Viestimies

Viestiupseeriyhdistyksen julkaisu 81. vsk Numero 2 Kesä 2026

www.viestiupseeriyhdistys.fi

COMBITECH

Combitechin TEMPEST Center hyväksytty NATO- ja EU-tasolle

TEMPEST-hajasäteilymittaukset, toimitusvalvonta sekä asiantuntija- ja koulutuspalvelut – Combitechin TEMPEST Centerin vuosikymmenten osaamisella.

Combitech

www.combitech.fi/tempestcenter

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: Kimmo Kaipainen.

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 14.8.2026. Lehti ilmestyy viikolla 39.

Hyvää kesää!

Viestimies-lehti viettää kuluvana vuonna 80-vuotisjuhliaan. Juhlavuoden kunniaksi tämän vuoden numeroissa katsotaan myös menneeseen. Vuoden 1946 elokuussa julkaistussa Viestimies-lehden kautta aikain toisessa numerossa julkaistiin puheenjohtajan kynästä seuraava pääkirjoitus.

***

Viime tammikuussa pidetyssä Viestiupseeri-kerhon vuosikokouksessa päätettiin – lähinnä viestiupseerien ammattialan kysymysten käsittelemiseksi ja kerhon jäsenten yhteenkuuluvaisuuden lujittamiseksi – luoda kaksi uutta työmuotoa, nim. oman lehden julkaiseminen ja viestiupseeripäivien pitäminen.

Ensimmäinen tavoite on jo saavutettu: Viestiupseerikerhon lehti ”Viestimies” on julkaissut ensimmäisen numeronsa. Vallitseva aika kaikkinaisine puutteineen on kuitenkin asettanut tietyt rajoituksensa julkaisutoiminnalle, joten lehden painoasun suhteen tulee jatkuvasti olemaan toivomisen varaa. Kerhon jäsenten lehteänsä kohtaan tuntemasta harrastuksesta ”Viestimiehen” tulevaisuus ja jatkuva menestyminen lähinnä onkin riippuvainen, ja varsinaisesti heidän lähettämänsä julkaisumateriaalin turvin lehti pystyy jatkamaan ilmestymistään. Ja toisaalta: täten lehden sisältö kuvastaa sen tarpeellisuutta lukijakunnalleen.

Mitä tulee viestiupseeripäiviin, on Viestiupseerikerhon johtokunnan tarkoituksena järjestää ne syyskuun 13–14 päivinä Riihimäellä. Kuten toisaalla lehdessämme tarkemmin mainitaan, tullaan niillä esitelmien, alustusten ja keskustelujen muodossa käsittelemään ammattialan keskeisiä kysymyksiä. Uskomme tällaisen yhteisen neuvonpidon avartavan kerhon jäsenten näköaloja eri pääaselajien, maa-, meri- ja ilmavoimien piirissä.

Molemmat nämä uudet työmuodot ovat vielä tavallaan kokeiluluontoisia. Päämäärä, johon pyrimme – ammattitaitomme kohottaminen, näkemyksemme laajentaminen ja yhteenkuuluvaisuutemme lujittaminen – koituu jokaisen jäsenen hyödyksi. Siksi olkoon kunkin Viestiupseerikerhoon kuuluvan kunniakas velvollisuus työskennellä tämän päämäärän siivuttamiseksi! – Puheenjohtaja

***

Ilahduttavasti on todettava, että molemmat pääkirjoituksessa mainituista uusista työmuodosta jatkuvat omilla tavoillaan edelleen. Viestiupseeriyhdistyksen Viestimies-lehti on elänyt ajassa ja myös muovautunut ajan saatossa. Nykyisellään lehdessä käsitellään viestiaselajin lisäksi laajemmin johtamisjärjestelmäkentän asioita. Lehtemme onkin viesti-, johtamisjärjestelmä- ja ICT-alojen sekä kyberturvallisuuden päättäjien ja asiantuntijoiden lehti, joka jatkaa ilmestymistään lehteen tarjotun julkaisumateriaalin turvin.

Viestiupseeripäivien sijasta nykyään vietetään Viestimiespäiviä. Löydätkin kutsun vuoden 2026 Viestimiespäiville tämän numeron sivuilta.

Kokeiluluontoiseksi mainitut työmuodot ovat siis lopulta kestäneet aikaa ja palvelleet tavoitteitaan. Ammattitaidon kohottaminen, näkemysten laajentaminen ja yhteenkuuluvaisuuden lujittaminen vaikuttavat edelleen tavoittelemisen arvoisilta päämääriltä.

Tämän lehden ilmestyessä kesäkuu on aluillaan. 4.6. ylennettiin ja palkittiin taas ansioituneita. Lämpimät onnittelut kaikille ylennetyille ja palkituille! Kesäkausi tarjoaa toivottavasti meille kaikille mahdollisuuden nauttia suven lämmöstä ja yöttömistä öistä. Toivotankin kaikille lukijoille erittäin rentouttavaa kesää!

Ps. Oheisen 2/1946 numeron tyylikkään kansikuvan on piirtänyt taiteilija Urho Salomaa.

Kimmo Kaipainen

Päätoimittaja


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

Teksti ja kuvat: Kimmo Kaipainen

”Viestiupseeriyhdistyksen seminaari – Ukrainan sodan opit”

Jo neljä vuotta jatkunut Venäjän laiton hyökkäyssota Ukrainaa vastaan on saanut useat maat arvioimaan uudelleen kyvykkyyksiään vastata tämän päivän turvallisuusuhkiin, myös niistä pahimpiin. Viestiupseeriyhdistys järjesti keskiviikkona 29.4.2026 seminaarin tarkastelemaan Ukrainan sodasta saatuja oppeja ja niiden vaikutuksia johtamisjärjestelmiemme sekä kyber- ja informaatiopuolustuksemme järjestelyihin. Seminaaripaikkana toimi Helsingin yliopiston päärakennus.

Seminaarin avaus

Seminaarin aluksi Viestiupseeriyhdistyksen puheenjohtaja eversti (evp) Pertti Hyvärinen toivotti seminaariyleisön tervetulleeksi lähes 150 osallistujaa keräänneeseen tilaisuuteen. Viestiupseeriyhdistyksen toiminnassa seminaarit ovat olleet keskeisiä jo vuosikymmeniä. Ensimmäinen seminaari järjestettiin jo vuonna 1973.

Alan nopea kehitys on vuodesta toiseen taannut mielenkiintoiset ja haastavat seminaarisisällöt. Tälläkin kertaa monia mielenkiintoisia aihepiirejä jouduttiin rajaamaan käsittelyn ulkopuolelle. Ukrainan jo neljä vuotta jatkunut sota valittiin tämän vuoden seminaarin punaiseksi langaksi. Kukin puhuja tarjosi seminaarissa Ukrainan sodan oppeja omasta näkökulmastaan, sisältäen myös ajatuksia siitä miten näitä oppeja pystytään viemään käytäntöön. Seminaarin järjestelyissä arvokkaan tuen yhdistykselle mahdollisti Patria Oy. Verkostoituminen oli seminaari ytimessä tälläkin kertaa aivan yhdistyksen alkuperäisen perustamisajatuksen mukaisesti. Päivän seminaariohjelmassa edettiin Tero Palokankaan (VP Defence and Security Digia Oy) toimiessa tilaisuuden puheenjohtajana.

Puolustusvoimien tervehdys

Puolustusvoimien johtamisjärjestelmäalan tervehdyksen tilaisuuteen toi Pääesikunnan johtamisjärjestelmäosaston apulaisosastopäällikkö kommodori Petteri Kuosmanen. Kuosmasen näkemyksen mukaan Ukrainan sodan opit ovat oppeja sodan käynnin murroksesta. Oppien ytimessä on kysymys siitä miltä sota näyttää nyt ja tulevaisuudessa. Kuosmasen mukaan ennakointia ja varautumista tulee tehdä kaikkien, jotta olemme paremmin valmiit tulevaisuuden haasteisiin. Millä tavoin tulevaisuuteen tulee sitten varautua? 5 vuotta sitten nykyisen kaltainen turvallisuusympäristö vaikutti Kuosmasen mukaan epätodennäköiseltä. Nyt sodan liekit lyövät kuitenkin jo Itämerenkin rannoilla. Kamppailua käydään sekä fyysisessä että informaatioulottuvuudessa.

Kuosmasen mukaan Naton perusteita on haastettu ja Yhdysvaltojen läsnäolo Euroopassa ei ole enää itsestäänselvyys. Naton jäsenenä Suomi on etulinjan maa ja arktinen ulottuvuus on monilta osin keskiössä. Teknologiamurros on vaikuttanut sodan kuvaan tavalla, jota on ollut vaikea ennalta tunnistaa. Teknisestä näkökulmasta muutoksia ovat olleet läpinäkyvyys, elektronisen sodankäynnin vaikuttavuus, yhteyksien tarve laadulla ja määrällä mitattuna, laadun korvaaminen määrällä ja kalliin korvaaminen halvalla. Tekoälyn mahdollisuudet ovat myös hiipineet osaksi arkeamme.

Venäjä on Kuosmasen mukaan luottanut omiin vahvuuksiinsa. Massamaiseen kulutussotaan liukuma on kuitenkin ollut

Viestiupseeriyhdistyksen puheenjohtaja eversti (evp) Pertti Hyvärinen avasi vuoden 2026 seminaarin.

Venäjälle hämmästyttävän helppoa. Miten me sitten varaudumme? Kuosmasen mukaan me perehdymme sodan oppeihin ja sovellamme oppeja omaan operaatioympäristöömme. Kaikkea saatua ja tunnistettua ei kannata ottaa huomioon sellaisenaan. Opit sotakokemuksista tulee yleistää ja siirtää omaan ympäristöömme. Oppeja tulee peilata sotataidollisiin sodan käynnin periaatteisiin, jotka ovat kestäneet teknologiamuutokset ja toistuvat akateemisessakin tutkimuksessa. Kaikki kulminoituu lopulta johtamiseen ja sen yhtenäisyyteen. Ukrainalaiset ovat tässä Kuosmasen mukaan onnistuneet.

Lopuksi Kuosmanen huomautti, että Ukrainan sodan oppeja ei voi suoraan siirtää Suomeen, se olisi Venäjän aliarvioimista. Tulevaisuutta tulee tarkastella usealla eri aikaperspektiivillä. Tulee ymmärtää suuret kehityslinjat ja kokonaisuudet sekä ratkaista ongelmia nopeasti ja konkreet-

tisesti. Kuosmanen korosti tekniikan ja taktiikan vuorovaikutusta sekä sodankäynnin lainalaisuuksien ymmärtämistä, kun kehitämme omia suorituskykyjämme.

Ukrainan sodan oppeja

Suomalaisen ja eurooppalaisen puolustusteollisuuden kehittämistä ja teollisuuden Ukrainan oppeja käsitelleessä esityksessään Leadership Advisor Esa Rautalinko (Patria Oyj) nosti esiin eri toimijoiden roolit puolustuskyvyn rakentamisessa. Euroopan unioni on poliittinen ja taloudellinen liitto, joka yksinkertaistaen resursoi yhteisten hankkeiden kautta. Nato tekee yhteistä puolustussuunnittelua, ja ohjaa esimerkiksi teollisuutta standardoinnilla. Jäsenvaltiot toisaalta tekevät omia suvereeneja päätöksiään turvallisuuteensa ja puolustukseensa liittyen.

Naton artikla 3 edellyttää valtioiden omia toimia puolustuskyvyn ylläpitämiseksi. Eurooppalaisilla Nato-mailla on kuitenkin Rautalingon mukaan 1990-luvun alusta alkaen syntynyt merkittävä vaje puolustusinvestoinneissaan. Eurooppa panostaakin puolustusinvestointeihin jatkossa enenevissä määrin.

Suomessa puolustusteollisuuden kasvu on ollut merkittävää. Viennin osuus on yli puolet liikevaihdosta ja yhteenlasketun liikevaihdon määrä on kasvanut vuosittain. Myös Puolustus- ja ilmailuteollisuus (PIA) ry:n jäsenyritysten määrä on kasvanut. Alalla onkin Rautalingon mukaan mahdollisuus nousta yhdeksi Suomen talouden tukipilareista.

Keskeisiä oppeja Euroopalle on, että on rakennettava ”interchangebilityä”, eli kykyä vaihtaa suorituskykyjä tai varaosia liittolaisten kesken. Nykyisellään eurooppalaisten valtioiden kalusto on hajanaista ja keskenään erilaista, eikä kaluston vaihdettavuus valtioiden välillä ole itsestäänselvyys. Hankinta- ja päätöksentekomalleja on myös uudistettava. Nopea ja dynaaminen hankintojen tekeminen on haastavaa. Toisaalta taloudelliset tai henkilöstöresurssit eivät aina tue tarvittavaa varustautumisnopeutta.

Yhteishankkeet ovat teollisuudelle välttämättömyys ja niitä on lisättävä. Toimitusketjujen on oltava järeitä ja mahdollistettava vaihtoehtoisia kumppaneita. Teollisuuden investoinnit ovat kasvaneet voimakkaasti ja kasvavat edelleen. Tilausnäkymät, joita on hankala ennustaa pitkäjänteisesti eivät toisaalta teollisuuden näkökulmasta mahdollista kapasiteetin oikeanlaista mitoittamista.

Leadership Advisor Esa Rautalinko vastasi keskustelua herättäneen esityksensä jälkeen yleisökysymykseen. Kysymystä kuuntelemassa myös seminaarin puheenjohtaja Tero Palokangas.

Rautalingon ajatuksen mukaan ”perinteiselle kalustolle” on jatkossakin tarve. Teknologiamuutos edellyttää kuitenkin uusiakin tuulia. Vaikuttamisen yksikkökustannukset on saatava sopivalle tasolle, jotta yhteiskunta kestää pitkittyneessä kriisissä vaadittavat kustannukset. Kriittisiä materiaalikykyjä on oltava myös omalla maaperällä. Toisaalta tuotteiden valmistettavuuteen ja valmistuksen skaalautuvuuteen on kiinnitettävä entistä enemmän huomiota. Euroopan puolustusteollisuus kuitenkin investoi Rautalingon mukaan jatkuvasti.

Tutkija Jyri Lavikainen (Ulkopoliittinen Instituutti) käsitteli esityksessään ydinasepelotetta sodankäynnin välineenä Ukrainan sodassa. Pelote on Lavikaisen mukaan monin tavoin informaatiovaikuttamista, jonka kohdeyleisönä usein väestö, ei siis vain päättäjät. Tutkijoiden havaintojen mukaan ydinasepelote on toiminut nykyisissäkin sodissa suunnilleen peloteteorian esittämällä tavalla. Pelotteessa on kyse sanattomasta kaupankäyntiprosessista, jolla määritellään sallitun toiminnan rajoja. Tutkijoiden valtavirta on pitänyt vaaraa ydinaseiden käytöstä todellisena, mutta arvioi, ettei ydinaseita ei vieläkään käytetä kevein perustein.

Viimeisenä parina vuonna on Lavikaisen mukaan vahvistunut käsitys, että tukea Ukrainalle annettiin liian varovaisesti ja hitaasti, koska eskalaatiota, jopa ydinsotaa, pelättiin. Lännen toimissa on korostunut pyrkimys välttää Venäjän ydinaseiden käyttöä sen sijaan, että keskityttäisiin analysoimaan, miten sota voidaan pelotetta käyttämällä kokonaan estää tai sodan syttyessä omat tavoitteet saavuttaa. Sodan ennaltaehkäisyyn tulee siis panostaa. Pelote onkin sodankäynnin väline, jota täytyy hyödyntää. Pelotteen uskottavuus on luotava pitkäjänteisesti ennen sotaa tehtävillä toimilla.

Johtaminen kohteena

Prikaatikenraali Jarkko Karsikas (NCISG) piti Johtaminen Venäjän kohteena Naton näkökulmasta -seminaariesityksensä Keski-Euroopasta verkon yli. Karsikas käsitteli asiaa koneiden sodan ja operatiivisen resilienssin näkökulmista. Havaintoja Karsikkaan esitykseen oli poimittu JATEC:n (NATO-Ukraine Joint Analysis, Training and Education Centre) tuottamien johtopäätösten kautta. Karsikas pyrki esityksessään hahmottelemaan seminaariyleisölle tulevaisuuden C2-ark-

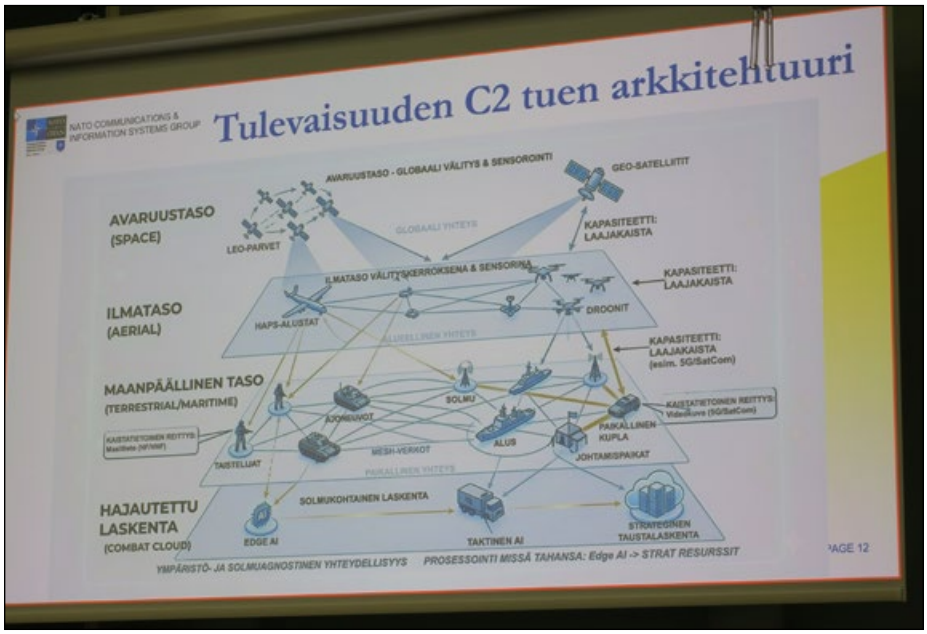
kitehtuurin rakenneosia. Nato pyrkii toiminnassaan kuromaan umpeen sodan ”adaptation gap” -innovaatiosyklin. Pyrkimys on adaptaatiosta ennakointiin ja sitä kautta aloitteen tempaamiseen. Nato on Karsikkaan mukaan johtamisrakenne, joka käyttää kansakuntien suorituskykyjä. Onkin keskeistä mahdollistaa tämän toiminnan johtaminen.

Karsikas peilasi käsiteltyjä havaintoja Jyri Kosolan 2026 julkaisemasta Koneiden sota -kirjasta johdettujen teesien kautta. Massamainen droonien käyttö on johtanut siihen, että halvoilla järjestelmillä pystytään nykyisellä taistelukentällä neutralisoimaan erittäin kalliita järjestelmiä. Droonit ovat siis nykytaistelukentällä merkittävä resurssi. FPV-droonit ovat havaintojen mukaan muuttuneet ammuksiksi, ja niistä on siis tullut asejärjestelmä, jotka on integroitava kokonaisjärjestelmään. Järjestelmiä on kyettävä hyödyntämään, mutta niiltä on myös pystyttävä suojautumaan tai niitä on pystyttävä torjumaan.

Taistelukenttä on muuttunut läpinäkyväksi, erityisesti etulinjassa. Selviytymisen mahdollistamiseksi on pystyttävä sulautumaan toimintaympäristöön. Johtamisen onkin mahdollistettava joustavuus ja nopeus. Sähkömagneettinen spektri ja navigointi on myös nykytaistelukentällä haastettu. Paikantamiseen on pystyttävä ilman GNSS-paikannuskykyä ja johtamisjärjestelmien on mahdollistettava erilaiset yhteyskeinot.

Autonominen tekoälypohjainen tunnistus ja torjunta ovat keskiössä uusien uhkien torjunnassa. Massamaiset parvet ja liitopommit saturoivat puolustuksen ja tämä edellyttää tekoälyn hyödyntämistä puolustuksen rakentamisessa. Käytettäviä tekoälymalleja on myös nopeasti pystyttävä päivittämään saadun datan perusteella.

Yksi tulevaisuuden C2-rakenteiden rakennuspala on Karsikkaan mukaan globaalisti hajautettu laskentateho AI-mallien päivittämiseksi. Tarvitaan myös reunalaskentaa (EDGE AI) autonomisen tunnistuskyvyn mahdollistamiseksi silloin kun toimivia tiedonsiirtoyhteyksiä ei ole tarjolla. Tiedonsiirron on Karsikkaan mukaan oltava monikerroksista.



Prikaatikenraali Karsikas hahmotteli esityksessään tulevaisuuden C2 tuen arkkitehtuuria.

Karsikkaan mukaan ohjelmistokeskeinen sodankäynti ja algoritminen ylivertaisuus ovat uusia globaaleja C2-standardeja. Innovaatiosyklissä on pysyttävä mukana. Toimintaympäristöön on sulauduttava, toimintoja on hajautettava ja toimijoita, myös algoritmeja, on vastuutettava päätöksentekoon. Vain muutos on siis varmaa, ja muutoksia on pystyttävä käsittelemään nykyistä nopeammin.

Kyberulottuvuus

Ylijohtaja Anssi Kärkkäinen (Traficomin Kyberturvallisuuskeskus) käsitteli esityksessään Ukrainan sodan kyberseurantaa. Seuranta lähtee aina liikkeelle tiedon keräämisestä, johon on useita menetelmiä, joista erityisesti luottamukselliset suhteet kansainvälisten tietoturvayritysten ja eri maiden viranomaisten kanssa sekä suoraan Ukrainan kanssa tehtävä yhteistyö ovat keskeisiä. Tietoa on merkittävissä määrin kaivettavissa myös julkisista lähteistä. Euroopan maat pyrkivät jakamaan keskenään tietoa siitä millaista yhteistyötä kukin tekee Ukrainan kanssa. Tavoitteena on välttää Ukrainaakin kuormittavaa päällekkäisyyksiä.

Kärkkäinen nosti esille myös havaintoja Ukrainan opeista. Ensimmäisenä huomiona oli, että vakavien kyberhyökkäysten määrä moninkertaistuu sodassa. On siis pystyttävä skaalaamaan toimintaa merkittävästi. Tämä haastaa kaikkia alan toimijoita mukaan lukien viranomaiset. Toisena oppina Kärkkäinen korosti, että on kyettävä korjaamaan ja palauttamaan järjestelmiä kyberhyökkäysten jäljiltä. Oppina on nostettavissa myös se, että kyberhyökkäykset integroituvat nykysodassa kineettiseen vaikuttamiseen. Vaikutuksiin pyritään monipuolisella keinovalikoimalla.

Digitaalisesti toteutettavia palveluita on myös kyettävä siirtämään pois vaikutusten ulottuvilta, jopa toisten valtioiden alueelle. Kaikkea tietoa ei toki voi tai saa siirtää. Tilannekuvaa on myös pystyttävä jakamaan eri toimijoiden välillä. Mielenkiintoisena näkökulmana Kärkkäinen nosti esiin myös insider-uhkan, eli sisäpiirin soluttautuneen toimijan aiheuttamat riskit. Tietoon pääsy on siis pidettävä tarveperusteisena.

