

Viestimies

Viestiupseeriyhdistyksen julkaisu 76. vsk Numero 2 Kesä 2021



6G -todellisuutta 2030-luvulla, sivu 6

ESSOR - Eurooppalainen aaltomuoto, sivu 15

Multidomain C2, sivu 20

www.viestiupseeriyhdistys.fi



COMBITECH

Experts in Digitalizing Defence

Viestimies-lehti

Päätoimittaja
Samuli Terämä
p 050 3399038
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Hanna Liitola
p 040 5930675
henkilotoimittaja@viestiupseeriyhdistys.fi

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

Toimituskunta
Vähätiitto Jarmo (pj)
Blomqvist Reima
Holma Harri
Isomäki Pekka
Mikkonen Mauri
Petäjäinen Juha
Ståhlberg Mika
Tunkkari Antti
Wirman Kari
Yli-Äyhö Janne

Toimituksen osoite:
Päivölärinne 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 09 873 6944, 050 592 2722
juha.halminen@kolumbus.fi

Painopaikka
Newprint Oy, Raisio
p 010 231 2600

Toimitus jättää kirjoittajille vastuun heidän
esittämistään mielipiteistä. Kirjoitusten
lainaaminen sallittu vain toimituksen lu-
valla.
ISSN 0357-2153



Kansikuva: Yhteistoimintaa Northern Forest
21-harjoituksessa

Tässä numerossa

- 5 Pääkirjoitus: – Pitäkääpä huoli...kesää kohti!
- 6 6G lähestyy
- 10 Venäjän elektronisen sodankäynnin joukot 2020-luvulla
- 15 Katsaus eurooppalaiseen aaltomuotokehitykseen (ESSOR)
- 18 Ajatuksia Viestikiltojen toiminnan kehittämisestä
- 20 C2 for a new paradigm: addressing the challenges of multi-domain warfare
- 23 Maailmanluokan sotahistoriakohteen nousu ja tuho
- 25 Vapaaehtoinen maanpuolustus kyberturvallisuuden kansallisessa kehittämisessä
- 29 Analysaattori: Autotallin taika
- 31 Viestimies 50 vuotta sitten
- 32 5.3.2021 myönnetty viestiristit
- 34 A. R. Saarmaa -seminaari-ilmoitus

Seuraavan numeron aineistopäivä on 13.8.2021. Lehti ilmestyy viikolla 38.

Patria 100

Patria vuodesta 1921

Sata vuotta on vahva perusta yhdessä tekemiselle ja menestymiselle.
Se on perusta turvalliselle tulevaisuudelle.

Tutustu sataan tarinaan osoitteessa
patriagroup.com



– Pitäkääpä huoli...kesää kohti!

Kesä tulee kohisten. Tätä kirjoittaessa ensimmäinen lämpöaalto hellii Suomea - toivottavasti ei viimeinen. Kaikki varmasti odottavat innolla kesää ja riittävää rokotekehitystä, jotta rajoituksia voitaisiin purkaa. Tällä hetkellä väestöstä on rokotettu noin 35% eli noin 2 miljoonaa kansalaista. Kesälomakauden alkaessa toivottavasti luku on reilusti tätäkin suurempi. Kesää ja kesälomia odotellessa siis.

Olemme lukeneet uutisointeja erilaisista lieveilmiöistä koronaan liittyen. Etätöiden lisääntyä merkittävästi myös rikolliset, erityisesti verkkorikolliset, ovat aktivoituneet. Lunnas- ja muiden kiristyslaittojen esiintyvyys on kasvanut huomattavasti korona-aikana. Valtionhallintokaan ei ole säästynyt kyberhyökkäyksiltä. Valtori ilmoitti muun muassa mahdollisesta tietomurrosta sen palvelin alustoihin, laajasti etäyhteyskäytössä olevan ohjelmiston kautta. Hyökkäyksen tekijää, laajuutta ja vaikutavuutta selvitetään - tutkinta on kesken. Check Point Software Technologies Finland Oy julkaisi hiljattain raportin, jossa todettiin muun muassa, että vuonna 2020 etäyhteyksiä hyödyntävistä yrityksistä 97% ovat kohdanneet useita hyökkäysmenetelmiä hyödyntäviä haittaohjelmia. Varautuminen on myös tietovarautumista, ei vain materiaalia ja logistiikkaa.

Korona on vaikuttanut varautumiseen ja nostanut siitä käytävää keskustelua yhä useammin päivän uutisotsikoihin. Ekologisuus liikenteessä ja päästökauppa sekä yleisesti päästöjen vähentäminen ovat aiheuttamassa yhden lieveilmiön lisää. Autokannan sähköistyessä Huoltovarmuuskeskus ja Puolustusministeriö ovat esittäneet huolensa Suomen liikenteen kriisin kestävydestä. Poikkeusolojen varalle luotuja järjestelmiä, kuten pakko-otettavien ajoneuvojen hyödyntäminen maanpuolustuksessa ja polttoainoiden varmuusvarastointi, on pakko miettiä uudelleen. Mikäli autokanta sähköistyy merkittävästi tulevaisuudessa, ei kriisin tullen sähköautoja ole mahdollista hyödyntää vastaavalla tavalla kuin aiemmin. Latauspistokkeita ei ole tarjolla joka kuusen juurella. Ainakin toistaiseksi polttomoottoriautot, joiden käyttövoimaa voidaan varastoida, ovat jatkossakin merkittävässä roolissa Puolustusvoimien ja Suomen kriisin keston kulmakivinä.



Telealalla varautuminen ja kehitys ovat myös menossa osin huolestuttavaan suuntaan. Matkapuhelinverkko-operaattorit yhdistävät verkkojaan ainakin osin kustannussäästöjen vuoksi. Esimerkiksi Pohjois- ja Kaakkois-Suomessa Telia ja DNA ovat yhdistämässä verkkojaan. Yhteisverkon myötä operaattoreiden omat 2G ja 4G verkot lakkautetaan ja painopistettä siirretään 5G verkkoihin. Telia on ilmoittanut myös lakkauttavan oman 3G verkkonsa vuoden 2023 loppuun mennessä. Huoli haja-asutusalueiden verkkopeitosta on olemassa. Tälläkään hetkellä 3G kuuluvuutta ei ole joka paikassa, saati 4G verkkoa. Näillä muutoksilla on väistämättä vaikutusta myös valmiudellisista näkökulmista tarkasteltuna. Yhteistyössä turvallisuusviranomaisien ja operaattoreiden kanssa asiassa varmasti löydetään osapuolia tyydyttävä yhteisymmärrys varautumisen kannalta. Tilanne edellyttää sopeutumista ja laaja-alaista suunnittelua, jotta vaikutukset kyetään huomioimaan.

Puolustusministeri Antti Kaikkonen totesi hiljattain, että Puolustuselonteko

on valmistumassa ja tuotaneen eduskuntaan kesäkuussa, noin kaksi kuukautta suunniteltua aikataulua myöhemmin. Kyberturvallisuuden on uumoiltu nousevan yhdeksi merkittävimmäksi aiheeksi, unohtamatta puolustusyhteistyötä tai HX hanketta. Kyberturvallisuus ja kyberpuolustus ovat olleet keskiössä erityisesti näin korona pandemian aikana, kun verkkorikollisuus on lisääntynyt ja kohdentunut mm. pankkipalveluihin ja rahaliikenteeseen. Kyberpuolustuksen keinovalikoimaan on toivottu myös välineitä vaikuttamiseen, jolla kyettäisiin vastaamaan mahdollisiin vihamielisiin vaikuttamisyrityksiin ja jopa ennaltaehkäisevään toimintaan. Tiedustelulakien päivittymisen myötä toimivaltuudet kehittyivät selkeämpään suuntaan ja niistä on ollut konkreettista hyötyä. Näin totesi myös Pääesikunnan tiedustelupäällikkö kontra-amiraali Juha Vauhkonen. Kybertoiminnassa toimivaltuuksien tulee olla selkeät, jotta toiminnalla on lain suoma selkänöja.

HX-hanke on edennyt loppusuoralle, kun ehdokkaat ovat toimittaneet lopulliset tarjouksensa. Suurta mielenkiintoa herättää mihin konetyyppiin valinta kohdistuu. Kyse ei ole vain pelkästä kone-tyypistä, vaan mukana päätöksessä ovat myös huolto- ja koulutusjärjestelmä, muu teollinen yhteistyö eikä vähäisempänä käytettävissä oleva aseistus. Näin viestimiehen silmin kiinnostaa luonnollisesti minkälainen johtamisjärjestelmä konetyypin mukana tulee ja miten se kyetään integroimaan olemassa olevaan maasi-joitteeseen infrastruktuuriin sekä miten sitä tulisi kehittää. Perinteisten puolustushaarojen maa-, meri- ja ilmavoimien lisänä ovat avaruus- ja kyberulottuvuudet. Tämän Multidomain ajattelun myötä kaikki ovat kytköksissä toisiinsa. Merkityksellisintä on tilannekuva ja sen perusteella luotava tilanneymmärrys sekä resurssien kohdentaminen oikea-aikaisesti sinne, missä sillä on suurin vaikutus operaation kannalta. Kaikkien puolustushaarojen ja toimialojen yhteistoiminta koordinoitusti mahdollistaa Suomen puolustuksen kustannustehokkaan ja vaikuttavan valmiuden osoittamisen, mikäli sitä joskus tarvittaisiin.

Päätoimittaja

Samuli Terämä



Teksti ja kuvat: Jyrki Penttinen, Senior Technology Manager, GSMA North America

6G lähestyy

TkT, ins-ltn (res) Jyrki Penttinen on toiminut telealalla vuodesta 1994 lähtien Suomessa, Espanjassa, Meksikossa ja Yhdysvalloissa. Penttinen työskentelee nykyään GSMA:n Pohjois-Amerikan organisaatiossa teknologiapäällikkönä. Muitten töittensä ohessa Penttinen on luennoinut televiestintäteknologioista englanniksi, espanjaksi ja suomeksi. Penttinen on julkaissut useita 5G-kirjoja, joista viimeisin on ”5G Second Phase Explained” (Wiley, 2021) ja ”The 5G Dictionary” (Amazon, 2021). Penttisen artikkeleihin voi tutustua osoitteessa www.linkedin.com/in/jypen_seka_blo-gissa_5g-simplified.com.

6G edustaa 5G-verkkojen jälkeisiä viestintäjärjestelmiä, joiden oletetaan olevan todellisuutta 2030-luvulla. Vaikka useat operaattorit ovat ottaneet käyttöön rajoitetusti 5G-verkkojaan vuodesta 2019 lähtien, niiden laajamittainen käyttö on vielä vuosien päässä. Teollisuus on kuitenkin jo visioinut innokkaasti tulevan sukupolven perusteita. Tämä artikkeli analysoi tärkeimpiä näkemyksiä ja viitteitä 6G-vaatimuksista.

Yleistä

Ensimmäisestä matkaviestintäsuukupolvesta lähtien – 1980-luvulla käytöön otettujen ja nyttemmin lopetettujen analogisten matkaviestintäjärjestelmien – uuden sukupolven syntyminen on ollut järjestelmällisenä ilmiönä jokaisella sen jälkeisellä vuosikymmenellä. 2G, 3G, 4G ja nyt myös 5G ovat tällä hetkellä monessa maassa rinnakkaisessa käytössä. Toisaalta on jo nähtävissä, että useat operaattorit ovat lopettaneet, tai harkitsevat 2G- ja 3G-verkkojensa tuen lopettamista siirtäen liikennettä spektrinkäyttöään tehokkaampiin 4G- ja 5G-verkkoihin.

Kuva 1 esittää matkaviestinnän suhteellisen käytön ennusteen GSMA Intelligencen tuoreiden tilastojen perusteella. [1] Kuten kuvasta voidaan nähdä, spektritehokkuudeltaan heikoimman 2G:n (sen suosituimpana edustajana GSM) merkitys vähenee nopeasti, vaikka se palveleekin edelleen erityisesti IoT-laitteita ja kehittyviä markkinoita myös tulevina vuosina. Tällä välillä, 5G:n käyttöönotto tapahtuu vähitellen, ja vuoteen 2025 mennessä sen osuus maailmanlaajuisesta matkaviestinnän käyttäjäkunnasta on arviolta 20%, siinä kun kehittyneillä markkinoilla Yhdysvalloissa, Euroopassa ja Aasiassa alueellinen käyttöaste voi olla lähellä 50%. Ennusteessa on erityisen huomionarvoista se, että 4G on selvästi hallitseva sukupolvi vielä vuonna 2025.

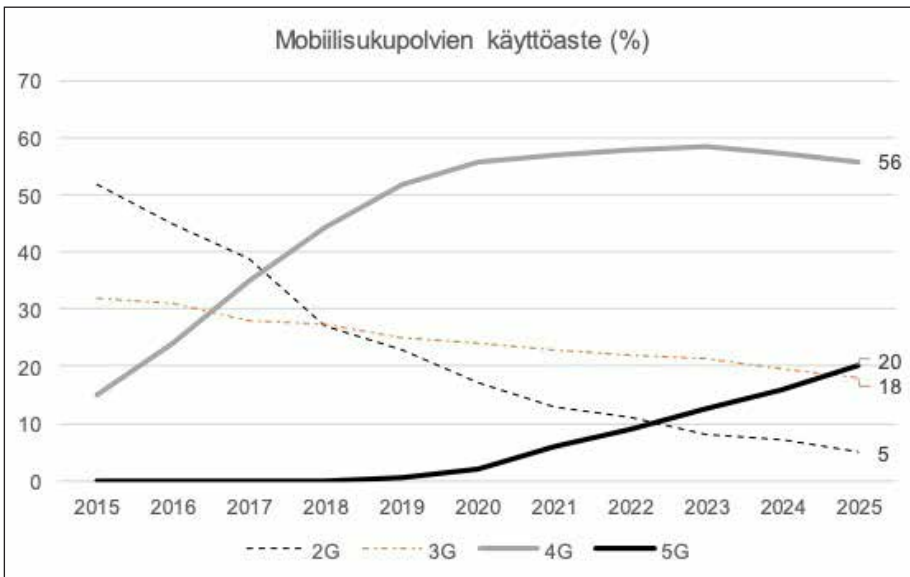
6G on puolestaan vasta visiointivaiheessa, teollisuuden aikomuksena saada se kaupalliseen käyttöön ensi vuosikymmenen alussa. Tällä hetkellä seuraavan sukupolven kehityksessä tärkein edustaja

on kansainvälinen teliitto ITU, joka valmistelee korkean tason suorituskykyvaatimuksia 6G-järjestelmille siihen kehitettävien IMS (International Mobile Telecommunications) –määritysten mukaisesti.

ITU huolehtii 6G:n vaatimusten luonnista loogisena jatkumona, samalla tavoin kuin se julkaisi IMT-2000 –vaatimukset 3G:lle, IMT-Advanced –vaatimukset 4G:lle ja IMT-2020 –vaatimukset 5G:lle. Kuten aiemmin on ollut tapana, myös 6G:n maailmanlaajuiset vaatimukset, joita todennäköisesti kutsutaan termillä IMT-2030, tulevat olemaan teollisuuden ja standardointielinten yhteistyön tulos. Jälkimmäisistä tärkein on 3GPP, kuten on ollut tilanne 3G:n (UMTS/HSPA) spesifioinnista lähtien.

Esimerkkinä maailmanlaajuisesti tunnus-tetuista 5G-järjestelmistä, ITU hyväksyi hiljattain kolme radiotekniikkaa, jotka täyttävät IMT-2020-vision ja suorituskykyvaatimukset: 3GPP 5G-SRIT, 3GPP 5G-RIT ja 5Gi, joista jälkimmäinen on tulos Intian televiestinnän standardointi-kehityksestä (TSDSI). ITU:n IMT-visio edellyttää, että ehdokasteknologiat ovat riittävän yksityiskohtaisia, jotta niiden toiminta ja laitteet, mukaan lukien verkko-ovierailu, ovat maailmanlaajuisesti yhteensopivia. ITU:n arviointiprosessin tuloksena IMT-2020:n ensimmäinen 5G-julkaisu sisältää nyt joukon maan-päällisiä radiorajapintamäärittäjiä, jotka on sisällytetty ITU-R:n IMT-2020:n radioliitäntöjen maailmanlaajuiseen standardiin.

ITU soveltaa samaa prosessia myös 6G:n



Mobiilisukupolvien suhteellisen käytön kehitys.

määrittäisiin, ja kuten on totuttua, 3GPP ottaa muiden standardointiorganisaatioiden ohella tämän huomioon teknisten spesifikaatioiden kehittämisessä hyvissä ajoin ennen vuotta 2030.[2]

6G-työryhmiä

Vaikka IMT on olennainen osa 6G:tä, ITU:n työ on vasta alkuvaiheessa. Konkreettisenä esimerkkinä, ITU:n työryhmä SG-13:n tuotti viime vuonna spesifikaation uuden sukupolven arkkitehtuurin yleisraameista, mutta se ei vielä sisällä yksityiskohtaisia, normatiivisia määrittämiä sen enempää kuin vaatimuksiakaan. Samaan aikaan teollisuus ideoi ja visioi ehdokasteknologioita. Tämä keskustelu on siten iteratiivinen prosessi, joka auttaa ITU:a muodostamaan konkreettiset IMT-vaatimukset 6G:lle.

Seuraavassa on lueteltu joitakin tähän prosessiin osallistuvista tahoista ja niiden näkemyksiä.

ITU-T SG-13 keskustelee tulevaisuuden verkkotekniikoista ja tarkastelee ehdokasideoita IMT-2030-vaatimuksiin. [3]

ITU-R eli ITU:n radiotekninen jaosto tutkii 6G-radiotekniikan vaatimusten määrittäystä. ITU-R-työryhmä 5D on kutsunut organisaatioita toimittamaan panoksensa kesä- ja lokakuun kokouksiinsa vuonna 2021 ”Tulevaisuuden teknologiasuunnaukset vuoteen 2030 ja sen jälkeen” -raportin laatimiseksi. [4]

ITU-R WRC on ITU:n maailmanlaajuisen radiokonferenssi, joka toteutetaan muutaman vuoden välein keskustelemaan taajuusjakoperusteista. Tulevissa konferensseissa keskustellaan siten radiokaistojen laajennuksista, joiden tarkoituksena on palvella 6G-verkkoja vuonna 2030 ja sen jälkeen.

3GPP edustaa useita maailmanlaajuisesti merkittäviä telealan standardointiorganisaatioita. 3GPP:llä on tärkeä rooli 6G:n konkreettisten spesifikaatioiden laatimiseksi siten, että ne täyttävät 6G:n IMT-vaatimukset.

Euroopan unioni on perustanut EY:n kautta useita tutkimusohjelmia 5G:lle, ja valmistelee niitä myös 6G:lle. Esimerkkejä jälkimmäisistä ovat Hexa-X ja SNS-PPP. [5]

ATIS on Pohjois-Amerikan teollisuusyhteisliittymä. ATIS on perustanut **NextG Alliance** -ryhmän keskustelemaan ja edistämään 6G-aikakauden ratkaisuja Pohjois-Amerikan teollisuuden edustajien kanssa.

Yhdysvaltojen hallitus korostaa **Federal Communications Commissionin** (FCC) kaltaisten virastojen välityksellä tarvetta alueelliseen osallistumiseen tulevien viestintätekniikoiden standardointiin ja tekniseen kehittämiseen.

Esimerkkinä Aasian tavoitteista olla 6G-kehityksen etuasemissa, **Japanin hallitus** (Ministry of Internal Affairs and Communications) on tuottanut aktiivisesti visioita 6G-tavoitteista.

6G-visioista

6G-aikakausi on noin vuosikymmenen päässä kaupallisesta käyttöönotosta. Monista keskusteluista ja julkisuuden uutisista huolimatta alalla ei vielä ole konsensusta visiosta. Julkisiin tietolähteisiin perustuen voidaan arvioida, että 6G yhdistää fyysiset ja digitaaliset ”maailmat” ja toimii alustana digitaalisen vertaismallin (digital twin) toteuttamiseksi. Digitaalinen verrokki viittaa tässä yhteydessä järjestelmän kykyyn edustaa reaali maailman olioita ja esineitä digitaalisessa muodossaan lähes reaaliajassa. Esimerkkinä tästä on alkuperäisen olion avatar, joka muistuttaa läheisesti fyysisestä esikuvaansa niin fyysisesti kuin toiminnaltaan.

