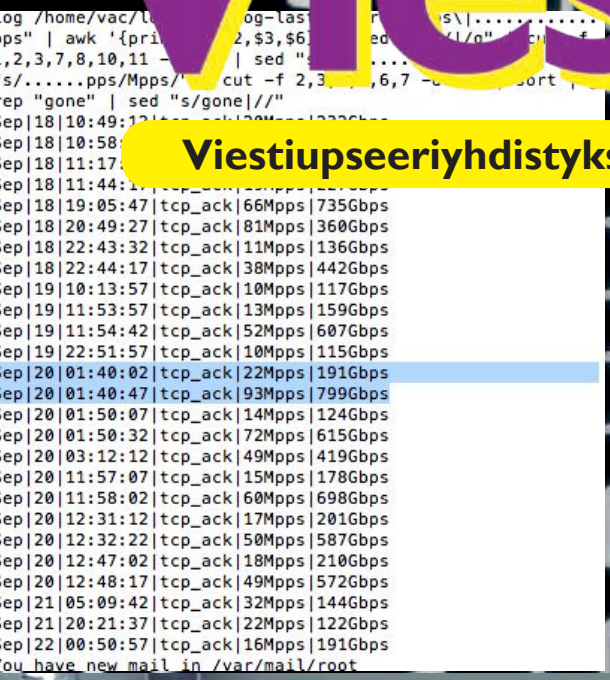
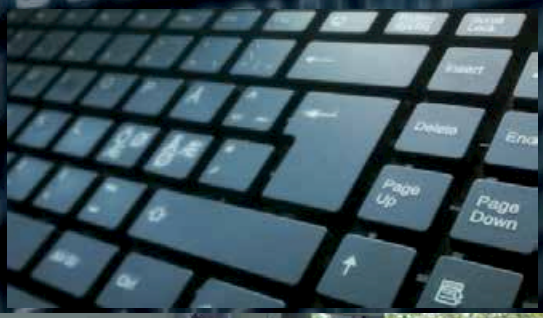
Viestimies

Viestiupseeriyhdistyksen julkaisu 73. vsk Numero 4 Talvi 2018





www.viestiupseeriyhdistys.fi

COMBITECH DEFENCE
YHTEISKUNNAN TURVAAJA

Yhteiskunnan turvallisuus ja sen puolustaminen on meille tärkeä tehtävä.

Toimitamme asiakkaillemme tiedusteluun ja tilannekuvaan, johtamiseen ja viestintään sekä logistiikkaan ja huoltoon liittyviä ohjelmistoratkaisuja vuosikymmenien kokemuksella.

Meiltä löydät osaamisen vaativaan ohjelmistokehitykseen, järjestelmäintegraatioihin sekä asiantuntijapalvelut kokonaisuuksien tukemiseen.

PALVELUMME

OHJELMISTOKEHITYS

JÄRJESTELMÄINTEGRAATIOT

ASIANTUNTIJAPALVELUT

Lisätietoja
info@combitech.fi
http://www.combitech.fi

COMBITECH

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 18.1.2019. Lehti ilmestyy viikolla 10.

PUOLUSTUSVOIMIEN STRATEGINEN KUMPPANI

INSTA

Tiedustelu-, valvonta- ja johtamisjärjestelmät

Kyber- ja tietoturvaratkaisut

Hätä- ja hälytyskeskusjärjestelmät

Datakeskeiset ratkaisut ja edistynyt analytiikka

Rikostorjunnan ratkaisut

Harjoittelu-, koulutus- ja simulointiratkaisut

Kokonaisarkkitehtuurin, hankejohtamisen ja elinkaaren tukipalvelut

Insta DefSec – kriittisten tietojärjestelmien ja kyberturvallisuuden erikoisosaaja vuosikymmenien kokemuksella

Ymmärrämme sotilaallisen toimintaympäristön vaatimukset ja tuomme digitalisaation mahdollisuudet turvallisesti osaksi kriittisiä toimintaympäristöjä. Autamme asiakkaitamme hyödyntämään uusia toimintamalleja, kehittämään viranomaisyhteistyötä, ratkaisemaan kansainvälisen yhteensopivuuden kysymyksiä, tehostamaan tilannetietoisuutta ja suorituskykyä sekä nostamaan tietoturvallisuuden toiminnan edellyttämälle tasolle.

Insta DefSec on osa riippumatonta suomalaista Insta-konsernia, johon kuuluvat myös Insta ILS Oy, Insta Automation Oy ja Intopalo Digital Oy.

insta.fi
instadefsec.fi

”Talven ensipuraisu”

Kuten kesä, oli syksykin poikkeuksellisen lämmin. Samaa ei ehkä voi sanoa vallitsevasta poliittisesta ilmapiiristä maailmanlaajuisesti. Talvi tekee tuloaan. Vaikuttaa siltä, etteivät kaikki ole puhaltamassa yhteen hiileen. Euroopassa on kuohuntaa muun muassa Schengen alueesta ja sen väliaikaisista rajatarkastuksista, Italian velkaantumisesta ja Saksan liittokanslerin mahdollisesta seuraajasta. Kotimaassa taas vaalit lähestyvät ja valtasuhteet ovat tehosekoittimessa. Tasapainoa ja konsensusta haetaan varmasti ensi keväänä taas kerran. Vaikka valta vaihtuu suurella todennäköisyydellä, ei kuitenkaan pidä mennä asioissa ja spekulaatioissa liian pitkälle. Selailtuani vanhoja Viestimies-lehden arkistoja pisti silmääni 70 vuotta vanha teksti. Ohessa siitä katkelma, jonka sanoma toimii vielä tänäkin päivänä. Tämä ehkä muistutuksena siitä mielentilasta, johon on hyvä pyrkiä.

”Yhteistyö – puolustusvoimain ja kansan välillä on kaikkina aikoina ollut menestymisen ehto. Kansan, jota puolustuslaitos palvelee, tulee tuntea tämä oma turvansa mahdollisimman hyvin, jotta yhteistyölle muodostuisi luja perusta. Viimeksi käydyt sodat osoittavat, että meillä tämä tosiasia on täysin oivallettu. Ne merkittävät saavutukset, joita mm. viestialalla kiinteän yhteistyön kautta sukeltautui esiin, muodostuivat ratkaiseviksi tekijöiksi viestiaselajin suurenmoiselle sotapanokselle.

Parhaana todisteena oikean yhteistyön vaalimiseksi ja edelleenkehittämiseksi on tämä viestimiesten oma julkaisu, joka leviää laajalti myös puolustuslaitoksen ulkopuolelle. Samaa asiaa edistää myös suuresti viestiupseerikerho, johon aktiivipalveluksessa

A.R. Saarmaa”

Puolustusvoimat 100-vuotta teemavuoden tullessa päätökseen voinen todeta, näin 70 vuotta myöhemmin, että Viestiaselajin ”Grand Old manin” joulutervehdys ja sen sanoma - yhteistyön voima - pätee edelleen. Viestiaselajin perinteitä ja yhteistyötä on vaalittu ja jatketaan edelleen. Oiva esimerkki tästä yhteistyöstä on jatkuva materiaalisten suorituskykyjen kehittäminen tiiviisti siviiliyritysten kanssa ja operaattoriyhteistyö. Monen tasoinen yhteistyö edellyttää jatkuvia ponnisteluja sen jatkumiseksi unohtamatta kansainvälisiä yhteistyöfoorumeja. Ilman tätä jatkuvaa ja saumatonta yhteistyötä tämän päivän ”puolustuslaitos” olisi todennäköisesti hyvin erilainen. Toisaalta puolustusvoimat on kiinteä osa yhteiskuntaa ja jatkuva vuorovaikutus mahdollistaa kehittymisen puolin ja toisin.

olevien viestiupseerien lisäksi lukeutuu yhä suureneva määrä viestialan reservin upseeristoa, insinöörejä ym. alaa lähellä olevia henkilöitä.

Nämä viestiaselajin taholta tehdyt alotteet tuntemuksen ja yhteistyön jatkuvaksi edistämiseksi tulevat varmasti kantamaan hedelmää. On ilahduttavaa, että on löydetty tällaiset yhteistyömuodot, jotka kauniilla tavalla edistävät meille kaikille arvokasta asiaa – omaa viestialaamme.

Tuntemukseni perusteella voin vakuuttaa, että myöskin viestialan siviilipiireissä on asiaan paljon ymmärtämystä ja hyvää tahtoa. Niillä on, samoin kuin puolustuslaitoksellakin, tavoiteltavana päämääränä koko viestialan kehitys yhä suurempiin saavutuksiin. Yhteistyö siis tältä taholta on erittäin toivottavaa ja edelleenkehittämisen arvoista.

Hyvää Joulun odotusta ja onnellista Uutta Vuotta kaikille!

Päätoimittaja

TEKSTI JA KUVAT: ISMO IKONEN

Kokemuksia M18 johtamisjärjestelmän käyttöönotosta

Kirjoittaja työskentelee Maavoimien esikunnassa johtamisjärjestelmäosastolla sektorijohtajana ja on työskennellyt M18 johtamisjärjestelmän käyttöönotossa usean vuoden ajan.

Tässä artikkelissa tarkastelen omia ja organisaatiomme kokemuksia M18 johtamisjärjestelmän kehittämisessä, käyttöönotossa ja näkemyksiä tulevaisuudesta.

M18 johtamisjärjestelmän kehittäminen ja käyttöönotto ovat osa Maapuolustuksen johtamisen kehittämisohjelmaa, jonka nykyinen vaihe alkoi 2015. Sen taustat ovat kuitenkin 2010-luvun vaihteessa. M18 käyttöönotto, jota toteutetaan hankkeena, on organisoitu projekteiksi. Hankkeen nykyinen vaihe on artikkelin kirjoittamishetkellä ollut käynnissä jo lähes neljä vuotta. Tässä kohtaa on hyvä tarkastella historian näkökulmasta miten tähän tilanteeseen on tultu, arvioida käyttöönoton nykytilaa sekä katsoa miltä käyttöönoton tulevaisuus näyttää.

Kehityspolku ideasta sotavarusteeksi

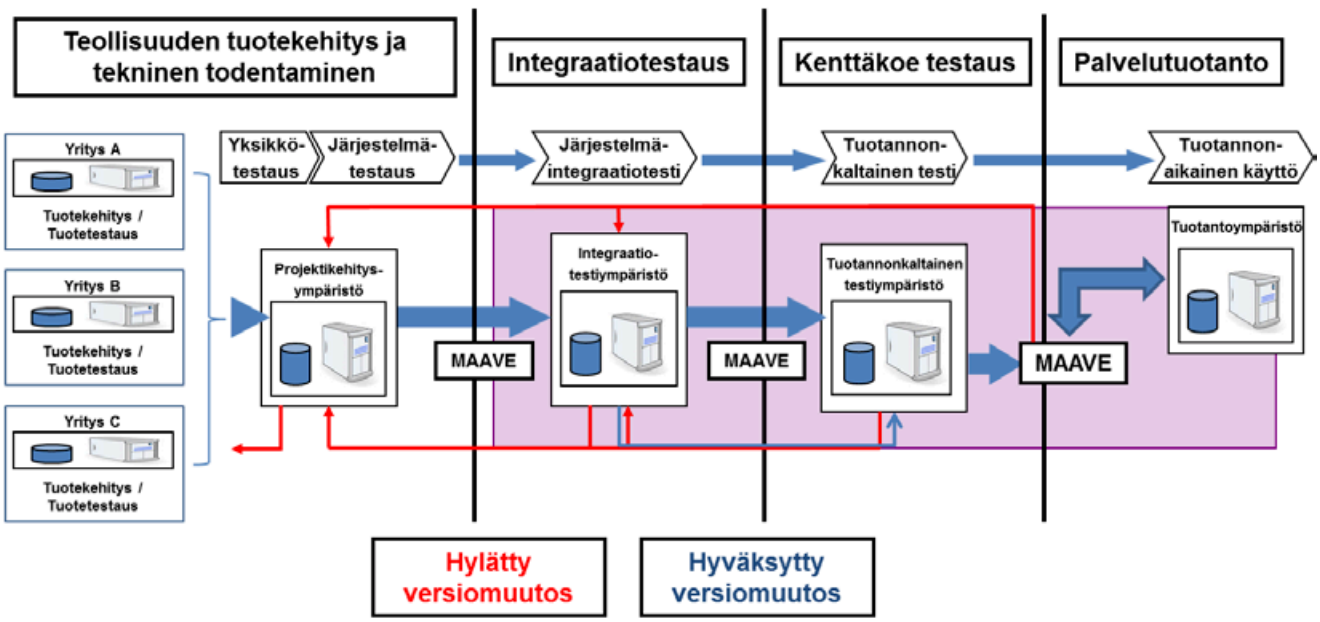
M18 johtamisjärjestelmän kehittäminen edellytti jo alkuvaiheessa linjaorganisaation rinnalla toimivan kehitysorganisaation perustamista. Sen tehtävänä oli suunnitella, ohjata ja antaa linjaorganisaatiolle toteutettavaksi kehittämisen sekä käyttöönoton tehtävät. Kehitysorganisaation tärkeimmät toimijat ovat integraatio- ja kenttäkoeorganisaatiot, jotka ovat saaneet perusteet toiminnalleen Maavoimien esikunnasta. Se, miten teollisuuden ideat ja tuotteet ovat kehittyneet joukolle jaetuksi sekä käytössä olevaksi sotavarusteeksi, voidaan jakaa neljään vaiheeseen. Ne ovat teollisuuden tuotekehitys ja tekninen todentaminen, integraatiotestaus, kenttäkoetoiminta ja palvelutuotantoon siirto.

Teollisuuden tuotekehityksessä ja siihen liittyvässä teknisessä todentamisessa ideoista, tuotteista ja palveluista muodostetaan suorituskyky- sekä käyttövaatimuksien mukaisesti tuotteita. Näiden siirtäminen seuraavaan vaiheeseen toteutetaan erillisen päätöksentekoprosessin kautta.

Integraatio-organisaation tehtävä on testata ja kehittää teollisuudelta vastaanotetuista laitteista ja ohjelmistoista toimiva järjestelmäkokonaisuus. Tämä on toteutettu integraatiotestauksena, jolloin hallitussa ja rajatussa ympäristössä on arvioitu teollisuuden tuotteita suorituskyky- ja käyttövaatimuksia vastaan. Testaamisen ohessa integraatio-organisaatio aloittaa järjestelmien ja sovellusten teknisten ohjeiden laadinnan. M18 johtamisjärjestelmän kehittämisessä integraatiotestaukseen ja testausharjoituksiin on osallistunut merkittävä määrä Puolustusvoimien ja yritysten henkilöstöä. Pienemmissä testaustapahtumissa on ollut mukana useita kymmeniä henkilöitä ja laajoissa harjoituksissa useampi sata.

Kenttäkoeorganisaation tehtävänä on kehittää integraatiotestausta kokonaisuudesta palvelutuotantoon soveltuva. Tämä tapahtuu todentamalla integraatiotestatun järjestelmän toimivuutta oikeassa toimintaympäristössä, oikeiden loppukäyttäjien toimenpitein. Käytännössä nousujohteisesti etenevä, kenttäkokeessa tapahtuva, testaaminen edellyttää suuria ja pitkäkestoisia harjoituksia. Kenttäkoeorganisaatio laatii, testaamisen lisäksi, loppukäyttäjien käyttöohjeita sekä kehittää järjestelmän käyttöä. Tähän liittyy myös taktisten ja taisteluteknisten periaatteiden ja toimintatapojen kehittäminen, jota tehdään yhdessä Maasotakoulun kanssa.

M18 johtamisjärjestelmän kenttäkoeorganisaationa toimii tällä hetkellä Kainuun prikaati, jossa suurimman vastuun asiasta on kantanut Pohjois-Suomen Viestipataljoona. Kainuun prikaati on suurena joukko-osastona mahdollistanut omassa harjoitustoiminnassaan kenttäkoetoiminnan edellyttämän, riittävän laajan ja monipuolisen testausharjoitusympäristön. Lisäksi prikaatissa ovat edustettuina tärkeimmät aselajit ja toimialat, jotka ovat mahdollistaneet testaamisen ja kehittämisen siten, että kaikki tarvittavat toimijat ovat olleet siinä mukana alusta alkaen. Menettelyllä on turvattu riittävä määrä loppukäyttäjiä, viestiasemia jne. harjoituksiin. Tämä on ollut perusedellytys sille, että suurien harjoituksien yhteydessä on kyetty todentamaan ke-



Tuotekehitysprosessi.

hitettävän järjestelmän toimivuus sekä kehitetty sen käyttöperiaatteita käyttäjälähtöisesti.

Palvelutuotantoon siirto on tapahtuma, jossa kenttäkokeessa ollut kokonaisuus siirretään kaikille kyseistä järjestelmää käyttäville tahoille. Ennen kuin tämä voidaan tehdä, on järjestelmien käyttöönoton, käytön, ylläpidon, tuen ja huollon kokonaisuudet rakennettava fyysisesti sekä osaamisen osalta valmiiksi. M18 johtamisjärjestelmän käyttöönoton rinnalla on rakennettu ja päivitetty mm. järjestelmien asennus- ja ylläpitojärjestelmiä, joukko-osastojen varastointijärjestelyitä, käyttöhuollon ja kunnossapidon toimenpiteitä sekä vastuita, palvelutuotannon paikallistukea sekä keskitettyä tukea ja koulutusympäristöjä.

Pitkään jatkuneen kehityshankkeen osalta on ollut keskeistä varmistaa henkilöstön osaaminen. M18 johtamisjärjestelmän osalta se on varmistettu tapauskohtaisesti toteutetuilla erillisillä koulutustapahtumilla, vuosittaisilla koulutustilaisuuksilla ja etenkin mahdollistamalla joukko-osastojen henkilöstön osallistuminen integraatiotestaukseen.

Käyttöönoton nykytila

Jokaisessa kehityshankkeessa tulee vaihe, jossa valmisteltu muutos täytyy siirtää käyttäjille. M18 käyttöönotossa on tehty useita pieniä ja kaksi suurempaa palvelutuotantoon siirtoa. Näistä merkittävin toteutettiin kesällä 2018. Tämä tunnistettiin tulevaksi jo vuotta ennen toteuttamista, koska integraatiotestaukseen tulevan kokonaisuuden siirtyminen kenttäkokeen kautta palvelutuotantoon kestää ajallisesti vuoden.

Joukkotuotanto M18 johtamisjärjestelmällä alkoi vuonna 2017 kaikissa Maavoimien joukko-osastoissa. Tämä on näkynyt siinä, että hankkeen kautta materiaalia on saapunut enenevissä määrin joukko-osastoihin. Samalla osaamisen kehittämisen tukena on parannettu järjestelmän dokumentaatiota laatimalla sekä päivittämällä käyttöohjeita, oppaita ja ohjesääntöjä. Näillä toimenpiteillä joukko-osastoja valmistettiin ottamaan järjestelmä käyttöön ja luotiin edellytyksiä suuremman muutoksen toteuttamiselle palvelu-tuotannossa. Muutos koski kaikkia M18 johtamisjärjestelmää kouluttavia joukko-osastoja, yli puolustushaararajojen.

