Viestimies

Viestiupseeriyhdistyksen julkaisu 81. vsk Numero 1 Kevät 2026

Johtamisjärjestelmäala ja kyberpuolustus puolustusvoimien johtamisen tukena, sivu 9

Pohjoisen operointisuunnan johtamisen vahvistaja: DCM-yksikön rakentaminen Suomeen, sivu 15

Kyberpelotteen haasteet ja mahdollisuudet, sivu 18

www.viestiupseeriyhdistys.fi


COMBITECH
Yhteistyötä yli rajojen
Kumppanisi kansainvälistyvässä puolustuksessa niin pohjoismaissa kuin NATO:ssa.
www.combitech.fi

Viestimies-lehti

Päätoimittaja
Kimmo Kaipainen
p 040 7222646
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Outi Tuisku
henkilotoimittaja@viestiupseeriyhdistys.fi

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

Toimituskunta
Vähätiitto Jarmo (pj)
Blomqvist Reima
Hyvärinen Pertti
Isomäki Pekka
Nyqvist Antti
Pellikka Jarkko
Puhakka Pasi
Sipilä Olli
Suokko Harri
Tunkkari Antti

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: Puolustusvoimat.

Tässä numerossa

4 Pääkirjoitus: Viestimies-lehti 80 vuotta.

8 2.pääkirjoitus: Juhlavuodesta aktiiviseen arkeen.

9 Johtamisjärjestelmäala ja kyberpuolustus puolustusvoimien johtamisen tukena

15 Pohjoisen operointisuunnan johtamisen vahvistaja: DCM-yksikön rakentaminen Suomeen

18 Kyberpelotteen haasteet ja mahdollisuudet

23 Datakeskeinen ja algoritminen sodankäynti
– katsaus johtamisjärjestelmien kehitykseen länsimaissa

28 ISAC: Kehittynyttä sensorointia

32 Define accelerator
-kiihdyttämöohjelma kaksikäyttöratkaisujen edistäjänä

37 Viestikiltojen Liiton strategia 2030
– jotain uutta ja jotain vanhaa

41 Tutkimusta, julkaisuja, näyttelyitä, esitelmiä jopa elokuvia
– tutkimuksella sotahistoriaa tutuksi

43 Viestiupseeriyhdistyksen kevätkokouskutsu

44 Ilmoitus Viestiupseeriyhdistyksen jäsenmatkasta

44 Puolustusvoimien johtamisjärjestelmäkeskuksen johtajat tapasivat

45 Viestiupseeriyhdistys 80 vuotta -juhlaottelu

46 Telealan uutisia

47 Viestimies 50 vuotta sitten

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

Mukana lehdessä
–
Mukana päätöksiä tehdessä!

Seuraavan numeron aineistopäivä on 24.4.2026. Lehti ilmestyy viikolla 23.

Viestimies-lehti 80 vuotta

Mukavaa alkanutta vuotta lehtemme lukijoille. Juuri kun olemme toipuneet Viestiupseeriyhdistyksen 80-vuotisjuhlien humusta, on jälkeen tarjolla uutta juhlan aihetta, sillä myös Viestimies-lehti saavuttaa kunniakkaan 80 vuoden iän. Juhlavuotta tullaan muistamaan lehden sivuilla vuoden mittaan erilaisilla tavoilla. Näin juhlavuoden aluksi on mielestäni paikallaan heittäytyä hetkeksi ensimmäisen numeron tunnelmiin tutustumalla ensimmäisen lehden pääkirjoitukseen.

Kansikuvamme on luutnantti Uusipaikan ehdotus Viestiupseerikerhon merkiksi. Ko. merkkiajatus on mielestämme sangen kannatettava, sillä olisihan se tunnusmerkkinä siviilipuvussa esiintyvien jäsenten kesken. Mikäli ajatus hyväksytään lukijoiden keskuudessa, niin pyydämme lähettämään luonnoksia ja arvosteluja niistä. Tarkoitus on nimittäin julkaista ne näin kansikuvina.

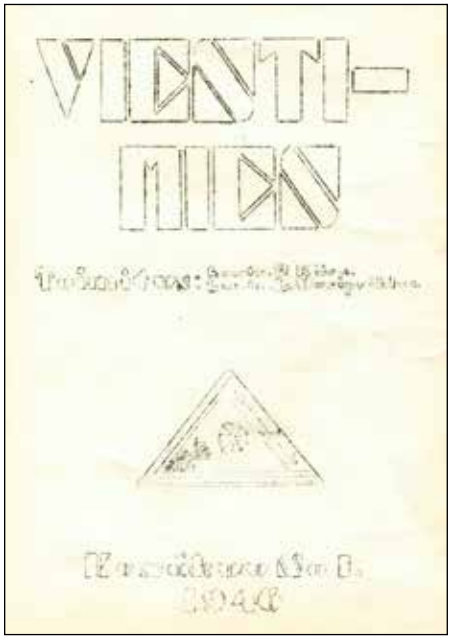
Viimeinkin on saatu "Viestimies" hengittämään. "Alku aina hankalaa, mutta lopuksi - -" pitää tässäkin täysin paikkansa. Pula on ollut paperista, rahasta, vahoista ja kaikesta muusta paitsi hyvästä tahdosta. Sitä on Luojan kiitos näin pula-aikanakin vielä ollut vapaassa kaupassa. Luotamme arv. lukijoiden hyväntahtoisuuteen arvostellessaan tätä tekelettä. Tämähän onkin vain näytenumero ja sen tarkoitus on vain kokouksessa tehtyjen hyvien päätösten toteuttaminen. Kuten tiedetään on päätösten teko ja niiden toteuttaminen kaksi aivan eri asiaa, eli kuten naisväki sanoo: "Lupaaminen ja täyttäminen on eri juttu".

Tehtyjen päätösten mukaan on kerhon julkaisutoiminnan tarkoituksena pitää yhteyttä eri aselajien ja reservissä olevien viestimiesten kesken. Tämä on nykyään melkoisen vaikeaa. Syyt siihen ovat hyvin monet,kuten jokainen lukija hyvin tietää. Ellei tiedä niin ajatelkoon Itsensä lehden toimittajaksi ilman kirjallisia ominaisuuksia, aputoimittajia ja valmiita kirjoituksia.

Niistä kaikista kuitenkin aiotaan selviytyä ennenkaikkea lukijoitten avulla. Tarkoitus on nimittäin kehittää tilausmaksujen avulla julkaisusta oikea lehti, jossa jokainen lukija on sekä toimittaja että kannatusvoima taloudellisessa mielessä. Tämän vuoden aikana julkaistaan neljä numeroa, jonka saa tilata 75:- valtion inflaatiorahalla ja johon jokaiselta toivotaan tai oikeastaan jokainen velvoitetaan kirjoittamaan kirjoituksia. Siis arvoisat Herrat: lähettäkää kirjoituksia! Ei ole väliä, mitä, kunhan vaan on jotain, jonka voi näin kaikille julkituoda. Lähettäkää myöskin osoitteita henkilöistä, jotka voivat ilman kirjoituspalkkiota kirjoittaa teknillisistä aiheista, sillä Toimitus ei pysty itse sellaisia pykäämään. Erikoisesti vetoomuksemme on tarkoitettu meri- ja ilmaherroille. Me maavoimissa olevat pidämme itseämme ainoina oikeina viestimiehinä ja unohdamme sen tärkeän tosiseikan, että merellä ja ilmassa tarvitaan miehiä, jotka ovat viestimiehiä aivan yhtähyvin kuin mekin. Että tämä suhde selvenisi on sieltä päin tultava usein muistutuksia.

Viestimiesterveisin, Riihimäellä 1.6.46

Toimitus



Pääkirjoituksen sanoma tuntuu edelleen monilta osin paikkaansa pitävältä, ainakin näin päätoimittajan silmin.

Erinomaisen menestyksekästä alkuvuotta toivottaen,

Kimmo Kaipainen

Päätoimittaja


EMPOWERING THE BEST
TO ALWAYS DO THEIR BEST
SAVOX
www.savox.com

Ukrainan sodan opit

Jo neljä vuotta jatkunut Venäjän laiton hyökkäyssota Ukrainaa vastaan on saanut useat maat arvioimaan uudelleen kyvykkyyksiään vastata tämän päivän turvallisuusuhkiin, myös niistä pahimpiin. Viestiupseeriyhdistys järjestää seminaarin tarkastelemaan Ukrainan sodasta saatuja oppeja ja niiden vaikutuksia johtamisjärjestelmiemme sekä kyber- ja informaatiopuolustuksemme järjestelyihin. Seminaari järjestetään **Helsingin yliopiston päärakennuksessa** (Fabianinkatu 33) keskiviikkona **29.4.2026.**

Ohjelma

8.30	Ilmoittautuminen ja kahvit
9.00	Avaussanat - puheenjohtaja Pertti **Hyvärinen**, Viestiupseeriyhdistys ry
9.10 – 9.30	Puolustusvoimien johtamisjärjestelmäalan tervehdys - apulaisosastopäällikkö, kommodori Petteri **Kuosmanen**, Pääesikunta
9.30 – 10.00	Suomalaisen ja eurooppalaisen puolustusteollisuuden kehittäminen sekä teollisuuden opit Ukrainasta - toimitusjohtaja Esa **Rautalinko**, Patria Oy
10.00 – 10.30	Ydinasepelote sodankäynnin välineenä Ukrainan sodassa - tutkija Jyri **Lavikainen**, Ulkopoliittinen instituutti
10.30 – 11.00	Johtaminen Venäjän kohteena Naton näkökulmasta - prikaatikenraali Jarkko **Karsikas**, Naton johtamis- ja tietojärjestelmäjohtoporras
11.00 – 11.30	Ukrainan sodan kyberseuranta - menetelmät ja opit - ylijohtaja Anssi **Kärkkäinen**, Traficom
11.30 – 12.30	LOUNAS

12.30 – 14.15	Ukrainan sodan opit teletoiminnan varautumiseen - alustukset ja paneelikeskustelu Moderaattorina Jaakko **Wallenius**, VP Resilience and Defence Elisa Oyj Panelistit: - turvallisuusjohtaja Seppo **Pekonen**, DNA Oyj - osastopäällikkö Heidi **Kivekäs**, Kyberturvallisuuskeskus, Traficom - teknologiajohtaja Antti **Kauppinen**, Suomen Erillisverkot Oy - johtaja, insinöörieversti Janne **Jokinen**, Puolustusvoimien Johtamisjärjestelmäkeskus
14.15 – 14.40	TAUKO
14.40 – 15.10	Innovaatiosyklin kasvava rooli, Ukraina ja Suomi - työelämäprofessori Valtteri **Vuorisalo**, Tampereen yliopisto
15.10 – 15.40	Kriittisen infran suojaaminen – Ukrainan opit - yksikön johtaja Jarna **Hartikainen**, Huoltovarmuuskeskus
15.40 – 16.10	Informaatio sodankäynnin vaikuttamisalueena - osastoesiupseeri, majuri Pasi **Lepistö**, Pääesikunta
16.10 – 16.40	Droonit taistelukentällä – Ukrainan sodan opit ja Sensofusionin johtopäätökset - johtaja Misa **Kangaste**, Sensofusion Oy
16.40 – 17.00	Loppuyhteenveto - toimitusjohtaja Charly **Salonius-Pasternak**, Nordic West Office
17.00 – 18.30	Verkostoituminen

Seminaarin puheenjohtajana toimii everstiluutnantti Tero **Palokangas**.

Seminaarin osallistumismaksut ovat 400 € (yritysten edustajat), 340 € (julkisen hallinnon ja järjestöjen edustajat) sekä 160 € (yksityishenkilöt ja eläkeläiset, jäsenet -50 %). Viestiupseeriyhdistys laskuttaa seminaarimaksun huhti-toukokuun 2026 vaihteessa.

Sitovat ilmoittautumiset pyydetään tekemään **15.4.2026 mennessä** yhdistyksen verkkosivuilla www.viestiupseeriyhdistys.fi (suositeltavin tapa) tai sähköpostitse seminaari@viestiupseeriyhdistys.fi.

Oikeus muutoksiin pidätetään.

Lämpimästi tervetuloa!

Lisätietoja tilaisuudesta: puheenjohtaja Pertti Hyvärinen, puheenjohtaja@viestiupseeriyhdistys.fi ja p. 0400 377359, sekä toiminnanjohtaja Harri Reini, toiminnanjohtaja@viestiupseeriyhdistys.fi ja p. 040 5142497.

Juhlavuodesta aktiiviseen arkeen

Toivotan kaikille Viestiupseeriyhdistyksen jäsenille sekä muille tämän lehden lukijoille mitä parhainta alkanutta vuotta 2026! Samalla haluan kiittää niitä, jotka omalla aktiivisella panoksellanne olitte mahdollistamassa onnistuneen 80- vuotisjuhlavuotemme tapahtumien toteuttamisen. Toukokuussa järjestetty juhlaseminaari kokosi yhteen noin 140 henkilöä, 80-vuotishistoriikki julkaistiin onnistuneesti aikataulussa, pääjuhlaamme Katajanokan Kasinolle saimme mukaamme arvovaltaisen kutsuvierasjoukon ja ikään kuin sokerina pohjalla, halusi Suur-Savon Reserviupseeripiiri brändätä Mikkelissä 5.12.2025 pelatun Jukurit-Saipa-jääkiekkopelin yhdistyksemme juhlavuoden teemalla – tästä tarkemmin toisaalla lehdessä. Edellisten lisäksi juhlavuosi sai myös Viestimies-lehteen paljon sisältöä ja näkyvyyttä, alkaen jokaisen viime vuoden numeron kanteen painetusta heraldikko Harri Rantasen suunnittelemasta juhlavuoden logosta.

Maanpuolustustyössä, myös vapaaehtoisessa sellaisessa, mukana olevat näkevät tämänkin vuoden haasteellisena ja varmaan myös yllätyksiä täynnä olevana. Ainakin itse koen näin. Venäjä on edelleen jatkanut rikollisia toimiaan eri tasoilla ja suunnilla. Mutta aiempiin vuosiin nähden täysin uutta on se, että nyt joudumme olemaan varpaillamme myös läntisen maailman suurimman mahdin ja liittolaisemme, Yhdysvaltojen, vaikeasti ennakoitavien toimien vuoksi. Tätä kirjoitettaessa Grönlannin omistuksesta esitetyt Yhdysvaltojen vaatimukset ovat sekoittaneet tai ainakin sekoittamassa pahasti läntisen puolustusliiton arkea. Tämä kaikki valuu valitettavasti Venäjän laariin, joka tyytyväisenä seurannee kehitystä – toki voihan siellä joillain tavoin olla myös idän sormet pelissä mukana. Ja kaiken tämän lisäksi Ukrainan sota on jatkunut jo neljä vuotta – ilman oikeudenmukaista ratkaisua näköpiirissä. Euroopalla jos milloinkaan on nyt näytön paikka. Tarvitaan päättäväisiä ja voimakkaitakin toimenpiteitä osoittamaan, että maanosamme ei ole ajopuu vaan itsenäinen ja halutessaan eduistaan huolta pitävä toimija.

Miten edellä kuvattu vaikuttaa Viestiyhdistyksemme toimintaan alkaneena

vuonna? Sääntöjemme mukaisesti jatkamme korkeatasoisten ja ajankohtaisten turvallisuusseminaarien järjestämistä. Huhtikuun lopussa järjestettävässä seminaarissamme, jonka ilmoitus löytyy toisaalta tästä lehdestä, on teemana Ukrainan sodan opit. Yhdistyksemme haluaa omalta osaltaan olla mukana jakamassa kokemuksia ja tietoa niistä opeista, joiden mukaisesti Suomella ja myös Natolla on mahdollista kehittää eri sektoreidensa toimintaa. Seminaari pyrkii tuomaan esille sekä onnistuneesti jalkautettuja oppeja kuin myös sellaisia sodan kokemuksia, joista emme ole jostain syystä osanneet oppia ottaa – ja miksemme ole. Seminaari on samalla jatkumoa pitkälle yhdistyksemme perinteelle, ja myös sääntömääräiselle tehtävällemme, yhdistää ja verkostoida sotilas- ja siviilitehtävissä toimivia ja toimineita toimialamme henkilöitä. Seminaarissa on jaossa tietopaketti, jota lienee vaikea muualta saada. Kannattaa ilmoittautua mukaan varsinkin, kun jälleen kerran yhdistyksemme jäsenille on räätälöity oma edullinen osallistumismaksunsa. Nähdään siis seminaarissa sankoin joukoin.

Viestiupseeriyhdistyksen rinnalla toimii Maanpuolustuksen viestisäätiö. Säätiön hallituksen muodostaa yhdistyksen säätiö täydennettynä erillisellä puheenjohtajalla sekä Viestisäätiön kannatusyhdistyksen puheenjohtajalla. Maanpuolustuksen viestisäätiö voi, ja myös haluaa, tukea toimialamme maanpuolustusvalmiuden kehittämistä sekä tätä tukevaa tutkimus- ja julkaisutoimintaa, opintoja sekä perinnetyötä. Uskon, että esimerkiksi huhtikuun seminaarimme tulee nostamaan esille paljon sellaisia jatkotutkimusta ja -kehittämistä edellyttäviä asioita, jotka liittyvät toimialamme maanpuolustusvalmiuteen. Pidänkin tärkeänä, että tietoa näistä säätiön tukimahdollisuuksista levitettäisiin mahdollisimman laajalle siten, että säätiön hallitus saisi hyvin perusteltuja tukihakemuksia käsiteltäväkseen ja myönteisissä tapauksissa tuettavakseen. Lisätietoja säätiöstä löytyy Viestiupseeriyhdistyksen verkkosivuilta. Jakakaa siis itse kukin tätä tietoa eteenpäin potentiaalisille hakijoille.

Edellisten lisäksi yhdistyksemme muu toiminta jatkuu viime syyskokouksen hyväksymän toimintasuunnitelman mukaisesti. Kevätkokous järjestetään tänä vuonna Suomen Erillisverkot Oy:n isännöimänä 23.4.2026. Esityslistalla on edellisen vuoden tilinpäätöksen hyväksyminen sekä sen ohessa luonnollisesti tutustuminen isäntämme, Erillisverkkojen, toimintaan. Syyskokouksen vuoro on jälleen 25. syyskuuta, yhteistyössä A. R. Saarmaa -seminaarin järjestäjien kanssa. Syyskaudelle on suunnitteilla myös jäsenmatka, jonka toteutumiseen merkittävästi vaikuttaa mukaan ilmoittautuneiden lukumäärä. Toivon todella, että tällä kertaa matka toteutuisi usean vuoden tauon jälkeen. Seuratkaa siis lehtemme ja verkkosivujen ilmoittelua ja tulkaa tilaisuuksiimme mukaan, toivottavasti pääsen niissä tapaamaan teistä mahdollisimman monia.

Pertti Hyvärinen

Puheenjohtaja

Eversti evp.

TEKSTI: KENRAALIMAJURI JARMO VÄHÄTIITTO

Johtamisjärjestelmäala ja kyberpuolustus puolustusvoimien johtamisen tukena

Puolustusvoimien johtamisjärjestelmäala ja kyberpuolustus kykenee täyttämään niille asetetut tehtävät. Keskeisintä on valmius ja operatiivinen kyky tukea Puolustusvoimien toimintaa. Artikkelissa keskitytään Puolustusvoimallisiin valmiuden ja operatiivisen kyvyn taustalla oleviin ilmiöihin johtamisesta teknologioihin.

ICT-johtaminen

Teknologian kehitys muuttaa Puolustusvoimien henkilöstön osaamisprofiileja. Puolustusvoimat ei ole vain järjestelmien käyttäjä, vaan sen tulee olla yhä vahvemmin teknologian soveltaja ja kehittäjä. Nykyinen palkatun henkilöstön koulutusjärjestelmämme ei kuitenkaan merkittävästi tue tätä kehityssuuntaa. Tästä johtuen teknologioiden opetuksen tulisi olla vahvemmin osa peruskoulutusta ja myös upseereille pitäisi mahdollistaa paremmat osallistumismahdollisuudet teknologisiin siviiliopintoihin joko työuransa aikana tai eritasoisiin virkauraopintoihin kytkeytyen.

Kyberturvallisuuden merkitys korostuu entisestään ja tarve kymmenille uusille kyberasiantuntijoille on jatkuva. Nykyajan ICT-johtajalta vaaditaan kykyä yhdistää sotilaallinen operatiivinen taito ja nopeasti kehittyvä teknologinen kyky sekä ymmärrys muutoksesta. Itseohjautuvuus ja kyky toimia verkostoituneissa ekosysteemeissä ovat keskiössä.

Nato-jäsenyyden myötä osaamisen on oltava myös yhteensopivaa liittolaisten kanssa. Tämä tarkoittaa teknisten standardien lisäksi kielellistä ja kulttuurista osaamista kansainvälisissä esikunnissa, työryhmissä ja komiteoissa. Erityisesti suorat henkilökohtaiset suhteet ovat merkityksellisiä luottamuksen aikaansaamiseksi ja aloitteiden edistämiseksi.

Puolustusvoimat ei suinkaan kehitä kaikkea itse, vaan käytössä on ns. yhteiskehittämisen malli. Tiivis yhteistyö ICT-talojen ja teollisuuden kanssa varmistaa, että käytössä on aina uusin teknologinen osaaminen ilman, että kaikkea tarvitsee omistaa itse. Innovaatioverkostoilla ja vastaavilla keskuksilla sekä yrityksillä on mahdollisuus toimia solmukohtina, joissa tekoälyä, autonomisia ratkaisuja ja viestijärjestelmiä kyetään testaamaan suoraan operatiivisten tarpeiden pohjalta. ICT-johtamisen tulevaisuus on siirtymistä pois siiloista kohti integroitua, datalla johdettua ja tekoälyavusteista puolustusta, jossa ihminen ja kone toimivat yhteistyössä. Lisäksi valtionhallinnon ICT-johtamisen on kyettävä mahdollistamaan Puolustusvoimien ja kaikkien turvallisuusviranomaisten saumattoman yhteistyön. Se on mahdollista nykyistä turvallisuusverkkoa kehittämällä ja siirtämällä johtajuutta sekä ratkaisu- ja päätöksentekovastuuta turvallisuusviranomaisten hallinnonaloille.

Datan hyödyntäminen johtamisessa ja tietojohtaminen

Datalla johtamisen muutos Puolustusvoimissa on kulminaatiopisteessä. Vuonna 2025 julkaistu data- ja tekoälystrategia on niputtanut tien kohti ”datakeskeistä tietojohtamista”, jossa tavoitteena on muuttaa hierarkkinen päätöksenteko dynaamisemmaksi ja laajempaan sekä saavutettavampaan informaatioon ja tietoon perustuvaksi. Datalla johtamisen tulevaisuutta tukevat tekijät ovat datakeskeisyys, kyky operoida sekä kulttuurin muutos. Tärkeimpänä on tukea Puolustusvoimien kykyä operoida yhdessä kaikilla tarvittavilla Puolustusvoimien kyvyillä samanaikaisesti vaikutuksen aikaan saamiseksi sekä kansallisesti että osana liittoumaa.

Puolustusvoimat pyrkii siirtymään kohti datakeskeistä organisaatiota, jossa tieto ei ole vain päätöksenteon tuki, vaan keskeinen strateginen resurssi. Yhtenä tavoitteena on minimoida manuaalinen raportointi. Tieto kerätään automaattisesti järjestelmistä ja esitetään visuaalisessa muodossa tilannekuvatyökaluissa. Tekoälyä käytetään suodattamaan ja analysoimaan sensoreista, lennokeista ja satellii-

teista tulevaa mittavaa tietovirtaa, jolloin johtajille tarjotaan olennaisin ja haluttu tieto päätöksentekoon. Teko- ja tukiäly auttaa tunnistamaan poikkeamia ja analysoimaan vastustajan toimintamalleja nopeammin kuin ihminen. Pysyäkseen teknologian kärjessä ja operointikyvyn varmistamiseksi Puolustusvoimat tarvitsee myös erittäin kyvykkäitä yhteistoimintakumppaneita. Strategisena valintana on mahdollisimman syvä ja tiivis yhteistyö kotimaisten toimijoiden kanssa unohtamatta sitä, että Naton ja liittolaisten kanssa tehtävä yhteistyö lisää osaamista ja yhden liittolaisen onnistuminen on hyödynnettävissä myös Suomessa. Onnistumalla nopeutamme uusien teknologioiden kansallista käyttöönottoa.

Datan hyödyntäminen ei ole vain hallinnollista, vaan se on kriittinen osa taistelukentän hallintaa. Esimerkkinä siitä on sensori-integraatio, jota edustaa vaikkapa F-35-hävittäjät toimien ”lentävinä datakeskuksina” tuottaen massiivisia määriä tietoa jaettavaksi myös muille puolustushaaroille. Rutiinitehtäviä on automatisoitava, jotta henkilöstö voi keskittyä yhä enemmän kriittiseen päätöksentekoon.

Teknologia on vain osatotuus. Vähintään yhtä suuri muutos tapahtuu toimintakulttuurissa. Koko organisaatio on koulutettava datan hyödyntämiseen johtamisessa. Tämä tarkoittaa sitä, että jokaisen johtajan on ymmärrettävä datan lukutaitoa ja osattava toimia oman työnsä kautta teknologian kehittäjänäkin. Se taas edellyttää välitöntä operaattorin ja teknisen henkilöstön välistä vuoropuhelua toimien ohjelmistokehityksen moottorina. Sotilaallinen tekoälyn käyttö mielletään usein eettisesti ja tietoturvankin osalta poikkeussääntelyn piiriin kuuluvaksi. Sitäkin on, mutta asetettu regulaatio on kyettävä ottamaan huomioon. Resurssointi on käynnistetty, mutta kokonaan uuden henkilöstön ja virkojen kohdentaminen uusiin tarpeisiin on harhanäky, joten meidän jokaisen on kyettävä päivittämään myös omaa osaamistamme. Reserviläisten siviiliammatissa hankkimaa IT- ja data-analyysiosaamista tulee kyetä hyödyntämään entistä aktiivisemmin esimerkiksi kertausharjoitusten asiantuntijatehtävissä. Data ei saa olla enää pelkkä apuväline, vaan keskeinen resurssi, jota on johdettava kuin mitä tahansa muuta suorituskykyä.

Tietojohtaminen ei ole enää vain historian tarkastelua, vaan Puolustusvoimat keskittyy lisäämään ennakoivaa analytiikkaa, joka auttaa arvioimaan esimerkiksi logistiikan tarpeita tai vastustajan mahdollisia toimintamalleja etukäteen. Puolustusvoimien toiminta Natossa vaatii, että tietojohtaminen on yhteensopivaa liittokunnan standardien kanssa. Tiedon on liikuttava saumattomasti liittolaisten välillä. Tämä vaatii yhtenäisiä tiedonhallinnan sääntöjä ja teknisiä rajapintoja. Tietojohtamisen tulevaisuus on tasapainoilua ”tarve tietää” (need to know) ja ”tarve jakaa” (need to share) välillä, jotta liittouma voi toimia tehokkaasti yhdessä.

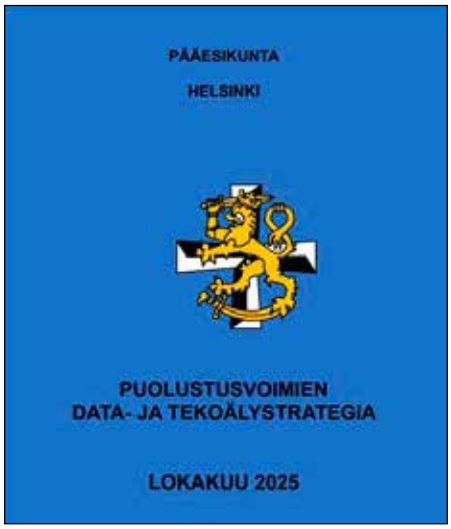
Mitä siis pitäisi saada aikaan?

1) Dataan perustuva ennustettavuus ja nopeus päätöksenteon tueksi. Rutiinitehtävien automatisointi, joka tarkoittaa vähemmän paperitöitä, enemmän aikaa johtamiselle.

2) Saumaton tiedonvaihto Puolustusvoimissa, viranomaisten ja Nato-kumppanien kanssa sekä toimintaa tukeva yhtenäinen tiedonhallinta. Tieto säilyy ja on hyödynnettävissä hankinnasta poistoon.

3) Ekosysteemejä, jotka yhdistävät sotilaallista tarvetta tukevan yritystoiminnan.

4) Henkilöstön datalukutaidon kehittämistä. Jokainen sotilas osaa hyödyntää ja suojata dataa.