ITU-T SG13 on siten tällä hetkellä yksi konkreettisimmista 6G-tietolähteistä, koska se luo pohjan ITU:n 6G-IMT-vaatimuksille. SG13 ottaa huomioon 5G-ominaisuuksien jatkokehittämisen ja arvioi todennäköisiä käyttöympäristöjä, kuten holografista viestintää, ja niiden vaatimuksia, joihin 5G:n suorituskyky ei tulle riittämään edes kehittyneessä muodossaan. Esimerkiksi SG13 NET-2030 -työryhmän kesäkuussa 2020 tuottaman Architecture Framework –spesifikaation sisällöstä voidaan tulkita, että 6G:n on tarjottava 10-100 kertaa nopeampia datayhteyksiä kuin edeltäjänsä, huomattavasti suurempi järjestelmän kapasiteetti, taajuuksien hyötysuhde ja päätelaitteen liikkumisnopeus, parempi radiopalvelun kattavuus, ja pienempi viive. Lisäksi 6G:n odotetaan toimivan entistä tehokkaammin IoT-ympäristössä.

Kuten lähde [6] toteaa, ITU-T NET-2030:n vaatimuksiin kuuluu yksinkertaisuus, sisäänrakennettu ohjelmoitavuus ja juoheva arkkitehtuurien mukautuminen, yhteensopivuus edellisten järjestelmien kanssa, monimuotoinen viestintä, laskenta, varastointi, palvelu ja niiden integrointi, verkkoon integroitu verkko- viipalointi (Network Slicing), yksiselitteinen verkkotoimintojen ja -palvelujen nimeäminen, luontainen tietoturvatuki kaikille verkkotoiminnoille, ja joustavuus. Näiden saavuttamiseksi NET-2030 esittää seuraavia näkökohtia:

Uuden palvelun lisääminen virtualisoi- tuun verkkoon on suoraviivaista, mutta voi siksi samalla lisätä kokonaispal- veluiden monimutkaisuutta ja johtaa virheisiin. 6G-ratkaisujen on siten oltava mahdollisimman yksinkertaisia.

Verkkoarkkitehtuurin on oltava erittäin joustava.

6G-verkon on tuettava palvelujen ja

verkkolaitteiden toiminnallista eriyttämistä.

Alkuperäisten verkkoviipaleiden tulisi mahdollistaa monentyyppisten 6G-palvelujen tehokas käyttö.

Käyttäjät ja järjestelmät eivät luo yhteyttä tiettyyn palvelimeen vaan pikemmin isännöityyn sisältöön, toimintoon tai palveluun.

6G-verkko on yhä selkeämmin mielletty kriittiseksi kansalliseksi infrastruktuuriksi turvallisuuden ja talouden kannalta. Tulevien verkkohyökkäysten välttämiseksi 6G-verkolla on siksi oltava riittävä sietokyky, mukaan lukien valvonta- ja hallintatasot.

6G-verkon on tarjottava tiedonsiirtolaatu sovellusvaatimusten kautta.

Lähde [7] toteaa, että 6G:n on ratkaistava 5G:n rajoitukset, kuten järjestelmän peitto ja IoT:n kehittyneen version, IoE:n (Internet of Everything) rajat. Lähteen mukaan 6G:n on palveltava kaikkialla olevaa älykstä matkaviestintäyhteiskuntaa. Tämä lausunto osoittaa ekosysteemin korkeat odotukset 6G-tekniikoille niiden toimiessa yhä tärkeämpänä alustana kehittyvässä yhteiskunnassa.

Lähde [8] mainitsee, että erityisesti holografinen media ja moniaistiperusteinen tieto ovat 6G-tietoliikennöinnin tyyppiesimerkkejä. Nykyisissä 5G-käyttöpauksissa mainitaan usein multimedia laajennetun todellisuuden ja virtuaalitodellisuuden (AR / VR) kautta, mutta 5G:n suorituskyky on vielä rajallinen lähes reaaliaikaisen holografisen viestinnän toteuttamisessa. 6G:n voidaan olettaa tarjoavan kiinnostavia ja realistisia käyttökokemuksia objektin todellisuutensa koostamisen avulla. Holografiset sovellukset sisältävät monia käyttökohteita, kuten viihdesovellukset, puhelin-neuvottelut ja holografisen etäyhteyden.

Lähde [5] kuvaa Hexa-X -vision, joka yhdistää reaali maailman, fyysinen ja digitaalisen maailman 6G:n teknologioiden kautta. EU-rahoitteisessa Hexa-X:ssä on mukana telealan yrityksiä ja tutkimusyksiköitä, jotka harkitsevat 6G-kehitystä. Hexa-X -hanke tutkii mm. uusia radioaajuustekniikoita korkeilla RF-taajuuksilla, sekä tarkkoja paikannusteknologioita ja aistipohjaisia sensortechniikoita, kehittyviä älyteknologioita, ja 6G-arkkitehtuurin dynaamisia näkökohtia.

Lähde [9] toteaa, että Next G Alliancen tavoitteena on edistää Pohjois-Amerikan johtajuutta 5G:n evoluutiopolulla ja 6G:n varhaisessa kehityksessä. Next G Alliancesella voidaan olettaa olevan tärkeä

rooli alueellisessa 6G-valmiudessa. Sen työ keskittyy teknologian kaupallistamiseen kattaen tutkimuksen ja kehityksen, valmistuksen, standardoinnin ja markkinavalmiuden elinkaaren. Matkaviestinnän keskeisiä sidosryhmiä edustavien jäsenjärjestöjen kautta Next G Alliancen vaikutus tuleviin standardeihin voi olla merkittävä.

Edellä kuvatut esimerkit 6G-visioista edustavat kehityskohteita, joita ei ehkä ole mahdollista toteuttaa 5G:n kautta sen elinkaaren aikana. Nämä indikaattorit ovat hyödyllisiä tietolähteitä ITU:n IMT-2030 -vaatimuksien luonnissa.

Perustavia tekniikoita

Voidaan yleistää, että 6G on joukko tekniikoita, jotka muodostavat uudistetun, entistä tehokkaamman verkkoarkkitehtuurin.[4] Siten voidaan olettaa, että 6G on yhdistelmä maanpäällisiä ja ilma-aluksiin asennettuja tukiasemia sekä satelliitipohjaisia avaruusjärjestelmiä. Nykyisen kehityksen perusteella voidaan arvioida, että jotkut tekniikoista, kuten verkkotoimintojen virtualisointi (Network Functions Virtualization, NFV) ja ohjelmistopohjainen verkottuminen (Software Defined Networking, SDN), kehittyvät ja palvelevat käyttäjiä myös 6G-aikakaudella. Tämä tarkoittaa, että niihin liittyvillä palveluilla, kuten verkkopaljoittelulla, on edelleen tärkeä rooli 6G:ssä.

Alla on yhteenveto joistakin 4G:n ja 5G:n tekniikka-alustoista, jotka voivat olla ehdokkaita myös 6G-aikakaudella.

Verkkoviipalointi (Network Slicing): Verkkotoimintojen virtualisoinnin lisäksi verkon viipalointi tarkentuu ja palvelee verkkoresursseja optimoivien vertikaalien vaihtelevia tarpeita entistä paremmin.

Yhteiset sovellusliittymät (Common API): 3GPP SA6-työryhmän kehittämien rajapintojen (Northbound Interface) yhteiset sovellusliittymät voivat lisätä ohjelmistokehittäjien mahdollisuuksia käyttää verkon resursseja entistä tehokkaammin 6G-aikakaudella.

Palveluarkkitehtuuritaso SEAL (Service Enabler Architecture Layer for Verticals): 3GPP SA6:n määrittämällä palvelukerroksella tuetaan monien vertikaalien sovelluksia, esimerkkinä ajoneuvojen tietoliikennöinti V2X.

Ajoneuvotietoliikennöinnin sovellustaso (V2XAPP): V2X-palvelujen sovelluskerroksen tuki mahdollistaa V2X-palvelujen käytön 3GPP-järjestelmissä. V2X

Application Enabler -kerros sijaitsee SEAL-arkkitehtuurin päällä. Tällä hetkellä V2XAPP tarjoaa 4G:n ominaisuuksia, kuten V2X-viestien jakelun, palvelun jatkuvuuden, sovelluksen resurssien hallinnan ja dynaamisen ryhmähallinnan 4G-järjestelmän ominaisuuksien kautta, joita myös 6G voinee aikanaan tukea.

Radioliityntä: OFDM on toiminut radiotien perusteknologiana LTE:ssä ja 5G:ssä (New Radio, NR). OFDM, sen kehittyessä, voi toimia kelvollisena teknologiana myös 6G:ssä, joskin myös muita vaihtoehtoja voi ilmetä radioteknologioiden kehittyessä 2020-luvulla.

Avoin radioverkko (Open RAN): Avoin radioyhteysverkko on parhaillaan kehittyvä teknologia, jolla radioverkko voidaan optimoida avointen rajapintojen ja radioverkon toimintojen kehittyneen jaottelumallin kautta. Esimerkkinä, osa tukiaseman toiminnoista voidaan siirtää pilvipalveluun siten, että se voi jakaa käytettävissä olevaa radiokapasiteettia tehokkaammin myös muille tukiasemille. Avoin radioverkkokonsepti on oletettavasti tärkeä mahdollisuus myös 6G:ssä.

Johtopäätökset

6G:stä keskustellaan jo aktiivisesti, mutta tällä hetkellä olemme vasta visiointivaiheessa. Siitä huolimatta, teollisuuden ja tutkimuksen lähteistä voimme jo tulkita konkreettisia viitteitä 6G:n tulevasta tarpeesta vastaamaan ekosysteemin suorituskykyvaatimuksiin, jota ei voida toteuttaa 5G-verkoilla. Samalla ITU SG13 NET-2030 on jo yksilöinyt mahdollisia verkkomalleja ja käyttöesimerkkejä, joihin nykyinen 5G-aikakausi ei kykene näillä näkymin vastaamaan. Kuten aikaisemmillä matkaviestintä sukupolvilla on jo ollut ”perinteenä”, myös 6G näyttää olevan kaupallisesti saatavilla vuosikymmenen kuluttua.

Tämän hetkiset ja tulevat teknologiat, jotka mahdollistavat verkkojen yhä optimaalisemman resurssien käytön, kehittyvät ja toimivat alustana myös 6G-verkoissa. Yksi konkreettisimmistä esimerkeistä on verkkoviipalointi. Siitä huolimatta 6G:n kehitys hyötyy erityisesti realistisista vertikaalien vaatimusten ja käyttötapauksien syvällisestä ymmärtämisestä. Niiden arviointi on yksi ekosysteemin keskeisistä tehtävistä, jotta standardointielimet voivat suunnitella vastaavia ratkaisuja 6G:n toimiessa uuden aikakauden palvelualustana.

MILCON

Valmis vaativien kumppaneiden haasteisiin

- Liittimet
- Kenttävalokaapelit Pro Beam Jr. liittimin
- Viestilaitteiden erikoisvaraosat ja varusteet
- Ruggeroidut tietokoneet ja näytöt
- Puhelulaitteet ja audioliitännät
- Kaapelisarjat
- Antennit ja teholahteet



MILCON OY

Kolmionkatu 5 D
33900 Tampere.

Puh. 010 239 2170
info@milcon.fi

www.milcon.fi

Lähteitä

GSMAi, "Mobile Economy Report 2020," 2020. https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf.

ITU, "ITU completes evaluation for global affirmation of IMT-2020 technologies". 26.11.2020. <https://www.itu.int/en/mediacentre/Pages/pr26-2020-evaluation-global-affirmation-imt-2020-5g.aspx>.

ITU, "Focus Group on Technologies for Network 2030". <https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx>.

ITU, "Beyond 5G: What's next for IMT?". 2.2.2021. <https://www.itu.int/en/myitu/News/2021/02/02/09/20/Beyond-5G-IMT-2020-update-new-Recommendation>.

EU, "Hexa-X vision on 6G and research challenges". Horizon 2020. <https://hexa-x.eu/>.

FG-NET2030, "Technical Specification: Network 2030 Architecture Framework". ITU-T, 2020.



Lisätietoja Jyrkin 5G-julkaisuista:
www.amazon.com/author/jype

Y.-C. L. Shanzhi Chen, "Vision, Requirements, and Technology Trend of 6G: How to Tackle the Challenges of System Coverage, Capacity, User Data-Rate and Movement Speed". IEEE Wireless Communications, pp. 1-11, February 2020.

ITU-T, "Network 2030: A Blueprint of Technology, Applications and Market

Drivers Towards the Year 2030 and Beyond". ITU T NET-2030, 2020.

Next G Alliance, "Next G Alliance FAQ". ATIS. <https://nextgalliance.org/about/>.



Teksti ja kuvat: Matti Ruotsalainen

Venäjän elektronisen sodankäynnin joukot 2020-luvulla

Kirjoittaja toimii Maanpuolustuskorkeakoulun, Sotataidon laitoksen, maasotalinjan, sotatieteen kandidaatin ja -maisteri opetusryhmän JOJÄ- ja ELSO-opettajana.

Venäjän federaation asevoimat ovat kehittäneet elektronisen sodankäynnin suorituskykyjään päättäväisesti viimeisten vuosikymmenen ajan. Venäläisten, kansainvälisestikin poikkeuksellisen vahva panostus elektronisen sodankäynnin joukkoihin sekä kalustoon tekee sen tärkeästä mielenkiintoisen, kun arvioidaan kuinka elektronisen sodankäynti voi vaikuttaa tämän päivän taistelulentä. Johtamisjärjestelmien ja niiden joukkojen käytöllä pitää kyetä tukemaan yleisjoukkojen johtamista tulenkäyttöä. Kuinka tämä onnistuu elektronisesti kiistetyssä ympäristössä?

Paikallispataljoonan taistelujohtokeskus siellä jossakin

Paikallispataljoonan taistelujohtokeskuksessa tunnelma on kireä. Yhteys painopistesuunnan yksiköihin on menetetty hetki sitten samalla, kun ensimmäiset ilmoitukset vihollisen joukkojen liikkumisesta paikallispataljoonan vastuualueelle saatiin tiedusteluryhmiltä. Luutnantti Juutilainen, yksi taistelujohtokeskuksen tilanneupseereista laskee kenttäpuhelimien ja ilmoittaa keskuksen päällikölle, kapteeni Ilmajolle ”Esikunta- ja viestikomppanian vikapartiot ovat liikkeellä.

Kaapeliyhteys viestikeskuksesta toiseen jääkärikomppaniaan katkesi, kun epäsuoratuli alkoi kakkosen alueella. Eivät tiedä kuinka kauan kestää.” ”Piru vie!” Ilmajoki mutisi karttaa tuijottaen. Kenttäpuhelin yhteydet poikki, puheradioverkossa kuuluu pelkkää särinää ja yhteenkään toisen tai kolmannen jääkärikomppanian tiedossa oleviin kännykkänumeroihin ei saada yhteyttä. Ilmajoen omassa kännykässä on kyllä kenttää ja vasenta sivustaa suojaavan varusmieskomppanian päällikkö vastaa kyllä puheluihin. Jollain keinolla pitäisi epäsuoraatulla saada kakkosen ja kolmosen käyttöön nyt, kun tykistöpatteristo saatiin pataljoonan alueelle. Ilmajoen katse harhailee tilannekartalta Juutilaisen vieressä istuvaan Virtaseen. Virtanen pyörittelee käsissään yhtä aikaa peitteistöjä, tarkistustunnuksia, kenttäpuhelimia, kännykkää ja radion kuulopuhelinta. ”Herra kapteeni! Meidän oma lennokka on kohta toisen komppanian alueella. Voitte ottaa lennokin videokuvan näkyviin omalle päätteellenne. Lisäksi tykistöpatteristo ilmoitti olevansa ampuvalmiina.” Virtanen kailottaa Savolaismurteellaan. ”Mahtava homma. Virtanen - suuntauta tykistöpatteristo valmiiksi maalipisteeseen VM109. Se on lähellä kakkosen vastuualueenrajaa, siitä on hyvä varmaan aloittaa. Valmistelkaa lisäksi tulikomento – Heti kun saadaan lennokilta kuvaa, niin tulenjohtokomentaja saa alkaa kaataa kaiken liikenevän sinne risteukseen!” Ilmajoki kommentaa ja ottaa lennokin videokuvan auki omalla koneella. ”Tuossa on voimalinja, tuossa pelto - Vielä hetki...” Hän mutisee seuraten videokuva ja tilannekarttaa yhtä aikaa. Samalla hetkellä videokuva vaihtuu mustaksi. ”Ei nyt!” Sadatellen Ilmajoki alkaa tarkistaa koneen kaapeleita ja ohjelman asetuksia. Samassa Virtanen kailottaa puhelimen ääreltä ”Herra kapteeni! Lennokiryhmä ilmoitti, että

yhteys lennokkiin katkesi. Eivät saa enää videota tai ohjaussignaalia.” Ilmajoki taistelee kasvavaa halua vastaan heittää tietokone seinään. Voisiko joku asia vielä mennä huonommin? Kuin vastaukseksi Juutilainen nostaa kätensä puhelin ääreltä. ”No mitä vielä?” Ilmajoki kysyy. ”Tykistöpatteriston alueelle tulee epäsuoraatulla. Tappioista ei vielä tietoa.” Juutilainen toteaa. ”Miten hitossa ne ehtivät löytämään patteriston? Lennokeista ei ole ollut havaintoja ja patteristo ei ole vielä ampunut laukaustakaan eli vastatykistötutkakaan se ei voi olla?” Juutilainen ihmettelee. Ilmajoen mielessä käy paha aavistus samalla, kun hänen katseensa hakeutuu pöydällä olevaan kännykään, joka piippaa viestin merkiksi. Juutilainen poimii kännykän ja lukee ääneen viestin: ”Tiedän missä te olette.” Ilmajoki tajuaa mistä on kyse, kun taistelujohtokeskuksen ulko-ovella oleva vartiomies karjaisee ”Epäsuoraa tulta – Suojaan!”.

Taustat

Tässä artikkelissa tutustutaan Venäjän federaation elektronisen sodankäynnin (ELSO) joukkoihin, kalustoon ja niiden käyttöön, painottuen maavoimien käytössä oleviin elektronisen vaikuttamisen (ELVA) ja elektronisen tiedustelun (ELTI) yksiköihin. Venäjää on käytetty tässä artikkelissa esimerkkinä, koska sillä on prikaati tasolla ELTI- ja ELVA-joukkoja, jota muilla mailla on lähinnä armeija tai armeijakunta tasalla. Tämä luo haasteellisen tilanteen, johon voi verrata omia suorituskykyjä ja toimintatapoja. Lisäksi artikkelissa tarkistellaan tapausesimerkkinä millaista häirintää ukrainalaiset joukot ovat kokeneet vuosien 2014-2017 aikana taistellessaan Itä-Ukrainassa.

Artikkelin materiaali perustuu täysin avoimiin lähteisiin ja ne ovat esitelty artikkelin lopussa. Lähteistä löytyy kaluston tarkempia tietoja ja kuvia, jos kiinnostus aiheeseen herää tekstiä lukiessa. Artikkelissa olevat kuvat ovat kirjoittajan itsensä tekemiä, lähteitä mukaillen.

