Viestimies

Viestiupseeriyhdistyksen julkaisu 73. vsk Numero 2 Kesä 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

Kansikuva: Kuvat SA-kuva.

Tässä numerossa

Seuraavan numeron aineistopäivä on 6.8.2018. Lehti ilmestyy viikolla 38.

”...kylmästä lämpimään...”

Alkuvuosi on ollut työntäyteinen varmasti kaikilla. Pitkä ja varsin vilakka talvi sekä kevään ankara harjoitusputki ovat takana ja on tullut aika vähitellen rauhoittua ja vetää henkeä. Kuluvaa vuotta ja kevättä ovat leimanneet Puolustusvoimat 100-vuotta tapahtumat sekä monet kansalliset ja kansainväliset tapahtumat ja harjoitukset. Yhteiset voimain ponnistukset ovat kehittäneet valmiutta, teknistä kypsyyttä, osaamista ja yhteistyötä. Työtä on vielä edessä, mutta päämäärä kuitenkin siintää kuin aavameri ja auringon kehrä heijastuksena laineilta.

Kansainvälisyys ja verkottuneisuus lisääntyvät vuosi vuodelta. Tästä esimerkkinä voidaan todeta muun muassa kevättalvella järjestetty FMN-seminaari, useat kyber-harjoitukset ja Steadfast Cobalt-harjoitus, jossa kansainvälistä yhteensopivuutta kehitetään. Verkottuneisuus taas nousi puheisiin Facebookin tietovuotojen seurauksena. Käyttäjätietoja on kaupiteltu, ehkä jopa kyseenalaisesti käyttäjien tietämättä. Toisaalta voidaan pohtia kyseisen palvelun käyttäjien halua kuitenkin hyödyntää sitä riippumatta sen mahdollisista riskeistä tietosuojan ja yksityisyyden kannalta ajatellen. EU:n tietosuojadirektiivi astui voimaan 25.5.2018, jolloin sen soveltaminen alkoi kaikissa jäsenmaissa. Tietosuoja-asetus vaikuttaa mm. yrityksien henkilötietorekisterien pitoon ja sen tavoitteena on vahvistaa yksilön suojaa sekä huomioida globaalit toimijat ja toiminta. Tällä on tuskin suoraa vaikutusta Facebookin kaltaisiin yrityksiin, joiden kotipaikka on Yhdysvallat.

Suomessa keskustelua on herättänyt myös toisen samaan aihepiiriin kuuluvan lain valmistelu. Tiedustelulain valmistelu on aiheuttanut intohimoja suuntaan ja toiseen. Yhtäältä pelätään yksityisyyden suojan katoavan kun ”Isoveli” valvoo ja seuraa kaikkea verkkoliikennettä, ja toisaalta pohditaan verkossa tapahtuvan rikollisuuden ja tiedustelun estämisen sekä havaitsemisen mahdollisuuksia. Lain valmistelu jatkuu ja toivottavasti voimaantullessaan toisi kauan kaivattua selkeyttä ja pelisäännöt siihen, mitä voi tehdä ja miten – laillisesti.

Tässä numerossa päästään tutustumaan katsauksiin FMN-seminaarista, Viestiaselajin vuosipäivän tapahtumista Mikkelissä ja tiedustelulain valmisteluun liittyvistä artikkeleista. Lisäksi saamme lukea Viestikoulun johtajan artikkeli rajapintaharjoituksesta, joka keräsi taas tänäkin vuonna runsaslukuisen testaajajoukon pohtimaan yhteyksien muodostamisen problematiikkaa. Harjoituksen pääpaikkana toimi Riihimäki ja toimintaa oli useilla toimipaikoilla ympäri Suomea. Harjoitukseen osallistui merkittävä määrä myös siviiliyrityksien edustajia yhdessä eri viranomaisten kanssa. Yhdessä tekeminen ja järjestelmien sekä toimintatapojen kehittäminen on voimavara, jota tulee jatkossakin hyödyntää. Rajapintaharjoituksen kaltaista testaustoimintaa tulee jatkaa myös jatkossa. Testauksen ja riittävän henkilöstöresurssin kohdentaminen tukemaan kansallisia ja kansainvälisiä harjoituksia on ensiarvoisen tärkeää onnistuneen lopputuloksen mahdollistamiseksi.

Kesälomat ja toivottavasti lämpimät säät odottavat meitä jokaista. Grillit on putsattu, kaasupullot täynnä, lihat lämpenemässä ja marinadit valmiina – ja ei kun grillaamaan! Vedetään henkeä, nautitaan ja valmistaudutaan taas syksyn uusiin koitoksiin vereksin voimin.

Päätoimittaja

Samuli Terämä

Maailma ympärillämme on muuttumassa kovaa vauhtia, paluuta vanhaan ei ole. Laajasti jaetun arvion mukaan todistamme parhaillaan seuraavaa sivilisaation vallankumousta, missä taustavoimina ovat esineiden tai kaiken internet, digitaalinen data, analytiikka, suuren tietomassan piilotettu tieto (big data), robotisaatio, koneoppiminen ja keinoäly. Arvioiden mukaan kone saavuttaa ihmisaivojen suorituskyvyn eli singulariteetin seuraavan kymmenen vuoden kuluessa ja noin vuonna 2050 yhden tietokoneen suorituskyky vastaa koko ihmiskunnan aivokapasiteettia. Totta vai tarua, se näkee joka elää.

Digitalisaatio ei ole ilmiönä uusi, mutta sen vaikutus on laajempi kuin olemme ajatelleet. Edessämme on vallankumouksellista, työtä ja toimintaa mullistavaa uudistumista. Selviytyäkseen Suomen on kuljettava digitaalisten yhteiskuntien eturintamassa. Digitalisaatio tarkoittaa kyberulottuvuuden merkityksen laajentumista osin fyysisen maailman kustannuksella, fyysinen ja digitaalinen maailma kytkeytyvät yhä voimakkaammin toisiinsa. Ennusteiden mukaan seuraavan kymmenen vuoden kuluessa toteutuu koneen ja aivojen suora käyttöliittymä. Tällä hetkellä koneiden puheohjaus on vielä haparoivaa, mutta ei kestä kauaa, kun kotiemme voicebotit pystyvät tekoälyn tukemina tekemään päätöksiä puolestamme. Se, että haluammeko tätä on kokonaan toinen kysymys.

Tätä vallankumousta edesauttavat toisiinsa kytkeytyvät, itsestään oppivat järjestelmät, yksilöiden saumaton vuorovaikutus tehostetun todellisuuden tukemana ja jokaisen yksilön toimiminen tiedon tuottajana ja jakajana. Yhteiskuntamme on jo nyt ratkaisevan riippuvainen verkostoista ja niiden toiminnan mahdollistavasta informaatioinfrastruktuurista eli kyberistä, tämä riippuvuus ei ainakaan vähene tulevaisuudessa.

Mitä tämä sitten tarkoittaa ihmiselämälle ja työnkuvalle? Muuttuuko kaikki tässä murroksessa? Korvaako kone ihmisen? Tuhoaako teknologia sivilisaation? Vapautuuko ihminen työn orjuudesta? Miten minun, lasteni ja lastenlasteni käy?

Tutkimusten mukaan tekniikka ei ole muuttanut ihmisen perusluonnetta tai toimintaa. Keinoälyn kehitys ja robotisaatio tulee varmasti lopettamaan paljon erilaisia työtehtäviä, mutta tilalle syntyy uusia. Tässä suhteessa voimme olla kohtuullisen levollisia. Robotista tulee ainakin lyhyellä aikavälillä enemmän työtoveri kuin kilpailija. Voimme helposti keksiä työnkuvistamme toimintoja, joita konekin voisi tehdä. Kehitystä täytyy seurata, jotta sen mukana voi elää ja toimia. Kehityksen kiistävällä foliohattuajattelulla ei muutokseen vastata.

Teknistyminen tarkoittaa vääjäämättä myös uhkaa, miltä pitää suojautua. Kehittyneet hyökkäykset edellä kuvaamaani ICT-infrastruktuuria kohtaan ovat lisääntyneet merkittävästi. Määrän lisäksi myös uhkan laatu on kehittynyt merkittävästi. Mielikuvituksemme rajoittaa uhkakuvaamme tekniikkaa enemmän. Hyökkäykset kohdistetaan tyypillisesti salassa pidettävään tietoon, aineettomaan pääomaan tai henkilötietoihin. Viimeaikoina tosin taloudellisen edun tavoittelun motiivi on ollut yleisin uhkatyyppi. Kohdeorganisaation heikkouksia hyödynnetään mahdollisimman hyvin, hyökkäyksiä muunnetaan ja kehitetään dynaamisesti. Hyökkäys voi tulla mistä tahansa, verkon lisäksi esimerkiksi radiorajapinnasta, ruudusta, päätelaitteen mikrofonista tai kamerasta, älyrannekkeesta, joko organisaation sisältä tai ulkoa. Vakavimpia hyökkäyksiä on äärimmäisen vaikea havaita. Uhkat ovat niin jokapäiväisiä, että perustellusti voi sanoa, että elämme kyberuhkan uutta normaalia mihin liittyy jatkuva epävarmuus.

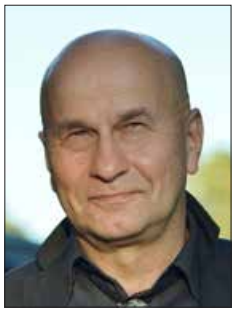
Kuvaamani kehittynyt uhka ei mitenkään mahdollista täydellistä suojaamista. Täydellisen suojaamisen tavoittelemisen sijaan siirrymmekin yhä enemmän riskien hallintaan, vaikutuksen rajaamiseen, toipumiskykyyn ja resilienssiin. Kyberuhkilta suojautumisen merkitys kasvaa kuvaamassani muutoksessa aivan toiseen ulottuvuuteen kuin mihin tähän mennessä on totuttu. Sodankäynnin termein kyberistä tulee oikeasti taistelukentän viides ulottuvuus, mikä tulee huomioida kaikissa neljässä muussa ulottuvuudessa eli perinteisissä maalla, merellä, ilmassa ja avaruudessa toimivissa järjestelmissä.

Puolustus ei voi rajautua verkon ulkorajoille, vaan sen tulee olla kokonaisvaltaista. Informaatioteknologiaan liittyvät uhkat ja haavoittuvuudet tulee tunnistaa tuotantoprosessin kaikissa vaiheissa, erityisesti jo kehitysvaiheessa. Autonomisten järjestelmien ja robottien kehittämiseen liittyvät eettiset ja turvallisuuskysymykset odottavat vielä ratkaisua. Keinoälyn kehittämiseen ja soveltamiseen liittyvästä moraalisesta ja eettisestä vastuustamme ei ole vielä edes vakavasti keskusteltu.

Yhä enemmän digitalisoituvassa yhteiskunnassamme kyberturvallisuuden merkitys tulee kasvamaan merkittävästi. Meidän tulee kyetä navigoimaan turvallisesti digitaalisten palveluiden, strategisen viestinnän, informaatio-operaatioiden sekä kyberuhkien miinakentässä. Viestiupseeriyhdistyksen jäsenien ja Viestimiehen lukijoiden tulee olla edelläkävijöitä niin palvelutuotannossa kuin kyberuhkaan liittyvässä varautumisessa.

Puolustusvoimain johtamisjärjestelmäpäällikkö

Prikaatikenraali Mikko Heiskanen



TEKSTI: TAPIO TEITTINEN
KUVAT: PEKKO HEIMOLA

Viestijoukot 100 vuotta 5.3.2018”

Saksalaiset hyökkäävät Ranskan rintamalla.

16000 vankia ja 200 tykkiä

(Kipinäsähkösanoma)

Berliinistä, maaliskuun 23 päivä (klo 20.30 illalla)”

Näin alkoi Mikkelin Sanomien 24.3.1918 julkaistun lehden ulkomaan uutinen. Miten oli mahdollista, että pienen savolaisen kaupungin lehdessä julkaistaan ”uunituoreita” uutisia maailmalta tilanteessa, jossa lähes koko maa on tietoliikennemotissa ja varsinkin valkoisen puolen yhteysmahdollisuudet ulkomaille olivat lähes olemattomat?

Tuohon aikaan vähäiset tiedot ulkomailta kulkeutuivat Mikkeliin Vaasan kautta ja ne toimitettiin morselennättimellä lankoja pitkin. Tietoja tuli vähän ja niissä oli usein muutaman päivän viive.

Maaliskuun 5. päivänä 1918 kerääntyi kaupungin laidalla olevalle Liukkosen torpalle, noin 400 metrin päähän asutuksen ylle kurottavasta tuomiokirkon tornista, erikoinen seurue. Kolme usean hevosen vetämää vaunua ja joukkueellinen jääkäreitä ryhtyi kantamaan tavaroita ja pystyttämään korkeita salkoja pihamaalle. Yksi painava laite sijoitettiin talon piskuiseen keittiöön ja muut laitteet kamariin. Pihalla oleviin salkoihin viriteltiin lankoja pitkin ja poikin. Paikan ylimpänä päällikkönä komensi yliluutnantti E. Heimbürger, jolla oli monta muutakin asiaa vastuullaan, olihan hän radioaseman päällikkyyden ja radiokoulun johtajan tehtävien lisäksi myös määrätty vasta perustetun Kenttälennätinpataljoonan 1. komppanian päälliköksi. Käytännössä esimiehenä toimi siten vänrikki E. Reims. Radisteina kipinälennätinasemalla toimivat luutnantti J. Kröger, sekä vänrikit A. Gottlebe, Into ja Karl Nyström.

Kohta alkoi keittiöön raahattu sähkögeneraattori pitää meteliä. Luutnantti J. Kröger istui kamarissa kuulokkeet päässä ja väänteli edessään olevan suuren laitteen nappuloita. Jääkäreitä singahteli sisään ja ulos käyden välillä pihalla olevan lankavirityksen kimpussa.

Sankarivainajien muistopatsaalle kukkalaitteen laskivat prikaatikenraali Mikko Heiskanen, everstiluutnantti Jukka-Pekka Virtanen ja Kaakkois-Suomen Viestikillan puheenjohtaja Tapio Teittinen.

Viimein hymy nousi laitteen ääressä olevien luutnantin kasvoille. Hän kirjoitti jotain paperille keskittyneesti, nosti sitten katseensa ja totesi: ”Saatiin sitten Berliini kuulumaan, nyt yritetään yhteyttä Vaasaan”.

Kyseessä oli jääkäreiden Saksasta mukanaan tuoma ”kevyt” kipinälennätinasema. Laitetta kuljettamaan tarvittiin kahdesta kolmeen valjakkoa. Eri vaunuissa olivat radiolaitteet, masto antennitarvikkeineen ja sähkövoimageneraattori. Masto oli 17 metrin teleskooppimasto ja antenni oli sateenvarjotyyppinen, neljälankaisella vastapainolla varustettu. Taajuusalue oli muutamista kymmenistä hertseistä aina kahteen tuhanteen hertsiin asti. Tehoa piti lähtemän 1,5 kW.

Nimi ”kipinälennätin” tuli radiolaitteen toimintaperiaatteesta, jossa muuntajan ensiökäämiin kytkettyä releen tapaan toimivaa automaattista katkojaa ohjattiin sähkötysavaimella. Muuntajan toisiokelan rakenteessa oli virtapiirissä katkos (elektrodeista tehty kipinäväli), jolloin toisiokelaan indusoitunut suurjännite aiheutti katkosväliin kipinöintiä. Toisiopiirin kapasitanssia ja induktanssia (kondensaattoria ja käämiä) muuttelemalla pystyi määrittämään, millaista taajuutta kipinöinti pääosin edusti. Kipinöivään osaan oli liitetty lanka, joka siirsi syntyneen värähtelyn sähkömagneettisena aaltona ilmaan. Tällainen laite kehitti melkoisen sähkömagneettisen spektrin häiriten muita mahdollisesti alueella olevia kipinälennättimiä. Ilmaisimena eli vastaanottimena oli kidevastaanotin.

Maaliskuun loppupuolella 1918, sai Mikkelin Sanomien toimittaja Vihtori Simonen alueen viestipäälliköltä puhelinsoiton, jossa kerrottiin, että tuon Liukkosen torpalla sijaitsevan radioaseman kautta voisi myös kaupungin lehdistö saada tietoja maailmalta.

Niinpä toimittaja Simonen meni joka ilta Liukkosen torpalle, josta hänelle luovutettiin maailmalta tulleita sähkösanomia. Varmaankin lehdistön edustajalle luovutettiin sellaisia tietoja, jotka katsottiin sopiviksi julkistaa. Erityisen mielenkiinnon kohteena olivat Saksan päämajan tiedonannot Berliinistä, mutta tietoja tuli Räävelistä, Libausta, Tsarskoje Selosta ja Ruotsin eri asemilta.

Vuonna 1919 julkaistussa kirjassa ”Puolesta Savon ja syntymämaan” muistelee toimittaja Vihtori Sivonen seuraavasti:

”Aina kun joutohetkinäni olen kävelyllä kaupungin ulkopuolella ja tieni sattuu johtamaan Liukkosen torpan ohi, tekee mieleni ottaa hattu päästäni. Muistan aina silloin elävästi viikot, jolloin tuon matalan katon alla yötä päivää kuunneltiin avaruudessa soivia piipittäviä ääniä ja merkittiin ne paperille sanoiksi ja lauseiksi. Ilma oli ja on aina täynnä noita ääniä, jotka ajatuksen nopeudella aaltoilevat kaikkiin suuntiin. Mutta pientä viisaria siirtelemällä hallitsee kipinäsähköttäjä tätä soivien ääniaaltojen tulvaa ja ottaa samanaikaisista sanomista sen, mikä niistä on tärkein.”

Juhlapäivän tapahtumia

”Tää harjanne silloin itki verta,
kun sankarin maa poveensa peitti.
Kyynelehti rinne jokainen kerta,
kun jäähyväisensä ystävät heitti.

Hiljaisena käyn luo isänmaan uhrin.
Nöyränä kiitän tekoja sun.
Sä kaikkesi annoit maallemme tälle,
et‘hyvä ois täällä asua mun.”

Näillä kirjoittamansa runon ”Sankarihaudoilla” sanoilla Pellervo Pekkola vei kuulijat perimmäisten aatosten äärelle, kun Viestijoukot sata vuotta - tapahtumapäivä käynnistyi seppeleen laskulla Mikkelin Pitäjänkirkon sankarihaudoilla. Avoneliöön järjestäytynyt juhlaväki kuunteli hartaana sankaripatsaan äärellä sinisen taivaan alla lausuttuja säkeitä.

Viestijoukot sata vuotta -tapahtumapäivä oli koonnut Mikkeliin Puolustusvoimien ylimmän viestijohdon sekä runsaasti viestikiltalaisia ympäri valtakuntaa. Tapahtuman taustaorganisaationa oli Viestikiltojen liitto ry ja tapahtumaa tuki myös Maanpuolustuksen Viestisäätiö. Käytännön järjestelyistä vastasi Kaakkois-Suomen Viestikilta.

Radiokeskuksen muistolaatan Urpolan kartanolla paljasti prikaatikenraali Mikko Heiskanen. Kunniavartiossa Juha Ruuskanen ja Vesa Kauppinen. Pensaan takana laatan paljastuspuheen pitänyt DI Martti Susitaival.

Viestijoukkojen synty-näyttelyn avasi Maavoimien esikuntapäällikkö, kenraalimajuri Markku Myllykangas, avustajana Tapio Teittinen. VKL:n kunniapuheenjohtaja Markus Virrankoski tarkkailee operaation onnistumista.

Seuraavaksi juhlaväki kokoontui Urpolan kartanolle, jonka lähes 200-vuotias päärakennus oli vilkkaan toiminnan keskuksena Jatkosodan ja Lapin sodan aikana. Tuolloin rakennuksessa toimi Päämajan radiokeskus kaikkine laitteineen ja antenneineen. Puolustusvoimien johtamisjärjestelmäpäällikkö, prikaatikenraali Mikko Heiskanen paljasti kartanon seinään Mikkelin kaupungin luvalla kiinnitetyn Päämajan radiokeskuksen muistolaatan. DI Martti Susitaival kertoi paljastuspuheessaan radiokeskuksen taipaleesta ja toiminnasta.

Kartanolta juhlijoiden tie vei varsinaiselle juhlapaikalle, Kulttuuritalo Tempolle, jossa nautittiin suolaisen

eväspalan kanssa kahvit ja pidettiin vauhdikkaasti Viestikiltojen liiton kevätkokous. Kokouksen sujumista avitti kokouksen puheenjohtajana toimineen Seppo Kiisken vuosien kokemus eri järjestöjen puheenjohtajana. Niin tulivat hyväksytyksi edellisvuoden toimintakertomus kuin tilipäätöskin ilman nikotteluja. Kokoukseen osallistumattomille oli tarjolla mahdollisuus piipahtaa samaan aikaan Päämajamuseossa.

Juhlijoiden matka jatkui kiven heiton päässä olevan Viestikeskus Lokin uumeniin, jossa Maavoimien esikuntapäällikkö, kenraalimajuri Markku Myllykangas avasi Kaakkois-Suomen Viestikillan toteuttaman näyttelyn ”Viestijoukkojen synty - Marskin johtamisjärjestelmä M18”. Näyttely kertoo kuvin, piirroksin, tekstein ja laittein viestiasioista syksyltä 1917 aina kevääseen 1918 asti. Tämä näyttely siirretään syksyllä 2018 Museo Militariaan Hämeenlinnaan.

Pääjuhlapaikkamme, tuolloinen Työväentalo, oli vallattu verettömästi valkoisille tammikuun lopulla 1918. Rakennuksessa perustettiin 5.3. Kenttälennätinpataljoona, jonka kasarmina tila toimi, koska muut kasarmit olivat täynnä. Nykyään rakennuksessa toimii monipuolisia ruoka- ja tapahtumapalveluita tuottava Kulttuurikeskus Tempo.

Viestijoukkojen kunniamarssin kajahtaessa komeasti Hämeen Reserviläissoittokunnan soittamana, nousivat kaikki ylös kunnioittamaan airueiden Seppo Kiisken ja Heikki Huttusen sisään tuomia Suomen ja Viestikiltojen liiton lippuja.

Tilaisuuden avaussanoissa Viestikiltojen liiton puheenjohtaja, everstiluutnantti Jukka-Pekka Virtanen tervehti kiitoksin paikalle saapunutta arvovaltaista kutsuvierasjoukkoa ja juhlaväkeä. Hän kertoi Viestikiltojen liiton toiminnassa olevan nyt positiivisen vireen. Liiton yksi tärkeimmistä tavoitteista on kehittää viestikiltojen roolia paikallispuolustuksen johtamisjärjestelmä- ja viestikoulutuksessa. Yhteistoiminta niin valtakunnallisella kuin alueellisella tasolla on lisääntynyt puolustusvoimien, Maanpuolustuskoulutusyhdistyksen sekä muiden alalla toimivien vapaaehtoisjärjestöjen kanssa. Toisaalta perinneasiat ovat edelleen merkittävässä asemassa Museo Militarian ja erilaisten alueellisten hankkeiden myötä. Hän totesi olevansa vakuuttunut siitä, että

Viestijoukkojen kunniamarssi soi, lippuairueena Seppo Kiiski ja Heikki Huttunen.

Eversti Seppo Uro kertoi juhlapuheessaan Viestijoukkojen synnystä ja taipaleesta läpi vuosisadan.

Viestikilloilla on nyt ja tulevaisuudessa tärkeä rooli niin maanpuolustustahdon kuin poikkeusolojen kansallisen johtamisvalmiuden kehittämisessä.

Viestijoukkojen syntyvaiheet, organisaatiomuutosten vaikutukset viestijoukkoihin vuosikymmenten saatossa ja joukko-osastojen merkkipäivät tulivat tiedoksi kaikkien tunteman viestin historioitsijan, eversti Seppo Uron juhlapuheessa. Onneksi tuo tietopaketti löytyy hänen kirjoittamastaan jutusta edellisestä Viestimiehen numerosta 1/2018.

Viestitarkastaja, eversti Eero Valkola kertoi huumorilla kevennetyssä tervehdyssanoissaan siitä, miten viestijoukoissa vietetään juhlavuotta eri puolilla Suomea. Hän kertoi myös niistä odotuksista jotka kohdistuvat uuteen kotimaista valmistetta olevaan M18-viestijärjestelmään.

Omat tervehdyksensä Viestijoukot sata vuotta –juhlaan toivat Puolustusvoimien johtamisjärjestelmäpäällikkö, prikaatikenraali Mikko Heiskanen, Maavoimien esikuntapäällikkö, kenraalimajuri Markku Myllykangas, Puo-

lustusvoimien Johtamisjärjestelmäkeskuksen johtaja, eversti Mikko Soikkeli, Ilmavoimien johtamisjärjestelmäpäällikkö, insinöörieversti Jouni Muranen sekä Erillisverkkojen toimitusjohtaja Jarmo Vinkvist.

Juhlassa palkittiin Viestikiltojen liiton pienoislipulla Arto Pekkola, liiton kunniajäseniksi nimitettiin Pellervo Pekkola, Tapio Teittinen, Jarmo Seppä, Erkki Renberg ja Pekka Kastemaa. Aiemmin luovutettuun Viestiristiinsä soljen sai Martti Susitaival, Viestiristillä soljen kera palkittiin Seppo Halminen ja Viestiristillä palkittiin Pertti Pukarinen. Viestiristit jakoi Viestitarkastaja, eversti Eero Valkola ja Viestikiltojen liiton puheenjohtaja, everstiluutnantti Jukka-Pekka Virtanen.