Tietoverkot ja -liikenne

Tietoverkkojen liitettävyyden ja tietoliikenteen on Puolustusvoimissa perustuttava saumattomaan, nopeaan ja häiriösietoiseen tiedonsiirtoon kaikissa olosuhteissa. Jatkamme siirtymistä perinteisistä radioverkoista kohti hybridiratkaisuja, joissa kaupallinen teknologia ja sotilaallinen suorituskyky yhdistyvät nykyistä älykkäämmin.

Puolustusvoimien taktisen tason radioverkot ovat jo nykyisellään erittäin kehittyneitä ja nykyaikaisia verrattuna niitä mihin tahansa liittolaiseen tai muihin maihin. Ne jatkavat edelleen kehittymistä ja ohjelmistopohjaisuus, aaltomuodot, varsinaisen raudan sekä antennitekniikan integraatio-osaaminen on niin keskeinen osaamisalue, että siihen on kyettävä resursoimaan jatkossa riittävästi. Sotilaskäytössä uudempana kyvykkyytenä toimii 5G ja jatkossa 6G, jonka hyödyntämisessä yksi tapa on verkon viipalointi sotilaalliseen käyttöön. Se mahdollistaa priorisoidun ”viipaleen” varaamisen sotilaskäyttöön julkisessa verkossa, taaten yhteydet myös ruuhkatilanteissa. Puolustusvoimat onkin edelläkävijä kaupallisten 5G-verkkojen hyödyntämisessä liittoumassa. Yhtenä esimerkkinä oli vuonna 2025 toteutetut kokeilut. Ne osoittivat, että 5G-viipaleet voivat jatkua katkeamatta maarajojen yli, mikä on kriittistä mm. liittouman operaatioissa. 6G-kehityksessä Suomi on jo mukana ja kansallisessa 6G-tiekartassa tavoitellaan mm. ”AI-natiiveja” verkkoja ja senttimetritason paikannustarkkuutta 2030-luvulle tultaessa. Myös satelliittiyhteyksien merkitys on kasvanut räjähdysmäisesti, erityisesti Ukrainan sodassa nähdyllä tavalla.

Tietoverkkojen ja -liikenneratkaisujen kuten tietojärjestelmienkin on oltava teknisesti yhteensopivia liittolaisten kanssa. Tässä keskeisimpänä yhteentoimivuusohjelmana toimii edelleen Federated Mission Networking (FMN) ohjelma. Puolustusvoimien keskeisin tuote on Protected Core Network (PCN) standardien mukaan rakennettu Puolustusvoimien Liityntäverkko (PVLIVE). FMN-ohjelman standardien mukaiset tuotteet ovat ”natolaisittain” synonyymi Naton kehittyvälle operaatioverkolle, jota kutsutaan nimellä ”VeVa”.

Tulevaisuuden liitettävyys ei ole vain nopeita verkkoja vaan myös niiden kestävyyttä. Sodan olosuhteissa on kyettävä toimimaan yhtäältä vaikkapa tykistö- ja ohjustulenkäytön ja toisaalta voimakkaan elektronisen sodankäynnin vaikutuspiirissä. Tällaisessa toimintaympäristössä korostuvat suomalainen hajautettujen verkkojen toteutustapa, jossa yhden solmun tuhoutuessa verkko muodostaa reitin automaattisesti uudelleen. Lisäksi verkon salaus mukaan lukien valmistautuminen kvanttitietokoneiden aikaan vaatii uusia omissa käsissämme olevia salausalgoritmeja viestinnän turvaamiseksi pitkällä aikavälillä. Verkot ovat käytännössä nimensä mukaisesti taistelukentän ja operoinnin hermosto. Ilman niitä data ei liiku, eikä tekoälyllä voida johtaa.

Mitä siis pitäisi saada aikaan?

1) Jatkaa nykyisten maailmanluokan taktisten verkkojen kehittämistä ja ottaa sotilaalliseen käyttöön kaupalliset 5G- ja privaatti 5G-verkot laajasti Puolustusvoimia hyödyntämään mm. tukikohdissa, sensoriverkoissa, miehittämättömien laitteiden tukena aikaansaaden nopeampaa ja monipuolisempaa kenttäviestintää.

2) Lisätä satelliittitietoliikenteen määrää hankkimalla useamman kerroksen kyvykkyyksiä itsenäisesti ja yhdessä liittolaisten kanssa.

3) Lisätä merkittävästi ohjelmistoradioiden määrää kehittäen niiden joustavia käyttötapoja. Samalla on varmistettava kehittyvien ohjelmistojen, aaltomuotojen ja raudan kehittyminen.

4) Joustavampi taajuuksien hallinta ja häirinnän siedon jatkuva kehitys.

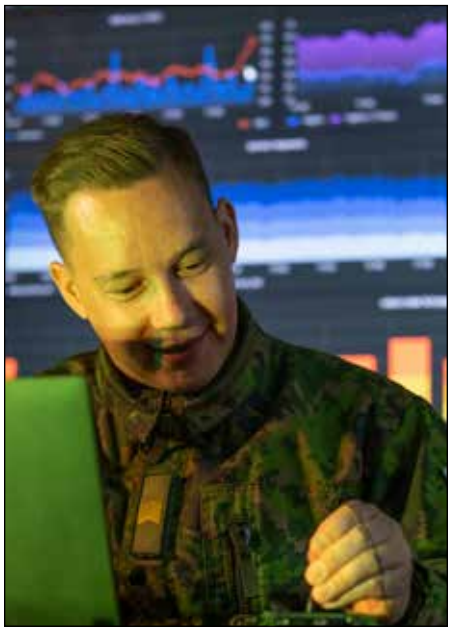
5) Tekoälyohjattu verkkoalusta, joka mahdollistaa verkko- ja radiolaitteiden monikäyttöisyyden perinteisen viestinvälityksen lisäksi esim. automaattiseen reititykseen ja taajuushallintaan, tiedustelusensorina toimimiseen ja kyberhyökkäysten torjuntaan.

Kyberpuolustus suorituskykynä

Kyberpuolustus on kehittynyt tosiasialliseksi suorituskyvyksi Puolustusvoimissa ja kiinteäksi osaksi kansallista koskemattomuutta ja suvereniteettia. Verkkorajamme ovat yhtä kriittisiä kuin maarajammekin. Kyberpuolustusta ei nähdä pelkästään IT-tukitoimintona, vaan se on integroitu osaksi jokaista operaatiota – niin maalla, merellä, ilmassa kuin avaruudessakin. Kyberpuolustus on myös välttämättömyys toimivalle informaatiopuolustukselle ja sen integraatio elektroniseen sodankäyntiin tuo operatiivisia hyötyjä Puolustusvoimille.

Olemme siirtyneet asteittain passiivisesta suojautumisesta kohti aktiivista kyberpuolustusta, vaikka lainsäädäntö asettaa rajoitteita sotaa alempiasteisille tilanteille. Siitä huolimatta kyberpuolustuksen ei tule olla vain kilpimuuri, vaan sen tulisi sisältää kyvyn vaikuttaa vastustajan tietoverkkoihin ja estää hyökkäykset jo niiden lähtöpisteessä. Kybertoimintaympäristössä, Puolustusvoimien ulkopuolisissa verkoissa tapahtuva aktiivinen seuranta ja analyysi toteutuu pääosin Sotilastiedustelulain toimivaltuuksin.

Hyökkäysten nopeus ja volyymi ovat kasvaneet niin suuriksi, ettei ihminen ehdi reagoida niihin manuaalisesti. Siksi tarvitsemme automaattista vastetta. Tekoälyjärjestelmillä on kyky tunnistaa poikkeamia verkkoliikenteessä millisekunneissa ja eristää saastuneet järjestelmät automaattisesti. Kaiken kattavasti tähän on kuitenkin vielä matkaa, mutta algoritmikehitystä jatketaan tavoitteena paremmin hyökkäyksiä ennustamaan kehittyvät algoritmit, jotka analysoivat datavirtaa ja toiminnallisia poikkeamia. Onneksi tässäkään asiassa kaikki toiminta ei ole kiinni Puolustusvoimien omista resursseista vaan tiivis yhteistoiminta tie-



toturvayritysten kanssa lisää kyvykkyyttämme merkittävästi. Lisäksi Puolustusvoimien aktiivisen toiminnan kautta on perustettu Puolustusvoimien ja Traficomin Kyberturvallisuuskeskuksen yhteinen toimintaryhmä (MIL-ISAC), joka varmistaa puolustusjärjestelmään kytkeytyvien yritysten tiedonvaihtomenetelmän Puolustusvoimien kanssa.

Nato-jäsenyys on muuttanut kyberpuolustuksen luonnetta yksilösuorituksesta joukkuepeliksi. Yhteinen tilannekuva erityisesti läheisimpien liittolaisten kesken on välttämättömyys fyysisille valtioiden rajoille agnostisille valtiollisten uhkatoimijoiden kyberhyökkäyksille. Tiedonvaihto liittolaisten kesken onkin jatkuvaa, ja hyökkäys yhtä jäsenmaata vastaan voidaan tulkita hyökkäykseksi koko liittokuntaa vastaan.

Kyberpuolustuksessa kuten muussakin Puolustusvoimien toiminnassa Puolustusvoimien erityispiirteet huomioon ottava osaaminen on keskeistä. Osaamisen kehittämisessä on itsestään selvää koko henkilöstön osaaminen. Viime vuosina on panostettu yhä enemmän niin varusmies- kuin reserviläiskoulutukseen. Johtamisjärjestelmäkoulussa tuotetaan vuosittain kymmeniä huippuosaajia, joilla on aktiivisen kyberpuolustuksen asenne ja taidot, jopa valkohattuhakkerimentaliteettia. Siviilityössään IT-alalla sekä tietoturvatehtävissä toimivat reserviläiset muodostavat strategisen reservin, jonka osaamista pidetään yllä säännöllisillä re-


MILDEF
Behind the
mission
At MilDef, we build trust by protecting what matters most:
people, information and missions.
Our real strength comes not only from the tough and rugged IT solutions we develop, but also from the dedicated people behind them.
We are at our best where others hesitate.Because for us, it's about empowering the people who keep our world safe.
WE ARMOR IT.™

servin kyberharjoituksilla, kuten *Locked Shields*. Reserviläisten osaamisessa merkittävä rooli on myös Maanpuolustuskoulutusyhdistyksen (MPK) kursseilla ja harjoituksilla. MPK on myös kantanut merkittävää roolia myös Puolustusvoimien osallistumisessa kansainvälisiin harjoituksiin kokoamalla ja harjoittamalla osaavia reserviläisiä harjoitusjoukkoon.

Mitä on siis pitäisi saada aikaan?

1) Uhkien tunnistaminen ennen niiden aktivoitumista. Kehittyvien työkalujen, koneoppimisen ja SIGINT:n tuki osaksi toimintaa.

2) Kyettävä varmistamaan operaatiovarmuus kybertoimintaympäristössä jatkaen ja tukien Puolustusvoimien operointia hyökkäyksen alla.

3) Kybervarusmiesten ja -reservin hyödyntäminen ja osaamisen kehittämisen jatkaminen. Vapaaehtoisen operointiin viiveettä osallistuvan kyberreservin muodostaminen ja mahdollisuus operoida myös NO:ssa.

4) Julkisen ja yksityisen sektorin tiivis yhteistyö ja kumppanuus operoinnin ja tiedonvaihdon mahdollistaen laajasti kansallisesti ja kansainvälisesti. Lainsäädännön kehittäminen.

COMSEC- toiminta

COMSEC (Communications Security) eli viestintäturvallisuus on merkittävä kyvykkyys ja osa-alue, kun liitettävyys ja dataan perustuva johtaminen lisääntyvät. Tällöin viestinnän salaamisen ja suojaamisen merkitys kasvaa entisestään. COMSEC-toiminnan kehitystä ohjaavat kvanttiturvallisuus, automaatio ja Nato-yhteensopivuus. COMSEC ei ole vain salauskoodeja, vaan myös kykyä viestiä häirinnän alla.

Suurin teknologinen muutos COMSEC:n alalla on valmistautuminen kvanttitietokoneiden tuomaan uhkaan. Perinteiset salausalgoritmit voivat tulevaisuudessa murtua sekunneissa. Puolustusvoimat on onneksi jo aloittanut siirtymisen kvanttisietoisiin salausmenetelmiin. Toimintaa kiihdyttämään on käynnistetty Puolustusvoimien kvantti-inventaario, joka parantaa tilannekuvaa ja mahdollistaa jatkotoimet kvanttiturvalliseen viestintään.

Perinteinen, fyysisiin avaintenjakolaitteisiin ja manuaalisiin päivityksiin perustuva COMSEC on jäämässä historiaan. Toiminta Puolustusvoimissa on kehittynyt liikkuvan ja hajautetun sodankäynnin sekä Nato-liittouman vaatimuksia vasten. Salausavaimia voidaan päivittää ja jakaa suojatusti radioyhteyden tai tietoverkon yli ilman, että laitetta tarvitsee tuoda varikolle. Tämä on elinehto liikkuvassa ja hajautetussa sodankäynnissä. Koneidentiteettien (lennokit, sensorit, autonomiset järjestelmät) määrä on jopa räjähtämässä. Toiminnan on keskityttävä varmistamaan, että jokainen verkkoon kytketty laite on aito ja sen viestintä on suojattu yksilöllisillä avaimilla.

NATO-jäsenyys vaatii saumatonta viestintää liittolaisten välillä eri turvallisuusluokissa. Puolustusvoimat jatkaa investointeja uuden sukupolven kryptolaitteisiin, jotka tukevat liittokunnan yhteisiä standardeja. Federated Mission Networking (FMN) mukainen COMSEC-toiminta mahdollistaa sen, että suomalaiset joukot voivat liittyä Naton operaatioverkkoon säilyttäen silti kansallisen viestinnän turvallisesti erillään.

Mitä siis pitäisi saada aikaan?

1) ”Lukitusta ovesta” dynaamiseen, älykkääseen ja jatkuvasti muuntuvaan suojakerrokseen. Lisäksi yhden solmun vaarantuessa, järjestelmän tulee kyetä eristämään se ja mitätöimään kyseisen solmun avaimet välittömästi koko verkosta.

2) Nykyistä laajempi sähköinen avaintenhallinta- ja jakelujärjestelmä henkilöstöineen.

Asevelvollisuus

Suomalaisen asevelvollisuuden kehittäminen johtamisjärjestelmä- ja kyberyksiköissä vaatii perinteistä massa-ajatteluakin, mutta samalla yksilöllisempää ja teknisempää osaamispolkua joukkueurheilusta mallia ottaen. Painopiste on siirtynyt yhä enemmän siviiliosaamisen hyödyntämiseen ja jatkuvaan oppimiseen. Osaamispohjaiset valintamenetelmät ja jopa ”fast track”-polut mahdollistaisivat suoran erikoistumisen niille, joilla on valmiiksi korkea tekninen osaaminen. Tällöin he pääsevät nopeammin operatiivisiin tehtäviin. Asevelvollisen siviilissä hankkima osaaminen on siis tunnistettava jo ennen kutsuntoja. Esivalintakyselyt tulee kyetä tekemään datapohjaisesti seuloen, jotta tunnistetaan koodaus-, verkko- ja tietoturvaosaajat jo ennen palveluksen aloitusta tai löydetään heidät reservistä, kun heille on kertynyt alan osaamista.

Kyberpuolustus ei pääty varusmiespalveluksesta kotiutumiseen. Tarvitaan malli, jossa osaaminen pysyy tuoreena myös reservissä. Säännölliset, kotoa käsin tehtävät etäharjoitukset tai Capture the Flag -kilpailut, voisivat ylläpitää teknistä suorituskykyä. On myös kehitettävä edelleen esim. Maanpuolustuskoulutusyhdistyksen kanssa polkuja, joissa IT-alan yrityksissä työskentelevät reserviläiset voivat osallistua harjoituksiin johtamisjärjestelmien kehittämistehtävällä. Kyberpuolustuksessa varusmiehiä ja reserviläisiä ei kohdella vain ”apukäsinä”, vaan he muodostavat kriittisen osan Puolustusvoimien digitaalista puolustuslinjaa. Heidän koulutuksensa on oltava tasoltaan sellaista, että se vastaa alan huippustandardeja.

Nykyaikainen taistelukenttä vaatii johtajia, jotka ymmärtävät sekä taktiikkaa että bittejä.

Tarvitsemme uusia rooleja myös asevelvollisille. Niissä keskitytään datan analysointiin ja sensoridatan integraatioon etulinjassa. Varusmiehiä ja reserviläisiä tulee kouluttaa toimimaan tilanteissa, joissa vaaditaan ohjelmointikyvykkyyksiä yhdessä palveluja toimittavien yritysten kanssa. Tämä vaatii kykyä itsenäiseen päätöksentekoon ja paikallisten verkkojen pystyttämiseen ja ohjelmointiin.

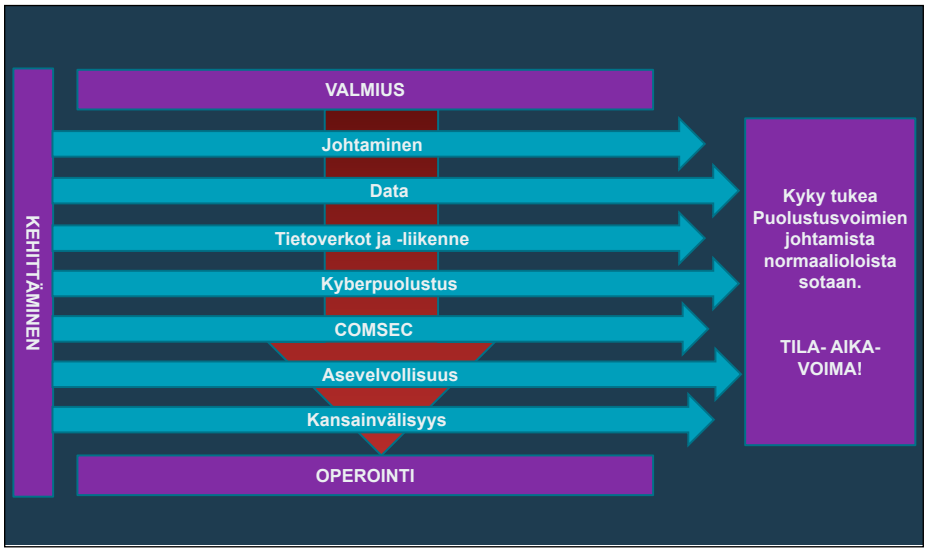
Mitä siis pitäisi saada aikaan?

1) Digitaalinen osaamisportfolio kutsunnoissa. Oikea henkilö oikeaan paikkaan.

2) Turvallinen harjoittelu todellisilla haittaohjelmilla, mutta myös osallistuminen varsinaisiin operaatioihin tulee mahdollistaa.

3) Aktiivinen kyber- ja johtamisjärjestelmäreservi-malli kriisitilanteita varten.

4) Yhteistyö oppilaitosten kanssa osaamisen kehittämiseksi palveluksen houkuttelevuuden lisäämiseksi.



Kansainvälisyys

Puolustusvoimien johtamisjärjestelmäalan kansainvälinen kehittäminen ja yhteistyö liittolaisten kanssa on nykyisessä geopoliittisessa tilanteessa kriittisempää kuin koskaan.

Suurin haaste ja mahdollisuus on yhteensopivuuden täysimääräinen toimeenpano. Tämä tarkoittaa, että suomalaisten johtamisjärjestelmien on oltava joustavia ja kykeneviä liittymään saumattomasti osaksi liittokunnan verkostoja ilman viivettä. Kehityksen painopisteen on oltava standardien mukaisten rajapintaratkaisujen toteuttamisessa, joilla mahdollistetaan datan liikkuminen eri maiden välillä. Taistelukentän datan käsittelyä on siirrettävä lähemmäs toimijoita eli edgeä, mutta samalla tulisi kyetä hyödyntää Naton kehittyviä yhteisiä pilvipalveluita ja muita palveluja tilannekuvan jakamiseen.

Pohjoismainen ja maantieteellisesti lähellä olevien liittolaisten välisen yhteistyön on mahdollista olla syvemmälle tasolle integroitua. Näiden maiden kesken tarvitaan aktivoidut verkot ja palvelut, joilla kyetään tukemaan operaatioita sekä yhteinen, jatkuva johtamisjärjestelmäalan ja kyberpuolustuksen tilannekuva-alue, joka kattaa Arktisen alueen ja Itämeren.

Johtamisjärjestelmien elinkaarikustannuksia voidaan laskea ja huoltovarmuutta parantaa tekemällä yhteisiä järjestelmä- ja lisenssihankintoja sekä kehitysprojekteja vaikkapa Pohjoismaiden kesken.

Kyberpuolustuksen tiedonvaihtoa ja erityisesti uhkatiedonvaihtoa on automatisoitava myös kansainvälisesti. Teknologia on kuitenkin vain työkalu ja ihmiset sekä prosessit ratkaisevat. Kohdentamalla upseereita ja siviiliasiantuntijoita Naton rakenteisiin ja kumppanimaiden esikuntiin koko Puolustusvoimat kehittyy. Harjoitustoiminnassa painopistettä tulisi siirtää kohti skenaarioita, joissa harjoitellaan ja operoidaan häirityssä ja kiistetyssä sähkömagneettisessa ympäristössä.

Kehityksessä on tasapainoteltava kansallisen huoltovarmuuden ja kansainvälisen riippuvuuden välillä. Suomen on säilytettävä kyky hallita omia kriittisiä järjestelmiään myös silloin, kun ulkopuoliset yhteydet ovat poikki. Huolestuttavaan kehityskulkuun, jossa globaalit teknologiatalot ovat rakentaneet lähes kaikkien suomalaisten toimijoiden riippuvuuden itseensä on vaarallinen. Tätä muutosta on aloitettava purkamaan esimerkiksi luomalla edellytyksiä avoimen lähdekoodin ohjelmistojen ja kansallisen ohjelmistojakelun kehittämiselle Suomessa, jolloin ei olla niin riippuvaisia globaaleista pilvitoimijoista.

TEKSTI: PRIKAATIKENRAALI JARKKO KARSIKAS

KUVA: NATO

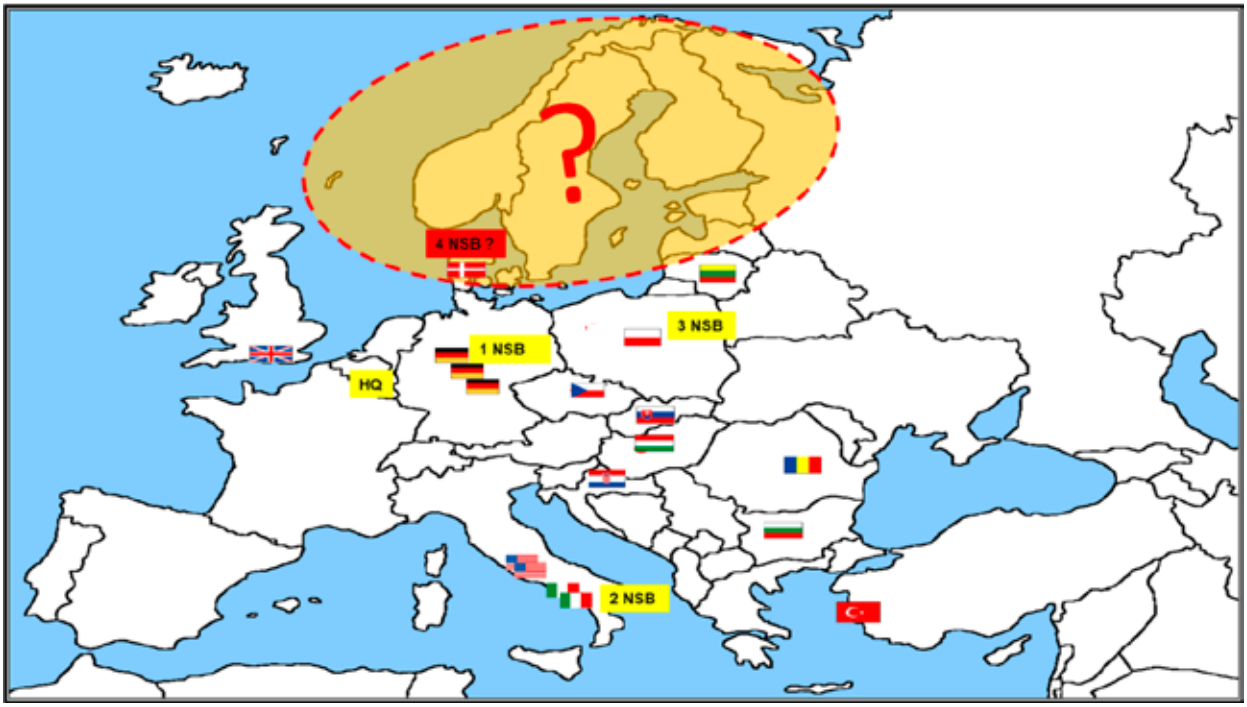
Kirjoittaja prikaatikenraali Jarkko Karsikas työpisteellään.

Pohjoisen operointisuunnan johtamisen vahvistaja: DCM-yksikön rakentaminen Suomeen

Tämä artikkeli on jatkoa syyskuussa 2025 julkaistuun artikkeliin Naton johtamisjärjestelmätoiminnasta ja NCISG:stä.

Johdanto: Strategisesta tarpeesta käytännön toimeenpanoon

Naton paluu kollektiivisen puolustuksen ytimeen on vaatinut liittokunnan johtamisjärjestelmähermoston merkittävää vahvistamista. Venäjän hyökkäyssota Ukrainassa osoitti, että staattiset rauhanajan rakenteet eivät riitä vastaamaan suurvaltakonfliktin vaatimuksiin. Strategiset analyysit osoittivat nopean tarpeen nostaa NATO CIS Groupin (NCISG) henkilöstömäärää 1550:sta noin 2000:een. Tämä kasvu ei ole vain numeerista, vaan se tarkoittaisi kokonaisen uuden joukkoyksikön, 4. Naton viestipataljoonan (4th NATO Signals Battalion, 4NSB), perustamista.



NCISG:n nykyiset yksiköt ja pohjoisen haaste.

Suomen ja Ruotsin jäsenyys on siirtänyt Naton operatiivista painopistettä merkittävästi kohti pohjoista. Tällä alueella NCISG:llä ei ole aiemmin ollut pysyvää läsnäoloa, mikä on jouduttu huomioimaan alueellisissa puolustussuunnitelmissa (Regional Plans). Puolustusministeri Antti Häkkäsen marraskuussa 2025 tekemä vastaus Naton pyyntöön tarjota Suomen isännöimää DCM-yksikköä on suora ja strateginen vastaus tähän tyhjiöön. Suomi ei enää tyydy olemaan suorituskykyjen kuluttaja, vaan se ottaa paikkansa johtamisen tuen aktiivisena tuottajana.

DCM-yksikön anatomia: 59 johtamisjärjestelmien ammattilaista

DCM-yksikkö on NCISG:n operatiivinen perusyksikkö, jonka kirjavahvuus on kaksi upseeria ja 57 aliupseeria. Tämä painotus kertoo yksikön luonteesta; kyseessä on erittäin korkean osaamisen ja teknisen toimeenpanon organisaatio, jossa aliupseeriston rooli on keskeinen. Yksikkö jakautuu vähintään kolmeen toiminnalliseen osastoon (NDD, NATO DCIS Detachment), jotka kykenevät tukemaan erikokoisia ja eri valmiustasoilla olevia johtamispaikkoja.

NDD-osasto on se nyrkki, joka kytkee taktisella tasolla operoivat esikunnat Naton strategisiin verkkoihin. Jokaisen aliupseerin on hallittava laaja kirjo osaamista: satelliittikommunikaatiosta ja IP-verkoista aina palvelinhallintaan ja loppukäyttäjätukeen saakka. Nykyaikaisen monikansallisen taistelukentän keskellä tämä vaatii paitsi teknistä suvereniteettia, myös kykyä operoida Naton standardien (STANAG) mukaisesti, usein vieraalla kielellä ja olosuhteiltaan vaativassa ympäristössä. Suomeen perustettava yksikkö tarjoaa suomalaisille upseereille, ammattialiupseereille, järjestelmäasiantuntijoille ja miksei myös määräaikaisille reserviläisille poikkeuksellisia urapolkuja kansainvälisessä tehtävässä niin kotimaassa kuin Naton koko operaatioalueella.

DCIS-suorituskyky: Raskaasta raudasta pilvipalveluihin

NCISG:n suorituskyvyn ytimessä on DCIS (Deployable Communications and Information Systems). Perinteisesti tämä on tarkoittanut raskaita esimerkiksi konttipohjaisia ratkaisuja, kuten Dragonfly-järjestelmää. Se on suunniteltu tarjoamaan merkittävä laskentateho ja tietoliikennekapasiteetti staattisemmille esikunnille. Ukrainan sodan oppi on kuitenkin selvä: staattisuus on kuolemaksi. Tämän vuoksi NCISG:n tekninen kehitys kulkee kohti ketteryyttä ja modulaarisuutta.

