

Viestimies

Viestiupseeriyhdistyksen julkaisu 74. vsk Numero 3 Syksy 2019

Teemana 5 G

5G

Viestimies kybertoimintaympäristössä, sivu 6

5G-aikakausi alkoi, sivu 11

Merivoimien johtamisjärjestelmä 2025, sivu 24

www.viestiupseeriyhdistys.fi



COMBITECH

Experts in Digitalizing Defence

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

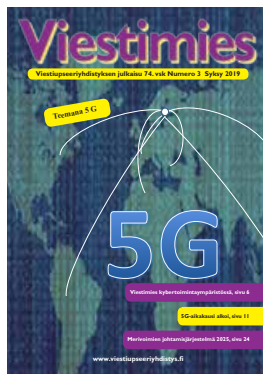
Pankkitili FI 21 5780 5520 017 7 44
Vuosikerta 35 Eur

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

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



Tässä numerossa

- 5** Pääkirjoitus: Tuulet puhalttaa.... mutta minne?
- 6** Viestimies kybertoimintaympäristössä
- 11** 5G-aikakausi alkoi
- 15** 5G-teknologia tuo nopeata datasiirtoa, suurta luotettavuutta ja pientä viivettä
- 21** Digitalisoinnin työkalupakki
– Lohkoketjuteknologia ja Arvon internet
- 24** Merivoimien johtamisjärjestelmä 2025
- 26** Viestimiespäivillä Lyyssä 10.-11.8.2019
- 29** Analysaattori:Houston, meillä on tietokone!
- 31** Viestimies 50 vuotta sitten
- 32** Onnittelemme: Viestiupseeriyhdistyksen kunniajäsen
Olli Vuorio 100 vuotta.
- 34** Henkilöasiat

Seuraavan numeron aineistopäivä on 14.10.2019. Lehti ilmestyy viikolla 49.



PUOLUSTUSVOIMIEN STRATEGINEN KUMPPANI

TURVALLISEN DIGITALISAATION EDELLÄKÄVIJÄ

Tiedustelu-, valvonta- ja johtamisjärjestelmät

Harjoittelu-, koulutus- ja simulointiratkaisut

Datakeskeiset ratkaisut ja edistynyt analytiikka

Autonomiset järjestelmät

Kokonaisarkkitehtuurin ja hankejohtamisen palvelut

Avioniikan elinkaaren tukipalvelut ja tuotteet

Hätä- ja hälytyskeskusjärjestelmät

Rikostorjunnan ratkaisut

Kyber- ja tietoturvaratkaisut

Insta Group on turvalliseen digitalisaatioon, automaatioon ja johtamisen ratkaisuihin keskittynyt teknologiakonserni, johon kuuluvat Insta DefSec Oy, Insta ILS Oy, Insta Automation Oy, Insta Response Oy ja Intopalo Digital Oy.

insta.fi

Tuulet puhaltaa...mutta minne?

Mikään ei ole niin pysyvää kuin muutos. Puolustusvoimien johto vaihtui elokuun alussa. Uusi hallitus painii ensimmäisen budjettiriihensä kanssa. Valtion rahoituksen painopisteet vaihtuvat hallituksien myötä. Nämä ovat kuitenkin usein aikaan sidottuja muutoksia. Teknologian muutos ruokkii itse itseään. Lisääntynyt laskentateho luo mahdollisuuksia mallintaa asioita eri tavalla ja tehokkaammin lyhyemmässä ajassa. Laskentateho lisääntyy jatkuvasti. Älypuhelimissa on nykyisin enemmän laskentatehoa kuin ensimmäisessä tietokoneessani vuodelta 1995, joka oli 486-prosessorilla varustettu PC. Siinä oli 385 Mt kovalevytilaa ja taisi olla huimat 512 Kt keskusmuistia. Sovelluskehitys ja lisääntynyt kapasiteetti ovat ajaneet markkinat tilanteeseen, missä koko ajan tulee suoltaa uusia ja entistä innovatiivisempia ohjelmia ulos kuluttajille. Haittapuolena lieenee sovelluksien keskeneräisyys, joka vaatii jatkuvaa päivittämistä ja ”bugien” korjausta. Tämä luo mahdollisuuksia rikollisille elementeille hyödyntää ohjelmissa ja järjestelmissä olevia aukkoja.

5G merkitsee todennäköisesti samaa kuin mobiilipuhelimien tulo markkinoille lankapuhelimen jälkeen. Tätä on luonnollisesti vaikea todentaa vielä tässä vaiheessa kehityskaarta. Tutkimukset ja visiot luonnehtivat, että 5G teknologialla toteutetut palvelut mahdollistavat täysin uudenlaisten tuotteiden kirjojen. Tästä olemme saaneet lukea jo aiemmin lehden palstoilla. IoT eli Internet of Things luo verkkoja kaikkialle ja jokaiseen laitteeseen. Lisääntyvät verkot ja kehittyneemmät taajuudenhallinta teknologiat mahdollistavat yhä suuremmat tiedonsiirtonopeudet. Langattomuus on tätä päivää, mutta mikä on huomista?

