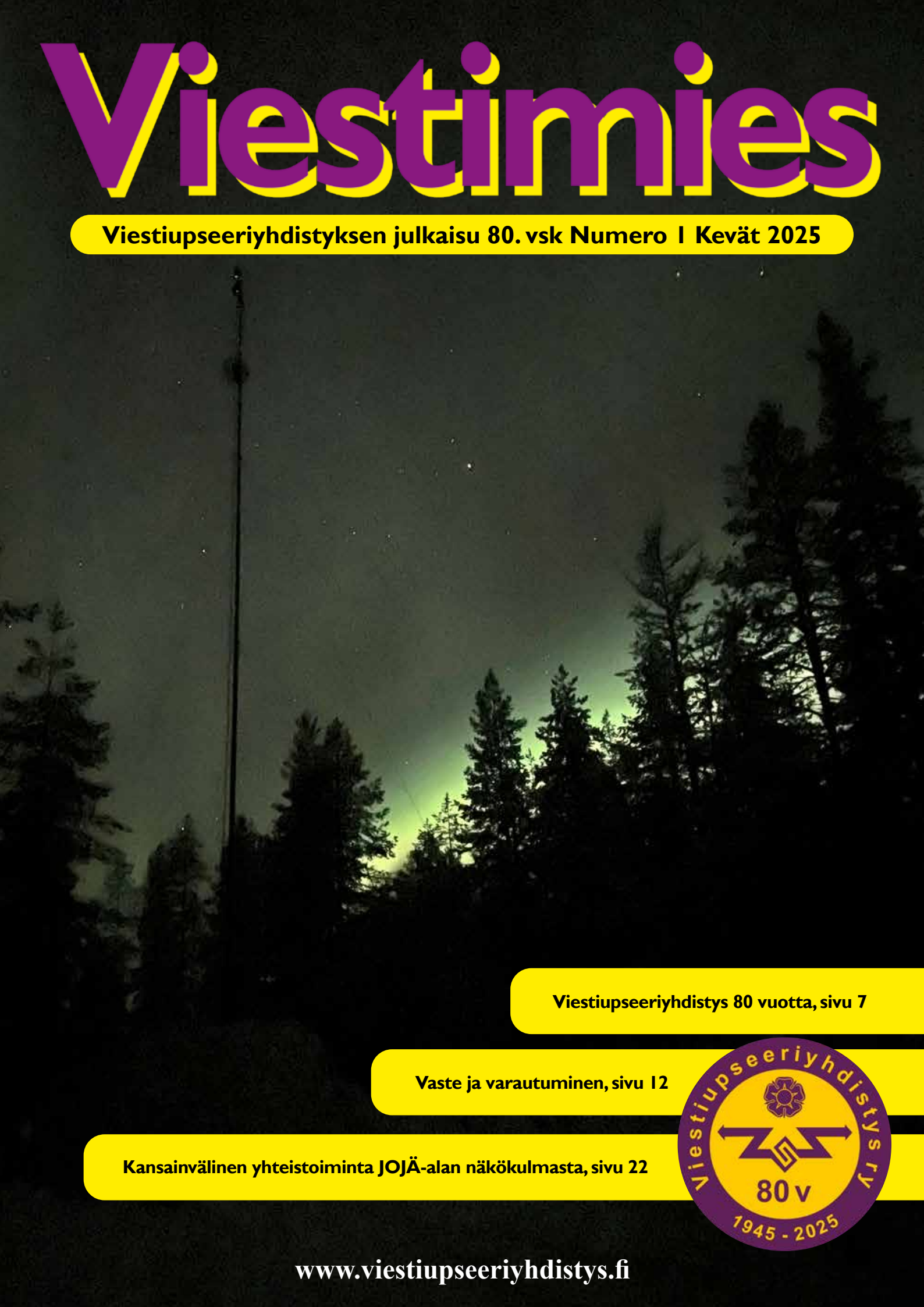
Viestimies

Viestiupseeriyhdistyksen julkaisu 80. vsk Numero 1 Kevät 2025



Viestiupseeriyhdistys ry 80 v 1945 - 2025

www.viestiupseeriyhdistys.fi

COMBITECH

Kovaa softaa

Nopeampaa päätöksentekoa
suorituskykyisillä ohjelmistoilla.

Combitech Finland

www.combitech.fi

Viestimies-lehti

Päätoimittaja
Kimmo Kaipainen
p 040 7222646
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
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. Viestiasema revontulien äärellä Lapin erämaassa. (Kuvaaja Tiia Impiö)

Tässä numerossa

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

Mukana lehdessä
–
Mukana päätöksiä tehdessä!

Seuraavan numeron aineistopäivä on 25.4.2025. Lehti ilmestyy viikolla 22.

Vaste ja Varautuminen

Valtioneuvoston hyväksyi 19.12.2024 uuden puolustusselonteon antamisen eduskunnalle. Kyseinen selonteko on Nato-ajan ensimmäinen ja sen linjauksilla rakennetaan Suomen Nato-jäsenyyden tulevia askeleita vuosiksi eteenpäin. Edellinen puolustusselonteko julkaistiin 2021, siis ennen Venäjän laajamittaisen hyökkäyksen alkua, joten tarkennuksille oli tilausta.

Selonteossa todetaan läntisten asevoimien, siis myös Suomen, kehittämistä ohjaavan ajattelutapa, jossa huomioidaan kaikki toimintaympäristöt. Tähän liittyy myös liittokunnan yhteistä lähestymistapaa kuvaava Multi Domain Operations, MDO-malli. MDO-mallin operatiiviset toimintaympäristöt ovat maa, ilma, meri, kyber ja avaruus. Lisäksi informaatiopuolustusta toteutetaan kaikissa toimintaympäristöissä. Toiminnalla tavoitellaan haluttuja yhteisvaikutuksia fyysisessä, virtuaalisessa sekä kognitiivisessa ulottuvuudessa.

Viestimiehen silmin selontekoa lainatessa ”*MDO-toimintamallissa korostuvat digitaalinen ja nopea tiedonkulku sekä datakeskeisyys, jotta kyetään johtamaan ja tekemään päätöksiä vastustajaa nopeammin. Tämä edellyttää kykyä ja toiminnanvapautta sähkömagneettisessa spektrissä.*” Tässä riittää tavoiteltavaa ja toimeenpantavaa jokaiselle asian parissa työskentelevälle.

Selonteossa todetaan myös, että ”*Kansallinen puolustuskyky muodostuu sotilaallisesta puolustusjärjestelmästä ja kokonaismaanpuolustuksen tuesta sille*.” Kokonaismaanpuolustus on osa kokonaisturvallisuuden laajempaa kokonaisuutta. Kokonaisturvallisuuden toimintamallia määrittävä uusi Yhteiskunnan turvallisuusstrategia julkaistiin Valtioneuvoston periaatepäätöksenä 16.1.2025. Strategiassa turvallisuuden tekeminen on uudella tavalla hahmotettu vasteen ja varautumisen kautta. Tässä numerossa saamme näkökulmaa kumpaankin. Eero Havu ja Anni Hakaniemi käsittelevät erinomaisen ajankohtaisessa artikkelissaan strategiassa määriteltyä vastetta, jonka *päämääränä on minimoida toteutuneiden uhkien vaikutuksia, edistää yhteiskunnan elintärkeiden toimintojen toipumista ja antaa perusteita varautumiselle*.

Varautumisen päämääränä puolestaan on pienentää uhkien toteutumisen todennäköisyyttä, edistää omaa valmiutta kohdata niitä ja luoda edellytykset vasteelle. Varautuminen on siis suorituskykyjen ja osaamisen rakentamista tarpeen varalle. Varautuminen ei tapahdu itsestään, siitä tehdään todellisuutta määrätietoisella työllä ja harjoittelulla. Varautuminen on puolustushallinnolle arkipäivää, mutta muun yhteiskunnan osalta taso on vaihtelevaa. Harjoitteluun tarvitaan yhteisiä harjoitusalustoja. Erinomaisena esimerkkinä tällaisesta alustasta toimii Tieto-harjoitus, jonka vuoden 2024 toimeenpanon toteumasta saamme erinomaisen näkymän Antti Nyqvistin artikkelissa.

Puolustusvoimat ottaa jatkuvasti askeleita digitalisaation tiellä. Kesällä 2024 niin tehtiin myös asevelvollisten asioinnin suhteen. *OmaIntti* on palvelu, joka kokoaa Puolustusvoimien verkkosisällöt ja asiointipalvelut yhteen käyttöliittymään. Palvelun kirjautujalle näyttämät palvelut on räätälöity kunkin asevelvollisen tilanteen mukaisesti. 4.6.2024 OmaIntissä julkaistu ”Omat tiedot” -osio mahdollistaa omien tietojen, kuten sodanajan sijoituksen tilan ja ylennysten tarkastelun. Reserviläiset voivat myös päivittää tietojaan Puolustusvoimille palvelun kautta ja varmistaa tietojensa ajantasaisuuden. OmaIntin kehitys jatkuu myös tulevaisuudessa. Tähän saakka tehty kehitystyö sai tunnustusta, kun ItSMF Finland ry palkitsi Puolustusvoimat ja OmaIntti -palvelun vuoden 2024 palvelujohtamisen tekona. Lämpimät onnittelut asian parissa töitä tehneille! Muista sinäkin päivittää tietosi, jotta myös maanpuolustuksen tehtävissä voidaan huomioida esimerkiksi koulutuksesi. OmaIntti -palvelun löydät osoitteesta https://omaintti.fi/

Viestiupseeriyhdistys juhlii kuluvana vuonna 80-vuotisjuhliaan. Yhdistyksen juhlavuosi tulee näyttäytymään eri tavoin myös Viestimies-lehden sivuilla. Juhlavuoteen liittyvien artikkeleiden lisäksi lehdissä tullaan vuoden teemojen mukaisesti näkemään artikkeleita ainakin Natoon sekä aselajin ja toimialan operointiin että koulutukseen liittyen. Edellä mainittujen ajankohtaisten ja mielenkiintoisten teemojen lisäksi käsitellään tuttuun tapaan myös teknologian uusia kehitystuulia.

Tervetuloa Viestimies-lehden 80. vuosikerran pariin!

Kimmo Kaipainen

Päätoimittaja

Viestiupseeriyhdistys 80 vuotta

Toivotan kaikille yhdistyksen jäsenille ja muille lehden lukijoille mitä parhainta alkanutta vuotta 2025! Toivotaan, että tämä vuosi kääntäisi globaalin turvallisuustilanteen kehityksen vihdoin parempaan suuntaan. Venäjän hyökkäyssodan alettua helmikuussa 2022 olemme valitettavasti joutuneet todistamaan huolestuttavaa globaalia turvallisuustilanteen kehitystä ja siihen sisältyvänä myös uusia hybridisodankäynnin toimintamuotoja.

Uskon, että me viestimiehet olemme tarkasti seuranneet erityisesti Itämerellä aiheutettuja tietoliikennekaapelivaurioita ja niiden tutkintaa. Viimeisimmän tapahtuman, öljytankkeri Eagle S:n sujuvasti käynnistynyt tutkinta ja kansainvälinen yhteistyö ovat onneksi lähettäneet positiivisen viestin joka suuntaan – päättäväisellä toiminnalla nämä tapahtumat ovat estettävissä, aiheuttajat saatavissa kiinni ja korvausvastuuseen. Kymmenen pistettä suomalaisille viranomaisille ja heidän saumattomalle yhteistyölleen, jonka piirissä toki ovat olleet myös liittolaisemme etelästä ja lännestä.

Huolestuttavien maailmantuulien puhaltaessa meillä on tänä vuonna myös merkittävä juhlinnan aihe. Viestiupseeriyhdistyksen perustamisesta tulee 23.9.2025 kuluneeksi tasan 80 vuotta. Tämä on luonnollisesti merkkipaalu, jota aivan olan kohautuksella ei voi ohittaa emmekä näin tietenkään aiokaan tehdä. Yhdistyksemme historia ja sen toiminta ansaitsevat saada tänä juhlavuonna normaalia enemmän näkyvyyttä ja juhlavuutta. Näin sen itse, nuorempien sukupolvien edustajana, vahvasti koen.

Merkkipäivävuoden teemalla yhdistys järjestää juhlaseminaarin toukokuun 6. päivänä. Tästä on toisaalla lehdessä sekä myös verkkosivuillamme erilliset ilmoitukset. Olen erittäin iloinen siitä, että niin monet oman alansa korkeatasoiset asiantuntijat ovat ilmaisseet käytettävyytensä tulla puhumaan seminaariimme ja näin jakamaan kuulijoille ajantasaista tietoa turvallisuusympäristöstämme, johtamisjärjestelmäalan kansallisista ja kansainvälisistä järjestelyistä sekä tietenkin myös teknologiakehityksen vaikutuksesta tulevaisuuden toimintamalleihimme. Seminaarissa saamme kuulla myös mielenkiintoisen paneelikeskustelun Itämeren kaapelivaurioista, niiden tutkinnasta sekä saaduista opeista. Toivon, että tilaisuus mahtuisi teistä mahdollisimman monen kalenteriin.

Toinen juhlavuoden merkkitapahtuma tulee olemaan Helsingissä järjestettävä pääjuhla. Tämä kutsuvierastilaisuus järjestetään 24. syyskuuta ja yhtenä tavoitteena tilaisuudella on juhlimisen ohessa jakaa puolustusvoimien, muun hallinnon sekä yrityselämän johdolle tietoa yhdistyksestämme. Myös tämän vuoden palkitsemiset pyritään mahdollisuuksien mukaan keskittämään tähän tilaisuuteen ja siten osaltaan lisäämään tapahtuman juhlavuutta.

Kolmas merkittävä juhlavuoden ponnistus on Viestiupseeriyhdistyksen historiikin toisen, päivitetyn painoksen valmistelu. Edellinen, ensimmäinen painos julkaistiin vuonna 2005 yhdistyksen 60-vuotisjuhlavuonna. Eversti evp Seppo Uron kirjoittama Yhteyksien hyväksi -historiikki on tänäkin päivänä hyödyllistä luettavaa yhdistyksen eri vaiheista ja toimintamuodoista kiinnostuneille. Uuteen päivitettyyn painokseen lisätään kahden edellisen vuosikymmenen tapahtumia ja samalla tarkistetaan edellisen painoksen tekstiä. Uusi painos on tarkoitus julkaista pääjuhlan yhteydessä syyskuussa. Jo tässä vaiheessa lämpimät kiitokset toiminnanjohtajan johdolla ahertavalle kirjoittajaryhmälle.

Juhlavuosi tulee monin tavoin näkymään myös Viestimies-lehden sivuilla. Juhlaseminaari, pääjuhla ja päivitettävä historiikki tulevat tarjoamaan runsaasti jutunaiheita. Pidän tärkeänä, että lehtemme tällä tavoin jatkaa hienoa perinnettään yhdistyksemme tapahtumien dokumentoijana. Omasta kokemuksesta tiedän, että Viestimies-lehdistä kootut nidotut nelivuosikertapainokset ovat monelle tutkimustyön tekijälle tai kirjoittajalle korvaamattomia lähteitä. Lehtemme rooli taltioida yhdistyksemme ja koko toimialamme kehityksen kehityspolkuja on erittäin tärkeä.

Juhlinnan ohella myös yhdistyksemme normaali toiminta toki jatkuu. Kevätkokous järjestetään tänä vuonna Elisa Oyj:n isännöimänä 24.4.2025. Esityslistalla on edellisen vuoden tilinpäätöksen hyväksyminen sekä sen ohessa luonnollisesti tutustuminen isäntämme, Elisan, toimintaan. Syyskokouksen vuoro on jälleen syyskuussa, yhteistyössä A. R. Saarmaa -seminaarin järjestäjien kanssa. Seuratkaa siis lehtemme ja verkkosivujen ilmoittelua ja tulkaa mukaan, toivottavasti pääsen näissä tapahtumissa tapaamaan teistä mahdollisimman monia.

Pertti Hyvärinen

Puheenjohtaja

Eversti evp.

Viestiupseeriyhdistyksen seminaari 6.5.2025

Viestiupseeriyhdistys – yhdessä turvallisuutta 80 vuotta

Viestiupseeriyhdistyksen perustamisesta tulee tänä vuonna kuluneeksi **80 vuotta**. Osana juhlavuoden tapahtumia Viestiupseeriyhdistys järjestää juhlaseminaarin **Helsingin yliopiston päärakennuksessa** (Fabianinkatu 33) **tiistaina 6.5.2025.**

Ohjelma

8.30	Ilmoittautuminen ja kahvit
9.00	Avaussanat - puheenjohtaja Pertti Hyvärinen, Viestiupseeriyhdistys ry
9.10 – 9.30	Puolustushallinnon tervehdys - strategiapäällikkö, kenraalimajuri Sami Nurmi, Pääesikunta
9.30 – 10.00	Venäjän tavoitteet ja toiminta turvallisuuspoliittisen ympäristön muuttajana - johtava tutkija Sinikukka Saari, Ulkopoliittinen instituutti
10.00 – 10.30	Tietoturvan menneisyys ja tulevaisuus - tutkimusjohtaja Mikko Hyppönen, WithSecure Oyj
10.30 – 11.00	Naton johtamisjärjestelmätoiminta ja sen johtaminen - prikaatikenraali Jarkko Karsikas, Naton johtamis- ja tietojärjestelmäjohtoporras
11.00 – 11.30	Suomen puolustusvoimien johtamisjärjestelmä osana Nato-rakenteita - johtamisjärjestelmäpäällikkö, kenraalimajuri Jarmo Vähätiitto, Pääesikunta
11.30 – 12.30	LOUNAS

12.30 – 14.15	Case Itämeren kaapelivauriot - alustukset ja paneelikeskustelu Moderaattorina verkostojohtaja Jukka Savolainen, HybridCoE Panelistit: johtaja Taneli Vuorinen, Cinia Oy ylijohtaja Anssi Kärkkäinen, Kyberturvallisuuskeskus toimitusjohtaja Janne Känkänen, Huoltovarmuuskeskus työelämäprofessori Isto Mattila, Turun yliopisto
14.15 – 14.40	TAUKO
14.40 – 15.10	Tekoälyn tulevaisuus - professori Laura Ruotsalainen, Helsingin yliopisto
15.10 – 15.40	Tulevaisuuden energiaratkaisut - toimitusjohtaja Olli Sirkka, Helen Oy
15.40 – 16.10	Kyberturvallisuuden strateginen kehittäminen - kyberturvallisuusjohtaja Rauli Paananen, liikenne- ja viestintäministeriö
16.10 – 16.40	Avaruus osana kokonaisturvallisuutta - professori Minna Palmroth, Helsingin yliopisto
16.40 – 17.00	Loppuyhteenveto
17.00 – 18.30	Verkostoituminen

Seminaarin puheenjohtajana toimii Eero Valkola, eversti (evp.), MilDef Oy.

Seminaarin osallistumismaksut ovat 350 € (yritysten edustajat), 270 € (julkisen hallinnon ja järjestöjen edustajat) sekä 150 € (yksityishenkilöt ja eläkeläiset, jäsenalennus -50 %). Viestiupseeriyhdistys laskuttaa seminaarimaksun huhti-toukokuun 2025 vaihteessa.

Sitovat ilmoittautumiset pyydetään tekemään **22.4.2025 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.

TEKSTI: PERTTI HYVÄRINEN

Viestiupseeriyhdistys – maanpuolustustyötä 80 vuotta

Kuluvana vuonna vietämme Viestiupseeriyhdistyksen 80-vuotisjuhlaa. Sen vuoksi on paikallaan luoda katsaus menneisiin vuosiin, yhdistyksen toiminnan virstanpylväisiin ja toiminnan keskeiseen sisältöön. Vuodesta 1983 alkaen olen itse toiminut yhdistyksessä niin rivijäsenenä, Viestimies-lehden päätoimittajana, hallituksen jäsenenä ja nyt parhaillaan puheenjohtajana. Kirjoituksessa painottuvat siten myös henkilökohtaiset kokemukseni.

Yhdistyksen perustaminen

Viesti, puolustusvoimien yksi aselaji, oli jo viime sotien aikana joukko, jossa henkilöstö pitkälle tunsi toisensa. Haastavissa sodan olosuhteissa tässä joukossa kehittyi luja asevelihenki ja yhteenkuuluvaisuuden tunne. Sellainen, että asevelijiin haluttiin pitää yhteyttä myös rauhan tultua voimaan. Tämä yhteenkuuluvaisuuden tunne konkretisoitui Riihimäen varuskunnassa 23.9.1945, jolloin järjestettiin Viestiupseerikerhon perustava kokous.

Viestiupseerikerho aloitti toimintansa tukeutuen vahvasti Riihimäen varuskunnan upseerikerhoon. Koska kyseisenä aikana punaisen Valpon silmissä erilaisten puolustusvoimataustaisten järjestöjen toiminta nähtiin ongelmallisena, jopa kiellettynä, voitaneen kahden kerhon välistä yhdistettyä toimintamallia pitää onnistuneena – saatiin olla rauhassa. Vuodesta 1952 näiden kahden kerhon toiminta eriytettiin ja vuonna 1955 Viestiupseerikerho muutti nimensä Viestiupseeriyhdistys ry:ksi, kerhon jatkaessa toimintaa paikallisella tasolla.

Yhdistyksen ensimmäisissä säännöissä määritettiin toiminnan päämäärä ja muodot, eivätkä ne perusolemukseltaan ole sen jälkeen muuttuneet vaikkakin toki ajantasaistamista on tehty muutamia kertoja. Keskeistä säännöissä oli, ja on edelleen, että tavoitellaan yhteenkuuluvaisuuden ja asevelihengen vahvistamista, tarjotaan jäsenille mahdollisuus mieluisaan ja hyödylliseen yhdessäoloon, järjestetään ammattitaitoa kohottavaa toimintaa, vaalitaan aselajin perinteitä sekä edistetään säätiöiden kautta aselajin kehitystä.

Viestiupseerikerhon perustavan kokouksen osanottajia Riihimäen varuskunnassa 23.9.1945 (Kuva VM 4/1965)

Alusta alkaen yhdistyksen asioita on hoitanut hallitus puheenjohtajansa johtamana. Hallituksen neuvoa-antavaksi elimeksi perustettiin vuoden 1955 säännöissä valtuuskunta. Yhdistyksen alkuvuosikymmeninä valtuuskunnalla oli tärkeä rooli muun muassa yhteydenpidossa puolustusvoimien ja teleteollisuuden johtoon. Lähestyttäessä vuosituhannen vaihetta valtuuskunnan rooli kuitenkin vähitellen pieneni ja se lakkautettiin vuonna 2001. Viimeinen valtuuskunta sekä kunniajäsenet kutsuttiin viimeisen kerran koolle jouluillalliselle Katajanokan upseerikerholle 18.12.2001. Sain itse olla mukana, tunnelma oli nostalginen ja haikeakin, mutta en tunnista etteikö tehtyä lakkautuspäätöstä laajalti myös ymmärretty. Silloin puheenjohtajamme Asko Inkilä hoiti tämän tilanteen tyylikkäästi.

Jäsenkunta

Leimaa-antavin piirre Viestiupseeriyhdistyksen jäsenkunnassa on aina ollut se, että jäsenistö on suhteellisen tasapainoisesti edustanut sekä puolustusvoimien että alan teollisuuden osaajia. Jäseninä on sekä työssä käyviä että jo työelämästä vetäytyneitä. Toki aivan aluksi, sotien jälkeen, jäsenistön rakenteessa korostuivat silloisen puolustuslaitoksen ja rajavartiolaitoksen palveluksessa olleet. Vuoden 1947 sääntötarkistuksen jälkeen jäseniksi voitiin hyväksyä myös evp-henkilöitä sekä ei-sotilastaustaisia.

Nykyisissä säännöissä jäsenyyden kelpoisuusehdot määritetään seuraavasti: ”Yhdistyksen varsinaiseksi jäseneksi voidaan hyväksyä toimialan tehtävissä toimiva tai toiminut, tai muutoin toimialan toiminnasta kiinnostunut henkilö ja yhteisö.” Henkilöjäsenyyden lisäksi muita jäsenyysmuotoja ovat kannattajajäsenet, kunniajäsenet ja kunniapuheenjohtajat. Yhdistyksen jäsenet hyväksyy hakemuksesta hallitus. Kunniajäsenet ja kunniapuheenjohtajat hyväksyy yhdistyksen kokous hallituksen tekemästä esityksestä.

Vuodesta 1978 alkaen Viestiupseeriyhdistyksellä on ollut myös jäsenenä silloisen Posti- ja lennätinlaitoksen henkilöstöstä muodostettu kerho. Tämä oli luontainen kehitysaskel, sillä muodostettiinhan jatkosodanaikainen Viestipataljoona 10 nimenomaan silloisen Posti- ja lennätinlaitoksen henkilöstöstä ylläpitämään valtakunnallista puhelinverkkoa.

Ajan saatossa nimi on muuttunut Telian kerhoksi ja jäseniä kerhossa on vajaa kaksi sataa. Kerho on ansioitunut muun muassa vapaaehtoisten harjoitusten järjestämisessä.

Tällä hetkellä Viestiupseeriyhdistyksessä on noin tuhat henkilöjäsentä. Puheenjohtajana on ollut mieluisaa havaita, että eronneiden tilalle yhdistys saa jatkuvasti uutta jäsenistöä nuoremmasta päästä. Toimivan jäsenrakenteen eteen yhdistyksen hallitus tekee kuitenkin jatkuvasti työtä, jakaen tietoa toiminnastamme erityisesti Reserviupseerikoulun viestilinjalta sekä Kadettikoulun johtamisjärjestelmälinjalta valmistuville, osallistuen erilaisiin tilaisuuksiin sekä seminaarien kautta.

Opinto- ja jäsenmatkat

Jäsentensä ”teknillisten tietojen lisäämiseksi” yhdistys aloitti vuonna 1969 opintomatkojen järjestämisen ulkomaille. Ensimmäinen matka suuntautui Ruotsiin, jossa tutustumiskohteina olivat teleteollisuuden ja -operaattoreiden kohteet. Tuohon aikaan erityisesti valtion viroissa palvelevilla oli rajalliset mahdollisuudet ammatilliseen matkustamiseen, mikä on varmasti lisännyt yhdistyksen tarjoamien tutustumismatkojen tarvetta ja kysyntää. Tänä päivänähän tilanne lienee aivan toinen.

Ulkomaisia opintomatkoja tehtiin Ruotsin vierailun jälkeen runsaasti, seuraavina vuosina olivat vuorossa matkat Saksan liittotasavaltaan (1970), Ranskaan, Saksaan ja Hollantiin (1972), Berliiniin (1974), Sveitsiin (1976) ja Iso-Britanniaan (1978). Myöhemmin matkojen sisältöön ovat tulleet mukaan myös erilaiset sotahistorialliset ja turistiluonteiset kohteet, mitkä toki ovat hyvin ansainneet paikkansa.

Osallistuin vaimoni kanssa yhdelle jäsenmatkalle vuonna 2003 Liettuaan ja voin todeta, että jo vuoden 1945 säännöissä mainittu toiminnan päämäärä ”antaa jäsenille tilaisuus mieluisaan ja hyödylliseen ajan viettoon sekä keskinäiseen kanssakäymiseen” toteutui täydellisesti. Kiitokset silloiselle puheenjohtajalle Pertti Ruotsalaiselle ja hallituksen jäsenelle Pirkko Kinnuselle loistavista matkajärjestelyistä.

Seminaarit

Viestiupseeriyhdistyksen ohjelmassa on vuosikymmeniä ollut, ja on edelleen, keskeisellä sijalla korkeatasoisten yhdistyksen toimialan varautumiseen ja kehityksen tarkasteluun liittyvien seminaarien järjestäminen. Ensimmäinen

Yhdistyksen toisella matkalla Sveitsiin laskettiin kukkalaite marsalkka Mannerheimin haudalle Montreax'ssa. Kuvassa rouva Tyyne Karkaus (vas.), eversti Heikki Nurmi, everstiluutnantti Arthur Grüninger, insinöörikenraalimajuri Pentti Myyryläinen ja eversti Kalevi Markkula (Kuva S Uro)

seminaari järjestettiin Heimarissa maaliskuussa 1973. Tilaisuuteen oli kutsuttu 36 johto- ja suunnittelutehtävissä toimivaa henkilöä puhelinlaitoksista ja puolustusvoimista. Teemana seminaarissa oli tuolloin ajankohtainen aihe, automaattipuhelintekniikan sovellutusmahdollisuudet liikkuvassa johtamistoiminnassa. Tietotekniikan ja -turvallisuuden eri osa-alueiden valtava kehitysnopeus on taannut, että ajankohtaisista seminaariaiheista ei ole ollut pulaa, sanoisin että päinvastoin. Viestiupseeriyhdistyksen korkeaa arvostusta on osoittanut myös se, että seminaareihin on kerta toisensa perään saatu korvauksetta puhujiksi valtakunnan parhaita asiantuntijoita.

Yhdistyksen viides seminaari järjestettiin ensimmäistä kertaa laivaseminaarina 26.–27.11.1987, mikä malli on ollut käytössä tähän päivään saakka – pois luettuna koronavuodet. Seminaarin perusrakenteeksi on muotoutunut malli, jossa aloitus on maissa erikseen sovitun yrityksen tai viraston isännöimänä ja sen jälkeen illaksi siirrytään laivalle. Toisen seminaaripäivän esitelmät pidetään laivan konferenssitiloissa. Tämä malli on osoittautunut erittäin toimivaksi mahdollistaen melkoisen määrän asiantuntijapuheenvuoroja sekä myös – vanhoja yhdistyksen sääntöjä kunnioittaen – tilaisuuden mieluisaan ja hyödylliseen ajan viettoon.

