoimijoiden keskinäisiä tehtäviä ja rooleja. Tähän liittyy myös suhde Maanpuolustuskiltojen Liittoon, jossa osa alueellisista viestikilloista on tällä hetkellä jäsenenä, Viestikiltojen Liitto taas ei. Tämän tarkastelun pohjaksi olemmekin jo selvitelleet verrokkina Pioneeriaselajin Liiton toimintaa ja organisoitumista, sama tullaan tekemään vielä muidenkin verrokkijärjestöjen osalta. Merkittävä rooli strategiatyössä on Viestikiltojen Liiton arvovaltaisella valtuuskunnalla puheenjohtajansa Esa Salmisen johdolla. Valtuuskunnan on tarkoitus lanseeraamansa C5i-alan sateenvarjon alla koordinoida toimialan vapaaehtoiskentän kokonaisselvitystä. Työssä tullaan konsultoimaan tiiviisti Puolustusvoimia, jotta toimialan vapaaehtoiskentän toiminnan tuki saadaan jatkossakin maksimaalisesti kohdennettua sotilaallisen maanpuolustuksen tarpeisiin. Jäädään näiltä osin odottamaan strategiatyön etenemistä sekä sen pohjalta mahdollisesti jatkossa tehtäviä kehittämisesityksiä.

Lopuksi

Otin vastaan Viestikiltojen Liiton puheenjohtajuuden tämän vuoden alussa Jukka-Pekka Virtaselta. Haluan kiittää edeltäjääni aivan huikeasta kahdeksan vuoden puheenjohtajuudesta. Sen aikana uhkana ollut toiminnan näivettyminen käännettiin takaisin aktiiviseksi ja entistäkin merkityksellisemmäksi viestikiltatoiminnaksi. Saappaat ovat isot täytettäväksi, mutta teen jatkossa parhaani liiton tavoitteiden täyttämiseksi ja toimialan vapaaehtoistoiminnan edelleen kehittämiseksi. Samalla kutsun kaikki toimialan toimijat mukaan yhteisiin talkoisiin. Vapaaehtoisella maanpuolustuksella ja viestikiltatoiminnalla sen osana on mahdollisuus olla jatkossakin merkittävä osa kokonaismaanpuolustusta. Se ei kuitenkaan tapahdu odottamalla tai toisaalta pakottamalla. Osana käynnistettyä strategiatyötä on nyt esimerkkinä hyvä mahdollisuus kaikilla tahoilla päästä aktiivisesti mukaan määrittämään viestikiltatoiminnan tulevaisuuden tavoitteita ja toimintamuotoja. Historia ei näiltäkään osalta vain tapahdu, sitä tehdään yhdessä kaikkien yhteistyökumppaneiden kanssa. Toivotan samalla lehden lukijoille kaikkea hyvää uudelle vuodella 2024. Viestikiltakentillä tavataan.

Viestikiltojen Liitto 60 vuotta 1963–2023 juhlakirja ”Kipinä kantaa”

”Viestikiltojen Liiton tarkoituksena on edistää maanpuolustustyötä, lisätä jäsentensä ja kansalaisten maanpuolustustahtoa, vaalia viestialan historiallisia perinteitä sekä tukea ja edistää jäsentensä toimintaa. Liitto toimii jäsentensä yhdyssiteenä ylläpitäen ja kehittäen yhteistyötä myös muiden maanpuolustusjärjestöjen kanssa. Se pyrkii ulottamaan toimintansa mahdollisimman laajoihin kansalaispiireihin sukupuoleen ja sotilasarvoon katsomatta.” Näillä esipuheen sanoilla alkaa Viestikiltojen Liitto ry:n 60-vuotisen taipaleensa kunniaksi julkaisema juhlakirja ”Kipinä kantaa” (2023).

Kipinä Kantaa kuvaa tiiviillä tavalla Viestikiltojen liiton kuusikymmenvuotisen toimintahistorian tapahtumien ja henkilökuvien kerronnalla. Toiminnan ja tapahtumien kuvaaminen tiivistyy monella tapaa avainhenkilöihin, jotka ovat killan historian aikana sementoineet itsensä toiminnan primus motoreiksi. Primukset ovat henkilökohtaista panostaan säästämättä edistäneet Viestikiltojen liiton ja sen kiltojen toimintaa niin juhlassa kuin arjessakin. Kirja antaa muun muassa syväluotaavan kuvan Martti Rusista Viestikillan perustajajäsenenä ja heraldikkona, jonka kynästä on syntynyt muun muassa aselajin yksi merkittävimmistä henkilöstön palkitsemisen muistoesineistä – Viestiristi.

Henkilökerronnan lisäksi oman osuutensa kirjassa saavat ansaitusti viestiaselajin historian vaalijana Riihimäellä sijainnut Viestimuseo, sekä aselajin museotoiminnan ylläpidon myöhemmin perinyt Museo Militaria Hämeenlinnassa. Osansa kirjan sivuilla saavat myös sodanaikaisen viestitoiminnan historiatiedon ylläpitämisestä vastaava Lokki-viestikeskus -museo sekä Jalkaväkimuseon radiohuone ja sotilasradioamatööriasema Mikkelissä.

Historiaosuuksien ohessa lukija kuljetetaan perehtymään viestikiltojen koulutus- ja kilpailutoimintaan sekä Puolustusvoimien viestitoimialan ja vapaaehtoisjärjestöjen yhteistoiminnan nykymuotoihin. Järjestötoiminta nimensä mukaisesti elää ja voi hyvin toiminnan järjestämisen ja toimintaa pyörittävien ihmisten kautta. Luku koulutus- ja kilpailutoiminnasta avaa jälleen yhden grand old manin, Pellervo Pekkolan henkilöhaastattelun ja -kerronnan kautta muiden muassa kotirata-ammuntojen merkityksiä vapaaehtoisen viestimies- ja maanpuolustustyön kentässä. Koulutustoiminnan kirkkaimmaksi helmeksi nimetty A.R. Saarmaa seminaari Puolustusvoimien, Viestikiltojen liiton sekä muiden maanpuolustusyhdistyksien yhteisponnistuksena saa arvoisensa paikan kirjan kerronnassa.

Kirjan painoarvollisesti merkittävimpiä henkilö- ja historiaosuuksia on onnistuttu keventämään kerronnalla muiden muassa pohjoismaisesta kiltatoiminnasta, liiton hallinnosta ja tukitoiminnasta sekä Viestikiltojen liiton valtuuskunnasta. Niin monesti maanpuolustustyöhön liittyvässä raportoinnissa ja kirjallisessa ilmaisussa suosittu kaava – menneisyys, nykyisyys ja tulevaisuus – on valikoitunut myös Kipinä Kantaa kirjan rakenteeksi. Kirja noudattaa edellä mainittua ja hyväksi havaittua kolmen aikadimension kuvaamista, mutta tällä kertaa aloittaen raikkaasti käsittelyn tulevaisuuden näkymistä, kulkien nykyhetkeen ja viimein painottaen – luonnollisesti – 60-vuotista taivaltaan.