Vaikka langattomuus helpottaa ja



mahdollistaa erilaisia asioita, ei se vielä lähitulevaisuudessa tule korvaamaan langallista tiedonsiirtoa. Valokuituteknologia kehittyy siinä missä langattomat teknologiatkin. Puolustusvoimat on kehittämässä verkkotekniikoita ja kytkeytyvyyttä verkkoihin muun muassa PVLIVE-ohjelmassa. PVLIVE eli Puolustusvoimien Liityntä Verkko mahdollistaa yhä vaivattomamman liityntätavan. Uusi tapa vapauttaa henkilöstöä ”konffaamasta” ja automatisoi liityntä metodia. Tätä koestettiin esimerkiksi kevään Bold Quest 19.1 tapahtumassa onnistuneesti. Keväällä järjestetty, varsin mittava, testaus ja todentamistapahtuma onnistui verkko-teknisesti loistavasti. Puolustusvoimat rakensi yhdessä kumppaneiden kanssa kattavan ja tiedonsiirtokapasiteetiltaan riittävän verkon, jossa kaikki puolustushaarat ja aselajit kykenivät testaamaan ja todentamaan omia järjestelmiään yhdessä kumppanimaiden kanssa.

Kansainvälinen kehitys ja yhteistoiminta edellyttää yhteen toimivia ja sopivia johtamis- ja viestijärjestelmiä. Kansainvälisen yhteistyön merkitys ei tulevaisuudessa varmasti vähentymään. Yhteistyömuodot

voivat olla kahdenvälisiä tai monenvälisiä riippuen tarpeista ja joukoista sekä järjestelmistä. Tätä kirjoittaessa EU-maiden puolustusministerit kokoontuvat Helsingissä pohtimaan yhteistyömahdollisuuksia. Siviili- ja sotilasteknologiat ovat vuosi vuodelta lähentyneet toisiaan. Nykyisin uudet teknologiset ratkaisut tulevat käyttöön ensin siviilipuolelle ja vasta sen jälkeen sotilaskäyttöön. Tulevaisuuden uusia puolustusyhteistyömahdollisuuksia ovat tekoäly, yleinen digitalisaatio ja Big Data eli datamassojen hyödyntäminen. Aika näyttää mihin yhteistyö vie ja mitä se mahdollistaa.

Merivoimat on tehnyt jo pitkään yhteistyötä mm. Ruotsin kanssa merellisen valvonnan saralla. Teknologinen kehitys ulottuu vahvasti kaikkiin puolustushaaroihin. Merivoimat siirtyy vahvasti 2020-luvulle Laivue 2020 -hankkeen myötä. Samaa on tekemässä ilmavoimat HX-hankkeen myötä. Maavoimat on juuri saanut käyttöön M18-järjestelmän, jonka skaalautuvuus ja ohjelmallinen päivittäminen ovat viimeisintä huutoa. Kehityksen kelkasta ei voi jäädä pois tai muutoin potentiaaliset uhkatekijät ajavat ohi. Kyberulottuvuus on yhä uusia muotoja saava toimintaympäristö. Viestiupseeriyhdistyksen julkaisu Kyberajan viestitaktiikkaa pyrkii avaamaan tätä. Kehotankin kaikkia kiinnostuneita hankkimaan ja lukemaan kyseisen kirjan. Lisäksi kannustan kaikkia lukijoita tarttumaan rohkeasti ajankohtaisiin aiheisiin ja kirjoittamaan artikkeleita lehden palstoille. Tämä mahdollistaa laaja-alaista keskustelua ja uusien näkökulmien esiin tuontia, joka johdattaa koko alaa eteenpäin.

Miellyttävää syksyn jatkoa lehden parissa.