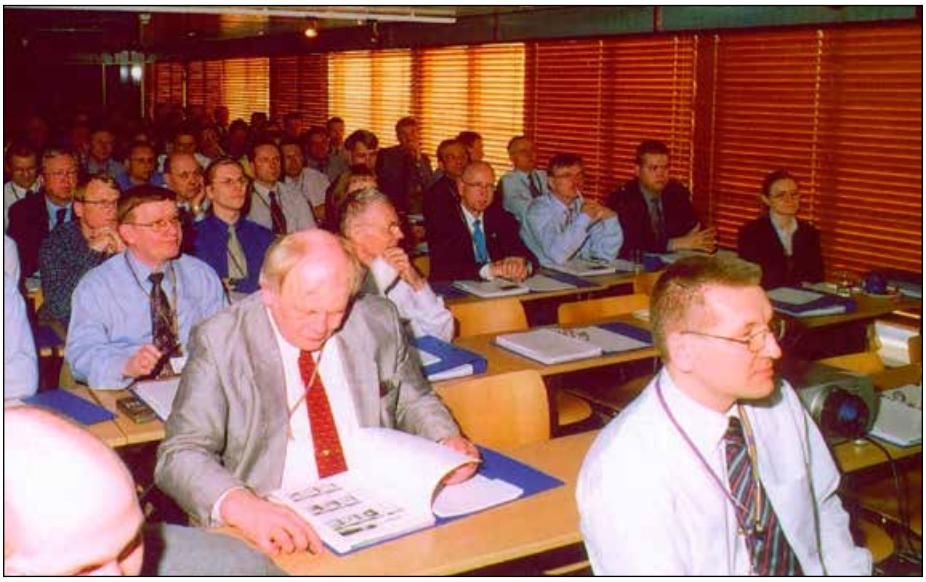
Viimeisin seminaari järjestettiin helmikuussa 2024 Digia Oyj:n isännöidessä tilaisuuden maaosuutta. Osallistujia oli mukana noin 80. Esitelmissä käsiteltiin tämän päivän ajankohtaisia aiheita, kuten Nato-jäsenyyden vaikutuksia puolustusvoimien johtamisjärjestelmätoimintaan, tekoälyn käytön lisääntymiseen liittyviä tietoturvahaasteita, satelliittiteknologian tulevaisuuden näkymiä sekä droonien käytöstä saatuja oppeja Ukrainan sodassa.

Julkaisutoiminta

Viestiupseeriyhdistyksen ulospäin näkyvin toimintamuoto on oman jäsenlehden, Viestimiehen, julkaiseminen. Lehden tarve oli todettu jo yhdistyksen perustamisvuonna ja ensimmäinen numero julkaistiinkin 13-sivuisena monisteena heti seuraavana vuonna eli kesällä 1946. Sen jälkeen lehti on ilmestynyt painettuna neljä kertaa vuodessa. Lehden ulkoasua on modernisoitu useita kertoja sisällön pysyessä koko ajan korkeatasoisena. Useiden viime vuosien ajan lehti on ollut luettavissa myös verkosta yhdistyksen sivuilta.

Viestimies-lehden toimittamisesta vastaa päätoimittaja apunaan toimitussihteeri, henkilötoimittaja ja kirjanpitäjä. Toimituksen tukena on Pääesikunnan johtamisjärjestelmäpäällikön johdolla toimiva toimituskunta. Kunkin toimintavuoden neljään lehteen kirjoittaneista nimetään perinteisesti Vuoden kirjoittaja, joka palkitaan myös Maanpuolustuksen viestisäätiön stipendillä.

Lehden taloudellisten toimintaedellytysten mahdollistamiseksi lehden ilmoitusmyyjä hankkii kaupallisia ilmoituksia toimialan yrityksiltä. Vuosikymmenien aikana on ollut hienoa havaita, että yritykset näkevät tarpeellisena ja haluavat näkyä myös jäsenlehtemme sivuilla. Tulkitsen tämän myös vahvana maanpuo-



Vuoden 2004 seminaariin m/s Operalla osallistui lähes sata henkeä (Kuva K. Saarenheimo)

lustustahdon osoituksena, mistä kaikille ilmoittajille lämpimät kiitokset.

Tiedon jakamisen lisäksi lehdellä on myös toisena tärkeänä tehtävänä yhdistyksen toiminnan dokumentointi. Kokemuksestani tiedän, että Viestimies-lehdistä kootut nidotut nelivuosikertapainokset ovat monelle tutkimustyön tekijälle tai kirjoittajalle korvaamattomia lähteitä.

Merkittävänä saavutuksena yhdistyksen julkaisutoiminnassa on myös viestimiehen käsikirja ”Viestimies”. Sen ensimmäinen 3000 kappaleen painos julkaistiin vuonna 1955. Ensimmäisinä vuosikymmeninä kirjaa päivitettiin 2–3 vuoden välein. Kalustekohtaisen sekä viestitaktisen ohjesäännöstön puuttuessa se muotoutuikin keskeiseksi käsikirjaksi niin kouluttajille, varusmiehille kuin reserviläisillekin.

Viestimies-kirja on ollut Viestiupseeriyhdistykselle menestystarina. Tuskin muiden aselajien vastaavaa käsikirjaa on toimitettu yhtäjaksoisesti yli 70 vuotta, 19 painosta ja yli 100 000 painettua kirjaa. Viimeisin painos on vuodelta 2011 ja sitä on edelleen saatavissa. Maanpuolustuskoulutuksessa käytettävän virallisen ohjesäännöstön kehittyessä ja sähköisten dokumenttien yleistyessä perinteinen painettu käsikirja on tullut jo käyttöikänsä päähän eikä uusien painosten tekeminen enää näytä todennäköiseltä. Näin ollen itse kunkin kirjahyllystä löytyvillä vanhemmilla painoksilla saattaa kohta olla myös museaalista arvoa.

Säätiöt viestitoiminnan tukena

Viestiaselajissa palvelleet eivät ole voineet välttyä kuulemasta aselajin ”grand old manin” jääkärieversti Arthur Reinhold Saarmaan nimeä. Hänen nimeään kantavan säätiön edeltäjä, stipendirahasto, perustettiin lahjana 50 vuotta täyttävälle Saarmaalle 23.9.1942. Rahaston peruspääomaksi oli lahjoituksin kerätty 20 000 silloista markkaa. Varsinainen säätiö aloitti toimintansa vuonna 1947 kun säädekirja virallistettiin. Säätiön hallituksena on alusta alkaen toiminut Viestiupseeriyhdistyksen hallitus sillä täydennyksellä, että säätiön hallituksen puheenjohtajana toimii puolustusvoimien (nykyisin maavoimien) viestitarkastaja Viestiupseeriyhdistyksen puheenjohtajan toimiessa varapuheenjohtajana.

Eversti A. R. Saarmaan säätiön tehtävänä oli muun muassa tukea toimialan opiskelijoita sekä viestialan julkaisu- ja tutkimustoimintaa. Säätiölle perustettiin vuonna 1955 4-tasoinen ansiolevykesarja jaettavaksi huomionosoituksina toimialan varusmiehille, reserviläisille, palkatulle henkilöstölle sekä myös toimintaa tukeneille organisaatioille.

Toinen viestitoimialan säätiö, Viestisäätiö, perustettiin vuonna 1950. Säätiöllä oli oma hallituksensa, jolla ei ollut kuitenkaan muodollista liittymäkohtaa Viestiupseeriyhdistykseen. Erona Saarmaan säätiön toimintaan oli, että erityisesti ensimmäisinä vuosikymmeninä Viestisäätiö myönsi stipendejä myös siviilialojen opiskelijoille ja tutkijoille.

Viestisäätiöllä ja Saarmaan säätiöllä oli toiminnassaan paljon päällekkäisyyksiä, minkä vuoksi ne huolellisen valmistelun jälkeen yhdistettiin vuonna 2004 uudeksi Maanpuolustuksen viestisäätiöksi. Tänä päivänä tämä säätiö hallinnoi noin 1,5 miljoonan euron varallisuutta ja jakaa siitä apurahoina ja stipendeinä vuosittain noin 50 000 euroa.

Yhdistyksen muu toiminta

Viestiupseeriyhdistyksen toiminta kuluneen 80 vuoden aikana on ollut erittäin monipuolista, mistä edellä kerrotut antavat toki keskeisen mutta eivät läheskään täydellisen kuvan. Toiminnasta voisi vielä nostaa esille:

Viestimiespäivät erilaisten maanpuolustuksellisten ja yritysvierailujen toteuttajana.

Muu julkaisutoiminta, muun muassa Viestijohtajan opas (1979–1980) ja Kyberajan viestitaktiikka (2018).

Omien internet-sivujen avaaminen (2000) sekä niiden ylläpito ja kehittäminen, mukaan luettuna Viestimies-lehden verkkoversiot.

Alueellisen yhdysmiesverkoston muodostaminen ja alueellinen toiminta.

Kansallinen ja kansainvälinen yhteistoiminta muiden maanpuolustusjärjestöjen kanssa.

Viestiupseeriyhdistyksen naistoimikunnan perustaminen (1980–2011), sekä

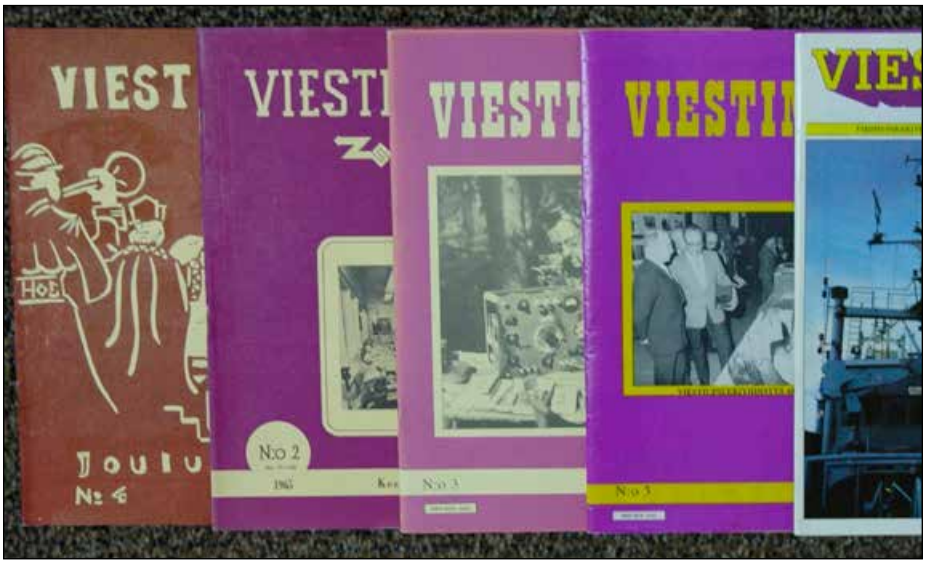
Yhdistyksen toiminta viestiperinteiden tallentajana ja ylläpitäjänä.

Yhdistyksen tulevaisuudennäkymät

Yhdistysten täytyy elää ajassa, toki perinteitään kunnioittaen. Perehtyessäni Viestiupseeriyhdistyksen toimintaan voin todeta, että juuri näin on toimittukin. Tämä muutoskyky on taannut yhdistyksen elinvoimaisuuden.

Viestiupseeriyhdistyksen kyvykkyys ajassa elämiseen tulee hyvin esille myös eri vuosikymmenillä järjestettyjen seminaarien teemoista sekä Viestimies-lehden artikkeleista. Tänä päivänä ajassa eläminen tarkoittaa paneutumista kyber- ja hybridiuhkien maailmaan, krypto- ja tekoälykehityksen seuraamista, älykkyyden dataverkkoratkaisujen kehittymisen seuraamista sekä muun muassa Nato-liittoutumisen seurannaisvaikutuksia suomalaisen viranomaiskentän johtamisjärjestelmiin.

Viestiupseeriyhdistyksen toiminnalle on edelleen vahva tilaus ja tarve erityisesti tässä ajassa, jolloin kiinnostus maanpuolustustoimintaa kohtaan on kasvanut. Yhdistyksen tulevaisuus näyttää vahvalta



Viestimies-lehden kansia eri vuosikymmeniltä.

Kuva 5. Jääkärieversti Arthur Reinhold Saarmaa (1892–1971) oli keskeinen aselajihengen luoja viestijoukoissa 1920-luvulta alkaen (SA-Kuva)

sen täyttäessä oman osuutensa suomalaisen kokonaismaanpuolustuksen kentässä.

Pertti Hyvärinen, eversti evp, toimii parhaillaan Viestiupseeriyhdistyksen puheenjohtajana. Hän valmistui kadettikurssi 68:n viestilinjalta vuonna 1984, suoritti yleisesikuntaupseeritutkinnon vuonna 1993 ja siirtyi täysin palvelleena reserviin vuoden 2011 lopussa. Urallaan hän palveli useissa sekä aselajin että operatiivisen alan tehtävissä eri joukko-osastoissa sekä puolustusministeriössä.

Kirjoittajan omien muistojen lisäksi on kirjoituksessa käytetty lähteinä Viestiupseeriyhdistyksen Yhteyksien hyväksi -historiikkia (toimittanut eversti evp Seppo Uro 2005) sekä majuri Jarmo Myyrän Viestiupseeriyhdistys ry 40 vuotta -artikkelia Viestimies-lehden numerossa 3/1985.

Eero Havu.

Anni Hakaniemi.

TEKSTI: EERO HAVU JA ANNI HAKANIEMI

Vaste ja varautuminen – uusia vaatimuksia sotilas- ja siviilitoimijoiden yhteistyölle

Uudistettu yhteiskunnan turvallisuusstrategia tunnustaa vasteen merkityksen kokonaisturvallisuudelle perinteisen varautumisen rinnalla. Vasteeseen liittyy siviili- ja sotilastoimijoiden ennakoivaa suunnittelua, harjoittelua, ja tilanteenmukaisia toimia, mikä asettaa vaatimuksia yhteisen tilanneymmärryksen, yhteistoiminnan ja johtamisjärjestelmien kehittämiseen. Resilienssiä, eli yhteiskunnan kriisinsietokykyä, kehitetään kokonaisvaltaisesti niin kansallisella tasolla kuin Naton ja Euroopan unioninkin piirissä. Turvallisuusympäristön muutoksissa vasteen merkitys resilienssin keskeisenä osatekijänä korostuu.

Suomenlahden merivartioston vartioima öljytankkeri Eagle S Svartbäckin sisäänkuripaikalla uudenvuodenaattona 2024. Kuva: Puolustusvoimat, kuvaaja Jarno Kovamaki.

Turvallisuusympäristön muutos asettaa vaatimustason koko yhteiskunnan varautumiseen

Joulupäivän Eagle S -tapaus havainnollisti, että vasteen muodostaminen kriittiseen infrastruktuuriin kohdistuviin uhkiin on ajankohtainen kysymys. Suomalainen viranomaisyhteistyö ja tapa puuttua haitalliseen toimintaan päättäväisesti saivat myös kansainvälistä näkyvyyttä ja arvostusta. Vasteen muodostamisessa hyödynnettiin useiden viranomaisten toimivaltuuksia, suorituskykyjä ja ennalta harjoiteltuja yhteistoimintamenetelmiä.

Viime aikoina on toistuvasti havahduttu kriittiseen infrastruktuuriin kohdistuviin monimuotoisiin uhkiin sekä erilaisiin vastuu- ja toimivaltakysymyksiin näiden torjunnassa. Tämän tyyppiset tapaukset muistuttavat, että toimintaympäristön ilmiöt saattavat edellyttää välitöntä reagointia ajankohdasta riippumatta, mikä korostaa tarvetta ennakoitiin ja viiveettömän johtamiskyvyn ylläpitoon.

Viime aikojen sodan kuva Ukrainassa ja Lähi-idän alueella on osoittanut voimankäytön kohdistuvan usein yhteiskunnan kriittisimpiin toimintoihin, kuten energian tuotantoon ja jakeluun, terveydenhuoltoon ja muihin elintärkeisiin toimintoihin. Kuten Suomessa on jo pitkään tunnistettu, laajamittaisen sodan uhkamalli asettaa korkean vaatimustason koko yhteiskunnan varautumiselle. Myös erilaiset matalamman kynnyksen hybridoitimet kuormittavat viranomaisia laajasti Euroopan alueella. Nykyaikaisessa toimintaympäristössä uhka näyttäytyykin usein monimuotoisena ja vähemmän tarkkarajaisena. Konfliktien ja muiden häiriötilanteiden seurannaisvaikutukset ulottuvat aiempaa laajemmalle yhteiskunnan toimintaan. Epäselvissä ja muuttuvissa olosuhteissa korostuu toiminnan jatkuvuuden turvaaminen, missä eri toimijoiden vastuiden tulee olla selkeät.

Turvallisuusympäristön muutosten seurauksena varautumisen kehittämisen tarve niin siviili- kuin sotilasympäristössä on tunnistettu akuutiksi myös Naton


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

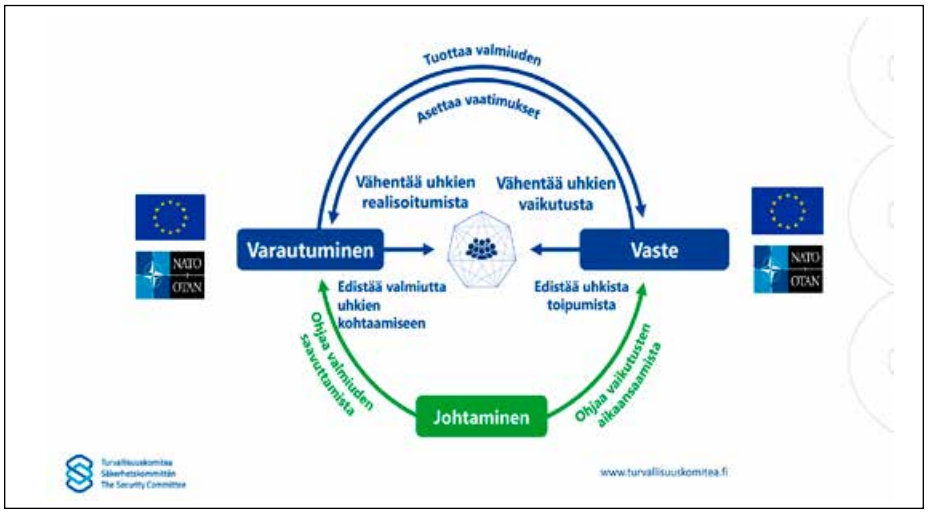
ja Euroopan Unionin puitteissa. Naton 360-turvallisuusperiaatteen mukaisesti liittokunta varautuu kaikkiin uhkiin koko liittokunnan alueella. Pelotteen ja puolustuksen vahventamisen osana resilienssin kehittäminen nähdään olennaisen tärkeäksi. Tällä tarkoitetaan liittokunnan ja sen jäsenvaltioiden kykyä vastata erilaisiin häiriöihin ja kriiseihin ja jatkaa toimintaansa näiden aikana. Resilienssi rakentuu siviilivarautumisen ja sotilaallisen suorituskyvyn yhdistelmästä. Siviiliyhteiskunnan toimivuus on edellytys sotilaalliselle vasteelle ja puolustukselle ylipäätään.

Resilienssin, kriisivarautumisen ja vasteen kehittämisen tarve on vastaavasti tunnistettu akuutiksi myös Euroopan Unionin piirissä. EU:ssa onkin käynnissä useita näiden vahvistamiseen tähtääviä aloitteita, kuten koko unionin kattavan varautumisstrategian laatiminen. Lisäksi presidentti Niinistön raportissa komissiolle EU:n siviili- ja puolustusvalmiuden vahvistamiseksi tunnistetaan tarve vahvistaa sotilas- ja siviilitoimijoiden välistä koordinaatiota, yhteistä suunnittelua, johtamisjärjestelmiä ja tilanneymmärrystä tehokkaan vasteen varmistamiseksi. Suomen esimerkkiä varautumisesta seurataan tarkasti kansainvälisellä areenalla ja jatkossakin on syytä pitää huolta sen ajanmukaisuudesta.

Vasteen käsite kokonaisturvallisuuden mallissa on laajentunut

Vaste on käsitteenä suomalaisessa kokonaisturvallisuusmallissa yhdistynyt aikaisemmin esimerkiksi onnettomuuksiin reagointiin tai katastrofien ensivasteeseen. Uudistettu yhteiskunnan turvallisuusstrategia nostaa vasteen käsitteen kuitenkin taktiselta toiminnan tasolta osaksi kokonaisturvallisuuden strategista viitekehystä. Tässä kontekstissa vasteella tarkoitetaan laajemmin kaikkia niitä toimia, joilla vastataan erilaisiin uhkiin hyödyntäen varautumisella rakennettuja suorituskykyjä. Kun varautumisella luodaan perusta toimia erilaisten uhkien aikana, vasteella puolestaan tarkoitetaan toimintaa, jolla minimoidaan realisoituneiden uhkien vaikutuksia tai estetään ennakoivasti niitä tapahtumasta.

Vaste on tilanne- tai kontekstisidonnaista. Kansallisen turvallisuuden kontekstissa vasteella voidaan viitata esimerkiksi konkreettisiin vastatoimenpiteisiin tai vastineeseen erilaisten uhkien realisoituessa tai ennakoiviin toimiin niiden ennaltaehkäisemiseksi. Sillä voidaan esimerkiksi estää yksittäistä vihamielistä tekoa muuttumasta laajemmaksi hyökkäykseksi tai rajoittaa uhkien vaikutusta ja mittakaavaa. Vasteella tarkoitetaan siis johdettua ja suunnitelmallista viranomaistoimintaa, jolla vastataan häiriötilanteisiin tai niiden uhkiin.



Yhteiskunnan turvallisuusstrategia korostaa vasteen ja varautumisen merkitystä kokonaisturvallisuuden muodostamisessa. Kuva: Turvallisuuskomitea.

Suomalaisessa kokonaisturvallisuuden mallissa hallinnonalat vastaavat omien lainsäädäntöön pohjautuvien strategisten tehtäviensä toteuttamisesta kaikissa tilanteissa sekä valmistautuvat tukemaan toimivaltaista vastuuviranomaista eri häiriötilanteiden aikana. Varautumalla ja suunnittelemalla strategisten tehtävien toteuttaminen kaikissa tilanteissa luodaan myös valmius vasteeseen. Kuhunkin tilanteeseen sopiva vaste määrittyy uhkan edellyttämällä tavalla. Esimerkiksi energiahuollon ja vesihuollon turvaaminen tai liikenneverkkojen ja -palveluiden varmistaminen edellyttävät erilaista vastetta kuin sotilaalliset uhat. Lähtökohtana on, että vaste toteutetaan normaaliolojen toimivaltuuksin. Vakavammissa tai laaja-vaikutteisemmissa häiriötilanteissa vaste voi kuitenkin edellyttää poikkeusolojen toteamista ja erikseen käyttöönotettavia lisätoimivaltuuksia eri viranomaisille.

Vasteen käsitteen nostaminen osaksi yhteiskunnan turvallisuusstrategiaa ei ole sattumaa. Natossa vaste- ja valmiudensäätelyjärjestelmiä on viime aikoina uudistettu Ukrainan sodan opit ja laaja-alaisen vaikuttamisen ilmiöt huomioiden. Kuten valtioneuvoston puolustusselonteossakin todetaan, kansallisia toimintamalleja järjestelmien yhteensovittamiseksi kehitetään poikkihallinnollisena yhteistyönä. Liittokunnan vaste- ja valmiudensäätelyjärjestelmien tarkoituksena on tukea liittokunnan oikea-aikaista päätöksentekoa kaikentyyppisissä kriisitilanteissa. Tyypillisesti vastetoimet ovat skaalautuvia ja moniportaisia, mikä mahdollistaa joustavuuden eri tilannekehityksiin. Kansallisesti on keskeistä, että vasteeseen liittyvät päätöksentekoprosessit on riittävällä tavalla tunnistettu ja harjoiteltu.

Kyky toiminnan sopeuttamiseen luo edellytykset yhteiskunnan kriisinkestävyydelle

Yhteiskunnan turvallisuusstrategian mukaan varautuminen ja kyky toimia ennakoimattomissa tilanteissa ovat edellytyksiä vasteelle. Varautumisajattelussa korostuu kyky yleiseen kriisinkestävyyteen eli resilienssiin, koska uhkien moninaisuudesta johtuen niiden yksityiskohtainen ennakointi on vaikeaa. Naton kontekstissa resilienssin kehittäminen perustuu liittokunnan perussopimuksen kansallista puolustusta käsittelevään kolmanteen artiklaan. Resilienssi muodostuu liittokunnan sekä sen jäsenvaltioiden kyvystä varautua, vastata ja toipua erilaisista häiriötilanteista ja shokeista. Resilienssin kehittäminen on liittokunnan jäsenmaiden kansallisella vastuulla, mutta myös kollektiivinen sitoumus. Suomi

osallistuu aktiivisesti Naton resilienssityöhön.

Nato tunnistaa, että resilienssi rakentuu yhtä lailla sekä siviiliyhteiskunnan varautumisen että sotilaallisten suorituskykyjen seurauksena. Natossa siviiliyhteiskunnan resilienssi muodostuu yhteiskunnan kolmen päätehtävän kautta, joita ovat valtionhallinnon jatkuvuuden turvaaminen, yhteiskunnan elintärkeiden toimintojen ja palveluiden turvaaminen sekä siviilisektorin tuen takaaminen asevoimille. Päätehtävien turvaamiseksi Naton jäsenvaltiot ovat hyväksyneet resilienssin seitsemän perusvaatimusta, joilla varmistetaan sekä tarvittava tuki asevoimille että yhteiskunnan toimivuus kriisien aikana. Jäsenvaltiot vastaavat itse resilienssin perusvaatimusten toteutumisesta. Näitä perusvaatimuksia ovat:

1. Valtionhallinnon ja kriittisten yhteiskuntapalveluiden jatkuvuuden varmistaminen

2. Energiahuollon turvaaminen

3. Kyky hallita kontrolloimattomia väestöliikkeitä

4. Elintarvike- ja vesihuollon turvaaminen

5. Kyky käsitellä suuria määriä siviiliuhreja

6. Teleliikennejärjestelmien turvaaminen

7. Kuljetusjärjestelmien turvaaminen.

Kuten resilienssin perusvaatimuksista käy ilmi, siviiliyhteiskunnan vasteen voidaan ajatella koostuvan toiminnan sopeuttamisesta tai mukautumisesta. Yhteiskunnan kriittiset toiminnot pyritään ylläpitämään kaikissa tilanteissa, mikä on keskeinen edellytys sekä puolustusvalmiudelle että sotilaalliselle vasteelle. Toisaalta sotilaallinen tuki voi puolestaan olla kriittistä siviilitoimijoille jo normaaliolojen häiriötilanteissa. Resilienssin ylläpito edellyttääkin sekä siviili- että sotilastoimijoiden välistä yhteistyötä, mikä on jo itsessään sisäänrakennettu ajatus kokonaisturvallisuusmallissamme.

Yhteistoimintamalliamme haastaa kuitenkin toimintojen välinen keskinäisriippuvuus, mistä johtuen eri toimijoiden vastuurajojen määrittely on usein hankalaa, esimerkkinä kybertoimintaympäristön läpileikkaavuus kaikkiin yhteiskunnan palveluihin. Eri toimijoiden roolit ja yhteistoiminnan organisoinnin periaatteet tulisikin vähimmillään olla tunnistettu jo normaalioloissa, sillä epäselvät vastuukysymykset voivat pahimmillaan muodostaa toimintaa haittaavaa kitkaa eri toimijoiden välille. Johtovastuiden selkeyttämisen lisäksi on nähtävissä tarve kehittää koordinaatiota, tilanneymmärrystä ja yhteistä suunnittelua, mikä havaittiin jo korona-aikana.

Vastetta voidaan vahvistaa yhteisellä suunnittelulla ja harjoitustoiminnalla

Vasteajattelussa tärkeää on, että turvallisuusympäristön tapahtumiin reagoidaan, vaikkei ilmiöiden perimmäiset syyt olisikaan lähtökohtaisesti selviä. Puolustusselonteossa kuvattu laaja-alaisen vaikuttamisen viitekehys tunnistaa välillisen vaikuttamisen mahdollisuuden, mikä ilmenee usein viranomaisten vastuualuei-

den välisissä saumakohdissa. Yksittäinen tapahtuma voi laukaista usean viranomaisen muodostaman vasteen, johon eri viranomaiset osallistuvat omien lakisääteisten tehtäviensä mukaisesti. Sama tapahtuma voi näyttäytyä esimerkiksi sekä onnettomuutena että tarkoituksellisena tuhotyönä. Yhteisen tilanneymmärryksen kannalta on välttämätöntä tarkastella tilannekuvaa kokonaisvaltaisesti ja pitkäjänteisesti, ja huomioida mahdollinen vaikutusnäkökulma ilmiöiden tarkastelussa.

Sotilaallisessa ajattelussa vaste kytkeytyy operatiiviseen toimintaympäristöön, joita Naton hyväksymiä on viisi (maa, meri, ilma, avaruus, kyber). Toimintaympäristöjen integroitumisen painopiste on MDO-konseptin (Multi-Domain Operations) mukaisesti sotilaallisissa suorituskyvyissä, mutta myös siviilikomponentin merkitys tunnistetaan keskeisenä operaatioiden tukemisessa. Siviili-sotilasyhteistyö (CIMIC) onkin yksi MDO:n operatiivisista toiminnoista tulenkäytön, liikkeen ja informaation tapaan. Useiden erilaisten toimintojen yhteensovittaminen ajassa ja tilassa edellyttää yhteisen operatiivisen viitekehyksen muodostamista. Tavoiteltujen vaikutusten aikaansaaminen edellyttää tyypillisesti usean eri toimijan välistä koordinoitua toimintaa.

Sotilaallisessa vasteajattelussa korostuu liittokunnan operatiivisen suunnitelmaperheen kokonaisuus, sen harjoittelu ja kyky toimeenpanoon. Tähän voi liittyä erilaisia vaatimuksia siviilikomponentin suuntaan, esimerkiksi sotilaallisen liikkuvuuden mahdollistamiseksi tai jo mainitun kriittisen infrastruktuurin toiminnan varmistamiseksi. Vasteen toteuttaminen tuleekin suunnitella siviili- ja sotilastoimijoiden yhteistyönä osana varautumista. Konkreettinen tapa todentaa eri toimijoiden välisen yhteistoiminnan sujuvuutta, toimintamallien tehokkuutta sekä tunnistaa vaatimuksia kehittämiselle, on yhteinen harjoitustoiminta. Naton harjoituksissa siviilikomponentti onkin usein aktiivisesti mukana. Haasteena on tunnistaa jo suunnitteluvaiheessa kaikki ne prosessit ja tapahtumat, joihin siviilitoimijat on kytkettävä mukaan, ja löytää yhteinen ajallinen resurssi toteuttaa mainittua suunnittelua.