Joukko-osastojen henkilöstön osaamista oli kehitetty vuodesta 2015 lukien. Laajan muutoksen varmistamiseksi tunnistettiin tarve järjestää erillinen koulutus- ja asennustilaisuus kenttäkoeorganisaation toimesta. Tällä haluttiin varmistaa kyky toteuttaa muutos, koska palvelutuotantoon siirrettävä kokonaisuus piti sisällään uusia asioita ja ominaisuuksia, joiden oikea käyttö sekä loppukäyttäjän oikeat toimenpiteet tuli varmistaa. Samalla tuettiin joukko-osastojen kykyä ottaa järjestelmä käyttöön.

Henkilökunnan osaamisen kehittäminen on ollut keskeistä muutoksen läpiviennissä. Pitkään jatkuneen kehitystyön aikana on normaalin urakehityksen myötä kehitysorganisaation henkilöstöä siirtynyt uusiin tehtäviin ja osiltaan pois. Samalla uutta henkilöstöä on tullut mukaan. Ajan saatossa on organisaatioihin ja ympäristöihin syntynyt omanlaista organisaatiokulttuuria sekä tapaa toimia. Osa-organisaatioissa keskitytään tavallisesti omaan tekemiseen, jolloin ymmärtämys oman toiminnan vaikutuksesta muihin tai kokonaisuuteen voi hämärtyä. Pahimmillaan se jää kokonaan tunnistamatta. Edellä esitetyt asiat yhdessä aiheuttavat tilanteita, jois-

sa vasen käsi ei tiedä mitä oikea tekee ja tieto ei liiku joustavasti organisaatiolta toiselle. Näin on tapahtunut osin myös tämänkin kehitystyön osalta. Sen seurauksena syntyi viivettä asioiden tunnistamisessa ja tarvittavien toimenpiteiden käynnistämisessä.

Tarkasteltaessa, miten laaja palvelutuotantoon siirto toteutui, tunnistamme sieltä kokonaisuuksia, jotka tulivat yllätyksenä. Tältä osin asiat olisivat voineet mennä sujuvammin ja paremmin. Todellisuudessa on kuitenkin hyväksyttävä se, että kaikkeen ei voi varautua. Suuren ja monimutkaisen kokonaisuuden hallinnassa tulee vastaan tilanteita, joissa huomataan, ettei oma ymmärtämys kaikista asioista ole ollut täydellinen ja asioiden todellisia vaikutuksia muihin asioihin ei ole tunnistettu oikein.

Laaja palvelutuotantoon siirto oli suuren muutoksen toteuttamista. Osiltaan se on vielä käynnissä, mutta havaintojen mukaan siinä on onnistuttu. Suuri palvelutuotantoon siirto haastoi koko kehitysorganisaation ja pakotti tarkastelemaan eri toimijoiden tehtäviä, vastuita ja keskinäistä toimintaa. Havaintojen pohjalta kehitystyö on jo aloitettu linjaorganisaation vastuiden mukaisesti, osana normaalia toiminnan kehittämistä.

Tärkein asia laajan muutoksen läpiviennistä oli kokonaisuuden hallinta. Sen taustalta löytyy oikein rakennettu tilannekuva ja johtajuus. Niiden avulla esille nousseet haasteet saatiin tunnistettua oikein ja niiden ratkaisemisessa kyettiin hyödyntämään koko laajan organisaation osaamista. Tätä toimintamallia käytettiin muutoksen läpiviennin suunnittelussa ja toimeenpanossa. Toiminta johdettiin linjaorganisaationa Maavoimien esikunnasta.

Tulevaisuus

M18 johtamisjärjestelmän kehittäminen ja siihen liittyvä hanke päättyy aikanaan. Tällöin hanke- ja kehitysorganisaatiolla olleet tehtävät ja vastuut siirtyvät linjaorganisaatiolle. Se ei kuitenkaan tarkoita, että kehitys päättyisi. Taktisten käyttöperiaatteiden, toimintatapojen, organisaatioiden ja johtamisen osalta kehittäminen jatkuu niin kauan kuin järjestelmä on käytössä.

Kehitys- ja hankeorganisaation toiminnan siirtäminen osiltaan linjaorganisaatiolle on suunniteltava samanlaisella tarkkuudella kuin suuri palvelutuotantoon siirto suunniteltiin. Käytännössä toiminnan siirron suunnittelun on jo alkanut. Tämän suunnittelun aikajänne on yli vuosi. Kehitysorganisaation toiminnan loppuminen, eli toiminnan siirtäminen linjaorganisaatiolle on tapahtuma, jossa vaiheittain kehitysorganisaation toiminnan volyymi laskee. Merkittävä tekijä tässä on se, miten aikoinaan johtamisjärjestelmän kehittämiselle asetetut vaatimukset ovat täyttyneet. Osiltaan kehityksessä kesken jääneiden asioiden kehittämistä voidaan jatkaa uuden hankkeen osana, mikäli tämä nähdään tarpeellisena. Tavallisesti se on ohjelmistojen kehittämistä ja päivittämistä sekä niihin liittyvää testaamista.

VM

TEKSTI:ALEKSI MELDO, COMBITECH, KUVA: SAAB AB.

Virtuaalitodellisuus ja lisätty todellisuus puolustusjärjestelmissä

Viimeisen viiden vuoden aikana on nähty nopeaa kehitystä virtuaalitodellisuuden (VR – Virtual Reality) ja lisätyn todellisuuden (AR – Augmented Reality) teknologioissa. Nämä teknologiat tuovat käyttöön aivan uudenlaisen tavan tiedon visualisointiin sekä vuorovaikutukseen tietokoneiden kanssa. Ne tulevat myös väistämättä olemaan osa tulevaisuuden puolustusjärjestelmiä ja sodankäyntiä.

Kuvittele laittavasi silmälasia hieman isommat lasit päähäsi. Yhtäkkiä näkökenttääsi ilmestyy erilaisia esineitä, jotka näyttävät lähes oikeilta, mutta ovat tosiasiassa lasien luomia virtuaalisia objekteja. Sinulla on edessäsi kartta, jota pystyt liikuttelemaan helposti käsilläsi. Kartalla näkyy esimerkiksi tilannekuva omista joukoista sekä oletetuista vihollisjoukoista. Osoitat kädelläsi kartalla olevaa hävittäjälaivuetta, joka suurenee kartan yläpuolelle neljäksi yksittäiseksi hävittäjäksi. Pieni tietoikkuna avautuu hävittäjien viereen josta näkyy tiedot laivueesta, sen tehtävästä ja yksittäisten hävittäjien polttoaine sekä ammustilanne. Toisella puolella näkyy nappuloita, joista painamalla voit antaa laivueelle uuden käskyn. Uusin tiedustelutieto päivittyy tilannekuvaan ja tekoäly laskee sinulle eri vaihtoehtoja laivueen reitiksi. Näiden tietojen perusteella lähetät hävittäjälaivueen uuteen tehtävään.

Kuulostaako liian futuristiselta tai tietokonepeliltä? Tämä skenaario on jo lähempänä nykypäivää kuin voisi luulla. Lähes kaikki osat edellä mainitusta skenaariosta on toteutettavissa nykyisillä VR ja AR – teknologioilla. Suurimpana esteenä teknologian yleistymiselle on tällä hetkellä laitteistovaatimukset sekä lasien näennäisen suuri koko ja huono resoluutio. Alan laitteistovalmistajat, kuten Oculus ja HTC, sekä alan startupit, kuten Magic Leap ja suomalainen Varjo, tekevät kuitenkin jatkuvasti

töitä teknologian parantamisen parissa. Lopulta laitteisto on mahdutettavissa silmälaseja hieman suurempaan kokoon ja kuvan tarkkuus tulee olemaan lähes ihmissilmää vastaava.

Virtuaalitodellisuus tulee olemaan merkittävä osa erilaisia koulutus- ja simulaatiojärjestelmiä. Se mahdollistaa virtuaalisen harjoittelun todellisuutta vastaavissa ympäristöissä ja alentaa koulutuksen kustannuksia merkittävästi. Virtuaalitodellisuutta käytetään jo esimerkiksi kouluttamaan pilotteja aidosti mallinnetuissa ohjaamoissa, joissa painikkeiden toiminnallisuus vastaa oikean lentokoneen ohjaamoa.

Teknologioista on hyötyä johtamisjärjestelmien ja koulutuksen lisäksi myös taistelukentällä. Lisätty todellisuus on käytössä moderneissa hävittäjissä, joissa 360-kamerat yhdistettynä lisätyn todellisuuden kypärälaseihin mahdollistavat pilotille näkymän koneen rungon läpi. Myös muuta tietoa on helposti mahdollista tuoda tähän kypärään. Pilotti voi nopeasti nähdä taistelun kannalta merkittävää tietoa ja tehdä päätöksiä salamannopeasti. Sama teknologia ja sovellutukset ovat tulossa myös mm. tankkeihin.

Yksittäiselle taistelijalle lisätyn todellisuuden sovellutukset tulevat myös ajan myötä, tosin myöhemmin kuin esimerkiksi hävittäjiin, tankkeihin ja laivoihin. Tämä vaatii teknologista kehitystä ja laitteistojen kustannusten merkittävää alenemista. Lopulta kuitenkin yksittäinen taistelijakin voidaan ”augmentoida” eli tuoda hänen tehtävään liittyvää tietoa suoraan näkökenttään taistelukyvykkyyden parantamiseksi.

Virtuaalitodellisuuden ja lisätyn todellisuuden järjestelmien kehittämisessä löytyy myös haasteita. Eräs suuri haaste on kuinka toteuttaa vuorovaikutus ja käyttöliittymät niin, että ne tuntuvat luonnolliselta ja ovat helppo käyttää erilaisissa olosuhteissa. Monissa virtuaalitodellisuuden järjestelmissä on omat ohjainratkaisut, jotka toimivat melko hyvin, mutta vaativat jonkin verran totuttelua. Tähänkin on tulossa erilaisia ratkaisuja, kuten LeapMotionin IR-kameroihin perustuva käsientunnistus. Käsientunnistuksella omat kädet toimivat luonnollisena ohjaimena ja käyttöliittymänä VR/AR-sovelluksiin, jolloin jo ensikertalainen voi käyttää järjestelmiä sujuvasti. Myös puheentunnistus on varteenotettava vaihtoehto käyttöliittymäksi VR/AR-sovelluksiin.

VR ja AR –teknologioihin yhdistetynä kehittyneet tekoäly- ja puheentunnistussovellukset tulevat pian mullistamaan tavan, jolla vuorovaikutamme tietotekniikan kanssa. Järjestelmät tulevat yhä itsenäisimmiksi ja jalostavat tietoa sekä visualisoivat sen niin, että käyttäjän on mahdollista tehdä nopeita päätöksiä vaihtoehdoista, jotka kone on jo analysoinut. Tämä muutos tulee vaikuttamaan väistämättä myös puolustusjärjestelmiin: sodankäynnin johtamiseen, harjoitteluun ja jopa yksittäisen taistelijan toimintaan.

VM

TEKSTI JA KUVAT: VIESTIMIES-LEHTI

Viestiupseeriyhdistyksen vuosikokous ja Viestikiltojen liiton paikallispuolustusseminaari 22.9.2018, Riihimäellä.

Tilaisuuksien sarja alkoi kello 10.00 lauantaina Viestikoulun luokkarakennuksessa. Aamusta alkaen Riihimäelle oli kokoontunut runsaslukuinen joukko. Paikalle oli saapunut runsaslukuinen joukko aktiivisia yhdistyksen jäseniä. Vuosikokouspäivä alkoi majuri Markus Tanskasen tiiviillä esitelmällä M18-viestijärjestelmästä, jonka jälkeen kokousväellä oli mahdollisuus tutustua järjestelmän osiin Viestikoulun ympäristössä. Tutustuttavana oli M18-viestijär-

Kuva 1. Majuri Markus Tanskanen esitelmöi M18-järjestelmästä ja kokousväki tutustumassa järjestelmään.

Viestiupseeriyhdistyksen syyskokousyleisöä.

jestelmän E- ja C-asema sekä komentopaikan laitesuoja B. Tutustuminen toteutettiin kolmessa ryhmässä kiertoperiaatteella. Onneksi, syksyn ensimmäisen myrskyn saapuessa, tilaisuuden ulkona tapahtuva osuus saatiin vietyä läpi poutaisessa, mutta tuulisessa säässä. Uudet järjestelmät kiinnostivat ja esittelijöitä pommitettiin lukuisilla kysymyksillä, joihin osattiin vastata ammattitaidolla ja tyhjentävästi.

Vuosikokouksen yhteydessä palkittiin lukuisa joukko ansioituneita viestiaselajin toimintaa kehittäneitä ja tukeneita henkilöitä. Henkilöitä palkittiin muun muassa Viestisäätiön kultaisella, hopeisella ja pronssisilla levykkeillä sekä lisäksi palkittiin Vuoden Viestiupseeri ja Viestimies-lehden vuoden kirjoittaja. Kultaisella levykkeellä palkittiin mm. Puolustusvoimien henkilöstöpäällikkö kenraalimajuri Ilkka Korkiamäki ja johtamisjärjestelmäpäällikkö prikaatikenraali Mikko Heiskanen. Kenraalimajuri Korkiamäelle luovutettiin juuri julkaistu Kyberajan viestitaktiikkaa-kirjan tuoreispainos, joka on myynnissä Viestiupseeriyhdistyksen sivustolla. Vuoden viestiupseerina palkittiin vääpeli Simone Mossa Kaartin jääkärirykmentistä. Viestimies-lehden vuoden kirjoittajina palkittiin Janne Kastepohja ja Jukka-Pekka Virtanen.

Vuoden viestiupseeri vääpeli Simone Mossa.

Palkitsemisten jälkeen aloitettiin varsinainen syyskokous, jonka avasi Viestiupseeriyhdistyksen puheenjohtaja Jussi Liesiö. Kokouksen puheenjohtajaksi valittiin Veli-Pekka Kuparinen ja sihteeriksi Martti Aho. Yhdistyksen puheenjohtaja esitteli vuoden 2019

toimintasuunnitelman, joka noudatteli pääosiltaan perinteistä kaavaa. Vuoden 2019 merkittävämpänä tapahtumana on järjestettävä VUY:n seminaari, jonka teemana on ”Turvallisuusympäristön muuttuminen ja siihen vastaaminen”. Seminaari toteutetaan kahdessa osassa, joista jälkimmäinen osuus laivalla.

Julkaisutoimintaa käsiteltiin yhdistyksen lehden ja muiden painotuotteiden osalta. Viestimies-lehti ilmestyy viikoilla 10, 23, 39 ja 49. Viestimieskirjan 19. painoksen myyntiä päätettiin jatkaa ja sitä hyödynnetään rekrytoinnin tukena. Esille nostettiin ajatus uuden Viestimieskirjan tekeminen, jolloin kirja päivitettäisiin vastaamaan nykypäivää. Sosiaalisen median hyödyntäminen tulisi ottaa käyttöön täysimääräisesti. Viestimieslehteä käytetään yhdistyksen tiedotuskanavana myös jatkossa. Seppo Uro käytti puheenvuoron liittyen yhdistyksen omaisuuteen. Yhdistyksellä on lukuisia tauluja, jotka ovat pääosin sijoitettu Riihimäen upseerikerhon tiloihin. Puolustusvoimien luopuessa kiinteistöistään, syntyy huoli mihin taulut sijoitetaan, mikäli kerhorakennuksesta joudutaan luopumaan. Tällä hetkellä tilanne ei ole akuutti, mutta tilanteeseen on hyvä varautua, kun hetki koittaa.

Puheenjohtaja esitteli vuoden 2019 talousarvion, joka hyväksyttiin huomioitta. Talouden jälkeen siirryttiin uuden puheenjohtajan valintaan Jussi Liesiön tilalle. Viestiupseeriyhdistyksen uudeksi puheenjohtajaksi valittiin yksimielisesti 60-vuotias Juha Petäjäinen. Lisäksi muutamia vaihdoksia tehtiin hallituksen kokoonpanoon erovuorossa olevien tilalle. Hallituksen uusiksi jäseniksi valittiin Juha Vallenius Elisalta ja komentaja Juha Ravanti merivoimista.

Muissa asioissa Seppo Uro esitteli Museo Militariassa avattua uutta näyttelyä, jonka on koonnut Kymen Viestikilta Rukajärven suunnan taisteluista.

Martti Aho kannusti kokousedustajia osallistumaan laivaseminaariin 11.-12.2.2019 ja hän kertoi myös Matti Lehtimäen tekemästä kirjasta Suomenlahden ilmatorjunnasta.

Vuoden kirjoittaja Jukka-Pekka Virtanen.

Syyskokouksen palkittuja.

Ilkka Korkiamäelle luovutettiin tuoreispainos Kyberajan viestitaktiikkaa kirjasta.

Syyskokouksen puheenjohtaja ja sihteeri.

Viestiupseeriyhdistyksen uusi puheenjohtaja Juha Petäjäinen.

Syyskokouksen Viestimies-illallinen.

Vuosikokouksen jälkeen, yhteistoiminnassa Viestiupseeriyhdistyksen, Viestikiltojen liiton ja Maanpuolustuskoulutusyhdistyksen järjestetty paikallispuolustuksen seminaari toteutettiin samanaikaisesti usealla paikkakunnalla Riihimäellä ja verkkotuetusti. Seminaaripäivän päätteeksi joukko kokoontui Riihimäen upseerikerholle nauttimaan juhlapäivällistä.

VM

Viestiupseeriyhdistys järjestää seminaarin

Turvallisuusympäristön muuttuminen ja siihen vastaaminen

11.-12.2.2019

Seminaarissa käsitellään turvallisuusympäristössä tapahtuneita muutoksia ja arvioidaan niiden vaikutuksia yhteiskunnan toimivuuteen.
Seminaari on tarkoitettu organisaatioiden tietoverkkojen toimintavarmuudesta, suunnittelusta, ratkaisuista ja tietoturvallisuudesta vastaaville.
Puhujina toimitusjohtaja Klaus Ahlstrand, tutkimusjohtaja Mikko Hyppönen, kansliapäällikkö Jukka Juusti, tutkija Veli-Pekka Kivimäki, apulaispäällikkö Olli Kolstela, kyberturvallisuusjohtaja Jan Mickos, dosentti Mikko Möttönen, everstiluutnantti Simo Pesu, tutkimusjohtaja Hanna Smith, eversti Pekka Turunen, eversti Timo Viinikainen, toimittaja Salla Vuorikoski ja turvallisuusjohtaja Jaakko Wallenius.
11.2. iltapäivän tilaisuus on CGI Finland Oy:n tiloissa Pitäjänmäellä ja ilta- sekä 12.2. ohjelma risteilynä Helsingistä Tallinnaan m/s Silja Europalla.
Seminaarin tarkempi ohjelma sekä ohjeet ilmoittautumisesta on julkaistu Viestimies-lehdessä 3/2018 ja www.viestiupseeriyhdistys.fi. Paikkoja rajoitetusti.

Tarvittaessa lisätietoja antavat:
Juha Petäjäinen 050 520 1403 tai juha.petajainen@elisa.fi ja
Martti Aho 040 581 7773 tai seminaari@viestiupseeriyhdistys.fi

TERVETULOA

VIESTIUPSEERIYHDISTYS ry

TEKSTI: JUKKA-PEKKA VIRTANEN, VIESTIKILTOJEN LIITON HALLITUKSEN PUHEENJOHTAJA
KUVAT: SAMULI TERÄMÄ, JUKKA-PEKKA VIRTANEN

Paikallispuolustuksen johtaminen rulettaa

- Koko maata puolustetaan!