Kaiken kaikkiaan Kipinä Kantaa on laaja katsaus viestiaselajin kilta- ja vapaaehtoistoiminnan kenttään merkittävien jäsenten henkilötarinoiden kautta rakennettuna tarinana. Kirjan sivut täyttyvät mukaansa tempaavilla, viestiaselajin vapaaehtoistoiminnalle ja maanpuolustukselle merkittävillä tuokiokuvilla, henkilötarinoilla, tapahtumilla, asioilla ja paikoilla. Kuvitus elävöittää kerrontaa visualisoimalla tapahtumat ja sitomalla ne, sekä henkilöt liiton historian aikajanalle. Kirjassa asiat muodostavat kerroksellisia tarinoita valtakunnallisen kiltatoiminnan kentässä paikallisten ja alueellisten kiltojen toiminnan kuvauksien kautta. Tarinoiden kerrokset valtakunnalliselta tasolta kytkeytyvät useissa tapauksissa toimintaa pyörittäneiden ja edelleen pyörittävien henkilöiden kautta paikallistason toimintaan ja toisin päin. Näitä kerroksellisia ja historiallisesti merkittäviä tapahtumia kuvatessaan toimitustyöryhmä on tehnyt ansiokkaan työn kerätessään Viestikiltojen liitto ry:n, sitä edeltäneen Viestikillan, alueellisten kiltojen sekä toimintaan liittyvien henkilöiden ja lähteiden tiedot yksiin kansiin.

Tiivistettynä *Kipinä Kantaa* kokoaa Viestikiltojen liiton, Viestikillan ja liittoon kuuluvien viestikiltojen historian aikajanalle kuvailemalla vapaaehtoisen maanpuolustustyön, maanpuolustustahdon kasvattamisen sekä viestiaselajin historian ja perinteiden vaalimisen merkittävimmät tapahtumat ja henkilökuvat. Ehdottomia kohokohtia ovat Viestikiltojen liiton historiallisten tapahtumien merkityksien kuvaaminen ja sitominen tarinankerronnallisesti laajempaan kuvaan ja välillä jopa hyvinkin tarkkoihin yksityiskohtiin.

Lopuksi

Kirja läpileikkaa kattavasti Viestikiltojen liiton toimintaa vuosien varsilta samalla paneutuen liiton toimintaan merkittävästi osallistuneiden henkilökuviin ja tapahtumavirtaan maalaten kuvan kansalaisjärjestöstä Viestimieshenkeä ylläpitävänä ja kasvattavana toimijana. *Kipinä Kantaa* kuuluu jokaisen viestiaselajiin itsensä lukevan maanpuolustustyöaktiivin, sekä vapaaehtoistoiminnan historiasta kiinnostuneen lukulistalle.

Kirjaa voi ostaa Museo Militarian myymälästä ja verkkokaupasta, sekä alueellisilta viestikilloilta.

- Pasi Puhakka -

TEKSTI: JUKKA-PEKKA VIRTANEN

KUVAT: JUKKA-PEKKA VIRTANEN, JUHA PELTOMÄKI JA SA-KUVA

Muistomerkkejä ja -laattoja viestihistoriallisesti merkittäviin kohteisiin

Päämajan erikoisviestipataljoonalle muistolaatta Helsingin postitalolle

Viestijoukkojen 50-vuotissyntymäpäivänä 5.3.1968 Riihimäellä paljastetusta valtakunnallisesta viestimuistomerkistä alkaen ovat Viestikilta ry ja sen paikallisosastot sekä vuonna 1989 perustettu Viestikiltojen Liitto ry jäsenkiltoineen perustaneet muistomerkkejä ja kiinnittäneet muistolaattoja viestihistoriallisesti merkittäviin kohteisiin eri puolilla Suomea. Viestijoukot ovat paljastaneet myös muutamia muistomerkkejä ja muistolaattoja omille sijoituspaikoilleen.

Viestikiltojen Liitto ry on jatkanut edeltäjänsä Viestikilta ry:n 1960-luvun jälkimmäisellä puoliskolla käynnistämää muistomerkki- ja muistolaattaprojektia kunnioittaen näin menneiden sukupolvien työtä Isänmaan hyväksi.

Tosiasiallisesti projekti sai alkunsa, kun ensimmäinen muistolaatta paljastettiin Mikkelissä Päämajan viestikeskus Lokkiin 30.1.1966. Laattaan tuli kuitenkin virheellisesti maininta, että Lokki olisi toiminut Päämajan viestikeskuksena jo talvisodassa, ja näin ollen muistolaatta poistettiin Lokin saneerauksen yhteydessä. Vapaussodan kenttälennätinpataljoona sai laatan Riihimäelle Kasakkakallioon 5.3.1982. Myöhemmin muistolaattoja on paljastettu muun muassa Kotkassa 17.9.1988 muistuttamaan Suomen ensimmäisestä radioyhteydestä ja Mikkelissä, jossa 5.3.1990 paljastettiin ensimmäisen varsinaisen viestijoukko-osaston, Päämajan Kenttälennätinpataljoonan pronssinen muistolaatta paikallisella työväentalolla. 6.3.2010 paljastettiin Santahaminassa Uudenmaan viestikillan aloitteesta Viestipataljoona 1:n ja Radiopataljoonan muistolaatta.

Jääkäri A.R. Stenholm (Saarmaa) perusti Saksasta salakuljettamallaan kalustolla vastaanotinaseman Vaasan Vaskiluotoon ja vastaanotti ensimmäiset sanomat Libausta laivaston radioasemalta 4.10.1917. Tästä muistuttava muistolaatta paljastettiin jääkärieversti A.R. Saarmaan 125-vuotispäivänä 23.9.2017.

Kenraalimajuriksi ylennyt jääkäri Leo Ekberg perusti 15.12.1917 vastaanotinaseman Helsingin Kulosaareen ja toimi aseman hoitajana aina Helsingin valloitukseen asti. Ekbergin ja hänen perustamansa radioaseman muistoksi oli tarkoitus paljastaa muistolaatta syksyllä 2018. Alkuperäinen huvila oli purettu, eivätkä paikalla nykyisin olevan kiinteistön osakkaat halunneet muistolaattaa rakennukseensa. Muistomerkki päätettiin perustaa läheiseen Eugen Schaumanin (Kluuvin) puistoon. Muistomerkin edellyttämä suunnitteluprosessi ja lupamenettely olivat hyvin monivaiheisia siirtäen paljastustilaisuuden ajankohtaa vuodella eteenpäin. Lopulta muistomerkin paljastustilaisuus järjestettiin 23.11.2019. Muistomerkkihankeen kokonaisbudjetti kohosi lähes 19 000 euroon.

Viimeaikaisia muistolaattoja on paljastettu muun muassa Mikkelissä Päämajan Radiokeskuksen (2018), Riihimäellä talvisodan aikaisen koulutuskeskuksen (2019), Piikkiössä Viestipataljoona 33:n (2020), Karkun Evankelisella Opistolla jatkosodan aikaisen koulutuskeskuksen (2021) ja Kouvolan vanhalla kasarmialueella Viestipataljoona 15:n (2022) muistolle.