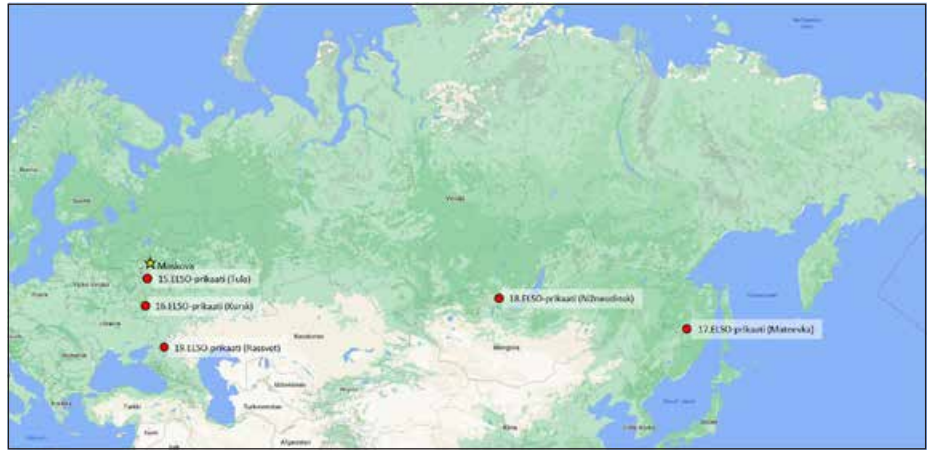
Lähteitä lukiessa pitää muistaa, että osa tiedoista perustuu itse järjestelmiä valmistavien yhtiöiden jakamaan tietoon. Lisäksi itse raporttien kirjoittajat, tai ainakin heidän edustamansa organisaationsa voivat olla osapuolena konfliktissa, josta he itse raportoivat, tavoitteena mahdollisesti suurentaa uhkakuvaa. Lähteisiin pitää siis suhtautua varauksella. Niistä saatavia tietoja voidaan pitää suuntaa-antavina, todellisen suorituskyvyn ollessa jotakin valmistajan kertoman ja radiohorisontin välissä.

Sotilaspiirin ELSO-joukot

Venäjällä elektronisen sodankäynnin joukoilla käsitetään häirintään ja vaikuttamiseen tarkoitettuja joukkoja ja niiden kalustoa. Elektroninen tiedustelu on osa tiedustelua ja sen joukot ovat osa sotilaspiirin sekä joukko-osastojen tiedusteluyksiköitä. Tämä on hyvä muistaa, kun käsitellään Venäjän ELSO-joukkoja.

Tällä hetkellä Venäjän jokaisella sotilaspiirillä on yksi ELSO-prikaati, pois lukien läntinen sotilaspiiri, jolla on kaksi ELSO-prikaatia. Yhteensä Venäjällä on siis viisi ELSO-prikaatia. Kaikki prikaatit on perustettu vuoden 2009 jälkeen, uusin vuonna 2015, osana Venäjän maavoimien uudistusta. Jokaisessa ELSO-prikaatissa on arvioitu olevan kolme tai neljä ELSO-pataljoonaa ja/tai yksi erillinen ELSO-komppania. Yksi prikaatin pataljoonista on tarkoitettu maasijoitettuja järjestelmiä vastaan, yksi pataljoona ilmasijoitettuja järjestelmiä vastaan, yksi avaruuteen sijoitettuja järjestelmiä vastaan ja yksi pataljoona/komppania tukemaan vastavallankumouksellista toimintaa (terrorisminvastaista toimintaa). Nämä prikaatit toimivat ilmeisesti runkona sotilasalueen ELSO-joukkoja perustettaessa ja on sotilasalueen ensivasteen joukko, jos ELSO-suorituskykyä vaaditaan ennen liikekannallepanoa.

Maasijoitettuja järjestelmiä vastaan suunnatun pataljoonan kalustona on ainakin strategisen tason HF-taajuusalueen häirintään tarkoitettu *Murmansk-BN*, joka vilahdanut Suomenkin mediassa. Lisäksi pataljoonalla on matkapuhelimien häirintään tarkoitettu *Leer-3* lennokki. RB-341V "Leer 3" lennokki kykenee häiritsemään 890-915, 935-960, 1710-1765



Venäjän sotilaspiirin elektronisen sodankäynnin prikaatien sijainnit ja numeroinnit.

Taajuusalue		Aallon pituus		Käyttö	
Taajuuden nimi	Taajuus	Aallon pituus	Aallon nimi	Siviili	Sotilas
HF	3-30 Mhz	1-100 m	Dekametri	Radio, laivaliikenteen yhteydet	Taktisen ja strategisen tason radioyhteydet ja niiden avaruusaallot
VHF	30-300 Mhz	1-10 m	Metri	Radio, televisio lähetykset	Taktisen tason radioyhteydet ja pitkän matkan valvontatutkat
UHF	300-3000 Mhz	1-10 dm	Desimetri	Satelliittiyhteydet (SATCOM) ja satelliittipaikannus (GPS)	
				Televisio, GSM, laivaliikenteen yhteydet	Radiolinkit, taktisen tason radioyhteydet, ilmasta-maahan yhteydet ja ohjusvaroitukset järjestelmät
SHF	3-30 Ghz	1-10 cm	Senttimetri	Siviilitutkat	Tutkat (maalinosoitukset ja tulenjohto)
				Satelliittiyhteydet (SATCOM) ja radiolinkit	

HF-SHF taajuusalueet ja niiden käyttö siviili- ja sotilaskäytössä.

ja 1805-1880 MHz alueita, joilla pääosa GSM yhteyksistä toimii. Järjestelmä ilmeisesti kykenee muodostamaan myös valetukiasemia GSM-yhteyksiä varten ja järjestelmän kautta kyetään lähettämään tekstiviestejä sekä soittamaan tukiasemaan liittyneisiin puhelimiin. Kolmantena järjestelmänä pataljoonalla on *Borisevsk-2* järjestelmä, joka on tarkoitettu HF-UHF alueen radioita vastaan. Järjestelmään kuuluvat HF-VHF-UHF alueelle suunnatut häirintäasemat R-378BMV, R-330BMV, R-934BMV, R-325UMV ja RK-330KVM johtoasema. Nämä edustavat ilmeisesti uusinta maavoimien käytössä olevaa häirintäjärjestelmää, jolla kyetään vaikuttamaan myös uusimpiin taajuushyppiviin radioihin.

Ilmasijoitettuja järjestelmiä vastaan suunnatun pataljoonan kalustona on ainakin *R-330ZH "Zhitel"*, jolla voidaan häiritä GSM, GPS, Galileo ja satelliittipuhelinyhteyksiä. Pataljoonalla on lisäksi ilmasijoitettuja tutkia vastaan suunnatut *Krasukha-2* ja *Krasukha-4* järjestelmät. Avaruuteen sijoitettuja järjestelmiä (sa-

telliitteja) vastaan suunnatun pataljoonan kalustosta ei ole juuri tietoja. Niihin kuuluvat ainakin *Krasukha-4*, jota voidaan käyttää matalalla toimivissa satelliitteja vastaan sekä *Tirada-2S*, joka on tarkoitettu satelliitti yhteyksien häirintään. Terroristijärjestelmiä vastaan suunnatun pataljoonan kalustoa ei missään artikkeleissa juuri avata. Voidaan olettaa järjestelmään kuuluvan kaupallisia viestimiä- ja etälaukaistavia pommeja vastaan tarkoitettuja järjestelmiä.

Venäjän merivoimien laivastoilla (neljä) kaikilla on oma ELSO-keskus, pois lukien Tyynenmeren laivastolla, jolla on kaksi keskusta. Näiden ELSO-kykyjä ovat laivoihin asennetut häirintäjärjestelmät. Maahanlaskujoukkojen maahanlaskuprikaateille on organisaatioihin lisätty oma orgaaninen ELSO-komppania 2010-luvulla. Ilmavoimilla on jokaisella sotilaspiirillä oma ELSO-pataljoona, jotka todennäköisesti on tarkoitettu ilmavoimien ilmatorjuntadivisioonien tukemiseen sekä erillisiä häirintähelikopteri- ja lentokone osastoja vastaan.

Moottoroitujen jalkaväkiprikaatien ELSO-joukot

Merkittävä ero ELSO-joukoissa länsimaihin verrattuna on Venäjällä orgaaninen ELSO-komppania osana moottoroitua jalkaväkiprikaattia (MTJVPK), joka on Venäjän pää joukko-osasto tyyppi tällä hetkellä. Länsimaissa millään maalla ei ole ELSO-joukkoja prikaati (yhtymä) tasolla, mutta Venäjällä jokaiselle prikaatille kuuluu oma ELSO-komppaniansa sekä tiedustelupataljoonan kuuluva elektronisen tiedustelun komppania. Prikaati kykenee tukemaan omaa taisteluaan elektronisella vaikuttamisella (ELVA) ja paikantamaan maaleja sekä täydentämään tilannekuvaansa elektronisella tiedustelulla (ELTI). Ainakin osa prikaateista kouluttaa omat ELSO-komppaniansa, joten ainakin osia niistä kyetään kokoamaan osaksi ensivasteen joukkoja, koostuen sopimusosilaista ja varusmiehistä.

Moottoroidun jalkaväkiprikaatin ELSO-komppanian häirintäkyky koostuu:

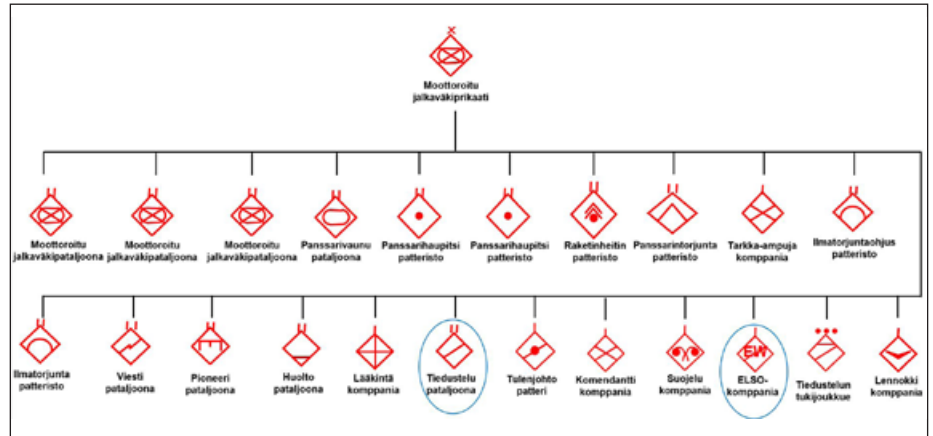
HF-alueen häirintäjoukkueesta, kaksi ryhmää R-378B kalustolla, jotka kykenevät tiedustelemaan ja häiritsemään 1,5-29,9 MHz aluetta.

VHF-alueen häirintäjoukkueesta, neljä ryhmää R-330B kalustolla, jotka kykenevät tiedustelemaan ja häiritsemään 30-100 MHz aluetta.

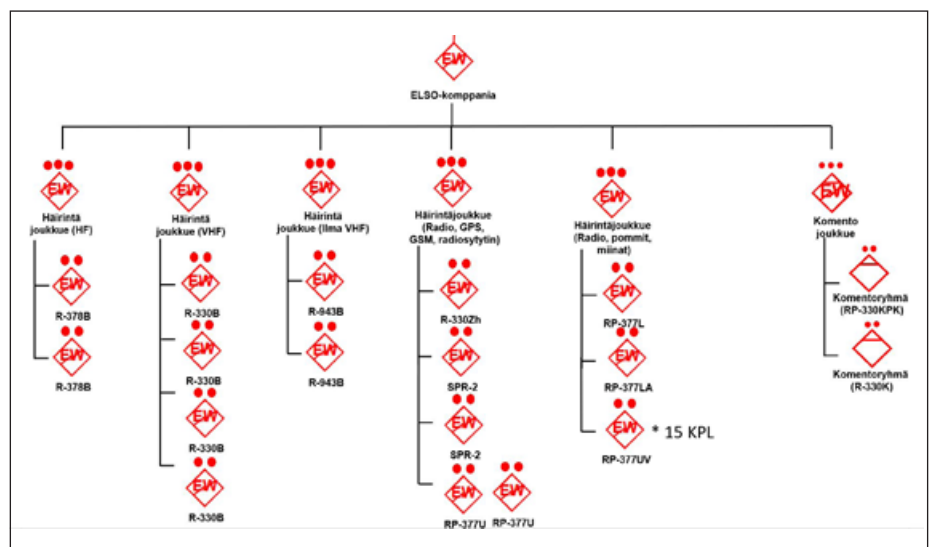
Ilmailu VHF-alueen häirintäjoukkueesta, kaksi ryhmää R-943B kalustolla, jotka kykenevät tiedustelemaan ja häiritsemään 100-399,975 MHz aluetta.

Radio, GPS, GSM ja herätesyöttin alueen häirintäjoukkueesta, jossa on yksi R-330Zh asema, kaksi SPR-2 asemaa ja kaksi RP-377U järjestelmää. R-330Zh ”Zhitel” on SATCOM/GSM/GPS alueen tiedusteluun ja häirintään tarkoitettu asema, joka kykenee tiedustelemaan ja häiritsemään 100 - 2000 MHz aluetta. SPR-2 asemia käytetään epäsuorantulen herätesyöttimen häirintään. Yhdellä asemalla kyetään suojaamaan noin 50 hehtaarin alue. RP-377U on ajoneuvoihin asennettava C-IED (counter IED, Improvised Explosive Device) järjestelmä eli kotimaisittain tunnettu ”jammeri”, joka toimii 20 - 1 000 MHz alueella.

Radioiden, etälaukaistavien pommien ja miinojen häirintäjoukkueesta yhdellä RP-377L ja yhdellä RP-377LA asemalla ja viidellätoista RP-377UV kalustolla. RP-377L on kannettava ja 377LA-ajoneuvoon asennettu järjestelmä, jolla voidaan tiedustella 20 -2000 Mhz ja häiritä 100-500 Mhz taajuusaluetta. RP-377UV



Venäläisen moottoroidun jalkaväkiprikaatin kokoonpano.



Venäläisen moottoroidun jalkaväkiprikaatin ELSO-komppanian kokoonpano ja kalusto.

on kannettava tai ajoneuvoon asennettava häirintäjärjestelmä, jonka taajuusalue on 25-960 MHz.

ELSO-kompanialla on kyky häiritä yleisimpiä sotilaskäytössä olevia komppania- ja pataljoona tason viestilaitteita. Häirintäjoukkueet on jaoteltu taajuusalueen ja toiminnallisuuden kautta. Pääosa tänä päivänä käytössä olevista sotilasradioista toimii HF (3-30 MHz) tai alemman VHF-alueella (30-107,975). Ilmailu VHF-alue sotilaskäytössä on 150-400 MHz ja aluetta käyttävät esimerkiksi ilmatulenjohtajien käyttämät radiot, uudet dataradiot sekä esimerkiksi Suomessa TETRA-verkko. Lisäksi kompanialla on kyky häiritä GSM, GPS, tykistön herätesyöttimiä ja etälaukaistavia miinoja. HF-, VHF- ja ilmailu-VHF-alueen joukkueita käytetään vihollisen johtamisyhteyksien häirintään painopistesuunnassa. Herätesyöttin häirintäjoukkueita käytetään omien tuliasemien ja komento-

paikkojen suojaukseen. Etälaukaistavien pommien ja C-IED häirintäjoukkueilla suojataan marssirivistöjä. GPS- ja GSM-häirintäjoukkueilla lamautetaan nämä yhteydet prikaatin painistealueella.

Prikaatin tiedustelupataljoonaan kuuluu lähteiden mukaan elektronisen tiedustelun komppania, johon kuuluu kolme kuuntelutiedustelujoukkueita ja mittaustiedustelujoukkue. Kuuntelutiedustelujoukkueiden kalustona on R-381T ”Taran” järjestelmä, johon kuuluu seitsemän eri asemaa. Yksi johtoasema R-381T3, neljä VHF-alueen tiedusteluasemia R-381T2, joiden tiedustelualue on 30-100 MHz ja kaksi HF-UHF alueen tiedusteluasemia R-381T1, jotka kykenevät tiedustelemaan HF aluetta, 1,5-30 MHz, ylempää VHF- aluetta 100-400 MHz sekä alemmaa UHF aluetta 300-1000 MHz. Mittaustiedustelujoukkueen kalustona on 85V6 Vega järjestelmä, joka

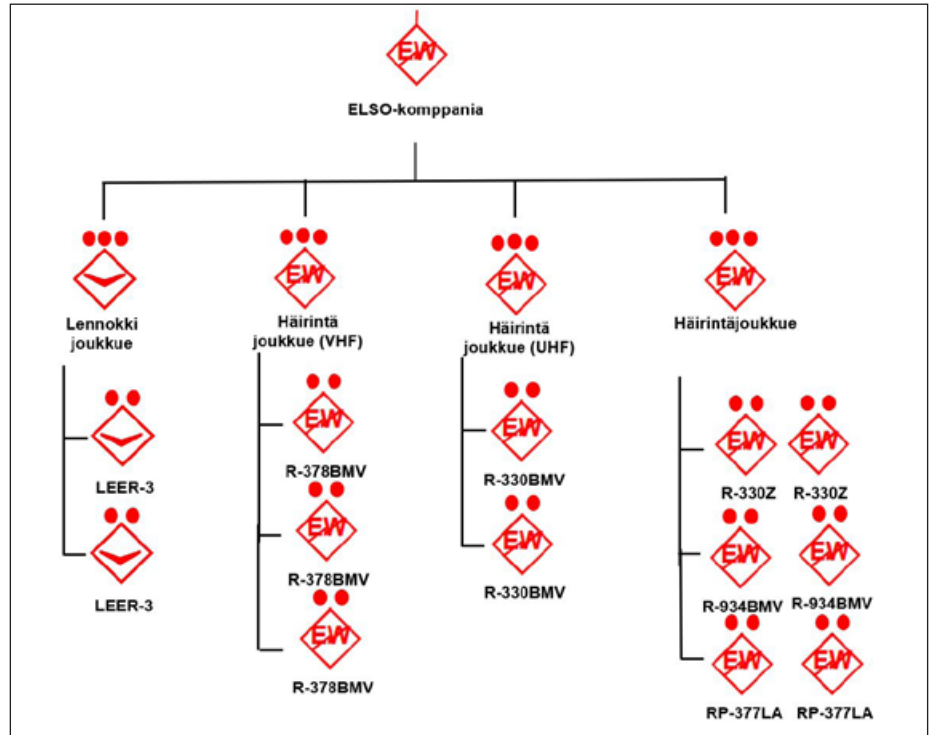
koostuu kolmesta tiedusteluasemasta ja johtoasemasta. Tiedusteluasemat kykenevät tiedustelemaan 0,2-18 GHz aluetta, joita käytetään radiolinkeillä ja erilaisilla tutkilla.

Prikaati kykenee tiedustelemaan 1,5 - 1000 MHz sekä 2000 - 18 000 MHz (0,2-18 GHz) aluetta itsenäisesti ja vaikuttamaan omalla kalustollaan 1,5 - 2000 MHz alueelle. Sen käytössä olevasta kalustosta osa näyttäisi olevan melko vanhaa, osin 90-luvulta asti käytössä ollutta kalustoa. Ukrainan asevoimien tekemässä artikkelissa näkyy kaluston modernisoituja versioita. Ottaen huomioon, että ELSO-joukot ovat olleet kalustohankintojen painopisteessä, niin ainakin osalla prikaateja on käytössä modernisoidut järjestelmät.

Havainnot ELSO-joukkojen käytöstä Ukrainassa

Ukrainassa Separatisteja tukevien ELSO-joukkojen toiminta ajallisesti on jaoteltu ennen taistelua tapahtuvaan ja taisteluiden aikaiseksi toiminnaksi. Tukevana elementtinä on lähteisiin perustuen ollut erillinen ELSO-komppania, jonka kalusto ja organisaatio on esitelty kuvassa viisi. Ennen taisteluiden alkua ELSO:lla ja ELTI:lla on pyritty selvittämään ukrainalaisten johtosuhteet sekä etsimään parhaat sijainnit häirintä- ja tiedusteluasemille. Ajoittaisella häirinnällä on pyritty arvioimaan sen vaikutusta ukrainalaisten eri viestiverkkoihin sekä seurata heidän vastatoimiaan. Lisäksi tällä häirinnällä on pyritty lamauttamaan ukrainalaisten johtamisyhteydet joihinkin omiin taisteluliikkeisiin liittyen, esimerkiksi estämällä tiedustelutiedon jakaminen joukkojen ryhmitysmuutoksista. Tavoitteena ennen taisteluiden alkua on ollut: 1. Paljastaa joukkojen johtosuhteet ja johtamisjärjestelmät. 2. Löytää parhaat häirintätavat, jolla johtamisjärjestelmät saadaan lamautettua. 3. Oppia kuinka ukrainalaisten toimivat, kun yhteydet katkeavat.