Yhteistoimintaa on harjoiteltava, jotta edellytykset poikkeusolojen toiminnalle on luotu jo rauhan aikana. Kyberturvallisuuden kehyksessä tämä edellyttää laajasti viranomaisten ja yhteiskunnan muiden toimijoiden yhteistä harjoittelua. Loppuun Kärkkäinen muistutti, että viime kädessä perusasiat, kuten sähkönsaanti, ratkaisevat toiminnan onnistumisen.

Opit teletoiminnan varautumiseen

Seminaariin kuuluneen maukkaan lounaan jälkeen siirryttiin paneelikeskusteluosuuteen. Paneelikeskustelut käytiin Jaakko Walleniuksen (Elisa Oyj:n VP Resilience and Defense) toimiessa keskusteluiden moderaattorina. Ukrainan sodan oppeja teletoiminnan varautumiseen käsiteltiin DNA Oyj turvallisuusjohtaja Seppo Pekosen, Kyberturvallisuuskeskuksen osastopäällikkö Heidi Kivekkään, Suomen Erillisverkot Oyn teknologiajohtaja Antti Kauppisen sekä Puolustusvoimien Johtamisjärjestelmäkeskuksen johtaja insinöörieversti Janne Jokisen alustuksissa sekä paneelikeskustelussa. Alustuksissa painotettiin panelistien tärkeinä pitämiä erilaisia näkökulmia teletoiminnan varautumiseen.

Ylijohtaja Anssi Kärkkäinen käsitteli esityksessään Ukrainan sotaa kybernäkökulmasta.

Kivekäs nosti alustuksessaan esille Ukrainan käynnillä saatuja havaintoja. Varautumissuunnittelua ja valmiutta kannattaa havaintojen mukaan rakentaa ennakkoon työkalupakiksi, jolloin nopeissa tilanteissa asioita voidaan ratkaista valmiiden mallien pohjalta. Suomessa tämän kaltaisia asioita on tehty jo aiemmin, mutta työ jatkuu muun muassa sääntelyn rakentamisessa ja noudattamisen valvonnassa. Suomessa viranomaisten ja yrityskentän yhteistoiminta on myös säännöllistä ja toimivaa.

Jokinen kuvaili alustuksessaan seminaariyleisölle PVJJK:n roolia Puolustusvoimien tele- ja palveluoperaattorina. PVJJK operoi myös kyberpuolustuksen toimijana. Ukrainan sodan havaintoina Jokinen nosti esiin taistelukentän läpinäkyvyyden, maalittamissyklin nopeuden,

elektronisen sodankäynnin nopean kehityksen, sekä sodankäynnin pidäkkeettömyyden esimerkiksi kriittisen infrastruktuurin osalta. Kehittämistyötä on Jokisen mukaan tehtävä pitkäjänteisesti, ketterästi ja Nato-jäsenyyden mahdollistamilla keinoilla sekä valmiutta ja varautumista toimeenpannen.

Kauppinen käsitteli alustuksessaan turvallisuuteen liittyvien palveluiden resursoinnin keskeisyyttä. Palveluiden saatavuus erilaisissa tilanteissa on keskeistä ja edellyttää varautumista. Kipupisteitä ja kehitettävää kyllä löydetään, vaikka hyviäkin esimerkkejä varautumisesta on.

Pekonen vuorostaan korosti alustuksessaan teleoperaattoreiden suorituskyvyn merkitystä yhteiskunnalle ja kansalaisille. Viranomaismääräyksillä ohjataan varautumista. Pekonen esitti, että aiemmin on keskitytty lyhytaikaisiin häiriötilanteisiin varautumiseen ja nyt on syytä kääntää huomio pitkäaikaisiin kriiseihin. Esiin nousi myös kansainvälisten yhteyksien varmentamisen merkitys.

Syvällisen, laaja-alaisen ja erittäin informatiivisen paneelikeskustelun aikana sivuttiin muun muassa pienen maan ja verkostoitumisen etuja, jatkuvan säädös- ja lakipohjan kehittämisen tarvetta, laaja-alaisen huoltovarmuuden merkitystä, sähkövarautumisen tilannetta ja merkitystä sekä viranomaisten ja kaupallisten toimijoiden välistä ainutlaatuisen sujuvaa yhteistyötä.

Sodan uudet ilmentymät

Iltapäiväkahvien jälkeen jatkettiin asiantuntevien puhujien kattausta. Työelämäprofessori Valtteri Vuorisalo (Tampereen Yliopisto) käsitteli esityksessään innovaatiosyklin kasvavaa merkitystä. Vuorisalon mukaan sodan uusi rytmi ei odota meitä. Innovaatioiden, tuotannon ja hankintojen sykli onkin mukautettava sodan uuteen todellisuuteen. Ukrainassa valtio ei Vuorisalon mukaan yritä johtaa tai hallita kehitystä, vaan mahdollistaa sen.

Ukrainan tärkein oppi ei Vuorisalon mukaan olekaan teknologia vaan tempo, jolla havainto muutetaan toiminnaksi vastustajaa nopeammin. Ukrainan rintama on muuttunut testausympäristöksi. Teknologian käyttöarvo mitataan Vuorisalon mukaan vastatoimien, häirinnän ja kulutuksen keskellä, ja palaute kentältä on uskottavuuden mittari. Ukrainaan meneminen on kuitenkin puolustusteollisuudelle haastavaa. Uudet innovaatiot ja tuotteet edellyttävät prototyypin käsillä olevan ongelman ratkaisemiseksi, mutta myös kyvyn skaalata tuotanto massamaiseksi. Innovaatiosyklin mittaaminen onkin Vuorisalon mukaan uusi keino mitata valtion puolustuskykyä.

Paneelikeskustelussa tarkasteltiin Ukrainan sodan oppeja teletoiminnan varautumiseen.

Yksikön johtaja Jarna Hartikainen (Huoltovarmuuskeskus) käsitteli esityksessään kriittisen infran suojaamista Ukrainan oppien näkökulmasta. Toimintaympäristömme uhkakuvat vaikuttavat Hartikaisen mukaan toisiinsa. Sotilaallinen konflikti, laaja-alainen vaikuttaminen sekä globaalin talouden vakavat häiriöt nivoutuvat uhkakuvana yhteen.

Hartikaisen mukaan Suomen huoltovarmuusmalli hakee oppeja Ukrainasta. Huoltovarmuuden häiriöt kehittyvät vaiheittain ja niiden vaativuus vaihtelee. Häiriöitä ratkotaan monia eri tahoja sisältävissä ekosysteemeissä, joissa luottamus muihin toimijoihin on ratkaisevaa. Ukrainan kokemukset tarjoavat monia oppeja esimerkiksi yritysten varautumiseen ja erinomainen suomalainen huoltovarmuusmalli vaatii jatkuvaa kehittämistä ja luottamuksen rakentamista. Kriittisille yrityksille varautumisen tueksi onkin luotu Huoltovarmuuskeskuksen tuore julkaisu Suomeen kohdistuva sotilaallinen voimankäyttö ja huoltovarmuus -skenaario.

Osastoesiupseeri majuri Pasi Lepistö (Pääesikunta) käsitteli esityksessään informaatiota sodankäynnin vaikuttamisalueena. Ihmiset käyvät sotaa, eivät kalusto tai aseet, joten ihmisen ymmärrys, päätöksenteko ja toiminta ovat Lepistön mukaan keskeisiä vaikuttamisen kohteita. Näin ollen informaatio on yksi muihin keinoihin kiinteästi liittyvä käytettävä keino. Kognitioon vaikuttaminen tapahtuu virtuaalista ja fyysistä kerrosta käyttäen ja niissä tehtäviä toimia hyödyntäen. Vaikuttaminen on nykyisin monikanavaista eri kerroksissa ja digitaalinen tietotulva on valtava. Näin ollen luotettavan tilannekuvan muodostamiseen ja seurantaan tarvitaan siihen erityisesti rakennettuja järjestelmiä. Toinen avaintekijä informaatiosuojautumisessa on tiedon tulkitsijoiden tarve suojattavien ihmisten kognitiivisen saturaation, eli kyllästymisen, välttämiseksi. Avainasemassa Suomessa on luottamuksen ylläpitäminen.

Informaatiovaikuttamista tapahtuu Lepistön mukaan strategisella, operatiivisella ja taktisella tasolla, jossa vain asetetut tavoitteet vaihtelevat. Usein vaikutukset ulottuvat ja liikkuvat kaikkiin tasoihin digitaalisen globaalin informaatioympäristön takia. Sodankäynnissä kineettinen ja ei-kineettinen vaikuttaminen on Lepistön mukaan nivottava yhteen halutun kokonaisvaikutuksen aikaansaamiseksi.

Johtaja Misa Kangaste (Sensofusion Oy) käsitteli esityksessään drooneja taistelukentällä sekä Sensofusionin johtopäätöksiä niihin liittyen. Drooni on taistelukentän uusi realiteetti ja niiden kehitys on ollut räjähtävää. Kangasteen esittämän arvion mukaan 70–80 prosenttia Ukrainan rintaman kohteista tuhotaan drooneilla. Taistelukentällä voittaa siis se, joka voi torjua massaiskun edullisemmin kuin vastustaja voi hyökätä.

Halpoja drooneja tulee kyetä torjumaan halvoilla vastatoimilla. Hyökkäykset tulee pystyä sekä tunnistamaan että torjumaan. Droonien suhteen taistelukentän innovaatiosykli on erittäin lyhyt, Kangasteen esittämän arvion mukaan jopa vain 14 vuorokautta. Myös vasta-aseita on siis pystyttävä kehittämään ketterästi. Eräs työtä vaativa kehityskohde on komponenttien huoltovarmuus, sillä esitetyn arvion mukaan Ukrainassa käytettävien droonien komponenteista merkittävä osa tulee Kiinasta. Tässäkin asiassa tarvitaan jatkossa eurooppalaista omavaraisuutta.

Työelämäprofessori Valtteri Vuorisalo käsitteli esityksessään innovaatiosyklin kasvavaa merkitystä.

Seuraavaa seminaaria odotellessa

Seminaari päätettiin toimitusjohtaja Charly Salonius-Pasternakin (Nordic West Office) seminaarihavainnot summaavaan yhteenvetoon. Seminaari oli Salonius-Pasternakin näkemyksen mukaan erinomainen ja esitetyt analyysit erittäin laadukkaita. Salonius-Pasternak summasi monien asioiden kulminoituvan edelleen ihmisiin ja heidän valmiuksiensa sekä hyödynnettävyytensä kehittämiseen. Yhteisen asian merkitys oli Salonius-Pasternakin ajatuksissa keskeisin Ukrainan oppi.

Tilaisuuden puheenjohtaja kiitti päätöspuheessaan seminaarin esiintyjiä ja osallistujia. Vastaavia seminaareja järjestetään myös jatkossa, ja palautetta sekä kehitysideoita otetaan mielellään vastaan. Seminaarin päätteeksi siirryttiin tälläkin kertaa verkostoitumaan ja jatkamaan erinomaisen kiinnostavien seminaariaiheiden puimista.

Evl Jaakko Tuomi palvelee Maavoimien esikunnassa.

Teksti: Jaakko Tuomi

Ajatuksia Maavoimien johtamisjärjestelmän kehittämisestä

Edellisessä numerossa Pääesikunnan johtamisjärjestelmäpäällikkö kenraalimajuri Jarmo Vähätiitto kirjoitti johtamisjärjestelmäalasta ja kyberpuolustuksesta puolustusvoimien johtamisen tukena. Tässä artikkelissa pohditaan, mitä nämä ilmiöt tarkoittavat Maavoimien, maataistelun sekä näiden johtamisen tuen näkökulmasta. Kuvituskuvat on generoitu tekoälyllä (Gemini). Teksti perustuu vuorovaikutuksen kautta hioutuneeseen ihmisajatteluun.

Maavoimien esikunta vastaa maapuolustuksen johtamisjärjestelmän kehittämisestä. Johtamisjärjestelmällä mahdollistetaan maapuolustuksen johtaminen ryhmätasolta Naton yhteisoperaatiojohtoportaaseen – kaikissa valmiustiloissa vuoden jokaisena päivänä. Maavoimien johtamisjärjestelmää kehitetään osana Puolustusvoimien kokonaisuutta. Tässä artikkelissa pohditaan kehittämistä Maavoimien näkökulmasta, taistelijasta puolustushaaratasolle saakka.

Johtamisjärjestelmä mahdollistaa komentajien johtamistoiminnan kansallisesti, kahden- ja monenvälisesti sekä osana liittokuntaa kaikissa valmiustiloissa ja toimintaympäristöissä 24/7/365. Tässä artikkelissa keskitytään johtamisjärjestelmän osaan, joka muodostuu viestijoukoista, tietoliikenne- ja tietojärjestelmistä, johtamisjärjestelmäpalveluista sekä näiden käyttöperiaatteista. Kyseessä on järjestelmien järjestelmä keskinäisriippuvuuksineen. Maavoimissa se ilmenee sotilasjoukkoina ja niiden käyttäminä järjestelminä, kuten esimerkiksi viestijärjestelmä M18 viestiasemineen ja komentopaikkoineen. Maavoimien taistelija puolestaan tarvitsee puhetta, sanomia ja tilannekuvaa.

Havainnollistavana tapausesimerkkinä käytetään kevään 1940 Sedanin taistelua. Se oli osa operaatio Keltaista, saksalaisten hyökkäystä Ranskaan. Saksalaiset yllättivät hyökkäämällä läpitunkemattomana pidetyn Ardennien vuoriston kautta, saavuttivat läpimurron Sedanissa ja jatkoivat hyökkäystään kohti Kanaalin rannikkoa. Seurauksena oli Ranskan nopea kukistuminen. Kirjoittaja osallistui viime syksynä matkalle, jolla pohdittiin paikan päällä operaation tapahtumia, taustoja ja seurauksia, eikä rinnastuksilta tähän päivään voitu välttyä.

Keskeisiä kehittämistä ohjaavia kysymyksiä ovat ”Millaiset Maavoimat meillä on 2030-luvun lopulla?” ja ”Millaisen johtamisjärjestelmän 2030-luvun Maavoimien joukot tarvitsevat osana monitoimintaympäristöoperaatiota? (Multi Domain Operation, MDO)”. Suunnittelun on perustuttava tunnistetuista muutostekijöistä tehtyyn perusteelliseen analyysiin sekä ymmärrykseen aiemmin tehtyjen ratkaisuiden asettamista mahdollisuuksista ja rajoitteista.

Suorituskyvyn kehittäminen on pitkäjänteistä työtä, jonka on huomioitava jatkuvasti muuttuva toimintaympäristön muutos. Edellisten vuosikymmenten aikana systemaattisesti rakennetun järjestelmän tuottama suorituskyky on peruskallio, jonka päälle jatkokehittäminen tehdään. Puolustusvoimat on kouluttanut ja varustanut joukkoja systemaattisesti vuosikymmeniä, minkä seurauksena meillä on nykyään kansainvälistä ihailua herättävä laaja sodan ajan reservi. Uudistaminen on jatkuvaa työtä, eikä se tapahdu yhdessä yössä.

Maavoimat osana monitoimintaympäristöoperaatiota

Muutostekijöitä

Keskeisimpiä muutostekijöitä kehittämisen näkökulmasta ovat havainnot viimeaikaisista sodista, teknologian kehittyminen sekä tuoreimpana liittoutumisen vaikutukset. Varsinkin kaksi ensiksi mainittua ovat toisiinsa erottamattomalla tavalla yhteen kietoutuneet. Suomen liittyminen Naton jäseneksi on muuttanut pelikenttää myös johtamisjärjestelmän ja sen kehittämisen osalta.

”Varmin keino laadullisen paremmuuden perustuksien repimiseksi on muualla käytäntöön otettujen välineiden ja menetelmien jäljitteleminen ilman niiden sopivuutta koskevaa harkintaa.” Wolf H. Halsti: Suomen puolustaminen, 1939.

Halstin toteamuksen tulee olla kehittämisen johtolauseena. Harkintaa ei tule erehtyä pitämään jämähtäneisyytenä tai muutosvastarintaisuutena, siitä ei ole kyse. On ymmärrettävä syvällisesti oma ympäristö erityispiirteineen sekä nykyisten ratkaisuiden alkuperä ja ajattelu niiden taustalla. Jäljittelemisen sijaan on tuotettava juuri omaan toimintaympäristöön sopivat ratkaisut.

Kuten Halsti toteaa, kukin sota eroaa toisistaan mm. tavoitteiden, maantieteen sekä osapuolten asevoimien voimasuhteiden, teknisen tason, organisoinnin sekä koulutustason osalta. Muualla tehdyistä ratkaisuista tulee ottaa oppia, mutta niitä ei saa kopioida sellaisenaan ymmärtämättä syitä niiden taustalla. Pelkkään muutokseen keskittymisen lisäksi on ymmärrettävä, mikä ei ole muuttunut.

Esimerkkinä voidaan käyttää Saksan ja Ranskan ensimmäisen maailmansodan jälkeen valitsemia kehityssuuntia. Johtopäätökset olivat päinvastaisia, vaikka sotakokemukset ja ympäristö olivat molemmille samat. Yksinkertaistettuna Ranska keskittyi painottamaan doktriinissaan tulenkäyttöön perustuvaa staattista puolustusta, keskitettyä johtamista sekä tiukasti kontrolloitua ja aikataulutettua toimeenpanoa, saksalaisten valittua päinvastaisen lähestymistavan.

Vaikka lopputulokseen vaikutti tässäkin tapauksessa suurelta osin sattuma ja tuuri, osoittautui saksalainen lähestymistapa jälkiviisaana katsoen oikeaksi. Vaikka tapahtumat olisivat voineet päättyä toisinkin, historiantutkimus on todennut kevään 1940 käsikirjoituksen olleen pitkälti ennalta kirjoitettu, vaikkeivat näyttelijät sitä tuolloin tienneet.

Talvisodasta nykypäivään

Yhteisoperaatiosta Multi Domain -operaatioon.

Viimeaikaisista sodista tehtäviä havaintoja

Näkyvin uusi tekijä viimeaikaisissa sodissa on ollut miehittämättömien järjestelmien, etenkin lentävien, määrän ja merkityksen kasvu. Julkisuudessa on puhuttu läpinäkyvästä taistelukentästä, missä varsinkin lähellä ”etulinjaa” piiloutuminen ja suojautuminen on muuttunut jatkuvasti vaikeammaksi.

Huomionarvoista on, että Ukrainan sodan viimeisten neljän vuoden aikana käytetyt välineet ja keinot ovat kehittyneet jatkuvalla tahdilla. Mediahuomion kohteena on ollut vuorollaan Javelin -panssarintorjuntaohjus, Bayraktar -lennokki sekä viimeisimpinä kuituohjatut FPV -lennokit. Uusien välineiden merkitystä ei tule vähätellä, mutta aseen ja vasta-aseen voimasuhteiden vaihtelu tuntuu edustavan historiallista pysyvyyttä.

Kineettiseen vaikuttamiseen yhdistyy kyber- ja elektroninen vaikuttaminen. Kamppailu ulottuu fyysisestä ympäristöstä myös sähkömagneettiseen spektriin. Elektroniselta tiedustelulta ja vaikuttamiselta suojautumisen merkitys ei ole ainakaan vähentymässä. Kaikki säteilevä voidaan havaita. Se mikä voidaan havaita, siihen voidaan myös vaikuttaa.

Sodankäynnin uudet muodot ja tavat eivät syrjäytä vanhoja, vaan täydentävät niitä. Venäläiseen sodankäyntitapaan kauan kuuluneet joukkojen ja tulen massamainen käyttö, kaukovaikuttaminen eri keinoin ja infrastruktuurin tuhoaminen ovat edelleen keskeinen osa keinovalikoimaa, päivittyneenä uusilla välineillä. Tämän johdosta kehittämisessä on huomioitava kaikki sodankäynnin muodot kuudennen sukupolven etäsodankäynnistä perinteiseen ”kulutussodankäyntiin”.

Liittoutumisen vaikutukset

Kansainvälinen ulottuvuus on saanut EU:n rinnalle Naton, mikä edellyttää kansainvälisten standardien kautta rakennettavaa yhteistoimintakykyä. Yhteistoiminnan tulee olla mahdollista niin eri johtamistasojen, puolustushaarojen, liittolaisjoukkojen sekä muiden viranomaisten ja siviilikomponentin kanssa tarkoituksenmukaisella tavalla.

Yhteisoperaatioiden sijaan nykyään puhutaan Multi Domain -operaatioista, joissa maa-, meri- ja ilmaulottuvuudet ovat saaneet rinnalleen avaruus- ja kyberympäristöt. Tämä voidaan käsittää kotimaisen kokonaisturvallisuuden strategian kaltaisena kokonaisuutena, jossa Puolustusvoimat on toimija muiden joukossa.

Multi Domain -operaatioiden konsepti ja siihen liittyvä any-sensor-to-any-shooter -ajattelu asettaa vaatimuksia myös tiedonsiirrolle ja tietojärjestelmille. Tekninen kyky on rakennettava siten, että tilanteen edellyttäessä tiedonsiirto on mahdollista niin datan, sovellusten, salauksen kuin tiedonsiirtostandardienkin osalta. Teknisten ratkaisuiden lisäksi tulee toimintatapojen niiden käyttämiseksi oltava ennalta määritettyjä ja harjoiteltuja. Naton Federated Mission Networking -hanke on tälle oivallinen viitekehys.

Teknologian kehittyminen

Siinä missä ennen sodat olivat teknologisen kehityksen muutosajuri, vaikuttaisi nykyään asia olevan päinvastoin. Jo mainittujen miehittämättömien järjestelmien lisäksi, ja niiden vaikutuksesta, verkottuneisuuden ja digitalisaation merkitys on kasvanut entisestään. Nurkan takana olevan kvanttilaskennan tulee olla kiikaritähystyksen alla jo nyt.

Yhteistyö yritysten kanssa

Järjestelmien määrän ja laadun kasvun seurauksena myös niiden tuottaman datan määrä kasvaa kiihtyvällä vauhdilla. Sen tallentaminen, siirtäminen ja hyödyntäminen edellyttää uusia ratkaisuja ryhmätasolta (device edge) ylemmälle yhtymätasolle (core). Uusien ratkaisujen tulee tuoda uutta suorituskykyä ”pää pilvissä”, pitäen jalat tiukasti aiemmin rakennetun peruskallion pinnalla. Hankittavan materiaalin elinkaaret vaihtelevat, ollen pisimmillään vuosikymmeniä. Yksikään asevoima ei kykene uudistamaan koko materiaaliaan kerralla. Käytössä on aina eri aikoina hankittuja osia.

Kehittäminen edellyttää tiivistä yhteistyötä ja vuoropuhelua, niin Puolustusvoimien ja yritysten välillä kuin yritysten kesken. Datakeskeinen johtaminen edellyttää tiedon liikkumista osajärjestelmien kesken. On keskeistä, että eri järjestelmissä syntyvä data saadaan myös muiden tarvitsijoiden hyödynnettäväksi. Tällaista kykyä ei rakenneta siiloissa.