Tiedonvaihtotarpeet määrittävät vaatimuksia johtamisjärjestelmien kehittämiselle

Siviili- ja sotilastoimijoiden yhteistyötä voidaan kehittää tiedonvaihdon vahvistamisella. Yksi tapa tähän on tunnistaa erilaisia toimintaketjuja ja niihin liittyviä tiedonvaihtotarpeita. Esimerkiksi vasteen suunnittelun ja toimeenpanon prosesseista voidaan tunnistaa sellaisia vaiheita, joissa tietoa tulee vaihtaa eri toimijoiden välillä. Sotilaspuolella yhteistoiminnan konseptitasoisia (MDO) tiedonvaihdon vaatimuksia jalostetaan johtamisjärjestelmien yksityiskohtaisiksi vaatimuksiksi muiden muassa FMN-yhteistyön (Federated Mission Networking) puitteissa. Määrittelytyössä haasteena eivät yksistään ole teknologiaan liittyvät kysymykset, vaan erilaiset käsitykset esimerkiksi integroimisen tavasta ja asteesta. Naton piirissä kansalliset tulkinnat siviili-sotilasyhteistyöstä eroavat merkittävästikin toisistaan. Haastetta pyritään ratkaisemaan yhtäältä doktriineja ja sovellusohjeita kehittämällä. Kansallisia toimintatapoja joudutaan tarkastelemaan kriittisesti ja tunnistamaan niistä ylläpidettäviä ja kehitettäviä kokonaisuuksia.

Siviili- ja sotilastoimijoiden tieto on usein pirstaloitunutta eli se sijaitsee hajallaan useissa sisäisissä tietojärjestelmissä tai pahimmillaan dokumentoimattomana hiljaisena tietona. Tieto ei siis ole välttämättä digitaalisin keinoin saavutettavissa tai käsiteltävissä. Ensimmäisenä haasteena onkin tunnistaa ja määritellä keskeisiltä osin sellainen toimintaan liittyvä tieto, millä on käyttöarvoa myös omaa toimintaa laajemmassa kehyksessä. Toisena haasteena on ratkaista tiedon hallintaan liittyviä kysymyksiä, esimerkiksi miten dataa kerätään ja käsitellään. Kolmantena voidaan pohtia, miten dataa hyödynnetään suunnittelun ja päätöksenteon tukena ja missä määrin tiedonkäsittely tulee automatisoida. Tiedon hyödyntämiseen liittyvät valinnat edellyttävät teknologisten ratkaisujen lisäksi usein perustavanlaatuisia muutoksia organisaatioiden toimintakulttuureihin ja käytäntöihin. Datakeskeisyys ei toisin sanoen yksistään ratkaise tiedonkäsittelyyn liittyviä kysymyksiä. Täydentävinä ratkaisuina yhteisten alustojen kehittäminen tai integroitumisen syventäminen voivat olla perusteltuja.

Voivatko siviili- ja sotilastoimijat vaihtaa saumattomasti tietoa keskenään? Vaikka tiedonvaihto olisi teknisesti mahdollistettu, eri toimijoilla voi olla vaihtelevia tulkintoja lain mukaisista velvollisuuksista tai esteistä tiedon jakamiseen. Toisaalta tieto on myös kriittistä pääomaa organisaatioille, eikä sitä välttämättä haluta jakaa ulkopuolisille, vaan käyttää ensisijaisesti omiin tarpeisiin. Eri toimijoiden välillä voi olla myös kilpailullinen asetelma esimerkiksi tietyn palvelun tuottamisesta. Monesti kyse on yksinkertaisesti näkökulmaeroista. Tiedonvaihtoon liittyy keskeisesti luottamuksellisuus. Suomen mallissa tietoa vaihdetaan usein eritasoisten virallisten tai epävirallisten yhteistoimintaverkostojen puitteissa. Tiedon anonymisointiin voidaan hyödyntää myös teknisiä ratkaisuja.

Tekoälyn merkitys suurten tietomassojen käsittelyssä kasvaa. Erilaisten tilannekuvatietojen koostaminen ja ennusteiden laadinta niiden perusteella on koneellisesti merkittävästi tehokkaampaa kuin ihmistyönä, etenkin kun kysymys on suurista tietomassoista. Tekoälyn avulla voidaan periaatteessa tuottaa objektiivisempaa tietoa päätöksenteon tueksi. Tämä edellyttää järjestelmiin syötetyiltä lähtötiedoilta laadullista eheyttä ja kattavuutta. Ajatusvinoumia voi silti muodostua sekä tekoälyjärjestelmiä kehitettäessä että niitä käytettäessä. Joka tapauksessa tiedon tulkintaan vaikuttavat ennakko-oletukset ja intressit eri vaiheissa. Kognitiivisten prosessien läpinäkyväksi tekeminen edesauttaa selviytymistä nykyaikaisen sodankäynnin olosuhteissa. Vasteen ja varautumisen onnistumisen ehtona on, että tulkintamme ja ymmärryksemme tilanteesta on sokeine pisteineenkin riittävän oikeansuuntainen.

Päätäntä

Vasteen kehittäminen on noussut vaatimukseksi niin kansallisesti kuin Naton kontekstissa perinteisen varautumisen rinnalle. Suomen kokonaisturvallisuusmalli on monin tavoin yhteensopiva Naton resilienssi- ja vasteajattelun kanssa. Mallit tunnistavat, että tehokas vaste perustuu varautumisen ja resilienssin kokonaisvaltaiseen kehittämiseen monimuotoinen uhkaympäristö huomioiden.

Kansallisessa toimintamallissamme vaste muodostuu viranomaisten yhteistyönä usean eri hallinnonalan välillä. Tämä korostaa eri toimijoiden roolien tunnistamista sekä yhteisen tilanneymmärryksen ja toiminnan koordinoinnin merkitystä. Yhteistoimintaa voidaan kehittää esimerkiksi yhteisellä suunnittelulla ja harjoittelulla.

Tiedonvaihdon kehittämisen lähtökohtia ovat tunnistettu tieto ja tapa vaihtaa tietoa. Johtamisjärjestelmien on mahdollistettava siviili- ja sotilastoimijoiden yhteisen suunnittelun lisäksi tilanneymmärryksen muodostaminen, vasteen toimeenpanon johtaminen vastuuviranomaisen johdolla ja toiminnan vaikuttavuuden yhteinen arviointi. Integroitumisen ratkaisujen on oltava kansainvälisesti yhteensopivia, skaalautuvia ja mahdollistettava tiedon luottamuksellisuuden ja eheyden säilyttäminen. Päätöksenteon prosessit on tunnistettava ja arvioitava niihin liittyviä riskejä.

Lähteitä:

Yhteiskunnan turvallisuusstrategia 16.1.2025

Valtioneuvoston puolustusselonteko 19.12.2024

Ulko- ja turvallisuuspoliittinen selonteko 20.6.2024

Report: Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness. Presidentti Sauli Niinistön raportti Euroopan komissiolle 30.10.2024

Kirjoittaja everstiluutnantti Eero Havu on koulutukseltaan yleisesikuntaupseeri ja palvelee tällä hetkellä Pääesikunnassa. Työssään hän on perehtynyt operatiiviseen suunnitteluun, kyberpuolustuksen kysymyksiin sekä johtamisjärjestelmien vaatimusmäärittelyyn. Hän osallistui viime syksynä Etelä-Suomen alueelliselle maanpuolustuskurssille yhdessä toisen kirjoittajan kanssa.

Kirjoittaja Anni Hakaniemi toimii erityisasiantuntijana valtioneuvoston kanslian valmiusyksikössä. Työssään hän on keskittynyt erityisesti valtioneuvoston varautumiseen, jatkuvuussuunnitteluun sekä harjoitustoimintaan. Koulutukseltaan hän on yhteiskuntatieteiden maisteri ja käsitteli pro gradu -tutkielmassaan korona-aikaista resilienssiä ja kriisijohtamista.

TEKSTI: ANTTI NYQVIST

Tiedonvaihtoa häiriötilanteissa selviytymiseen – TIETO24-harjoitus

Jokaisen yrityksen on syytä miettiä kuinka varautua hybridivaikuttamiseen eli informaatiovaikuttamiseen, kyberhäiriöihin ja jopa fyysisen maailman tapahtumiin – nyt jos koskaan on varmaa, että häiriöitä kohdataan yritysarjessa. Varautumisen taso ratkaisee sen, mikä vaikutus tällä häiriöllä on liiketoiminnan jatkuvuuteen tai siihen huoltovarmuuskriittiseen vastuuseen joka tekemiselläsi on yhteiskunnan kannalta. Varautuminen siis kannattaa ja tässä kirjoituksessa avataankin niitä aiheita ja sitä toimintaa, johon nyt tulee varautua, jotta organisaatio on valmis kohtaamaan vaikka kyberhäiriön.

Digipoolista

Huoltovarmuusorganisaation poolit ovat yritysten verkostoja, joiden tehtävänä on edistää elinkeinoelämän jatkuvuudenhallintaa ja varautumista. Toiminta on täysin vapaaehtoisuuteen perustuvaa yhteistyötä yritysten, julkishallinnon ja järjestöjen välillä. Vapaaehtoisuudesta johtuen yrityksiltä ei voida varsinaisesti mennä vaatimaan asioita, vaan paras tapa edistää varautumista on sparrata yrityksiä – eli tukea ja vahvistaa heidän omia kehitysajatuksiaan.

Digipoolin kaksijakoinen tehtävä on oman alan yritysten tukeminen kokonaisturvallisuuden aiheissa, sekä kollegoiden eli muiden alojen yritysten tukeminen edistämällä kybervarautumista. Pyrimme siis vaikuttamaan siihen, että suunnitelmia syntyy jatkuvuudenhallinnan ja varautumisen aiheissa. Yritysten sparraukseen on monia tapoja, mutta näistä ehdottomasti tehokkain tai paras tapa on järjestää toimintaa, missä yritykset kohtaavat ja jakavat tietoa näissä aiheissa. Ja mikä parempi tapa tähän onkaan kuin harjoitella häiriötilanteiden varalle suunniteltuja toimintatapoja.

Harjoituksissa kohtaavat niin verkostoitumisen hyödyt kuin tiedon ja keinojen jako kehityksen tueksi. Digipooli vastaa kahden vuoden välein järjestettävistä TIETO-harjoituksista, joissa ideana on harjoitella yhteistoimintaa ja tiedonvaihtoa häiriötilanteiden varalle.

TIETO-harjoituksista

TIETO-harjoitukset eli tietoyhteiskunnan valmiusharjoitukset omaavat jo pitkät perinteet, kun 70-luvun lopulla puolustusvoimien vetämät Tele-harjoitukset lähtivät edistämään tietoverkkoihin perustuvan toiminnan varautumista. Lähestyttäessä nykypäivää on painopiste tämän alueen varautumisessa siirtynyt elinkeinoelämälle ollen siitä täysin riippuvainen. Tämän takia harjoitusten järjestämisvastuu on siirtynyt Huoltovarmuuskeskuksen kautta Digipoolille. Harjoituksen tavoitteet ovat kuitenkin samat – edistää verkottuneen tietoyhteiskunnan yhteistoimintaa ja saada aikaan valmiutta, jolla kestetään erilaiset laajatkin häiriötilanteet, joissa ilmenee fyysisiä-, informaatio- ja kyberhäiriöitä.

TIETO-harjoituksiin kootaan pienoisyhteiskunta, missä yritykset muodostavat toimitusketjuja ja viranomaiset pääsevät heidän kanssaan varmistamaan ketjujen toimintaa. Harjoittelemaan kutsutaan toimijoita, jotka ovat kulloiseenkin verkostoon, toimitusketjuun tai muuhun kokonaisuuteen relevantteja – yrityksiä, yleisesti merkittäviä viranomaisia tai toimialakohtaisia vastuuviranomaisia. Harjoituksessa käsitellään sen verkoston toimintaa ja tiedonvaihtoa, joka tulee tapahtua, jotta laajastakin häiriötilanteesta päästään jatkamaan toimintaa ja minimoidaan tiedon ja keinojen vaihdolla ne vaikutukset, joita häiriöistä koituu – toisin sanoen kestetään kohdatut haasteet ja ollaan resilienttejä.

TIETO24 Pelin organisaatiot.

TIETO24-harjoituksen teemana ollut Energiasektorin tuontiriippuvuudet johti siihen, että mukaan varmistettiin erityisesti energia- ja logistiikkasektorien elinkeinoelämää sekä sektoriviranomaisia. Energian saannissa ja logistisissa yhteyksissä koetut häiriöt aiheuttivat vaikutuksia laajasti myös muille toimialoille. Häiriöitä laivaliikenteessä tai tietoliikenteessä sekä varaosien tai raaka-aineiden saannissa simuloitiin ja pohdittiin kuka on keneenkin yhteydessä ja mitä tulisi kertoa missäkin tilanteessa. TIETO24-harjoitukseen oli rekisteröitynyt henkilöitä 170 yrityksestä ja 10 julkishallinnon organisaatiosta yli 20 toimialalta. Rekisteröityneitä henkilöitä oli yli 750, joista 90 henkilöä energiasektorilta ja 80 logistiikan alalta.

Kansainvälisestä yhteistyöstä ja harjoittelusta

TIETO24-harjoitukseen osallistui tarkkailijoina ennätysmäärä myös naapurivaltioiden viranomaisten edustajia. Harjoitukseen tutustuivat niin MSB:n (Myndigheten för samhällsskydd och beredskap) ja MPF:n (Myndigheten för Psykologiskt försvar) edustajat Ruotsista kuin RIA (Riigi infosüsteemi amet) Virosta. Lisäksi harjoituksessa vieraili NATO:n kyberkomitea Ulkoministeriön saattajien kera. 28 NATO jäsenvaltion edustajat pääsivät paikalle harjoitukseen tutustumaan ja imemään vaikutteita.

Kansainvälisten tarkkailijoiden havainnoista kirkkaimpana kaikkien mieliin jäi havainto siitä, että elinkeinoelämän ja viranomaisten harjoittelua tulee tehdä valtiorajat ylittäen – erityisesti nykyisessä tilanteessa ja koska sitä ei tällä tavalla ole tehty. Tiedonvaihdon edellytykset tulee läpikäydä ja varmistaa, jotta kaikki sujuu häiriötilanteiden kannalta. Arviona oli, että varsinaisia esteitä ei olisi ja yhteistyösopimuksiakin on, mutta lainsäädäntö ja välineistö olisi hyvä tarkistaa ja sopia – sekä harjoitella. Tuleviin TIETO-harjoituksiin lieneekin syytä kutsua laajempikin joukko kansainvälisiä kontakteja harjoittelemaan.

Puolustusvoimien tavoitteista TIETO-harjoitukselle

TIETO24-harjoitus käsitteli normaaliolojen laajoja häiriötilanteita, eli tilanteita missä ei valmiuslain toimivaltuuksia ole aktivoitu, mutta päästään näkemään tarpeita niille. Normaalioloissakin on

TIETO24 white team, kuva Meeri Utti.

Puolustusvoimilla kuitenkin tiedonsaantitarpeita muun yhteiskunnan toiminnasta – jotta voidaan varautua, vaikka tilanteen tiukkenemiseen. Näistä lähtökohdista puolustusvoimat tukee Tieto-harjoitusta ja pääsee samalla havainnoimaan oman kumppanuusverkostonsakin toimintaa ja tiedonjakoa. Tässä oleellisena on PVLOGL, joka vastaa sopimuksista ja niiden mukaisesti yhteistyöstä elinkeinoelämän kanssa. Pääesikunnan ja PVLOGL yhteistyötä myös harjoiteltiin samalla – harjoituksen tukemiseksi. Erityisen kiinnostavaa tästäkin näkökulmasta on logististen yhteyksien toiminta, jota harjoituksessa käsiteltiin myös useiden alan toimijoiden kanssa.

Kyberhäiriötilanteissa toimittaessa huomioitavaa

TIETO-harjoitusten konseptiin kuuluu myös kouluttaa osallistujia erilaisilla aiheilla, jotka liittyvät kyberhäiriötilanteisiin tai erottamattomana myös informaatiovaikuttamiseen, eli hybridivaikuttamiseen myös sen fyysisine ilmentymineen. Kyberhäiriöihin varautuessa tai jatkuvuudenhallinnassa tulee näitä kaikkia huomioida yhdenaikaisesti. Seuraavat kappaleet esittelevät harjoituksen koulutussisältöä – asioita, joita tulee huomioida suunnitelmissa ja joita harjoitellaan siltä varalta, että kohdataan se mahdollinen laaja häiriö.

Ensimmäinen havainto mietittäessä kyberhäiriötilanteissa toimintaa on, että yksin ei kannata jäädä ihmettelemään, vaan verkostossa on voimaa, jonka avulla tilanteesta selviää. Silti itselle ja omalle organisaatiolle jää paljon tehtävää ja asioita, joita kannattaa huomioida. Harjoituksessa pyritäänkin saamaan aikaan tukemaan verkostoitumista ja tiedonvaihtoa niin strategisella, taktisella kuin operatiivisellakin tasolla, ja siksi mukaan on kutsuttu osallistujia yritysorganisaatioiden eri tasoilta.

Kaikkien organisaatiossa tulisi ymmärtää prioriteetit oikein ja kaikkea varautumista ja jatkuvuudenhallintaa tuleekin ohjata liiketoimintojen priorisoinnilla. Ajattelu lähtee siitä, että jokainen yritys on käynyt läpi liiketoimintansa ja priorisoinut toimintonsa liiketoiminta-arvon ja suojaa ainakin tärkeimmät toiminnot. Eikä sovi unohtaa sitä huoltovarmuuskriittisyyttäkään – joskus liiketoimintakriittinen toiminto on myös huoltovarmuuskriittinen, mutta useinkaan ei ja silti sen pitäisi priorisoinnissa nousta kärkisijoille.

Toimintojen prioriteetti tulee myös kommunikoida organisaation eri tasoilla sekä toimitusketjussa, jotta tärkeimmät saavat sen suojan, jonka ansaitsevat. Parhaimmillaan toimitusketjun eri toimijat ovat priorisoinnin tehneet ja silloin myös varautumistoimien kohdistaminen on selkeämpää ja rajatumpaa ja tuottaa sitä turvallisuutta, jota todella tarvitaan.

Näiden priorisoitujen toimintojen varmistaminen on siis jatkuvuudenhallinnan ja varautumisen ytimessä ja ensimmäinen tehtävä onkin tehdä henkilöstösuunnittelua. Pitää siis läpikäydä se, että kaikissa tilanteissa (myös sotatila) olisi yrityksellä kyky tehdä töitä kriittisen toiminnon varmistamiseksi. Ennen kaikkea

siis suunnitellaan se, ketkä ovat oleellisia työn tekemiseksi ja toissijaisesti sitten yrityksen toiminnan varmistamiseksi siinä ympärillä. Kotimainen Henkilövarausjärjestelmä (https://puolustusvoimat.fi/asiointi/henkilovaraukset) auttaa niissä tilanteissa, missä henkilöstösuunnittelun mukaan kriittinen henkilö tulee varata työtä tekemään myös kriisien aikana. Yhä useammin näissä ns. VAP-listoissa näkyy myös varattavan ICT-asiantuntijoita ja muita järjestelmien ja kyberturvallisuuden kanssa työtä tekeviä henkilöitä, joita myös Puolustusvoimat tarvitsee kriisitilanteissa.

Kun sitten ollaan tekemässä työtä sen kriittisen toiminnon ja siihen liittyvien tietojärjestelmien kanssa tulee ymmärtää oma kybertoimintaympäristö. Digipoolin teettämien kyberkypsyys toimialoilla selvitysten (https://www.digipooli.fi/fi/ajankohtaista/uutinen/toimialojen-kyberkypsyys-2022-selvitys-kertoo-digitaalinen-turvallisuus) 2020 sekä 2022 perusteella kotimaiset yritykset eivät tarvittavalla tasolla muodosta tilannekuvaa, saati jaa sitä organisaationsa sisällä sitä tarvitseville. Esimerkiksi palkkahallinto tai reskontratoiminnot harvoin tietävät tietojärjestelmiensä tilaa tai uhkapinta-alaa, vaikka työ on siitä täysin riippuvaista. Eli tilannekuvaa tulisi muodostaa monin tavoin ja monelle tasolle yrityksissä. Yrityksen johto tarvitsee myös tilannekuvaa liiketoimintaa ohjatakseen, mutta erityisesti ne tiimit, jotka kriisissä kootaan ja pääsevät tekemään päätöksiä tiukassa tilanteessa tarvitsevat monipuolista tilannekuvaa päätöksenteon tueksi.

Toisaalta tilannekuvia on yhtä monta kuin on tilannettakin, joten tässäkin riskienhallinta ja erilaiset toimintaa uhkaavat skenaariot ohjaavat hyvän tilannekuvan äärelle ja tämä tuleekin suunnitella etukäteen. Mitkä ovat ne relevantit tietolähteet mistä muodostamme tilannekuvaa jos kohtaamme informaatiovaikuttamista, palveluestohyökkäyksen tai kiristyshaittaohjelman tai järjestelmämme tuhoutuvat. TIETO24-harjoituksen sekä 2022 tehdyn selvityksemme perusteella näyttää siltä, että vaikka verkostojen kautta saadaan tietoa yrityksiin kohdistuvista uhista ei se realisoidu yrityksissä toiminnaksi, koska myös yleinen osaaminen tai ymmärrys ei ole kautta linjan tarvittavalla tasolla (tai ei ole resursseja sen toteuttamiseen).

Oleellisista tietolähteistä puhuttaessa ei voi olla mainitsematta verkoston voimaa ja viranomaisten tukea. Erilaiset **tiedonvaihtoverkostot** ja erityisesti **ISAC-ryhmät** eri toimialoilla jakavat kyberhäiriötietoa. Ryhmien toiminnassa yritysten asiantuntijat pääsevät jakamaan kokemuksiaan ja saavat vinkkejä toimenpiteistä, joita tehdä eri tilanteissa. Lisäksi Kyberturvallisuuskeskus on viranomaisena mukana jakamassa heille kertynyttä tilannekuvaa ja on toisaalta muodostamassa sitä jaetun tiedon perusteella. TIETO-harjoituksissa osallistujien antaman palautteen perusteella nimenomaan ISAC-verkostoja tai vastaavia muita luottamuksellisia vertaistukiryhmiä pidetään arvokkaana elementtinä häiriötilanteessa selviytymisessä. Kannattaa verkostoitua ja kysellä kollegoilta kokemuksia ja jakaa niitä.

Viranomaisyhteistyö on myös erinomainen tapa kehittää omaa tilannekuvaa ja auttaa selviämään häiriöistä. Samalla rakentuu kansallinen tilannekuva ja ymmärrys. Yhteistyö on helppoa aloittaa **raportoimalla häiriöistä matalalla kynnyksellä** – samalla pääsee em. tietolähteiden äärelle ja hyötyy tiedonvaihdosta. Kaikista kyberhäiriöistä kannattaa siis ilmoittaa Kyberturvallisuuskeskukseen.

Suomessa Traficomin Kyberturvallisuuskeskus vastaa kyberturvallisuuden tilannekuvasta ja jakaa siihen liittyvää tietoa eri muodoissaan julkisesti jakaen muun muassa ns. CIP-listat, haavoittuvuustiedotteet sekä kybersään, jotka kertovat Suomessa ilmenneistä häiriöistä kyberkentällä ja tarjoavat tietolähteitä omaan tilannekuvaan. Poliisiin kannattaa olla yhteydessä nettivinkillä tai rikosilmoituksella, kun epäilee rikoksen tapahtuneen. Ja tietysti jos häiriössä on vaarantunut henkilöön liittyvää tietoa, tulee siitä ilmoittaa tietosuojavaltuutetun toimistoon. Hyviä tietolähteitä ovat myös muut ns. neljännen sektorin toimijat, jotka vapaaehtoispohjalta tukevat häiriöiden kohteiksi joutuneita.

Oman mausteensa laajojen kyberhäiriötilanteiden hallintaan tulee tuottamaan **EU:n lisääntyvä regulaatio**. Direktiivit kuten NIS2 ja CER tulevat vaikuttamaan laajasti kyberaiheiden hallintaan. Vaikuttamaan tulevat myös toimialakohtaiset asetukset tai muu ohjaus, kuten finanssialan DORA-asetus tai energiasektorin NCCS periaatteet, tai näiden takia tehty tuore kotimainen lainsäädäntö, jotka alkavat edellyttämään näitä asioita toimijoilta useimmilla toimialoilla ja jopa pieniä ja keskisuuria yrityksiä koskien. Direktiivien ja lainsäädännön myötä turvallisuudenhallinnan tilaa ja häiriötilanneilmoituksia päästään tekemään myös toimivaltaisille sektoriviranomaisille.

Kyberhäiriötilanteissa ei kuitenkaan yleensä ole kyse vain kybertoimintaympäristön tapahtumista, vaan niihin liittyy informaatioulottuvuus tai jopa fyysisiä häiriöitä, jolloin puhutaan hybridivaikuttamisesta. Informaatioulottuvuus tulee myös sikäli kyseeseen, että kyberhäiriötilanteita varten on suunniteltava se kuinka asioista viestitään, jottei eskaloida tilannetta tai saadaan se hallittua. Puhutaan **kriisiviestinnästä**, missä kriisejä joihin varautua voi olla monia, sekä kyberhäiriöitäkin useita erilaisia ja niistä yritykselle koituvia vaikutuksia, jotka usein viestinnässä tulee huomioida.

Kyberhäiriötilanteet eivät ole siis vain ICT-asiantuntijoiden toimintakenttää, vaan mukana tulee olla viestinnän asiantuntijoita. Viestintää tai kommunikaatiota tulee varautua tekemään niin sisäisesti kuin asiakkaiden, alihankkijoiden ja viranomaisten kanssa, mediaviestintää unohtamatta. Media on myös tilannekuvan muodostamisen kannalta oleellinen huomioitava lähde. Yhä useampi yrityksen viestintätoiminne tekee aktiivista mediaseurantaa jo arjessakin, joten se on syytä saada osaksi häiriötilanteessa toimintaa. TIETO-harjoituksissa osallistuneet yritykset ovat toistuvasti heränneet siihen, että kyberhäiriötilanteissa mediaseuranta vaatii resursointia ja *relevantteja tietolähteitä tulee rajata, jotta seuranta on mahdollista*.

Kriisitiimit eli ns. CMT (Crisis management team) -tiimit ovat myös etukäteen suunniteltu tiimi tai tiimejä, joilla on ennakolta suunnitellut osallistujat ja toimintatavat. Ei siis ole yhtä ja ainutta mallia kriisitiimin koostumukselle, mutta tyypillisesti kyberhäiriötilanteissa tulee olla mukana ICT- tai kyberasiantuntijuutta, viestintää ja liiketoiminnan ymmärrystä – eikä jurististakaan haittaa ole. Vähän tapauksen mukaan mukana on syytä olla henkilöstöhallintoa tai logistiikan edustusta tai joku sellainen kuka kyseistä häiriön vaikutuksen kohdetta substanssin puolesta tuntee. Tällä monitaitoisella joukolla ja hyvällä tilannekuvalla päästään tekemään päätöksiä, joilla selvitään kyberhäiriöistä.

TIETO24 CMT-tiimien tiedotustilaisuutta seurataan myös vieraiden toimesta, kuva Meeri Utti.

Kriisitiimin perustaminen vie jo pitkälle, mutta jos ja kun kohdataan häiriötilanne on tiedettävä kuinka toimia. Tuleekin olla valmiiksi mietityt **toimintatapamallit** erilaisten häiriöiden varalle. Usein puhutaan *playbookeista*, eli pelikirjoista, jotka kuvaavat roolit tai vastuut tilanteessa ja toimenpiteet, joita tulee tehdä tilanteessa. Puhutaan myös prosesseista, jotka käynnistetään ja mitä suurempi yritys sen todennäköisempää on, että talosta löytyy MIM (*Major Incident Management process*). Ja mitä suurempi häiriö, sen todennäköisemmin mukana on vastuita myös ylimmälle johdolle. Toimintatapamalleihin liittyy toimenpiteitä teknisistä tehtävistä aina viestintään ja päätöksentekoon asti – valtuuksia unohtamatta. Hyviä toimintatapoja on myös syytä harjoitella, jotta niissä todella osataan toimia tiukan paikan tullen – harjoitteluhan on myös paras tapa kehittää toimintatapoja ja saada ne saumattomiksi tosipaikkaa varten.

Edellä mainitun Digipoolin kyberkypsyys toimialoilla selvityksen mukaan kotimaisten yritysten akilleen kantapäänä on **alihankintaketjun hallinta** tai alihankintaketjun kanssa yhteinen riskienhallinta tai yhteistyö siinä määrin, että toimintatapoja harjoiteltaisiin. Olettaen, että edellä mainittu liiketoimintojen priorisointi on tehty ja prioriteetin mukaiset varautumisvaatimukset ovat sopimuksella alihankkijalle valutettu olisi suositeltavaa kirjata sopimukseen myös kuvaukset yhteisistä riskienhallinnan periaatteista ja yhteisestä harjoittelusta. Aidolla riskitkin jakavalla yhteistyöllä kestetään mitä häiriöitä tahansa. ”Organisaatio voi ryhtyä toimimaan erilaisissa (erityisesti pahoissa) häiriötilanteissa korkeintaan niin hyvällä tasolla kuin on asioita etukäteen säännöllisesti harjoitellut.”