Taisteluiden aikana ELSO:lla on pyritty lamauttamaan ukrainaisten johtosuhteet taistelualueella ja estämään ukrainalaisten lennokkien ohjaussignaalien käyttö. Lisäksi ELTI:lla on pyritty paikantamaan radiolähteet, vastapuolen häirintäasemat, vastatykistötutkat sekä ohjata epäsuoraat näiden alueelle. Tavoitteena taisteluiden aikana on ollut: 1. Estää joukkojen johtaminen taistelualueella. 2. Vastatykistötutkien ja häirintäjärjestelmien lamauttaminen epäsuoralla tulella. 3. Estää lennokkien käyttö taistelualueella.



Erillisen ELSO-komppanian kokoonpano ja kalusto Ukrainassa.

Johtopäätökset ELSO:n käytöstä Ukrainasta

Ukrainalaisten käyttämistä johtamisjärjestelmistä tai radioista on hajanaista tietoa. Ilmeisesti pääosa radiosta on Neuvostoliiton aikaisia salaamattomia, ylempään HF ja alemman VHF-alueen kenttäradioita, kenties Suomessakin tuttuja LV623 nimellä toimivia R-123 vaunu-radioita sekä osa Motorolan kaupallisia radioita, joista ainakin osa on toiminut 137-180 MHz ja 400-470 Mhz taajuusalueella. Näitä järjestelmiä ELSO-joukot ovat kyenneet häiritsemään tehokkaasti. Osalla joukoista on ollut länsimaisia Harrisin taajuushyppiviä radioita, joihin häirintä ei ole tehokkaasti toiminut. Joukoilla on ollut paljon erilaista radiokalustoa, jonka yhteensopivuus on ollut huonoa. Ainoa varma, eri radioilla varustettujen joukkojen välinen johtamisyhteys on ollut matkapuhelin.

Ennen hyökkäyksen alkua on pyritty lyhyillä häirintä jaksoilla löytää maasijoitteisille häirintäasemille sopivat paikat, jotta taisteluiden alkaessa tiedetään, että halutut järjestelmät kytetään lamauttamaan. Samalla lyhyillä häirintä jaksoilla on pyritty paljastamaan vastatoimet, väistotaajuudet ja varajärjestelmät. Koska ukrainalaisten varajärjestelmät ovat olleet kännykät, niin samaan aikaan alueella on ollut GSM-alueen tiedusteluun tarkoitettu lennokki, jossa on valetukiasema. Häirintälennokilla ja

maasijoitteisilla häirintäasemilla on häiritty ukrainalaisten matkapuhelinverkon tukiasemia ja pakotettu ukrainalaisten kännykät lennokin valetukiasemaan. Tämän kautta on kyetty selvittämään johtosuhteet ja joukkojen sijainti ennen hyökkäyksen alkua.

Hyökkäyksen alettua, etukäteen tiedustelluista asemista aloitetaan häirintä, jolla radioverkot lamautetaan. Ne matkapuhelimet, jotka tuottavat parhaan tiedustelutiedon annetaan toimia ja muut lamautetaan. Arvokkaiksi tunnistettuihin kohteisiin ohjataan tiedustelulennokki ja se valmistaudutaan tuhoamaan epäsuoralla tulella. Vastapuolen lennokit toiminta pyritään kiittämään häiritsemällä niiden ohjaussignaalia. Vastatykistötutkat paikannetaan elektronisella tiedustelulla ja lamautetaan epäsuoralla tulella.

Ukrainassa havaitut ELSO-järjestelmät ovat lähteiden mukaan osin päivitettyjä versioita alun perin Neuvostoliittolaisista tai Venäläisistä kalustoista, osa on samaa ja osa kokonaan uutta. Päivitysten voidaan olettaa parantavan järjestelmän suorituskykyä esimerkiksi hyppivätaajuisia radioita vastaan, laajentavan käytettävää taajuusaluetta ja mahdollistavan paremman tiedonsiirtokyvyn ELSO-asemien välillä. Kuvista päätellen ainakin osassa asemissa on tiedonsiirtoa varten oma UHF-alueen radiolinkki mastossa, mikä tarkoittaisi, että erillistä viestiasemaa ei tarvita häirintäaseman mukana, mutta toisaalta se rajoittaa asemien ryhmittä-

mistä, koska asemapaikalta pitää myös saada muodostettua yhteys toisiin ase-
miin maasto huomioiden.

Havainnot kalustoista sijoittuvat vuosien 2014-2017 välille, jolloin kalusto on ollut vähintään kenttäkoekäytössä niin pitkällä, että sitä käytetään osana taistelua ja henkilöstö on koulutettu sille. Voidaan olettaa, että ainakin tärkeimmillä joukoilla vastaava kalusto on käytössä ja korvannut tai korvaamassa vanhan kaluston. Jos vastaava kalusto olisi esimerkiksi Venäläisellä MTJVP:llä ja oletetaan organisaation pysyvän samana, niin yhdellä joukkueella voidaan kattaa useampi taajuusalue vanhan ”joukkue per taajuusalue” sijaan ja ELSO-yksiköiden suorituskyky kasvaa merkittävästi. Painopiste on HF-VHF alueella, alemmalla UHF-alueella (>1000 MHz) ja GSM/GPS alueella. Täysin uutena järjestelmänä, joita ei MTJPR:n tasolla lähteiden mukaan ole ollut, on lennokkialustalle rakennettu RB-341V ”Leer 3”. Tämä järjestelmä muodostaa uhkan erityisesti kännyköiden käytölle, joko häiritsemällä niitä, luomalla valetukiaseman tai osoittamalla niihin viestejä ja puheluita. Lennoilla kyetään myös kasvattamaan radiohorisonttia lentämällä korkeammalla ja häirintälähetin saadaan helposti lähelle haluttua kohdetta.

Mitä voimme täällä Suomessa ottaa opiksi Ukrainan havainnoista?

Pelkkiin viestilaitteiden omaan salaukseen tai häirinnän väistämiseen luottaminen ei tee autuaaksi. Elektronisen tiedustelun ja häirinnän väistämisen toimenpiteet pitää osata aina yksittäisen taistelijan tasolla. Sotilaan käsikirjastakin tuttu radionkäyttäjän ELSO-ohje ”Jatka liikennöintiä, vaikka taajuutta häiritään” on artikkeleiden perusteella - Yhä varsin hyvä ohje. Omien järjestelmien ja toimintatapojen pitäminen salassa säteilykiellolla mahdollisimman pitkään on ensiarvoisen tärkeää, jotta tiedustelu ja sen jälkeinen häirintä tai tulivaikutus voidaan välttää. Säteilykieltojen ja rajoitteiden mukaisten, niihin sopivien johtamisvälineiden ja toimintatapojen kehittäminen sekä harjoittelu yhtymä tasolla on erinomainen harjoittelun kohde.

ELSO:n merkitys vastapuolen suorituskykyjen kiistämisessä häirinnällä tulee lähiaikoina vain kasvamaan, kun yhä useamman asejärjestelmän käyttö tulee perustumaan kattavaan tilannekuvaan ja maalinosoitukseen. Vaikka tulenjohtaja näkisi maalin, niin ilman viestiyhteyttä tuliyksikköön ei rautaa saada kohtaamaan lihaa oikeassa paikassa, oikeaan aikaan.

Lähteet:

EW LESSONS LEARNED Russian Hybrid Warfare in Ukraine. Major General Borys Kremenetskyi Defence and Air Attache, Embassy of Ukraine to the UK. 20.3.2019. Слайд 1 (rusi.org)

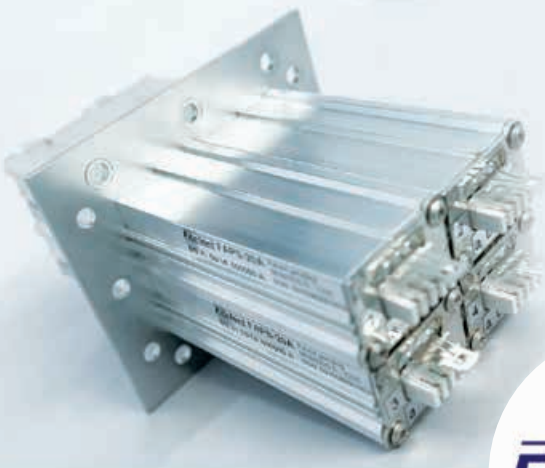
“Russia’s Arms & Technologies: The XXI Century Encyclopedia, Volume 13: Control, Communication and Radio Electronic Warfare System.” 2006. Kustantaja Oruzhie i tekhnologii

“Russia’s Electronic Warfare Capabilities to 2025”. Roger N. McDermot. Republic of Estonia, ministry of defence. Syyskuu 2017. [ICDS Report Russian Electronic Warfare to 2025.pdf](https://icds.ee/reports/Russian_Electronic_Warfare_to_2025.pdf)

“Russia’s Electronic Warfare Capabilities to 2025” – YouTube. Center for Strategic & International studies

“Russian/Soviet/WarPac Ground Based ECM Systems” Air power Australia. [Russian/Soviet/WarPac Ground Based ECM Systems \(ausairpower.net\)](http://ausairpower.net)

“Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces”, Försvarsdepartementet/Ministry of Defence, September 2018. FOIR4625.pdf



FITELNET.FI | MYYNTI@FITELNET.FI

SISÄRADIOVERKOT

VIRVE- ja monioperaattoriverkkojen toteutus luottamuksellisesti avaimet käteen –periaatteella.

EMP/HPM-SUOJAUS

Fitelnet Oy:n suojausratkaisut kriittisten tietoliikennejärjestelmien tehokkaaseen ja luotettavaan suojaamiseen IEMI-uhkia vastaan.

Fitelnet

FITELNET OY, JOUKONTIE 42 A, VANTAA



Teksti: Pekka Heikkinen, Janne Romppainen, Sami Savolainen, Reima Kettunen, Bittium Wireless OY

Kuvat: Bittium

Katsaus eurooppalaiseen aaltomuotokehitykseen (ESSOR)

2000-luvun ensikymmenen puolivälissä muutaman eurooppalaisen johtovaltion kesken, osana tiivistyvää puolustusyhteistyötä ja itsenäisempää toimintakykyä, päätettiin aloittaa yhteiseurooppalaisen taktisen tason aaltomuodon kehittäminen. Uusi nouseva tekninen ratkaisu, ohjelmistoradio, vaikutti mahdollistavan yhteisen ohjelmistolla toteutettavan aaltomuodon siten, että kukin maa voi hyödyntää omaa radiokalustoaan sen käyttämiseksi. Tavoitteiksi asetettiin ilmarajapinnan yli saavutettava yhteensopivuus eri maiden radioiden välillä sekä luotettava datansiirtokyky.

Merkittävä motivaatio hankkeelle oli kehittää ohjelmistoradiotekniikan osaamista Euroopassa, jotta säilytettäisiin tasapuolisempi kilpailuasetelma transatlanttisessa yhteistyössä. Yhdysvaltojen merkittävät panostukset omaan Joint Tactical Radio System (JTRS) -ohjelmaan herättivät mielenkiintoa ja osin huoltakin Euroopassa. Koettiin, että Yhdysvaltojen investoinnit voisivat johtaa tilanteeseen, jossa käytännössä tarjolla olisi vain Yhdysvaltojen kehittämiä ja hallinnoimia aaltomuotoja myös Euroopassa.

Yhtä suuri motivaattori kehitystyön aloittamiselle oli edellisen vuosikymmenen aikana käynnistyneet EU-, YK- ja NATO-johtoiset rauhanturvaamisoperaatiot Euroopan eri osissa, erityisesti entisen Jugoslavian alueella. Operaatioissa havaittiin, että liikkuvan johtamisen ja tilannekuvan jakamisessa osallistuvien maiden kesken oli puutteita radiojärjestelmien yhteensopimattomuuden takia ja tämä vaikutti operaatioiden suunnitteluun ja toteutukseen.

European Secure Software defined Radio eli ESSOR-ohjelma alkoi vuonna 2009 ensimmäisellä vaiheella, jossa tärkeimpänä tavoitteena oli kehittää aaltomuoto edistyneillä viestintäominaisuuksilla koalitiijoukkojen yhteydenotomivuuden saavuttamiseksi. Ohjelman ensimmäisessä vaiheessa määriteltiin, simuloitiin ja toteutettiin uusi MANET-verkko aaltomuoto (ESSOR High Data Rate Waveform, ESSOR HDR



Ryhmä ajoneuvossa.

WF). Aaltomuodon toiminta varmistettiin toteuttamalla se erilaisiin kansallisiin ohjelmistoradioalustoihin sekä suorittamalla yhteentoimivuustestit laboratoriossa 2015. Aaltomuodolle tehtiin lisäksi onnistunut monikansallinen kenttätestaus Riihimäellä 23.11.2016, jossa kolmen ESSOR-ohjelmaan osallistuvan maan (Suomi, Ranska, Italia) radiot toimivat samalla radiokanavalla realistisessa operaatiokehityksessä mahdollistaen yhteisen johtamisen. Muut ohjelmaan ensimmäisessä vaiheessa osallistuneet maat olivat Espanja, Puola ja Ruotsi.

Operatiivista suorituskykyä

Ohjelman toinen vaihe ESSOR OC1 (Operational Capability 1) alkoi vuonna 2018 ja sen tavoitteena on aaltomuodon operatiivisen suorituskyvyn kehittäminen. Kolme tärkeintä suorituskykyä kehittävää toiminnallisuutta ovat radiohiljaisuus, komentoverkkopuhe (pikayhteyshetkely eli Push To Talk, PTT) ja tuki ortogonaalisille verkoille. Lisäksi sopimukseen kuuluu ensimmäisen vaiheen aikana kehitetyn ESSOR-ohjelmistora-

dioarkkitehtuurin dokumentaation julkaiseminen vapaasti saataville sekä ESSOR HDR -aaltomuotospesifikaation julkaiseminen ja ratifiointi NATO:n standardiksi (STANAG/ACoMP) laajakaistaiselle taktisen tason aaltomuodolle. Edelleen OC1-vaiheessa määritellään ESSOR-aaltomuodon elinkaarimalli (Through Life Management - TLM).

Aaltomuodon toteutuksen kansallisiin radioihin tekevät Suomi, Puola, Italia ja Ranska. Kansallisten testien jälkeen suoritetaan yhteiset yhteentoimivuustestit, joissa todennetaan, että aaltomuoto täyttää kaikki sopimusvaatimukset ja yhteistoiminta saavutetaan kaikkien kansallisten radioiden välillä. Tämän vaiheen on määrä alkaa syksyllä 2021.

Konsortio laajenee

Maaliskuussa 2020 tehtiin sopimuslaajennus, jonka myötä Saksa liittyi mukaan ESSOR-ohjelmaan. Sopimuksen mukaan Saksa hankkii samat oikeudet ESSOR-aaltomuotoon kuin alkuperäisillä jäsenmailla on. Näin Saksasta on



Ohjelmistoradiot LV382 ja LV181.

tullut täysivaltainen ESSOR-ohjelman jäsen. Saksan kansallisena teollisuuskumppanina toimii Rohde & Schwarz. Sopimuslaajennuksen puitteissa Rohde & Schwarz toteuttaa ESSOR-aaltomuodon Saksan kansalliseen ohjelmistoradioalustaan (SVFuA). Toteutuksen valmistuttua järjestetään toinen yhteentoimivuudesta teollisuuskumppanien kesken Saksan kansallisen toteutuksen yhteensopivuuden varmistamiseksi.

Saksan mukaantulo lisää konsortion voimavaroja sekä maiden että teollisuuskumppaneiden näkökulmasta. Esimerkiksi Saksan tietoturvaorganisaatio (BSI) tulee tekemään aaltomuodolle tietoturva-arvioinnin RESTRICTED-tasolle, jonka lopputulos ja havainnot saadaan kaikkien ESSOR-maiden käyttöön.

ESSOR OC1 -vaiheen päätyminen siirtyy Saksan liittymisen myötä syksyllä 2021 maaliskuulle 2023.



LV181 kenttämittauksessa.

Projektin tilanne

OC1-vaiheen uusien toiminnallisuuden osalta aaltomuodon määrittelyn ja spesifikaation päivitys valmistuivat vuoden 2019 lopussa. Aaltomuodon yhteinen referenssitoteutus (Base Waveform) valmistui vuoden 2020 syksyllä ja on tätä kirjoitettaessa viimeisessä tilaajan hyväksyntäprosessissa. Lisäksi ESSOR-arkkitehtuurin dokumentaatio on julkaistu OCCAR:n nettisivustolla (<http://www.occar.int/programmes/essor>, Expert Area).

Aaltomuodon toteuttaminen kansallisiin alustoihin alkoi rinnan yhteisen referenssitoteutuksen verifoinnin kanssa. Ensimmäiset kansalliset hyväksyntätestit valmistuvat kevään 2021 aikana, Suomen ollessa tässä eturintamassa. Yhteistoimintatestien on tällä hetkellä arvioitu alkavan syksyllä 2021 koronapandemias- ta aiheutuneista hankaluuksista huolimatta. Hyväksyntätestit perustuvat yhteisesti määriteltäviin testitapauksiin ja yhteiseen testiympäristöön. Kunkin kansallisen toimijan tulee läpäistä testit ensin kansallisesti ennen osallistumista yhteisiin testeihin.

Suomen kansallisena radioalustana ESSOR OC1 -ohjelman yhteistoimintatesteissä käytetään Bittiumin kehittämää Lähiradiota LV181 (tuotenimi: Bittium Tough SDR Handheld™), johon ESSOR OC1 -aaltomuoto on toteutettu. Lisäksi kansallisesti ESSOR OC1 -aaltomuoto toteutetaan samanaikaisesti myös Ajoneuvoradioon LV382 (Bittium Tough SDR Vehicular™). Työ on edistynyt haastavista ajoista huolimatta erinomaisesti ja konsortion ensimmäinen PTT-puhelu soitettiin syksyllä 2020 Bittiumin Kajaanin testiympäristössä. Ensimmäiset kenttämittaukset on myös jo tehty ja tulokset suorituskyvystä ovat lupaavia. Esimerkiksi PTT-puhelu parantaa käytettävyyttä merkittävästi verrattuna aiemmin käytettyyn VoIP-puheluun.

ESSOR-aaltomuotospesifikaatio on päivitetty NATO:n STANAG-prosessin mukaiseksi ja dokumentaatio on toimitettu tilaajalle ja ESSOR-ohjelman osallistujamaille katselmoitavak-

si. ESSOR-maiden tavoitteena on toimittaa hyväksytty spesifikaatio NATO:n standardointiprosessiin. Näin aaltomuoto voitaisiin myös saada osaksi NATO:n operaatioverkko- ja toimintakonseptia (Federated Mission Networking, FMN).

ESSOR OC1 -vaihe pitää sisällään myös ohjelman seuraavaan vaiheeseen tähtäävän Through Life Management (TLM) työkokonaisuuden, jossa tutkitaan mahdollisia uusia ominaisuuksia aaltomuotoon sekä kehitetään aaltomuodon ylläpitoprosessia. Työpaketti valmistuu kesäkuussa 2021 ja sisältää muun muassa mallinnustyökalun tulevien aaltomuoto-ominaisuuksien toteutuksen vaikeusasteen, aikataulun ja kustannusten arvioimiseksi.

Euroopan tiivistyvä yhteistyö

ESSOR-ohjelma on yksi eurooppalaisista lippulaivoista Euroopan Unionin pysyvän rakenteellisen yhteistyön (Permanent Structured Co-operation, PESCO) hankkeissa. Euroopan unionin sopimuksen 46 artiklat 42.7 ja 42.6 sekä pöytäkirja 10 luovat puitteet rakenteelliselle yhteistyölle, jossa keskitytään vahvistamaan eurooppalaista puolustusalan teollisuus-, tutkimus- ja kehitysyhteistyötä.