Suorituskykyä on saatava välittömästi käyttöön pitkien kehitysprojektien ohella. On kyettävä ketterään kehittämiseen ja innovaatioiden hyödyntämiseen. Nykyiset ohjelmistopohjaiset järjestelmät tuovat päivitettävyyden näkökulmasta täysin uudenlaisia mahdollisuuksia – ominaisuudet eivät ole enää lukittu rautaan koko elinjakson ajaksi.

Kuten eivät tienneet maailmansotien välissä kehitystä suunnitelleet ja toimeenpanneet, emme mekään voi varmuudella tietää, miten kehityskulut jatkuvat. Lähes varmuudella voidaan silti todeta, että miehittämättömät järjestelmät, niiden tuottama data sekä tarve sen käsittelyyn kaikilla johtamistasoilla eivät tule katoamaan. Jatkona analogialle toisesta maailmansodasta, voidaan päätellä, että suhteellisen etulyöntiaseman saavuttaminen niin yksilö- ja ryhmätasolla, komppania- ja pataljoonatasolla sekä ylemmillä yhtymätasoilla on jatkossakin menestyksen edellytys.

Etulyöntiaseman saavuttaminen ei välttämättä edellytä uuden välineen tai teknologian keksimistä. Monesti läpimurtoon johtanut innovaatio onkin ollut seurausta jo olemassa olevien välineiden yhdistämisestä tai uudesta käyttötavasta. Tunnettu esimerkki on saksalaisten oivallus yhdistää panssarivaunu, lentokone ja radio – kaikki pitkään olemassa olleita välineitä, jotka yhdistettynä aloitteellisuutta suosivaan johtamistapaan olivat salamasodan resepti.

Salamasodan ainesosien tapaan ratkaisun elementit ovat jo paljolti olemassa. Ne tulee yhdistää ratkaisuksi, jolla tuotetaan tulevaisuuden suhteellinen etulyöntiasema. Ajattelutapaa tulisi pystyä kehittämään kohti älypuhelinmaailmasta tuttua modulaarista ”appien ekosysteemiä”, jossa järjestelmät, laitteet ja niiden sisältämät sovellukset kykenevät kommunikoimaan keskenään – tarjoten käyttäjien tarvitsemat palvelut.

Data ja sen hyödyntäminen

Kasvava datamäärä edellyttää työkaluja sen hyödyntämiseen. Datakeskeisyys, tekoäly ja automatisaatio tuottavat ratkaisuja, mutta niille asettuvat vaatimukset ovat erilaisia eri joukkotasoilla. Yksinkertaistaen voitaisiin tietokonepelitermein todeta taistelutilan näyttävän ryhmätasolla Doom -räiskintäpeliltä, pataljoona-prikaatitasolla Command & Conquer -taktiikkapeliltä, ja ylimmillä tasoilla Civilisationin tapaiselta strategiapeliltä, jossa keskitytään resurssien jakamiseen ja kyvykkyyksien kehittämiseen. Eroja on myös aikajänteissä. Alemmilla tasoilla heti on heti, ylemmillä ”heti” voi tarkoittaa päiviä, viikkoja tai kuukausia. Kullekin tasolle on kyettävä tuottamaan sen edellyttämät välineet johtamiseen ja tiedonkäsittelyyn.

Kaikilla joukkotasoilla tulee kyetä hyödyntämään dataa oman toiminnan tukena sekä välittämään ylemmille tasoille niiden tarvitsemaa tietoa. Joukkojen tulee kyetä jatkamaan toimintaansa tilanteessa, jossa yhteydet ylempien johtoportaiden järjestelmiin eivät jatkuvasti ole käytettävissä. Pelkän raakadatan välittymisen

Johtamistasojen erot

lisäksi tieto jalostuu matkan varrella. Alempien tasojen datasta jalostama tieto voi olla ylempien tasojen näkökulmasta dataa jatkoanalyysin pohjaksi.

Automatisaatio voi vapauttaa ihmisen rutiinityöstä siihen, mihin kone ei vielä kykene, luovaan ajatteluun. Siinä, missä esikuntaupseeri kykenee käsittelemään kirjoitettua tekstiä enimmillään 40–50 sivua tunnissa, ylittää tekoälypohjainen kielimalli tämän miljoonakertaisesti. Kone ei tarvitse kahvitaukoja, nuku öisin tai kaipaa lomaa. Kuten artikkelin kuvien yksityiskohdista havaitsee, on koneen tuottaman aineiston kanssa tosin oltava tarkkana.

Nopeutta ja ketteryyttä

”He who can handle the quickest rate of change survives.” John Boyd

Yhdysvaltalaisen eversti John Boydin (1927–97) kuuluisa OODA-loop kiteyttää päätöksenteon syklin neljään vaiheeseen: havainto (observe), orientaatio, päätös (decide) ja toiminta (act). Saksalaisella operaatiotaidolla toisessa maailmansodassa oli merkittävä vaikutus Boydin pohdintoihin. Boydinsa lukeneet tietävät, ettei kyse ollut ainoastaan oman syklin nopeuttamisesta, vaan suhteellisen edun saavuttamisesta. Keinoja nopeuttamisen lisäksi olivat ketteryys, eli nopeampi kyky muutoksiin, sekä vastustajan päätöksentekokyvyn hidastaminen tai estäminen.

Sedanin taistelussa ranskalaisten johtamisyhteydet häiriintyivät tykkitulen katkottua ennalta rakennetut kaapeliyhteydet, jotka oli rakennettu maan pinnalle ohjesäännön vastaisesti. Radioita olisi ollut käytettävissä, mutta niiden käyttöön siirtyminen olisi edellyttänyt lupaa ylemmältä esikunnalta. Viestiyhteyksien puute haittasi erityisesti ranskalaisen taistelutavan keskeistä kulmakiveä, tykistön tulenkäyttöä.

Katkenneet yhteydet aiheuttivat lisäksi etäällä sijaitseville ranskalaisesikunnille jatkuvasti kasvavaa epätietoisuutta nopeasti kehittyvästä tilanteesta. Saksalaiset johtajat sijoittuivat lähelle etulinjaa, pystyen muodostamaan omakohtaisen ymmärryksen tapahtumista. Alimmalla tasolla puolestaan saksalaisten päätös asentaa radio jokaiseen panssarivaunuun antoi merkittävän edun verrattuna ranskalaisiin, joilla näin ei ollut tehty.

Nykyaikana tiedonsiirron mahdollisuudet ovat huomattavasti 1940-lukua kattavammat. Oleellinen tarve on säilynyt samana, tiedon on kuljettava tarvitsijoiden välillä luotettavasti. Vaihtoehtoiset yhteystavat lisäävät mahdollisuuksia viestin välittämiseen, vähentämättä kaapeleiden, kuitujen ja radioverkkojen käyttöarvoa. Sodan kitka voi ilmentyä rikkoutuneina laitteina, lukuisten muiden muuttujien ohella, jotka tekevät yksinkertaisesta vaikeaa.

Elektronisen tiedustelun vaarat ja suojautumisen tarve ilmenivät Sedanissakin. Murtauduttuaan puolustuksen läpi, joukkojaan kohti Kanaalin rannikkoa johtanut Guderian havaitsi omakohtaisesti salaamattoman radioliikenteen vaarat. Hän siirtyi käyttämään kaapeliyhteyksiä komentopaikkojensa välillä, ylempien esikuntien alettua vaatimaan etenemisen pysäyttämistä tultuaan huolestuneeksi liian nopeasta etenemisestä.

Tukea tiedonkäsittelyyn

Kaapeliyhteys antaa suojaa havaituksi tulemiselta ja häirinnältä, kuten FPV -droonien kehitys on osoittanut. Peruskoulutukseen on syystä kuulunut jo kauan elektronisen suojautumisen perustaistelumenetelmät, joita tulee täydentää järjestelmien ominaisuuksien jatkokehittämisellä. Toimivuus tulee säilyttää tappioista ja elektronisesta häirinnästä huolimatta.

Skaalattavuus, kustannustehokkuus, käytettävyys

”Määrällä on oma laatunsa” Josif Stalin

Maavoimien sodan ajan joukkojen vahvuus on 180 000 sotilasta, jotka varustetaan niiden tehtävien edellyttämällä tavalla. Reservijärjestelmään perustuva puolustusratkaisu asettaa skaalattavuuden keskeiseksi suunnitteluperusteeksi. On löydettävä ratkaisu, jolla kyetään saavuttamaan riittävä laadullinen etulyöntiasema, säilyttäen samalla kustannustaso sellaisena, että kyetään hankkimaan ja ylläpitämään riittävä määrä. Laadullakin on oma laatunsa.

Erilaisilla järjestelmillä on toisistaan eroavat elinjaksot. Elektroniikalla on nykyään lyhyt elinkaari, mutta raskaalla kalustolla se voi olla kymmeniä vuosia. Ohjelmistopohjaisten järjestelmien päivitettävyys tarkoittaa mahdollisuutta niiden ominaisuuksien parantamiseen niiden elinjakson ajan. Modulaarinen ajattelutapa tulisi ulottaa ohjelmistoista myös komponentteihin ja laitteisiin. Uuden hankkimisen lisäksi on myös löydettävä ratkaisuja jo käytössä olevien järjestelmien ominaisuuksien, suojan ja käytettävyyden parantamiseksi.

Laajaan reserviin perustuva ratkaisu tarkoittaa, että järjestelmien tulee olla helppokäyttöisiä ja nopeasti opittavia. Suomalaisen yhteiskunnan korkea koulutustaso luo edellytykset uusien välineiden nopealle oppimiselle, mutta kertausharjoituksissa uusien välineiden opettamiseen käytössä oleva aika on rajallinen.

Sodan todellisuuteen kuuluvat inhimilliset väsymys ja pelko heikentävät kykyä monimutkaisiin toimintoihin. Etenkin etulinjan taistelijan käyttöön hankittavan materiaalin tulee olla helppokäyttöistä tehtävässä selviytymisen näkökulmasta – välineiden tulee tukea toimintaa. Joissain tilanteissa laitteet saattavat lisätä käyttäjän kognitiivista kuormaa aiheuttaen vaarallisen häiriötekijän, kuten John Spencer kirjoittaa MWI:n artikkelissa vuodelta 2019. Keskittyminen laitteiden käyttöön saattaa aiheuttaa tappioita, mikäli se haittaa ympäristön havainnointia.

Lopuksi

Maavoimat ei taistele irrallaan muista puolustushaaroista. Siinä missä Sedanissa jalkaväkitaistelijan tukena oli Stuka -syöksypommittaja, jonka tuottama keskeisin vaikutus oli itse asiassa psykologinen, tuetaan maataistelua nykyään ilma- ja merivoimien lisäksi avaruus- ja kyberulottuvuuden vaikutuksilla. Sodankäynnin välineet ovat kehittyneet halki historian. Menestys on yleensä seurannut sitä, joka on osannut soveltaa kehitystä.

Kuten ei toisessa maailmansodassakaan, eivät pelkät välineet ratkaise taisteluiden lopputulosta. Ranskalaiset olivat laadullisesti ja määrällisesti saksalaisiin nähden ylivoimaisia, mutta saksalaisten doktriini ja johtamistapa osoittautuivat parem-

miksi. Joukkojen koulutus ja varustelu mahdollisti aloitteellisen ja aktiivisen toiminnan. Yksittäisiin vaunuihin asennetut radiot mahdollistivat nopeamman toimeenpanokyvyn alimmilta tasoilta alkaen. Seurauksena oli saksalaisten jatkuvasti kasvanut suhteellinen etu kevään 1940 taisteluissa.

Kuten Halsti toteaa, ei muualla tehtyjä ratkaisuja tule kopioida ilman harkintaa niiden soveltuvuudesta. Boydia mukaillen, muutokseen sopeutuva on se, joka selviytyy. Voittaja puolestaan on se, joka ei ainoastaan selviydy, vaan kykenee ennakoimaan muutoksen. Pelkät välineet eivät takaa voittoa, tarvitaan myös niiden käytön edellyttämää taitoa. Suomalainen sotataito perustuu maaston hyödyntämiseen, liikkuvuuteen ja hajautettuun taktiikkaan. Kehitettävien ratkaisujen tulee tukea näitä piirteitä, skaalautua laajan reservin edellyttämällä tavalla, toimien pohjolan olosuhteissa. Tekniikka on tuottanut kyvyn ampua kauemmas ja nähdä paremmin, mutta se ei ole poistanut tarvetta yllättää, keskittää voimaa tai murtaa vastustajan tahtoa.

Taistelijan välineet

Teksti: Lauri Hyry

Kohti datakeskeistä sodankäyntiä – Ukrainan Delta -johtamisjärjestelmä

Ukrainan johtamisjärjestelmäkenttä koostuu useista rinnakkain käytettävistä tietojärjestelmistä. Ukrainan puolustusministeriön mukaan Delta- ja Kropyva -järjestelmät ovat kolmen käytetyimmän johtamisjärjestelmän joukossa. Nämä kaksi järjestelmää täydentävät toisiaan ja jakavat tietoa, vaikka ne eivät ole täysin integroituja.Tässä artikkelissa pureudutaan näistä ratkaisuista todennäköisesti tunnetumpaan, Ukrainan asevoimien Delta -järjestelmään. Ukrainan puolustusministeriön mukaan Deltaa käyttää jo noin 200 000 käyttäjää.

Länsimaissa johtamisjärjestelmiä on perinteisesti rakennettu usein ylhäältä johdettuina “top-down” -hankkeina. Ukrainassa kehitys on lähtenyt liikkeelle käytännön tarpeista. Syyt taustalla toki selittävät tätä: järjestelmiä on jouduttu rakentamaan nopeasti sodan aikana, usein rajallisilla resursseilla ja ilman valmiita rakenteita. Tämä on ohjannut kehitystä kohti ratkaisumallia, jossa ongelmia ratkaistaan yksi kerrallaan ja kokonaisuutta laajennetaan vähitellen. Kehitystapa mahdollistaa nopean etenemisen, mutta siihen liittyy myös omat haasteensa. Sotaa käyvällä maalla ei ole vuosia aikaa odottaa toimivaa ratkaisua.

DELTA -järjestelmä. Lähde: Ministry of Defence of Ukraine.

Delta -järjestelmän synty ja kehitys

Ukrainan asevoimien Delta -järjestelmän alkuperäinen tarve oli yksinkertainen. Tarvittiin keino muodostaa yhteinen tilannekuva. Ensimmäinen ratkaisu oli digitaalinen kartta, johon voitiin merkitä havaintoja vihollisen toiminnasta ja omien joukkojen tilanteesta. Vuosien aikana Deltaan liitettiin viestintä, videokuva, suunnittelu ja muita työkaluja. Kehitys ei ollut ennalta suunniteltu ja ylhäältä johdettu kokonaisuus, vaan jatkuva prosessi, jossa järjestelmää laajennettiin tarpeen mukaan. Tuloksena on alusta, joka yhdistää useita toimintoja yhdeksi kokonaisuudeksi.

Delta -järjestelmän kehitys liittyy tiiviisti Aerorozvidka -ryhmään, joka syntyi Ukrainan sodan alkuvaiheessa vuonna 2014. Ryhmä koostui vapaaehtoisista, joilla oli teknistä osaamista ja suora yhteys rintaman tarpeisiin. He alkoivat etsiä ratkaisuja tilanteessa, jossa käytössä olevat tietojärjestelmät eivät tukeneet tehokasta tilannekuvan muodostamista. Tietoa oli hajallaan eri lähteissä, eikä sitä pystytty yhdistämään tai jakamaan nopeasti.

Deltan kehityksen taustalla oli myös laajempi kansainvälinen kehys. Sen juuret ulottuvat vuoden 2014 NATO:n Walesin huippukokoukseen, jossa perustettiin NATO-Ukraina C4 Trust Fund. Tämän ohjelman tavoitteena oli kehittää Ukrainan viestintä-, johtamis- ja tietojärjestelmiä sekä parantaa tilannekuvaa. Delta kehittyi osana tämän ohjelman tilannekuvahanketta, ja sen kehittäjät osallistuivatkin useisiin NATO:n kehitys- ja testausympäristöihin, kuten TIDE -sprintteihin, hackathoneihin ja CWIX -yhteensopivuusharjoituksiin. Näiden


MILDEF
Behind the
mission
Military missions come in many forms. But they all have one thing in common: The tactical IT systems that support them must never fail.
At MilDef, we understand the challenges our customers face, and the impact every solution must deliver.
Our solutions are proven where it matters most – not on paper, not in theory, but in real missions, under real conditions. Battle-tested for what ever is thrown at them.
But real strength comes not only from the rugged and reliable IT solutions we develop, but also from the dedicated people behind them.
We are behind the mission. Every mission. And when pressure peaks, what stands behind the mission must never fail.
WE ARMOR IT.™

kautta Delta -järjestelmää testattiin ja kehitettiin yhteensopivaksi liittolaisten järjestelmien kanssa.

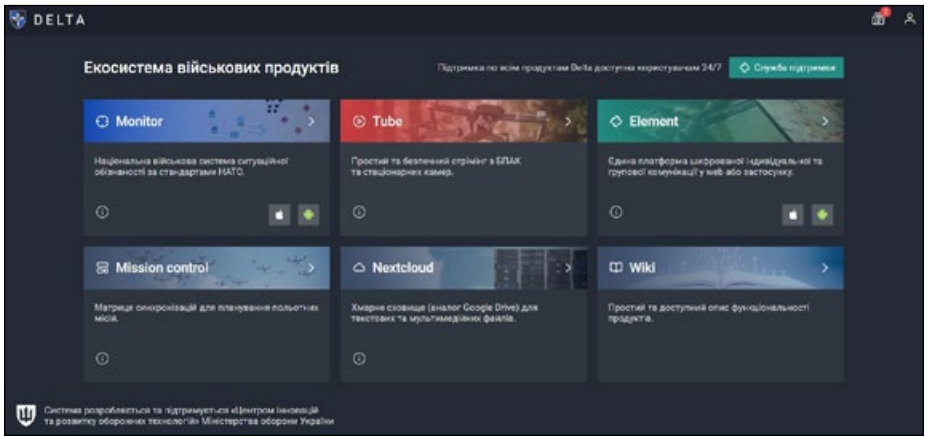
Deltan ensimmäinen ratkaisu oli yksinkertainen karttapohjainen sovellus, jonka avulla eri lähteistä saatua tietoa voitiin yhdistää yhteen näkymään. Kartta toimi ytimenä, jonka ympärille alettiin lisätä uusia toimintoja sitä mukaa kun tarpeet kasvoivat. Viestintä, videokuva ja operatiivinen suunnittelu eivät muodostaneet erillisiä tietojärjestelmiä, vaan ne kytkettiin “moduuleina” osaksi samaa kokonaisuutta.

Deltan kehittäjät seurasivat myös länsimaisia ratkaisuja. Yksi keskeinen esikuva oli tanskalaisen Systematicin Sitaware -järjestelmä. Ukrainan puolustusministeriön innovaatiokeskuksen varajohtaja Artem Martynenko on todennut, että Sitaware tarjosi mallin siitä, millaisia tehtäviä tällaisen järjestelmän tulisi tukea. Lähtökohdat olivat kuitenkin täysin erilaiset. Siinä missä Sitaware on rakentunut vuosikymmenten aikana vakaassa ympäristössä , Deltaa on kehitetty nopeasti sodan keskellä pienellä tiimillä. Tästä huolimatta tavoitteet ovat samat. Molemmissa pyritään yhdistämään eri lähteistä tuleva tieto ja tukemaan päätöksentekoa.

Delta -järjestelmän arkkitehtuuri ja keskeiset moduulit

Delta -järjestelmän taustalla oleva teknine arkkitehtuuri perustuu hajautettuun ja pilvipohjaiseen malliin. Järjestelmä kokoaa dataa useista eri lähteistä, kuten drooneista, sensoreista, satelliiteista ja muista tiedustelujärjestelmistä, ja yhdistää ne yhdeksi kokonaisuudeksi. Dataa ei käsitellä yhdessä suljetussa järjestelmässä, vaan sitä tuotetaan ja hyödynnetään useiden sovellusten kautta. Keskeistä on, että eri moduulit käyttävät samaa tietopohjaa ja jakavat tiedon reaaliaikaisesti. Arkkitehtuuri on suunniteltu siten, että järjestelmää voidaan käyttää erilaisilla päätelaitteilla ja vaihtelevissa olosuhteissa. Samalla se mahdollistaa uusien toiminnallisuuksien lisäämisen ilman, että koko järjestelmää tarvitsee rakentaa uudelleen. Tämä tekee Deltasta enemmän alustan kuin yksittäisen järjestelmän.

Delta -järjestelmä koostuu useista toisiinsa integroiduista moduuleista, jotka muodostavat yhden käyttöympäristön. Keskeisiä osia ovat Delta Monitor, Delta Tube, Mission Control, Element sekä



DELTA -tietojärjestelmän moduulit. Lähde: Ministry of Defence of Ukraine

Nextcloud. Näiden tarkoituksena ei ole toimia erillisinä työkaluina, vaan täydentää toisiaan siten, että tilannekuva, viestintä ja operatiivinen toiminta tapahtuvat samassa tietojärjestelmässä.

Delta Monitor on järjestelmän ydin. Se on karttapohjainen tilannekuvasovellus, joka yhdistää eri lähteistä tulevan tiedon yhdeksi näkymäksi. Kartalla voidaan esittää joukkojen sijainteja, havaintoja ja muita merkittäviä kohteita. Käyttäjä voi tarkastella tietoa eri tasoilla ja suodattaa sitä tarpeen mukaan. Monitor toimii käytännössä yhteisenä näkymänä tilanteeseen eri johtamistasoilla.

Delta Tube tuo järjestelmään reaaliaikaisen videon. Sen kautta voidaan välittää kuvaa drooneista, kameroista ja muista lähteistä suoraan käyttäjille. Tämä mahdollistaa tilanteen tarkemman havainnoinnin ja tukee päätöksentekoa erityisesti nopeasti muuttuvissa tilanteissa.

Mission Control keskittyy operatiiviseen suunnitteluun ja erityisesti droonioperaatioiden koordinointiin. Sen avulla voidaan aikatauluttaa tehtäviä, määrittää kohteita ja sovittaa eri yksiköiden toimintaa yhteen. Käytännössä tämä vähentää päällekkäistä toimintaa ja parantaa resurssien käyttöä tilanteessa, jossa käytössä on suuri määrä miehittämättömiä järjestelmiä.

Element toimii järjestelmän viestintämoduulina. Se tarjoaa salatun kanavan käyttäjien väliseen kommunikointiin ja mahdollistaa tiedon jakamisen nopeasti eri yksiköiden välillä. Viestintä on integroitu osaksi muuta järjestelmää, mikä tekee siitä suoran osan operatiivista toimintaa eikä erillistä työkalua.

Nextcloud täydentää kokonaisuutta tiedonhallinnan osalta. Se toimii alustana dokumenteille, kuville ja muulle aineistolle, jota tarvitaan operatiivisessa toiminnassa. Vaikka se ei ole suoraan taistelun johtamiseen liittyvä moduuli, se tukee järjestelmän käyttöä ja mahdollistaa tiedon jakamisen laajassa organisaatiossa.

