Viestimies

Viestiupseeriyhdistyksen julkaisu 74. vsk Numero 4 Talvi 2019

www.viestiupseeriyhdistys.fi

www.combitech.fi

Viestimies-lehti

Päätoimittaja
Samuli Terämä
p. 050 3399038
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p. 040 553 6182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Jani Liitola
p. 0299 510 612
henkilotoimittaja@viestiupseeriyhdistys.fi

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

Toimituskunta
Heiskanen Mikko (pj)
Blomqvist Reima
Helenius Mika
Isomäki Pekka
Mikkonen Mauri
Putkonen Jyri
Ståhlberg Mika
Suokko Harri
Valkola Eero
Wirman Kari
Yli-Äyhö Janne

Toimituksen osoite
Päivölänrinne 7 A 1
04220 Kerava

www.viestiupseeriyhdistys.fi/viestimies

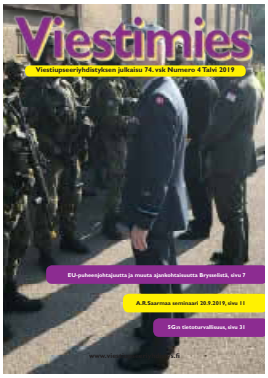
Pankkitili FI 21 5780 5520 017 7 44
Vuosikerta 35 Eur

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

ISSN 0357-2153



Tässä numerossa

Seuraavan numeron aineistopäivä on 7.2.2020. Lehti ilmestyy viikolla 10.

Historiaa... ja tulevaisuuden suuntaviivoja

Hyvät lukijat, historiaa on tehty ja tehdään monella alueella. Tätä kirjoittaessa Suomi varmisti ensimmäistä kertaa pääsyn jalkapallon EM-lopputurnaukseen. Hyvä Suomi!! Lähes samaan aikaan, marraskuun lopussa, Talvisodan syttymisestä tuli täyteen

80 vuotta. Vain muutos on jatkuvaa historian saatossa. Teknologian kehitys on vaikuttanut myös sodankäyntiin, mukaan lukien viestitaktiikkaan. Nämä uudet teknologiset innovaatiot mahdollistavat uusia keinoja viestitaktiikan entuudestaan tuttujen perusolettamusten toteutukseen. Teknologia ja sen muutokset tulee huomioida muuttuvassa maailmassa. Reservin varaaminen, yllätyksellisyys ja aktiivisuus, yksinkertaisuus, olosuhteiden hyväksikäyttö sekä suunnitelmallisuus ovat kaikki perusteesejä, joita on hyvä vaalia. Uusien teknologioiden käyttöönotto on vääjäämätöntä, mikäli haluamme pysyä ajan tasalla ja kyvykkäinä vastaamaan mahdollisiin uhkiin.

Teknologista kehitystä ja yhteistyötä vaalitaan usealla rintamalla. Suomen kolmas EU-puheenjohtajuuskausi on päättymässä tältä erää. Tavoitteina on ollut muun muassa digitalisaation ja tekoälyn edistäminen. Näiden ohella johtamisjärjestelmäalan näkökulmasta keskiössä ovat olleet johtamisjärjestelmien yhteensopivuus sekä kybertoimintaympäristön yhteistyö. Euroopan Unioni on ollut vahvassa käymistilassa siitä asti, kun Iso-Britannia ilmoitti eroavansa EU:sta. Tämä on leimannut myös Suomen puheenjohtajuuskautta. Huomio on valitettavasti kiinnittynyt sekä kansainvälisesti että EU:n sisällä siihen, eroaako Iso-Britannia sopimuksen kanssa vai ilman. Tämä on aiheuttanut merkittäviä epävarmuustekijöitä niin yrityksissä kuin valtioissa. Eri tahot pohtivat millaiseksi tilanne muodostuu jatkossa suhteessa saarivaltioon. Eron jälkeenkin yhteistyö jatkuu, mutta se saattaa edellyttää täysin erilaista sopimista ja eri yksityiskohtien huomioimista kuin aiemmin.

Yleisesti ottaen erilaisia hypejä tulee ja menee – tässä ajanhetkessä mukana ovat 5G, digitalisaatio ja kybertoimintaympäristö. Tehdyn tutkimuksen mukaan suomalaisten innokkuus ottaa 5G käyttöön heti kun se on saatavilla, on laskenut noin 5%. Silti moni odottaa innokkaana, mitä tuo paljon puhuttu 5G tuo tullessaan. Taajuusalueiden jako ja taajuuslupien hinnat sekä niiden regulaatio vaihtelevat maittain. Tämä voi vaikuttaa haitallisesti kilpailukykyyn sekä taajuusalueen yhteiskunnalliseen käytettävyyteen ja sitä kautta sen vaikuttavuuteen sekä levinneisyyteen.

Kyberiin liittyviä seminaareja ja tapahtumia järjestetään runsaasti. Hyökkäyksiä erityisesti yrityksiä, mutta myös valtiollisia toimijoita vastaan tapahtuu jatkuvasti. Näistä kaikista ei kuitenkaan välitetä tietoja julkisuuteen. Osasyynä tähän on julkisuuskuva ja ehkä toisaalta se, ettei haluta kertoa, miten tai mihin hyökkäys on vaikuttanut.

Digitalisaatio sisältää muun muassa automatisaatiota, koneoppimista, tekoälyä, robotiikkaa ja pilviteknologiaa. Esimerkiksi pilvipalveluiden ja käytössä olevien legacy-järjestelmien vaatimukset ovat hyvin erilaisia yrityksestä ja yhteisöstä riippuen. Hyperconnectivity on perusedellytys datakeskuksien välillä, jotta palveluista kyetään mittaamaan niiden hyödyt irti. Tiedonsiirtoon ja sen kehittämiseen tuleekin siis panostaa vielä jatkossakin. Kasvavat datamäärät edellyttävät vakaampia ja parempia yhteyksiä. Uplink-yhteyden vaatimus kasvaa 5G:n myötä, jotta sensoreilta ja dataa tuottavilta järjestelmiltä saadaan tieto analysoitavaksi pilveen. Tämä tarkoittaa, että vähintään paikkatieto, äänet ja kuvat tulee tallentaa pilveen. Jää nähtäväksi mitä se tarkoittaa tietoturvan ja yksityisyyden kannalta. Hyödyt ja haitat kulkevat usein käsi kädessä.

Erään tutkimuksen mukaan älykäs automaatio tekee läpimurron vuonna 2020. Hidastavin tekijä digitalisaation ja automaation saralla on edelleen ihminen. Ihmisten osaamisvaje hidastaa merkittävästi automaation lisääntymistä ja laajentumista. Tarvitsemme siis osaavia ihmisiä kertomaan koneelle, mitä sen tulisi tehdä. Iso-Britanniassa tehdyn tutkimuksen mukaan digitalisaatio ei vie työpaikkoja, vaan ennemminkin luo uusia. Ihmisiä tarvitaan edelleen tekemään innovaatiotyötä ja strategista ajattelua, johon koneet eivät ainakaan vielä toistaiseksi ole kyenneet. Olisiko tässä seuraava työn murros? Uusien teknologioiden soveltaminen nykyisessä työympäristössä vaatii työntekijöiltä erilaista osaamista kuin aiemmin. Koulutus ja jatkuva uuden oppiminen ovat oleellisia taitoja tulevaisuuden työelämässä. Yritysten ja yhteisöjen, kuten viranomaistenkin, tulisi huomioida entistä paremmin kehittämisen ja innovaatioiden jatkuminen panostamalla ihmisiin, tuottavuuden ja ulkoisten verkostojen sijaan. Jatkuva oppiminen on työmarkkinoiden perusedellytys tänään ja huomenna.

Hyvää Joulua ja onnellista Uutta Vuotta toivoo koko Viestimies-lehden toimitus!

Päätoimittaja VM

Kulunut vuosi on ollut historiallinen puolustusvoimien johtamisjärjestelmäalalle. Järjestelmäämme on rakennettu kansainvälisesti yhteentoimivaksi jo lähes kahdenkymmenen vuoden ajan. Yhteentoimivuutta on testattu erilaisissa tapahtumissa tähän mennessä lähinnä ulkomailla. Siirryimme uuteen aikakauteen, kun Suomi ja Yhdysvallat järjestivät keväällä 2019 yhdessä puolustusvoimien historian suurimman johtamisjärjestelmän testaus- ja todentamistilaisuuden. Bold Quest 19.1 oli osa Yhdysvaltojen Joint Staff J6:n johtamaa harjoitussarjaa, missä demonstroidaan vaikuttamisen prosesseja johtamisjärjestelmän tukemana. Viimeisten vuosien aikana Bold Questissa on testattu Naton operaatioverkkokonsepti FMN:n mukaista federoitua johtamisjärjestelmää. Tämän kevään tapahtuma oli kautta aikojen suurin ja laajin Bold Quest, siihen osallistui kokonaisuudessaan 2200 henkilöä 14 maasta. Harjoitusverkko rakennettiin kiinteän runkoverkon päälle ja testejä tehtiin hajautetusti useasta eri maasta ja fyysisesti useammalla paikkakunnalla Suomessa. Tapahtuman johtoesikunta perustettiin Sodankylään kotijoukkoni Jääkäriprikaatin autohalliin, johtamisjärjestelmän johtoesikunta ja päätestipaikka olivat Riihimäellä.

Päävastuun harjoitusverkon ja sen palveluiden rakentamisesta kantoi Puolustusvoimien johtamisjärjestelmäkeskus. Verkon ja sen palveluiden rakentamiseen osallistui kaikkien puolustushaarojen, Logistiikkalaitoksen ja muiden Pääesikunnan alaisten laitosten johtamisjärjestelmähenkilöstöä. Tapahtuman ainutlaatuisuus ja laajuus edellyttivät uuden toimintamallin testaamista. PVJJK:n johdolla perustettiin toteutuksessa vaadittu C5-tehtäväkokoonpano,

joka vastasi tapahtuman operaatioverkon perustamisesta, sen johtamisesta ja valvonnasta. Tapahtuma mahdollisti hyvin kustannustehokkaalla tavalla puolustusvoimien johtamisjärjestelmän kansainvälisen yhteensopivuuden testaamisen sekä edisti osaltaan Puolustusvoimien kolmannen tehtävän mukaisia valmiuksiamme antaa ja vastaanottaa sotilaallista apua kiinteänä osana kansallisen puolustuskykymme kehittämistä. Yhdessä, yhtenä tiiminä järjestimme johtamisjärjestelmän isäntämaatuen. Tiimiin kuului henkilöstöä kaikista henkilöstöryhmistä, sotilaita ja siviilejä, miehiä ja naisia, palkattua henkilökuntaa ja asevelvollisia, varusmiehiä ja reserviläisiä. Tapahtuma suojattiin luonnollisesti kyberulottuvuudessa in and around -periaatteella

Koruttomasti voidaan todeta, että harjoitusverkko mahdollisti monikansalliset pinta- sekä ilmasta maahan ammunnat, laajuudessaan laajimmat puolustusvoimien historiassa. Bold Quest oli ensimmäinen yhteentoimivuuden kansainvälinen testaus- ja todentamistapahtuma Suomessa. Otimme aikamoisen riskin lähtemällä suoraan kovapanosammuntojen tukeen, mutta jälkikäteen voidaan todeta riskinoton kannattaneen. Mitään ylitsepääsemättömiä esteitä ei matkan varrella ilmennyt. Ylpeydellä esittelin suorituskykyämme eri puolilla Suomea yhdysvaltalaiselle kollegalleni, US Joint Staff J6:lle, kenraaliluutnantti B-J Shwedolle. Ylpeys tuli siitä, että joka puolilla näytettiin osaamista eikä powerpointteja tai tyhjiä puheita. Viesti oli yhtenevä: Mikään ei ole meille mahdotonta, vaikeat tehtävät tarvitsevat vain hieman aikaa. Saatu palaute oli jäätävää positiivisessa mielessä, vaikka siitä poistaa kaiken amerikkalaisen kohteliaisuuden.

Tästä on hyvä jatkaa eteenpäin. Tuleva seuraava laaja kansainvälinen harjoitus, jossa testaamme yhteensopivuuttamme on Arctic Lock -21, joka tarjoaa johtamisjärjestelmän näkökulmasta vastaavan kehittämismahdollisuuden kuin Bold Quest 19.1.

Bold Quest paransi merkittävästi johtamisjärjestelmäalan valmiutta kansallisen puolustuksen näkökulmasta. Yhtään liioittelematta voin todeta, että nyt meillä on todennettu isäntämaatuen toteuttamisvalmius ja varmistettu puolustusvoimien johtamisjärjestelmän kansainvälinen yhteensopivuus.

Puolustusvoimien johtamisjärjestelmäpäällikkö

Prkenr Mikko Heiskanen

TEKSTI: TERO PALOKANGAS
KUVAT: SUOMEN ERITYISEDUSTUSTO NATOSSA, SUOMEN PYSYVÄ EDUSTUSTO EU:SSA SEKÄ PÄÄESIKUNTA

EU-puheenjohtajuutta ja muuta ajankohtaista Brysselistä

Kirjoittaja palvelee apulaissotilasedustajana Brysselissä (johtamisjärjestelmien yhteensopivuus sekä kyberpuolustus) Suomen erityisedustustossa Natossa sekä Suomen pysyvässä edustustossa EU:ssa. Aikaisemmin hän on palvellut muun muassa pataljoonan komentajana Kainuun prikaatissa sekä osastoesiupseerina pääesikunnan operatiivisella osastolla.

Suomi on toiminut syyskauden 2019 EU:n neuvoston puheenjohtajamaana. Samaan ajankohtaan ovat ajoittuneet myös EU:n uuden komission muodostaminen, Brexit-keskustelut sekä EU:n tulevan budjetin ja Euroopan puolustusrahaston valmistelut. Sotilaallisen yhteistyön osalta Suomen painopistealueina ovat olleet digitalisaatio ja tekoäly. Syksyn aikana onkin käyty mielenkiintoisia keskusteluita siitä, miten nämä elintärkeäksi tunnistetut osa-alueet saadaan juurrutettua kiinteäksi osaksi EU:n sotilaallisten suorituskykyjen kehittämistä. Johtamisjärjestelmien yhteensopivuuden ja kyberpuolustusyhteistyön osalta ajat ovat pysyneet kiireisinä, sillä kyseiset osa-alueet ovat keskeisessä osassa puhuttaessa puolustusyhteistyöstä ihan minkä tahansa tahon kanssa.

Puolustusministeri Antti Kaikkonen seurueineen saapumassa Naton puolustusministerikokoukseen lokakuussa 2019. Suomi on luotettavana partnerimaana saanut viime vuosina säännönmukaisesti kutsun osallistua Naton päämies- ja ministeritason kokouksiin.

Kolmannen puheenjohtajuuden arkea

Puheenjohtajuus Euroopan Unionin neuvostossa kiertää vakiintuneessa järjestyksessä EU-maiden kesken ja vaihtuu puolivuosittain. Nykyinen 1.7.2019 alkanut puheenjohtajuuskausi on Suomelle kolmas, edelliset toteutuivat vuosina 1999 ja 2006. Puheenjohtajan tehtävänä on viedä eteenpäin EU:n lainsäädäntötyötä ja politiikka-aloitteita neuvostossa sekä huolehtia EU-asioiden käsittelyn jatkuvuudesta. Lisäksi puheenjohtaja edustaa neuvostoa suhteissa muihin EU:n toimielimiin, erityisesti

Euroopan parlamenttiin ja komissioon. Suomen EU-puheenjohtajakauden prioriteetteja ovat tällä kertaa olleet yhteisten arvojen ja oikeusvaltioperiaatteen vahvistaminen, kilpailukykyisempi ja sosiaalisesti eheämpi unioni, EU:n aseman vahvistaminen globaalina ilmastojohtajana sekä kansalaisten kokonaisturvallisuuden takaaminen. Puheenjohtajakaudet hoidetaan kolmen peräkkäisen puheenjohtajamaan ryhmissä. Maat tekevät yhdessä niin sanotun trio-ohjelman 18 kuukaudeksi. Suomi on toiminut kaudellaan samassa triossa edellisen puheenjohtajamaa Romanian ja seuraavan puheenjohtajamaa Kroatian kanssa.

Suomen pysyvällä EU-edustustolla (EUE) Brysselissä on ollut keskeinen rooli puheenjohtajakauden valmistelussa ja läpiviennissä. Konkreettisesti tämä on näkynyt esimerkiksi siinä, että EUE:n normaali ”rivivahvuus” on tuplaantunut normaalista noin sadasta henkilöstä hieman reiluun kahteensataan työntekijään. Koska samanaikaisesti ei puheenjohtajuuskautta varten vuokrattu mitään lisätoimitiloja, ovat edustuston toimistot ja yleiset tilat olleet varovaisestikin arvioiden kovalla käytöllä. Parhaimmillaan kahden hengen toimistoihin on puheenjohtajuuskauden ajaksi ahdettu neljä työntekijää ja lähes joka päivä edustuston yleisissä kokous- ja edustustiloissa on ollut useampia yhteistyötapahtumia. Toisaalta tiivis tunnelma on osaltaan ollut luomassa edustustoon puheenjohtajuuskauden ilmapiirin, jossa eri hallinnonalojen edustajat ovat aidosti puhaltaneet yhteiseen hiileen yhteisten etujen edistämiseksi ja puheenjohtajuuskauden onnistumiseksi.

Suomen puheenjohtajuuskauden kannalta haasteellista on ollut sen ajankohta. Vuoden jälkimmäinen puolisko on elokuun lomakuukaudesta ja joulun ajasta johtuen noin puolitoista kuukautta kevätkautta lyhyempi. Käytännössä siis puheenjohtajuuskaudelle asetetut tavoitteet on pitänyt saavuttaa esimerkiksi Romaniaan verrattuna huomattavasti lyhyemmässä ajassa. Toinen haaste on ollut uuden komission muodostaminen, joka on kestänyt ehkä tavanomaistakin pidempään. Käytännössä tämä on tarkoittanut, ettei Suomen puheenjohtajuuskaudella ole ollut mahdollista saada mitään uusia aloitteita liikkeelle. Kolmas iso haaste on ollut

EU:n sotilaskomitea toteuttaa osana kulloisenkin puheenjohtajamaan virallista ohjelmaa vierailukäynnin (EUMC Away Days) kyseiseen maahan. Kuvassa sotilaskomitean jäsenet yhteiskuvassa Säätytalon portailla Helsingissä syyskuussa 2019.

Brexit- neuvotteluiden hidas eteneminen. Vaikka EU-puheenjohtajamaalla ei neuvotteluiden etenemisessä ole juurikaan roolia, olisi päätöksen saaminen syksyn aikana ollut kaikkien osapuolten osalta toivottavaa. Nyt viimeisimpien päätösten perusteella lisäaikaa neuvotteluille on jatkettu tammikuun 2020 puolelle. Nähtäväksi jääkin päästäänkö silloinkaan asiakokonaisuudessa mihinkään pysyvämpään ratkaisuun.

Digitalisaatio ja tekoäly puolustuksessa

Euroopan unionin sotilaskomitea (englanniksi EUMC) on Euroopan unionin sotilaallista toimintaa johtava toimielin. Se on vastuussa yhteiseen turvallisuus- ja puolustuspolitiikkaan (YTPP) kuuluvien sotilaallisten toimenpiteiden valmistelusta. Sen tehtävä on myös ohjata sotilaallisten suorituskykyjen kehittämistä EU:ssa sekä antaa sotilaalliseen toimintaan liittyviä kannanottoja sekä suosituksia poliittisten ja turvallisuusasioiden komitealle (englanniksi PSC). Sotilaskomitea koostuu jäsenvaltioiden asevoimien komentajista, joilla kullakin on säännöllisissä kokoontumisissa oma sotilasedustajansa. Suomen sotilasedustajana toimii tällä hetkellä kontra-amiraali Juha Vauhkonen. Sotilaskomitea valitsee itse kolmeksi vuodeksi kerrallaan puheenjohtajan, jonka Euroopan unionin neuvosto valinnan jälkeen nimittää virkaan. Sotilaskomitean ensimmäisenä puheenjohtajana toimi vuosina 2001-2004 kenraali Gustav Hägglund. Sotilaskomitean puheenjohtajana toimii tällä hetkellä Italian asevoimien edellinen komentaja kenraali Claudio Graziano.

Suomen puheenjohtajuuskauden sotilaallisina kärkiteemoina ovat olleet digitalisaatio ja tekoäly puolustuksessa. Teemoihin liittyen laati Suomi yhdessä Hollannin, Ranskan, Saksan ja Viron kanssa keväällä ajatuspaperin digitalisaation ja tekoälyn huomioimisesta sotilaallisessa toiminnassa. Ajatuspaperissa nostetaan esille tarve hyödyntää jo yksityisellä sektorilla käytössä olleita ja siten luotettavia tekoälysovelluksia myös sotilaallisissa sovelluksissa. Keskeistä olisi kyetä tunnistamaan ne toiminnan osa-alueet, joilla tekoälysovellusten käytöstä olisi saatavissa parhaat hyödyt. Tekoälyssä ja sen tukemissa digitalisointiprojekteissa puhutaan mitä suurimmissa määrin ihmisten ja koneoppimisen kautta myös sovellusten osaamisesta, joka on keskeinen huomioitava tekijä. Tärkeää on myös kyetä löytämään ne yhteiseurooppalaiset instituutiot ja hankkeet, joissa asiakokonaisuuksia kyettäisiin parhaiten edistämään. Eettiset ja lainsäädäntönäkökulmat on ajatuspaperissa myös nostettu esille, mutta niihin ei ole ollut tarvetta suuremmin keskittyä. Poiketen maailmalla nousseista kysymyksistä tappajaroboteista ja niiden toiminnan eettisyydestä, ei osana EU:n puolustus-

ta kyseisiä suorituskykyjä olla missään tapauksessa kehittämässä.

Suomen johdolla digitalisaation ja tekoälyn kokonaisuutta osana eurooppalaista puolustusta on systemaattisesti käsitelty kuluneen puheenjohtajuuskauden aikana. Muun muassa sotilaskomitean eri tapahtumissa aihealueista on keskusteltu tiiviisti, ja niiden keskeinen merkitys on selkeästi tunnistettu. Haasteena asiakokonaisuuksien osalta on päästä kiinni konkreettiseen kehittämiseen. Sen verran paljon osin itseaiheutettuakin mystifiointia ja hypetystä varsinkin tekoälyn ja sen hyödyntämisen osalta on ollut havaittavissa. Tavoitteena onkin syyskauden aikana saada määritettyä konkreettiset ”askelmerkit” digitalisaation ja tekoälyn hyödyntämisestä eurooppalaisessa puolustuksessa. Keskeistä on saada ideat elämään EU:n rakenteissa myös Suomen puheenjohtajuuskauden jälkeen, ettei näissä elintärkeissä asiakokonaisuuksissa pääsisi jatkossa tapahtumaan mitään unohduksia. Suomen tavoitteena onkin saada ennen vuoden vaihdetta annettua EU:n sotilaskomitean kautta selkeä toimeksianto digitalisaation ja tekoälyn mahdollisuuksien selvittämiseksi ja käyttöönottamiseksi osana EU:n sotilaallisia toimenpiteitä ja suorituskykyjen kehittämistä.