Muistolaatoilla ja muistomerkeillä on monia tarkoituksia. Niiden avulla pystymme hahmottamaan eri paikkoihin kytkeytyviä historiallisia tapahtumia, kunnioittamaan sekä menneiden että

nykyisten sukupolvien työtä ja lisäämään viestillisen historian tuntemusta eri tahoilla. Juhlallisilla paljastustilaisuuksilla on ollut suurta paikallista ja jopa valtakunnallista merkitystä niiden muistuttaessa meitä menneiden sukupolvien työstä Isänmaan hyväksi.

Päämajan erikoisviestipataljoonan muistolaatan paljastaminen

Arvokas projekti sai jatkoa Viestikiltojen Liiton syyskokouksen yhteydessä 25.11.2023, jolloin paljastettiin muistolaatta Posti- ja lennätinlaitoksen henkilöstöstä perustetun Päämajan alaisen Viestipataljoona 10 (VP 10) yhdellä perustamispaikalla Helsingin vanhalla postitalolla yhteistoiminnassa Viestikiltojen Liiton, Uudenmaan Viestikillan, Viestiupseeriyhdistyksen, Telian Kerhon ja Puolustusvoimien kanssa. Laatan paljastivat Puolustusvoimien sotatalouspäällikkö kenraaliluutnantti Mikko Heiskanen ja liiton puheenjohtaja Jukka-Pekka Virtanen. Juhlallinen paljastustilaisuus käynnistetiin Pääesikunnassa, jossa puheenjohtajan avaussanojen jälkeen kuultiin Telian Kerhon puheenjohtaja Kimmo Fransilan VP 10 perustamista ja jatkosodan aikaista toimintaa käsitellyt juhlaesitelmä.

VP 10 oli erikoisviestipataljoona, jonka tehtävänä oli valtakunnan kiinteiden viestiyhteyksien käytön ja rakentamisen turvaaminen. Pataljoonaan kuului esikunta, viisi puhelinkomppaniaa hajautettuna eri puolille maata, radiokomppaniaksi yhdistetyt puhelinpaja, radiopaja ja tarvikevarastot sekä kolme erillistä erikoispuhelinjoukkuetta. VP 10 perustettiin 18.6.1941 hajautetusti ympäri Suomea. Pataljoonien osia toimi Helsingissä (Esikunta), Karjaalla, Keravalla, Porissa, Turussa, Hämeenlinnassa, Tampereella, Seinäjoella, Jyväskylässä, Äänekoskella, Pieksämäellä, Iisalmella, Lahdessa, Raahessa ja Haapamäellä. Pataljoonan komentajana toimi Kapteeni Honkasalo

Telian Kerhon puheenjohtaja Kimmo Fransila piti juhlaesitelmän käsitellen VP 10 perustamista ja jatkosodan aikaista toimintaa linkittäen sen tämän päivän valmius- ja varautumisvaatimuksiin.

Viestipataljoona 10 muistolaatan Helsingin postitalon kivijalkaan paljastivat Puolustusvoimien sotatalouspäällikkö kenraaliluutnantti Mikko Heiskanen ja VKL:n puheenjohtaja Jukka-Pekka Virtanen.

Viestipataljoona 10 oli Posti- ja telelaitoksen henkilöstöstä 18.6.1941 Päämajan johtoon hajautettuna ympäri Suomea perustettu erikoisviestipataljoona, jonka tehtävänä oli kiinteiden viestiyhteyksien ylläpito. Pataljoonan komentajana oli Kapteeni M Honkasalo.

TEKSTI JA KUVAT: SEPPO SIMOLA

Viestin joukko-osastotunnukset ovat lähes tyystin kadonneet

Ennen omia tunnuksia oli jopa komppaniaportaasta alkaen

Artikkeli luo katsauksen joukko-osastotunnusten historiaan erityisesti viestiaselajin näkökulmasta. Tarkastelu painottuu vuoden 1968 uudistuksen jälkeiseen aikaan vuosituhannen vaihteeseen asti. Vuoden 1984 Sotilas- ja virkapukumääräyksissä (SPVM) tunnusten määrä on ollut mahdollisesti runsaimmillaan. Nykyisin ainoa omaa joukko-osastotunnusta käyttävä organisaatio, joka edes etäisesti periytyy viestiaselajista, on Puolustusvoimien Johtamisjärjestelmäkeskus.

Idea joukko-osastotunnuksista esitettiin jo vuonna 1918 ja ensimmäiset sellaiset vahvistettiin seuraavana vuonna. Nykyisen malliset joukko-osastotunnukset – eli inttislangilla satiaiset – otettiin käyttöön vuonna 1968.Tunnusten määrää supistettiin merkittävästi 2000-luvulle tultaessa. Toki uusiakin merkkejä on tarvittaessa suunniteltu ja otettu käyttöön organisaatiomuutosten tai uusien joukkojen perustamisen myötä. Tunnuksista kertoessani käytän aikamuotona pääosin preesensiä, vaikka kirjoittaisin käytöstä poistuneista merkeistä.

Lisää merkkejä vuoden 1968 uudistuksessa

Ennen vuoden 1968 uudistusta aika harvalla joukko-osastolla oli oma tunnus. Yleensä käytettiin aselajin yleismerkkiä, kuten jalkaväen ristikkäisiä kivääreä tai jääkärijoukkojen polkupyörän etupyörän ja suksien muodostamaa tunnusta sekä näiden yhteydessä numero- tai kirjaintunnuksia.

Monen joukon numeroon perustuva nimi muutettiin vuonna 1957 maakunnalliseksi, jolloin esimerkiksi Jääkäripataljoona 4:stä tuli Hämeen jääkäripataljoona ja 1. Prikaatista Pohjan prikaati. Omia joukko-osastotunnuksia uudelleen nimetyt joukot saivat kuitenkin odottaa kymmenisen vuotta.

Tunnukset olkapäillä ja hihassa

Messinkisiä joukko-osastotunnuksia kannetaan perinteisesti sotilaspuvun olkapoleteissa. Niihin kiinnitettyinä tunnukset ovat edelleen maavoimien puvuissa m/58 ja m/83 sekä ilmavoimien puvuissa m/51 ja m/83. Uudeksi kantopaikaksi tuli maastopuku m/91:n myötä vasen hiha. Maastopuvun osalta poistui myös parillisuus, koska maastopuvussa tunnus on vain vasemmassa hihassa. Päällystakeissa joukko-osastotunnuksia ei enää käytetä, koska niiden perinteisellä paikalla eli olkapäillä pidetään monessa takkimallissa arvomerkkikaluunoita.