Viestikiltojen Liiton yhteistoiminnassa Viestiupseeriyhdistyksen, Maanpuolustuskoulutusyhdistyksen ja puolustusvoimien kanssa järjestämä A.R. Saarmaa -seminaari kokosi noin 150 vapaaehtoista maanpuolustajaa Riihimäen lisäksi 13 eri paikkakunnalle Rovaniemeltä Helsinkiin. Paikallispuolustuksen johtamisen tukemiseen keskittyneessä tilaisuudessa viestimiehet kenraalista sotamieheen pohdiskelivat yhdessä arjen välineiden käyttömahdollisuuksia poikkeusolojen haasteellisissa johtamisympäristöissä, paikallispataljoonan viestikoulutusta ja vapaaehtoiskentän tehtäviä. Seminaarin luonteen mukaisesti pidettiin osa esityksistä videoneuvottelulaitteiston välityksellä maakunnista. Tilaisuus oli samalla osa viestijoukkojen 100-vuotista juhlavuotta.

Paikallispuolustuksen johtamisen tukeen keskittynyt A.R. Saarmaa -seminaari kokosi noin 150 vapaaehtoista maanpuolustajaa Riihimäen lisäksi 13 eri paikkakunnalle Rovaniemeltä Helsinkiin.

Arjen välineillä hybridiuhkien torjuntaan

Seminaarin ensimmäinen osa käsitteli paikallispuolustuksen johtamista ja viestitoimintaa. Sen avasi Pääesikunnan johtamisjärjestelmäpäällikkö prikaatikenraali Mikko Heiskanen tuoden tilaisuuteen vapaaehtoisen maanpuolustuksen tarkastajan prikaatikenraali Jukka Sonnisen terveiset. Heiskanen viittasi puheenvuorossaan vuoden takaiseen Viestimies-lehden pääkirjoitukseen, jossa hän muistutti Euroopan ja Itämeren ympäristön muuttuneesta turvallisuuspoliittisesta tilanteesta. Varautumisen painopiste on siirtynyt entisaikojen laajamittaisesta hyökkäyksestä hybridiuhkien torjuntaan, johon myös kyberuhkat ja kyberpuolustuksen kehittäminen keskeisesti liittyvät. Toiminnan ytimessä on valmiuden kehittäminen, jonka asettamiin vaatimuksiin on monipuolisella keinovalikoimalla vastattava.

Kenraali Heiskanen palasi esityksessään Pääesikunnan Johtamisjärjestelmäosaston vuonna 2016 julkaisemaan johtamisen tuen konseptiin, jossa on nostettu yhtenä keskeisenä teemana esille arjen välineiden merkitys. Arjen välineissä on valtava potentiaali, jonka käytön innovointiin kenraali viestivä-kеä kannusti. Tarkastelussa ovat päivittäisessä käytössä olevat palvelut, kuten sosiaalinen media, pikaviestit ja pilvipalvelut. Kysymyksessä on suuri kult-

tuuri- ja toimintatapamuutos. Arjen välineissä puolustusvoimat haluaa tarjota maanpuolustushenkisille reserviläisilleen mahdollisuuden näyttää osaamistaan. On aika valjastaa arjen välineet kansallisen turvallisuuden palvelukseen ja kutoa yhdessä sellainen järjestelmien verkosto, joka mahdollistaa johtamisen kustannustehokkaasti kaikissa uhkakuvissa, Heiskanen korosti.

Seminaarin puheenjohtajana toiminut viestitarkastaja eversti Eero Valkola muistutti, että monipuolistuvasta keinovalikoimasta huolimatta on vastustajan käytössä edelleen mittava arsenaali perinteisiä sodan käynnin välineitä kuten tykkejä, ohjuksia ja panssarivaunuja. Viestitarkastajan mukaan paikallispataljoonan johtamisessa korostuu normaaliaikana tehdyt valmistelut. Paikallispataljoonan johtamisjärjestelmä mahdollistaa liittymisen puolustusvoimien ja maapuolustuksen tieto- ja viestijärjestelmiin, omien joukkojen tilanteen seurannan ja johtamisen sekä yhteistoiminnan muiden viranomaisten kanssa. Lisäksi se mahdollistaa yhteistoiminnan perustajan, materiaalin hajauttajan ja operatiivisen käyttäjän välillä.

Valmiutta kohotettaessa paikallispuolustuksessa otetaan käyttöön puolustusvoimien, maapuolustuksen johtamisjärjestelmän ja operaattoreiden palveluita, joita laajennetaan poikkeusolojen tilanteen edellyttämällä tavalla. Viranomaisradioverkon (VIRVE) lisäksi johtamisessa käytetään viranomaisten kenttäjohtamisjärjestelmän ja matkapuhelinjärjestelmän palveluita. Tilannekuvan vaihtamiseen ja yhteistoimintaan muiden viranomaisten ja toimijoiden välillä käytetään yhteysupseereita.

Operaattoriyhteistyöllä resurssien järkevämpään käyttöön

ICT-yrityksen näkökulman tilaisuuteen toi Marko Kallio Kainuussa, Ylä-Savossa ja Pohjois-Karjalassa operoivasta Kaisanet Oy:stä. Yritys on tehnyt pitkäaikaista yhteistyötä puolustusvoimien kanssa muun muassa Kajaanin varuskunnan varusmiesverkkojen ja Vieremän varalaskupaikan yhteyksien rakentamisessa. Kallio esitti paikallispuolustuksen johtamisjärjestelmän kehittäjille kysymyksen: Miksi puolustusvoimat suunnittelee, rakentaa ja ylläpitää liityntäpisteitä, laitetiloja ja verkkoratkaisuja liiketoimintaa toteuttavien toimijoiden palveluiden käytön sijaan?

Tutkija Eero Rikkosen mukaan arjen ratkaisujen hyödyntämisessä on keskeistä toimintatavan joukkokohtainen suunnittelu ja käskeminen. Tutkimusten perustella hän sallisi hallitun käytön, mutta hillitsisi suunnittelematonta käyttöä ja säätelisi sitä tilanteen ja toimintaympäristön mukaan.

Kallio suhtautui kriittisesti ”mustakuituun”, jota käytetään paikallispuolustuksen yhteysjärjestelyjen perusratkaisuna. Perusteluina ovat heikko kustannustehokkuus ja ylläpidolliset haasteet. ”Mustakuitu” on hidas korjata, vaikeasti laajennettavissa ja kaiken lisäksi paikkasidonnainen. Itse laitteiden lisäksi kustannuksia syntyy laitetilojen ylläpidosta. Lisäksi vastuu yhteyden toimintakunnon valvonnasta on puolustusvoimilla. Vasta-argumentteina kuulijakunta esitti muun muassa vaatimuksia ratkaisujen taistelunkestävyydestä ja tietoturvasta.

Uutena paikallispuolustuksen johtamisjärjestelmäratkaisuna Kallio esitti kokonaisvaltaisen tietoliikennepalvelun käyttöä. Esitystään hän perusteli muun muassa sillä, että operaattorin tietoliikennepalvelut ovat ympäri vuorokauden valvottuja. Keskustilojen kytkimet ja siirtolaitteet sijaitsevat pääsääntöisesti varmistetulla sähkönsyötöllä varustetuissa laitetiloissa. Tietoliikennepalveluiden ylläpito on etähallittua, mistä johtuen fyysinen käynti laitetiloissa tai liityntäpisteellä ei ole useinkaan tarpeellista. Operaattorin tietoliikennepalvelu mahdollistaa ”mustakuitua” nopeamman käyttöönoton, viankorjauksen ja paremman käytettävyyden. Esityksensä päätteeksi Kallio muistutti, että puolustusvoimien tietoturvaratkaisut voidaan rakentaa yrityksen tarjoaman tietoliikennepalvelun ”päälle”.

”Muuten toimiva joukko, mutta viestivälineet puuttuivat”

Tutkija Eero Rikkonen Puolustusvoimien tutkimuslaitokselta käsitteli omassa esityksessään arjen ratkaisujen käyttöä johtamisessa esimerkein tarkasteltuna. Käyttömahdollisuuksia on tutkittu muun muassa Maanpuolustuskorkeakoulun opinnäytetöissä ja paikallispuolustusharjoituksissa, joissa on johdonmukaisesti kartoitettu tarpeita, syvennetty ymmärrystä rajoitteista ja kerätty käyttäjäkokemuksia. Rikkosen mukaan arjen ratkaisuilla parannetaan merkittävästi kykyä johtaa, jakaa tilannetietoa ja toimia yhdessä. Arjen

ratkaisuilla varmennetaan toiminnan jatkuminen operatiivisten järjestelmien vikatilanteissa ja vastataan myös varautumisen vaatimuksiin.

Esimerkkeinä paikallispataljoonan johtamisessa oli esillä puhe- ja pikaviestintä, aluevalvonta, tehtävälistat, yhteydet viranomaisiin, sotapäiväkirja ja tilanneselostukset. Matkapuhelin soveltuu komppanian, joukkueen ja ryhmän johtamisvälineeksi muissa kuin varsinaisissa taistelutilanteissa. Havaintojen perusteella omien matkapuhelimien hallitsematon käyttö väheni, joskin viestiliikennekurin merkitys korostui. Sähkönsaanti ei rakennetulla alueella ja moottoriajoneuvoilla toimittaessa ole ongelma. Myöskään matkapuhelimien rajallinen maastokelpoisuus ei estä niiden käyttöä. Huomion arvoista on myös se, että joukot pystyvät toiminnan aikana kehittämään itse uusia käyttötapoja ja -tarpeita.

Valvonnan arjen ratkaisuna kokeiltiin valvonta- ja riistakameroiden ohella matkapuhelimen omaa kameraa. Toiminnassa hyödynnettiin kuvien automaattista luokittelua sekä pilvipalvelua tallennuksen ja automaattisen arkistoinnin tukena. Valvontaratkaisu koettiin hyödylliseksi. Esimerkkinä IP-kamera tuotti elävää kuvaa kohteesta, jossa partion tarkastuskäyntien välillä olisi muuten kulunut useampi tunti. Myös logistiikan johtamisessa on paljon arjen välineiden käyttömahdollisuuksia. Tilausten ja toimitusten hallinta on automatisoitumassa ja huollon luonne muuttumassa ennakoivammaksi, johon muun muassa tehtävänhallintasovellus, Trello tarjoaa monia mahdollisuuksia.

Johtopäätöksinä Rikkonen korosti arjen ratkaisujen valtavaa potentiaalia. Niiden hyödyntämisessä on keskeistä toimintatavan joukkokohtainen suunnittelu ja käskeminen, jossa hyödynnetään julkisessa ympäristössä sovellettavia tiedon turvaamisen menetelmiä. Sallitaan hallittu käyttö, mutta hillitään suunnittelematonta käyttöä ja säädellään sitä tilanteen ja toimintaympäristön mukaan, Rikkonen painotti. Arjen ratkaisut luovat resilienssiä operatiivisille järjestelmille, jossa puolustusvoimien on luotettava yhteiskunnan ylläpito- ja korjautumiskykyyn. Siviililaitteilla tulee luoda “riittävän” tietoturvallinen

Joonatan Kuorikoski (keskellä) keskittyi esityksessään esikunta- ja viestikomppanian (PAIKP) reserviläispäällikön rooliin joukkonsa pääkouluttajana. Mahdollisuuksina hän toi esille osaavat ja innostuneet reserviläiset, osaamistarveperusteisesti räätälöidyn koulutuksen ja paikallistuntemuksen.

käyttöympäristö, joka on tekniseltä suojaustasoltaan viranomaiskäyttöinen (ST IV), mutta julkisessa verkossa toteutettu.

Radioamatöörit viranomaisyhteyksien turvaajana

Pohjois-Karjalan varaverkkokatsauksen tilaisuudessa esittivät videoneuvottelujärjestelmän välityksellä Joensuusta paikallisen radiokerhon (OH7AB) edustajat Antti Tiilikainen ja Pertti Karttunen. Verkon historia kytkeytyy puolustusvoimien harjoituksiin, Radioamatööriliiton TURVA-harjoituksiin ja yhtäältä Maanpuolustuskoulutuksen kursseihin. Pohjois-Karjalan Radiokerhon jäsenistä kokoonpantu projektiryhmä hyväksyttiin yhdistyksen hallituksen kokouksessa vuonna 2013, josta kehittäminen toden teolla käynnistyi. Verkon nimen taustalla on ”edesmennyt” Liikenne- ja viestintäministeriön omistama ja Huoltovarmuuskeskuksen rahoittama 2V-verkko.

Missiona Pohjois-Karjalassa on kehittää ja ylläpitää varaverkkojärjestelmää siten, että häiriötilanteissa sen kautta voidaan välittää viranomaisten tietoliikennettä vuorokauden ympäri. Visiona on, että vuonna 2018 alueen varaverkkojärjestelmä toimii luotettavasti ja on sekä tunnustettu että tunnettu jatkuvasti kehitettävä kokonaisuus. Tavoitteena on paitsi luoda viranomaisille varaverkon yhteydet, kehittää radioamatööritoimintaan uusia osallistumistapoja ja lisätä samalla toiminnan tunnettavuutta. Strategiana on tavoitteiden saavuttaminen sitouttamalla yhteistyötahot ja amatöörit alusta lähtien mukaan kehittämiseen ja toteuttamiseen. Järjestelmän rakentaminen ja ylläpito tapahtuu vapaaehtoisvoimin Pohjois-Karjalan Radiokerhon vastatessa toteutuksesta viranomaisten ja muiden yhteistyötahojen kanssa.

Projektiryhmän perustamisen jälkeen käynnistyi verkon suunnittelu sekä rakentamisessa ja ylläpidossa tarvittavan osaamisen kehittäminen. Alkuun allekirjoitettiin yhteistyösopimus Pohjois-Karjalan pelastuslaitoksen kanssa, joka tiivisti yhteistyötä myös muiden viranomaisten sekä eri yhteistyökumppaneiden kanssa. Vuosina 2014-2015 tehtiin tutkimustyötä ja toteutettiin ensimmäisen vaiheen asemien rakentaminen. Jatkumona edelliselle oli vuosina 2016-2018 toteutettu toisen vaiheen

asemien rakentaminen ja kehittäminen. Toteutusta seurataan järjestelmällisesti vuosittaisen toimintakertomuksen ja raporttien avulla. Alueen radioamatöörit, viranomaiset ja yhteistyökumppanit järjestävät säännöllisesti harjoituksia, joissa testataan varaverkon toimivuutta. Verkon ylläpitokustannuksiin sisältyy muun muassa laitteistojen ja ohjelmistojen uusimisia, koulutusta, tutkimusta ja taajuusmaksuja.

Nykytilassa varaverkko jakaantuu Puhe-, Sanoma- ja Datavarveen. Puhetoistinten runkoverkko on laajennettavissa ja se muodostuu kiinteistä ja tilapäisesti siirrettävistä toistimista. Asemat ovat valvotuissa tiloissa ja niissä on varmennettu sähkönsyöttö. Sanomatoistinten runkoverkko soveltuu muun muassa lyhyiden teksti- ja kuvatiedostojen siirtoon. Verkko voidaan kytkeä Internetiin ja se toimii ilman yleistä sähkö- ja tietoliikenneverkkoa. Datatoistinten runkoverkko on tarkoitettu nopeammalle dataliikenteelle. Toistinasemilla on liityntä kiinteille ja liikkuville asemille. Verkko voidaan kytkeä Internetiin ja sekin toimii ilman yleistä sähkö- ja tietoliikenneverkkoa.

Paikallispuolustus korostaa viranomaisyhteistyötä

Seminaarin jälkimmäisessä osassa keskityttiin paikallispataljoonan viestikoulutukseen ja vapaaehtoiskentän tehtäviin. Teemaan liittyen kertoi Pohjois-Pohjanmaan ja Kainuun aluetoimiston päällikkö everstiluutnantti Mika Seppä kokemuksistaan paikallispuolustusharjoituksista. Vuosina 2017-2018 harjoituksia on järjestetty Oulussa, Kajaanissa, Kuopiossa ja viimeisin elo-syyskuun vaihteessa Joensuussa. Painopiste on ollut paikallispataljoonan toiminnoissa ja viranomaisyhteistyössä. Keskeisinä teemoina ovat olleet viranomaisten välinen tiedonkulku ja yhteisen tilannekuvan muodostaminen. Painopistettä siirretään tulevina vuosina sotilasalueeseen ja maakunnalliseen viranomaisyhteistyöhön. Uutena teemana keskitytään yhteisen tilannekuvan käyttämiseen.

Harjoitushavaintoina Seppä toi esille pataljoonatason johtamisessa

Paikallispuolustuksen johtamisjärjestelmien kehittämiseen keskittynyt seminaari sai varauksettoman kiitoksen monipuolisista ja ajankohtaista sisällöistään. Myös teknistä toteutusta etäosallistumismahdollisuuksineen kiiteltiin. Kehittämisesityksenä oli aikataulun tiivistäminen.

tehtävätaktiikan ja toiminta-alueen ”staattisuuden”, jolle luonteenomaista on rakennuksissa sijaitsevat lukuisat joukkuetason toimipaikat. Tehtävien toimeenpanossa korostuu välitön johtaminen sekä yhteysupseereiden sijoittaminen tärkeimpiin kumppaneihin. Yhteysjärjestelyjä helpottaa se, että laajakaistaista tiedonsiirtoa on tarjolla runsaasti. Myös viranomaisyhteistyöhön on tarjolla toimivat johtamisjärjestelmäpalvelut. Pataljoonan johtamisen pääväline on Maavoimien tietojärjestelmä (MATI), joko ulotetaan jopa joukkuetasolle asti. Vanhaa kenttäradiokalustoa voidaan hyödyntää yksikön sisäisen, ja parikaapelia kiinteiden toimipaikkojen sisäisen johtamisen varmentamiseen. Haasteena on johtamispaikkoina käytettävien matkailu- ja henkilöpakettiautojen sekä toimistokonttien taistelunkestävyys.

Viestintä muodostaa oman tärkeän kokonaisuuden, johon pitää valjastaa koko viranomaisviestinnän kirjo. Sosiaalisen median käyttö on ollut menestys, jonka hyödyntämistä poikkeusoloissa tulee vakavasti harkita. Viestinnän koulutus on avainasemassa. Kehittämisen osalta esille nousivat myös salausmenetelmät. Paras tulos saavutettaneen sopivasti vanhan osaamista palauttamalla (puhe- ja paikanpeitteistöt) ja uutta johdonmukaisesti käyttöönottamalla (liitetiedostosalaus), johon kytkeytyy suunniteltu, ohjattu ja valvottu kaupallisten (“arjen”) järjestelmien ja palveluiden hyödyntäminen. Myös paikallisia radiojärjestelmiä kannattaa hyödyntää. Johtamisessa tietojärjestelmäosaamisen kehittäminen on avainasemassa. Tavoitteiden saavuttamiseksi tulee reserviläisistä perustettavilla joukoilla edellä mainitut toimet olla kiinteä osa kaikkia koulutustapahtumia.