ESSOR-ohjelmaan on tulossa laajennus tämän vuoden kuluessa, jolloin Euroopan puolustusteollisen kehittämisohjelman (European Defence Industrial Development Programme, EDIDP) käynnistettyä aloitetaan uusien koalition aaltomuotojen määrittely ja kehittäminen sekä tiivistetään eurooppalaisen puolustusteollisuuden yhteistyötä ohjelman tavoitteiden mukaisesti.

ESSOR-ohjelman muodostaa kuuden valtion puolustusministeriöt: Suomi, Ranska, Saksa, Italia, Puola ja Espanja. Tilaajan puolelta ohjelmaa johtaa Conjointe de Coopération en Matière d'Armement (OCCAR), jonka tehtävä on hallinnoida eurooppalaisia puolustusalan yhteishankkeita.

Teollisuuskumppaneiden puolelta hanketta hallinnoi Alliance for ESSOR -konsortio (a4ESSOR), jonka muodostavat Bittium, Indra, Leonardo, Radmor, Rohde & Schwarz ja Thales. A4ESSOR on rekisteröity Ranskaan ja sen toimipaikka on Pariisi.

Kansallinen käyttö

Vaikka eurooppalaisella tasolla ESSOR-ohjelmassa luodaan kykyä johtaa monikansallisten operaatioiden taktista



Työryhmä testitoiminnassa.



ESSOR testityöryhmä.

toimintaa ja jakaa tilannekuvaa radioverkkojen avulla, soveltuisi aaltomuoto hyvin myös kansalliseen käyttöön. Aaltomuoto mahdollistaa luotettavan puheen ja datan siirron rinnakkain samassa verkossa johtamisen ja tilannekuvan jakamiseksi käyttäjien kesken. IP-pohjainen tiedonsiirto ja PTT-puhe rakenteetomassa MANET-verkossa luovat kyvyn muodostaa komentoverkkoja ja muita taktisen tasan tiedonsiirtorakenteita, joihin perinteiset digitaaliset kenttäradiot eivät kykene. Tiedon käsittelyn alati

jatkuva automatisoituminen, näennäisesti irrallisten tietohippujen yhdistäminen osaksi tilannekuvaa, robotisaatio, miehitämättömät järjestelmät, sensoriverkot, tekoäly sekä ELSO-suorituskyvyn jatkuvan parantamisen tarve asettavat perusteet muutokselle. ESSOR-aaltomuoto ja moderni laajakaistainen radioalusta voivat olla suurempi suorituskyvyn lisäys komentoverkkoihin kuin radiolinkeistä ja televerkoista muodostetun taktisen rungon muutos MANET-rakenteisiin IP-verkkoihin viime vuosikymmenellä.



Teksti: Harri Suokko

Kuvat: Pohjanmaan Viesti-kilta

Ajatuksia Viestikiltojen toiminnan kehittämisestä

Tulin valituksi Pohjanmaan viestikillan hallitukseen 2019, ja vuoden 2021 alusta minut valittiin killan puheenjohtajaksi, josta tietysti kiitos syyskokouksen osallistujille. Olen ollut killan jäsenenä omien laskujeni mukaan jo yli kymmenkunta vuotta. Alun perin lähdin mukaan työkaverin haastamana, joka ilmeisesti oli ollut mukana killan toiminnassa jo hieman pidempään. Rivijäsenenä osallistuin lähinnä vuosikokouksiin ja yksittäisiin tapahtumiin sen mitä työltäni ehdin. Ilmeisesti pätevyys hallitustehtäviin tuli lopulta iän mukana.

Uutena puheenjohtajana tulee katsottua ensin kokonaistilannetta, ihan kuin aloittaisi yrityksessä uutena toimitusjohtajana. Yleensä tarkistan, mikä olikaan toiminnan tarkoitus. Viestikillan säännöissä kerrotaan tarkoitukseksi vapaasti lyhennettynä: Killan tarkoitus on edistää vapaaehtoista maanpuolustustyötä ja lisätä maanpuolustustahtoa, sekä toimia viestitehtävissä palvelevien ja palvelleiden jäsenten ja veteraanien tukena, sekä kehittää yhteistoimintaa muiden vastaavien järjestöjen kanssa. Myös perinteiden ja historia vaaliminen on koettu tärkeäksi.

Jäsenhankinnan haasteet

Hyvin on killan tarkoitus kuvattu, joten seuraavaksi tulee mieleen, että miten näin hyvään tarkoitukseen on niin haastavaa löytää uusia killan jäseniä. Jäsenmäärä kun näyttää olleen ollut vähenevä jo monen vuoden ajan.

Paria potentiaalista uutta jäsentä olen ohimennen haastatellut, ja kuva alkaa selkeytyä. Potentiaaliset killan uudet jäsenet, eli esimerkiksi ne henkilöt, jotka ovat juuri varusmiespalveluksensa suorittaneet, suhtautuvat maanpuolustukseen hieman eri tavalla kuin me, joiden vanhemmat tai isovanhemmat kokivat talvi/jatkosodan.

Parhaan tuntuman olen saanut nykyi-
kaan omia poikia (25v ja 30v) haastat-
telemalla ja muistelemalla, mitä pojat
aikoinaan omasta intin käynnistään
kertoivat, sen aikana ja jälkikäteen. Eivät
ole muuten vielä saaneet yhtäkään kerta-
usharjoituskutsua, joka taitaa olla yksi
juurisyy maanpuolustusasioissa passivoi-
tumiseen. Verkossa toki ovat pelanneet
tietokoneillaan ja mielikuvat maanpuo-
lustuksesta eri muodoissa taitavat olla
enemmän pelikokemusten ja intin jälkeen
kavereiden kanssa käytyjen tarinoiden
kautta muodostuneita.

Itsekin muistan aikoinaan kiinnostuneeni
tämä kiltatoiminnasta jonkin kertaushar-
joituksen yhteydessä siten, että samassa
tilaisuudessa mukana ollut killan jäsen
kertoi porukasta, joka sen muodostaa,
sekä killan tarkoituksesta. Osa killan
jäsenistä oli työn puolesta vanhoja tuttuja
ja jäsenmaksukin pieni, joten jäseneksi
liityin ja osallistuin satunnaisesti tapah-
tumiin.

Maanpuolustushenki

Maanpuolustushenki on kaikesta huo-
limatta Suomessa vahva, se vaan tulee
nuoremmissa esiin eri tavoilla kuin mihin
itse olen tottunut. Positiivinen yllätys oli
se, miten paljon varusmiespalvelus on
kehittynyt 1980 luvusta tähän päivään.
Sain itse tilaisuuden tutustua nykyaikai-
seen varusmiespalvelukseen osallistues-
sani maanpuolustuskurssille syksyllä
2017. Paljon oli karsittu aikoinaan tur-
haksi kokemiani asioita ja keskitytty
paremmin olennaiseen, eli oman tehtä-
vään ja sen osaamiseen. Hyvä pohja on
siis olemassa killan kehittämiseksi tämän
uuden sukupolven varaan.

Miten siis aktivoida tämä uusi sukupolvi
mukaan kiltatoimintaan?

Oma johtopäätökseni kaiken tähän men-
nessä keräämäni tiedon perusteella on,



Pohjanmaan Viestikillan logo.

että todennäköisesti Killan pitää kertoa
enemmän itsestään ja toiminnastaan
nykyisen jäsenistön ulkopuolelle. Pitää
siis mennä sinne missä viestitehtävissä
olevat, mutta kiltaan kuulumattomat ih-
miset kokoontuvat, eli tapaamaan varus-
miespalvelustaan suorittavia tai vaikkapa
kertausharjoituksiin osallistujia, ja sen
lisäksi pitää osallistua aktiivisesti tai jopa
järjestää erilaisia tapahtumia verkossa.
Tapahtumat verkossa, kun mahdollistavat
isonkin porukan kokoontumisen kes-
kustelemaan jostain mielenkiintoisesta
aiheesta ja kiinnostusta herättävien esiin-
tymien hankkimisen mukaan tapahtumaan
pitkänkin matkan päästä. Sen lisäksi
meidän pitää harkita killan nimissä kir-
joittelua ja viestintää verkkoympäristössä
aktiivisilla keskustelufoorumeilla tai
sosiaalisessa mediassa, ehkä jopa osal-
listumista verkkopelaamisen tapahtumiin
vaikkapa killan omalla tiimillä. Lisäksi
olen miettinyt, että viestitehtävissä ole-
vien henkilöiden tukeminen neuvoilla on
varmasti paikallaan ja verkossa kerro-
tuilla hyvillä tarinoilla sekä vastauksilla

verkossa nousseisiin kysymyksiin on oma osallistujajoukkonsa. Eli käytännössä olemalla paljon enemmän mukana nykypäivän yhteisöllisessä toiminnassa. Fyysiset kohtaamiset kun ovat muuttuneet erityisiksi juhlatapahtumiksi, joita voidaan jatkaa sitten kun pandemiarajoitukset lopulta ne sallivat.

Mitä jatkossa

Näistä kiltatoiminnan uusista jäsenhankinnan toimenpiteistä ajattelin itse keskustella Pohjanmaan Viestikillan hallituksessa, ja suosittelem samaa muillekin jäsenhankintaansa miettiville. Toiminnan tarkoitusta ei siis tarvitse muuttaa, mutta toimenpiteet pitää sovittaa tilanteeseen ja kohdata potentiaaliset uudet killan jäsenet myös uusilla tavoilla.

Oikein hyvää kesää kaikille Viestimies-lehden lukijoille.
Muistattehan ottaa rokotuksen, sitten kun oma vuoronne tulee.

Harri Suokko

Pohjanmaan Viestikilta, puheenjohtaja. Päätyössäni olen teleoperaattori Länsilinkki Oy:n toimitusjohtaja.

Koulutukseni on tietokonetekniikan insinööri ja sotilasarsenaltani olen reservin kapteeni. Varusmiespalveluksen suoritin 80-luvun alussa Niinisalossa. Maapuolustuskurssi 223.



Viestikillan lippu.

VARMISTAMME LIIKETOIMINTASI JATKUVUUDEN DIGITAALISESSA MURROKSESSA

Huolehdimme koko digitaalisesta ekosysteemistäsi, ja yksinkertaistamme prosessisi kustannustehokkaasti, skaalautuvasti ja tietoturvalisesti.

www.teliacygate.fi



Text: *Major General (rtd.) Henrik Røboe Dam is the former head of the Royal Danish Air Force and a Director at Systematic.*

Pictures: Systematic

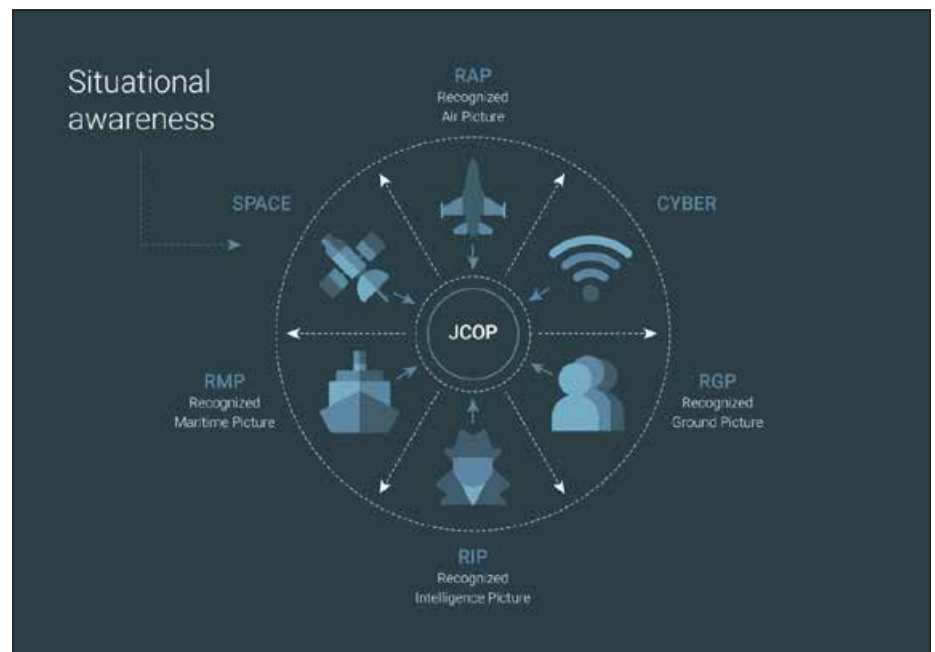
C2 for a new paradigm: addressing the challenges of multi-domain warfare

Militaries have been preparing for multi-domain operations (MDO) for some time - shifting their focus from Counter Insurgency operations to address peer and near-peer threats. However, the challenge has broadened significantly with the increased emphasis on the cyber and space domains alongside the traditional land, air, and sea mix, and now a greater dependency and significant growth in users of the electromagnetic spectrum as yet another domain for consideration.

Added to the difficulties facing many militaries are a host of other low-intensity and asymmetric threats, and non-combat tasks, where even non-state adversaries have the freedom of manoeuvre between multiple domains.

Modern operations are typically coalition endeavours and members often bring Joint capabilities to the fight. Interoperability – and indeed intraoperability – will be a determining factor in a multi-domain conflict, where speed of action is of paramount importance and information sharing is essential to enable effects from across a coalition to be brought to bear.

It is here that C2 systems that support interoperability between coalition partners can bring significant benefits, indeed, enabling partner forces to work together – no matter what C2 system and communications standards are used – can be a force multiplier.



Visualising the operating picture in different domains – such as the airspace – and making this available to commanders across the battlespace enables them to gain a comprehensive and clear understanding of an area of operations, improving situational awareness and speeding up decision making. (credit Systematic)

Systematic's SitaWare software is an example of a system that enables interoperability, with users able to exchange tracks, plans/orders, and messages in a wide range of formats, including APP-11, OTH-Gold, AIS, USMTF, Link 16, ADS-B, NFFI, and MIP, among many others. Furthermore, the software supports the exchange of critical information with users of different C2 systems.

Multinational exercises

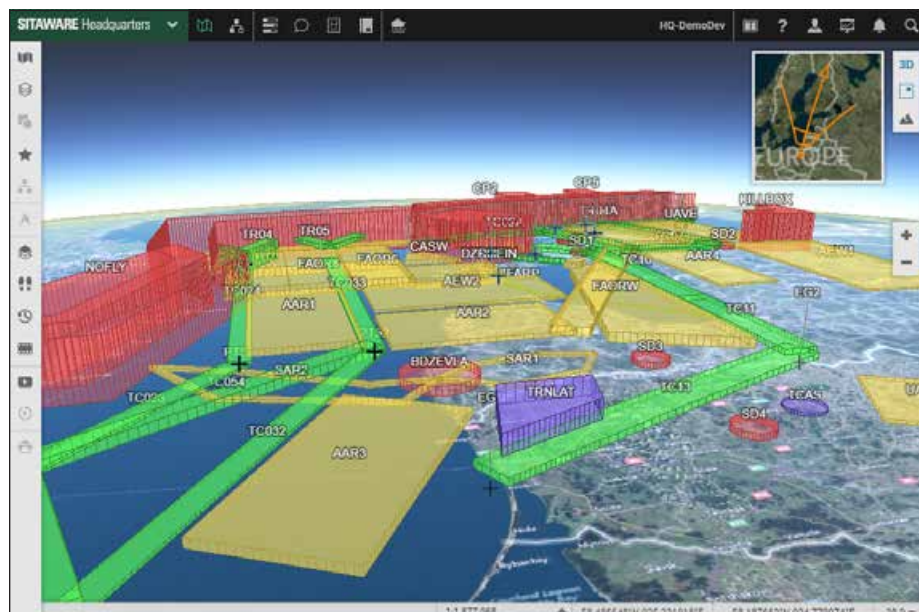
Interoperability and Joint operations are increasingly becoming key features of exercises, and these are essential for the development of capabilities and doctrine for multi-domain warfare. While the full range of systems envisaged for multi-domain warfare are not yet in service, tactics, techniques, and procedures can be worked on, albeit in a limited manner and not at large scale. Militaries cannot wait for legacy systems to be phased out in their entirety and future capabilities brought online, the development of best practice must take place alongside the development and fielding of systems and many exercises include aspects that enable this to take place.

In late 2020 SitaWare Headquarters was used at UK Standing Joint Force Headquarters' (SJFHQ's) Exercise JOINT QUEST, where the software delivered a range of decision support and planning functions and a multi-domain Joint Common Operational Picture (JCOP).

At the exercise SJFHQ planners employed an innovative Joint operational planning capability to prepare a synchronised, multi-domain, multinational plan combining defence and partner organisations across government and with allies.

The objectives of JOINT QUEST included understanding the role and application of a strategic-level operational headquarters in a multi-domain environment – air, land, maritime, space, cyber, and electromagnetic – and specifically how to achieve 'information advantage', described by SJFHQ as the ability to outmanoeuvre adversaries in the information age.

Most recently, Warfighter 21-4 (WFX 21-4) tested the ability of a US Army Corps to plan and lead a largescale multinational operation. The scenario for the event was a coalition of US, British, and French forces undertake a high-intensity mission, with operations across domains, including space and cyber.



For multi-domain operations commanders will require a common operational picture that incorporates the full spectrum of modern warfare.
(credit Systematic)

For the exercise, the British Army's 3rd Division utilised SitaWare Headquarters command-and-control software, while the US Army's III Corps employed the SitaWare Headquarters-based Command Post Computing Environment (CPCE) as their mission command system.

Doctrine development

In addition to using the most effective C2 systems and technologies available, militaries should assess where doctrinal changes are necessary for multi-domain operations. A far greater emphasis must be placed on localised decision making based on the commander's intent, rather than direct orders. The idea of 'democratising' decision making is not new, but the extent to which MDO will demand the decentralised execution of the mission is far greater than before, the speed of action required in a conflict with a near-peer or peer means that in the time taken for battlefield commanders to seek approval from higher echelons the fight may have already moved on, or worse still, been lost.

If intent is established and well defined at higher levels of command, subordinates can be empowered to execute missions knowing that they are operating freely within the parameters that have been set, and are employing effectors that have been approved and allocated to them – or

they at least have been given access to. They will then only be required to seek approval or guidance if they are looking to make decisions outside of the established framework and/or matrix. This freedom will be essential in enabling missions to be conducted at speed and also when operating in environments where there may be degraded communications due to enemy action, which it is universally accepted will be the case in a conflict with a peer or near-peer adversary.

Achieving seamless operation between partners and across domains also demands that commanders have the ability to 'reach' outside of their silos to access and share relevant information, furthermore this can enhance combat effectiveness. The decision-making process of a ground component commander, for example, could be greatly enhanced if they have a broader understanding of the supporting assets that they may need as their mission unfolds, such as fires or CAS, and an awareness of the overall operational picture. While at present this information may be available to them via command channels, at lower echelons they are less likely to have the direct access that could bring the greatest benefit. The challenge is one of information management and lies in deciding what level of access commanders are granted and ensuring that the right information hits the right commander at the right time.