Vaikka nykyisten tunnusten vuonna 1968 alkanut perinne elää yhä, niin suuri määrä tunnuksia on poistettu käytöstä. Ne olivat ennen pataljoona- tai jopa komppaniakohtaisia, mutta nykyisin koko prikaatilla on usein sama joukko-osastotunnus – yleensä jonkin aiemman pataljoonan tunnus lehväseppeleen ympäröimänä. Tähän käytäntöön siirryttiin vuosituhannen vaihteessa.

Merkkejä sadan vuoden takaa

Esimerkiksi Panssariprikaatin nykyinen tunnus on johdettu Hyökkäysvaunurykmentin yli sadan vuoden takaisesta merkistä, jonka muodostavat koukistuneet haarniskoidut käsivarret välissään rihlatun tykinputken suu. Vuoden 1984 ohjesääntö selittää haarniskakäsien välissä olevan kuvion telapyöräksi, mutta alkuperäisessä HVR:n merkissä tykinputken suu hahmottuu selvästi, ja sellaiseksi se merkin selityksessäkin mainitaan.

Erillisen viestikomppanian tunnuksena oli viestin yleismerkki ja sen alla komppanian numero.

Viestikoulun ja Viestivarikon tunnuksissa viestin yleismerkin alapuolella oli kirjaintunnus.

Maakuntien mukaan nimetyillä joukko-osastoilla oli tunnuksessaan usein maakunnan vaakunaeläin, kuten Keski-Suomen viestipataljoonan metso ja Pohjois-Suomen viestipataljoonan kärppäryhmä.

PSPR:n tunnuksessa toistuu edellä mainittu kuva-aihe pienemmässä koossa ja lehväseppeleen ympäröimänä. Prikaatiin aiemmin kuuluneen Hämeen jääkäripataljoonan ilveksenpää ja jahtitorvi ovat jo siirtyneet historiaan pataljoonan mukana, ja sama kohtalo on ollut monella muullakin pataljoonalla tunnuksineen.

Noin sadan vuoden takaa periytyy tankkimiesten merkin ohella muutama muukin yhä käytössä oleva joukko-osastotunnus kuten Kadettikoulun ja Reserviupseerikoulun merkki. Molemmissa oli aluksi sellainen heraldinen kömmähdys, että ristikkäisten miekkojen terät osoittivat alaspäin. Virhe korjattiin pian, joten miekat alaspäin olevat tunnukset ovat jonkinasteisia keräilyharvinaisuuksia.

Myös Pääesikunnan tunnus on sinnitellyt läpi vuosikymmenten perinnemuutosten, ja nykyisin käytössä oleva Karjalan prikaatin tunnus on sellaisenaan perintöä Karjalan kaartin rykmentiltä.

Puku-uudistus vähensi tunnusten näkyvyyttä

Joukko-osastotunnusten vähenemisen ohella myös tilaisuudet käyttää tunnusta ovat harventuneet. Yksi harvennus oli puvun m/58 käytön lopettaminen juhlapukuna ja siirtyminen mustaan juhlapukuun m/87, jossa ei joukko-osastotunnuksia kanneta. Kun puvussa ei ole edes kauluslaattoja tai muuta aselajiin viittaavaa värielementtiä, niin sotilaan palveluspaikkaa on mahdoton päätellä, kun juhlapuvussa ei kanneta edes joukko-osastoristiä.

Puolustushaaroistakin erottaa vain merivoimat, koska maa- ja ilmavoimien juhlapuku m/87 on identtinen. Vain juhlapuvun lippalakin merkki kotkasymboleineen kertoo, että kyse on ilmavoimien sotilaasta. Lentäjän voi sentään juhlapuvussa tunnistaa pienoiskokoisesta lentomerkistä.

Eräänlainen heraldinen epäloogisuus on myös ilmavoimien lakkimerkissä. Sen kotkasymboli on nimittäin pakeneva, koska sen lentosuunta on kantajansa vartalon keskilinjasta poispäin.

Kömmähdyksiä sattuu joskus myös joukko-osastotunnuksia kannettaessa. Monet tunnuksista ovat immuuneja kätisyydelle – kuten edellä kuvattu tankkimiesten merkki, mutta erityisesti eläinsymbolit ovat joskus tuottaneet päänvaivaa. Olkapäällä tai hihassa kannettavan merkin kuva-aiheen – esimerkiksi leijonan – on katsottava eteenpäin. Tällöin tarvitaan oma merkki oikeaan ja vasempaan olkapäähän.

Joukko-osastotunnusten yleisin materiaali on ollut ja on yhä messinki, mutta pari poikkeustakin historia tuntee. Joukko-osastotunnuksia ommeltiin eli brodeerattiin sarkapohjalle, joka taitettiin olkapoletin ympärille. Näitä näki erityisesti varusmiehillä ennen sotia. Joskus merkkejä myös maalattiin sarkapohjalle keltaisella maalilla sapluunan avulla. Sota-aikana tunnuksia puolestaan stanssattiin messingin sijasta harmaasta korvikemetallista. Varhaisimmat merkit olivat valettuja.

Viestijoukoilla jopa komppaniakohtainen tunnus

Viestijoukoissa on ollut oma joukko-osastotunnus jopa komppaniaportaassa. Kukin erillinen viestikomppania käytti vuoden 1984 ohjesäännön mukaan viestin yleistunnusta eli kahta toisiinsa yhdistynyttä salamaa ja sen alla komppanian numeroa.

Erillisiä viestikomppanioita on ollut kaikkiaan viisi. Viides erillinen viestikomppania tosin ehti toimia vain vuosina 1967–1976. Panssariprikaatin viestikomppania (myöhempi Panssariviestikomppania) sekä Panssariviestipataljoona käyttivät edellä kuvattua Panssariprikaatin tunnusta.

Valtakunnan Puolustusvoimien virkapukuohjesääntö eli V.P.O. vuodelta 1930 tuntee kuvaliitteessään Viestipataljoona 1:n ja 2:n sekä erillisen viestikomppanian tunnuksen. Näiden lisäksi ohjesäännössä on teknillisten sekä viesti- ja huoltojoukkoien yhteinen merkki, jossa esiintyvät myös viestin salamat. Ratsuväkeen kuuluneen Viestieskadroonan merkissä on ratsuväen ristikkäiset sapelit ja niiden alla V-kirjain.

Maakuntavaakunoita ja numerotunnuksia

SVPM määrittelee Viestirykmentin tunnukseksi pystyssä olevan miekan päällikkeenään kaksi toisiinsa yhdistettyä salamaa. Rykmentti perustettiin Viipurissa 1938, ja seuraavana vuonna viesti sai itsenäisen aselajin statuksen. Siihen asti se oli osa teknillisiä joukkoja.

Keski-Suomen viestipataljoonan merkissä on SVPM:n mukaan kaksi toisiinsa yhdistettyä salamaa, joiden yläpuolella on Keski-Suomen vaakunan soidinmetso. Pohjois-Suomen viestipataljoonan tun-

Sota-aikana joukko-osastotunnuksia tehtiin säästösyistä korvikemetallista, kuten oikeanpuoleinen Viestirykmentin merkki kertoo.