Viestitarkastaja ja Erillisverkkojen toimitusjohtaja jakoivat viestiristit, joista osa soljen kera, seuraaville Erillisverkkojen henkilöille: Sami Orakoski, Harri Hildén, Antti Koponen, Pekka Lehtimäki, Ilkka Meriläinen, Ari Puustinen, Jukka Leskinen, Heikki Kasila, Sami Kilkkilä, Mika Lehto ja Petri Nuutinen.

Viestitarkastaja ja Viestikiltojen liiton puheenjohtaja valmistautuvat jakamaan viestiristejä.

Pääjuhla päätettiin seisten kuunneltuun Porilaisten marssiin.

Viestijoukot sata vuotta tapahtumapäivän kääntyessä iltaan nautittiin juhlatalossa erittäin mureaa Roinilan Tilan härkää monien tykötarpeiden kera ja jälkiruuaksi maistuvaa mustaherukkavispilää, lakritsikermaa ja valkosuklaata. Olipa mukava jatkaa Viestijoukkojen juhlaa näiden herkkujen äärellä.

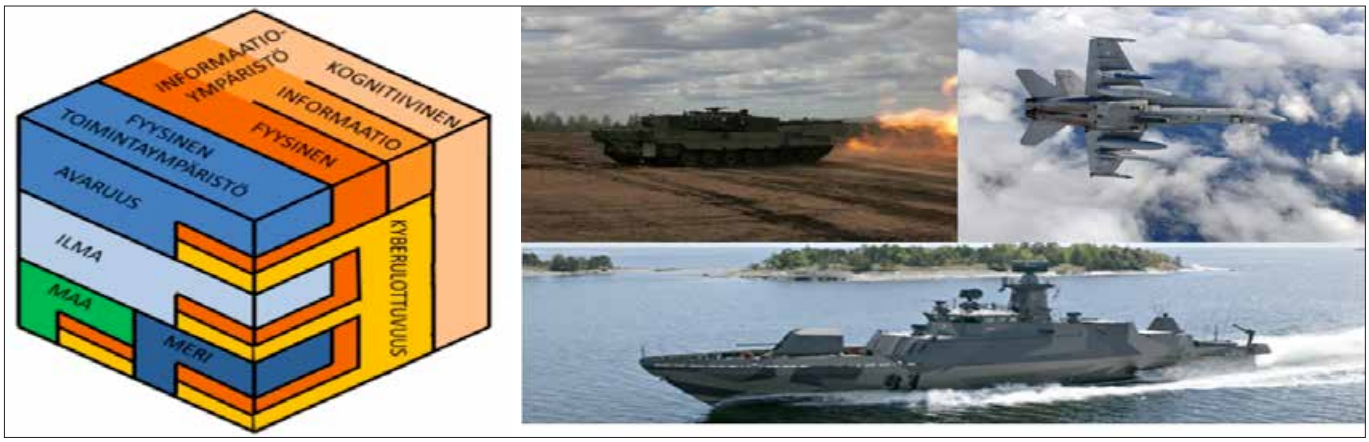
TEKSTI: EVERSTILUUTNANTTI ESKO LIIMATTA

Rajapintaharjoitus18 - vuosittainen sadonkorjuu

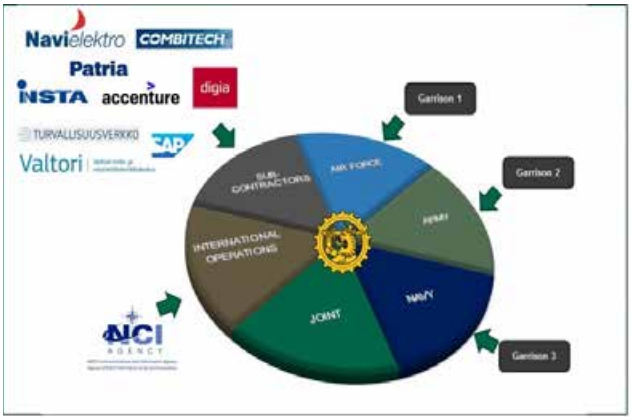
Rajapintaharjoitus on merkittävin vuosittainen johtamisjärjestelmä-toimialan ja viestiaselajin teknispainotteinen testaus- ja integraatioharjoitus. Harjoitus on vuosien saatossa laajentunut kattamaan johtamisjärjestelmän valmiuden todentamisen ja kehittämistarpeiden määrittelyn laaja-alaisesti ko. suorituskykytaksonomian osalta. Tekninen näkökulma on edelleen testaustoimintaa voimakkaimmin ohjaava näkökulma, mutta johtamisjärjestelmä- ja viestitaktiikan kehittäminen, johtamiskyvyn toiminnallisten vaatimusten tarkentaminen ja johtamisen tilannesidonnaiset toimintoketjut olivat tämän vuoden harjoituksessa myös voimakkaasti esillä.

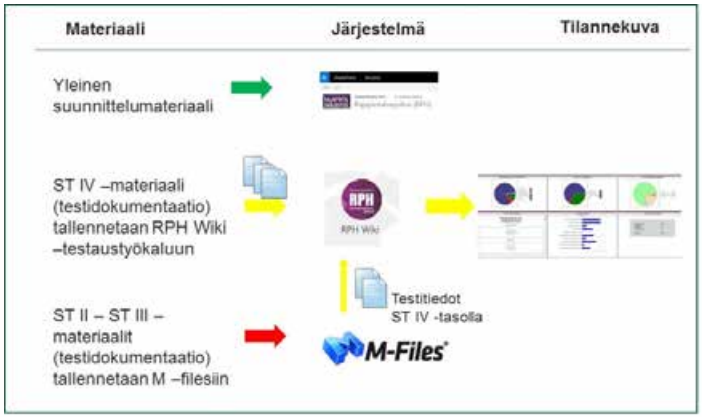
Rajapintaharjoitus-18 yleiskuvaus

Rajapintaharjoitus, RPH-18, toteutettiin 11.-18.4.2018. Allekirjoittaneella oli kunnia toimia harjoituksen johtajana. Harjoituksen päätoimipiste oli Riihimäen varuskunta, mutta testauksia toteutettiin myös kahdellatoista muulla testauspaikkakunnalla - Santahaminasta Kajaaniin ja Säkylästä Lappeenrantaan. Harjoitusjoukkojen kokonaisvahvuus oli 736 henkilöä muodostuen puolustusvoimien, strategisten kumppaneiden, viranomaisyhteistyötahojen sekä yritysten henkilöstöstä. Puolustusvoimien osalta harjoitukseen osallistuivat kattavasti sekä Joint-tasoiset että kaikkien puolustushaarojen alajohtoportaiden ja toimialojen keskeiset toimijat. Eri vai-



RPH-18 tavoiteasetannan 'Rubikin kuutio'.





RPH-18 harjoituksen testaus- ja dokumentointiympäristöt.

heissa elinkaartaan olevia sovelluksia, tietojärjestelmiä tai tiedonsiirtojärjestelmän ratkaisuita oli testattavana 42 kpl ja eritasoisia toiminnallis-teknisiä testejä toteutettiin dokumentoidusti harjoituksen aikana noin 270 kpl. Voidaankin pelkistää, että harjoituksen aikana puitiin johtamisjärjestelmä- ja viestitaktisesta näkökulmasta nykyinen teknisen suorituskyvyn pelto kutakuinkin viimeistä aaria myöten. Kultajyvät tallennettiin myös onnistuneesti suorituskyvyn valmiuden todentamisen ja jatkokehittämistarpeiden laareihin. Torajyvistä ja hukkakaurasta pyrittiin tietenkin samalla pääsemään eroon.

Tämän vuoden harjoituksessa erityispiirteinä olivat perinteisten tietojärjestelmä- ja tiedonsiirtotestien rinnalla, ja niitä tukemassa, tulenkäytön, logistiikan ja järjestelyalan toimintoketjutestit (skenaario-ohjatut testitapahtumat). Näiden skenaariotestien liittäminen testausrakenteeseen paransikin merkittävästi edellytyksiä kytkeä yksittäiset tekniset testit osaksi laajempaa valmiudellista toimintoketjua. Toinen merkittävä edistysaskel aiempiin rajapintaharjoituksiin verrattuna oli testausten toteutus aidosti tuotannonkaltaisessa testausympäristössä. Puolustusvoimien logistiikkalaitoksen (PVLOGL) ylläpitämä Puolustusvoimien Integrointi- ja testausympäristö, PVITY, paljastikin harjoituksessa leijonan luonteensa; Ympäristö tuki erinomaisesti tarvittavien testausverkkojen ja -ympäristöjen luomista ja hallintaa. Testausraporttien jatkohyödynnettävyys johtamiskyvyn valmiuden edelleen kehittämiseksi onkin todennäköisesti huomattavasti aiempia vuosia paremmalla tasolla.

Testausympäristöjen kehittäminen

RPH-18 tyyppisen moniulotteisen ja tavoitteiltaan haastavan harjoituksen johtaminen ei ole mahdollista pelkästään ’reisitasku’ muistiinpanojen avulla. Erityisesti jatkosuunnittelua tukevien testaustulosten järjestelmällinen dokumentointi vaatii perinteistä Excel-taulukointia tehokkaampia työkaluja. PVITY-ympäristön ja uuden käyttöönotetun testien suunnittelu, dokumentointi ja raportointityökalun, RPH Wiki, joka pohjautui CWIX-harjoituksessa käytettyyn Wiki:in, käytön yhteensovittaminen olikin yksi mittavimmista haasteista harjoituksen valmisteluvaiheessa. Tästäkin tehtävästä harjoitusorganisaatio asiaankuuluvien alkukankeuksien jälkeen kuitenkin selvisi erinomaisesti.

Virtualisoidun testausympäristön ja järjestelmien suorituskyvyn koko elinkaarta tukevan dokumentointiympäristön käyttöönotto oli erinomainen esimerkki RPH-18 harjoituksen useista välillisistä tavoitteista. Tässä onnistuttiin. Tarkoituksenmukaisiksi ja käytettävyydeltään käyttötarkoitukseen soveltuviksi todetut ratkaisut luovat aiempaa kypsemmän lähtökohdan vastaavien harjoitusten jatkosuunnittelulle ja toimeenpanolle. Käyttöönotettujen ratkaisuiden avulla on mahdollista jatkossa hajauttaa keskitetyn integraatiotestauksen työkuormaa toteuttamalla yksittäisiä järjestelmiä koskevat integraatiotestaukset kehittämishankkeiden ja -projektien kannalta tarkoituksenmukaisessa aikataulussa. RPH- harjoituksen mukainen testausympäristö, on siis haluttaessa käytettävissä 24/7/365 periaatteen mukaisesti. Ympäristö mahdollistaa myös edellytettävien testausten ja yhteensopivuuden todentamisen kansainväliseen yhteistyöhömme liittyvien osapuolten kanssa. PVITY kykenee hyödyntämään myös Naton vastaavaa testaus- ja dokumentointiympäristöä (CFBLNet, Combined Battle Laboratories Network, on kansainvälisen yhteensopivuuden testauslaboratorioiden yhteisö, jota käytetään mm. FMN-ohjelman integraatio- ja konfirmointitestausten alustaratkaisuna).

Tekniset edellytykset testaustoiminnan tehokkuuden ja jatkuvuuden kehittämiseksi ovat olemassa ja todettu myös toimiviksi RPH-18 yhteydessä. Testaustoiminnasta vastanneena PVLOGL ja erityisesti sen Järjestelmäkeskus on tältä osin ruusunsa ansainnut.

Testaustoiminnan rakenteet ja keskeiset tulokset

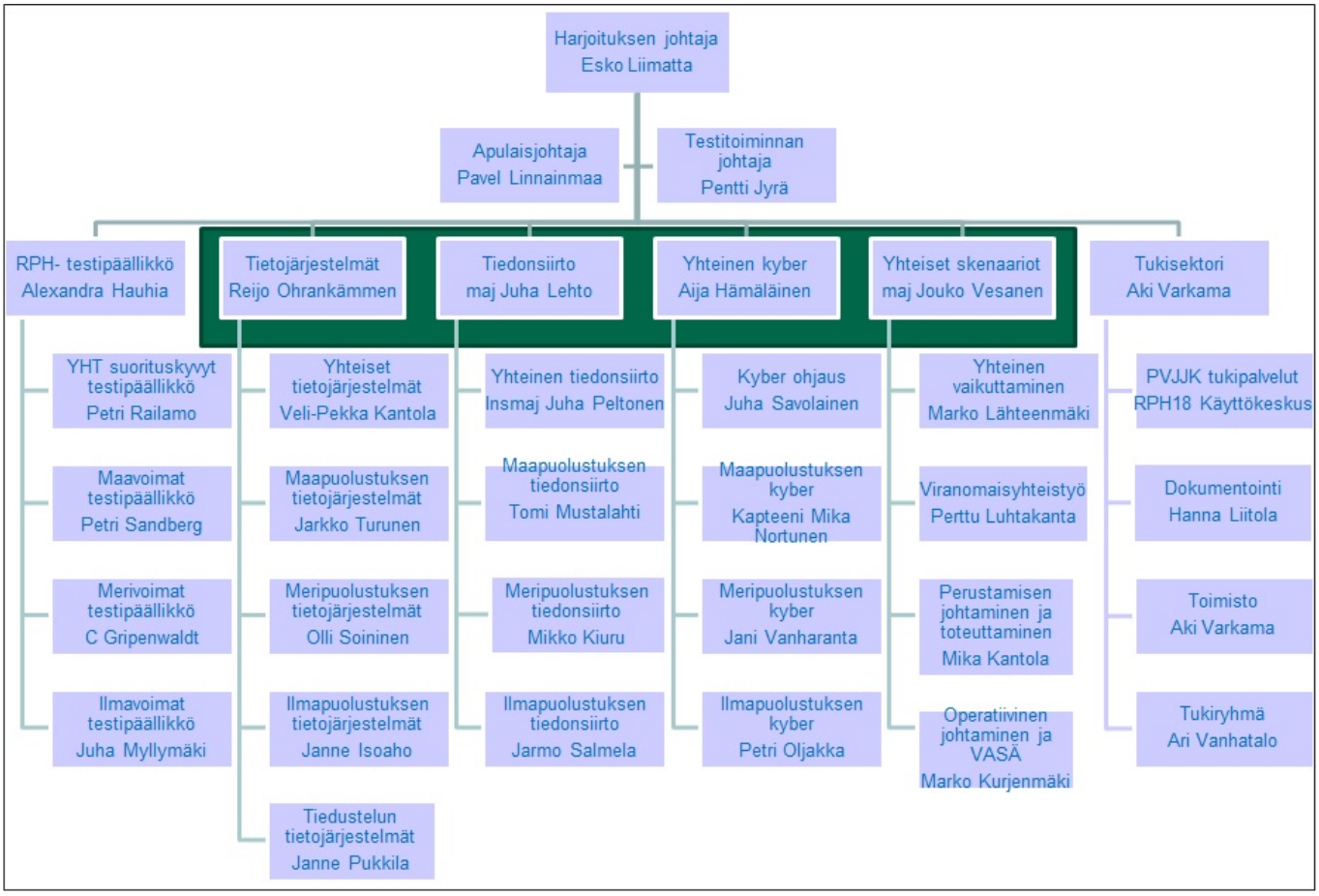
Testaustoiminnasta harjoituksessa vastasi PVLOGL Järjestelmäkeskus, joka oli asettanut testitoiminnan johtajaksi insinöörieverstiluutnantti Pentti Jyrän ja Testipäälliköksi kapteeni (evp) Alexandra Hauhian. Testaustoiminta organisoitiin toteutettavaksi neljän testisektorin kautta; Tietojärjestelmät, Tiedonsiirto, Yhteinen kyber ja Yhteiset skenaariot. Testisektoreiden alla testausryhmät oli vastaavasti järjestetty puolustushaara- ja toimialajaottelun mukaisesti. Rakenne vastasi Johtamisen kehittämisohjelman hanke- ja projektirakenteita.

Rajapintaharjoitus 2018 testaustoiminta kyettiin toteuttamaan laaditun testaussuunnitelman mukaisesti. Eritasoisia teknis-toiminnallisia testejä toteutettiin 258 kpl, joista onnistuneita (Success) 159 kpl, onnistuneita huomautuksin (Limited success) 63 kpl ja yhteensopivuusvirheitä sisältäneitä (Interoperability issue) vain 18 kpl.

Testaustulosten alustavan analysoinnin perusteella johtamisen operatiiviset toimintamallit ovat toimivia ja johtamisjärjestelmä kykenee tuottamaan keskeisten toimintoketjujen edellyttämät johtamisen tuen palvelut pääosin hyvällä tasolla. Testattaessa uusia ohjelmistoversioita ja näiden toiminnallisuuksia ei ollut toisaalta mitenkään yllättävää, että toiminnallisuuksissa, ohjelmistoissa, konfiguraatioissa sekä laitteissa esiintyi vielä jatkokehitystarpeita. Virheiden ja jatkokehittämistarpeiden todentaminen onkin tämän tyyppisen testausharjoituksen havaintojen osalta ihan yhtä arvokas tuotos, kuin testiraporttien perusteella hyväksytysti toteutuneet testitapaukset.

Onnistuneet testit alueellisen johtamisen tuen, logistiikan johtamisen, tulenkäytön toimintaketjujen sekä tilannekuvan muodostamisessa ja jakelussa vahvistivat näkemystä johtamisjärjestelmämme teknisen suorituskyvyn tilasta; Hankkeet ja projektit ovat onnistuneet hyvin tehtävissään vuonna 2017. Tiedonsiirron osalta uusi liityntäverkkokonsepti vaikuttaa onnistuneelta vaikkakin jatkokehittämistä edellytetään vielä erityisesti uuden sanomanvälitysjärjestelmän tuotteistuksen osalta.

Rajapintaharjoituksessa oli testattavana myös uusia innovaatioita. Näistä mainittakoon satelliittipohjaisen tiedonsiirron suorituskyvyn kehittämiseksi testattu ’kenttäkelpoinen’ satelliittiantenni, GATR, joka osoittautui testeissä suorituskyvyltään vaatimukset täyttäväksi. Antenni on ilmatäytteinen ja tästä syystä pakattavissa pieneen tilaan (kahteen ’matkalaukkuun’). Tulevalle syksylle suunnitellun ohjelmistopäivityksen myötä myös antennin tiedonsiirtokapasiteetti nousee tasolle 10.1 Mbit/s, joka on riittävä suunniteltuun käyttötarkoitukseen.



Harjoituksen testiorganisaatio.

Keskellä liityntäreitittimen konfigurointiasema 'Tehdas' ja laidoilla sanomanvälitystesteihin liittyvää testauskalustoa.

Kohti uusia haasteita - rph-18 tulosten jatkohyödyntäminen

Rajapintaharjoitus-18 oli mittava ponnistus Johtamisjärjestelmäalalle ja Viestiaselajille. Harjoituksen suunnittelu ja toimeenpano vaativat yhteensä noin 30 henkilötyövuoden panostuksen, joten olisi suotavaa, että harjoituksesta saatava hyöty ei rajoittuisi pelkästään varsinaisen testausvaiheen aikana 11.-18.4.2018 tehtyihin havaintoihin ja esiintyneiden jatkokehittämistehtävien ideointiin. Mittavimmat hyödyt ovatkin ulosmitattavissa vasta harjoituksen jälkeen toteutettavissa joukkokohtaisissa harjoituksissa, suorituskykyhankkeiden alaisissa kehitysprojekteissa ja kehittyvissä koulutusohjeistuksissa. Tuotettu mittava testausdokumentaatio tarjoaa myös laajan ja systemaattisesti käsitellyn lähtöaineiston toimialan tutkimusten lähdeaineistona. Toivottavasti testiraportit kuluvat käytössä myös tutkijoiden käsissä.

2,4 m:n satelliittiantenni, GATR.

Haluan kiittää kaikkia harjoituksen suunnitteluun, valmisteluun ja toimeenpanoon osallistuneita henkilöitä yhdessä ja erikseen. Erityiskiitos 'kilpailutoimiston' rouville pikatilanteiden tyylikkäästä hoitamisesta ja kapteeni Pavel Linnainmaalle, joka harjoituksen johtajan apulaisena teki harjoituksessa todellisen miehen työn. Hyvin suunniteltua ja toimeenpanovaiheessa hyvähenkistä harjoitusta oli helppo johtaa. Harjoitus konkretisoi eri toimijoiden yhteistyökykyisyyden erinomaista tasoa ja yhteistä tavoitetta järjestelmien ja toimintamallien kehittämisessä: "Viesti perille".

Everstiluutnantti Tero Palokangas palvelee apulaissotilasedustajana (johtamisjärjestelmät ja kyberpuolustus) Suomen Nato- ja EU-edustustoissa Brysselissä.

Everstiluutnantti Jarmo Sinkkonen toimii Suomen kansallisena edustajana Naton operaatioesikunnassa (SHAPE) FMN-sihteeristössä Monsissa.

TEKSTI: TERO PALOKANGAS JA JARMO SINKKONEN
KUVAT: PUOLUSTUSVOIMAT

Federated Mission Networking etenee kohti tavoitetilaansa

Ajankohtaisseminaari Helsingissä oli menestys

Naton ”sponsoroiman” FMN-ohjelman tavoitteena on mahdollistaa yhteisen tiedustelun, tulenkäytön ja johtamisen kokonaisuus, tarvittavat palvelut sekä tiedonsiirto monikansallisessa operaatiossa. Käytännössä tämä tarkoittaa, että aikanaan operaatioon osallistuvat joukot voidaan viiveettömästi verkottaa ja mahdollistetaan operaatiotehokkuus heti operaation käynnistyessä. Helmi-maaliskuun vaihteessa Helsingissä järjestetty FMN-seminaari oli järjestelyjen ja sisältönsä puolesta menestys, joka osaltaan tukee FMN-tuntemusta ja –ymmärrystä osallistujamaiden johdon ja muun avainhenkilöstön keskuudessa. Keskeistä seminaarissa oli saada eri toimialojen, erityisesti operatiivisen ja tiedustelualan loppukäyttäjät saman pöydän ääreen keskustelemaan FMN-suorituskykyjen kehittämisestä ja niiden optimaalisesta käytöstä osana tulevaisuuden mahdollisia operaatioita.

FMN-ohjelmasta

FMN-ohjelmassa ei ole kysymys pelkästään teknisistä ratkaisuista, vaan suorituskykykokonaisuudesta, joka sisältää teknologiaa, doktriineja, johtajuutta, järjestelmiä ja niiden palveluita, toimintamalleja, tietojärjestelmiä ja turvallisuutta. Ohjelma on vasta muutaman vuoden ikäinen ja on nyt saavuttanut ensimmäiset käytännön tu-

Seminaari mahdollisti ohjelman nimen (Networking) mukaisesti hyvän tapahtuman ajatusten vaihtoon ja henkilökohtaisten kontaktien luomiseen.

lokset – eri jäsenmailla on tällä hetkellä käytössään yhteensopivat johtamisen peruspalvelut. Aiemmin Nato-maat laativat standardoimisasiakirjoja (STANAG:t), joiden ohjeistamana niin Nato-maat kuin kumppanitkin kehittivät verkkojaan ja johtamisjärjestelmäpalvelujaan. Tämä ei ole kuitenkaan aikojen saatossa tuottanut aivan toivottua tulosta. FMN-ohjelman tärkein tuotos on, että se korjaa pala palalta, kahden vuoden sykleissä, yhteentoimivuuspuutteet olemassa olevien johtamisjärjestelmäpalveluiden osalta. Ajan kanssa siis yhä isompi osa verkoista ja niiden palveluista on FMN-määrittelyjen mukaisia. Kehityksen myötä mukaan tulee uusia teknisiä ratkaisuja ja myös uusia palveluja.

FMN-verkkoarkkitehtuurissa osallistujamaat liittyvät useisiin naapureihinsa ja siten yhteydet ovat varmennettuja. Palveluiden tarjoamiseen kykeneviä osallistujamaita on useampia, joka parantaa verkon taistelunkestävyyttä. Operaatioverkon johto-organisaatio perustuu federaatioajatteluun – malli, jossa kaikki operaatioon osallistuvat maat kontribuoivat johto-organisaatioon sen kaikille tasoille. Kun johto-organisaatio miehitetään jokaisen osallistujamaan asiantuntijoilla, he tuovat samalla mukanaan oman maansa parhaan asiantuntemuksen. Tämä tehostaa merkittävästi operaatioverkon johtamista. FMN-ohjelma laatii yhtenäiset operaatioverkon perustamiseen ja ylläpitoon vaadittavat asiakirjapohjat. Tämä nopeuttaa muodostettavan verkon toimeenpanoa, kun asiakirjat ovat pääosin jo valmiina ja niiden rakenne ja sisältö on kaikille tuttu.

Operaatiopäällikkö, kenraaliluutnantti Eero Pyötsiä toi seminaarin iltatilaisuuteen (Ice Breaker) Puolustusvoimien tervehdyksen.

Seminaarissa esillä olleet Suomen FMN-ratkaisut olivat suuren mielenkiinnon kohteena.

Osallistujat ja organisaatio

FMN-ohjelman jäseninä ovat lähes kaikki Nato-maat, kuusi kutsutuista kumppanimaista sekä Naton komentorakenne yhtenä tasavertaisena jäsenenä. Mukana ovat kaikki Pohjoismaat Islantia lukuun ottamatta. Jäseniä kutsutaan affiliaateiksi (koska kaikki eivät ole maita), joita on tällä hetkellä yhteensä 35. Kiinnostusta ohjelmaa kohtaan on myös EU:lla ja joillain toistaiseksi ohjelmaan vielä liittymättömillä mailla.