Uuden sukupolven DCIS-suorituskyky kykenee tuottamaan vähintään kolmen eri turvallisuusluokitustason (esim. NATO SECRET ja MISSION SECRET) ympäristöt huomattavasti aiempaa pienemmässä koossa. Erityisen mielenkiintoinen kehityssuunta on pilvipalveluympäristöjen (Tactical Cloud) tuominen taistelukentälle. Tämä mahdollistaa tiedon tallentamisen ja prosessoinnin hajautetusti, mikä parantaa johtamispaikkojen eloonjäämiskykyä. Kyseisiä ratkaisuja on kokeilussa tietyissä operaatioissa, joissa ne mahdollistavat laajan tiedonvaihdon. Suomeen mahdollisesti perustettava DCM-yksikkö mahdollistaisi teknologisen murroksen toteuttamista, sillä Suomen tietotekninen infrastruktuuri on poikkeuksellisen kehittynyt ja kehitetty kriisitilanteita kestäväksi.

Kyberpuolustus ja operatiivinen resilienssi

Kyberpuolustus ei ole NCISG:lle pelkkä IT-osaston lisäpalvelu, vaan se on koko operatiivisen toiminnan onnistumisen elinehto. Liikuteltavat johtamispaikat ovat erityisen haavoittuvia sähköisen sodankäynnin ja kybervaikuttamisen yhdistelmille. NCISG onkin kehittänyt omaa erikoiskalustoa ja -ohjelmistoja, joilla kyetään valvomaan ja suojaamaan DCIS-yksiköiden verkkoja reaaliajassa kenttäolosuhteissa.

Resilienssi tarkoittaa tässä yhteydessä kykyä jatkaa tehtävää, vaikka osaan verkoista kohdistuisi hyökkäys. Suomen DCM-yksikkö tulee olemaan osa tätä suojamuuria. Suomalainen henkilöstö tuo mukanaan kansallisen osaamisensa kyberturvallisuudesta, mutta saa vastavuoroisesti pääsyn NCISG:n sekä Naton kybersuojamekanismeihin ja tilannekuvatietoon. Kybersuojatut järjestelmät ovat nykypäivän toimintaympäristöissä elinehto, josta NCISG:llä on vahva käytännön kokemus.

Logistiikan ja siirrettävyyden haasteet

NCISG hallinnoi yli 90 prosenttia koko Naton komentorakenteen (NCS) ajoneuvokalustosta. Tämä tarkoittaa yli 1300 ajoneuvoa, konttia ja perävaunua. Viestitoiminta on nykypäivänä vaativaa erikoislogistiikkaa. DCM-yksikön on kyettävä siirtymään nopeasti sinne, missä johtamista tarvitaan – oli se sitten tunturissa tai rannikolla.

Suomeen sijoitettavan kaluston on vastattava pohjoisen sääolosuhteiden ja maaston haasteisiin. Siirrettävyysvaatimukset ovat tiukat: yksikön on kyettävä itsenäiseen toimintaan ja liikkeeseen JFC Norfolkin operatiivisten tarpeiden mukaisesti. Tämä asettaa suuria vaatimuksia paitsi kaluston ylläpidolle, myös henkilöstön osaamiselle. Jokainen viestimies on tässä kontekstissa myös logistikko, jonka on ymmärrettävä miten monimutkainen tekninen laitteisto pidetään toimintakuntoisena jatkuvassa liikkeessä ja vaativissa olosuhteissa.

Rahoitusmalli: Jaettu vastuu ja yhteinen hyöty

DCM-yksikön perustaminen ja ylläpito noudattavat Naton vakiintunutta rahoitusmallia, joka perustuu jaettuun vastuuseen. Suomi vastaa isäntämaana ja henkilöstön lähettäjänä palkkakustannuksista, kansallisesta henkilökohtaisesta varustuksesta kuten aseistuksesta, sekä tietyistä logistisista valmiuksista. Tämä on merkittävä kansallinen investointi, mutta se on suhteutettava saavutettavaan hyötyyn.

Naton yhteinen rahoitus (Military Budget) puolestaan kattaa yksikön varsinaisen operatiivisen kaluston, henkilöstön jatkuvan koulutuksen, matkakulut ja johtamisjärjestelmien operoinnin kustannukset. Myös tarvittavat rakennushankkeet ja infrastruktuurin kehittäminen kuuluvat pääsääntöisesti yhteisrahoituksen piiriin. Tämä malli on osoitus siitä, että DCM ei ole Suomen oma hanke, vaan liittokunnan yhteinen investointi pohjoisen puolustuksen uskottavuuteen. Se takaa, että yksiköllä on käytössään aina modernein teknologia ilman, että kaikki kehityskustannukset lankeaisivat yksin isäntämaalle.

Ammatillinen kehittyminen: Uusia urapolkuja viestimiehille

Upseereille ja aliupseereille DCM-yksikkö tarjoaa historiallisen mahdollisuuden kansainväliseen uraan poistumatta kotimaasta. Työskentely Naton komentorakenteessa on jatkuvaa ”kielikylpyä” ja kulttuurien välistä yhteistyötä. Vaikka yksikkö sijaitsee Suomessa, sen toimintatavat, ohjesäännöt ja päivittäinen viestintä noudattavat Naton monikansallisia käytänteitä.

Kokemus SHAPE:sta ja NCISG:n esikunnasta on osoittanut, että suomalainen sotilasosaaminen on erittäin arvostettua. Meidät tunnetaan pragmaattisuudesta ja kyvystä ratkaista ongelmia. DCM-yksikössä tämä osaaminen pääsee testiin, kun suomalaiset asiantuntijat operoivat rinta rinnan muiden jäsenmaiden kollegoiden kanssa. Tämä ei ainoastaan kehitä yksilön osaamista, vaan se tuo arvokasta pääomaa takaisin kansalliseen puolustukseen, kun Naton parhaat käytännöt ja uusin teknologinen ymmärrys leviävät laajemmalle organisaatioon.

Johtopäätökset: Suomi johtamisjärjestelmäosaamisen keskiössä

DCM-yksikön perustaminen Suomeen on kouriintuntuva osoitus maamme integraatiosta Natoon. Se ei ole pelkkä hallinnollinen päätös, vaan teknologinen ja operatiivinen sitoumus liittokunnan yhteiseen puolustukseen. Yksikkö muodostaa sen ratkaisevan linkin, joka varmistaa pohjoisen alueen johtamiskyvyn kaikissa olosuhteissa.

Olemme siirtymässä vaiheeseen, jossa suomalainen johtamisjärjestelmäosaaminen on kiinteä osa Naton globaalia suorituskykyä. Tämä polku vaatii panostuksia, ”poisoppimista” vanhoista rauhanajan malleista ja rohkeutta tarttua uusiin teknologioihin. Lopputuloksena on kuitenkin vahvempi ja yhteentoimivampi puolustus. NCISG on keskeinen osa ACO:n sodankäyntikykyä ja jo nyt teknologisesti sekä operatiivisesti kiinni liittokunnan hermokeskuksessa – valmiina varmistamaan, että viesti kulkee, johtaminen toimii ja pelote on uskottava.

NATO – Stronger Together.

TEKSTI: EVERSTILUUTNANTTI, SOTATIETEIDEN TOHTORI MARIA KEINONEN

MAANPUOLUSTUSKORKEAKOULU

Kyberpelotteen haasteet ja mahdollisuudet

Pelote esiintyy terminä lähes päivittäin uutisissa, politiikkojen puheissa ja kansalaisten keskusteluissa. Vaikka pelote mielletäänkin usein ydinaseen kautta, on kyseessä huomattavasti laajempi kokonaisuus, joka ulottuu fyysisen maailman lisäksi myös kybertoimintaympäristöön. Tässä artikkelissa paneudutaan kyberpelotteen piirteisiin, haasteisiin ja mahdollisuuksiin tieteellisen tutkimuksen näkökulmasta.

Pelotteesta lyhyesti

Valtion pelote tarkoittaa pyrkimystä vakuuttaa uhkatoimija siitä, ettei hyökkäys kannata ja tällä tavoin ennaltaehkäistä valtioon kohdistuvia aggressioita. Klassisen peloteteorian mukaan vaihtoehtoja on kaksi: rankaisu- ja kieltopelote. Valtio voi joko kertoa omasta kyvystään ja tahdostaan vastata mahdolliseen aggressioon vähintään yhtä suurella voimalla tai viestiä, että hyökkäyksen hinta tulee olemaan ennakoitua suurempi sen vaikutusten jäädessä oletettua vähäisemmiksi. Suomen pelote on aina perustunut tähän jälkimmäiseen vaihtoehtoon, tosin Nato-jäsenyyden myötä olemme siirtyneet samalla ydinasesateenvarjon alle. Ydinaseen olemassaolo perustuu rankaisupelotteeseen.

Ihmisellä on luontainen tarve jäsennellä monimutkaisia kokonaisuuksia yksinkertaisiksi malleiksi, jotta ne olisi mahdollista ymmärtää edes konseptin tasolla. Pelote on hahmoteltavissa kolmen elementin kautta: valtion voima, tahto käyttää tätä voimaa suvereniteetin suojaamiseen ja viestintä kahdesta ensimmäisestä elementistä. Voima voidaan käsittää valtion voiman instrumenteiksi esimerkiksi DIMEL-mallin kautta (Diplomacy, Information, Military, Economic, Legal). Tahto ilmenee valtiotason strategian muodossa, jolloin aikomus on suunniteltu ja toiminnalle on varattu resurssit. Vaikka kaikki kolme elementtiä ovat edellytys uskottavalle pelotteelle, on viestintä pelotteen keskiössä. Ilman selkeästi ilmaistua aikomusta, ei pelotteella ole mahdollisuuksia aikaansaada ennaltaehkäisevää vaikutusta potentiaalisen uhkatoimijan mielessä.

Klassisen peloteteorian mukainen perustavanlaatuinen kahtiajako hyökkäyksellisen ja puolustuksellisen näkökulman välillä on säilynyt läpi vuosikymmenten, vaikka rinnalle onkin noussut moderneja tulkintoja pelotteesta. Erityispiirre nykyajan peloteteorioissa on, etteivät ne poissulje toisiaan. Valtio voi valita näistä vaihtoehdoista omiin tarpeisiinsa sopivimman yhdistelmän. Valintoja tehdään esimerkiksi sen mukaan, missä, milloin, millä voimalla ja kenen kanssa omaa suvereniteettia puolustetaan. Pienen valtion pelotestrategia painottuu yleensä puolustuksellisiin valintoihin ja oman valtion alueella toimimiseen, usein uskottavuus- ja resurssisyistä.

Kyberpelotteen monet kasvot

Akateemisessa keskustelussa kyberpelotetta käsitellään erilaisista näkökulmista, joita ovat muun muassa kyber- tai sotilaallisten suorituskykyjen käyttö kyberhyökkäysten estämiseksi tai kybersuorituskykyjen käyttö konventionaalisten hyökkäysten ennaltaehkäisemiseksi. Valittu näkökulma vaikuttaa merkittävästi tutkimustuloksiin ja siihen, kuinka vaikeana tai toteuttamiskelpoisena kyberpelotetta pidetään.

Nykyään tutkijoiden huomio on kohdistunut kokonaisvaltaiseen pelotteeseen, jossa valtion kaikkia voiman instrumentteja käytetään sekä fyysisen että kybertoimintaympäristön suojaamiseksi. Osana tällaista kokonaisuutta kybersuorituskykyjen käyttö kybersuvereniteetin suojaamiseen on säilynyt relevanttina näkökulmana, koska kyberkeinot tarjoavat usein täsmällisimmän ja oikea-aikaisimman keinovalikoiman kohdata ja ennaltaehkäistä kyberhyökkäyksiä. Tässä artikkelissa keskitytään kyseiseen näkökulmaan.

Kybersuvereniteetille ei ole yhteisesti hyväksyttyä määritelmää. Esimerkiksi Euroopan unioni määrittelee sen mahdollisuudeksi toimia itsenäisesti digitaalisessa maailmassa. Tässä artikkelissa kybersuvereniteettia lähestytään kybertoimintaympäristön kolmen kerroksen kautta (fyysinen, looginen, käyttäjäkerros). Niinpä kybersuvereniteetilla tarkoitetaan valtion fyysisen ja digitaalisen kyberympäristön suojelemista, jossa inhimillinen näkökulma ilmenee kansalaisten ja heidän henkilötietojensa digitaalisen turvallisuuden varmistamisena.

Poiketen perinteisestä pelotteesta, joka epäonnistuu hyökkäyksen konkretisoituessa, kyberpelotetta ei nykyään lähestytä samanlaisen näkökulman kautta. On hyväksyttävä, että ennen pitkää kyberhyökkäys onnistuu, koska hyökkäysvektoreita on joko liikaa tai niistä kaikki eivät ole puolustajan tiedossa tai hallinnassa. Sen tähden kyberpelote ei voi olla absoluuttinen, mutta sen tulisikin keskittyä vakavimpien kyberuhkien ennaltaehkäisyyn.

Parhaimmillaan kyberpelote toimii opportunistisia uhkatoimijoita kohtaan, jotka voidaan vakuuttaa siitä, että toiminta aiheuttaa hyökkääjälle itselleen enemmän haittaa kuin kohteelle. Tällainen lähtökohta edellyttää jonkinasteista rationaalisuutta, eli olettamusta uhkatoimijan tekemästä hyöty-panossuhteen arvioimisesta. Sen sijaan irrationaalisesti toimivien uhkatoimijoiden kohdalla pelotevaikutuksen aikaansaaminen on erittäin haastavaa, koska nämä kiinnittävät vähemmän huomiota toiminnan kustannuksiin ja mahdollisiin seurauksiin. Vastaava ongelma koskee pelotetta yleisemminkin, mutta kybertoimintaympäristön erityispiirteet tekevät hyöty-panossuhteen laskemisesta mahdollisesti monimutkaisempaa kuin fyysisessä maailmassa.

Kyberpelotteen haasteita

Kybersuorituskykyjen käyttöön keskittyvä lähestymistapa pohjautuu usein klassiseen peloteteoriaan. Tämä on luonteva valinta, koska se tarjoaa teoreettisen viitekehyksen, johon kyberiin liittyviä erityisnäkökulmia on suhteellisen helppo peilata. Ongelma klassisen peloteteorian ja kyberpelotteen suorissa analogioissa liittyy kybertoimintaympäristön erityispiirteisiin verrattuna fyysiseen maailmaan. Tämä haaste on johtanut useisiin argumentteihin, joiden mukaan kyberpelote ei ensinkään ole mahdollista tai että se edellyttää klassisesta peloteteoriasta poikkeavaa lähestymistapaa.

Aiemmin mainittu, akateemisessa keskustelussa vallitseva yksimielisyys on, ettei kyberpelote voi olla absoluuttinen, koska aina lopulta jokin hyökkäys onnistuu. Siksi kyberpuolustus edellyttää priorisointia, sillä se ei voi olla kaikkialla yhtä vahva. Kyberpelote tulisikin ymmärtää hyökkäysten määrän vähentämisenä, ei niiden täydellisenä ennaltaehkäisynä. Tämä on yksi harvoista kyberpelotteen peruslähtökohdista, joista akateemisessa keskustelussa ollaan yksimielisiä.

Monet kyberpelotteeseen liittyvät haasteet johtuvat vaikeuksista attribuoida hyökkääjät sekä vastata hyökkäyksiin reaaliaikaisesti ja uskottavalla voimalla. Kybervastahyökkäysten haasteiksi on havaittu nopeuteen, tarkkuuteen ja toistettavuuteen liittyviä seikkoja sekä epävarmuus omien kyberhyökkäysten vaikutusten leviämisen hallinnasta. Potentiaalinen eskalaatioriski vastattaessa valtiollisten tahojen kyberhyökkäyksiin on tunnistettu länsimaissa yhdeksi epävarmuustekijäksi, ja haasteita aiheuttavat myös ei-valtiolliset (irrationaaliset) toimijat sekä omaan kybertoimintaan liittyvät oikeudelliset kysymykset. Edellä mainittuihin epävarmuustekijöihin liittyvä keskeinen haaste liittyy attribuutiokykyyn, joka ei rajoitu pelkästään hyökkääjän tunnistamiseen. Siihen sisältyy myös uskottavan todistusaineiston kerääminen sekä vastatoimien tekeminen hyväksyttäviksi poliittisten päättäjien sekä kansallisen ja kansainvälisen oikeuden näkökulmista. Tarkasteltaessa kyberpelotteen haasteita pelotteen kolmen elementin kautta, voidaan haasteita ja ratkaisuja niihin jäsentää systemaattisesti.

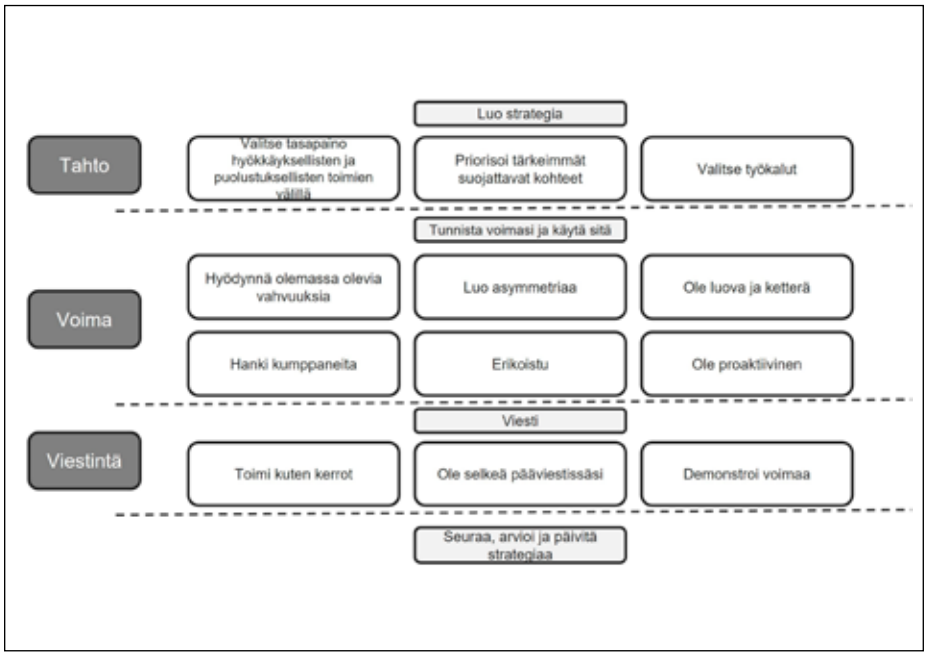
Valtion voima kybertoimintaympäristössä

Pelotteen ensimmäinen elementti, valtion voima, voidaan kybertoimintaympäristön näkökulmasta ymmärtää kyberkyvykkyyksien olemassaolona sekä hyökkäyksellisten ja puolustuksellisten kyberoperaatioiden toteuttamisena valtion pelotestrategian mukaisesti. Klassinen peloteteoria sisältää uhkaamisen voimankäytöllä, mutta ei voimankäyttöä itsessään, koska tällöin pelote on epäonnistunut. Tämä näkökulma ei kuitenkaan välttämättä ole optimaalinen kyberpelotteen kannalta. Päinvastoin, pelotevaikutuksen vahvistamiseksi saattaa olla hyödyllisempää toteuttaa proaktiivisia kyberoperaatioita kuin kokonaan pidättäytyä toiminnasta.

Pelotteen näkökulmasta hyökkäyksellisen kybervoiman käyttö on kybertoimintaympäristössä haasteellinen kokonaisuus, koska vastustajaa on vaikea uhata tuhoavalla voimalla pelkästään kyberkeinoin. Lisäksi kybervastatoimet voivat olla kertakäyttöisiä, sekä hyökkääjän identiteetti ja sijainti kybertoimintaympäristössä voivat olla vaikeasti määriteltävissä. Tämä herättää kysymyksen siitä, voiko hyökkäyksellinen kybervoima olla riittävän uskottavaa toimiakseen pelotteena. Tällainen näkemys perustuu rankaisupelotteeseen, jossa tuhoavan sotilaallisen voiman uhka saa vastustajan pidättäytymään hyökkäämisestä.

Puolustuksellisesta näkökulmasta kyberpelotteen ytimeen nousee kyky toipua hyökkäyksistä. Kun vastustaja ei saavuta hyökkäyksellään haluamaansa vaikutusta, se voi jo itsessään vähentää tämän halukkuutta hyökätä. Resilienssi on keskeinen kieltopelotteen tekijä, mutta kybertoimintaympäristö edellyttää myös aktiivisia keinoja hyökkääjän eristämiseksi ja vaikutusten lieventämiseksi. Pelkkään resilienssiin tukeutuminen poissulkee aloitteen tempaamisen, joka on hyökkäyksellisen kybervoiman keskeinen vahvuus. Lisäksi puolustuksellista kybervoimaa voidaan käyttää myös proaktiivisesti. Siten uskottavan kyberpelotteen rakentaminen edellyttää sekä hyökkäyksellisiä että puolustuksellisia kybertaktiikoita ja kaikkien valtion voiman instrumenttien hyödyntämistä kybersuvereniteetin suojaamiseen.

Pienen valtion näkökulmasta kybertoimintaympäristö voi tarjota mahdollisuuksia asymmetrian luomiseen ja sen hyödyntämiseen suurempaan uhkatoimijaan nähden. Tämä tosin edellyttää kykyä, tahtoa ja uskallusta hyödyntää puolustuksellisten kybersuorituskykyjen lisäksi myös hyökkäyksellistä voimaa, yksin tai yhdessä kumppanien ja liittolaisten kanssa. Länsimaissa ei tällaisista asioista juurikaan puhuta julkisesti ja akateemisessa keskustelussa esiintyy toistuvasti eskalaation pelko, vaikka tieteellinen todistusvoima tällaisen argumentoinnin taustalla on heikko. Kenties on oikeutettua kysyä, onko uhkatoimijamme pelote purrut länsimaihin, kun epäröimme käyttää hyökkäyksellisiä kybersuorituskykyjämme. Nyrkkeilyotteluun ei kuitenkaan kannata valmistautua kädet sidottuina selän taakse.



Kyberpelotteen teoreettinen malli.

Valtion tahto kybersuvereniteetin suojaamiseen

Pelotteen toinen elementti, tahto käyttää valtion voimaa sen suvereniteetin suojaamiseksi, ilmaistaan valtion strategiana. Strategian luominen ja tahtotilan kirjaaminen valtiotason asiakirjoihin edellyttää ymmärrystä siitä, miten valtion voiman instrumentteja halutaan käyttää asetetun tavoitetilan saavuttamiseksi. Tällaisen ymmärryksen kehittäminen edellyttää riittävää tieteellistä pohjaa esimerkiksi teoreettisen mallin muodossa.

Akateemiset pyrkimykset jäsentää kyberpelote ymmärrettävään muotoon ovat tuottaneet useita teoreettisia ja käytännöllisiä malleja. Nämä mallit perustuvat yleensä klassisen peloteteorian viitekehykseen ja rankaisu- ja kieltopelotetta täydennetään esimerkiksi yhteiskunnan resilienssillä, kyberdiplomatialla sekä innovatiivisella ja proaktiivisella kybersuorituskykyjen käytöllä. Ehdotetuille malleille on yhteistä ajatus siitä, ettei kyberpelotetta tulisi käsitellä erillisenä strategiana, vaan osana valtion kokonaisvaltaista pelotetta ja kyberturvallisuutta. Pienen valtion näkökulmasta tällainen kokonaisvaltainen lähestymistapa on erityisen kiinnostava, koska se mahdollistaa voimatasapainon kompensoinnin suurempaan vastustajaan nähden hyödyntämällä kaikkia valtion voiman instrumentteja pelotevaikutuksen luomiseen.

Kansallinen pelotestrategia ilmentää valtion tahtoa suojella suvereniteettiaan sekä fyysisessä maailmassa kuin kybertoimintaympäristössäkin. Se viestii sekä kansalaisille että muille valtioille, että asia on järjestelmällisesti suunniteltu, resursseja toiminnalle on osoitettu, ja valtio on valmis toimimaan turvallisuustilanteen edellyttämällä tavalla. Perusvalinta pelotestrategiassa tehdään hyökkäyksellisten ja puolustuksellisten toimintamallien painotuksessa erilaisiin tilanteisiin. Tämän jälkeen valitaan sopivat valtion voiman instrumentit ja määritellään suojeltavat kohteet, kuten esimerkiksi kybertoimintaympäristössä sijaitsevat yhteiskunnan elintärkeät toiminnot.

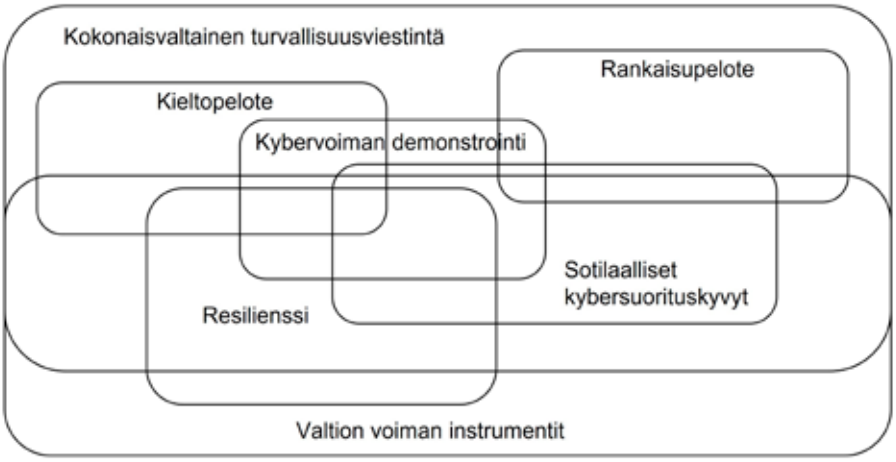
Valtion kyberpeloteviestintä

Pelotteen kolmas elementti on peloteviestintää tahdosta käyttää valtion voimaa sen suvereniteetin suojaamiseen. Kyberpelotteen osalta tämä tarkoittaa sitä, että valtio viestii kyberhyökkäyksestä koituvan seurauksia. Joidenkin tutkimusten mukaan on hyödyllistä vetää raja sallitun ja tuomittavan toiminnan välille sekä määritellä, millainen toiminta johtaa vastatoimiin. Näiden rajojen viestiminen voi lisätä pelotteen selkeyttä ja uskottavuutta. Pienelle valtiolle tämä voi kuitenkin merkitä vähiä resursseja kuluttavaa riskiä, jos uhkatoimija testaa toistuvasti näitä julkilausuttuja rajoja. Esimerkiksi Suomen näkökulmasta Venäjän voitaisiin olettaa toimivan juuri näin, jolloin ei ole kannattavaa julkisesti julistaa selkeitä rajoja.

Kybertoimintaympäristössä peloteviestintää heikentävät usein salassapito ja narratiivien epäselvyys. Valtiot haluavat usein pitää todelliset kyberkyvykkyytensä piilossa, jolloin niillä ei ole samaa mahdollisuutta voiman demonstrointiin kuin fyysisessä ympäristössä. Silti pelotteen ydin on voimasta viestiminen ja ilman tällaista narratiivia pelotetta ei ole. Siksi kyberpelotetta koskevassa tutkimuksessa on pyritty löytämään keinoja kybervoiman osoittamiseen ilman, että valtion kyberkyvykkyyksistä paljastetaan liikaa.

Sodankäynti on valtiolle yksiselitteisin tapa osoittaa sotilaallista voimaansa. Koska pelotteen tarkoitus on estää aggressio, voimaa on demonstroitava ennen kuin jännitteet kärjistyvät aseelliseksi konfliktiksi. Normaaliaikoina valtiot voivat osoittaa sotilaallista voimaansa esimerkiksi sotaharjoituksilla, yksin ja yhdessä muiden kanssa. Näitä keinoja voidaan käyttää myös hankalammin paljastettavan voiman, kuten kybersuorituskykyjen, demonstrointiin.

Huolimatta valtioiden halusta salata todelliset kybersuorituskykynsä, useat tutkimukset keskittyvät kybervoiman demonstrointiin tosielämän tilanteissa. Näiden tutkimusten mukaan kyberpelotetta voidaan signaloida erityisesti jatkuvilla kyberoperaatioilla ja -kampanjoilla. Jatkuvat kyberoperaatiot viestivät uhkatoimijalle valtion kypsyydestä suojautua ja vastata kyberhyökkäyksiin. Puolustajan näkyvä läsnäolo kybertoimintaympäristössä voi toimia kieltopelotteen yhtenä



Valtion turvallisuusstrategioiden ja kyberturvallisuuteen liittyvien keskeisten elementtien limittyminen toisiinsa.

elementtinä ja näin vähentää uhkatoimijan hyökkäyshaluja. Omien kybersuorituskykyjen paljastaminen voi kuitenkin aiheuttaa riskejä, kuten vastustajan pääsyn oman järjestelmän sisään.