Vasemmalla on Viestirykmentin tunnus sekä keskellä Sähköteknillisen koulun ja Elektroniikkakeskuskorjaamon yhteinen tunnus. Oikeanpuolimmaista merkkiä käyttivät useat erilliset sotilaslaitokset. Viestijoukkoihin niistä viittasivat Viestikeskuskorjaamo ja Sähköteknillinen tutkimuslaitos.

Ilmavoimiltakin löytyy viestiin viittaavia joukko-osastotunnuksia kuten Ilmavoimien viestikoulun (vas.) ja Ilmavoimien viestivarikon (oik.) merkki.

nuksena ovat tutut salamat, mutta niiden päällikkeenä on kolme juoksevaa kärppää Pohjois-Pohjanmaan vaakunasta.

Numeron liittäminen viestikomppanian tunnukseen käskettiin jo vuonna 1948 edellisen merkkisukupolven aikana. Tunnuksena oli tuolloin pystyssä oleva miekka päällikkeenään poikittainen puhelimen kuulotorvi sekä ristikkäiset salamat. Silloin kun oli vain yksi erillinen viestikomppania, se merkittiin lisäämällä viestin tunnuksen alle E-kirjain.

Muita viestiin viittaavia joukko-osastotunnuksia

Viestikoulun merkki on SVPM:ssä samanlainen kuin erillisillä viestikomppanioilla, mutta numeron paikalla on K-kirjain. Viestivarikon tunnuksessa on salamoiden alla V-kirjain. Sähköteknillisen koulun merkin muodostaa pystyssä oleva miekka päällikkeenään kolmipolvekkeinen salama. Sama merkki tuli myös Elektroniikkakeskuskorjaamolle. Vuonna 2003 Sähköteknillisen koulun tunnuksen alapuolelle lisättiin K-kirjain samalla kun tunnus perusmuodossaan jäi Elektroniikkakeskuskorjaamolle.

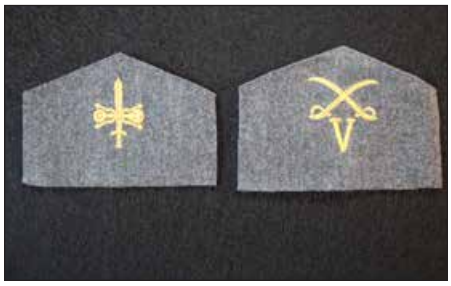
Viestiin viittaavia joukko-osastoja tai laitoksia SVPM tuntee myös Viestikeskuskorjaamon sekä Sähköteknillisen tutkimuslaitoksen. Kummankin tunnuksena on pystyssä oleva miekka päällikkeenään leijonakoristeinen kilpi. Samaa tunnusta käytti moni muukin sotilaslaitos, kuten ohjesäännön termi kuuluu.

Joskus jatkumot joukko-osastojen tai sotilaslaitosten nimissä on vaikea hahmottaa, koska nimiä aika ajoin päivitetään terminologian nykyaikaistuessa tai organisaatiomuutosten yhteydessä. Esimerkiksi Viestikeskuskorjaamo muuttui Elektroniikkakeskuskorjaamoksi, ja vuonna 1949 perustettu Ilmavoimien esikunnan tutkakorjaamo muuttui monien vaiheiden kautta Sähköteknilliseksi kouluksi.

Viestin tunnuksia Ilmavoimilla ja Sotakoirakoululla

Ilmavoimien viestikoulun tunnuksessa toistuu maavoimista tuttu salamapari, mutta siipiparin välissä. Aiempi symboli oli vanha Radiopataljoonan merkki määritykseltään kaksikärkisen salaman nuoli. Välillä joukko-osaston nimi oli Ilmavoimien viestipataljoona.

Sotakoirakoulun vanhaa tunnusta voisi äkkipäätä luulla viestikoulun



Joukko-osastotunnuksia valmistettiin 1920- ja 1930-luvuilla sarkapohjalle brodeeraamalla. Esimerkkeinä tästä ovat ohessa Viestirykmentin sekä Viestieskadroonan tunnukset. Tunnuksia valmistettiin myös maalaamalla sapluunan avulla.

Sotakoirakoulun tunnus on johdettu viestijoukkojen merkistä. Sotakoirakoulutus nimittäin aloitettiin vuonna 1924 Kenttälennätinpataljoonassa.

Nykyisin ainoa omaa joukko-osastotunnusta käyttävä joukko, joka edes jotenkin periytyy viestiaselajista, on Puolustusvoimien Johtamisjärjestelmäkeskus.

Vuoden 1930 V.P.O.:ssa teknillisillä, viesti- ja huoltojoukoilla oli yhteinen aselajitunnus, jossa miekka on vaakasuorassa. Kuva on V.P.O:n liitteestä.

tunnukseksi, koska siinä on Viestirykmentin tunnuksen alla K-kirjain. Sotakoirakoulun tunnuksen johtaminen viestiaselajin merkistä on loogista, koska sotakoirakoulutus aloitettiin vuonna 1924 Kenttälennätinpataljoonassa, ja sotakoiria käytettiin viestikoirina.

Lähteitä:

Valtakunnan Puolustusvoimien virkapukuohjesääntö V.P.O. (1930)

Sotilas- ja virkapukumääräykset SVPM (1984)

Sotilas- ja virkapukuohjesääntö (1991)

Kari K. Laurla: Sotilasheraldiikka – Liput, merkit ja tunnukset (2.p 2003)

Marko Palokangas: Puolustusvoimat – Joukko-osastoperinteet (2008)

Markku Palokangas: Puolustusvoimat – Entiset joukko-osastot (2013)

TEKSTI: JYRKI PENTTINEN

Telealan uutisia

Mobiilipohjainen satelliittiviestintä kehittyy

3GPP (3rd Generation Partnership Project) on viime aikoina luonut teknisiä spesifikaatioita liittyen matkaviestintäverkkojen satelliittikomponenttiin mahdollistaen entistä kehittyneempiä menetelmiä myös laajojen alueiden mobiiliviestintään.[1] 3GPP-mallit sisältävät satelliittien toistinkomponentin sekä satelliittiin asennettavan tukiaseman. Satelliittiyhteydet avaavat uusia mahdollisuuksia loppukäyttäjien hyötyessä paremmasta radiopeittoalueesta myös merialueilla ja vaikeasti teleinfraa sisältävillä seuduilla samalla, kun ne auttavat luomaan uusia liiketoimintamalleja yhteistyössä perinteisten matkaviestintäoperaattoreiden ja satelliittioperaattoreiden kanssa. 3GPP kutsuu tekniikkaa nimellä ei-maanpäällinen verkko (non-terrestrial network, NTN).

Tämän kehityksen tekee erityisen mielenkiintoiseksi se, että yhteys maanpäällisten verkkojen ja satelliittiverkkojen kautta voidaan luoda käyttäen yhteistä verkkoalustaa ja kaupallisia kännyköitä. NTN-ekosysteemi mahdollistaa siten täysin uusien palveluiden maailmanlaajuisen käytön niin yksityisten tilaajien kuin yritysten tarpeisiin.