Nimensä mukaisesti työskentely perustuu federaatiomalliin, jossa kaikki verkkonsa kehittämiseen sitoutuneet jäsenet (kaksi erilaista osallistumistasoa) osallistuvat samanarvoisina kaikkiin tehtäviin ja työvaiheisiin. Tasavertainen osallistuminen sitouttaa ja kaikilla on mahdollisuus vaikuttaa. Kolmas osallistumistaso on tietynlainen tarkkailijajäsenyys, jolloin velvoitteet ovat rajatummat, mutta nämäkin jäsenet osallistuvat päätöksentekoon. Päätökset tekee kahdesti vuodessa kokoontuva ohjausryhmä, johon kuuluu kaikkien jäsenten edustajat. Pääesikunnan johtamisjärjestelmäpäällikkö on Suomen edustaja ohjausryhmässä.

Naton operaatioesikuntaan (SHAPE) sijoitetussa FMN-sihteeristössä on edustajat kaikista verkkoaan kehittävistä jäsenmaista. Sihteeristö vastaa päätöksenteon valmistelusta ja ohjausryhmän päätösten toimeenpanosta sekä koordinoi ja ohjaa työryhmien välistä työskentelyä. Päätyön tekevät viisi monikansallista työryhmää, joiden päätehtävät ovat: operatiivisten vaatimusten asettaminen, spiraalikohtaisten teknisten spesifikaatioiden laatiminen, teknisen yhteensopivuuden testaus, palveluiden

ylläpito ja muutoksenhallinta sekä turvallisuus ja kyber-asiat. Työskentelyn saumattomuutta tehostetaan työryhmien yhteiskokouksilla sekä ryhmien johtajien säännöllisillä kokoontumisilla ja yhteydenpidolla.

Vaiheittainen kehitystyö

FMN-ohjelman tärkein tuotos, verkkojen ja järjestelmien yhteentoimivuus, varmistetaan vaiheittain siten, että osallistujamaat sitoutuvat kahden vuoden välein saavuttamaan yhdessä sovittujen ja suunniteltujen johtamisjärjestelmäpalvelujen osalta FMN-valmiuden. Näitä kahden vuoden välein valmistuvia työkokonaisuuksia kutsutaan spiraaleiksi. Koska kunkin spiraalin kehitystyö vaatimusmäärittelystä valmiuteen kestää useita vuosia, kolmen eri spiraalin kanssa työskennellään aina samanaikaisesti: yksi on tuotantokäytössä, seuraava kehitysvaiheessa ja kolmatta määritellään.

Tällä hetkellä ensimmäisen spiraalin osalta valmius on jo saavutettu. Siinä varmistettiin peruspalveluiden, kuten esimerkiksi sähköpostin, puhelupalveluiden, chat-palveluiden ja videoneuvottelun toimivuus. Toinen spiraali sisältää ensimmäisen spiraalin jatkokehitettäviä palveluita sekä uusina ominaisuuksina muun muassa tilannekuvapalveluita, tiedustelun työkaluja, järjestelmien tietoturvallisuusratkaisuja sekä sanoma- ja tiedostojakoratkaisuja. Kyseisen spiraalin osalta affiliaattien valmius tulee saavuttaa kuluvan vuoden loppuun mennessä.

FMN ja Suomi

Suomi on ottanut aktiivisesti osaa FMN-ohjelmaan. Suomi on valinnut osallistumistasokseen haastavimman vaihtoehdon (A) ja on panostanut asetettuja minimivaatimuksia enemmän osaan työryhmätyöskentelystä osoittamalla asiantuntijoita työn tueksi. Tällä päästään jo suunnitteluvaiheessa vaikuttamaan yhteisesti valittaviin ratkaisuihin siten, että ne olisivat meille mahdollisimman edullisia ja samalla oma asiantuntijuus kehittyy ulkomaisten kontaktien kautta.

Suomen kannalta FMN-ohjelma tukee Puolustusvoimien uudeksi tehtäväksi määritetyn kansainvälisen avun anto- ja vastaanottokyvyn velvoitetta. Samalla kehitämme myös kykyämme vastata isäntämaasopimuksen asettamiin vaatimuksiin. FMN-kyvykkyydet tukevat vastaavalla tavalla osallistumistamme sotilaalliseen kriisinhallintaan ja vaativaankin kansainväliseen harjoitustoimintaan. FMN osallistumisen myötä kehitettäviä yhteisiä tietoverkkoratkaisuja ja -palveluita hyödynnetään täysimääräisesti kansallisen puolustuksen kehittämisessä. FMN-kyvykkyydet tukevat suoraan kahden- ja monenvälisen puolustusyhteistyömme tavoitteiden edistämiseksi tehtävää työtä, esimerkkinä NORDEFCO- ja FISE (Suomi-Ruotsi) yhteistyö.

Puolustusvoimain komentaja, kenraali Jarmo Lindberg kunnioitti läsnäolollaan seminaaritilaisuutta.

FMN-seminaarista

FMN-ohjelmaan on kuulunut sen perustamisesta asti määräajoin järjestettävät ajankohtaisseminaarit, joissa on ollut tarkoituksena esitellä saavutettuja tuloksia isommalle yleisölle ja siten sitouttaa palveluiden käyttäjät ja päätöksentekijät mukaan yhteiseen kehitystyöhön. Kaksi aikaisempaa FMN-seminaaria on järjestetty Vilnassa ja Istanbulissa. Tänä vuonna seminaari järjestettiin helmi-maaliskuun vaihteessa Helsingissä. Tapahtumaan osallistui noin 250 henkilöä, jotka edustivat 29 erillistä osallistujatahoa (affiliaattia). Seminaarin järjesti Naton operaatioesikunta yhteistyössä isäntämaa Suomen kanssa. Seminaari koostui alustusvaiheesta, jonka aikana valitut pääalustajat toivat esille omia näkökulmiaan FMN-ohjelmasta ja sen merkityksestä. Alustusten jälkeen seminaarijoukko jakautui viiteen työryhmään, joissa mietittiin tietyn osa-alueen näkökulmasta FMN-ohjelman nykytilaa ja tulevaisuutta.

Seminaari edeltävänä iltana järjestettiin kansainvälisen käytännön mukainen tervetulotilaisuus (Ice breaker), jossa osallistujilla oli mahdollisuus asianmukaisten tarjoiluiden siivittämänä verkostoitua ja vaihtaa kuulumisiaan. Tapahtumaan toivat tervehdyksensä FMN-ohjelman ohjauksesta vastaavan Management Groupin puheenjohtaja, kenraalimajuri Walter Huhn sekä Puolustusvoimien operaatiopäällikkö, kenraaliluutnantti Eero Pyötsiä. Kenraalimajuri Huhn kiitteli omassa puheenvuorossaan kaikkia seminaarin järjestelyihin osallistuneita tahoja, erityiskiitos osoitettiin luonnollisesti isäntämaa Suomelle. Kenraaliluutnantti Pyötsiä korosti omassa puheenvuorossaan FMN-ohjelman mukaisten suorituskykyjen kehittämisen tärkeyttä Puolustusvoimille sen lakisääteisten tehtävien toteuttamiseksi. Iltatilaisuudessa oli myös konkreettisesti esillä

Suomen FMN-määrittelyjen mukaista johtamisjärjestelmälaitteistoa, jotka kiinnostivat kovasti kansainvälistä osallistujajoukkoa.

Varsinaisen seminaaripäivän avasi kenraalimajuri Walter Huhn. Hän korosti puheessaan FMN-ohjelman ainutkertaisuutta ja sitä, että kaikkien mukana olevien on varmistettava, että jatkossakin yhdessä tuotetaan operatiivisille käyttäjille käsin kosketeltavaa suorituskykyä. Huhn oli myös leikkisästi mielissään siitä, että isäntämaa Suomi oli kyennyt varmistamaan seminaarin ajaksi mitä suurimmassa määrin ainutkertaiset, talviset olosuhteet (seminaarin aikaan oli Helsingissä noin -20 asteen pakkaset). Suomen tervehdyksen seminaariin toi Puolustusvoimain komentaja, kenraali Jarmo Lindberg. Hän toi esille kansainväliselle osallistujajoukolle Puolustusvoimien toimintaa ja nykytilaa. Lindberg korosti myös Suomen sitoutuneisuutta FMN-ohjelman kaltaiseen kansainväliseen yhteistyöhön, joka suoraan hyödyttää mitä suurimmassa määrin kansallisen puolustuksen kehittämistarpeita.

Seminaarin päätuotokset syntyivät ryhmätöiden kautta. Kyberturvallisuuteen keskittynyttä työryhmää johti Pääesikunnan johtamisjärjestelmäpäällikkö, prikaatikenraali Mikko Heiskanen.

Seminaarin avauspuheenvuoroissa (key note speakers) nostettiin esille muun muassa FMN-ohjelman merkitys Natolle ja sen mahdollisesti tulevaisuudessa johtamille operaatioille. FMN-suorituskykyjen kehittäjien ja operatiivisten loppukäyttäjien välistä yhteistyötä korostettiin myös keskeisenä tulevaisuuden menestystekijänä. Tästä nyt järjestetty seminaari nähtiin

myös erinomaisena esimerkkinä. Ohjelman luonteen mukaisesti myös ei Natoon kuuluvien osallistujien näkökulma nousi avauspuheenvuoroissa esille. Keskeistä onkin kyetä takaamaan kaikkien mukana olevien osallistujien (affiliaattien) yhtäläinen osallistumismahdollisuus niin FMN-ohjelmaan ja sen mukaiseen kehitystyöhön, kuin myös tulevaisuudessa mahdolliseen ”FMN-pohjaiseen” operaatioon. FMN-määrittelyjen mukaisia johtamisjärjestelmiä tulee kyetä käyttämään operaatiossa huolimatta siitä, onko kyse Nato-, EU- tai esimerkiksi YK-johtoisesta operaatiosta. FMN nähtiin myös mitä suurimmassa määrin johtamisjärjestelmäalan kehitystyötä aktivoivana ja tehostavana työnä.

FMN-jäsenyysvaihtoehdot:

FMN-ohjelma sisältää kolme osallistumistasoa, lupausta siitä, miten FMN-jäsenet kansallista suorituskykyään kehittävät.

Vaihtoehto A - Sisältää itse tuotetun siirtoverkon ja informaatioinfrastruktuurin sekä valmiuden tuottaa operaation vaatimat palvelut. Suomi on valinnut tämän vaihtoehdon, joka on luonnollinen rooli, jos ajatellaan ulkomaisen avun vastaanottotilannetta.

Vaihtoehto B - Operaatioverkkolaajennus sisältää itse tuotetun siirtoverkon ja osan palveluista. Osa palveluista käytetään muiden tuottamina.

Vaihtoehto C - Operaatioverkon osallistuja, jolla ei ole itsenäistä kykyä rakentaa infrastruktuuria ja palveluita. Palvelut saadaan käyttöön joko muilta osallistujilta tai operaatioon lähetetään esimerkiksi esikuntaupseereja, jotka käyttävät tietyn kumppanimaan (Vaihtoehto A/B) fasiliteetteja.

Ryhmätöiden keskeisistä havainnoista

Ensimmäinen työryhmä keskittyi FMN-ohjelman etuihin ja vaikutuksiin operaatioiden näkökulmasta. Keskeisinä havaintoina oli se, että affiliaattien tulee resurssihaasteistaan huolimatta kyetä täysimääräisesti tukemaan FMN-ohjelman eri työryhmien toimintaa. Toinen havainto oli se, että jatkossa tarvitaan yhteisiä tapoja ja foorumeita eri affiliaattien FMN-suorituskykyjen kehittämiseksi ja yhteentoimivuuden varmistamiseksi. FMN-ohjelmalla ja sen mukaisilla suorituskyvyillä nähtiin olevan suuri menestyspotentiaali, mutta operaatiivisen yhteisön laajempi mukaan saaminen edellyttää hyötyjen konkreettista osoittamista tulevaisuuden harjoituksissa ja operaatioissa. Tiedonvaihtokäytäntöjen osalta todettiin myös, että vaikka federaation sisällä onkin todellinen tarve jakaa tietoa, tulevat kansalliset käytännöt ja määräykset jatkossakin tavalla tai toisella vaikuttamaan toimintaan.

Toinen työryhmä keskittyi operatiiviseen suunnitteluun. Keskiössä oli Naton ”toimintaketjujen” (Mission threads: tavoitteena määritellä operaation eri toiminnallisiin osakokonaisuuksiin liittyvät toimijat ja heidän väliset tiedonvaihtotarpeet toiminnan eri vaiheissa) hyödyntäminen FMN-työskentelyssä. Kyseisen lähestymistavan nähtiin automaattisesti kehittävän yhteensopivuutta, ja sitä tulee kaikin keinoin tukea. FMN:n toimintaketjujen kehittämiseksi nähtiin tarvittavan riittävän hyvät, geneeriset esimerkit. Lisäksi operatiivisen yhteisön tulee tukea FMN-yhteisöä täysimääräisesti tässä määrittelytyössä. Tämä edellyttää alan asiantuntijoiden sitouttamista yhteiseen työskentelyyn ja tiedonvaihdon tehostamista eri affiliaattien ja työryhmien välillä.

Kolmas työryhmä keskittyi puolestaan suorituskykyjen kehittämiseen. Työryhmässä tunnistettiin tarve ketterämpään kehitystyöhön havaituista suorituskykypuutteista käytännön demonstraattoreihin ja sitä kautta käytännössä todennetuihin parannuksiin. Suorituskykyjen todentamiseen tarkoitettujen testien tietoturvamääräyksiä esitettiin myös tarkistettavaksi, jotta jatkossa varmistetaan kaikkien affiliaattien tehokas osallistumismahdollisuus. Teollisuuden sitouttaminen FMN-kehittämiseen ja sitä kautta saatavien tulosten hyödyntäminen nähtiin keskeisenä tulevaisuuden menestystekijänä. Nato-maat näkivät keskeisenä myös FMN:n laadullisten spiraalitavoitteiden tiiviimmän kytkemisen NDPP-prosessiin (Nato Defence Planning Process) ja sen jäsenmaakohtaisiin tavoitteisiin. Kaiken kaikkiaan keskeisenä ei nähty kysyä mitä FMN maksaa, vaan paljonko sen kautta tullaan säästämään.

Neljättä, kyberpuolustusta käsitellyttä työryhmää johti Pääesikunnan johtamisjärjestelmäpäällikkö, prikaatikenraali Mikko Heiskanen. Keskeisenä tarpeena ja siten operaation menestystekijänä työryhmässä tunnistettiin kybertilannekuvan jakamistarve eri affiliaattien kesken. Jo aikaisemmin käsitellyt ”operaatioketjut” nähtiin myös keskeisinä tekijöinä federaation yhteisen kyberpuolustuksen näkökulmasta. Tiedonjakamiskäytännöt ja kyberpuolustuksen toimivaltuudet eli ROE:t (Rules of Engagement) nähtiin myös kriittisinä menestystekijöinä, jotka tulee ennen operaatiota saada ratkaistua. Työryhmä näki myös tärkeänä, että FMN-yhteisö aloittaa federoidun kyberpuolutuksen harjoittelun tulevissa harjoituksissa. Työryhmä esitti myös erillisen työpajan kokoon kutsumista federoidun kyberpuolustuksen määrittelemiseksi ja konkreettisen toimeenpanosuunnitelman laatimiseksi.

Viides työryhmä käsitteli puolestaan FMN:n vaikutuksia koulutukseen ja harjoitteluun. Työryhmä totesi osuvasti loppuesityksessään, että FMN ei ole vielä ”osa DNA:tamme”, koska kohtuullisen uutena kokonaisuutena FMN-vaatimuksia ei ole kyetty vielä viemään osaksi koulutus- ja harjoitustoimintaa. Työryhmän mukaan jokaisen affiliaatin vastuulla on jatkossa itse pe-

ruskouluttaa oma henkilöstönsä yhdessä asetettujen FMN-vaatimusten mukaisesti. Näitä perustaitoja tulee sen jälkeen yhdessä harjoitella ja mitata osana FMN-ohjelman mukaisia harjoituksia. FMN:n koulutus- ja harjoitustoiminnan kehittäminen esitettiin työryhmän toimesta nostettavaksi koko projektin vastuulle, joko pysyvästi tai tilapäisesti. Koulutus- ja harjoitustoiminta esitettiin samalla jatkossa pysyvästi ja kiinteästi yhdistettäväksi osakokonaisuudeksi jo kalenteroituihin FMN-tapahtumiin.

Tulevaisuuden näkymiä

Seminaarin perusteella keskeinen kehitysalue on strateginen kommunikaatio, jota FMN-ohjelman ja sen merkitysten osalta tulee jatkossa tehostaa. Kyberpuolustuksen kytkeminen entistä tiivimmin FMN-ohjelmaan nähtiin myös tärkeänä. Muun muassa erilaiset tiedonvaihtokäytännöt sekä kybertapahtumien hallinta federoidussa ympäristössä koettiin tärkeiksi tulevaisuudessa ratkaistaviksi kysymyksiksi. FMN-suorituskykyjen yhdistäminen kiinteäksi osaksi operatiivista toimintaa ja suunnittelua oli myös yksi keskeisiksi tunnistetuista menestystekijöistä. FMN-osaaminen nähtiin myös vielä kehitettävänä osa-alueena. Systemaattisella, laadukkaalla koulutus- ja harjoitustoiminnalla nähtiin olevan suuri merkitys FMN-ohjelman ja sen mukaisten suorituskykyjen toimeenpanon onnistumisessa. FMN-ohjelman mukaisen, spiraalimaisen kehitystyön tiivis yhdistäminen kansallisiin kehittämisohjelmiin ja –hankkeisiin koettiin myös yhtenä tulevaisuuden kulmakivenä.

Havaituista kehittämisalueista huolimatta voidaan todeta, että ”FMN-juna” on tällä hetkellä mitä suurimmassa määrin raiteillaan ja kiihdyttämässä vauhtiaan kohti seuraavia väliasemia. FMN on tapa rakentaa FMN-jäsenten suorituskykyjä yhteentoimivaksi siten, että suorituskyky ja operatiivinen hyöty saavutetaan tehokkaasti. Sovitut määräajat takaavat yhdenaikaisesti valmistuvat valmiudet ja huolellinen tekninen testaus sekä harjoituksissa todennettava suorituskyky varmistavat tavoitteiden saavuttamisen. Luottamusta FMN-ohjelmaan osoittaa se, että Nato on edellyttänyt NRF-valmiusyksiköiltään FMN-yhteensopivuutta vuoden 2017 valmiusvuorosta lähtien. Samoin eFP-joukot (enhanced Forward Presence, Naton uudet valmiusjoukot Baltian maissa ja Puolassa) rakentavat operaatioverkkonsa FMN:n mukaisesti.

Suomi saa FMN:n myötä nyt ja tulevaisuudessa komentajille, operatiiviselle johdolle sekä joukoille modernin ja tehokkaan työkalun tehtäviensä täyttämiseksi. Ja kriisitilanteessa – tapahtuipa se omassa ympäristössämme tai muualla maailmalla - FMN mahdollistaa monikansallisten joukkojen optimaalisen tiedonvaihdon, johtamisen ja yhteistoiminnan. Tämä parantaa ratkaisevasti suorituskykyä ja operaatiotehokkuutta. Suomi osoitti myös tämän vuoden FMN- seminaarijärjestelyillään jälleen kerran omaa osaamistaan ja sitoutumistaan tähän johtamisjärjestelmien kannalta elintärkeääntyöhön. FMN-ohjelman ja sen mukanaan tuoman johtamisjärjestelmien yhteesopivuuden kannalta tulevaisuus näyttääkin tällä hetkellä erittäin valoisalta.

TEKSTI: KIMMO FRILANDER

Kybermaailma ja kansainvälinen oikeus

Internet – mikä se oikeastaan onkaan

Internetin ja WWW:n liberaalit henkiset juuret, koko olemus sekä erityisesti hallinnointitapa, tai lähinnä sen puute, antavat perustellun syyn varautua pahimpaan. Internetiä ei hallinnoi yksikään henkilö, yhtiö tai hallinnollinen toimija, vaan kyseessä on globaali tietoverkko tai ”verkkojen verkko”. Internet koostuu useista vapaaehtoisesti, mutta monimutkaisillakin kaupallisilla sopimuksilla, toisiinsa liitetyistä verkoista. Jokainen osaverkko voi sisäisesti määritellä omat sallitut menettelytapansa, kuitenkin paikallinen lainsäädäntö huomioiden. Yksityisten ja julkishallinnollisten toimijoiden yhteenliittymät hallinnoivat ainoastaan standardeja, joilla internet pysyy teknisesti yhteentoimivana. Yhtenäinen nimi- ja osoiteavaruus sekä tietyt tietoliikenne-protokollat ovat näistä parhaiten tunnetut.

Niin kauan kuin on ollut tietoliikennettä, on ollut myös hakkereita, ja heidän määrä ei tule vähenemään. Mutta miten määritellä onko hakkeri rikollinen vai turvallisuuden tutkija? Lain kirjaimen edessä asia on toki selvä, mutta eettisessä ja jopa filosofisessa mielessä asiat eivät välttämättä ole mustavalkoisia. Kenties provokatiivisestikin muotoillun kysymyksen taustalla ovat historialliset tapaukset eettisistä hakkereista, jotka ovat paljastaneet yhteisen hyvän eduksi tietoturva-aukkoja joilla olisivat voineet rikastua loppuelämäkseen. Yhtenä varhaisimmista voisi pitää Alan Turingia, yhtä tietojenkäsittelyn uranuurtajista. Hän hakeutui toisen maailmansodan keskellä vapaaehtoisena Enigman salauksen murtaneeseen tutkijaryhmään, ja toimi siinä ratkaisevassa roolissa.

Hakkeri voidaan yksinkertaistuksena määritellä teknisesti orientoituneeksi normaalia osaavammaksi tietokoneen käyttäjäksi, joka muokkaa sekä ohittaa tietojärjestelmän normaaleja toimintoja. Laillisesti toimiva ”white hat” hakkeri tekee tämän saadakseen aikaan jotain yleisesti hyödyllistä ja hyväksyttävää. Valkohattuisia työskentelee esimerkiksi yritysmaailman ja julkishallinnon palveluksessa. Laittomasti toimiva ”black hat” hakkeri aiheuttaa tarkoituksellisesti haittaa tietojärjestelmälle. Mustahattuisen motiivina voi olla esimerkiksi taloudellisen hyödyn tai anarkian tavoittelu.

Osaavien hakkereiden voimaa pelätään, mutta miten heidät saataisiin pysymään ”voiman” oikealla puolella? Parhaimmillaan valkohattuiset turvallisuuden tutkijat toimivat vertauskuvallisesti internetin immuunijärjestelmänä. Tiettyjen inhimillisten perustarpeiden täyttymisen jälkeen erilaiset motiivit vaikuttavat suuresti siihen mitä päätämme ja miten toimimme. Kiellot ja rajoitukset ovat osoittautuneet tehottomiksi, ainakin kun kyse on kaikkein osaavimmista yksilöistä sekä ryhmistä. Aivan uudenlaisen tutkimuksen paikka saattaisi olla sille, mikä saa hakkerin valitsemaan ”voiman” oikean puolen?

Kyber on vakiintunut sellaisten yhdyssanojen etuliitteeksi (esimerkiksi kyberrikollisuus), joilla kuvataan jonkin aiemmin tunnetun ilmiön tai asian esiintymistä kybermaailmassa, eli tietoverkoissa ja tietojärjestelmissä. Kreikan kielen kantasana ”kybereo” tarkoittaa ohjata, opastaa ja hallita. Voidaan siis todeta että ihmiskunnan ennusteet, ja pelotkin, tietojärjestelmien käytöstä jopa yhteiskunnallisen tason toimintojen ohjaamiseen sekä hallinnointiin ovat toteutuneet. Kybermaailma on, kuten tietojärjestelmäkin klassisesti määritellään, ihmisistä, datasta, tietoverkoista, tietoteknisistä laitteista ja ohjelmistoista muodostuva sosio-tekninen kokonaisuus - ekosysteemi. Internetin laajamittaisen käytön sekä kaupallistumisen myötä datan määrä on lisääntynyt eksponentiaalisesti ”analogiseen aikaan” verrattuna. Tiedonvälityksessä päivät ja viikot ovat muuttuneet minuuteiksi ja sekunneiksi. Datasta, informaatiosta ja tiedosta on kehittynyt öljyyn verrattava hyödyke ja kaupankäynnin kohde. Verkostoajattelu on laajentunut ”taitorakenteista” tietojärjestelmiin ja niiden mahdollistamiin sosiaalisiin verkostoihin. IoT:hen liittyen verkottuneiden laitteiden määrän kasvaminen tarkoittaa myös entistä suurempaa ”hyökkäyspinta-alaa”.

Sosiaalinen tietojenkäsittely ja globaali ”kyberturvattomuus”

Arabikevään kansannousujen yhteydessä jotkin valtiot yrittivät estää internetin käyttämisen kansalaisiltaan, mutta huonolla menestyksellä. Edes konkreettinen yhteyksien katkaiseminen ei auttanut, vaan aktivistit siirsivät tietoliikenteen muutaman sukupolven vanhempaan tekniikkaan. Aktivistiryhmät alkoivat esimerkiksi tarjota Egyptiläisille dial-up yhteyksiä Euroopan kautta. Dial-up yhteyksien numerot lähetettiin faxilla Egyptiläisiin yliopistoihin ja Internet kahviloihin, jotta ne olivat mahdollisimman laajan joukon saatavilla.