Päätoimittaja





TEKSTI: MARIA KEINONEN

KUVAT: MARIA KEINONEN

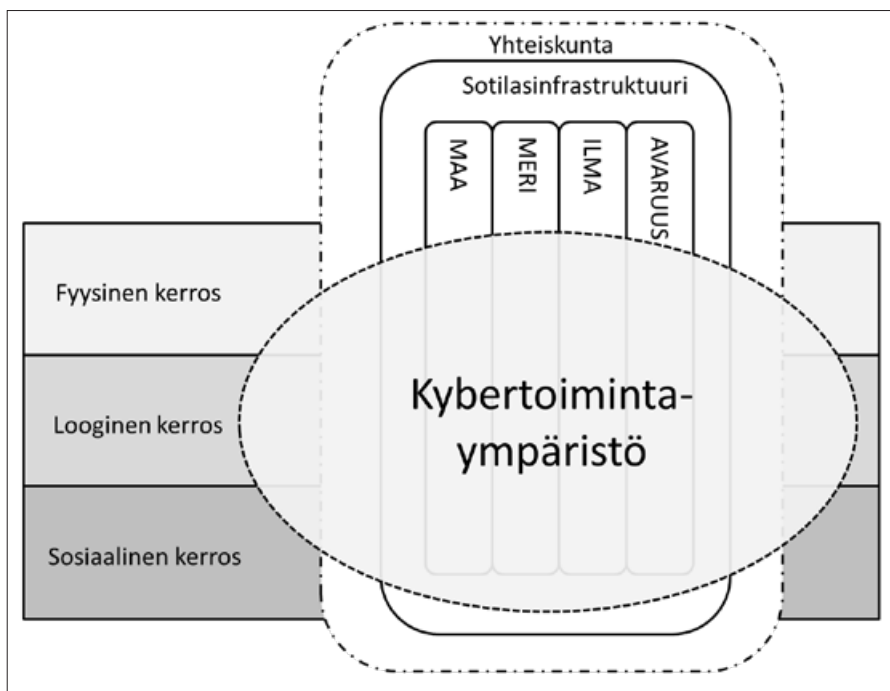
Viestimies kybertoiminta- ympäristössä

(TOIM.)

Kirjoittaja työskentelee Puolustusvoimien johtamisjärjestelmäkeskuksessa ja opiskelee kyberturvallisuuden maisteriohjelmassa Jyväskylän yliopistossa.

Viestimiehen rooli on muutoksessa. Siinä missä yhteiskunta odottaa sotilaalta asiantuntijuutta turvallisuuspolitiikassa, odottavat muut sotilaat viestimieheltä perinteisesti asiantuntijuutta johtamisjärjestelmiin ja tietotekniikkaan liittyen. Teknologian kehityksen myötä odotukset ovat laajentuneet koskemaan myös kybertoimintaympäristön, tekoälyn ja robotiikan tuntemista. Viestimiehen rooli ei ole enää vain asiantuntija tai ongelmien ratkaisija, vaan myös opastava ja valmentava, etenkin tieto- ja kyberturvallisuuteen sekä digitaalisilta uhkilta suojautumiseen liittyen. Tällainen rooli edellyttää viestimieheltä edellä mainittujen osa-alueiden perustuntemusta. Tässä artikkelissa keskitytään kybertoimintaympäristön ominaisuuksien ymmärtämiseen.

Älyteknologian yleistymisen myötä monet aiemmin toisistaan erillään olleet elementit yhdistyvät ja vaativat uudenlaista suhtautumista johtamis- ja asejärjestelmien käyttöön sekä operatiiviseen suunnitteluun ja taisteluiden johtamiseen. Kybertoimintaympäristöä ei tule käsittää perinteisestä sotilaallisesta toimintaympäristöstä erilliseksi elementiksi. Sen sijaan tulee ymmärtää sen liittyminen sotilaallisiin toimintoihin voiman käytön ja oman toiminnan vapauden säilyttämisen näkökulmasta. Viestimies omalla toiminnallaan turvaa tätä toiminnanvapautta.



Kybertoimintaympäristön läpileikkaavuus (Lähde: Nato: AJP-3.20 Allied Joint Doctrine for Cyberspace Operations Version I, Edition A, 2nd Study draft. Kuvaa on muokattu vastaamaan kansallista näkökulmaa.)

Kybertoiminta- ympäristön määrittelyä

Kybertoimintaympäristö on osa taistelulukentaa. Siihen kohdistuu tiedustelua ja vaikuttamista sekä sen osia tarvitsee suojata. Sen avulla voidaan tuottaa vaikutuksia vastustajan toimintaan. Ymmärtääkseen kybertoimintaympäristöä tulee ensin hahmottaa sen rakentuminen ja siihen kuuluvat elementit. Määritelmiä on monia, mutta kybertoimintaympäristöä on yksinkertaisinta lähestyä määrittelemällä se fyysisten ja

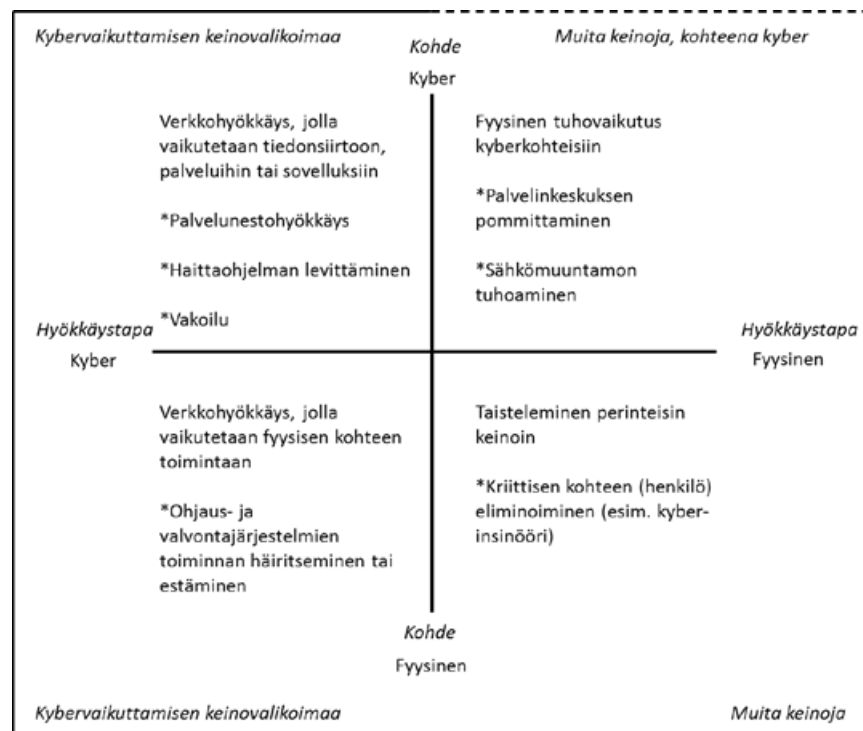
ei-fyysisten elementtien muodostamaksi kokonaisuudeksi.