Suomikuvan ja tärkeiden asiakohtien tukemista

EU:ssa on parin viime vuoden ajan keskusteltu osin kiihkeästikin Euroopan autonomiasta. Kysehän on pitkälti siitä, että pitkässä juoksussa Euroopan kiristyvät globaalit kilpailuasetelmat eivät pelkästään näytä positiivisilta. Muun muassa Yhdysvallat ja Venäjä sekä etenkin Kiina ovat haastamassa eurooppalaista hyvinvointia. Keskusteluilla on ollut myös turvallisuuspoliittinen näkökulmansa. Euroopan tulee kyetä jatkossakin vastaamaan tarvittaessa alueensa turvallisuudesta ilman ulkopuolisten tahojen tukea. Etenkin Natopuolella ja sen Pohjois-Amerikkalaisten jäsenmaiden keskuudessa ajatusten on osin tulkittu haastavan perinteisen Transatlanttisen yhteistyön. Tästähän ei asiakokonaisuudessa ole kuitenkaan lopunperin kysymys. On kaikkien läntisten yhteistyöosapuolten etujen mukaista,

Arkiseen aherrukseen tarvitaan välillä sopivaa vastapainoa. Brysselin varuskunnan väki perheineen perinteisellä sotahistorian matkalla keväällä 2019. Matka suuntautui tällä kertaa Hollantiin operaatio ”Market Gardenin” maisemiin.

että Eurooppa on mahdollisimman vahva ja yhtenäinen toimija. Esimerkkinä jo mainitun digitalisaation ja tekoälyn näkökulmasta on huolestuttavaa, että kaikki keskeiset alan teknologiajätit ovat muulta kuin Euroopasta. Sama koskee keskeisten IT-alan komponenttien omavaraisuutta, jota ainakaan tällä hetkellä ei eurooppalaisittain ole riittävästi olemassa. Globaalissa kilpailussa menestyminen edellyttäisikin jatkossa entistä enemmän IT-alan tutkimus- ja kehittämistoimintaan satsaamista.

Sotilaallisten suorituskykyjen kehittämiseen liittyvä taloudellinen vipuvarsi on ollut rakentumassa jo pitkään suunnitellun Euroopan puolustusrahaston (European Defence Fund, EDF) varaan. Rahasto on ennen kaikkea EU:n puolustusteollisuutta tukeva aloite, joka samalla tukee loppukäyttäjien eli unionin jäsenmaiden asevoimien suorituskykytarpeita. Monivuotisen rahoituskehyksen vahvistuttua ja rahaston toteutuessa suunnitellussa muodossaan, olisi sen kautta tiettyjen ehtojen täyttyessä mahdollista kohdentaa vuosina 2021-2027 noin 13 miljardin euron rahoitus puolustusta tukeviin projekteihin. Lisäbonusta voisi ansaita projekteista, jotka toimeenpannaan pysyvän rakenteellisen yhteistyön (PRY) puitteissa. PRY:n osalta ”kivenä kengässä” on kuitenkin viime aikoina ollut niin sanottu kolmansien maiden osallistumisoikeus. Kyse on siis siitä, millä ehdoilla esimerkiksi Yhdysvalloilla, Norjalla tai jatkossa Isolla-Britannialla olisi mahdollista päästä mukaan EDF:n rahoituksella tuettuihin projekteihin. Asiaan linkittyy voimakkaasti jo aikaisemmin mainitut EU:n pyrkimykset strategiseen autonomiaan, ts. riittävän omavaraiseen teknologiaan ja teollisuuteen, sekä toisaalta eri osapuolten kauppapoliittiset intressit. Parhaillaan kolmansien maiden osallistumiskysymystä pyritään ratkaisemaan Suomen tekemän kompromissiesityksen pohjalta, joka toteutuessaan toisikin mainion ”lisäsulan” puheenjohtajuuskautemme hattuun.

EU-Nato yhteistyö on Suomelle keskeinen aihe, jota pyritään kaikin keinoin edesauttamaan. Esimerkkinä digitalisaatioon ja tekoälyyn liittyen Suomi on alusta alkaen puhunut EU-Nato yhteistyön merkityksestä myös kyseisillä osa-alueilla. Mielestämme ei ole mitään järkeä pyrkiä taklaamaan näitä samoja haasteita useassa eri paikassa samaan aikaan. Jatkossa olisikin tärkeää kyetä tunnistamaan entistä aikaisemmin yhteisiä intressejä sisältävät hankkeet ja pyrkiä kustannustehokkaasti toisiaan tukien asetetut tavoitteet saavuttamaan. EU ja Nato ovat jokunen vuosi sitten virallisesti sopineet yhteistyöstä 74:llä eri osa-alueella. Parhaillaan selvitellään virallisestikin edistymistä noilla eri osa-alueilla, mutta selvää on, että ihan maalissa ei kaikkien tavoitteiden osalta vielä varmastikaan olla. Keskeisiä haas-

teita yhteistyölle ovat ainakin rajoitteet luokiteltujen tietojen vaihdossa sekä poliittiset jännitteet järjestöjen eri jäsenmaiden kesken. Välillä onkin ollut turhauttavaa seurata, miten poliittisten linjausten perusteella ollaan valmiita uhraamaan muuten lupaavilta vaikuttavia konkreettisia yhteistyön muotoja.

Samaan aikaan Natossa

Suomen erityisedustusto Natossa (NAE) on hieman reilun kahdenkymmenen ihmisen työyhteisö, joka edesauttaa paikan päällä Brysselissä Suomen puolustusyhteistyötä Naton kanssa. Tehtäviin kuuluu myös Naton kehittymisen seuraaminen ja siitä kotimaahan raportoiminen. Kuluvan vuoden aikana keskustelua Natossa ovat hallinneet keskustelu pelotteesta ja puolustuksesta. Natohan on vuoden 2014 jälkeen palannut omaan perustehtäväänsä eli oman alueen puolustamiseen. Pitkään Naton agendaa täyttivät kriisinhallintaoperaatiot ja erilaiset kumppanuudet, mutta nykyisin painopiste on selvästi kollektiivisen puolustuksen (artikla 5) asiakokonaisuuksissa. Toinen merkittävä seikka on ollut keskustelu taakanjaosta ja etenkin vaatimus riittävistä panostuksista puolustukseen. Etenkin Yhdysvallat on tiukasti vaatinut kahden prosentin tason saavuttamista puolustusrahoituksen osalta (BKT:n verrattuna), johon tällä hetkellä Naton jäsenmaista vain pieni osa yltää. Loputkin liittolaiset ovat viime vuosina panostuksiaan lisänneet, mutta ihan lähivuosina ei kaikkien jäsenmaiden osalta tuohon asetettuun tavoitteeseen tulla pääsemään.

Kuluvaa vuotta Natossa on leimannut keskustelut Yhdysvaltojen ja Venäjän välisen INF-ohjussopimuksen päättymisestä. Vaikka Nato ei ole ollut varsinaisena jäsenenä sopimuksessa, voivat sen päättymisen vaikutukset luonnollisesti vaikuttaa osaltaan kaikkiin Nato-maihin. Nato on tukenut julkisesti suurimman jäsenmaansa toimia todetessaan sopimuksen päättyneen, vaikka pinnan alla on ollut toki havaittavissa päinvastaisiakin äänenpainoja. Aivan viime aikoina liittokunnan välejä on kiristänyt myös Turkin hyökkäykset Syyriassa. Jäsenmaiden keskuudessa onkin välillä esitetty poikkeuksellisenkin voimakkaita ja luonteeltaan teot tuomitsevia puheenvuoroja, vaikka pääosa liittokunnan jäsenistä ymmärtää hyökkäyksen taustalla olevat Turkin turvallisuusongelmat. Tähän kiehuntaan voidaan lisätä vielä Turkin tekemä päätös S-400 ilmatorjuntajärjestelmän ostamisesta Venäjältä ja Yhdysvaltojen samalla perumat F-35 kaupat. Kovistakin puheenvuoroista huolimatta on Turkki Naton jäsenmaana niin tärkeä, että muulla liittokunnalla ei varmastikaan lopunperin ole intressejä sitä erottaa. Etenkään kun erottamiselle ei Naton perusasiakirjasta edes löydy omaa kohtaansa ja siten valmista prosessia.

FMN johtamisjärjestelmien yhteensopivuuden mahdollistajana

Federated Mission Networking (FMN) on Naton sponsoroima operaatioverkkokonsepti, jossa on tarkoituksena jo normaalioloissa rakentaa valmiiksi erilaisissa mahdollisissa käyttötarkoituksissa (esimerkkinä operaatiot) tarvittava johtamisjärjestelmien yhteensopivuus. Ohjelmassa yhteensopivuuden kehittäminen toteutetaan iteratiivisen kehittämisen periaattein niin sanottujen spiraaleiden kautta. Tällä hetkellä käytössä ovat ohjelman spiraali kahden mukaiset kyvykkyydet. Samanaikaisesti kolmannen spiraalin suorituskykyjä rakennetaan ja neljännen spiraalin vaatimuksia viimeistellään. Ohjelmassa päivitetään jatkuvasti aina kymmenen vuoden päähään ulottuvaa suunnitelmaa, jossa pyritään asetettujen operatiivisten vaatimusten perusteella ennustamaan eri vaiheissa mahdollisesti käyttöön otettavia teknologioita ja sovelluksia. Yhteensopivuudessa on teknisen yhteensopivuuden lisäksi keskeistä myös toimintatapoihin ja ihmisten väliseen yhteensopivuuteen liittyvät osakokonaisuudet. Tavoitetilassa puhutaan siis todennetusta operatiivisesta yhteensopivuudesta FMN-valmiiden joukkojen ja johtoportaiden välillä. Hyvänä käytännön esimerkkinä käy keväällä 2019 Suomessa toteutettu kansainvälinen Bold Quest 19.1 -harjoitus, jonka johtamisjärjestelmäratkaisut toteutettiin FMN-ohjelman periaatteiden ja vaatimusten mukaisesti.

FMN-ohjelmassa on lähestytty johtamisjärjestelmien yhteensopivuutta pragmaattisesti. Tavoiteasettelussa ensimmäisten spiraalien osalta on puhuttu lähinnä kiinteiden johtoportaiden välisestä yhteistoiminnasta niin sanottujen johtamisen peruspalveluiden osalta. Jatkospiraaleissa tavoitteet siirtyvät kohti liikkuvien joukkojen välistä taktisen tason yhteensopivuutta. Vaatimustason kasvaessa on samalla ollut havaittavissa myös ensimmäiset todelliset haasteet. Ohjelman aikataulua aikoinaan määritettäessä päädyttiin ensimmäisten spiraalien osalta niin sanottuun kompressoituun aikatauluun, jossa tietylle spiraalille ei ollut varattu sille tavoitetilassa varattua aikaikkunaa (kaksi vuotta määrittelyä, kaksi vuotta rakentamista ja kaksi vuotta käyttöä). Pääosalle jäsenistä aikataulu onkin ollut liian tiukka. Siksipä viime kevään ohjauskokouksessa päätettiin ottaa vuoden aikalisä spiraalin neljä lopullisten määritysten hyväksymisen osalta. Samalla päädyttiin selvittämään perusteellisesti ohjelman työryhmärakenne ja toimintatavat, jotta jatkossa vältyttäisiin vastaavilta haasteilta. Selvitystyö onkin vauhdissa ja sen mukaisia alustavia havaintoja ja

Euroopan Unionin sotilaskomitean puheenjohtaja kenraali Claudio Graziano Kaartin jääkärirykmentin apulaiskomentajan eversti Rainer Kuosmasen vieraana tutustumassa varusmieskoulutukseen Santahaminassa syyskuussa 2019.

toimenpide-esityksiä käsitellään kuluvan syksyn ohjauskokouksessa.

Suomelle FMN-ohjelma on tällä hetkellä keskeisin väline johtamisjärjestelmien kansainvälisen yhteensopivuuden varmistamiseksi. Kansallisten johtamisjärjestelmien kehittämisessä pyritäänkin varmistamaan kaikin keinoin, että muun muassa tehdyt teknologiavalinnat ja järjestelmäratkaisut ovat linjassa FMN-ohjelman tulevien kehitysspiraaleiden kanssa. Suomelle on myös tärkeää, että kansainvälisesti yhteensopivia järjestelmiä ei tarvitse olla useampia, vaan riippumatta tarpeen laadusta (esimerkkinä Nato, EU- tai YK-johtoiset operaatiot), voidaan tarpeeseen vastata samoilla FMN-pohjaisilla järjestelmillä. Suomen kannalta olisikin ehdottoman tärkeää, että EU:n sotilasesikunta (EUMS) pääsisi vihdoin liittymään ohjelmaan mukaan. EUMS on ollut ohjelmassa jo useiden vuosien ajan tarkkailijajäsenenä, ja on nyt viimeisen vuoden ajan pyrkinyt pääsemään täysjäseneksi. Käytännön tasolla yhdelläkään osapuolella ei varmasti ole mitään liittymistä vastaan. Poliittinen peli Naton päämajassa on kuitenkin toistaiseksi estänyt sellaisten liittymissanamuotojen hyväksymisen, jotka kaikille osapuolille kävisivät. Toivottavasti tässäkin diplomatiahaasteessa päästäisiin pian maaliin ja jatkamaan konkreettista yhteistyötä eri osapuolten välillä.

Kyberpuolustusyhteistyön haasteista

Natossa kyberulottuvuus tunnistettiin operatiivisena toimintaympäristönä vuoden 2016 Varsovan huippukokouksessa. Siitä lähtien Nato on entistäkin systemaattisemmin kehittänyt omaa kyberpuolustustaan. Konkreettisena esimerkkinä tästä on Naton Euroopan joukkojen pääesikuntaan (SHAPE) perustettu kyberoperaatiokeskus, jonka tehtävänä on koordinoida kyberoperaatioita osana Naton harjoituksia ja kokonaisoperaatioita. Kyber on esiintynyt Naton viimeaikojen isoissa harjoituksissa tasavertaisena toimintaympäristönä, jonka pohjalta jäsenmaat ovat pyrkineet tunnistamaan kyberpuolustukseen liittyviä mahdollisuuksia ja rajoitteita. Nato ei lähtökohtaisesti kehitä hyökkäyksellisiä suorituskykyjä kyberoperaatioihin liittyen, mutta tietyt jäsenmaat ovat ilmoittaneet antavansa omia hyökkäyksellisiä suorituskykyjään tarvittaessa Nato-operaatioiden tueksi. Toinen merkittävä keskustelun kohde on ollut kybertapahtumien rinnastaminen aseelliseen vaikutukseen ja siten Naton artikla viiden kynnyksen ylittymiseen. Nato ei tule julkisesti kyseistä määrittelyä julkistamaan, koska se antaisi samalla mahdollisille vastustajille etulyöntiaseman operoida tuon kynnystason alapuolella. Joka tapauksessa harkinta kybertoimien rinnastettavuudesta artikla viiden mukaisiin tapahtumiin tehdään liittokunnassa joka kerta tapauskohtaisesti erikseen.

Suomella on ainoana Naton kumppanimaana voimassa oleva yhteistyösopimus kyberpuolustuksen osalta. Sopimukseen liittyen on laadittu erillinen toimeenpanosuunnitelma yhteistyön konkreettisista muodoista. Suunnitelmaa päivitetään aina vuosittain käytävien yhteistyöneuvottelujen yhteydessä, jolloin tarkastellaan suunniteltujen yhteistyömuotojen toteutumista sekä määritetään seuraavan vuoden tavoitteet. Keskeisiä yhteistyömuotoja ovat olleet muun muassa tutkimusprojektit, koulutus- ja harjoitustoiminta sekä tilannetietoisuuden vahvistaminen. Jatkossa on tarkoituksena päästä yhteistyössä yhä enemmän konkreettisempaan tekemiseen. Käytännössä tämä voisi tarkoittaa esimerkiksi tilannesidonnaisen informaation jakamista erilaisista kybertapahtumista sekä asiantuntijoiden vaihtoa. Haasteelliseksi kansainvälisen kyberyhteistyön tekee tietojen vaihtamiseen liittyvät sopimukset ja rajoitukset, jotka etenkin monenvälisessä yhteistyössä ovat haastavia. Toiseksi haasteen muodostaa henkilöstöresurssien rajallisuus. Vaikka Puolustusvoimissa parhaillaan satsataankin merkittävästi kyberpuolustukseen, ovat samat asiantuntijat haluttuja sekä kotimaan puolustuksessa että kansainvälisisillä foorumeilla. Kyberpuolustusyhteistyö eri toimijoiden kesken vaatiikin mitä suurimmissa määrin jatkuvaa tarveharkintaa ja resurssien tarkkaa priorisointia.

EU on etenkin yhteiskuntien kyberturvallisuuden osalta merkittävä toimija, onhan sillä jäsenmaihin nähden lainsäädäntövaltaa. EU:ssa onkin säädetty viime vuosina muun muassa kyberturvallisuuden perusvaatimuksiin

Suomen Nato- ja EU-edustustojen yhtenä tavoitteena on tuoda esille kansallista osaamistamme aina sopivissa tilanteissa. Kuvassa kapteeni Juha Kukkola Maanpuolustuskorkeakoulusta esittelemässä "Game Player" –tutkimuksen tuloksia Naton päämajassa järjestetyssä lounastilaisuudessa heinäkuussa 2019.

liittyviä säädöksiä. Samoin EU:n niin kutsutun kyberdiplomatiatyökalupakin käyttö on asiakokonaisuus, jota jatkuvasti harjoitellaan ja kehitetään. Työkalupakki sisältää merkittävän määrän erilaisia poliittisia ja taloudellisia vastatoimenpiteitä, jos vihamielisiä kybertoimia EU:n jäsenmaihin kohdistuisi. Tässä päästään myös kybertoiminnan yhteen merkittävimpään haasteeseen eli syyksi lukemiseen (attribuutio). Kyberympäristössä kybertoimen teknisten jälkien peittäminen on taitavan toimijan näkökulmasta kohtuullisen helppoa. Tällöin syyksi lukemisessa joudutaan todennäköisimmin aina turvautumaan tapahtuman poliittiseen kokonaisarviointiin muiden käytettävissä olevien todisteiden perusteella. EU:ssa kyber on syyskuussa sotilaskomiteassa tehdyn päätöksen perusteella tunnistettu nyt myös operatiiviseksi toimintaympäristöksi. EU:n sotilasesikunta (EUMS) rakentaakin parhaillaan tuon samaisen päätöksen perusteella toimeenpano-ohjelmaa vuosille 2020-2023 EU:n sotilaallisten rakenteiden suojaamiseksi sekä YTPP-operaatioiden kyberpuolustuskykyjen kehittämiseksi.

Puolustusvoimain tuore komentaja kenraali Timo Kivinen toivottamassa Euroopan Unionin sotilaskomitean jäsenet puolisoineen tervetulleiksi juhlaillalliselle osana EUMC Away Days -ohjelmaa syyskuussa 2019.

Lopuksi

Puolustusyhteistyö niin Natossa kuin EU:ssa on laisemme pienen maan kannalta välttämättömyys. Mahdollisen eurooppalaisen kriisin tapauksessa on epätodennäköistä, että pysyisimme ainakaan täysin sen ulkopuolella. Toisaalta taas mahdollisen alueellisen kriisin kohdistuessa meihin, on kansainvälisen yhteistyön ja avun vastaanottamisen merkitys ilmeinen. Ollaksemme auttamisen arvoinen, on meidän kyettävä se asema päivittäisellä työllämme ansaitsemaan. Tässä työssä monenvälisellä puolustusyhteistyöllä EU:ssa ja Natossa on aivan keskeinen merkityksensä. Erityisesti EU meidän keskeisenä viitekehyksenä ja arvoyhteisönä on taho, jonka kanssa yhteistyöhön meidän soisi jatkossa, ehkä nykyistäkin enemmän panostavan.

Puolustusyhteistyön keskiössä ovat toiminnan luonteesta riippumatta (Nato, EU, kahdenvälinen) mitä suurimmassa määrin aina johtamisjärjestelmien yhteensopivuus ja kyberpuolustus. Näiltä osin onkin henkilökohtaisesti ollut erittäin haastavaa ja mielenkiintoista olla pieneltä osaltaan tässä työssä mukana, johon viime aikoina Suomen EU-puheenjohtajuus on tuonut myös oman ainutkertaisen mausteensa mukaan. Vaikka puheenjohtajuuskautemme alkaa tämän artikkelin ilmestyessä olla ohi, riittää kansainväliseen yhteensopivuuteen liittyen meillä kaikilla jatkossakin työsarkaa. Yhteistyössä on jatkossakin muistettava teknisten näkökulmien lisäksi myös prosessien ja ennen kaikkea ihmisten välinen yhteensopivuus.

TEKSTI: SEPPO URO
KUVAT: SEPPO URO, SA-KUVA JA MUSEOVIRASTO

Talvisodan viestitaktiikasta

Talvisodan syttymisestä tuli marraskuun lopulla kuluneeksi kahdeksankymmentä vuotta. Neuvostojoukkojen hyökkäys yllätti niin suomalaiset kuin myös Suomen puolustusvoimat hyvin puutteellisesti varautuneina tuleviin taisteluihin. Näin oli asianlaita myös viestiaselajin kohdalla. Perustettuihin viestijoukkoihin ei rauhan vuosina ollut koulutettu riittävästi henkilöstöä eikä joukkoja yleensä voitu varustaa edes supistettujen määrävahvuuksien mukaisella materiaalilla. Lisäksi käytössä olleen kaluston suorituskyky oli tuleviin tehtäviin nähden vaatimatonta. Myös viestitaktiikan kehittely ja koulutus oli jäänyt varsin vähäiseksi ja alaa ohjeistava kirjallisuus saatiin joukkojen ja johtoportaiden käyttöön vasta aivan talvisodan kynnyksellä. Varsinaiset viestitaktiikan ohjesäännöt syntyivät vasta viime sotien jälkeen.