Hallittu kybersuorituskykyjen paljastaminen edellyttää valintoja tehokkaan peloteviestinnän ja valtion turvallisuuden säilyttämisen välillä. Mikäli voimaa halutaan demonstroida tosielämän kybertoiminnalla, on teoreettisesti esitetty vaihtoehtoja asian toteuttamiseen. Esimerkiksi kyberoperaatioista voidaan paljastaa valittuja seikkoja, kuten vaikkapa attribuutiokyvykkyys jättäen kuitenkin tekniset yksityiskohdat salaisiksi. Akateemisessa keskustelussa tällainen hallittu kyberpeloteviestintä vaikuttaa sarjalta yksinkertaisia valintoja, mutta tosielämä lienee monimutkaisempi kokonaisuus ja kybersuorituskykyjen demonstrointi pitkälti tapauskohtaista.

Tosielämän kybertapahtumista viestimisen lisäksi valtio voi hyödyntää muitakin elementtejä kyberpelotteessaan. Esimerkiksi yhteiskunnan ja siellä toimivien tahojen, kuten viranomaisten ja kaupallisten yritysten, kyberkypsyydestä viestiminen muun muassa teknologisten innovaatioiden, sotilaallisten harjoitusten, tutkimuksen ja osaamisen kautta luovat mielikuvia valtion kyvystä vastata kyberuhkiin. Kokonaisuuden kannalta olennaista on systemaattisesti viestiä valtion maturiteetista kybertoimintaympäristön toimijana yhteisen ydinnarratiivin mukaisesti, pienetkin voitot hyödyntäen.

Yhteenveto

Akateemisessa keskustelussa oiotaan usein mutkia ja asiat muotoillaan näennäisesti yksikertaisiksi teorioiksi. Tosielämä on kuitenkin monimutkainen kokonaisuus, jossa tieteellisiä teorioita voidaan toki hyödyntää pelotteen muodostamiseen, mutta todennäköisemmin lopputulos on kudelma valtion turvallisuuteen liittyviä elementtejä, joiden välille ei ole aina kannattavaa piirtää rajoja. Tämä pätee myös kyberpelotteeseen.

Valtion suvereniteettiin kybertoimintaympäristössä liittyy monenlaisia elementtejä. Esimerkiksi yhteiskunnan resilienssi vankistaa turvallisuutta kybertoimintaympäristön jokaisella kerroksella ja vahvistaa myös kyberpuolustusta. Keinovalikoima kyberturvallisuuden, kyberpuolustuksen ja kyberpelotteen vahvistamiseen on pitkälti yhtenevä ja perustuu valtion kykyyn suojata kybertoimintaympäristöä sen kaikilla kerroksilla sekä ennaltaehkäistä siihen kohdistuvia hyökkäyksiä. Samoin valtion voiman instrumentteja, kuten vaikkapa kyberdiplomatiaa, käytetään saumattomasti näiden kolmen kokonaisuuden mahdollistamiseksi. Pienen valtion näkökulmasta olemassa olevien vahvuuksien hyödyntäminen peloteviestintään voi parhaimmillaan

olla erittäin kustannustehokasta, mikäli aikeet konkretisoituvat toiminnaksi tilanteen niin vaatiessa.

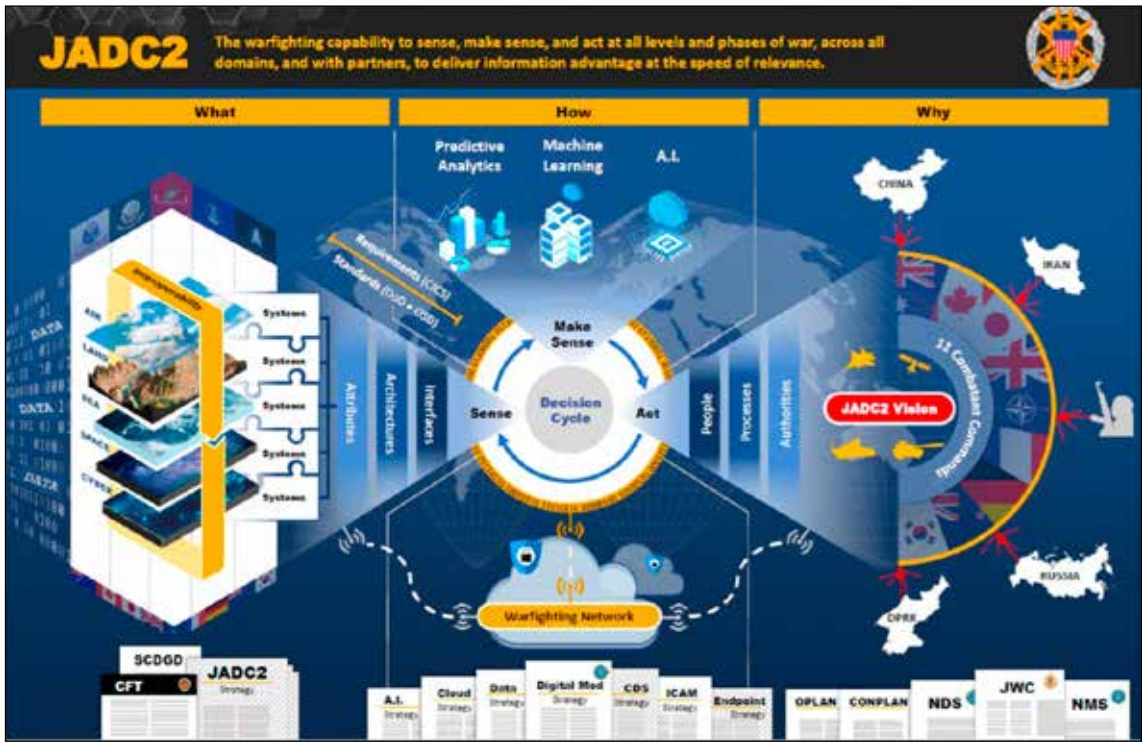
Ideaalitilanteessa kyberpelote nivoutuu saumattomasti valtion kokonaisvaltaiseen pelotestrategiaan. Tällöin valtion tahto suojata suvereniteettiaan fyysisen maailman lisäksi myös kybertoimintaympäristössä on tunnistettu sekä keinot siihen ovat suunniteltu ja kirjattu strategian muotoon. Samalla tällainen tahdon ilmaus itsessään toimii viestinä eri kohdeyleisöille. Perustavanlaatuinen valinta tehdään hyökkäyksellisten ja puolustuksellisten lähestymistapojen välillä ja tasapainossa, klassisen peloteteorian periaatteiden mukaan.

Tehokkaimmillaan peloteviestintä on osa valtion strategista ja kokonaisvaltaista turvallisuusviestintää, jonka ydinnarratiivi räätälöidään kohdeyleisön mukaan. Kohdeyleisöinä eivät ole vain potentiaaliset uhkatoimijat, vaan myös kumppanit ja liittolaiset sekä oman maan kansalaiset. Näin ollen systemaattisesti toteutettu strateginen turvallisuusviestintä tavoittaa yhdellä sanomalla monta yleisöä, joko luoden luottamusta tai aiheuttaen epävarmuutta. Yhteisen ydinnarratiivin käyttö yksinkertaistaa ja selkeyttää viestiä myös pelotteen näkökulmasta.

Tärkeintä kyberpelotteen muodostamisessa ei ole termin käyttö itsessään. Oleellisempaa on tunnistaa kybersuvereniteetin suojaamiseen liittyen valtion tahto, voima ja keinovalikoima sekä ne tavat, joilla edellä mainituista elementeistä viestitään kohdeyleisöille. Kybermaturiteetti syntyy pitkän ajan kuluessa, samoin kyberpelote. Kyseessä onkin ennen kaikkea valtion maine kybertoimintaympäristön toimijana. Tietynlaisen maineen luominen edellyttää pitkäjänteisyyttä ja systemaattisuutta kaikessa toiminnassa. Voidaankin todeta, että huomisen pelote luodaan tänään.

Artikkeli perustuu kirjoittajan väitöstutkimukseen Cyber Deterrence of a Small State. Kirja on ladattavissa osoitteesta https://www.doria.fi/handle/10024/193552.

TEKSTI: LAURI HYRY



Yhdysvaltain puolustushallinnon JADC2-viitekehystä kuvaava havainnekuva (lähde: U.S. Department of Defense, Joint All-Domain Command and Control Strategy, 2022).

Datakeskeinen ja algoritminen sodankäynti – katsaus johtamisjärjestelmien kehitykseen länsimaissa

Sotilaallisten johtamisjärjestelmien kehityksessä on käynnissä perustavanlaatuinen murros. Kyse ei ole yksittäisistä uusista teknologioista. Kyse on siitä, miten johtaminen toimii tilanteessa, jossa tietoa on enemmän kuin koskaan ja aikaa sen hyödyntämiseen vähemmän kuin koskaan.

Kehityssuunta näkyy konkreettisesti Yhdysvalloissa, Iso-Britanniassa ja Ukrainassa. Yhdysvalloissa kehitystä kokoaa Combined Joint All-Domain Command and Control (CJADC2) -ajattelu. Iso-Britanniassa puolestaan pyritään vastaamaan haasteeseen Digital Targeting Web (DTW) -konseptilla. Ukrainassa ratkaisuja on syntynyt sotaa käyvän maan käytännön tarpeista. Toteutukset eroavat toisistaan, mutta peruskysymys on sama. Miten monimutkaistuvassa ympäristössä tehdään parempia ja nopeampia päätöksiä kuin vastustaja?

Tulevissa konflikteissa päätöksentekoon käytettävissä oleva aika mitataan minuuteissa tai jopa sekunneissa. Samalla toimintaympäristö monimutkaistuu ja vaikutuksia tuotetaan yhtä aikaa maa-, meri-, ilma-, avaruus- ja kybertoimintaympäristöissä. Tämä yhdistelmä asettaa perinteiset johtamisjärjestelmät haasteeseen. Ihmistyöhön nojaava malli ei kykene käsittelemään havaintojen määrää eikä koordinoimaan vaikutuksia riittävällä nopeudella. Tarvitaan tukea päätöksentekoon.

Tässä artikkelissa tarkastellaan, miksi datakeskeinen ja algoritminen sodankäynti on noussut keskeiseksi kehityssuunnaksi. Lisäksi arvioidaan, mitä kansainvälisistä kokemuksista voidaan realistisesti oppia Suomen puolustuksen näkökulmasta.

Johdanto

Sotilaallisten johtamisjärjestelmien perimmäinen tehtävä on pysynyt muuttumattomana: tukea komentajaa päätöksenteossa epävarmassa ja vastustajan aktiivisesti häiritsemässä toimintaympäristössä. Toimintaympäristön luonne on kuitenkin muuttunut olennaisesti. Nykyiset sensorit, järjestelmät ja verkot tuottavat enemmän dataa kuin yksikään organisaatio tai johtamisrakenne kykenee käsittelemään perinteisin menetelmin. Samanaikaisesti päätöksenteon aikajänteet ovat lyhentyneet.

Tässä ympäristössä johtamisjärjestelmien keskeinen haaste on tiedon käsittely ja jakaminen päätöksenteon kannalta merkitykselliseksi kokonaisuudeksi. Datakeskeinen johtaminen ja tekoälyn hyödyntäminen vastaavat tähän haasteeseen. Niiden tarkoituksena ei ole korvata inhimillistä johtamista, vaan tukea sitä tilanteessa, jossa käsittelykyky ei enää riitä kokonaisuuden hallintaan. Kyse on siitä, miten datasta rakennetaan jaettu ymmärrys, miten päätöksentekoa tuetaan eri tasoilla ja miten johtaminen säilyy toimintakykyisenä myös häirityissä ja katkonaisissa olosuhteissa.

Yhdysvaltain kolmas offset -strategia – algoritmisen ja datakeskeisen sodankäynnin synty

Datakeskeisen ja algoritmisen sodankäynnin juuret voidaan vetää Yhdysvaltojen 2010-luvun puolivälissä julkaisemaan kolmanteen offset -strategiaan. Strategian taustalla oli havainto, että Yhdysvaltojen sotilaallinen etumatka oli kaventumassa vastustajiin nähden. Sillä välin, kun USA:n huomio oli pitkään keskittynyt Irakin ja Afganistanin operaatioihin, Kiina ja Venäjä olivat kehittäneet kyvykkyyksiä, jotka haastoivat Yhdysvaltojen sotilaallisen etumatkan.

Kolmannen offset -strategian ytimessä ei ollut yksittäinen teknologinen ratkaisu. Kyse oli ajattelutavan muutoksesta. Kilpailun nähtiin siirtyvän kohti päätöksenteon nopeutta ja laatua. Tämä korostui tilanteessa, jossa sensorien ja järjestelmien tuottaman datan määrä ylitti inhimillisen käsittelykyvyn. Tekoäly, koneoppiminen ja autonomia nousivat keinoiksi tukea johtamista. Niiden tehtävänä oli jalostaa hajanaisesta tiedosta päätöksenteon kannalta olennaista ymmärrystä.

Tämä ajattelu loi perustan algoritmiselle ja datakeskeiselle sodankäynnille. Strategian perusajatuksen mukaan kilpailuetu ei synny yksittäisistä asejärjestelmistä vaan se syntyy kyvystä yhdistää dataa, tukea päätöksentekoa ja toimia vastustajaa nopeammin. Kolmas offset -strategia ohjaa sotilaallista kehitystä kohti järjestelmätason ja johtamisen uudistamista. CJADC2 voidaan nähdä tämän kehityskulun jatkumona. Sen tavoitteena on viedä strategian periaatteet pysyviksi ja yhteistoiminnallisiksi rakenteiksi.

Yhdysvaltojen puolustushaarojen CJADC2 -suurhankkeet

Combined Joint All-Domain Command and Control (CJADC2) ei ole yksittäinen ohjelma tai järjestelmä. Se on strateginen viitekehys, jonka tavoitteena on muuttaa sotilaallisen johtamisen tapaa. CJADC2 pyrkii yhdistämään eri puolustushaarojen ja toimintaympäristöjen tuottaman tiedon yhteiseksi päätöksenteon perustaksi. Tavoitteena on lyhentää aikaa havainnosta päätökseen ja vaikutukseen.

CJADC2:n ydin on päätöksentekonopeudessa ja vaikuttamisen tehokkuudessa. Tulevissa konflikteissa päätöksiä on tehtävä minuuteissa tai jopa sekunneissa. Samalla toimintaympäristö on moniulotteinen. Vaikutuksia tuotetaan yhtä aikaa maa-, meri-, ilma-, avaruus- ja kybertoimintaympäristöissä. Perinteinen, ihmistyöhön nojaava johtamismalli ei enää riitä. Tämän vuoksi CJADC2 nojaa laajasti datan hyödyntämiseen, automaatioon ja tekoälyyn. Dataa yhdistämällä pyritään hahmottamaan tilanne, tunnistamaan vaihtoehdot ja kohdentamaan vaikutukset yli domain- ja organisaatiorajojen.

Käytännössä CJADC2 ei toteudu yhtenä keskitettynä kokonaisuutena. Sen toimeenpano on hajautunut puolustushaarojen omiin kehityshankkeisiin. Yhdysvaltain ilmavoimat kehittävät kokonaisuutta Advanced Battle Management System -ohjelman kautta. Merivoimien panos rakentuu Project Overmatch -hankkeen ympärille. Maavoimat vievät vastaavaa ajattelua eteenpäin Project Convergence -kokonaisuudessa. Lisäksi avaruus- ja kybertoimintaympäristöjen kyvykkyydet kytkeytyvät kokonaisuuteen omien kehityspolkujensa kautta.

Esimerkkinä konkreettisesta toimesta CJADC2-kyvykkyyden rakentamisessa voidaan nostaa US Armyn merkittävä kehityshanke: Next Generation Command and Control (NGC2). Kyseessä on täysin clean sheet -lähestymistapa, jossa US Armyn uusi C2-järjestelmä rakennetaan alusta asti ilman ”legacyä”. Tavoitteena on saada ratkaisu käyttöön 30 kuukaudessa. Hankkeen taustalla on tunnistettu tarve modernisoida C2 -tietojärjestelmät. Kokemukset Ukrainasta ja Israelista sekä uhka-arviot INDOPACOMin alueelta ovat osoittaneet, että nykyiset järjestelmät ei tue riittävästi komentajia laajamittaisissa taistelutoiminnoissa.

“NextGenC2 is a data-centric, end-to-end command and control warfighting system. It’s built on four interdependent layers: Applications – simple, intuitive user interfaces; Data – sharing and interoperability at the core; Infrastructure – cloud-native but not cloud-dependent; Transport – resilient, intelligent networks. It’s about putting the commander back in command — enabling faster, better decisions.”

— BG Michael Kaloostian C2 Cross-Functional Team Director

Yhteenvetona voidaan todeta, että CJADC2 on koko puolustushallinnon laajuinen toimintamalli, jonka tavoitteena on varmistaa yhteinen tilannekuva, nopea päätöksenteko ja vaikuttaminen kaikissa toimintaympäristöissä, myös häirityissä ja kiistetyissä olosuhteissa. Kyse ei ole yksittäisistä järjestelmistä, vaan enterprise -tason muutoksesta, jossa data, teknologia ja ihmiset yhdistetään yhteiseksi päätöksentekokyvyksi. CJADC2:n ytimessä on kyky integroida tietoa yli domain- ja organisaatiorajojen, muuttaa data ymmärrykseksi ja tukea komentajan päätöksiä

Tekoäly osana Yhdysvaltojen CJADC2 -kehitystä

Project Maven oli yksi ensimmäisistä hankkeista, joissa tekoälyä hyödynnettiin laajamittaisesti operatiivisen johtamisen tukena. Se syntyi konkreettisesta tarpeesta käsitellä valtavia määriä sensoridataa, erityisesti droonien tuottamaa videomateriaalia. Ihmistyöhön perustuva analyysi ei enää riittänyt. Maven osoitti nopeasti, että tekoäly voi tuottaa todellista operatiivista arvoa. Tilannekuva parani ja päätöksenteko nopeutui.

Project Mavenin myötä kävi kuitenkin ilmeiseksi, että yksittäinen toimiva ratkaisu ei vielä ratkaise kokonaisuutta. Jokai-

nen uusi käyttötapaus edellyttää erillistä integraatiota, omia tietovirtoja ja omia ylläpitokäytäntöjä. Kokemusten myötä alettiin hahmottaa laajempi ilmiö. Kyse ei ollut siitä, toimiiko tekoäly, vaan siitä, miten sen käyttöä voidaan toistaa, ylläpitää ja laajentaa. Tätä eroa on helppo jäsentää käsitteillä kyvykkyys (Capability) ja kapasiteetti (Capacity). Kyvykkyys tarkoittaa, että jokin voidaan tehdä taistelukentällä. Kapasiteetti kertoo, kuinka laajasti ja kuinka pitkään tätä voidaan tehdä.

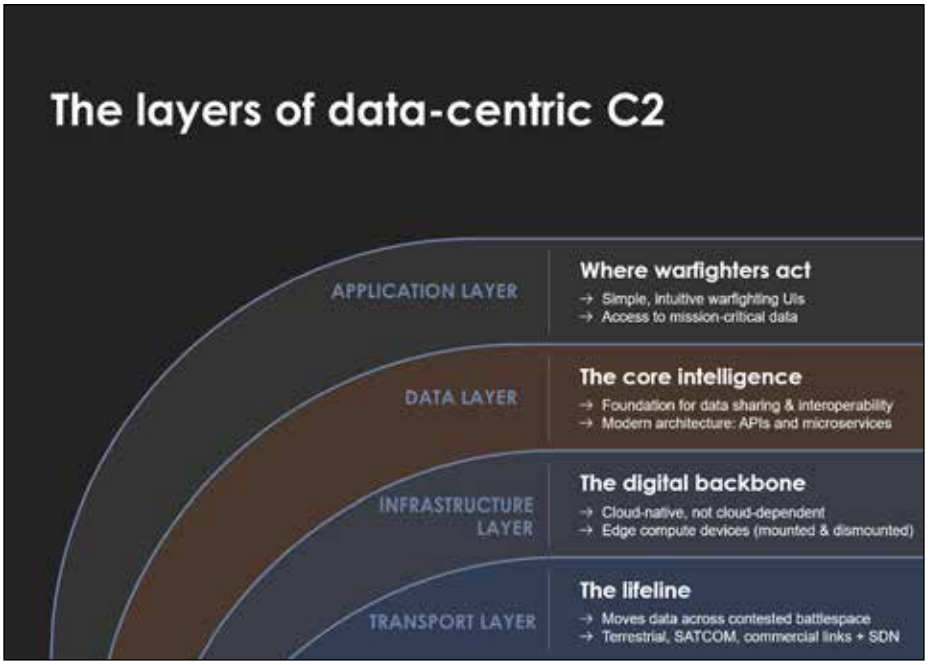
"The military's general philosophy toward AI has created a problem where the enterprise is focused on the development of capability without sufficiently considering capacity. Capability means we can do something on the battlefield. Capacity is the measurement of how much of that thing we can do. A good historical example of this is the Germans in WWII. Their tanks were the best, but we had way more pretty good tanks."

— Bradley L. Boyd, Visiting Fellow, Hoover Institution; Lecturer, Stanford University

Vertaus tekee algoritmisen sodankäynnin perusongelman näkyväksi. Yksittäinen tekoälysovellus, kuten automaattinen maalin tunnistus, voi toimia erinomaisesti ainakin alkuvaiheessa. Vastustajan mukautuessa tilanne kuitenkin muuttuu. Tunnisteet vaihtuvat, data vanhenee ja mallit alkavat menettää tehoaan. Tällöin ratkaisevaa ei ole enää se, toimiiko algoritmi jossakin yksittäisessä tilanteessa, vaan se, kuinka nopeasti ja kuinka kattavasti sitä voidaan päivittää ja ottaa käyttöön koko joukon tasolla. Ilman tätä kapasiteettia kyvykkyys jää väistämättä paikalliseksi ja hetkelliseksi.

Tässä kontekstissa Yhdysvaltain armeijan Project Linchpin nousee keskeiseksi. Linchpin ei ole uusi tekoälysovellus eikä operatiivinen johtamisjärjestelmä, vaan yritys rakentaa yhteinen ohjelmisto- ja datainfrastruktuuri, jonka varaan tekoälykyvykkyydet voidaan aidosti skaalata. Sen painopiste on yhteisissä datastandardeissa, mallien elinkaaren hallinnassa ja turvallisissa jakelumekanismeissa, jotka mahdollistavat ohjelmistojen ja datamallien päivittämisen myös hajautetuissa ja häirityissä ympäristöissä. Kyse ei ole ensisijaisesti tekoälystä, vaan ohjelmistoista ja datasta. Tekoäly on vain yksi ohjelmistotyyppi muiden joukossa.

Linchpinin merkitys korostuu juuri suhteessa Maveniin. Project Maven osoitti, että tekoäly voi tukea päätöksentekoa. Linchpin pyrkii varmistamaan, että tämä tuki ei romahda ensimmäisen vastustajan mukautumisen jälkeen. Se siirtää painopisteen yksittäisten sovellusten rakentamisesta infrastruktuuriin, joka mahdollistaa jatkuvan sopeutumisen.



Datakeskeisen johtamisjärjestelmän kerrosmalli. Kirjoittajan tulkinta Yhdysvaltojen maavoimien Next Generation Command and Control (NGC2) -ajattelusta.

Iso-Britannia ja Digital Targeting Web: kunnianhimoinen konsepti

Digital Targeting Web on Iso-Britannian puolustushallinnon vastaus pitkään tunnistettuun ongelmaan, kykyyn yhdistää eri puolustushaarojen ja toimintaympäristöjen tiedustelu, päätöksenteko ja vaikuttaminen toimivaksi kokonaisuudeksi. Kyse ei ole yksittäisestä järjestelmästä, vaan laajasta käsitteellisestä kehyksestä, jonka tavoitteena on integroida olemassa olevia ja kehittyviä kyvykkyyksiä koko puolustuksen laajuisesti. Lähtökohtana on ajatus, että sodankäynnin nopeuden, tarkkuuden ja vaikuttavuuden kasvu edellyttää yhteistä digitaalista perustaa, jossa data liikkuu nopeasti ja tarkoituksenmukaisesti.

Käytännössä Digital Targeting Web yhdistää havainnoinnin, päätöksenteon ja vaikuttamisen verkkomaiseksi kokonaisuudeksi. Sensorit eri toimintaympäristöissä tuottavat dataa, jota jalostetaan päätöksenteon tueksi. Keskeistä ei ole tiedon määrän lisääminen, vaan epävarmuuden vähentäminen suodatuksen ja priorisoinnin avulla. Tekoäly ja automaatio tukevat erityisesti datan käsittelyä ja jakelua, jotta tieto saadaan nopeasti oikealle tasolle.

UK:n kehitys kokonaisuuteen on liittynyt myös kritiikkiä. Royal United Services Instituten (RUSI) näkemyksen mukaan Digital Targeting Webin keskeiset haasteet eivät ole ensisijaisesti teknologisia, vaan organisatorisia ja hallinnollisia. Kyseessä ei ole projekti eikä ohjelma, vaan kehys, jolle ei ole määritelty selkeää lopputilaa tai mitattavia tavoitteita. Tämä vaikeuttaa edistymisen arviointia ja altistaa kehityksen etenemiselle ilman todellista vaikutusta johtamiseen.

RUSI:n arvion mukaan haastetta asettaa myös se, että toimeenpano on hajautunut useille toimijoille, eikä yhdelläkään ole kokonaisvastuuta budjetista tai päätösvallasta. Hajautettu malli tukee joustavuutta, mutta samalla se lisää riskiä, että vanhat siilot ja puolustushaarakohtaiset ratkaisut säilyvät. Myös rahoituksen ja teollisen osallistumisen ajoitus suosii suuria toimijoita ja kaventaa innovaatiopohjaa.

Johtopäätöksenä voidaan todeta, että Digital Targeting Web on ennen kaikkea johtamis- ja toimeenpanokysymys. Suurin osa tarvittavista teknologioista on jo olemassa, mutta ne ovat hajallaan. Onnistuminen edellyttää selkeää ohjausta, mitattavia tavoitteita ja pitkäjänteistä resursointia, jotta konsepti ei jää kunnianhimoiseksi visioksi.

Ukraina: Käytännön sanelema lähestymistapa datakeskeiseen johtamiseen

Ukrainan kehitys datakeskeisessä johtamisessa poikkeaa selvästi länsimaisista lähestymistavoista. Siinä missä Yhdysvalloissa ja Iso-Britanniassa on rakennettu viitekehyksiä ja ohjelmia, Ukrainassa vastaava kyvykkyys on syntynyt sotaa käyvän maan käytännön ratkaisuna. Keskiössä on Delta -järjestelmä, joka on kehittynyt nopeasti tilannekuvakartasta laajaksi ohjelmistoekosysteemiksi.

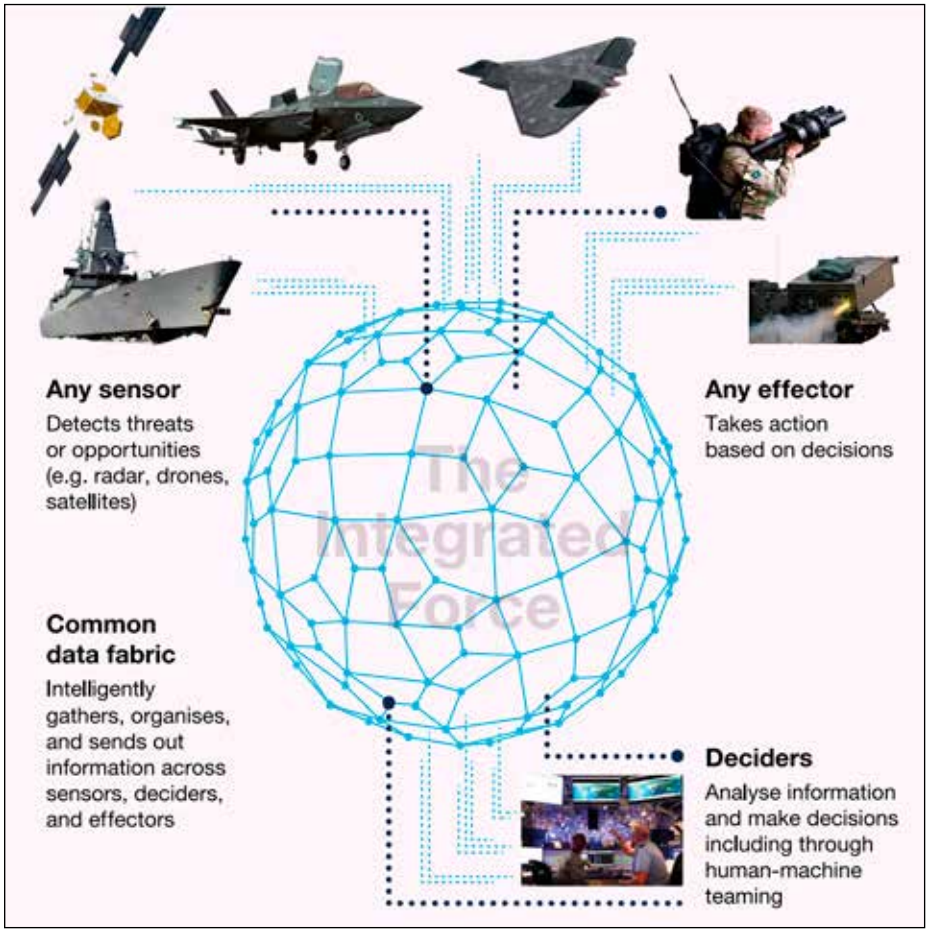
Deltan perusidea on ollut pragmaattinen. Dataa kerätään eri lähteistä, yhdistetään yhteiseen näkymään ja hyödynnetään nopeasti eri johtamistasoilla. Järjestelmää käytetään sekä etulinjassa että ylemmillä tasoilla, mikä on lyhentänyt tiedonvälitysketjuja. Teknologisesti Delta edustaa ohjelmistokeskeistä ajattelua, jossa karttapohjaisen käyttöliittymän päälle rakennetaan sovelluksia tarpeen mukaan.