Fyysisiä elementtejä ovat tiedon käsittelemiseksi tarkoitetut päätelaitteet, kuten tietokoneet, älypuhelimet ja urheilukellot. Fyysisiä elementtejä ovat myös tiedon säilyttämiseen ja siirtämiseen tarkoitetut laitteet ja verkkojen osat, kuten valokuitukaapelit, radiolinkit ja palvelimet. Ei-fyysinen kokonaisuus muodostuu sellaisista elementeistä, jotka mahdollistavat tiedon jakamisen ja käsittelyn tietoverkoissa. Näitä ovat esimerkiksi ohjelmistot,

protokollat ja verkoissa kulkeva data. Ei-fyysinen osuus kybertointaympäristöstä tekee siitä uniikin ja myös erilaisen fyysiseen maailmaan verrattuna. Fyysisestä ja ei-fyysisestä kokonaisuudesta puhutaan usein kybertointaympäristön fyysisenä ja loogisena kerroksena. Tässä artikkelissa puhutaan ei-fyysisistä elementeistä, mutta kerroksiin viitattaessa loogisesta kerroksesta.

Kybertointaympäristöstä puhuttaessa ei tule kuitenkaan unohtaa sen sosiaalista ulottuvuutta, jonka keskiössä on ihminen. Ihminen on kybertointaympäristössä fyysinen toimija omana itsenään, mutta myös virtuaalinen toimija esimerkiksi hallinnoimiensa käyttäjätilien kautta. Näistä virtuaalisista identiteeteistä käytetään usein termiä ”kyberpersoonaa”. Kybertointaympäristön sosiaalisesta ulottuvuudesta tekee monimutkaisen se ominaisuus, että yksilöllä voi olla monta erilaista kyberpersoonaa ja toisaalta taas ryhmä ihmisiä voivat muodostaa keskenään yhden kyberpersoonan esimerkiksi jaetun käyttäjätilin kautta. Kyberpersoonat eivät ole myöskään sidottuja mihinkään tiettyyn fyysiseen sijaintiin, esimerkiksi samaa käyttäjätiliä voivat käyttää ihmiset eri puolilla maailmaa. Kybertointaympäristö jaetaan usein fyysisen ja loogisen kerroksen lisäksi sosiaaliseen kerrokseen tai kyberpersoonakerrokseen, jotka kumpikin tarkoittavat edellä kuvattua inhimillistä ulottuvuutta.

Perinteisesti taistelukentän ulottuvuuksiksi on käsitetty maa, meri, ilma ja avaruus. Jokaisessa ulottuvuudessa toimiminen edellyttää informaatioteknologian käyttöä eri tavoin. Informaatioteknologian käyttöä on esimerkiksi kaikenlainen tietoverkoissa toimiminen sekä johtamis-, TVM- ja asejärjestelmien käyttö. Kybertointaympäristö on yhdistävä elementti näille neljälle ulottuvuudelle. Nykyään kybertointaympäristö käsitetään taistelukentän viidentenä ulottuvuutena, vaikka se ominaisuuksiensa puolesta on enemmän neljää muuta läpileikkaava kuin oma itsenäinen ympäristönsä. Tämä läpileikkaavuus tulee ymmärtää myös asevoimien ja muun yhteiskunnan kytkeytymisenä toisiinsa, koska sotilainfrastrukturi käyttää usein yhteisiä tietoliikennejärjestelmiä, palveluita ja sovelluksia muun yhteiskunnan kanssa. Esimerkkinä tästä voidaan mainita vaikkapa tiedonsiirtoon tarkoitetut



Kybertointaympäristöön vaikuttamisen keinovalikoima (Lähde: Kuusisto, Tuija (toim.): Kybertaistelu 2020, Maanpuolustuskorkeakoulun julkaisusarja 2, No. 1/2014, Juvenes print, Tampere 2014. Kuvaa on muokattu artikkelin aiheeseen sopivaksi.)

langalliset ja langattomat järjestelmät, kaupalliset laitteistot tai Internet.