Vaikka satelliittiviestintä on perinteisesti ollut eräällä tavalla suljetumman ekosysteemin toimintaa, yhteensopivien standardien merkitys on kasvamassa. Yhtenä konkreettisista esimerkeistä tästä kehityksestä on Iridiumin hiljattainen päätös hylätä laitevalmistajakohtainen ratkaisunsa, jota se kehitti Qualcommin kanssa. Sen sijaan Iridium päätti ottaa käyttöön 3GPP-spesifikaatioihin perustuvan yhteysmenetelmän, joka käyttää kaupallisten 5G-matkavistinten radiorajapintaa matalan satelliittikonstellaationsa yhteyksiin. [2] Hyödyt ovat ilmeiset laajan laitemarkkinan ja sitä myötä hintakilpailun kautta. Iridium aikoo ottaa palvelun käyttöön tavallisten ja hätäviestien välitykseen vuonna 2026 perustuen 66 satelliitin settiinsä.

Maanpuolustuksen näkökulmasta, kuten uutiset Ukrainan kenttätaisteluista osoittavat, satelliittipohjainen viestiliikenne on tärkeässä asemassa tilannekuvan välittämiseen yhtä lailla kuin droonien komento- ja ohjauskommunikointiin (C2, command and control). SpaceX:n operoima Starlink on toiminut alueella käytännöllisenä datanvälitysratkaisuna maanpäällisten verkkojen infrastruktuurin ollessa haavoittuva. Mielenkiintoisena yksityiskohtana Starlink on jo kokeillut ensimmäisiä suoria satelliittien ja 5G-matkaviestinten (direct to cell) yhteyksiä vuoden alussa. SpaceX on tammikuussa laukaissut kuusi uutta satelliittia, jotka pystyvät kytkemään modifioimattomat mobiililaitteet suoralla satelliittilinkillä tekstiviestien välitykseen.[3]

Wi-Fi -verkot kehittyvät

IEEE 801 -pohjaiset langattomat WLAN (wireless local area network) verkot ovat olleet kustannustehokas ratkaisu kotien, toimistojen ja julkisten paikkojen Internet-yhteyksiin jo vuosikymmenten ajan. IEEE 802.11ax määrittää suositun Wi-Fi 6 -variantin, ja Wi-Fi Alliance on nyt aloittanut sertifioinnin myös uusimman määrityksen Wi-Fi 7:n laitteille. Wi-Fi 7 on tällä hetkellä langattoman viestinnän kehittynein versio, ja sen tyyppihyväksynnän referenssinä toimii Wi-Fi Certified 7 takaamaan laitteiden yhteensopivuuden mukaan lukien matkaviestimet, läppärit ja kiinteästi asennettavat pääsypisteet. Wi-Fi 7 parantaa edellisten Wi-Fi -varianttien suorituskykyä ja kapasiteettia, ja mahdollistaa uusia toimintoja eri käyttöympäristöissä palvellen esimerkiksi virtuaalitodellisuuden sovelluksia aiempaa jouhevammin.

IEEE 802.11be määrittää Wi-Fi 7:n tekniikan. Se on yhteensopiva Wi-Fi 6:n 6 GHz:n radiotaajuuden kanssa laajentaen sen kaistaa 320 MHz:iin saakka. Uusi tekniikka mahdollistaa toimintapeittoalueellaan huippunopean datan perustuen 4096-QAM:iin ja 16:een spatiaaliseen striimiin.

Wi-Fi 7:lle odotetaan merkittävää markkina-asema siten, että tämän vuoden aikana laitteita olisi 233 miljoonaa ja vuonna 2028 yli kaksi miljardia. 3GPP:n 5G-verkkospesifikaatiot sallivat Wi-Fi -pääsypisteiden integroinnin rinnakkain 5G-tukiasemien kanssa siten, että 5G-kytkentäverkko huolehtii käyttäjien tunnistuksesta ja radiorajapinnan suojauksesta. Tämä periaate toimii myös uusille Wi-Fi 7 -varianteille.[4]

Paikannuspalvelut maanpuolustuksessa

Langattoman viestinnän laitteiden paikannus on tärkeässä osassa esimerkiksi mobiililaitteisiin perustuvassa navigoinnissa. Matkaviestintälaitteiden integroidessa useita palveluita ja ratkaisuja samoihin kuoriin, ml. GPS:n, kehitys on ollut perustavanlaatuinen, sillä erillislaitteisiin perustuva navigointi on käytännössä romahtanut. Monenlaisten sovellusten yleistyessä mobiilipaikannusmenetelmät tarjoavat niiden oheen yhä tarkempaa paikannustietoa. Nykyiset 3GPP-spesifikaatiot mahdollistavat useita tekniikoita yhdistellen satelliitti- ja matkaviestintäverkkojen toimintoja. Esimerkiksi 5G-järjestelmä määrittää paikannukseen liittyvän verkkotoiminnon (location management function, LMF), joka sisältää aiemmista matkaviestintäsukupolvien paikannuspalveluista edelleen kehitettyjä ja lisäominaisuuksia. Samalla paikannukseen liittyvät haittapuolet ovat myös yleistyneet, ja nykyiset hyökkäysvektorit liittyvät osaltaan matkaviestinnän käyttäjien sijaintitietoon.

Maanpuolustuksen näkökulmasta asia on kahtiajakoinen; toisaalta tilannetiedon yhteyteen saadaan matkaviestinnän tekniikoilla oleellinen paikannus esimerkiksi helpottamaan pelastustoimia, mutta samalla vihollinen voi yrittää selvittää tilannekuvaa haitallisten aikeidensa toteutukseen. Perustuen käytännön kokemuksiin Ukrainassa, ENEA:n hiljattain julkaistu raportti koostaa konkreettisia taistelukentän mobiililaitteiden paikannukseen liittyviä paikannustyyppejä jaotellen ne

radion, verkon ja laitteiden mahdollistamiin menetelmiin. [5]

Radioon perustuvat menetelmät sisältävät perinteisen *passiivisen RF-suuntimisen* perustuen rajoitettuun vastaanottoon silloin kun kohde lähettää tietoa, *aktiivisen suuntimisen* perustuen siihen, että signaloimalla matkaviestin voidaan pyytää lähettämään paikannustieto sekä esimerkiksi SIM- ja laitteen tyyppinumero, sekä paikannustiedon pyyntöön *radioverkkojen kautta*. Näistä jälkimmäinen on kaikkein monimutkaisin menetelmä ja siihen sovellettava käytännön tekniikka riippuu matkaviestintäverkon sukupolvesta. Perusperiaatteena 2G- ja 3G-verkoissa on se, että erillislaite, joka toimii IMSI-kaappaajana (IMSI cather) voi lähettää myös erityisiä radiomittauskäskyjä seurattaville mobiililaitteille. Sovellettaessa matemaattisia menetelmiä ja useita mittauspisteitä, voidaan matkaviestimen paikka selvittää.