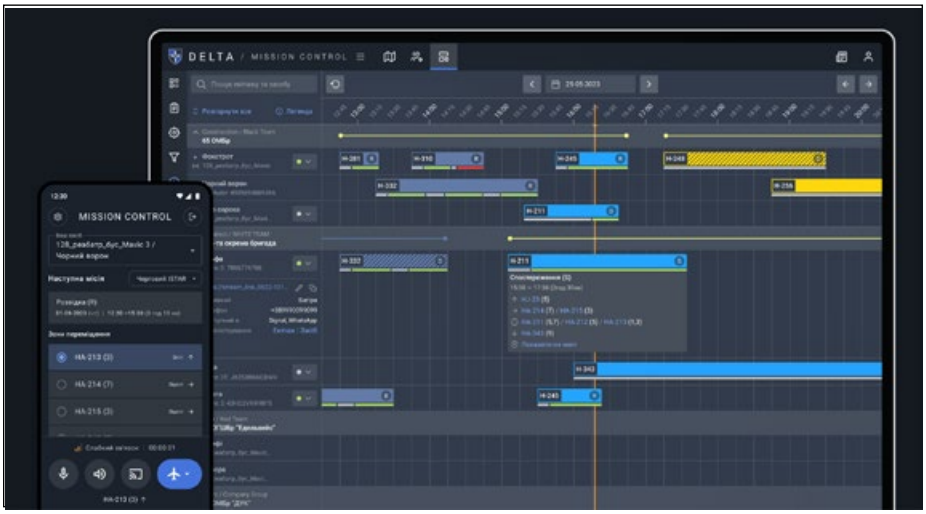
Yhdessä nämä moduulit muodostavat kokonaisuuden, jossa tilannekuva, havaintodata, viestintä ja operatiivinen suunnittelu ovat tiiviisti yhteydessä toisiinsa. Tämä on keskeinen ero verrattuna perinteisiin johtamisjärjestelmiin, joissa nämä toiminnot ovat usein omissa tietojärjestelmäsiiloissaan.

Delta mahdollistaa yhteisen tilannekuvan

Delta -järjestelmä edustaa modernin sodankäynnin kehityssuuntaa, jossa tiedon kerääminen, yhdistäminen ja hyödyntäminen nousevat ratkaisevaan rooliin. Deltan suurimmat hyödyt liittyvät sen kykyyn luoda reaaliaikainen ja jaettu tilannekuva, joka kattaa kaikki johtamisen

tasot yksittäisistä sotilaista aina ylimpään johtoon asti. Tämä yhteinen tilannekuva muodostuu laajasta datalähteiden verkostosta, johon kuuluu esimerkiksi droonien tuottama kuva- ja videomateriaali, satelliittidata, sensorit sekä tiedustelutieto. Kun kaikki tämä informaatio kootaan yhteen järjestelmään, käyttäjät saavat kokonaisvaltaisen näkymän taistelukentän tilanteeseen lähes reaaliajassa.

Tällainen tiedon keskittäminen mahdollistaa ennen kaikkea nopeamman ja paremman päätöksenteon. Perinteisesti sotilaallinen päätöksenteko on kärsinyt viiveistä ja tiedon pirstaleisuudesta, mutta Delta vähentää näitä ongelmia tarjoamalla analysoitua ja ajantasaista tietoa suoraan päätöksentekijöille. Järjestelmä ei pelkästään kerää dataa, vaan myös tukee sen analysointia ja jalostamista käyttökelpoiseksi tiedoksi, mikä tekee operaatioiden suunnittelusta ja toteutuksesta tehokkaampaa.



Kuva 3. DELTA Mission Control. Lähde: Ministry of Defence of Ukraine

Toinen keskeinen etu on eri joukkojen ja toimijoiden välinen koordinointi. Delta toimii yhteisenä alustana, jonka kautta eri aselajit ja yksiköt voivat jakaa tietoa ja synkronoida toimintaansa. Esimerkiksi miehittämättömien ilma-alusten käyttöä voidaan hallita keskitetysti, mikä vähentää päällekkäistä toimintaa ja minimoi virheet. Lisäksi järjestelmään integroidut ominaisuudet, kuten reaaliaikainen videon suoratoisto ja kohteiden tunnistus, nopeuttavat tiedon kulkua tiedustelusta iskujen toteuttamiseen.

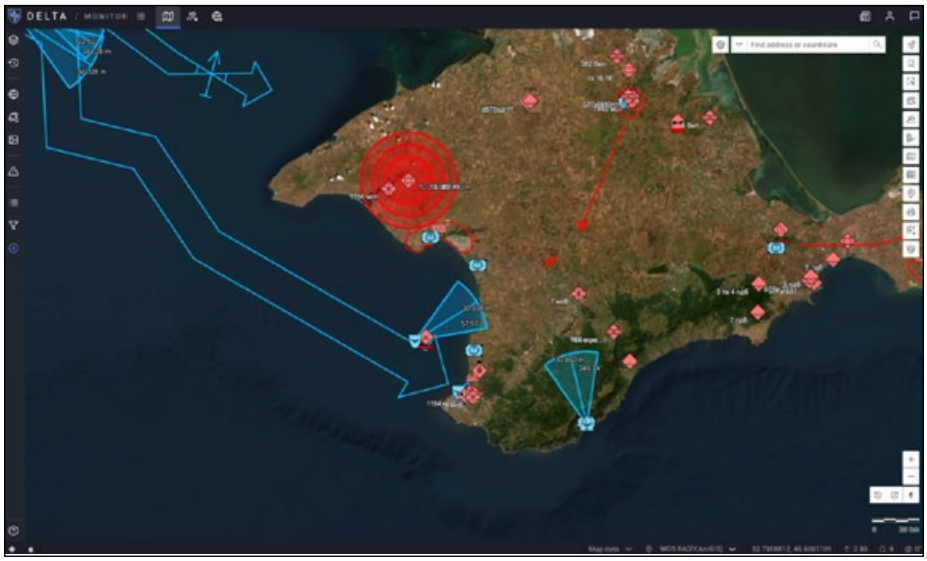
Kokonaisuutena Delta mahdollistaa siirtymän kohti verkottunutta ja dataohjautuvaa sodankäyntiä. Sen keskeinen arvo on siinä, miten se yhdistää eri toiminnot yhdeksi yhteentoimivaksi johtamisjärjestelmäksi. Tämä tekee siitä tehokkaan työkalun, joka parantaa tilannekuvaa, nopeuttaa päätöksentekoa ja tehostaa operaatioiden toteutusta.

On syytä nostaa esiin vielä tekoäly. Tekoälyratkaisujen keskeinen edellytys on laadukas ja ajantasainen data. Ukrainassa Delta ja muut johtamisjärjestelmät tuottavat dataa päivittäin suuria määriä suoraan taistelukentältä. Tekoälyratkaisuja on jo nähty käytännössä, mutta laajamittainen hyödyntäminen antaa vielä odottaa itseään. Tämän kehityksen saralta mielenkiintoisen mahdollisuuden tuo Palantirin Foundryn päälle rakennettu Ukrainan Brave1 Dataroom, joka tarjoaa ympäristön sotilaallisten tekoälyratkaisujen kehittämiseen.

Deltan rajoitteet ja haavoittuvuudet

Delta nojaa laajaan digitaaliseen infrastruktuuriin. Se perustuu pitkälti länsimaisten ja yksityisten teknologiayritysten ratkaisuihin, kuten pilvipalveluihin, satelliittiyhteyksiin ja mobiilialustoihin. Tämä mahdollistaa nopean tiedonkulun, mutta tekee järjestelmästä riippuvaisen toimijoista ja tekijöistä, joita Ukraina ei hallitse. Häiriöt näissä palveluissa heikentävät suoraan Deltan toimintaa.

Järjestelmän toiminta on vahvasti sidoksissa yhteyksien toimivuuteen. Rintamaolosuhteissa viestintä ei ole vakaata, ja vastustaja pyrkii aktiivisesti häiritsemään tiedonsiirtoa. Yhteyksien katkeaminen heikentää järjestelmän hyötyä välittömästi. Samalla Delta ja sen käyttäjät ovat jatkuvien kyberuhkien kohteena, mikä edellyttää jatkuvaa suojaamista ja ylläpitoa.



DELTA Monitor. Lähde: Ministry of Defence of Ukraine

Delta on kehittynyt alhaalta ylöspäin käytännön tarpeista. Tämä on mahdollistanut nopean kehityksen, mutta kokonaisuutta ei ole suunniteltu yhtenäiseksi alusta alkaen. Uusia toimintoja on lisätty vaiheittain, mikä lisää järjestelmän monimutkaisuutta ja voi vaikeuttaa hallintaa pitkällä aikavälillä. Tämä näkyy myös käytössä. Esikuntatasolla järjestelmä toimii vakaammin, mutta etulinjassa yhteydet katkeilevat ja olosuhteet ovat epävarmat.

Kokonaisuutena Delta on tehokas mutta jatkuvasti kehittyvä järjestelmä. Sen nopeus ja joustavuus tuovat merkittäviä etuja, mutta samalla myös rajoitteita. Järjestelmä vaatii jatkuvaa suojaamista, ylläpitoa ja kehittämistä, eikä se ole koskaan täysin valmis.

Johtopäätös

CSIS -ajatushautomon raportissa Katerina Bondar esittää osuvasti kysymyksen Does Ukraine Already Have Functional CJADC2 Technology? Onko Ukraina siis jo käytännössä saavuttanut sen, mitä muualla vasta kehitetään? Deltan perusteella vastaus näyttää ainakin osittain myönteiseltä. Järjestelmä on NATO-yhteensopiva, taistelussa testattu ja käytössä laajasti koko organisaatiossa. Se mahdollistaa tiedon jakamisen ja koordinoinnin tavalla, joka vastaa monilta osin niitä tavoitteita, joita länsimaisissa hankkeissa on asetettu. Lopulta ratkaisevaa ei ole se, miltä järjestelmä näyttää suunnitelmissa, vaan se, miten se toimii käytännössä.

Kirjoittajan näkemyksen mukaan Deltan kehitysperiaatteissa on paljon samaa ajattelua kuin Yhdysvaltain NGC2 -hankkeessa. NGC2 -hanketta kuvattaessa on todettu: “in the past warfighting functions, such as intelligence, logistics or fires, were siloed in their own staff sections with their own systems slowing down sharing and situational awareness. NGC2 aims to collapse all those systems and functions into applications analogous to an iPhone so a commander or units will have access to all the data and information.”

Datakeskeisissä johtamisjärjestelmissä kehityssuunta on kohti yhteistä tietopohjaa, jonka päälle eri toiminnallisuudet rakentuvat. NGC2 -hanke ja Delta -järjestelmä ovat tästä hyviä esimerkkejä. Molemmissa tavoitteena on, että sama data on eri käyttäjien hyödynnettävissä eri näkymien ja sovellusten kautta, sen sijaan että tieto olisi siiloissa erillisissä tietojärjestelmissä.

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

TEKSTI: Jyrki Penttinen, Sr. Program Manager, Alphacore Inc., USA

Droonipohjaiset matkaviestintäverkot

Miehittämättömien droonien käyttö on kasvanut merkittävästi viimeisen vuosikymmenen aikana. Droonien etäohjaus- ja dataliikennöinti voi perustua esimerkiksi Wi-Fi-yhteyteen tai mobiiliverkkoon. Droonien avulla voidaan myös luoda matkaviestintäverkon radiopalvelu niissä olevien tukiasemien kautta. Tällainen ratkaisu sopii nopeasti käyttöönotettavaan paikalliseen hätäviestintään esimerkiksi katastrofialueella, ja tukiasemadrooneja voidaan käyttää moniin muihinkin tilanteisiin niin siviili- kuin maanpuolustuksen sovelluksissa.

Droonien kehitys ja niiden mahdollistamat sovellukset

Miehittämättömät ilma-alukset eli droonit (Unmanned Aerial Vehicle, UAV; uudistettuna terminä myös Uncrewed Aerial Vehicle) ovat viimeisen vuosikymmenen aikana kehittyneet merkittävästi niin teknisesti kuin kaupallisesti. Alun perin sotilaskäyttöön tarkoitetut UAV-järjestelmät (Unmanned / Uncrewed Aerial System, UAS) ovat laajentuneet siviilisovelluksiin, kuten logistiikkaan, maatalouteen, infrastruktuurin tarkastuksiin sekä pelastus- ja valvontatehtäviin. Kehitystä ovat osaltaan tukeneet autonominen navigointi, modernit sensorit sekä tekoälypohjaiset ohjaus- ja analyysijärjestelmät.

Droonien ohjaus- ja dataliikennöinti voivat perustua esimerkiksi Wi-Fi-yhteyteen tai mobiiliverkkoon. Viestimies-lehden artikkeli ”Matkaviestintäverkkoihin liitetyt droonit” (3/2024) kuvaa aihetta siviili- ja sotilassovelluksia peilaten. Matkaviestintäverkkoihin kytketyt droonit (cellular-connected UAV, C-UAV) ovat nopeasti kehittyvä tekniikan ala, joka tarjoaa taajuushallinnan määrityksistä riippuen mahdollisuuden droonien ohjaukseen myös (radio)näköyhteyden takana (Beyond Line of Sight, BLOS). Seuraava kehitysaskel on droonien käyttö myös osana matkaviestintäverkkoa siten, että ne voivat toimia ilma-aluksina 4G- tai 5G-tukiasemille tai -toistimille.

Kantokyvyllä (payload) tarkoitetaan droonin kykyä kuljettaa hyötykuormaa, kuten kameroita, sensoreita tai tietoliikennelaitteita. Nykyiset keskikokoiset ja suuret droonit kykenevät kuljettamaan useiden kilogrammojen hyötykuormia, mikä voi soveltua myös mobiiliverkon tukiasemakomponenttien asentamiseen ja operatiiviseen käyttöön.

Samanaikaisesti akkuteknologian kehitys on parantanut sähköllä toimivien droonien lentoaikaa. Akun kesto on kriittinen tekijä erityisesti tietoliikennesovelluksissa, joissa droonin tulee pysyä ilmassa pitkiä aikoja. Litium-polymeeri- ja litiumioniakkujen energiatehokkuus on kasvanut, ja lisäksi hybridiratkaisut, esimerkiksi polttokennoihin tai generaattoreihin perustuvat järjestelmät, mahdollistavat droonien useiden tuntien operoinnin.

Monien muiden sovellusten ohella droonien kehitys tukee myös tietoliikenteen tarpeita. Drooneja voidaan siten käyttää esimerkiksi tilapäisten radioverkkojen luomiseen katastrofitilanteissa, kapasiteetin lisäämiseen ruuhkautuneilla alueilla, ja verkon kattavuuden laajentamiseen vaikeapääsyisissä ympäristöissä. Droonien käyttö matkaviestintäverkkojen osana on siten luonnollinen kehityspolku mukautuvasti laajennetun palvelualueen luomiseen.

5G-järjestelmien kehitys

Vaikka 4G:n suorituskyky riittää sinänsä droonipohjaisten tukiasemien vaatimuksiin, 5G tarjoaa erityisiä hyötyjä verkkotoimintojen virtualisoinnin sekä kehittyneiden ja kustannustehokkaiden liikennöintimenetelmien myötä. 5G voidaan toteuttaa esimerkiksi Open RAN -pohjaisena toteutuksena, jonka laitteisto kootaan markkinoilta saatavissa olevista (commercial off-the-shelf, COTS) komponenteista, ja jonka tehonkulutus voidaan optimoida drooniympäristöön soveltuvaksi. Droonien kautta voidaan siten tarjota kaikkia 5G-mobiiliverkkon yhteystekniikoita: eMBB (enhanced Mobile Broadband); korkean datanopeuden palvelut. URLLC (Ultra-Reliable Low Latency Communications); erittäin luotettavat ja matalan viiveen sovellukset. mMTC (massive Machine Type Communications); massiivinen IoT-laitteiden liitettävyys.

3GPP (3rd Generation Partnership Project) on standardointiorganisaatioiden yhteenliittymä, joka määrittää nykyisten mobiiliverkkojen tekniset spesifikaatiot sisältäen globaalit 2G-5G -järjestelmät ja joka on hiljattain aloittanut normatiivisen 6G-spesifikaatioiden työstämisen. 3GPP on ottanut huomioon 4G- ja 5G-matkaviestintäverkkoihin kytkettyjen droonien tuen 3GPP:n Release 15–18 -julkaisuissa. Nykyisissä spesifikaatioissa 3GPP on tunnistanut drooneille kaksi pääroolia: UAV käyttäjänä; tässä roolissa droonit toimivat verkkoon kytkettyinä viestintälaitteina hyödyntäen 5G-yhteyksiä. UAV verkon komponenttina (tukiasema tai toistinasema); tässä roolissa droonit toimivat osana verkon infrastruktuuria.

Droonien käyttämiseen vaadittavia teknisiä kehityskohteita ovat seuraavat: 1) Kolmiulotteinen peittoalue. Matkaviestinnän radioverkkosuunnittelu on perinteisesti tehty katutason peittoalueen perusteella kaksiulotteisesti, mutta ilmassa operoivien droonien myötä 5G-verkkojen suunnittelu laajentuu kolmiulotteiseen tilaan. Se vaatii muutoksia niin suunnit-

telutyökaluihin kuin rakennusstrategioihin. 2) Häiriönhallinta. Droonipohjaisten tukiasemien ja toistinasemien korkea sijainti voi aiheuttaa häiriöitä useille tukiasemille niin maatasossa kuin muiden droonien verkkoelementeille. 3) UAV-tunnistus ja hallinta. Verkko tunnistaa UAV-laitteet ja optimoi resurssien käytön dynaamisesti sen mukaisesti, kuinka droonit ovat kulloinkin asemoituneet ilmatilassa. 4) Lentoturvallisuuden integraatio. 3GPP on alusta asti todennut tärkeäksi koordinoinnin muun ilmailuliikenteen kanssa ja siten integrointi ilmailujärjestelmiin (UAS Traffic Management, UTM).

3GPP on julkaissut useita UAV-aiheisia teknisiä raportteja (TR, techical report) ja spesifikaatioita (TS, technical specification), kuten TR 36.777 (LTE-tuki UAV-laitteille), TS 23.256 (UAV-tunnistus ja hallinta 5G-kytkentäverkossa) ja TR 38.811 (5G-radiorajapinnan tuki ilmassa ja avaruudessa sijaitseville alustoille).

UAV:n ja 5G:n integraatio mahdollistaa useita käyttökohteita, joista esimerkkejä ovat reaaliaikainen videovalvonta, teollinen tarkastus (esim. sähkölinjat, öljyputket), hätäviestintä ja pelastustoimet, sekä autonominen logistiikka.

5G-verkon luonti droonien avulla

Droonipohjaiset 5G-radioverkot edustavat uuden sukupolven mukautuvaa tietoliikenneinfrastruktuuria, jossa miehittämättömät ilma-alukset toimivat tukiasemina (next generation node B, gNB) osana radioverkon arkkitehtuuria. Tällaiset verkot mahdollistavat nopean, väliaikaisen käyttöönoton tilanteissa, joissa maanpäällinen infrastruktuuri puuttuu, on vaurioitunut tai ei muuten tarjoa riittävää kapasiteettia. 5G-radioverkon luonti droonien avulla toteutetaan siten, että drooni toimii joko tukiasemana, toistimena (relay node) tai verkon reunalaskentayksikkönä (edge computing node).

Riippuen fyysisestä mallista, yksittäinen drooni voi kantaa ilmassa kevyen 5G-tukiaseman. Tällainen ratkaisu sisältää 5G-radioyksikön (Radio Unit, RU), mahdollisesti hajautetun yksikön (Distributed Unit, DU) ja antennijärjestelmän (Antenna Unit, AU). Yhteys kytkentäverkkoon (5G Core, 5GC) voidaan toteuttaa esimerkiksi satelliittiyhteyden kautta, mikroaaltolinkillä tai toisella maa-asemalla.

Ratkaisu soveltuu erityisesti hätätilanteisiin nopeasti käyttöönotettavana ensimmäisen vaiheen viestintäjärjestelmänä, jos esimerkiksi luonnonkatastrofi on romahduttanut pelastusalueen tietoliikenneinfrastruktuurin. Drooniverkkoja voidaan hyödyntää myös lisäkapasiteetin tarjoamiseen erilaisissa yleisötapahtumissa, joissa kapasiteettitarve moninkertaistuu väliaikaisesti.

Drooneja voidaan käyttää lisäksi parvena (swarm) parantamaan edelleen kapasiteettia ja peittoaluetta. Drooniryhmän luoman verkon avulla saavutetaan dynaamisesti laajennettava peittoalue. Se parantaa väliaikaisverkon palvelutasoa ja vikaantumisen sietoa varmentavien yhteyksien myötä adaptiivisen verkon topologian myötä.

Parviratkaisuissa droonit voivat muodostaa mukautuvan mesh-verkon, jossa ne kommunikoivat keskenään ja jakavat liikennettä maanpinnalla oleville käyttäjille. Tämä muistuttaa ad hoc -verkkoja (Mobile Ad Hoc Networks, MANET) 5G-integraatiolla siten, että droonien asemointi 3D-tilassa voidaan toteuttaa droonien keskinäinen etäisyys sekä droonien korkeus maanpinnasta optioiden esimerkiksi keinoälyä soveltaen ja reaaliaikaista radioverkkosuunnittelua hyödyntäen.

Käytännön esimerkkejä kaupallisista sovelluksista

Metsäpalojen monitorointi. Droonipohjaisia 5G-verkkoja voidaan käyttää metsäpalojen havainnointiin. Tässä käyttökohteessa droonit luovat paikallisen verkon, jonka kautta drooneihin integroidut sensorit ja kamerat lähettävät reaaliaikaista dataa. Pelastusviranomaiset saavat tällöin mahdollisimman nopean ja kattavan tilannekuvan jo siinä vaiheessa, kun muut valvontamenetelmät ovat vielä tavoittamattomissa. 5G:n matala viive mahdollistaa nopean reagoinnin ja tekoälypohjaisen analyysin. Samalla drooniverkko voi tarjota paikallisen radiopalvelun pelastustyöntekijöille, mikäli tulipalo on vaurioittanut teleinfrastruktuuria.

Hätäverkot. Katastrofitilanteissa, kuten maanjäristyksissä ja myrskyissä, perinteinen infrastruktuuri voi tuhoutua osittain tai kokonaan. Tällaisissa tilanteissa droonit voidaan ottaa nopeasti käyttöön tilapäisinä tukiasemina ja viestintälinkkeinä pelastushenkilöstölle ja apua tarvitseville.

Kaupunkialueen kapasiteetin lisäys. Suurissa yleisötapahtumissa droonit voivat lisätä verkon kapasiteettia tarjoten kapasiteettia tarpeen mukaisesti.

Droonipohjaiset 5G-verkot sotilaskäytössä. Sotilaskäytössä droonipohjaiset 5G-verkot tarjoavat merkittäviä etuja hajautettuun, nopeasti käyttöönotettavaan taktiseen viestintään, joka voidaan optimoida elektroniseen sodankäyntiin.