Ukrainan lähestymistapa on korostetun ”bottom-up”. Se on mahdollistanut nopean iteroinnin ja sopeutumisen muuttuvaan taistelukenttään, mutta samalla tuonut mukanaan haasteita. Nopeasti syntyneet ratkaisut eivät aina ole yhtenäisiä, dokumentaatio voi jäädä jälkeen ja yhteensovittaminen vaatii jatkuvaa työtä. Ilman keskitettyä ohjausta paikallisesti toimivat ratkaisut voivat olla vaikeasti skaalattavia.

Ukrainan kokemus osoittaa, että ratkaisuja voidaan rakentaa nopeasti käytännön tarpeista käsin, mutta se ei vapauta hallinnan, standardoinnin ja pitkäjänteisen ylläpidon tarpeesta. Todellinen haaste on tasapainon löytäminen ketteryyden ja hallittavuuden välillä. Juuri tässä Ukraina tarjoaa arvokkaita oppeja länsimaisille kehityshankkeille.

Opit Suomelle: mitä datakeskeisestä johtamisesta on ymmärrettävä

Tämän artikkelin keskeisin opetus Suomen kannalta on, että datakeskeinen johtaminen ei ole järjestelmävalinta vaan kyky tuottaa parempia ja nopeampia päätöksiä häirityssä ja epävarmassa toimintaympäristössä. Edellä mainituista kokonaisuuksista voidaankin nostaa kolme keskeistä nostoa mitä onnistuminen vaatii: selkeää ja mitattavaa tavoiteasetantaa, datan käsittelyä johtamisen perusinfrastruktuurina sekä kykyä erottaa kyvykkyys kapasiteetista.



Digital targeting web osana Ison-Britannian puolustushallinnon Integrated Force -mallia (lähde: UK Ministry of Defence, Strategic Defence Review 2025, s. 49).

Ensimmäinen ja kaikkein ratkaisevin oppi liittyy tavoiteasetantaan. Datakeskeinen johtaminen ei voi edetä pelkkänä viitekehyksenä tai kehityssuuntana, vaan sillä on oltava selkeä ja mitattava päämäärä. Ilman konkreettista lopputilaa, omistajuutta ja mittareita kehitys uhkaa jäädä jatkuvaksi tekemiseksi, jonka vaikutus päätöksentekokykyyn jää epäselväksi.

Toinen oppi on, että data on johtamisen perusinfrastruktuuria. Yksikään tarkastelluista esimerkeistä ei onnistunut tekoälyn tai analytiikan hyödyntämisessä ilman yhteistä datapohjaa, standardeja ja ohjelmistokäytäntöjä. Suomelle tämä tarkoittaa, että datan saatavuus, laatu, luokittelu ja päivitettävyys on otettava tekemisen keskiöön.

”JADC2 is all about data. It’s about standardizing our data. It’s about how we transport the data, how we store the data and how we secure it. We talk a lot about machine learning and artificial intelligence, but until you deal with the data problem, you really don’t have a system.”
— **General James C. McConville**, U.S. Army Chief of Staff (2019-2023)

Kolmas oppi on kyvykkyyden ja kapasiteetin erottaminen. Yksittäinen hyvin toimiva sovellus tai kokeilu ei vielä muodosta sotilaallista suorituskykyä, jos sitä ei pystytä ottamaan käyttöön laajasti, ylläpitämään pitkään ja päivittämään vastustajan sopeutuessa. Pienen maan etu ei ole monien erikoisratkaisujen rakentaminen, vaan sellaisten ratkaisujen kehittäminen, jotka toimivat ja kestävät myös kriisin ja sodan kuormituksen.

Mainittujen kolmen keskeisimmän opin lisäksi kehityksen organisointitapa on keskeinen tekijä onnistumisessa. Ukrainan kokemus osoittaa, että käyttäjälähtöinen bottom-up -kehitys voi tuottaa nopeasti toimivia ratkaisuja, mutta ilman ohjausta se pirstaloituu. Yhdysvaltojen ja Iso-Britannian kokemukset puolestaan osoittavat, että puhtaasti top-down -mallit ovat usein hitaita ja jäykkiä. Toimivin malli onkin todennäköisesti näiden yhdistelmä: kentällä syntyvät kokeilut sallitaan, mutta ne kytketään varhaisessa vaiheessa yhteisiin periaatteisiin, rajapintoihin ja päätöksentekoon, ja niille määritellään selkeä polku jatkoon.

Huomionarvoista on myös se, että merkittävä osa dataan ja tekoälyyn liittyvästä kehityksestä syntyy perinteisen puolustussektorin ulkopuolella. Erityisesti Yhdysvaltojen kokemukset osoittavat kaupallisen ohjelmisto- ja teknologiasektorin keskeisen roolin. Tämä haastaa perinteiset hankintamallit ja korostaa tarvetta joustavammille yhteistyömuodoille, joiden avulla uusia toimijoita voidaan tuoda mukaan ilman raskasta byrokratiaa, mutta puolustuksen erityisvaatimukset säilyttäen.

Lopulta on ymmärrettävä, että datakeskeinen ja tekoälyä hyödyntävä johtaminen on johtamiskulttuurin muutos, ei IT-hanke. Teknologia voi tukea päätöksentekoa, mutta se ei poista epävarmuutta, vastuuta eikä sodankäynnin kitkaa.

Yhteenveto

Tässä artikkelissa tarkastellut Yhdysvaltojen, Iso-Britannian ja Ukrainan esimerkit osoittavat, että datakeskeinen johtaminen ei ole valmis ratkaisu tai yksittäinen malli, vaan joukko valintoja, joilla pyritään tukemaan päätöksentekoa tilanteessa, jossa dataa on enemmän kuin koskaan ja toimintaympäristö on häiritympi kuin koskaan. Samalla ne osoittavat, että jokainen lähestymistapa sisältää myös selkeitä rajoitteita. Nopeus ja integraatio törmäävät hallittavuuteen, kunnianhimo realismiin ja teknologiset lupaukset sodankäynnin reunaehtoihin.

On tärkeää tunnistaa myös tämän tarkastelun rajat. Datakeskeinen ja algoritminen sodankäynti on kokonaisuutena valtava, ja merkittävä osa siihen liittyvästä kehityksestä jää väistämättä julkisen tarkastelun ulkopuolelle. Avoimissa lähteissä esitellyt järjestelmät, konseptit ja kokeilut ovat valikoituja, osin keskeneräisiä ja usein tarkoituksellisesti viestinnällisesti muotoiltuja. Ne palvelevat kehittämisen ohella deterrenssiä ja sisältävät väistämättä myös markkinointipuhetta, niin teollisuuden kuin puolustushallintojenkin toimesta. Julkinen kuva kertoo suunnasta ja kunnianhimosta, ei koko todellisuudesta.

PS. Tutkimusmatka aiheeseen jatkuu. Juuri tätä artikkelia viimeistellessäni postilaatikkooni kilahti Amos Foxin ja Franz-Stefan Gadyn tuore teos Multi-domain Operations: The Pursuit of Battlefield Dominance in the 21st Century. Kirja tarkastelee multi-domain -operointia sen syntyhistorian, käytännön soveltamisen ja akateemisen kritiikin kautta sekä esittää terävän väitteen: MDO on monin paikoin kehittynyt ratkaisuksi, joka lupaa enemmän kuin se kykenee toimittamaan. Fox ja Gady kuvaavat MDO-ajattelua strategisesti kapeaksi, taktisesti epämääräiseksi ja osin huonosti sovitettavaksi liittolaisten erilaisiin realiteetteihin.

Jos tämä kirjoitus herättää ajatuksia, kysymyksiä tai eriäviä näkemyksiä, keskustelen niistä mielelläni.

Lauri Hyry vastaa Solitalla puolustus- ja turvallisuusasiakkuuksista. Hän työskentelee turvallisten tekoäly-, data- ja digiratkaisujen parissa vaativissa ja säädellyissä viranomais- ja puolustusympäristöissä.

TEKSTI: JYRKI PENTTINEN, SR. PROGRAM MANAGER, ALPHACORE INC,. USA

ISAC: Kehittynyttä sensorointia

Matkaviestintäverkot kehittyvät vahvasti, ja juuri alkaneen 3GPP:n 6G-spesifiointityön myötä on suunnitteilla jälleen useita uusia toimintoja. 6G sisältää 5G:stä tutut peruspilarit parannettuina versiona, eli mobiililaajakaista, massiivinen IoT, ja korkean luotettavuuden liikennöinti. Lisäksi 6G:n täydentäviin pilareihin tulee uutuuksia, joista yksi tämän hetken kuumista aiheista on mobiilijärjestelmien tukema samanaikainen liikennöinti ja sensorointi, eli ISAC.

Johdanto

Nykyiset langattomat verkot on suunniteltu pääosin dataviestintään siten, että palvelut ovat keskittyneet puheen, viestien, videon ja Internet-palveluiden välittämiseen. Monet nykyaikaiset palvelut, kuten autonominen liikenne, teollisuuden automaatio, sekä älykaupungeissa ja puolustussovelluksissa käytettävät sovellukset hyötyvät kasvavassa määrin myös ympäristön reaaliaikaista ymmärtämistä eli sensorointia tai anturointia.

ISAC (Integrated Sensing and Communication), jota voidaan kutsua myös termillä JCAS (Joint Communication and Sensing), yhdistää järjestelmän sensoroinnin ja tietoliikenteen toiminnot siten, että radiolinkki toimii sekä perinteiseen tietoliikenteeseen että myös "tutkana" ympäristön havainnointiin. Tämä mahdollistaa esimerkiksi auton kulkureitin seuraamisen, droonien havaitsemisen ja ihmisten tai esineiden sijainnin ja nopeuden arvioinnin perustuen samoihin radiolähetyksiin, joita verkko muutenkin käyttää datan välittämiseen.[1][2]

Siviilikäytössä ISAC:n periaatetta voidaan hyödyntää esimerkiksi liikenteen turvallisuusjärjestelmissä ja ajoneuvojen tietoliikennöinnin rakenteissa (V2X, Vehicle to Everything), joissa ajoneuvot havaitsevat ja tiedottavat ympäristöstään. ISAC on hyödyllinen myös teollisuudessa, missä koneet voivat havaita esteitä samalla kun ne kommunikoivat ohjausjärjestelmien kanssa. Puolustussovelluksissa samanaikainen sensorointi ja viestintä mahdollistaa tilannetietoisuuden ja uhkien havaitsemisen ilman erillisiä antureita tai tutkia. Verkko voi esimerkiksi tunnistaa suojatulle alueelle luvattomasti tunkeutuvat droonit (UAV, Uncrewed Aerial Vehicle) hyödyntämällä oman tiedonsiirtonsa radiosignaaleja sensorointitarkoituksiin.

ISAC:in periaate on toimia osana radiojärjestelmää, joka sekä viestii että havaitsee ympäristöä. ISAC avaa siten uusia mahdollisuuksia reaaliaikaisiin datapalveluihin ja lisää verkkojen hyödynnettävyyttä, koska sama laitteisto voi toteuttaa molemmat toiminnot yhdessä.

Standardointi

3GPP (3rd Generation Partnership Project) on tärkein maailmanlaajuinen telealan yhteistyöjärjestö, joka kehittää ja julkaisee teknisiä raportteja ja spesifikaatioita. Tämän hetken pääpaino 3GPP:n työssä on 5G ja sen kehittynyt jatkumo, 5G-Advanced. 3GPP on sisällyttänyt ISAC-teknologian alkuvaiheen työn osaksi jo Release 19 -teknisiä raportteja, joissa määritellään ISAC-käyttötilanteita ja vaatimuksia, ja valmistautuu 6G:n teknisten määritysten luomiseen piakkoin työn alle otettavan Release 21:n myötä.

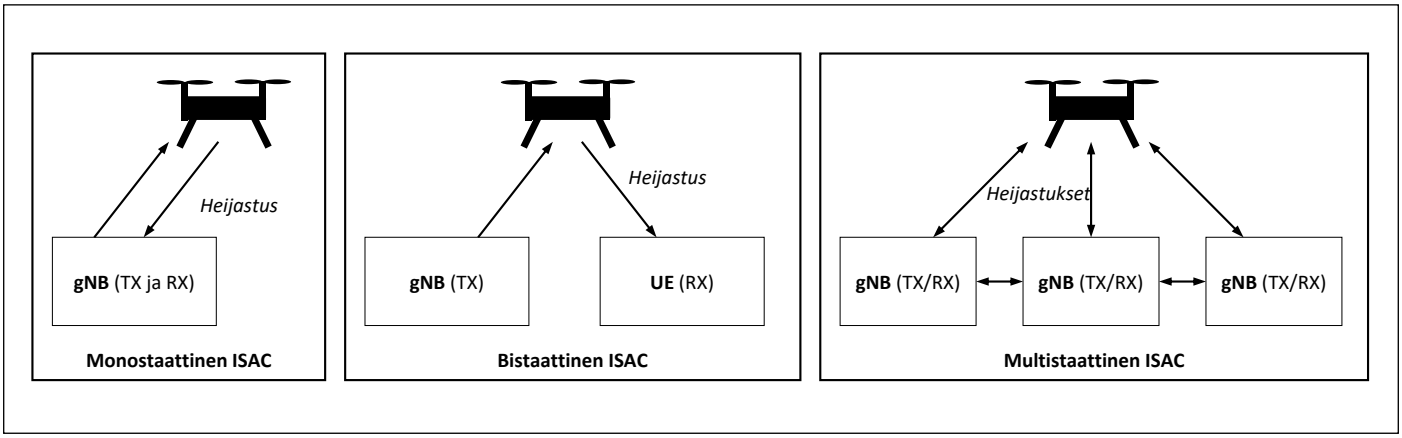
Tällä välillä ETSI (European Telecommunications Standards Institute) on perustanut Industry Specification Group (ISG) Integrated Sensing and Communications -ryhmän, joka keskittyy ISAC:iin liittyvään varhaisen vaiheen standardisointityöhön ja valmistaa teknisiä raportteja sekä kehysrakenteita, joita 3GPP ja muut standardointielimet voivat myöhemmin käyttää 6G-spesifikaatioiden luomisessa. ETSI ISG ISAC laatii esimerkiksi priorisoituja 6G-käyttötapauksia, kanavamalleja, arkkitehtuurimalleja ja teknisiä suorituskykymittareita (KPI, Key Performance Indicator) erityisesti 6G-kehitykseen.[3] Osa näistä tähtää suoraan 6G-julkaisuihin.

3GPP Release 19:n tekninen raportti TR 22.837 [4] on perusta ISAC:in vaatimuksille ja kuvaa mm. objektien havaitsemista, ympäristön seurannan ja liikkeen tunnistamisen esimerkkejä sekä niihin liittyviä suorituskykytavoitteita. Lisäksi 3GPP on aloittanut työn ISAC:iin liittyvän kanavamallinnuksen standardoinnissa osana radioverkkoryhmän (RAN, Radio Access Network) työtä.

6G:n spesifikaatiot sisältävät valmistuttuaan ISAC:in alkuperäisesti integroituna perusominaisuutena, ei vain lisäpalveluna. ETSI ISAC ISG toimii siten osaltaan siltana 5G/5G-Advanced -työn ja 6G-kehityksen välillä.

ISAC:n tekninen periaate

ISAC:n tekninen perusta muistuttaa Dopplertutkan periaatteita, jossa lähetetään radiopulssi, ja sen heijastuksia vastaanotetaan ja analysoidaan viestinnän ohella, jolloin voidaan arvioida kohteiden sijaintia, liikettä ja muita geometristen parametrien ominaisuuksia.



Kuva 1: ISAC-toimintamuodot.

3GPP:n määrittämä radiojärjestelmän arkkitehtuuri perustuu 5G NR:n (New Radio) perusrakenteeseen, jossa OFDM-pohjainen (Orthogonal Frequency Division Multiplexing) ilmaisin mahdollistaa dynaamisesti sensoritoimintojen sisällyttämisen viestintään. Samaa signaalia voidaan käyttää tiedon välitykseen datana ja heijastuneen signaalin analysointiin objektien tunnistamiseksi.[2]

ISAC-integraatio voidaan toteuttaa seuraavilla tavoilla:

Paikallinen resursointi, jolla sensorointi ja dataviestintä voivat jakaa taajuuskaistaa ja laitteistoa optimoiden resurssien käytön.

Syvä integraatio mahdollistaa samojen OFDM-symbolien toiminnan sekä datansiirtoon että sensorimittauksiin ilman erillisiä signaaleja.

Täysi synkronointi tarkoittaa sitä, että verkko käsittelee sensorointia ja viestintää yhtenäisenä kokonaisuutena, mikä mahdollistaa reaaliaikaisten päätösten teon molemmista toiminnoista yhdessä.

Aktiivinen sensorointi hyödyntää RF-signaalin heijastuksia objektien ympäriltä. Palautuvien signaalien avulla voidaan määrittää mm. objektin etäisyys, Doppler-nopeus ja etenemissuunta. Tekniikat ovat samankaltaisia kuin tutkateknologioissa, mutta ne integroidaan langattomaan verkkoon siten, että erillistä sensoria ei tarvita, vaan sensorointitieto saadaan suoraan viestintäsignaaleista.

Uudet 3GPP:n sensorielementit

TRP (Transmission Reception Point) on 3GPP:n verkkosolmu, kuten tukiasema, jonka tehtävänä on lähettää ja vastaanottaa radiosignaaleja. ISAC:ssa TRP:t voivat toimia sekä viestintäankkureina että sensorisolmuina, ja siten ISAC voi hyödyntää matkaviestintäverkon laajaa kattavuutta ja riittävää lähetystehoa ympäristön tilannetiedon saantiin.

3GPP:n arkkitehtuurimallissa 5G-tukiasematoiminnot (gNB, next generation node B), joko hajautettuina tai keskitettyinä radioelementteinä (DU, Distributed Unit; CU, Centralized Unit), lähettää ja vastaanottaa OFDM-perustaisia ISAC-signaaleja ja voi suorittaa sensoridatan esikäsittelyä paikallisesti.

Myös matkaviestin (UE, user equipment), kuten älypuhelin tai IoT-anturi, voi osallistua sensorointiin ja raportoida verkolle signaaliheijastusten vastaanottomittaukset. ISAC-kykyinen UE voi osallistua sensorointiin esimerkiksi lähettämällä sensorisignaaleita heijastusanalyysiä varten, tai prosessoiden vastaanotettuja sensorointisignaaleja.

3GPP:n uusi sensoroinnin prosessointiyksikkö (Sensing Processing Entity, SPE) kerää sensorointidataa useista radioverkon lähteistä (joukosta UE- ja gNB-elementtejä) ja analysoi niiden perusteella objektien paikannustiedon, nopeuden ja kulkureitin. Näiden tietojen perusteella 5G-kytentäverkossa oleva sensoroinnin sovellustoiminto (AF, Application Function) toimittaa tulokset sovelluksille (esim. UTM, V2X ja puolustus).

Mobiiliverkon ISAC perustuu siis olemassa oleviin, jo määritettyihin verkon komponentteihin, ja 3GPP täydentää määrityksiä ISAC:n vaatimien lisätoimintojen tukeen.

Toimintamuodot

ISAC voidaan toteuttaa kolmella tavalla 3GPP TR 22.837 -dokumentin mukaisesti: monostaattisena, bistaattisena tai multistaattisena (kuva 1).

Monostaattinen sensorointi (monostatic sensing) tarkoittaa sitä, että lähetin (TX, Transmitter) ja vastaanotin (RX, Receiver) ovat fyysisesti samassa paikassa (esim. UE:ssa tai gNB:ssä). Monostaattisen toteutuksen perusta on siten sama kuin perinteisessä tutkassa.

Bistaattisessa sensoroinnissa (bistatic sensing) lähetin ja vastaanotin ovat fyysisesti eri paikoissa. Tällä välimatkaeroon perustuvalla toteutuksella saavutetaan laaja sensorointialue ja tarkennettu havainnointi mukaan lukien topologialtaan vaativat ympäristöt.

Multistaattinen sensorointi (multi-static sensing) mahdollistaa monimuotoisen, useiden lähettimien ja vastaanottimien yhteistoiminnan, joka parantaa edelleen sensoroinnin tarkkuutta ja tiedon luotettavuutta.

Esimerkkejä ISAC:n käytöstä maanpäällisissä verkoissa

ISAC soveltuu erityisen hyvin maanpäällisiin langattomiin verkkoihin, joissa infrastruktuuri on kattava ja radiotaajuuksia käytetään laajasti. Esimerkkejä erityisen kiinnostavista käyttökohteista ovat V2X-(Vehicle-to-Everything) ja UAV-sensorointisovellukset.[5]

V2X (ajoneuvot ja liikenne) -käyttötilanteissa ISAC mahdollistaa tehokkaasti ajoneuvojen ympäristön reaaliaikaisen sensoroinnin ja kommunikoinnin samanaikaisesti, mikä kohentaa turvallisuutta, kun verkko voi havaita jalankulkijoita, esteitä tai ajoneuvoja ja välittää tiedot samalla kuin verkko mahdollistaa datayhteyden ajoneuvoille.

UAV-monitorointi ja ilmatilan hallinta on puolestaan käyttökohde, jossa verkon kautta voidaan havaita miehittämättömiä ilma-aluksia, kuten drooneja, sekä niiden liikeratoja analysoimalla radioaaltojen heijastuksia. Tämä auttaa niin ystävällis- kuin vihamielisten droonien tilannehallinnassa. ISAC:n avulla voidaan tunnistaa tunkeilijoita tai auttaa ystävällisten laitteiden navigoinnissa, reittisuunnittelussa ja törmäyksen välttämisessä.

Lisäksi erilaiset teollisuuden automaatiota tukevat sovellukset, kuten esteiden tunnistus sisätiloissa, voivat hyödyntää verkon sensorointikykyä erillisten tutkien tai LiDAR-ratkaisujen sijaan, jolloin kokonaisratkaisu on kustannustehokkaampi ja vähemmän laiteintensiivinen.

UAV-pohjainen ISAC

Siinä, missä ISAC voi auttaa tunnistamaan drooneja, voidaan ISAC toteuttaa myös UAV:hen asennettuna. Tällöin UAV:n 3D-liikkuvuuden kautta saavutetaan erityisiä hyötyjä kohteiden etsintään ja tunnistamiseen esimerkiksi osana kriisialueilla olevien loukkaantuneiden paikallistamiseksi.

3GPP TR 22.873 esittää käytännönläheisiä esimerkkejä ISAC:n käyttökohteista, ml. UAV. Eräs näistä skenaarioista liittyy UAV-lennon reitin seurantaan ISAC-tekniikalla.

Tausta ja tarve

Kaupallisten droonien käyttö lisääntyy esimerkiksi pakettikuljetuksissa, ympäristön seurannassa, ilmakuvauksessa ja julkisessa turvallisuudessa. Näissä sovelluksissa droonit lentävät ennalta määritettyjä ja viranomaisten hyväksymiä lentoreittejä, joissa on tarkat vaatimukset korkeudelle, nopeudelle ja sijainnille. Vaikka UAV:t sisältävät omia sensoreita, kuten kamera, tutka ja GPS, ne eivät aina toimi luotettavasti. Kamera voi häiriintyä valaistusolosuhteista ja UAV:n tutkan luotettavuus voi heikentyä sateessa tai lumessa. Tällöin drooni ei välttämättä kykene itse määrittämään tarkkaa sijaintiaan tai seuraamaan sallittua reittiä. Ulkoinen, verkon tarjoama lennon seuranta on siksi tarpeen.

Perinteiset UAV-valvontatutkat ovat kalliita ja haastavia käyttöönotettaviksi laajoilla alueilla. ISAC-pohjainen 5G-verkkoon integroitu sensorointi tarjoaa tähän käyttökohteeseen erityisen kustannustehokkaan vaihtoehdon.

ISAC:ssa 5G-verkko ei ainoastaan välitä dataa, vaan toimii samalla ”radiohavaitsijana”. 5G-tukiasemat (gNB) ja osa päätelaitteista (UE) havaitsevat UAV:n radioaaltojen heijastusten avulla, ja niiden kautta saatavilla 3GPP-sensorointitiedoilla verkko voi arvioida droonin sijainnin, etäisyyden, kulman ja liikesuunnan. Erityinen etu syntyy siitä, että päätelaitteita on tyypillisesti paljon (enemmän kuin tukiasemia). Ne voivat sijaita lähempänä UAV:ta tai paremmassa heijastuskulmassa, mikä parantaa havaintojen tarkkuutta ja luotettavuutta.

Tässä käyttökohteessa osapuolina ovat UAV-operaattori, joka vastaa droonien liikenteestä, 5G-verkon operaattori, joka tarjoaa ISAC-pohjaisen seurantapalvelun, ja 5G:n radiokomponentit (radioverkko ja siihen liittyneet UE:t), jotka suorittavat varsinaisen radiohavaintotyön. 3GPP-verkon kautta havaintodata voidaan kerätä 5G-sensoriprosessointiyksikköön, joka yhdistää ja analysoi havainnot (esimerkiksi droonin lentorata voidaan laskea ja päivittää reaaliajassa). UAV-operaattori tilaa palvelun ja antaa verkolle tiedot UAV:n ominaisuuksista sekä seuranta-alueesta ja ajasta.

Palvelun periaate

Tässä käyttökohteessa on seuraavat askeleet:

1) 5G-verkko aktivoi UAV-seurannan sovitulla alueella ja ajanjaksolla. 2) UAV lähtee lentoon ja seuraa sallittua reittiä. 3) Tukiasemat ja UE:t havaitsevat UAV:n ISAC-sensoroinnilla. 4) Havaintodata yhdistetään ja UAV:n sijainti ja nopeus lasketaan 5) Verkko optimoi sensorointia (esim. vaihtaa tukiasemia UAV:n liikkuessa). 6) UAV-operaattori saa reaaliaikaisen lentoradan. 7) Jos drooni poikkeaa reitiltä, operaattori voi ohjata sen takaisin.

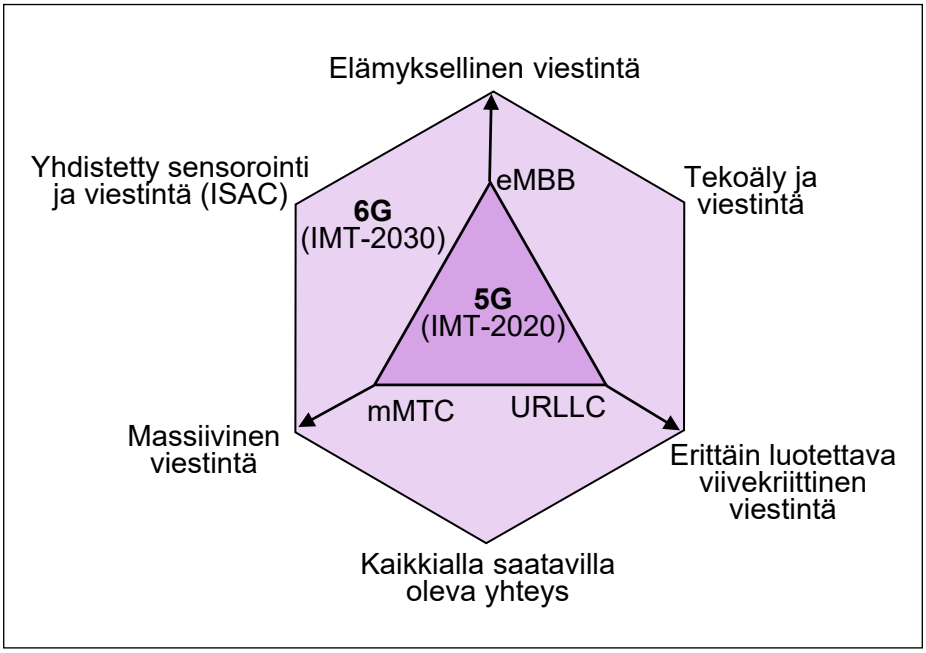
Lopputuloksena, UAV kulkee sallitun reitin mukaisesti, tai jos poikkeama tapahtuu, se havaitaan ajoissa ja siihen voidaan puuttua. ISAC tekee UAV-liikenteen valvonnasta skaalautuvaa, kustannustehokasta ja verkkoon alun perin integroitua ilman erillisiä tutkajärjestelmiä.