Koko sosiaalisen median olemassa olon ajan sitä on käytetty tavoilla, joita ei ole osattu ennakoida. Perinteiset instituutiot, jopa valtiot, ovat yllättyneet sosiaalisen media joukkovoimasta mm. radikalisoitumiseen ja terroristien rekrytointiin liittyen. Tiedusteluorga-

nisaatiot ovat hädin tuskin kyenneet seuraamaan paikallisten konfliktien ”viraalia” leviämistä globaaleiksi digitaalisessa muodossa. Osa syntyneistä ”kyberkonflikteista” on luonteeltaan sellaisia, että valtiot eivät joko tunnista rooliaan, tai niiltä puuttuu kyky sekä tahtotila osallistua asian ratkaisemiseen.

Internetin ”vertaisturvallisuuden” kehittämisestä on ajoittain esitetty idealistisia ajatuksia. Vertaisturvallinen Internet muodostuu yksilöistä, jotka ovat sitoutuneet toimimaan ”luotettuina henkilöinä” verkottuneessa maailmassa. Kannatan ajatusta, mutta en jaksa uskoa sen toteutumiseen. Ajatus sai kuitenkin minut palauttamaan mieleen mistä kansallisvaltiossa oikein onkaan kysymys.

”Vapaa kilpailu vapailla markkinoilla on saattanut kansallisvaltiot ja niiden hyvinvointitavoitteet uuteen asemaan. Kyky ohjata kansantaloutta on vähentynyt. Yhteinen etu ajoi 1990-luvulla valtioita ryhmittymään talousliitoiksi eri puolilla maailmaa. Suuntaus jatkuu 2000-luvulla kimmokkeena Kiina- ja Intia-ilmiöt. Kiina on jo sitä, mitä se oli 1800-luvun alkupuolellakin ennen imperialismin aikaa – maailman suurin tavarantuottaja.” (Opetushallitus, etälukio. 2015. Kansainväliset suhteet, Mihin tarvitaan kansallisvaltiota?)

”Maailmanhistoria ei anna aihetta kovin suureen optimismiin ihmiskunnan kyvykkyydestä ratkaista ongelmiaan rauhanomaisin keinoin. Yksi asia on kuitenkin varma: kilpailu maailmanpolitiikan näyttämöllä jatkuu, jatkuu, jatkuu…” (Opetushallitus, etälukio. 2015. Kansainväliset suhteet, epilogi)

”Jos kaikki kansat nykyään haluaisivat perustaa valtion, maailman kartta muuttuisi tilkkutäkiksi, eivätkä silti kaikki olisi tyytyväisiä. Rajasodat olisivat arkipäivää.” (Opetushallitus, etälukio. 2015. Kansainväliset suhteet, valtion suvereniteetti)

Globaalia tilannetta on todella haastava hahmottaa, varsinkaan tietoverkoissa. Kansallisvaltioiden asema perinteisessä mielessä on osin kyseenalaistettu, mutta lähes poikkeuksetta äärimmäinen voimankäyttö (asevoimat) on edelleen niiden vastuulla. Toisaalta valtioilla ei ole varsinaista hallinnollista roolia internetissä koskaan ollutkaan, tai ainakaan voimasuhteita ei ole julkisesti kerrottu. Tästä huolimatta valtioilla on ollut turvallisuuden takaamisen kannalta perusteltuja pyrkimyksiä olla edes selvillä siitä mitä verkossa tapahtuu.

Internet on siis rajaton maailma, jossa toimii ihmisiä ja ryhmittymiä ainakin yksityisillä, kaupallisilla, valtiollisilla, poliittisilla, sotilaallisilla, uskonnollisilla ja ideologisilla motiiveilla. Tämän kohtaamiseen perinteiset turvallisuusinstituutiot tarvitsevat substanssiosaamista – ihmisiä jotka elävät ja hengittävät tietoverkko-operaatioita.

Yleensä kyberuhkien ajatellaan kohdistuvan tietojärjestelmiin, mutta kybervaikuttamisella voidaan aiheuttaa myös aiemmin vain asevoimien kykyihin kuulunutta kineettistä tuhoa. Kyberuhkia voidaan jaotella yksityiskohtaisemmin hyökkäyksen toteuttavan tahon motiivien ja/tai menetelmien mukaan. Mielenkiintoista erityisesti kyberoperaatioiden näkökulmasta ovat laillisuusnäkökulmat sekä niihin liittyvät puolustajan toimivaltuuskysymykset. Kyberhyökkäysten kohteet voidaan jakaa esimerkiksi sotilaallisiin, poliittisiin ja yhteiskunnallisiin. Uhkakuvatarkastelussa eri näkökulmia yhdistäviksi tekijöiksi nousevat laillinen ja laiton tiedonhankinta sekä taloudellisen hyödyn tavoittelu.

Kyberhyökkäyksellä voidaan tarkoittaa rajoituksetta kaikkia oikeudettomia toimia, jotka kohdistuvat tietoverkkoihin, tietojärjestelmiin tai niissä oleviin tietoihin. Tällainen toiminta voi olla säädetty rikoslaissa rangaistavaksi, tai kansainvälisen oikeuden mukaan kiellettyä voimankäyttöä. Rikos voi kohdistua kybertoimintaympäristöön, tai se voi olla rikos joka on tehty kybertoimintaympäristöä hyödyntämällä. Oikeudellisen käsittelyn kannalta suurin haaste on YK:n määrittelemään hyökkäyskäsitteeseen liittyvä aseen käyttö. Kyberaseelle tai asejärjestelmille ei ole olemassa yksiselitteisiä määrittelyitä. Yksi tapa lähestyä asiaa on arvioida vaikuttiko tapahtuma tiedon ja/tai tietojärjestelmän luottamuksellisuuteen (confidentiality), eheyteen (integrity) tai käytettävyyteen (availability).

Useimmiten kyberoperaation tavoitteet voidaan yleistää oman tietoylivoiman tavoitteluun sekä vastustajan suoristuskykyjen lamauttamiseen. Uusia teknisiä keinoja ja menetelmiä syntyy tietojärjestelmien kehittämisen tahdissa, niille ominaista ovat nopeus ja ulottuvuus (reach). Kyberoperaation toteuttaminen on hyökkääjälle houkuttelevaa, koska kohde ja keinovalikoima muodostavat usein ”Low Risk – High Payoff” yhtälön. Suhteellisen pienillä resursseilla ja kiinnijäämisen riskillä voidaan aiheuttaa jopa kineettiseen vaikuttamiseen verrattavaa tuhoa.

Kybersodankäynnin osalta informaatioon kohdistuva vaikuttaminen näyttäisi olevan keskeisin yhdistävä tekijä, esimerkkeinä mm. tapahtumat Virossa 2007, Georgiassa 2008 ja Ukrainassa 2014 alkaen. Mielenkiintoista on myös pohtia, miksi fyysisiin tuhoihin johtavaa kybervaikuttamista ei ole vielä nähty. Onko tavoitteet saavutettu muilla, ns. perinteisillä, keinoilla? Halutaanko salata todellinen vaikuttamiskyky mahdollisesti vieläkin kriittisempiin operaatioihin? Vai onko taustalla pelko kybersodankäynnin eskaloitumisesta (vrt. ydinaseiden käyttö) hallitsemattomaksi?

Oikeuden käsitteet kybermaailmassa

Kansainvälisen oikeuden olemassaolon perustan luo valtioiden välinen poliittinen järjestelmä. Oikeus heijastaa toimintayhteisönsä olosuhteita, kulttuuriperinteitä ja näin ollen myös aikojen saatossa muodostuneita arvoja. Nämä kokonaisuutena määrittelevät kunkin aikakauden oikeuden kehittymistä. Oikeusjärjestyksen määrittelyssä syntyy oikeuksia ja velvollisuuksia, joita on säädeltävä. Säätely ja rauhanomainen valtioiden välinen yhteistyö laajentavat kansainvälisen oikeuden sisältöä. Kansainvälinen oikeus on vain niin hyvä kuin sitä kehittävät valtiot haluavat.

Globalisaatio on luonut monimutkaisia keskinäisriippuvuuksia nykyiseen maailmanjärjestykseen. Kestävyyskriisi ja valtiolliset, taloudelliset sekä aatteelliset jännitteet kiristyvät käsi kädessä. Toisen maailmansodan jälkeen nähtiin teollistumisen teknologisen tason nousu, kun ihmiskunta tyydytti ikiaikaisia liikkumisen teknologiautopioita. Osin sodan katalyysin ansiosta saavutettiin jopa fysiikan lakien rajoja. Siirtyminen tietoyhteiskuntaan on käytännössä tapahtunut, ja käynnissä on siirtymä ”ubiikkiyhteiskuntaan”. Ubiikkiyhteiskunnassa tietotekniikka on läsnä kaikkialla, ja sosiaalisen tietojen käsittelyn merkitys kasvaa.

Edellä kuvatulla kehityksellä on huomattava vaikutus oikeuden perus-

luonteeseen. Uudet toimintatavat luovat jännitteitä suhteessa olemassa oleviin oikeussääntöihin. Tällöin tulee selvittää voidaanko olemassa olevia tulkinta- ja soveltamiskäytäntöjä soveltaa, vai syntyykö tarvetta uudelle oikeussäätelylle.

Kansainvälisoikeudelliselle järjestelmälle on luonteenomaista, ettei siinä ole selkeää ylintä suvereenia tahoa tai pakkovallan käyttäjää. Tämä liittyy mielenkiintoisella tavalla aiemmin kuvaamiini Internetin ominaispiirteisiin, ilmiöihin, hallinnointiin ja uhkiin. Teknologisella puolella pääosin suuryritykset kaupallisine intresseineen luovat käytäntöjä. Kansainvälistä oikeussääntöjen ja niiden käyttösääntöjen muodostamaa oikeusjärjestelmää puolestaan muokkaavat valtiot. Poliittisten ja taloudellisten järjestelyiden sopiminen tapahtuvat eri foorumeilla, mutta käytännössä asiat kuitenkin kietoutuvat toisiinsa. Lisäksi sopimusteitse syntyy kansainvälistä tapaoikeutta ja/tai valtio-sopimuksia.

Valtion suvereniteetti eli täysivaltaisuus jaetaan sisäiseen ja ulkoiseen. Sisäinen suvereenisuus tarkoittaa sitä, että valtion sisäpuolella valtiovalta on edustaa korkeinta oikeudellista valtaa. Ulkoinen suvereenisuus tarkoittaa valtion vapautta päättää itsenäisesti suhteistaan toisiin valtioihin ja kansainvälisiin järjestöihin. Valtion toimivalta johdetaan suvereenisuudesta. Valtiolla on oikeus vastata (puolustautua) siihen kohdistuviin asevoiman käyttöä vähäisempiin toimiin sekä aseellisen voiman käyttöön. Oikeudelliset perusteet ovat yleisessä kansainvälisessä oikeudessa sekä YK:n peruskirjassa.

Oikeusalat kybermaailmassa

Sisältöjä koskevia sääntöjä (substantive law) on lukuisia, monikaan niistä ei välttämättä suoraan käsittele kybertoimintaympäristöä ts. tietojärjestelmiä ja -verkkoja. Jos sen sijaan kybervaikuttaminen aiheuttaa fyysisessä maailmassa havaittavia seurauksia, niin todennäköisesti suurin osa oikeusaloista on sovellettavissa. Rajatummassa kehyksessä tästä hyvä esimerkki on suomalaisen rikoslain välineneutraalius, mikä on osoittanut vahvuutensa tietoverkkorikosten oikeuskäsittelyissä.

Kansainvälisen oikeuden subjektius, ts. entiteetin ja yksikön määrittely, on haaste kybermaailmassa, koska perinteisesti kyseessä on valtio tai mahdollisesti kansainvälinen järjestö. Subjektille ominaiset oikeudet, velvollisuudet, vastuu ja kyvykkyydet ovat, jonkin toimijan niin halutessa, helpompi häivyttää kuin fyysisessä maailmassa. Aiemminkin tässä luvussa mainitut suuryritykset muodostavat kybermaailman kannalta mielenkiintoisen kokonaisuuden siitä huolimatta etteivät ne ole subjekteja, vaan sääntelyn kohteena olevia objekteja. Niiden toiminta, erityisesti Internetissä, ylittää valtiorajat. Yritysten resurssit saattavat olla suuremmat kuin pienimmillä valtioilla ja kokonaisuutena niiden toiminnalla voi olla tosiasiallisia valtiollisia vaikutuksia. Kansainvälisen oikeuden osalta keskeistä on se, että yrityksen toimien voidaan katsoa tapahtuvan myös valtion lukuun (attribution to). Tällöin toimista voi seurata valtiolle kansainvälisoikeudellinen valtiovastuu (state responsibility). Esimerkiksi valtionyritys voi kuitenkin syytöstilanteessa vedota valtioimmuniteettiin (state immunity), millä ne pyrkivät välttämään vieraan valtion tuomioistuimen.

Myöskään yleiskielessä kansalaisjärjestöinä tunnetut NGO:t (Non-Governmental Organzation) eivät ole subjekteja, vaan kansainvälisen oikeuden objekteja. Ne saattavat kuitenkin tuottaa informaatiota kansainväliseen päätöksentekoon (esim. Bellingcat), tai käyttää haktivismia omien päämäärien-sä tavoitteluun.

Kybermaailman tapahtumien oikeudellinen arviointi – esimerkkinä Viron Pronssisoturi tapaus

Globaalin verkottuneen maailman ristiriitojen ennaltaehkäisyyn ja kiistojen rauhanomaiseen ratkaisemiseen on oikeudellisia menettelyitä ja ”pelisääntöjä”, jos niitä vain halutaan käyttää. Reaktioita voidaan säädellä, ja voimankäyttöä rajoittaa. Jopa kansainvälisen kehityksen ennakointi on jossain määrin mahdollista. Kuitenkin aina välillä tapahtuu odottamattomia, ei-toivottuja, asioita. Miten tällaisen monimutkaisen globaalin kyberympäristön, missä ”mikään ei toimi – mutta kaikki järjestyy”, tapahtumia voisi arvioida oikeudellisesti? Valtiorajat ylittävien kansainvälisoikeudellisten tapahtumien arviointi on mahdollista, kun niitä tarkastellaan esimerkiksi seuraavien tekijöiden perusteella.

1) Tunnistetaan ja määritellään teko (tapahtuma), kohde sekä sen toteuttajat. Kyseessä voi olla myös tekemättömyys liittyen valtion vastuuseen. Syyksiluettavuus on kybermaailmassa haaste anonymisointi mahdollisuuksien vuoksi. Jos tekijä saadaan tunnistettua, arvioidaan onko tällä taholla aiempia vastaavia tekoja.

2) Selvitetään ja arvioidaan teon tavoitteet ja vaikutukset. Tämä on erityisen tärkeä vaihe, koska kyberaseiden/-asejärjestelmien laillisuuden määrittely on haastavaa. Arvioitavia seikkoja ovat mm. maalittaminen ja ihmisen sijainti päätöksentekoketjussa. Laittomuuteen viittaavia piirteitä ovat mm. vaikutuksen sattumanvaraisuus ja epäinhimillisyys, sodan oikeussääntöjen vastaiset ympäristötuhot, sekä ristiriidat kansainvälisten valtiosopimuksien ja tapaoikeuden kanssa. Kriteereinä voivat toimia esimerkiksi:

- Vakavuus (severity) suhteessa tietojärjestelmän luottamuksellisuuteen, eheyteen ja käytettävyyteen. Tiedusteltiinko haavoittuvuuksia, vai tehtiinkö tietomurto?
- Ilmenevätkö vaikutukset välittömästi, ja ovatko ne suorassa yhteydessä itse tekoon?
- Ilmeneekö sotilaallisen toiminnan elementtejä?
- Aiheuttiko teko vahinkoja ihmisille tai omaisuudelle, toisin sanoen voidaanko rinnastaa aseelliseen voimankäyttöön?

3) Selvitetään teon sekä tekijöiden avulla mahdollinen valtioyhteys. Yksi tapa tulkita asiaa on määritellä valtion hyötyä. Jos valtio hyötyy, asia menee valtion lukuun. Toisaalta valtion vastuu voi laueta myös huolenpitovelvollisuuden laiminlyönnistä. Tämä vaihe edellyttää kokonaisarviointia tavoitteiden suhteen.

4) Selvitetään mahdollisten useiden osatapahtumien ja toimintaympäristön yhteydet. Kyberoperaatioissa erityisesti reitityksen selvittäminen on keskeistä.

5) Kokonaisarvioinnissa tarkentavina kriteereinä voivat toimia esimerkiksi:

- Tekninen toteutus ja todistusaineiston kerääminen

- Mille oikeudenalalle asia kuuluu?
- Miten voidaan reagoida ja kenellä on toimivalta?

Oikeudellisen arvioinnin esimerkkinä käytän Pronssisoturin siirtoa Virossa, ja siihen liittyneitä tapahtumia huhti- ja toukokuussa 2007.

1) Tunnistetaan ja määritellään teko (tapahtuma), kohde sekä sen toteuttajat.

Operaatiossa nähtiin useita valtioon ja kansaan kohdistuneita informaatiovaikuttamisen keinoja, joihin tässä yhteydessä liitän laajasti katsoen myös mellakoinnin ja ilkivallan. Näillä luotiin epävarmuutta sekä pelkotiloja, ja toiminta laajeni pian tämän jälkeen myös tietoverkkoihin. Kohteena olivat niin valtion kuin yksityisenkin sektorin tietoverkot sekä tietojärjestelmät. Näiltä osin hyökkäyksen kriteeristö täyttyy.

2) Selvitetään ja arvioidaan teon tavoitteet ja vaikutukset.

Kyseessä oli operaation toteuttajan voimannäyttö sekä epävarmuuden ja pelkojen levittäminen kansalaisten keskuuteen. Ongelmia oli valtion rahaliikenteessä, pankkitoiminnoissa, media-alalla, valtion johdon tietojärjestelmissä sekä verkko-operaattoreiden järjestelmissä. Tästä syntyi lyhytaikaisia taloudellisia haittoja. Ei voitu soveltaa sodan oikeussääntöjä, koska ei syntynyt fyysistä vahinkoa. Myöskään YK:n peruskirjan ”Use of Force” ei täyttynyt. Kyse oli enemmänkin valtiollisen tason haitasta ja ”epämukavuudesta”.

3) Selvitetään teon sekä tekijöiden avulla mahdollinen valtioyhteys.

Joidenkin agitaattoreiden etninen tausta saatiin selvitettyä, ja muutama IP-osoite jäljitettiin Valtion X hallintoon. Operaation toinen vaihe tapahtui Valtiolle X myönteisten ryhmien tuella. Varsinainen tietoverkkovaikuttaminen oli kuitenkin hajautettu yli 170 maahan. Maakohtaisessa tarkastelussa suurin osa DDoS:ssa (palvelunestohyökkäys) käytetyistä koneista sijaitsi Egyptissä. Egyptillä ja Virolla ei ole asiaan liittyviä kiistoja, joten on arvioitu että syynä olivat vanhat, haavoittuvat ja mahdollisesti myös lisenssittömät ohjelmistot egyptiläisissä koneissa. Ne oli helppo kaapata hyökkäystä varten bottiverkon osaksi. Kaapattujen koneiden IP-osoitteet olivat pääosin yksityisiä.

4) Selvitetään mahdollisten useiden osatapahtumien ja toimintaympäristön yhteydet.

Järjestäytynyt, laaja ja teknisesti kehittynyt toiminta viittaa valtiollisten resurssien hyödyntämiseen. Osa operaation intensiivisimmästä vaiheesta osui Valtiolle X merkityksellisen toiseen maailmansotaan liittyvän päivämäärän yhteyteen. Kokonaisuutena vaikuttamiseen pyrkineen Valtion X asema jäi epäselväksi. Oliko tietoinen? Hyväksyikö hiljaa? Ohjasiko toimintaa? Internet mahdollisti riittävän oikeudellisen näytön edellyttämien todisteiden häivyttämisen. Toimivaltuuksien ja vastatoimien määrittely oli hankalaa hajautetun hyökkäyksen vuoksi.

Jatkuu seuraavassa numerossa.

Kirjoittaja Martti J. Kari on filosofian maisteri, eversti evp ja on Jyväskylän yliopiston opettaja ja väitöskirjatutkija. Hän oli vuosina 2014-2017 mukana valmistelemassa sekä sotilas- että siviilitiedustelulainsäädäntöä ja tiedustelun valvontaa.

TEKSTI JA KUVAT: MARTTI J. KARI

Sotilastiedustelulaki ja tietoverkkotiedustelu

Eduskunnassa käsittelyssä oleva sotilastiedustelulaki mahdollistaisi sotilastiedustelun toiminnan viidenneksi toimintaulottuvuudeksi muotoutuneessa kybertoimintaympäristössä ja näin lisäisi puolustuksemme uskottavuutta. Lisäksi sotilastiedustelulaki mahdollistaisi maamme alueellisen koskemattomuuden turvaamisen myös kybertoimintaympäristössä.

Sotilastiedustelulakia on valmisteltu jo yli viisi vuotta

Vuonna 2013 hyväksytyn kyberturvallisuusstrategian linjausten mukaan Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään. Sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Strategian mukaan Puolustusvoimat suojaa omat järjestelmänsä siten, että se kykenee suoriutumaan tehtävistään huolimatta kybertoimintaympäristön uhkista. Tämän varmistamiseksi kehitetään tiedustelu- ja vaikuttamiskykyä kybertoimintaympäristössä osana muun sotilaallisen voimankäytön kehittämistä. Toinen Puolustusvoimia koskenut strategian linjaus oli, että puolustusministeriön johdolla laaditaan kyberpuolustuskyvyn kehittämiseen ja käyttöön tarvittava toimivaltuussäännöstö. Ennen säännöstön luomista tuli arvioida sitä, oliko syytä luoda vastuuviranomaisille paremmat mahdollisuudet ennalta kerätä, koota ja saada tietoa kyberuhista ja niiden aiheuttajista. Huomiota tuli kiinnittää perusoikeuksina olemassa oleviin yksityisyyden suojaan ja luottamuksellisen viestin suojaan.

Kyberturvallisuusstrategian linjausten mukaisesti puolustusministeri asetti joulukuussa 2013 työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista. Työryhmään kuului edustajia eri ministeriöistä, puolustusvoimista ja suojelupoliisista. Työn käynnistyttyä työryhmän aihealue laajeni koskemaan tietoverkkotiedustelun lisäksi koko tiedustelutoimintaa, sisältäen sekä sotilas- että siviilitiedustelua. Työryhmän mietintö, ”Suomalaisen tiedustelulainsäädännön suuntaviivoja”, luovutettiin puolustusministerille tammikuussa 2015. Mietinnössä työryhmä esitti harkittavaksi, että hallitus käynnistäisi tarvittavat toimenpiteet tiedustelua koskevan säädösperustan luomiseksi.