Kybertointaympäristö toiminnan kohteena ja kanavana

Langatonta tiedonsiirtotekniikkaa hyödyntävien älylaitteiden yleistymisen myötä ovat elektronisen sodankäynnin ja kybersuorituskykyjen käyttö lähentyneet entistä enemmän toisiaan. Samoja järjestelmiä on suojaamisen, tiedustelun ja vaikuttamisen kohteena elektromagneettisen spektrin tai kybertointaympäristön kautta. Joukkojen on kyettävä salaamaan ja suojaamaan oma toimintansa tässä alati muuttuvassa ja monimutkaisessa ympäristössä.

Yhtymäkohtia löytyy myös taistelukentän muista kineettisistä ja ei-kineettisistä toiminnoista. Kybertointaympäristö voi toimia alustana esimerkiksi informaatio-operaatioille ja psykologisille operaatioille. Käytännössä tämä voi tarkoittaa esimerkiksi

bottiarmeijoiden käyttöä propagandan levittämisessä sosiaaliseen mediaan tai jollekin tietylle internet-sivustolle murtautumisen avulla tehtyä valheellisen tiedon levittämistä. Kyberhyökkäyksen vaikutukset itsessään voivat olla psykologista vaikuttamista, jos vaikkapa maksujärjestelmän häiriöiden aiheuttamat hankaluudet aiheuttavat yhteiskunnassa levottomuuksia

Kybertointaympäristön fyysiset, ei-fyysiset ja sosiaaliset elementit voivat toimia taistelukentällä varsinaisena hyökkäyksen kohteena tai välineenä muulle vaikuttamiselle. Kybertointaympäristössä sijaitseviin kohteisiin voidaan vaikuttaa sekä kineettisin että ei-kineettisin keinoin. Jos halutaan esimerkiksi rajoittaa vastustajan tilanetietoisuutta jollain maantieteellisellä alueella, voidaan ensin tuhota fyysisesti paikallisen verkon solmu ja näin pakottaa vastustaja siirtymään johonkin tiettyyn verkkoon ja siihen kohdistuvalla kyberhyökkäyksellä pimentää tilannekuva kokonaan. Vastaavasti kyberhyökkäyksellä voidaan vaikuttaa fyysisten

elementtien toimintaan, esimerkiksi katkaisemalla sähköt tai estämällä polttoaineenjakele valitulla alueella. Kybertoimintaympäristö tarjoaa siis välineitä virtuaalisiin ja fyysisiin kohteisiin vaikuttamiseen ja se voi myös itsessään olla kohde sekä kineettiselle että ei-kineettiselle toiminnalle.

Kyberuhka

Kyberuhkaa voidaan lähestyä pohtimalla, mitä ovat kybertoimintaympäristössä toimivat vihamieliset toimijat, millaisia kohteita vastaan hyökätään, millainen hyökkäysvalikoima on käytössä ja millaisia vaikutuksia hyökkäyksellä voidaan saada aikaan. Vihamieliset toimijat ovat niitä henkilöitä, ryhmittymiä tai organisaatioita, joilla on jokin intressi toimia kyberavaruudessa jotakin toista tahoa vastaan. Näillä toimijoilla on laaja keinovalikoima, jonka avulla haluttu vaikutus kohteessa saadaan aikaan. Kohde on se järjestelmä, johon vaikutus kohdistetaan tai jonka kautta halutaan vaikuttaa johonkin toiseen kohteeseen. Toiminnasta seuraa jokin tietty vaikutus, josta toimija hyötyy.

Kyberhyökkäyksien toteuttajina voi olla sekä valtiollisia että ei-valtiollisia toimijoita. Valtiollisilla toimijoilla on laajat resurssit ja motiivit suorittaa esimerkiksi tiedustelua sotilaallisessa kybertoimintaympäristössä. Ei-valtiolisten toimijoiden motiivina voi olla esimerkiksi rahallisen hyödyn hankkiminen tai ideologiset perusteet.

Kyberhyökkäysten keinovalikoima on laaja. Yksi tapa ryhmitellä keinovalikoimaa on jakaa se neljään kategoriaan: käyttäjän manipulointi, haittaohjelmat, kohteeseen tunkeutuminen ja kohteen elinkaareen vaikuttaminen. Käyttäjän manipulointi tarkoittaa yksilön hyödyntämistä jonkin sellaisen toiminnon suorittamiseen, jolla mahdollistetaan kyberhyökkäyksen toteuttaminen joko suoraan tai paljastamalla informaatiota kohteesta tai toimintaympäristöstä. Käyttäjän manipuloinnin keinoja ovat esimerkiksi sosiaalisen median hyödyntäminen tietojen kalasteluun tai käyttäjän houkutteleva klikkaamaan linkkejä, jotka johtavat haittaohjelman asentamiseen. Haittaohjelmat ovat tietokoneen, älylaitteen tai verkon vahingoittamiseen, hyödyntämiseen