TIETO24-harjoituksen havainnoista

TIETO-harjoituksissa käsitellään siis tiedonvaihtoa. Harjoitukseen kuuluu myös kolmipäiväinen roolipeli, missä pienoisyhteiskunta tekee tiedonvaihtoa laajoista kyberhäiriöistä selvitäkseen. Tiedonvaihdon kannalta löydetään myös aiheita, joita tulee seurata tai joissa olisi kehitettävää. Tässä harjoituksen perusteella seurattavia aiheita:

- Kriisitilanteissa resursseja on kohdennettava tilannekuvatuotantoon ja tiedon keruuseen (ml. median seuranta) ja viestintään. Automaatioasteen kasvaessa on kiinnitettävä huomiota tiedon oikeellisuuteen.

- Luotettavien tietolähteiden tunnistaminen ja määrittely on varautumistehtävä. Verkoston toiminta ja koordinaatio perustuu luotettavan tiedon jakoon kahden ja monenvälisesti.

- Jäsennellyn tiedon tuottamista (tilannetietoisuuden tueksi) vaikeuttaa yleinen osaamattomuus kyberturvallisuus aiheissa.

- Vaikuttamisen ja Informaatiokampanjoiden tietoisuutta henkilöstössä on kasvatettava.

- Informaatiokampanjoiden tunnistamista haastaa kiire ja tapahtumien runsaus. Aikaa ja asiantuntevia resursseja tulee varata analyysille.

- Tiedon jakoa on pystyttävä tekemään reaaliajassa organisaation eri toiminnoille tarpeiden mukaan ja julkisuuteen ”tilan” ottamiseksi haltuun.

- Toimitusketjun toimijoiden välillä on sovittava laajemmin yhteisistä häiriötilannetoimintamalleista. Toipumissuunnitelmia on kehitettävä ja testattava.

- Huoltovarmuusorganisaation ja Huoltovarmuuskeskuksen rooli ja vastuut häiriö- ja poikkeusoloissa on syytä jatkossa nostaa esiin harjoituksessa.

- HVK:n, HVO sihteereiden ja viranomaisten yhteistoimintaa häiriötilanteissa on hyvä harjoitella ja harjoituttaa elinkeinoelämää jatkossa harjoitellun mallin osana.

- Elinkeinoelämän ja viranomaisten yhteistoimintaa tulee harjoitella yhä enemmän myös kansainvälisesti.

Hyvin varautuneen organisaation tulee siis huomioida paljon asioita häiriötilanteista selvitäkseen, mutta huomioimalla näitä pääsee jo varsin pitkälle. Ja muistetaan, että laajojen häiriöiden ollessa kyseessä on verkostossa voimaa.

Kirjoittajaesittely

Antti Nyqvist

Valmiuspäällikkö, Huoltovarmuusorganisaation Digipoolin pääsihteeri Teknologiateollisuus ry:ssä.

HVO Digipooli on ICT-alan yritysten verkosto, joka toiminnallaan tukee yritysten kokonaisturvallisuuden kehitystä erityisesti digitaalisen turvallisuuden aiheissa. Antilla on pitkä yritysmaailman kokemus ohjelmistoprojektien ja palveluliiketoiminnan parista, projekteista sekä liiketoimintayksikön johtotehtävistä.

Kirjoittaja majuri Matti Kauppila työskentelee Kainuun prikaatissa operatiivisella osastolla johtamisjärjestelmäsektorin johtajana.

TEKSTI: MATTI KAUPPILA

Kansainvälinen yhteistoiminta johtamisjärjestelmäalan näkökulmasta

Christopher Mewettin kirjoituksessa Understanding War's Enduring Nature Alongside its Changing Character sanotaan, että "sotilaallisena dogmana on, että sodan luonne ei muutu koskaan, vain se, kuinka suoritamme sen kohtalokkaat rituaalit. Sodankäynnin toimialueet, joilla nämä teot ilmenevät, ovat pysyneet määriteltyinä ja ymmärrettyinä läpi historian – maa, meri, ilma – lisäksi erityisesti viime aikoina – avaruus ja kyberavaruus."

Johtamisjärjestelmän käyttöön ei liity rituaaleja, vain taito ja osaaminen ratkaista mitä johtamisjärjestelmää tai johtamislaitetta käytetään missäkin taistelun vaiheessa, kuka sitä käyttää ja mitä sillä halutaan saavuttaa. Yksinkertaista, mutta ajoittain varsin haastavaa sillä kaikki odottavat, että "kaikki yhteydet ja palvelut" toimivat. Meillä on kansainvälisen yhteistoiminnan lisääntymisen myötä käsillä yksinkertaisia, mutta toisaalta haastavia tehtäviä ratkaistavana ja harjoiteltavana. Kuinka sovittaa yhteen eri maiden johtamisjärjestelmät niin, että voimme priorisoida käytössämme olevat resurssit järkevästi ja kustannustehokkaasti.

Johtamisjärjestelmän rakentamisen ja käytettävyyden kitkaa aiheuttavat pääsääntöisesti käyttäjät itse. Siksi on edelleen tärkeää tiedostaa, että johtamisjärjestelmän rakentamisessa noudatetaan jo varusmiespalvelusaikana opetettuja periaatteita: takaa eteen, vasemmalta oikealle, ylhäältä alas ja aluevastuussa olevasta alueelle tulevaan. Näiden periaatteiden jalostaminen kansainvälisessä yhteistoiminnassa on tärkeää. Liittolaisten tulee tietää miten ja millä periaatteilla toisten maiden kansalliset järjestelmät rakennetaan ja mitä palveluita ne sisältävät. Integroitumisen merkitys ja kielitaidon karttuminen korostuu aina miehistöstä upseeristoon saakka. Tämä oli yksi keskeisimmistä asioista esimerkiksi Nordic Response 24 -harjoituksessa, jossa yhteistoimintaa harjoiteltiin käytännössä.

NORDIC RESPONSE 24 -harjoitus johtamisjärjestelmän rakentamisen näkökulmasta

Taistelukentän tärkeimmät elementit ovat edelleen tuli ja liike. Nämä elementit aikautetaan ja sovitetaan yhteen johtamisjärjestelmän avulla. Lisäksi johtamisjärjestelmän yksi keskeisimmistä tavoitteista nykypäivänä on, että taistelun elementit (WfF, War fighting functions) pystytään ottamaan huomioon, kun operaatioverkon sekä taktisen verkon suunnittelua tehdään eri toimijoiden kesken. Natoon liittymisen myötä taistelun elementtien yhteensovittaminen astui uutena kokonaisuutena myös johtamisjärjestelmäalan suunnittelun ja toteutuksen kokonaisuuteen. Kokonaisuus muodostuu seitsemästä elementistä, jotka ovat englanniksi command and control (C2), fires, protection, information, intelligence, logistics sekä movement&maneuver. Lisäksi käsite P.A.C.E (Primary, Alternative, Contingency, Emergency) nousi merkittävänä osana mukaan johtamisjärjestelmän suunnitteluun.

P.A.C.E tarkoittaa yhteyksien tai palveluiden käytettävyyden tärkeysjärjestystä. Tällä pystytään selkeästi erottelemaan eri toimijoiden välillä ne keskeisimmät laitteet ja järjestelmät, jotka on priorisoitu käytettävyyden mukaan eri taistelujen vaiheeseen sitoen. Taistelun elementtien tarkoituksena on turvata ja taata kaikki käytössä olevat kriittiset kyvyt komentajan, esikunnan ja alajohtoportaiden tueksi taistelukentällä. P.A.C.E tukee näiden tavoitteiden saavuttamista.

Nordic Response (NR) -harjoituksessa keväällä 2024 rakennetussa operaatioverkossa käytettiin kaikkien harjoitukseen osallistuneiden maiden yhteensopivia johtamisjärjestelmiä. Tilannekuva muodostettiin yhtenäiseksi koko johtoportaan osalta. Kaikki liittolaiset ja kumppanit olivat käytännössä kiinni samassa verkossa. Jokainen osallistuva maa rakensi ja ylläpiti omat sisäiset johtamisjärjestelmänsä. Järjestelmien käytettävyyttä, haasteita, onnistumisia ja kehitettäviä kokonaisuuksia käsiteltiin useissa kokouksissa yhteisen taistelurytmin mukaisesti. Olemassa olevat yhteiset standardit mahdollistivat ja mahdollistavat edelleen järjestelmien yhteensopivuuden.

Puolustusvoimien Johtamisjärjestelmäkeskus (PVJJK) järjesti kansainväliset yhteydet Suomeen ja vastasi yhteyksien toteuttamisesta kansallisille joukoille. Lisäksi PVJJK vastasi järjestelmien ylläpidosta. Taktisella tasolla johtoportaiden johtamisjärjestelmäalan avainhenkilöt vastasivat teknisten yksityiskohtien yhteensovittamisesta taistelurytmiin sopivaksi. NR24 ei kuitenkaan ollut laatuaan ensimmäinen harjoitus, jossa harjoittelua tehtiin, sillä esimerkiksi vuonna 2019 Bold Quest -harjoituksessa tehtiin merkittävää testaustoimintaa eri maiden välillä.

Kansainväliseen harjoitteluun liittyen maavoimien omien orgaanisten joukkojen tulee huomioida paikallisesti, että kansainvälisten joukkojen liittämistarpeet ja rajapinnat otetaan huomioon suunnittelussa. Kyseessä on erittäin mielenkiintoinen kokonaisuus, jossa yhteistoiminta tarkoittaa molempien yhteistoimintapuolten järjestelmien ja niiden käyttöperiaatteiden tuntemista.

Kansainvälisten harjoitusten suunnitteluprosessi eri toimijoiden välillä

Käytössä olevalla johtamisjärjestelmällä on suora vaikutus joukon tapaan taistella. Tilannekuvan laatu ja tulenkäyttö ovat riippuvaisia johtamisjärjestelmän suorituskyvystä. Johtamisjärjestelmän osalta suunnittelun käynnistämisvaiheessa tarkoituksena on määrittää johtamisjärjestelmän rakentamiselle vaatimukset ja rajoitukset, sekä antaa yleiset suunnitteluperusteet kansainvälisille toimijoille. Johtamisjärjestelmän suunnittelun näkökulmasta keskeisin yhteensovitettava asia on johtamisjärjestelmien rajapintojen muodostamisen toteutus taktisella tasolla. Keskeistä on tunnistaa kriittiset reunaehdot ja kansainvälisten toimijoiden johtamisjärjestelmäkaluston toimintamahdollisuudet. Lisäksi tulee tunnistaa ne suorituskyvyt, jotka lisäävät molempien osapuolten toimintakykyä taistelukentällä menestymisessä. Siksi on tärkeää tuntea liittoutuneiden kalusto ja kuinka sitä käytetään.

Viestiasema revontulien äärellä Lapin erämaassa (Kuvaaja Tiia Impiö)

Onpa kyseessä liittäminen langattomasti tai langallisesti, tulee se huomioida omassa suunnitteluprosessissa. Kansainvälinen yhteensopivuus on ymmärrettävä toisaalta myös yhteentoimivuutena (interoperability) 24/7. Meidän on ymmärrettävä, että nykyaikana on kyettävä toimimaan ja johtamaan joukkoja nopeasti ilman ennakkovaroitusta. Johtamisen ja kansainvälisen toiminnan näkökulmasta on keskeistä, että kykenemme muodostamaan ajantasaisen tilannekuvan ja johtamaan omia suorituskykyjämme. Siksi on tärkeää harjoitella aktiivisesti niitä toimintatapoja, jotka tukevat menestymistä taistelukentällä.

Suunnitteluprosessin edetessä tulee molempien osapuolten ymmärtää vähintään seuraavat asiat; harjoitusten tavoite ja sen edellyttämä operatiivinen/taktinen tehtävä, toiminnan päämäärä ja loppuasetelma, harjoituksen operaatioajatus, suunnittelulle asetetut reunaehdot ja oletukset, alajohtoportaiden toiminta ja liikesuunnitelma operaation aikana sekä onnistumisen edellytykset. Johtamisjärjestelmä tulee rakentaa niin, että se mahdollistaa nopean suunnittelun ja toimeenpanon. Toimintaympäristö ei saa asettaa rajoituksia johtamisjärjestelmän rakentumiselle, ja sen tulee mukautua liittoutuneiden asettamiin vaatimuksiin. Kokonaisuuden tulee olla kaikissa tilanteissa taistelunkestävä ja vastata molempien toimijoiden tarpeisiin. Tiedonsiirrossa hyödynnetään eri mahdollisuuksia riippuen siitä mitä kalustoa halutaan käyttää.

Mikäli liittoutuneet joukot käyttävät harjoituksessa toistensa kansallisia johtamisjärjestelmiä sen edellytyksenä on, että käyttäjänä on lähtökohtaisesti laitteen hallinnoija. Välttämättä ei tarvitse tietää mitä järjestelmää käytetään, mutta tulee ymmärtää järjestelmän tietotarpeet, formaatit ja käytettävät standardit. Esimerkiksi miten ja minne tietoa kerätään ja mitä varten.

Vaikka kansainvälinen yhteistoiminta johtamisjärjestelmän testaamisen, valmistelun, suunnittelun, yhteensovittamisen, rakentamisen, ylläpidon ja huollon osalta vaatii monelta eri toimijalta oman panoksensa, voisin silti varsin luontevasti kiteyttää edellä kirjoittamani kokonaisuuden seuraavaan Nils Marius Rekkedalin teoksen *Nykyaikainen sotataito: sotilaallinen voima murroksessa* lauseeseen:

”Ratkaiseva tekijä taisteluissa, teknologiasta ja aseista riippumatta on yksittäinen sotilas”!

TEKSTI: OUTI TUISKU

Haastattelussa Traficomin Kyberturvallisuuskeskuksen ylijohtaja Anssi Kärkkäinen

Insinöörieverstiluutnantti (evp), TkT, DI Anssi Kärkkäinen nimitettiin Traficomin Kyberturvallisuuskeskuksen (KTK) ylijohtajaksi 4.3.2024. Millaisten mutkien kautta Anssi on päätynyt nykyiseen tehtäväänsä ja mitä kaikkea KTK:n johtajan ensimmäiseen toimintavuoteen on mahtunut? Muun muassa näihin ja moniin muihin kysymyksiin saadaan vastaus VM-lehden henkilökuvassa.

Mistä olet kotoisin?

Olen kotoisin Oulun seudulta. Kadettikoulun aloitus vuonna 1996 toi minut etelään.

Millainen on opiskelutaustasi sekä uran kehitys ja tehtävät Puolustusvoimissa?

Kadettikoulun aloitin 1996 ja valmistuin vuonna 2000 viestilinjalta, jonka jälkeen palvelukseen Viestirykmenttiin varusmiehiä kouluttamaan. Aloitin myös DI-opinnot työnohessa silloisessa TKK:ssa Otaniemessä heti palveluksen aloittamisen jälkeen ja valmistuin alkuvuodesta 2005.

Vuonna 2005 siirryin Viestikoulun tutkimus- ja kehittämisosastolle tutkijaesiupseeriksi, josta joulukuussa 2006 silloiselle Pääesikunnan Maavoimaesikunnan materiaaliosastolle osastoesiupseeriksi vastuualueena maavoimien viestiaselajin materiaalihankkeiden edistäminen.

Maavoimaesikunnan siirtyessä Mikkeliin vuoden 2007 loppupuolella siirryin Pääesikunnan johtamisjärjestelmäosastolle (J6) osastoesiupseeriksi. Tehtävään kuului muun muassa TUVE-, TACOMS- ja TISO-projektit. Vuonna 2011 perustettiin J6:lle kyberpuolustussektori, jossa aloitin ensimmäisten joukossa. Esiupseerikurssin kävin 2010–2011 ja yleisesikuntaupseerikurssin 2012–2013.

Seuraavaksi siirryin vuoden 2015 alussa perustetun Puolustusvoimien johtamisjärjestelmäkeskuksen (PVJJK) kyberosaston ensimmäiseksi osastopäälliköksi ja tästä tehtävästä palasin kahden ja puolen vuoden jälkeen Pääesikuntaan J6:lle vastuualueena kehittämisohjelman koordinointi. Siirryin yksityiselle sektorille marraskuussa 2017. Olin aloittanut jatko-opinnot vuonna 2006 ja väittelin tekniikan tohtoriksi Aalto-yliopistossa syksyllä 2015.

Miten viihdyit Puolustusvoimissa?

Viihdyin Puolustusvoimissa erinomaisesti. Sain olla mukana mielenkiintoisissa asioissa, kuten TUVE-hanke, ensimmäiset kyberpuolen Nato-projektit ja kyberosaston käynnistäminen. Sain tehdä työtä myös hienojen työkavereiden kanssa. Päivääkään en vaihtaisi pois.

Millainen työpaikka Puolustusvoimat on ollut verrattuna muihin työnantajiin, joissa olet työskennellyt?

Puolustusvoimat on ollut hyvä työpaikka, toki erilainen kuin yritys tai Traficom. Sotilasorganisaatio tuo tietysti oman jäykkyytensä toimintaan, mutta toisaalta prosessit ja käytänteet ovat usein huomattavasti selkeämmät kuin muualla. Byrokratiaa ja hierarkiaa on enemmän, mutta sillä on tietysti oma tarkoituksensa sotilasorganisaatiossa. Isoin ero on asiakirjojen määrässä, joita tarvitaan vaikkapa jonkin uuden asian aikaansaamiseksi. Yrityksessä riittää melkeinpä puhelin soitto tai sähköposti.

Päivittäinen työ ei sinällään eroa; esimies asettaa tavoitteet, joita kohti sitten ponnistellaan.

Millaisia muistoja sinulla on työuran varrelta Puolustusvoimissa? Mitkä palvelusurasi tehtävät tai projektit ovat olleet kaikkein mielenkiintoisimpia tai haastaneet eniten?

Hienoja hetkiä on ollut paljon. Tulee mieleen esimerkiksi se, kun ensi kerran saimme Internet-yhteyden tuotua taktisella tiedonsiirrolla maastoon Riihimäen lähialueella. Mielenkiintoisimpia projekteja olivat Naton tietoliikenteen standardointiprojekti TACOMS, jossa monikansallisesti yritettiin saada rajapintaa standardisoitua.

Haastavista tulee mieleen TUVE-hanke, johon liittyi vahvaa hallinnonalojen välistä vääntöä hankeen sisällöstä ja rahojen käytöstä. Myös kyberosaston käynnistämiseen liittyi omat haasteensa, mutta enemmän siitä on jäänyt mieleen

positiivinen yritys osaston kehittämisessä.

Mieleen on tietysti jäänyt se hetki, kun piti valita suuntautuminen kyberpuolustuksen alalle. Tämä tapahtui kesällä 2011 kun silloinen J6 AOP Mikko Heiskanen kysyi, haluanko tehdä töitä tietoliikenteen vai kyberin parissa. Pari millisekuntia mietin ja vastasin, että kyber. Kiitos Mikolle mahdollisuuden antamisesta!

Miten päädyit töihin KTK:lle?

Työskentelin Cinia Oy:ssä kyberliiketoiminnan rakentajana ja vetäjänä 2017–2023. Vuoden 2023 keväällä hyppäsin mukaan startup-yritykseen, josta kuitenkin jäin pois tammikuussa 2024 ja huomasin, että Traficom hakee Kyberturvallisuuskeskukselle vetäjää. Ajattelin, että pitkä ja monipuolinen kokemus kyberpuolustuksen ja -turvallisuuden parista sekä julkisella että yksityisellä puolella voisi olla hyvä yhdistelmä tehtävään. KTK oli myös tuttu toimija mm. PV:n ajoilta ja siellä oli monta tuttua kasvoa, joten päätin hakea.

Miten näet, mitkä ovat vahvuutesi KTK:n tehtävässäsi?

Uskon, että laaja kokemus sekä sotilas- että siviilipuolen kyberasioissa on synnyttänyt ainutlaatuista kompetenssia kybersuorituskykyjen kehittämiseen ja asiantuntijaorganisaation johtamiseen. Ymmärrystä on kehittynyt niin teknisestä kuin operatiivisesta ja strategisestakin tasosta.

Vuosien varrella muodostunut laaja verkosto ja eri toimijoiden tunteminen auttaa myös tehtävän hoitamisessa.

Mitkä arvot ohjaavat toimintaasi KTK:n ylijohtajana?

Vastuullisuus, luottamus ja yhteistyö. *Vastuullisuus* tarkoittaa oman roolin hoitamista tinkimättä, mihin kuuluu mm. huolehtiminen sääntöjenmukaisuudesta, taloudellinen vastuu ja vastuu hyvinvoinnista ja työilmapiirin kehittämisestä. *Luottamus* on taas ansaittava pitämällä lupaukset, liittyivätpä ne sitten vaikkapa kollegalle luvattuun työtehtävään tai tiedonvaihtoon eri toimijoiden välillä. Kansallinen kyberturvallisuuden tilannekuvan muodostaminen ei olisi mahdollista ilman luottamusta, koska valtaosa tiedosta, mitä saamme, on vapaaehtoisesti ja luottamuksella meille jaettua olipa tiedonjakaja sitten yksityinen yritys, kansalainen tai toinen viranomainen. *Yhteistyö* on tärkeää sekä yksilötasolla että organisaatiotasolla. Kyberturvallisuuden ja -puolustuksen haasteet taklataan vain tiiviillä yhteistyöllä. Yhteistyö viranomaisten ja yksityisen sektorin kesken on ainutlaatuista, kun sitä vertaa vaikkapa muihin Euroopan maihin.

Traficom on vastikään julkaissut uuden strategian, joka painottaa ennakointia ja muutoskyvykkyyttä. Miten KTK:lla ylläpidetään osaamista, jotta teillä pystytään vastaamaan strategian toteuttamiseen, kun puhutaan johtamisjärjestelmistä ja kybertoiminnasta (onko teillä esim. omaa koulutustarjontaa)?

Ennakointi- ja muutoskyvykkyys lähtee henkilöstöstä ja sen osaamisesta ja asenteesta. Muutosmyönteisen kulttuurin luominen on pitkäjänteistä toimintaa ja lähtökohdat siihen ovat hyvät. Henkilöstö ymmärtää muutoksen vääjäämättömyyden varsinkin teknologisella alalla.

Pyrimme kehittämään osaamista entistä suunnitelmallisemmin. Osaamista kehitetään ulkoisia ja sisäisiä koulutuspalveluja käyttämällä. Myös vertaisilta oppiminen on tärkeää.

Osaamisen osalta meitä tulee haastamaan mm. pilven turvallisuus ja tekoäly kokonaisuudessaan. Näillä alueilla on kehitettävä osaamista, jotta pystytään vastaamaan niistä nouseviin uhkiin.

Miten Nato-jäsenyys on vaikuttanut KTK:n toimintaan? Näkyykö se esim. strategiassa tai toimintamalleissa jollain tavalla?

Nato-jäsenyys on näkynyt vielä enemmän osallistumisena eri työryhmiin, mitä on koordinoitu yhdessä Puolustusvoimien kanssa. Lisäksi on ollut kasvava tarve Nato-järjestelmien auditoinneille. Myös kriittisen infran resilienssin osalta on vahvoja Nato-kytköksiä.

Miten näet Suomen Nato-jäsenyyden vaikuttavan virastojen väliseen yhteistoimintaan kybertoiminnallisuuksien osalta niin lyhyellä kuin pitkällä aikavälillä?

Uskon, että Nato-jäsenyys tulee lisäämään yhteistoimintatarvetta sekä lyhyellä että pitkällä aikavälillä. Sekä kansallinen kyberpuolustus että Naton kyberkyvykkyys kehittyy ja osana sitä tarve siviili–sotilas-yhteistyölle lisääntyy. Digitaalisen infran suojaaminen ja kyberuhkien torjuminen on yhä enemmän yhteistyötä kaikkien viranomaisten ja yrityskentän kesken. Tarvitaan enemmän tiedon jakamista uhkiin, osaamiseen ja teknologiaan liittyen.

Millaisia haasteita työssäsi kohtaat? Mistä työssäsi pidät erityisesti?

Haasteena on kyky palvella kaikkia sidosryhmiä kyberturvallisuuden saralla. Valtionhallinnon säästöohjelma koskettaa myös Kyberturvallisuuskeskusta, mikä rajoittaa mahdollisuuksia resursoida kaikkiin nykyisiin ja tuleviin tehtäviin tasapuolisesti. Joudumme pohtimaan toiminnan painopisteitä ja tekemisen tasoa. Omassa roolissani pyrin lisäämään ymmärrystä keskuksen merkityksessä kansallisen kyberturvallisuuden kehittämisessä ja uhkien torjunnassa ja sitä kautta varmistamaan, että keskuksella on riittävä rahoitus myös tulevina vuosina.

Erityisen hienoa on tehdä päivittäin työtä noin 200 rautaisen kyberammattilaisen kanssa. Meillä on paljon valtakunnan parasta osaamista, jolla pystymme tukemaan sidosryhmiä eri kokonaisuuksiin liittyen. Hienoa on myös nähdä keskuksen tekemä laaja-alainen työ kyberturvallisuuden eri alueilla tilannekuvasta auditointeihin ja sääntelyn toimeenpanosta EU-rahoitustukeen. Kansallisen tilannekuvan tuottamisessa olemme ainutlaatuinen virasto.

Millaisten harrastusten parissa viihdyt vapaa-ajalla?

Talvisin tulee viihdyttyä hiihtoladulla ja kesäisin ainakin Jukolan viesti on ohjelmassa sekä joku polkujuoksutapahtuma.

Haluatko sanoa vielä jotain haastattelun päätteeksi?

Olen saanut tehdä työtä kyberpuolustuksen parissa yli 15 vuotta ja vaikka olen työskennellyt sekä siviili- ja sotilaspuolella ja julkishallinnossa ja yksityisellä, päämäärä on aina ollut sama: yhteiskunnan suojaaminen kyberuhkia vastaan ja kyberturvallisuustason parantaminen.

Kyberturvallisuuskeskuksen sisältöön pääset tutustumaan osoitteessa https://www.kyberturvallisuuskeskus.fi

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

AI-perustainen kyberturvallisuus

Keinoälyä käytetään yhä enemmän kyberuhkien ennustamiseen, havaitsemiseen ja niihin vastaamiseen. Keinoälypohjaiset kyberturvallisuustyökalut voivat auttaa puolustamaan sotilasverkkoja edistyneitä hyökkäyksiä vastaan, mahdollistaen uhkien aiempaa tehokkaamman todentamisen ja asianmukaiset vastatoimenpiteet. Keinoälyn pohjalla olevat koneoppimisalgoritmit voivat mukautua kehittyviin uhkiin ja havaita tunkeutumismalleja, mikä tekee näistä työkaluista välttämättömiä niin maanpuolustukselle kuin sotilasoperaatioille olennaisten viestintä- ja komentojärjestelmien suojaamisessa. Tämä artikkeli esittää näkökohtia ja esimerkkejä puolustusjärjestelmien ja verkkojen suojaukseen keinoälyn avulla.

Keinoälyn käsitteitä

Keinoäly on vahvasti kehittyvä tekniikan alue, joka näkyy nykyään päivittäisessä elämässä niin käytettävissä olevien sovellusten kuin markkinauutisten kautta. Keinoäly eli artificial intelligence (AI) tarkoittaa ihmisen älykkyyden simulointia koneilla tai laitteilla, jotka on ohjelmoitu miettimään, järkeilemään, oppimaan ja ratkaisemaan ongelmia. AI mahdollistaa tietokone- ja järjestelmäpohjaisen tehtävien suorituksen, joka tyypillisesti vaatii ihmisälyä esimerkiksi päätöksenteossa, kielten ymmärtämisessä, asioiden tulkinnassa ja kuvioiden hahmottamisessa.

Keinoäly voidaan jaotella **kapeakaistaiseen** ja **yleiseen** kategoriaan. Kapeakaistainen AI (”narrow AI” tai ”weak AI”) on suunniteltu suorittamaan kohdennettuja tehtäviä. Esimerkkejä tästä kategoriasta ovat keskustelupalvelut (chatbotit) ja erilaiset järjestelmät, jotka kykenevät suosittelemaan eri vaihtoehdoista tilanteeseen sopivimpia. Yleinen AI (”general AI” tai ”strong AI”) on puolestaan edellistä kehittyneempi ja monimuotoisempi malli, joka sisältää ihmisten tapaan kognitiivisia kyvykkyyksiä. Kognitio tarkoittaa ihmisen älyllisiä ja psykologisia toimintoja, joiden avulla voidaan käsitellä tietoa ja ympäristöään; kognitiivinen toiminta on siten monimutkaista tiedon käsittelyä hahmottaen ja suorittaen vaativia tehtäviä. Tämä periaate kehitettynä datan prosessointina mahdollistaa AI:n kyvyn suorittaa inhimillisiä älyllisiä tehtäviä.

Koneoppiminen (machine learning, ML) on AI:n osajoukko, joka perustuu kehittyviin algoritmeihin. Nämä algoritmit mahdollistavat tietokoneiden oppimisen, ennustamisen ja päätöksenteon käytettävissä olevaan tietoaineistoon perustuen siten, että tietokoneita ei tarvitse varta vasten ohjelmoida kyseisiin toimiin. Yleisperiaatteena ML-mallien suorituskyky paranee ajan myötä samalla, kun ne prosessoivat enemmän tietoa. Alustava ML-mallin oppiminen on avainasemassa sen ”järkevään” toimintaan – epäpätevästi opetettu malli heikolla algoritmilla tai huonolla opetusdatalla voi aiheuttaa enemmän harmia kuin hyötyä. ML-mallin epäoptimaalisesta opetusjaksosta voi aiheutua materiaalista tai pahimmillaan jopa terveyttä uhkaavia tilanteita esimerkiksi mallien heikoissa käyttöönotoissa terveydenhoidossa. [1]

ML-tekniikat sisältävät seuraavia komponentteja: 1) **valvottu oppiminen**, jossa oppimismallit pohjautuvat merkittyyn dataan, 2) valvomaton eli **itsenäinen oppiminen**, jossa etsitään toistuvuutta merkitsemättömästä datasta ja 3) **vahvistettu oppiminen**, jossa oppiminen tapahtuu yrityksen ja erehdyksen kautta ja joka perustuu palkitsemiseen. Koneoppimista sovelletaan nykyään yhä laajenevassa määrin mitä erilaisimmissa sovelluksissa esimerkiksi petosten havaitsemiseen, puheentunnistukseen ja autonomisten järjestelmien toimintoihin.