Tasavallan presidentti Sauli Niinistö on antanut tukensa ja asettanut vaatimuksia tiedustelulainsäädännön ja tiedustelun suorituskykyjen kehittämiselle. Puhuessaan Suomen puolustuskyvyn varmistamisesta eduskunnassa vaalikauden päättäjäisissä 15.4.2015 tasavallan presidentti sanoi edessä olevan uuden haasteen, puolustuskykymme ajantasaisen suorituskyvyn varmistaminen. Presidentin mukaan kansallinen turval-

4 luku - Tiedustelumenetelmät
63 – 71 § Tiedonhankinta tietoliikenteestä

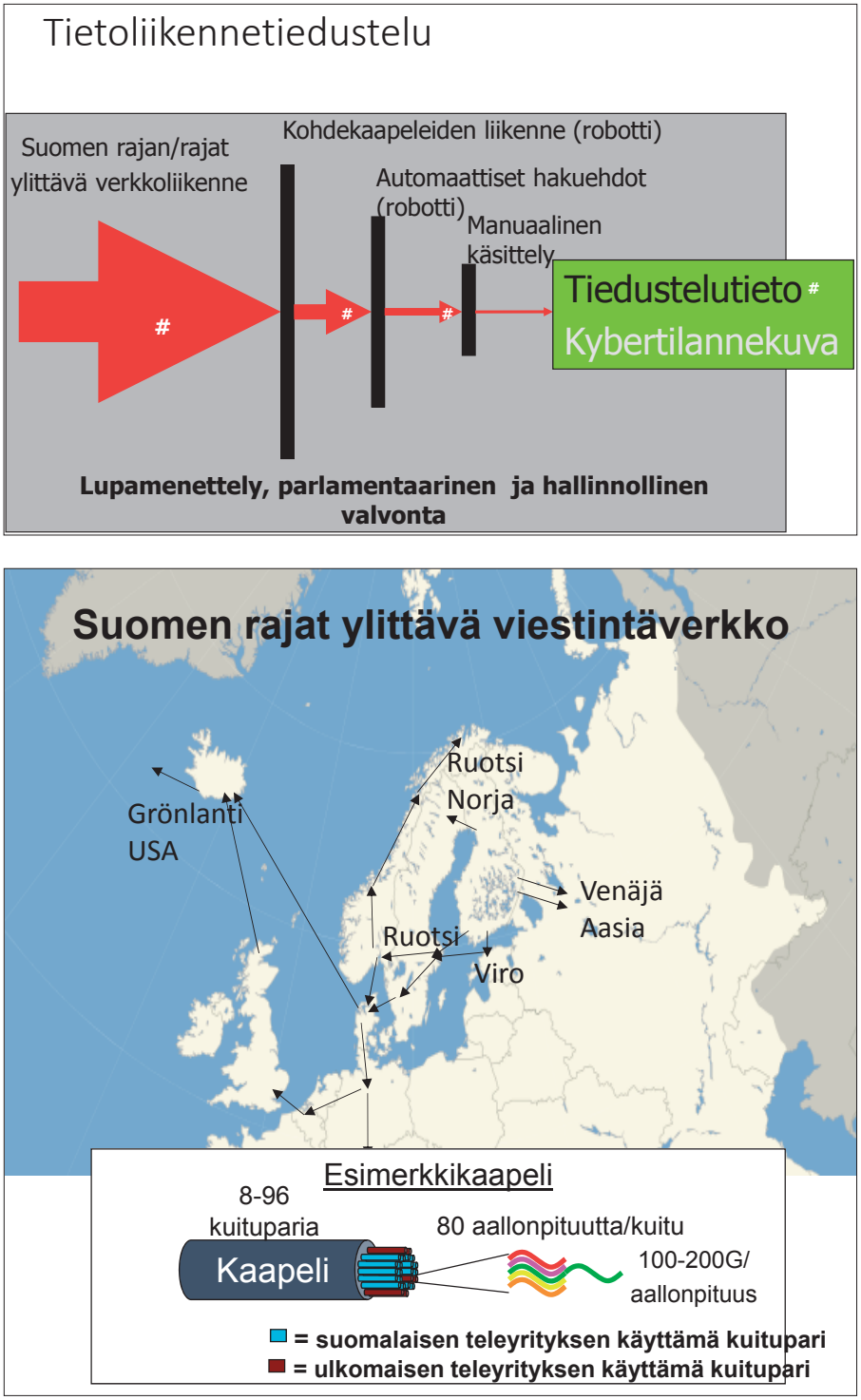
§	Menetelmä	Kuvaus	Päätös	Huom
63 - 64	Teknisten tietojen käsittely	Tietoliikenteen teknisten tietojen hetkellinen kerääminen tilastollista analyysia varten	Tuomioistuin	Ei tietoa, jolla voi tunnistaa luonnollisen henkilön 3 kk, Data hävitettävä, kun analyysi valmis
65 - 66	Valtiollisen toimijan tietoliikennetiedustelu	viestiliikenteen keräys Suomen rajan ylittävästä tietoliikenteestä hakuehtojen perusteella	Tuomioistuin (1)	6 kk, Hakuehtona ei Suomessa olevan henkilön telepäätelaitteen/-osoitteen yksilöiviä tietoja
67 - 68	Ei-valtiollisen toimijan tietoliikennetiedustelu	viestiliikenteen keräys Suomen rajan ylittävästä tietoliikenteestä hakuehtojen perusteella	Tuomioistuin (1)	6 kk, Välttämätöntä Hakuehtona ei Suomessa olevan henkilön telepäätelaitteen/-osoitteen yksilöiviä tietoja Haku ei viestin sisällön perusteella pl haittaohjelma
69	Kytkennän toteuttaminen	Kytkennän suorittaja kytkee ja ohjaa luvan mukaisen liikenteen PVTIEDL:lle (2)		
70	Tietoliikennetiedustelun toteutus Supon (3) puolesta	Tietoliikenteen teknisten tietojen hetkellinen kerääminen tilastollista analyysia varten Viestiliikenteen keräys Suomen rajan ylittävästä tietoliikenteestä hakuehtojen perusteella	Tuomioistuin (1) PVTIEDL hankkii luvat	PVTIEDL ei saa selvittää viestin sisältöä
71	Haittaohjelmatietojen luovuttaminen yrityksille ja yhteisöille	Sotilastiedusteluviranomainen saa luovuttaa tietoja haittaohjelmasta ja sen toiminnasta yrityksille, yhteisöille tai viranomaisille		Sotilaallinen maanpuolustus Kansallisen turvallisuuden suojaaminen Yrityksen tai yhteisön etujen turvaaminen

(1) = toiminta voidaan aloittaa pikatilanteessa sotilaslakimiehen tai perehtyneen virkamiehen päätöksellä, haettava lupa tuomioistuimesta 24 h sisällä
(2) = Puolustusvoimien Tiedustelulaitos

lisuus edellytti muun muassa ajantasaista tiedustelukykyä ja sen vaatimaa lainsäädäntöä. Kesäkuussa presidentti Niinistö muistutti, että verkkotiedustelu on tullut jäädäkseen ja jollei Suomella ole kykyä verkkotiedusteluun, ei ole kykyä suojautumiseenkaan.

Pääministeri Sipilän hallitusohjelman toukokuussa 2015 julkaistujen ulko- ja turvallisuuspoliittisten linjauksien mukaan kasvavat riskit ja uudet uhat edellyttivät yhteiskunnalta uudenlaista valmiutta ja varautumista. Hallitusohjelman mukaan hallitus vahvisti kokonaisturvallisuusajattelua kansallisesti, EU:ssa ja kansainvälisessä yhteistyössä. Tämä koski erityisesti uusien ja laajaalaisten uhkien kuten hybridivaikuttamisen, kyberhyökkäysten ja terrorismin torjuntaa. Hallitus esitti linjauksissaan säädösperustaa ulkomaantiedustelulle ja tietoliikennetiedustelulle. Hallituksen linjauksessa toistettiin kyberturvallisuusstrategiassa esitetty vaatimus kiinnittää huomiota perus†ja ihmisoikeuksien toteutumiseen.

Hallituksen linjausten mukaisesti puolustusministeriö asetti 1.10.2015 hankkeen ja perusti työryhmän, jonka tehtävänä on valmistella ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Sisäministeriö asetti lokakuun alussa oman työryhmänsä valmistelemaan ehdotusta siviilitiedustelua koskevaksi lainsäädännöksi. Ryhmien työn lähtökohtana oli ”Suomalaisen tiedustelun suuntaviivoja”- mietintö. Työryhmien toimikausi oli 1.10.2015-31.12.2016. Oikeusministeriö asetti tiedustelun valvontaa pohtineen työryhmän. Työryhmissä oli mukana kaikkien asianosaisten ministeriöiden ja muiden organisaatioiden, kuten suojelupoliisin ja pääesikunnan, samoin kuin elinkeinoelämän, yliopistomaailman ja lakimiesliiton edustajia. Työryhmät kokoontuivat joka toinen viikko käsittelemään sihteeristöjen kirjoittamia lakiesitysluonnoksia, kuulemaan asiantuntijoita ja koordinoimaan työtä muiden työryhmien kanssa. Työn etenemistä seurasi parlamentaarinen seurantaryhmä, jossa oli edustajat kaikista eduskuntapuolueista. Ryhmän tehtävänä oli pitää omat eduskuntaryhmänsä tietoisena lakivalmistelusta ja lakien tulevasta sisällöstä. Lisäksi parlamentaarinen seurantaryhmä antoi työryhmille lakien valmisteluun liittyviä linjauksia.



Sotilas- ja siviilitiedustelutyöryhmien toimikautta jatkettiin helmikuun 2017 lopulle, jotta työryhmien esitykset valmistuivat samaan aikaan kuin tiedustelun valvontaa pohtineen työryhmän esitys. Lakiesitysluonnosten valmistuttua käynnistyi laaja lausuntokierros, jonka tulokset huomioitiin, kun lakiesitykset hiottiin syksyllä 2017 lopulliseen muotoonsa. Lakiesitykset annettiin eduskunnalle tammikuussa 2018, ja huhtikuussa 2018 esitykset ovat eduskunnassa valiokuntakäsittelyssä. Työryhmien työn käynnistyessä syksyllä 2015 tiedustelulakeja oli siis valmisteltu jo kolme vuotta, koska kyberturvallisuusstrategian valmistelu oli aloitettu vuonna 2012. Eduskuntakäsittelyyn tammikuussa tulleen sotilastiedustelulakiesityksen valmistelu ja sitä tukeva pohjatyö on kestänyt kuusi vuotta, joten esitystä ei voi väittää liian nopeasti valmistelluksi.

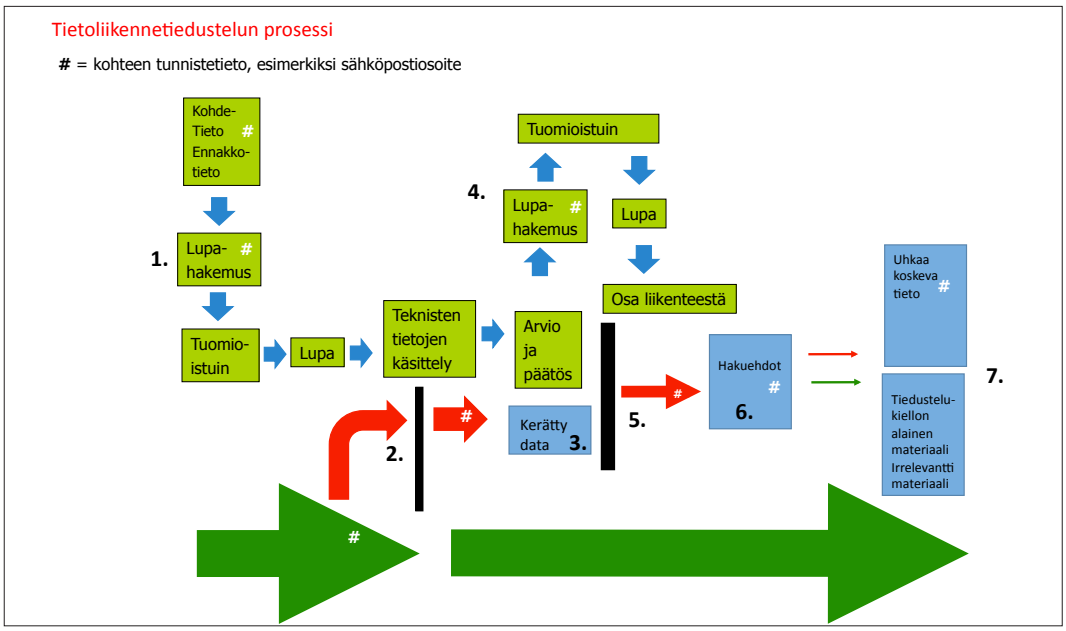
Muuttunut toiminta-ympäristö ja sen tuomat haasteet

Puolustusvoimien tehtäviin kuuluu maamme alueellisen koskemattomuuden, kansan perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen. Sotilastiedustelu muodostaa tilannekuvaa lähialueemme sotilaallisesta toiminnasta ja tuottaa tarvittaessa ennakkovaroituksen Suomeen kohdistuvasta sotilaallisesta uhasta. Sotilastiedustelu tuottaa tilannekuvaa myös alueilta, missä suomalaisia joukkoja osallistuu kriisinhallintaoperaatioihin ja antaa ennakkovaroituksen kriisinhallintajoukkoon kohdistuvista uhista. Sekä kotimaan puolustukseen, että kriisinhallintaan liittyvien tehtävien toteuttamisessa sotilastiedustelu käyttää tietojen keräämiseen myös signaalitiedustelua.

Sotilastiedustelun ja signaalitiedustelun toimintaympäristö on muuttunut sadassa vuodessa kaksiulotteisesta viisiulotteiseksi. Lentokone muutti ensimmäisen maailmansodan myötä toimintaympäristön kolmiulotteiseksi. Avaruuden valloitus 1950-luvulta alkaen lisäsi toimintaympäristöön neljännen ulottuvuuden. Kolmekymmentä vuotta sitten käynnistynyt digitalisaatio on luonut toimintaympäristöömme viidennen ulottuvuuden. Digitalisaatio ja kyberulottuvuuden muotoutuminen viidenneksi toiminta-alueeksi ovat tuonut mukanaan uusia uhkia. Yhdysvaltojen edellinen kansallinen tiedustelujohtaja James Clapperin mukaan muutos on tapahtunut nopeammin kuin kykenemme ymmärtämään muutoksen kaikkia vaikutuksia turvallisuuteemme.

Tietoverkkovakoilu ja tietoverkkovaikuttamisen valmistelut ovat jo nyt muuttuneet osaksi uutta normaalia. Sotilastiedustelun mahdollisuudet kerätä tiedustelutietoa ovat heikentyneet, koska osa tilannekuvan muodostamiseen ja ennakkovaroituksen antamiseen tarvittavasta kohteiden kommunikaation seuraamiseen perustuvasta tiedosta on kadonnut eetteristä perinteisen signaalitiedustelun ulottumattomiin kaapeleihin ja tietoverkkoihin ja lainsäädäntömme ei mahdollista kohteen kommunikaation seuraamista kybertoimintaympäristössä.

Yhtä tärkeää kuin kohteiden kommunikaation seuraaminen tietoverkoissa on toimintaympäristötietoisuuden muodostaminen kybertoimintaympäristöstä. Ilman pääsyä kybertoimintaympäristöön ei pystytä muodostamaan kuvaa kybermaailman normaaleista uhkaan liittyvistä ilmiöistä eikä havaitsemaan ja tunnistamaan maahamme kyberympäristössä tai sen kautta kohdistuvia uhkia. Lainsäädäntömme ei mahdollista tällä hetkellä kybervakoilun ja kybervaikuttamisen valmistelun havaitsemiseen tähtääviä toimintoja. Lainsäädännön puutteista johtuen puolustusvoimat ei kykene toteuttamaan maamme alueellista koskemattomuuden turvaamiseen liittyviä tehtäviään kybertoimintaympäristössä.



Vihreä nuoli on maamme rajan tietyllä ajan hetkellä ylittävä tietoliikenne. Kohteen kommunikaation tunnistamisen mahdollistava ominaispiirre on merkitty symbolilla #. Tämä ominaispiirre voi yksinkertaisimmillaan olla esimerkiksi sähköpostiosoite.

1. Tiedusteluviranomainen hakee tuomioistuimelta luvan teknisten tietojen käsittelyyn löytääkseen kaapelin, kuidun tai aallonpituuden, mistä kyseinen kommunikaatio on kerättävissä.

2. Tiedusteluviranomainen toteuttaa tuomioistuimen antavan luvan mukaisen teknisten tietojen käsittelyn

3. Teknisten tietojen käsittelyssä syntyvä materiaali hävitetään analyysin jälkeen

4. Kun kohteen kommunikaatio analyysin perusteella löytyy, haetaan ko liikenteeseen keräyslupa ja keräys aloitetaan.

5. Kytkennän suorittaja kytkee tiedusteluviranomaiselle vain luvan mukaisen kuidun (vast) liikenteen

6. Tiedusteluviranomainen toteuttaa ko liikenteeseen haun tuomioistuimen hyväksymien hakukriteerien perusteella

7. Irrelevantti ja tiedustelukiellon alainen materiaali hävitetään ja tiedustelutieto siirretään analyysiin.

Tietoverkkotiedustelu

Nyt eduskunnan käsittelyssä olevalla olevassa laissa sotilastiedustelun kohteet rajataan tarkasti puolustusvoimien tehtävien toteuttamiseen liittyviin kohteisiin. Lakiesityksen mukaan sotilastiedustelu saa hankkia tietoa alla mainituista kohteen toiminnoista,

mikäli toiminta on luonteeltaan sotilaallista:

1) vieraan valtion asevoimien ja niihin rinnastuvien järjestäytyneiden joukkojen toiminta ja toiminnan valmistelu;

2) Suomen maanpuolustukseen kohdistuva tiedustelutoiminta;

3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö;

4) vieraan valtion sotatarvikkeiden kehittäminen ja levittäminen;

5) kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi;

6) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta;

7) Suomen kansainvälisen avun antamisen ja kansainvälisen muun toiminnan turvallisuutta uhkaava toiminta.

Lisäksi tiedustelumenetelmällä saadaan hankkia tietoa vieraan valtion toiminnasta tai muusta sellaisesta toiminnasta, joka voi vaarantaa Suomen maanpuolustusta tai yhteiskunnan elintärkeitätoimintoja.

Lakiesityksellä pyritään mahdollistamaan puolustusvoimien, ja erityisesti sotilastiedustelun toimintamahdollisuudet kybertoimintaympäristössä. Sotilastiedusteluviranomaisille, joita ovat Puolustusvoimien tiedustelulaitos ja pääesikunta, esitetään valtuuksia muun muassa tietoverkkotiedusteluun. Tietoverkkotiedustelu tarkoittaa kybertoimintaympäristössä tapahtuvaa tiedustelua, jolla hankitaan tietoja kohteista ja sodan aikana hyökkääjästä poliittisen ja sotilaallisen päätöksenteon tueksi, tilannekuvan muodostamiseksi, ennakkovaroituksen tuottamiseksi ja maalittamisen tueksi. Tietoverkkotiedustelu jakautuu tietojärjestelmätiedusteluun ja tietoliikennetiedusteluun ja on osa signaalitiedustelua.

Tietojärjestelmätiedustelu tarkoittaa tietoteknisin menetelmin suoritettavaa tietojen hankkimista kohteiden tietojärjestelmistä eli tunkeutumista kohdeorganisaation tietojärjestelmään, tiedon keräämistä kyseisestä tietojärjestelmästä ja tiedon kotiuttamista siten, että tiedonkeruu ei paljastu. Tietojärjestelmätiedustelussa tiedonhankinta kohdistuu rauhan aikana kohteen ja sodan aikana vastustajan informaatiojärjestelmiin tiedonhankintasovellusten avulla. Sodan aikana tapahtuvaan kybervaikuttamiseen tarvittavien tietojen keräys ei ole mahdollista ilman perusvalmiudessa tehtävää tietojärjestelmätiedustelua. Lisäksi tietojärjestelmätiedustelun tavoitteena on luoda suojautumisen ja vaikuttamisen edellyttämä toimintaympäristötietoisuus, tiedustelutieto ja maalittamistukitieto.

Tällä hetkellä rikoslakimme kieltää tietojärjestelmätiedustelun kaltaisen toiminnan tietomurtona. Valmisteilla olevan sotilastiedustelulain mukaan Puolustusvoimien tiedustelulaitos saa kohdistaa tiedustelun kohteena olevan organisaation tietojärjestelmään tietojärjestelmätiedustelua, jos sillä voidaan olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta. Pääesikunnan tiedustelupäällikkö päättää tietojärjestelmätiedustelusta. Koska tietojärjestelmätiedustelu, eli tunkeutuminen kohdeorganisaation tietojärjestelmään, voi olla ulkopoliittisesti sensitiivistä, tietojärjestelmätiedustelua toteuttaa vain Puolustusvoimien tiedustelulaitos tiedustelupäällikön päätöksellä. Lisäksi sotilastiedusteluviranomaisen on pidettävä puolustusministeriö tietoisena käynnissä olevasta tietojärjestelmätiedustelusta.

Tietoliikennetiedustelu tarkoittaa Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tuomioistuimen luvalla tapahtuvaa tietoliikenteen automatisoituun erotteluun perustuvaa teknisestä tiedonhankintaa sekä hankitun tiedon käsittelyä. Käytännössä tämä tapahtuisi siten, että teleoperaattorin ja Puolustusvoimien tiedustelulaitoksen välissä toimiva kytkijä ohjaa tiedusteluviranomaisella tuomioistuimen luvan mukaisen osan tietoliikenteestä. Kyseiseen tietoliikenteen osaan tiedusteluviranomainen kohdistaisi tuomioistuimen luvan mukaisten hakuehtojen mukaisen haun. Tietoliikennetiedustelu pyritään kohdistamaan mahdollisimman tarkasti, jotta kerätyssä materiaalissa olisi vain kohteeksi tarkoitetun organisaation tai muun kohteen liikennettä.

Tietoliikennetiedustelun kohdentaminen tapahtuu useassa eri vaiheessa. Tiedusteluviranomaisella tulee olla ennen toiminnan käynnistämistä jokin tieto, jonka mukaan keräys voidaan kohdistaa. Tämä tieto voi yksinkertaisemmassa tapauksessa olla esimerkiksi kohteen käyttämä sähköpostiosoite tai kohteeseen liitettävissä oleva ip-osoite. Ennen varsinaisen keräyksen alkua Puolustusvoimien tiedustelulaitos voi kerätä ja tallentaa hetkellisesti tietoliikenteen teknisiä tietoja ja käsitellä kerättyjä tietoja tilastollista analyysia varten. Tästä keräyksestä käytetään nimitystä teknisten tietojen käsittely. Teknisten tietojen käsittely toteutetaan tuomioistuimen myöntämän luvan perusteella ja sen tarkoitus on selvittää, onko teknisten tietojen käsittelyn kohteena olevassa kuidussa tai aallonpituudessa kohteen kommunikaatioita. Tuomioistuimen antama lupa on voimassa kolme kuukautta. Tilastollisen analyysin perusteella ei saa syntyä tietoa, jonka perusteella olisi mahdollista tunnistaa yksittäinen luonnollinen henkilö. Kerätyt ja tallennetut tekniset tiedot on hävitettävä sen jälkeen, kun analyysin tulos on selvillä.

Jos teknisten tietojen käsittelyssä tehty analyysi osoittaa, että kyseisessä tietoliikenneyhteydessä on kohdeorganisaation liikennettä, haetaan tuomioistuimelta lupa varsinaiseen keräykseen. Keräyksen kohteena voi olla valtiollisen toimijan tai ei-valtiollisen toimijan kommunikaatio. Keräysluvassa on eritelty se verkon osa (kaapeli, kuitu tai aallonpituus), johon keräys voidaan kohdistaa sekä hakuehdot, joiden mukaan haku kohdistetaan. Luvan voimassaoloaika on kuusi kuukautta. Hakuehtona ei saa käyttää Suomessa oleskelevan henkilön hallussa olevan telepäätelaitteen yksilöiviä tietoja. Muuhun kuin valtiolliseen toimijaan kohdistettavassa keräyksessä hakuehtona ei saa käyttää viestin sisältöä vaan ainoastaan teknisiä tietoja. Valtiolliseen toimijaan ja haittaohjelmaan kohdistettavassa keräyksessä hakuehdot voidaan lakiehdotuksen mukaan kohdistaa myös viestin sisältöön.

Teleoperaattorin ja tiedusteluviranomaisen välissä toimiva kytkennän suorittaja kytkee Puolustusvoimien tiedustelulaitokselle luvan mukaisen osan liikenteestä. Operatiivisista ja kustannussyistä, ja keräyksen mahdollisimman hyvän kohdentamisen vuoksi tiedusteluviranomaisella ohjattava osa liikenteestä pyritään pitämään mahdollisimman pienenä. Tähän liikenteen osaan toteutetaan varsinainen haku tuomioistuimen hyväksymien hakuehtojen mukaisesti. Keräyksen tuloksena syntyy kolmenlaista materiaalia. Suurin osa haun tuottamasta materiaalista on tiedustelutietoa. Osa kerätystä materiaalista ei liity tiedustelutehtävään vaan se on tehtävän kannalta irrelevanttia materiaalia. Kolmas ryhmä on

tiedustelukiellon alaista materiaalia, millä tarkoitetaan laissa erikseen mainittujen henkilöiden, kuten pappien ja muiden uskontoryhmien vastaavien sielunhoitajien, lakimiesten ja lääkärien ammattinsa harjoittamisen yhteydessä käymää kommunikaatiota. Irrelevantti ja tiedustelukiellon alainen materiaali hävitetään. Tiedustelutietoa sisältävä materiaali siirretään edelleen analyysiin ja sitä kautta osaksi tilannekuvaa ja muita tiedustelun tuotteita. Asiakkaan saamassa tiedustelutuotteessa ei ole mainintaa siitä, että kyseisen tuotteen raakatietoa on kerätty tietoliikennetiedustelulla.

Sotilastiedustelulakiluonnoksen ja lakiluonnoksessa tietoliikennetiedustelusta siviilitiedustelussa määritetään, että Puolustusvoimien tiedustelulaitos toteuttaa suojelupoliisin tietoliikennetiedustelun. Suojelupoliisi voi antaa Puolustusvoimien tiedustelulaitokselle toimeksiantoja sekä teknisten tietojen käsittelyä että varsinaista tietoliikennetiedustelun keräystä varten. Sotilastiedusteluviranomainen ei saa selvittää suojelupoliisin puolesta kerätyn materiaalin sisältöä vaan kerätty raakamateriaali annetaan suojelupoliisille keräyksen jälkeen.

Lakiesityksen mukaan sotilastiedusteluviranomainen saa tiedustelupäällikön päätöksellä luovuttaa tietoliikennetiedustelulla hankittuja tietoja haittaohjelmasta yrityksille, yhteisöille ja viranomaisille, mikäli tietojen luovuttaminen on tarpeen maanpuolustuksen kannalta tai esimerkiksi yrityksen etujen turvaamiseksi. Lisäksi sotilastiedusteluviranomaisen tulee välittömästi ilmoittaa keskusrikospoliisille havaitsemansa rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Tällaisia rikoksia ovat muun muassa murha, sotarikos, rikos ihmisyyttä vastaan, maanpetos, törkeä huumausainerikos ja törkeä lapsen seksuaalinen hyväksikäyttö. Sotilastiedusteluviranomainen saa ilmoittaa keskusrikospoliisille tietoliikennetiedustelulla havaitsemansa rikokset, joista ankarin rangaistus on vähintään kolme vuotta vankeutta. Näitä ovat muun muassa törkeä viestintäsalaisuuden loukkaus, terroristisessa tarkoituksessa tehtävän rikoksen valmistelu ja pakottaminen seksuaaliseen tekoon.