Toiminnan taso/ kybertoimintaympäristön kerros	Taktinen	Operatiivinen	Strateginen
Fyysinen	Yksittäisen taistelijan USB-tikku, älykännykkä tai tabletti	Alueellinen valokuitukaapeliverkko, sähkönjakelujärjestelmä	Valtionhallinnon tai merkittävän julkisen sektorin toimijan palvelinkeskus
Looginen	Komentopaikan tai esikunnan tietokoneiden ohjelmistot	Ilmapuolustuksen tilannekuvasovellus	Ydinaseen laukaisujärjestelmän hallintaohjelma
Sosiaalinen	Yksittäisen joukon tilannekuvasovelluksen admin-tili	Puolustushaaran komentajan tunnukset operatiiviseen järjestelmään	Presidentin tai valtionhallinnon avaintoimijoiden sähköpostitilit

Esimerkkejä eri tasoilla sijaitsevista kybervaikuttamisen ja tiedustelun kohteista kybertoimintaympäristössä (Lähde: Conti, Gregory, Tom Cross, Michael Nowatkowski & David Raymond: Key Terrain in Cyber-space: Seeking the High Ground, 2014 6th International Conference on Cyber Conflict. Brangetto, Pascal, Markus Maybaum & Jan Stinissen (toim.), Viro, 2014. Kuvaa on muokattu artikkeliin sopivaksi.)

tai tunkeutumisen mahdollistamiseen tarkoitettuja ohjelmistoja. Niitä voidaan levittää tietokoneiden lisäksi mihin tahansa verkkoon liitettyyn älylaitteeseen, kuten älypuheliiniin ja tabletteihin. Kohteeseen tunkeutuminen on edellytys kyberhyökkäyksen toteuttamiselle ja se voidaan toteuttaa kolmella tavalla. Fyysinen tunkeutuminen tarkoittaa suoran yhteyden saamista kohdelaitteeseen tai -verkkoon. Haittaohjelma asennetaan esimerkiksi USB-laitteen avulla. Lähiyhteyden avulla tehtävä tunkeutuminen tarkoittaa toimenpiteitä, joilla päästään kohteeseen käsiksi jonkin alueella olevan välillisen yhteyden kautta. Tällainen voi olla esimerkiksi hyödyntämällä WIFI-yhteyksiä tai käyttäjän manipuloinnin avulla, jolloin kohteen lähellä työskenteleviä henkilöitä houkutellaan asentamaan esimerkiksi USB-laite kohteeseen. Etäyhteyden kautta suoritettava tunkeutuminen tapahtuu fyysisen ja virtuaalisen välimatkan päästä kohteesta ja kohdejärjestelmän verkon ulkopuolelta. Kohteen elinkaareen vaikuttamisesta voi tapahtua uuden laitteen toimittamisen tai vanhan laitteen huollon yhteydessä, jolloin laitteeseen asennetaan vahingollisia komponentteja. Nämä voivat vaikuttaa laitteen käyttö- ja tietoturvallisuuteen sekä toimintaan.

Mitä ovat kyberoperaatiot?

Valtioiden asevoimat jakavat kyberoperaatiot eri tavoin riippuen organisaatorakenteista ja asevoimien käyttöperiaatteista. Yhteistä näille on hyökkäykselliset ja puolustukselliset toiminnot. Hyökkäyksellisillä kyberoperaatioilla pyritään saamaan aikaan jokin vaikutus vastustajan toiminnassa. Puolustuksellisilla operaatioilla suojataan omia järjestelmiä ja mahdollistetaan omien joukkojen toiminnan vapaus. Kumpaankin operaatiotyyppiin sisältyy elementtejä tiedustelusta, vaikuttamisesta ja oman toiminnan suojaamisesta.

Kybervaikuttamisella pyritään kieltämään, häiritsemään, tuhoamaan tai manipuloimaan vastustajan kykyä käyttää tieto- ja asejärjestelmiään ja näin ollen kiistämään vastustajan toiminnan vapaus sotilaallisessa toimintaympäristössä. Kybervaikuttamisen keinot voivat kohdistua strategisen, operatiivisen tai taktisen tason kohteisiin. Usein kybervaikuttaminen on osa muuta vaikuttamista, jolloin yhdessä kineettisin ja ei-kineettisin keinoin saadaan aikaan laajempi ja kokonaisvaltaisempi vaikutus, kuin käyttämällä vain yhtä menetelmää. On kuitenkin ymmärrettävää,

että kybervaikuttaminen tarjoaa muiden ei-kineettisten keinojen tavoin lähinnä pehmeitä keinoja, joilla ei ole välitöntä vaikutusta ihmishenkien menetykseen. Se on kuitenkin vahva työkalu yhdistettynä muuhun vaikuttamiseen, jolla voidaan vaikuttaa kokonaisvaltaisesti vastustajan toimintaan.