”Itsekin tekemällä voi tulla ihan hyvä lopputulos” (K Räikkönen)

Joonatan Kuorikoski toi seminaariin esikunta- ja viestikomppanian (PAIKP) päällikön näkemyksen joukkonsa kouluttamisesta ja reserviläispäällikön roolista pääkouluttajana. Kuorikoski on poikkeuksellisen aktiivinen vapaaehtoinen maanpuolustaja. ”Kasvualustana” hänellä on toiminut Maanpuolustuskoulutusyhdistyksen Helsingin Viesti- ja johtamisjärjestelmäkouluttajaoukkue. Taustastaan johtuen hän on ollut vahvalla panoksella mukana myös MPK:n johtamisjärjestelmä- ja viestikoulutusohjelmatyössä. Esityksessään Kuorikoski toi esille kiinteän yhteistoiminnan Kaartin jääkärirykmentin kanssa, missä hänen näkemyksensä mukaan hyödynnetään vapaaehtoisten kouluttajien osaamista laajamittaisesti.

Haasteista reservin yliluutnantti toi esille rajoitetun pääsyoikeuden luokiteltuun materiaaliin, joka näyttäytyy erityisesti oman joukon sodan ajan suunnitelmien taustatietojen hankkimisessa ja oman joukon tehtävän ymmärtämisessä osana kokonaisuutta. Osaamisen kehittämisen näkökulmasta on huomattava, että esikunta- ja viestijoukon päällikkyys edellyttää viestitoiminnan lisäksi tietämystä komentopaikkojen toiminnasta, tiedustelusta, pioneeritoiminnasta ja huollosta. Eräänlaiseksi haasteeksi hän listasi myös joukkojen saamisen vapaaehtoisiin harjoituksiin, koska sitoutumisen aste ei esikunta- ja viestiyksikössä ole samaa luokkaa kuin esimerkiksi maakuntakomppanioissa.

Mahdollisuuksiin Kuorikoski listasi henkilöstön, joka on pääsääntöisesti osaavaa ja innostunutta. Toisena mahdollisuutena hän listasi koulutuksen, joka nykyisin voidaan suunnitella yhä enemmän osaamistarpeiden mukaisesti. Vapaaehtoisen koulutuksen avulla on helposti löydettävissä motivoituneet henkilöt. Parin viimeisen vuoden aikana Kuorikoski on ollut mukana pääkaupunkiseudulla ja sen läheisyydessä järjestetyissä Kehä- ja Uusimaa-harjoituksissa. Toiminta on ollut nousujohteista ja siten koko joukkoa motivoivaa. Kerää palautetta ja kuuntele aidosti, kertasi Kuorikoski periaatteitaan. Joukkueen ja ryhmänjohtajat tulee saada viiveettä töihin, jonka edellytyksenä on koulutusmenetelmien hallinta. Tarvittaessa joukon pääkouluttajan tulee järjestää kertaava peruskoulutus valveutuneimpien alaistensa tuella. Kolmantena mahdollisuutena Kuorikoski otti esille paikallistuntemuksen, jonka merkitystä ei voi liiaksi korostaa.

Koulutusohjelman toimeenpano tiivistää yhteistoimintaa

Seminaari oli monella tapaa merkittävä virstanpylväs paikallispuolustusjoukkojen viestikoulutuksen kehittämisessä. Tilaisuudessa julkaistiin vuoden takaisessa seminaarissa päätetty Maanpuolustuskoulutusyhdistyksen johtamisjärjestelmä- ja viestikoulutuksen koulutusohjelma. Sen tavoitteena on tuottaa reserviin ja paikallisjoukkoihin suorituskykyisiä johtajia ja taistelijoita, jotka omaavat johtamisjärjestelmä- ja viestialalta riittävät tiedot ja taidot selviytyäkseen heille suunnitelluista sodan ajan tehtävistään. Tavoitteena on myös tuottaa koulutusohjelman toimeenpanon edellyttämä määrä osaavia kouluttajia. Koulutusohjelma huomioi myös arjen välineiden käyttömahdollisuuksien kehitystyön.

MPK:n koulutuspäällikkö Juha Niemi kertoi omassa esityksessään ohjelman sisällöstä. Ohjelma jakaantuu seitsemään kokonaisuuteen, jotka ovat Esikunta- ja viestikomppaniaan sijoitettujen koulutuskokonaisuus (EVK JOJÄ), Paikallispataljoonan esikunnan ja komppanioiden johtamisjärjestelmä- ja viestikoulutuskokonaisuus, Taistelijan perusviestitiedot ja -taidot koulutuskokonaisuus – tietoiskuja, Sähkövoima ja -turvallisuus koulutuskokonaisuus (SVJK), Sissiradistikoulutuksen koulutuskokonaisuus (SR), Johtaja- ja kouluttajakoulutuksen koulutuskokonaisuus ja Arjen välineet koulutuskokonaisuus.

MPK:n tavoite on rekrytoida ja kouluttaa parin seuraavan vuoden aikana kurssien toimeenpanossa tarvittavat kouluttajat ja kurssinjohtajat. Niemi korosti toimeenpanon onnistumisessa Viestikiltojen ja Maanpuolustuskoulutusyhdistyksen välistä yhteistoimintaa. Motivaattoreina nuoret ja halukkaat viestikiltalaiset saavat mielekästä tekemistä, toiminta tukee jäsenrekrytointia ja tarjoaa erinomaisen mahdollisuuden kiltojen koulutustoiminnan kehittämiselle. Osallistuminen varmistaa samalla, että kilta saa sille kuuluvan osan kansallisista resursseista.

Viestikiltakenttä vastaa haasteeseen. Johtamisjärjestelmä- ja viestikouluttajapoolin muodostamisessa hyödynnetään Viestikiltojen Liittoa ja viestikilloista muodostuvaa alueorganisaatiota. Kouluttajapoolien ylläpidossa viestikillat pitävät yhteyttä alueella toimiviin puolustusvoimien joukkoihin, joista tärkeimpinä aluetoimistot, alan yrityksiin ja yhdistyksiin sekä oppilaitoksiin. Kuluvan vuoden aikana käynnistetään toimeenpanon suunnittelu, perehdytään koulutusohjelmaan ja sovitaan yhteistoiminnasta Maanpuolustuspiirien päälliköiden kanssa. Toimeenpanoa tukee Viestikiltojen Liiton valtakunnallisen koulutuspäällikön ja viestikiltojen alueellisten koulutuspäälliköiden rekrytointikampanja. Tarjolla on mielekästä tekemistä hyvässä seurassa kansallisen varautumisen hyväksi!

VM

TEKSTI: SEPPO URO, KUVAT: SA-KUVA

Jääkärieversti Eric Heimbürger, ensimmäinen viestitarkastaja

Eric Heimbürger kuului siihen pieneen jääkäriupseerien joukkoon, jonka johdolla puolustusvoimien viestijoukot saivat alkunsa sata vuotta sitten. Hän lienee tuolloin ollut eräs aikakautensa perusteellisimman viestikoulutuksen saaneista jääkäreistä. Heimbürgerin syntymästä tuli viime kesänä kuluneeksi 130 vuotta.

Eric Alexander Amandus Heimbürger syntyi Espoossa 16.6.1888. Hänen vanhempansa olivat kartanonomistaja Nicolai Heimbürger ja hänen puolisonsa Therese von Jessen. Heimbürger kirjoitti ylioppilaaksi Helsingin uudesta ruotsalaisesta yhteiskoulusta vuonna 1908, minkä jälkeen hän aloitti opinnot Helsingin yliopiston lainopillisessa tiedekunnassa. Mutta jo seuraavana lukuvuonna hän siirtyi opiskelemaan Teknillisen korkeakoulun konerakennusosastoon, josta vuonna 1913 jatkoi tekniikan opintoja Saksassa. Vuonna 1914 hän suoritti diplomi-insinöörin tutkinnon Karlsruhen teknillisessä korkeakoulussa. Ensimmäisen maailmansodan puhkeaminen kesällä 1914 vaikeutti pääsyä kotimaahan, minkä vuoksi Heimbürger monien muiden suomalaisten tavoin jäi töihin Saksaan.

Suomen itsenäisyyttä tavoitelleiden aktivistien tehtyä Saksan kanssa sopimuksen suomalaisille vapaaehtoisille annettavasta sotilaskoulutuksesta tieto asiasta levisi myös Saksassa opiskelevien ja työskentelevien suomalaisten keskuuteen. Kun Heimbürger sai tästä tietää, hänkin päätti liittyä maanmiestensä pariin ja ilmoittautui Lockstedtin leirillä ensimmäisten joukossa jo ns. Pfadfinder-kauden alkaessa 25.2.1915. Samana päivänä astui palvelukseen myös hänelle läheiseksi jääkäritoveriksi tuleva insinööri Väinö Pasanen. Kolme viikkoa myöhemmin joukkoon liittyi myös diplomi-insinööri Lars Birger Homén. Jääkäreille ryhdyttiin jo Pfadfinder-kaudella antamaan myös viestikoulusta. Sitä ohjasi aluksi saksalainen luutnantti, joka käytti apukouluttajina myös muutamia suomalaisia jääkäreitä, heidän joukossaan myös Heimbürger. Näissä tehtävissä hän ansioitui niin, että hänet nimitettiin Hilfsgruppenführeriksi jo syyskuussa 1915 ja Gruppenführeriksi tammikuussa 1916. Heimbürger osallistui itse sekä oppilaana että opettajana useille jääkäreille järjestetyille viestikursseille ja sai ensimmäisten joukossa myös radiosähköttäjän koulutuksen. Jääkärikauden lopulla hän kävi myös johtajatehtäviin valmentaneen sotakoulun A-kurssin ja ylennettiin yliluutnantiksi 11.2.1918. Heimbürger osallistui Jääkäripataljoona 27:n mukana myös Missejoen, Riianlahden ja Aajoen taisteluihin. Hän palasi Suomeen jääkärien pääjoukon mukana 25.2.1918.

Puolustusvoimien viestijohtoa neuvottelupäivillä Äänislinnassa maaliskuussa 1942. Eturivissä vasemmalta Mauno Liesi, Veikko Veijola, Eric Heimbürger, Leo Ekberg, Arthur Saarmaa, Rainer Kirjokallio ja Eero Erto. Seisomassa vasemmalta Jouko Pohjanpalo, Walter Alho, Matti Virva, Risto Kare, Antero Muukkonen, Veikko Saura, K. Himberg, K. Lönnroth, Mauno Liukkonen ja A. Rostedt.

Maaliskuun alussa 1918 annetulla Ylipäällikön sotilaskäskyllä määrättiin puolustusvoimiin perustettavaksi sen ensimmäinen viestijoukko-osasto,

Kenttälennätinpataljoona. Pataljoonan komentajaksi määrättiin jääkärimajuriksi ylennetty Birger Homén, 1.Komppanian päälliköksi jääkäriyliluutnantti Eric Heimbürger ja 2.Komppanian päälliköksi jääkäriyliluutnantti Väinö Pasanen. Pataljoonan toiminta käynnistyi kantahenkilökunnan kokoontuessa Mikkelin työväentaloon 5.3.1918. Mikkeliin tuotiin Saksasta myös suuritehoinen kenttäradioasema, jonka päälliköksi määrättiin Heimbürger. Maaliskuun puolivälissä kaupunkiin perustettiin myös Kipinälennätinkoulu, "Funkkerikoulu" radiosähköttäjien kouluttamiseksi. Heimbürger määrättiin edellisten tehtävien lisäksi myös koulun johtajaksi. Huhtikuun alussa Kenttälennätinpataljoona muutettiin jääkäripataljoonaksi, joka osallistui Homénin johdolla vapaussodan lopputaisteluihin Karjalankannaksella. Jääkärikapteeniksi ylennetty Heimbürger luovutti komppanianpäällikön tehtävät kuitenkin nyt jääkärivänrikki Bertel Falleniukselle ja toimi vapaussodan loppuun saakka Päämajan radioasemien päällikkönä.

Kun vapaussodan jälkeen ryhdyttiin perustamaan rauhan ajan puolustusvoimia ja niiden viestijoukkoja, Heimbürger määrättiin aluksi Yleisesikunnan yhteysosaston päälliköksi ja samalla tiedonantojoukkojen komentajaksi, jossa tehtävässä hän toimi vuosina 1918-20. Hän toimi myös puolustusvoimien ensimmäisen viestikurssin ylivalvojana kesällä 1918. Keväällä 1920 tiedonantojoukkojen komentajan virka siirrettiin Sotaväen esikuntaan ja muutettiin tiedonantojoukkojen tarkastajan viraksi. Heimbürgeriä voitaneen siis pitää nykyisen viestitarkastajan varhaisena edeltäjänä, ensimmäisenä tämän tittelin haltijana. Tämä vaihe jäi kuitenkin lyhyeksi, sillä kaikkien teknillisten joukkojen johtoon perustettiin joulukuussa 1920 teknillisten joukkojen komentajan virka ja hänelle oma esikunta. Ensimmäiseksi teknillisten joukkojen komentajaksi määrättiin everstiluutnantti, varatuomari Onni Hämäläinen. Hänet määrättiin kuitenkin jo seuraavana vuonna puolustusministeriksi ja hänen tilalleen määrättiin jääkärieverstiluutnantti Unio Sarlin. Virka muutettiin vuonna 1927 teknillisen tarkastajan viraksi. Sarlin oli koulutukseltaan diplomi-insinööri ja pioneeriupseeri ja hän toimi tehtävässä aina

Kuninkaalliseen Preussin Jääkäripataljoona 27:een perustettiin tiedonanto-osasto 2.10.1917. Vasemmassa reunassa jääkäri Eric Heimbürger.

Viestijoukkojen lähetystöä onnittelukäynnillä: eversti Winter, everstiluutnantti Erto, everstiluutnantti Turunen, majuri Sepperi, lotta Koroskari, korpraali Backlund, korpraali Pyhtää, sotilasmestari Nissilä, majuri Loikkanen, eversti Heimburger, kapteeni Laitinen. Mikkeli, Tuukkala 20.7.1944.

talvisotaan saakka. Jääkärimajuriksi ylennetty Heimbürger määrättiin vuonna 1921 teknillisten joukkojen esikuntapäälliköksi ja Sarlinin apulaiseksi, joka edusti käytännössä ylintä viestijohtoa. Tässä tehtävässä hän oli aina vuoteen 1927 saakka toimien useina vuosina myös viestipalveluksen tuntiopettajana Kadettikoulussa. Tämän jälkeen Heimbürger määrättiin Riihimäellä perustetun ja keväällä 1928 Viipuriin siirretyn Erillisen kenttälennätinkomppanian (vuodesta 1930 Erillisen viestikomppanian) päälliköksi. Tässä tehtävässä hän perehtyi hyvin Karjalankannaksen oloihin ja toimikin Erillisen viestikomppanian lakkauttamisen jälkeen vuodesta 1933 aina talvisotaan saakka Viipurissa sijainneen Armeijakunnan esikunnan, ts. käytännössä maavoimien esikunnan pioneeri- ja viestitoimiston päällikkönä. Everstiluutnantiksi hänet ylennettiin vuonna 1933.

Talvisodan liikekannallepanossa vuonna 1939 Heimbürger määrättiin rauhan ajan virkansa mukaisesti II Armeijakunnan viestikomentajaksi, jossa tehtävässä hän toimi kesään 1940 saakka. Sen jälkeen hän toimi aina jatkosodan alkuun saakka Puolustusvoimien Pääesikunnan viestiväline- ja sotasaalistoimiston päällikkönä. Jatkosodan aikana 1941-44 Heimbürger toimi Helsingissä sijainneen Päämajan sotatalousesikunnan viestiosasto II:n päällikkönä. Osasto vastasi viestimateriaalin kehittämisestä ja hankinnoista puolustusvoimille. Osastopäällikkönä Heimbürger teki materiaalihankintoihin liittyen useita komennusmatkoja ulkomaille. Jatkosodan päätyttyä hän siirtyi eläkkeelle, minkä jälkeen hän toimi vielä joitakin vuosia Sähkötarkastuslaitoksen tarkastavana insinöörinä Helsingissä. Jääkärieversti Eric Heimbürger kuoli vuonna 1954 ja hänet on haudattu sukuhautaan Helsingin Hietaniemeen.

VM

TEKSTI JA KUVAT: JANNE KASTEPOHJA

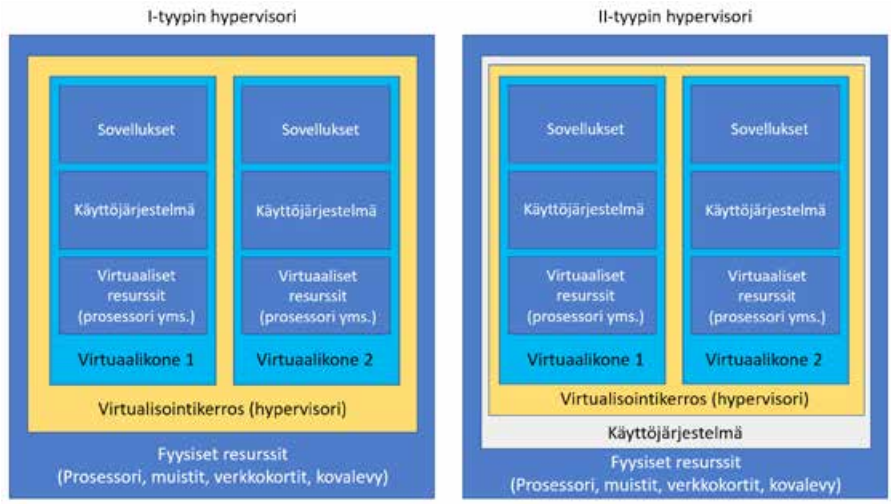
Virtualisointi-infrastruktuurin haavoittuvuudet

Kirjoittaja opiskelee Kyberturvallisuuden maisteriohjelmassa Jyväskylän yliopistossa.

Virtualisointi on muun muassa pilvipalveluissa hyödynnetty konsepti, jonka avulla voidaan tarjota asiakkaille virtuaalikoneita, alustoja tai ohjelmistoja. Tällöin asiakkaiden ei tarvitse omistaa tai hallinnoida fyysistä työasemia, palveluita tai ohjelmistolisenssejä, vaan he maksavat ainoastaan pilvipalveluresurssien käytöstä palveluntarjoajan liikemallin mukaan. Toinen virtualisoinnin yleinen käyttötarkoitus on ajaa yhdellä fyysisellä työasemalla tai palvelimella useita eri palveluja, mikä mahdollistaa resurssien säästämisen, kun voidaan hallinnoida keskitetysti infrastruktuuria ja monistaa valmiiksi konfiguroituja työasemia. Yrityksissä virtualisoinnin hyödyntämisessä on pääasiassa taloudellinen motiivi, kun työasemien hankkimiseen, ylläpitämiseen ja uusimiseen käytettäviä resursseja kyetään vähentämään.

Edellä mainittujen syiden lisäksi virtualisointi mahdollistaa ohjelmistojen tai päivitysten tuotannon yhteydessä testaamisen niin eristetyssä ympäristöissä kuin erilaisilla kokoonpanoillakin. Virtuaalikoneita hyödynnetään myös esimerkiksi haittaohjelmien ja virusten toiminnan ja rakenteen tutkimuksessa, vaikka nykyään moni haittaohjelma pyrkii havaitsemaan, onko se todellisessa vai virtualisoidussa ympäristössä.