Terminologiasta ”hyökkäys”, joka tulkitaan yleensä tietoturvauhkaksi, voi johtaa turvallisuushaasteisiin tai päinvastoin. Esimerkkinä tästä on malli, joka tuottaa haitallista sisältöä tai paljastaa luottamuksellista henkilökohtaista tietoa. Voidaan todeta, että *keinoälyn tietoturvan* ja *turvallisuuden* risteyskohta korostaa tarvetta kattavaan keinoälyn *riskienhallintaan*, jossa käsitellään sekä tietoturvaan että turvallisuuteen liittyviä huolia samanaikaisesti.

Toisin sanoen, keinoälyn tietoturva (security) ja turvallisuus (safety) ovat kaksi eri asiaa, mutta ne liittyvät käsitteinä toisiinsa. Tietoturva viittaa siihen, kuinka hyvin keinoälyjärjestelmä on suojattu ulkoisilta ja sisäisiltä uhilta, kuten haitalliselta hakkeroinnilta, tietomurroilta tai haittaohjelmilta. Turvallisuus puolestaan tarkoittaa sitä, kuinka hyvin keinoälyjärjestelmä toimii ilman, että se aiheuttaa vahinkoa ihmisille, ympäristölle tai keinoälylle itselleen esimerkiksi virheellisten päätösten tai hallitsemattoman käyttäytymisen vuoksi. Tämän kahtiajaon ydinajatus on, että kyseiset näkökulmat tulee huomioida samanaikaisesti ja että kumpaakaan ei saa tarkastella erillisenä ongelmana. Tämä vaatii kattavaa lähestymistapaa tekoälyn riskienhallintaan, jossa tunnistetaan ja ehkäistään sekä tietoturvariskit että turvallisuusriskit. [2]

Keinoäly maanpuolustuksessa

Modernissa nopeasti kehittyvässä ympäristössä maanpuolustus on murrosvai-

heessa yhä sofistikoituneempien kyberuhkien mahdollistaessa täysin uusia hyökkäysmenetelmiä. AI on käyttökelpoinen työkalu ennustamaan, valvomaan ja ehkäisemään uhkia, joten AI:n sisällyttäminen kyberturvallisuuden strategioihin on jo oleellinen elementti maanpuolustuksessa. On huomattavaa, että AI on yhä käyttökelpoisempi komponentti suojaustyökalupakissa, mutta siihen tukeutuminen tulisi olla täydentävää, ei kokonaan korvaavaa, sillä AI voi myös erehtyä siinä missä ihmisetkin.

Joka tapauksessa, osana nykyaikaista puolustusstrategiaa, ML-algoritmit AI:n alajoukkona mahdollistavat mukautuvia toimintoja ja kyvykkyyksiä, joiden avulla on mahdollista havaita nopeasti tiedostettuja ja ennalta tuntemattomia tietoliikennejärjestelmien ja -verkkojen hyökkäysvektoreita ja suojautua riittävän ajoissa hyökkäysten aiheuttamilta vahingoilta esimerkiksi sotilasverkoissa ja komentojärjestelmissä.

Maanpuolustuksen heikkouksia

Moderni sotilaallinen ympäristö on vahvasti riippuvainen yhteen liitetyistä verkoista ja kehittyneistä verkkoteknologioista. Modernit verkot ja järjestelmät parantavat puolustus- ja operointikyvykkyyttä, mutta ne avaavat samalla laajoja vastustajien hyökkäysmahdollisuuksia siksi että niiden kaikkia uusia haavoittuvuuksia ei ole ehkä pystytty tutkimaan. Toisaalta aiempien järjestelmien ja verkkojen jatkuva tuki uudempien ratkaisujen rinnalla voi aiheuttaa haasteita vanhentuvine tekniikoineen ja heikkenevine suojauksineen. Ongelma on verrattavissa kuluttajamarkkinoiden haasteisiin uusien tietokoneiden hallintajärjestelmien korvatessa vanhoja siten, että jälkimmäisten suojaustaso heikkenee tietoturvapäivitysten päättyessä. On huomattavaa, että maanpuolustuksen laiteinvestoinnit ovat usein pitkäjänteisiä ja siten vanhaakin kalustoa niiden heikentyvine suojaustasoineen saattaa jäädä käyttöön modernien ratkaisujen rinnalle niitä täydentämään.

Toinen merkittävä haaste on monimutkainen laitteiden toimitusketju. Nykyiset elektroniikkalaitteet ja tietoliikennejärjestelmät ovat yhä monipuolisempia ja kyvykkäämpiä, ja niiden kehitykseen ja valmistukseen saattaa liittyä niin suuri joukko yrityksiä alihankkijoineen, että kaikkien toimijoitten todellisia tarkoituksia on mahdotonta varmistaa. Laitteiden tietoturvallisuus saattaa tämän myötä heikentyä. Esimerkkejä tästä ongelmasta löytyy runsaasti, kuten uutiset laitteisiin asennetuista dokumentoimattomista takaporteista tai käyttäjien tietämättä laitteista tai sovelluksista lähetettävä data ulkopuolisille tahoille osoittavat. [3] On selvää, että tällaisten haavoittuvuuksien kautta myös vihollinen voi päästä käsiksi kriittisiin maanpuolustusjärjestelmiin.

Kolmas merkittävä tietoturvan uhka – ellei merkittävin – ovat sisäpiirissä olevat huijarit, joko tahtomattaan tai tarkoituksellisesti. Esimerkiksi kriittistä infrastruktuuria operoivan tai erikoislaitteita valmistavan yrityksen yksittäisellä henkilöllä, jolla on motiivi pahantekoon, saattaa olla pahimmassa tapauksessa tarpeettoman laaja pääsy järjestelmiin, laitekomponentteihin tai piirikytkentäkaavioihin, ja kyky vaarantaa niiden kautta tietoturvallisuuden tason monella tavalla muiden huomaamatta.

Neljäntenä uhkana on nopea uusien teknologioiden integrointi, joka nykyisessä varsin hektisessä liiketoiminnassa saattaa vaarantaa tietoturvallisuuden riittävän tason varmennuksen ja testauksen, jättäen tietoturva-aukkoja, jotka mahdollistavat täysin uusia hyökkäysmenetelmiä.

Lisätietoja nykyisistä uhkakuvista, statistiikasta ja suojautumisohjeista on saatavissa esimerkiksi Verizon julkaisemasta vuosittaisesta raportista. [3]

Kyberuhkien malleja

Kyberuhkien kenttä on hyvin laaja ja dynaaminen. Uusien yhä kehittyneempien hyökkäysmallien vuoksi niihin varautuminen on yhä haastavampaa perinteisin puolustusmenetelmin. Esimerkki tyypillisistä kyberhyökkäyksistä on kehittynyt systemaattinen uhka (advanced persistent threat, APT), joka on pitkäaikainen, kohdennettu kyberhyökkäys, tyypillisesti taidokkaan erillisryhmän tekemänä, tarkoin harkittuna ja kohdennettuna, ja yleensä valtion sponsoroimana. Kohteena voivat olla yritykset tai yksityishenkilöt, joiden kautta voi esimerkiksi pyrkiä saamaan pääsyn valtionsalaisuuksiin, taloudellisesti merkittäviin muihin tietoihin, tai haittaamaan yleisesti operaatiota tai valtioiden laillista järjestystä.

Toinen vahvasti kasvava kyberuhkan laji on kiristysohjelmat (ransomware), eli haitakkeet, jotka salaavat datan, tuhoavat alkuperäisen datan, ja vaativat maksun datan palauttamiseen. Kiristysohjelmat ovat luoneet kokonaisen rikollisen palveluekosysteeminsä, jossa toimijat kehittävät haittakoodien tuotanto- ja jakeluketjut käyttöohjeineen, joten käytännössä tietämättömyys tekniikoiden yksityiskohdista ei nykyisissä uhkakuvissa estä haittaohjelmien käyttöä nk. ”avaimet käteen” periaatteella omana palvelunaan. Pidemmälle kehittyneessä AI-pohjaisessa kiristyshyökkäyksessä haittaohjelma voi AI:n avustamana identifioida automaattisesti järjestelmien ja sovellusten heikkouksia, suunnitella hyökkäyksiä, ja mukautua suojaustoimien väistämiseen reaaliaikaisesti. [4] Tämä on kenties yksi pahimmista uhkakuvista orastavalla AI-aikakaudella.

Rikolliset tahot voivat myös pyrkiä käyttämään AI:ta toimitusketjuhyökkäyksiin kohdentaen hyökkäyksiä kolmansien osapuolten luottamuksellisiin tietoihin tai ohjelmistopäivityksiin, joiden kautta rikolliset voivat saada pääsyn edelleen uusiin kohteisiin.

AI:n käyttö väärennettyjen videoiden ja audion luonnissa (deepfake) on kasvanut vahvasti viime aikoina. AI:n kehittyvää alkuperäisen sisällöntuoton ”matkintakyvykkyyttä” voidaan käyttää – ja on jo käytetty – disinformaatiokampanjoissa. AI:n tuottama sisältö reaaliajassa yhä parempilaatuisena on jo aiheuttanut hämminkiä, oli kyseessä ulkopuolisten toimijoiden vaikuttamisyritykset vaikkapa valtioiden sisäisessä poliittisessa ympäristössä (mielipiteiden manipulointi ja psykologiset vaikuttamisyritykset) tai yksityishenkilöiden huijaaminen taloudellisen hyödyn tavoittelussa. AI:n osuus rikollisen toiminnan jatkeena on jo selviö, ja AI:n kautta haittavaikutus voi ulottua laajalti yrityksissä, puolustusvoimissa, kuin yksityishenkilöiden elämässäkin.

Ei ole siis kaukaa haettua ajatella, että huijareiden AI:n avulla tekemiin hyökkäyksiin on syytä varautua yhä tehokkaimmilla AI-pohjaisilla analysointi- ja suojausmenetelmillä – olemme siis jo todistamassa eräänlaista keinoälyjen taistelua.

AI maanpuolustuksen kybersuojauksessa

Globaalilla tasolla AI on jo kasvavassa määrin puolustusvoimien eri sektoreiden käytössä kyberturvallisuuden vahvistamisessa. AI-pohjaisiin avainsovelluksiin kuuluvat mm. toimet poikkeavien tapahtumien tiedostamiseen verrattuna tyypilliseen ympäristöön. AI-järjestelmät voivat todentaa ja hälyttää poikkeavia tapahtumia huomattavasti manuaalista analysointia nopeammin ja tehokkaammin myös tilanteissa, joissa poikkeava data jää muutoin havaitsematta (tilanne on verrattavissa eräänlaiseen ”kohinatason” alapuoliseen monitorointiin), ja AI:n avulla voidaan korreloida dataa monipuolisesti reaaliajassa.

Kuten Redhat toteaa, AI-pohjainen tietoturvallisuus on toimiva menetelmä AI-järjestelmien riskien hallintaan. AI-pohjainen turvallisuus suojaa järjestelmiä ulkopuolisilta ja sisäisiltä uhkilta sillä aikaa, kun AI-pohjainen turvallisuusympäristö antaa käyttäjilleen luottamuksen siitä, että järjestelmä ja sen data eivät uhkaa yksilöitä, yhteiskuntaa tai ympäristöä mallien operaation, opetukseen tai käyttöön liittyen. Siitä huolimatta raja AI-pohjaisen turvallisuuden ja yleisen tietoturvan välillä on häilyvä. [2]

Keinoälyä voidaan soveltaa ennakoivaan analytiikkaan. Perustuen historiadataan, AI voi ennustaa tehokkaasti potentiaalisia hyökkäysvektoreita ennen kuin varsinainen hyökkäys edes ehtii alkaa, ja samalla varmistaa riittävän, mukautetun suojauksen ennalta käsin. Tämä pätee niin tietoliikenneverkkoihin, -järjestelmiin kuin kenttätilanteeseen. Jälkimmäisestä mainittakoon esimerkki keinoälyn hyödyntämisestä potentiaalisesti vahinkoa aiheuttavien lähestyvien droonien tunnistamisessa, ja vaadittavissa toimissa niiden etenemisen estämiseen kriittisillä alueilla.

Keinoälyä voidaan soveltaa myös automatisoituun vastaukseen esimerkiksi tietoliikenneverkoissa siten, että AI eristää järjestelmän haavoitetut segmentit ja estää hyökkäykseen käytetyn liikennöinnin. Automatisointi nopeuttaa huomattavasti hyökkäykseltä suojautumiseen vaadittavaa vasteaikaa silloin, kun hyökkäys on jo ehtinyt materialisoitua. ICT-ekosysteemi on jo huomannut AI:n hyödyt riskienhallinnassa maailmanlaajuisesti, ja tällä hetkellä noin kolme neljäsosaa yrityksistä priorisoi keinoälyn ja koneoppimisen tietohallintabudjeteissaan. Tärkeänä syynä tähän on nykyinen valtava tietomäärä, joka vaatii automaattisia analysointimenetelmiä tietoturvan tehokkaaseen suoritukseen.

Arvioiden mukaan tietoliikenneyhteyksiä käyttävien laitteiden data voi olla 79 zettatavua (yksikkö, joka vastaa informaation määrää 10^{21} eli 2^{70} tavua) vuonna 2025. Tällaista datamäärää on mahdotonta analysoida manuaalisesti, joten AI on looginen pohja kyberuhkiin varautumisessa. [5] AI toimii siis tukevana tekniikkana, joka voi yhdistää eri tietolähteitä, korreloida tietoa ja analysoida isoja määriä dataa, ja se mahdollistaa nopeita johtopäätöksiä päätöksenteon tueksi.

Tosielämän esimerkkejä kyberpuolustuksesta

Esimerkkinä monista markkinoilla jo olevista AI-pohjaisista palveluista Darktracen AI oppii organisaation käyttäjien, laitteiden ja verkkojen normaalin käyttäytymisen. Kun malli on kerran selvittänyt referenssiaktiviteetit, AI-algoritmi tutkii jatkuvasti normaaliliikenteen poikkeamia, jotka voivat olla mahdollisia kyberuhkia. Esimerkkinä, jos työntekijän laite alkaa ladata normaalia suurempia datamääriä tyypillisen työajan ulkopuolella, AI hälyttää epäilyttävästä toiminnasta. Darktracen AI-alusta toimii siten, että sen AI toteaa kyberuhkia ja vastaa niihin reaaliajassa. Darktrace on tämän toimintaperiaatteen kautta estänyt useita teollisuusyrityksiin kohdistuneita kyberhyökkäyksiä, ml. finanssilaitokset, sairaalat ja energia-ala.

Eräässä dokumentoidussa tapauksessa Darktracen AI paljasti ja neutralisoi kiristyshyökkäyksen, joka oli suunniteltu terveydenhuolto-organisaatioon. Kyseinen suojaustoimi tapahtui niin nopeasti, että hyökkäys ei ehtinyt edetä rikollisten suunnittelemaan vaiheeseen, jossa kriittinen pilvidata olisi salattu. Tämä esti taloudelliset tappiot, ja vielä tärkeämpänä seikkana, se suojasi myös mainehaitoilta. [6]

Toisena esimerkkinä voidaan mainita Yhdysvaltojen armeijan projekti ”Linchpin”. Kyseinen projekti on kehittänyt AI-pohjaisen alustan parantamaan kybersuojausta, koska keinoälyn odotetaan kasvattavan merkitystään Yhdysvaltojen armeijassa. AI:n avainhyötynä on kehittynyt kyberpuolustus, ja se mahdollistaa esimerkiksi ihmisten ja robottien yhteistyön ja siten uuden sukupolven komento- ja kontrollimenetelmät (command & control). Projekti Linchpin on rakennettu nopeuttamaan ja laajentamaan AI:n käyttöä armeijan tarpeisiin, ml. taktiset ympäristöt.

Linchpin-projektin mukainen alusta on skaalautuva ja se toteuttaa alustojen ja verkkojen jatkuvaa turvallisuusmonitorointia. Järjestelmä analysoi uhkakuvia, turvallisuusprosessien määritysten noudattamista ja yleistä kyberuhkien kenttää todentaen epäilyttäviä aktiviteetteja ja tietoliikenteen ja -järjestelmien normaalipoikkeamia, mikä nopeuttaa suojaustoimien vasteaikoja merkittävästi manuaaliseen seurantaan verrattuna. [7]

Kolmantena esimerkkinä on CrowdStriken AI-pohjainen kehittynyt haitakkeiden havaitsemiseen suunniteltu palvelu. CrowdStrike käyttää AI:ta analysoimaan ja paljastamaan järjestelmien käyttäytymistä, joka voi liittyä haittaohjelmien (malware) ilmestymiseen. Palvelun AI-komponentti tutkii käytöstä, ja estää saastuneen ohjelmiston ajon ennen kuin se esimerkiksi ehtii salata tiedostoja tai vaarantaa muutoin järjestelmien suojauksen. CrowdStrike on ennaltaehkäisevä ratkaisu, ja se on osoittautunut toimivaksi estämään teollisuuden riesana olevien ransomware-tyypisten kiristysohjelmien tuhoja. [8]

Seuraava esimerkki on Google Geminin väärinkäytöstä. Kansainväliset ICT-järjestelmiä tuntevat rikollisjoukot ovat käyttäneet AI-perustaisia chatbotteja, kuten Googlen Gemini, vahvistaakseen kyberhyökkäyksiään. Menetelminä on ollut perustaa hyökkäyksiä käyttäen teknologiaa kirjoittamaan haittaohjelmia ja tutkimaan tietoturva-aukkoja. [9] Tämä on esimerkki siitä, kuinka rikolliset voivat tukeutua julkisesti saatavilla oleviin AI-alustoihin käyttäen niitä kehittämään hyökkäysmenetelmiä.

Jatkaen keinoälyyn liittyviä varjopuolien esimerkkejä, Kiinassa kehitetty DeepSeek-chatbot on ollut näkyvästi uutisissa sen heiluttaessa merkittävästi jopa pörssikursseja. Huolimatta toteutuksen teknisistä meriiteistä DeepSeek:n keinoälysovellus on herättänyt sen verran huolta, että Yhdysvaltojen merivoimat kielsi sen käytön siihen liittyvien mahdollisten tietoturva- ja eettisten riskien vuoksi erityisesti maanpuolustuksen näkökulmasta.

[10] Eräinä huolenaiheista ovat kysymykset siitä, ovatko esimerkiksi DeepSeek-sovelluksen ilmeisesti keräämät tiedot käyttäjien näppäinpainalluksista ja IP-osoitteista potentiaalinen riski maanpuolustukselle.

AI:n tulevaisuus kyberpuolustuksessa

Kyberuhkien kasvaessa ja kehittyessä on selvää, että keinoälyn rooli myös maanpuolustuksen kybersuojauksessa kehittyy ja laajenee. Tulevaisuuden AI:ta voidaan hyödyntää mm. itsekonfiguroitavien verkkojen kehityksessä ja käytössä, sillä AI-pohjaiset sovellukset voivat tehokkaasti ja itsenäisesti havaita verkko-operoinnin ja -liikennöinnin poikkeamia paljastaen järjestelmien omia haavoittuvuuksia. AI voi siten tukea verkkojen uudelleenkonfigurointia ja uusien tietoturvapäivitysten asentamista, pienentäen rikollisten toimijoiden hyökkäykseen käytettävissä olevaa tehollista aikaikkunaa. [11]

Toinen voimakkaasti kehittyvä alue liittyen AI:n mahdollistamaan kyberpuolustukseen on quantumlaskenta ja AI:n hyödyt sen teholaskentaan. AI:n ja quantumlaskennan yhdistelmä mahdollistaa tehokkaan datan prosessoinnin ja voi myös auttaa kehittämään uuden sukupolven entistä tehokkaampia AI-algoritmeja. Nimenomaan algoritmit ovat AI:n perusta, ja niiden avulla voidaan AI säätää vastaamaan yhä tehokkaammin kyberpuolustusta.

Maanpuolustuksen näkökulmasta on mielenkiintoista seurata ihmisen ja koneiden välisen ”yhteistyön” kehitystä. AI:n liittäminen ihmisten prosesseihin nopeuttaa ja tehostaa päätöksentekoon käytettävää aikaa, ja auttaa varmistamaan havaintojen ja päätösten oikeellisuuden kyberpuolustuksessa.

Maanpuolustuksen intresseihin liittyen myös AI:n mahdollistamat simuloinnit ja oppimisympäristöt tehostuvat. AI:n avulla puolustusvoimat voi luoda todellisenomaisia kyberhyökkäyksiä henkilöstön tehokkaaseen koulutukseen, ottaen huomioon lähes reaaliaikaisesti kehittyvän ympäristön uusine hyökkäysvektoreineen ja niihin valmistautumisineen.

AI auttaa myös yhtenä osana kokonaisuutta löytämään mahdollisia hyökkäyksiä ennalta käsin ennen niiden toteutumista tutkimalla jatkuvasti ja laajalla kentällä eri hyökkäyskuviota.

Yhteenveto

Keinoälyn liittäminen maanpuolustuksen kyberturvallisuuden järjestelmiin on hyödyllistä, ja itse asiassa välttämätöntä nykyaikaisten yhä monimutkaisempien kyberhyökkäysten materialisoituessa. AI:n toiminnot auttavat merkittävästi hyökkäysten todentamisessa, ennaltaehkäisevässä analysoinnissa ja automaattisessa nopeassa reagoinnissa.

Lähteet

[1] I. C. T. E. S. G. B. Babic, ”When Machine Learning Goes Off the Rails,” HBR, 1/2021. https://hbr.org/2021/01/when-machine-learning-goes-off-the-rails

[2] H. S. H. C. M. B. G. M. E. Fox, ”Building trust: Foundations of security, safety and transparency in AI,” 27.1.2025. https://www.redhat.com/en/blog/building-trust-foundations-security-safety-and-transparency-ai

[3] Verizon, ”2024 Data Breach Investigations Report,” 2024. https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf

[4] Crowdstrike, ”CrowdCast Series: 2025 Top Cybersecurity Trends,” 2025. https://www.crowdstrike.com/en-us/

[5] V. Shutenko, ”AI in Cybersecurity: Exploring the Top 6 Use Cases,” 8.8.2024. https://www.techmagic.co/blog/ai-in-cybersecurity

[6] A. Jamil, ”Case Studies: Successful Implementations of AI in Cyber Defense,” Umetech, 3.9.2024. https://www.umetech.net/blog-posts/successful-implementations-of-ai-in-cyber-defense

[7] G. Seffers, ”Army Cyber Researchers Develop AI Red Teaming Capabilities,” AFCEA, 1.8.2024. https://www.afcea.org/signal-media/cyber-edge/army-cyber-researchers-develop-ai-red-teaming-capabilities

[8] Redress Compliance, ”Top 15 Real-Life Use Cases For AI In the Cybersecurity Industry,” 25.7. 2024. https://redresscompliance.com/top-15-real-life-use-cases-for-ai-in-the-cybersecurity-industry/

[9] R. M. D. Volz, ”Chinese and Iranian Hackers Are Using U.S. AI Products to Bolster Cyberattacks,” The Wall Street Journal, 29.1.2025. https://www.wsj.com/tech/ai/chinese-and-iranian-hackers-are-using-u-s-ai-products-to-bolster-cyberattacks-ff3c5884

[10] S. Galvin, ”US Navy bans members from using China’s DeepSeek AI app out of security fears,” New York Post, 28.1.2025. https://nypost.com/2025/01/28/us-news/us-navy-bans-members-from-using-chinas-deepseek-ai-app-out-of-security-fears

[11] S. L. Sanchez, ”Artificial Intelligence (AI) enabled cyber defence,” European Defence Matters, 2017. https://eda.europa.eu/webzine/issue14/cover-story/artificial-intelligence-%28ai%29-enabled-cyber-defence

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 blogissaan www.5g-simplified.com.

TEKSTI: MIKKO KYLLÖNEN

Kognitiivinen ja laajakaistainen HF-ohjelmistoradiotekniikka Puolustusvoimissa

Toimintavarmat ja nopeat tietoliikenneyhteydet ovat kriittisiä joukkojen johtamisessa sekä reaaliaikaisen tilannekuvan muodostamisessa modernilla taistelukentällä. Aiemmin ylenkatsottu HF-tietoliikenne on kokenut viimeisten vuosien aikana renessanssin ohjelmistoradiotekniikan käyttöönoton myötä. Uusi tekniikka on yleistynyt yhä voimallisemmin myös sotilaallisessa toiminnassa sen mahdollistaessa nykyaikaisten johtamis- ja tilannekuvasovellusten käytön haastavassa radiotaajuisessa ympäristössä.

Tässä artikkelissa tarkastellaan HF-tietoliikenteen erityispiirteitä, tuotekehityksen historiaa, kenttätestien tuloksia ja sitä, miten kognitiivinen ja laajakaistainen teknologia on muuttanut kyseisellä taajuusalueella toimivien tietoliikennejärjestelmien suorituskykyä.

HF-kommunikaatiojärjestelmistä

Kiinteästä infrastruktuurista riippumattomien ja omavaraisten tietoliikennejärjestelmien rooli on korostunut viimeisten vuosien aikana samanaikaisesti, kun ymmärrys kaapeliyhteyksien, kaupallisten mobiiliverkkojen ja satelliittijärjestelmien haavoittuvuuksista on kasvanut. Näistä haavoittuvuuksista on saatu käytännön esimerkkejä Suomen lähialueilla muun muassa katkottujen merikaapeleiden ja GPS-häirinnän muodossa. Puolustusvoimat on vastannut näihin haasteisiin rakentamalla monikerroksisia ja toisiaan varmentavia tietoliikenneratkaisuja, joissa yhtenä osa-alueena on HF-taajuusalueella (high frequency) toimivat langattomat tietoliikennejärjestelmät.

HF-tietoliikennejärjestelmät toimivat 3–30 megahertsin taajuusalueella, jonka erityispiirteenä on ilmakehän sähköisesti varautuneen kerroksen eli ionosfäärin kautta tapahtuvat heijastumat, joilla on mahdollista saavuttaa horisontin taakse ulottuvat, jopa tuhansien kilometrien päähän yltävät johtamisyhteydet. HF-tietoliikennejärjestelmien taajuusalueen alaraja alkaa usein jo alle 2 megahertsin taajuuksista. Ionosfääri- eli avaruusaaltoyhteyksien lisäksi HF-taajuusalueen lähetteet voivat edetä joko suoraan tai kaartuvana pinta-aaltona, joka perustuu maan- ja merenpinnan sähköiseen johtavuuteen. Näillä etenemismenetelmillä yhteysetäisyydet rajoittuvat useimmiten muutamiin kymmeniin kilometreihin. Poikkeuksena ovat korkean suolapitoisuuden ja sähköisen johtavuuden valtameriolosuhteet, joissa pinta-aaltoyhteydet voivat kantaa selvästi pidemmälle kuin esimerkiksi pohjoisella Itämerellä.

Ionosfääriyhteyksien hyödyntämisen haasteena on fyysisen kerroksen luontainen kaoottisuus ja lähes jatkuva muutostila, joka ilmenee taajuuksien käytettävyyden aikaan ja paikkaan sidottuna voimakkaana vaihteluna. Tämä muutostila johtuu auringon aktiivisuuden vaihtelusta, joka noudattaa 11 vuoden sykliä sekä vuorokaudenajasta, joka määrittää ionosfäärin sähköisiä ominaisuuksia ja kerrostumien ilmenemisiä eri vuorokaudenajoille. Taajuuksien käytettävyyteen vaikuttaa myös yhteysetäisyydet, asemien sijainnit sekä käytettyjen antennien säteilykuviot. Merkittävänä tiedonsiirron suorituskykyyn liittyvänä muuttujana on lisäksi paikallinen kohinataso, joka voi heikentää tai pahimmillaan jopa lamauttaa radioaseman vastaanottokyvyn. Lisäksi se tekee radiolinkeistä usein epäsymmetrisiä, jolloin sama taajuus ei ole optimaalinen sekä lähetykseen että vastaanottoon. Luonnollinen ja keinotekoinen kohina on useimmiten korkeimmillaan HF-taajuusalueen alaosassa, jonka käytettävyys on erityisen tärkeää lyhyillä ja keskipitkillä ionosfääriyhteyksillä kuten Suomen sisäisessä liikennöinnissä.

Taajuuksien käytettävyyden arviointiin on kehitetty erilaisia ennustesovelluksia, jotka laskevat syötettyjen muuttujien perusteella optimaaliset taajuudet eri ajanhetkiin ja käyttökohteisiin. Näiden ennustesovellusten antamat tulokset ovat kuitenkin vain suuntaa antavia ja osin epätarkkoja erityisesti pohjoisille leveyspiireille, eivätkä ne huomioi paikallista kohinatasoa, ionosfäärin hetkellisiä muutoksia tai siinä ilmeneviä anomalioita.

Viimeisen kolmen vuosikymmenen aikana HF-radioiden oheen on kehitetty erilaisia tekniikoita, joiden tarkoituksena on ollut automatisoida taajuudenvalintamekanismit. Nämä automaattiset linkinmuodostus- eli ALE-tekniikat (automatic link establishment) ovat perustuneet useimmiten kansainvälisesti standardoituihin toisen, kolmannen tai neljännen sukupolven ratkaisuihin, joiden suorituskyky on ollut vaatimatonta. Linkinmuodostus voi kestää useita kymmeniä minuutteja, se epäonnistuu verraten usein, käytettävien taajuuksien lukumäärä on rajallinen eivätkä ne tue epäsymmetristä taajuuksien käyttöä. Etenkin taajuuksien käyttöön liittyvät rajoitteet tekevät edellisen sukupolven järjestelmistä alttiin elektroniselle tiedustelulle ja vaikuttamiselle. Heikkoutena on myös synkronoitu taajuuksien skannaus, joka perustuu yleensä GPS-signaalilla tuotettuun ulkoiseen tahdistukseen. ALE-tekniikan lisäksi HF-tietoliikennejärjestelmään kuuluu modeemi sekä automaattisen virheenkorjauksen tuottava protokolla, joka osaltaan säätelee modeemin toimintaa vallitsevan pakettivirhesuhteen perusteella. Nämä tekniset ratkaisut ovat niin ikään olleet

Kuva 1. LV562

rajoittuneita johtaen edellisen sukupolven HF-tietoliikennejärjestelmien heikkoon suorituskykyyn.