Sotilaskäytössä perinteiset radioverkot ovat haavoittuvia. Esimerkkejä haasteista ovat kiinteästi asennetut tukiasemat, joiden toimintaa ja linkkien laatua vihollinen voi häiritä. Drooniverkot mahdollistavat sen sijaan hajautetun ja dynaamisen arkkitehtuurin, jota on haasteellisempaa häiritä tai tuhota droonien vaihtaessa paikkaansa kolmiulotteisessa tilassa. Droonipohjaiset tukiasemat voidaan ottaa käyttöön nopeasti taistelukentällä, ja verkko mukautuu tilanteeseen ad-hoc -viestintäjärjestelmien periaatteiden mukaisesti.

5G mahdollistaa korkean datanopeuden esimerkiksi laadukkaaseen ja korkean kapasiteetin reaaliaikaiseen videolähetteeseen. 5G:n matala viive sopii erityisesti nopeaan droonien ohjaukseen ja keinoälyyn liitettynä se mahdollistaa autonomiset järjestelmät. Elektronisen sodankäynnin osalta droonit voivat toimia myös signaalin häirintäalustoina ja tiedustelujärjestelminä.

3D-yksityisverkkojen malleja

5G-yksityisverkko (Non-Public Network, NPN) tarkoittaa yksityistä mobiiliverkkoa. Ne soveltuvat pelastuspalvelun ja sotilaalliseen käyttöön ja syrjäisiin ympäristöihin erillisverkkoina. Yksinkertaisten arkkitehtuurimallien kautta ne ovat erityisen sopiva myös UAV-pohjaisiin tilapäisverkkoihin.

Taulukko 1 koostaa 5G-yksityisverkkojen tyypillisiä vaihtoehtoja perustuen 3GPP:n määrityksiin ja esittää niiden hyötyjä ja heikkouksia mukautettuina drooniympäristöön.

Kuva 1 esittää SNPN-pohjaisen drooniverkon periaatteen perustuen lähteessä [1] esitettyyn tutkimukseen.

Kuvassa 1 esitetty järjestelmä perustuu yksinkertaistettuun 5G SNPN-arkkitehtuuriin, jossa yksittäinen drooni toimii 5G-tukiasemana (gNB) ja tarjoaa paikallisen yhteyden sen alapuolella oleville käyttäjälaitteille. Ratkaisu on suunniteltu erityisesti tilanteisiin, joissa perinteinen mobiiliverkko ei ole käytettävissä, mahdollistaen nopeasti käyttöönotettavan tilapäisen verkon.

Järjestelmässä UAV sisältää radioverkon toiminnallisuudet. Kytkentäverkon perustoiminnot (esim. UPF, User Plane Function; CP, Control Plane; UDM; Unified Data Management) voidaan sijoittaa samaan UAV:hen, toiseen UAV:hen tai radiolinkin kautta erilliseen maa-asemaan. Kyseinen arkkitehtuurimalli voidaan laajentaa usean droonin järjestelmäksi, jossa UAV-parvi muodostaa verkon esimerkiksi droonien välisten matalan viiveen PC5-sidelink-yhteyksien avulla. Tuloksena on dynaamisesti hajautettu 5G-radioverkko (mesh-RAN), jolla voidaan laajentaa radiopeittoa ja -kapasiteettia sekä mahdollistaa varmennetut yhteydet.

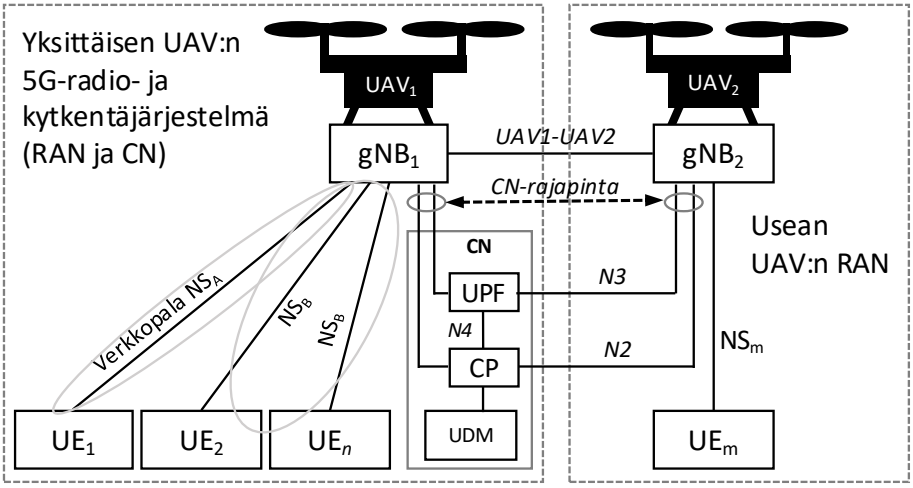
Drooniverkkojen hyödyt ja rajoitteet

Droonien yleistymisen myötä niiden tukemat sovellukset monipuolistuvat. Matkaviestintäverkon väliaikainen käyttöönotto on malliesimerkki uuden tekniikan hyödyistä esimerkiksi kriisitilanteissa vaikkapa myrskyn jälkeisen paikallisen ensiapuverkon luomiseen silloin, kun muu infrastruktuuri on lamaantunut tai tuhoutunut.

Drooniverkon hyötynä on tässä käyttötilanteessa nopea käyttöönotto. Matkaviestintäverkon palveluun suunniteltu UAV voidaan lähettää ilmaan minuuteissa siitä hetkestä, kun sen operaattori saapuu paikalle. Koska tässä käyttötilanteessa tarkoitus on etsiä alueella olevia uhreja tarjoten heille verkkopalvelu vielä toimivien matkaviestintensä kautta, ei ratkaisun käytössä tarvita muuta infrastruktuuria.

Verkkomalli	Hyödyt	Heikkoudet
SNPN (Standalone Non-Public Network). Itsenäinen verkko. Kaikki verkon komponentit (radio- ja kytkentäsegmentit) voidaan sijoittaa drooniin tai hajauttaa usean droonin ja maa-asemien välille.	Verkon haltijalla on täysi verkon hallinta ml. eristetty tietoturva. Nopea käyttöönotto. Ei riippuvuutta ulkoisesta infrastruktuurista.	Rajoitettu kapasiteetti ja skaalautuvuus. Energiarajoitteet UAV-alustalla.
PNI-NPN (Public Network Integrated NPN). Integroitu julkiseen verkkoon. Voi perustua jaettuun radioverkkoon (RAN sharing) tai jaettuun kytkentäverkkoon (core sharing).	Hyvä skaalautuvuus. Mahdollisuus verkkovierailuun (roaming) ja siten laajaan kattavuuteen.	Riippuvuus operaattorista. Monimutkainen integraatio.
Yksittäinen UAV-tukiasema. Perusarkkitehtuurissa on UAV ja integroitu gNB, mahdollisesti kevyet kytkentäverkon toiminnot droonissa tai maa-asemassa. Mahdollistaa paikallisen UE–UAV–UE -viestinnän.	Yksinkertainen toteutus. Nopea käyttöönotto. Hyvä yksittäinen LOS (Line-of-Sight) -yhteys.	Rajallinen peitto. Yksittäinen vikapiste.
UAV-parvi. Usean droonin verkko mahdollistaa mesh-topologian, droonien väliset yhteydet (esim. PC5 sidelink) ja hajautetun RAN-arkkitehtuurin.	Parempi peitto ja kapasiteetti. Redundanssi. Adaptiivinen topologia.	Synkronoinnin haasteet. Yhteysvastuun vaihdon haasteet (ping-pong -ilmiö).

Taulukko 1. Esimerkkejä matkaviestintäpohjaisista yksityisverkoista.



Kuva 1. Esimerkki SNPN-pohjaisen drooniverkon periaatteesta. Kuvassa on esitetty 5G-verkon toteutus yksittäisen droonin kautta (RAN ja CN) sekä laajennettu, usean droonin RAN.

Esimerkin skenaariossa voidaan jo pelkän 5G-peruspalvelun avulla saada vaikkapa välitettyä alueella oleville käyttäjille tekstiviestejä. Yksi mahdollisuus on luoda droonin kautta kansallisten operaattoreiden palvelut omilla verkkotunnuksillaan siten, että drooni lähettää operaattoriasiakkailleen tietoja (tekstiviestejä) opastamaan käyttäjiä ottamaan yhteyttä paikalla olevaan pelastusryhmään.

Toinen vaihtoehto on tarjota yleinen verkkopalvelu, johon alueella olevat kännykän käyttäjät voivat kytkeytyä riippumatta operaattoritunnuksesta 3GPP:n määritysten mukaisesti siten, että hätäpuhelu (tässä tapauksessa paikalliselle pelastusryhmälle ohjattuna) voidaan muodostaa riippumatta verkkotunnuksesta, myös ilman SIM-korttia. Droonit voidaan varustaa lisäksi kuva- ja radiosensoreilla, ja siten drooniparvella voidaan

suuntia alueella olevien aktiivisten matkaviestimien sijaintitietoja ja nopeuttaa uhrien löytämistä.

Droonipohjaisen matkaviestintäverkon kautta voidaan luoda adaptiivinen peittoalue, ja alueen signaalien perusteella UAV:t voivat sopivia tekniikoita käyttäen asemoitua optimaalisesti lähelle käyttäjiä ja välittää UAV-parven kautta ketjuna viestejä pelastusryhmälle. Droonien kautta luotu 3D-verkko mahdollistaa maanpinnalle asennettuja tukiasemia paremmat yhteydet radiolinkkien näköyhteys optimoiden, koska yhteysvälillä on korkeammalla vähemmän esteitä mahdollistaen tehokkaamman signaalien etenemisen.

Droonipohjaisten verkkojen kautta voidaan käyttää 5G-palveluita tilanteen mukaisesti optimoiden. Käyttö saadaan tasapainoteltua soveltamalla esimerkiksi IoT (mMTC) -yhteysmenetelmää laajalla peittoalueella perusviestintään, ja eMBB-moodia paikallisempaan korkean kapasiteetin viestintään.

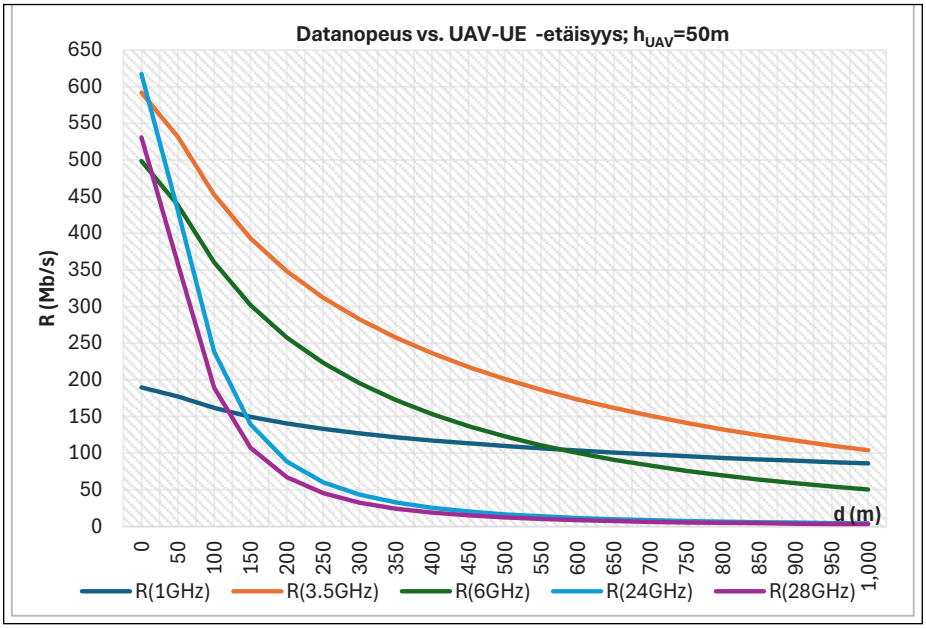
Heikkoudet

Drooniverkoilla on rajoituksia, joista tärkeimmät liittyvät energian rajoitteisiin. 5G:n gNB-laitteiston tehonkulutus voi olla 25–40 W, joskin ottamalla käyttöön vain kaikkein perustavimmat toiminnot ja pienimmät käyttökelpoiset säteilytehot, voidaan UAV:n kyydissä olevan laitteiston tehonkulutusta minimoida.

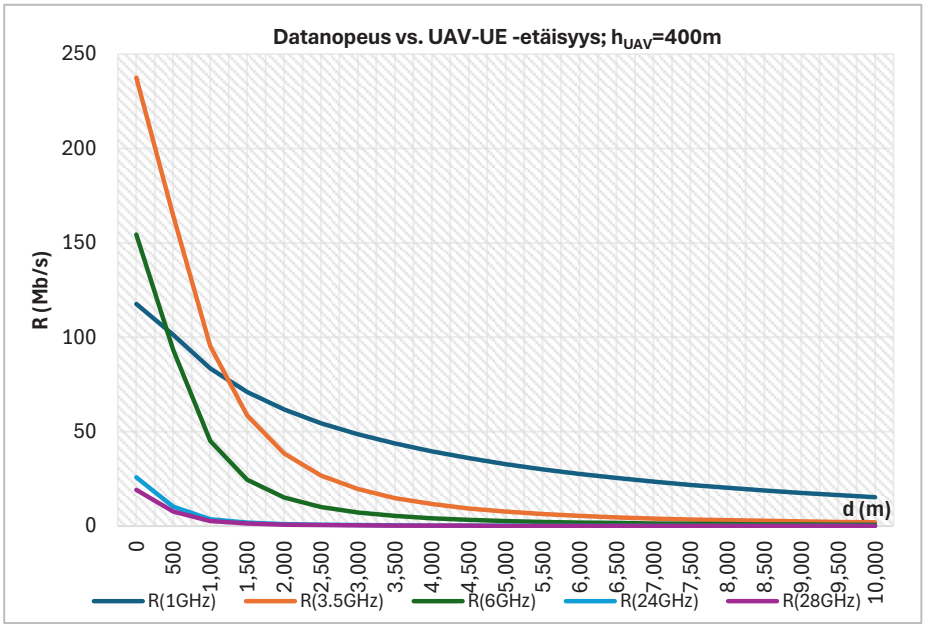
Toisena rajoitteena on lentoaika, joka droonityypistä riippuen voi olla esimerkiksi luokkaa yksi tunti sähkökäyttöisille ratkaisuille. Vaihtoehtoisia droonin tehonlähteitä voidaan valita tilanteen mukaan, ja polttomoottorit tai hybridiratkaisut ovat myös mahdollisia. Kussakin tilanteessa on joka tapauksessa huomioitava lentoajan rajoitteet. Pitempiaikaiseen droonipohjaiseen verkkopalveluiden mahdollistamiseen tarvitaan lataus- tai tankkausstrategia, esimerkiksi vaihdellen kahta drooniparviryhmää siten, että yhden ollessa aktiivinen toista huolletaan.

Kolmantena haasteena ovat radiotekniset seikat, joista esimerkkinä ovat droonisparven keskinäiset solujen radiohäiriöt, mikä on otettava huomioon radioverkon dynamiikassa solujen liikkuessa alueella. Häiriöitä voidaan hallita esimerkiksi tekoälypohjaisesti ja itseoptimoitavilla verkkotoiminnoilla. Toisaalta korkeat radiotaajuudet vaimenevat matalia enemmän, mikä pitää ottaa huomioon laajan alueen skenaarioissa. Lisäksi jatkuva verkkotopologian muutos voi aiheuttaa epävakautta droonien väliseen yhteysvastuun vaihtoon.

Rajoitteena voi olla myös regulaation drooneille asettamat korkeusrajoitukset (esim. 120 m maan pinnasta Euroopassa ja 400 jalkaa Yhdysvalloissa) sekä spektrirajoitteet ja RF-säteilyn tehorajoitteet.



Kuva 2. Esimerkki droonin gNB:n eMBB-yhteyden datanopeudesta etäisyyden funktiona (gNB-UE), kun droonin korkeus maanpinnasta on 50 m.



Kuva 3. Esimerkki droonin gNB:n eMBB-yhteyden datanopeudesta etäisyyden funktiona (gNB-UE), kun droonin korkeus maanpinnasta on 400 m.

Suorituskykylaskelmia

Lähteessä ”Design Feasibility and Link Budget Assessment of Aerial 5G IoT and eMBB Connectivity” [1] esitetään tutkielmia drooniverkkojen kautta luotavasta 5G-radiopalvelun peittoalueesta ja vastaavasta datanopeudesta. Tutkimus keskittyy suhteellisen avoimeen topologiaan radiolinkkibudjetin periaatteita soveltamalla. Monimutkaisempiin topologioihin on järkevintä käyttää radioverkkosuunnittelun työkaluja ja digitaalisia karttoja, mutta kyseinen tutkimus tarjoaa mahdollisuuden korkean tason radiolinkin suorituskykyvertailuihin ottamalla huomioon droonin etäisyys maanpinnasta.

Kuvat 2 ja 3 koostavat esimerkkiskenaarion oletuksilla saavutettavia datanopeuksia droonin korkeudella 50 m ja 400 m käytettäessä radiotaajuutta 1 GHz – 28 GHz.

Kuvat 2 ja 3 havainnollistavat UAV-tukiaseman (UAV-gNB) korkeuden (hUAV) vaikutusta välillä 50–400 m yksittäisen käyttäjälaitteen (UE, User Equipment) vastaanottamaan datanopeuteen sekä suoraan UAV:n alapuolella, että sitä ympäröivällä alueella. Tulokset perustuvat analyyttiseen mallinnukseen, jossa radiokanavan vaimennus on arvioitu yleisesti tunnetulla vapaan tilan etenemismallilla ja linkkibudjettilaskelmilla, joiden perustana on gNB:n tehotaso +23 dBm eli noin 0.2 W. Droonin antennina on tässä tutkimuksessa ideaalinen ympärisäteilevä malli.

Tulokset osoittavat, että käytettävällä taajuusalueella on ratkaiseva vaikutus saavutettavaan datanopeuteen ja sen alueelliseen jakaumaan. Millimetrialueen taajuuksilla (24 GHz ja 28 GHz) saavutetaan korkeita datanopeuksia silloin, kun käyttäjä sijaitsee lähellä UAV-tukiasemaa. Tämä johtuu laajasta kaistanleveydestä, joka mahdollistaa korkean spektritehokkuuden ja siten yksittäisen linkin gigabittiluokan tiedonsiirtonopeudet. Näiden taajuuksien voimakas vaimeneminen aiheuttaa kuitenkin sen, että datanopeus heikkenee nopeasti etäisyyden kasvaessa. Jo muutaman sadan metrin etäisyydellä signaalin heikkeneminen johtaa merkittävään suorituskyvyn laskuun, mikä rajoittaa millimetrialueen taajuuksien käytön käytännössä pienialaisiin, korkean kapasiteetin “hotspot”-skenaarioihin.

Tässä esitetyn tutkimuksen perusteella keskitaajuusalueet (erityisesti 3.5 GHz ja 6 GHz) tarjoavat huomattavasti tasapainoisemman suorituskyvyn. Näillä taajuuksilla saavutetaan edelleen korkeat datanopeudet lyhyillä etäisyyksillä, mutta suorituskyky säilyy vakaampana myös UAV:n ympäröivillä alueilla. Tämä tekee keskitaajuusalueesta käytännössä tehokkaimman kompromissin kattavuuden ja kapasiteetin välillä erityisesti tilanteissa, joissa käyttäjät eivät sijaitse suoraan tukiaseman alapuolella vaan jakautuvat laajemmalle alueelle.

Kun UAV:n etäisyyttä maanpinnasta kasvatetaan 50 metristä kohti 400 metriä, havaitaan kaksi avainvaikutusta. Ensinnäkin peittoalue laajenee, koska suurempi korkeus mahdollistaa laajemman näkyvyysalueen (LOS). Toisaalta samanaikaisesti keskimääräinen etäisyys käyttäjiin kasvaa, mikä lisää vaimennusta ja heikentää signaalinvoimakkuutta. Tämä kompromissi näkyy kuvissa 2 ja 3 siten, että droonin ollessa korkealla, saavutetaan laajempi, mutta keskimäärin matalamman datanopeuden peittoalue, kun taas droonin ollessa matalammalla, nopea data keskittyy pienemmälle alueelle UAV:n läheisyyteen.

Tärkeä havainto on, että korkean taajuuden järjestelmät hyötyvät matalasta droonin sijainnista, joissa etäisyys käyttäjiin pysyy lyhyenä, kun taas matalammat taajuudet kykenevät hyödyntämään laajempia lentokorkeuksia säilyttäen käyttökelpoisen datanopeuden myös laajemmalla alueella. Tämä korostaa sitä, että UAV-tukiaseman optimaalinen etäisyys maanpinnasta ei ole vakio, vaan se riippuu suoraan käytettävästä taajuusalueesta sekä palvelun tavoitteista (kapasiteetti vs. kattavuus).

Yhteenvetona voidaan todeta, että kuvien 2 ja 3 tulokset vahvistavat keskeisen suunnitteluperiaatteen droonipohjaisille 5G-verkoille: korkeat taajuudet soveltuvat paikallisiin, korkean kapasiteetin käyttötapauksiin, kun taas keskitaajuudet tarjoavat käytännössä parhaimman kokonaisratkaisun dynaamisissa ja laajemmissa käyttöympäristöissä. UAV:n lentokorkeuden optimointi yhdessä taajuusvalinnan kanssa on siten merkittävä tekijä verkon suorituskyvyn kannalta.

Yhteenveto

Droonien ja 5G-teknologian yhdistämisellä saavutetaan uudenlainen adaptiivinen viestintäarkkitehtuuri, joka mahdollistaa nopean verkon käyttöönoton, joustavan kapasiteetin hallinnan ja radiopeittoalueen kattavuuden laajentamisen. Teknologiset avaintekijät tässä kehityksessä ovat kehittynyt UAV-teknologia, 3GPP:n standardointi ja hajautettu verkkoarkkitehtuuri.

Vaikka droonien ja 5G:n teknologiat ovat kehittyneet vahvasti viime vuosina, haasteita erityisesti droonipohjaisille tukiasemille ovat edelleen energiatehokkuus ja regulaatio (ilmailu ja taajuudet), mikä on osaltaan syynä siihen, etteivät droonipohjaiset matkaviestintäverkot ole vielä yleistyneet laajasti.

Tulevaisuudessa drooneihin perustuvat 5G-verkot voivat toimia merkittävänä osana sekä siviili- että sotilasviestintäjärjestelmissä erityisesti tilanteissa, joissa perinteinen infrastruktuuri ei ole käytettävissä tai riittävä.

Lähteet

[1] J. Penttinen, ”Design Feasibility and Link Budget Assessment of Aerial 5G IoT and eMBB Connectivity,” IARIA AIVTS 25, Barcelona, Spain, July 2025. https://www.thinkmind.org/library/AIVTS/AIVTS_2025/aivts_2025_1_10_50022.html.

Artikkelin kirjoittaja

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

Teksti: Mauri Mikkonen, evp-komkapt, Palo Alto Networks

Tekoäly: Viestimiehen uusi rintama

Johdanto: Kun bitti on taisteluväline

Puolustusvoimien data- ja tekoälystrategia 2025 asettaa selvän suunnan, jossa tekoäly ei ole vain tekninen lisäominaisuus, vaan keskeinen osa tulevaisuuden päätöksentekokykyä ja operaatioiden tukemista. Strategian ytimessä on datakeskeinen ja verkostoavusteinen multidomain -kyvykkyys, joka mahdollistaa saumattoman tiedonjaon myös liittolaisten kanssa. Viestimiehelle tämä tarkoittaa uutta vastuualuetta, sillä on varmistettava, että tietoverkoissa kulkeva äly on luotettavaa ja suojattua.