Virtualisoinnin hyötyihin kuuluu myös mahdollisuudet ottaa järjestelmän palauttamista varten tallenteita virtuaalikoneen nykytilasta vikatilanteita varten sekä useiden eri käyttöjärjestelmätyyppien ylläpitämisen samanaikaisesti samalla palvelimella. Ongelmatilanteissa virtuaalikone voidaan poistaa ja luoda uudelleen melko vaivattomasti. Virtuaaliverkon rakentaminen työasemalle on hyödyllistä opetellessa tietoliikenteen, tietoverkkojen tai kyberturvallisuuden perusteita.



Virtuaalikoneiden rakenne ja hypervisorien erot.

Virtualisoinnin hyödyt ovat kiistattomat, mutta mitä haavoittuvuuksia siihen liittyy? Onko se hyödyistä huolimatta turvallinen tapa toteuttaa yrityksen tai kodin verkkoratkaisut? Tämän artikkelin tavoitteena on esitellä ja pohtia virtualisoinnin turvallisuutta yksittäisen ihmisen näkökulmasta suoraan kotitietokoneella toteutettuna tai välillisesti pilvipalvelujen käyttämisen muodossa.

Virtuaalikoneiden rakenne

Virtualisoinnin haavoittuvuuksien ymmärtämiseksi ja niiltä suojautumiseksi täytyy ensin ymmärtää sen toteutusta ja rakennetta. Virtualisoinnissa keskeisin komponentti on konseptissa käytettävä ohjelma, hypervisori (*Hypervisor*, *Virtual Machine Monitor*), määrittää virtuaalikoneelle käytössä olevat resurssit, muun muassa prosessorin ytimet eli laskentatehon sekä levytilan ja muistit. Muut pääkomponentit ovat käyttöjärjestelmä, työkalut tai ajurit sekä fyysiset resurssit, joita virtuaalikoneelle on annettu lupa käyttää. Tallennukseen virtuaalikone voi käyttää isäntäkoneen levytilaa, ulkoista laitetta tai verkkolevyä.

Hypervisorin tehtävänä virtuaalisoinnissa on koneiden eristämisen ja resurssien allokoinnin lisäksi komentojen ja syötteiden ohjaaminen virtuaalikoneiden käyttöjärjestelmien ja ohjelmien sekä isäntäkoneen prosessorin, muistien, syöttö- ja vastelaitteiden (*I/O*) sekä levyresurssien välillä. Hypervisoreita kahta tyyppiä: tyypin I hypervisorit (esim. VMware ESXi) voidaan asentaa suoraan isäntäkoneen fyysisten resurssien laiteohjelmiston päälle. Tyypin II hypervisorit (esim. VMware Workstation ja Fusion, Oracle Virtualbox) asennetaan isäntäkoneen käyttöjärjestelmän päälle, mikä lisää yhden kerroksen virtualisointi-infrastruktuuriin. Hypervisorin valinta riippuu virtuaaliverkon toteutuksesta: käytetäänkö isäntänä

toimivaa työasemaa vai toimiiko se ainoastaan virtuaaliverkon palvelimena.

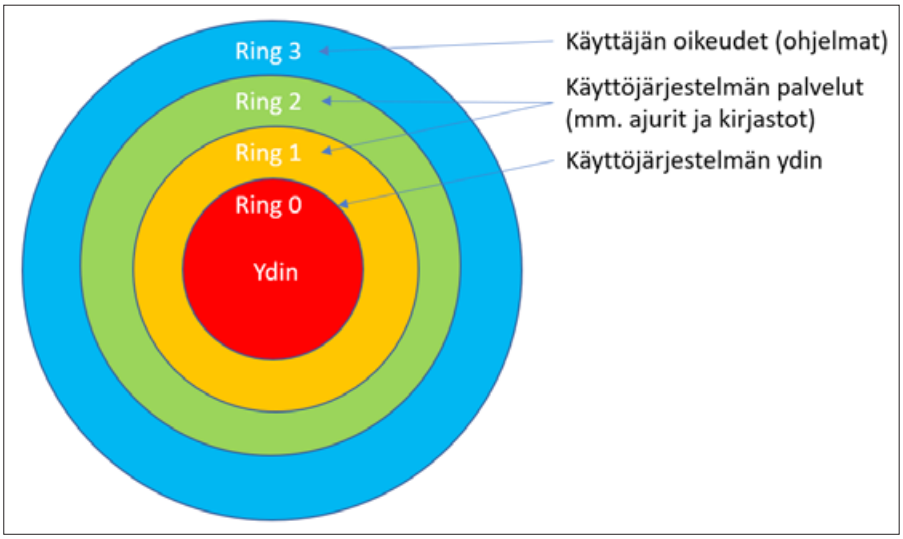
Muut keskeiset erot hypervisorityyppien välillä ovat käyttöoikeustasot x86-arkkitehtuurissa. Tyypin I hypervisori toimii käyttöjärjestelmän oikeuksilla (Ring 0) ja hypervisorin avulla toteutetut virtuaalikoneet käyttäjän oikeuksilla (Ring 3). Tyypin II hypervisori toimii ainoastaan käyttäjän oikeuksilla, koska se toimii käyttöjärjestelmän päällä.

Virtualisointi-infrastruktuurin tietoturvauhkat

Suurimmalle osalle käyttäjistä virtualisointi on ollut ja on edelleen turvallinen tapa välttää työaseman saastuminen tai siihen tunkeutuminen. Virtualisointi-infrastruktuuria uhkaavat samat uhkat kuin fyysistä infrastruktuuria, vaikka niiden esiintymistapa ja -muoto voi erota. Uhkat voivat olla seurausta heikosta tai puutteellisesta konfiguroinnista tai järjestelmien päivittämättömyydestä ja paikkaamattomuudesta siihen, kun ulkoiset (tai sisäiset) hyökkääjät pyrkivät tarkoituksellisesti väärinkäyttämään järjestelmiä tietojen varastamiseksi, luvattomaan tunkeutumiseen tai virtualisointi-infrastruktuurin hyödyntämiseksi uusiin hyökkäyksiin.

Virtualisoinnin ominaisuudet täytyy ottaa huomioon etenkin infrastruktuurin rakennusvaiheessa, ettei luoda turvallisuusuhkia vahingossa tai huolimattomuuden vuoksi:

- Koska virtuaalikoneita voidaan luoda ja poistaa nopeasti, puutteellisen tai heikon konfiguraation mahdollisuus on todellinen. Virtuaalikoneita ei aina konfiguroida kunnolla, koska ne voidaan nähdä ongelmien ilmetessä helposti hävitettäviksi ilman että suuria määriä esimerkiksi dataa menetetään. Virtuaalikoneiden markkinointi turvallisina voi antaa valheellisen turvallisuudentunteen ja vähentää tietoturvaohjeiden sekä turvallisten toimintatapojen noudattamista.
- Virtuaaliverkon liikennettä, etenkin hypervisorin ja virtuaalikoneiden välistä, ei yleensä valvota vastaavalla tavalla kuin fyysisten verkkojen sisäistä liikennettä.



Käyttöoikeudet x86-arkkitehtuurissa.

- Virtuaaliverkkojen valvontavastuut ja käyttöoikeushallinnan toteuttaminen on haasteellisempaa virtuaaliverkoissa niiden verkoille tyypillisten nopeiden muutosten vuoksi, etenkin laajemmissa tai monimutkaisemmissa verkoissa.

Virtuaalikoneesta poistuminen (*virtual machine escape*)

Hypervisoreista on niiden yleistymisen myötä löydetty ohjelmistovirheitä tai haavoittuvuuksia, jotka mahdollistavat haitallisen koodin suorittamisen isäntäkoneen käyttöjärjestelmässä tai isäntäkoneen ytimessä (kernel) läpäisten käyttöoikeusmallin osittain tai kokonaan. Haitallisella koodilla voidaan pyrkiä luomaan, muokkaamaan tai poistamaan virtuaalikoneita. Vaihtoehtoisesti on mahdollista muokata olemassa olevien virtuaalikoneiden ominaisuuksia eli esimerkiksi allokoitua levytilan tai muistin määrää tai käyttöoikeuksia. Osassa havaituista haavoittuvuuksista hyökkääjä pystyy hankkimaan kontrollin päällimmäiseen, eli virtualisointi-, kerrokseen ja kiertämään käyttöoikeudet, toimimaan luotetulla vyöhykkeellä tai pääsemään käsiksi muilla virtuaalikoneilla tai isäntäkoneella ajettuihin ohjelmiin tai niiden sisältämään tietoon.

Kriittisimmät haavoittuvuudet mahdollistavat hyökkääjän murtautumisen ulos virtuaalikoneesta niin, että käyttäjä pystyy suorittamaan luvatta haitallista koodia isäntäkoneen ytimessä, mikä tekee siitä virtualisoinnin vakavimman tietoturvauhkan. Koska virtuaalikoneet käyttävät isäntäkoneen fyysistä muistia ja levytilaa, aiheuttaa isäntäkoneen haltuunotto käytännössä kaiken virtuaalikoneiden tietojen vaarantumisen ja tapahtuessa pilvipalvelimilla on suoranainen katastrofi.

Virtuaalikoneesta poistumiseen liittyvät haavoittuvuudet voidaan jakaa seuraaviin kategorioihin:

- Virtuaalikoneen hypyttäminen tai ”hyper jumping” ovat hyökkäyksiä, jossa yhtä virtuaalikonetta (esim. pilvipalvelusta ostettua) käytetään hyökkäyksiin muita virtuaalikoneita vastaan hyödyntämällä hypervisorissa olevia haavoittuvuuksia. Ensimmäinen kohde voi olla virtuaalikone, jossa on esimerkiksi päivittämätön käyttöjärjestelmä tai ohjelmisto. Tämän jälkeen kohteeksi valitaan hypervisori, jotta kyetään ”hyppäämään” virtuaalikoneesta toiseen eli päästä tunkeutumaan hypervisorin muihin virtuaalikoneisiin.
- Sivukanavahyökkäykset virtuaalikoneiden sisällä tai välillä kohdistetaan vuokrattuihin alustoihin tai fyysiseen infrastruktuuriin, kun virtuaalikoneet ajetaan samalla palvelimella. Jos tietojen jakaminen (esim. leikepöytä) on sallittu virtuaalikoneiden välillä, samaa fyysistä muistia jaetaan useille

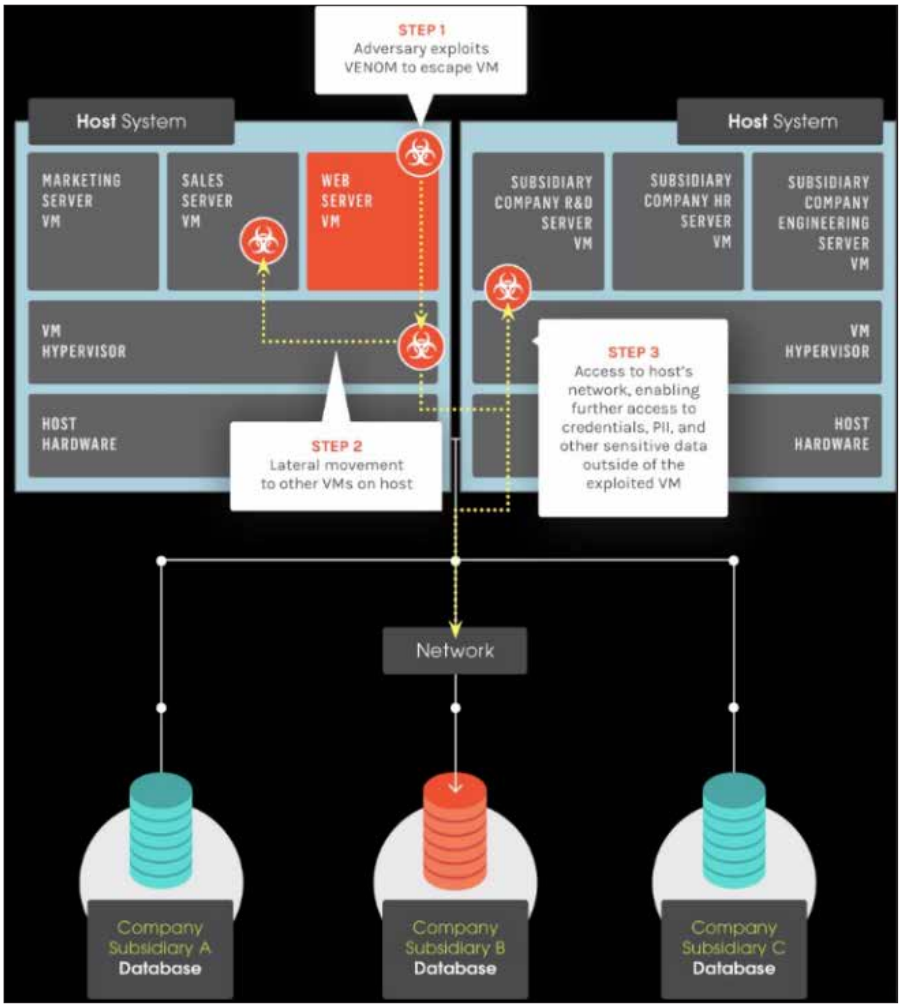
eri virtuaalikoneille. Silloin hyökkääjä kykenee tyhjentämään ja lataamaan muistin eli voi yrittää lukea tietoa, esimerkiksi tunnuksia ja salasanoja, toisen virtuaalikoneen muistista. Toinen vastaava hyökkäystapa ei vaadi edes sivujen jaon sallimista.

- Virtuaalikoneiden hallintaohjelmistot (*Virtual Machine based rootkits, VMBR*) on paritettu virtuaalikoneiden levykuvien (*image*) kanssa. Hallintaohjelmistot asentavat itsensä isäntäkoneen laiteohjelmiston päälle. Tässä tapauksessa kyse ei ole teknisesti virtuaalikoneesta poistumisesta, vaan virtualisointiin liittyvästä haittaohjelmasta, joka latautuu esimerkiksi saastuneen levykuvan yhteydessä.
- ”Hyperjacking” on hyökkäys, jossa hyökkääjä luo saastutetun hypervisorin virtuaalikoneiden kontrolloimiseen tai ottaa haltuun hypervisorin, jotta saa haltuunsa kaikki serverillä ajettavat virtuaalikoneet. Hyökkäys on lähinnä teoreettinen, koska hyökkääjän tarvitsee käytännössä saada fyysinen pääsy serverille tai huijata järjestelmäylläpitäjä ajamaan haitallista koodia.

Kuinka virtuaalikoneiden haavoittuvuuksilta suojaudutaan?

Kuten tietoturvallisuudessa yleensä, ei ole 100 % turvallista tapaa hyödyntää virtualisointia, vaikka kaikkia komponentteja pystyttäisiin kontrolloimaan itse. Kuitenkin on olemassa tiettyjä tapoja suojata järjestelmää ja vähentää järjestelmään tunkeutumisen todennäköisyyttä:

- Älä käytä mitään ylimääräisiä virtuaalikoneiden hallintaan käytettäviä sovelluksia, jotka asennetaan virtuaalikoneeseen vaan hallitse virtuaalikoneita ainoastaan isäntäkoneen kautta.
- Älä jaa resursseja virtuaalikoneiden välillä, vaan hoida resurssien käyttö hypervisorin kautta.
- Käytä mahdollisimman turvallista käyttöjärjestelmää.
- Pidä käyttöjärjestelmät, ohjelmistot ja hypervisori päivitettyinä.
- Käytä vain yksityistä virtuaalista lähiverkkoa (*Private VLAN*), jotta virtuaalikoneista ei ole näkyvyyttä toisiin virtuaalikoneisiin ja niistä voi asioida ainoastaan yhdyskäytävälle.
- Jos haluat todella eristää virtuaalikoneita toisistaan, älä pinoa niitä saman hallintatyökalun alaisuuteen.
- Käytä virtualisoinnissa palomuureja ja eristä konfiguroinnilla verkkoalueet toisistaan.
- Estä yhdistäminen tietokantapalvelimeen suoraan sisäverkon virtuaalikoneilta.
- Valvo verkkoliikennettä isäntäkoneen ja virtuaalikoneiden välillä epätyypillisen verkkoliikenteen havaitsemiseksi, esimerkiksi tunkeutumisenesto-ohjelmalla (*IDS*).



Esimerkki Venomin hyödyntämisestä.

Esimerkkejä virtualisointi-infrastruktuurin haavoittuvuuksista

Suuri osa virtuaalikoneista poistumisen mahdollistavista haavoittuvuuksista vaativat ainakin vähän muiden haavoittuvuuksien hyödyntämistä ja osa hyökkäyksistä on ainoastaan teoreettisia, eikä niitä hyödyntäviä tunnettuja haittaohjelmia ole kehitetty eikä koodi ole julkisesti saatavilla. Havaitut virtuaalikoneesta poistumisen mahdollistaneet haavoittuvuudet ovat olleet hypervisorissa, muistissa tai ytimessä. Fyysiseen muistiin kohdistut hyökkäykset eivät riipu käyttöjärjestelmästä, koska ne kohdistetaan ytimeen. Useassa tapauksessa myöskään hypervisorin haavoittuvuudet eivät riipu käyttöjärjestelmästä, koska niistä on versioita eri alustoille.

Cloudburst

Cloudburst oli yksi ensimmäisistä tietoturvatutkijoiden havaitsemista vakavista haavoittuvuuksista, joka mahdollisti virtuaalikoneessa syötetyn koodin ajamisen isäntäkoneen käyttöjärjestelmässä. Haavoittuvuus havaittiin vuonna 2009 ja se esiintyi useissa eri VMwaren hypervisoreissa. Hyökkäyksessä tavoitteena oli muuttaa tarkoituksella komennon lähde- tai kohdemuistipaikka virtuaalikoneelle allokoidun muistialueen ulkopuolelle. Operaatio kopioi

komennot isäntäkoneen muistipuskurista eli tekniikasta riippuen sai ohjelman lukemaan isäntäkoneen muistista tietoa virtuaalikoneen käyttäjälle. Vaihtoehtoisesti kohdemuistipaikan väärentäminen mahdollistaa hyökkääjän kirjoittaa muutamien kilobittien mittaisia komentojonoja ajettavaksi isäntäkoneen käyttöjärjestelmässä.

Ongelmana tässä haavoittuvuudessa oli muistipuskurin jakaminen isäntä- ja virtuaalikoneen välillä. Tosin hyökkääjän täytyi ensin kyetä murtautumaan virtuaalikoneelle ja sen jälkeen tietää kontrolloimalleen virtuaalikoneelle allokoidun muistialueen raja-arvot, jotta hän pystyi määrittämään lähde- tai kohdemuistipaikan sen ulkopuolelle.