Kybertiedustelulla tarkoitetaan usein tietoverkkotiedustelua, joka voidaan jakaa edelleen tietoliikennetiedusteluun ja tietojärjestelmätiedusteluun. Tietoliikennetiedustelulla selvitetään verkkoliikenteen sisältöä. Tietojärjestelmätiedustelulla selvitetään kohdejärjestelmän ominaisuuksia ja käyttötapoja. Kyberkohteisiin liittyviä tiedustelukysymyksiä voidaan selvittää useilla tiedustelumenetelmillä, kuten esimerkiksi avointen lähteiden tiedustelulla, signaalitiedustelulla ja henkilötiedustelulla.

Kybersuojaamisen toimenpiteillä suojataan omat tieto- ja asejärjestelmät passiivisin ja aktiivisin keinoin. Passiivisia keinoja voivat olla esimerkiksi ohjelmistojen päivittäminen sekä käyttäjätilien ja pääsyoikeuksien hallinta. Aktiivisia keinoja ovat esimerkiksi havaitun uhkan rajoittaminen ja eristäminen sekä vastahyökkäykset uhkan lyömiseksi. Hyökkäykselliset vastatoimet puolustuksellisisa operaatioissa ovat usein maltillisia ja tähtäävät vastustajan voiman lyömiseen tai vähentämiseen omista järjestelmissä. Suojaamiseen sisältyy myös valvonta, joka kohdistuu omista järjestelmissä havaittujen poikkeamien havaitsemiseen, tunnistamiseen ja rajoittamiseen. Kybersuojaamista ovat myös järjestelmien koko elinkaareen vaikuttavat suojaamisen keinot sekä yksilöiden ja organisaatioiden tietoturvaan tähtäävät toimenpiteet.

Viestimiehen rooli kybersuojautumisessa

Artikkelin alussa todettiin, että viestimiehen ammatilliset vaatimukset ovat muuttuneet. Viestiaselaji ei käsitä enää pelkästään sotilaallisten viestijärjestelmien vaatimaa osaamista, koska digitaalinen ympäristö kytkeytyy monin tavoin yhteiskuntaan ja osittain myös globaaliin informaatioavaruuteen. Kybertoimintaympäristön läpileikkävyyden takia yksikään informaatiota digitaalisesti käsittelevä järjestelmä ei ole täysin eristetty tai itsenäinen.

Kenttäviestijärjestelmäänkin voidaan tunkeutua käyttämällä yhdistelmää elektronisen sodankäynnin ja kybervaikuttamisen keinoista.

Informaatioteknologian käyttö ei ole nykypäivänä enää yksin viestimiehen vastuulla, koska erilaisia teknisiä päätelaitteita on runsaasti käytössä ryhmä- ja yksilötasalla saakka. Päätelaitteiden käyttöönotto, käyttäminen ja yksinkertaisten vikatilanteiden hallinta on jokaisen soturin perusosaamisvaatimus omassa aselajissaan tai toimialallaan sotilasrivistä riippumatta. Samoin näihin laitteisiin ja järjestelmiin liittyvä tietoturvallisuus sekä suojautuminen elektronisen sodankäynnin ja kybervaikuttamisen uhkilta kuuluu jokaiselle taistelijalle.

Kybersuojautuminen koostuu organisaation ja yksilön toimenpiteistä. Organisaation toimenpiteisiin kuuluu muun muassa järjestelmän elinkaaren aikainen kyberturvallisuus alkaen järjestelmän rakentamisesta päättyen siitä luopumiseen sekä ajantasaisen tietoturvan ylläpitäminen kaikissa organisaation järjestelmissä. Kyberturvallisuus tulee rakentaa järjestelmään jo sitä hankittaessa, koska jälkikäteen haavoittuvuuksien paikkaaminen voi olla erittäin haastavaa. Vastaavasti tietoturvallisuuden ylläpitämisen tulee olla jatkuvaa, aktiivista ja ennakoivaa. Tämä sisältää niin tekniset toimenpiteet kuin myös henkilöstön osaamisen kehittämisen. Yksilö onkin kyberturvallisuuden heikoin lenkki, koska yksikin virhe voi johtaa organisaation toiminnan vaarantumiseen. Tämä vuoksi henkilöstön kouluttaminen, säännöt tiedon käsittelemiseen ja muu tietoturvaohjeistus ovat ensiarvoisen tärkeitä tietoturvallisuuden ja kybersuojautumisen keinoja. Henkilöstön tulee tiedostaa oma vastuunsa kyberturvallisuudessa.