Tekoäly on voimankertoja, joka tarjoaa valtavia mahdollisuuksia esimerkiksi sensorifuusiossa ja kohteen tunnistamisessa, mutta samalla se on uusi hyökkäysvektori, joka pakottaa meidät ajattelemaan turvallisuutta uudella tavalla. Tekoälyn hyödyntämistä on viime aikoina tarkasteltu pääasiassa tuottavuuden parantamisen näkökulmasta, mutta turvallisuus tulee huomioida tässäkin asiassa. Tässä artikkelissa tekoälyä tarkastellaan pääasiassa kyberturvallisuuden näkökulmasta.

Tekoäly hyökkääjän voimakertoimena

Tekoäly ei ole hyökkääjille pelkkä tulevaisuuden visio, vaan päivittäinen operatiivinen työkalu. Hyökkääjillä on merkittävä suhteellinen etu, koska heitä eivät sido puolustajaa rajoittavat laillisuus- tai moraalikysymykset. Havainnot osoittavat, että tekoälyavusteisten hyökkäysten nopeus on kasvanut räjähdysmäisesti.

Siinä missä hyökkääjältä kesti vuosi sitten keskimäärin viisi tuntia päästä sisäänpääsystä tiedon anastamiseen, on aika nyt puristettu keskimäärin 72 minuuttiin. Uusimmat havainnot osoittavat, että nopeimmat hyökkäykset voivat edetä täydelliseen tiedon luvattomaan vientiin jopa 25 minuutissa. Hyökkääjä kykenee suorittamaan massiivista tiedustelua sekunneissa etsiessään kriittisiä haavoittuvuuksia. Jatkuvasti monimutkaistuva tietotekninen ympäristö aiheuttaa puolustajalle ison haasteen; etätyön lisääntyminen, pilvipalvelut, SaaS, mobiilipalvelut jne. Puolustuksen heikko kohta löytynee melko varmasti.

Autonomiset agentit ja realisoituneet uhat

Tekoälyn hyödyntäminen tehostaa ja nopeuttaa “perinteisten” hyökkäysten valmistelua ja toteuttamista. Uudenlaista uhkaa edustavat autonomiset tekoälyagentit, kuten OpenClaw, joilla on kyky käyttää pysyvää muistia pitkäkestoisiin hyökkäysketjuihin. McKinseyn tapauksessa AI-agentti murtautui yrityksen sisäiselle chatbot -alustalle alle kahdessa tunnissa ja anasti valtavan määrän dataa. Tämä on esimerkki siitä, kuinka yrityksen sisäiset tekoälyassistentit on mahdollista manipuloida paljastamaan salassa pidettävää tietoa tai järjestelmän taustalla olevia ohjeistuksia. Nämä ”mini-työntekijöinä” toimivat agentit voivat tulla saastutetuiksi pelkästään lukemalla haitallisen sähköpostin tai verkkosivun, jolloin ne alkavat toimia hyökkääjän lukuun varastaen esimerkiksi selainevästeitä ja kirjautumistunnuksia taustalla.

Samaan aikaan ilmiö nimeltä ”vibe coding”, eli ohjelmistojen luominen tekoälyllä ilman perinteistä tietoturvaosaamista, luo organisaatioihin uusia haavoittuvuuksia. Huhtikuun alussa kohistiin Anthropicin Claude Mythos tekoälymallin esiversiosta. Malli on niin tehokas, että se on löytänyt aiemmin tuntemattomia tietoturvahaavoittuvuuksia vuosia tai vuosikymmeniä toimineista ohjelmista. Yhtiö itse on todennut, että seuraukset taloudelle tai turvallisuudelle voivat olla vakavat jos malli päätyy vääriin käsiin. Anthropic ja 11 muuta johtavaa tietoturvatoimijaa ovat käynnistäneet projektin ”Glasswing”, jonka pyrkimys on valjastaa nämä kyvykkyydet puolustukselliseen käyttöön.

Syvälle mallin ytimeen: Näkymättömät uhat

Monet järjestelmät käyttävät nykyään tekoälyä valvomaan toista tekoälyä, mutta nämä niin kutsutut tekoälytuomarit ovat alttiita manipulaatiolle. Hyökkääjät voivat käyttää fuzzing -tekniikkaa löytääkseen näistä portinvartijoista heikkouksia, joilla haitallinen sisältö saadaan näyttämään turvalliselta pelkkien muotoilukikkojen avulla. Tutkimukset ovat paljastaneet myös ns. ”Agent Session Smuggling” -hyökkäyksiä, joissa hyökkäävä agentti pystyy salakuljettamaan haitallisia komentoja toisen agentin istuntoon ilman ihmisen valvonnan väliintuloa. Perinteiset skannerit näkevät tekoälymallit vain tavallisina tiedostoina, eivätkä ne kykene purkamaan mallin arkkitehtuuria, jolloin mallin sisään piilotetut haitalliset koodit jäävät näkymättömiin.

Ukrainan opetukset: Algoritmien välinen sota

Ukrainan taistelukentiltä saadut kokemukset osoittavat, että tekoäly on jo muuttanut sodankäynnin luonnetta. Sota on osoittanut, että tekoäly ei ole staattinen kyvykkyys, vaan dynaaminen ”kissa ja hiiri” -peli algoritmien välillä. Vastustaja kykenee muuttamaan elektronisen

Patria

Kun kaiken on pakko toimia

Suomi tunnetaan korkeasta teknologiastaan ja poikkeuksellisesta kyvystään selviytyä ja sopeutua. Vaativat luonnonolosuhteet ja rajalliset resurssit ovat opettaneet meitä oppimaan ja innovoimaan. Perusteellinen valmistautuminen on kulttuurimme selkäranka.

Patria on moderni ja kansainvälinen puolustus- ja teknologiayritys, jolla on yli 100 vuoden kokemus. Käytämme resursseja viisaasti, luomme innovatiivisia ratkaisuja ja rakennamme älykkäitä järjestelmiä, jotka takaavat parhaan mahdollisen selviytymiskyvyn kaikissa olosuhteissa.

Teemme yhteistyötä asiakkaidemme kanssa koko elinkaaren ajan varmistaaksemme parhaan mahdollisen suorituskyvyn ja saatavuuden. Rehellinen ja suora yhteistyö on toimintamme ydin. Rakennamme poikkeuksellisia kumppanuuksia, jotka kestävät myös kriittisissä operaatioissa.

Patria - #1 kumppani kriittisissä olosuhteissa - maalla, merellä ja ilmassa.

häirinnän (EW) taktiikoitaan, kohteiden naamiovärityst tai droonien lentoratoja päivittäin, mikä tekee jäykistä, kerran koulutetuista tekoälymalleista nopeasti käyttökelvottomia.

Keskeinen opetus on, että tekoälyjärjestelmien on kyettävä oppimaan ja mukautumaan lähes reaaliajassa. Tämä vaatii katkeamatonta sensoridatan virtaa rintamalta takaisin koulutusympäristöihin ja päivitettyjen mallien nopeaa palauttamista takaisin kentälle. Ukrainassa on myös nähty, kuinka vastustaja pyrkii ”myrkyttämään” tekoälypohjaisia maalinosoitusjärjestelmiä syöttämällä niille vääristeltyä tilannetietoa, mikä korostaa datan alkuperän ja eheyden varmistamisen merkitystä.

Datan laatu ratkaisee

Suojautuminen vaatii monitasoista lähestymistapaa, jossa perinteinen kyberturvallisuus kohtaa uuden tekoälyspesifin suojauksen. Puolustusvoimien strategian mukaan dataa on kohdeltava strategisena voimavarana. Datan laatu ratkaisee, onko tekoäly suorituskyky vai taakka. Datan alkuperä ja eheys on varmistettava läpi koko elinkaaren. Perinteinen ajatus luotetusta sisäverkosta ei enää toimi, vaan puolustuksen tulee olla kattava “sipulipuolustus” tai nykytermein “zero trust”. Mitään käyttäjää, sovellusta tai laitetta ei tule pitää automaattisesti luotettavana.

Tekoäly tarjoaa erinomaisia organisaation ja yksilön tuottavuutta parantavia palveluita, alkaen vaikka kielenkäännöksistä tai artikkelien tiivistelmistä. Ellei organisaation tekoälyn käyttö ole hallittua, voi julkisiin palveluihin päätyä luottamuksellista tietoa. Tämä “varjotekoäly” on analoginen varjo-IT:lle, jossa käyttäjät käyttävät luvattomia palveluita, laitteita tai ohjelmistoja helpottaakseen tai tehostaakseen omaa työtään.

AI Runtime Security: Suojaus käytön aikana

Koska esivalmisteluvaiheen turvatarkastukset eivät riitä kattamaan kaikkia tekoälypohjaisia uhkia, katse on käännettävä suojaukseen, joka tapahtuu tekoälyn suorituksen aikana (Runtime Security). Pelkkä lopputuloksen monitorointi ei enää riitä, vaan järjestelmien on kyettävä valvomaan tekoälyagenttien toimintaa ja päättelyketjuja reaaliajassa.

Moderni tekoälyn aikainen suojaus tarkoittaa kykyä nähdä agentin tekemät työkalukutsut, sen käsittelemä data ja polut, joita se on kulkenut tehtävää suorittaessaan. Tähän kuuluu olennaisena osana reaaliaikaiset (guardrail) suojaukset, jotka tunnistavat prompt -injektiot, tiedon luvattoman ulosvirtauksen ja luvattomat toimintopyynnöt ennen kuin ne ehtivät aiheuttaa vahinkoa. Jokainen tekoälyagentti on kohdattava kuin se olisi itsenäinen työntekijä omine oikeuksineen, ja automaattinen zero trust -perusteinen oikeuksien hallinta on välttämätöntä kompromissien rajaamiseksi konevauhdilla.

Infrastruktuuri ja mallien tarkastus

Puolustuksen on oltava yhtä nopeaa kuin hyökkäyksen, mikä edellyttää modernia datainfrastruktuuria, joka tukee skaalautuvaa analytiikkaa ja turvallista tiedonvaihtoa. Mallien tarkastus on voitava tehdä niiden alkuperäisessä, suojatussa ympäristössä ilman datan siirtelyä (in-place scanning), jotta operatiivinen turvallisuus ja immateriaalioikeudet säilyvät. Järjestelmien on tarjottava syvällinen näkyvyys mallin sisälle – sen arkkitehtuuriin, painotuksiin ja upotettuun koodiin – jotta piilotetut riskit ja haitalliset hyötykuormat voidaan tunnistaa.

Tietojohtamisen kulttuurinen muutos

Tekoälystrategia painottaa, ettei tiedolla johtaminen ole vain tekninen ratkaisu, vaan koko organisaation läpileikkaava ajattelumalli, jossa tieto on yhteinen voimavara. Viestimiehelle tämä tarkoittaa siirtymää datakeskeisyydestä informaatiokeskeisyyteen, sillä voitto saavutetaan ymmärtämällä, mikä datasta on relevanttia ja muuttamalla se päätöksenteon tueksi. Tekoäly voi hallusinoida tai tulla harhaan johdetuksi, jos se irrotetaan opintojen ja doktriinien kontekstista, joten ihmisen rooli ankkurina ja päätöksentekijänä säilyy kriittisenä.

Yhteenveto: Tekoälyä on hyödynnettävä, mutta suojatusti

Tekoäly on tullut jäädäkseen ja se on herkkä järjestelmä, joka vaatii jatkuvaa huoltoa ja monitorointia aivan kuten perinteiset radiolaitteetkin. Hyökkääjällä on epäsymmetrinen etu, sillä heidän tarvitsee onnistua vain kerran, mutta puolustajan on onnistuttava joka kerta, ja nyt jopa muutaman minuutin aikaikkunassa. Meidän on vastattava hyökkääjän nopeuteen tekoälypohjaisella suojauksella, joka ymmärtää mallien kieltä ja agenttien logiikkaa. Puolustusvoimien strategian mukaisesti perustettava data- ja tekoälykeskus tulee olemaan tässä työssä keskeisessä roolissa. Käyttöönotto on tehtävä rohkeasti, mutta aina suojatusti.

Teksti: Juha-Matti Laurio, kouluttaja, MPK Lounais-Suomen piiri

Digitaalinen taistelukenttäforensiikka

Venäjän Ukrainaan kohdistaman hyökkäyssodan aikana taistelukentälle ja siviilikohteisiin jää jatkuvasti valtava määrä asejärjestelmiä. Niistä voidaan kerätä välitöntä tiedustelutietoa sekä tietoja esimerkiksi laitteiden komponenttien alkuperämaasta. Havainnollistamisen vuoksi artikkeli sisältää runsaasti valokuvia.

Digitaalinen taistelukenttäforensiikka, englanniksi Battlefield Digital Forensics, kattaa toiminnan, jossa tunnistetaan, kerätään, otetaan haltuun, turvataan ja analysoidaan taistelukentälle jääneitä vihollisen laitteita. Teknisten ja taktisten käyttötarkoituksien lisäksi laitteista voi löytyä myös valokuvia ja aikaleimatietoja, jotka voivat toimia oikeuskelpoisina todisteina sotarikosten tutkinnassa. Artikkeli painottuu tämän harvinaisen, mutta ei uuden, toimialan johtamisjärjestelmäulottuvuuksiin sekä kuvaa toimialan luonnetta ja kehitysmahdollisuuksia. Selkeyden vuoksi toiminnan kohteista käytetään artikkelissa käsitettä ”laite”.

Laitteiden valtava kirjo

Ukrainaan liittyen kattavan kokonaiskuvan laitekirjosta saa Kyiv Independent -julkaisun koosteista, jotka tilastoivat hyökkäävän osapuolen kalustotappioita 13 eri kategoriassa. Somealustat X ja Telegram ovat puolestaan vahvoja lähteitä usein sijaintitiedollisenkin kuvamateriaalin hankkimisessa, vaikka viestilaitteiden kuvia onkin suhteellisen haastavaa löytää.

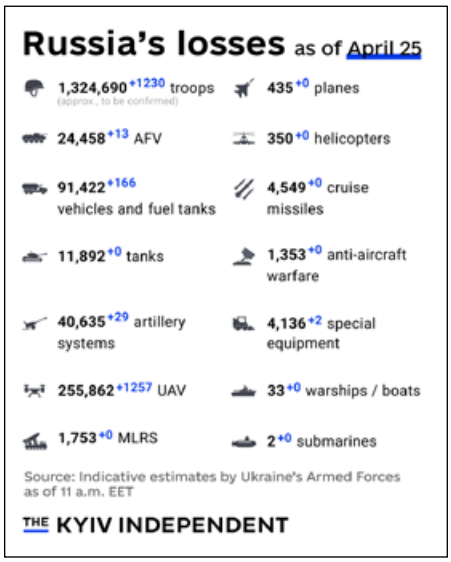
Taistelukentällä on valtavasti digitaalisia laitteita, jotka sisältävät dataa taistelutilanteesta: taajuuksia, komentorakenteita, kerättyä tilannekuvaa ja drone-videoita vihollisen asemista. Aselajin näkökulmasta laitteiden kirjo onkin valtava. Ohjuksissa ja droneissa on runsaasti elektroniikkaa, joista voidaan päästä valmistusmaan ja komponenttien alkuperän jäljille. Myös maalidataa tallentuu digitaalisesti. Esimerkiksi Gazassa Hamasin tunneliverkostosta löytyi kokonaisia konesaliratkaisuja.

Valokuvia ja videoita tuhotuista asejärjestelmistä on kerätty muun muassa Oryx -hankkeen sivuston blogiosioon https://www.oryxspioenkop.com. Operaatioturvallisuussyistä asetyypeittäin, tarkkoine malleineen ja valmistusmaineen jaoteltu luettelo ja tämä artikkeli eivät sisällä aivan tuoreinta aineistoa. Informatiivisimmillaan videot näyttävät dronella tuhotusta ELSO-vaunusta myös ehjän vaunun kuvan tunnistamisen helpottamiseksi.

Välittömiä tiedustelutietoja

Erikoisjoukot, ja tilanteesta riippuen jotkin viranomaiset vastaavat seuraavista digitaalisen taistelukenttäforensiikan taktisen vaiheen tehtävistä: 1) etsiminen, 2) tunnistaminen, 3) laitteiden valinta ja 4) haltuun ottaminen.

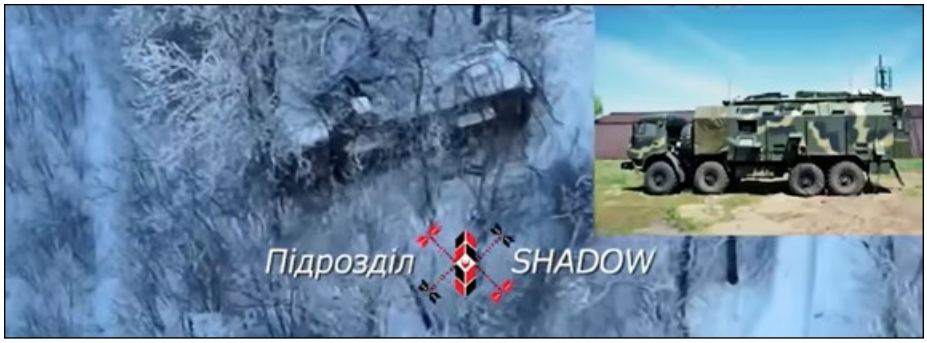
Ensiarvoisen tärkeää on turvata laitteen sisältämän datan eheys ja esimerkiksi radiot sijoitetaan sähkömagneettisesti eristävän materiaalin sisään, kuten Faradayn häkkiin. Tuli-iskusta selvinneen tuliasemapäätteen muistissa voi olla selväkielistä dataa, joka on saatava kopioitua forensiikkatyökaluilla talteen ennen laitteen virran katkaisua. Kiire onkin toiminnassa jatkuvasti läsnä. Vaihetta kokonaisuutena kutsutaan Tactical Site Exploitation -vaiheeksi.



Kuva 1: Seuranta Venäjän kalustotappioista, kuva:The Kyiv Independent.

Nopea tunnistaminen keskiössä

Kentällä valokuvatulla ja dokumentoidulla aineistolla sekä someen kertyvällä kuva-aineistolla tuhoutuneista asejärjestelmistä ja välillä vahingoittumattomistakin laitteista on suora yhteys laitteen hyödyllisyyden arviointiin. Taktisen vaiheen kiireestä, vaarallisuudesta ja eräänlaisesta kokonaisvaltaisesta kaoottisuudesta huolimatta laitteet on saatava taistelevien joukkojen keskeltä turvaan kauemmas ja erikoisvälineiden avulla analysoitavaksi.



Kuva 2: ELSO-järjestelmä RB-109A ”Bylina” maalina, kuva: Shadow of Ukraine/YouTube.

Laite suurennuslasin alle

Tekniseksi vaiheeksi kutsutaan vaihetta, jossa haltuun otettu laite analysoidaan turvallisemmassa ympäristössä. Dokumentoidun laitteen analysointi voi alkaa täysipainoisesti ja forensiikkaohjelmisto osaa näyttää esimerkiksi laitteelta poistetut valokuvat. Aselajiosaamista omaava henkilöstö on osannut jo taktisessa vaiheessa tunnistaa laitteen käyttötarkoituksen ja arvioida tulevan käyttöarvon. Teknisen vaiheen aikana laitteen viestit ja lokitiedot analysoidaan ja niistä voidaan tunnistaa yhteyksiä vaikkapa tiedustelun jo aikaisemmin selvittämiin johtajiin. Syntyvä tilannekuvatieto on arvokasta, mutta nopeaa hyödyntämistä vaativaa.

Vastatoimista

Sotatoimien osapuolilla on luonnollisesti tarve hankaloittaa, viivästyttää ja myös kokonaan estää forensiikkatoimia. Vastatoimet voivat kohdistua niin itse laitteisiin kuin niitä tunnistaviin ja kerääviin. Menetelmiä ovat esimerkiksi miinoitus, sähköansoitus, tappokytkin tai älypuhelimista tuttu verkon yli tapahtuva wipetykseksi kutsuttu tyhjennys. Toimenpiteillä sotatoimien osapuolet pyrkivät rajoittamaan laitteista löydettävän datan määrää tai jopa ilmoittamaan laitteen joutuneen ulkopuolisen, tyypillisesti vihollisen haltuun.

Aselajin vastatoimista

Viestimiehellä on monia vastatoimia käytössään: laitteen ottaminen joukon mukaan irtautuessa, ohjelmoitujen taajuuksien tyhjentäminen, laitteen muistin tyhjentäminen tai verkkolaitteen palauttaminen tehdasasetuksiin. Jokaisen laitetta käyttävän taistelijan on tunnettava vastatoimet ja osattava käyttää niitä viiveettä. Laite dokumentaatioineen ja johtamisjärjestelmäkäsky voidaan taistelutilanteen salliessa myös tuhota. Arjen välineiden osalta vastatoimet ovat käyttäjän itsensä vastuulla.

Kansalliset mahdollisuutemme

Digitaalisen taistelukenttäforensiikan osaamisen laajentamiseksi Suomessa tulisi hyödyntää yhteistyötä forensiikkaa

Kuva 3: Myös siviilikäyttöön tarkoitetut laitteet on tunnistettava, kuva: Defense Blog.

tekevien kyberturvallisuusyritysten, väärinkäytöstutkintaa tekevien yritysten sekä poliisin forensiikkayksiköiden kanssa. Digitaalista forensiikkaa päivätyökseen tekevissä on niin aktiivireserviläisiä kuin MPK:n sitoumuksen tehneitä reserviläisiä. Eri aselajiin kuuluvalla reserviläisellä taas voi olla forensiikkaosaamista, mutta esimerkiksi sijoitus on päivittämättä.

Kyberosaamisemme on tunnetusti korkeatasoista ja forensiikkahenkilöstöllä on jo työnantajan lukuun hankittua alan koulutusta. Konkreettisia forensiikkaharjoituksia testiympäristöineen voitaisiin toteuttaa MPK:n jatkokurssien alaisuudessa, tarvittaessa Naton kyberpuolustuksen osaamiskeskus CCDCOE:n tukemana. Kalustotunnistus, dokumentointi ja ansoituksen tunnistaminen vaatii kuvastojen lisäksi harjoitusmateriaalia. Toimiala tarvitseekin riittävät resurssit jo digitaalisen maailman nopeasti muuttuvan luonteen takia.

Lähteitä

C. Braccini, T. Väisänen ym., ”Battlefield Digital Forensics. Digital Intelligence and Evidence Collection in special operations”, CCDCOE, 2016.