Ensimmäinen viestitaktiikkaakin hiukan käsitellyt teos oli toukokuussa 1934 julkaistu Viestimiehen käsikirja. Sen laativat luutnantti Reino Arimo (1908-91) ja luutnantti Valtteri Makkonen (1902-81), jotka molemmat palvelivat tuolloin kouluttajina Viestipataljoona 1:ssä Santahaminassa. Kirjaa voinee hyvällä syyllä pitää nykyisen Viestimies-kirjan varhaisena edeltäjänä ja se olikin tarkoitettu käytettäväksi lähinnä asevelvollisten viestialiupseerien ja -miesten opetuksessa jonkinlaisena käsikirjana ja näiden luettavana oppikirjana. Tekijöiden mukaan 190-sivuinen kirjanen sopi kuitenkin käytettäväksi myös suojeluskuntien viestiosastoissa, eri kursseilla, sotakouluissa yms., missä tuli kyseeseen viestipalveluksen alkeitten tunteminen. Kirja antoi perustiedot viestipalveluksen yleisistä järjestelyistä ensisijaisesti viestipataljoonan ja sitä pienempien viestiyksiköiden näkökulmasta. Viestitaktiikan peruskäsitteistä kuvattiin viestirunko, viestihaarat, viestiasemat, viestikeskukset ja viestinkeräyspaikat. Lyhyesti käsiteltiin myös tykistön viestipalvelusta sekä viestipalveluksen järjestelyä taistelutoiminnan eri vaiheissa. Huomiota herättää käsittelytapa, jossa hyökkäystaistelun johtamis- ja viestitoiminta esitetään ensimmäisenä. Perusteellisimmin kirjassa käsitellään puhelinyhteyksien rakentamista sekä viestiliikennettä. Kirja levisi varsin laajasti viestihenkilöstön keskuuteen ja siitä valmistui jo kolmas painos juuri ennen talvisotaa. Neljäs painos otettiin jatkosodan alkaessa vuonna 1941.

Ensimmäisen varsinaisen viestitaktiikan oppikirjan "Alijohdon viestitaktiikan pääpiirteet" käsikirjoitus valmistui syyskuussa 1939. Kirjan laati kapteeni Risto Kare (1905-82), joka vuodesta 1934 aina talvisotaan saakka toimi Reserviupseerikoulun viestilinjan johtajana ja pääkouluttajana. Kirjan sisällön Kare koosti lähinnä siitä oppimateriaalista, jota hän käytti koulutuksessaan. Kirja tuli painosta vasta keväällä 1940, mutta syntyhistoriastaan johtuen ainakin 1930-luvun loppuvuosina RUK:n käynyt nuorempi viestiupseeristo tunsi kirjassa käsitellyt asiat. Noin 180-sivuisessa kirjassa käsitellään varsin johdonmukaisella tavalla mm. viestijohtajan tehtäviä, yhteyksien aikaansaamisen yleisiä periaatteita sekä yhteyksiä eri taistelulajeissa. Tekstiä elävöittävät lukuisat havainnolliset kuvat ja kaaviot. Ilmeisen merkittävä on myös luku, jossa käsitellään viestitilanteen arvostelua, viestisuunnitelmaa ja viestikäskyjä. Vaikka aineisto oli tarkoitettu ensisijaisesti joukkueenjohtajatasoisille viestiupseereille, monet asiat olivat varsin yleispäteviä ylemmillekin viestijohtajille.

Laajemmin myös ylempien johtoportaiden viestitoimintaa ja viestitaktiikkaa käsittelevä teos "Viestitoiminta" ilmestyi painosta vuoden 1939 lopulla. Kirjassa ei ole mainintaa sen tekijästä eikä siinä ole johdantoa kertomassa teoksen tavoitteista, sisällöstä eikä syntyhistoriasta. Kirjan kirjoittivat 1930-luvun lopulla yhteistoiminnassa everstiluutnantti Veikko Veijola (1900-76) ja kapteeni Veikko Saura (1901-49), osittain myös luutnantti Martti Honkasalo (1909-85). Heistä Veijola kävi Sotakorkeakoulun sekä Ranskassa että Suomessa ja toimi Sotateknillisen Koulun johtajana vuosina 1936-39. Saura opiskeli Sotakorkeakoulussa vuosina 1936-38 ja palveli sen jälkeen toimistoupseerina Puolustusministeriössä. SKK:ssa hän laati diplomityön aiheesta "Missä määrin nykyinen viestijohto ja nykyiset viestijoukot vastaavat tarkoitustaan meikäläisissä olosuhteissa". Ehkäpä tästä syystä Sauran panos kirjan aikaansaamisessa lienee ollut suurin. Honkasalo opiskeli Sotateknillisessä Koulussa vuosina 1938-39, minkä jälkeen hän toimi Pää-

majassa viestikomentajan adjutanttina. Kirjan syntyhistoria ilmenee lyhyesti K. J. Mikolan Viestitoiminta Suomessa -teoksesta, mutta tarkempi kuvaus paljastui eversti Honkasalon kuoltua hänen perillistensä Viestimuseolle luovuttamasta materiaalista. Sen joukossa oli myös Viestitoiminta-kirja, jonka nimilehdellä näkyy himmeällä punaisella em. tekijöiden nimet. Kirjan välissä oli ruutupaperille käsin kirjoitettu seuraava selostus:

"Huom. Punaisella merkitty mainінta "Viestitoiminta"-kirjan tekijöistä pitää paikkansa. Kirjaa kirjoitettiin iltaisin keväällä 1939 Sauran kotona. Minäkin osallistuin työhön jonkin verran. Työtä jatkettiin syyskuussa 1939, mutta silloin ei Veijola ollut mukana. Käsikirjoitus Sauran käsialalla kirjoitettuna saatiin valmiiksi syys-lokakuun vaihteessa. YH:n alkuaikana sitä yritettiin saada painoon ohjesäännön luontoisena ja virallisella vahvistuksella varustettuna. Kun tähän ohjesääntöpuolella ei suostuttu se annettiin sellaisenaan Otavalle koneella kirjoitettuna. Painokseksi yritettiin muistaakseni saada 800 kpl, mutta montako sitä lopulta painettiin en enään muista. Ollessani YH:n aikana Tilkassa viikon verran ylirasituksen takia toimitti Saura korehtuuria siellä luettavakseni. Sotien jälkeen Sauran kuoltua lähetti rva Saura minulle monta kansiota Sauran papereita. Näiden joukossa oli mainitsemani käsikirjoitettu kappale, jonka päälle Saura oli kirjoittanut nimeni niinkuin muissakin saamissani kansioissa, jotka pääasiassa sisälsivät SKK:ssa pidettyjä luentoja. Kirjan jakelu tehtiin Viestiosastossa ilmeisesti YH:n lopussa ja joulukuussa. Jakelutapaa en muista, mutta selvinnee se Viestiosaston arkistosta. Olin jakelussa avustamassa adjutantin ominaisuudessa. M. Honkasalo 2.11.78"

Noin 230-sivuisessa kirjassa käsitellään varsin perusteellisesti viestitoimintaa valtakunnalliselta tasolta sotatoimiyhtymään ja joukko-osastoon saakka. Päälukuja ovat Viestijohdon sekä viestijoukkojen ja -elimien järjestely, Viestitoiminnan yleinen järjestely sekä Viestitoiminnan järjestely erilaisten sotatoimien yhteydessä. Puhelinyhteyksien keskeinen merkitys näkyy tässäkin ohjesäännössä, mutta mukana ovat edelleen myös vilkut, liput, tuli- ja savumerkkivälineet samoin kuin viestikyyhkynen ja viestikoira. Monipuolisuudessaan kirja on aikanaan antanut eri johtoportaissa toimineille viestijohtajille hyvät perusteet alan järjestelyille. Kirja olisi luonnollisesti pitänyt olla käytettävissä jo vuosia aikaisemmin, jotta se olisi laajemmin ollut tuttu alalla toimineille johtajille. Muistitiedon mukaan kirjan aineistoa jaettiin eräille viestiupseereille kuitenkin jonkin verran jo käsikirjoitusvaiheessa, niin että ainakin osa viestijohdosta lienee tuntenut kirjan sisällön viimeistään jo YH:n aikana. Viestitaktisten ohjesääntöjen niukkuutta talvisodassa helpottivat jonkin verran mm. Kenttäohjesäännön yleinen osa, Esikuntaopas sekä vuonna 1934 ilmestynyt Viestiliikenneohjesääntö.

Evl Veikko Saura.

Evl Risto Kare.

Edellä kerrottuun viitaten on hyvä tarkastella, kuinka talvisodan johtamis- ja viestitoiminnassa onnistuttiin. Jo sodan aikana joulukuussa 1939 Päämajan viestitoimiston päällikkö jääkärieverstiluutnantti Mauno Liesi laati kriittisen muistion, jossa hän kertoi Päämajan viestikomentajalle eräitä havaintoja mm. YH:n aikaisesta toiminnasta. Yleisenä havaintona hän toteaa, että "viestitoimintaa YH:ssa vaikeutti suuresti se tietämättömyys tilanteesta ja tehtävästä, joka yleisenä vallitsi. Se kaksinaisuus, jota ylläpidettiin osaksi rauhantilana osaksi sotatilana, lisäsi vaikeuksia ja aiheutti varsinkin kalustohankinnoissa viivytyksen, jonka tulokset uhkaavat vaikuttaa kohtalokkaasti kaluston loppumisen muodossa". Liesi kritisoi voimakkaasti mm. heikkoa tiedonkulkua, tietämättömyyttä sotajaotuksesta ja yhtymien esikuntien sijoituspaikoista, posti- ja lennätinlaitoksen yhteyksien käytön heikkoa lkp-valmiutta, viestiupseeriston niukkuutta ja kalustohankintojen sekavuutta. Hän kiinnittää huomiota myös siihen epäluottamukseen, jota yleisjohtajat tunsivat viestiyhteyksien toimivuutta kohtaan. Hän päättää muistionsa toteamalla, että "se halveksiva suhtautuminen tämän aselajin tehtävään, jonka aselaji on saanut osakseen rauhanaikaisissa valmisteluissa oli hyvin lähellä johtaa arvaamattomaan sekaannukseen koko YH:n tärkeässä tehtävässä".

Sodan jälkeen laadittiin lukuisia laajoja selvityksiä ja tutkimuksia, joissa pyrittiin kartoittamaan eri alojen toimintaa sodan aikana. Myös välirauhan aikainen Maavoimien viestikomentaja jääkärieverstiluutnantti A. R. Saarmaa laati laajan selvityksen otsikolla "Sodan antamia kokemuksia viestitoiminnasta". Näiden havaintojen perusteella käynnistettiin välirauhan aikana lukuisia toimenpiteitä, joilla tehostettiin koulutusta, kehitettiin ja hankittiin uutta viestimateriaalia sekä parannettiin toimintamenetelmiä. Näitä havaintoja ja toimenpiteitä on aikanaan käsitelty myös Viestimies-lehden palstoilla.

TEKSTI JA KUVAT: VIESTIMIES

Viestiupseeriyhdistyksen syyskokous 20.9.2019

Viestiupseeriyhdistyksen syyskokous pidettiin perinteisesti Riihimäellä Maasotakoululla Viestikoulun tiloissa. Tilaisuuteen saapui runsaslukuinen joukko yhdistyksen jäseniä. Paikalla oli aamupäivällä noin 50 henkilöä ja lisää väkeä saapui iltapäivän A.R. Saarmaa-päivän paikallispuolustusseminaariin.

Tilaisuuden avasi Viestiupseeriyhdistyksen puheenjohtaja Juha Petäjäinen. Syyskokouksen puheenjohtajaksi valittiin Veli-Pekka Kuparinen ja sihteeriksi Harri Reini. Tulevan vuoden toimintasuunnitelma noudatteli pääpiirtein tuttuja linjoja. Erityisesti keskustelua ja kommentteja herätti toimialan vapaaehtoiskentän yhdistymiseen ja yhteistyön tiivistämiseen tähtäävä työ. Esityslistan kohdassa talous todettiin yhdistyksen talouden olevan varsin vakaalla pohjalla kahden vuoden sykleissä tarkasteltuna. Joka toinen vuosi järjestettävät seminaarit tasapainottavat taloutta mukavasti. Kokouksessa päätettiin hallituksen esityksestä nostaa jäsenmaksua 20 eurosta 25 euroon.

Yhdistyksen kevät kokous on suunniteltu järjestettävän kiertävällä periaatteella, tällä kertaa, Merisotakoululla huhtikuun aikana. Syyskokous perinteisesti Riihimäellä 25.9.2020. Yhdistyksen jäsenmatkaa on suunniteltu elo-syyskuulle, mutta kohde ei ollut vielä selvillä. Ilmoitus jäsenmatkasta tullaan julkaisemaan lehden sivuilla viimeistään numerossa 2/2020. Lisäksi jatketaan yhdistyksen jäsenille tarjottavaa mahdollisuutta vierailla/tutustua johtamisjärjestelmäalan erilaisten toimijoiden luona. Toimituksen ja yhdistyksen sihteerille voi ilmoittautua, mikäli haluaa isännöidä tilaisuuksia.

Viestiupseeriyhdistyksen toiminnan viestintää pyritään kehittämään kokonaisvaltaisesti ja yhdistää myös osaksi Viestimies-lehden viestintä kanavana. Syyskokous valitsi yhdistyksen puheenjohtajaksi jatkamaan yksimielisesti Juha Petäjäisen.

Viestiupseeriyhdistyksen puheenjohtaja Juha Petäjäinen avasi kokouksen.

Kokouksen puheenjohtajana toimi Veli-Pekka Kuparinen ja sihteerinä Harri Reini.

Muissa asioissa Rauli Parmes esitteli tekemäänsä kirjaa Siviilivarautumisen historiaa – kriisit ja hallinto. Kirjoittaja lupasi laatia artikkelin Viestimies-lehteen, joten kaikki pääsevät kurkistamaan teokseen artikkelin verran. Artikkeli julkaistaan 1/2020 lehdessä ja sen yhteyteen laitetaan linkki, mitä kautta kirjaa voi tilata itselleen.

Kokouksen päätyttyä siirryttiin Luokkatalon aulaan palkitsemisiin. Palkittavia oli runsaasti ja pääosa oli myös päässyt paikan päälle. Tilaisuuden alussa Seppo Uro toi terveiset ikikaaderin Olli Vuorion 100-vuotissyntymäpäiviltä, jotka vietettiin Marsalkka Mannerheimin hengessä nauttien hyvästä ruuasta, juomasta ja seurasta. Onnea vielä ikikaaderille. Palkittavia oli kultaisella-, hopeisella- ja pronssisella ansiolevykkeellä sekä Vuoden viestiupseerin julkistaminen että Vuoden Viestimies-lehden kirjoittajien palkitseminen.

Kultaisella ansiolevykkeellä palkittiin seuraavat henkilöt: Jussi Liesiö, Veli-Pekka Kuparinen, Pertti Hyvärinen, Tarja Tahvanainen, Esa Kaakinen ja Harri Virtanen.

Hopeisella ansiolevykkeellä palkittiin Pirkko Kuparinen, Auli Hänninen, Martti Vasankari, Jukka-Pekka Pelttari ja Mikko Hyppönen.

Pronssisella ansiolevykkeellä palkittiin Pekka Kastemaa, Martti Susitaival, Hannu Wallenius, Esko Sutela, Antti Tiilikainen, Kalevi Halonen, Hannu Harklin ja Jouni Salmi. Lisäksi jaettiin edellisenä vuotena jakamatta jääneet pronssiset ansiolevykkeet seuraaville henkilöille Aki Kallio, Mikko Karikytö, Marko Lähteenmäki, Mauri Mikkonen, Soili Puranen, Heikki Rantanen, Jouko Seitakari, Mika Seppä, Petri Siivonen, Aki Siponen ja Ismo Viljanen.

Vuoden viestiupseeriksi valittiin komentajakapteeni Carl-Magnus Gripenvaldt. Henkilötoimittaja haastatteli Vuoden viestiupseeria ja artikkeli on tämän lehden lopussa. Viestimies-lehden vuoden kirjoittajina palkittiin Pasi Mäkinen ja kapteeni Kimmo Frilander. Pasi Mäkinen kirjoittaa Analysaattorin vakiopalstaa johtamisjärjestelmäalan arjen haasteista pakina tyylillä. Toisena kirjoittajana palkittiin kapteeni Kim-

Kokouksen osanottajia oli runsaasti paikalla.

Seppo Uro toi terveiset ikikaaderin Olli Vuorion 100-vuotissyntymäpäiviltä.

mo Frilander, joka kirjoitti useamman artikkelin kyberistä viime vuoden lehteen, joissa hän toi uusia tai ainakin toisenlaista näkökulmaa kyberiin ja sen mahdollisuuksiin.

Toimitus onnittelee kaikkia palkittuja!

Palkitsemisten jälkeen kokousväki siirtyi Varuskuntaravintola Lieteen kokouslounaalle, jonka jälkeen päivä jatkui A.R. Saarmaa – paikallispuolustusseminaarin puitteissa. Seminaarin jälkeen nautittiin perinteinen Viestimiespäivällinen Riihimäen Upseerikerholla.

Toisena vuoden kirjoittajana palkittiin Kimmo Frilander.

Yhdistyksen puheenjohtaja Juha Petäjäinen onnitteli vuoden viestiupseeria Carl-Magnus Gripenwaldtia.

Seminaarin jälkeen nautittiin perinteinen Viestimiespäivällinen Riihimäen Upseerikerholla.

TEKSTI: JUHA PELTOMÄKI
KUVAT: JUHA PELTOMÄKI, MPK RY., PUOLUSTUSVOIMAT

A.R. Saarmaa seminaari 20.9.2019

Paikallispataljoonan valmistautuminen taisteluun

Viestikiltojen liitto järjesti paikallispuolustuksen johtamista ja viestitoimintaa käsittelevän A.R. Saarmaa -seminaarin 20.9.2019 klo 12.00 - 16.00. Tilaisuuden järjestelyt toteutettiin yhteistoiminnassa puolustusvoimien, Viestiupseeriyhdistyksen ja Maanpuolustuskoulutusyhdistyksen (MPK) kanssa. Tilaisuuden keskuspaikka oli Riihimäellä Viestikoulun luokkatalossa, luokka Saarmaassa. Seminaarin puheenjohtajana toimi eversti Jarmo Vähätiitto Pääesikunnan johtamisjärjestelmäosastolta.

Tilaisuuteen osallistui yhteensä noin 160 henkilöä 16 paikkakunnalta. Suurin osanottajamäärä oli Riihimäellä, jossa osallistujat mahtuivat juuri ja juuri luokka Saarmaahan. Paikkakunnat liitettiin seminaariin PV:n joukko-osastojen ja aluetoimistojen kautta TUVE-videoneuvottelupalvelun välityksellä.

Seminaarin teemana oli “Paikallispataljoonan valmistautuminen taisteluun”. Seminaarin tavoite oli syventää luennoin ja case-tarkasteluin osallistujien tietoutta paikallispuolustuksen joukoista, johtamisesta ja johtamisjärjestelmästä sekä puolustushaarojen ja Puolustusvoimien johtamisjärjestelmäkeskuksen roolista ja tehtävistä paikallispuolustuksen tukena.

Seminaarin kohderyhmänä oli paikallispataljoonaan sijoitetut johtajat ja viestihenkilöstö, paikallispuolustuksen kehittämiseen osallistuva henkilöstö, viesti- ja johtamisjärjestelmäalan vapaaehtoisten maanpuolustusjärjestöjen jäsenet sekä maanpuolustuskoulutusyhdistyksen henkilöstö ja jäsenjärjestöjen jäsenet.

Ohjelman punainen lanka - lähtökohtatilanteesta yksityiskohtaisempaan, teoreettisesti konkreettisempaan.

Tavoitteena oli päästä yhtenäiseen, kohtuullisen syvälle porautuvaan näkökulmaan huomioiden esitysten korkein suojaustaso STIV - käyttö rajoitettu. Esitysten painopiste oli tällä kertaa paikallispuolustuksen sotilaallisten joukkojen johtamisessa, ei viranomaisyhteistyössä.

Seminaarin ohjelman suunnittelun perusajatuksena oli yhteinen paikallispuolustuksen lähtökohtatilanne, jota kaikki esitykset tarkensivat ja syvensivät omasta näkökulmasta. Jokainen esitys porautui lähtökohtatilanteeseen tuoden esille oman puolustushaaran,

toimialan tai joukon erityispiirteitä. Lähtökohtatilanne oli kuin joulukalenteri, josta kukin esiintyjä aukaisi oman luukun esityksellään.

Seminaarin avasi Viestikiltojen liiton puheenjohtaja evl Jukka-Pekka Virtanen. Hän toivotti osallistujat tervetulleiksi kertoen Saarmaa-päivään liittyvää historiatietoa. Tilaisuudessa oli yhteensä 10 esitystä. Seminaarin aluksi oli kaksi esitystä taustoittamaan käsitteitä ”paikallispuolustus” ja hybridiuhka.

Paikallispuolustus - lähellä kansalaista ja yhteiskuntaa

Panssariprikaatin operaatiopäällikkö, evl Petri Siivonen, kertoi paikallispuolustuksen tehtävistä, merkityksestä ja kehittämisestä.

Paikallisjoukot ovat paikallisiin taistelu- ja tukemistehtäviin käytettäviä sodan ajan joukkoja, joiden kokonaisvahvuus maavoimien joukoista on 20%. Paikallispataljoona on aluevastuussa oleva paikallisjoukko, joka luo muille alueella oleville joukoille toimintakentän perustan. Paikallispataljoona johtaa viranomaisyhteistyön vastuualueellaan ja tukee muita viranomaisia sotilaallisen maapuolustuksen tehtäviä vaarantamatta.

Paikallisjoukkojen päätehtäviä ovat alueiden valvonta, kohteiden suojaaminen ja joukkojen perustaminen. Lisäksi tehtävinä voi olla erikoisjoukkojen vastainen toiminta, taistelutehtävät, sissitoiminta, vastuualueen tiestön ja alueiden käytön suunnittelu ja johtaminen, liikenteen ohjaaminen, etsintä- ja pelastustehtävät, sotavankien käsittely, joukkojen koulutus ja asevelvollisuusasioiden hoito.

Paikallispuolustuksen merkittävimpiä kehittämiskohteita ovat mm. johtamisrakenne ja toimintatavat, tulivoima kalustolla ja materiaalihankinnoilla, osaamisen kehittäminen ja yhteistyö MPK:n kanssa sekä johtamiskyky uudistetulla organisaatiolla ja innovatiivisilla arjen välineillä.

Jos kaikki on hybridisodankäyntiä - mikään ei ole hybridisodankäyntiä.

Kapteeni Niko Makkonen Maavoimien esikunnasta tarkasteli esityksessään hybridisodankäynnin käsitettä, hy bridioperaatioiden rakennetta ja kansallista varautumista hybridiuhkiin. Kapteeni Makkonen esitti hybridisodankäynnille kaksi määritelmää: ”Toiminta, jolla pyritään erilaisia, toisiaan täydentäviä keinoja käyttäen ja kohteen heikkouksia hyödyntäen saavuttamaan omat tavoitteet.” Toisena määritelmänä mainittiin: ”Tavanomaisten ja epätavanomaisten sodankäynnin menetelmien yhdistäminen.”

Toimintaympäristö on muuttunut monimutkaisemmaksi ja ilmiöiden keskinäisriippuvuus on lisääntynyt, jolloin sodankäynnin keinovalikoima on monipuolistunut. Hybridivaikuttamisen keinot voivat olla esimerkiksi taloudellisia, poliittisia tai sotilaallisia. Hybridivaikuttamisessa voidaan käyttää myös teknologiaa ja sosiaalista mediaa. Keinoja voidaan käyttää samanaikaisesti tai siten, että ne seuraavat toisiaan. (Hybridi)vaikuttaminen räätälöidään aina kohteen ja tavoitteiden mukaisesti. Laajan keinovalikoiman joustava käyttö sekä vaikuttamisen intensiteetti vaihtelevat tilanteen ja tavoitteiden mukaisesti.