Esimerkkejä ISAC:n toimivuudesta satelliittiverkoissa

Satelliittiverkot (Non-Terrestrial Network, NTN) ovat merkittävä 5G/6G-ekosysteemin osa-alue, jossa ISAC voi toimia tehokkaasti. NTN kattaa satelliitit, korkean ilmakehän alustat (HAP, High Altitude Platform) ja UAV-pohjaiset toistinsolmut, jotka mahdollistavat yhteydet alueilla, joilla perinteinen infrastruktuuri on puutteellinen tai olematon.

NTN-järjestelmät voivat integroida ISAC-toiminnot siten, että datansiirto ja ympäristön sensorointi tapahtuvat samassa signaalivirrassa. Tämä on oleellista vaikkapa hätätilanteissa, jolloin yhdistetty ISAC-NTN -verkko voi tarjota sekä luotettavan yhteyden että kohennetun tilannekuvan. Tekniikan avulla voidaan esim. etsiä loukkuun jääneitä tai arvioida liikkuvia kohteita haastavissa maastoissa.

Tutkimukset ovat myös osoittaneet, että ISAC voi tehostaa resurssien jakoa ja linkin optimointia satelliittiympäristöissä, erityisesti monikanavaisissa ja monitaajuusjärjestelmissä, joissa reaaliaikainen aaltotietojen havaitseminen laskee radiohäiriöitä ja parantaa tiedonsiirron laatua. [6][7]



Kuva 2: ISAC on yksi ITU:n määrittämistä 6G:n peruspilareista.

Esimerkkejä ISAC:sta maanpuolustuksessa

Maanpuolustuskäytössä ISAC tarjoaa erityisiä hyötyjä, kuten parannettu tilannetietoisuus sekä alueellinen seuranta. ISAC-toiminto voi esimerkiksi havaita tunkeutuvia UAV-laitteita, luokitella radiohäiriöitä tai tarjota reaaliaikaista dataa kenttäoperaatioihin.

Asian tärkeydestä maanpuolustuksen tarpeisiin on esimerkkinä hiljattainen IEEE Military Communications -konferenssi, joka on käsitellyt ISAC-sovelluksia kaupallisen ja kansallisen turvallisuuden kontekstissa, ml. robotiikan automatisointi, ajoneuvojen turvallisuusjärjestelmät, radiokanavien passiivinen monitorointi ja majoitusalueiden ulkoinen sensorointi. Näissä sovelluksissa ISAC voi toimia kuin liikkuva sensori, joka yhdistää RF-viestinnän reaaliaikaiseen havaitsemiseen.[8]

Maanpuolustuksessa tällaisia kyvykkyyksiä voidaan käyttää esimerkiksi hyökkäyksen varhaiseen varoitukseen, rajanylitysten seurannan automaatioon tai joukkojen ympäristön havainnointiin ilman tarvetta erillisille tutkajärjestelmille.

Tulevaisuus

ISAC on parhaillaan työn alla. ISAC:n varsinainen tavoite on toteuttaa 6G-järjestelmä, jossa langattomat verkot eivät rajoitu vain dataviestintään, vaan mahdollistavat reaaliaikaisen tilannetiedon käyttäjän ympäristöstä. Standardointityö jatkuu siten 3GPP Release 20 ja 21 -sarjojen kehityksen myötä 6G:n toiminnallisten määrittelyjen osalta, joskin osa ISAC:n toiminnoista tullaan integroimaan myös 5G-Advanced -ympäristöön. 6G:n myötä ISAC:lle liitetään laajempia vaatimuksia sekä kyvykkyyksiä, kuten millimetriaalto- ja THz-taajuudet, dynaamiset kanavamallit ja AI/NLP-pohjaiset sensorointialgoritmit.

Lisäksi standardointielimet kuten ITU-R ovat tunnistaneet ISAC:in yhtenä kuudesta keskeisestä käyttötapauksesta 6G-kehityksessä (IMT-2030), kuten kuva 2 osoittaa. Tämä tarkoittaa, että tulevat standardit eivät pelkästään tue ISAC:ia, vaan tekevät siitä natiivin osan verkon perustoiminnallisuutta, mahdollistaen tarkemman paikannuksen, ympäristön reaaliaikaisen kartoituksen ja entistä paremmat autonomiset järjestelmät.

Lähteet

[1] ETSI, ”ISAC-teknologia ja näkökulmia radiotutkaan perustuvasta ympäristön havaitsemisesta,” https://www.etsi.org/technologies/integrated-sensing-and-communications

[2] R. Baldemair, ”ISAC yleiskatsaus,” Ericsson, 2024. https://www.ericsson.com/en/blog/2024/6/integrated-sensing-and-communication

[3] ETSI, ”ISAC: Use cases; channel modeling,” https://www.etsi.org/committee/2295-isac

[4] 3GPP, ”Feasibility Study on Integrated Sensing and Communication (Release 19),” https://www.3gpp.org/ftp/Specs/archive/22_series/22.837/

[5] 5GACIA, ”Use Cases and Requirements for ISAC in Connected Industries and Automation,” https://5g-acia.org/whitepapers/use-cases-and-requirements-for-integrated-sensing-and-communication-isac-in-connected-industries-and-automation-2/

[6] B. Ciloglu et al, ”ISAC-over-NTN: HAPS–UAV Framework for Post-Disaster Responsive 6G Networks,” 2026. https://arxiv.org/abs/2601.15422v1

[7] L. Leyva-Mayorga et al, ”ISAC-Powered Distributed Matching and Resource Allocation in Multi-band NTN,” 2025. https://arxiv.org/abs/2512.02843v1

[8] ”ISAC Applications for Commercial and National Security Use,” IEEE Military Communications Conference, 2025. [Online]. Available: https://milcom2025.ieee-milcom.org/program/technical-panels/pan-07-integrated-sensing-and-communications-isac-applications-commercial

Artikkelin kirjoittaja

TkT, tietokirjailija Jyrki Penttinen on toiminut telealalla vuodesta 1994 Suomessa, Espanjassa, Meksikossa ja Yhdysvalloissa. Penttinen työskentelee nykyään Pohjois-Amerikassa pääaiheenaan 5G ja luennoi televiestintäteknologioista. Penttisen julkaisuihin voi perehtyä LinkedIn:n kautta www.linkedin.com/in/jypen ja blogissaan www.5g-simplified.com.

TEKSTI: TATU TAHKOKALLIO

Define accelerator -kiihdyttämöohjelma kaksikäyttöratkaisujen edistäjänä

Vuonna 2024 julkaistu Valtioneuvoston puolustusselonteko korostaa teknologisen etumatkan merkitystä pitkäkestoisen kulutussodankäynnin pidäkkeenä. Lähtökohtaa tukevat Ukrainan sodasta tehdyt havainnot, joissa siviili- ja puolustussektorin eri tutkimus-, kehittämis- ja käyttäjätahot edistävät teknisiä sotilasratkaisuja tiiviissä yhteistyössä. Pidäkkeen pysyvyyttä haastavat nopeasti kehittyvä teknologia ja tästä johtuvat muutostarpeet sotilastaktiikassa. Täten on välttämätöntä, että pidäkettä ylläpidetään ja kehitetään jatkuvasti. Riihimäen kaupunki tarttui haasteeseen perustamalla Define-innovaatioekosysteemin, jonka keskeisenä tavoitteena on saattaa rahoittajia, puolustussektorin vakiintuneita toimijoita sekä puolustushallinnon ja uusien kaksikäyttöratkaisujen kehittäjiä yhteen. Tämä artikkeli kertoo Define Accelerator -yrityskiihdyttämöohjelmasta ja sen ensimmäisen kauden kasvuyrityksistä, näiden tuottamista innovaatioista sekä ohjelman saavuttamista tuloksista.

Mistä kaksikäytössä on kyse?

Kaksikäyttötuotteiden määritelmä juontaa juurensa vuonna 1995 allekirjoitettuun Wassenaarin sopimukseen, joka koskee tavanomaisten aseiden ja kaksikäyttötuotteiden vientivalvontajärjestelyä. Edelleen voimassa olevan sopimuksen tavoitteena on alueellisen ja kansainvälisen turvallisuuden sekä vakauden edistäminen siten, että tavanomaisten aseiden ja kaksikäyttötuotteiden ja -teknologioiden siirrot ovat läpinäkyviä allekirjoittajamaiden kesken. Suomessa vientivalvonnasta vastaa ulkoministeriö.

Ulkoministeriön kaksikäyttötuotteiden määritelmä perustuu Euroopan parlamentin ja neuvoston asetukseen 2021/821. Asetus käsittelee kaksikäyttötuotteita laajasti ja laskee tällaisiin mm. teknologiat, joita voidaan käyttää sekä siviili- että sotilastarkoituksiin. Suomen Teollisuussijoituksen (TESI) määritelmä on parlamentin kanssa yhteneväinen ja taannoisessa (Defence, Market Study on Finnish military product and dual use companies, syyskuu 2024) selvityksessä TESI linjasi kaksikäyttöteknologioihin kuuluvan sellaiset innovatiiviset tuotteet ja palvelut, joilla on sekä siviili- että sotilaskäyttöä.

Vientivalvontaan ja vientilupien myöntämiseen liittyvät vastuut jakautuvat eri viranomaisten kesken. Ulkoministeriö vastaa siviilituotteiden vientivalvonnasta ja puolustusministeriö vastaa puolustustarvikkeiden vientivalvonnasta. Siviiliaseiden- ja patruunoiden vientiluvista vastaa poliisihallitus.

Yrityskiihdyttämö kaksikäyttöteknologioille

Define Accelerator -yrityskiihdyttämöohjelma aloitti marraskuussa 2024 ja muodosti luonnollisen jatkumon samana vuonna Riihimäellä järjestetyille MaanpuolustusAreena, Pitch Finland DefSec - ja Define Hackathon -tapahtumille. Kaksitoistakuukautisen kiihdyttämöohjelman rahoittajina toimivat Riihimäen Kaupunki ja Kanta-Hämeen rakennerahasto-ohjelma. Jälkimmäisen hallinnoinnista vastaa Hämeen ELY -keskus ja osarahoittajana on Euroopan Unionin Euroopan aluekehitysrahasto. Kiihdyttämöohjelman ohjauksesta vastasi Riihimäen kaupungin johtama ohjausryhmä. Ohjelman toteuttajaksi oli valittu julkisen kilpailutuksen perusteella riskipääomasijoittaja Redstone Nordics.

Ohjelman tavoitteena oli löytää, kouluttaa ja tukea yrityksiä, jotka kehittävät ja kaupallistavat kaksikäyttötuotteita, -palveluja tai näiden tuotantomenetelmiä. Ohjelma toteutettiin kolmessa vaiheessa ja jokaiseen vaiheeseen valittiin kahdentoista yrityksen kohortti. Keskeisimpiä valintakriteerejä olivat mm. idean uutuusarvo, toteuttamiskelpoisuus, teknologinen valmiusaste, kaksoiskäyttöisyys sekä tiimin kokemus. Sotilasulottuvuuden takia hakemuksia arvioitiin erikseen sotilaallisen kiinnostavuuden näkökulmasta. Ryhmiä ei muodostettu teemapohjalta, vaan kuhunkin ryhmään valittujen yritysten taustat ja innovaatiot saattoivat poiketa merkittävästi toinen toisistaan.

Kiihdyttämöohjelman perusrakenne oli kaikille ryhmille sama. Viikoittain osallistujille järjestettiin sekä yhteisluento että yrityskohtainen valmennussessio. Osa luennoista pidettiin lähisessioina Riihimäen veturitallille sijoittuneessa Define-hubissa ja osa taas etäluentoina Internetin yli. Ryhmät osallistuivat erilaisiin puolustusalan tapahtumiin, kuten SecDDay-messuille, Aalto yliopiston Defence Linkage -kurssin päätöstilaisuuteen, Arctic15-kasvuyritystapahtumaan ja Knights of Nordics sijoittajatapahtumaan, joka oli myös Slushin sivutapahtuma. Lisäksi ryhmät tekivät vierailuja useisiin puolustusalan vakiintuneisiin yrityksiin, kuten Sako, Saab Finland ja Insta Oy sekä tutustuivat Puolustusvoimien toimintaan mm. Panssariprikaatissa Parolannummella. Puolustusvoimien edustajat osallistuivat myös varsin runsaslukuisesti kiihdyttämön järjestämiin sidosryhmätilaisuuksiin, kuten Demo Day -tapahtumiin. Näissä sotilaille tarjoutui hyvä mahdollisuus nähdä ja keskustella uusista innovaatioista suoraan startupyrittäjien kanssa.

Yksilöllistä valmennusta

Kiihdyttämöohjelman valmentajina toimivat päävalmentaja ja Redstone Nordics:n toimitusjohtaja Kaj Hagros, pääomasijoittaja Oskari Lehtonen, sotilasprofessori eversti evp Mika Hyytiäinen ja allekirjoittanut. Kukin valmentaja vastasi omista valmennusteemoistaan ja käsitteli näitä viikoittaisissa valmennussessioissa yhdessä kulloinkin valmennettavana olevan yrityksen kanssa.

Valmennusteemoja olivat mm. myynti, markkinointi, rahoitus, teknologia ja sotilasorganisaatiot. Yksittäisistä teemojen alla käsitellyistä asioista mainittakoon esimerkiksi hissipuhe, go-to-market strategia, kaksikäyttöteknologioiden innovointi, sotilaallisen organisaation toimintatavat, sotilaallisen suorituskyvyn käsitemalli, konseptien testaaminen, teknologiset kypsyystasot ja tulevaisuuden ennakointi.

Tärkeän osan yksilöllistä valmennusta muodostivat keskustelut ja pohdinnat siitä, miten ”navigoida” sotilasorganisaatioissa. Samalla osallistujat saivat oppia sotilasorganisaatioiden toimintatavoista liittyen esimerkiksi suorituskykyjen suunnitteluun, rakentamiseen ja hankintaprosesseihin. Laajaa ja välillä syväl-

Startup	Ratkaisu	Url
Ryhmä 1		
Atle Defence	Panssarintorjuntasimulaattori	atledefence.fi
Lowkey	Tietoturvallinen viestintäratkaisu	lowkeychatgov.com
Monava	Akustinen sensorijärjestelmä	monava.io
Rain	Matkapuhelinverkkojen tekoälyä hyödyntävä hallintajärjestelmä	rain.global
Refamo	Hitsattujen teräsrakenteiden ennakoiva kunnossapitoratkaisu	refamo.fi
ReLoc	Häirinnästä riippumaton paikannus-, navigointi- ja ajoitusratkaisu	reloc.fi
Sapper	Tekoälyavusteinen maatutka	sapper-intelligence.com
SeeTrue	Silmänliikkeen seurantaratkaisu	seetruetechnologies.com
Tambest	Lasiteknologiaratkaisut	tambest.com
Tespack	Älykkäät liikkuvat energiaratkaisut	tespack.com
Viima Aerospace	Joukkoistettavat 3D-droonit	viima.aero
Foxa	Armeijakankaat (yritys myyty, jatkaa nimellään)	foxa.fi
Ryhmä 2		
Aestus Systems	MESH-sensoriverkko	aestus.fi
AlionLife	Stressiä säätelevä neuroteknologiaratkaisu	alionlife.com
Avartek	Drooniratkaisut	avartek.fi
Battleboxes	Kuljetus- ja kätköratkaisu	battleboxes.com
Donut Defence	Sähköinen donitsimoottori (yritys myyty)	donutdefence.com
Litqu	Ympäristöystävällinen puhdistusmenetelmä	litqu.com
Pleno	Autonominen AI-drooniagentti (yritys myyty)	pleno.tech
Rebelvolt	e-generaattori	rebelvolt.com
SemiQon	Erittäin kylmien olosuhteiden CMOS-piirit	semiqon.tech
Sharpnav	Matalan maan kiertoradan satelliittiratkaisu	sharpnav.com
SkyDoc	Autonominen droonien lataustelakka	luftvejen.dk
Tytan	Tekoälyä hyödyntävä vastadrooniratkaisu	tytan-technologies.com
Ryhmä 3		
Alvidiotech	Konenäköön perustuva logistiikkaratkaisu	alvidiotech.com
Strato-B	Korkean ilmanalan kuljetusratkaisu	cgfrance.com
Contai	Autonominen maassa liikkuva evakuointiratkaisu	contai.eu
Delta Technics	Autonominen tarkka-ampujajärjestelmä drooniin	deltatechnics.fi
Eagle Ray Robotics	Merenalainen parveileva drooniratkaisu	eaglerayrobotics.co
Rescue Drones	Drooneihin perustuva palo- ja pelastusratkaisu	rescuedrones.fi
Rhoshield	Kriittisen infrastruktuurin autonominen kehäpuolustusratkaisu	rhoshield.fi
SelectAM	3D-mallien onlinekirjasto ja -kauppapaikka	selectam.io
Sostex	Grafeenipohjaiset puettavat teknologiat	sostex.fi
Thistle Shield	Vastalennokkijärjestelmä	thistleshield.com
Viva Jets	Sähköinen pintadrooni	vivaelectricjets.com
Wield VR	Fyysinen asetuki virtuaalisotapeleihin	wieldvr.com

Kiihdyttämöön osallistuneet kasvuyritykset ryhmittäin.

Riihimäen kaupungin teknologia- ja innovaatiojohtaja Teemu Seppälä avaamassa ensimmäistä Define-kiihdyttämöä Riihimäen veturitalleilla.
Kuva: Riihimäen Kaupunki/Juho Haavisto.

listäkin keskustelua käytiin myös siitä, miten sovittaa kasvuyrityksen lyhyen jänteen tarpeet ja ketterät toimintamallit jäykän sotilasorganisaation vakiintuneisiin prosesseihin ja käytänteisiin. Monia yrityksiä ihmetytti myös se, miten nopeasti vastinparit Puolustusvoimissa voivat upseerien urakierrosta johtuen vaihtua. Haasteista huolimatta osa yrityksistä onnistui kiihdyttämöjakson kuluessa löytämään vastinparin Puolustusvoimista tai jostain muusta sotilasorganisaatiosta ja käynnistämään konkreettisen yhteistyön.

Sekalainen seurakunta kasvuyrityksiä

Kiihdyttämöohjelmaan osallistui yhteensä kolmekymmentäkuusi yritystä (taulukko 1). Näistä valtaosa oli peräisin Suomesta, mutta mukaan mahtui myös muutama yritys Virosta, Ruotsista, Tanskasta, Iso-Britanniasta, Ranskasta ja Saksasta.

Usea yritys työskenteli miehittämättömän tai autonomisen järjestelmän parissa. Ajan hengen mukaisesti myös tekoäly oli keskeinen osa monia ratkaisuja. Nousevien ja murroksellisten teknologioiden lisäksi joukossa oli silti yrityksiä, jotka edustivat perinteisempiä teollisuus- tai teknologia-aloja, kuten lasin, kankaiden tai integroitujen piirien valmistus.

Seuraavassa kustakin ryhmästä esitellään yksi yritys, jonka innovaatio oli poikkeuksellisen mielenkiintoinen ja/tai teknologisesti edistyksellinen ja jolle löytynee lähes välittömästi sotilaallista käyttöä.

Monava

Monava on Göteborgissa vuonna 2020 perustettu startup, joka kehittää älykästä akustiseen sensorointiin perustuvaa tunnistus- ja valvontajärjestelmää. Monavan akustinen sensori kykenee havaitsemaan ja paikantamaan äänilähteitä sekä tunnistamaan yksittäisen lähteen. Tunnistamiseen järjestelmä hyödyntää yksilöllisiä äänijälkiä ja näillä opetettua koneoppivaa neuroverkkoa. Monavan ratkaisu on passiivinen, eli se ei itsessään lähetä mitään vaan toimii kuuntelutilassa.

Monavan toimitusjohtaja Alexander Hebbe esittelee liiketoimintakonseptiaan. Kuva: Riihimäen Kaupunki/Juho Haavisto.

Rebelvoltin tiimi ratkaisunsa kanssa kiihdyttämön Demo-dayssa maaliskuussa. Kuva: Riihimäen Kaupunki/Juho Haavisto.

Monava on testannut järjestelmäänsä mm. lentokenttien yhteydessä hyvin tuloksin. Järjestelmä on kyennyt havaitsemaan pienempien droonien lähestymisiä satojen metrien päästä ja suurempien jopa kilometrien etäisyydeltä. Järjestelmän etuna on, ettei havaitsemista estä heikko visuaalinen kontakti kohteeseen eikä muut suoraa näköyhteyttä haittaavat rakenteet.

Sotilaallisesta näkökulmasta Monavan kaltaiset äänilähteisiin perustuvat sensorit ovat mielenkiintoisia, ja näille voidaan löytää useita eri käyttötarkoituksia sekä maalla, merellä että ilmassa. Ajankohtaisia esimerkkejä akustisista sensoreista ja niiden hyödyntämisestä puolustustarkoituksessa on löydettävissä yhtä lailla lähivesiltämme kuin myös Ukrainasta, jossa akustisia sensoriverkkoja (esim. Sky Fortress ja ZVOOK NW0) käytetään ilmatorjunnan osana havaitsemaan lähestyviä ohjuksia ja drooneja.

Rebelvolt

Vuonna 2023 perustettu Rebelvolt on Rajamäeltä kotoisin oleva kasvuyritys, jonka ideana on korvata perinteinen polttomoottorilla toimiva sähkögeneraattori akustoon perustuvalla e-generaattorilla. Suomen kaltaisessa maassa ajatus voi tuntua oudolta, koska sähkön jakeluverkko ja sähkön saanti ovat isoilta osin hyvin toteutettu ja ylläpidetty. On kuitenkin tilanteita, joissa virransyöttötarpeet muuttuvat nopeasti eikä yleiseen jakeluverkkoon voi joko luottaa tai sitä ei ole lähettyvillä. Tällaiset tilanteet koskevat normaalioloissa erityisesti teollisuusyrityksiä ja poikkeusoloissa viranomaisia ja sotajoukkoja.

Rebelvolt on lyhyen historiansa aikana kehittänyt useita eri kokoisia ja eri tarkoituksiin soveltuvia versioita tuotteestaan. Tärkeimpinä asiakastoimialoina yritys tavoittelee rakennusteollisuutta sekä puolustus- ja turvallisuussektoria. Jälkimmäisen tarpeita heijastelee hyvin Pitch Finland DefSec -kilpailun voitto, kun Rebelvolt esitteli kannettavan e-generaattoriratkaisun toukokuussa 2025. Vaikka yritys on omien sanojensa mukaisesti aloittanut pilotoinnin Puolustusvoimien kanssa, lienee tulevaisuuden tähtäimessä muutkin Nato-maat, mistä osoituksena yritykselle jo tässä vaiheessa myönnetty Nato NSN-sertifikaatti.

Sotajoukolle akkupohjaisten e-generaattorien hyödyt ovat ilmeisiä. Ensinnäkin suojan näkökulmasta akkupohjaisen generaattorin havaittavuus verrattuna polttomoottoriin on selvästi pienempi johtuen matalammasta lämpöjäljestä ja akustisesta äänettömyydestä. Huollon näkökulmasta ylläpito helpottuu eikä esim. arktiset olosuhteet sen enempää kuin kuumuus, pöly tai kosteus vaikuta generaattorin toimintaan. Taktisesta näkökulmasta hyötyjä on löydettävissä myös yhä useampien sähkövirtaa tarvitsevien sotavarusteiden lataamisen helpottumisesta sekä keskitetyissä että hajautetuissa ryhmityksissä.

Thistle

Tallinnalainen Thistle perustettiin vuonna 2024 kehittämään miehittämättömien ilma-alusten torjuntaan (counter-UAS) soveltuvaa vastajärjestelmää. Yrityksen ThistleShield-ratkaisu perustuu joukon käytössä olevien käsiaseiden, kuten ryn-

Thistlen tiimi esittelemässä counter-UAV konseptiaan ja vastaamassa esiupseerikurssi 76:n oppilasupseerien kysymyksiin.
Kuva: Riihimäen Kaupunki/Juho Haavisto.

näkkökiväärien tai haulikkojen, hyödyntämiseen järjestelmän vaikuttavina osina. Ratkaisu itsessään käsittää kolmijalan, kuuden aseen kiinnittämiseen soveltuvan laukaisuihin kykenevän rungon, kolme kamerasensoria sekä tekoälykomponentin. Järjestelmää voidaan käyttää sekä kauko-ohjattuna että sensorihavaintoihin perustuvassa tekoälyavusteisessa man-in-the-loop -tilassa.

Thistlen ratkaisua on testattu Ukrainassa ja yhteistyö taistelevien joukkojen kanssa on käynnissä. Kotimaassaan Thistle on jo allekirjoittanut ensimmäisen aiesopimuksen Viron puolustusvoimien kanssa.

Sotilaallisesta näkökulmasta mielenkiintoiseksi Thistlen ratkaisun tekee se, että järjestelmä ei vaadi kokonaisen uuden asejärjestelmän hankintaa, vaan olemassa olevaa huoltoa, logistiikkaa ja ammuksia voidaan hyödyntää täysimääräisesti. Koska innovaatio on suhteellisen edullinen ja siirrettävä, voidaan yksittäiseen joukkoon sijoittaa useampia järjestelmiä ketterästi hajautettavaksi.

Kiihdyttämön saavutukset

Julkisrahoitteisena ohjelmana Define-kiihdyttämöllä oli ennakkoon asetetut tavoitteet. Ohjelman suorien saavutusten odotettiin näkyvän toisaalta osallistuneiden kasvuyritysten menestyksenä ja toisaalta innovaatioekosysteemin kehityksenä.

Kasvuyritysten menestystä voidaan kuvata liiketoiminnan kehittymisenä ja kasvuna. Ennen kiihdyttämöohjelman loppua kaksi yrityksistä myytiin ja seitsemän keräsi merkittävän riskipääomasijoituksen. Monet yrityksistä solmivat Suomen ja muiden maiden puolustusvoimien kanssa aiesopimuksia tai tekivät sopimuksen joko pilotti- tai varsinaisesta toimitusprojektista.

Myös ekosysteeminäkökulmasta kiihdyttämöohjelma loi kasvua. Kasvuyritykset synnyttivät vuoden aikana kymmeniä uusia työpaikkoja, joista monet Riihimäen ympäristöön. Uudet innovaatiot ja innovaattorit vahvistavat täten jo ennestään merkittävää puolustussektoritoimijoiden alueellista keskittymää.

Kaksikäyttöratkaisujen yrityskiihdyttämönä Define Accelerator teki Suomessa pioneerityötä ja toimi kiistattomana suunnannäyttäjänä puolustustoimialan kehittämisessä. Definen vanavedessä on sittemmin aloittanut uusia kaksikäyttökiihdyttämöitä, sijoitusyhtiöitä ja innovaatio-organisaatioita, kuten 17Tech, Finnish Defence House, Nato Diana sekä kokonaan puolustusratkaisuihin keskittyvä Aalto Defence -opiskelijajärjestö.

Vuosi 2026

Näkymä alkaneen vuoden sotilaallisille innovaatioaktiviteeteille on todella lupaava. Puolustusvoimat ilmoitti vuodenvaihteessa perustaneensa Puolustusvoimien tutkimuskeskuksen alle sijoittuvan PVI-NYX-yksikön, jonka tehtävänä on toimia linkkinä kasvuyritysten ja puolustusvoimallisten tahojen välillä. Uskoa tulevaan luo yksikön julkisesti aloittamat rekrytoinnit. Samankaltaista kehitystä edustaa alkuvuodesta käynnistynyt Suomessa VTT:n operoima Diana-kiihdyttämö, johon osallistumisen edellytyksenä on aina kaksikäyttöinnovaatio. Tämäkin on erittäin hyvä merkki panostuksesta innovaatioihin.