Telegram-, X- ja YouTube-lähteet

Kirjoittajan opetusmateriaali

Keskeisiä lyhenteitä

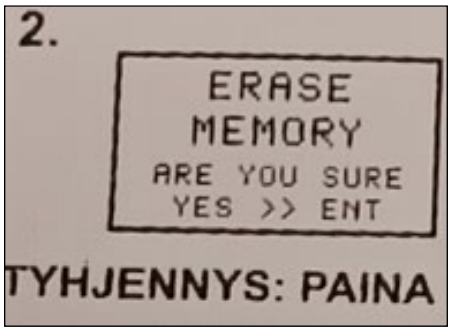
BFA – Battlefield Forensics and Acquisition; taistelukenttäforensiikka ja kerääämistoimet.

DF – Digital Forensics; digitaalinen forensiikka.

TSE – Tactical Site Exploitation; etsintä->tunnistus->keräys->haltuunotto->turvaaminen.

Artikkelin kirjoittaja

Juha-Matti on Luonetjärven varuskunnassa palvellut yliluutnantti evp, tietokirjailija ja MPK:n Lounais-Suomen piirin kyberkouluttaja. Kirjoittaja on pitänyt aiheesta tietoiskuja Maanpuolustuskoulutus MPK:n kyberturvallisuus- ja johtamisjärjestelmäkursseilla keväästä 2025 lähtien. Tietoiskuun kuuluu havainnollistava kokoelma erilaisia vaurioitettuja siviilielämän elektronisia laitteita.



Kuva 4: Erään kenttäradion tyhjennystoiminto.

Teksti: Kimmo Kaipainen

Kuvat: Kimmo Kaipainen, Juha Peltomäki

Viestiaselajin vuosipäivää vietettiin Turussa

Merivoimat isännöi aselajimme vuosipäivän viettoa 5.3.2026 aurinkoisessa Turussa Forum Marinumin hienoissa puitteissa. Viestiaselajin vuosipäivän vietto oli nyt ensimmäistä kertaa merivoimien isännöimä. Merivoimien puolesta isännöinnistä vastasi merivoimien johtamisjärjestelmäpäällikkö kommodori Kristian Isberg.

Juhlapäivän aluksi vieraat pääsivät tutustumaan tyylikkäästi laadittuun Forum Marinumin näyttelyyn, joka sisälsi myös laajan merivoimia koskevan osuuden. Museovierailun jälkeen ohjelmassa oli yhteinen lounas, joka nautittiin museon vieressä ravintola Göranissa.

Juhlan luonteeseen osuvasti paikalla kuultiin useita juhlapuheita ja tervehdyksiä. Toimialan tervehdyksen tilaisuuteen toi Pääesikunnan johtamisjärjestelmäpäällikkö kenraalimajuri Jarmo Vähätiitto, joka kuvasi juhlapuheessaan suomalaisen sotilaan ominaisuuksia. Perinteisen suomalaisen sisun lisäksi varusmiehille syntyy Vähätiiton mukaan varusmiespalvelusaikanaan myös teknisiä ja kybervalmiuksia. Viestiupseeriyhdistyksen puolesta puhetta käytti yhdistyksen puheenjohtaja ev (evp) Pertti Hyvärinen, joka palkitsi tervehdyksensä ohessa Viestimieslehden vuoden 2025 kirjoittajaksi valitun evl, sotatieteiden tohtori Maria Keinosen.

Viestikiltojen liiton tervehdyksen tilaisuuteen toi puolestaan Viestikiltojen liiton koulutuspäällikkö ev Juha Peltomäki. Peltomäki julkisti tilaisuudessa samalla Vuoden Viestikilta -valinnan. Tiukalla piste-erolla vuoden viestikiltana palkittiin Pirkanmaan viestikilta. Maavoimien Viestitarkastajan puolesta tervehdyksen esitti Maavoimien esikunnan johtamisjärjestelmäosaston apulaisosastopäällikkö evl Tuomas Arajuuri, joka korosti puheessaan aselajiamme palveluiden tuottajana, sillä vain viesti perille menneenä ratkaisee.

Aselajivuosipäivän juhlallisuuksien musiikillisesta annista vastasi Turkuun sopivasti merivoimien soittokunnan saksofonitrio. Tilaisuuden päätteeksi juhlavierailla oli vielä mahdollisuus jatkaa Forum Marinumin näyttelyihin tutustumista. Merivoimien järjestämä vuosipäivä oli järjestelyiltään erittäin onnistunut ja Turku näytti aurinkoisena päivänä parhaita puoliaan.

Kuva 1: Juhlan virallinen osuus aloitettiin kommodori Kristian Isbergin avaussanoilla, joissa käsiteltiin kiinnostavasti merivoimien nykyisyyttä.

Kuva 2: Komentaja Ville Vänskän piti juhlaesitelmän 1925 uponneesta itsenäisen Suomen merivoimien torpedovene S2:sta. Koskettava ja erinomaisen kiinnostava esitelmä puhututti juhlayleisöä vielä tilaisuuden jälkeenkin.

Kuva 3: Viestimies-lehden vuoden 2025 kirjoittajana palkittiin evl, sotatieteiden tohtori Maria Keinonen.

Kuva 4: Edellisten johtamisjärjestelmäpäälliköiden ja samalla reserviläisten tervehdyksen tilaisuuteen toi kenraaliluutnantti Mikko Heiskanen (kuvassa alimman rivin keskellä).

5.3.2026 myönnetyt viestiristit ja soljet viestiristeihin

Viestiristi soljella

Isberg	Kristian	Kommodori	Turku
Moilanen	Mikko	Insinöörimajuri	Jyväskylä

Solki viestiristiin

Antikainen	Arto	Vanhempi asentaja	Kuopio
Bark	Jarmo Tapani	Insinöörikapteeni	Lohja
Hannula	Mika	Everstiluutnantti	Tampere
Hautala	Matti	Kapteeni	Rovaniemi
Heikkilä	Ville	Ylivääpeli	Kajaani
Hietanen	Sakari	Majuri	Sodankylä
Hirvonen	Tatu	Insinöörikapteeni	Kouvola
Holmlund	Tomas	Majuri	Turku
Huhtamella	Jukka	Kapteeni	Inari
Huotari	Jarno	Insinöörimajuri	Tuusula
Hämäläinen	Kari	Kapteeni	Jyväskylä
Ikonen	Ismo	Everstiluutnantti	Vantaa
Jaakola	Timo	Majuri	Helsinki
Kaivonurmi	Paavo	Everstiluutnantti	Kouvola
Kohonen	Juha	Everstiluutnantti	Lahti
Lehtonen	Tomi	ICT-erityisasiantuntija	Tampere
Mikkonen	Tuomas	Teknikkokapteeni	Kajaani
Mäkinen	Jarkko	Kapteeni	Tampere
Nevala	Jussi	Kapteeni	Jyväskylä
Nieminen	Vesa-Matti	Majuri	Hämeenlinna
Nikkola	Olli	ICT-järjestelmäpäällikkö	Hämeenlinna
Nenonen	Päivi	ICT-erityisasiantuntija	Mikkeli
Palin	Henri	Insinöörikapteeni	Eura
Pereläinen	Eino	Komentajakapteeni	Helsinki
Pulkkinen	Janne	Insinöörieverstiluutnantti	Tampere
Ranta	Esa	Yliluutnantti	Inari
Rintala	Markku	Liikenneopettaja	Lapua
Saarinen	Teemu	ICT-tukihenkilö	Säkylä
Valkeajärvi	Jarmo	Komentajakapteeni	Raisio
Valta	Janne	Ylivääpeli	Kuopio
Vepsäläinen	Mikko	Majuri	Mikkeli
Virtanen	Tarja	ICT-erityisasiantuntija	Tampere
Virtanen	Vesa	Erikoissuunnittelija	Jyväskylä
Vähäkoski	Juha	ICT-järjestelmäpäällikkö	Ylöjärvi
Ylönen	Sami-Petteri	Ylivääpeli	Riihimäki

Viestiristi

Ahola	Juha	Vanhempi tietoturvakonsultti	Vantaa
Ahonen	Panu	Vääpeli	Perniö
Arkko	Kari	Tietoturvallisuuspäällikkö	Kintaus
Aspela	Teemu	Vääpeli	Hyvinkää
Ekström	William	Ylikersantti	Inkoo
Fagerstedt	Oliver	Ylikersantti	Raasepori
Finnberg	Jari-Matti	Kyberturvallisuusasiantuntija	Hämeenlinna
Haanpää	Tomi	Filosofian tohtori	Lapua
Hellman	Esa-Jaakko	Kapteeni	Rovaniemi
Herrala	Soili	ICT-erityisasiantuntija	Riihimäki
Hirvonen	Erno	Tietoturva-asiantuntija	Jyväskylä
Hållfast	Mika	Kehitysjohtaja	Helsinki
Hännikäinen	Mikko	ICT-asiantuntija	Vantaa
Höyhtyä	Marko	Tutkimusprofessori	Ii
Idström	Antti	Kapteeni	Loviisa
Isokangas	Pia	Tiiminjohtaja	Tampere
Johannson	Marcus	Insinööriluutnantti	Karjaa
Jokiniemi	Jouni	Vääpeli	Riihimäki
Jokiranta	Pekka	ICT-tukihenkilö	Kouvola
Juntunen	Sari	Suunnittelija	Nurmijärvi
Juuti	Otto	Vääpeli	Kouvola
Kallionpää	Johannes	Kapteeni	tuntematon
Kalliomäki	Mikael	Majuri	Kouvola
Kinnunen	Hannu	Vääpeli	Salo
Kokkonen-Kangas	Linda	Yliluutnantti	Vantaa
Kuri	Jukka	Insinööriyliluutnantti	Hyvinkää
Kåll	Oskar	Ylikersantti	Salo
Laakko	Jari	Ylivääpeli	Rovaniemi
Lakonen	Mikko	Suunnittelija	Jyväskylä
Liimatainen	Rauni	Asiakaspalvelun asiantuntija	Jyväskylä
Luopa	Anne-Maija	Suunnittelija	Tuusula
Luukka	Kirsi	Financial Controller	Järvenpää
Lähteenkorva	Mikko	Kapteeni	Kouvola
Mikkonen	Tuomas	Teknikkokapteeni	Kajaani
Mäkinen	Janne	Kapteeni	Kouvola
Nirkko	Mika	Insinööri	Mikkeli
Palola	Jussi	ICT-asiantuntija	Tampere
Puumalainen	Heidi	Tradenomi	Tuusula
Puumalainen	Toni	ICT-erityisasiantuntija	Mikkeli
Raitanen	Hanna	Kyberturvakoulutustiimin johtaja	Vihti
Riihimäki	Reetta	Tiedonhallintapäällikkö	Tampere
Riikonen	Leo	Vanhempi rajavartija	
Rintala	Tarja	Diplomi-insinööri	Tampere

Ruotsalainen	Jan	Vääpeli	Rovaniemi
Ruotsi	Sami	Pursimies	Espoo
Ruuska	Matti	Vääpeli	Lahti
Ruuskanen	Jussi	Kapteeniluutnantti	Espoo
Rytilahti	Kalle	Vääpeli	Rovaniemi
Santakivi	Riku	Lead Development Manager	Hämeenlinna
Siljander	Anssi-Pekka	Quality Manager	Padasjoki
Strandman	Jaana	Kansanedustaja	Mikkeli
Sutela	Esko	Vääpeli	Lahti
Taipola	Toni	Vääpeli	Sodankylä
Taka-aho	Anna-Maaria	Sotilasmestari	Rovaniemi
Takala	Tuomas	Opettaja	Seinäjoki
Tankkala	Sami	Insinööri	Orivesi
Turkia	Tero	Vanhempi rajavartija	Kuusamo
Valtola	Oskari	Kansanedustaja	Mikkeli
Viljanen	Vesa	Testipäällikkö	Orimattila
Vuojalahti	Kalle	Kapteeniluutnantti	Helsinki
Wikholm	Rabbe	Merivartiomestari	Raasepori

Viestiupseeriyhdistyksen kevätkokous Suomen Erillisverkot Oy:n tiloissa Espoossa.

Viestiupseeriyhdistys ry vietti kevätkokoustaan 23.4.2026 Espoossa ERVE:n isännöimänä 25 osallistujan voimin. ERVE:n edustajat, Jarmo Vinkvist, Harri Hilden ja Ilkka Palttala järjestivät erinomaiset puitteet yhdistyksen kevätkokoukselle, kiitos siitä heille.

Kevätkokouksessa vahvistetiin hallituksen valmistelemat toimintasuunnitelma ja tilinpäätös sekä myönnettiin tili- ja vastuuvapaus tilivelvollisille.

Ansioituneita palkittiin.

Viestiupseeriyhdistys ry:n puheenjohtaja eversti Pertti Hyvärinen luovutti kokouksen aluksi Maanpuolustuksen Viestisäätiön hopeisen ansiolevykkeen Jyri Putkoselle ansiokkaasta toiminnasta maanpuolustuksen hyväksi. Puheenjohtaja onnitteli myös juuri merkkipäiviään viettäneitä Pirkko Kinnusta ja Juhani Tapiolaa 80-v syntymäpäivien johdosta.

Suomen Erillisverkkojen katsaus: ERVE tänään ja VIRVE 2-verkko.

Kokouksen päätteeksi ERVE:n edustajat esittelivät toimintaansa sisältäen yleisesittelyn yrityksestä ja VIRVE 2-verkon tilanteen. Tekninen johtaja Harri Hilden päivitti tietomme ERVE:n nykytilasta ja sen haasteista. ERVE on 100%:sti valtion omistama osakeyhtiö ja sen keskeisimmät toiminnot ovat VIRVE-veverkon palvelut, Krivat-palvelut, verkko-operaattoripalvelut, turvapilvi- ja konesalipalvelut, Leijonaverkkojen tarjoamat suojatila- ja konesalipalvelut sekä johtotietopalvelut.

Ilkka Palttala esitteli VIRVE 2 verkon tilanteen kertoen sen aikatulusta ja merkittävistä eroista nykyiseen VIRVE-verkkoon. VIRVE 2 verkon liittymiä on tällä hetkellä vähän yli 10 000 ja nykyisessä VIRVE-verkossa liittymiä noin 50 000. VIRVE-verkon pääkäyttäjinä ovat poliisi, pelastustoimi, sosiaali- ja terveydenhuolto, Puolustusvoimat, Rajavartiolaitos, Tulli ja Hätäkeskuslaitos.

Kuva 1: Kokousväki ERVE:n tiloissa. (kuva: Harri Reini)

Kuva 2: Jyri Putkonen vastaanotti hopeisen ansiolevykkeen VUY:n puheenjohtajalta. (kuva: Harri Reini)

Kuva 3: Puheenjohtaja Pertti Hyvärinen luovutti standaarin ERVE:n edustajalle, Harri Hildenille. (kuva: Harri Reini)

Lopuksi

Tilaisuuden päätteeksi yhdistyksen puheenjohtaja luovutti Viestiupseeriyhdistyksen standaarin kokouksen isännille ja kiitti hienoista järjestelyistä.

Kutsu Viestiupseeriyhdistyksen syyskokoukseen

Viestiupseeriyhdistyksen hallitus kutsuu yhdistyksen jäsenet **syyskokoukseen ja seminaaripäivään Riihimäelle perjantaina 25.9.2026 kello 08.30 alkaen.** Varsinainen syykokous pidetään Riihimäen Varuskunnassa klo 14.30–15.30 rak162:n (entinen SÄHKÖTK) elokuvasalissa. Kokoukseen on mahdollista liittyä myös etänä linkin kautta, joka lähetetään ilmoittautuneille.

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

1) Kokouksen puheenjohtajan valinta

2) Kokouksen sihteerin valinta

3) Kahden pöytäkirjan tarkastajan ja äänten laskijan valinta

4) Kokouksen laillisuuden ja päätösvaltaisuuden toteaminen

5) Kokouksen työjärjestyksen hyväksyminen

6) Toiminta- ja taloussuunnitelman hyväksyminen vuodelle 2026

7) Jäsenmaksujen suuruuden päättäminen vuodelle 2026

8) Hallituksen puheenjohtajan valinta vuodelle 2026

9) Hallituksen jäsenten lukumäärän päättäminen ja hallituksen jäsenten valinta vuodelle 2026

10) Toiminnantarkastajan ja varahenkilön valinta

11) Muut asiat: kunniajäsenen kutsuminen, sääntömuutos

Päivän ohjelma 25.9.2026

klo 8.30–9.00	**Aamukahvi**
klo 09.00–11.00 ja 12.00–14.00	**AR Saarmaa-seminaari**
klo 11.00–12.00	**Lounas, Varuskuntaravintola Liesi**
klo 14.30–15.00	**Palkitsemiset**
klo 15.00–16.00	**Viestiupseeriyhdistyksen syyskokous**
klo 16.30–18.30	**Päivällinen, Riihimäen Upseerikerho**

Kuljetus Helsingistä lähtee Kiasman edestä turistipysäkiltä (Mannerheimin aukio) kello 07.30 ja palaa päivällisen jälkeen samaan paikkaan.

Ilmoittautumiset päivän tilaisuuksiin **17.9.2026 mennessä** www.viestiupseeriyhdistys.fi (toivottavin tapa), sähköpostitse toiminnanjohtaja@viestiupseeriyhdistys.fi tai puhelimitse 040 514 2497.

Voit ilmoittautua samalla VUY:n syyskokoukseen, kuljetukseen, seminaariin ja päivälliselle.

Tervetuloa!

Viestiupseeriyhdistys ry:n hallitus

Saarmaa-seminaari 2026

pe 25.9.2026 klo 09.00 – 14.00

” Vähän – riittävästi – paljon – liikaa?”

Toimintaympäristö myllerryksessä – kuinka johtamisjärjestelmät ja kyberpuolustus pysyvät mukana? Tule kuuntelemaan missä mennään! Tavoitteena on syventää osallistujien tietoisuutta

- paikallispuolustuksen johtamisesta ja johtamisen tukemisesta,
- kyberharjoituksen toimeenpanosta,
- PV:n HF-koulutuksesta,
- kyläradioverkoista sekä
- kansainvälisestä yhteistyöstä.

Ilmoittautumiset seminaariin to 17.9.2026 klo 16.00 mennessä osoitteessa:

https://ctfinland.com/vkl/

Seminaarin keskuspaikkana on Riihimäen varuskunta. Seminaariin voi osallistua etäyhteydellä (PV:n toimipiste) seuraavilta paikkakunnilta: Hamina, Helsinki, Joensuu, Jyväskylä, Kajaani, Kouvola, Kuopio, Lahti, Lappeenranta, Mikkeli, Niinisalo, Oulu, Rovaniemi, Sodankylä, Tampere, Turku, Vaasa.

Seminaaria koskeviin kysymyksiin vastaa:

- Juha Peltomäki, puh. 0299 510602, juha.peltomaki@mil.fi
- Facebook: Viestikiltojen liitto ry

Tervetuloa valtakunnallisille Viestimiespäiville Haminaan!

Linjat auki, taajuudet kohdilleen ja reput valmiiksi – **Viestimiespäivät 2026** kutsuvat Reserviupseerikouluun Haminaan **22.–23.8.2026**!

Vuosittainen merkkitapahtuma tarjoaa tuttuun tapaan:

ajankohtaista asiaa (mutta ei kuivaa)

yhteistä touhua (mutta ei pakkopullaa)

paikallisia makupaloja (sekä ohjelmassa että lautasilla).

Kaukaa tullaan – ja hyvissä ajoin!

Pitkämatkalaisille tarjotaan etumatkaa: **perjantaina 21.8. klo 19.00–21.00** voi saapua ja majoittua **Esikunta- ja viestikomppanian** tiloissa ja nauttia aamupalan varuskuntaruokala Rokassa. Näin lauantai starttaa ilman turhaa kiirettä ja navigointisäätöä.

Lauantai 22.8. – asiaa, älyä ja vähän äksöniä

Varsinaiset Viestimiespäivät käynnistyvät:

Ilmoittautuminen klo 10.00–11.00 (Esikunta- ja viestikomppania)

Avajaiset klo 11.00 – nyt ollaan tosissaan, mutta hyvällä mielellä!

Päivän aikana luvassa:

Maasotakoulun ajankohtaiset ja katsaus viestiaselajin upseerioppilaiden koulutukseen

Johtamisjärjestelmäpäällikön ajankohtaiskatsaus – missä mennään ja miksi

Tutustuminen koulutuskalustoon – ei pelkkää ”kelmusulkeista”.

Lounaan jälkeen mitataan älyä, taitoa ja nokkeluutta, kun **Herrashenkilökilpailu** laittaa partiot liikkeelle visaisille tehtävärasteille.

Päivän päätteeksi:

Saunat lämpimäksi ja

Viestimiesillallinen, jossa jaetaan palkinnot ja päivän tarinat viimeistellään klassikkoasemaan.

Sunnuntai 23.8. – historiaa, perinteitä ja päätös yhteisellä pöydällä

Sunnuntai käynnistyy aamupalalla ja huoneiden luovutuksella, jonka jälkeen:

- Kannatusyhdistyksen esittäytyminen
- Opastetut kierrokset:
  - RUK-museossa sekä
  - rauhanturvaamisen ja kriisinhallinnan museo Wanhassa Veteraanissa.

Viestimiespäivät päättyvät **yhteiseen lounaaseen** klo 13.00 mennessä – maatielle ei lähdetä nälkäisinä tai ilman viimeisiä kuulumisia.

Ilmoittaudu mukaan!

Katso tarkemmat yksityiskohdat ja varmista paikkasi viimeistään **3.8.2026 klo 16.00 mennessä**:

VKL - Centerfield Team Finland
(https://ctfinland.com/vkl/)

Osallistumismaksut:

- PE–SU / 90 euroa, LA–SU / 85 euroa, 1 Päivä / 65 euroa

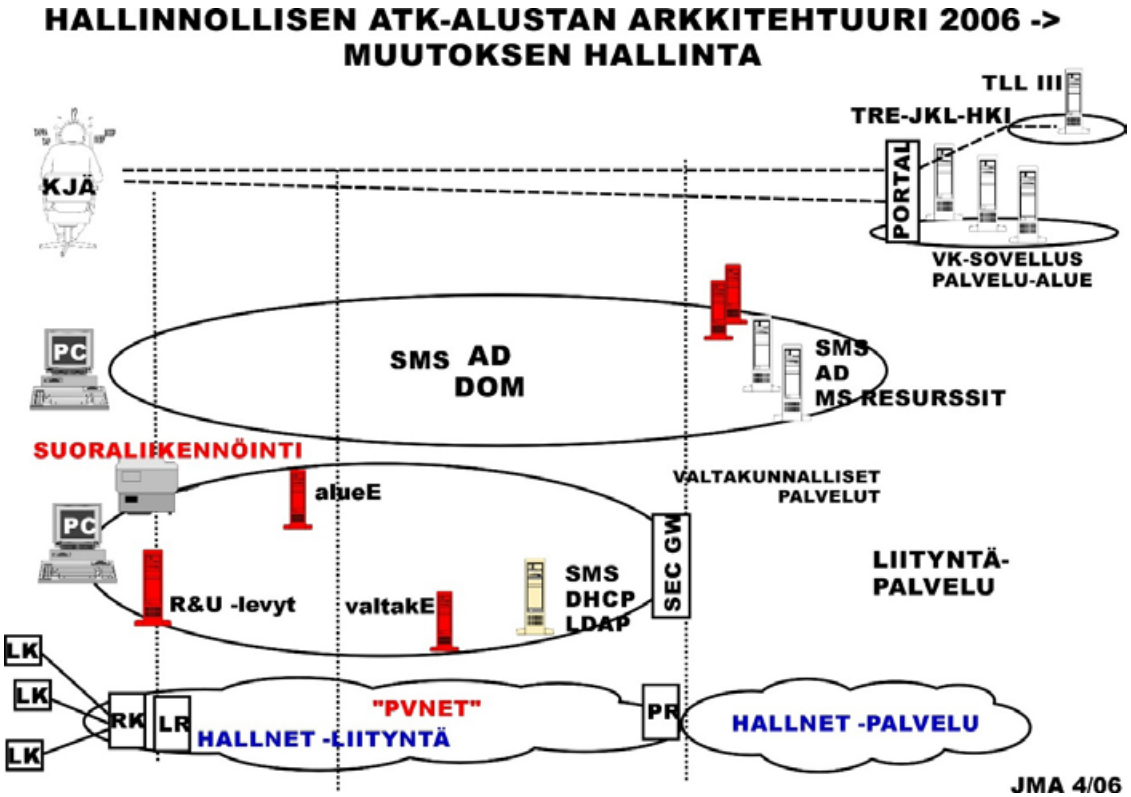
Lopuksi!