Hybridivaikuttamista voi olla vaikeaa tunnistaa. Suomalainen kokonaismaanpuolustuksen periaate luo vahvan perustan hybridiuhkiin varautumiselle. Varautumista tukee mm. kansallinen riskiarvio 2018 sekä yhteiskunnan turvallisuusstrategia.

Lähtökohtatilanne - paikallispataljoonan taistelujaotus ja alueella toimivat joukot.

Kaikki esitykset sidottiin Varsinais-Suomen aluetoimiston päällikön, everstiluutnantti Joni Lindemanin, laatimaan lähtökohtatilanteeseen. Lähtökohtatilanne oli laaja ja perusteellinen. Lähtökohtatilanteesta kyettiin esittämään kuulijoille annetussa ajassa ainoastaan pintaraapaisu, mutta sillä pystyttiin luomaan perusta paikallispataljoonan toiminnalle esittelemällä paikallispataljoonan tehtävät, toimintaympäristö, yhteistyötahot ja paikallispataljoonan vastuualueella olevat toimijat. Suunnitteluvaiheessa lähtökohtatilannetta täydennettiin siten, että kaikille esityksille löytyi oma ”kalenterinluukku”.

Kybertoimintaympäristö operaatioalueena

Kapteeni Maria Keinonen PVJJK:sta kertoi PVJJK:n roolista ja tehtävistä osana kyberpuolustusta. PVJJK tuottaa omalla toiminnallaan välillisen kybersuojan paikallispataljoonan taistelulle. Tarvittaessa paikallispataljoonaa voidaan tukea vaikkapa analysointikykyisten partioiden toiminnalla.

Kybertoimintaympäristö operaatioalueena ei ole yhteneväinen fyysisen maailman rajojen kanssa, vaan ulottuu niitä laajemmalle. Tämän takia kyberpuolustus on monimutkainen kokonaisuus, johon tarvitaan toimenpiteitä alkaen puolustusvoimallisista kokonaisuuksista päätyen yksilön tekemiin toimenpiteisiin. Kyberpuolustuksessa tulee huomioida kaikki joukon käyttämät johtamis-, TVM- ja asejärjestelmät ja niiden suojaaminen.

Puolustusvoimien vastuualueena ovat operatiiviset ja taktiset järjestelmät sekä verkot. Puolustusvoimien toiminta, data ja informaatio eivät kuitenkaan rajoitu vain näille alueille, vaan sijaitsevat tai riippuvat myös TUVE-runkoverkosta ja TUVE-palveluista. Internetin merkitystä ei ole syytä väheksyä, koska se muodostaa keskeisen toiminta-alueen tiedonsiirron, informaatioympäristön, tiedonhankinnan, kansalaisten asioinnin sekä joidenkin korkeamman suojaustason palveluiden tiedonsiirtoalustana.

Kyberpuolustusta käytetään palveluihin ja toimintaan kohdistuvien uhkien havaitsemiseen sekä tieto- ja tietoliikennejärjestelmien suojaamiseen. Pääperiaatteena on, että Puolustusvoimien johtamisjärjestelmäkeskus vastaa yhteiskäyttöisten palveluiden suojaamisesta ja puolustushaarat omista järjestelmistään. Kyberpuolustus edellyttää myös aktiivista viranomaisyhteistyötä ja yhteistyötä kumppanien kanssa.

PVJJK:n taistelee yhteyksien puolesta

Kapteeni Juha-Matti Salmenpohja PVJJK:sta kertoi verkko-osaston tuesta paikallispataljoonalle. Normaaliolojen valmisteluvaiheen tukimuotoja ovat mm. liityntäpisteiden rakentaminen ja testaus, osallistuminen arjen välineiden kehittämiseen ja testaukseen, koulutta-

jatuki eri harjoituksissa ja operatiivinen suunnittelu yhteistyössä tuettavien joukkojen kanssa

PVJJK liittää paikallispataljoonan sen esitysten mukaisesti kiinteään runkoverkkoon liityntäpisteiden kautta. Liityntäpiste voi olla nopeasti käyttöönotettava, etukäteen valmisteltu liittymä esim. viestiasemalla. Toisena mahdollisuutena on ottaa käyttöön operaattoreiden kuituja ja viestiasemia. Kolmantena vaihtoehtona liityntäpisteen rakentamiseksi on PVJJK:n johtamisjärjestelmäpataljoonan toteuttamat kaapeli- ja linkkiyhteydet.

Liityntäpisteen kautta saatavia palveluita ovat mm. operatiiviset-, hallinnolliset- ja kohdearkkitehtuurin palvelut.

Meri- ja Ilmavoimat paikallispuolustuksen tukena ja tuettavana

Majuri Sauli Hongisto Merivoimien esikunnasta ja majuri Jari Koskinen Ilmasotakoulusta kertoivat meri- ja ilmapuolustuksen toiminnasta paikallispataljoonan tukeen liittyen. Puolustushaarojen ja paikallisjoukkojen välisessä yhteistoiminnassa korostuvat alueen käyttöön ja suojaamiseen liittyvät asiat.

Ilmavoimien osalta taistelutukikohdat ja tukikohtaosastot vastaavat paikallisten järjestelyjen tarkentamisesta johtamisen ja yhteistoiminnan varmentamiseksi sekä kohteiden suojauksen, johtamisjärjestelmäyhteyksien ja huollon järjestelyiden toteuttamiseksi.

Tärkeimmät yhteen sovitettavat asiat ovat tilannetietoisuuden ylläpito, tilannekuvan vaihto, logistiikan ja tukeutumisen järjestelyt, alueiden ja tiestön käytön sopiminen, tulenkäytön järjestelyt, alueiden vartiointi, erikoisjoukkotoiminnan havainnointi ja mahdollinen estäminen, yhteiset paikallispuolustuksen järjestelyt sekä tukikohtien ja kenttien käyttö tai kenttien käytön estäminen.

”Nyt on lupa tehdä ja käyttää arjen ratkaisuja.”

Seminaarissa joulukalenterin ”aatonluukku” oli ”Arjen ratkaisut” -demo, jossa majuri Niko Koivula Viestikoululta ja Tuomo Muuttoranta esittelivät konkreettista ”arjen ratkaisua” - Reserviläisen tilannekuvajärjestelmää

Arjen ratkaisujen toimintamalli. Taustakuvan lähde: https://cyberwarzone.com/wp-content/uploads/2014/05/cyber-warfare-wallpaper-WORLD-cyberwarzone.com_.jpg.

RESTIKU. RESTIKU:a käytettiin lähtökohtatilanteessa paikallispataljoonan maakuntakomppanian johtamisjärjestelmänä.

RESTIKU on omaehtoisesti toteutettu kehitysprojekti sekä demonstraatio kyvykkyyksistä, joita avoimen lähdekoodin ohjelmistoilla on mahdollista saada aikaan. Tavoitteena on tuottaa vaatimusten mukainen johtamiskyvykkyys, joka vastaa myös kyberturvallisuuden sekä käytettävyyden haasteisiin.

RESTIKU on järjestelmä, joka sisältää taistelunjohtojärjestelmään kuuluvat oleellisimmat palvelut: puhe, sanoma, tiedostonhallinta sekä paikkatieto- ja karttapalvelut. Tietoliikennealustana toimii Internet. Järjestelmän looginen arkkitehtuuri perustuu useiden ilmaisten, avoimen lähdekoodin ohjelmistojen hyödyntämiseen. Järjestelmä voidaan asentaa eri tietokonemalleille, ja siihen liittyvän loppukäyttäjän päätelaite voi olla käytännössä mikä tahansa henkilökohtainen arjen viestiväline.

RESTIKU on yksi esimerkki aktiivisten reserviläisten innovaatioista ja kyvystä hyödyntää omaa osaamistaan toimivien palveluiden rakentamiseksi. Teknisen kyvykkyyden lisäksi on luotava toimintamallit ja käyttöohjeet palveluiden tehokkaan käytön mahdollistamiseksi. Erilaiset tarpeet havaitaan ja opitaan parhaiten harjoituksissa. RESTIKU-ratkaisua onkin käytetty mm. paikallispuolustusharjoituksissa tänä syksynä.

Vapaaehtoiset paikallisjoukkojen kouluttajina - merkittävä voimavara.

MPK:n koulutuspäällikkö Juha Niemi ja Viestikiltojen liiton koulutuspäällikkö evl Juha Peltomäki kertoivat MPK:n johtamisjärjestelmä- ja viestikoulutuksen koulutusohjelman toimeenpanosta. MPK:n johtamisjärjestelmä- ja viestikoulutuksen koulutusohjelma muodostuu seuraavista kokonaisuuksista:

MPK:n johtamisjärjestelmä- ja viestikoulutusohjelma päivitetään kuluvan vuoden loppuun mennessä. Arjen välineet kursseja uusitaan nykyisen näkemyksen mukaiseksi. Uutena kokonaisuutena koulutusohjelmaan tulee johtamisjärjestelmä- ja viestijohtajien johtajakoulutuksen suunnittelu (komppanian päällikkö-, joukkueenjohtaja- ja ryhmänjohtajakurssit). Sähkövoima ja -turvallisuuskoulutuskokonaisuus koulutusohjelma siirretään PVLOGL:n ohjaukseen.

MPK:n tavoite on, että parin seuraavan vuoden aikana rekrytoidaan sekä koulutetaan kouluttajat ja kurssinjohtajat, jotka jalkauttavat koulutusohjelman kurssit kentälle. Viestikiltojen jäsenten on osallistuttava aktiivisesti MPK:n koulutustarjontaan, hankittava osaaminen ja päästävä mukaan MPK:n kouluttajapooleihin jalkauttamaan koulutusohjelmaa.

Evl Juha Peltomäki kertoi kokemuksiaan yhdestä MPK:n aselajikouluttajakurssin toimeenpanosta, jonka hän johti Riihimäellä. Harjoituksen toteutettiin reserviläiskouluttajien toimesta. Kouluttajat olivat sekä teknisesti että pedagogisesti osaavaa joukkoa. Koulutustapahtumat toteutettiin kaikin puolin laadukkaasti ja asiantuntevasti. Aselajikouluttajakurssin oppilaat olivat erittäin motivoituneita ja innokkaita. Reservissä on voimaa!

MPK:n johtamisjärjestelmä- ja viestikoulutusohjelman rakenne.

Arjen määritelmät.

Saarmaa-seminaari 2020 - konkreettisesti ja käytännönläheisesti paikallispuolustuksen parissa.

Saadun palautteen perusteella osallistujajoukko oli varsin tyytyväinen päivän antiin. Esityksien sisältö oli aikaisempiin seminaareihin verrattuna konkreettisempaa, yksityiskohtaisempaa ja toisiaan tukevia. Puheenjohtaja piti tilaisuuden erinomaisesti hallinnassa. Tilaisuuden tekniset järjestelyt toimivat hyvin, ja tilaisuus saatiin vietyä läpi suunnitellulla tavalla.

Osa yleisöstä kaipasi esityksiin lisää konkretiaa ja käytännön kokemuksia harjoituksista, vuorovaikutteisuutta, lisää aikaa keskustelulle, aiheiden ja joukon hajauttamista pienempiin osakokonaisuuksiin sekä esitystä operaattoreiden kriisivalmiudesta.

Yleisesti voidaan todeta, että esitykset olivat korkealaatuisia ja tilaisuudelle asetetut tavoitteet saavutettiin. Järjestävä organisaatio esittää parhaimmat kiitokset tilaisuuden esiintyjille ja osallistujille. Tilaisuuden puheenjohtaja, eversti Vähätiitto, jakoi esiintyjille muistoksi ja kiitokseksi Viestiupseeriyhdistys ry:n julkaisun ”Kyberajan viestitaktiikka”.

Ensi vuonna tilaisuus järjestetään 25.9.2020 pääpaikkana Riihimäki. Aihepiiri muodostunee käytännönläheisesti paikallispuolustuksen ympärille: kokemukset arjen ratkaisuista paikallispuolustuksen harjoituksissa, arjen ratkaisujen tuotteistaminen ja ylläpito, arjen infra, kybersietoisuus sekä koulutus. Jotakin tuon suuntaista, vuoden 2019 seminaarista saatu palaute huomioiden. Tervetuloa.

TEKSTI: TATU TAHKOKALLIO
KUVAT: TATU TAHKOKALLIO, PUOLUSTUSVOIMAT

Varusmiehistäkö arjen ratkaisujen kehittäjiä?

DI Tatu Tahkokallio tekee siviili jatko-opiskelijana MPKK:n Operaatiotaidon ja taktiikan laitokselle väitöskirjatutkimusta, joka pyrkii selvittämään millaista taktiikkaa tulee taisteluteknisellä tasolla noudattaa, kun johtamisjärjestelmäsuorituskyvyt perustuvat arjen ratkaisuihin. Tahkokallio on toiminut tutkijana PVTO2017 3.1-projektissa ja toimii siviilissä Space Systems Finland Oy:n Defence -liiketoiminta-alueen päällikkönä.

Arjen ratkaisuja on kokeiltu ja tutkittu vuodesta 2015 alkaen Puolustusvoimien tutkimuslaitoksen ja Maanpuolustuskorkeakoulun ohjauksessa. Toteuttavina käsipareina projekteissa ovat toimineet sekä reserviläiset että MPKK:n opiskelijat. Vuonna 2017 tutkimustyö sai lisäpontta Verkostoituminen arjen ratkaisuilla -tutkimusprojektin (PVTO2017 3.1) käynnistyttyä. Projekti on tehnyt yhteistyötä mm. Aluetoimistojen ja Maanpuolustuskoulutusyhdistyksen kanssa jalkauttamalla kokeiluja paikallispuolustusharjoituksiin ja MPK:n sotilaallisia valmiuksia palveleviin harjoituksiin. Kuluvan vuoden kevättalvella projektikonsortio, KAARTJR ja kirjoittaja kävivät keskustelua arjen ratkaisujen hyödyntämisestä KEHÄ19 harjoituksessa. Aiemmista kokeiluista poiketen harjoitukseen ei ollut tarjolla valmiita ratkaisuja, vaan varsinaiset käyttäjät - sotilaspoliisikomppanian varusmiehet - päätettiin ottaa mukaan innovoimaan ja kehittämään omat ratkaisunsa. Syntyi Arjesta suorituskykyä -varusmieskerho.

Arjesta suorituskykyä -varusmieskerhon ideana oli palvella kahta eri tavoitetta. Ensinnäkin KAARTJR oli halukas jatkamaan arjen ratkaisujen kokeiluja ja toisaalta tutkimusprojektin intressinä oli kerätä havaintoja arjen ekosysteemin kehittymisestä. Tutkimusprojektille ekosysteemi edustaa toimijoita, toimintaa, kehitettyjä ratkaisuja ja muutosta, jotka yhdessä tähtäävät arjen ratkaisujen käytön edistämiseen. Kerhon päätavoitteiksi asetettiin arjen välineisiin perustuvan push-to-talk (PTT) puhepalvelun kehittäminen sekä palvelun perustamiseen, käytön tukeen ja hallintaan tarvittavien varusmiesvalmiuksien edistäminen.

Kerhon valmistelu, suunnitelma ja ohjaajat

Paikallispuolustusharjoituksen (PAPU) valmistelutyö alkoi konsortion ja KAARTJR:n välillä helmikuussa 2019. Varsinainen kerhoon liittyvä valmisteluvaihe alkoi kuitenkin vasta huhtikuussa. Tällöin pidettiin ensimmäinen suunnitelupalaveri, jossa läsnä olivat konsortion edustajat (Elisa, Bittium, Insta DefSec), KAARTJR:n edustaja sekä allekirjoittanut tutkijan roolissa.

Kenelle tahansa lupaa varusmiesten tutkimiseen tai heitä tutkimukseen osallistamiseen ei PV myönnä. Tämän lisäksi osallistumisen tulee aina perustua vapaaehtoisuuteen. Tässä tapauksessa tutkimus oli osa Puolustusvoimien omaa tutkimusohjelmaa (PVTO2017) ja siksi ylipäätään mahdollista. Lopullinen puoltava päätös tarvittiin kuitenkin joukko-osastosta. Ilman joukko-osaston lupaa ei kerhoa voitaisi järjestää.

Toukokuussa pidettyyn toiseen suunnittelupalaveriin saatiin iloisena uutisena tieto, että KAARTP:n komentaja oli myöntänyt kerholle luvan. Samalla saatiin myös tietää, että kerhon tueksi oli luvattu sotilaspoliisikomppaniasta palkattu kouluttaja, joka sai käyttää työtunteja kerhoiltojen toteuttamiseen. Kouluttajan osallistuminen kerhon toimintaan osoittautui nopeasti hyvin tärkeäksi, sillä hänen avullaan voitiin koordinoida lukuisia käytännön asioita, kuten komppanian luokkatilan varaaminen, kerhoiltojen sovittaminen komppanian palvelusrytmiin, kerhon muiden vetäjien päästäminen sotilasalueelle ja kerhon tavoitteiden sitominen tulevaan PAPU2-harjoitukseen.

Kerhon lopulliset tavoitteet lyötiin lukkoon kesäkuun alussa pidetyssä suunnittelupalaverissa. KAARTJR:n näkemykseen mukaan suurin tarve olisi push-to-talk puhepalvelulle, jonka avulla voi puhua puhelimeen VHF-

radiopuhelimien kaltaisesti painamalla tangenttia tai tätä vastaava painiketta pohjaan. Samassa yhteydessä pohdittiin tietoturva-asioita ja keskusteltiin mm. omalle tietokoneelle asennettavan PTT-palvelimen hyödyistä ja haitoista verrattuna valmiin pilvipalvelun käyttöön.

Kerholle annettiin mahdollisuus ajan ja resurssien puitteissa innovoida PTT-puhepalvelun lisäksi muitakin arjen ratkaisuja. Lisäksi tehtävätaktiikkaan liittyvien toimintamallien dokumentointi koettiin jo tässä vaiheessa tärkeäksi, mutta varusmiesten koulutus- ja kokemuspohjan epäiltiin olevan tehtävään liian suppea. Vastuu toimintamallien dokumentointi- ja kehitystyöstä jäi lopulta henkilökunnan hartioille.

Kerhon ohjaajatiiminä toimi palvelumuotoilija Ville Raassina Elisalta, sotilaspoliisikomppanian kouluttaja ja allekirjoittanut. Taustatukea ohjaajatiimi sai kadetti Sami Rauténilta, joka auttoi mm. puhepalvelupalvelimen konfiguroinnissa sekä Elisan palvelumuotoilijoilta Reetta Mailalta ja Laura Hiedolta, jotka pitivät varusmiehille palvelukehitysluennon ja ideointisession.

PTT-puhepalvelu ja käytetyt laitteet

Konsortiolla ja KAARTJR:llä oli kokemusta edellisen vuoden KEHÄ18-harjoituksesta, jossa kokeiltiin Internetistä ladattavaa ilmaista Wire-pikaviestipalvelua. Kokemukset tästä olivat hyviä ja vastaavalla mallilla etsittiin nyt sopivaa PTT-puhepalvelua. Nopean Googletuksen ja työpöytävertailun jälkeen ensisijaiseksi PTT-palvelukandidaatiksi haarukoitui Zello, samalla kun muitakin ehdokkaita oli tarjolla: kaupallinen Voxer ja online-pelaajien keskuudesta alkunsa saaneet TeamSpeak ja Mumble. Lopulta päädyttiin open source -ohjelmistokoodiin perustuvaan Mumbleen lähinnä siksi, että palvelu oli täysin ilmainen ja tähän liittyvä palvelinohjelmisto oli mahdollista asentaa omalle palvelintietokoneelle.

Eräs arjen ratkaisujen käyttöön liittyvä perusperiaate on, että arjen ratkaisua ei voi muuttaa, vaan ratkaisuun on tyydyttävä sellaisena kuin se on saatavilla. Pikaviestipalvelu WhatsAppin käyttöönotto toimii tästä hyvänä esimerkkinä; sovelluskaupasta ladattava sovellus on kaikille sama ja palveluun ei juuri voi lisätä tai poistaa toiminnallisuuksia. *Arjen ratkaisun kehittäminen tarkoittaakin olemassa olevan ratkaisun konfigurointia omaan tarpeeseen sopivaksi*, eikä kokonaan uuden tuotteen tai palvelun kehittämistä. Ajattelu saattaa tuntua kankealta, mutta käytännössä mallin hyvänä puolena on mahdollisuus ottaa uusia ja valmiiksi testattuja ratkaisuja nopeasti käyttöön. Huonona puolena on, ettei ratkaisujen kehittämistä tai lopettamista (esim. poistoa sovelluskaupoista) voi ulkopuolelta käsin ohjata.

Arki-kerhon rekrytointiesite.

Valitun avoimeen lähdekoodiin perustuvan Mumble-puhepalvelun kehitystyö oli käytännössä päättynyt versioon 1.2 vuonna 2009, paljon ennen kerhon alkamista. Palvelinohjelmisto (Mumble) ja päätelaiteohjelmat eli Appit sekä iOS (Mumblefy) että Android (Plumble) käyttöjärjestelmille ovat tästä huolimatta edelleen ladattavissa Internetistä. Silti arki pääsi yllättämään kerhon ohjaajat, kun välittömästi viimeisen kerhoillan jälkeen Mumble-palvelimesta ilmestyi uusi versio 1.3 kymmenen vuoden kehitystauon jälkeen (www.mumble.info). Valitettavasti uusia versioita päätelaiteohjelmista ei samanaikaisesti ilmaantunut, joten projekti päätyi käyttämään palvelimen vanhempaa versiota 1.2.19.

Harjoituksen suunnitteluvaiheessa KAARTJR linjasi, että varusmiesten omia puhelimia ei syksyn PAPU2-harjoituksessa käytetä. Koska kerhon toiminta tähtäsi kyseiseen harjoitukseen, oli toiminta sovitettava linjauksen mukaiseksi. Avuksi tulivat KAARTJR:n erikseen hankkimat älypuhelimet sekä PVTUTKL:lta lainatut kannettavat tietokoneet, joihin puhepalvelin oli tarkoitus asentaa.

Rekrytointi

Rekrytointia varten Elisan palvelumuotoilijat tekivät A3-kokoisen julisteen, jonka varusmiesten kouluttaja kiinnitti komppanian ilmoitustauluille. Viestin perillemenoa tehostettiin pitämällä komppanian päällikön luvalla viikko-ohjelmaan merkitty rekrytointioppitunti. Oppitunnilla kerrottiin kerhon tavoitteista, painotettiin kerhon vapaaehtoisuutta ja yritettiin motivoida varusmiehiä mukaan kerhoon lupaamalla ilmaista pizzaa ja virvoitusjuomia kerhoiltoihin. Nämä osoittautuivatkin matkan varrella hyviksi porkkanoiksi.