Julkisten toimijoiden lisäksi innovaatioiden syntymistä edistävät yksityiset toimijat. Rahallinen panostus sotilasinnovaatioihin on kasvussa, ja suomalaisia enkelisijoittajia edustava FiBAN:n järjestänee tänäkin vuonna puolustusalan pitching-tilaisuuksia. Näitä jäämme odottamaan.

Lopuksi todettakoon, että alan kasvuyrityksiä kiinnostaa varmasti kaikki uudet konferenssit, hackathonit ja muut tapahtumat, joissa omaa osaamista ja ratkaisuja voi tuoda esille. Siksi onkin ilahduttavaa, että pelkästään tammikuussa järjestettiin kaksi uutta tapahtumaa: Winter Satellite Workshop Espoossa ja Drone Innovation Hackathon Tampereella. Molemmat tapahtumat vetivät puoleensa sekä teknologioihin vihkiytyneitä propellihattuja että puolustussektorin ammattilaisia. Uusille innovaatioille on selvästi olemassa sekä puolustuksellinen että sosiaalinen tilaus!

Tatu Tahkokallio on koulutukseltaan sähkötekniikan Diplomi-insinööri ja toimii opettavana tutkijana sotatekniikan laitoksen tutkimusryhmässä Maanpuolustuskorkeakoulussa. Vapaa-ajallaan Tahkokallio valmistelee väitöskirjatutkimusta puolustushallinnon ja yksityisen sektorin sotilaallisten ratkaisujen kehittämisyhteistyöhön liittyen.

TEKSTI: TERO PALOKANGAS

KUVAT: TERO PALOKANGAS, JUHA PELTOMÄKI

Viestikiltojen Liiton strategia 2030 – jotain uutta ja jotain vanhaa

Viestikiltojen Liitto Ry:ssä saatiin viimeisteltyä vuoden 2025 aikana strategiatyö, jossa pyritään määrittämään mitä viestikillat haluavat olla vuonna 2030 osana toimialan vapaaehtoiskenttää. Työ toteutettiin varsin perinteisen mallin mukaisesti, jossa pyrittiin ensin tunnistamaan toimintakentän muutokset 2030 mennessä sekä nykyisen toiminnan vahvuudet ja heikkoudet. Tämän jälkeen muodostettiin liitolle visio ja missio sekä keskeiset toiminnan osa-alueet, joilla pyritään viemään viestikillat elinvoimaisena 2030-luvulle. Parhaillaan on käynnissä strategian mukaisen toimeenpanosuunnitelman valmistelu, jolla varmistetaan ideoiden ja tavoitteiden siirtyminen myös käytännön toimintaan.

Nykytilasta ja tulevaisuudesta

Nykytilaa lähdettiin hahmottamaan perinteisen SWOT-analyysin keinoin. Keskeisinä tunnistettuina vahvuuksina voidaan mainita ainakin koeponnistetut toimintatavat ja perinteet, museotoiminnan tukeminen ja kehittäminen (Museo Militaria, Viestikeskus Lokki), Viestiristi talouden tukijalkana, yhteistyö Puolustusvoimien ja muiden vapaaehtoisten toimijoiden kanssa sekä alueellisten viestikiltojen tuoma maantieteellinen kattavuus. Tunnistetuista heikkouksista voidaan puolestaan mainita ainakin jäsenistön vanheneminen ja osittainen passiivisuus, nykyaikaisen viestinnän ja aktiivisen rekrytoinnin puute, oman koulutustoiminnan rajallisuus sekä nykyisen rahoituspohjan rajoitteet toiminnan monipuolistamiselle.

Kristallipalloa tutkittaessa 2030 näkökulmasta, tunnistettiin huomioitavana seikkana ainakin MPK:n korostuva rooli sotilaallisten valmiuksien (SOTVA) kouluttajana. MPK on selkeästi Puolustusvoimien sopimuskumppani nyt ja jatkossa SOTVA-tehtävän osalta. Viestikiltojen roolin hahmottaminen tulvaisuuden ekosysteemissä on vahvasti linkitetty myös liiton valtuuskunnan johtamaan koko toimialan vapaaehtoiskentän selvitystyöhön, johon puolestaan on saatu ohjaus Puolustusvoimista. Toinen huomioitava seikka on varmasti entisestäänkin lisääntyvä kamppailu ihmisten vapaa-ajasta. Toiminnan pitää olla entistäkin kiinnostavampaa ja siitä on myös sopivasti ”pidettävä meteliä”. Kolmas huomioitava seikka on mielenkiintoisen toiminnan mahdollistavien taloudellisten toimintaedellytysten varmistaminen, ”löysää rahaa” vapaaehtoistoiminnan tukemiselle kun ei jatkossakaan ole olemassa.

Tulevaisuuteen liittyvinä mahdollisuuksina nähtiin muun muassa turvallisuuspoliittisen tilanteen hyödyntäminen (vapaaehtoinen maanpuolustus kiinnostaa), entistäkin tiiviimpi yhteistyö muiden vapaaehtoisten toimijoiden kanssa, osaavan jäsenistön osaamisen hyödyntäminen ja aktiivinen käyttöön tarjoaminen, kokonaismaanpuolustusnäkökulman (sotilas- ja siviilikomponentin yhdistäminen) korostaminen sekä kansainvälistyminen. Merkittävimpinä uhkina puolestaan nähtiin ainakin toiminnan mahdollinen näivettyminen (jäsenistö, rahoitus),

Viestikiltojen yhteistyössä Puolustusvoimien ja muiden vapaaehtoisten toimijoiden kanssa vuosittain järjestämä A.R. Saarmaa -seminaari on vakiinnuttanut paikkansa keskeisenä toimialan koulutustilaisuutena. Kuvassa otteita vuoden 2025 seminaarista.

mahdollinen ajautuminen ”ulkokehälle” sotilaallisen maanpuolustuksen koulutusvastuiden osalta, Puolustusvoimien tuen vähentyminen entisestäänkin sekä epäonnistuminen kilpailussa ihmisten vapaa-ajasta.

Viestikiltojen Liiton visio ja missio 2030

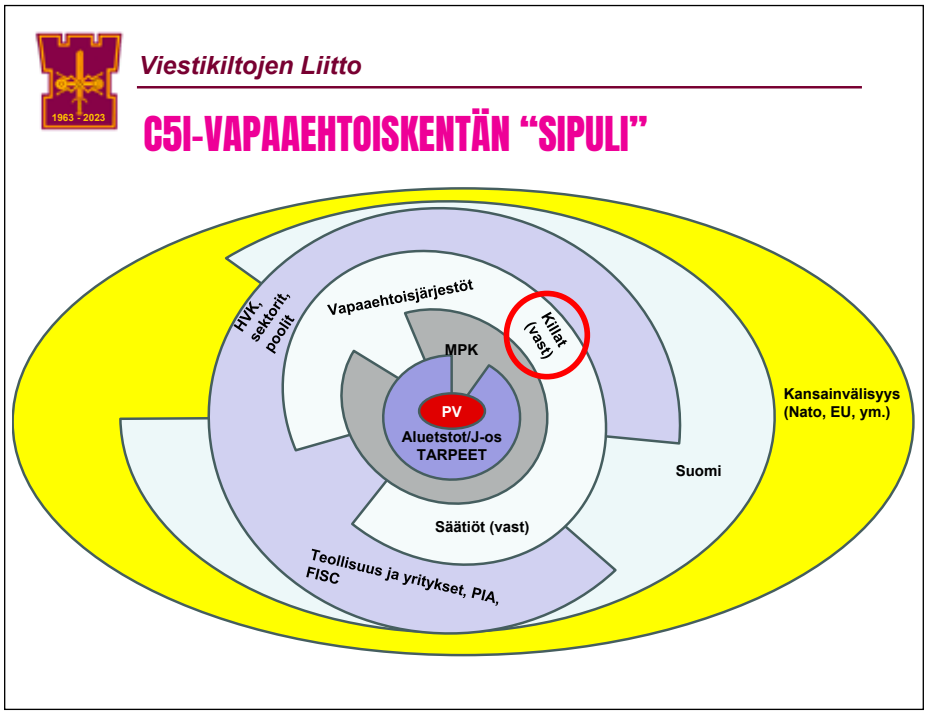
Nykytilan sekä tulevaisuuden mahdollisuuksien ja haasteiden tunnistamisen perusteella määritettiin Viestikiltojen Liitolle visio vuoden 2030 tavoitetilasta. Sen mukaisesti ***liitto on aktiivinen, ammattitaitoinen ja kiinnostava kokonaismaanpuolustuksen johtamisvalmiuksien kehittäjä ja kouluttaja sekä viestialan perinteiden vaalija***. Visiossa haluttiin tietoisesti korostaa kokonaismaanpuolustuksen näkökulmaa, aktiivisuutta niin toiminnassa kuin myös siitä viestimisessä sekä kehittämisnäkökulmaa perinteisemmän koulutustehtävän lisäksi. Myös perinteistä vahvuusaluetta viestialan perinteiden vaalijana haluttiin edelleen tavoitteena korostaa. Voisi kai sanoa, että mitään sivuaskelia tai ”hyppyjä tuntemattomaan” liitto ei ole ottamassa.

Vision jälkeen mietittiin mitä toiminnalla halutaan 2030 saavuttaa, siis puhutaan missiosta. Liitto haluaa jatkossakin toimia yhdyssiteenä vanhojen ja nykyisten toimialan ihmisten välillä, ovatpa sitten aktiivipalveluksessa tai reservissä. Liitto aikoo tulevaisuudessa myös tarjota johtamisjärjestelmä- ja viestialasta kiinnostuneille valtakunnallisen, alueellinen kattavuus samalla varmistaen, alustan vapaaehtoisen maanpuolustuksen harrastamiselle. Tähän liittyen jatketaan myös jäsenten maanpuolustushengen ja -tahdon ylläpitämistä ja kehittämistä.

Vuonna 2030 liitto osallistuu aktiivisena toimijana viesti- ja johtamisjärjestelmien kehittämiseen sekä ajantasaisen tiedon jakamiseen. Liitto tulee järjestämään laadukkaita kokonaismaanpuolustuksen poikkeusolojen johtamisvalmiuksiin liittyviä koulutustilaisuuksia, maantieteellinen kattavuus huomioiden. Jatkossakin tullaan tukemaan myös MPK:ta sotilaallisten valmiuksien kouluttamisessa ammattitaitoisella viestikiltojen kouluttajapoolilla. 2030-luvulla liitto haluaa myös edelleen osallistua viestialan arvokkaiden perinteiden valtakunnalliseen vaalimiseen.

Viestikilta 2030 osa-alueet toiminnan keskiössä

Vision ja mission määrittämisen jälkeen päätettiin tulevaisuuden tavoitetilaa jäsentää alueellisen viestikillan näkökulmasta, pilkkoen toiminta toisiaan tukeviin osa-alueisiin (ydintoiminnot). Toiminnan keskeisten osa-alueiden voidaan nähdä oheisen kuvan mukaisesti muodostavan lentokoneen potkurin. Sujuvan toiminnan mahdollistaminen edellyttää osa-alueiden (yksittäiset potkurin lavat) tasapuolista kehittämistä. Jos joku lavoista ei ole riittävän vahva, se tulee repeytymään irti pyörimisnopeuden (toiminnan aktiivisuus) kasvaessa. Osa-alueita onkin kehitettävä tasapuolisesti kokonaistoiminnan tavoitetilan saavuttamiseksi. Luonnollisesti osa-alueiden sisällä on mahdollista (kuten nykyäänkin) alueellisesti erikoistua toisistaan eroaviin kehittämis- ja koulutuskokonaisuuksiin. Sama sapluuna ei varmuudella jatkossakaan toimi eri viestikilloissa, erikoistumiselle ja omille painotuksille on tärkeä jättää myös liikkumavaraa.



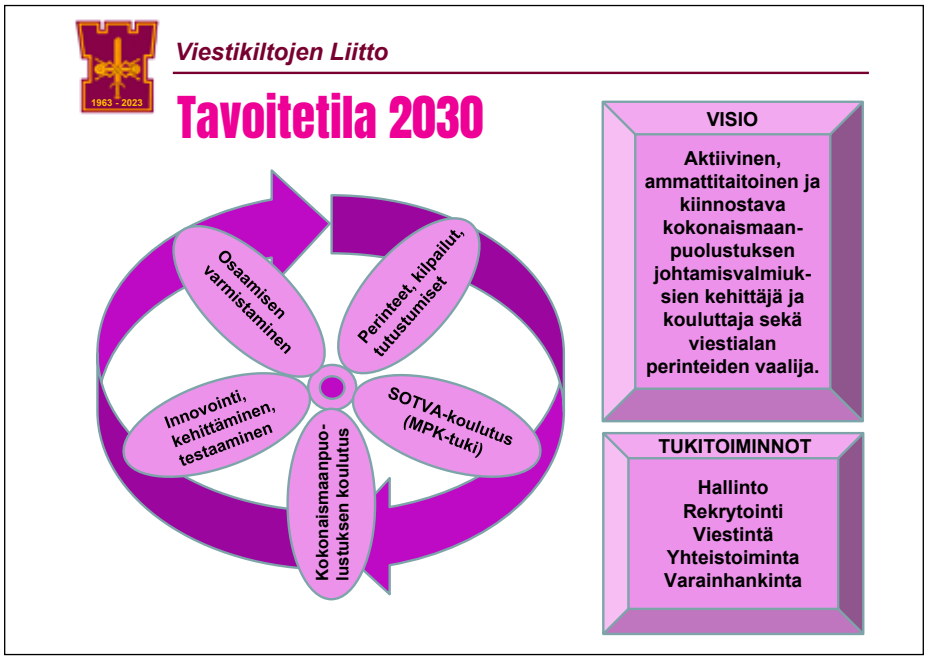
Liiton valtuuskunnan johdolla laadittu näkemys C5I-vapaaehtoiskentän rakenteesta.

Viestikiltojen nykytilanteesta laaditun SWOT-analyysin keskeiset havainnot.

Ensimmäisen määritellyn osa-alueen muodostaa perinteet, kilpailut ja tutustumismatkat. Osa-alueen sisällä tarkoituksena on ainakin jatkaa Museo Militarian ja Viestikeskus Lokin tukea, muitakaan perinteiden vaalimistehtäviä unohtamatta. Lisäksi osa-alueeseen kuuluvat jatkossakin vuoden viestikilta ja mahdollisesti myös viestikiltalainen kilpailut, valtakunnalliset viestimiespäivät ja perinteiset kotirata-ammunnat. Kaikkien tapahtumien osalta on samalla syytä tarkastella niiden toteutustapaa ja sopivaa päivitystä (”facelift”) 2030-luvulle. Myös valtakunnallisilla sekä ennen kaikkea alueellisilla vierailuilla ja tutustumisilla nähdään jatkossakin oma arvonsa. Niitä on luontevaa myös hyödyntää osana paikallista viestintää ja jäsenrekrytointia.

Toinen osa-alue on sotilaallisia valmiuksia tukeva (SOTVA) koulutus. Osa-alueessa korostuu ennen kaikkea paikallisjoukkojen tarvitseman koulutuksen tuki MPK:lle viestikiltojen valtakunnallisen ja alueellisen koulutuspoolin kautta. Tehtävään liittyen viestikillat tulevat jatkossakin olemaan aktiivinen toimija MPK:n eri koulutusohjelmien suunnittelussa ja toimeenpanossa. Kolmannen osa-alueen puolestaan muodostaa kokonaismaanpuolustuksen johtamisvalmiuksiin liittyvä koulutus. Tähän voi kuulua esimerkiksi erilaiset kyläradiot ja varaviestijärjestelyt, dronet eri muodoissaan ja käyttötarkoituksissaan, arjen johtamisvälineet sekä yleiset kyberturvallisuustaidot. Sekä SOTVA- että kokonaismaanpuolustusta tukevassa koulutuksessa on merkittävä mahdollisuus alueelliseen erikoistumiseen viestikiltojen omien intressien, osaamisalueiden sekä saatavilla olevien yhteistyö- ja tukimahdollisuuksien mukaisesti.

Neljännessä osa-alueessa korostuvat innovointi, kehittäminen ja testaaminen. Ajatuksena on tarjota vapaaehtoiskentän resursseja niin Puolustusvoimien, muiden viranomaisten kuin myös kotimaisen puolustusteollisuuden käyttöön. Toiminnassa voisi painottua esimerkiksi kaluston tai ohjelmistojen testaaminen (kokeilukäyttö, kenttätestaaminen), sekä palautteen antaminen mahdollisine kehitysideoineen. Viidentenä osa-alueena on määritetty osaamisen varmistaminen. Tähän kuuluu muun muassa kouluttajapoolien kokoaminen, perehdyttäminen, harjoittaminen sekä parhaiden käytäntöjen jakaminen. Osaamisen kehittämisessäkin on huomioitava erikseen niin valtakunnallinen kuin myös alueellinen näkökulma valittuine painopisteineen.



Viestikiltojen Liiton visio 2030 ja toiminnan keskeiset osa-alueet.

Tukitoiminnot ja yhteistyö luovat mahdollisuuksia

Ydintoiminnot edellyttävät tuekseen keskeisiä tukielementtejä, joilla varmistetaan Viestikilta 2030 mukaisen potkurin tasainen pyöriminen ja tarvittaessa toiminnan kiihdyttäminen. Tukitoiminnot toimivat ikään kuin moottorina ja toisaalta voiteluaineena, mahdollistaen tasapainoisen toiminnan. Yhdistyksen hallinto on keskeinen tukijalka toiminnalle jatkossakin. Tässä on syytä jatkossa tarkastella hajautettua hallinnollisten tukipalveluiden käyttöä (esimerkiksi Maanpuolustuskiltojen Liiton jäsenpalvelut) sekä pää- tai osatoimisten toimijoiden käyttöä toimialan eri yhdistysten hallinnollisiin tehtäviin. Puhtaasti vapaaehtoisilla luottamustehtävillä 2030-luvulla ei hallinnon tukitoiminnot ole enää todennäköisesti toteutettavissa.

Rekrytointiin on jatkossa saatava selkeä tason nosto ja ”lisäboostaus”. Kaikissa tapahtumissa on jatkossa oltava mukana rekrytointinäkökulma. Pelkästään nykyisille jäsenille suunnattujen tapahtumien aika on ohi, jos haluamme pitää jäsenistön jatkossa elinvoimaisena. Keskeisiä kokonaisuuksia ovat jatkossakin liiton taloudellinen tuki alueellisten viestikiltojen rekrytointiin, sekä laadukkaan rekrytointia tukevan materiaalin laatiminen ja jako niin valtakunnalliseen kuin myös alueellisiin tarpeisiin.

Viestintää on tukielementtinä saatava entistä aktiivisemmaksi. Nykyisten viestintäkanavien lisäksi alati kehittyvä sosiaalinen media on otettava haltuun. Tämä edellyttää lisäresursointia myös viestintään, nuoria ja innokkaita somevaikuttajia on saatava toimintaan mukaan. Jotta voidaan jatkossa tehokkaasti viestiä, tulee viestittävän ”tuotteen” toki olla myös kunnossa. Koulutustarjonnan ja järjestettävien eri tapahtumien on oltava jatkossakin laadukkaita ja itsessään jo kiinnostusta herättäviä. Viestinnällä voidaan sen jälkeen toimintaa hyvin tehostaa ja positiivisia mielikuvia vahvistaa.

Yhteistoimintaa tarvitaan jatkossa entistä enemmän ja tiiviimmin. Yhteistyötä onkin kyettävä tiivistämään niin valtakunnallisella kuin myös alueellisella tasolla, niin Puolustusvoimien kuin myös muiden toimijoiden (esimerkiksi muut turvallisuusviranomaiset, kunnat/kaupungit/hyvinvointialueet, puolustusteollisuus, muut vapaaehtoisjärjestöt) kanssa. Toimialan osalta iso mahdollisuus sisältyy myös liiton valtuuskunnan johtamaan C5I -kokonaisuuteen ja yhteistyön konkreettiseen tiivistämiseen sen sateenvarjon alla.

Talous tulee näyttelemään jatkossakin isoa roolia toiminnan kehittämisessä. Ilman lisärahoitusta on unennäköä yrittää uudistaa ja monipuolistaa viestikiltatoimintaa 2030-luvulle. Nykyinen toiminnan päärahoituslähde ovat viestiristit, eikä niiden varaan voida merkittävää lisätuotto-odotusta rakentaa. Kehitys- ja koulutusyhteistyön tiivistäminen Puolustusvoimien, MPK:n ja puolustusteollisuuden kanssa voisi tuoda lisärahoitusmahdollisuuksia, esimerkkinä vastineeksi viestikiltojen toteuttamasta testaustoiminnasta omaan kokeilu- ja koulutuskäyttöön saatavan materiaalituen muo-

dossa. Toinen harkinnan arvoinen seikka voisi olla entistäkin laadukkaimmiksi rakennettavien tapahtumien (esimerkkinä A.R. Saarmaa -seminaari) muuttaminen maksulliseksi.

Lopuksi

Viestikiltojen liitto jatkaa yhdessä paikallisten viestikiltojen kanssa 2030 strategiansa mukaisen tavoitetilan suunnittelua. Tavoitteena on vuoden 2026 aikana rakentaa toimeenpanosuunnitelma, jossa määritetään vuosille 2027–2029 toteutettavat konkreettiset toimenpiteet sekä vastuutetaan viestikiltakentän eri toimijat samalla näihin tehtäviin. Toimeenpanoon tarvitaan kaikkien yhteistyötahojemme tukea ja kutsunkin tässä samalla kaikki halukkaat mukaan sekä sparraamaan ajatuksiamme että tukemaan strategiamme toimeenpanoa. Yhdessä olemme tässäkin kokonaisuudessa takuulla vahvempia. Viestikiltakentillä (nykyisillä ja uudistuvilla) tavataan!

Kirjoittaja toimii Viestikiltojen Liitto ry:n puheenjohtajana

Viestikiltojen Liiton järjestämät viestimiespäivät ovat erinomainen tilaisuus koko toimialan eri toimijoiden väliselle verkostoitumiselle. Kuva vuoden 2025 viestimiespäiviltä, jotka järjesti Päijät-Hämeen Viestikilta Lahden alueella.

TEKSTI JA KUVAT: TAPIO TEITTINEN, KAAKKOIS-SUOMEN VIESTIKILTA RY

Tutkimusta, julkaisuja, näyttelyitä, esitelmiä jopa elokuvia – tutkimuksella sotahistoriaa tutuksi

Kiltojen yksi keskeisimmistä tehtävistä on vaalia aselajin tai joukko-osaston perinteitä. Yksi etenemisreitti on tutkimuksen tekeminen ja sitä kautta saatavan tietopääoman avulla voidaan tutkimuksen tuloksia jatkojalostaa tuottamalla julkaisuja, näyttelyitä, esitelmiä ja jopa elokuvia.

Päätös lähteä tutkimustielle vaatii lievää hulluutta, sitoutumista ja pitkäjänteisyyttä. On oltava mielenkiintoiselta vaikuttava tutkimuskohde, on laadittava tutkimussuunnitelma siitä mitä tutkitaan, miten tutkitaan aikatauluineen ja ennen kaikkea tutkimuskysymykset, jotka ohjaavat välillä harhaisella tutkijan polulla.

Tutkimustyö vaatii, ainakin pääkaupungista kaukana asuvilta, useampia reissuja Helsinkiin, koska siellä sijaitsevat Kansallisarkiston arkistoaarteet. Yksittäisiä mappeja voi tilata myös ”periferiaan” maakunta-arkistojen tiloihin, mutta tuokin maksaa melkoisesti.

Edellä mainitusta voi jo päätellä, että tutkimustyö vaatii jonkin verran rahaa, varsinkin jos kunnianhimoisena tavoitteena on laatia tutkimustyö julkaisuksi. Onneksi maasta löytyy tahoja, jotka voivat auttaa asiassa. Kiltamme on saanut apurahoja tutkimuksiin ja näyttelyiden pystytyksiin ainakin seuraavilta tahoilta: Maanpuolustuksen Viestisäätiö, Sotavahinkosäätiö ja Suomen Kulttuurirahaston Etelä-Savon rahasto. Kaikille säätiöille on aikanaan raportoitava rahan käytöstä varsin perusteellisesti. Apurahan saamiseksi on tutkimussuunnitelman oltava kaikin puolin kunnossa – eikä aina onnikaan potkaise.

Paljon löytyy materiaalia myös netistä, erityisesti sotapäiväkirjojen osalta. Kansallisarkistojen kansioita selvitellessä on pystyttävä tilaamaan tutkijasaliin halutut kansiot ennakolta. Tämä haluttujen kansioiden ennakkoselvitys on välillä melkoista lottoa. Vaikka onkin perehtynyt tutkittavien kohteiden organisaatioihin niin kansioiden sisällyskuvausten perusteella voi käydä niin, että kansiosta ei löydy kuin yksi asiakirja, josta on mahdollisesti hyötyä. Pitkämatkalainen ei voi käyttää aikaansa asiakirjojen asioiden kirjaamiseen muistiinpanoihin, vaan parasta on vain kuvata kyseinen asiakirja vaikkapa matkapuhelimella ja siirtyä seuraavan asiakirjan kimppuun. Näitä satoja valokuvia voi sitten kotona rauhassa lukea.

Hamid Al-Sammarraee kuvaa Lokin keskusta.

Jotkut museot ja järjestöt ovat olleet aikanaan kaukaa viisaita ja keränneet sodassa mukana olleiden henkilöiden haastatteluja aluksi haastattelunauhoille, jotka myöhemmin on siirretty tekstimuotoon. Olemme saaneet omiin tutkimuksiimme esimerkiksi Päämajan viestikeskus Lokissa ja Rukajärven suunnalla taistelleiden henkilöiden kertomuksia.

Erinomaiseksi hyödyksi tutkimustyölle on taho, jolla on tietotaitoa ohjata työtä. Meillä on ollut onni nauttia runsaasti tutkimustyötä ja julkaisuja tehneen eversti Seppo Uron ohjauksesta.

Tutkimuksen valmistuttua alkaa seuraava vaihe, työn jatkojalostaminen julkaisuksi. Tähän liittyvät tekstiasun muotoilu ja kuva- sekä piirrosmateriaalin hankinta. Tätä työtä kannattaa tehdä ainakin osittain rinnan itse tutkimustyön kanssa. Varsinkin Kansallisarkistosta saatavat kartat ja tekniset piirustukset ovat hyvä mauste julkaisussa. On syytä huolehtia mahdollisten kuvien ja piirrosten immateriaalioikeuksista ja käyttöluvista.

Julkaisuun on hyvä merkitä lähdeviitteet varsin tarkasti, jotta sitä voidaan hyödyntää muissa tutkimuksissa. Oikolukua ei voi koskaan tehdä liikaa, on korjattava joukko-osastojen kirjoitusasuja, varsinkin lyhenteiden osalta, lauseenrakenteita ja ihan perus pilkkuvirheitä. Tämä on

varsin tuskastuttavaa hommaa, mutta kiittää lopussa tekijäänsä.

Julkaisun taitto- ja painotyö kannattaa kilpailuttaa, koska näissä on melkoisia eroja. Julkaisun kustannuksiin vaikuttavat sivumäärän lisäksi kansitus ja paperin laatu. Monivärisiä julkaisuja ei ainakaan apurahoilla kannata ajatella.

On mahtava olo, kun kilta voi järjestää noin parin vuoden aherruksen jälkeen uuden tutkimuksen julkistamistilaisuuden. Taas on pieni palanen historiaa saatu kasatuksi jäsennellyksi kokonaisuudeksi jälkipolville. Tutkimuksen myötä saatua tietoa voidaan jalkauttaa eri muodoissa aiheesta kiinnostuneiden nähtäväksi ja kuultavaksi näyttelyiden, esitelmien ja lehtijuttujen muodossa.

Näyttelyiden kasaaminen on ihan oma projektinsa. Materiaalin kerääminen ja lainaaminen eri museoista vaatii luottamuksellisia suhteita. Aiheen esillepano vaatii myös oman suunnittelunsa, valokuva- ja piirrossuurennokset, sekä selitetaulut, eli koko kokonaisuus sellaiseen muotoon, että näiden nostojen kautta asia avautuu katsojalle. Joskus käy niin hyvä tuuri, että Kansallisesta audiovisuaalisesta Instituutista (Kavi) löytyy sopivaa TK-filmimateriaalia elävöittämään näyttelyä. Kavin filmivuokrat ovat varsin kohtuullisia. Näyttelyitä kannattaa myös kierrättää eri paikkakunnilla. Tällöin tuosta materiaalista ja työstä saadaan suurempi hyöty.

Kaakkois-Suomen Viestikilta on tehnyt kolme tutkimusta ja niistä julkaisut: ”Päämajan salainen radiokeskus”, ”Viestisotaa Rukajärvellä” ja ”Ylijohdon viestiverkot Suomen sodissa 1918–1945”. Kirjoittajina ovat toimineet kaikissa Tapio Teittinen ja Martti Susitaival sekä ensimmäisessä myös Heikki Huttunen.