Toivotamme **kaikki vapaaehtoisen maanpuolustuksen ystävät** runsaslukuisesti tervetulleiksi perinteiseen, mutta elinvoimaiseen **viesti-, johtamisjärjestelmä-, ICT- ja kyberalan kesätapahtumaan "maailmanluokan pikkukaupunki"** Haminaan.

Viestikiltojen liitto ry
Kymen Viestikilta ry

Teksti: Juha Mattila

Tuokiokuvia Johtamisjärjestelmäalan eilisestä



Puolustusvoimien hallinnollisen tietojenkäsittely-ympäristön (HALNET 2006) muutos

Puolustusvoimien tietohallinnon rakenteet muutettiin Tietohallinnon Rationalisointi (TIERA)-hankkeessa 2004–2008 tukemaan Puolustusvoimien siihen mennessä suurinta rakennemuutosta 2008. Rakennemuutos mahdollistettiin Puolustusvoimien sisäisillä pilvi-palveluilla, kuten asianhallinnalla ja toiminnanohjauksella. Hallinnollinen tietojenkäsittelyn ympäristö (HALNET) järjestettiin uudelleen osana TIERA-muutosta. Yli sataan varuskuntaan hajautetut palvelimet, sovellukset ja tukipalvelut keskitettiin kolmeen Puolustusvoimien virtualisoituun datakeskukseen, nostettiin liityntäverkon kapasiteettia, rationalisoitiin sovelluksia ja yhtenäistettiin työasemakantaa. Lisäksi muutettiin paikallinen tulostaminen valtakunnalliseksi palveluksi, päivitettiin toimistosovellukset ja vahvistettiin tietoturvaa Viranomaiskäyttö-tasoon sekä avattiin tiedonvaihto ylempiin tietoturvaluokkiin yhdysväylän kautta.

Puolustusvoimien Johtamisjärjestelmäkeskus perustettiin 2007 kehittämään ja tuottamaan HALNET:n palveluita tavalla, jota nykyisin kutsutaan Software as a Service (SaaS). Muutoksen jälkeen käyttäjät liikkuivat saumattomasti työasemasta toiseen toimikortilla identifioituen (nykyisin Multi-Factor Authentication). Hallinnolliset sovellukset tarjottiin portaalin läpi virtuaalisesti jostakin kolmesta datakeskuksesta (nykyisin On-Premises Cloud Infrastructure). Uusina sovelluksina tarjottiin SameTime-kollaboraatiopalveluita, jotka mahdollistivat etätyön Puolustusvoimien toimipisteiden välillä. SAP-toiminnanohjauspalvelu laajennettiin kattamaan hallintoon ja joukkotuotantoon liittyvät tehtävät. HALNET-ympäristön digitaaliset palvelut mahdollistivat hallinnollisten tietojenkäsittelypalveluiden keskittämisen ja tukivat Puolustusvoimien rationalisointia 2008 ja 2015 rakennemuutoksissa.

Kuvassa näkyy HALNET-infrastruktuurin teknisen arkkitehtuurin muutos neljässä tasossa. Alimmalla tasolla PVNET-verkko jaettiin liityntä- ja palveluverkoksi. Liityntäverkossa aiemmat lähiverkkorakenteet (LAN) rationalisointiin päätelaitteiden liityntää palveleviksi. Uusi rakenne perustui Lii-

tyntäkytkin(LK) - Runkokytkin(RK) - Liityntäreititin(LR) -topologiaan. Kolmen datakeskuksen välille muodostettiin palveluverkko, joka mahdollisti keskusten virtualisoinnin, korkean käytettävyyden ja tietoturvallisuuden näkymättömästi loppukäyttäjälle. Toisella liityntäpalvelukerroksella päätelaitteet erotettiin datakeskuksista ja päätelaiteyhteydet suojattiin Virtual Private Network (VPN)-salauksella. Ylimenoa tuettiin tilapäisillä, alueellisilla tai paikallisilla levyresursseilla, jotka myöhemmin lakkautettiin. Tässä kerroksessa toteutettiin myös päätelaitteiden ja tulostimien etähallinta. Kolmannessa resurssikerroksessa tarjottiin jaettuja Microsoft-perusteisia resurssipalveluita Active Directory (AD) -puusta. Neljännessä käyttäjäistuntokerroksessa kevennetyt päätelaitesovellukset kytkettiin istunnoilla HALNET-portaalin roolipohjaiseen pääsyoikeuksien hallintaan ja edelleen autorisoituihin sovelluspalveluihin.

HALNET-muutos suunniteltiin strategisena kumppanuutena vuonna 2004 ja toteutettiin pääasiassa oman henkilöstön voimin vuosina 2005–2006 rinnakkain iTVJ-verkkomuutoksen kanssa. HALNET-muutos toteutettiin nopeammin, halvemmin ja vähemmillä palvelukatkoksilla, kun sitä verrataan vastaaviin keskittämis- ja rationalisointihankkeisiin muissa asevoimissa (kirjoittajan kokemuksiin perustuen). Eräs keskeinen tekijä muutoksen onnistumisessa oli joukko-osastojen osaava ATK-henkilöstö ja HALNET-muutokseen henkilökohtaisesti palkattu projektipäällikkö, joka karismaattisesti innosti, ohjasi ja valvoi ATK-henkilöstön muutostyötä ja johti liikkuvaa iskuryhmää, joka ratkaisi vaikeimmat migraatiotapaukset.

Tietoteknisen alustan, sovellusten ja prosessien digitalisoinnin avulla Puolustusvoimat kykeni 2008 ja 2015 rakennemuutoksissaan keskittämään hallinnollisia palveluita, muuttamaan organisaatioitaan nopeammin, ulkoistamaan ylläpitopalveluitaan, keskittämään hankintarakenteitaan, hallitsemaan keskitetymmin hankerakenteitaan ja vähentämään henkilöstöään ja varuskuntia.

Kirjoittaja:

Juha Mattila on pitkän linjan viestimies, joka aloitti tykistön viestissä 80-luvun alussa,valmistui viestiupseeriksi 1984, toimi noin 13 eri tehtävässä viesti- ja-johtamisjärjestelmäalalla ja jäi reserviin viestitarkastajan tehtävästä 2012. Sen jälkeen hän on neuvonut kahta asevoimaa Lähi-Idässä johtamisjärjestelmäalaan ja digitaaliseen transformaatioon liittyvissä kehitystehtävissä. Koulutukseltaan Mattila on yleisesikuntaupseeri ja tekniikan tohtori.

Teksti: Jyrki Penttinen

Telealan uutisia

Suomi

Drooneista. Traficom avasi helmikuussa lausuntokierroksen vuoden 2026 UAS (Unmanned Aerial Systems) -vyöhykkeistä. Ehdotus lisää ja muuttaa droonialueita kriittisen infrastruktuurin, satamien, voimaloiden, pelastusasemien ja tutkimusympäristöjen osalta sekä nostaisi VTT:n ehdotuksesta Nokia Oulu Zonen ylärajan lentopintaan FL90. FL (Flight Level) on lentopinta, joka vastaa korkeutta standardipaineella (1013,25 hPa). FL90 tarkoittaa 9000 jalkaa, eli noin 2740 metriä merenpinnasta. Kyseinen kehitys heijastaa Suomen droonisääntelyn päivitystä turvallisuuden, testauksen ja teollisten käyttötapausten tueksi sekä tulevien kaupallisten verkkojen operointitarpeiden huomioimiseksi kansallisesti. [1]

Satelliiteista. SAR-tutka (Synthetic Aperture Radar) on satelliittipohjainen aktiivinen kaukokartoitustutka, joka tuottaa korkearesoluutioisia kuvia maan pinnasta hyödyntämällä satelliitin liikettä “synteettisenä antennina”. SAR mittaa maahan lähetetyn mikroaaltosignaalin heijastuksen siten, että satelliitin liike yhdistetään laskennallisesti suureksi antenniksi, millä saavutetaan tarkempi resoluutio kuin fyysisellä antennilla. SAR toimii yöllä, pilvien läpi ja säästä riippumatta. Suomalainen ICEYE kertoi maaliskuussa uusista kaupallisista SAR-satelliittisovelluksista, joita ovat mm. trooppisten metsäkatojen seuranta ja Antarktiksen jäämassojen muutosten mittaaminen. Uutiset korostavat Suomen asemaa tutkasatelliittien laaja-alaisena kehittäjänä, sillä sama teknologia palvelee ilmastoanalyysiä, pelastustoimea ja turvallisuutta. Se myös vahvistaa suomalaisen avaruusliiketoiminnan kansainvälistä roolia, koska kaupallinen SAR-data yleistyy nopeasti viranomais-, vakuutus- ja ympäristökäytössä. [2]

Eurooppa

5G. Ukrainan Kyivstar käynnisti tammikuussa ensimmäisen 5G-pilottialueensa Lvivissä. Ukrainan hallitus on valinnut testialueet perustuen asukastiheyteen ja teleinfrastruktuurin valmiuteen. Lviv valittiin erityisesti sen 5G-kykyisten kaupallisten päätelaitteiden keskittymän vuoksi. Hanke on symbolisesti tärkeä, sillä 5G:n rakentaminen nähdään osana maan digitaalista jälleenrakennusta, ja kokeilua aiotaan laajentaa myöhemmin muihin kaupunkeihin. Uutinen osoittaa, että 5G-kehitys jatkuu myös poikkeusoloissa, kun verkkojen häiriönsiedosta tulee strateginen kilpailutekijä sekä varteenotettava Itä-Euroopan teollisen viestinnän perusta. [3]

Amerikka

5G. AT&T ilmoitti maaliskuussa investoivansa verkkoihinsa 250 miljardia dollaria seuraavan viiden vuoden aikana. Painopisteinä ovat kuitu, 5G-kotilaajakaista, mobiiliverkon laajennus ja satelliittiyhteydet harvaan asutuille alueille. Uutinen antaa osviittaa siitä, että 5G nähdään Yhdysvalloissa yhä laajemmin infrastruktuurialustana tekoälylle, pilvipalveluille ja kriittisille yhteyksille. Nykyinen kehitys ei siten ole ainoastaan perinteistä puhelinverkkojen päivitystä, vaan se liittyy kasvavasti myös kansallisen kilpailukyvyn, turvallisuuden ja palvelukattavuuden kasvualustaan. [4]

Aasia

5G. 5G:n kehitys Vietnamissa nousi otsikoihin maaliskuussa, kun valtiollisen Mobifonen kerrottiin neuvottelevan uusista verkkosopimuksista kiinalaistoimittajien kanssa. MobiFone on laajentamassa 5G-peittoaluetta nopealla aikataululla yli 20 kaupungissa tai provinssissa, 4G:n peittoalueen ollessa jo laaja maaseutualueilla. Nyt hallituksen strategian mukaisesti operaattori on keskittymässä 5G-teknologiaan, digitaalisiin palveluihin ja keinoälysovelluksiin. Uutinen kuvastaa alueen peruskehitystä, jossa 5G:n rakennusta edistävät kustannustehokkuus ja nopea peitto, mutta samalla turvallisuus, investointisuhteet ja teknologiariippuvuus ovat merkittävässä osassa käyttöönottostrategioissa. Nämä päätökset vaikuttanevat toimittajavalintoihin myös laajemmin Kaakkois-Aasiassa sekä alueen tuleviin 3GPP:n 5G-Advanced ja -yksityisverkkoinvestointeihin. [5]

3GPP

6G. 3GPP vahvisti keväällä, että Release 20 on 6G:n tutkimusvaihe ja Release 21 aloittaa virallisesti varsinaisen normatiivisen työn, jonka tuloksena saadaan ensimmäiset varsinaiset 6G-tekniset spesifikaatiot. Maaliskuun kokous Fukuokassa Japanissa todisti kehityksen siirtyvän visiokeskustelusta järjestelmälliseen standardointiin. Tämä on telealalle tärkeä signaali investointien, tutkimuksen ja ekosysteemivalintojen suhteen, ja edistää laitevalmistajien tuotekehitystä yhtä lailla kuin ekosysteemin taajuusstrategioiden valmistelua 6G:n kaupallisen vaiheen häämöttäessä 2030-luvun alkupuolella. [6]

Lähteitä

[1] Lausuntopyyntö UAS-ilmatilavyöhykkeistä (OPS M1-29) 2026. 17.2.2026. https://www.traficom.fi/fi/uutiset/lausuntopyynto-uas-ilmatilavyohykkeet-ops-m1-29-2026

[2] All the latest press releases, news, media assets and more. https://www.iceye.com/newsroom/press-releases/all

[3] Kyivstar Launches 5G Pilot Program in Lviv. 12.01.2026. https://investors.kyivstar.ua/news-releases/news-release-details/kyivstar-launches-5g-pilot-program-lviv-0

[4] https://www.reuters.com/business/media-telecom/att-invest-250-billion-over-five-years-us-boost-infrastructure-2026-03-10

[5] MobiFone Review: Coverage & Performance In Vietnam 2026. https://go-hub.com/tr/esim-carriers/vietnam-mobile

[6] Release 20. 3GPP. https://www.3gpp.org/specifications-technologies/releases/release-20

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

Alkuperäisen artikkelin kirjoittaja: Ei tiedossa

Sota- ja aselajimuseot

Kesälomien ja matkailukauden alkaessa Viestimies haluaa muistuttaa lukijoitaan siitä, että maassamme on monia puolustusvoimiemme kunniakkaasta historiasta kertovia sota- ja aselajimuseoita. Niistä monet antavat meille mieluisia muistoja omasta varusmiesajastamme. Meitä viestimiehiä on lähinnä Viestimuseo Riihimäellä (Nyk. Museo Militaria, Hämeenlinna), mutta kannattaa varmasti pistäytyä muissakin.

Sotamuseo

Sotamuseo on puolustusvoimien museo, jolla aselajimuseoihin nähden on keskusmuseon asema. Se on sotahistoriallinen erikoismuseo, jonka toiminta-alueena on koko Suomi. Sotamuseon tehtävinä on koota Suomen puolustusvoimiin ja yleiseen sota- ja puolustuslaitoshistoriaan liittyvää esineistöä ja perinnettä, säilyttää, tutkia ja luetteloida hallussaan olevaa esineistöä museaalisten menetelmien mukaan sekä harjoittaa näyttelytoimintaa.

Museon kokoelmat käsittävät noin 40 000 esinettä ja kartunta tapahtuu pääasiassa yksityisten lahjoitusten sekä puolustusvoimien hylätyn materiaalin siirtojen avulla. Esineistö koostuu lippu-, kunniamerkki-, varus-, ase-, ampumatarvike-, aselajikokoelmista sekä yli 40 000 valokuvaa käsittävästä kuva-arkistosta. Erilaisia lippuja on noin 700, tykkejä 75 ja taideteoksia yli 800. Panssarivaunut, lentokoneet ja sota-alukset edustavat raskainta kalustoa, josta osa on sijoitettu aselajimuseoihin tai varastoitu.

Uudenmaan kasarmissa oleva perusnäyttely rakentuu historiallisista ja aselajikokoelmista. Näytteillä ovat Ruotsin vallan aikaiset kokoelmat, ns. Marskin huone, talvi- ja jatkosotien osastot sekä pienehköt ilma- ja merivoimien kokoelmat.

Suomenlinnaan perustettiin v. 1948 Rannikkotykistöupseeriyhdistyksen ja Sotamuseon toimesta Rannikkotykistömuseo, missä on pysyvästi esillä rannikkotykistön aseita, ampumatarvikkeita, tulenjohto- ja mittauskalustoa sekä sotilaspukuja ja valokuvia. Museo sijaitsee 1760-luvulta peräisin olevassa ruutikellarissa Kustaanmiekalla. Suomenlinnan Tykistölahden rannalla oleva museosukellusvene Vesikko avattiin yleisölle kesällä 1973 ja se saavutti heti suuren yleisömenestyksen. Vene onnistuttiin pelastamaan romuttamiselta 1950-luvun lopulla ja entistettiin sukellusveneveteraanien ja liikelaitosten tuella.

Sotamuseon tutkimustoiminta käsittää esineistön dokumentaatiota, yksityisten ja viranomaisten esittämien tiedustelujen selvittämistä, näyttelytoimintaan liittyviä tutkimuksia sekä puolustusvoimien perinne-esineistöstä pyydettyjen lausuntojen ja luonnosten laatimista. Julkaisutoimintaan sisältyy näyttelyluetteloiden ja -julisteiden painattaminen sekä Sotamuseon ja Sotahistoriallisen seuran yhteisen vuosikirjan toimittaminen.

Viestimuseo tänään

1. Viestimuseon syntymästä

Viestimies-lehden lukijoille (n:o 1/74:ssä) on maj Matti Juusti valottanut varsin seikkaperäisesti Viestimuseon syntyhistoriaa, josta painotettakoon vain kahta asiaa. V 1965 perustettu Viestikilta on saanut kunniakkaan tehtävän vastata Viestimuseo-hankkeen edelleen kehittämisestä ja koko materiaali on siirtynyt mainitusta vuodesta alkaen Viestikillan hallintaan. Vuoden 1973 syksyllä Viestimuseolle osoitettiin nykyisen Upseerikerhon viereisestä rakennuksesta noin 100 m2. Varusmiesten talkootyöllä kiltaveljien Matti Juustin ja Olavi Havian ansiokkaasti johtaessa suoritettiin korjaus- ja entisöintityöt varsin lyhyessä ajassa. Niinpä jo 25.5.1974 voitiin suorittaa Viestimuseon juhlalliset avajaiset.

2. Viestimuseon esineistö

Museon kunnostettuihin tiloihin on saatu näytteille noin 900 esinettä. Pakkilaatikoissa odottaa esillepääsyä ainakin saman verran materiaalia. Näyttelyesineistä mainittakoon neljä suurempaa kalustokokonaisuutta, jotka ovat puhelin- ja lennätinkalusto, radiokalusto, puhelinkeskuskalusto sekä erilaiset mittarit ja komponentit. Viestijoukkoja ja -kalustoa käsittelevää kuvamateriaalia on kaikissa näyttelyhuoneissa, erityisesti Viestirykmentin perinnehuoneessa. Vedottakoon jälleen kerran kaikkiin viestimiehiin. Lähettäkää viestiaiheisia valokuvia. Merkitkää valokuviin, mitä ne esittävät, missä ja milloin otettu. Myöskin muuta museolle arvokasta materiaalia otetaan kiitollisuudella vastaan, kuten viestivälineitä, vanhoja komponentteja, kalusto-oppaita ja ohjesääntöjä.

Pioneerimuseo

Pioneerimuseon perustajana pidetään evl evp Eero-Eetu Saarista, joka 1929 nuorena vänrikkinä palvellessaan Korialla esitti perustamisajatuksen pataljoonan silloiselle komentajalle evl V H Vainiolle, joka hyväksyi ajatuksen ja niin ryhdyttiin välineistöä keräämään. Talvi- ja jatkosodan poikkeuksellisten aikojen päätyttyä pidettiin Pioneerimuseon

viralliset avajaiset 12.05.1945. Tällöin oli näytteillä 86 nimikettä, nykyisin niitä on yli 2 500.

Vanhan museorakennuksen, sodanaikaisen esikuntaparakin, alkaessa lahota ryhdyttiin toimenpiteisiin uuden museorakennuksen saamiseksi aikaan. Pioneerikillan suosiollisella tuella seisookin Kivimäessä nyt entistä ehompi museo.

Museossa, joka avattiin 01.05.1975, on mm. seuraavat osastot

muistojen osasto

kenttärakenteiden ja siltojen osasto

pukuosasto

valokuvaosasto

pioneeriohjesääntöosasto

miinoittamisen,

raivaamisen,

hävittämisen ja

ansoittamisen osastot

työkaluosasto

nykyvälineosasto ja

kone-esittelyosasto.

Lisäksi esitellään ulkoalueella raskasta pioneerikalustoa, linnoitteita ja koneita.

Sota- ja aselajimuseot

Viestimuseo, Viestirykmentti PL 5 11311 Riihimäki 31. Omistaja Viestikilta ry. Nykyinen osoite: Museo Militaria Vanhankaupunginkatu 19, 13100 Hämeenlinna.

Pioneerimuseo, PL 5 45600 Koria. Omistaja: Pioneerikilta ry. Nykyinen osoite: Museo Militaria Vanhankaupunginkatu 19, 13100 Hämeenlinna.

Sotamuseo, Maurinkatu 1 00170 Helsinki 17. Omistaja Puolustusvoimat. Nykyinen osoite: Sotamuseon Maneesi ja Tykistömaneesi, Iso Mustasaari c 77, 00190 Helsinki

Rannikkotykistömuseo, Suomenlinna, Kustaanmiekka. Omistaja: Sotamuseo / Puolustusvoimat. Toiminnassa vuoteen 2006 saakka.

Sukellusvene Vesikko, Suomenlinna, Tykistölahti. Omistaja: Sotamuseo / Puolustusvoimat.

Ilmatorjuntamuseo, Ilmatorjuntakokoulu PL5 04301 Hyrylä. Omistaja: Ilmatorjuntasäätiö. Nykyinen osoite: Klaavolantie 2, 04300 Tuusula.

Kadettimuseo, Kadettikoulu PL 7 00861 Helsinki. Omistaja: Kadettikoulu.

Panssarimuseo, 13700 Parolannummi. Omistaja: Panssarikilta ry. Nykyinen osoite: Hattulantie 334, 13700 Parola.

Ratsuväkimuseo, Linnoitus, 53900 Lappeenranta. Omistaja: Lappeenrannan kaupunki. Nykyinen osoite: Kristiinankatu 2, 53900 Lappeenranta.

RUK-Museo, Reserviupseerikoulu PL 54 49401 Hamina. Omistaja: RUK:n oppilaskunnan kannatusyhdistys ry. Nykyinen osoite: Kadettikoulunkatu 8, 49400 Hamina.

Viestimies 50 vuotta sitten artikkelin kirjoittaja: Pasi Puhakka

Yhteydet maastoon Nestorin tuotteilla

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

nestor cables

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

Mittarikuja 5,
90620 Oulu
PL 276, 90101 Oulu