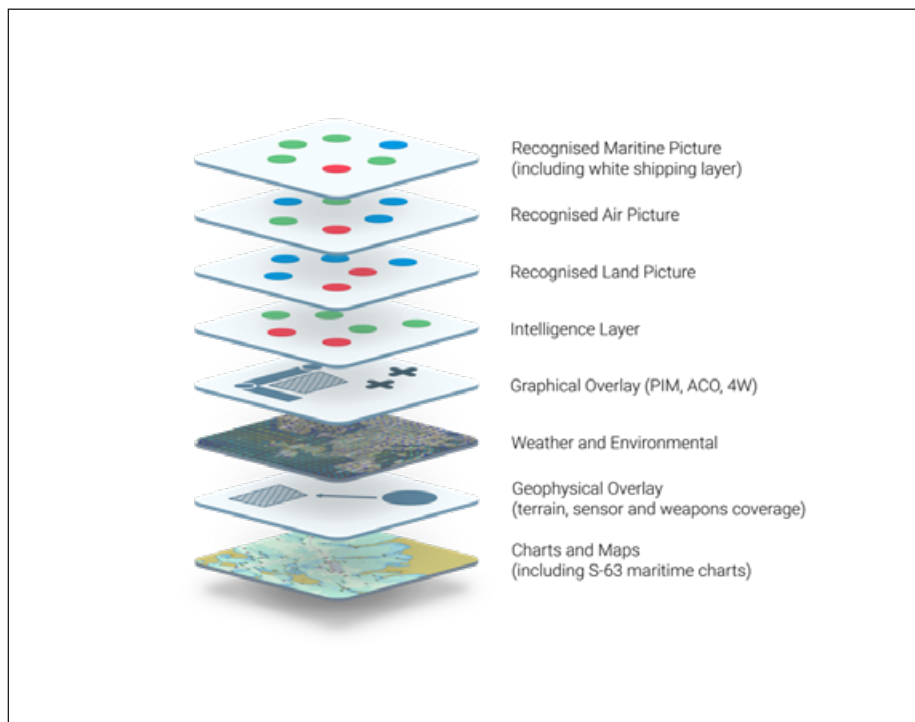
A further aspect that must be considered in flattening command structures and empowering decision-making and mission execution at lower echelons is that of security, and there is no 'silver bullet' to solve this problem. At times commanders will require quick access to information beyond their security level – whether within their own silo or across silos – enabling this without compromising security is a significant challenge and has the potential to be a stumbling block in streamlining C2. Moving from 'need to know' to 'need to share' is a huge undertaking and requires not only technical solutions, but also a major change in the traditional mind-set.

Complex operational picture

The one constant for commanders, no matter what the mission, is the need for comprehensive situational awareness via an effective COP. Ultimately, at the theatre level – and even before – the COP available to commanders will inherently be multi-domain in nature and be composed of information from across the full spectrum of warfare, with elements including the recognised air, land, and maritime pictures, intelligence layers, Cyber and Space information, weather and environmental information, geophysical overlays, and a variety of maps and charts, among other information.

Building a COP for multi-domain C2 is no mean feat, the sheer volume and diversity of data available on the modern battlespace has the potential to overwhelm resources and cannot be handled by simply scaling-up manpower. Processing the source data is a significant task and, in an attempt, to overcome this challenge many militaries have already started to apply advanced technologies, such as artificial intelligence, which is going some way to automating processes and removing burden from analysts and other personnel.

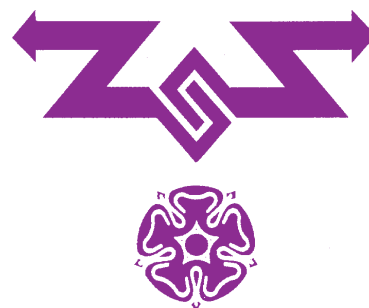
Modular designs and open architectures bring further utility to commanders conducting multi-domain operations and who, as noted, will draw on a wealth of data in developing a COP and informing command decisions. Simplifying the integration of third-party applications, tools, and information, enables operators to quickly introduce other capabilities into a C2 system and make them readily accessible. Additionally, the provision of a software development kit enables customers and third parties to build extensions that facilitate the integration of other systems or develop bespoke applications.

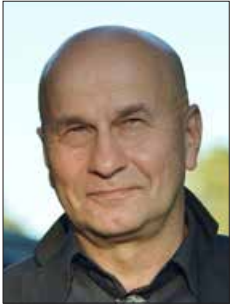


Building an operational picture in layers of information will enable commanders to tailor and filter the information that they want to see at any time, providing a clear understanding of the battlespace. (credit Systematic)

Operators are increasingly demanding the ability to tailor C2 software to meet their individual requirements, and much success has been achieved through the integration of bespoke and third-party applications. For example, the US Army's CPCE features a number of extensions and applications, and a number of SitaWare users integrated civilian applications as they used the software to help in their response to the Coronavirus pandemic.

Multi-domain warfare is a more complicated construct than militaries have had to address before, and there is little real-world experience to draw upon in developing the necessary capabilities and doctrine. There is a prevailing sentiment that in the contemporary operating environment 'a conflict anywhere will be a conflict everywhere'. While, this is most pertinent when facing a peer or near-peer adversary, even non-state actors can project force across domains and at distance, as such, for an MDO militaries must be prepared for all known threats – and ready themselves to respond to those that have yet to emerge.





Teksti: Tapio Teittinen

Kuvat: Tapio Teittinen, SA-kuva

Maailmanluokan sotahistoriakohteen nousu ja tuho

Päämajan Viestikeskus Lokin entisöinti nousi esiin ensimmäistä kertaa jo vuonna 1974 kun Päämajamuseo avattiin Mikkelissä. Lokki oli oleellinen toiminnallinen osa Päämajaa. Luolatilasta oli päässyt kuitenkin pahasti rapistumaan, jolloin työmäärä ja kustannukset vaikuttivat liian suurilta.

12.3.1991 sai Kaakkois-Suomen Viestikilta ry tehtäväkseen aloittaa Lokin entisöintiin tähtäävät toimenpiteet, tuekseen kiltta sai jo tuossa vaiheessa Mikkelissä toimivien teleyritysten sekä puolustusvoimien viestiaselajin tuen viestitarkastaja, eversti Kalevi Markkulan johdolla.

Lokin luolatilasta kerättiin kaapeleita, valaisimia ja muuta alkuperäistä materiaalia talteen kyllä jäsenistön toimenpitein. Luolassa olleet parakit olivat romahtaneet ja lahonneet. Siellä piti liikkua kypärä päässä ja vahvapohjaiset saappaat jalassa.

Ikävänä lisänä ilmeni se, että luolastossa oli asbestia. Hätiin tuli Puolustusministeriö, joka kustansi ulkopuolisen urakoitsijan tyhjentämään luolaston. Uudelleen rakennettavaan Lokkiin tarvittiin runsaasti varoja. Tämän johdosta käynnistettiin valtakunnallinen keräys, jonka tulokseen vaikuttivat myös kyllä kumppaneina olevat viestiaselajin maanpuolustusjärjestöt kuten Viestisäätiö ja Viestiupseeriyhdistys. Lahjoituksia saatiin niin teleyrityksiltä kuin elektroniikkateollisuudeltakin. Paikalliset yrittäjät lahjoittivat rakennusmateriaaleja. Mikkelin lääninhallitus ja Mikkelin kaupunki tukivat projektia siten, että parakin rakentamiseen saatiin myös työllistämisvaroja.

Laitteita saatiin Viestimuseolta, Teleltä, LM Ericssonilta sekä yksityisiltä lahjoittajilta. Toiminnasta kerättiin tietoja Lokissa palvelleita lotilta. Museointisuunnitelman laati filosofian maisteri Pia Puntanen.

Päämajan viestikeskus Lokki avattiin



Hamid Al-Sammarraee kuvaa Lokin keskusta.

4.12.1995. Avaajana toimi puolustusministeri Anneli Taina. Kunniavieraina olivat mm. maaherra Juhani Kortessalmi, kaupunginjohtaja Myllyvirta, kenraaliluutnantti Penttinen ja viestiaselajin everstit Jarmo Myyrä ja Seppo Uro. Suuren työn tehneet Kauko Salo ja Juhani Pasanen saivat huokausta helpotuksesta Lokin viimein valmistuttua.

Päämajan viestikeskus Lokki on maailmanluokan harvinaisuus. Toisen maailmansodan armeijoiden ylijohdon viestikeskuksia on kunnostettu näyttelytiloiksi vain Englannissa ja Suomessa. Viestikeskus Lokki on ollut yleisölle auki kesäisin ja tilauksesta. Lokissa kävi heti avaamisensa jälkeen 90-luvulla noin 10 000 vierailijaa vuodessa ja myöhemmin vierailijamäärä on ollut keskimäärin 7 400 vierailijaa vuodessa. Erityisesti ulkomaalaiset turistit ovat olleet kiinnostuneita Lokista.

Päämajan viestikeskus Lokin kattotilan osalta vapaiden tilojen ”rusnausta” eli kolistelua on suoritettu tilojen turvalli-

suuden takaamiseksi. Tällä kertaa tyhjän luolan katosta putosi arviolta noin 800 kg painava lohkar. ”Rusnausta” toteutaneen yrityksen Power Mining Oy:n edustajan mielestä luolaston seinät ja katto ovat rapautuneet huolestuttavasti ja luolastossa kiven laatu on huono. Varsinaisen viestikeskus Lokin kattoa ei päästy tutkimaan, koska kyseiseen parakin ja luolan katon väliseen tilaan ei pääse.

Käytännössä tämä tarkoittaa sitä, että Lokin kunnostamiseksi on koko näyttely ja parakki purettava, kalliota käsiteltävä joko betonoimalla tai muulla tukirakenteella ja Lokki on rakennettava kokonaan uudestaan. Sitä ennen on Lokkiin vierailta pääsy kielletty. Jos tällaiseen perusteelliseen korjaukseen päästään, niin se tulee maksamaan satoja tuhansia euroja.

Kaakkois-Suomen Viestikilta päätti tuottaa Lokista dokumenttifilmin, jossa kerrotaan Lokin alkuperäisestä rakentamisesta, toiminnasta Jatkosodan aikana, Lokin tuhoutumisesta ja uudelleen rakentamisesta. Tämän filmin avulla Lokin

historiaa ja rakenteita ja laitteita voidaan esitellä, vaikka itse tiloihin ei vuosi-kausiin pääsisi. Filmin taloudellisena päätukijana toimii kiltamme kunniajäsen Pellervo Pekkola, filmin kuvauksesta ja editoinnista vastaa Hamid Al-Sammarrae *3heditoinnista*. Kertojaäänenä toimii Mikkelin Teatterin näyttelijä Aapo Oranen. Käsikirjoituksen on tehnyt killan puheenjohtaja Tapio Teittinen. Filmistä tulee noin puoli tuntia pitkä ja siitä tehdään myös lyhytversio Päämajamuseon/Muistin vierailijoita varten.

Kaakkois-Suomen Viestikilta tekee yhdessä Päämajamuseon ja Muistin kanssa Lokkia esittelevän näyttelyn Päämajamuseon/Muistin tiloihin. Tämä näyttely tehdään yhteistyönä ja kiltamme puolelta siinä ovat suunnittelijoina Martti Susitaival ja Tapio Teittinen. Maanpuolustuksen Viestisäätiö on antanut apurahan tämän näyttelyn pystytystyöhön. Käytännön töihin tarvitaan aikanaan paljon killan jäsenten tukea näyttelyn pystytyksen yhteydessä mm. kaluston siirrossa Lokista museotiloihin.



Kenraali Penttinen ja everstit Myyrä ja Uro.



Lokin luolaston katosta pudonnut lohokare.

**Height/
Max. topload**

- 20m**
50kg
- 12m**
200kg
- 6m**
350kg
- 3m**
400kg

SkyHigh

– NEW VEHICLE MAST

- 20 m unguyed telescopic composite mast
- raising heavy payloads up to 600 kg
- deployable to 20 m in less than 2 minutes
- several vehicle mounting options
- intelligent diagnostics and operation options
- compact footprint
- minimal and easy maintenance thanks to modular construction



Mastsystem Int'l Oy

Telescopic Composite Mast Systems from Finland

T: +358 20 775 0810



Teksti ja kuvat: Pertti Hyvärinen, Eversti evp

Vapaaehtoinen maanpuolustus kyberturvallisuuden kansallisessa kehittämisessä

Kirjoittaja on Viestiupseeriyhdistyksen varapuheenjohtaja ja on toiminut Viestimies-lehden päätoimittajana vuosina 1999-2002. Tällä hetkellä hän toimii Cinia Oy:ssä liiketoiminnan kehitysjohdajana.

Viestiupseeriyhdistys järjesti 20.5.2021 webinaarin teeman Vapaaehtoinen maanpuolustus kyberturvallisuuden kansallisessa kehittämisessä. Tilaisuudessa käsiteltiin valmisteilla olevaa kansallisen kyberturvallisuuden kehittämisohjelmaa ja vapaaehtoisen maanpuolustuskentän roolia tämän ohjelman toimeenpanossa. Tilaisuus oli yhdistyksen ensimmäinen webinaari ja noin sadan hengen osallistujamäärällään ja onnistumisellaan osoitti tämän tyyppisten tilaisuuksien vahvuudet.

Webinaarin juontajana toimi Viestiupseeriyhdistyksen puheenjohtaja Juha Petäjäinen. Avauksessaan hän totesi ajankohdan olevan oikea tarkastella kaikkeen toimintaan vähitellen laajenevan digitaalisuuden ja tämän mukana myös digitaalisen turvallisuuden roolia vapaaehtoisessa maanpuolustuskentässä. Alustajiksi ja panelisteiksi oli perinteisen tavan mukaan saatu aihealueen vahvimpia suomalaisia asiantuntijoita.

Kyberturvallisuuden kehittämisohjelma

Ensimmäisessä alustuksessa kyberturvallisuusjohtaja Rauli Paananen (liikenne- ja



viestintäministeriö) esitteli kansallisessa valmistelussa loppumetreillä olevaa Kyberturvallisuuden kehittämisohjelmaa. Ohjelma on tarkoitus julkaista vielä kuluvan kevään aikana valtioneuvoston periaatepäätöksenä siten, että ensimmäistä kertaa poliittiset päätöksentekijät sitoisivat kehittämiseen myös tarvittavat rahoitukset.

Kehittämisohjelma konkretisoi vuonna 2019 julkaistua Suomen kyberturvallisuusstrategiaa, jossa laajemmiksi tavoitteiksi asetettiin kansainvälisen yhteistyön kehittäminen, kyberturvallisuuden johtamisen, suunnittelun ja varautumisen koordinoimisen kehittäminen, sekä kyberturvallisuuden laaja-alaisen osaamisen kehittäminen. Kehittämisohjelman toimenpiteet on sovitettu yhteen muiden kyberturvallisuuteen liittyvien kehittämiskokonaisuuksien kanssa. Näitä ovat Huoltovarmuuskeskusten Digitaalinen turvallisuus 2030-ohjelma, Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 sekä lainsäädännön kehittämistarpeita ja muita tietoturvan ja tietosuojan kehittämistoimia käsittelevä LVM:n raportti (TITUKRI).

Kyberturvallisuuden kehittämisohjelman toimenpiteiden on tarkoitus ulottua hallituskausien yli. Tavoitteena on rakentaa alan toimijoiden yhteistyönä vahva suomalainen kyberturvallisuuden ekosysteemi. Kehittämisohjelmassa on neljä teemaa, jotka ovat huippuluokan osaaminen, kiinteä yhteistyö, vahva kotimainen kyberturvateollisuus sekä tehokkaat kansalliset kyberturvavykykkydet.

Alustuksen jälkeisessä keskustelussa nousi esille riittävän rahoituksen saaminen välttämättömille toimenpiteille sekä johtamisen selkeyteen liittyvät tavoitteet. Erittäin tärkeäksi nähtiin, että vakavan cyberkriisin sattuessa meillä on selkeät kansalliset johtamismallit ja näiden edellyttämä lainsäädäntö osoitettuine toimitusvaltuuksineen.

Puolustusvoimat osana kansallista kyberturvallisuutta

Toisena alustaja toimi Pääesikunnan johtamisjärjestelmäosastolta, insinööriversti Janne Jokinen. Hän esitteli erinomaisella tavalla sitä, miten kyberpuolustukseen liittyvät toimet nivoutuvat

puolustusvoimien lakisäätöihin tehtäviin. Puolustusvoimissa kyberpuolustusta ei ole nähty erillisen puolustushaaran tyyppisenä kokonaisuutena, vaan kiinteänä osana puolustusvoimien ja puolustushaarojen toimintaa kaikissa valmiustiloissa.

Terminä ”kyberpuolustus” on määritelty kyberturvallisuuden maanpuolustukselliseksi osa-alueeksi, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskäytännöistä. Näiden suorituskäytännöjen kehittämistä on tukenut vuonna 2019 voimaan tullut laki sotilastiedustelusta, jolla säädettiin selkeät tehtävät, prosessit ja toimivaltuudet tietoverkkotiedusteluun, tietoliikennetiedusteluun sekä ulkomaan tietojärjestelmätiedusteluun.

Eräänä mielenkiintoisena kehityksenä Jokinen toi esille kyberturvallisuuden niin sanotun ”uuden normaalin”. Erityisesti informaatio- ja kyberympäristössä konfliktin rajat ovat hämärtyneet ja lähentyneet, on siirrytty jatkuvan kamppailun tilaan.

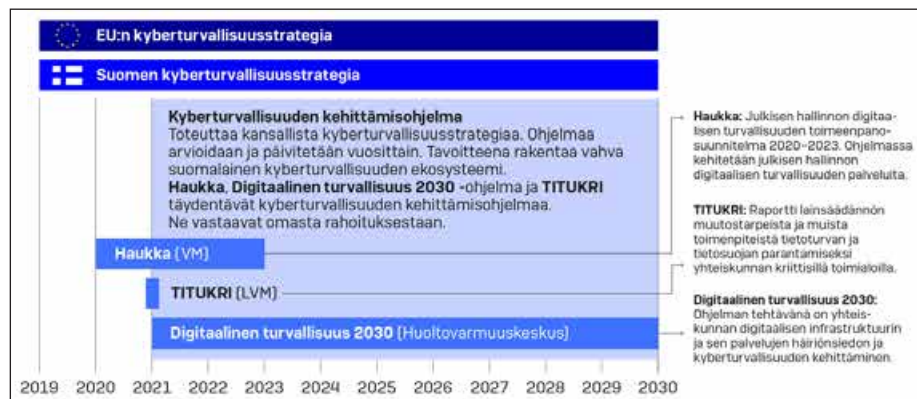
Jokisen mukaan Suomen puolustusvoimien kyberkyvykkyydet ovat korkeaa kansainvälistä tasoa. Osoituksena tästä, ovat suomalaiset harjoitusjoukot, saaneet kansainvälisissä kyberpuolustusharjoituksissa erinomaista palautetta.

Näkökulmia kansalliseen kyberturvallisuuteen

Kolmannen alustuksen pitämisestä vastasi F-Securen tutkimusjohtaja Mikko Hyppönen. Hän totesi jo aloituksessaan puheen sisältävän aiheita syksyllä julkaistavasta kirjasta. Näin ollen kuulijakunta pääsi jo näin etukäteen tutustumaan Hyppösen ajantasaiseen pohdintaa kyberturvallisuuden trendeistä ja niiden muutoksista.

Hyppösen mukaan riippuvuutemme teknologiasta kasvaa jatkuvasti kovaa vauhtia – halusimme sitä tai emme. Tämä tuo mukanaan laaja-alaisen keskinäisriippuvuuden, jossa erillisiksi aiemmin miellettyjen järjestelmien toiminta riippuu kokonaan toisen toimivuudesta. Esimerkiksi sähkönjakelu ei enää toimi ilman tietojärjestelmiä – ja päinvastoin!

Toinen kasvava trendi on uusien laitteiden liittäminen internetiin. Kun 1990-luvulla tapahtui laajamittainen tietokoneiden liittyminen tai liittäminen internetiin, on tämä sama kehitys nyt käynnissä melkein kaikissa laitteissa. Tässä kehityksessä Hyppönen näki huolestuttavana sen, että nykyään laitteen omistaja ei välttämättä aina ole tietoinen tästä nettiyhteydestä. Ymmär-



Kyberturvallisuuden kehittämisohjelman viitekehys ja aikataulu. Kuva LVM.



Kybertoimintaympäristö kattaa osan jokaista puolustushaaraa. Kuva Puolustusvoimat.

rettävästi laitteen valmistaja tarvitsee monistakin syistä tätä yhteyttä, mutta on ”ehkä unohtanut kertoa siitä”.

Hyppönen analysoi myös viime aikojen suurimpia tietovuotoja ja niiden seurauksia. Esimerkkinä Facebookilta vuotaneet miljoonat puhelinnumerot, mikä on aiheuttanut monenlaista harmia erityisesti niille, jotka ovat halunneet pitää numeronsa salaisena.