Kahdesta ensin mainitusta on laadittu näyttelyt, jotka ovat olleet esillä vaihtuvien näyttelyiden talossa Museo Militariassa. Lisäksi ensin mainittu on ollut esillä myös Päämajan viestikeskus Lokissa ja jälkimmäinen Lieksassa Rukajärvikeskuksessa. Päämajan viestikeskus Lokin sulkeuduttua rakensi kilta sekä Radiokeskuksen että Lokin näyttelyn Päämajamuseoon. Kaikkia aiheita on käyty esitelmöimässä Helsingissä, Iisalmessa,

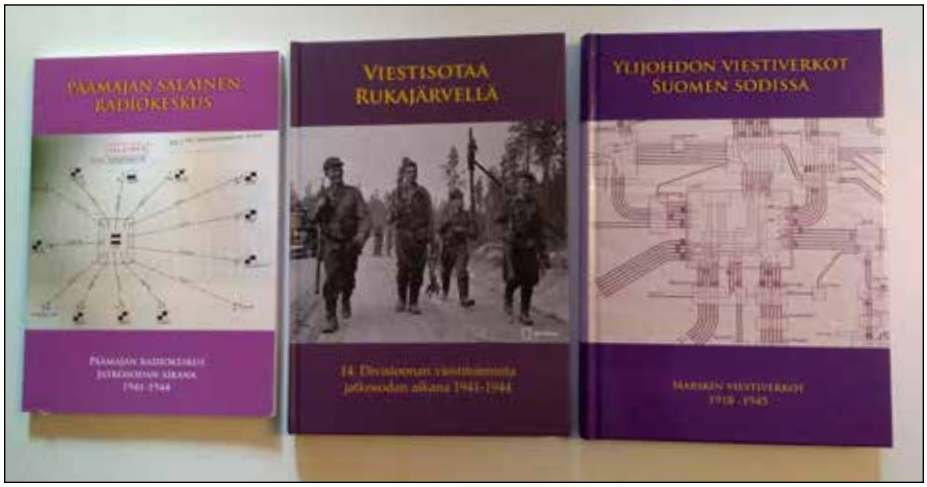
Lokki-filmin kuvauksissa Pia Tiilikka ja kirjoittaja.

Seinäjoella, Lahdessa, Kouvolassa, Pieksämäellä, Hämeenlinnassa, Petäjävedellä, Savonlinnassa, Ristiinassa ja Mikkelissä hankkeiden puuhamiesten Martti Susitaipaleen ja Tapio Teittisen toimesta.

Viimeisenä tuotettuna hankkeena oli Lokista kertovan dokumenttifilmin valmistus. Filmi palkittiin Suomen filmi- ja videokuvaajien liiton SM-kisoissa hopeasijalla dokumenttisarjassa. Filmin lyhennelmä pyörii non-stoppina Päämajamuseossa ja sitä näytetään kokonaisena eri tilaisuuksissa. Käsikirjoittajana ja ohjaajana toimi Tapio Teittinen, kuvauksen ja editoinnin toteutti Hamid Al-Sammarraee ja Mikkelin Teatterin näyttelijä Aapo Oranen luovutti äänensä kertojan roolissa. Filmin pääsponsorina toimi Pellervo Pekkola.

Nyt on killalla työn alla Lokin purkaminen ja aikanaan kokonaan uuden Lokki-näyttelyn pystyttäminen Naisvuoren luolastoon yhteistoiminnassa Mikkelin kaupungin, Sodan ja rauhankeskus Muistin ja Päämajamuseon kanssa.

Kirjoittaja Tapio Teittinen on Kaakkois-Suomen Viestikillan kunniapuheenjohtaja.



Killan julkaisemat kirjat.

Kutsu Viestiupseeriyhdistys ry:n kevätkokoukseen

Viestiupseeriyhdistys ry:n hallitus kutsuu yhdistyksen jäsenet **kevätkokoukseen Espooseen, Erillisverkkojen tiloihin, torstaina 23.4.2026 klo 14.00 alkaen**. Käyntiosoite: Tekniikantie 4 D Otaniemi, 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 ERVE:n tiloihin klo 14.00 mennessä, Auditorio Tapio 1.krs

Kahvit klo 14.00–14.30

Kevätkokous klo 14.30–15.30

Erillisverkot liiketoimintojen esittely 15.30–17.00

Tilaisuuden päättäminen noin klo 17.00.

Julkisilla pääsee kätevästi Helsingin Päärautatieasemalta metrolla Aalto Yliopiston asemalle ja sieltä kävellen (n 600m) ERVE:n tiloihin.

Omilla autoilla tuleville on kiinteistössä vieraspaikkoja talon edessä kahdella seinustalla. Kannattaa huomata, että pääovemme on parkkipaikan puolella ja siinä lukee isolla INFO. Vastaanotosta saa parkkilupia, jotka tulee laittaa autossa näkyvälle paikalle. Parkkisakkoja on annettu pihalla kovin herkästi.

Ilmoittautumiset **16.4.2026 mennessä** tai vaikka saman tien www.viestiupseeriyhdistys.fi -sivuilla olevalla lomakkeella (toivottavin tapa), sähköpostitse toiminnanjohtaja@viestiupseeriyhdistys.fi tai puhelimitse 040 514 2497.

Tervetuloa kevätkokoukseen! Viestiupseeriyhdistys ry:n hallitus

Viestiupseeriyhdistyksen jäsenmatka Norjaan

Viestiupseeriyhdistys järjestää jäsenmatkan Norjaan, Osloon ja Lillehammeriin, 27.8. - 30.8.2026. Matkan aloitetaan to 27.8.2026 tutustumisella Suomen Suurlähetystöön Oslossa, josta siirrytään saman päivän aikana Lillehammeriin. Lillehammerissa on tarkoitus tutustua Norjan Puolustusvoimien Jörstadmoen Varuskuntaan sisältäen mm. esittelyn Cyber Defense -keskuksesta. Matkalla vieraillaan myös Lillehammerin Olympialaisten kohteissa ja alueen kulttuurikohteissa.

Matkan pääpiirteinen aikataulu on seuraava:

- to 27.8 lento Hki-Oslo aikaisin aamulla, vierailu Oslossa Suomen suurlähetystössä ja sieltä junalla Lillehammeriin, jossa majoittuminen hotelliin illalla.
- pe 28.8 tutustumiset Lillehammerin kohteisiin ja Jörstadmoen varuskuntaan.
- la 29.8 kulttuuripäivä: vierailut mm. Maihaugen museo ja Olympic Park sekä illalla yhteinen päivällinen.
- su 30.8 paluukuljetukset junalla ja lennolla siten, että Suomessa n. klo 18.00 mennessä.

Tilaisuuden tarkempi ohjelma, ohjeet ilmoittautumisesta ja matkan hinta julkaistaan maaliskuun aikana jäsenille lähetettävällä sähköpostiviestillä. Jos olet kiinnostunut, niin varaa ajankohta jo nyt kalenteriisi.

Lopullinen ohjelma sekä muut tarkemmat tiedot ja ohjeet lähetetään sähköpostilla matkalle ilmoittautuneille kesäkuun 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!

Puolustusvoimien johtamisjärjestelmäkeskuksen johtajat tapasivat

Puolustusvoimien johtamisjärjestelmäkeskuksen (PVJJK) nykyisen johtajan, insinöörieversti Janne Jokisen kutsusta keskuksen entiset johtajat oli kutsuttu tapaamiseen keskuksen esikuntaan Jyväskylään tiistaina 13.1.2026. Tilaisuuteen pääsi osallistumaan kuusi johtajaa.

Tapaamisen yhteydessä saimme tutustua PVJJK:n nykypäivään, tehtäviin, teknologiaratkaisuihin, Nato-jäsenyyden vaikutuksiin sekä moniin muihin tehtyihin kehitystoimiin – ja toki myös kehittämis- ja resurssitarpeisiin. Maailman sotilas- ja turvallisuuspoliittinen tilanne näkyy luonnollisesti keskuksen arjessa monin tavoin. Kuullun ja käytyjen keskustelujen perusteella jäi kuva, että keskus pystyy hyvin vastaamaan sille annettuihin tehtäviin eri valmiustiloissa.

Janne Jokisen isännöimän vierailun jälkeen meillä oli mahdollisuus jatkaa keskusteluja ja laajemminkin kuulumisten vaihtamista yhteisellä päivällisellä. Mukaan pääsi myös muutama PVJJK:n esikunnan henkilö. Lämmin kiitos Esa Salmiselle päivällisen mahdollistamisesta.

PVJJK perustettiin 1.1.2007 osana laajempaa puolustusvoimien tietohallinnon rationalisointia silloisen Puolustusvoimien Tietotekniikkalaitoksen (PVTietoTL) rungolle. PVTietoTL:n silloinen johtaja oli määrätty 1.6.2006 alkaen, oman toimensa ohella, myös Puolustusvoimien Johtamisjärjestelmäkeskuksen johtajaksi ja teki mm. suuren osan tulevan keskuksen tehtävänimityksistä (minkä vuoksi myös Esa Salminen lukeutuu ”johtajakaartiimme”). Tietohallinnon rationalisoinnissa valtaosa puolustusvoimien yhteisestä ICT-hankinnasta, -operoinnista ja -palvelutuotannosta keskitettiin yhdelle joukolle. Tuloksena syntyi kovan ammattitaidon palveluoperaattori ja samalla myös noin 800 hengen valmiusjoukko.

Suuret kiitokset kaikkien vieraiden puolesta Jannelle tämän vierailun kutsusta ja järjestelyistä. Entisenä johtajana sai tuntea suurta ylpeyttä siitä, miten keskus on kuluneen vajaan kahdenkymmenen vuoden aikana asemoinut itsensä puolustusvoimien johtamisen ja valmiuden kohottamisen mahdollistajaksi.

Pertti Hyvärinen

Eversti evp.

Viestiupseeriyhdistys 80 vuotta -juhlaottelu

Mikkelin Let´s Go Areenalla 5.12.2025 järjestetty jääkiekkoliigan ottelu pelattiin Viestiupseeriyhdistys 80 vuotta -teemalla ja brändivärein. Kyseessä oli jo yhdeksäs kerta, Suur-Savon Reserviupseeripiirin johdolla järjestettiin maanpuolustusteemainen jääkiekko-ottelu.

Viestiupseeriyhdistyksen 80-vuotisjuhlavuoden tapahtumien loppuhuipentumaksi voitaneen kutsua Mikkelin Jukurien ja Saimaan Pallon välillä 5.12.2025 pelattua liigajääkiekko-ottelua, jossa yhdistyksemme oli esillä monin tavoin. Kotijoukkue pelasi Viestiupseeriyhdistyksen brändivärien mukaisissa peliasuissa, hallin näyttötauluilla komeili yhdistyksemme juhlavuoden logo ja pelin päätteeksi minulla oli yhdistyksen puheenjohtajana kunnia jakaa parhaimman pelaajan palkinnot. Pelitapahtumaan liittyi myös kutsuvierastilaisuus, johon paikallinen reserviupseeripiiri oli kutsunut maanpuolustuksen piirissä toimivien organisaatioiden edustajia noin 20 henkilöä. Tunnelmaan aitiossamme yhdistyivät sekä voimakas maanpuolustushenki että ottelun mukanaan tuoma jännitys.

Teemaottelun historiaa

Mikkelissä on jo yhdeksän vuoden perinne järjestää joulukuun liigaottelu valitulla maanpuolustusaiheisella teemalla. Järjestelyjä koordinoi Suur-Savon Reserviupseeripiiri ja mukana ovat Maanpuolustuskoulutusyhdistys, Puolustusvoimien Etelä-Savon aluetoimisto sekä Mikkelin Jukurit -jääkiekkoseura. Tilaisuuteen liittyy kutsuvierastilaisuus, jossa tälläkin kertaa vieraille jaettiin tilaisuuden teeman mukaiset pelipaidat – ja vielä itse kunkin sukunimellä painettuna.

Ensimmäinen maanpuolustusteemainen ottelu järjestettiin vuonna 2017, jolloin teemana oli Suomi 100 vuotta. Sen jälkeen omilla tasavuosijuhlillaan on ottelun teemoiksi valittu muun muassa Suomen puolustusvoimat 100 vuotta, Suomen Reserviupseeriliitto 90 vuotta, Maanpuolustuskoulutusyhdistys 30 vuotta, Vapaaehtoinen pelastuspalvelu 60 vuotta – ja tällä kertaa Viestiupseeriyhdistys 80 vuotta. Saimme siis liittyä arvokkaaseen seuraan!

Let´s Go Areenan näyttötauluilla näkyi tilaisuuden teema ja yhdistyksemme juhlavuoden logo.

VUY 80v -teema

Kesällä 2025 Suur-Savon Reserviupseeripiiri tiedusteli Viestiupseeriyhdistyksen kantaa siihen, voitaisiinko joulukuun jääkiekko-ottelu pelata yhdistyksemme 80-vuotisjuhlan teemalla. Pyyntöön oli helppo vastata myöntävästi, varsinkin kun tästä ei koituisi yhdistykselle ylimääräisiä kustannuksia. Päinvastoin, Viestiupseeriyhdistys sai positiivista näkyvyyttä, mikä toivottavasti näkyy myös uusien jäsenhakemusten määrässä.

Kutsuvierastilaisuuden yhteydessä minulla oli kunnia palkita Suur-Savon Reserviupseeripiiri yhdistyksemme standaarilla. Kiitokset loistavasti onnistuneesta tilaisuudesta saivat myös muut järjestelyistä vastaavat. Yhdessä muiden Viestiupseeriyhdistyksen edustajien kanssa meillä oli suuri kunnia osallistua tähän tilaisuuteen.

Pertti Hyvärinen

Viestiupseeriyhdistyksen puheenjohtaja Pertti Hyvärinen luovutti yhdistyksen standaarin Suur-Savon Reserviupseeripiirin puheenjohtajalle Jan-Aulis Hiltuselle. Molemmilla päällä yhdistyksemme värein painetut pelipaidat.

TEKSTI: JYRKI PENTTINEN

Telealan uutisia

ETSI julkaisi keskeisen selvityksen 6G:n monikäyttötekniikoista

Euroopan telealan standardointijärjestö ETSI on julkaissut Industry Specification Group (ISG) Multiple Access Technologies (MAT) -ryhmän raportin, joka käsittelee tulevien 6G-radiojärjestelmien monikäyttötekniikoita. Raportti ETSI GR MAT 001 tukee suoraan 3GPP:n tulevia Release-20:n 6G-tutkimuksia. Selvityksessä verrataan perinteisiä tekniikoita, kuten ortogonaalista monikäyttöä ja MU-MIMO:a eli monikäyttäjien monitieantenneja (Multi User, Multiple In Multiple Out) edistyneempiin ratkaisuihin. Esimerkkejä jälkimmäisistä ovat RSMA (Rate-Splitting Multiple Access), tehotasoon perustuva NOMA (Non-Orthogonal Multiple Access) sekä välimuistia hyödyntävä MU-MIMO. Tulokset osoittavat, että eri tekniikat tarjoavat merkittäviä etuja eri käyttötapauksissa erityisesti spektritehokkuuden ja käyttäjäkohtaisen pääsyn hallinnan (”oikeudenmukaisuuden”) osalta. Kyseinen raportti muodostaa teknisen perustan 6G:n fyysisen kerroksen vaihtoehtojen arvioinnille ja on hyödyksi 3GPP:n tulevissa RAN-työryhmissä.[1]

Glasgow’n yliopisto esittelee metapinta-antennin 6G-käyttöön

Glasgow’n yliopiston tutkijat ovat kehittäneet digitaalisen, dynaamisesti ohjattavan metapinta-antennin (Dynamic Metasurface Antenna, DMA), joka toimii noin 60 GHz:n millimetriaaltotaajuudella. 60 GHz on yksi keskeisistä taajuusalueista varhaisille 6G-konsepteille, joten tutkimus on varsin mielenkiintoinen. Antenni yhdistää metamateriaalirakenteet FPGA-pohjaiseen (Field-Programmable Gate Array, kenttäohjelmoitava porttimatriisi) ohjaukseen mahdollistaen reaaliaikaisen antennin säteilykuvion muodostuksen ja sen muokkauksen ilman tarvetta monimutkaisille RF-laitteistoille. Esitetty ratkaisu parantaa keksijöidensä mukaan merkittävästi spektrin käyttöä ja joustavuutta tiheissä verkoissa, jotka ovat keskeisiä 6G:n suorituskykytavoitteita. Käytännön prototyyppi tuo metapintateorian lähemmäs todellisia järjestelmiä ja tuottaa mittausdataa, jota voidaan hyödyntää 3GPP:n kanavamalleissa ja järjestelmäsimulaatioissa.[2]

3GPP on järjestänyt ensimmäiset 6G-RAN-kokoukset

3GPP:n radiotyöryhmät (RAN, Radio Access Network) kokoontuivat Bengalurussa, Intiassa, viime elokuussa käsittelemään ensimmäistä kertaa samanaikaisesti 5G-Advanced-määritysten viimeistelyä (Release 19) ja 6G-työn käynnistämistä Release-20 -kehyksessä. Kokoukset merkitsivät konkreettista siirtymää 6G-tutkimuksesta varsinaiseen standardointiprosessiin. Käsiteltyjä aiheita olivat alustavat radio- ja arkkitehtuuritutkimukset, käyttötapausvaatimukset sekä tulevien 6G-tutkimusaiheiden kokonaisuuksien valmistelu. Laaja teollinen osallistuminen osoittaa vahvaa kansainvälistä sitoutumista 6G-standardien kehittämiseen 3GPP:n puitteissa.

Sittemmin, 3GPP on keskustellut 6G:stä viimeaikaisissa työryhmien pää- ja työryhmäkokouksissa, joista allekirjoittanut osallistui hiljattain toteutettuihin kokouksiin Dallasissa ja Baltimoressa. Varsinainen spesifiointityö on tosin vielä lähtökuopissaan Release 21:n alkamista odotellessa ensimmäisten normatiivisten 6G-arkkitehtuuri- ja toiminnallisten määritysten toteutuksineen, mutta näissä viimeaikaisissa kokouksissa käsiteltyjen 6G-aiheiden lukumäärä osoittaa teollisuuden aktiivista kiinnostusta uuden sukupolven määrittämiseen.[3]

Qualcomm ja Nokia Bell Labs demonstroivat tekoälypohjaista 6G:n fyysistä kerrosta

Qualcomm ja Nokia Bell Labs ovat esitelleet tekoälyyn perustuvia fyysisen kerroksen (PHY) ratkaisuja, jotka edustavat askelta kohti AI-natiivista 6G:tä. Tutkimuksessa hyödynnetään peräkkäistä oppimista (sequential learning) kanavatiedon (CSI, Channel State Information) palautteen ja esikoodauksen optimointiin reaaliajassa. Tulokset osoittavat parempaa läpimenokykyä verrattuna perinteisiin, 3GPP:n määrittelemiin CSI-mekanismeihin. Tämä työ korostaa siirtymää staattisista PHY-ratkaisuista kohti adaptiivisia, koneoppimista hyödyntäviä järjestelmiä, jotka ovat merkittävä teema tulevissa 6G-tutkimusaihekeskusteluissa. Demonstraatiot perustuvat realistisiin järjestelmäalustoihin, mikä tekee niistä erityisen relevantteja standardointityölle.[4]

Piifotoniikkaratkaisu avaa tien 6G:n terahertsitaajuuksille

Tutkijat ovat kehittäneet ultralaajakaistaisen terahertsialueen polarisaatiomultiplekserin, joka on toteutettu piialustalla. Ratkaisu toimii taajuusalueella 220–330 GHz ja vastaa yhteen 6G:n suurimmista teknisistä haasteista, mikä on terahertsispektrin tehokas hyödyntäminen. Polarisaatiomultipleksointi mahdollistaa useiden samanaikaisten signaalivirtojen käytön samalla taajuudella ja kasvattaa merkittävästi spektritehokkuutta. CMOS-yhteensopiva toteutus tekee ratkaisusta erityisen kiinnostavan 3GPP:n tuleville terahertsiradio- ja laitetutkimuksille, sillä se yhdistää teoreettiset 6G-konseptit käytännöllisiin, piiritasolla toteutettaviin ratkaisuihin.[5]

Lähteitä

[1] ETSI issues new Report on Multiple Access Techniques for 6G, 28.1.2026. https://www.etsi.org/newsroom/news/2633-etsi-issues-new-report-on-multiple-access-techniques-for-6g

[2] Metasurface antenna. https://www.timeshighereducation.com/research/university-glasgow/research-breakthrough-6g-communications-networks

[3] India Hosts First-Ever 3GPP Radio Access Network Meetings On 6G Standardisation In Bengaluru. 26.8.2026. https://www.ndtvprofit.com/technology/india-hosts-first-ever-3gpp-radio-access-network-meetings-on-6g-standardisation-in-bengaluru

[4] Qualcomm is demonstrating low-band capacity gains and infrastructure reuse in the upper-mid band. 1.8.2026. https://www.rcrwireless.com/20250401/6g/6g-systems-qualcomm

[5] Silicon chip propels 6G communications forward. 29.2024. https://www.sciencedaily.com/releases/2024/08/240829184328.htm

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

Alkuperäisen artikkelin kirjoittaja: Olavi Larkas

YLEISRADIO POIKKEUKSELLISTEN OLOJEN PALVELUKSESSA

Yleisradion palvelukset eivät suinkaan rajoitu yksinomaan jokapäiväiseen viihde-, dokumentti- tai opetusohjelmien ja uutisten välittämiseen, vaan se pyrkii toiminnassaan ottamaan huomioon myös kaiken kattavan tiedotustoiminnan, joka palvelee suurta yleisöä. Rajan veto normaaliolojen ja poikkeuksellisten olojen välillä on vaikea määritellä. Olosuhteet luovat varsin erilaisia käyttömuotoja, jotka on etukäteen suunniteltava.

Käyttö normaaliaikojen pelastustoimintaan

Pelastuspalvelua suorittavat viranomaiset voivat pyytää Yleisradiota välittämään lähetystensä yhteydessä kiireellisiä yleisölle, pelastuspalvelun suorittajalle tai etsittäville henkilöille tarkoitettuja tiedotuksia.

Viranomaisten tiedotukset voidaan lukea joko ohjelman välitiedotuksena radion ja/tai television valtakunnallisessa verkossa tai radiossa vain tietyllä alueella säännöllisten alueohjelmien yhteydessä tai erityistapauksissa erottamalla Yleisradion alueverkko tai lähetinasema näitä varten valtakunnallisesta verkosta.

Oikeus tiedotteen antamiseen Yleisradion välitettäväksi on pelastustoimintaa johtavalla viranomaisella.

Yleistä pelastuspalvelua koskevat tiedotukset voidaan antaa läänien pääkaupunkien palo- ja poliisilaitosten, lentopelastuspalvelua koskevat tiedotukset lentopelastuskeskusten ja meripelastuspalvelua koskevat tiedotukset meripelastuskeskusten välityksellä.

Onnettomuustapauksen tai pelastustoiminnan vakavuudesta ja laajuudesta riippuen ja viranomaisen pyydettyä virka-apua on ohjelma-alueen päälliköllä oikeus määrätyissä olosuhteissa ryhtyä toimenpiteisiin alueellisen ohjelman lähettämiseen ohjelma-alueeseensa kuuluvien tai kuuluvan lähetinaseman kautta.

Viranomaisten tiedotuksia voidaan antaa radiossa ja televisiossa luettavaksi hätätilanteissa, joissa ihmishenki on välittömässä ja ilmeisessä vaarassa tai on vaarana menettää huomattavan suuria omaisuusarvoja ja jolloin tiedotuksen avulla on ilmeisesti mahdollista edistää ihmishengen tai omaisuuden pelastamista tai muutoin huomattavasti edistää pelastustoimien suorittamista.

Yleisölle suunnattujen määräysten ja ohjeiden tarkoituksena voi olla esimerkiksi vaaranalaisen alueen tyhjentäminen, suojautumisohjeiden antaminen, liikenteen ohjaaminen ohi vaarakohteen ja sieltä pois, taikka onnettomuudesta tiedottaminen ja siinä yhteydessä tapahtuva väestön rauhoittaminen ja järjestyksen tukeminen.

Käyttö poikkeuksellisten olojen toimintoihin

Tehtävä ja vastuu.

Mitkään säännökset eivät aseta Yleisradion ohjelmatoiminnalle erityisiä velvoitteita poikkeuksellisten olojen varalta. Vain väestönsuojelulain 5 §:ssä mainitaan, että julkisten yhteisöjen asiana on kohdaltaan ryhtyä sellaisiin erityisiin suojelutoimenpiteisiin, jotka ovat tarpeen muun toiminnan turvaamiseksi. Puolustusneuvosto on kuitenkin katsonut tarpeelliseksi suosittaa Yleisradion tehtäväksi muun kuin suojelutoiminnan osalta seuraavaa:

Jatkaa toimintaansa normaaliaikoihin nähden mahdollisimman vähäisin muutoksin. Itsenäisen ohjelmatoiminnan ohella Yleisradion tulisi valmistautua palvelemaan eri viranomaisten tarpeita – tiedostusvälineenä siten, että valtakunnallinen tiedotusorganisaatio voi antaa sen avulla kaikille kansalaisille ajankohtaisen ja oikean kuvan vallitsevasta tilanteesta ja sen velvoituksista sekä valtiojohdon ratkaisuista ja niiden tavoitteista – koulutus- ja valistusvälineenä siten, että eri viranomaiset voivat sen kautta jakaa kaikille kansalaisille poikkeuksellisten olojen aikana välttämättömiä tietoja ja ohjeita, sekä – erikoisohjelmia puolustusvoimille ja ulkomaille välittävänä laitoksena.

Yleisradion tulee myös tukea valtakunnallisen ilmapuolustusjärjestelmän ja väestönsuojelun edellyttämää varoitus-, hälytys ja selostustoimintaa.

Toiminnan jatkuvuuden turvaaminen

Johtuen Yleisradion ilmapuolustuksen ja väestönsuojelun tukitehtävistä tulee Yleisradion radio-ohjelmalähetys olemaan ympärivuorokautista. Samoin mahdollisia poikkeuksia lukuunottamatta lähetetään vain yhtä valtakunnallista ohjelmaa kaikissa verkoissa. TV jatkaa toimintaansa niin kauan kuin se on teknisesti mahdollista. Alueellista ohjelmatoimintaa silmällä pitäen maa on jaettu yhdeksään ohjelma-alueeseen. Tuotantoyksikköjen osalta voidaan ohjelmatuotanto turvata Helsingistä käsin melko kriittiseen pisteeseen saakka myös radioaktiivinen laskeuma huomioon ottaen. Mm uutis- ja ajankohtaistoimintaa varten ovat tilat olemassa kalliosuojassa. Suojatusta pientuotantoyksiköstä ovat lähetykset mahdollisia myös Tampereella.

Yleisradion linkkiverkko ulottuu tällä hetkellä Helsingistä Yllästunturille, mutta tultanee lähivuosina jatkamaan Kemijärven Pyhätunturin kautta aina Inariin saakka. Verkko on Ouluun saakka rakennettu kahta tietä ja on näiden välit yhdistetty Jyväskylä korkeudella ja Oulu – Puokiovaara tasolla.

Kaikki lähetinasemat ovat yleensä varustettu käyttöhenkilöstöä varten rakennetuilla työpaikkasuojilla. Ula-lähettimet ja linkit on sijoitettu lähetinasemilla S-1 luokkaa vastaavaan laitesuojaan.

Milloin erityisesti määrätään, voidaan ilmapuolustuksen ja väestönsuojelun tiedotukset antaa suoraan lähetinasemien kautta määräalueille. Tämä säädellään vielä erityisen releistön välityksellä etuoikeusluokkiin. Erityisen tärkeätä on, että vastaanottopäässä ja erityisesti väestönsuojien antennit on huolellisesti rakennettu, koska lähetinaseman sattuessa radioaktiivisen laskeuman saastealueelle joudutaan aseman tehoa laskemaan.

Palvellakseen kansalaisia eräänä merkittävänä valtakunnallisena tiedotusvälineenä tulee Yleisradion ottaa huomioon myös kaikkinaiset toiminnan jatkuvuuteen vaikuttavat turvallisuusnäkökohdat. Valitettavasti yhtiö joutuu itse rahoittamaan kuuntelijoiltaan keräämillään varoilla tämän toiminnan ilman, että valtio tukisi sitä edes osalta. Siis päinvastoin kuin esimerkiksi Norjassa (valtion tuki 1,5 milj N kr/v), mistä johtuu, että valmistelut turvallisuuden lisäämiseksi ovat toista luokkaa kuin meillä.

Viestimies 50 vuotta sitten palstan kirjoittaja: Pasi Puhakka

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