Näistä lähtökohdista Puolustusvoimat on yhdessä teollisen kumppanin kanssa kehittänyt kognitiivista ja laajakaistaista HF-tietoliikennejärjestelmää, jonka tehtävänä on ollut parantaa HF-liikenteen tiedonsiirtonopeutta, varmuutta ja taistelunkestävyyttä. Tuotekehitystä on tehty yli kymmenen vuotta ja se tulee jatkumaan aktiivisena aaltomuotokehityksenä järjestelmän koko elinkaaren ajan. Tämä järjestelmä tunnetaan Puolustusvoimissa nimellä LV562 ja sen arkkitehtuuri perustuu ideaaliseen ohjelmistoradioon. LV562 on esitetty kuvassa 1. Järjestelmän kaupallinen tuotenimi on CNHF1 ja sen valmistaja on suomalainen KNL.

Kognitiivisuus ja adaptiivisuus

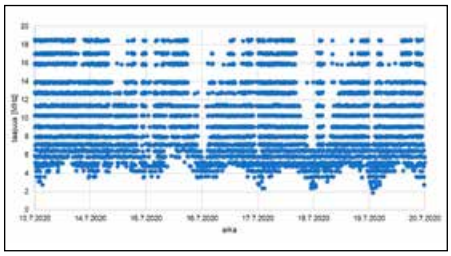
Edellä kuvattuihin HF-taajuusalueen fyysisen kerroksen haasteisiin on mahdollista vastata kognitiivisella tekniikalla, joka tekee autonomisesti päätökset käytettävistä liikennöintitaajuuksista perustuen reaaliaikaiseen ja laajakaistaiseen taajuustilannekuvaan. LV562-järjestelmä muodostaa tämän tilannekuvan lähettämällä yleislähetystyyppisesti lyhytkestoisia tilannekuvasanomia verkon muille asemille ja jotka tallennetaan vastaanottavan radion muistiin. Aaltomuodon kognitiivinen moottori analysoi vastaanotettujen tilannekuvasanomien sisältämän asemakohtaisen informaation ja tekee näiden perusteella päätöksen kunkin yhteysvälin linkinmuodostustaajuuksista. Linkinmuodostuksen yhteydessä aaltomuoto valitsee varsinaiset läheteparametrit kullekin liikennöintitapahtumalle: datan lähetys- ja vastaanottotaajuudet, signaalikaistanleveyden, modulaation ja kanavakoodaussuhteen.

Tämänkaltaisen toimintaperiaatteen ja teknisen toteutuksen ytimessä on laajakaistainen vastaanotin, joka kykenee kä-

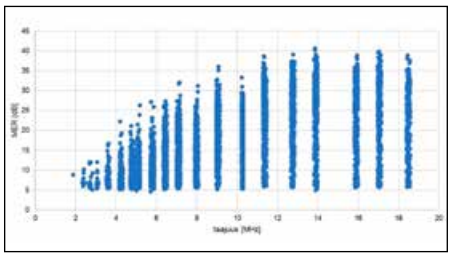
sittelemään lukuisia kutsukanavia samanaikaisesti. Kutsukanavia ei siis skannata taajuus kerrallaan, vaan radio vastaanottaa kokonaisia taajuusalueita yhtäaikaisesti. Tämä nopeuttaa linkinmuodostusta ja poistaa riippuvuuden ulkoisista aikalähteistä, kun taajuuksien käyttö on asynkronista. Puolustusvoimien käyttämän LV562-järjestelmän vastaanotinarkkitehtuuri perustuu suoranäytteistystekniikkaan ja se kykenee vastaanottamaan yli 2 500 kutsukanavaa samanaikaisesti.

Kuvassa 2 on esitetty vuoden 2020 kenttätestin yhteydessä muodostettu taajuustilannekuva kahden LV562-aseman välillä. Asemat sijaitsivat Saaristomerellä (A) ja Pohjois-Lapissa (B) ja niiden välinen etäisyys oli noin 950 kilometriä. Kuvasta voidaan nähdä miten matalimmat käytettävät taajuudet ovat noudattaneet odotettua vuorokautista vaihtelua noin 2 megahertsistä 5 megahertsiin. Sen sijaan korkeimmat käytettävät taajuudet ovat olleet odotettua merkittävästi korkeammat yltäen muutamaa ajankohtaa lukuun ottamatta lähes 19 megahertsiin asti. Korkeimmat taajuudet ovat olleet noin 10 megahertsiä korkeammat kuin ennusteohjelmistoilla lasketut taajuudet. Tulos osoittaa, miten kognitiivinen ja laajakaistainen aaltomuoto kykenee hyödyntämään ionosfäärin odottamattomia anomalioita, jotka muutoin jäisivät käyttämättömäksi taajuusresurssiksi.

Kuvassa 3 on esitetty saman kenttätestin taajuustilannekuvasanomien modulaatiovirhesuhde taajuuden funktiona. Siitä voidaan havaita miten matalilla alle 5 megahertsin taajuuksilla modulaatiovirhesuhde on ollut korkeimmillaan noin 10–15 desibeliä. Modulaatiovirhesuhde on kasvanut lineaarisesti taajuuden kanssa ollen suurimmillaan yli 40 desibeliä. Havainto on odotettu ja se selittyy osaltaan luonnollisen ja keinotekoisen kohinan sijoittumisesta HF-taajuusalueen alaosaan, kuten edellä on todettu. Mittaustulos osoittaa myös sen, että liikennöinnissä kannattaa suosia mahdollisuuksien mukaan korkeimpia taajuuksia, joiden matalampia taajuuksia parempi laatu mahdollistaa nopeampien läheteparametrien hyödyntämisen. Epätyypillisen korkeiden taajuuksien ilmeneminen on pitkällä aikavälillä toki harvinaisempaa, eikä niiden käytettävyyteen voi perustaa liikennöintiä etenkään edellisen sukupolven kapeakaistaisissa teknisissä ratkaisuissa. Huomattakoon, että kyseisen kenttätestin aikana LV562-järjestelmän laajakaistainen aaltomuoto käytti konvoluutiokoodausta, joka on sittemmin



Kuva 2. Vastaanotettujen tilannekuvasanomien taajuus ajan funktiona (A)



Kuva 3. Vastaanotettujen tilannekuvasanomien modulaatiovirhesuhde taajuuden funktiona (A)

korvattu robustimmalla turbokoodauksella. Tämä mahdollistaa operoinnin signaalikohina-suhteilla, jotka ovat alhaisimmillaan lähellä 0 desibelin raja-arvoa. LV562-järjestelmän laajakaistaisen aaltomuodon rinnalla on robusti ja kapeakaistainen aaltomuoto, joka kykenee operoimaan selvästi alle 0 desibelin signaali-kohinasuhteella. Se on suunniteltu erittäin haastaviin radiotaajuisiin olosuhteisiin.

LV562-järjestelmän läheteparametrit mukautuvat automaattisesti vallitseviin etenemis- ja kohinaolosuhteisiin ja niiden valinnassa huomioidaan myös lähetettävän datan määrä. Käytännössä vähäiselle datamäärälle valitaan automaattisesti robusti läheteparametrien kombinaatio, jolloin liikennöintiin soveltuvia kanavia on käytettävissä oletettavasti enemmän. Mikäli lähetettävän datan määrä on suuri, pyrkii aaltomuoto etsimään HF-spektristä ne liikennöintitaajuudet, joilla on mahdollista operoida nopeilla mutta vähemmän robusteilla läheteparametreillä.

Etenemis- ja kohinaolosuhteita mitataan reaaliaikaisesti modulaatio- ja pakettivirhesuhteilla, jotka määrittelevät yksittäisen liikennöintikanavan laadun ja siten korkeimman mahdollisen tiedonsiirtonopeuden kullekin ajanhetkelle.

Latenssi ja tiedonsiirtonopeus

Viime vuosina monet teolliset toimijat ovat keskittyneet HF-tekniikoiden kehittämisessä kansainvälisesti standardoituihin ja laajakaistaisiin modeemeihin, jotka tarjoavat nopeimmillaan useiden kymmenien kilobittien, jopa yli sadan kilobitin sekuntinopeuksia. Sen sijaan standardoiduissa linkinmuodostustekniikoissa ei ole tapahtunut merkittävää kehitystä. Tämä tuotekehityksen vääristymä on johtanut siihen, että HF-tietoliikennejärjestelmien tarjoama hetkellinen tiedonsiirtonopeus on kasvanut samaan aikaan, kun latenssi ja tiedonsiirtovarmuus ovat pysyneet vaatimattomalla tasolla. Suuri hetkellinen tiedonsiirtonopeus menettää kuitenkin merkityksensä, mikäli linkinmuodostus on pitkäkestoinen ja epäluotettava.

Linkinmuodostus on HF-tietoliikenteen kokonaissuorituskyvyn pullonkaula ja merkittävin latenssia määrittävä muuttuja. Kun huomioidaan kriittisimmät taktisen johtamisen palvelut kuten formaalit johtamissanomat, pikaviestit, sensoridata ja tilannekuvan välittäminen havaitaan, että lyhyt latenssi on arvokkaampi ominaisuus kuin hetkellinen suuri tiedonsiirtonopeus. Tämä korostuu erityisesti palveluissa, joissa välitettävän datan määrä on vähäinen. Korkealle tiedonsiirtonopeudelle on toki käyttötapauksensa esimerkiksi suurten tiedostojen kuten tunnistusvalokuvien välittämisessä.

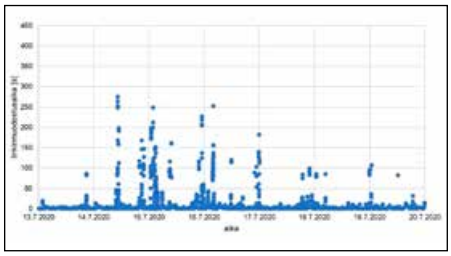
Puolustusvoimien LV562-järjestelmän tuotekehityksessä linkinmuodostustekniikka on ollut alusta asti tärkeässä roolissa. Yhteyskättelyyn ja automaattiseen virheenkorjaukseen liittyvät prosessit on pyritty pitämään suoraviivaisina ja nopeina ylimääräisiä vaiheita välttäen. Tavoitteena on ollut nopea ja toimintavarma linkinmuodostus, jonka rinnalla operoidaan adaptiivisella ja laajakaistaisella modeemilla, joka kykenee nopeimmillaan yli 100 kilobitin sekuntinopeuteen.

Kuvassa 4 on esitetty vuoden 2020 kenttätestin yhteydessä toteutettujen datansiirtotestien linkinmuodostusajat. Viikon aikana lähetettiin automatisoidusti yhteensä 168 vakioitua sähköpostisanomaa, joiden kunkin koko oli yhteensä 69 kilotavua sisältäen 50 kilotavun kuvatiedoston. Kuvasta nähdään, miten linkinmuodostusajat ovat olleet pääsääntöisesti alle 10 sekuntia. Pisimmät linkinmuodostusajat ovat olleet noin 4 minuuttia ja ne ovat sijoittuneet useimmiten vuorokauden vaihteeseen, joka on etenemisolosuhteiden osalta kaikkein haastavin ajankohta. Kenttätestissä linkinmuodostustapahtumia oli yhteensä 998. Niiden keston mediaani oli 6,6 sekuntia ja nopeimmillaan linkinmuodostus tapahtui 0,8 sekunnissa. Yksittäisen liikennöintitapahtuman linkinmuodostustaajuudet olivat usein epäsymmetrisiä ja ne vaihtelivat 1,9 ja 18,6 megahertsin välillä taajuuksien eron ollessa suurimmillaan 11,1 megahertsiä. Kaikki kenttätestin aikana lähetetyt 168 sähköpostisanomaa toimitettiin vastaanottajalle onnistuneesti.

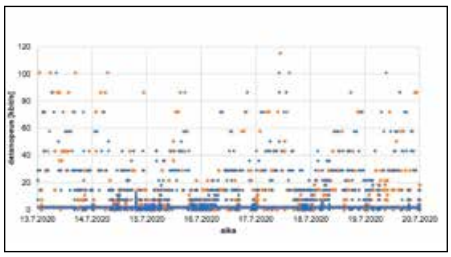
Kuvassa 5 on esitetty saman kenttätestin datansiirtotestien hetkelliset tiedonsiirtonopeudet. Tiedonsiirtonopeus on vaihdellut 1,8 ja 115 kilobitin sekuntinopeuden välillä nopeusmuutosten korreloidessa etenemis- ja kohinaolosuhteiden luontaisen ja keinotekoisen vaihtelun kanssa. Järjestelmän teoreettinen maksiminopeus on saavutettu kertaalleen keskipäivällä 17.7.2020, jolloin aaltomuoto on käyttänyt 256 QAM modulaatiota 24 kilohertsin signaalikaistanleveydellä. Kenttätestissä tiedonsiirtonopeus on ollut pääsääntöisesti 10 ja 40 kilobitin sekuntinopeuden välillä. Datansiirtotestissä välitetty 69 kilotavun sähköpostisanoma oli kooltaan verraten suuri, joten aaltomuodon kognitiivinen moottori pyrki valikoimaan HF-spektristä ensisijaisesti ne liikennöintitaajuudet, joilla kyettiin operoimaan nopeilla läheteparametreillä.

Kenttätestin yhteydessä maksimisignaalikaistanleveys oli 24 kilohertsiä. Sittemmin aaltomuotoon on tullut tuki 48 kilohertsin signaalikaistanleveydelle, joka nostaa teoreettisen maksiminopeuden lähelle 300 kilobitin sekuntinopeutta. Hetkellistä maksimitiedonsiirtonopeutta tärkeämpi ominaisuus on kuitenkin kyky mukautua vallitseviin radiotaajuisiin olosuhteisiin liikennöintitaajuuksien ja läheteparametrien valinnan nopealla automatiikalla.

Maksiminopeus edellyttää korkeaa modulaatiovirhesuhdetta ja sen saavuttaminen on harvinaista etenkin ionosfääriyhteyksillä ja korkean kohinatason cosite-käyttökohteissa. Lyhyillä ja tavallisesti laadukkailla pinta-aaltoyhteyksillä maksiminopeus on mahdollista saavuttaa useammin.



Kuva 4. Linkinmuodostuksen kesto ajan funktiona (A)



Kuva 5. Tiedonsiirtonopeus ajan funktiona (A ja B)

Liikennöintimenetelmät ja -protokollat

HF-rajapinnassa käytetään kahta liikennöinnin päämenetelmää: yksilölähetystä eli unicast-liikennöintiä ja yleislähetystä eli broadcast-liikennöintiä. LV562 tukee molempia menetelmiä.

Unicast perustuu varmennettuun tiedonsiirtoon, jossa jokainen datapaketti kuitataan lähettäjälle automaattisesti vastaanottavan aseman toimesta. Mikäli vastaanotettu datapaketti on korruptoitunut, pyytää vastaanottava asema lähettämään kyseisen datapaketin uudestaan. Tämä menetelmä on osa tiedonsiirron protokollaa ja se tunnetaan termillä ARQ (automatic repeat request). ARQ on kriittinen osa-alue varmennetussa HF-liikennöinnissä sen mahdollistaessa automaattisen virheenkorjauksen, adaptiiviset läheteparametrit ja sanomien automaattiset toimituskuittaukset. Tältä osin se vertautuu kuljetuskerroksen TCP/IP-liikennöintiin. ARQ-liikennöinti ei toimintaperiaatteensa vuoksi mahdollista datan vastaanottoa radiohiljaisuudessa.

Broadcast perustuu varmentamattomaan tiedonsiirtoon, jossa datapaketit lähetetään samanaikaisesti yhdelle tai useammalle vastaanottajalle lähetä ja unohda periaatteella. Tämä menetelmä tunnetaan termillä non-ARQ. Koska pakettien virheetöntä toimitusta ei kyetä varmenta-

maan, on LV562-järjestelmään kehitetty erilaisia aikaan ja taajuuksiin sidottuja toistosyklejä ja menetelmiä, joiden tarkoituksena on nostaa datapakettien onnistuneen toimituksen todennäköisyyttä broadcast-liikennöinnissä. LV562-järjestelmän laajakaistainen vastaanotinarkkitehtuuri on muuttanut radikaalisti myös kyseisen liikennöintimenetelmän suorituskykyä: datapakettien toimitusvarmuus on kasvanut huomattavasti, kun dataa kyetään vastaanottamaan tuhansilla taajuuksilla minä ajanhetkenä tahansa. Non-ARQ-liikennöinti mahdollistaa datan vastaanottamisen radiohiljaisuudessa, mutta se ei tue adaptiivisten läheteparametrien käyttöä ja vertautuu näin ollen kuljetuskerroksen UDP/IP-liikennöintiin. Toimintaperiaatteensa vuoksi se soveltuu hyvin muun muassa pintatilannekuvan välittämiseen.

LV562-järjestelmän unicast-liikennöinnin oheen on kehitetty releointi, jonka avulla kahden aseman välinen dataliikenne voidaan välittää automaattisesti kolmannen aseman kautta. Tämä ominaisuus tunnetaan termillä HF multihop ja sitä voidaan käyttää tilanteessa, jossa asemien välillä ei ole suoraa yhteyttä esimerkiksi epäsymmetristen antenniratkaisujen tai muiden radiotaajuisten rajoitteiden vuoksi. Tällöin kolmas asema voi toimia datan välittäjänä edellyttäen, että molemmilla liikennöivillä asemilla on siihen yhteys. Releoinnissa jokaisella radiolinkillä eli hypyllä käytetään linkkikohtaisia ja yhteysväleistä riippumattomia adaptiivisia linkinmuodostus- ja datansiirtomenetelmiä. Sen avulla on mahdollista pidentää laadukkaita pinta-aaltoyhteyksiä ja välttää kahden aseman välinen katvealue eli niin sanottu skip zone vyöhyke. Lisäksi liikennöivistä radioasemista etäälle sijoitettu releointiasema mahdollistaa korkeampien ja laadukkaampien taajuuksien käytön sekä laajemman taajuusdiversiteetin. Releoinnilla on roolinsa myös elektronisessa suojautumisessa, jossa sen laajamittainen käyttö vaikeuttaa signaalitiedusteluun perustuvaa verkkoanalyysia.

Tietojärjestelmäintegraatio taktisiin sanoma- ja tilannekuvasovelluksiin tuotetaan ensisijaisesti standardien mukaisilla sovellus- ja kuljetuskerroksen rajapinnoilla. Tämä mahdollistaa integraation kolmannen osapuolen toteuttamiin ohjelmistoihin. LV562-järjestelmä tukee yleisesti käytettyjä sähköposti- ja pikaviestiprotokollia (SMTP ja XMPP) sekä internetprotokollaa (IP), joiden avulla ulkoiset asiakasohjelmistot ja palvelimet kykenevät kytkeytymään radioon ja liikennöimään HF-rajapinnan yli. Internetprotokolla ei ole tehokkain mahdollinen tapa liikennöidä HF-rajapinnassa, mutta se tuottaa laajat integrointimahdollisuudet ja mahdollistaa esimerkiksi päästä-päähän IPSec-salauksen. Sen kautta voidaan toteuttaa myös laajakaistainen HF-rajapinta niille tulenkäytön palveluille, jotka hyödyntävät JREAP-C-protokollaa taktisten datalinkkien rinnalla.

Sulautettu aaltomuotoarkkitehtuuri

HF-kommunikaatiojärjestelmät ovat perustuneet vuosikymmenien ajan hajautettuun tekniseen arkkitehtuuriin, jossa laitekokonaisuuden muodostavat osakomponentit on toteutettu fyysisesti erillisillä radio-, modeemi-, linkinmuodostus- ja salauslaitteilla. Näiden laitteiden väliset kaapeliyhteydet on tehty tyypillisesti audio- ja sarjaliikennerajapintojen kautta. Tämänkaltainen arkkitehtuuri on johtanut monimutkaiseen, suurikokoiseen ja kalliiseen ratkaisuun, joka on altis teknisille vioille eikä mahdollista joustavaa operoinnin aikaista kehitystä. Hajautettu tekninen arkkitehtuuri on ollut yleinen eritoten laivastojoukoilla ja kiinteissä käyttökohteissa.

Moderni ohjelmistoradio mahdollistaa sulautetun eli niin sanotun full stack aaltomuotoarkkitehtuurin, jossa kaikki tietoliikennepinon muodostavat osakomponentit on integroitu samaan aaltomuoto-ohjelmistoon. Tämä vähentää fyysisten laitteiden ja kaapeleiden lukumäärää, poistaa tarpeen vanhanaikaisille tietoliikennerajapinnoille ja tekee järjestelmän käyttöönotosta sekä ylläpidosta suoraviivaisempaa kuin hajautetussa teknisessä arkkitehtuurissa. Ohjelmistoradiotekniikan käyttöönoton myötä aaltomuodon kehittäminen ja parantaminen on muuttunut ketteräksi ilman, että muutoksia tehdään fyysisiin laitteisiin. LV562-järjestelmän aaltomuoto- ja alustaohjelmistoja on kehitetty aktiivisesti vuosien ajan. Tätä kautta tuotetut uudet ominaisuudet ovat parantaneet järjestelmän suorituskykyä ja antaneet lisää mahdollisuuksia viestitaktiikan suunnitteluun. Aaltomuodon uusien ominaisuuksien teknisessä määrittelyssä on huomioitu loppukäyttäjien kehitysideat sekä muutokset modernin taistelukentän vaatimuksissa.

Yhteenveto

Kognitiivinen ja laajakaistainen HF-ohjelmistoradioteknologia on tullut jäädäkseen sen etujen ollessa kiistattomat edellisen sukupolven kapeakaistaisiin järjestelmiin verrattuna. Uusi tekninen ratkaisu on jalkautettu puolustushaaroihin käyttöönoton laajetessa johtamisen kaikille tasoille. Järjestelmän suorituskyky on herättänyt kiinnostusta myös Puolustusvoimien tärkeimmissä kumppanimaissa johtaen muun muassa ensimmäiseen monikansalliseen ja valtioiden rajat ylittävään testitapahtumaan vuonna 2024.

Artikkelin kirjoittaja

Mikko Kyllönen työskentelee Järjestelmäkeskuksen Maajärjestelmäosastolla ja toimii projektipäällikkönä Puolustusvoimien WBHF-projektissa.

Kuvien lähteet: kuva 1 KNL, kuvat 2–5 Mikko Kyllönen.

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

TEKSTI: TATU TAHKOKALLIO, ERIKOISTUTKIJA, MAAVOIMIEN TUTKIMUSKESKUS

Taktisen tason johtamisjärjestelmäkonsepti: Secure But Unclassified

Taktisen tason johtamisjärjestelmien kehitys on murroksessa. Ratkaisuja on tarjolla sekä kaupallisesti että avoimen lähdekoodin pohjalta ja perinteisten järjestelmätoimittajien ja käyttäjien raja hämärtyy, kun ohjelmistoihin voi ohjelmoida lisäosia melkein kuka tahansa.Yhtä lailla tarve liittää julkisia ja ei-julkisia tietolähteitä, kiinteitä ja liikkuvia sensoreita ja jopa lavetteja ja asejärjestelmiä kasvaa, kun pyrkimyksenä on johtaa entistä tehokkaampia yhteisoperaatioita eri aselajien, puolustushaarojen ja liittolaisten kesken. Erään ratkaisun edellä mainittuihin haasteisiin tarjoaa Secure but unclassified – johtamisjärjestelmäkonsepti.

SBU-konseptin tausta

Kesällä 2018 US Army heräsi jäykän turvaluokittelun negatiivisiin vaikutuksiin sotilasoperaatioissa. Silloisen US Army Soldier Warrior -hankkeen hankepäällikkö eversti Ed Barkerin totesi kesäkuussa 2018 AFCEA:n (Armed Forces Communications & Electronics Association International) isännöimässä tapahtumassa, että taktisella ja taisteluteknisellä tasolla moni tieto menettää nopeasti merkityksensä ja että tiedon suojaamiseksi on löydettävä turvaluokittelun sijasta tarkoituksenmukaisempia keinoja. Hänen mukaansa toiminnan ketteryyttä ei saanut vaarantaa tarpeettomilla hidasteilla.

Ratkaisuksi US Army ehdotti liike-elämässä käytössä olevia vahvoja salausmenetelmiä. US Army katsoi, että salausmenetelmiä käyttämällä taktisella tasolla voidaan siirtää ja käsitellä tietoa ilman, että verkkoja ja päätelaitteita tarvitsee tietoturva-auditoida ja turvaluokitella. Samalla US Army näytti vihreää valoa julkisten tietoverkkojen ja muiden siviiliteknologioiden operatiiviselle käytölle (mm. Wifi, LTE ja 4G). Muutos oli merkittävä ja osaltaan uraauurtava, joskin Yhdysvaltain erikoisjoukot olivat hyödyntäneet siviiliratkaisuja jo jonkin aikaa.

Secure but unclassified (tietoturvallinen mutta turvaluokittelematon) -konsepti merkitsi US Army:lle ennen kaikkea oman toiminnan ketteröittämistä, kun tiedon käsittelyyn ja välittämiseen tuli tarjolle muitakin kuin ensisijaisesti sotilaskäyttöön suunniteltuja vaihtoehtoja.

Kaikuja arjen järjestelmistä?

Suomen Puolustusvoimat ryhtyi 2010-luvun alkupuolella pohtimaan siviilimaailmasta tuttujen toimintamallien ja välineiden, esimerkiksi matkapuhelinverkkojen ja -päätelaitteiden, sotilaallista hyödyntämistä. Pohdinta kulminoitui silloisen johtamisjärjestelmäpäällikön tammikuussa 2016 julkistamaan Johtamisen tuen konsepti 2030 -asiakirjaan, jossa arjen järjestelmät asemoitiin omaksi kokonaisuudekseen taistelunjohtojärjestelmien ja viranomaisten yhteisten järjestelmien rinnalle.

US Army:n SBU-konseptissa ja Puolustusvoimien arjen järjestelmät -konseptissa on selviä yhtäläisyyksiä. Molemmat pyrkivät edistämään siviilikäyttöön suunniteltujen päätelaitteiden ja infrastruktuurin hyödyntämistä ja toisaalta muokkaamaan sotilaallista ajattelua myötämielisemmäksi uusia teknologioita kohtaan.

Konsepteissa on kuitenkin eroja. SBU-konseptissa korostettiin alusta alkaen tiedon teknistä suojaustarvetta ja teknisesti kaikkein edistyksellisimpien kaupallisten salausratkaisujen käyttöä. Tiedon suojaustarve oli tunnistettu myös Puolustusvoimissa, mutta ongelmakenttää ei lähestytty niinkään teknisten menetelmien avulla vaan etsimällä tietoturvaan ratkaisuja joukkojen käyttö- ja toimintaperiaatteiden kautta.

Uusi viestiprotokolla

SBU-konseptin rinnalla rakentui kovaa vauhtia teknologia, jonka ensi askeleet otettiin kesällä 2002. Tuolloin MITRE Corporationin tutkijat kehittivät Yhdysvaltain Massachusetissa yksinkertaisen ja helposti toteutettavan viestiprotokollan, joka mahdollisti yksittäiseen kohteeseen liittyvän paikka- ja aikatiedon siirtämisen eri tietojärjestelmien välillä. Teknologian perimmäisenä tavoitteena oli luoda menetelmä, joka ratkoo tilannekuvan ylläpitoon liittyviä mitä? missä? ja koska? kysymyksiä.

Teknologia sai nimekseen Cursor-on-Target (CoT). Kenraali Jumperin huhtikuussa 2002 US Air Force C2 Summitissa pitämän puheen perusteella, jossa hän totesi, että ”the sum of all wisdom is a cursor over the target”. Nimi on lyhyt ja

RATKAISU-KONSEPTI	STANDARDIT	TURVA-LUOKKA	TUNNUSOMAISIA KOVENNUSKEINOJA	PÄÄTELAITE-ESIMERKKI
ARJEN JÄRJESTELMÄ, COTS Commercial off-the-shelf	perustuu siviilistandardeihin	julkinen, auditoimaton	ei kovennuksia	käyttäjien omat Android tai iOS COTS-päätelaitteet
SBU–ARKI Secure But Unclassified	perustuu siviilistandardeihin ja noudattaa vähintään CoT mil-standardia	julkinen, auditoimaton	▪ kokonaan puuttuva tai osittainen päätelaitehallinta ▪ päätelaitteiden toimintorajoitukset	käyttäjien omat Android tai iOS COTS-päätelaitteet
SBU–MIL Secure But Unclassified			▪ SBU-ohjelmistot allekirjoitettu käyttäjäorganisaation ei-julkisella varmenteella ▪ täysi tai osittainen päätelaitehallinta ▪ päätelaitteiden toimintorajoitukset ▪ APN-liittymä ▪ VPN-yhteys ▪ palvelin yksityisessä pilvessä, saarekkeisessa palvelimessa tai vast.	käyttäjäorganisaation jakamat Android COTS-päätelaiteet
GOTS Government off-the-shelf	perustuu siviilistandardeihin ja voi noudattaa mil-standardeja	TL IV, auditoitu	▪ täysi päätelaitehallinta ▪ päätelaitteiden toimintorajoitukset ▪ palvelin yksityisessä konesalissa ▪ APN-liittymä ▪ VPN-yhteys	Valtorin eTUVE-päätelaite
MOTS Military off-the-shelf	perustuu siviili- ja mil-standardeihin	TL III, auditoitu	▪ päätelaitteen fyysinen kovennus ▪ käyttöjärjestelmä-kovennukset ▪ täysi päätelaitehallinta ▪ päätelaitteen toimintorajoitukset ▪ palvelin yksityisessä konesalissa ▪ APN-liittymä ▪ VPN-yhteys	Bittium Tough Mobile 2

Taulukko: Ratkaisukonseptien luokittelu.

ytimekäs mutta sikäli harhaanjohtava, että CoT-protokollalla ei etäohjata tilannekuvajärjestelmien osoittimia (”cursor”) vaan siirretään maalipisteitä ja tilannekuvamerkkejä järjestelmien kesken.