Tietoliikennetiedustelu ja perusoikeudet

Tiedustelu ei saa loukata perustuslaissamme taattuja perusoikeuksia, sen pitää perustua lakiin, tiedustelun on palveltava hyväksyttyjä tarkoitusperiä, sen on oltava välttämätöntä ja saavutetun hyödyn tulee olla suhteessa suurempi kuin haittojen. Tiedustelun tulee olla läpinäkyvää, mihin kuuluu muun muassa tiedonannot anotuista, hyväksytyistä ja hylätyistä keräyspyynnöistä ja kansalaisten informointi keräyksen luonteesta ja siihen liittyvästä lainsäädännöstä. Riippumattoman valvontaelimen tulee varmistaa toiminnan läpinäkyvyys ja laillisuus. Valvontaorganisaatiolla tulee olla pääsy keräyksen laillisuuden todentamiseksi tarvittavaan informaatioon. Tämä on ollut jo tiedonhankintalakityöryhmän mietinnön johtoajatus. Mietinnössä korostetaan, että tietoliikennetiedustelukeräyksen tulee perustua lupaan, jonka riippumattoman tuomioistuin myöntää varmistuttuaan, että keräys on oikeutettua, riittävän rajattua ja täsmällisesti kohdennettua. Mietinnön johtoajatukset on sisällytetty tiedustelulakiesityksiin.

Sähköisen viestinnän vapautta kannattavien järjestöjen laatimien periaatteiden mukaan tietoliikenteen valvontaan liittyvien yksityisyyden rajoitusten tulee perustua lakiin. Valvontaa saa suorittaa vain tehtävään määrätty viranomainen. Toimenpiteitä ei saa kohdistaa esimerkiksi kohteen rodun tai poliittisen mielipiteen perusteella eikä muuten syrjivästi. Tietoliikennettä saa tiedustella vain, jos se on välttämätöntä eikä tarvittavan tiedon hankkimiseen ole muuta keinoa tai muut keinot loukkaisivat yksilönsuojaa. Keräyksestä saatava hyöty ja sen aiheuttamat haitat tulee arvioida ennen keräyspäätöksen tekoa. Edellä mainitut periaatteet ovat yhtenevät puolustusvoimien tietoverkkotiedustelun kehittämisajatuksen kanssa ja ne on huomioitu lakien valmisteluvaiheessa. Tietoliikennetiedustelu on viimesijainen keino eli sitä käytetään, mikäli kohteesta ei muuten saada kerättyä tiedustelutietoja.

Tietoliikennetiedustelu ei ole verkkoeikä massavalvontaa eikä se kohdistu kaikkeen verkkoliikenteeseen. Tarkoituksena ei ole valvoa tietoverkkoja, vaan löytää luvanvaraisten hakuehtojen perusteella maan rajat ylittävästä tietoliikenteestä tiedustelutiedon kannalta oleellista liikennettä. Perusoikeuksiin kuuluvan luottamuksellisen viestin sisällön salaisuuden loukkaamattomuus varmistetaan sillä, että tietoliikennetiedustelua toteutetaan valvottuna riippumattoman tuomioistuimen myöntämän luvan perusteella. Lupa myönnetään, mikäli tiedusteluviranomainen perustelee tarpeen kerätä tiedustelutietoa ja kuvaa hakuehdot riittävän tarkasti, jotta voidaan varmistua, että keräys kohdistuu oikein. Massavalvontamahdollisuus rajataan pois sillä, että tiedusteluviranomainen ei pääse suoraan kiinni tietoliikenteeseen vaan ulkopuolinen kytkennän toteuttaja ohjaa tiedusteluviranomaiselle vain tuomioistuimen luvan mukaisen liikenteen osan.

Sotilastiedustelulaki on erittäin tervetullut, vaikka se on yli vuosikymmenen myöhässä. Tullessaan voimaan sotilastiedustelulaki mahdollistaa sotilastiedustelun toiminnan aloittamisen kybertoimintaympäristössä ja näin osaltaan mahdollistaa alueellisen koskemattomuuden valvonnan ja turvaamisen myös viidennessä toimintaympäristössä ja lisää puolustuksemme uskottavuutta huomattavasti.

TEKSTI JA KUVAT: SAMULI TERÄMÄ

Viestiupseeriyhdistyksen kevätkokous

Viestiupseeriyhdistys kokoontui kevät kokoukseensa Karjalan prikaatiin runsaslukuisena. Paikalla oli noin 40 henkeä kauniissa keväisessä säässä. Tilaisuus alkoi kahvilla ja suolapalalla Karjalan prikaatin sotilaskodissa, mistä siirryttiin prikaatin esikuntarakennukseen ja Viipurisaliin.

Karjalan prikaatin esikuntapäällikkö everstiluutnantti Jarmo Vähätiitto ilmoitti Viestiupseeriyhdistyksen kokoukseen osallistuvan joukon prikaatin komentajalle Prikaatikenraali Pasi Välimäelle, joka avasi tilaisuuden ja kertoi tunnuslukuja prikaatin (KARPR) toiminnasta, kalustosta ja toimintaympäristöstä.

Everstiluutnantti Vähätiitto piti prikaatin esittelyn. KARPR:n historia alkoi valmiusyhtymä konseptista ja on kehittynyt vähitellen nykytilaan. Juuret prikaatilla ovat kuitenkin jo Kustaa II Adolfin ajoilta, Karjalan Rykmentin perustamisesta 6.5.1618 eli 400-vuoden takaa. Prikaatin tehtävien ja organisaation esittelyn jälkeen esiteltiin tarkemmin prikaatiin liittyviä tunnuslukuja. Lisäksi Vähätiitto esitteli alueen infrastruktuurin kehittämistä ja tulevaisuutta. Pääpaino esittelyssä oli KARPR:n harjoitus- ja koulutusjärjestelmän esittelyssä sekä M18-johtamisjärjestelmän käyttöönotossa. Koulutusjärjestelmän muutos 2020-luvulla, joka on kokeilukäytössä Kainuun prikaatissa, laajennetaan koko valtakuntaan, kun kokemukset ja mahdolliset korjaustarpeet on huomioitu. Koulutusjärjestelmästä siirryttiin sujuvasti joukkojen käytettävyyden esittelyyn eli miten koulutetulla joukolla operoidaan harjoitusjärjestelmän puitteissa. Esikuntapäällikkö toi esille myös varusmiessaapumiserittäin esiintyviä haasteita, mutta korosti kuitenkin pääosan suorittavan palveluksensa mallikkaasti sekä kuinka varusmiehet ovat lähentyneet henkilökuntaa ja myös toisin päin.

Maavoimien valmius ja Karjalan prikaatin toiminta sen osana perustuu sen joukkorakenteeseen, materiaaliin, henkilöstöön ja muihin resursseihin. Prikaatissa korostuu valmiuden ylläpidossa yhteistoiminta ja yhdessä tekeminen kaikkien aselajien voimin ja

Karjalan Prikaatin komentajan avaus.

Esikuntapäällikön esitys.

Kapteeni Koskinen esitteli M18 -järjestelmää.

Kokousväki tutustuu M18-järjestelmään.

Kokouksen puheenjohtajana toimi Asko Inkilä ja sihteerinä Harri Reini.

Veli-Pekka Kuparinen esitelmöi Kouvolan varuskunnan historiasta.

Kokouksen jälkeen kokousväki nautti maittavan päivällisen.

Paikalla oli runsaslukuinen joukko Viestiupseeriyhdistyksen jäseniä.

kumppaneiden kanssa. Valmiusyksikkökoulutuksen kokemukset ovat olleet positiivisia ja palaute joukolta on ollut korkealla tasolla. Esittelyn jälkeen oli kysymyksien ja vastauksien vuoro. Kokousyleisö kyseli aktiivisesti mm. miten yhteiskunnan muutos näkyy varusmiesaineksessa ja suhteessa koulutukseen.

Yleisesittelyn jälkeen siirryttiin KARPR:n JOJÄ-hallille tutustumaan M18-järjestelmään, jota esitteli asiantunteva henkilöstö kapteeni Petri Koskisen johdolla. Nähtävillä ja tutustuttavana olivat M18 järjestelmään kuuluvat viestiasemat A, C ja E sekä komentopaikan laitesuoja että verkonhallinta-ajoneuvo. Lyhyen alkuesittelyn jälkeen kokousväellä oli mahdollisuus tutustua lähemmin kalustoon ja kysellä tarkentavia kysymyksiä. Esittelyn jälkeen siirryttiin takaisin prikaatin esikunnan tiloihin, missä aloitettiin varsinainen kevät kokous.

Viestiupseeriyhdistyksen kevätkokous 2018 vietiin läpi esityslistan mukaisesti. Kokouksen puheenjohtajaksi valittiin Asko Inkilä. Kokouksessa käsiteltiin vuoden 2017 toimintakertomus ja tilinpäätös. Jäsenistön määrä oli hieman vähentynyt, ollen tällä hetkellä yhteensä 1026 henkeä. Kokouksessa todettiin mm. Viestiupseeriyhdistyksen järjestämien seminaarien tarpeellisuus myös jatkossa. Seminaarit järjestetään joka toinen vuosi ja seuraavan kerran vuoden 2019 helmikuussa.

Taloudellisen tilanteen todettiin olevan vakaa. Kokouksessa yhdistyksen uudeksi kunniajäseneksi kutsuttiin everstiluutnantti evp Martti Aho. Viestimies-lehti onnittelee lämpimästi kunnianosoituksen johdosta.

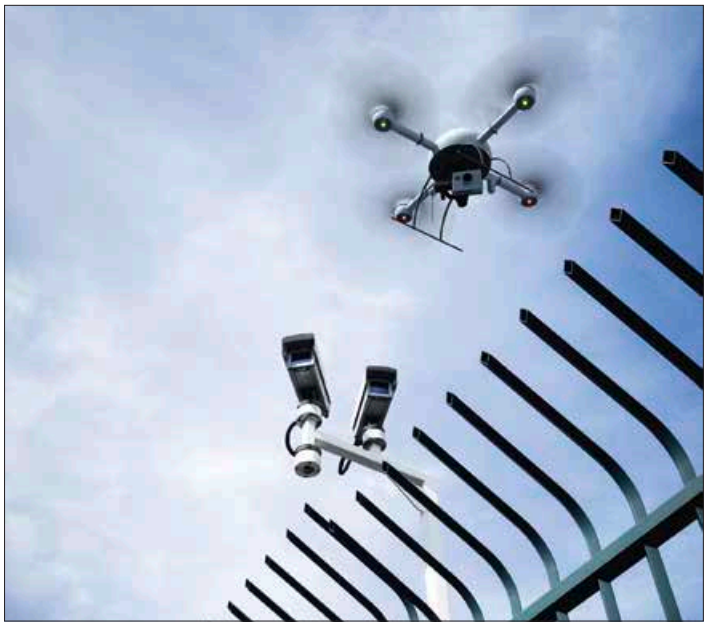
Kokouksessa tuotiin myös esille mahdollisuus osallistua 7.6.2018 vierailulle teemalla ”Jyväskylä kybertoiminnan ytimessä”. Varsinainen ilmoitus ilmestyy verkkosivuille toukokuun alussa. Viestiupseeriyhdistyksen syyskokous ja seminaari järjestetään Riihimäellä lauantaina 22.9.2018.

Kokouksen jälkeen kokousväki nautti maittavan kokouspäivällisen seisovasta pöydästä. Päivällisen ohessa eversti Veli-Pekka Kuparinen kertoi elävästi Kouvolan varuskunnan historiasta. Miellyttävän yhteisen kokouspäivän, runsaan ja maittavan aterian jälkeen pääosa kokousväestä siirtyi yhteiskuljetuksella kohti pääkaupunkiseutua.

TEKSTI: JOUNI SALMI
KUVAT: ROHDE & SCHWARZ

Pienlennokkihälytys!

DI Jouni Salmi työskentelee Rohde & Schwarz Finlandilla viranomaisjärjestelmien teknisenä konsulttina.



Kaupallisten pienlennokkien markkinat kukoistavat. Nopeasti kasvava pienlennokkien määrä asettaa niin turvallisuusviranomaiset kuin myös monet siviiliorganisaatiot uuden tilanteen eteen. Pienlennokeilla voidaan loukata yksityisyyttä tai harjoittaa teollisuusvakoilua, uhata julkisuuden henkilöiden henkeä ja tehdä jopa terrori-iskuja. Pienlennokkien valvontajärjestelmä auttaa suojaamaan kohteita ja henkilöstöä.

Kuva 1. Potentiaalisia uhkatilanteita.

Kaupallisista pienlennokeista megatrendi

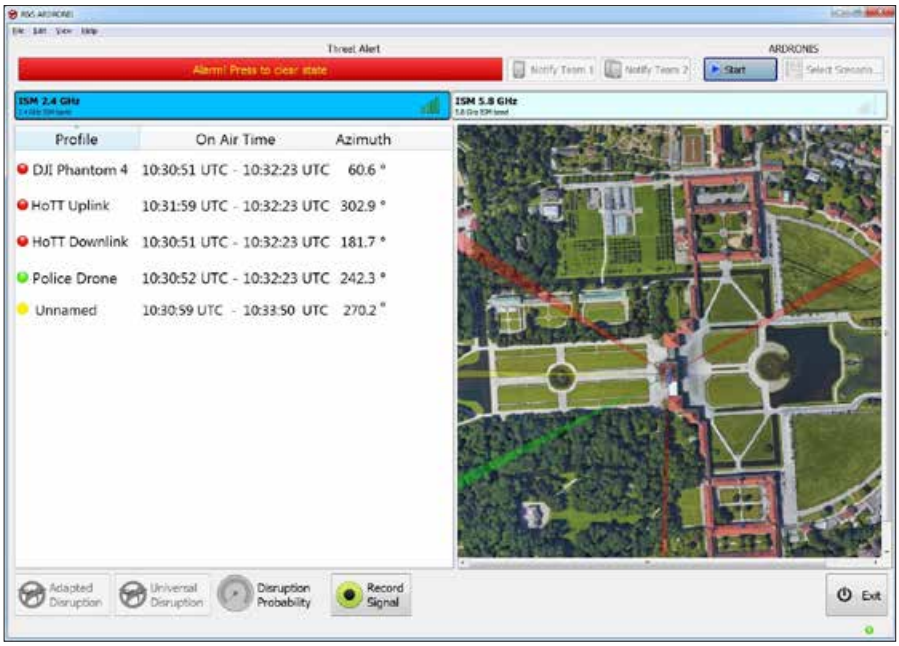
Pienlennokkien markkinat ovat kasvaneet räjähdysmäisesti. Suhteellisen edullisten ja helppokäyttöisten pienlennokkien määrän räjähdysmäinen kasvu muodostaa uudenlaisen haasteen julkisten ja yksityisten tilojen suojaamiselle. Mediassa raportoidaan säännöllisesti erilaisista välikohtauksista kaupallisten pienlennokkien kanssa. Milloin tuntemattomia pienlennokkeja on havaittu lentokenttien läheisyydessä tai jopa lentokoneiden lentoreiteillä, milloin niitä on havaittu voimalaitosten ja hallintorakennusten yllä, poliittisissa tapahtumissa, autojen testiradoilla tai yleisötapahtumien yllä. Koska pienlennokit ovat vaikeasti havaittavissa ja ne pystyvät kuljettamaan usean kilon hyötykuormia, ne muodostavat kasvavan uhan kriittisille infrastruktuureille, julkisuuden henkilöille ja julkisille tilaisuuksille. Turvallisuusorganisaatiot ja yksityiset yritykset tarvitsevatkin teknisiä välineitä näiden uhkien torjumiseen.

Muutamia faktoja pienlennokeista

Pieniä lennokkeja, joita kutsutaan myös mini- tai mikro-UAV:eiksi (Unmanned Aerial Vehicles), kauko-ohjataan pääsääntöisesti maasta käsin. Lentävät miehittämättömät ilma-alukset jaetaan seuraaviin käyttöryhmiin: yksityiskäyttöön tarkoitetut pienlennokit (lelut, harrastuskäyttö), kaupalliseen käyttöön tarkoitetut pienlennokit (ilmakuvaus, logistiikka, yms.) ja sotilaskäyttöön tarkoitetut pienlennokit (tiedustelu, taistelu). Pienlennokeista on olemassa kahta erilaista tyyppiä: multikopterit ja kiinteäsiipiset lennokit. Kiinteäsiipisiä käytetään suuremman kantamansa ja lentokorkeutensa vuoksi ensisijaisesti erikoistehtävissä, kuten kartoituksessa. Kun media raportoi pienlennokeista, on lähes aina kyse pienistä multikoptereista. Pienlennokkien määrittelyssä kiinnitetään huomio kokoon, hyötykuormakapasiteettiin, nopeuteen, lentoaikaan, kantamaan, lentokorkeuteen ja ohjaustapaan.

Kuvassa 2 on katsaus markkinoilla tarjolla olevista radio-ohjausvaihtoehdoista. Yli 90 % kaikista pienlennokeista kommunikoivat radioluvasta vapailla ISM-kaistoilla, joita käytetään myös telekommunikaatiotarkoituksiin, kuten esim. WLAN ja Bluetooth®. Pääsääntöisesti käytössä ovat taajuusalueet 2,4 GHz ja 5,8 GHz ja joskus harvoin 433 MHz.

Kuva 2. Kauko-ohjaustekniikat.

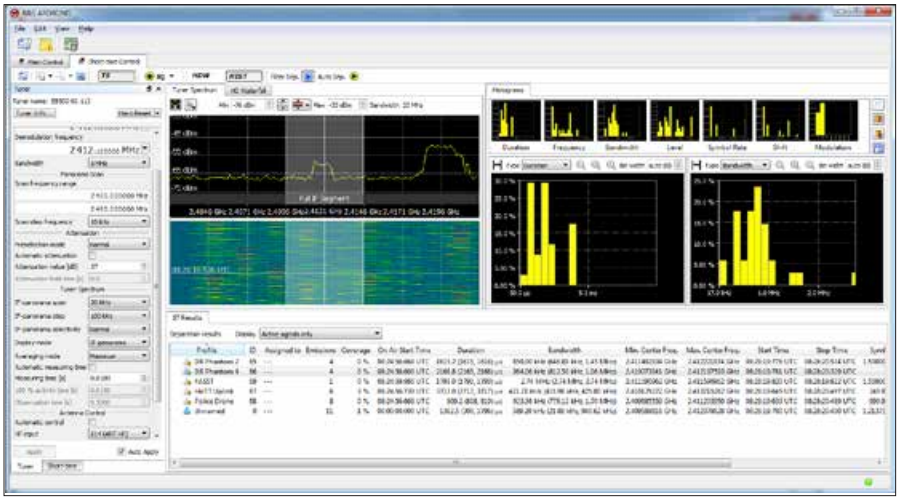


Kuva 3. Selkeä käyttöliittymä.

Ylivoimaisesti eniten käytetyt radioteknologiat pienlennokkien kauko-ohjauksessa ovat hajaspektritekniikat taajuushyppely FHSS (Frequency Hopping Spread Spectrum) ja suorasekvenssi DSSS (Direct-Sequence Spread Spectrum). Nämä tekniikat kattavat yli 80 % nykyisistä kaupallisista pienlennokeista. FHSS vaihtaa lähetteen kantoaaltotaajuutta pseudosatunnaisesti kymmenien, jopa satojen megahertsien kaistalla. Lähettimen ja vastaanottimen on oltava keskenään synkronoituja ja

niiden tulee käyttää samaa hyppelyalgoritmia yhteyden ylläpitämiseksi. DSSS puolestaan käyttää kiinteää, erittäin suurta kaistanleveyttä, mutta se pienentää spektrin tehotiheyttä siinä määrin, että haluttu signaali lähestulkoon peittyy kohinaan ja se voidaan saada esiin vain koherentilla demodulaattorilla. Molemmat menetelmät, joita käytetään myös yhdessä, sopivat erinomaisesti ruuhkaisille ISM-kaistoille. Yhteysetäisyys riippuu luonnollisesti pienlennokin ja kauko-ohjaimen lähetintehosta sekä ympäristöstä. Ihanteellisissa olosuhteissa se on yhdestä kolmeen kilometriä.

Hajaspektritekniikat vaikeuttavat signaalien havaitsemista ja häirintää. Tehokkaiden suojausjärjestelmien pitää siis pystyä reaaliaikaiseen taajuushyppelyanalyysiin. Järjestelmä analysoi tekniset radioparametrit, kuten hyppelynopeuden, modulaatiotyypin ja symbolinopeuden, ja pystyy näiden perusteella määrittämään lähetinjärjestelmän esim. HOTT (Graupner), FASST (Futaba), M-Link (Multiplex), DSMX (Spektrum) tai Ocusync (DJI) (kuva 4). Jokaisen lähetteen teknisiä parametreja verrataan tallennettuihin referenssiprofiileihin ja signaalit, joille on vastaavuus, luokitellaan kolmeen ryhmään: musta lista (esim. potentiaaliset uhat), valkoinen lista (esim. omat pienlennokit) ja nimeämättömät (esim. tuntemattomat pienlennokit).



Kuva 4. Asiantuntijanäkymä antaa kattavat tiedot signaaliympäristöstä.

Kuva 5. R&S®ARDRONIS -järjestelmä.

Radiovalvonnan edut

Pienlennokkien ohjaussignaalien ilmaisun edut verrattuna tutka-, optiseen tai akustiseen havaitsemiseen ovat:

· **Luotettava havaitseminen** ilman aiheettomia hälytyksiä. Järjestelmää eivät häiritse muut lentävät esineet, kuten linnut, ilmapallot tai leijat.

· **Tunnistus varhaisessa vaiheessa.** Hälytys saadaan heti, kun kauko-ohjauslaite alkaa lähettää signaalia, siis käytännössä jo ennen kuin pienlennokki on noussut ilmaan. Vastatoimiin voidaan varautua välittömästi jo ennen akuuttia uhkatilannetta.

· **Pienlennokin lennättäjän paikantaminen.** Koska järjestelmä havaitsee lennokin kauko-ohjaussignaalin, se pystyy määrittämään pienlennokin lennättäjän suunnan. Käytettäessä useita sensoreita saadaan lennättäjän tarkka sijainti ristisuuntimalla.

· **Kokonaiskuva tilanteesta.** Edistyksellinen valvontajärjestelmä ei ainoastaan havaitse kaikkia pienlennokkeja tietyllä valvonta-alueella, vaan usein se kykenee ilmoittamaan myös pienlennokin tyypin analysoimalla sen radiosignaalia, mikä mahdollistaa uhkan arvioinnin. Lisäksi pienlennokin lähettämä signaali analysoidaan, esimerkiksi lähettääkö se videokuvaa.

· **Signaalin häirintä.** Valvontajärjestelmään voidaan liittää häirintälähetin häiritsemään tehokkaasti pienlennokin radioliikenneyhteyttä. Tämä pakottaa pienlennokin ns. Fail-Safe-moodiin, jolloin se joko laskeutuu hallitusti tai palaa lähtöpisteeseen. Häirintä on selektiivistä, joten se ei vaikuta muuhun saman taajuusalueen radioliikenteeseen (esim. WiFi).

R&S®ARDRONIS

R&S®ARDRONIS on Rohde & Schwarzin markkinoille tuoma luotettava, kokonaisvaltainen automaattinen valvontajärjestelmä, joka soveltuu niin paikallaan pysyvään kuin liikuteltavaan käyttöön. R&S®ARDRONIS sieppaa kauko-ohjausyksikön ja pienlennokin välisen kauko-ohjausyhteyden ja paikantaa sen perusteella pienlennokin ja sen lennättäjän, joten se havaitsee riskit jo varhaisessa vaiheessa. Havaitseminen tapahtuu välittömästi sen jälkeen, kun kauko-ohjausyksikkö on kytketty päälle, ennen kuin pienlennokki on edes ilmassa, mikä mahdollistaa varhaiset vastatoimet.

Käyttäjäystävällinen käyttöliittymä listaa havaitut pienlennokit ja nii-

den havaintotiedot (kuva 3). Mikäli käytössä ovat suuntimistoiminnot (R&S®ARDRONIS-D/P), karttapohjalla näytetään suuntimolinjat tai ristisuuntiman osoittama paikka.

Asiantuntijanäkymä tarjoaa radioanalyytikoille yksityiskohtaista tietoa havaituista signaaleista sekä mahdollisuuden muokata profiilikirjastoa (kuva 4).

R&S®ARDRONIS –järjestelmästä on saatavana neljä erisisältöistä kokoonpanoa. R&S®ARDRONIS-I on oikea ratkaisu, kun halutaan selvittää, esiintyykö pienlennokkeja tietyllä rajoitetulla alueella. R&S®ARDRONIS-R soveltuu jatkuvaan tarkkailuun ja alueen suojaukseen, kuten viranomaiskohteisiin. Mikäli suoja-aluetta loukataan, ryhdytään automaattisesti vastatoimiin. Mikäli pienlennokin lennättäjä on paikannettava, suositellaan käytettäväksi kokoonpanoja R&S®ARDRONIS-D tai R&S®ARDRONIS-P.

Tuotteeseen lisätään jatkuvasti uusia toimintoja ja säännölliset järjestelmäpäivitykset sisältävät profiilikirjaston päivittämisen uusilla pienlennokkimalleilla.

Eräät lennokkimallit on varustettu myös navigointitekniikalla, mikä mahdollistaa pienlennokin lentämisen itsenäisesti etukäteen määriteltyä reittiä. Nämä autonomiset pienlennokit eivät lähetä havaittavissa olevia radiosignaaleja. Radioliikenteen häirintäkään ei riitä pakottamaan pienlennokkia kääntymään takaisin tai laskeutumaan, jos sille on ohjelmoitu kiinteä lentoreitti. Näiden lennokkien vastatoimenpiteiksi R&S®ARDRONIS voidaan integroida avoimien rajapintojen kautta kehittyneisiin monisensorijärjestelmiin, jotka voivat sisältää muita sijainnin määritysmenetelmiä, kuten tutkan tai akustisia sensoreita sekä tehokkaita vastatoimia.