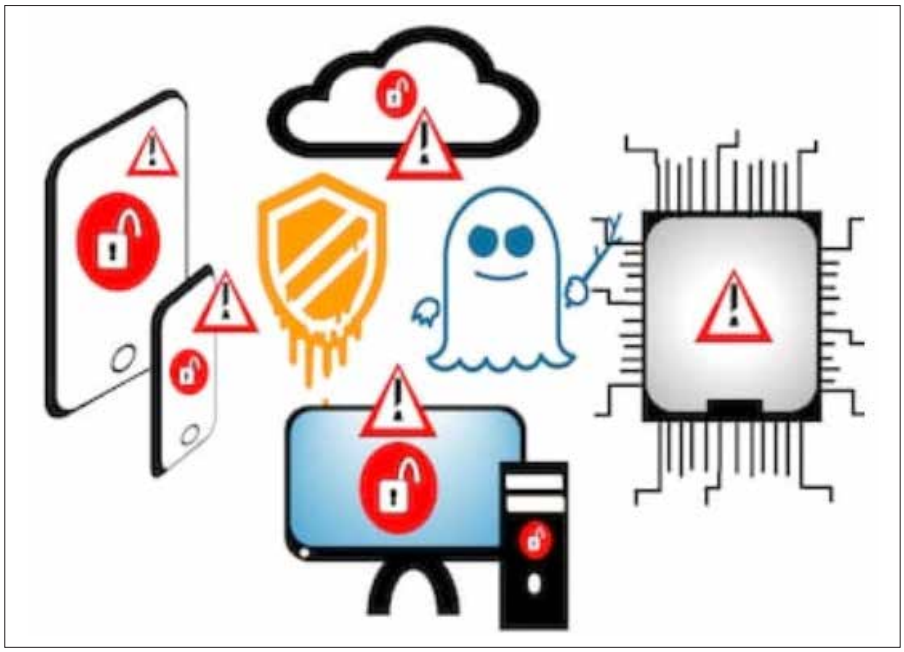
Venom

Yksi vakavimmista virtuaalikoneesta poistumisen mahdollistavista haavoittuvuuksista löydettiin vuonna 2015 ja nimettiin Venomiksi. Se hyväksikäytti Quick Emulators (QEMU) -ohjelman ominaisuutta, koska QEMU:n levyaseman kontrollointiin käytettävässä virtuaalisessa komponentissa oli muistin ylivuotohaavoittuvuus, joka mahdollisti koodin ajamisen isäntäkoneen muistissa.

Hyökkäys on vaativa toteuttaa, koska se vaati järjestelmävalvojan oikeudet virtuaalikoneessa, jossa se suoritetaan, ja muistin ylivuotohaavoittuvuuden hyväksi käyttäminen ei ole yksinkertaista. Haavoittuvuus kuitenkin esiintyi käytännössä kaikissa hypervisoreissa, koska avoimen koodin projektina QEMU oli laajasti käytetty myös muissa tuotteissa. Huvittavaa tilanteessa on QEMU:n asetus, jossa haavoittuvuuden sisältävä koodi oli sisällytetty kaikkiin sen avulla luotaviin järjestelmiin, vaikka niissä ei edes simuloitaisi levyasemaa lainkaan.

Meltdown ja Spectre

Vuoden 2018 alussa Grazin yliopiston tietoturvatutkijat paljastivat kolme vakavaa haavoittuvuutta, jotka he olivat nimenneet Meltdowniksi (variantti 3) ja Spectreksi (variantit 1 ja 2). Kaikki haavoittuvuudet liittyivät hyökkäyksen toteuttamiseen suoraan tietokoneen



Spectre vaikutti laajasti erilaisiin laitteisiin.

prosessorin ytimessä. Koska paljastetut haavoittuvuudet toimivat myös virtualisoidun muistin suhteen, voidaan niitä hyödyntää virtuaalikoneesta poistumiseen.

Tutkijat kykenivät todistamaan kummankin Spectre-variantin toiminnan myös käytännössä: haavoittuvuuden varianttia 1 pystyttiin käyttämään käyttöoikeusrajoitusten kiertämiseen ja muistin lukemiseen luvatta, kun taas variantin 2 avulla pystyttiin lukemaan isäntäkoneen muistia jopa 1500 bitin sekuntinopeudella.

Spectre hyväksikäyttää AMD:n, Intelin ja ARM:n prosessoreissa yleisesti käytettyä ominaisuutta ”speculative execution”, jossa prosessori arvaa ohjelmien seuraavaksi tarvittavia tietoja ja lataa ne välimuistiin. Mikäli tietoja ei tarvita, niin ne poistetaan muistista. Tavoitteena on nopeuttaa näin prosessorin toimintaa. Meltdown mahdollistaa Intelin prosessorien muistin suojausten kiertämisen käyttöoikeuksia korottamalla. Meltdown on helpompi estää paikkaamalla laiteohjelmiston tietty funktio.

Haastavaksi tilanteen teki Mozillan vahvistus Spectren ja Meltdownin toimivuudesta myös selainten kautta, mikä loi yhden hyökkäysvektorin lisää ja mahdollisti hyökkäysten toteuttamisen verkon yli. Hyökkäykset voitiin toteuttaa syöttämällä verkkosivulle komentoja JavaScript-muodossa tai ohjaamalla käyttäjän selain edelleen haitalliselle verkkosivustolle. Uusimmat selaimet on tosin jo paikattu näiden haavoittuvuuksien osalta.

Johtuen Spectren laajoista vaikutuksista, käytännössä kaikki serverit ja pilvipalvelujen toimittajat olivat vaarassa ennen laitteiden paikkaamista. Spectren avulla toteutetut hyökkäykset ovat käytännössä mahdottomia havaita, koska niistä ei jää jälkiä perinteisiin lokitiedostoihin. Hyökkäys hyödyntää samaa olemassa olevaa ominaisuutta kuin moni muukin ohjelma tai toiminto, joten sille ei voi luoda sormenjälkiä perinteisiä virustorjuntaohjelmia tai tunkeutumisenesto-ohjelmia varten. Sen vuoksi on mahdotonta sanoa, oliko näitä bugeja koskaan hyväksikäytetty ennen niiden paljastamista.

Yhteenveto

Virtuaalikoneiden käyttö ei tee toiminnasta 100 % turvallista tai eristä sitä aukottomasti isäntäkoneesta johtuen virtualisointikerroksen toteutuksessa havaituista haavoittuvuuksista, jotka ovat mahdollistaneet virtuaalikoneen käyttäjän komentojen suorittamisen isäntäkoneella, tietojen varastamisen tai pahimmillaan isäntäkoneen haltuunoton. Suurin osa virtualisointi-infrastruktuuria koskevista hyökkäyksistä

toteutetaan muistipaikkojen kautta isäntäkoneen muistissa olevien tietojen paljastamiseksi tai komentojen suorittamiseksi isäntäkoneen käyttöjärjestelmässä. Vakavimmat haavoittuvuudet mahdollistavat koodin suorittamisen suoraan ytimessä ja koneen suorittimen valmistajan autentikointimekanismien kiertämisen. Etenkin pilvipalvelujen tarjoajien näkökulmasta virtuaalikoneesta poistumisen mahdollistavat haavoittuvuudet ovat äärimmäisen vakavia, koska yhtä fyysistä palvelinta hyödyntää lukuisia asiakkaita. Kuitenkin suurin osa näistä hyökkäyksistä ovat vaikeita toteuttaa ja vaativat vähintään niiden yhdistämistä muiden haavoittuvuuksien hyväksikäyttöön.

Tällä hetkellä Meltdown ja Spectre sekä niiden variantit ovat vakavimpia uhkia virtuaalijärjestelmille. Koska kaikkia järjestelmiä ei voida paikata ja koodi on julkistettu, tulee sen variantit olemaan läsnä vielä pitkään. Spectren vaikutusten täydellinen ehkäiseminen vaatii prosessorivalmistajilta koko prosessorien toimintarakenteen muuttamista.

Virtualisoinnin toteuttamisen voidaan sanoa olevan turvallista etenkin yksittäiselle ihmiselle johtuen sen kautta toteutettavien hyökkäysten teknisen toteutuksen haastavuudesta ja harvinaisuudesta. Suurin osa löydetyistä haavoittuvuuksista ovat olleet tietoturvatutkijoiden löytämiä ja ainoastaan laboratorio-oloissa todistettuja. Lisäksi niiden toteutukselle on yleensä vaadittu kohdejärjestelmän perusteellinen tuntemus ja fyysinen pääsy. Myöskään haavoittuvuuksia hyödyntäviä työkaluja tai haittaohjelmia ei juurikaan ole julkisesti saatavilla.

Todennäköisempää on, että hyökkäykset kohdistetaan perinteisemmillä tavoilla infrastruktuurin muihin osiin, esimerkiksi palvelimeen, käyttöjärjestelmään, käytettyyn protokollaan tai muuhun, kuin itse virtualisointi-infrastruktuuriin. Tavallisessa käytössä virtuaalikoneiden turvallisuuden takaa parhaiten tavallisilla turvallisuustoimenpiteillä: suunnittelemalla ja konfiguroimalla virtuaaliverkon asianmukaisesti, lataamalla verkkokuvat turvallisista lähdeosoitteista ja päivittämällä ohjelmistot säännöllisesti. Virtualisoinnista saatavat hyödyt ovat huomattavasti suuremmat kuin sen käytön mukana tulevat ylimääräiset uhkat.

VM

TEKSTI: SAKARI AHVENAINEN

Toffler-ennuste vuodelta 1994 informaatiosodankäynnistä

osa 1/2

Tiivistelmä: Lähes neljännesvuosisadan takainen ennustus informaatiosodankäynnistä pitää yllättävän hyvin paikkansa, niissä asioissa mitä se ennusti. Ennustuksen pahimmat puutteet ovat siinä, mitä se ei osannut ennustaa. Tärkeimmät, strategiset puutteet olivat tämän artikkelin mukaan intuition ja abstraktin ajattelun puuttuminen! Ajattelun pohjan muuttuminen intuitioksi saattaa olla aikamme tärkein, strategisin muutos, vieläpä kahdella tavalla, ihmisten ja tietokoneiden kautta.
Tämä on Viestimies-lehdelle muokattu ja päivitetty versio artikkelista, joka ilmestyi keväällä 2018 Maanpuolustuskorkeakoulun kirjasarjassa ”Tuleva sota” sen osana 2/3: ”Nykyhetki ennakointien valossa”

Johdanto

Tämän artikkelin tarkoituksena on verrata vuoden 2018 informaatioyhteiskunnan sotaa vuoden 1993 ennustukseen liittyen sekä selvittää sitä, mitä siitä on opittavissa sodankäynnin tulevaisuuden ennustamisessa. Ennustus on tulevaisuustutkijapariskunta Alvin ja Heidi Tofflerin alun perin vuonna 1993 englanniksi ilmestynyt teos, joka ilmestyi suomeksi seuraavana vuonna. Teoksen otsikko on ”Sodan ja rauhan futurologia – Miten selviydymme hengissä 2000-luvulla” (Otava 1994).

Tämä artikkelisarjan rakenne on seuraava: Ensimmäisessä osassa (tässä) esitellään tämän johdannon jälkeen Tofflereiden ennustusten arvioinnin pohjaksi vertailumalli, alustava teoria, joka on Quincy Wrightin sodankäynnin historian megamalli (QWM). Seuraavana esitetään Tofflereiden ”isot ja pienet ennustukset” ja arvioidaan niitä nykytiedon valossa.

Seuraavassa osassa 2/2 (Viestimies 1/2019) nostetaan esille sellaisia asioita, jotka ovat toteutuneet, mutta joita ei ole esitetty Tofflereiden teoksesta. Tämän jälkeen arvioidaan pienimuotoisesti ja oppimistarkoituksessa, mitä Suomessa olisi voinut tapahtua, jos vuonna 1993 Puolustusvoimien kehittäminen olisi linjattu Tofflereiden mukaisesti. Tässä osassa esitetään myös muutama kriittinen kanta Tofflereiden teokseen sen merkityksen avaamiseksi ja lopuksi esitetään kootut johtopäätökset ja arvioidaan mahdollisuuksia sodankäynnin muutoksen ennustamiselle.

Artikkelisarjan keskeiset kysymykset ovat: Mitä Tofflerit ennustivat teoksessaan ”Sodan ja rauhan futurologia – Miten selviydymme hengissä 2000-luvulla” (Otava 1994)? Miten ennustukset onnistuivat nykytiedon valossa? Mitä Tofflerit eivät osanneet ennustaa? Mitä peruskritiikkiä teoksesta on olemassa? Millaiset olisivat Suomen asevoimat, jos Tofflereiden ennustuksia olisi seurattu? Mitä tämän ennustuksen perusteella on opittavissa sodankäynnin tulevaisuuden ennustamisen vaikeassa taidossa?

Vertailupohja: Quincy Wright -malli (QWM) sodankäynnin historian megavaiheista

Tofflereiden teoksen näkemysten ja ennustusten asettamiseksi perspektiiviin käytetään vertailulähteenä kirjoittajalle tuttua ja Viestimies-lehdessäkin esiteltyä Quincy Wrightin käsitystä sodankäynnin megavaiheista (Wright, Quincy (1942): *A Study of War*. University of Chicago Press, Chicago). Niistä on kehitetty edelleen ennustus postmoderniksi sodankäynniksi ja osoitettu, että mallin taustalla ovat vielä laajemmat teoriat: evoluutioteoria, kybernetiikka ja systeemiteoria (Ahvenainen, Sakari (2016): *The Quincy Wright Model: Postmodern Warfare as a Fifth and Global Phase of Warfare*. Proceedings of the 15th European Conference on Cyber Warfare and Security – ECCWS 2016). Vertailulähde perustuu loogiseen ja systemaattiseen malliin. Siinä on ensin oleellista uuden tason muodostuminen useammasta alemmasta tasosta, esimerkiksi valtio useammasta heimosta. Toiseksi siinä on keskeistä se, että uuden tason ilmiöt ovat yleensä emergenttejä, uusia, niitä ei löydy ilmiöinä alemman tason systeemeistä. Kolman-

neksi siinä on oleellista uusi viestintäteknologia edellytyksenä seuraavalla suuremmalle vaiheelle.

Kirjoittaja on arvioinut aiemmin Quincy Wrightin teoksessaan ennustamia postmodernin sodankäynnin perusominaisuuksia. Ne ovat:

1. globaali taso, joka on esillä Tofflereiden teoksessa
2. sen monet toimijat, jotka ovat esillä Tofflereiden teoksessa
3. globaali kauppa ja työnjako, jotka ovat esillä Tofflereiden teoksessa
4. internet, joka on esillä Tofflereiden teoksessa
5. kaikkialla olevat tietokoneet ja tietokoneverkot, joka on esillä Tofflereiden teoksessa
6. informaatio, joka on esillä Tofflereiden teoksessa
7. kompleksisuus ja kompleksisuuden hallinta, joka on esillä Tofflereiden teoksessa
8. kaupungistuminen (megakaupungit) ja kaupunkisota, jotka eivät juurikaan ole esillä, koska Tofflerit keskittyvät lähinnä tietoon ja tietämykseen
9. hyvinvoinnin lisääntyminen, joka on esillä Tofflereiden teoksessa
10. globaalin kontrollin lisääntyminen, joka on esillä Tofflereiden teoksessa
11. nopeuden lisääntyminen, joka on esillä Tofflereiden teoksessa
12. abstraktiuden lisääntyminen, *joka ei ole esillä (!) Tofflereiden teoksessa*
13. ihmisen usealla tavalla aiheuttamat globaalit katastrofit, jotka myös ovat esillä Tofflereiden teoksessa.

Tofflereilla ei siis ole suuria eroja verrattuna vertailulähteen arvioon postmodernin sodankäynnin perusominaisuuksista. Merkittävin poikkeus on *abstraktiuden lisääntyminen*, jota Tofflerit eivät käsittele. Kun Tofflerit päätyvät tulevaisuuden tutkimukseen liittyvän vuosien käytännön työn jälkeen hyvin samansuuntaiseen tulokseen kuin vertailulähde, se ja Tofflereiden teos tukevat toisiaan. Mutta molemmat voivat myös olla väärässä.

”Suuret” ennustukset ja arvio niiden toteumasta

Tässä luvussa esitetään Tofflereiden teoksen sisällysluettelon tasolla esiintyviä ennustuksia, joita pidetään ”suurina” ennustuksina. Muuten teoksen tekstistä ennustuksiksi luokitellut tekstikappaleet ovat ”pieniä” ennustuksia.

Vain teoksen kolmas osa ”Tutkimusretki tulevaisuuteen” on otsikkotasolla selkeä iso ennustus. Kokonaisuutena teos käsittää kuusi osaa ja 25 lukua.

Teoksen kolmas osa sisältää viisi lukua seuraavasti:

Nissisodat[1]-luvun alaluvussa ”Naurua infosfäärissä” käsitellään ensin sitä, miten sota jatkuu edelleen ajassamme sotana, toisin kuin jotkut toiveikkaasti haluaisivat nähdä. Toiseksi alaluvussa käsitellään laajasti erikoisjoukkoja ja niiden kasvavaa merkitystä tulevaisuuden nissisotilaina. Alaluku ”LIC-Lobby” (LIC = Low Intensive Conflict) jatkaa erikoisjoukkojen käsittelyä ”pienten” sotien, huumesotien ja epävakaiden valtioiden aikakaudella ja työvälineenä. Alaluvussa ”Repputohtori” jatketaan edelleen erikoisjoukkojen käsittelyä tarkastelemalla huippukoulutettuja sotilaita ja heidän erikoisvarusteitaan. Alaluvussa ”Tavoitteena sotilastelepatia” käsitellään vielä erikoisempia uuden sodankäynnin ja erikoisjoukkojen välineitä, kuten vaivihkaa tehtyä DNA-tunnistusta, täydellistä verensiirtoa ja synteettistä telepatiaa. Se arvioi erikoisjoukkojen toimintaa myös muun muassa demokratiaa mahdollisesti vaarantavana tekijänä.

Tofflerit näkivät siis sotien jatkuvan, ja he pitivät erikoisjoukko-operaatioita tulevaisuudessa hyvin tärkeinä. Tästä muun muassa Venäjän Georgian, Krimin ja Ukrainan operaatiot ovat toteutuneita esimerkkejä; tunnuksettomat vihreä miehet (GRU (vast.)). Sodan jatkuminen ajassamme on erityisen suuri ja merkittävä oikeaan osunut ennustus.

Avaruussodat-luvun alaluvussa ”Neljäs ulottuvuus” käsitellään satelliittitiedustelua ja -paikannusta sekä avaruuden käyttöä taloudellisena tapana toimia ja osana taloudellisiakin toimia. Avaruus on Tofflereiden mukaan tullut myös osaksi suurvaltoja pienempien valtioiden toimintaa. Se on siirtynyt strategiasta ja suurvalloista taktiikkaan ja kaikkien kannalta oleelliseksi toiminnaksi. Alaluvussa ”Iranista Israeliin” käsitellään avaruuden käytön leviämistä suurvaltojen ulkopuolelle. Alaluvussa ”Ohjuksen kestävä maailma” käsitellään avaruuspuolustusta ja ohjustorjuntajärjestelmien kasvavaa merkitystä, jälleen myös suurvaltoja pienemmille valtioille. Alaluvussa ”Yhtä paha kuin ydinasehyökkäys” esitellään satelliittien tuhoamisen kehitystä ja sitä, että satelliittien tuhoaminen on yhtä paha kuin pieni ydinasehyökkäys. Alaluvussa ”Pystyyn tapetut satelliitit” käsitellään satelliittien tuhoamista ja niihin vaikuttamista muilla kuin fyysisillä menetelmillä, esimerkiksi häirinnällä, sanomien sieppauksella ja harhautuksella. Tällaisena menetelmänä pohditaan myös niihin ujutettuja vihamielisiä ohjelmistoja. Alaluvussa ”Mustia aukkoja ja salaovia” jatketaan satelliittien manipuloinnin ja harhauttamisen sekä vastatoimien vaikeuden pohdintaa, kun hyökkääjää ei pystytä varmasti tunnistamaan. Alaluvussa ”Avaruuden sydänmaa” esitellään maan, kuun ja auringon ulkoavaruudessa sijaitsevat tasapainopisteet, jotka voivat tulevaisuudessa olla merkittäviä toiminnalle avaruudessa.