Yksi CoT-protokollan lähtökohdista on olio-ohjelmoinnista tuttu polymorfismi. Polymorfismin määritelmän mukaisesti alaluokan olioita yhdistää yläluokalta perityt ominaisuudet samalla kun alaluokan olioilla voi olla myös omia yksilöllisiä ominaisuuksia. Yläluokka ei siis määritä alaluokalle sallittuja arvoja dominoivasti. Polymorfismin takia CoT ei salli lueteltujen tietotyyppien (engl. enume-

rated) käyttöä. Esimerkiksi kuvitteelliselle tietotyyppille r (reply) ei voisi antaa pelkkää kiinteää arvojoukkoa ”välitön”, ”viivästetty” ja ”pysäytetty”, vaan tietotyypille tulisi sallia myös muita arvoja, kuten ”välitetty” ja/tai ”salattu”. Käytännössä yksittäisen CoT-viestin sisältökenttä on aina merkkijono, esimerkiksi “a-h-G-E-V-A-T-t”, jonka yksittäisillä merkeillä voi olla lukuisia eri vaihtoehtoja ja jonka tulkitseminen vaatii sovelluskohtaista erityistietämystä.

CoT-viestiprotokolla on omaksuttu laajaan käyttöön Yhdysvaltojen puolustushallinnossa. Teknologia on standardoitu ei-julkiseen asiakirjaan MIL-STD-6090, Cursor-on-Target (CoT) Message Standard. Standardin jakelua hallinnoi nykyään US Defence Information Systems Agency (DISA) ja siitä voi löytää maininnan mm. Assist-hakukoneella (https://assist.dla.mil/).

SBU ja muut ratkaisukonseptit

Julkisista lähteistä on löydettävissä arjen järjestelmäkonseptin ja SBU-konseptin rinnalle kaksi muuta siviiliteknologioita hyödyntävää järjestelmäkokonaisuutta. Ensimmäisestä kirjallisuudessa käytetään nimeä Government off-the-shelf (GOTS, viranomaisjärjestelmä) ja toisesta Military off-the-shelf (MOTS, sotilasjärjestelmä). Taulukko 1. luokittelee eri ratkaisukonseptit ominaisuuksineen. Reserviläisarmeijan erityispiirteiden huomioimiseksi SBU-konsepti on taulukossa jaettu kahteen osaan.

Taulukon ratkaisukonsepteissa on eroja. Ensimmäinen liittyy standardien hyödyntämiseen. Arjen järjestelmät ja useimmat GOTS-järjestelmät perustuvat lähinnä siviilistandardeihin siinä missä SBU- ja MOTS-konseptit hyödyntävät aina yhtä tai useampaa MIL-standardia. Lisäksi SBU-konseptin tunnusomaiseksi piirteeksi voidaan katsoa nimenomainen CoT-standardin tuki. Myös järjestelmien turvaluokittelut poikkeavat toisistaan. GOTS- ja MOTS-ratkaisut ovat tietoturva-auditoitu ja omaavat turvaluokituksen, kun taas arjen järjestelmät ja SBU-ratkaisut ovat turvaluokittelemattomia.

Vaikka tavoitteena ei olisikaan auditoinnin läpäisy ja turvaluokitus voidaan kovennuskeinoja toteuttaa myös muiden ratkaisukonseptien yhteydessä. Lopullisen päätöksen käytettävistä kovennuskeinoista tekee lopulta käyttäjäorganisaatiot itse, eikä kaikkia taulukossa 1. kuvattuja menetelmiä ole lainkaan pakko hyödyntää.

SBU-konseptin jako kahteen eri versioon, ARKI ja MIL, tukee sekä reserviläisarmeijalle tyypillistä poikkeusolojen ottomenettelyä, jolla reserviläisten Android- ja iOS-päätelaitteita on mahdollista lunastaa Puolustusvoimien omaisuudeksi, että jakokalustoon perustuvaa toimintatapaa, jossa laitteet hankitaan ja jaellaan Puolustusvoimien toimesta asevelvollisille. Jälkimmäisen mallin etuna edelliseen verrattuna on yhtenäisemmät ja helpommin ylläpidettävät järjestelmä- ja laitekokonaisuudet.

SBU-ARKI- ja SBU-MIL -versiot voivat erota myös siinä, miten ja mihin tarvittavat palvelinratkaisut sijoitetaan. SBU–ARKI-konseptissa palvelimet sijoitetaan julkiseen pilveen, kun taas SBU–MIL palvelimet sijoitetaan joko yksityiseen pilveen tai saarekkeisiin palvelimiin. Kolmas ja kenties merkittävin ero versioiden välillä liittyy tapaan, jolla ohjelmistot varmennetaan. SBU-MIL-ohjelmistot tulisi allekirjoittaa aina käyttäjäorganisaation ei-julkisella varmenteella.

TAK-ohjelmistoperhe

Maavoimien tutkimuskeskus aloitti SBU-määritelmän mukaisen tilannekuva- ja johtamisjärjestelmän kenttäkokeet syksyllä 2022. Kenttäkokeet keskittyivät TAK-ohjelmistoperheeseen, joka oli nopeasti saavuttanut kansainvälistä mainetta ja kerännyt ympärilleen aktiivisen kehittäjäyhteisön. Koska ohjelmistosta on jakelussa sekä siviili- että sotilasversiot, on TAK-lyhenteestä vastaavasti kaksi eri tulkintaa; Team Awareness Kit ja Tactical Assault Kit.

TAK-ohjelmiston esiversion julkaisi US Air Force Research Laboratory elokuussa 2010. Sittemmin ohjelmisto laajeni kokonaiseksi ohjelmistoperheeksi ja sen kehitysvastuu on siirretty US Department of Defence:n alla toimivalle TAK Product Center:lle. Ensimmäinen Android-päätelaitteissa toimiva TAK-versio (ATAK) julkaistiin vuonna 2013 ja tällä hetkellä päätelaiteohjelmasta on saatavilla omat versionsa mm. Windows (WinTAK) ja iOS (iTAK) -käyttöjärjestelmille.

TAK-ohjelmiston käyttö on levinnyt laajasti sekä Yhdysvaltojen asevoimissa että Yhdysvaltojen liittovaltion ja osavaltioiden viranomaisten parissa. Näiden lisäksi ohjelmiston MIL-versiota on lisensoitu Yhdysvaltojen liittolaisille Foreign Military Sales -tuotteena. Maaliskuussa 2020 ohjelmiston jakelu vapautettiin siviilikäyttäjille ja syyskuussa 2020 se oli jo ladattavissa Google Play -kaupasta.

Saavutettavat hyödyt

TAK-ohjelmistoperheellä voidaan saavuttaa monenlaisia SBU-konseptia palvelevia hyötyjä. Reserviläisarmeijalle on iso etu, että järjestelmä on käytettävissä jokapäiväisillä viestivälineillä kuten matkapuhelimilla. Yhteensopivia ja päivittyviä päätelaitteita on yhteiskunnassa laajasti ja koska tarvittavat mobiilisovellukset ovat ilmaiseksi ladattavissa, voivat reserviläiset harjoitella ohjelmistojen käyttöä myös vapaa-ajallaan.

TAK-ohjelmiston loppukäyttäjiä on maailmalla satojatuhansia. Näiden toimesta on muodostettu yhteisöjä, joista eräs mielenkiintoisimmista lienee Naton TAK-käyttäjäyhteisö. Yhteisöllisyys yhdessä laajan käyttäjä- ja ohjelmistokehittäjäjoukon kanssa edistää TAK-ohjelmistojen luotettavuutta. Ohjelmistojen eheys, tietoturva ja toimivuus ovat jatkuvassa testissä ja löydetyistä vioista ja puutteista yhteisön jäsenet raportoivat suoraan TAK Product Center:lle. Havainnoista käydään myös jatkuvaa keskustelua yhteisön Discord-keskustelufoorumissa. Luotettavuutta edistävät myös tunnetut jakelukanavat (Google Play -kauppa, virallinen TAK.gov -sivusto sekä GitHub-palvelu), joista käyttövalmiit ohjelmiston osat ja avoimet lähdekoodit ovat ladattavissa.

Kuten viranomaisten olemassa oleviin tilannekuvajärjestelmiin, myös TAK-tilannekuvajärjestelmään voidaan liittää saatavilla olevia kiinteitä sensoreita ja muita rajapinnan tarjoavia tietolähteitä. Esimerkki edellisistä on liikennekameroiden verkosto ja jälkimmäisistä Maanmittauslaitoksen aineistopalvelut. Mikäli TAK-ohjelmistoja on tarve käyttää erillisverkossa, voidaan rinnalle asentaa erillinen kartta- ja olosuhdepalvelin, jonka tiedot kytketään suoraan TAK-ohjelmiston muodostamaan tilannekuvaan.

Kokonaan uudenlaista ajattelua edustaa TAK-ohjelmistoperheen räätälöitävyys erilaisia käyttötapauksia tukevaksi oh-

jelmistolaajennusten avulla. Laajennuksia on saatavilla sekä kaupallisesti että ilmaiseksi ja haluttaessa laajennuksia voi erityistarpeisiin teettää teollisuudella tai kehittää itse. Ohjelmistolaajennukset toimivat ohjelmistoperheen Android- ja Windows-päätelaiteohjelmissa. Laajennusten avulla järjestelmään voidaan helposti liittää ja kontrolloida erilaisia liikkuvia sensoreita tai vaikuttimia, esimerkiksi tiedustelulennokkeja tai maalla liikkuvia robotteja. Erityismaininnan ansaitsevat laajennusosat, jotka mahdollistavat kapean tekoälyn käytön osana tilannekuvan tulkintaa. Esimerkiksi, tekoälyllä voisi seurata vahvistamattomien raakahavaintojen ilmestymistä tilannekuvaan ja tehdä näiden perusteella ennusteita mahdollisen uhan laadusta, koosta ja suhteellisesta voimasta.

Kasvavaa kansainvälistä harjoittelua ja yhteistoimintaa ajatellen TAK-ohjelmistoilla voidaan kivuttomasti liittää eri joukkojen tilannekuvajärjestelmiä toisiinsa. TAK-ohjelmistoista löytyvät valmiit federointiominaisuudet ja standardoitu CoT-protokolla mahdollistavat tilannekuvamerkkien ja johtamisviestien hallitun siirron eri palvelimien välillä.

Lopuksi

Tulevaisuuteen katsottaessa joudutaan arvioimaan SBU-konseptin kaltaisten johtamisjärjestelmien tarpeellisuuta. Nopeasti kehittyvien siviiliteknologioihin, -päätelaitteisiin ja osittain myös -tietoliikenneverkkoihin nojaavat ratkaisut tuskin korvaavat operatiivisia ja turvaluokiteltuja johtamisjärjestelmiä, mutta ne voivat toimia niitä täydentävinä ja niiden rinnalla. Tietyissä tilanteissa voidaan törmätä päällekkäisyyksiin, mutta tällöinkin hyödyt lienevät haittoja suuremmat.

Olisiko SBU-konseptin mukaisia johtamisjärjestelmiä syytä edistää? Mielestäni olisi, koska reserviläisarmeijan tarpeet ovat monimuotoisia ja uusien teknologioiden esiinmarssi on sikäli nopeata, että uusia ratkaisuja tulee voida kokeilla ja opetella matalalla kynnyksellä. Reserviläisarmeijalla tulisi lisäksi tukea ratkaisuja, jotka mahdollistavat uusien innovaatioiden kehittämisen ja toteuttamisen reserviläisten itsensä voimin.

Viimeiseksi, reserviläisarmeija joutuu kaikissa tilanteissa optimoimaan panos-tuotos -suhdetta ja varmistamaan, että investoinnit ovat oikein mitoitettuja ja että ne eivät happane käsiin. Näihin tarpeisiin SBU-konseptilla on varmasti paljon annettavaa.

TEKSTI: JOUNI A KEMPPAINEN, AIRBUS DEFENCE AND SPACE OY

Operatiivista tehokkuutta turvallisella ryhmäviestinnällä

Turvallinen ja tehokas viestintä on avainasemassa operaatioissa, joissa on kysymys kansallisesta turvallisuudesta ja toiminnan jatkuvuudesta haastavissa tilanteissa. Tämä koskee erityisesti puolustusvoimia, pelastuslaitoksia ja muita turvallisuuskriittisiä organisaatioita, joiden on kyettävä varmistamaan viestinnän toimivuus kaikissa olosuhteissa. Airbusin Agnet-ryhmäviestintäratkaisu tarjoaa ratkaisun, joka yhdistää saumattoman viestinnän turvallisuuden ja skaalautuvuuden.

Agnet-ratkaisun ominaisuudet

Airbusin kehittämä Agnet-ratkaisu on suunniteltu tukemaan organisaatioiden operatiivisia kykyjä parantamalla viestintää, tiedonjakoa ja johtamista. Ratkaisu tuo salatun ryhmäviestinnän turvallisuuskriittisten organisaatioiden käyttöön hyödyntäen olemassa olevia 4G- ja 5G-verkkoja. Agnet voidaan toimittaa SaaS (Software as a Service) turvallisena pilvipalveluna. Lisäksi ratkaisusta on saatavilla toimitusversio, joka mahdollistaa TETRA-verkon käyttäjien integroimisen samaan viestintäpalveluun älypuhelimien kanssa, mahdollistaen yhteydenpidon eri viestintäkanavien välillä. Tämä on erityisen hyödyllistä organisaatioille, joissa viestintävälineiden kirjo on laaja ja kustannusten hallinta sekä operatiivinen tehokkuus edellyttävät eri laitteiden välistä yhteensopivuutta.

Ratkaisua on kehitetty tiiviissä yhteistyössä kriittisen viestinnän käyttäjien kanssa, mikä on varmistanut sen soveltuvuuden vaativiin toimintaympäristöihin. Agnet tukee tiimien, toimipisteiden ja yhteistyökumppaneiden välistä viestintää ja johtamista, tarjoten vaihtoehdon kuluttajakäytössä yleisesti käytetyille sovelluksille kuten WhatsApp, joita ei ole suunniteltu kriittisen viestinnän tarpeisiin. Palvelu mahdollistaa viestinnän turvallisen siirtämisen mobiililaajakaistassa ja tarjoaa lisäksi kartta- ja videopalveluita.

Teknologinen yhteensopivuus ja siirtymä uusiin viestintäkanaviin

Agnet-palvelun yksi merkittävimmistä eduista on sen yhteensopivuus nykyisten ja tulevien viranomaisverkkojen kanssa. ”Kriittisessä viestinnässä käytetään yhä laajalti perinteisiä radioita, mutta siirtyminen 4G- ja 5G-verkoissa tapahtuvaan viestintään on yleistymässä”, toteaa Airbusin tuotepäällikkö Marko Nurro. Tämä tarkoittaa, että organisaatiot voivat asteittain siirtyä uusien viestintäteknologioiden käyttöön hyödyntäen olemassa olevia verkkoinfrastruktuureja. Tällainen kehitysvaihe on menossa viranomaisverkoissa useissa Euroopan maissa kuten myös Suomen Virve-palvelussa.

Agnet tukee myös yhdyskäytäväratkaisuja, jotka mahdollistavat sen yhdistämisen esimerkiksi VHF-radiopuhelinjärjestelmiin. Tämä tarkoittaa, että älypuhelimen käyttäjät voivat kommunikoida suoraan VHF-radioiden käyttäjien kanssa, mikä parantaa viestintää erilaisissa kenttäolosuhteissa.

Nopeasti skaalautuva palvelu

Yksi Agnet-palvelun keskeisistä vahvuuksista on sen kyky skaalautua nopeasti ja tehokkaasti. Esimerkiksi kertausharjoituksiin osallistuvien satojen tai jopa tuhansien henkilöiden lisääminen viestintäjärjestelmään on mahdollista ilman viiveitä. Tämä on erityisen arvokasta suurissa harjoituksissa, joissa on tärkeää, että kaikki osallistujat saavat

reaaliaikaista tietoa ja voivat osallistua viestintään saumattomasti. Erilaisissa suuronnettomuusharjoituksissa on havaittu, että viestintä on usein haaste tehokkaalle toiminnalle – Miten jaetaan tieto mihin mennä ja mihin aikaan? Miten jaetaan kartta, josta osallistujat pystyvät suunnistamaan kohteeseen? Miten varmistetaan, että kaikki ovat tiedon saaneet ja lukeneet? Agnet-palvelussa nämä asiat voidaan hoitaa tehokkaasti perinteisen ryhmä- ja yksilöpuheen rinnalla.

Palvelu tallentaa kaiken viestinnän turvallisesti EU:n sisällä, ja viestit on suojattu päästä–päähän-salauksella. Tämä takaa, että kriittinen tieto on suojassa mahdollisilta kyberuhkilta. Lisäksi organisaatioilla on mahdollisuus säilyttää data paikallisesti omilla palvelimillaan, mikäli näin halutaan. Tämä joustavuus lisää luottamusta palveluun ja mahdollistaa sen käytön myös vaativissa turvallisuusympäristöissä. Tyypilliset Agnet-palvelun käyttäjäorganisaatiot ovat viranomaisten lisäksi erilaisia turvallisuustoimijoita, yksityisiä turvapalveluita, jalostuslaitoksia, satamia ja isojen tapahtumien järjestäjiä. Tämän tyyppiset organisaatiot toimivat ympäristössä, joissa voi häiriötilanteessa syntyä mahdollisuus

ihmis- ja omaisuusvahingoille sekä mittaville luonnonkatastrofeille.

Organisaation pääkäyttäjä määrittää palvelun asetukset selainpohjaisessa hallintajärjestelmässä, jonka jälkeen käyttäjät voivat ladata Agnet Work -sovelluksen älypuhelimeensa ja aloittaa viestinnän. ”Älypuhelin löytyy lähes kaikilta, joten organisaatioiden ei tarvitse erikseen kilpailuttaa laitetoimittajia tai odottaa toimituksia. Tämä vähentää viestintäjärjestelmän käyttöönottoon liittyviä kustannuksia ja nopeuttaa sen käyttöönottoa. Palvelun päästä–päähän-salaus täyttää vaativimpienkin käyttäjien tarpeet”, kiteyttää Airbusin markkinointipäällikkö Jouni Kemppainen.

Turvallisuus ja operatiivinen tehokkuus

Turvallisuus on ensiarvoisen tärkeää kaikissa viestintäratkaisuissa mutta erityisesti silloin, kun kyse on kansallisesta turvallisuudesta. Agnetin tarjoama päästä–päähän-salaus varmistaa, että kaikki viestit ja tiedonsiirto ovat suojattuja. Agnet-ratkaisun Multi-tenant SaaS toimitusversio on ISO 27001:2022 tietoturvahallintasertifioitu. Tämä on olennaista operaatioissa, joissa viestinnän eheyden säilyttäminen on kriittistä. Esimerkiksi kertausharjoituksissa tai kriisinhallinnassa on ratkaisevaa, että oikeat henkilöt saavat tiedon nopeasti ja turvallisesti.

Agnetin avulla puolustusvoimat ja muut turvallisuuskriittiset organisaatiot voivat hyödyntää monipuolista viestintäteknologiaa, joka yhdistää ääni-, data- ja videopalvelut yhdelle alustalle. Tämä mahdollistaa saumattoman viestinnän eri laitteiden ja tarvittaessa eri verkkojen välillä, mikä parantaa joukkojen välistä koordinaatiota. Palvelu tukee myös paikannuspalveluita, jotka tarjoavat reaaliaikaista tilannekuvaa kentältä. Tämä lisää johtamisen tehokkuutta ja parantaa operaatioiden onnistumista.

Erityisesti suurissa harjoituksissa, kuten kertausharjoituksissa, Agnet tarjoaa mahdollisuuden reaaliaikaiseen viestintään ja videon suoratoistoon vaikkapa drooneista tai vartalokameroista. Tämä antaa komentajille kattavan tilannekuvan harjoituksen kulusta ja mahdollistaa oikeiden päätösten tekemisen oikea-aikaisesti. Järjestelmän joustavuus mahdollistaa myös henkilöstömuutokset reaaliajassa, mikä varmistaa, että oikeat henkilöt ovat aina tavoitettavissa ja osallisina keskustelussa.

Laaja verkkoyhteyksien hyödyntäminen ja toimintavarmuus

Agnet on suunniteltu toimimaan saumattomasti eri verkkoympäristöissä, mikä takaa sen toimintavarmuuden kaikissa olosuhteissa. Se integroituu TETRA- ja 4G/5G-verkkoihin, mutta tukee myös satelliittiyhteyksiä, mikä varmistaa viestinnän jatkuvuuden tilanteissa, joissa maaverkot eivät ole käytettävissä. Esimerkiksi sähkökatkosten, sabotaasin tai luonnonkatastrofien sattuessa satelliittiyhteydet takaavat, että viestintä ei keskeydy ja kriittinen tieto kulkee nopeasti ja turvallisesti.

Satelliittiyhteyksien hyödyntäminen on erityisen tärkeää silloin, kun toimitaan syrjäisillä tai haastavilla alueilla, joissa maanpäälliset verkot eivät välttämättä ole saatavilla. Tämä parantaa organisaatioiden valmiutta toimia tehokkaasti kaikissa olosuhteissa ja mahdollistaa viestinnän jatkuvuuden myös kaikkein vaikeimmissa toimintaympäristöissä. Satelliittiyhteyden luotettavuutta on testattu tutkimusprojektissa kesällä 2024, yhdessä eri osapuolten kanssa. Tulokset osoittivat, että uudella matalan kiertoradan (LEO, Low Earth Orbit) OneWeb -satelliittiviestinnällä saavutetaan lyhyt latenssi ja korkea yhteysnopeus. Kenttätestissä keskityttiin liikkuvan yhteyden suorituskyvyn tutkimiseen liikkuvassa ajoneuvossa. Vaikka meillä Suomessa on maailman parhaat maanpäälliset verkot, ja 99% ajasta nämä verkot ovat tarpeeksi hyviä, ne eivät kuitenkaan ole riittäviä organisaatioille, jotka ylläpitävät yhteiskunnan turvallisuutta ja vakautta.

Joustava käyttöönotto eri tarpeisiin

Agnet-palvelun käyttöönotto on suunniteltu joustavaksi, jotta se vastaisi erilaisten organisaatioiden tarpeisiin. Se voidaan toteuttaa julkisena, yksityisenä tai hybridipilvipalveluna, mikä tarjoaa organisaatioille mahdollisuuden hallita viestintäinfrastruktuuriaan tarpeidensa mukaisesti. Tämä joustavuus varmistaa viestinnän vakauden ja turvallisuuden eri tilanteissa ja ympäristöissä.

Esimerkiksi organisaatiot, jotka toimivat useiden eri viranomaisten kanssa, voivat hyödyntää Agnet-palvelua moniviranomaistehtävissä, jolloin viestintä yli organisaatiorajojen on sujuvaa ja turvallista. Tämä on erityisen hyödyllistä kriisitilanteissa, joissa eri toimijoiden välinen yhteydenpito on ratkaisevan tärkeää.

Tulevaisuuden ratkaisuja turvalliseen viestintään

Teknologian edistys tuo mukanaan uusia viestintäratkaisuja, kuten Galileo PRS -paikannusjärjestelmän. Tämä satelliittipaikannusjärjestelmä tarjoaa viranomaisille entistä tarkempaa ja suojatumpaa paikannusta, mikä parantaa operaatioiden turvallisuutta ja tehokkuutta erityisesti tilanteissa, joissa kaupalliset paikannuspalvelut ovat alttiita häiriöille.

Galileo PRS tarjoaa korkeatasoisen turvallisuuden ja häirinnänkestävyyden, mikä tekee siitä erinomaisen työkalun operaatioihin, joissa turvallisuuden säilyttäminen on kriittistä. Tämä teknologia yhdistettynä Agnet-ryhmäviestintäpalveluun ja satelliittiyhteyksiin antaa organisaatioille mahdollisuuden hyödyntää olemassa olevaa viestintäinfrastruktuuria ja laitteita sekä integroida niihin uusia palveluita.

Kirjoittajaesittely

Jouni on työskennellyt kriittisen viestinnän parissa yli 10 vuotta ja on kiinnostunut tukemaan käyttäjiä kehittämään toimintojaan modernien ryhmäviestintäpalveluiden avulla. Hän on ollut mukana kehittämässä innovatiivisia digitaalisia ratkaisuja, kuten (triage) potilasluokittelua kenttäkäyttöön, ja hänellä on laaja kokemus kriittisen viestinnän käyttäjistä ja heidän tarpeistaan Euroopassa.

https://criticalcommunications.airbus.com/en/newsroom/web-story/airbus-demonstrates-low-latency-satellite-services-on-a-moving-vehicle-across-northern-finland

https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/satelliittipaikannus/galileon-viranomaispalvelu-prs

criticalcommunications.airbus.com/en/agnet

Kirjoittaja toimii Viestikiltojen Liitto ry:n puheenjohtajana.

TEKSTI: TERO PALOKANGAS, KUVAT: JUHA PELTOMÄKI

Viestikilloissa vaalitaan perinteitä, selvitetään uusia yhteistyömuotoja sekä haetaan askelmerkkejä tulevaisuuteen

Viestikiltojen Liitto Ry:ssä on jatkettu 2023 käynnistettyä strategiatyötä, jossa pyritään määrittämään mitä viestikillat haluavat olla vuonna 2030 osana toimialan vapaaehtoiskenttää. Toinen merkittävä kehityshanke on yhteistyön tiivistäminen Tykkimiehet Ry:n ja Pioneeriaselajin Liitto Ry:n kanssa. Perinteiden vaalimiseen liittyen on puolestaan käynnissä varsin mielenkiintoisia hankkeita liittyen Päämajan viestikeskus Lokkiin sekä viestihistoriallisiin muistomerkkeihin ja -laattoihin.

Yhdessä vahvempia

Viestikiltojen liitossa on jatkettu vuonna 2023 aloitettua strategiatyötä. Se on linkitetty liiton valtuuskunnan johtamaan koko toimialan vapaaehtoiskentän selvitystyöhön, johon puolestaan on saatu ohjaus Puolustusvoimien toimialajohdolta. Keskeisenä olemassaolon edellytyksenä viestikilloissa on tunnistettu ainakin laadukkaiden koulutustapahtumien järjestäminen, ennen kaikkea on kyettävä jatkossakin tukemaan MPK:n sotilaallisia valmiuksia edistäviä koulutustapahtumia. Toiminnan on lisäksi oltava jatkossakin riittävän monipuolista, ja kyettävä tarjoamaan jäsenistölle merkityksellistä sisältöä, jota muualta ei ole saatavissa. Erityisesti nuorempaa väkeä pitäisi saada nyt vahvasti ikääntyvään viestikiltatoimintaan mukaan. Liitto on samalla valmis avoimesti keskustelemaan omasta roolistaan ja tehtävistään osana toimialan vapaaehtoiskentän kokonaisuutta. Yhden toimialan kattojärjestön mallia tulee mielestäni jälleen kerran vakavasti tarkastella, jakaantuneet vastuut ja resurssit eivät lähtökohtaisesti parhaalla mahdollisella tavalla edesauta yhteisen tavoitetilan saavuttamista.

Viestikiltojen Liitto Ry on käynnistänyt myös yhteistyön tiivistämistä Tykkimiehet Ry:n ja Pioneeriaselajin Liitto Ry:n kanssa. Yhteistyön tiivistäminen juuri näiden yhdistysten kanssa on luontevaa yhteisen museomme (Militaria) kautta, yhteistyöverkostot ovatkin jo museon kautta alustavasti rakennettu. Olemme tähän asti muun muassa jakaneet tietoa toistemme järjestämistä tapahtumista. Maaliskuun lopussa tulemme järjestämään järjestöjen yhteistyötilaisuuden Museo Militariassa, johon osallistuvat yhdistysten hallitusten lisäksi aselajiemme tarkastajat Mikkelistä. Tuossa tilaisuudessa on tavoitteena kyetä tunnistamaan entistä paremmin nyt hyvin käynnistyneen yhteistyön tiivistämismahdollisuudet. Toimintavuoden aikana tullaan yhtenä esimerkkinä selvittämään pioneerien Hakku-harjoituksen mahdollisuuksia toimia jatkossa myös viesti- ja johtamisjärjestelmien sekä tulenjohdollisten kokonaisuuksien koulutustapahtumana. Eri aselaji- ja toimialaliittojen välisessä yhteistyössä on joka tapauksessa jatkossa nähtävä merkittävä toiminnan aktivoimisen mahdollisuus – yhdessä ollaan tässäkin asiassa varmuudella vahvempia kuin jokainen erikseen.

Museo Militaria jatkaa menestyskulkuaan

Vaikka Viestimuseon lakkauttaminen Riihimäellä oli aikoinaan shokki ja aiheutti huolta perinteiden vaalimisen osalta, on Museo Militaria osoittautunut lopunperin äärimmäisen onnistuneeksi ratkaisuksi. Museota ylläpitää Suomen Tykistö-, Pioneeri- ja Viestimuseoyhdistys ry (STPVMY Ry), jossa Viestikiltojen Liitto toimii yhtenä jäsenyhdistyksenä koko toimialan yhteisten etujen vaalijana. Vuosi 2024 oli järjestyksessään yhdistyksen kolmastoista ja Museo Militarian kahdestoista toimintavuosi. Yhdistys ja Museo Militaria ovat vakiintuneita toimijoita sota- ja sotilashistoriallisessa museokentässä. Museon näyttelyiden, tapahtumien sekä kokoelma- ja muiden palveluiden tuottaminen yleisölle, tutkijoille ja sota- ja sotilashistorian harrastajille on ollut laadukasta, ja palvelut on kyetty tuottamaan kustannustehokkaasti. Tämä on perustunut museotoiminnan kehittämisen ja ylläpitämisen jänteviin sekä toteuttamiskelpoisiin suunnitelmiin, talouskuriin sekä tarvittaessa nopeisiin päätöksiin ja niiden toimeenpanoon.