Rekrytointioppitunnilla kiinnostus kerhoa kohtaan vaikutti hyvin polarisoituneelta; joko kerho ei kiinnostanut lainkaan tai sitten arjen ratkaisujen kehittäminen innosti ja kirvoitti kielet vilkkaaseen keskusteluun. Oppitunnin jälkeen luokkaan jäi jopa kaksi varusmiestä keskustelemaan kerhosta tarkemmin.

Ensimmäinen kerhoilta

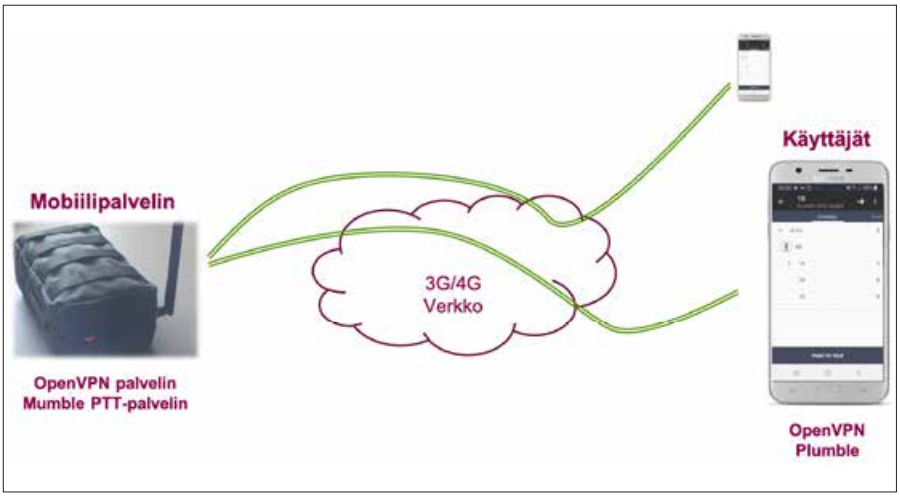
Rekrytointioppitunnin jälkeen ohjaajien odotukset olivat suhteellisen korkealla ja tunne siitä, että ensimmäiseen kerhoiltaan voisi saapua reilun ryhmän verran varusmiehiä oli vahva. Toisin kävi. Ensimmäisenä kerhoiltana (17.6.2019) luokkaan valui juuri ja juuri kolme henkilöä. Syykin selvisi pian: monilla oli alkanut iltavapaa ja kaupungin riennot olivat houkutelleet pois varuskunnasta. Ohjaajien keskuudesta oli aistittavissa pientä pettymystä; mikä meni pieleen?

Ilta saatiin lopulta käynnistettyä ja pienen alkukankeuden jälkeen varusmiehet kuuntelivat kokeilutoiminta- ja palvelumuotoiluluennon, osallistuivat tarpeiden ja käyttötapauksien ideointiin sekä asensivat tulevaa Mumble-palvelinta varten debian 9 -käyttöjärjestelmän yhdelle kannettavista tietokoneista. Kerholaiset sopivat myös yhteisen WhatsApp-ryhmän perustamisesta, jota käytettäisiin kerhon epävirallisena viestintäkanavana. Ja lopulta he söivät myös paikalle tuotua pizzaa...

Illan aiheista kokeilu- ja palvelumuotoilun teorialuento oli varusmiehille selvästi liian korkealentoinen. Abstraktit konseptit ja niiden käsittely ei ollut heille selvästikään tuttua. Ideoinnissa varusmiehet pysyivät jo selvästi paremmin mukana. Kuitenkin vasta alettaessa asentamaan tietokoneeseen käyttöjärjestelmää varusmiehet olivat elementissään ja selvästi paremmin omalla vahvuusalueellaan.

Teoriasta konkretiaan

Toinen kerhoilta pidettiin heinäkuun 10. päivä, jolloin paikalle saapui kahden partion verran varusmiehiä mukaan lukien kaksi viestialiupseeria. Ensimmäisestä kerhoillasta oli otettu oppia ja toisella kerralla panostettiin siihen, että varusmiehet saatiin nopeasti toiminnan pariin. Tässä hyödynnettiin ohjaajien Internettiin etukäteen asentamaa salasanalla suojattua Mumble-palvelinta. Varusmiesten tehtäväksi jäi KAARTJR:n hankkimien älypuhelinten käyttöönotto ja näihin PTT-puhepalvelusovellus Plumblen asennus ja konfigurointi palvelinta vasten.



Arjen PTT-palveluratkaisu.

Työ käynnistyi asettamalla puhelimiin prepaid SIM-kortit. Tämän jälkeen puhelimiin asennettiin Google-tili, jotta PTT-sovellus olisi mahdollista ladata Googlen sovelluskaupasta. Kunkin puhelimen tietoturvaa parannettiin siten, että puhelimiin aktivoitiin näytön lukituskoodi, paikkatietopalvelut kytkettiin pois päältä, käyttö- ja diagnostiikkadatan lähetys estettiin ja varmuuskopiointi kytkettiin pois päältä. Plumblen asentamisen jälkeen varusmiehille jaettiin luokan valkotaululla viestiperusteet Mumble-palvelimeen kytkeytymistä varten.

Puhelimet ja Plumble-sovellus saatiin käyttökuntoon reilun kolmen vartin kuluessa. Asennusprosessia häiritsi lähinnä puhelimiin automaattisesti tarjotut käyttöjärjestelmäpäivitykset. Yhteyskokeilut menivät hyvin läpi ja sovelluksen eri asetuksia päästiin kokeilemaan. PTT-puheyhteydet Plumblen ja palvelimen välillä muodostettiin matkapuhelinverkon datayhteyksillä OCB-AES 128bit salattuna.

Kotitehtävinä varusmiehet saivat selvittää kaupallisesti saatavissa olevia PTT-kuulokevaihtoehtoja, pohtia KEHÄ19:ssa tarvittavia kutsuryhmiä ja miettiä sekä varsinaista palvelun käyttöönottoprosessia että erilaisia tapoja kantaa älypuhelinta osana taisteluvarustusta.

Tietoturvallinen mobiilipalvelin ja päästä-päähän kokeilut

Kesän edetessä kerhon ohjaajien mielenkiinto oman ja liikuteltavan palvelinalustan edistämistä kohtaan kasvoi. Alustaa ruvettiin rakentamaan ohjaajien omakustanteisesti hankkimien edullisten Raspberry Pi 3+ tietokoneiden ja Teltonika 4G/LTE-mobiilireitittimien ympärille. Käytännössä lähes identtisiä alustoja rakennettiin kaksin kappalein. Lisäämällä mobiilireititin osaksi alustakokonaisuutta parannettiin palvelun päästä-päähän tietoturvaa ottamalla päätelaitteiden ja mobiilipalvelimen välillä käyttöön AES 256 salatut VPN-tunnelit. Lisäksi mobiilireitittimen tietoturvaa parannettiin ottamalla palomuuri käyttöön. Yksi mobiilireitittimen käytön hyödyistä oli mahdollisuus si-

joittaa mobiilipalvelin joko komppanian komentopaikalle tai vaihtoehtoisesti mihin tahansa julkiseen Internetin liityntäpisteeseen. Alustakokonaisuus paketoitiin maanpuolustushengessä M05-taskun sisään muoviseen suojakoteloon, joka sisälsi paitsi tietokoneen ja reitittimen myös ulkoisen LTE-antennin, suuren 5V akkupankin ja näitä yhdistävät liitäntäkaapelit. Käytännössä mobiilipalvelinta käytettiin aina verkkovirtaan kytkettynä 4G-verkon ylitse.

Kolmannen kerhoillan (7.8.2019) tarkoitus oli purkaa varusmiehille annettuja kotitehtäviä, mutta käytännössä vain puhelimen kantamiseen liittyvään kysymykseen oli haettu vastauksia ja niitäkin varsin yleisellä tasolla. Toisena tarkoituksena oli testata päästä-päähän palvelua uutta mobiilipalvelinta vasten, joka sisälsi nyt myös VPN-toiminnallisuuden.

Varusmiesten oli nyt ensi töikseen asennettava puhelimiin OpenVPN-sovellukset ja konfiguroitava nämä. Tehtävä oli varsin suoraviivainen ja tässä onnistuttiin hyvin. Ainoana haasteena oli lähinnä sertifikaatit sisältävien konfiguraatiotiedostojen tallennus puhelimiin. Tässäkin lopulta onnistuttiin, kun käyttöön otettiin jo aiemmin asennetut sähköpostitilit.

Illassa päätteeksi tutkittiin ja kokeiltiin kahta kotimaista PTT-käyttöön tarkoitettua nappikuuloketta. Toinen oli malli, joka kytkettiin puhelimeen 3,5 mm audio liittimen kautta langallisesti, kun taas toinen kytkettiin Bluetooth-yhteyden avulla langattomasti. Molemmissa malleissa kuulokeosa oli mahdollista irrottaa varsinaisesta painonappiosasta. Vertailun vuoksi kokeiltiin myös tavallisia puhelimien mukana tulevia nappikuulokkeita.

Varusmiehillä tuntui olevan omat mielipiteensä erilaisista kuulokeratkaisuista. Molempien PTT-kuulokkeiden mukana tullut yksinkertainen korvanappi sai lähes välittömästi tuomion: “tämä ei pysy korvassa eikä tätä voi käyttää kuulosuojainten alla.” Bluetooth-kuulokkeessa varusmiehiä arvelutti virrankulutus. Yhtenä isoimpana haasteena havaittiin Plumble-sovelluksen, älypuhelimen käyttöjärjestelmän ja PTT-kuulokkeen yhteispeli: jos puhelimen näyttö lukkiintui, ei push-to-talk toiminnallisuutta voinut käyttää kuulokkeen nappia painamalla, vaan näytön lukitus piti ensin avata käsin. Tämä koettiin merkittäväksi heikkoudeksi.

Tulikaste

Ennen neljättä kerhoiltaa (2.9.2019) varusmiehet yllätettiin käskemällä kehitetty PTT-puhepalvelu mukaan komppanian sisäiseen harjoitukseen, joka pidettiin vain kaksi viikkoa ennen KEHÄ19-harjoitusta. Tämä oli sikäli hyvä, että samalla kun varusmiehet pääsivät koeponnistamaan omaa arjen ratkaisun perustamiseen liittyvää osaamistaan, keräsivät he samalla havaintoja palvelun toimivuudesta aluevalvontatehtävässä.

Neljännessä kerhoillassa havainnot purettiin yhdessä ja todettiin, että laitteet olivat kestäneet kenttäkäyttöä hämmästyttävän hyvin eikä yhtään laitetta ollut kadonnut. Arjen ratkaisujen perustaminen oli tapahtunut nopeasti ja viestimisessä oli noudatettu koulutettua viestikuria sekä peitteistöä oli käytetty.

Sekä kouluttajan että varusmiesten mielestä sotilaspoliisikomppania oli valmis ottamaan arjen PTT-ratkaisun käyttöön pian alkavassa PAPU2-harjoituksessa. Näin myös tapahtui, joskin päätelaitteiden määrä oli KEHÄ19:ssa merkittävästi suurempi, kun käyttöön saatiin konsortion taholta lisää lainapuhelimia. Tästä vuorostaan seurasi harjoituksen valmisteluun liittyvää ennakoimatonta kitkaa. Myös komppanian lopulliset tehtävät poikkesivat KEHÄ19-harjoituksessa valmistavasta harjoituksesta, jolloin tehtävätaktiikkakin joutui koetukselle.

Kokeiltu langallinen PTT-nappikuuloke.

Iloinen kerho päättökuvassa, ohjaajat Tahkokallio ja Raassina laidoissa ja kuusi varusmiestä keskellä.

Mitä kerhosta opittiin?

Kokonaisuutena kerho oli lopulta hyvin onnistunut ja todisti sen, että varusmiehillä on vähintäänkin ohjattuina valmius kehittää, kouluttaa ja ottaa arjen ratkaisuja käyttöön. Kerhoilloista opittiin myös se, että onnistunut kokonaisuus vaatii hyvää etukäteissuunnittelua eikä mullistavia ratkaisuja kannata muutamalla kerhotapaamisella tavoitella. *Parhaaseen lopputulokseen pääsee, kun kerhoiltoihin tuodaan suhteellisen valmiita ja ennalta toimivaksi todettuja ratkaisuja*.

Kerhon ohjaamiseen liittyen opittiin, että kantahenkilökuntaan kuuluvan kouluttajan osallistuminen kerhon suunnitteluun ja varsinaiseen toimintaan on erittäin tärkeätä. Toisaalta kouluttajalta ei pidä odottaa varsinaisiin arjen ratkaisuihin liittyvää substanssiosaamista, vaan nämä tiedot ja taidot tulisi tulla muilta ohjaajilta.

Tärkeä oppi oli myös se, että koska kerho oli varusmiehille vapaaehtoinen ja pidettiin heidän omalla vapaa-ajallaan, rento ja kannustava ilmapiiri on kaiken a ja o. Kerhoon sitoutumisesta kuvaa hyvin esimerkki kerhon jäsenestä, joka saapui takaisin varuskuntaan yksikössä pidettyyn kerhoiltaan omalta vapaa-ajaltaan siviilivaatteissa.

Nähtäväksi jää, jatkuuko kerhoon osallistuneiden ja nyt jo kotiutuneiden varusmiesten kiinnostus arjen ratkaisujen kehittämistä kohtaan myös siviilissä. Mikäli näin käy, saavuttaa kerho perimmäisen tavoitteensa: askeleen kohti toimivaa arjen ratkaisujen ekosysteemiä!


Marko Koukka


Pasi Mäkinen

TEKSTI JA KUVAT: PASI MÄKINEN JA MARKO KOUKKA

Digitalisoinnin työkalupakki – Digitaalisen ekosysteemin haltuunotto

Tämän artikkelisarjan neljäs ja viimeinen osa nitoo yhteen digitalisaation keskeiset elementit, työkalut ja toteutukset. Olemme näissä artikkeleissa käyneet läpi digitalisaatiota eri näkökulmista ja pureutuneet tarkemminkin joihinkin merkittävimpiin toteutuksiin, kuten identiteetin hallintaan, lohkoketjuihin ja 5G teknologiaan. Kaiken keskiössä on kuitenkin ollut se tosiasia että käymme läpi erittäin merkittävää muutosta eli murrosta. Muutoksessa johtaminen on aina avainasemassa ja digitalisaation murrostilanteessa se korostuu erityisesti, sillä niin yritysten liiketoiminta kuin koko yhteiskuntakin on mukana tässä muutoksessa. Tässä artikkelissa keskitymme digitalisaation kannalta oleelliseen ympäristötekijään, Digitaaliseen ekosysteemiin. Tutustumme myös Tietohallintomalliin ja yhteen sen käytännön ilmentymistä, palveluintegraatioon.

Digitaalinen ekosysteemi

Ekosysteemi yleisesti määritellään järjestelmäksi jossa kaikki osat ovat balanssissa keskenään. Digitaalisella ekosysteemillä tarkoitetaan esimerkiksi sitä palveluketjua jossa

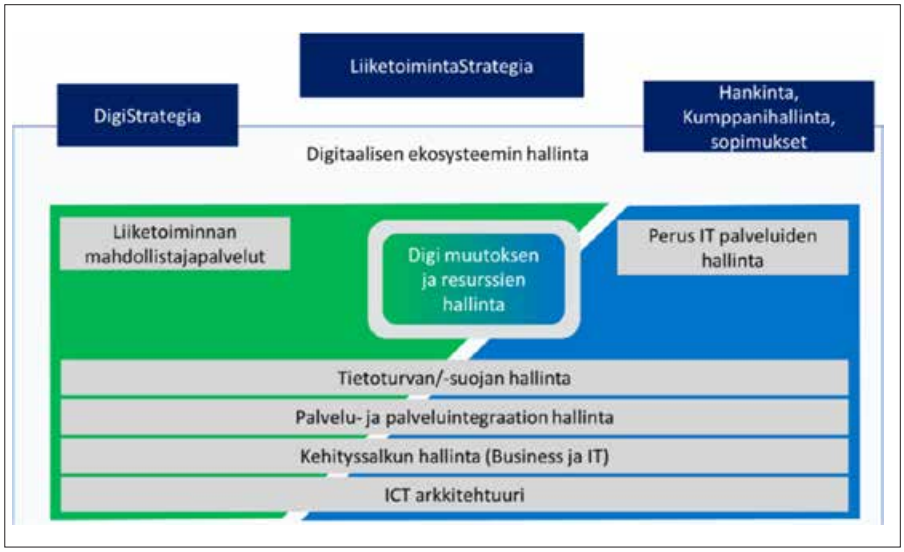
toimittajat, asiakkaat ja palvelut toimivat yhdessä ja tukevat toisiaan.

Kuinka digitaalista ekosysteemiä johdetaan ja hallinnoidaan, jotta se vastaa liiketoiminnan digitalisoitumisen muutosten vaatimuksiin. Liiketoiminnan digitalisoituessa digistrategian merkitys kasvaa osana liiketoimintastrategiaa, mutta edelleen liiketoiminta johtaa ja linjaa päätökset. Muutoksessa liiketoiminta on yhä riippuvaisempi tietoisuudesta sen suhteen mitä digitaalisessa ekosystemissä tapahtuu ja miten sitä hallitaan. Digitaalinen ekosysteemi on eittämättä toiminnallinen ja teknologinen monitoimijaympäristö. Tässä kokonaisuudessa kumppani- ja sopimushallinta korostuvat. Kuinka varmistetaan, että koko palveluketjussa kaikilla toimijoilla on yhtenäiset vaatimukset ja palvelutasot. Vaatimuksenmukaisuuden hallinta on myös huomioitava palveluketjussa koko elinkaaren ajalta.

Kuvassa 1 on viitteellisesti kuvattu johtamisen kannalta keskeisiä elementtejä. Yrityksestä tai organisaatiosta riippumatta lähes aina havaitsemme olevamme tilanteessa, jossa joudutaan rinnakkain johtamaan sekä vanhaa IT-infraa sekä uusia digitalisointia ja liiketoiminnan tavoitteita mahdollistavia palveluita. Hallitsemattomana tämä muutos tai murros voi tulla erittäin kalliiksi, etenkin jos vanhassa infrassa on paljon legacy-palveluita sekä korjausvelkaa jäljellä. Murroksen hallinnassa erityisesti kokonaisarkkitehtuuri korostuu. Tietoisuus nykyisestä arkkitehtuurista luo hyvän pohjan kehityspolulle kohti uutta liiketoimintalähtöistä tavoitetta ja kokonaisarkkitehtuuria.

Ekosysteemin on täytettävä liiketoiminnan asettaman jatkuvuuden, varautumisen sekä tietoturvan/-suojan vaatimukset. Ekosysteemissä on ymmärrettävä toimintaympäristön luonne ja sen vaatimukset. Esimerkiksi valtionhalllinnon ympäristöissä on tunnistettava kansallisen sääntelyn tuomat vaatimukset varautumiseen sekä salassa pidettävän tiedon käsittelyyn. Ekosysteemissä tulee olla formaali tapa käsitellä toimintaympäristön muutoksia ja niiden vaikutuksia arkkitehtuuriin ja käytännön tekemiseen.

Yllä olevassa kuvassa kaiken päällä on yhdistävänä tekijänä digitaalisen ekosysteemin hallinta. Tietoisuus arkkitehtuurista sekä koko palveluketjujen teknisistä komponenteista ja toimittajista on perusedellytys palveluiden hallinnalle. Valvonnan ja hallinnan näkökulmasta yrityksellä itsellään tai sen mandaatilla toimivalla toimijalla on oltava näkyvyys ja kontrolli koko palveluketjuun. Yrityksen näkökulmasta palveluketjun toimijoilla on oltavat yhteiset



Digitaalisen ekosysteemin hallinta.

pelisäännöt, työkalut ja prosessit sekä etukäteen sovitut vastuut ja mandaatit toimia palveluhallinnan eri tilanteissa. Erityisesti häiriötilanteissa prosessien mukainen toiminta korostuu.

Kuten edellä kuvattiin vaatimustenmukaisuuden hallinta muuttuvassa toimintaympäristössä on haastavaa. Esimerkkinä voidaan pohtia, miten julkishallinnon ekosysteemeissä varmistetaan yrityisten organisaatioden salassa pidettävän materiaalin luottamuksellisuus. Toisaalta, miten varmistetaan, että palveluketjussa olevat toimittajat täyttävät palvelulle ja sen tuottamiselle asetetut vaatimukset. Jo tällä hetkellä julkishallinnon haasteena on yhteismitallisten vaatimusten jalkauttaminen sekä elinkaaren hallinta. Uusi tiedonhallintalaki tuo tähän ensi vuoden alusta uudet hasteet. Osaltaan tätä haastetta on pyritty ratkaisemaan muun muassa VM:n Julkisen hallinnon pilvilinjauksilla sekä Pilvipalveuiden auditointi kriteeristöllä (Pitukri). Väestörekisterikeskuksen JUDO-hanke on tehnyt hyvää työtä tiedonhallintalain vaikutusten koulutuksessa. Kuitenkin meillä on vielä pitkästi matkaa siihen, että meillä olisi yhteismitalliset vaatimukset koko palveluketjussa, mukaan lukien julkishallinnon sisäiset toimijat sekä ulkoiset palveluntarjoajat.

Palveluintegraatio, SIAM

SIAM. Onko kyseessä vain uusi lyhenne vaiko peräti pelastusrengas? SIAM (Service Integration and Management) on Palveluintegraatiosta käytetty lyhenne. Hieman itämaiseltakin kuulostava lyhenne pitää kuitenkin sisällään paljon entuudestaan tuttuja elementtejä kuten ITIL-prosesseja ja toisaalta uuden tavan käyttää näitä. Digitaalisen ekosysteemin ja sen mukaisten liiketoimintamallien hallinta tarvitsee uudenlaista palvelutuotantoa, sillä digitalisaatiolle on ominaista palveluntoimittajien määrän kasvu. Digitalisoituvassa maailmassa palvelut syntyvät useiden eri toimijoiden tuottamina. Pitenevien monitoimittajaympäristöissä toimivien palveluketjujen hallinta edellyttää, että joku on vastuussa sekä palveluketjusta että sen valvonnasta. Tähän liittyvät myös toimittajien kesken sovitut toimintamallit. Jo pitkään on puhuttu ”yhden luukun” periaatteessa mutta vasta palveluintegraation toteutuksessa se toteutuu oikealla tavalla. On havaittavissa että SIAM on otettu tosissaan myös markkinakentässä ja siitä on osoituksena se että siitä on muodostumassa aivan oma erillinen liiketoiminnan alueensa. Palveluintegraation voi siis halutessaan myös ulkoistaa ja ostaa sen palveluntoimittajalta.

Palveluintegraatio on osa Tietohallintomallia ja Tietohallintomalli puolestaan on laajempi kuvaus tietohallinnon tekemisestä. Se tukee sekä tietohallintoa itseään että liiketoiminnan johtoa. Digitalisaatio on oleellinen osa jokaista Tietohallintomallin viitekehyksen modulia. Tietohallintomallin kokonaisuus on esitetty kuvassa 2.