Mielenkiintoisia ajatuksia kumpusi Hyppösen toteamuksesta, miten nuoremmat sukupolvet kokevat internetin, he jotka muuta aikaa eivät ole eläneetkään. Heille tämä kaikki on täysin normaalia toisin kuin niille, joille vielä 30-40 vuotta sitten globaalit ja reaaliaikaiset viestintäverkot olivat täyttä utopiaa. Tästä utopiasta sen toteututtua, on – valitettavasti – muodostunut myös painajainen. Ihmisten seuraaminen, profiilien rakentaminen meistä kaikista, verkkorikollisuus, vaalivaikutaminen ja esimerkiksi salaliittoteoriat ovat nyt osana ympäröivää todellisuuttamme. Ilmiöitä, joita kukaan ei kyennyt ennakoimaan, mutta niiden kanssa on nyt osattava elää.

Yhtenä haasteena Hyppönen nosti myös esille järjestelmien monimutkaisuuden lisääntymisen. Ohjelmointivirheistä muodostuu haavoittuvuuksia aina, kun laite on verkossa. Ja mitä enemmän järjestelmässä on koodia, sitä enemmän niihin mahtuu myös bugeja. Turvallisuutta pyritäänkin yhä useammin hallitsemaan rajoittamalla esimerkiksi käyttöjärjestelmissä käyttäjien oikeuksia – heidän suojelemisekseen.

Paneelikeskustelu

Webinaarin toinen osa rakentui paneelista, jonka teemana oli Vapaaehtoisen maanpuolustuskentän rooli yhteiskunnan digitaalisen turvallisuuden kehittämisessä. Panelisteina keskusteluun osallistivat kaikki kolme alustuksen pitäjää sekä Maanpuolustuskoulutus ry:n (MPK) koulutusjohtaja Timo Mustaniemi.

Mustaniemi kertoi, että vuonna 2020 voimaan tullut uudistettu laki vapaaehtoisesta maanpuolustuskoulutuksesta lisäsi MPK:n yhteistoimintaa puolustusvoi-

mien kanssa. Käytännössä tämä näkyy muun muassa siten, että tällä hetkellä MPK:n valmisteleva kyberkoulutusohjelma on Pääesikunnassa hyväksyttävänä. Näin voidaan varmistaa, että MPK:n kyberkoulutus yhteensovittuu puolustusvoimien oman koulutuksen kanssa. Kumatkin täydentävät toisiaan.

Keskustelussa nousi selkeästi esille, että merkittävä, ellei merkittävin osa Suomen kyberturvallisuuden osaamisesta ja osaajista on reservissämme. Tämän lisäksi korkean tason osaajia on myös niissä, jotka eivät kuulu puolustusvoimien reserviin. Tämän henkilöstöryhmän kouluttamisessa MPK:lla on merkittävä rooli.

Myös haasteita luonnollisesti tunnistettiin. Eräs niistä on yritysten mukaan saanti kansallisiin kyberturvallisuusharjoituksiin ja -harjoitteluun. Tätä kautta myös merkittävä määrä alan osaajia pääsisi kyberkoulutusjärjestelmän piiriin.

Jokinen totesi vapaaehtoisen maanpuolustuskoulutuksen olevan puolustusvoimille erittäin tärkeää. Tämä saa reserviläiset kehittämään tärkeitä taitojaan myös virallisten puolustusvoimien omien harjoitusten ulkopuolella, sekä myös vapaa-aikanaan. Verkon kautta osallistuneilta tuli myös tähän liittyvä rakentava

esitys siitä, että esimerkiksi valtionhallinnon aloitteesta käynnistetty Cyber eSport-toiminta voisi aktivoida laajojakin ryhmiä kehittämään omia taitojaan – yksilön hui ja kansallinen hyöty yhdistyisivät.

Kyberturvallisuuden osaajien puute huoletti kaikki panelisteja. Tämän ovat konkreettisesti kokeneet alan suomalaiset yritykset ja viranomaiset. Hyppönen kertoi tuoreen uutisen, jonka mukaan pelkästään USA:ssa on tämän kuun aikana ollut avoinna 465 000 kyberalan työpaikkaa.

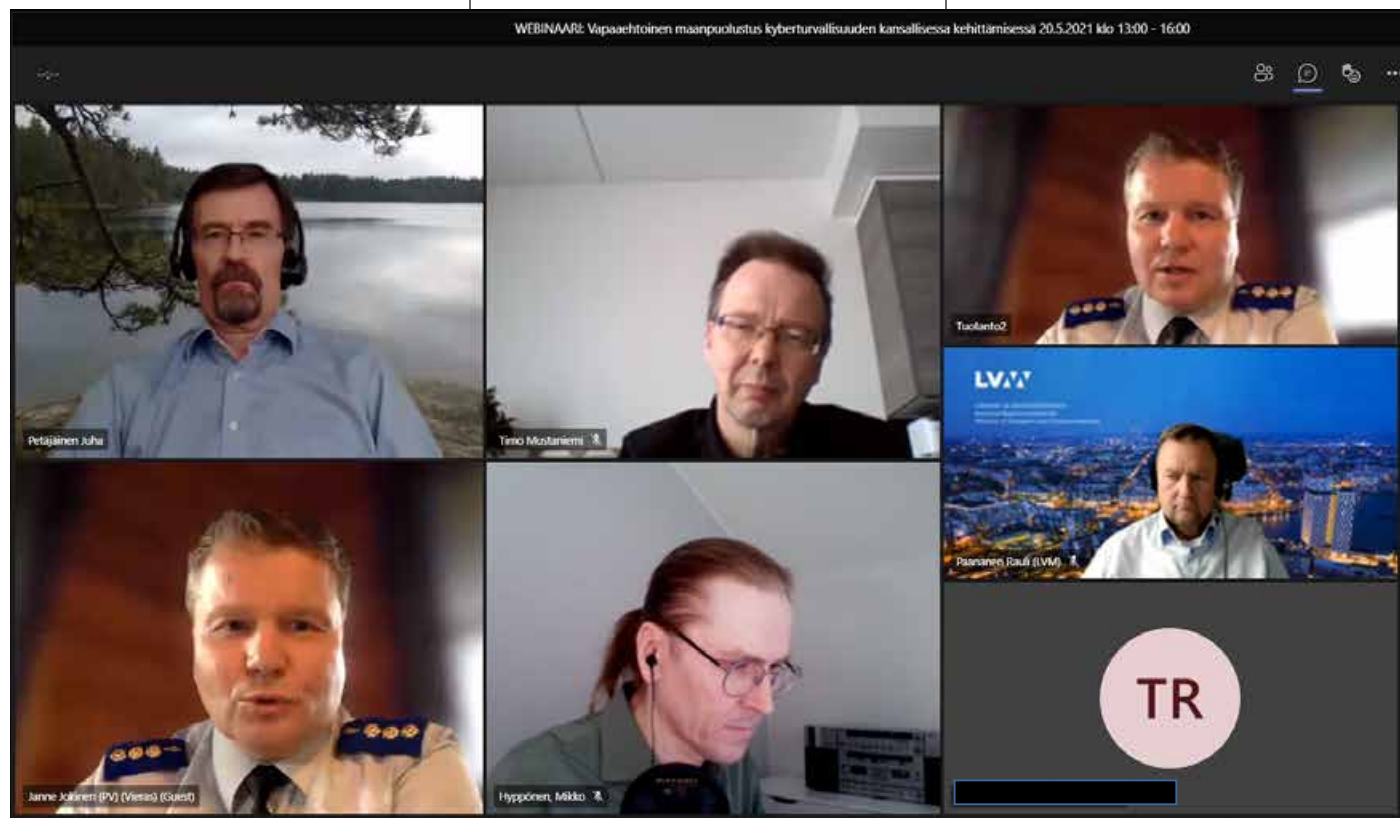
Lopuksi

Tilaisuuden päätteeksi puheenjohtaja kiitti alustajia, panelisteja sekä verkon kautta mukaan liittyneitä osallistujia. Puheenjohtaja totesi tilaisuuden yhtenä tavoitteena olleen myös perusteiden hankkiminen Viestiupseeriyhdistyksen oman toiminnan kehittämiseen. Tässä jo tunnistettiin tarve syvemmälle yhteistyölle muun vapaaehtoisen maanpuolustuskentän kanssa. Myös webinaarit yhtenä Viestiupseeriyhdistyksen toimintamuotona tulevat jatkumaan, sen verran positiiviset kokemukset tästä tilaisuudesta saatiin.



F-Securen tutkimusjohtaja Mikko Hyppönen vastaamassa webinaarin puheenjohtajan Juha Petäjäisen kysymyksiin. Kuva Viestiupseeriyhdistys.

Webinaarin tallenne on katsottavissa Viestiupseeriyhdistyksen verkkosivuilta www.viestiupseeriyhdistys.fi



Webinaarin paneelikeskustelussa Teams-sovellus osoitti toimivuutensa. Keskustelemassa (vasemmalta ylhäältä) puheenjohtaja Juha Petäjäinen, Timo Mustaniemi, Janne Jokinen, Mikko Hyppönen ja Rauli Paananen. Kuva Viestiupseeriyhdistys.

Turvallisen yhteiskunnan mahdollistaja



Fujitsu luo osallistavaa, kestävää ja luotettavaa tulevaisuutta

Turvallisuus syntyy luottamuksesta, osaamisesta ja vastuun kantamisesta. Fujitsu on sitoutunut edistämään ict-ratkaisuja, jotka auttavat organisaatioita ja yrityksiä rakentamaan tulevaisuutta turvallisesti ja kestävästi. Monipuolisen teknologia- ja palveluosaamisemme avulla autamme asiakkaitamme pysymään kehityksen kärjessä.

Teemme kaikkemme, jotta asiakkaamme saavat meiltä aina erinomaista palvelua riippumatta teknologiasta, hankkeen koosta tai asiakkaan tilanteesta. Tarjoamme asiakkaan luottokumppanin roolissa ict-ratkaisut tiedon saatavuuteen, integrointiin, jalostamiseen ja hyödyntämiseen, jotta yhteiskunta toimii aina – vaativissakin tilanteissa.

Lue lisää: www.fujitsu.com/fi

FUJITSU

Analysaattori



Autotallin taika

Pandemian runtelema yhteiskuntamme kurkottaa kevääseen ja toivoo, että jospa sieltä vielä tulisi tavallinen kunnon kesä. Tai edes syksy. Tai jotain. Tällaisen harrastelijakirjoittelijan materiaalipankkina toimiva lehdistö ja varsinkin sähköiset mediat yms. nettipalvelut ovat tällä hetkellä tylsiäkin tylsempiä lähteitä. Suosikkikohteessani Ruotsissakin keskitytään vain jo miljoonanteen koronaan sairastuneeseen ja sen ansiosta surkeisiin tilastoihin, vaikka siellä jossain rannikolla lojuu räjähtämäsillään oleva valaskin. Itänaapuri on mobilisoinut armeijansa Ukrainan rajalle, mutta kyse on vain klassisesta pullistelusta USA:n uudelle presidentille. Tuollaiset temput on siis niin 80-lukua. Täällä kotimaassa uutiskynnyksen ylittää vain hallituspuolueiden riitely, joka vaikuttaa sekin pelkältä vaalipeliltä, mutta ainoa mielenkiintoinen poliittinen uutinen on ollut se, kun vasemmistolainen politiikko potkii Audia. Siinä sitä on kunnon symboliikkaa mukana. Näin väsyneissä uutistunnelmissa lienee siis parasta taas keskittyä tälläkin kertaa teknologian kehitykseen tai kehittymättömyyteen. Se on aihepiiri, josta löytyy aina jotain mielenkiintoista.

Mennään talotekniikkaan. Tarkemmin sanottuna omakotitaloihin. Julkistan tässä ehdottomasti turhimman huoneen, joka usein löytyy juuri omakotitaloista. Kyse on Autotallista. Turhin siis siinä mielessä, että autoa siellä tyypillisesti ei säilytetä. Empiirisenä kokemuksena voin kertoa, että Analysaattorin 80-luvun lopulla rakentamaan taloon kuului myös autotalli, jossa säilytettiin lähinnä lautoja ja pingispöytää. Siitä ainoana merkittävänä hyötynä on jäljellä napakka rystylyönti. Autotallit ovat käytännössä siis isommilta ovilla varustettuja varastoja.

Mutta jotain muuta hyötyä niistä on kyllä ollut. Historia tunnistaa luultavasti tuhansia bändejä, jotka ovat aloittaneet juuri autotalleissa. Vanhemmasta päästä muutaman mainitakseni The Who, CCR,

The Kinks ja The Yardbirds (josta sikisi myöhemmin mm. Led Zeppelin). Kylmät ja kurjat tilat ovat ilmeisesti luovuudelle oiva kasvupohja. Ainakin Englantia puhuvissa maissa. Siperiassa lienee tässä mielessä hyvät olosuhteet, mutta en nyt kyllä nopeasti keksi yhtään saman sarjan orkesteria kuin nuo edellä luetellut. Sielähän siihen fiilikseen pääsyyn ei kyllä tarvita autotallia, muutkin huoneet kelpaisivat, joten jospa se juttu onkin siinä tilassa, ei olosuhteissa.

Varsinainen maailmanhistoriallinen menestystarina ovat kuitenkin autotalleissa perustetut yritykset. Lista on pitkä ja vaikeuttava. Disney, Hewlett Packard, Apple, Microsoft, Amazon, Google. Listaa voisi jatkaa aika pitkälle. Erityismaininnan annamme tässä yhteydessä kuitenkin Nikelle. Niken perustajat Bill Bowerman ja Phil Knight aloittivat nimittäin myymällä urheilukenkkiä auton takaluukusta perustamansa yrityksen Blue Ribbon Sportsin nimissä. Edes autotallia ei siis tarvittu ympärille. Ihan kivasti on Nikelläkin myöhemmin mennyt ja tilatkin jonkin verran kasvaneet.

Ihan ensimmäisiä autotallista ponnistaneita yrityksiä on Disney. Walt Disney aloitti työuransa lehtiä jymäällä, joka ei nyt ole aivan yhtä hyvä myyjän peruskoulu kuin pölynimurikauppiaana toimiminen, mutta opettaa paljon aikataulujen noudattamisesta. Myynti oli nimittäin Waltin vastuulla hänen ensimmäisessä yrityksessään Iwerks–Disney Commercial Artists jossa yhtiökumppanina oli hieman tuntemattommaksi jäänyt Ubbe Iwerks. Yritys kaatui aika nopeasti ja tarina kertoo Waltin syöneen varattomana nälkäänsä jopa koiranruokaa. Noihin aikoihin hän teki iltaisin jossain autotallissa elokuva-animaatioita ja loppu onkin sitten historiaa.

On selvää, kun tuota listaa tarkastelee, että erityisesti tietotekniikan pioneirit olivat autotallimyrönteisiä nuoria, yleensä miehiä. Ensimmäisiä IT-autotalliyrityksiä oli Hewlett-Packard, sillä yritys on pe-

rustettu jo 1939. Yrityksen ensimmäisiä asiakkaita oli juuri Walt Disney Studio, joka osti heiltä 8 kappaletta HP:n audio oskillaattoreita. Bill Hewlett ja David Packard muuten heittivät tarinan mukaan autotallissa siellä Palo Altossa kolikkoa päättääkseen kummassa järjestyksessä kavereiden sukunimet tulisivat esiintymään yrityksen nimessä. Ei siis ollut kovinkaan kaukana, että nuo tutut tuotteet tunnettaisiin PH-nimellä.

Tuosta Disneyn osuudesta HP:n varhaiseen kasvuun voi tehdä helposti johtopäätöksen, että näitä autotalleja voi siis ketjuttaa. Vahvistuksen tälle teorialle saa siitä, että eräs naapurissa asunut nuorukainen norkoili Larry Langin autotallissa niin intensiivisesti, että Larry vei kaverin omalle työpaikalleen Hewlett-Packardille nuorten tutkijoiden kerhoon. Tämä innostunut nuorukainen oli nimeltään Steve Jobs. Kyse ei siis ollut edes alkuperäisestä HP:n tallista vaan HP:llä insinöörinä toimineen Langin omasta, joten ketjulla alkaa tässä vaiheessa olla jo mittaa.

Ja sehän ei tietenkään ole siis yllätys, että Steve Jobs perusti ystävänsä Steve Wozniakin kanssa Applen nimenomaan Wozniakin autotallissa. Wozniak on vanhemmiten tosin kertonut, että tarina on vähintäänkin romantisoitu, mutta myytti elää vahvana. Applen ja Jobsin tarina on hyvin tunnettu, joten siihen emme jää tässä nyt jumiin. Meillä on vielä muitakin autotalleja koluttavana.

Oma lukunsa näissä yritysten perustamispaikoissa ovat myös opiskelija-asuntolat. Michael Dell perusti oman yrityksensä ”dormissa” ja siirsi sen sitten aika nopeasti autotalliin. Myös Facebook on käynnistetty asuntolassa, mutta se on aika luonnollistakin sillä sovelluksen kohderyhmä oli siinä mukavasti lähellä.

Siirrytäänpä sitten raskaaseen sarjaan. Jeff Bezos perusti oman yhtiönsä autotallelleen 1994, josta tuli sitten myöhemmin Amazon ja Bezosista maailman rikkain mies. Bezosille pitää nostaa kyllä kättä

hattuun, sillä hänellä oli tuolloin jo vahva ja täysin nappiin osunut näkemys siitä, miten Internet muuttaa maailmaa ja miten siitä voisi tehdä bisnestä. Luettuaan artikkelin, jossa kerrottiin Internetissä tapahtuvasta mainonnan valtavasta kasvusta, hän teki listan kahdestakymmenestä suositusta tuotteesta, joita voisi myydä netissä. Sitten hän rajasi listan viiteen tuotteeseen: CD-levyt, tietokoneiden osat, ohjelmistot, videot ja kirjat. Bezos varasi itselleen kaupankäyntiä varten domainin relentless.com (säälimätön). Nimi kuulosti hieman ikävältä, joten Bezos selaili sanakirjaa ja poimi sieltä eksoottiselta kuulostavan joen yhtiönsä nimeksi. Jotain jäi ilmeisesti kuitenkin kaivelemaan tuossa säälimättömässä alkuperäisessä nimessä, joten hän ei ole siitä vielääkään luopunut. Kokeilkaa itse: <http://relentless.com>.

Bezos pääsi sitten pari vuotta sitten historiaan myös luomalla itsestään ja rouvastaan maailman rikkaimmat sinkut. Jeff erosi vaimostaan MacKenzie Bezosista 25 vuoden avioliiton jälkeen. Rouvalle jäi kuitenkin kivasti kipurahoja, jotka lieventävät erotuskaa. MacKenzie on tällä hetkellä maailman toiseksi

rikkain nainen n. 61 miljardin nettovarallisuudellaan. Jotain temppuja Jeffin hihaan taisi silti jäädä, sillä hän on taas tällä hetkellä maailman rikkain ihminen huolimatta tuosta parin vuoden takaisesta pompusta.

Toinen mutta ei yhtään vähäisempi raskassarjalainen autotaliyritys on tietenkin Microsoft. Bill Gates ja Paul Allen perustivat yrityksensä pienessä autotalissa Albuquerque, New Mexicossa.

Pitkälti samankaltainen tarina kuin Steve Jobsillakin. Innostuneena uudesta teknistä molemmat jättivät opiskelunsa kesken ja alkoivat häärtä autotalleissaan.

Jonkin sortin teknologiauutinen lienee Bill ja Melinda Gatesin tuore avioerokin. Pari varakasta sinkkua siitäkin sopasta syntyy, mutta tuskin tarvitsee kummankaan alkaa Tinderissä swaippaamaan, vai miten sitä nyt käytetäänkin. Vannoutuneena Applen Mac-laitteiden käyttäjänä olen kyllä sitä mieltä, että tämä avioero tapahtui aivan liian myöhään. He menivät naimisiin 1994 ja seuraukset hakevat vertaistaan myös IT-maailmassa. Seuravana vuonna nimittäin ”syntyi” Windows

95 ja sitä himmeliä en anna Billille koskaan anteeksi. Vieläkin vähän puistattaa.