Rohde & Schwarzin automaattinen radio-ohjattu pienlennokkien tunnistusratkaisu R&S®ARDRONIS on jo todistanut toimivuutensa tehtävissä, joissa vaaditaan erittäin korkeaa turvallisuustasoa, kuten kesäkuussa 2015 G7-huippukokous Elmaun linnassa Baijerissa ja USA:n presidentti Obaman vierailulla Hannoverin messuilla 2016.

Paikallispuolustuksen johtaminen -seminaari 22.9.2018

Seminaarin järjestelyt ja tavoitteet

Viestikiltojen liitto järjestää paikallispuolustuksen johtamista ja viestitoimintaa käsittelevän A.R. Saarmaan seminaarin lauantaina 22.9.2018 yhteistoiminnassa puolustusvoimien, Viestiupseeriyhdistyksen ja Maanpuolustuskoulutusyhdistyksen kanssa.

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

Seminaarin tavoite on syventää osallistujien tietoisuutta
- paikallispuolustuksen johtamisen ja johtamisen tuen kehitysnäkymistä
- arjen välineisiin ja siviili-infrastruktuurin käyttöön perustuvista johtamisjärjestelmäratkaisuista sekä
- alan vapaaehtoiskentän tehtävistä paikallispataljoonan viestitoiminnan kehittämisessä.

Seminaari on tarkoitettu
- paikallispataljoonaan sijoitetuille johtajille ja viestihenkilöstölle
- viesti- ja johtamisjärjestelmäalan vapaaehtoisten maanpuolustusjärjestöjen jäsenille sekä
- Maanpuolustuskoulutusyhdistyksen jäsenjärjestöjen jäsenille.

Seminaaripäivän ohjelma 22.9.2018

1) Johtamisjärjestelmä M18 -esittely
· Klo 10.00 - 11.00 Riihimäki, Viestikoulun luokkarakennus ja ympäristö
2) Viestiupseeriyhdistyksen vuosikokous
· Klo 11.00 - 12.15 Riihimäki, Viestikoulun luokkarakennus
3) Palkitsemiset ja Viestijoukot 100 vuotta juhlakirjan julkaisu
· Klo 12.15 - 13.00 Riihimäki, Viestikoulun luokkarakennus
4) Kahvi ja suolapala, Ilmoittautuminen seminaariin
· Klo 13.00 - 14.00 Riihimäki ja alueelliset toimipisteet
5) Paikallispuolustuksen johtaminen -seminaari
· Klo 14.00 - 17.30 Riihimäki ja alueelliset toimipisteet
6) Päivällinen
· Klo 18.00 - 20.00 Riihimäen Upseerikerho

Seminaarin ohjelma 22.9.2018 klo 14.00 - 17.30

- Puheenjohtaja viestitarkastaja eversti Eero Valkola

Klo 14.00 - 14.05 Tilaisuuden avaus VKL:n pj

1. Osa: Paikallispuolustuksen johtaminen ja viestitoiminta

Klo 14.05 - 14.15 Puolustusvoimien johtamisjärjestelmäalan johdon tervehdys, PVJOJÄPÄÄLL
Klo 14.15 - 14.30 Paikallispuolustuksen johtamisjärjestelmä, MAAVE
Klo 14.30 - 15.00 Siviiliverkkojen ja -palveluiden käyttömahdollisuudet paikallispuolustuksen johtamisessa, ITC-operaattori
Klo 15.00 - 15.30 Arjen ratkaisut paikallispuolustuksen johtamisessa, esimerkkejä käyttötapauksista, PVTUTKL
Klo 15.30 - 15.45 VARVE-sanomavaraverkko, Pohjois-Karjalan RK, Radioamatöörit viranomaisyhteyksien turvaajana
Klo 15.45 - 16.00 Tauko

2. Osa: Paikallispataljoonan viestikoulutus ja vapaaehtoiskentän tehtävät

Klo 16.00 - 16.30 MPK:n viesti- ja johtamisjärjestelmäalan koulutusohjelma, MPK
Klo 16.30 - 16.55 Kokemuksia paikallispuolustusharjoituksista, MAAV
Klo 16.55 - 17.15 Esikunta- ja viestikomppanian (PAIKP) päällikkö joukkonsa pääkouluttajana,Haasteet ja mahdollisuudet, MPK
Klo 17.15 - 17.30 Seminaarin päättäminen, VTARK

Seminaaripaikkakunnat

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

·	Helsinki	Kadettikouluntie 7, Santahamina	Maanpuolustuskorkeakoulu
·	Riihimäki	Riihimäen varuskunta	Maasotakoulu (VIESTIK)
·	Tampere	Hautalankatu 19 B	2. Verkko-osasto/PVJJK
·	Turku	Rykmentintie 25	1. Verkko-osasto/PVJJK
·	Kouvola	Kauppalankatu 43C	3. Verkko-osasto/PVJJK
·	Mikkeli	Karkialampi	3. Verkko-osasto/PVJJK
·	Vaasa	Wolffintie 35	Pohjanmaan ALTSTO
·	Joensuu	Torikatu 36 B	Pohjois-Karjalan ALTSTO
·	Oulu	Hiukanreitti 40, Hiukkavaara	Pohjois-Pohjanmaan ja Kainuun ALTSO
·	Kajaani	Prikaatintie 97	Kainuun prikaati
·	Sodankylä	Kasarmintie 94	Jääkäriprikaati
·	Lahti	Kirkkokatu 12	Panssariprikaati

Ilmoittautuminen

Ilmoittautumiset seminaariin 31.8.2018 mennessä Viestikiltojen liiton sihteerille Carl-Magnus Gripenwaldtille sähköpostitse: cm.gripenwaldt@gmail.com. Seuraavat tiedot pyydetään ilmoittamaan: **Nimi, syntymäaika, yhteystiedot (puhelinnumero ja sähköpostiosoite), järjestö/yhdistys ja paikkakunta, jossa seminaariin osallistuu.**

Viestikiltojen Liitto

Jääkärieversti A.R. Saarmaa
- Viestiaselajin Grand Old Man

Arthur Reinhold Saarmaan
- 23.9.1892 – 31.1.1971.
- Jääkärieversti, sähköinsinööri

Eversti Saarmaa, alunperin Stenholm, kuului siihen pieneen jääkäriupseerien joukkoon, jonka tehtäväksi lankesi maamme viestiaselajin perustaminen ja kehittäminen itsenäisyytemme ensimmäisinä vuosikymmeninä.

Analysaattori

Digiraivoa

Sitä nimittäin esiintyy, ainakin täällä päässä. Eli ärsytyskynnykseni on ylittynyt ja tällä kertaa käsitellään niitä digitalisaation käytännön toteutuksia, jotka saavat aikaan digiraivoa. Joka on siis läheistä sukua laturaivolle, mutta tässä versiossa ei kuitenkaan mätkitä kohdetta sauvoilla, vaan ihan vain sanan säilällä. Sähköinen reklamaatio on digiraivo-ilmiön fyysisin toteuma.

No mikä se nyt sitten saa päällepäin ihan normaalilta vaikuttavan ihmisen kimpaantumaan niin, että sitä voi verrata jopa katuraivoon, jota mm. USA:ssa harjoitetaan moottoriteiden ruuhkissa. Otetaanpa tähän selvyyden vuoksi pari esimerkkiä. Aloitetaan huoltoasemalle sijoittuvalla kokemuksella. Ajan puutteen vuoksi en mainitse sitä ketjua, jonka polttoaineautomaatit ovat kyseessä, mutta sieltä aakkosten alkupäästä se löytyy. Olin tankkaamassa mainitun ketjun kylmäasemalla. Siinä kyseisessä kohteessa oli yksi korttiautomaatti ja neljä polttoaineen jakelumittaria. Polttoaineen maksaminen oli juuri vaiheessa, jossa pitää valita mittari, josta haluan polttoainetta pumpata. Näytöllä lukee: *”Mittari 1=valitse 2, Mittari 2=valitse 1, Mittari 3=valitse 4, Mittari 4=valitse 3.”* Nyt luulisin, että ymmärrätte mitä ajan takaa. Vähemmästäkin menee jotain sieraimeen ja siitä sitten eteenpäinkin. Tämä oli jo toistunut muutaman kerran kesän mittaan ja koskapa tällä kertaa fokukseni hetkellisesti katosi, siitä seurasi se, että toteutin valinnan vaistoillani. Katsoin autoani, joka oli mittarin 1 edessä ja painoin ykköstä. *”Aloita tankkaus 180 sekunnin kuluessa mittarista 2”*. Koska kyseessä on perheohjelma en avaudu näistä tunnelmista sen enempää. Sen verran kuitenkin petyin tuosta käyttöliittymäkoodauksen tasosta, että lähetin ketjun asiakaspalveluun sähköpostia. Kysyin vilpittömästi, että olivatko siellä aakkosissa tietoisia, että sen mittarin valinnan voisi koodata myös siten, että se käyttäjältä pyydetty mittarin numero olisi sama numero kuin itse mittarillakin. Rohkenin jopa epäillä, että kyse ei olisi kovin vaativasta tehtävästä. Sain sitten jonkin ajan kuluttua vastauksen, joka meni suunnilleen näin. *”Tämä on kyllä tiedossamme mutta se tuli meillekin yllätyksenä edellisen ohjelmistopäivityksen yhteydessä”*. Ei hyvää päivää. Luettelen tässä nyt muutaman asian, jotka tässä keississä meni huonosti: Vaatimusmäärittely, Suunnittelu, Toteutus, Testaus ja Viestintä.

Toinen omakohtainen kokemukseni korreloi suoraan ikääntymiseeni, jota ei kuitenkaan saa mielestäni käyttää tekosyynä, sillä käsittääkseni minulla on melkein 8 miljardia kohtalontoveria. Kaikki eri kohdassa aika-akselia, mutta suunta on sama. Ostin muutama vuosi sitten Golf-kellon. Siis sellaisen GPS-vastaanottimen, joka osaa siellä kentällä näyttää suoraan etäisyyden viheriölle. Koska etäisyyden arviointini on yhtä heikkoa, kuin sen tiedon hyödyntäminen mainitussa lajissa, on kyseessä puhtaasti halu näytellä laitetta asiantuntevan näköisenä ja herättää kateutta, ei niinkään sääliä. Laitteen näyttö on aika kookas, ja se etäisyys näkyy siinä aika hyvin. Valitettavasti tämän härpäkkeen arviolta n. 21 vuotias koodaaja ei tullut ajatelleeksi, että käyttäjät ovat todennäköisesti hieman iäkkäämpiä. Laite nimittäin näyttää pelattavan väylän numeron pienellä siinä etäisyyden alla. Erittäin pienellä. Siis niin hemmetin pienellä, että en näe sitä edes lukulaseilla. Joka aiheuttaa digiraivoa puhtaimmillaan, sillä siinä ympärillä siinä näytöllä olisi hyvää tilaa näyttää se väylänumero ihan kunnollakin. Periaatteessa se on kyllä tiedossani, mutta joskus se laite vähän kadottaa satelliittiyhteyden ja näyttää sitä etäisyyttä esim. edellisen väylän greenille, joka tarkoittaa siis sitä, että se etäisyys saattaa koko ajan kasvaa, vaikka kuinka pomputtelisin sitä hiton palloa oikeaan suuntaan. Enkä siis edes tiedä mille väylälle se sitä etäisyyttä laskee, sillä se tieto on piilotettu pariin pikseliin, joita pitäisi tarkastella laboratorio-olosuhteissa elektronimikroskoopilla.

Edellä esitetyt esimerkit edustavat molemmat puhtaimmillaan Analysaattorin lempiaihetta, huonoa koodaamista. Karkeasti yleistäen termillä digitalisaatio tarkoitetaan teknologian arkipäiväistymistä ja se on jo johtanut siihen, että ohjelmistoja ja koodia on kaikkialla. Mitä enemmän yhteiskunta on ohjelmistojen varassa, sitä enemmän saamme tottua toimimattomiin sovelluksiin. Ja siinähän se ongelma juuri sitten onkin. Niihin ei tarvitse, eikä kannata tottua vaan asialle pitää tehdä jotain.

Mutta suunnaton huoli kyllä nousee, kun yhdistän ajatuksissani näitä nykypäivän megatrendejä. Keinoäly, joka perustuu sysipaskaan koodiin. Mikä tässä nyt voisi mennä pieleen? Keinoälyn kiistämättömät edut saavat ihmisen harhaisesti luottamaan siihen ja seuraukset ovat sitten sen mukaiset ja riippuvaiset koodauksen tasosta. Teslan semi-autonominen auto ajoi Yhdysvalloissa betoniseen liikenteen jakajaan surmaten kuljettajansa. Lieventävänä asianhaarana todettakoon, että auto varoitti 150 metriä ennen kuljettajaa että *”tartu ohjauspyörään*”. En tiedä mistä kuljettajan suunnaton luottamus Teslan kykyyn hoitaa tilanne oli peräisin, mutta mainittakoon kuitenkin, että kyseessä oli Applella työskentelevä insinööri.

Keinoälyn käyttö myös taistelukentällä on noussut isosti uutisiin johtuen Yhdysvaltain armeijan Maven-projektista. Kyse on siitä, että tiedustelulennokit tuottavat niin valtavat määrät dataa, videokuvaa yms. että ihmisvoimin sen analysointi ja erityisesti jatkokäyttö ei ole enää mahdollista. Yhdeltä miehittämättömän lennokin lennolta kertyy kuvamateriaalia jo teratavukaupalla. Maven-projekti hyödyntää siviiliyrityksiä, jotka kehittävät keinoäly-algoritmeja, joiden avulla kuvamateriaalista voidaan tunnistaa esim. ajoneuvoja ja niiden liikkeitä myös ajassa taaksepäin nopeasti ja tehokkaasti. Mukana hankkeessa on jopa 100 yritystä, joista nimekkäimmät lienevät Google, Amazon ja Microsoft, mutta viime aikoina on alkanut kuulua vahvoja sorääniä juuri näiden yritysten henkilöstön taholta. Yli 3000 Googlen työntekijää lähetti tässä pääsiäisen aikoihin yrityksen johdolle kirjeen, jossa vaadittiin projektin lopettamista. Perustelut olivat kyllä painavat. Nämä henkilöt eivät halunneet olla osa ”War Businesta” ja ilmoittivat että Google on perustettu täysin päinvastaisia tarkoituksia varten. Kyseessä on siis Digiraivon käänteinen ilmiö, koodaajien ulostulo, joka perustuu eettisten arvojen puolustamiseen työn tekemisessä. Jäädään kanavalle ja odotellaan mitä tuosta ulostulosta seuraa.

Huonosta koodaamisesta tulivat myös jostain syystä mieleeni terveydenhoidon tietojärjestelmät, joiden huono maine perustuu toimimattomuuden lisäksi niiden korkeaan hintaan. Tämä on tietenkin vain Analysaattorin oma, mutta empiirinen mielipide. Tutustuessani tulevan SOTE-ratkaisun kustannuksiin olen lähinnä järkyttynyt. Tietojärjestelmäkustannusten on nimittäin arvioitu olevan miljardiluokkaa. Lisäksi uusin ”SOTE-yllätys” nousi julkisuuteen tässä aivan kalkkiviivoilla, sillä se kaiken ratkaiseva äänestys on tulossa, jo todennäköisesti kesäkuussa. Nyt meidät pisteytetään. Jokaiselle suomalaiselle lasketaan henkilökohtainen hinta, joka hänestä maksetaan terveysyritykselle tai maakunnan sote-keskukselle. Pisteytys perustuu terveyteen, elämäntilanteeseen liittyviin riskitekijöihin ja sairaushistoriaan. Päättäjät vakuuttavat muuten yhteen ääneen, että mitään tietosuojarikettä ei tässä tule syntymään, eikä tietoja kerätä erityisesti mihinkään keskitettyyn rekisteriin.

Juuri tuosta rekisterin puutteesta olen vähän ärsyyntynyt ja teenkin tässä nyt kansalaisaloitteen, joka nivoutuu näppärästi tietoyhteiskuntaan ja kansalliseen kyberturvallisuusstrategiaan. Oletetaanpas, että lähitulevaisuudessa meidät on kaikki siis huolellisesti pisteytetty terveystietojemme pohjalta ja Sote-keskukset ovat kaapanneet meidät omiin palvelurakenteisiinsa. Nyt tehdäänkin niin, että tämä informaatio integroidaan sekä Kansalliseen Palveluväylään että juuri tässä kehittämääni Sosiaalisen Median Palveluväylään. Kansallisen Palveluväylän kautta viranomaiset saavat meistä näitä tarpeellisia lisätietoja jaettavaksi esim. KELA:n, Verottajan, Työvoimaviranomaisten, tai minkä tahansa tiedonjanoisen viranomaisen tarpeisiin. Sosiaalisen Median Palveluväylän kautta saat kätevästi kiinnostavan kohdehenkilön terveystiedot, vaikka Tinderiin, etkä näin tuhlaa energiaasi esim. jalkavaivaisiin jos etsitkin tanssiseuraa. Ja sama toisinpäin, KELA saa nopeasti tietoja Instagramista siitä, kuinka laskettelureissusi alpeilla sujuu sairaslomasi aikana ja Verottaja puolestaan voi laskea suoraan myyntivoittosi Facebookin kirpputorikaupoistasi ja varmistaa näin kokonaisverotuksesi onnistumisen. Turvallisuusviranomaiset puolestaan hyödyntävät keinoäly-algoritmeja kaikesta mahdollisesta ja tunnistavat näin sekä yhteiskunnalle vaarallisia henkilöitä että niitä, jotka kannattaisi rekrytoida, ennen kuin he valuvat väärälle puolelle mustien ja valkoisten hattujen kamppailussa. Tässä ideassa ei ainakaan mikään voi mennä pieleen ja jos sitten meneekin, niin siitä voi ihan yksilötasolla aiheutua vaikka Sote-raivoa.

Sellaista on siis tämä Digiraivo. Mutta eihän tämä digi-kilahtaminen ole missään tapauksessa Analysaattorin keksintöä. Eräs edelläkävijöistä on Linus Torwalds, joka on julkisuudessa toistuvasti ”avautunut” samasta aiheesta hyvinkin vulgaaristi. Suurin ero Analysaattorin ja Torwaldsin välillä on tässä asiassa tietenkin se, että jälkimmäisellä on siihen yleinen hyväksyntä, lähes mandaatti. Sosiaalisessa mediassakin näkee runsaasti näitä huonoja toteutuksia ja se onkin eräs digiraivon kanavista, jonka avulla se pilkka osuu nopeasti sinne minne se kuuluukin.

Pasi Mäkinen

VM

Sähköteknillisen koulun 20-vuotisjuhlat Riihimäellä 1.4.1968.

Sähköteknillisen koulun 20. vuosipäivää vietettiin Riihimäellä 1.4.1968. Päivän juhlallisuudet alkoivat kunniakäynnillä Riihimäen sankarihaudalla, missä laskettiin seppele ja koulun johtaja maj A Heinäaro puhui. Puheessaan Riihimäen sankarihaudoilla koulun johtaja mm. totesi: ”Siihen aikaan, jolloin suurin osa tällä paikalla maan povessa lepäävistä sankarivainajista taisteli viimeisen taistelunsa, ei tutkasta tiedetty vielä Suomessa mitään, vaikkakin suurvalloilla näitä laitteita oli ollut kehitteillä jo 1930- luvun puolivälistä lähtien. Tästä johtuen emme me, eivätkä edeltäjämme, joutuneet viimeistä sotavuotta lukuun ottamatta osallistumaan näissä tehtävissä isänmaamme puolustamiseen. Sähköteknillisen koulun toiminta onkin, niin kuin sen vuosipäivien määrä jo osoittaa, kohdistunut yksinomaan rauhan aikana suoritettuun koulutus- ja kehitystyöhön. Me olemme omalla kohdallamme pyrkineet täyttämään velvollisuutemme, ei niinkään kouluttamalla taistelijoita vaan lähinnä teknillistä ammattikuntaa puolustusvoimiemme tarpeisiin.”

Koulun lipun naulaustilaisuudessa upseerikerholla koulun johtaja lausui mm: ”Noin kaksi vuotta sitten lähdimme esittämään oikeutta oman lipun saantiin. Asian ratkettua myönteisesti oli edessä käytännön toteutukseen ryhtyminen ja siinä ensinnä sopivan tunnuksen etsimien. Kieltämättä voidaan todeta, että tässä oli omat vaikeutensa, koska sähköteknillisellä alalla ei ollut perinteitä, joihin olisi voitu nojautua; eihän koululla ole tähän mennessä ollut edes omaa joukko-osastotunnusta. Monien luonnostelujen jälkeen päädyttiin lopulta ajatukseen nuolirististä keskustakuviona ja salamasta kulmatunnuksena. Tietysti asiantuntijoilla oli sanansa sanottavana lopullista muotoa haettaessa. Pohjimmiltaan kuitenkin suunnitelma oli omaa tekoa ja tässä mielessä voimme olla tyytyväisiä sillä yleensähän joukko-osastoliput ovat ulkopuolisten ammattisuunnittelijoiden käsialaa. Nyt naulattavan lipun värit ovat sinipunainen ja keltainen, siis viesti värit. Tällä valinnalla olemme halunneet näkyvällä tavalla muistuttaa tulevillekin polville, että sähköteknillinen ala on syntynyt viestiaselajin haarautumana, kuulunut siihen alkutaipalellaan elimellisenä ja tuntee jatkuvasti läheistä sukulaisuutta siihen. Keskustakuvion nuoliristi kuvaa koulun toimintaa puolustusvoimiemme kaikkien puolustushaarojen ja aselajien sähköteknillisen alan henkilöstön koulutuspaikkana. Sivutunnuksena oleva salamakimppu taas symbolisoi varsinaisesti itse alaa, elektroniikan hyväksikäyttöä.”

Päiväjuhlassa juhlapuheen piti Pääesikunnan Sähköteknillisen osaston päällikkö eversti E Veranen. Puheessaan hän lausui mm: ” Elektroniikkateollisuutta on pidettävä Suomelle hyvin soveltuvana teollisuuden haarana. Laitteissa ja järjestelmissä on raaka-aineiden ja puolivalmisteiden osuus usein verrattain vähäinen. Sen sijaan työ on monesti hyvin suunnitteluvoittoista. Sanotaankin, että elektroniikan parissa työskenteleminen on osoittautunut suomalaiselle mentaliteetille sopivaksi. Sähköteknillisen alan teknillinen taso, samoin kuin sähköteknillisen koulutuksen taso ovat tänään paremmat kuin koskaan ennen. Asejärjestelmien samoin kuin johtamisjärjestelmien teknillinen kehitys kohti automaatiota elektronisin keinon on ollut kuluneiden vuosikymmenten aikana valtavaa. Sanotaankin, että tietomäärä on kasvanut elektroniikka-alalla kaksinkertaiseksi 5-7 vuodessa. Kriisiaikaa silmälläpitäen onkin tämän alan henkilöstön oltava valmiiksi koulutettua ja jatkuvasti kehityksen tasalla pysyvää. Nykyinen Sähköteknillinen koulu pystyy täyttämään ne vaatimukset, mitä tänään alkava uusi 10 v kausi tulee koululle antamaan.”

Vuosipäiväänsä juhlivan koulun onnittelut aloitti PE:n viestitarkastaja eversti A Brandt, joka luovutti koululle Puolustusvoimain komentajan myöntämän hopeisen ansiolevykkeen. Koulua onnittelivat lisäksi lukuisat yksityiset henkilöt ja yhteisöt.

Toimittanut Veli-Matti Pesola

VM

Kutsu Viestiupseeriyhdistyksen syyskokoukseen

Viestiupseeriyhdistyksen hallitus kutsuu yhdistyksen jäsenet **syyskokoukseen ja seminaaripäivään Riihimäelle lauantaina 22.9.2018 kello 10.00 alkaen.** Varsinainen syyskokous pidetään Riihimäen Varuskunnassa klo 11.00-12.15, Viestikoulun luokkarakennus.

Kokouksessa käsitellään sääntöjen 5 §:ssä syyskokouksessa käsiteltäväksi mainitut asiat:
0) Palkitsemiset
1) Kokouksen puheenjohtajan valinta
2) Kokouksen sihteerin valinta
3) Kahden pöytäkirjan tarkastajan ja äänten laskijan valinta
4) Kokouksen laillisuuden ja päätösvaltaisuuden toteaminen
5) Kokouksen työjärjestyksen hyväksyminen
6) Toiminta- ja taloussuunnitelman hyväksyminen vuodelle 2019
7) Jäsenmaksujen suuruuden päättäminen vuodelle 2019
8) Hallituksen puheenjohtajan valinta vuodelle 2019
9) Hallituksen jäsenten lukumäärän päättäminen ja hallituksen jäsenten valinta vuodelle 2019
10) Toiminnantarkastajan ja varamiehen valinta
11) Muut asiat

Koko päivän ohjelma 22.9.2018

1) Johtamisjärjestelmä M18 -esittely
• Klo 10.00 - 11.00 Riihimäki, Viestikoulun luokkarakennus ja ympäristö
2) Viestiupseeriyhdistyksen vuosikokous
• Klo 11.00 - 12.15 Riihimäki, Viestikoulun luokkarakennus
3) Palkitsemiset ja Viestijoukot 100 vuotta juhlakirjan julkaisu
• Klo 12.15 - 13.00 Riihimäki, Viestikoulun luokkarakennus
4) Kahvi ja suolapala, Ilmoittautuminen seminaariin
• Klo 13.00 - 14.00 Riihimäki ja alueelliset toimipisteet
5) Paikallispuolustuksen johtaminen -seminaari
• Klo 14.00 - 17.30 Riihimäki ja alueelliset toimipisteet
6) Päivällinen
• Klo 18.00 - 20.00 Riihimäen Upseerikerho

Kuljetus Helsingistä lähtee Kiasman edestä turistipysäkiltä (Mannerheiminaukio) kello 08.30 ja paluu päivällisen jälkeen samaan paikkaan.