SIAM, mitä se on

Mitä tarkoittaa Palveluintegraatio? Tietohallintomallin mukaan SMO (Service Management Office) toteuttaa palveluintegraatiota yli kaikkien toimintojen ja toimittajien. Yksinkertaisimmillaan voidaan sanoa että se on keino johtaa monitoimittajaympäristöä. Jos nyt kuitenkin pitäisi nimetä Palveluintegraation kolme kulmakiveä, olisivat ne väistämättä Työkalut, Ihmiset ja Prosessit.

Asiakkaan näkökulmasta katsottuna Palveluintegraation hyödyt on selkeästi kuvattavissa, sillä toimivan Palveluintegraation voidaan katsoa parantavan mm. liiketoiminnan läpinäkyvyyttä, parempaa asiakaspalvelua ja erityisesti asiakkaan palvelukokemusta. Myös muutoksenhallinta toimii monimutkaisemmassakin ympäristössä halutulla tavalla ja palveluiden kehittämistä tuetaan hyvin. Voidaankin siis sanoa että Palveluintegraatio on liiketoimintaperusteista.

Mitä se vaatii ja mitä toteuttaminen edellyttää?

SIAM ei sellaisenaan pelasta maailmaa. Edelleen liiketoiminta ohjaa ja johtaa digitaalisten palveluiden kehittämistä ja hallintaa. Liiketoiminta tarvitsee vastaavasti parempaa tietoisuutta digitaalisen ekosysteemin kehittymisestä sekä digitaalisten palveluiden tuottamisesta liiketoimintapäätösten tueksi. Tämä edellyttää ekosysteemiltä systemaattista datan keräämistä ja analysointikyvykkyyttä. Datan systemaattinen kerääminen on jatkossa myös pohja automatiikalle sekä tekoälyn hyödyntämiselle.

SIAMin käyttöönotto ei myöskään tapahdu sormia napsauttamalla. Organisaatiolla tulee olla tarve sekä riittävä kypsyystaso sen käyttöönotolle. Liiketoimintanäkökulmsta katsottuna SIAM tulee suhteuttaa omaan liiketoimintaympäristöön. Palveluintegraation tarve kasvaa toiminnan digitaalisten palveluketjujen kompleksisuuden, toimijoiden määrän ja liiketoimintakriittisyyden myötä.

Organisaatiolla itsellään tulee olla riittävä osaaminen ja maturiteetti palveluhallinnan prosesseista sekä työkaluista. Toinen merkittävä seikka on tietoisuus olemassa olevista tai tulevista palveluketjuista. SIAM:n sekä myös normaalin palvelunhallinnan kannalta palveluketjuista tulee erityisesti tietää niiden liiketoiminnallinen vaikuttavuus, ketjussa olevat komponentit ja niiden toimittajat sekä riippuvudet sekä palveluketjun palvelusopimuksellinen tilanne. Sopimusten tulee olla kaikille komponenteille ja toimijoille yhteismitallinen ja asettujen tavoitteiden mukainen.

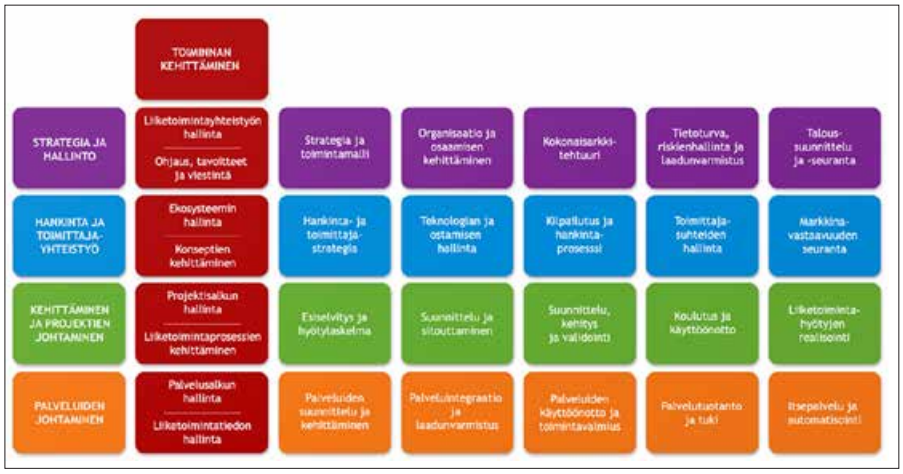
SIAM toteutusten taustalla on erilaisten organisaatioiden tahtotila ulkoistaa palveluita, jotka jonkun on myös otettava haltuun. SIAM:n on tuettava organisaation strategisia linjauksia ja päätettävä missä roolissa organisaation omat resurssit tulevat olemaan. Oleellista on huomata, että ulkoistus sinänsä ei vapauta organisaatiota kokonaan osallistumasta talkoisiin. Parhaimmillaan SIAM kuitenkin antaa joustavan viitekehyksen jossa kehittää ja ylläpitää organisaation omaa digitaalista ekosysteemiä.

Pelastetaanko Suomen kilpailukyky digitalisaatiolla?

Tuleeko SIAM:sta uusi liiketoimintakerros varmistamaan Digitaalisen ekosysteemin vaatimusten mukaisuuden täyttymistä, haluttua käyttäjäkokemusta, irrallisena palvelua tuottavista tahoista.

On selvää, että liiketoimintamallien mukaiset digitaaliset ekosysteemit tulevat vaatimaan uutta lähestymistapaa. Teknologian kehitys nopeutuu edelleen, datan ja laskentakyvyn määrä kasvaa, verkkoihin liitettävien laitteiden määrä kasvaa räjähdysmäisesti, mobiiliverkkojen kapasiteetti kasvaa, mobiiliteetti kasvaa, …

Teknologisen murroksen ja digitalisoinnin kautta myös toimintatapamme muuttuvat. Samalla odotamme yhä parempaa ja nopeampaa käyttäjäkokemusta ja häiriönsietokykymme vähenee. Tässä digitalisaation murroksessa johdetaan samaan aikaan teknologia-, toimintapa- ja liiketoiminnnan muutosta. Tällainen murros edellyttää väkisin muutosta myös liiketoiminnan ja palveluiden hallinnan johtamiseen. SIAM on yksi lähestymistapa, joka sopii alkuvaiheessa kompleksisiinkin monitoimittaja-ympäristöihin, joissa on riittävä kypsyystaso ottaa kokonaisuus haltuun. On kuitenkin päivänselvää, että digitaalisten palveluiden hallinta tulee muuttumaan kaikilla tasoilla pienistä organisaatioista globaaleihin mammutteihin. Automatisaatio, datan hyödyntäminen, integraatiot ja sähköiset palvelukanavat tulevat olemaan avaintekijöitä. Nämä ovat kaikki niitä junia joista ei meillä ole varaa myöhästyä.



Tietohallintomalli. (Tietohallintomallin tekijänoikeudet omistaa ICT Standard Forum.)

Jyrki Penttinen, Technology Manager, GSMA North America

TEKSTI JA KUVAT: JYRKI PENTTINEN

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 pääaiheenaan 5G. Muitten töittensä ohessa Penttinen on kirjoittanut matkaviestintäaiheisia kirjoja sekä luennoinut televiestintäteknologioista englanniksi, espanjaksi ja suomeksi. Penttisen uusimmat kirjat ovat ”5G Explained” (Wiley) ja “5G Simplified” (Amazon). Penttisen ajankohtaisiin artikkeleihin voi tutustua osoitteessa www.linkedin.com/in/jypen sekä blogissa 5g-simplified.com.

5G:n tietoturvallisuus

Yksi 5G:n merkittävimmistä uudistuksista liittyy tietoturvallisuusseikkoihin. 5G:n toiminnallinen arkkitehtuuri sisältää moninaisen kerrosrakenteen, jolla käyttäjien tietoturvaa on parannettu edellisiin matkaviestinnän sukupolviin verrattuna. Esimerkkeinä tästä ovat täysin uusi salausavainten joukko ja niiden hallinta sekä uudet SIM-kortin muodot.

Yleistä

Kuten Viestimies-lehden 4/2016 artikkelissa ”5G:n tietoturvallisuus” todettiin, 5G on huomattavasti aiempia sukupolvia kehittyneempi. Tuolloin järjestelmää vasta standardoitiin, ja alan toimijat testasivat eri radio- ja kytkentäverkkojen tekniikoiden soveltuvuutta. Nyttemmin, kun 3GPP:n ensimmäisen vaiheen eli Release 15:n mukaiset 5G-standardit ovat olleet tänä vuonna käyttöönotettujen verkkojen perustana, on tämä sopiva hetki katsastaa, mitä konkreettisia ratkaisuita on 5G-järjestelmään tuotu mukaan.

On huomattavaa, että kyseinen ensimmäinen vaihe on vasta alustava 5G:n versio, joka tarjoaa rajoitetun määrän kehittyneitä peruspalveluita. Seuraava 3GPP:n spesifikaatioiden julkaisupaketti eli Release 16 on vielä työn alla, ja siihen ollaan parhaillaan lisäämässä monia edistyksellisiä toimintoja, joilla 5G:n loputkin hyödyt saadaan käyttöön. Vuoden 2020 alkupuolella viimeisteltävään standardikokonaisuuteen tulee mm. kriittisen kommunkoinnin ja IoT-laitteiden kehittynyt tuki sekä päivitetyt tietoturvallisuusratkaisut. Tämän hetken Release 15 rakentaa kuitenkin perustan 5G:n uutuuksille, joihin sisältyvät uusi tietoturva-arkkitehtuuri, joukko uusia avaimia sekä uudistetut SIM-korttitekniikat.

Uudistettu tietoturva-arkkitehtuuri

5G on standardoitu siten, että se sisältää verkkoihin integroituna parannetun suojaustason niiden kaupallisen käyttöönoton alusta lähtien. Monet 5G:n tietoturvaratkaisujen vaatimukset ovat jo sinänsä tuttuja aiemmista matkaviestinnän sukupolvista, kuten tilaajan tunnisteet, tilaajan ja verkon molemminpuolinen autentokointi sekä viestinnän luottamuksellisuus, eheys ja suojaus. 5G on suunniteltu siten, että se sisältää lisävaatimuksia täysin uusien käyttäjien eli vertikaalien käytännön ympäristöistä.

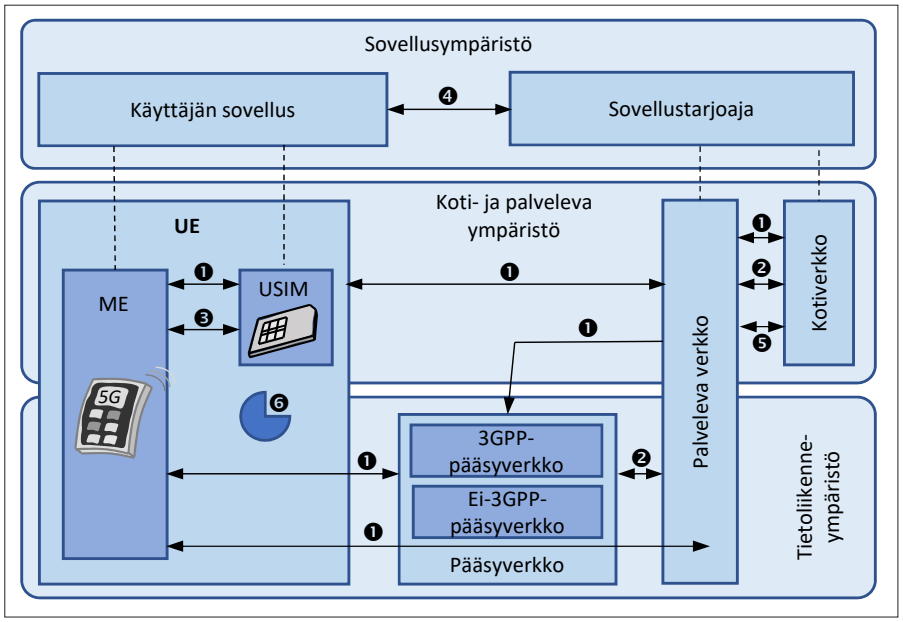
Esimerkkinä mainittakoon järjestyksenvalvonta, älykkäät kaupungit kehittyineine sensoriverkkoineen, virtuaalitodellisuuden hyöty- ja viihdesovellukset sekä erityisliiketoimintaympäristöt kuten tehtaiden automaatiovalmistuslinjat ja niiden kybersuojaus (fyysiset kyberjärjestelmät, Cyber-Physical System, CPS). Erityisesti jälkimmäisiin liittyen, CPS voidaan mieltää järjestelmiksi, jotka perustuvat yhteisiin laskennallisiin elementteihin, jotka ovat aktiivisessa yhteydessä ympäröivään fyysiseen maailmaan ja sen prosesseihin, ja jotka tarjoavat ja käyttävät samanaikaisesti Internetin datapääsyn ja datapalveluiden prosessointia. 5G toimii siis alustana mitä moninaisimmille jo olemassaoleville ja uusille vertikaaleille, yksinkertaisista IoT-laitteista itseohjaavien ajoneuvojen liikennöintiin.

Kuva 1 esittää 5G:n suojausarkkitehtuurin tulkittuna 3GPP:n teknisistä spesifikaatioista TS 33.401 ja TS 33.501. Kuvasta nähdään arkkitehtuurin suojauslohkot (Security Domain), jotka ovat: sovellusympäristö (Application Stratum, AS), kotiympäristö (Home Stratum, HS), palveleva ympäristö (Serving Stratum, SS) sekä tietoliikenneympäristö (Transport Stratum, TS). Kotiympäristö tarkoittaa tilaajan kotiverkkoa, joka suojaa ja sisältää käyttäjän yksilöllisiä tunnisteita. Palveleva ympäristö voi olla joko kotiverkko itse, tai vierailtava roaming-verkko, joka on merkinantoyhteydessä tilaajan kotiverkkoon.

Kuvan 1 suojausarkkitehtuurimallin rajapinnat (1-6) ovat seuraavat:

1: *Verkkopääsyn suojaus* sisältää matkaviestimen (UE, User Equipment) autentikoinnin ja salatun pääsyn verkon palveluihin. 5G-matkaviestin on yhdistelmä päätelaitteesta (ME, Mobile Equipment) ja siihen kytketystä SIM-kortista (USIM, Universal Subscriber Identity Module). Järjestelmän toiminnot suojaavat 5G-radiorajapinnan riippumatta siitä, onko kyseessä 3GPP:n mukainen 5G-teknologia tai jokin muu ei-3GPP-verkkopääsy, kuten Wi-Fi -reititin. Verkkopääsyn suojakseen kuuluu tietoliikenteen suojaus palvelevan verkon (SN, Serving Network) ja päätelaitteen välillä.

2: *Verkkoinfrastruktuurin suojaus* mahdollistaa 5G-verkon toiminnallisten elementtien välisen tiedonsiirron



Kuva 1. *3GPP:n määrittämä 5G:n järjestelmätason suojausarkkitehtuuri.*

ja merkinannon suojauksen. Malli mahdollistaa verkkotoimintojen näkyvyyden ja niiden suojatun tietoliikenneyhteyden vain niiden kanssa autorisoitujen toimintojen kanssa. NEF (Network Exposure Function) on tässä arkkitehtuurissa tärkeässä asemassa, sillä verkkotoiminnot saavat sen kautta selvitettyä tarvitsemansa toiminnon ja luvan kommunkoida sen kanssa.

3: *Tilaajan suojaus* sisältää toiminnot, joilla ainoastaan luvallinen käyttäjä pääsee käsiksi päätelaitteen toimintoihin ja tietoihin.

4: *Sovelluskerroksen suojaus* mahdollistaa turvatun sovellusten ja niitä tarjoavien tahojen välisen liikennöinnin ja merkinannon.

5: *Palvelupohjainen verkkoarkkitehtuuri* (Service-Based Architecture, SBA) sisältää joukon turvallisuustoimintoja, kuten toiminnallisten 5G-verkkoelementtien rekisteröinnin, hallitun löytämisen ja niiden sisäisen autorisoinnin sekä elementtien välisten rajapintojen salauksen.

6: *Suojaustoimintojen näkyvyyden ja säätöjen hallinta* tarkoittaa sitä, että järjestelmä mahdollistaa käyttäjälle menetelmät olla tietoinen kustakin sujaustoiminteesta.

Kuva 2 koostaa esimerkin 5G-verkkojen uudistetusta verkkoarkkitehtuurista ja sen suojaustoimintoihin liittyvistä toiminnallisista verkkoelementeistä (Network Function, NF). 5G:ssä on useita muitakin pakollisia ja valinnaisia elementtejä tilanteesta ja verkko-operaattorin ratkaisuista riippuen. Tämä nimenomainen esimerkki liittyy verkkovierailuun (roaming), joka tapahtuu suojatusti ja salatusti verkkojen välisen 5G-spesifisen SEPP-elementin (Security Edge Protection Proxy) kautta. Esimerkin suojaukseen liittyvät elementit ovat seuraavat:

AUSF (Authentication Server Function) huolehtii käyttäjän tunnistuksesta.

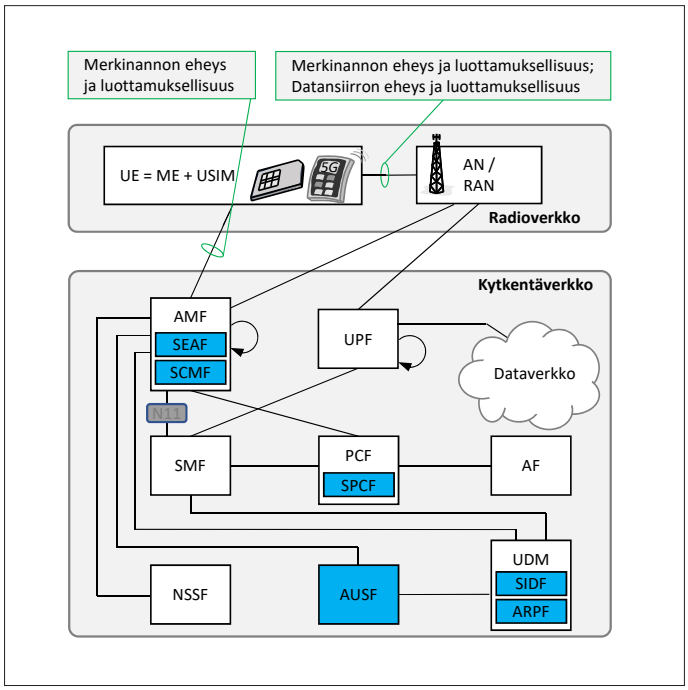
ARPF (Authentication Credential Repository and Processing Function) sijaitsee tilaajarekisterissä UDM (Unified Data Management). ARPF sisältää käyttäjien personoidut avaimet (K) ja se suorittaa suojausalgoritmeja autentikointivektoreiden laskentaan.

SCMF (Security Context Management Function) on osa avaintenlaskentaketjua 5G-verkon sisällä. SCMF voi olla fyysisesti 5G-verkon merkinantoon tarkoitetussa pääsyelementissä AMF (Access and Mobility Management Function).

SIDF (Subscription Identifier De-Concealing Function) huolehtii käyttäjän tunnuksen salatusta versiosta SUCI (Subscribtion Concealed Identifier), selvittäen sen alkuperäisen, suojaamattoman muodon SUPI (Subscription Permanent Identifier). 5G-järjestelmän SUPI ja SUCI korvaavat aiemmissa matkavistintäverkoissa käytetyt tilaajatunnisteet IMSI (International Mobile Subsriber Identity) ja sen väliaikaisen version TMSI (Temporal Mobile Subscriber Identity).

SEAF (Security Anchor Function) laskee yleisen ankkuriavaimen K_{SEAF} kaikille pääsytyypeille. K_{SEAF} suojaa viestinnän päätelaitteen ja palvelevan verkon välillä. Verkkovierailussa se sijaitsee vierailtavassa verkossa. On huomattavaa, että verkon on mahdollista luoda eri variantit K_{SEAF} -avaimesta eri pääsytyypeille kuten Wi-Fille.

SPCF (Security Policy Control Function) toimii suojaporttina tarjoten sääntöjä 5G-verkon elementtien väliseen kommunikointiin perustuen sovellustoimintoon (AF, Application Funtion). SPCF:n eräitä tehtäviä ovat viestinnän luottamuksellisuuden ja eheyden suojaus sekä avainten pituuden ja voimassaoloajan asetus.



Kuva 2. *5G-verkon suojaustoimintoihin liittyvät elementit (merkitty tummalla värillä).*

Avainten hallinta

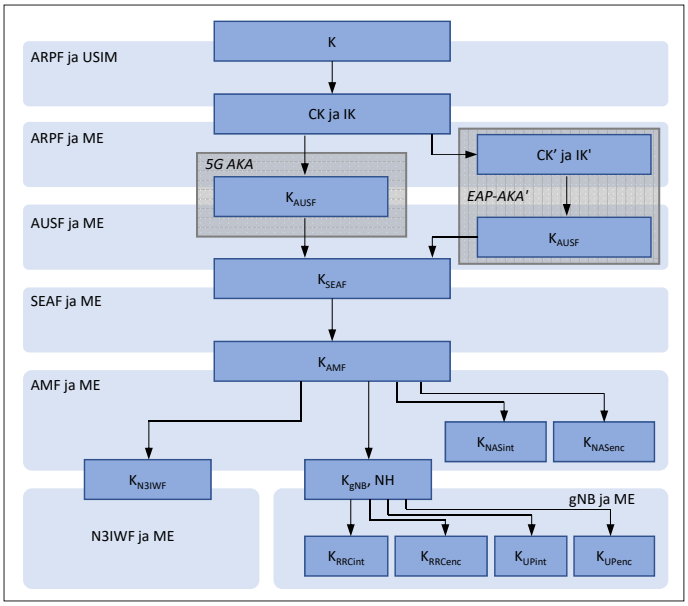
3GPP on suunnitellut 5G-verkon avainten periaatteet täysin uudelta pohjalta. 5G-avainten pituus on verkkojen alkuvaiheessa oletusarvoisesti 128 bittiä, ja verkon rajapinnat tukevat avainten maksimipituutta 256 bittiä tuleviin toteutuksiin.

Kuva 3 esittää 5G-avainten luontiperiaatteen. Kuten kuvasta havaitaan, tilaajakohtainen avain K on sekä 5G-SIM-kortin (USIM) muistissa että ARPF-elementissä. K ei missään tapauksessa poistu kyseisistä elementeistä, vaan verkko ja matkaviestin eli yhdistelmä SIM-korttista (USIM, Universal Subscriber Identity Module) ja matkaviestinlaitteesta ME (Mobile Equipment) luovat yhteyskohtaisia avaimia eri käyttötilanteisiin kuvan esittämien verkkoelementtien kautta (ARPF, AUSF, SEAF ja AMF), kunnes verkko toimittaa lopulliset avaimet 5G-tukiasemille (gNB, Next Generation Node B) tai muihin pääsypisteisiin, kuten Wi-Fi-reitittimiin (N3IWF, Non-3GPP Interworking Function). Avainten periaatteena on estää tiedon luvaton muokkaus (integrity) ja suojata yhteys (encryption). Verkko luo niiden mukaiset erilliset avaimensa sekä datansiirtoon että merkinantoon.