Koko vuoden kävijämäärissä vuosi 2024 oli museo Militarian historian toiseksi vilkkain. Näyttelyissä kävi yhteensä 25 109 henkilöä. Museotoiminnan painopistealueita vuonna 2024 olivat perusnäyttelyuudistuksen käynnistäminen sekä kokoelmatyön kehittäminen. Perusnäyttelyuudistuksessa viimeisteltiin 1920- ja 1930-lukujen osiota. Osio saatiin pääosin valmiiksi, mutta se täydentyy vielä kevätkauden 2025 aikana teknisillä ratkaisuilla ja kuuntelupisteellä. Museotoiminnan painopistealueena vuonna 2025 jatkuu perusnäyttelyuudistus, joka jatkuu vielä vuoteen 2026. Kokoelmatyön perustana käytetään vuonna 2024 ja edelleen vuonna 2025 jatkettavaa päivitettyä museon kokoelmaohjelmaa. Kehotankin lukijoita käymään aktiivisesti meidän yhteisessä museossamme, vaihtuvat teemanäyttelyt sekä etenevä perusnäyttelyuudistus takaavat, että käyntikerta on varmasti aina mielenkiintoinen ja ajankäytön arvoinen.

Viestikiltojen Liiton järjestämät viestimiespäivät ovat erinomainen tilaisuus koko toimialan eri toimijoiden väliselle verkostoitumiselle. Kuvia vuoden 2024 elokuun viestimiespäiviltä, jotka järjesti Etelä-Hämeen Viestikilta Riihimäen–Räyskälän–Hämeenlinnan alueella.

Viestikeskus Lokin kunnostuksesta ja muistolaattaprojektista

Jatkosodan aikainen Päämajan viestikeskus Lokki on Mikkelin Naisvuoreen louhitun kallioluolaston kattotilan osalta todettu edelleen turvattomaksi, ja Lokki on pysynyt viime vuosina suljettuna. Lokki-näyttely on ollut yleisölle avoinna Päämajamuseon tiloissa. Näyttelyn yhteydessä on esitetty myös Lokista kertovaa dokumenttifilmiä. Viime vuoden puolella ajatus Lokin kunnostuksesta nosti taas päätään, ja sen valmistelun edellyttävää yhteistyöverkostoa aktivoitiin Kaakkois-Suomen viestikillan toimesta. Iloinen uutinen saavutettiin loppuvuodesta, kun eduskunnan jakaessa joulurahaansa viestikeskus Lokille myönnettiin sadan tuhannen euron avustus. Tästä iso kiitos kuuluu Varsinais-Suomen viestikillan edustaja Juhani Pilpolalle sekä kansanedustaja Jari Ronkaiselle. Parhaillaan on käynnissä Lokin kunnostukseen liittyvä hankeselvitys, jonka myötä selviää myös kunnostukseen tarvittava lopullinen kokonaisrahamäärä. Lokista onkin jälleen muodostumassa merkittävä toimialallinen hanke, johon toivotaan mahdollisimman monen yhteistyötahon ja yrityksen jatkossa osallistuvan: kaikille riittää varmuudella roolia ja tekemistä.

Viestijoukkojen 50-vuotissyntymäpäivänä 5.3.1968 Riihimäellä paljastetusta valtakunnallisesta viestimuistomerkistä alkaen ovat Viestikilta ry ja sen paikallisosastot, sekä vuonna 1989 perustettu Viestikiltojen Liitto ry jäsenkiltoineen, perustaneet muistomerkkejä ja kiinnittäneet muistolaattoja viestihistoriallisesti merkittäviin kohteisiin eri puolilla Suomea. Liitto ei vuonna 2024 paljastanut uusia muistolaattoja. Sen sijaan toimintavuonna aloitettiin jo paljastettujen muistomerkkien ja -laattojen tietojen kokoaminen. Samalla varmistetaan jo paljastettujen muistomerkkien ja -laattojen kunto, sekä toteutetaan niiden tarvitsemat puhdistus- ja ehostustoimenpiteet. Ajatuksena on, että kerätyt tiedot paljastetuista muistomerkeistä ja -laatoista sekä niiden taustalla olevasta viestihistoriasta tullaan aikanaan julkaisemaan havainnollisessa muodossa Viestikiltojen Liitto Ry:n kotisivuilla. Näin varmistetaan näiden sotahistoriallisesti merkityksellisten tietojen käytettävyys myös jatkossa. Hanketta tukee rahallisesti Maanpuolustuksen viestisäätiö.

Lopuksi

Viestikiltojen liitossa ja sen jäsenkilloissa tehdään jatkossakin pyyteetöntä vapaaehtoistyötä osana kokonaismaanpuolustustamme. Toivottavasti mahdollisimman moni kokee jatkossakin mahdolliseksi osallistumisen viestikiltatoimintaan, tai sen konkreettisen tukemisen. Tässäkin asiassa olemme juuri niin vahvoja kuin yhdessä haluamme olla. Toivotan samalla kaikille menestystä toimintavuodelle 2025.

Viestikiltojen liitto jatkoi A.R. Saarmaan päivään liitettyä ajankohtaisseminaariperinnettä, jonka johti liiton varapuheenjohtaja ja koulutuspäällikkö Juha Peltomäki teemalla ”Jalat poterossa, katse avaruudessa”.

KUTSU VIESTIUPSEERIYHDISTYS RY:N KEVÄTKOKOUKSEEN

Viestiupseeriyhdistys ry:n hallitus kutsuu yhdistyksen jäsenet **kevätkokoukseen Helsinkiin, ELISAn tiloihin Pasilaan, torstaina 24.4.2025 klo 14.00 alkaen**.
Käyntiosoite: Ratavartijankatu 5, Helsinki

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 ELISAn tiloihin klo 14.00 mennessä
- Kahvit klo 14.00-14.30
- Kevätkokous klo 14.30-15.30
- ELISA ja sen toimintojen esittely 15.30-17.00
- Tilaisuuden päättäminen noin klo 17.00.

Julkisilla pääsee Pasilan asemalle ja sieltä kävellen ELISAn tiloihin.

Omalla autolla saapuminen: Elisalla on asiakkaille maksuton pysäköintihalli aivan Ratavartijankadun päässä, Resiinaparkin jälkeen. Kadun päässä on kääntöpaikka, jota ennen oikealla on asiakaspysäköinnin sisäänkäynti. Auton voi ajaa K1-kerroksen asiakaspaikoille, josta ohjaus Elisan aulaan. Mikäli asiakaspysäköinnin näyttötaulu näyttää täyttä, lisää pysäköintipaikkoja on viereisessä Resiinaparkissa (pysäköinti omakustanteisesti). Resiinaparkin ylimmästä kerroksesta on ohjaus Elisa-kyltein Elisan asiakaspysäköinnin puolelle.

Ilmoittautumiset 15.4.2025 mennessä tai vaikka samantien www.viestiupseeriyhdistys.fi -sivuilla olevalla lomakkeella (toivottavin tapa), sähköpostitse toiminnanjohtaja@viestiupseeriyhdistys.fi tai puhelimitse 040 514 2497.

Tervetuloa kevätkokoukseen!

Viestiupseeriyhdistys ry:n hallitus

TEKSTI:JYRKI PENTTINEN

Telealan uutisia

Yhdysvaltojen puolustusvoimat ja 5G:n integrointi

National Defense Magazine toteaa, että Yhdysvaltain puolustusministeriö DoD (U.S. Department of Defense) on jatkanut tutkimuksia 5G:n käytettävyydestä maanpuolustuksen viestinnässä. Erityisesti kehittyneen vaiheen 5G Advanced tukee jo käytännössäkin selkeästi korkeampia datanopeuksia, matalampia yhteysvälin viiveitä ja korkeampaa luotettavuutta aiempiin verkkosukupolviin verrattuna. Nämä 5G:n spesifioidut peruspilarit ovat oleellisia puolustusvoimien kriittisissä sovelluksissa, ml. taistelukentän reaaliaikainen tarkkailu, miehittämättömien ilma-alusten kuten droonien hallinta ja operointi, ja sotilasjärjestelmien kehittynyt komento ja ohjaus (C2, Command & Control). Riippumatta 5G:n mahdollistamasta laajasta kapasiteetista ja riittävästä suorituskyvystä, kaupallisten 5G-verkkojen soveltuvuus sotilasjärjestelmiin on vielä haasteellista korkean suojaustason vaatimuksista johtuen. Lisäksi sotilasverkot toimivat tyypillisesti kaupallisten matkaviestinverkkojen taajuuksista erillään, mikä vaatii erillislaitteita. Eräänä ratkaisuna ovat sotilaskäyttöön räätälöidyt 5G-pohjaiset erillisverkot (Non-Public Network, NPN). [1]

Defencescoop puolestaan mainitsee, että Pentagonilla on tällä välillä alustuksia liittyen aikakauteen 5G:n jälkeen (”Beyond 5G”), mikä tarkoittaa tulevaan 6G-järjestelmään varautumista. Pentagon on jo aloittanut projekteja, joiden tarkoitus on kehittää seuraavan sukupolven teknologioita. Nämä soveltavan tieteen tutkimushankkeet sisältävät näkökohtia esimerkiksi taistelijoiden uuden sukupolven radiospektrin käytöstä ajoneuvojen hallintaan. Tutkimusten tavoitteena on toteuttaa kehittyneitä verkkoja, jotka mahdollistavat riittävän nopean ja viiveettömän datan Pentagonin intressisovelluksiin, kuten robotiikkaan, autonomiaan, virtuaalitodellisuuteen ja kehittyneeseen havainnointiin. [2]

Yhdysvaltojen merivoimien yhteistyö Starlinkin kanssa

Wired raportoi USA:n merivoimien yhteistyöstä SpaceX:n Starlinkin kanssa kehittäen ja laajentaen nykyisiä yhteysmenetelmiä. Merivoimat testaa Starlink-satelliitteja ja niiden mahdollistamia korkean bittinopeuden Internet-yhteyksiä Sailor Edge Afloat ja Ashore (SEA2) -alustustensa kautta. Merivoimien aiemmat satelliittiyhteydet alkavat olla jo hitaita nykypäivän standardeilla siinä, kun Starlinkin ja muiden kaupallisten satelliittijärjestelmien kautta saavutetaan 30–50 Mb/s, joka voidaan skaalata edelleen arvoon 1 Gb/s erillisantenneja käyttämällä. Järjestelmä on jo valmiina USS Abraham Lincoln- ja USS Gerald R. Ford -aluksilla. Huolimatta hyödyistään, puolustusvoimien ulkopuolisena järjestelmänä Starlinkin kyberturvallisuus on todettu potentiaaliseksi haittapuoleksi. [3]

Teleoperaattoreiden AI-integrointi

Teleoperaattorit ottavat käyttöön lisääntyvissä määrin keinoälyä (artificial intelligence, AI), koska sen erityisenä hyötynä on mahdollisuus optimoida matkaviestintäverkkojen suorituskyky automaattisesti. Muita keinoälyn hyötyjä operaattoreille ovat automatisoitu asiakaspalvelu personoituihin asiakaskokemuksiin sekä operatiivisen tehokkuuden parantaminen. Telealan keinoälysovelluksia ovat mm. ennustava huolto, joka toteutuu keinoälyn mahdollistamilla ennakkoanalyyseillä, jotka indikoivat luotettavasti tulevia laitevikoja jo ennen kuin ne ilmenevät käytännössä. Keinoälyn soveltaminen matkaviestintäverkoissa tuo siten operatiivisia ja liiketaloudellisia hyötyjä, parantaen palvelun tasoa ja laskien operointikustannuksia. [4]

Kanada laajentaa valokuituverkon jakoa

Reuters raportoi, että Kanadan radio- ja televisiokomissio (Canadian Radio-television and Telecommunications Commission CRTC) on päättänyt, että helmikuusta 2025 lähtien Kanadan hallitsevien teleoperaattoreiden on jaettava valokuituinfrastruktuuriaan pienempien kansallisten Internetiä tarjoavien kilpailevien operaattoreiden kanssa. Ratkaisu mahdollistaa kuluttajille laajemman tarjonnan mistä valita nopean nopeuden Internet-palvelu nykyistä edullisimmilla hinnoilla, samalla motivoiden ekosysteemiä jatkamaan investointeja korkean luokan verkkoihin. Aiemmin kyseinen määräys oli koskenut vain Ontarion ja Quebecin alueita, mutta tästä lähtien se koskee koko maata. [5]

Lähteet

[1] L. Heckmann, “Military Struggles to Make Inroads With 5G Commercial Wireless Tech,” National Defense, 8/2024. https://www.nationaldefensemagazine.org/articles/2024/8/5/military-struggles-to-make-inroads-with-5g-commercial-wireless-tech

[2] M. Easley, “Beyond 5G: Pentagon sets sights on next-generation wireless tech with new projects,” Defensescoop, 8/2024. https://defensescoop.com/2024/08/13/beyond-5g-pentagon-sets-sights-next-generation-wireless-tech-new-projects/

[3] J. Keller, “The US Navy Is Going All In on Starlink,” Wired, 9/2024. https://www.wired.com/story/us-navy-starlink-sea2

[4] J. Kelly, “10 Telecom Industry Trends to Know in 2024,” 5/2024. https://www.invoca.com/blog/telecom-industry-trends

[5] Reuters, “Canada regulator expands internet network-sharing provision to telcos nationwide,” 8/2024. https://www.reuters.com/business/media-telecom/canada-regulator-expands-internet-network-sharing-provision-telcos-nationwide-2024-08-13/

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

Kapt E Rajahalme, Kapt J Vuohelainen

Prikaatin alueellisen ja johtosuhteiden mukaisen viestiverkon hyvyyden vertailu

Johdanto

Sotakorkeakoulun viestiteknillisellä opintosuunnalla suoritettiin järjestelmäanalyysin harjoitustyönä vuoden 1974 syksyllä prikaatin kahden eri periaatteella rakennetun viestiverkon hyvyyden vertailu, josta seuraavassa esitetään lyhennelmä.

Työn tarkoituksena oli kahden samasta materiaalista rakennetun viestiverkon keskinäisen paremmuuden määrittäminen. Työn tuloksena saatua menetelmää voitanee käyttää monimutkaisempienkin kenttäviestiverkkojen vertailuun.

PERUSTEITA

Rajoitukset

Prikaatin johtosuhteiden mukaisella viestiverkolla ymmärretään seuraavassa suoraan johtosuhteiden mukaisesti rakennettua tähtiverkkoa, joka ei sisällä muita kuin johtoportaiden tarvitsemia viestikeskuksia. Silmukointi tapahtuu ainoastaan alajohtoportaiden toimesta.

Prikaatin alueellisella viestiverkolla tarkoitetaan silmukkaverkkoa, jonka viestikeskuksina toimivat johtoportaiden viestikeskusten lisäksi alueelliset viestikeskukset. Näillä on myös radioliikenteen välitys- ja tai releointitehtävät VHF-alueella.

Työssä jätettiin aselajien viestiresurssit sekä yleisen puhelinverkon hyväksikäyttö tarkastelun ulkopuolelle. Prikaatin viestiresursseina otettiin huomioon ainoastaan viestikomppanian henkilöstö ja materiaali.

Yhteyksien tärkeyden huomioon ottaminen

Yhteyksien arvoa käyttäjilleen voidaan tarkastella usein eri perustein. Siviilikäytössä olevissa viestiverkoissa tärkeimmät kriteerit ovat tavallisesti taloudellisia. Nämä eivät voi olla sotilasverkoissa ratkaisevia, joskin taloudelliset tekijät on otettava rauhan ajan suunnittelussa tarkasti huomioon.

Työryhmä suoritti eri yhteysvälien keskinäisen tärkeyden määrittämisen subjektiivisin perustein suorittaen Sotakorkeakoulun oppilaiden keskuudessa mielipidekyselyn, jonka perusteella laskettiin painokertoimet osaverkoille ja niiden yhteysväleille.

Saatujen painokertoimien avulla voidaan nyt seuraavassa ominaisuuksittain tapahtuvassa tarkastelussa ottaa kunkin yhteyden tärkeys huomioon laskettaessa eri yhteyksien hyvyyslukujen perusteella koko verkolle ominaisuuskohtaisia hyvyyslukuja.

Painotusta voidaan jatkaa edelleen määrittämällä painokerroin kullekin tarkasteltavalle ominaisuudelle. Tarkasteltavaksi valittiin siirron laatu, operatiivinen luotettavuus, verkon rakentamisaika, yhteyksien saamiseen kuluva aika, materiaalin käyttö ja henkilöstön käyttö.

Tällöin verkon kokonaishyvyysluku (H_{kok}) saadaan kaavasta $H_{kok} = \Sigma P_k H_k$

P_k = ominaisuuden painokerroin

H_k = ominaisuuskohtainen hyvyysluku

Vihollisvaikutuksen huomioon ottaminen

Vihollisvaikutus otettiin työssä huomioon vain joukkojen liikkeen ja elektronisen häirinnän osalta. Tulivaikutus jätettiin tarkastelun ulkopuolelle koetulosten puuttumisen takia. Viestivälineiden haavoittuvuus eri aseiden tulessa on erittäin hankala teoreettisesti hallittavaksi välineiden erilaisen suuruuden ja muodon sekä lujuuden takia. Johdinlinja poikkeaa oleellisesti putkilla varustetusta radiosta tai kenttäpuhelimista niiltä ominaisuuksiltaan, jotka vaikuttavat haavoittuvuuteen.

SIIRRON LAATU PUHELINVERKOSSA

Laadun kriteerin valinta

Puhelinverkon laadun kriteerinä käytettiin vaimennusta tai signaalikohinasuhdetta. Kyseessä olevissa verkoissa eivät siirrettävän taajuuskaistan leveys, vaimennusvääristymä, kulkuaika, kulkuaikavääristymä ja ylikuuluminen aiheuta olennaisia vaikeuksia. Kuitenkin on todettava, että kenttäjohdinyhteydellä vaimennusvääristymä aiheuttaa selvästi yläarajataajuuden putoamisen. Ylikuuluminen on taas yhteydellä vaikeasti hallittavissa, vaikka se voi kenttäviestiyhteyksillä olla huomattavaakin.

Johdinyhteyden siirron laatu

Yhteysväleille laskettiin vaimennus osavaimennusten summana. Siirron laatu arvosteltiin käyttäen alla esitettyjä rajoja.

0 Np≤A ≤3,8 Np hyvä yhteys (H)

3,8 Np<A ≤4,8 Np tyydyttävä yhteys (T)

4,8 Np<A ≤5,8 Np välttävä yhteys (V)

5,8 Np<A ei yhteyttä

Linkkiyhteyden siirron laatu

Linkkijänteelle oletettiin kiinteä signaalikohinasuhde. Ratkaisevaksi linkkiyhteyden laadulle muodostuu tällöin taso linkin sisäänmenossa. Kun linkkiä käytetään osana kaapeliverkossa, jonka vaimennukset ovat suuria, voi vaimennus ennen linkin sisäänmenoa olla niin suuri, ettei tason asettelu riitä kumoamaan vaimennusta. Moduloivan signaalin taso ei tällöin täytä vaatimuksia, mikä aiheuttaa aliohjauksen modulaattorissa. Vaikutus tulisi mitata kokeellisesti, mutta oletettiin nyt lineaariseksi.

Verkkojen laskenta

Verkkojen laskenta suoritettiin yhteysvälien kaikille mahdollisille reiteille. Jos yhteysvälillä oli useampia samanaikaisia reittimahdollisuuksia, otettiin tämä huomioon perustuen siihen ajatukseen, että yhteyden suuri vaimennus huonontaa ymmärrettävyyttä ja lisää puhelun keskipituutta. Syntynyt lisäliikenne voidaan kuitenkin välittää, jos käytettävissä on useamman johdon väylä.

Seuraavaksi suoritettiin hyvyyslukujen yhdistäminen, jolloin verkoille saatiin siirron hyvyysluvut. Oleellista eroa ei hyvyysluvuilla siis ollut. Alueellinen verkko oli kuitenkin hieman parempi. Liikenteen välityskyky alueellisella verkolla on parempi, mutta sen vaikutus ei kokonaisuudessaan näy saaduissa hyvyysluvuissa.

OPERATIIVINEN LUOTETTAVUUS

Luotettavuustekniikalla tarkoitetaan niitä tilastollisia, teknillisiä ja hallinnollisia menetelmiä, joiden tarkoituksena on mahdollisimman luotettavan tuotteen aikaan saaminen. Tavoitteena on usein taloudellinen optimiratkaisu, jossa tekijöinä ovat kehitys-, tuotanto- ja huoltokustannukset.

Luotettavuuden osalta määritellään seuraavat peruskäsitteet

Vika

Vioittumistodennäköisyys F(t)

Luotettavuus R(t)

Käyttövalmius A

Vikaväli m

Operatiivinen luotettavuus Ro.

Prikaatin puhelinverkon operatiivisen luotettavuuden laskeminen on suoritettu kahdessa osassa. Eri viestivälineiden A- ja R-arvojen lähtökohdat on arvioitu karkeina suuruusluokkina. Näillä suuruusluokilla ei tässä työssä ole olennaista merkitystä, vaan johtopäätökset voidaan tehdä ainoastaan kahden eri verkkomallin välisten luotettavuuksien eroavaisuuksista.

Koko järjestelmän luotettavuus (R) ja käyttövalmius (A) lasketaan osien rinnan ja sarjakäytön laskuperusteiden mukaisesti kullekin yhteysvälille. Tällöin saadaan esimerkiksi johtosuhteiden mukaisen verkon yhteyden luotettavuudeksi $Ro = R_{IV} \times A_{IV}$.

Alueellisissa viestiverkoissa tulevat rinnakkaisten laitteiden ja yhteysteiden merkitys mukaan. Tällöin ei päde enää suora kertolaskusääntö, vaan on otettava huomioon rinnakkaisten teiden varmentava vaikutus.

Tarkastelu antaa selvän kuvan alueellisen viestiverkon paremmuudesta operatiivisen luotettavuuden suhteen, vaikka käytetyt toimintavalmius- ja luotettavuusarvot eivät olisikaan lähellä oikeita arvoja. Painotuksen jälkeen saatiin koko verkon operatiivisen luotettavuuden hyvyysluvuksi alueelliselle verkolle 0,69 ja johtosuhteiden mukaiselle verkolle 0,52.

AIKA, HENKILÖSTÖ JA MATERIAALI

Aika

Verkon hyvyyttä voidaan tarkastella myös aikatekijöiden perusteella. Verkon rakentamiseen kuluva aika on oleellinen nopeasti vaihtuvissa tilanteissa. Toisaalta yhteyksien välittämiseen kuuluva aika on myös tarkastelun arvoinen, sillä se kuluu johtajilta hukkaan ja sen piteneminen aiheuttaa myös varausajan pitenemisen kautta liikenteen kasvun.

Puhelinverkon rakentamisessa ratkaisevin aikatekijä on linjanrakennukseen kuluva aika. Työssä laskettiin yhteyksien rakentamiseen kuluvat ajat kummallekin verkkomallille ja niiden yhteysväleille.

Henkilöstö

Prikaatin viestikomppania on suunniteltu rakentamaan ja ylläpitämään alueellista viestiverkkoa tietyn tehtäväjaon mukaisesti. Siksi johtosuhteiden mukaisessa verkossa jää enemmän henkilöstöä reserviin. Tätä voidaan pitää vähäisenä etuna verrattaessa verkkoja keskenään.

Verkkojen ylläpito sitoo vikapartio- ja huoltohenkilöstön suoraan verrannollisesti rakennettuun yhteyskilometrimäärään. Tässä suhteessa alueellinen verkko sitoo selvästi enemmän henkilöstöä ja on näin jonkinverran epäedullisempi.

Materiaali

Puhelinkaluston osalta hyvyys laskettiin reserviin jäävän materiaalin määrän perusteella. Alueellinen viestiverkko käyttää selvästi enemmän materiaalia.

Johtopäätökset

Rakentamisvertailu on tässä verkkomallissa edullinen alueelliselle viestiverkolle. Kuitenkin nopeissa tilanteissa johtosuhteiden mukainen verkko saadaan kokonaisuudessaan nopeammin valmiiksi. Alueellisen verkon paremmuuden takasi yhteyksien keskinäinen tärkeys, sillä tärkeimmät yhteydet valmistuivat siinä selvästi nopeammin kuin johtosuhteiden mukaisessa verkossa.

RADIOYHTEYDET JA HÄIRINTÄ

Ulkomaisen sotilasaikakausilehdistön julkaisemien tietojen perusteella muodostettiin vihollisorganisaation radioverkot sekä sen elektronisen häirinnän yksiköt kalustoineen. Näillä perusteilla tutkittiin radioyhteyden tahallista ja tahatonta häirintää ottaen huomioon vihollisen hyökkäyksen aiheuttama liike prikaatin puolustusaseman syvyyteen.

Vihollisen radioverkoissa toimii n 950 lähetintä 140 eri verkossa. Varsinainen käyttökanavan häirintätodennäköisyydeksi saatiin 0,13. Todennäköisyys, että sekä varsinainen että varakanava joutavat tahattoman häirinnän kohteeksi oli 0,02.

Releointi lisäsi kanavien päällekkäin osumistodennäköisyyttä, mutta pienensi oleellisesti häirintäetäisyyttä.

Tahallinen häirintä maasta käsin suoritettuna vaatii olennaisesti suurempia tehoja tai pienempää häirintäetäisyyttä, kun pitkiä jänteitä lyhennetään releasemia käyttäen. Ilmasta suoritettuun häirintään ei releointi tuo juuri apua häirinnän suuren ulottuvuuden vuoksi.

Vertailluilla verkoilla ei häirinnän siedon suhteen ollut oleellista eroa. Releointia käyttävä alueellinen verkko selvisi kuitenkin jonkinverran parempana tarkastelusta.

YHDISTELMÄ

Johtopäätöksenä voidaan todeta, että alueellinen verkko on ylivoimainen johtosuhteiden mukaiseen verkkoon nähden varsinkin, jos materiaalireserville ei anneta suurta painoa.

Tärkeimmiltä ominaisuuksiltaan, luotettavuuden ja siirron laadun osalta on alueellinen verkko jopa parempi, kuin numerot antavat odottaa, sillä suurempi liikenteenvälityskyky ei tule esitetyissä hyvyysluvuissa esille.

Korjauksina prikaatin viestiresursseihin pidettiin tarpeellisina linjanrakentajavoiman lisäämistä 2–4 puhelinryhmällä, jotka varustetaan joko 1…4-kanavaisilla linkkikalustoilla tai johdinlinjan rakennustarvikkeilla sekä siirtymistä aktiivisten johtojen käyttöön kaikilla keskusyhteyksillä.

Nyt tarkastellussa tilanteessa olisi kaksi puhelinryhmää pudottanut verkkojen rakentamisajan noin kolmestakymmenestä tunnista neljääntoista tuntiin johdinlinjoja rakentaen. Jos keskusjohdot olisi korvattu linkeillä, olisi kokonaisaika pudonnut viiden tunnin suurusluokkaan.

Työryhmän käsityksen mukaan ovat rakentamisajat vain nyt käsitellyissä verkoissa alueelliselle viestiverkolle edulliset. Normaalisti johtosuhteiden mukainen verkko pystytään rakentamaan nopeammin. Tällöin on rakentaminen suoritettava siten, että ensin saadaan johtosuhteiden mukainen verkko pystyyn ja siitä laajennetaan alueellinen verkko. Yhteyksien rakentamisjärjestys on oltava tärkeyden mukainen

- yhteydet alayksiköihin,

- yhteydet alayksiköiden kesken ja

- yhteydet huoltoon.

VHF-radioyhteyksillä on edullista lyhentää pitkiä yhteyksiä releoimalla. Releasemat voidaan sijoittaa alueellisten viestikeskusten yhteyteen. Tämä pienentää olennaisesti häirintämahdollisuuksia. Toisaalta häirinnän väistäminen tulee tällöin vaikeammaksi ja releoidun yhteyden operatiivinen luotettavuus on heikompi kuin suoran yhteyden.

50 vuotta sitten -palstan kirjoittaja: Pasi Puhakka

Viestimies

MEDIAKORTTI 2025

ILMOITUSHINNAT (ALV 0%)

1/1 s	950 €
1/2 s	600 €
1/4 s	400 €
Takakansi	1200 €
Määräpaikkalisä 20 %.	

ILMOITUSTEN KOOT

1/1 s A4	210 x 297 mm	bleed 3 mm
1/1 s	180 x 260 mm	
1/2 s	180 x 130 mm	vaaka
1/2 s	90 x 260 mm	pysty
1/4 s	90 x 130 mm	pysty
1/4 s	180 x 65 mm	vaaka

Aineistot:

PDF, CMYK Fogra Coated 27
Kuvien resoluutio: 300 dpi

AINEISTO-OSOITE:

juha.halminen@mediaosasto.fi

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

Esillä lehdessä – mukana päätöksiä tehtäessä!

AIKATAULU VUONNA 2025

Valmiin materiaalin toimitus

N:o	Aineistot	Ilmestyy
1:	31.1.	7.3.
2:	25.4.	30.5.
3:	15.8.	19.9.
4:	31.10.	5.12.

ILMOITUSMYYNTI

Juha Halminen
Gsm 050 592 2722
Sähköposti:
juha.halminen@mediaosasto.fi

PÄÄTOIMITTAJA

Kimmo Kaipainen
Gsm 040 722 2646
Sähköposti: viestimies@viestiupseeriyhdistys.fi

PAINOPAIKKA

Newprint Oy
Tuijussuontie 1
21280 RAISIO
Puhelin 010 231 2600
www.newprint.fi

JULKAISIJA

Viestiupseeriyhdistys ry
HELSINKI
Y-tunnus 0223897-9
ISSN 0357-2153

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