Ilmoittautumiset päivän tilaisuuksiin 31.8.2018 mennessä www.viestiupseeriyhdistys.fi (toivottavin tapa), sähköpostitse toiminnanjohtaja@viestiupseeriyhdistys.fi tai puhelimitse 040 514 2497. Samalla kertaa pyydetään ilmoittamaan osallistuuko kuljetukseen.

Tervetuloa!

Viestiupseeriyhdistys ry:n hallitus

Onnittelemme merkkipäivänä

Esa Salminen 60 vuotta

Kangasalla syntynyt eversti (evp) Esa Salminen täytti 60 vuotta 14.5.2018. Salminen muutti juuri ennen koulun alkua Somerolle, missä hän kävi kansakoulun ja yhteiskoulun sekä myöhemmin Turkuun, jossa kävi lukion. Varusmiespalveluksen hän suoritti Porin Prikaatin Viestikomppaniassa, mikä jo osaltaan viitoitti hänen viestiupseeriuraansa.

Salminen oli isänsä kertoman mukaan sanonut jo 8-vuotiaana, että isona hänestä tulee sotilas. Innoittajana oli kuuleman mukaan se, että hän oli nähnyt isänsä kertausharjoituksissa ”upeassa sarkapuvussa”. Uravalinta oli siis tehty jo varsin nuorena ja se vain vahvistui iän myötä. Salmisen ensimmäinen harrastus oli partio Someron Mikonpojissa, jossa hän aloitti heti kouluun mennessään. Yhteiskoulussa partion lisäksi harrastuksiin tuli mukaan telinevoimistelu ja Turkuun muuton jälkeen partio ja voimistelu vaihtuivat pikajuoksuun Turun Urheiluliitossa.

Ylioppilaskirjoitusten jälkeen Salminen toimi koulussaan liikunnanopettajan sijaisena ja mietti myös liikunnanopettajan ammattia upseerin uran ohella. Varusmiespalveluksen jälkeen Kadettikoulu oli kuitenkin selkeä ykkösvaihtoehto, joka myös toteutui. Se, että Salminen päätyi varusmiespalveluksessa Viestikomppaniaan, oli puhdas sattuma. Tuohon aikaan Porin Prikaatissa oli pienehkö Viestikomppania, johon pääsääntöisesti otettiin viestialan ammattilaisia ja niihin opiskelevia henkilöitä, kuten insinöörejä, sähköasentajia jne. Silloin ei kuitenkin Säkylään saatu riittävästi alan erikoismiehiä, joten täydennykseksi tarvittiin muutama tavallinen ylioppilas.

Valmistuttuaan Kadettikoulusta vuonna 1983 Esa valitsi palveluspaikakseen Panssariprikaatin Viestikomppanian, jossa hän toimi mm. sähkötyskouluttajana. Vajaan vuoden palveluksen jälkeen hänet siirrettiin Haminaan Reserviupseerikoulun Viestikomppaniaan, jossa vierähti 6,5 vuotta. Haminassa Salminen suoritti myös radioamatööritutkinnon.

Esa ja ensimmäinen hirvi.

Haminan aikana Salminen sai myös ensi kosketuksen ATK-alaan toimiessaan RUK:n oppilaskunnan kuraattorina vuonna 1985. Salminen oli lukenut Helsingin Sanomista, että Nokia luovuttaa vanhempia Mikro Mikko 2 tietokoneita hyväntekeväisyystarkoituksiin. Tuolloin sattui RUK:n kurssilla olemaan silloisen Nokian pääjohtajan poika, jolta Salminen tiedusteli, josko Nokia voisi lahjoittaa RUK:n oppilaskunnalle kyseisiä koneita. Upseerioppilas Kairamo otti asian esille kotona seuraavana viikonloppuna ja tämän seurauksena oppilaskunta sai lahjoituksena uuden Mikro Mikko 3:n tarvittavine lisälaitteineen ja ohjelmistoineen. Salminen pääsi myös osallistumaan mm. tietokantaohjelmisto

K-miehen ja muiden hienouksien koulutukseen.

Sotakorkeakouluopintojen jälkeen vuonna 1993 Salminen siirtyi juuri perustetun Puolustusvoimien Materiaalilaitoksen Elektroniikkaosaston jaostopäälliköksi, missä pääsi työskentelemään mm. kolmenkymmenen insinöörin kanssa. Aika oli välillä erittäin haasteellista, kun piti rakentaa kokonaan uutta organisaatiota ja samalla hankkia valtavasti erilaisia elektronisia järjestelmiä puolustusvoimille esimerkkinä YVI 2-järjestelmä. Tämän tehtävän myötä Salmiselle tuli puolustusmateriaaliteollisuus tutuksi niin kotimaassa kuin ulkomaillakin.

Salminen päätti aloittaa opinnot vuonna 1993 Teknillisessä Korkeakoulussa Otaniemessä Sähkö- ja tietoliikennetekniikan osastolla työn ohessa. Opiskelusta olikin hyötyä tulevissa työtehtävissä. Tekniikan Lisensiaatiksi Salminen valmistui vuonna 2000.

Materiaalilaitokselta Salminen lähti vuodeksi Balkanille YK-operaatioon Pohjoismaisen pataljoonan operaatiopäälliköksi, missä hän pääsi mm. raportoimaan silloiselle YK:n erityisedustaja Elisabeth Rehnille. Suomeen palattuaan hän sai siirron Maanpuolustuskorkeakouluun viestitaktiikan ja myöhemmin viesti- ja johtamisjärjestelmätekniikan pääopettajaksi. Tämän jälkeen oli vuorossa Pääesikunta, josta tuli mieluisa siirto Puolustusvoimien Tietotekniikkalaitoksen johtajaksi. Joukko-osaston komentajuus on varmaan parasta, mitä upseeri voi urallaan kokea. Tehtävässä sai johtaa todellista huippuammattilaisten organisaatiota ja samanaikaisesti tukea mm. Pääesikunnan valmisteluja uuden organisaation Puolustusvoimien Johtamisjärjestelmäkeskuksen perustamiseksi, jonka ensimmäiseksi hallinnolliseksi johtajaksi hänet nimettiin. Viestillisesti muistoihin on tuolta ajalta elävästi jäänyt Kosovon kenttäviestijärjestelmän vaihto Tetra-perusteiseen kaupalliseen järjestelmään, jossa Tietotekniikkalaitoksella oli tärkeä rooli.

Tämän jälkeen seurasi siirto Riihimäelle Viestirykmentin komentajaksi ja varuskunnan päälliköksi. Toinen komentajuus oli myös upea vaihe, vaikka varuskunnassa olikin melkoisia muutoksia mm. Millog Oy:n perustamisen johdosta. Riihimäen vuosina 2006”2009 Salminen pääsi varuskunnan päällikkönä mukaan lähiseudun kuntien ja turvallisuusviranomaisten toimintaan. Varmasti yksi antoisimmista tehtävistä upseeriuran aikana oli seurata ja vastata Rykmentin antamasta koulutuksesta puolustusvoimien henkilökunnalle ja varusmiehille. Myös media tuli tutuksi Salmisen edustettua puolustusvoimia mm. TV:n ja radion ajankohtaisohjelmissa.

Esa ja Suomen mestaruus.

Vuonna 2009 Esa Salminen sai siirron Lontooseen Suomen puolustusasiamieheksi. Tästä on oma erillinen artikkeli Viestimies I/2013 -lehdessä. Yhtenä huippukohtana Lontoossa lienee sotilasasiamiesyhdistyksen puheenjohtajuus kalenterivuonna 2011, jolloin hän pääsi edustamaan 86 maata ja osallistumaan lukuisiin mielenkiintoisiin tapahtumiin. Lontoon olympialaisten jälkeen 2012 Salminen palasi Suomeen ja samalla hän sai tiedon sotilasuran päättymisestä keväällä 2013. Viimeinen puoli vuotta meni Pääesikunnan johtamisjärjestelmäosastolla erityistehtävissä, mikä tarkoitti käytännössä puolustusvoimien edustajaa VM:ssä VALTORIa perustavassa työryhmässä.

Kokonaisuutena sotilasura vastasi juuri niihin odotuksiin, mitä Salminen työlleen oli asettanut: haastava, mielenkiintoinen, vaihteleva, opettajan tehtäviä sisältävä ja koko uran ajan kehittyvä toiminta. Lisäksi hän pääsi työskentelemään ihmisten kanssa.

Aktiivisena henkilönä Salminen ei eläkkeelle siirryttyään ole malttanut jäädä kotiin lepäämään, vaan on hakeutunut takaisin työelämään. Tosin vaimon kehittämät lukuisat kotiaskareet osaltaan helpottivat päätöksen tekoa. Ensimmäinen vajaa vuosi vierähti Suomen Dell:llä neuvonantajana ja seuraavat kaksi vuotta Riihimäellä Sakon ja Berettan leivissä viranomaisliiketoimintayksikön vetäjänä. Vaikka tehtävä oli erittäin haastava, opetti se paljon uutta mm. yksityisen puolen liiketoiminnasta. Samalla pääsi matkustamaan ympäri maapalloa hyödyntäen mm. Lontoon vuosien aikana syntyneitä kontakteja.

Vuonna 2016 Esa Salminen siirtyi nykyiseen tehtäväänsä kyberturvayritys Nixulle, missä hän toimii yhdistävänä tekijänä Nixun ainoaan strategiseen asiakkaaseen Suomen Puolustusvoimiin. Salminen on viihtynyt tehtävässä erinomaisesti ja tuntenut olevansa omalla toiminta-alueellaan. Samalla hän on kyennyt hyödyntämään vuosien saatossa hankkimiaan taitoja.

Salminen löysi nykyisen vaimonsa Riinan jo kadettiaikana Turun suunnalta tanssilavoilta. Häitä vietettiin Turussa perinteisin sotilasmenoin. Perheeseen syntyi kaksi poikaa, jotka ovat jo aikuisia.

Liikunta on ollut aina tärkeä osa Salmisen elämää. Lasten kasvaessa hän lähti näiden harrastuksiin mukaan toimien fysiikkavalmentajana niin salibandy- kuin jalkapallojoukkueissa. Täytettyään 50 vuotta Salminen osti jälleen piikkarit ja päätti kokeilla veteraanipikajuoksua. Heti ensimmäisissä SM-kisoissa tuli hallissa 60 metrin

Suomen mestaruus ja se antoi kipinän jatkaa lajia. Erilaisia SM-mitaleita on tullut noin 20 ja niiden lisäksi viime vuodelta myös Pohjoismaiden mestaruus. Vuoden 2018 päätavoite on syyskuussa Espanjassa pidettävät MM-kisat. Lisäksi Salminen jatkaa keravalaisen salibandyseura Blackbirdsin miesten edustusjoukkueen fysiikkavalmentajana.

Uusiksi harrasteiksi eläkkeelle jäännin jälkeen on muotoutunut metsästys ja öljyvärimaalaus. Ensimmiset hirvet on kaadettu ja ensimmäiset taulut ovat olleet näyttelyssä.

Viestiupseeriyhdistykseen Salminen liittyi jo kadettikoulussa ollessaan ja on ollut siitä lähtien mukana sen toiminnassa. Mieleenpainuvimpana tapahtumana on VUY:n vierailu Lontooseen, jossa asiamies isännöi siellä noin 25 hengen vierailijaryhmää. Viestiupseeriyhdistyksen kautta Salminen on saanut uusia virikkeitä ja ideoita vuosien varrella sekä hyviä ystäviä.

Salmisella on ollut vuosien varrella myös erilaisia luottamustehtäviä, joista voi mainita aiemman asiamiesyhdistyksen puheenjohtajuuden lisäksi mm. AFCEA Helsinki Chapterin presidenttiys, Kadettikunnan varapuheenjohtajuus ja Aktiasäätiö Keski-Uusimaan hallituksen puheenjohtajuus.

Merkkipäiväänsä 14.5.2018 Salminen vietti Santahaminassa - mikä voisikaan olla parempi syntymäpäivätapahtuma evp-sotilaalle kuin puolustusvoimien järjestämä vapaaehtoinen jatkokoulutuspäivä Kaartin jääkärirykmentissä, jonne hän oli saanut kutsun. Viestimies-lehti esittää lämpimät onnittelut Esa Salmiselle merkkipäivän johdosta.

Toimittanut Jani Liitola

Henkilöasiat:

Siirrot ja tehtävään määräämiset

- kapteeni **Joona Hakulinen** (PSPR) Puolustusvoimien johtamisjärjestelmäkeskukseen 1.7.2018 lukien

- everstiluutnantti **Esko Liimatta** (MAASK) erityistehtävään Puolustusvoimien johtamisjärjestelmäkeskukseen 1.8.2018 lukien

- majuri **Jukka Nikkilä** (PEOPOS) Puolustusvoimien johtamisjärjestelmäkeskukseen 1.8.2018 lukien

- everstiluutnantti **Mano-Mikael Nokelainen** (PEJOJÄOS) rykmentin komentajaksi Helsingin ilmatorjuntarykmenttiin Panssariprikaatiin 1.8.2018 lukien

- everstiluutnantti **Juha Peltomäki** (PVJJK) koulun johtajaksi viestikouluun Maasotakouluun 1.8.2018 lukien

- komentaja **Olli Peltonen** (PEJOJÄOS) erityistehtävään Pääesikunnan johtamisjärjestelmäosastolla 1.8.2018 lukien

- eversti **Harri Suni** (PEJOJÄOS) Puolustusvoimien johtamisjärjestelmäkeskukseen 1.8.2018 lukien

TEKSTI JA KUVAT: ANTTI ASIALA

Radiomystiikkaa

Kirjoittaja on sähkövoimatekniikan diplomi-insinööri, joka toimii Insta DefSec Oy:ssä kehityspäällikkönä puolustusratkaisuissa ja omaa pitkällisen kokemuksen SW-kehityksestä, radiotekniikasta ja monesta muustakin aiheesta (kuten mökkeilystä ja jääkiekosta).

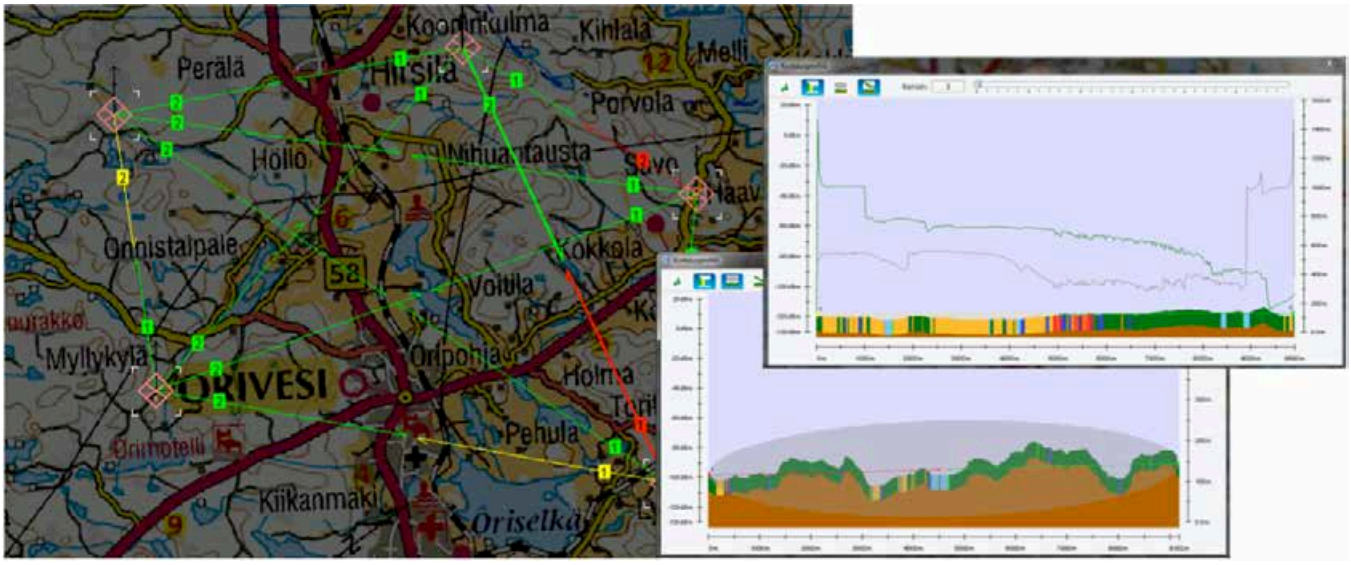
Radiovastaanottimien toiminta vaikuttaa toisinaan mystiseltä. Viime syyskuussa havaitsin kuvan kadonneen kesämökkini televisiosta. Hetken asiaa seurattuani jouduin toteamaan, että signaalin voimakkuus yksinkertaisesti romahti 90% tasosta aika ajoin nollaan, mikä kovasti häiritsi katselunautintoani. Onneksi huomasin uutisen erityisen voimakkaasta radiokelistä, ennen kuin ehdin liukkaalle katolle antennia kääntelemään. Kyse oli siis tietyn säätilatyypin aiheuttamasta erityisen voimakkaasta radioaaltojen kantautumisesta, minkä seurauksena useamman lähetysaseman signaali päätyi antenniini häiriten toisiaan epäreilulla tavalla. Samoja taajuuksia joudutaan uudelleenkäyttämään toisistaan etäällä olevilla asemilla, koska käytettävä taajuuskaista on rajallinen. Ratkaisin ongelman laittamalla toosan kiinni ja ryhtymällä saunan lämmitykseen.

Olemme tottuneet peukalosääntöihin tutun radiokaluston kanssa ja oletamme, että kalusto toimii niiden mukaisesti. Oletamme radion toimivan tietyn etäisyyden takaa ympärisäteilevällä antennilla ja vaikka kolminkertaisen matkan suuntaavalla antennilla. Peukalosäännöillä pääsee kyllä aika pitkälle arvioitaessa radioyhteyksien toimintaa, mutta entä sitten kun yhteys vaan ei muodostu? Vaikka Suomi onkin lähes pannukakku vaikkapa Norjaan verrattuna, saattaa matalakin nyppylä aiheuttaa haasteita peukalosäännön luotettavuudelle, puhumattakaan muiden radiolähettimien aiheuttamista häiriöistä (tai häirinnästä).

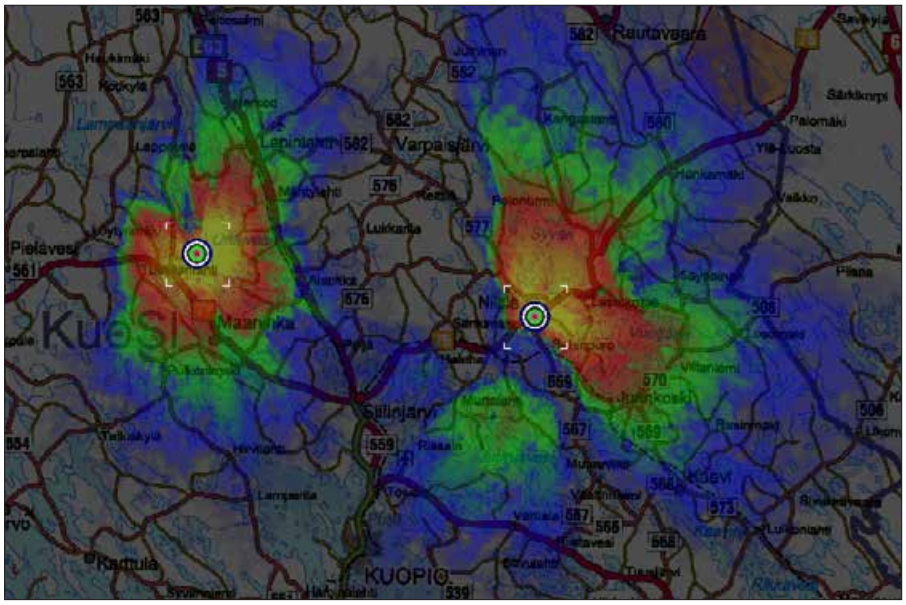
Televisiota viritellessäni olen itsekin nuorempana sortunut tarkastamaan liityntöjä ja hienosäätämään antennien suuntausta, suuremmin miettimättä ovatko toimenpiteeni kovinkaan järkeviä. Olisin saattanut päätyä toisenlaiseen ratkaisuun, kuten korottamaan mastoani tai ostamaan erilaisen antennin, mikäli minulla olisi ollut tuolloin käytössäni helppokäyttöinen (tai edes joku) työkalu radioyhteyden arvioimiseen.

Maailmalta löytyy monimutkaisia kaupallisia mallinnustyökaluja, joita käyttämällä yhteyksiä voi mallintaa (esim. HTZ Warfare). Siis mallintaa ja laskea voi, jos osaa, mutta mitä laskentamalleista tulisi käyttää milloinkin? Ja miksi laskenta kestää näin turkasen kauan? Mitenkäs sitten, kun otetaan huomioon radioverkon topologia, kun käytössä on suuntaavia antenneita? Lähettimen antenni kun ei voi osoittaa yhtä aikaa kaikkia vastaanottimia kohti, jos ne kerran ovat eri suunnissa.

Näitä haasteita lähdimme Instassa ratkaisemaan vuosikymmen sitten, jonka seurauksena - useampi diplomityö myöhemmin - Puolustusvoimilla on käytettävissä työkaluja, joiden käyttö ei vaadi syvällistä vihkiytymistä radiotekniikkaan. Ne antavat satunnaisellekin käyttäjälle mahdollisuuden ymmärtää syitä ja seurauksia sekä keksiä ratkaisuja haasteisiin.



Kuva 1:Viiden radion verkon yhteydet laskettuna ja esitettynä. (Vihreä=toimii, Keltainen=epävarma, Punainen=ei toimi). Yhteysväleihin voi pureutua tarkemmin ja radioita voi helposti raahailla kartalla eri paikkoihin.



Kuva 2: Radiopeitot laskettuna ja esitettynä kahdelle tukiasemalle. Radiopeitoista voi päätellä, että kuljettaessa siniselle alueelle, saattaa radioyhteyden ylläpitäminen tukiasemaan muodostua haasteelliseksi.

Yhteysvälien analysoinnissa kartta ja korkeusmalli ovat ensimmäinen askel, joita tuijottamalla voi päätellä parhaimpia alueita vastaanottoon. Tarkennusta asiaan saa käyttämällä esimerkiksi Instan toteuttamaa Radio Wave Propagation -sovellusta, jolla voi helposti ja nopeasti testata radioyhteyden muodostumista erilaisilla yhteysjänteillä ja lähetin-vastaanotin topologioilla (ks. Kuva 2). Työkalu soveltuu hyvin esim. kenttäradioiden käytön suunnitteluun ja sillä voi myös mallintaa mahdollisen häirinnän vaikutusta radioiden toimintaan. Sovelluksella voi myös esimerkiksi laskea ja esittää tukiasemien radiopeittoja (Kuva 1) tai tutkakantama-alueita. Radio Wave Propagation -sovelluksesta kiinnostuneet voivat ottaa minuun yhteyttä (antti.asiala@insta.fi). Puolustusvoimien henkilöstön yhteydenotot lupaan ohjata PV:n asianhoitajalle ja muiden osalta katsotaan tilanteen mukaan, miten edetään.

Viestiupseeriyhdistys järjestää seminaarin

Turvallisuusympäristön muuttuminen ja siihen vastaaminen

11. - 12.2.2019

Seminaarissa käsitellään turvallisuusympäristössä tapahtuneita muutoksia ja arvioidaan niiden vaikutuksia yhteskunnan toimivuuteen.

Seminaari on tarkoitettu organisaatioiden tietoverkkojen toimintavarmuudesta, suunnittelusta, ratkaisuista ja tietoturvallisuudesta vastaaville.

Puhujina mm. kansliapäällikkö Jukka Juusti, tutkimusjohtaja Mikko Hyppönen, tutkimusjohtaja Hanna Smith, eversti Pekka Turunen, eversti Timo Viinikainen, Veli-Pekka Kivimäki, prof Mikko Möttönen ja toimittaja Salla Vuorikoski

Seminaarin tarkempi ohjelma sekä ohjeet ilmoittautumisesta julkaistaan Viestimies-lehdessä 3/2018 ja www-sivuilla www.viestiupseeriyhdistys.fi. Paikkoja rajoitetusti.

11.2. iltapäivän tilaisuus on CGI Finland Oy:n tiloissa Pitäjänmäellä ja ilta- sekä 12.2. ohjelma risteilynä Helsingistä Tallinnaan m/s Silja Europalla.

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

TERVETULOA 5G

Vaikka 5G-verkkoja ja -laitteita saamme vielä hetken odottaa, on Elisa jo luonut liittymän, joka toimii pääsylippunasi tulevaan 5G-verkkoon. Jo tällä hetkellä Elisan 5G Ready -liittymät hyödyntävät 4G-verkon kaikkein nopeimpia, jopa 600 Mbit/s yhteyksiä.

Tervemenoa tulevaisuuteen.

5G READY

Saunalahti Mobiili-laajakaista 5G Ready

34,90 €/kk

Ensimmäiset 12 kk
(norm. 44,90 €/kk)

5G READY

Saunalahti Huoleton 5G Ready

39,90 €/kk

Ensimmäiset 12 kk
(norm. 49,90 €/kk)

elisa.fi/5G

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