5G käyttää tietosuojan perustana X.509-sertifikaattistandardin mukaista julkista avaintenhallintamenetelmää PKI (Public Key Infrastructure), jolla verkko suojaa käyttäjän identiteetin. PKI mahdollistaa rooleja, menetelmiä ja yhteyden sääntöjä, joilla kyseiseen suojaukseen liittyviä sertifikaatteja luodaan, hallitaan, jaetaan, käytetään, varastoidaan ja haetaan. 5G-kotiverkko hallinnoi PKI:n mukaista julkista avainta. Se varastoidaan pysyvästi käyttäjän USIM-elementtiin siinä, kun avainparin salainen avain varastoidaan ARPF-elementtiin.

SIM-kortin rooli 5G-aikakaudella

5G käyttää edelleen SIM-kortin periaatteita. Uuden järjestelmän myötä nykyiset SIM-kortit ovat kuitenkin jatkojalostettuja, ja ne sisältävät 5G-spesifisiä tiedostoja sitten, kun puhtaasti 5G-spesifiset verkot alkavat olla todellisuutta. Tällä hetkellä käytettävissämme olevat verkot ovat tyypillisesti hybridejä, jotka perustuvat jo olemassa olevaan 4G-infrastruktuuriin siten, että operaattorit lisäävät 4G-kytkentäverkkoon (core) 5G-radiotukiasemia (gNB). Jälkimmäiset toimivat aluksi sekundaarisina, 4G-tukiasemia (eNB) tukevina elementteinä kunnes verkkoinfrastruktuuri alkaa olla kypsä puhtaasti 5G-spesifisiin yhteyksiin ja sitä myötä uudistettuihin SIM-kortteihin.



***Kuva 3**. 5G-järjestelmän avainten periaate.*

Siksi nykyiset SIM-kortit toimivat vielä tässä välivaiheessa. Kehittyneeseen vaiheeseen tarvitaan vähintään SIM-korttien ohjelmallisia päivityyksiä, koska esimerkiksi uudet 5G-tilaajatunnisteet SUPI ja SUCI sekä niiden hallinta tulevat uusina aiheina käyttöön. Periaatteessa vanhat SIM-kortit kelpaisivat ohjelmistopäivitettyinä myös 5G-aikakaudella, mutta operaattorit todennäköisesti päivittävät uusien päätelaitteiden hankinnan myötä samalla SIM-kortitkin, jotta niiden tekninen suorituskyky ei osoittaudu pullonkaulaksi esimerkiksi entistä vaativamman kryptoprosessoinnin suhteen.

Samalla 5G avaa yhä laajemmin markkinat miniatyyri-SIM-elementeille. Nykyään jotkut päätelaitteet ja erityisesti lisälaitteet, kuten kuntoilurannekkeet, sisältävät jo sisäänrakennettuna SIM-elementin (eUICC, Embedded Universal Integrated Circuit Card). ETSI on standardoinut fyysisen MFF2-formaatin, joka toimii yhteensopivasti vanhojen SIM-periaatteiden kanssa, mutta ne kytketään pysyvästi laitteen elektroniikkaan.

5G avaa markkinat myös integroiduille SIM-elementeille (iUICC, Integrated UICC). Siinä, kun eUICC on vielä erillinen, viestimeen kiinteästi asennettu elementti, iUICC on integroitu syvemmälle laitteeen elektroniikkaan, kuten radiomodeemipiiriin (baseband). ETSI ja 3GPP ovat parhaillaan standardoimassa yhteismitallisia menetelmiä eUICC:n ja iUICC:n tilaajahallintaan. Kyseisen standardointiaiheen terminä on SSP (Smart Secure Platform), joka sisältää vastaavasti eSSP ja iSSP -variantit kiinteästi asennettujen ja integroitujen elementtien tilaajahallintaan. Elementtien perustoiminta pohjautuu kuitenkin edelleen ISO/IEC 7816 -älykorttistandardeihin, kuten on asianlaita ollut ensimmäisistä GSM-SIM-korteista lähtien.

SIM-kortti säilyttää siis asemansa vielä 5G-aikakaudellakin, ja on oletettavaa, että käytännön markkinoilla nähdään sekä ”perinteisiä” SIM-kortteja että jatkojalostettuja vartiantteja. Niiden pääasiallinen tehtävä on suojata käyttäjän henkilökohtainen avain K ja salattu PKI-avainparin avain, sekä suorittaa salauksen ja eheyden laskenta yhdessä käyttäjän laitteen kanssa. Niiden kansainväliseen suojausperustaan kuuluvat myös elementtien akreditointi, joista tunnettuna versiona toimii edelleen GSMA:n Security Accreditation Scheme (SAS). Koska eSSP:n ja iSSP:n ekosysteemi sisältää uusia toimijoita, kuten prosessorivalmistajia ja laitteen moduulivalmistajia, uudet avainten personointimenetelmät päivitetään vastaavasti, jotta koko valmistusketjun luottamus pysyy määritellyllä tasolla.

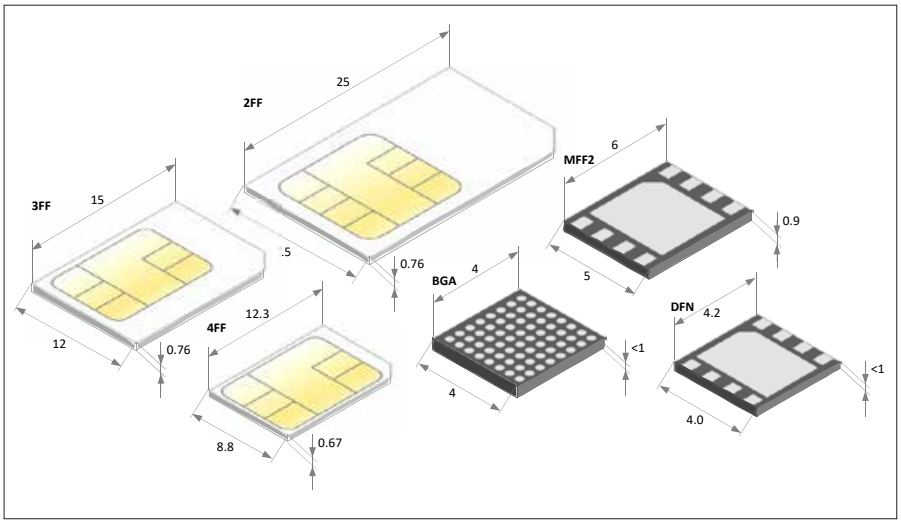
Kuva 4 koostaa nykyiset SIM-korttien muodot (Form Factor) kuten ETSI on ne määritellyt käytettäväksi 3GPP-verkoissa. Vaikka aiempien,

suurikokoisempien korttien käyttöaste on laskemassa, standardit eivät estä laitevalmistajia tarjoamasta vastaavia vielä 5G-laitteissakin. Release 16:n ollessa vielä työn alla, jää nähtäväksi, ehtivätkö eSSP- ja/tai iSSP-tilaajahallintamenetelmät kyseiseen standardiin, vai tarjoavatko alan toimijat tällä välillä rajoittuneempia, valmistajakohtaisia tilaajahallintaratkaisuita.

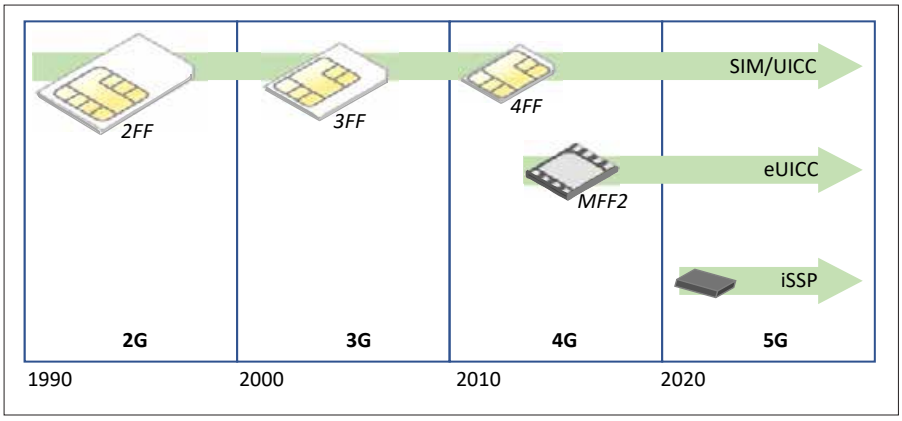
5G:n yhtenä merkittävistä hyödyistä liittyy uudistuneeseen ja parannettuun IoT-laitteiden tukeen. ITU (International Telecommunications Union) määrittää yhtenä vaatimuksena uusille 5G-verkoille tuen valtavaan määrään yhtäaikaisesti kommunikoivia sensoreita ja muita matkaviestinverkkoihin perustuvia IoT-laitteita. ITU mainitsee IoT-spesifisissä käyttöympäristöissä vaatimuksen miljoonan yhtäaikaisesti kommunikoivan laitteen tuesta neliökilometrin alueella. Koska kyseiset laitteet saattavat olla vuosia etäkäytössä ilman huoltotoimia, niiden virrankulutuksen spesifikaatiot ovat myös erityisen haastavia, ja saattavat vaatia pariston toiminta-ajaksi jopa kymmenen vuotta. Siksi myös SIM-evoluutio ottaa huomioon virransäästötarpeet – joiden pitää puolestaan olla tasapainossa tietoturvavaatimusten kanssa. Esimerkkinä tästä haasteesta on parhaimman suojaksen vaatima korkeampi prosessointiteho, mikä vähentää vastaavasti patterinkestoa, eli kaikkiin IoT-ympäristöihin ei ole välttämättä järkevää määrittää kaikkein tehokkainta suojausta.

IoT-laitteiden osalta, MFF2 (Machine-to Machine Form Factor 2) on edelleen validi myös 5G-aikakaudella. Se on toistaiseksi ainoa ETSI:n määrittämä kiinteästi asennettavan SIM-elementin muoto, mutta maailmalla on myös muita variantteja. Kuva 4 koostaa esimerkkejä siirrettävistä ja kiinteästi asennettavista SIM-moduuleista, jotka ovat mahdollisia 5G-aikakauden päätelaitteissa.

Jää siis nähtäväksi, sisältääkö 3GPP:n Release 16 yhteensopivan hallintamenetelmän jälkimmäisille. Tällä välillä GSMA on luonut menetelmiä eSIM-hallintaan operaattoreiden tilaajaprofiilien siirtämiseksi radiorajapinnan yli. Nykyinen menetelmä tunnetaan termillä Remote SIM Provisioning (RSP), ja kyseisen ekosysteemin suunnittelussa ovat olleet mukana myös GlobalPlatform ja SIMalliance.



Kuva 4. *"Perinteiset", siirrettävät SIM-kortit (FF2, FF3 ja FF4) voivat olla edelleen pohjana 5G-laitteissa, joskin laitteisiin kiinteästi asennetut variantit kasvattanevat suosiotaan. Jälkimmäisistä on standardoitu MFF2, ja markkinoilla on kasvava joukko laitevalmistajakohtaisia malleja. Kuvassa esiintyvät mittayksiköt ovat millimetrejä.*



Kuva 5. *SIM-korttien variaatit toimivat myös 5G-aikakaudella.*

Lähteitä ja lisätietoa

- 3GPP TS 33.501 (5G:n suojausarkkitehtuuri ja -proseduurit)
- GSMA RSP (tekninen spesifikaatio, versio 2.2)

TEKSTI/AUTHOR: HANS JØRGEN BOHLBRO IS VICE PRESIDENT FOR PRODUCT MANAGEMENT IN SYSTEMATIC'S DEFENCE DIVISION
KUVAT/PICTURES: SYSTEMATIC

The evolution of C2: from force tracking to AI

The contemporary operating environment presents significant command-and-control (C2) challenges. Many militaries, and in particular those in the West, have for close to two decades been largely focused on counter-insurgency (COIN) warfare, however, the re-emergence of near-peer adversaries as a priority brings a new dynamic to the battlespace and one which requires a capability set that must address complex threats.

While the concept of operations and technical requirements for extant COIN missions and potential conflicts against a near peer has only limited overlap, the requirement for a clear and accurate situational awareness (SA) picture is a constant and was the starting point for many C2 systems in the land domain.

Providing friendly-force tracking (FFT) to enhance force security and combat effectiveness was a focus in the requirements outlined by militaries for the C2 systems that emerged in the early-to-mid 2000s. While FFT may be the minimum expected in contemporary C2 systems, developing such capabilities was not an easy task. Radios capable of transferring the data necessary for FFT have been available for some time, but the awareness of how to organise and move the data was largely absent.

The initial iterations of Systematic's SitaWare C2 system, for example, were centred on providing force tracking at the battalion level and below, and as those capabilities were proven and matured a natural evolution to roll them out across the battlespace and to introduce more complex C2 tools took place, both of which bring technical challenges with regards to the enabling technology and the software itself.

Data limitations

Although advances in radio technology have brought improvements in data bandwidth, it remains a common limiting factor across all levels of the battlespace, and one which becomes more pronounced when providing C2 capabilities to lower echelons. While hardware issues are significant – established communications infrastructure with large bandwidth capacity is clearly more desirable and easier to work with than the limitations that local RF radio nets feature – software architectures and the management of data and bandwidth can overcome this issue to an extent.

The importance of data management has increased as users demand more functionality in their systems, C2 software now features a wide range of tools, from the ability to annotate digital maps and use 'chat' in dismounted systems, to offering full-motion video to users, and forming complex plans at the Joint level that draw on multiple and diverse sources of data.

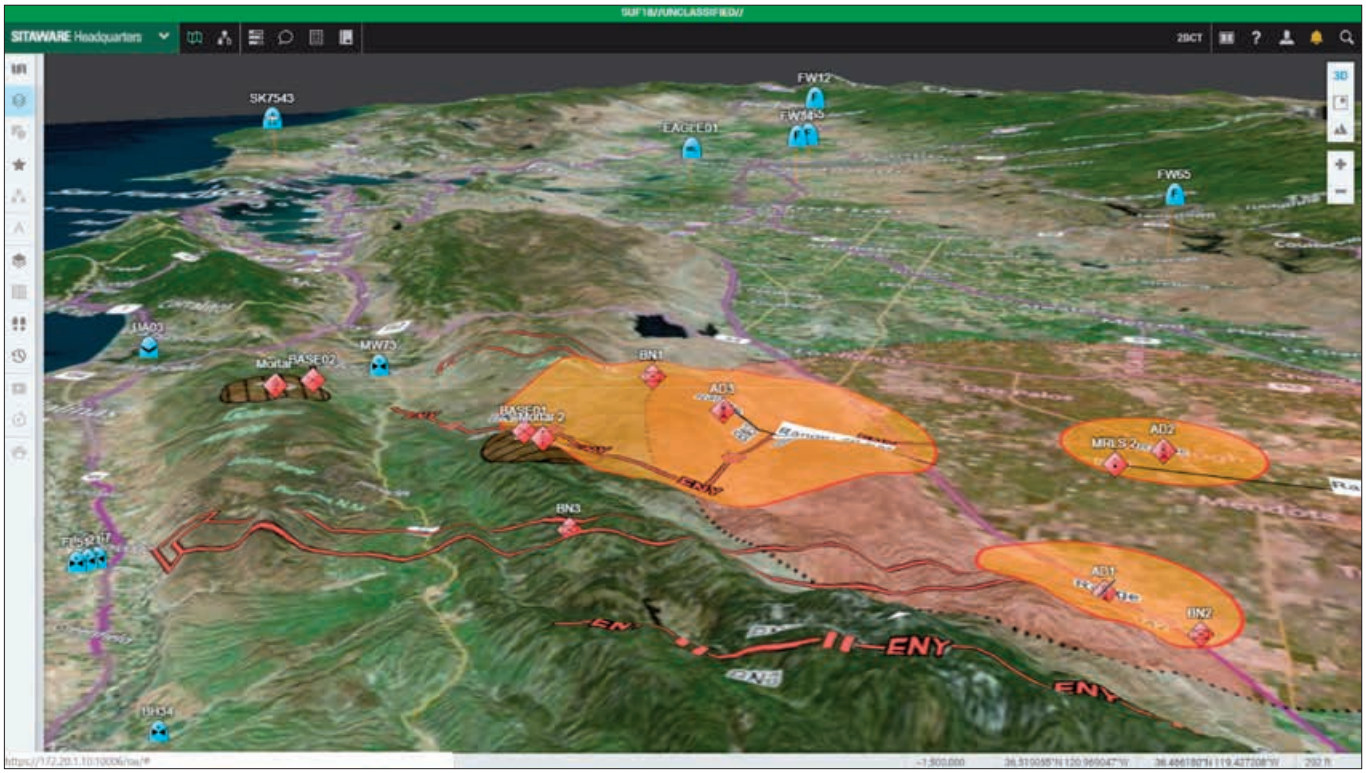
Denied, Disrupted, Intermittent, and Limited communications are typical of military operations and present a challenge to ensuring that all elements are provided with the latest information. Software design can address this and the SitaWare suite's underlying architecture, for example, enables users to maintain effectiveness when bandwidth may be limited, latency high, and connectivity intermittent. The software features intelligent data orchestration that automatically determines when is the best time to inject data into the network. For example, if units experience periods of operation without connectivity, its ability to pass data over very low bandwidth connections ensures that as soon as the opportunity arises to do so, the data is transmitted. Furthermore, it is timestamped, so the recipient is aware of the currency of the information.

Modern militaries possess a wealth of sensors, systems, and intelligence information that enable them to generate a detailed picture of their operating environment. While traditional sources continue to be important, emerging domains such as cyber warfare are adding a new level of complexity that must be taken into consideration. Understanding how best to manage and draw upon the information available is key to mission success.

Painting a clear picture

Determining exactly what information a commander needs to achieve his or her mission – no matter at what level of the battlefield they are operating – is of paramount importance, too little and they will not have what they need to execute their mission, too much and the picture can become cluttered and overwhelming. Collecting and storing a vast array of information is a relatively straightforward task for most C2 systems, sorting and filtering the information so it can be drawn upon quickly and accurately is the key differentiator.

Layering data efficiently enables the right information to be distributed to those who need it and at the level of granularity required, be they a dismount on patrol or a Joint Force Commander. Ideally, C2 systems should create the illusion of simplicity, with commanders seeing only the information they require but with the ability to quickly adjust the detail and scope of the data that



they are presented with. For example, at higher command levels there is typically no requirement to see the tracks of individual dismounts, however, if the need to do so should arise – for example in the case of a MEDEVAC – being able to quickly drill down to that level is highly beneficial. In this regard the system's interface is also of critical importance, ease of use and the ability to quickly adjust the parameters of the filters through simple drop-down menus is essential.

Better together

Interoperability is another important concern of users, as few militaries are likely to conduct missions independently and coalition operations are the norm. As such, it has become apparent that adhering to well-defined standards is crucial in the design of C2 systems, and this will become of increasing importance in the case of near-peer scenarios, where speed of action is a must. Even if partner nations are not using the same C2 systems they must be able to share their SA picture and mission critical information. It is here that well structured exercises that stress interoperability in a realistic manner are highly beneficial, the likes of NATO's Coalition Warrior Interoperability eXercise (CWIX) are an important vehicle for identifying weaknesses and developing best practice, and this must be continuous process.

In a similar vein, C2 systems with open architectures can act as force multipliers and this is a central principle in the design of the SitaWare suite. Gone are the days of the stovepiping of capabilities, a range of factors – from the fiscal constraints placed on militaries to the need to draw on a wealth of data sources – necessitate the ability to integrate diverse systems, and it is not for the vendor to dictate to the customer how they grow their C2 capabilities and leverage other systems. The provision of software development kits enables customers and third parties to build extensions that facilitate the integration of other systems or develop bespoke applications.

The near-peer threat is driving the development of the new capabilities emerging in C2 systems and amplifying many of those that have been evolutionary in their introduction.

Success in any action against a near peer will depend on the rapid exchange of information within and between forces and the ability to create a shared picture at the Joint level that is accurate and continuously updated. The speed of modern warfare demands quick decision making and therefore forces cannot operate within bubbles, a siloed approach to organising capabilities and sharing information limits the ability of forces to react quickly to changes and understand what is happening outside of their own domain or area of operations – land, air, and maritime components need a common operating picture.

The challenge commanders face lies in enabling the different silos to directly communicate with one another without 'democratising' the process too far and without jeopardizing security. A broad overview still needs to be maintained higher up the command chain to ensure that strategic decisions are well informed. Enabling a matrix organisation to operate with and alongside a traditional 'top down' command structure offers significant benefits.

Emerging technologies such as AI and machine learning can certainly aid in speeding-up decision making, with systems able to provide automatic filtering and configuration based on prior experience. Beyond this, however, these technologies promise the ability to examine command decisions and learn what should be done to achieve mission goals, automatically proposing and even carrying-out actions. AI and machine learning could be key when considering the vast volume and array of data and information generated by existing and future systems. Introducing new technologies could greatly shorten

command processes at a time when whoever gets ahead will win.

While much consideration is being given to how much benefit emerging technologies can bring to C2 systems, understanding the capabilities of these technologies and determining how much control should be handed over is an important consideration. What is clear, however, is that there will always need to be a 'man in the loop' at key positions in the command chain.

Future battlespace

The near-peer scenario will also be a battle for the electro-magnetic spectrum and involve emerging domains, such as cyber warfare. Forces will likely deploy in command-and-control denied or degraded environments (C2D2E) where multiple means of communication and sources of positional data, for example, will need to be drawn upon if operational effectiveness is to be maintained. Again, having open architectures and adhering to standards is crucial, for example, if GPS is not available but other sources of positional data can be drawn upon then systems must be able to utilise these. Likewise, denial of communications could see the loss of SATCOM, therefore C2 systems must be capable of working with localised RF communication nets when necessary – even at the highest echelons where bandwidth requirements are the greatest.

Cyber warfare presents a challenge for C2 systems, it is now accepted that cyber will be a part of future conventional warfare scenarios, but how to manage and display its complex data is a significant concern. Simply mapping cyber incidents is not a challenge, but when a commander needs to see their own cyber resources and where they can have an impact, the question of how to present this information in an actionable format arises. If a commander is not aware of the tools at their disposal and how they may affect operations, then they will likely not employ them or miss vital opportunities to impact operations.

The importance of C2 capabilities to 'winning the fight' in a potential near-peer conflict cannot be overstated. In its emerging Multi Domain Operations (MDO) concept, the US military has recognised that effective C2 will underpin the doctrine and likely be the determining factor. Early assessments of the US Army's recently concluded *Unified Challenge* exercise – an MDO-focused event – have noted that C2 software couldn't keep up with the pace of operations, and highlighted a number of issues that must be addressed: the need for a more sophisticated common operating picture that can show events in real time, over greater distances, at a faster pace, and in more domains; a new way of thinking and approach, including a 'cognitive understanding' of the operational environment is necessary; and emerging technologies such as AI will be required to enable commanders and staffs to appreciate and understand the large volume of information.