4G-järjestelmässä vastaavia radiomittauskomentoja voidaan saada passiivisesti matkaviestien paikannukseen siten, että signalointi on 4G:n tapauksessa suojaamatonta. Lisäksi 4G-järjestelmässä on menetelmä pyytää matkaviestimeltä signaalinvoimakkuustieto sekä GPS-dataa, mikä helpottaa tarkassa paikannuksessa.

ENEA:n raportti päättelee, että Ukrainassa on näistä mahdollisesti käytetty 2G/3G-järjestelmien haavoittuvuuksia, mutta on epäselvää, onko 4G:n paikannuksen suojauksen heikkouksia käytetty hyväksi.

Raportissa on varsin yksityiskohtaisia pohdintoja monesta matkaviestintään liittyvästä näkökulmasta taistelukentällä ja yhtenä yleissuosituksena se, että kaupallisia älypuhelimia olisi syytä välttää taistelualueilla. Käytännönläheisenä ja selkolukuisena raportti on suositeltavaa luettavaa kaikille asiasta kiinnostuneille.

Lähteet

[1] Using 3GPP technology for satellite communication. Ericsson, 1.6.2023. https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/3gpp-satellite-communication

[2] Iridium pivots to standardized direct-to-device satellite services. Spacenews, 10.1.2024. https://spacenews.com/iridium-pivots-to-standardized-direct-to-device-satellite-services/

[3] SpaceX exchanges first texts using its ‘Direct to Cell’ satellites. Telecoms Tech News, 11.1.2024. https://www.telecomstechnews.com/news/2024/jan/11/spacex-exchanges-first-texts-direct-to-cell-satellites/

[4] Wi-Fi CERTIFIED 7. https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-7

[5] Tracking on the battlefield. ENEA, tammikuu 2024. https://www.enea.com/insights/location-tracking-on-battlefield/

Vakiopalstan kirjoittaja, TkT, tietokirjailija Jyrki Penttinen toimii telealan konsulttitehtävissä Yhdysvalloissa. Voit lähettää Jyrkille kysymyksiä tietoliikennetekniikasta LinkedIn:n kautta www.linkedin.com/in/jypen.

Uusi HF-SSB sotilasviestilaitteiden sukupolvi

HF-radioyhteyksille on yhä edelleenkin hyödyllistä käyttöä. Viimeisimmät saavutukset yksisivunauhalaitteiden kehityksessä ovat kannettavan, ajoneuvossa kuljetettavan ja kiinteän radioaseman muunnokset, joissa on käytetty hyödyksi mikroelektroniikan tuoreimpia saavutuksia. Laitteiden käyttäjät voivat olla ammattitaidoltaan kenttähenkilökunnasta alkaen aina kiinteiden asemien kokeneisiin radioviestittäjiin.

Johdanto

Kannettavaa HF-SSB lähetinvastaanotinta, jota äskettäin valmistettiin Ranskan Armeijalle, on kuvattu jo aikaisemmin (1). Tämä ranskalaista suunnittelua oleva lähetinvastaanotin kehitettiin vuosina 1960–1968 Le Materiel Telephonique´ssa, ranskalaisessa ITT:n tytäryhtiössä. Jatkuva tämän alan kehittäminen, jossa käytetään mikroelektroniikkaa hyödyksi, on tuonut tuloksena uuden HF-SSB laitteiden sukupolven täysin digitaalisine taajuussyntetisoijineen. Tämä uusi laitesukupolvi eroaa aikaisemmista koon, sähkön kulutuksen ja mekaanisen monimutkaisuuden osalta. Nämä kaikki ominaisuudet ovat merkittävästi parantuneet, joten laitteesta on saatu taloudellinen ja luotettava.

Sovellutukset

Uudenaikaisilla, hyvin vakavia syntetisoijia käyttävillä HF-SSB -yhteyksillä on erityisasema varmoina sotilassovellutuksina vihollisuuksien aikana. Verrattuna VHF-yhteyksiin näillä on eräitä epäkohtia kuten interferenssi, kookkaat antennit, hankala virittäminen, suurempi paino, monimutkaisuus, rajoitettu nauhaleveys ja suurempi yksikköhinta. Alle 20 km:n yhteysväleille silloin, kun maaston laatu ei tuota hankaluuksia, ovat taajuusmoduloidut VHF-lähetinvastaanottimet eniten käytettyjä laitteita myös sotilassovellutuksissa.

Kuitenkin kahdessa sotilaallisessa tilanteessa HF-yhteyksistä on erityistä etua. Ensinnäkin vuorimaastossa, jossa HF-taajuuksilla saadaan aikaan vähemmällä teholla pidemmät kantamat kuin VHF-taajuuksilla. Avoimien vihollisuuksien tai sissitoiminnan aikana HF-yhteydet tarjoavat ainoan varman keinon saada radioyhteys eristettyjen joukkojen ja tukialueen välille. Rauhan aikana, kun muitakin keinoja on käytettävissä, sotavoimat voivat syrjiä HF-yhteyksiä, mutta sodan aikana haavoittumattomien yhteyksien ollessa elintärkeitä näitä tarvitaan.

Tekniset ominaisuudet

Tämän uuden sukupolven HF-lähetinvastaanottimen eri sovellutusten tekniset ominaisuudet ovat yhtäläiset. Sekoitusperiaate kaksine välitaajuuksineen takaa erinomaisen suorituskyvyn. Vastaanottimen sisäänmeno- ja lähettimen ulostulopiirit ovat laajakaistaisia, työskentelytaajuus määrätään yksinomaan taajuussyntetisoijalla. Tämä yksinkertaisuus on ollut mahdollista uuden taajuuden vaihtotekniikan ja taajuussyntetisoijan spektrin laadun avulla.

Vastaanottimen sisääntulopiirien erikoispiirteitä

Aina näihin päiviin saakka on hyvän vastanottimen ensimmäistä taajuuden muutosta edeltävät piirit olleet perinteisesti hyvin valintatarkkoja ja jonkin verran vahvistavia. Kohina- ja lineaarisuusominaisuudet eivät ole olleet erityisen hyviä. On osoitettu, että valintatarkkojen sisääntulopiirien automaattinen viritys voidaan aikaansaada elektronisesti, mutta tällä tavoin saatu valintatarkkuus on lisännyt merkittävästi laitteen hintaa. Uusimmat menetelmät suosivat vähäkohinaisia sekoittajia, vähäisiä sekotushäviöitä ja erittäin hyvää lineaarisuutta jopa suurilla sisääntulotasoilla. Näillä menetelmillä voidaan valinta suorittaa tarkasti pelkästään välitaajuuksilla käyttämällä tehokkaita kidesuotimia.

Todellisuudessa uudenaikaisten laajakaistaisten sekoittajien menestymistä rajoittaa taajuussyntetisoijan ulostulosignaalin spektrin laatu, jota täytyy tarkastella hyvin huolellisesti tältä kannalta. Vastaanottimen muut piirit eivät sisällä mitään erityistä teknistä uudistusta. Ne on suunniteltu huolellisesti hyvän suorituskyvyn saavuttamiseksi antamaan parhaan eri asteisiin jakautuvan vahvistuksen valintakykyä ja dynaamista aluetta vastaavasti.