Avaruus on vertailulähteen, QWM:n, mukaan yleisesti merkittävä tekijä postmodernin globaalin sodankäynnin vaiheessa. Avaruuden merkitystä korostaa myös kasvava ohjusvaltioiden määrä ja se, että satelliittipaikannusjärjestelmiä on Yhdysvaltojen (GPS) lisäksi Venäjällä (Glonass), Euroopan unionilla (Galileo) ja Kiinalla (BeiDou-2). Avaruuden sotilaallinen käyttö ja siviilikäyttö viittaavat myöhemmin tärkeäksi nousevaan kaksikäyttöteknologiaan. Myös Pohjois-Korean ohjusten kehitys on merkittävä esimerkki avaruuden strategisesta ja globaalista merkityksestä. Satelliittien sieppaus vihamielisillä ohjelmistoilla ja ko. tekijöiden vaikea selvitettävyys ovat selkeitä viittauksia kybersodankäynnin mahdollisuuksiin, joihin herättiin yleisemmin vasta myöhemmin. Ensimmäinen puolitoista vuotta kestänyt kybersota käytiin Yhdysvaltojen ja Venäjän välillä vuosina 1998–1999 (operaatio Moonlight Maze). Ennustus toteutui myös muun muassa Suomessa, kun ensimmäinen suomalainen satelliitti laukaistiin avaruuteen maaliskuussa 2017. Avaruus näkyy myös ohjuspuolustuksen ongelmallisuutena Suomen resursseilla ja muutenkin.

Robottisodat-luvun alaluvussa ”Taistelukentän säästölinja” käsitellään robotteja kalliiden ammattiarmeijoiden korvaajina, toimijoina ihmisille vaarallisissa ympäristöissä ja etenkin tappioita sietävinä järjestelminä. Alaluvussa ”Ykkösjoukkueen suojelu” käsitellään robotteja ulkokehällä ihmisten ollessa suojatummalla sisäkehällä. Lisäksi alaluvussa käsitellään robottien älykkyyden lisääntymiseen liittyviä vaaroja ja ennakoidaan nyt käytävää keskustelua keinoälystrategian tarpeesta. Alaluvussa ”Robotit aavikon yllä” käsitellään lennokkien monia käyttöjä Persianlahden vuoden 1991 sodassa. Alaluvussa ”Komentaja kauko-ohjaimissa” käsitellään kokonaisia robottiyksiköitä ihmiskomentajan johdossa ja robottien vartiointi- ja siviilitehtäviä. Alaluvussa ”Väijyjä” jatketaan valvontarobottien käytön ja tekniikan käsittelyä sekä esitellään Israelin robottikäyttöä alkaen vuoden 1982 sodasta. Alaluvussa ”Robottiterrori” käsitellään älykkäämpiä, autonomisia robotteja ja robottien manipulointia muun muassa terroristien välineenä. Alaluvussa ”Robotinvastustajat” käsitellään robotteja sotilaiden ja siviilien kilpailijoina ja mahdollisesti valtaa muuttavina elementteinä taistelukentällä ja tehtaissa sekä taistelukentän kompleksisuutta roboteille ja robottien käytön riskejä.

Robottiennusteet ovat toteutuneet erityisesti etäohjattavissa tiedustelulennokeissa sekä myöhemmin ilma-asenteisissa ase- ja vaikuttamislaveteissa, osin merivoimissa, mutta eivät vielä juurikaan maavoimien roboteissa. Tämä vaiheittaisuus viitaa siihen, että ilmatila on yksinkertaisempi sotilaallinen ulottuvuus kuin meri tai maa-alue ja siinä mielessä helpoimmin robotisoitavissa. Maan pinnalla viidakko ja etenkin kaupunkiympäristö ovat kompleksisia toimintaympäristöjä. Tämä liittyy sodankäynnin pitkäaikaisen kehityksen yhteen ydinaiheeseen, *kompleksisuuden kasvamiseen sodankäynnissä*. Siviilipuolella robotit ovat korvanneet ihmisiä paljon laajemmin. Tämä liittyy QWM:iin sillä tavalla, että talous ja teknologia ennakoivat sen mukaan muita, muun muassa organisatorisia muutoksia.

”**Leonardon unelmat**” -luvun alaluvussa ”Hollywood-haalari” käsitellään sotilaan muuttumista järjestelmäksi, jossa kehon ulkopuolinen keinotekoinen tukiranka on ”Hollywood-haalari”. Tavoitteena on muun muassa selvitä vähemmillä sotilailla. Alaluvussa ”Sotilasmuurahaiset” käsitellään mikro- ja nanoteknologiaa ja -koneita. Alaluvussa ”Superrutto” käsitellään DNA-manipuloinnin mahdollistamaa biologista sodankäyntiä, esimerkiksi rotukohtaisiksi ohjelmoituja tauteja. Alaluvussa käsitellään myös Neuvostoliiton biologista sodankäyntiä.

Nämä ennusteet eivät ole näkyneet nykyaikaisessa sodassa, ainakaan julkisissa lähteissä eivätkä laajemmin. Sinänsä niissä on suuri potentiaali sodankäynnin muutokseen.

Veretön sota? -luvun alaluvussa ”Huippusalaiset laboratoriot” käsitellään ei-tappavuuden ongelmia. Myös ei-tappavuuden eettisiä vaatimuksia pohditaan, samoin pohditaan esimerkiksi panssarivaunun lamauttamista vaikuttamalla vain pieneen osajärjestelmään. Eversti Wardenia, strategia vuoden 1991 Persianlahden sodan taustalla, lainataan todeten, että mahdollisesti elämme sodankäynnin muutoksessa isoa muutosvaihetta, jossa sota muuttuu todella merkittävästi, esimerkkisi ei-tappavuuden ja informaatiosodankäynnin suuntaan. Alaluvussa ”Näkymätön muuri” käsitellään esimerkiksi infraääniä massojen hallintaan. Alaluvussa ”Huumekuninkaita heikottaa” käsitellään sokaisuun käytettäviä lasereita, lamauttavia aineita, metallin haurastamista ja aiheeseen liittyviä vaikeuksia. Alaluvussa ”Ei-tappavuuden politiikka” käsitellään edellä mainittujen aseiden joutumista terroristien käsiin, ei-tappavien aseiden luokittelua ja salaamistarvetta, keskustelun tarvetta aiheesta sekä ei-tappavuuden strategian tarvetta. Alaluvussa ”Kun diplomatia pettää...” aiheita ovat ei-tappavuus täysin uutena mullistavana sodankäynnin ilmiönä sodan ja rauhan välissä, tieto keskeisenä uutena integroivana välineenä ja *uusien tietostrategioiden tarve*.

Nämä ennusteet eivät ole näkyneet nykyaikaisessa sodassa, ainakaan julkisissa lähteissä eivätkä laajemmin. Sinänsä myös niissä on todennäköisesti suuri potentiaali sodankäynnin muutokseen. *Jos informaation näkee väkivaltaan rinnastettavana vaikuttamisen välineenä*, *asetelma muuttuu*. Kaikki se, mitä on saatu aikaiseksi pelkällä informaatiolla ja siihen liittyvien seikkojen avulla on ei-tappavaa. Eli siis keskeisesti mm. kybersodankäynti, mm. sosiaalisen median vihamielinen manipulointi. Tällöin ei-tappavuus onkin keskeinen muutos, joskaan ei suoraan Tofflereiden ei-tappavuus-luokassa. Tämä taas selittäisi osaltaan sen, miksi sodan tappavuus ei ole kehittynyt Tofflereiden ja vertailumallin QWM:n edellyttämällä tavalla: informaatio on verettömämpi, mutta aikakaudellamme merkittävämpi vaikuttamisen väline kuin asevoimat ja perinteinen väkivalta. Onko tämä osa uuden tason uusia emergenttejä piirteitä? Pieneen osajärjestelmään vaikuttaminen on ennustus vaikutuskeskeisestä sodankäynnistä (Effect-Based Operations, EBO) ja kompleksisuuden sekä kokonaisuuden hallinnasta.

”Pienet” ennustukset ja arvio niiden toteumasta

”Pienet” ennustukset ovat sellaisia Tofflereiden tai muiden esittämiä, ennustuksen sisältäviä tekstikappaleita heidän teoksessaan, joita Tofflerit pitävät oikeansuuntaisina, esittämisen arvoisina. Alla esitetään ja arvioidaan yksitoista sellaista avainsana- tai käsiteluokkaa, joihin on eniten luokituksia, kun yksittäiset ennustekappaleet on ryhmitelty niiden sisällön perusteella avainsanaluokkiin, yhteen tai useampaan. Luokiteltuja ennustekappaleita löydettiin teoksesta 148 ja niiden avainsanaluokkia 237.

Sodan kehittyminen ja uuden tyyppiset sodat -luokka sai eniten luokituksia, 16 kappaletta. Tämä vaikuttaa melko loogiselta teoksen aihe huomioiden. Kyse on muun muassa aikakautemme yleisestä trendistä, *kompleksisuuden kasvamisesta*, joka sodankäyntiin sovellettuna merkitsee muun muassa sodankäynnin tyyppien kasvua, siis uudenlaisia sotia, myös uusia aselajeja, jopa puolustushaaroja. Edelleen esimerkkejä ovat muun muassa Venäjän hybridisodankäynti ja kybersodankäynti yleensä, jälkimmäisestä mm. vuoden 2016 Yhdysvaltojen presidentinvaaleihin vaikuttaminen. Tämän ennustuksen

arvioidaan myös toteutuneen, tosin monessa kohtaa Tofflereiden teoksessa on yleistyksiä ja ylisanoja. Suomen puolustuksen kannalta arvioidaan, että sama trendi vaikuttaa Suomessa, muun muassa pohdintana informaatio- tai kyberpuolustushaaran tarpeesta.

Kaksikäyttötekniikka-luokka sai toiseksi eniten luokituksia, 12 kappaletta. Tämä ennustus näyttää toteutuneen hyvin. Toteutuneita esimerkkejä ovat muun muassa tienvarsipommit, joiden sytyttimenä ja laukaisukeinona on käytetty kännyköitä, siviililentokoneet aseina Yhdysvalloissa 11. syyskuuta 2001, rekat aseina Berliinissä 11. joulukuuta 2016 sekä Israelissa 8. tammikuuta 2017, ehkä myös teräaseena Turussa 18. elokuuta 2017. Ennusteen toteutumista korostaa myös se, että tieto on yhä merkittävämpi vaikutuskeino sodassa. Tietotekniikka on myös tällä hetkellä pitkälti siviilitekniikkaa, tosin kuin vielä 1950- ja 1960-luvuilla. Suomen puolustuksen kannalta arvioidaan, että tässä on erityisiä mahdollisuuksia Suomelle kehittyneenä informaatioyhteiskuntana ja sen palveluiden tuottajana.

Media-luokka sai kolmanneksi eniten luokituksia. Myös tämä ennustus näyttää toteutuneen hyvin. Teoksessa kuvataan melko tarkkaan, miten mobiilia älypuhelinta tullaan myöhemmin käyttämään YouTube- ja Instagram-sovellutuksissa. Vuonna 1993 GSM-puhelin oli hyvin nuori eikä siinä ollut multimediaa. Teoksessa kuvataan myös, miten toimittajista tulee informaatiosodankäynnin kohteita ja miten heidän työnsä monilla maapallon alueilla on potentiaalisesti hengenvaarallinen ammatti. Samaa informaatiosodankäynnin korostumista on myös monien valtioiden kasvanut kontrolli mediaan ja erityisesti internettiin; Kiina, Venäjä, Turkki, Unkari, monet arabimaat. Strateginen kommunikaatio on myös osa tätä kehitystä, myös Suomessa, samoin valeuutiset. Näkyvämmin internetistä, Facebookista ja muun muassa Twitteristä on tullut merkittävä globaalin informaation taistelukenttä tosin vasta 2010-luvun puolivälissä. Snowden-NSA- ja CIA-Wikileaks-skandaalit viittaavat siihen, että median ja kyberin todellista vaikutusta sodankäynnissä ja globaalissa politiikassa on ollut jo aiemmin, mutta hyvin salaisena osaamisena.

Kompleksisuuden kasvaminen -luokka sai neljänneksi eniten luokituksia. Myös tämän ennustuksen arvioidaan toteutuneen hyvin. Tietokone on keskeisesti kompleksisuuden hallinnan väline ja muun muassa siinä mielessä keskeinen tekijä mahdollistamassa globaalia toimintaa yleensä, ei vain sodankäyntiin liittyen. QWM:ssa keskeisenä kompleksisuuden lisääntymisen lähteenä ovat uusi globaali taso ja sen uudet asiat. Kompleksisuus onkin yhdessä kaaoksen, tietokoneiden, (globaalin) tiedon ja hypoteesina ehkä myös intuition kanssa aikamme ja sen sodankäynnin ydintä. Suomen puolustuksen kannalta arvioidaan, että tämä koskee myös Suomea. Tämä saattaa olla ongelma Suomen pragmaattisessa kulttuurissa, joka korostaa käytännöllisyyttä, ei abstraktia ajattelua ja laajaa analyysiä. Tämä koskee erityisesti ylintä tasoa, siis strategiaa ja QWM:ssa globaalia tasoa.

Avaruus-luokka sai viidenneksi eniten luokituksia. Myös tämä ennustus näyttää toteutuneen hyvin. Iridium ja vastaavat satelliittiviestijärjestelmät eivät sen sijaan ole nyt niin merkittäviä kuin Tofflerit esittävät. Selitys lienee se, että ne ovat korvautuneet *globaaleilla* GSM-järjestelmillä vuodesta 1991 alkaen (1G, 2G) ja sen seuraajilla (3G, 4G) ja tulossa olevilla (5G). Suomen puolustuksen kannalta arvioidaan, että avaruus on samalla tavalla tärkeä kuin tässä esitetään. Ks. avaruus myös yllä ”isoissa” ennustuksissa.

Robotit ja autonomia -luokka sai kahdeksan luokitusta. Tämä ennustus näyttää toteutuneen, tosin ei niin merkittävänä kuin Tofflerit esittävät. Merkittävin alan toteutunut sovellutus ovat lennokit, myös Suomessa, aluksi tiedustelussa ja myöhemmin myös aselavetteina. Suomen puolustuksen kannalta arvioidaan, että ennustus koskee täysmääräisesti myös Suomea. Ks. robotit myös yllä ”isoissa” ennustuksissa.

Rauha lännessä (uhattuna) -luokka sai seitsemän luokitusta. Tämä ennustus näyttää myös toteutuneen, tosin ei niin pahana eikä niin nopeana muutoksena kuin Tofflerit esittävät. Aivan viime vuosina kehitys on kuitenkin ollut Tofflereiden ennustusten mukaista terrorismissa, internetissä sekä hybridi- ja kybersodankäynnissä. Mielenkiintoisen selitysmallin antaa tähän QWM:sta johdettu ennustus tai sovellutus: Kirjapainotaito mahdollisti entistä avoimempana ja halpana tietolähteenä tavalliselle ihmiselle Raamatun lukemisen ja oman tulkinnan siitä. Osin tästä syystä seurasi Euroopassa runsaan sadan vuoden veristen uskonsotien aikakausi 1500- ja 1600-luvuilla. Vastaavuus internettiin on ilmeinen, ja se näkyy kaaoksena ja liikehdintänä, jopa rauhan uhkaajana (lännen) yhteiskunnissa. Turun tapahtumat 18. elokuuta 2017 saattoivat osoittaa, että tämä ennustus koskee myös Suomea. Sen taas voidaan katsoa johtuvan siitä, että globaali taso on QWM:n mukaan aikamme megatrendi, ja se vaikuttaa yleisti ottaen kaikkialla, myös Suomessa.

Tiedustelu-luokka sai seitsemän luokitusta. Tämäkin ennustus näyttää toteutuneen. Osin asia johtuu siitä, tiedustelu on keskeisesti osa globaalia informaatiota, esimerkiksi satelliitteja ja kybersotaa (NSA-Snowden) sekä esimerkiksi julkisiin lähteisiin perustuvaa tiedustelua erityisesti internetissä ja sosiaalisessa mediassa. Suomen puolustuksen kannalta arvioidaan, että asia on myös ja täysimääräisesi näin. Yksi merkittävämpiä asioita on tähän liittyen Suomen puolustusvoimien apulaistiedustelupäällikön Martti J. Karin lausunto siitä, että Suomen kybertiedustelu *on 15 vuotta jäljessä muista*.

Globaali- ja geotalous -luokka sai kuusi luokitusta. Myös tämä ennustus näyttää toteutuneen. Kaksi kolmasosaa maailman konttiliikenteestä on *tehtaiden välisiä puolivalmistekuljetuksia*, ei valmiita tuotteita tehtaista kuluttajille. Valtioiden välinen kauppa on lisäksi kasvanut vuoden 1800 alle 10 prosentista tämän hetken yli 50 prosenttiin. Nämä kertovat paljon globaalista työnjaosta ja kaupasta. QWM:ssa talous ja teknologia edeltävät muun muassa organisatorisia muutoksia. Suomen puolustuksen kannalta arvioidaan, että ennustus koskee täysmääräisesti myös Suomea.

Sodan koon ja tappavuuden kasvu -luokka sai kuusi luokitusta. Maailmansodat, ydinsota, biologinen sodankäynti ja mahdollisesti laaja kybersodankäynti olisivat tämän asian toteumia.

Tämä ennustus ei näytä toteutuneen tappavuuden kasvuna. Sodankäynnin koko globaalina sodankäyntinä, josta esimerkkeinä ovat kybersota, terrorismi, hybridisodankäynti, on toteutunut. Sama ennustus esiintyy QWM:ssa. Sodankäynnin tappavuuden kasvusta on esitetty, että se on (toistaiseksi?) poikkeuksellisesti vähentynyt vuosina 1950–2000. Suomen puolustuksen kannalta arvioidaan, että ennustus pitää paikkansa.

Tieto ja tietämys -luokka sai kuusi luokitusta. Tämä ennustus näyttää toteutuneen. Osin asia johtuu siitä, että luokka on Tofflereillakin osa heidän keskeisintä ennustustaan, tiedon valtakautta. Jos edes osa tiedustelun, median ja kaksikäyttötekniikan viitauksista lisätään tähän tiedon sovellutuksina, tieto nousee suurimmaksi luokaksi. Tämä on vahva viittaus informaatiosodankäyntiin ja tämä ennustus esiintyy myös QWM:ssa. Suomen puolustuksen kannalta tämä vaikuttaa täysimääräisesti ja se on edelleen yksi keskeinen aihe, joka vaatii Suomessa perusteellista uudelleen arviointia ja strategisia kannanottoja. Asian vaikeutta pohditaan johtopäätöksissä osana ennustamisen vaikeutta.