Having all elements on the same page and enabling them to operate as a cohesive fighting force will be the difference between winning and losing the fight, be that on a COIN mission or against a near-peer, how to deliver this capability to the user is the challenge in front of industry and the military.

C2 community

Ultimately the development of C2 systems must not be undertaken by industry alone, working closely with customers and partners is essential, both in tailoring the solutions to meet individual requirements and introducing best practices that may have been developed.

As C2 systems are used for a diverse range of tasks, encompassing everything from manoeuvre warfare to humanitarian assistance and disaster relief missions, industry and wider user communities can leverage one another's experience. Being able to draw on a broad customer base that has deployed in diverse areas of operation is beneficial to the development of capabilities. Systematic is fortunate in this regard as the SitaWare suite is operationally proven with users in numerous theatres and has been employed at varying scales, be it with the Irish Defence Forces on localised maritime operations, the Finnish Army on peacekeeping missions, multiple nations in Afghanistan, or proven in Corps level exercises with the US Army.

- Hans Jørgen Bohlbro, Vice President for Product Management, Systematic

Komentajakapteeni Carl-Magnus Gripenwaldt vuoden viestiupseeriksi

Komentajakapteeni Carl-Magnus Gripenwaldt Merivoimien esikunnasta on valittu vuoden viestiupseeriksi. Viestiupseeriyhdistyksen puheenjohtaja Juha Petäjäinen julkisti valinnan Riihimäellä 20.9.2019 Viestiupseeriyhdistyksen syyskokouksen yhteydessä.

Komentajakapteeni Gripenwaldt asuu perheineen Raaseporissa. Hänen sotilasuransa alkoi varusmiehenä Viestirykmentissä ja jatkui VA-palveluksessa Helsingin Laivastoasemalla, Viestikeskus 2:ssa operaattorina sekä Laivaston Koulussa laivaradiosähköttäjien kouluttajana.

Gripenwaldt aloitti vuoden 1991 alussa opinnot Päällystöopistossa peruskurssilla 50 ja valmistui vuonna 1993 Ilmavoimien viesti- ja sähköteknisen linjan ELSO- opintosuunnalta, jonka jälkeen hän aloitti työnsä viestiupseerina Rauma-luokan ohjusveneillä Suomenlahden Laivaston Vartiolaivueessa. Gripenwaldt on suorittanut radiotiedustelijan ja mestariluokan radioviestittäjätutkinnot.

Vuonna 1996 Gripenwaldt siirtyi merivalvontaupseerin tehtävään ja edelleen Suomenlahden tilannekeskuksen päälliköksi vuonna 2001. Hän aloitti sotatieteen maisterin opinnot Maanpuolustuskorkeakoulussa 2002 ja valmistui vuonna 2005. Valmistumisen jälkeen hän toimi 7. Ohjuslaivueessa tiedusteluupseerina ja Suomenlahden Meripuolustusalueen tietotekniikkakeskuksen päällikkönä sekä turvallisuuspäällikkönä ennen siirtymistään sektorijohtajaksi Informaatiosodankäynnin sektorille Merivoimien esikunnan johtamisjärjestelmäosastolle 2009. Hän on suorittanut esiupseerikurssin ja tekniikan lisäopinnot vuosina 2010-12.

Vuodesta 2015 Gripenwaldt on toiminut merivoimien toimeenpanovastuulla olevien Puolustusvoimien johtamisen kehittämisohjelman hankkeiden hankepäällikkönä. Hankkeissa kehitetään ja rakennetaan tietojärjestelmäpalveluja sekä tiedonsiirto- ja liityntäratkaisuja meripuolustuksen tarpeisiin.

Gripenwaldt on toiminut toistakymmentä vuotta Viestikiltojen liiton (VKL) sihteerinä. Hän on hoitanut tehtävää erinomaisesti ja mahdollistanut siten VKL:n ja se hallituksen jäntevän toiminnan. Hän on tehtävässään toiminut kiltakentän ja puheenjohtajien tukena ja turvana. Gripenwaldt on ollut myös aktiivinen toimija Viestikiltojen liiton järjestämissä valtakunnallisissa tapahtumissa. Hän on ollut kehittämässä liiton, Viestikiltojen ja puolustusvoimien yhteistoimintaa. Gripenwaldt toimii lisäksi aktiivisesti Uudenmaan Viestikillassa, toimien tällä hetkellä killan varapuheenjohtajana.

Viestimies-lehti esittää lämpimät onnittelut vuoden viestiupseeriksi valinnan johdosta.

Analysaattori

Muureja ja mellakointia

Tällä kertaa piti kirjoitella palomuurien ihmeellisestä maailmasta, mutta juutuin heti kättelyssä lähdetietoihin, ihan sinne muurin juureen. Nimittäin juuri tätä kirjoitettaessa tuleekin päivälleen 30 vuotta Berliinin muurin kaatumisesta. Tai eihän se varsinaisesti kaatunut, kyllä sitä vähän kone- ja ihmisvoimin avustettiin. Merkittävin ihmisapu taisi olla kuitenkin silloisen Itä-Saksan kommunistipuolueen politbyroon jäsen Günter Schabowski. DDR:n johto oli päättänyt lieventää voimistuvien mielenosoitusten johdosta matkustussääntöjä ja Günter sai kunnian käydä televisioidussa tiedotustilaisuudessa kertomassa tämän uutisen kansalle.

Günter siinä tapahtumien tiimellyksessä unohti lukea kunnolla mukaansa saadun pöytäkirjan ja kun hän sitten kertoi, että matkustaminen länteen sallitaan, syntyi reporttereiden keskuudessa oletetusti innostunutta kohua. Italialainen journalisti Riccardo Ehrman ehti sitten kysymään Shabowskilta koska tämä päätös astuisi voimaan ja asiaan huonosti perehtynyt Günter vastasi hiukan improvisoiden, että hänen tietääkseen välittömästi, ilman viiveitä. Samana iltana alkoivatkin jo muurin palaset lennellä ja raja oli auki tunnetuin seurauksin. Ja siis huomatkaa, ilman mitään Twitteriä tai snäppiä tms. Tätä käännettä ei siellä DDR:n puolella varmaankaan osattu ennustaa sillä pääsihteeri Erich Honecker ennusti vielä vuotta aiemmin, että muuri on paikoillaan vielä sadankin vuoden päästä. Tämä Günter itse sitten palkittiin myöhemmin (vain) 3 vuoden vankeudella muurin ylitystä yrittäneiden Itä-saksalaisten murhista. Tuomiostaan hän kärsi tosin vain vuoden Spandaussa. Ei tosin siinä samassa Spandaussa, jossa joitain natseja pidettiin sotien jälkeen, joskin sekin olisi tavallaan ollut ihan soveliasta sillä Günter oli kuitenkin nuoruudessaan myös Hitler-Jugendin jäsen.

On sikäli merkittävä huomio, että elämän lainalaisuudet toistuvasti noudattavat samaa kaavaa niin yksilö- kuin yhteiskuntatasollakin. Tarkoitan siis siniaaltoa. Yhden ison muurin purkamisen 30-vuotisjuhlinnan ohessa uusia muureja nousee kuin sieniä sateella. Osa muureista on ihan fyysisiä osa sitten erilaisia sosiaalisia tai uskonnollisia tai jotenkin muuten vaikeammin määriteltäviä.

Siitä Trumpin muurista on puhuttu jo kyllästymiseen asti eikä siihen sellaisenaan varmaan usko mies itsekään. Alkuperäisen suunnitelman mukaan siihen nimittäin piti liittyä vedellä täytettyjä vallihautoja, jossa uiskentelisi krokotiilejä ja jotain sähköistettyjä piikkejä siellä harjalla. En viitsisi tässä edes ajatella kuinka Donald oli ajatellut ruokkivansa ne krokotiilit. Tai kuka sen sähkölaskun maksaisi. Uusin tieto muuten kertoo, että San Diegon alueella siihen muuriin saa kätevästi n. 100 dollarin arvoisilla leikkureilla aukon, josta on sitten helppo livahtaa lännen kultamaahan. Salakuljettajat taivuttavat yläpäästään polttoleikatut metallipilarit ”käytön” jälkeen takaisin ja aukkoa käytetään myöhemmin uudelleen. Tähän mennessä tätä surullista muuria on pystytetty jo 120 kilometrin matkalle ja ensi vuoden loppuun mennessä sitä pitäisi olla valmiina n. 720 kilometriä. Tämä tarkoittaa siis sen jo ennen Trumppia valmiina olleen noin tuhannen kilometrin muurin lisäksi. Kustannuksista ei tiedä kukaan tarkkaa lukua eikä sekään ketään yllätä.

Analysaattori kysyy, että missä on ATK? Eikö todella olisi mahdollista jotenkin vähemmällä vaivalla ja automatiikalla valvoa tuota rajaa vai onko kuitenkin niin, että sitä edullista vierastyövoimaa tarvitaan koko ajan lisää niin, ettei ole varaa sulkea sitä rajaa kokonaan. Saattaahan muuten olla niinkin, että Trumpin vastustajat käyttävät tässä erästä ikiaikaista strategiaa. Sehän menee niin, että joskus on ihan hyvä antaa ”vastustajan” tehdä hölmöyksiä ja itse katsella vain sivummalta. Sitten on helppo jälkeenpäin savun hälvettyä ja vaurioiden laskennan jälkeen liittyä voivottelemaan, että olipas tyhmästi tehty. Olen kyllä tuon metodin käyttöön itsekin joskus saattanut syyllistyä. En nyt tässä ala ajan puutteen vuoksi … no kyllähän te tiedätte.

Melko paljon onnistuneempi rakennelma on tietenkin Kiinan muuri. Pituutta yli 21000 kilometriä ja ikää on vanhimmilla osilla yli 2000 vuotta. Sen rakentamiseen eivät ilmeisesti poliittisen johtajan vaihdokset ole päässeet merkittävästi vaikuttamaan. Ainakin jossain määrin Kiinan muurikin on rakennettu samaan tarkoitukseen kuin tuo edellä mainittu tekele. Kiina rakensi sen suojaamaan alueitaan paimentolaisheimojen hyökkäyksiltä. Verrattuna tuohon USA:n vastaavaan oli toteutusmetodikin aika lailla erilainen, sillä jossain vaiheessa sen rakentamiseen oli osallistunut koko Kiinan miesväestö. Nykyään isoja osia muurista on kadonnut ja rapistuu ja sitä puretaankin muiden rakennustarpeiden alta. Mainittua siniaaltoa esiintyy siis Kiinassakin.

Yhteiskunnallista muuria itsensä ja Euroopan väliin rakentaa tarmokkaasti Ison-Britannian ja Pohjois-Irlannin

yhdistynyt kuningaskunta. Siinä onkin menossa sellainen manööveri, josta ei ääntä eikä draaman kaaren vaiheita puutu. Äly on kyllä jotakuinkin kateissa. Brittiparlamentin puhemies John Bercow nousi kurinpidollaan, Orderhuudoillaan ja hienostuneella käytöksellään Brexit-väännössä aivan kansainvälisen tason julkkikseksi. Eläköidyttyään lokakuussa hän kertoi haastattelussa, että Brexit-kompurointi sinänsä ei yllätä sillä koko maa on jo valmiiksi jakautunut. Jonkinlainen muuri siis sinnekin on noussut eikä sen kaatumisesta ole juuri nyt kyllä hajuakaan.

Bercow on aika pessimistinen EU:n ja Britannian suhteiden osalta, sillä hän sanoi mielipiteenään noista neuvotteluista näin: *”Väittely jatkuu vielä vähintään viisi vuotta, todennäköisesti kymmen vuotta, ja mahdollisesti 15 vuotta.”*

Nopea ratkaisu Brexitiin on kuitenkin olemassa. Twitterin mystisestä tarjonnasta löysin nerokkaan keinon tämän juupas-eipäs-väännön lopettamiseksi. Eikä siihen tarvita muuta kuin tekstinkäsittelyohjelmiston etsi-korvaa toimintoa. Se menee näin: Kaikki muut maat, paitsi Britannia, eroavat EU:sta ja perustavat BU:n. (Britishless Union, Brititön Unioni). Jäljelle jääköön sitten EU sinne itsekseen vääntämään omista asioistaan. Ja kun kaikki BU:n uudet jäsenet sopivat kertarysäyksellä asiasta niin homma hoituu jokaista direktiiviä ja lakipykälää myöten korvaamalla vain kaikissa asiakirjoissa EU -> BU:lla. Analysaattori kiittää tuntematonta innovaattoria ja suosittelee hänelle BU:n Byrokratian Purkupalkintoa.

Jotain huonosti käynyttä tai pilaantunutta on valahtanut juomaveteen nyt vähän joka puolella maailmaa. Syksyn mittaan kansa on mellakoinut ja osoittanut mieltään Hong Kongissa, Chilessä, Jakartassa, Englannissa, Bagdadissa, Libanonissa, Haitilla, Hollannissa, Perussa ja Ranskassa. Siis ainakin näissä paikoissa. Mellakoidaan Ilmaston tilan puolesta tai bensan hinnoista tai jostain mikä nyt vaan ylittää kansan syvien rivien ketutus-kynnyksen. Ainakin Hong Kongissa on kyse jo pidempään jatkuneista kahakoista ”emämaa” Kiinan lainsäädäntötoimia vastaan ja Ranskassa puolestaan maan poliittisesta päätöksentekojärjestelmästä. Ranskalaiset kun ovat vaan tottuneet muuttamaan poliittisia päätöksiä mellakoimalla. Mutta kaiken kaikkiaan, kummallista riehumista. Ja näitä tapahtumia kun tutkailee tarkemmin, niin demokratia on kyllä kateissa siinä missä ihmisoikeudetkin, sillä monessa paikassa valtio rajoittaa mm. Internetin käyttöä ja sosiaalista mediaa, sillä niitähän näissä kokoontumisien suunnittelussa yleensä käytetään. Jotkut valtiot ovatkin ottaneet käyttöön ns. kansallisia internettejä, joissa kansalaisten valvonta ja kontrollointi on helpompaa eikä yhteyksiä ulkomaille tilanteen niin vaatiessa enää olekaan saatavilla. Kiinan ”Suuri Palomuuri” ja Iranin ”Halal-Internet” ovat juuri tällaisia toteutuksia. Ja Venäjäkin on ilmoittanut harjoittelevansa maan irrottamista kansainvälisestä internetistä. Tässä voi varmaankin nyt sitten vaan todeta, että integraatio perinteisen palomuurin ja totalitäärisen diktatuurin kanssa on jo pitkällä.

Pohjoismaisista muureista tulee heti mieleen ruotsalaiset muurihankkeet. Viime vuonna naapurimaassamme Ruotsissa nousi nimittäin hieman toisenlainen muurikohu. Siellä ryhdyttiin rakentamaan aidoilla eristettyjä asuinalueita, joiden porteista pääsi sisään vain tunnistettuna. Kuuluisin näistä on Poppel Park, mutta näitä alueita oli tulossa sinne lisääkin. Smoolannissa on jo olemassa alue nimeltä Strandudd, jonka ympärillä on jopa kolmen kilometrin pituinen muuri. Asuntoja markkinoidaan turvallisuudella ja kritiikkiä tulee kansalta ja Ruotsista ennustetaan tulevan Etelä-Afrikka, jossa näitä rikkaiden turvallisia alueita on ollut jo pitkään.

Jos näitä eri yhteiskuntaluokkien välisiä vallihautoja nyt tarkkailee ikään kuin filosofisesti, etäämmältä ja globaalisti, niin en usko, että tähän touhuun mitään merkittävää käännettä tai suunnan muutosta on odotettavissa. Olen tästä vähintään yhtä varma kuin pääsihteeri Honecker muinoin oli muuristaan, siniaallon huipulla ollessaan.

VM

Henkilöasiat:

Siirrot ja tehtävään määräämiset

- everstiluutnantti **Jari Riihimäki** (PESUUNNOS) osastopäälliköksi projektiosastolle Järjestelmäkeskukseen 1.1.2020 lukien
- eversti **Jarmo Vähätiitto** (PEJOJÄOS) erityistehtävään (opiskelija, HCSC, Shrivenham, Iso-Britannia) Johtamisjärjestelmäosastossa Pääesikunnassa 1.1.2020 - 30.4.2020 väliseksi ajaksi
- everstiluutnantti **Jari Seppälä** (PEJOJÄOS) apulaisosastopäälliköksi Johtamisjärjestelmäosastossa Pääesikunnassa 1.1.2020 - 30.4.2020 väliseksi ajaksi
- everstiluutnantti **Janne Jokinen** (KARPR) osastoesiupseeriksi (palvelupäällikkö) johtamisjärjestelmäosastolle Maavoimien esikuntaan 1.2.2020 lukien
- everstiluutnantti **Samuli Terämä** (PVJJK) pataljoonan komentajaksi Pohjois-Suomen viestipataljoonaan Kainuun prikaatiin 1.2.2020 lukien
- everstiluutnantti **Tuomas Arajuuri** (MPKK) osastoesiupseeriksi johtamisjärjestelmäosaston tietoverkot sektorille Pääesikuntaan 1.2.2020 lukien
- everstiluutnantti **Mika Seppä** (KAIPR) apulaiskomentajaksi Kainuun prikaatissa 1.2.2020 lukien
- everstiluutnantti **Jari Seppälä** (PEJOJÄOS) osastopäälliköksi tiedustelu-, valvonta ja johtamisjärjestelmäosastolle Järjestelmäkeskukseen 1.5.2020 lukien

Virkaan nimittämiset:

Everstin virkaan 1.10.2019 lukien:
- eversti **Harri Suni** (PVJJK) 30.9.2024 saakka

Korjaus edellisiin numeroihin.
Virkaan nimittämiset:
Everstin virkaan 1.5.2019 lukien:
- eversti **Eero Valkola** (MAAVE) 30.4.2024 saakka

Elektroniikan alalla tapahtunutta kehitystä ja kehitysnäkymiä

Elektronisten komponenttien taso ja kehitys.

Uudet elektroniikan sovellutukset perustuvat suurelta osalta uusien elektronisten komponenttien luomiin mahdollisuuksiin. Tällä hetkellä polijohdekomponentit ovat täysin vakiinnuttaneet asemansa sotilaselektroniikkakaluston rakenneosina lisäten luotettavuutta ja pienentäen laitteiden kokoa ja tehontarvetta. Yksityisten komponenttien (transistorien, diodien jne.) linjalta kehitys on jo nykyisin johtanut tiettyjä elektroniikan perustoimintoja suorittaviin piirikokonaisuuksiin eli mikropiireihin. Tällä hetkellä voidaan puolijohdekomponentteja yhdistää satoja jopa tuhansia yksityisiä vastuksia, diodeja ja transistoreita käsittäviksi toiminnallisiksi kokonaisuuksiksi. Mikropiirien tuotannon nousu on viimeksi kuluneina parina vuotena ollut 100% vuotta kohti. Erityisen merkittävä piirre sotilaallisia sovellutuksia silmällä pitäen on ollut uusien mikroaaltoalueen puolijohdekomponenttien kehittyminen, mistä on seurauksena täysin puolijohdeelektroniikkaan perustuvien tutkien kehittämismahdollisuudet.

1970- luvun ennuste komponenttielektroniikan osalta on yleispiirteeltään selvä; mikroelektroniikan merkitys kasvaa jatkuvasti antaen mahdollisuudet yhä monimutkaisempien elektronisten toimintojen hallitsemiseen laitteiden koon kasvamatta ja luotettavuuden pienenemättä.

Elektroniset tietojenkäsittely- ja laskentalaitteet.

Yhä lukuisimpien ja monimutkaisimpien seikkojen vaikutus päätöksen tekoon on johtanut siihen, että tätä prosessia ei pystytä hallitsemaan vaadittavalla nopeudella ja tarkkuudella enää tavanomaisin keinoin. Siten on jouduttu turvautumaan automaattisiin tietojen käsittelykoneisiin (ATK). Ne ovat nykyisin elektronisia laitteita ja niitä on pöytäkoneista suuren kapasiteetin omaaviin ja huippunopeisiin, mm. avaruusohjelmissa esiintyviin tietokoneisiin. Myös maaoperaatioiden suorittamiseen käytetään lisääntyvässä määrin ATK- koneita, joihin ohjelmoidaan yhtymien johtamista palvelevia komento-, henkilöstö-, tiedustelu-, operaatio- ja huoltotietoa. Puolijohdemikroelektroniikan ansiosta on myös laskintekniikka kehittynyt valtavasti. Tiettyjen puolijohdekiteiden magneettisten ominaisuuksien hyväksikäyttö muistieliminä on johtamassa suurien tietomäärien talletusmahdollisuuksiin muistin koon ollessa silti vain kuutiosenttimetrin luokkaa. Näiden ns. kuplamuistien kehitystyö on vasta alkamassa ja sovellutusten arvioidaan tulevan käyttöön vasta useiden vuosien kuluttua.

1970- luvun laskintekniikan mahdollisuuksista voitaneen todeta, että lähinnä laskinten koon ja hinnan kehitys on suotuisa ja lisäksi käyttövarmuus tulee entisestään paranemaan.

Elektroninen sodankäynti.

Laite- ja asejärjestelmissä lisääntyneen elektronisen osuuden luonnollisena seurauksena on kiihtynyt toiminta elektronisen sodankäynnin alalla. Itse elektronisesta häirinnästä on muodostunut suorastaan aseelliseen vaikutukseen verrattava, operaatiokeskuksista, johdettu toiminta, jolla sopivana ajankohtana pyritään lamauttamaan vastapuolen elektroniset ase-, valvonta- ja johtamisjärjestelmät. Itse häirintälähettimet saattavat olla automaattisia, usein tietokoneella ohjattuja yhdistettyjä tiedustelu- ja häirintälaitteita. Niitä sijoitetaan mm. lentokoneisiin, aluksiin ja maa-ajoneuvoihin sekä taktillista että strategista toimintaa varten.

Yhdistelmä.

Elektroniikalla on sekä nykyisten näkymien että tulevaa kehitystä osoittavien merkkien valossa huomattava osuus sodankäynnin muovautumiseen, sillä johtaminen nopeutuu runsaiden, salattujen ja etäisyysrajoituksista vapaiden viestiyhteyksien sekä päätöksen tekoa helpottavien ATK- koneiden ansiosta. Lisäksi konventionaalinen tulivoima kasvaa asejärjestelmiin kuuluvien elektronisten tutkien, lasereiden ja laskinten ansiosta. Tästä on seurauksena, että potentiaalinen valtio voi suorittaa joukkojensa nopeita ja yllättäviä siirtoja lähes minä ajankohtana ja mille maailman kolkalle tahansa, ja johtaa myöskin sotatoimet tehokkaasti ilman teknillisiä rajoituksia.

Artikkelin kirjoittaja Veli-Matti Pesola

VM

elisa 5G

Nouse uudelle tasolle

elisa.fi/5G

Yhteydet maastoon Nestorin tuotteilla

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

nestor cables

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

Mittarikuja 5,
90620 Oulu
PL 276, 90101 Oulu