Laitetyypit

Kannettava laite (tyyppi 3451)

Kannettava laite on koko yhteysjärjestelmän ydin. Siihen kuuluu vastaanotin, syntetisoija ja 15 watin tehoinen lähetin sekä kaikki suoja- ja tehonkulutuksen säätölaitteet. Kannettavaa laitetta käytetään tavallisesti maassa 3–5 metrisen piiska-antennin ja vastapainon kanssa. Tämä on erittäin tehokas ja kantama ulottuu 40 km:iin. Laite voidaan asentaa käyttökuntoon muutamassa minuutissa ja lämpötilatasattu kideoskillaattori on heti valmis lähetykseen tai vastaanottoon valitulla taajuudella. Kun akku on täysin varattu, voidaan laitetta käyttää odotusasennossa 24 tuntia, vastaanotolla 6 tuntia ja puolituntia lähetyksellä.

Ajoneuvoasema

Peruslaitetta (tyyppi 3451) voidaan käyttää useiden ajoneuvoihin tai laivoihin tarkoitettujen versioiden perusosa-

na sopivien lisävarusteiden kera. Yksinkertaisin ajoneuvoversio on tarkoitettu keveitä ajoneuvoja varten (esim. maastoauto). Tarvittaessa lähetinvastaanotin 3451 ja lineaarinen vahvistin 3492 voidaan varustaa täydellä kauko-ohjauksella. Tällöin laitteiden etupaneelissa ei ole säätimiä, vaan ne kaikki on asennettu perusyksikön kokoiseen ohjausyksikköön.

Kiinteät asemat

Edellä käsitellyt sotilaslaitteet ovat tarkoitetut vaikeisiin ympäristöolosuhteisiin kokemattomille käyttäjille. Ne ovat tarvittaessa täysin vesitiiviitä, kannettava perusosa on erittäin pienikokoinen. Kaikki nämä ominaisuudet tekevät laitteista kalliita kiinteään tai puolikiinteään käyttöön, missä ympäristö- ja käyttöolosuhteet ovat paremmat. Kun sotilasversioiden suunnittelua ja neljän vuoden käyttökokeiluja voitiin käyttää apuna, oli kohtalaisen helppoa muuntaa laitteet kiinteisiin verkkoihin sopiviksi sekä saada erittäin edullinen hinta/suorituskyky-suhde.

Lopuksi

Tämä viestilaitteiden uusi sukupolvi on suunniteltu tyydyttämään sekä kansalliset että vientitarpeet ja vastaamaan ei vain yhden, vaan useimpien käyttäjien tarpeita. Tämä on johtanut suuren versio- ja lisälaitemäärän kehittämiseen. Nämä on testattu useissa maissa näytöksissä tai käyttökokeiluissa.

50 vuotta sitten -palstan kirjoittaja: Pasi Puhakka

Alun perin julkaistu Electrical Communication -lehdessä (Volume 48, Number 3, 1971), jonka jälkeen Viestimies-lehdessä käännöksenä.

Alkuperäiset kirjoittajat J. Lismaque, J. L. Ribour (Le Materiel Telephonigue, Paris).

KUTSU VIESTIUPSEERIYHDISTYS RY:N KEVÄTKOKOUKSEEN

Viestiupseeriyhdistys ry:n hallitus kutsuu yhdistyksen jäsenet kevätkokoukseen Espooseen, Nokian tiloihin, torstaina 25.4.2024 klo 14.00 alkaen.

Käyntiosoite: Karakaari 7, 02610 Espoo

Kokouksessa käsitellään sääntöjen 5 §:ssä kevätkokouksessa käsiteltäväksi mainitut asiat:

1) valitaan kokoukselle puheenjohtaja
2) valitaan kokouksen sihteeri
3) valitaan kaksi pöytäkirjan tarkastajaa ja ääntenlaskijaa
4) todetaan kokouksen laillisuus ja päätösvaltaisuus
5) päätetään kokouksen työjärjestys
6) käsitellään yhdistyksen toimintakertomus ja tilinpäätös
7) käsitellään toiminnantarkastajan kertomus
8) päätetään toimintakertomuksen ja tilinpäätöksen vahvistamisesta
9) päätetään hallituksen vastuuvapaudesta
10) muut asiat

Päivän ohjelma:

Saapuminen Nokian tiloihin klo 14.00 mennessä

Kahvit klo 14.00-14.30

Kevätkokous klo 14.30-15.30

Nokian ja sen toimintojen esittely 15.30-17.00

Tilaisuuden päättäminen noin klo 17.00.

Kuljetusta ei järjestetä yhteisesti. Julkisilla pääsee Karaporttiin esimerkiksi Keran asemalle junalla, josta n 900 m kävellen tai busseilla Pasilan asemalta.

Pysäköintimahdollisuus omalle autolle on rakennuksen edessä ja läheisyydessä.

Ilmoittautumiset 10.4.2024 mennessä www.viestiupseeriyhdistys.fi -sivuilla olevalla lomakkeella (toivottavin tapa), sähköpostitse toiminnanjohtaja@viestiupseeriyhdistys.fi tai puhelimitse 040 514 2497.

Tervetuloa kevätkokoukseen!

Viestiupseeriyhdistys ry:n hallitus

VIESTIUPSEERIYHDISTYKSEN JÄSENMATKALLE BRYSSELIIN

Viestiupseeriyhdistys järjestää jäsenmatkan Brysseliin 3.10. - 6.10.2024. Matkan tarkoituksena on tutustua Suomen EU- ja NATO-jäsenyyden keskeisiin toimijoihin. Matkalla vieraillaan myös alueen kulttuurikohteissa. Jos olet kiinnostunut, niin varaa ajankohta jo kalenteriisi.

Matkan pääpiirteinen aikataulu on seuraava:

To 3.10. Lento Brysseliin ja majoittuminen

Pe 4.10. – La 5.10. Tutustumiset EU- ja NATO-kohteisiin sekä erikseen valittuihin kulttuurikohteisiin

Su 6.10. Paluulento Suomeen

Tilaisuuden tarkempi ohjelma, ohjeet ilmoittautumisesta ja matkan hinta julkaistaan maaliskuun aikana yhdistyksen verkkosivuilla ja jäsenille lähetettävällä sähköpostiviestillä.

Lopullinen ohjelma sekä muut tarkemmat tiedot ja ohjeet lähetetään sähköpostilla matkalle ilmoittautuneille elokuun aikana.

Matka järjestetään, kun vähintään kaksikymmentä (20) henkilöä ilmoittautuu mukaan.

Yhteyshenkilönä toimii toiminnanjohtaja Harri Reini,
toiminnanjohtaja@viestiupseeriyhdistys.fi tai +358 40 514 2497

Varaa aika jo kalenteriisi!

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