Loppuyhteenvetona voidaan siis todeta, että autotalleja kannattaa rakentaa ja käyttää mutta ei autojen säilytykseen. Tai hei seis, mietitäänpä tätä hetki vielä.

Vanhan liiton polttomootorimiehenä Analysaattori ei lämpene sähköautoille. Mutta asiaan perehtyneenä, tosin heikosti, olen havainnut, että ei ne lämpene sähköautotakaan. Koska moottori ei tuota hukkalämpöä matkustamoon siellähän paleltuu. Ohjauspyörä ja istuimet voidaan lämmittää sähköllä, mutta ilmatilan lämmitykseen ei riitä tehoa. Moottori ei kaipa lämmitystä mutta akku sen sijaan sitä tarvitsee. Voisiko tähän olla ratkaisuna sähköautojen säilyttäminen autotalleissa. Ennustan että näin siinä käy, autotali saa uuden mahdollisuuden. Toivottavasti kuitenkin tämän päivän startup-yrityksillekin jää riittävästi kurjia ja kylmiä tiloja tehdä historiaa.

Pasi Mäkinen



**YHDESSÄ
PAREMPI
JA TURVALLINEN
TULEVAISUUS.**

**Turvaa kaluston
koko elinjaksole.**

Millog ylläpitää maa- ja
merivoimien kalustoja sekä
ilmavoimien valvonta-
järjestelmiä niin normaali-
kuin poikkeusoloissa.

Millog
millog.fi

f \ \ \ in

Insinöörieriverstiluutanti Erkki Hakulinen

Elektroniikan opetuksesta Sähkötekniillisessä koulussa

Tällä hetkellä lienee jo yleisesti tunnustettu ohjelmoidun opetuksen edut tavanomaiseen verrattuna. Tietty taito saavutetaan entistä lyhyemmässä ajassa tai, mikä Sähkötekniillisessä koulussa on todettu tärkeäksi, entisessä koulutusajassa saavutetaan parempia tuloksia.

Sähkötekniillisessä koulussa on siksi ryhdytty kokeilemaan uusia menetelmiä. Kokeilujen pääkohteeksi on valittu elektroniikan opetus, vaikka osittaisia uudistuksia on tehty muissakin oppiaineissa. Ohjelmoidun opetuksen periaatteiden mukaisesti opetettava aines on pelkistetty ja jaettu mahdollisimman itsenäisiin oppijaksoihin. Kunkin oppijakson sisällä on pyritty, osioihin jaon ohella, poistamaan juopa informatiivisen opetuksen ja laboratoriotyöskentelyn väliltä. Näin kehittyvää opetusmenetelmää voidaan sanoa integroiduksi opetuksiksi, koska siinä eri opetusmenetelmät ja opetusvälineet tavoitteen saavuttamisen kannalta optimativalla integroituvat.

Oppilaiden lähtötasoerojen poistamiseksi elektroniikan alkuun on liitetty johdantokurssi, jossa käsitellään aineen rakennetta, sähköilmiöiden atomiluonnetta ja eräitä sähköopin peruskäsitteitä. Eräs johdantokurssin päätavoitteista on motivoida oppilaat vastaanottamaan sähkötekniikan ja elektroniikan perustiedot, koska varsinaiseen työhön liittyvään kalustokoulutukseen päästään vasta kurssin loppupuolella.

Sopivien oppikirjojen hankkiminen on ollut vaikeaa. Tämän takia on jouduttu turvautumaan saatavissa olevan ulkolaisen aineiston soveltamiseen. Suoraan Sähkötekniillisen koulun kursseille sopivia oppijaksoja on saatu vain



rajoitustusti. Tämä käytettävissä olevien ohjelmoitujen oppijaksojen katkonaisuus johtaa väistämättä järjestelyyn, jossa klassiset oppitunnit, ohjelmoidut oppitunnit, ohjelmoidut laboratoriotyöt ja tavanomaiset laboratoriotyöt vuorottelevat. Tässä vuorottelussa on todettu sellainen huomionarvoinen etu, että oppilaat eivät pitkästy, kuten helposti muuten tapahtuu pitkän kurssin aikana.

Takaisinkytkennän puuttuminen oppilaalta opettajalle on tavanomaisen opetuksen pahimpia epäkohtia. Takaisinkytkennän kaksi päätehtävää ovat opetuksen perillemenon tarkkailu ja kunkin oppilaan edistyksen tarkkailu. Oikein järjestettynä takaisinkytkennällä voidaan tarkkailla informaatiohäviön suuruutta ja selvittää, missä vaiheessa se syntyy opettajasta, opetusmenetelmästä vai oppilaasta. Tehokas, jatkuva, yksilöllinen takaisinkytkentä on saavutettavissa vain vastauskoneen (tai opetuskoneen) avulla. Minkäänlainen

kyselytekniikka ei ole riittävän yksilökohtaista eikä minkäänlainen kirjallinen koejärjestely ole riittävän nopea. Sopivan vastauskoneen saamista on tämän takia pidetty välttämättömänä.

Oppilaiden arvostelemiseksi pidettävät kokeet on nyt aikaisempiin kokemuksiin perustuen jaettu useammiksi lyhyiksi suppeata kurssin osaa, yhtä oppijaksoa koskeviksi osakokeiksi. Kokeina käytetään aiheen mukaan sekä monivalintatyyppejä että tavanomaisia kokeita. Koska monivalintatyyppeiden kokeiden pitämisestä, erityisesti kysymysten laatimisesta on vielä varsin vähän kokemusta, annetaan loppuarvosanaa laskettaessa monivalintatyyppeille kokeille ainakin toistaiseksi pienempi painokerroin.

Monivalintatyyppeiden kokeiden pitämisessä voidaan käyttää vastauslomaketta tai vastauskoneetta. Koetyypeinä on käytetty sekä normaalia kolmen vaihtoehdon kysymystyyppiä että neljän vaihtoehdon kysymystyyppiä. Tässä jälkimmäisessä koetyypissä yksi vaihtoehto on oikein, yksi lähes oikein ja kaksi selvemmin väärin. Oppilaiden tehtävänä on valita väärät vaihtoehdot, joten tehtävästä on mahdollista saada kolme pistettä. Oikean vaihtoehdon valitseminen antaa taas kolme miinus-pistettä, joten kaikkien vaihtoehtojen valinta pitää oppilaan nolilla, samoin tietysti vastaamatta jättäminen. Vastauskoneetta käytettäessä voidaan koetulokset julkaista oppilaille välittömästi. Koneen avulla voidaan myös suorittaa tehtäväanalyysi, jota on pidettävä välttämättömänä vaiheena monivalintatyyppeiden kokeiden kehitystyössä.

Artikkelin kirjoittaja: Veli-Matti Pesola

5.3.2021 myönnettyt viestiristit

Viestiristi soljella

Hakkarainen	Pauli	ICT-erityisasiantuntija	Jyväskylä
Pilpolä	Juhani	Eläkeläinen	Lieto

Solki viestiristiin

Aho	Jari	Everstiluutnantti	Hämeenlinna
Heikkinen	Risto	Insinöörikapteeniluutnantti	Helsinki
Honkonen	Teppo	Insinöörikapteeni	Petäjävesi
Jokela	Veli-Matti	Kapteeni	Rovaniemi
Juola	Matti	Teknikkokapteeniluutnantti	Turku
Laakkonen	Pasi	Pääsuunnittelija	Mikkeli
Liukkonen	Risto	Insinöörimajuri	Orivesi
Nikkilä	Jukka	Everstiluutnantti	Vantaa
Pekkanen	Kai	Teknikkokapteeniluutnantti	Turku
Romakkaniemi	Esa	Työnjohtaja	Rovaniemi
Turunen	Jarkko	Majuri	Mikkeli
Tuura	Petteri	Insinöörikapteeni	Riihimäki
Yrjänä	Kimmo	Majuri	Turenki

Viestiristi

Aho	Harri-Pekka	yliluutnantti	Vaasa
Airaksinen	Veli-Matti	Kehityspäällikkö	Muurame
Do	Taneli	Pursimies	Inkoo
Guttorm	Jyrki	Valmiuspäällikkö	Helsinki
Harju	Jarkko	Kapteeni	Turku
Hemmilä	Nina	Viestittäjä	Tampere
Herd	Markku	Yliluutnantti	Turku
Huttunen	Marko	Insinööri	Laukaa
Härkönen	Lauri	Pursimies	Espoo
Juntunen	Pasi	Järjestelmäsuunnittelija	Jyväskylä
Kajander-Avellán	Mika	Majuri	Tampere
Karttunen	Matti	Museonjohtaja	Mikkeli
Kauppinen	Tomi	Insinööriluutnantti	Jyväskylä
Kauppinen	Vesa	Toimitusjohtaja	Jyväskylä
Keskimäki	Harri	Insinöörimajuri	Riihimäki
Kiiski	Osmo	Eläkeläinen	Mikkeli
Kolari	Pentti	ICT-järjestelmäpäällikkö	Tampere
Kuparinen	Ville-Matti	Insinööriyliluutnantti	Jokimaa
Kuusela	Veijo	Asentaja	Jyväskylä
Kärkkäinen	Sami	Insinööri	Jyväskylä
Laakkonen	Jari	Insinööriyliluutnantti	Jyväskylä
Laakso	Jukka	Everstiluutnantti	Tammela
Laine	Kari-Matti	Account Executive	Kirkkonummi
Lamminen	Jani	Insinöörimajuri	–
Lappalainen	Kimmo	ICT-erityisasiantuntija	Vantaa
Laurila	Kari	Kapteeniluutnantti	Espoo
Lehmonen	Janne	Insinööriluutnantti	Jyväskylä
Leinonen	Eero	Kapteeni	Kajaani
Lievonen	Risto	ICT-erityisasiantuntija	Porvoo
Luomajoki	Tiina	Henkilöstösuunnittelija	Jyväskylä
Luopa	Jari	Suunnittelija	Tuusula
Montonen	Vesa	Työnjohtaja	Mikkeli
Muikku	Petri	ICT-erikoissuunnittelija	Tampere
Mutonen	Marika	ICT-erityisasiantuntija	Viiala
Muuttoranta	Tuomo	Insinööri	Ylöjärvi
Määttä	Henrikki	Insinööri	Tampere

Nenonen
Nättinen
Palmunen
Petroff
Pitkänen
Rapala
Rautio
Roschier
Räisänen
Saukko
Sorri
Sorri
Suhonen
Takkinen
Tammelin
Tervo
Utter
Vaahteranoksa
Vainio
Valjakka
Viita-aho
Viitala

Päivi
Jari
Otto
Sami
Markku
Tuomas
Erja
Juha
Tuukka
Atro
Topi
Kanu-Jalmari
Janne
Ari
Jussi
Tatu
Henna-Mari
Kimmoo
Matias
Mia
Pekka
Ossi
ICT-erityisasiantuntija
Asentaja
Järjestelmäinsinööri
Yliluutnantti
Alueellinen suunnittelija
Kapteeni
Viestittäjä
Kapteeni
Pursimies
Majuri
Verkkosuunnittelija
Asentaja
Yliluutnantti
Tietohallintopäällikkö
Kapteeni
Ylikersantti
Yliluutnantti
ICT-erityisasiantuntija
Asentaja
ICT-erityisasiantuntija
ICT-asiantuntija
Varastomestari

Mikkeli
Jyväskylä
Jyväskylä
Kajaani
Kuopio
Pirkkala
Tampere
Heinävesi
Raasepori
Rovaniemi
Kangasala
Jyväskylä
Kontiolahti
Jyväskylä
Mikkeli
Kajaani
Pyhtää
Riihimäki
Jyväskylä
Mikkeli
Jyväskylä
Jyväskylä



Tervetuloa Museo Militariaan!

Vaihtuvat näyttelyt vuonna 2021:

**Kokoelmien kätöistä
ja**

**"Pimeys suurin ennen
aurinkon nousua" –
Katkelmia Risto Rytin
elämästä**

31.8. asti avoinna joka päivä
klo 10–17 (suljettu 25.6.)

Myös lounasravintola Militaria
palvelee asiakkaita.

www.museomilitaria.fi



MUSEO MILITARIA

Vanhankaupunginkatu 19, 13100 HÄMEENLINNA

Puh. 040 4507 479, asiakaspalvelu@museomilitaria.fi



A.R. SAARMAA -SEMINAARI 24.9.2021

• Paikallispuolustuksen johtaminen

Seminaarin järjestelyt ja tavoitteet

Viestikiltojen liitto järjestää paikallispuolustuksen johtamista ja viestitoimintaa käsittelevän A.R. Saarmaa -seminaarin **perjantaina 24.9.2021 klo 12.00 - 16.00** yhteistoiminnassa puolustusvoimien, Viestiupseeriyhdistyksen ja Maanpuolustuskoulutusyhdistyksen kanssa.

Seminaarin keskuspaikkana on Riihimäki. Seminaarissa hyödynnetään puolustusvoimien videoneuvottelujärjestelmää, jolloin siihen voi osallistua valituista puolustusvoimien toimipisteistä ympäri Suomen.

Seminaarin tavoite on syventää osallistujien tietoisuutta paikallispuolustuksen

- johtamisjärjestelmistä ja niiden toimintaympäristöstä
- kyberpuolustuksesta ja
- arjen välineiden käytöstä.

Seminaari on tarkoitettu

- paikallispataljoonaan sijoitetuille johtajille ja viestihenkilöstölle
- paikallispuolustuksen kehittämiseen osallistuville henkilöille
- viesti- ja johtamisjärjestelmäalan vapaaehtoisten maanpuolustusjärjestöjen jäsenille
- Maanpuolustuskoulutusyhdistyksen henkilöstölle ja jäsenjärjestöjen jäsenille
- Johtamisjärjestelmä- ja viestikoulutuksen kouluttajakoulutukseen kutsutuille MPK:n kouluttajille.

Seminaaripäivän ohjelma 24.9.2021 (Riihimäki)

- 1) Aamukahvi
 - Klo 08.30 - 09.00 Viestikoulun luokkarakennus
- 2) Viestiupseeriyhdistyksen vuosikokous
 - Klo 09.00 - 10.15 Viestikoulun luokkarakennus
- 3) Palkitsemiset
 - Klo 10.30 - 11.00 Viestikoulun luokkarakennus
- 4) Lounas
 - Klo 11.00 - 12.00 Varuskuntaravintola Liesi
- 5) **A.R. Saarmaa -seminaari**
 - **Klo 12.00 - 16.00 Viestikoulun luokkarakennus ja alueelliset toimipisteet**
- 6) Juhlapäivällinen
 - Klo 16.30 - 18.30 Riihimäen Upseerikerho

Seminaaripaikkakunnat

Seminaari toimeenpannaan seuraavilla paikkakunnilla (Osoite ja joukko-osasto):

- | | | |
|----------------|--------------------------------------|-------------------------------|
| • Helsinki | Santahamina, Ritaritalo (Yrjö-Maunu) | Maanpuolustuskorkeakoulu |
| • Riihimäki | Riihimäen varuskunta, Rak 23 | Maasotakoulu (Viestik) |
| • Tampere | Uimalankatu 1 | Pirkanmaan aluetoimisto |
| • Turku | Rykmentintie 15 | Lounais-Suomen aluetoimisto |
| • Kouvolaa | Kauppalankatu 43C | Kaakkois-Suomen aluetoimisto |
| • Mikkeli | Tyrjätie 9, Karkialampi, Rak 3 | Etelä-Savon aluetoimisto |
| • Vaasa | Wolffintie 35 | Pohjanmaan aluetoimisto |
| • Joensuu | Torikatu 36 B | Pohjois-Karjalan aluetoimisto |
| • Oulu | Hiukanreitti 40, Hiukkavaara | Pohjois-Pohjanmaan ja Kainuun |
| • aluetoimisto | | |
| • Kajaani | Prikaatintie 97 | Kainuun prikaati |
| • Sodankylä | Kasarmintie 94 | Jääkäriprikaati |
| • Lahti | Kirkkokatu 12 | Hämeen aluetoimisto |
| • Rovaniemi | Someronharjuntie, Rak 21 | Lapin aluetoimisto |
| • Kuopio | Vuorikatu 26 B | Pohjois-Savon aluetoimisto |
| • Jyväskylä | Asekatu 3D | Keski-Suomen aluetoimisto |
| • Niinisalo | Sairaالات 6 | Porin prikaati |
| • Lappeenranta | Lavolankatu 1 | Maasotakoulu |
| • Hamina | Kadettikoulunkatu 7 | Maasotakoulu (RUK) |

Ilmoittautuminen

Ilmoittautumiset seminaariin 3.9.2021 mennessä Viestikiltojen liiton sihteerille Carl-Magnus Gripenwaldtille sähköpostitse: cm.gripenwaldt@gmail.com. Seuraavat tiedot pyydetään ilmoittamaan: **Nimi, syntymäaika, yhteystiedot (puhelinnumero ja sähköpostiosoite), järjestö/yhdistys ja paikkakunta, jossa seminaariin osallistuu.**

Tiedustelut

Seminaaria koskeviin kysymyksiin vastaavat:

- Jukka-Pekka Virtanen, 0400840086
- Juha Peltomäki, 0299410601.

KUTSU VIESTIUPSEERIYHDISTYKSEN SYYSKOKOUKSEEN

Viestiupseeriyhdistyksen hallitus kutsuu yhdistyksen jäsenet syyskokoukseen ja seminaaripäivään Riihimäelle **perjantaina 24.9.2021 kello 08.30** alkaen. Varsinainen syyskokous pidetään Riihimäen Varuskunnassa klo 9.00-10.15, Viestikoulun luokkarakennus.

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

- 1) Kokouksen puheenjohtajan valinta
- 2) Kokouksen sihteerin valinta
- 3) Kahden pöytäkirjan tarkastajan ja ääntenlaskijan valinta
- 4) Kokouksen laillisuuden ja päätösvaltaisuuden toteaminen
- 5) Kokouksen työjärjestyksen hyväksyminen
- 6) Toiminta- ja taloussuunnitelman hyväksyminen vuodelle 2022
- 7) Jäsenmaksujen suuruuden päättäminen vuodelle 2022
- 8) Hallituksen puheenjohtajan valinta vuodelle 2022
- 9) Hallituksen jäsenten lukumäärän päättäminen ja hallituksen jäsenten valinta vuodelle 2022
- 10) Toiminnantarkastajan ja varamiehen valinta
- 11) Muut asiat

Päivän ohjelma 24.9.2021

- 1) Aamukahvi
 - Klo 8.30 - 9.00 Viestikoulun luokkarakennus
- 2) Viestiupseeriyhdistyksen syyskokous
 - Klo 9.00 - 10.15 Viestikoulun luokkarakennus
- 3) Palkitsemiset
 - Klo 10.30 - 11.00 Viestikoulun luokkarakennus
- 4) Lounas
 - Klo 11.00 - 12.00 Varuskuntaravintola Liesi
- 5) AR Saarmaa-seminaari
 - Klo 12.00 - 16.00 Viestikoulun luokkarakennus ja alueelliset toimipisteet
- 6) Päivällinen
 - Klo 16.30 - 18.30 Riihimäen Upseerikerho

Kuljetus Helsingistä lähtee Kiasman edestä turistipysäkillä (Mannerheiminaukio) kello 07.30 ja paluu päivällisen jälkeen samaan paikkaan.

Ilmoittautumiset päivän tilaisuuksiin 3.9.2021 mennessä www.viestiupseeriyhdistys.fi (toivottavin tapa), sähköpostitse toiminnanjohtaja@viestiupseeriyhdistys.fi tai puhelimitse 040 514 2497.

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

Tervetuloa!

Viestiupseeriyhdistys ry:n hallitus



Yhteydet maastoon Nestorin tuotteilla

Nestor Cablesin valikoimasta löytyvät vaatimaan kenttäkäyttöön soveltuvat valokaapelit väliaikaisten verkkojen rakentamiseen. Kaapelit ovat saatavilla erilaisilla liitinvaihtoehdoilla, ja niiden lisäksi valikoimassa ovat myös asennuslaitteistot sekä huoltotarvikkeet. 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