Yhteenvetona näistä ”pienien” ennustusten luokituksista todetaan, että yleisimmät ennusteet näyttävät onnistuneen hyvin, myös Suomessa, lukuun ottamatta sodan tappavuuden kasvua.

VM

Analysaattori

Keinoälyahdistusta

Tai voihan kyseessä olla allergiakohtauskin. Taudin aiheuttajaksi on nyt kuitenkin paljastunut niin ovista kuin ikkunoistakin tulviva keinoälybuumi. Mikähän siinäkin oikein on, kun jokin vastaava tauti toistuu lähes säännöllisesti, lähes amerikkalaismallisen kvartaalitalouden tavoin. Aina kun jotain uutta keksitään tai julkistetaan alkaa siis hemmetillinen humppa ja hulina. Ja usein ei edes keksitä mitään uutta. Ihan vaan esimerkkinä mainittakoon jo pitkään ilmassa ollut pilvi. Siis tietokonepilvi. Jota muuten aikaisemmin kutsuttiin konesaliksi. Sillä kysehän on pohjimmiltaan jonkun toisen tietokoneesta, johon olet verkon kautta yhteydessä. Tätä markkinahuumaa on jo pitkään kutsuttu hypetykseksi, joka sekin on tavallaan osa samaa ilmiötä. Aikoinaan sitä kutsuttiin liioitteluksi tai hehkutukseksi.

Keinoälyn kohdalla tämä meno johtuu osaltaan myös siitä, että näistä asioista on kohkattu jo niin kauan ennen kuin oli edes olemassa mitään, mistä pitää meteliä. Roboteista maalailtiin ennustuksia jo kymmeniä vuosia sitten ja pelko tietokoneiden kapinasta on synnytetty jo ennen tietokoneistumista, esi-digitaalisella aikakaudella. Se miksi tämä koneälyn ilosanoman hypetys aiheuttaa kirjoittajassa edellä mainittuja oireita johtuu siitä, että kyseessä on aidosti hyödyllinen kehityksen suunta. Keinoälyratkaisut muuttavat maailmaa juuri nyt, eikä kyse ole mistään markkinoiden luomasta illuusiosta. Keinoälynkin kohdalla on kuitenkin kyse osaltaan vanhasta keksinnöstä, sillä suurinta osaa jo pidempään käytössä olleista toteutuksista kutsutaan tuttavallisemmin automaatioksi.

Tavalliselle tallaajalle odotusarvot keinoälypalveluissa kohdistuvat erityisesti lääketieteeseen, jossa keinoälyltä odotetaan apuja mm. diagnoosien tekoon. Suomessa kehitetty menetelmä antaakin mahdollisuuden niin sanottuun personoituun lääketieteeseen. Systeemin avulla saadaan parempia hoitoennusteita juuri kyseessä olevalle yksilölle. Kyseessä on Itä-Suomen yliopiston, Kuopion yliopistollisen sairaalan ja Aalto-yliopiston tutkijoiden kehittämä uusi menetelmä, jollaista ei ole aikaisemmin lääketieteessä käytetty. Tässä kohdin Analysaattori kohottaa vähän harmaantuneita kulmakarvojaan ja kysyy, että onko meitä siis tähän asti diagnosoitu ikään kuin massana eikä yksilöinä? No, hiukan kun pudottaa tätä akateemista lähentymiskulmaa sinne reaalielämään ja terveyskeskuksen ruuhkaiseen päivystykseen niin saattaahan tässä pikaisesti tehdyssä johtopäätöksessä olla jotain perääkin. Siellä se yksilö todellakin tahtoo jäädä vähän jalkoihin.

Lääkealan turvallisuus- ja kehittämiskeskuksen Fimean ylilääkäri Päivi Ruokoniemi on kirjoittanut HS:n Vieraskynä-palstalla olevansa huolissaan erityisesti siitä, että keinoälypohjaiset ratkaisut saattavat suositella potilaalle turhia hoitoja. Tässä on kuitenkin kyseessä täysin turha huoli, sillä tulevat SOTE-ratkaisut pystyvät kyllä vastaamaan tähän haasteeseen.

Jokin aika sitten samalla palstalla kirjoitti tekoälystä lähes huojentavasti Aalto-Yliopiston professori Jussi Rintanen. Hän otsikoi juttunsa hienosti ”*Tekoäly on todellinen idiootti*”. Tarinan perimmäinen tarkoitus oli hälventää juuri tuota pelkoa tietokoneiden maailmanvalloituksesta. Rintasen mielestä kannattaisi olla enemmän huolissaan ihmisen toiminnasta, sillä tekoälyteknologian kehityksen myötä myös rikollisuus ja terrorismi saavat helpommin työkaluja käyttöönsä. Mielipiteiden muokkaus voisi myös olla eräs käyttökohde. Verkkosivustot ja hakukoneet suosittelevat mielellään erilaisia asioita käyttäjille ja mainostuksen kohdistaminen on täysin arkipäivää. Tekemällä pari hakua jonkin tietyn kaupungin hotelleista tai lennoista samaan kohteeseen havaitset helposti olevasi kauppatavaraa. ”Joku” on myynyt tietosi eteenpäin ja sen seurauksena kaikkialla sinulle mainostetaan samaa kohdetta, hotelleja jne. Tosin näissä kohdistetuissa mainoksissa on se keinoälyttömyys, että se jatkuu pitkään vielä senkin jälkeen, kun olet jo kotiutunut tuosta reissusta.

Noista aikaisemmin mainituista pilvipalveluista tulikin mieleeni ilmaston lämpeneminen ja eri tavat hyödyntää palvelimien tuottamaa hukkalämpöä. Mielenkiintoisin innovaatio tästä tulee Tampereelta, sillä ICT Elmo on ryhtynyt myymään palvelinpattereita. Palvelinpatteri on ikään kuin hajautettu pilvipalvelu, jossa palvelimet on sijoitettu lämpöpatterin sisään tuottamaan lämpöä ja patteri puolestaan on sijoitettu sinne missä lämpöä tarvitaan. Palvelua tarjotaan taloyhtiöille, yrityksille ja kiinteistöille, mutta ei ainakaan aluksi kotitalouksille. *”Suomi on erinomainen maa tällaiselle palvelulle, koska täällä tarvitaan lämmitystä kahdeksan kuukautta vuodessa*”, sanoo Elmon palvelujohtaja Kari Koivisto. Muuten hienossa tarinassa on Analysaattorin mielestä vähän aukkoja. Kuten esimerkiksi se, että hajautettu tietojenkäsittely pilvessä missä hyvänsä ei taida rajoittua kahdeksaan kuukauteen vuodesta, mutta se palvelinpatteri pukkaa siis surutta lämpöä läpi vuoden. Puhumattakaan keskikokoisesta tietoturvahaasteesta, jonka esim. kerrostalon kellariin sijoitettu palvelin muodostaa. ICT Elmolle toivotan voimia näiden haasteiden parissa painimiseen, sillä kyse on kuitenkin päänavauksesta oikeaan suuntaan. Tämä ICT Elmo muuten on nimestään huolimatta aika perinteinen tietoliikenneyhtiö, jonka leivissä Analysaattorikin on nuoruudessaan työskennellyt. Siihen aikaan sitä vielä kutsuttiin Tampereen Puhelinosuuskunnaksi eikä palvelimia siihen aikaan ollut vielä keksittykään.

Turvallisuuden parantaminen on luonnollisesti eräs merkittävä keinoälyn kohde. Tästä on hyvä esimerkki Kiina, jossa valtion turvallisuuden parantaminen tosin ei välttämättä tarkoita aina samaa yksilön näkökulmasta katsottuna. Kii-

nassa on käytössä jo 170 miljoonaa valvontakameraa ja lähivuosina asennetaan 400 miljoonaa lisää. Sekään ei vielä riitä, sillä Kiinan Poliisi on jo ottanut käyttöön aurinkolasit, joihin on integroitu kasvojentunnistus. Etsintäkuulutettu löytyy väkijoukosta ihan vaan konstaapelin vilkaisulla, sillä heillä on mukanaan erillinen kannettava ”yksikkö” johon on tallennettu kuvat etsityistä henkilöistä. Vertaamalla näitä kuvia näkökentässä oleviin kasvoihin saadaan tunnistus tehtyä melko reaaliaikaisesti. Tarina ei kerro onko käyttöolosuhteiden pakko olla aurinkoiset, jolloin lasien käyttö olisi hieman luontevampaa. Pimeässä ja/tai sateella poliisit eivät varmaankaan vaikuta kansalaisten silmissä kovinkaan älykkäiltä. Eivätkä varsinkaan näytä siltä. Se kannettava yksikkö ei ilmeisesti kuitenkaan ole verkkoyhteydessä isompiin tietokantoihin, joten osa poliisin työpäivästä menee jonkinlaiseen replikointiin kiinteän verkkoyhteyden äärellä, joka tekee tästä virityksestä vähän keskentekoisen tuntuisen. Ottaen huomioon kiinalaisten lukumäärän ja melko keveän kansallisen prosessin, jolla siellä voi päätyä etsintäkuulutetuksi, ovat järjestelmän tulokset vielä aika vaatimattomia. Toistaiseksi on saatu kiinni seitsemän rikollista ja 26 kappaletta väärillä papereilla liikkuvia ihmisiä. Tarina ei kerro sitäkään, kuinka nämä väärennettyjen papereiden käyttäjät osuivat aurinkolasien linsseihin. Voihan niissä laseissa tietenkin olla käytössä jotain optioita tarkempaankin henkilöanalyysiin.

Tekoälyn käyttöön liittyvistä haasteista puhuttaessa nousevat usein esille eettiset arvot ja moraali. Siirrymmekin nyt löysällä aasinsillalla keinoälystä autonomisten autojen kautta juuri moraaliin. Eräs maailman arvostetuimmista yliopistoista, Massachusettsin teknillinen korkeakoulu (MIT) on julkaissut Moraalikoneen. Moraalikone on verkkokysely, jossa kuka tahansa voi tehdä omat eettiset johtopäätöksensä siitä kuka voidaan uhrata ja kenet haluat säästää, kun itsestään ajavan auton jarrut pettävät. Kyselyn voit tehdä osoitteessa *http://moralmachine.mit.edu*. Noin 40 miljoonaa muutakin uteliasta on sen jo tehnyt. Mukaan lukien Analysaattori, joka tässä hämmästelee kahtakin erillistä asiaa tuossa kokeessa. Päällimmäinen kysymys kuuluu, että mitä näillä tuloksilla tehdään? Syötetäänkö ne sellaisenaan suoraan Googlen tai Teslan ohjelmistoihin?

Ja jos syötetäänkin, niin mikä on se menetelmä, jolla ne autonomiset autot, joista ne jarrut pettävät, pystyvät millisekunnissa tekemään diagnoosin siitä, että suojatiellä on juurikin kävelemässä asunnoton ihminen, rikollinen, urheilija, lapsi tai terveydenhuollon ammattilainen. Tämähän johtaa väkisinkin siihen salaliittoteoriaan, että meidät jotenkin sirutetaan ja sitä tietoa pidetään ”on-line” yllä koko yksilön elinkaaren ajan. Tätä tietoa sitten välitetään suoraan näille autonomisille autoille.

Yhteenveto kaikista Moraalikoneella tehdyistä testeistä on nähtävissä, kun olet suorittanut testin. Melkein 7 miljoonaa ihmistä testin suorittaneista säästäisi eläimen ja uhraisi ihmisen, joten ihan ilman vastarintaa en itse suostu tähän sirukäsittelyyn. Tai alan sitten jotenkin väistelemään suojateitä. Jotenkin tuntuisi kuitenkin helpommalta, jos keskityttäisiin niiden autojen jarrujen kehittelyyn kuin tähän keinotekoiseen evoluution ohjailuun. VM

Viestimiespäivät 27.9.-28.9.1968 Jyväskylässä

Ilmavoimien Viestikoulun suosiollisella avustuksella saatiin Viestimiespäivät järjestettyä tänä vuonna Luonetjärvelle. Viestiupseeriryhdistyksen jäsenistä 8,5 % ilmoitti kutsun saatuaan olevansa halukas lähtemään Keski-Suomeen tapaamaan viestiveljiään ja tutustumaan Ilmavoimien Viestikoulun uusiin koulutustiloihin ja -välineisiin.

Puolustusvoimain juhlavuoden kunniaksi sai yhdistys käyttöönsä ilmavoimien kuljetuskoneen, jolla osa päiville osallistuvista upseereista pääsi lentäen Helsingistä Jyväskylään. Luonetjärven lentokentällä toivottivat evl J Leinonen ja evl Falin saapuneet Viestimies- päivien osallistujat tervetulleiksi Tikkakosken ja Luonetjärven varuskuntiin.

Sään haltijan suotua Viestimies- päivien ajaksi kauniit ilmat, voitiinkin Luonetjärvellä viettää Farnbourghin ilmailunäytös pienoiskoossa. Alkajaisiksi esiteltiin ilmavoimien lentokoneita ja niiden suoritusarvoja sekä tutustuttiin lennonjohtoon. Ylil Janhunen suoritti viestimiehiä kiehtovan taitolentoesityksen Fouga Magister- suihkulentokoneella. Tämän jälkeen oli viestiupseeriyhdistyksen jäsenillä tilaisuus tutustua 18- antenniseen suuntimoon. Tämä suuntimo suorittaa lentokoneiden paikantamista ja toimii tutkahavaintojen ohella eräänä lentämisen turvallisuutta lisäävänä tekijänä.

Ensimmäisenä päivänä tutustuttiin myös Kulkulaitosministeriön ilmailuosaston alaiseen Lennonjohtokouluun. Siellä lennonjohtaja K Virva selvitteli koulun vaiheita ja tarkoitusperiä. Mielenkiintoinen opetusväline Lennonjohtokoulussa oli tutkasimulaattori, jolla voitiin saada tutkan kuvaputkelle erilaisia todellisia lentotilanteita vastaavia

kuvia mm. lentokoneen laskeutumisvaiheet lentokentälle. Tällöin oppilaat pyrkivät saamaan “lentokoneet” laskeutumaan onnellisesti kiitoradalle seuraamalla pelkästään tutkan kuvaputkella näkyvää maalipistettä sekä laskupolkua. Lennonjohtajan ja tutkan avulla voidaan lentokone tuoda puhumalla vaikka “hernerokkasumussa” onnellisesti kiitoradalle. Oppilaat joutuvat käyttämään komennoissaan kansainvälistä ilmailukieltä, englantia.

Ilta sujui saunomisen ja iltapalan merkeissä. Iltapalalla olivat läsnä myös Sisä-Suomen sotilaslääänin komentaja kenraalimajuri A. Brandt sekä Hämeen Lennoston ja Ilmavoimien Viestikoulun edustajat. Puheessaan kenrmaj Brandt korosti miten tärkeitä ovat viestimiehille henkilökohtainen tapaaminen ja tutustuminen eri aselajien viestipulmiin. Lisäksi hän ilmaisi tyytyväisyytensä hyvästä viestimieshengestä, minkä osoituksena oli Viestimies- päivien runsas osallistujamäärä.

Seuraavana päivänä oli varsinainen tutustuminen Ilmavoimien Viestikouluun. Majuri J Paavilainen esitti aluksi havainnollisesti Ilmavoimien Viestikoulun tehtäviä, eri kursseja ja koulutuksen läpivientiä. Koululla suoritettiin tutustumiskierros eri luokissa ja koulupajassa. Elektroniikkapuolen opetuksen tehostamiseksi oli Ilmavoimien Viestikoululle hankittu “opetustrainer”, jonka avulla oppilaille voidaan havainnollisesti esittää radio- ja tutkalaitteiden rakennetta sekä opettaa heitä suorittamaan piirien mittauksia.

Iltapäivä käytettiin tutustumalla Jyväskylässä Keski-Suomen Puhelin Osakeyhtiöön ja sen toimitustiloihin. Tutustumiskierroksen alussa toimitusjohtaja Erkki Ikonen esitteli yhtiön toimintaa, jolloin viestimiehet saivat todeta, että yhtiön verkostoon kytkettyjen puhelinkoneiden määrä oli yli 16 000 kappaletta. Toimitusjohtaja esitteli lisäksi keskuksien rakennusohjelmia sekä yhtiön tulevaisuuden suunnitelmia. Viestimies- päivät päättyivät kiertokäyntiin Keski-Suomen Puhelin OY:ssä, jolloin saatiin nähdä vielä yhtiön laite-, konttori-, ja varastohuoneet.

Artikkelin toimittaja: Veli-Matti Pesola

VM

Henkilöasiat:

Siirrot ja tehtävään määräämiset

- eversti **Jarmo Vähätiitto** (KAR-PR) apulaisosastopäälliköksi Pääesikunnan johtamisjärjestelmäosastolle 1.1.2019 lukien

- insinöörikomentaja **Petteri Kuosmanen** (PE) ainelaitoksen johtajaksi Maanpuolustuskorkeakoulun Tekniikan laitokselle 1.1.2019 lukien.

Seuraavat yritykset ovat tukeneet Viestisäätiön kannatusyhdistystä v. 2018:

Aerial Oy, Airbus Defence and Space Oy,
Blue Lake Communications Oy
Cojot Oy, Conlog Group Oy, Cygate Oy,
Ikaalisen-Parkanon Puhelin Oy
Kaisanet Oy, MPY Palvelut Oyj, Milcon Oy, Relacom Finland Oy
Telva Oy,Vakka-Suomen Puhelin Oy, Viria Oyj,
Ålands Telefonandelslag

Viestisäätiön kannatusyhdistys esittää parhaimmat kiitokset vuoden 2018 keräykseen osallistuneille yrityksille ja yhteisöille sekä lukuisille yksityisille henkilöille.

Toivotamme Rauhallista Joulua ja Onnellista Vuotta 2019!

Reima Blomqvist
Puheenjohtaja

Kirsi Salo
Sihteeri


VALITSE VAPAUS
Ei sitoutumispakkoa
Ei määräaikaisuutta
Ei datakattoa
VALITSE ELISA SAUNALAHTI
elisa
SAUNALAHTI

Yhteydet maastoon Nestorin tuotteilla

Nestor Cablesin valikoimasta löytyvät kenttäkäyttöön soveltuvat valokaapelit väliaikaisten verkkojen rakentamiseen. Kaapeleiden lisäksi valikoimassa ovat myös asennuslaitteistot sekä huoltotarvikkeet. Kaapelit ovat saatavilla erilaisilla liitinvaihtoehdoilla vaativaan käyttöön. Kenttäkaapelituotteita voidaan hyödyntää myös erilaisissa siviilitapahtumissa.

Nestorin valikoimasta löytyvät:

- Telineet keloille
- Kytkentäkotelot
- Kuituliittimet
- Kytkentäkaapelit
- Kuituliittimien puhdistussarja
- Etumittakuidut
- Kaapelinlevityslaite

nestor cables

www.nestorcables.fi • info@nestorcables.fi • Mittarikuja 5, 90620 Oulu • 020 791 2770