Mikä on siis viestimiehen rooli nykypäivän aselajinsa edustajana? Oman substanssiosaamisensa lisäksi viestimiehen tulee hallita edellä mainitut yksilön perustiedot ja -taidot kybersuojautumiseen liittyen. Tämän lisäksi viestimiehen tulisi ymmärtää tässäkin artikkelissa kuvatut kybertoimintaympäristön lainalaisuudet ja kytkeytyminen kaikkeen sotilaalliseen toimintaan, koska ymmärrys syventää viestimiehen ammattitaidon nykypäivän vaatimusten tasolle omalla osaamisalallaan. Oletusarvona on, että viestimies

kykenee ohjaamaan omassa roolissaan muita tietotekniikan käyttäjiä tietoturvallisuuden, elektronisen suojautumisen ja kybersuojautumisen osalta. Tämä asettaa vaatimuksen ymmärtää kybertoimintaympäristössä esiintyviä uhkia ja niiltä suojautumisen keinoja. Näihin sisältyy tietoturvallisuuden toteuttamisen lisäksi myös ymmärryksen sosiaalisen median ominaisuuksista ja niistä psykologisen vaikuttamisen keinoista, joilla voidaan yksilön kautta vaikuttaa koko organisaatioon. Esimerkkinä voidaan mainita käyttäjän manipulointi (Social Engineering), joka sisältää useita erilaisia keinoja saada käyttäjä itse asentamaan haittaohjelma organisaation järjestelmiin. Ei pidä myöskään unohtaa kybertoimintaympäristön fyysistä kerrosta, joka asettaa vaatimuksen ymmärtää muun muassa tilaturvallisuuden merkityksen sekä loogisen verkon häiriöiden suorat vaikutukset fyysisiin laitteisiin.



Patria

Kun kaiken on pakko toimia.





TEKSTI: JYRKI PENTTINEN, TECHNOLOGY MANAGER, GSMA NORTH AMERICA

TkT, ins-ltn (res) Jyrki Penttinen on toiminut telealalla vuodesta 1994 Suomessa, Espanjassa, Meksikossa ja Yhdysvalloissa. Penttinen työskentelee nykyään GSMA:n Pohjois-Amerikan organisaatiossa teknologiapäällikkönä pääaiheenaan 5G. Muitten töittensä ohessa Penttinen on kirjoittanut matkaviestintäaiheisia kirjoja sekä luennoinut televiestintäteknologioista englanniksi, espanjaksi ja suomeksi. Penttisen uusimmat kirjat ovat ”5G Explained” (Wiley) ja ”5G Simplified” (Amazon). Penttisen ajankohtaisiin artikkeleihin voi tutustua osoitteessa www.linkedin.com/in/jypen.

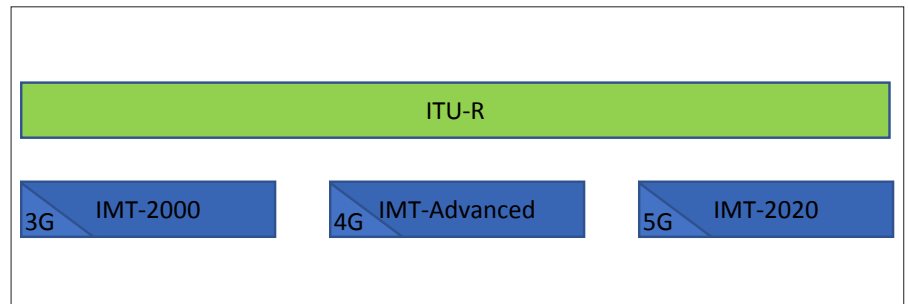
5G-aikakausi alkoi

3GPP sai valmiiksi ensimmäiset 5G-spesifikaatiot tämän vuoden alussa, ja useat operaattorit ovat jo avanneet kaupallisia 5G-verkkojaan. Verkkojen käyttöönotto on kuitenkin vielä alkuvaiheessa, ja kestää siten tovin, ennen kuin pääsemme nauttimaan uuden sukupolven mukanaan tuomista hyödyistä laajemmin.

5G:n määrittäminen

2G-aikakausi avautui suomalaisesta näkökulmasta katsottuna ETSI:n (European Telecommunications Standards Institute) standardoiman GSM:n myötä. GSM toi mukanaan uusia tekniikoita kuten integroidun digitaalisen tiedonsiirron, SIM-kortin tilaajaliittymän tietojen tallentamiseen ja radiorajapinnan suojaamiseen, sekä tekstiviestipalvelun. GSM oli aluksi eurooppalainen, ja siitä kehittyi sittemmin maailmanlaajuinen järjestelmä, joka on käytössä vielä nykyäänkin edustuen suosituinta 2G-järjestelmien varianttia. On kuitenkin odotettavissa, että 2G:n merkitys laskee. Eräinä syinä on sen heikompi spektritehokkuus ja suojaukseen liittyvät haasteet.

UMTS (Universal Mobile Telecommunications System) on kolmannen sukupolven suosituin edustaja. Sittemmin UMTS sekä muut 3G:n versiot, kuten amerikkalainen cdma2000, ovat kehittyneet tasaisen varmasti mahdollistaen



ITU on määrittänyt 3G-, 4G- ja 5G-järjestelmien yleiset vaatimukset.

nykyään datansiirtonopeudeksi satoja megabittejä sekunnissa. 3G oli ensimmäinen sukupolvi, jonka määrittämiseen ITU (International Telecommunications Union) otti kantaa IMT-2000 (International Mobile Telecommunications) -suorituskykyvaatimuksiin.

ITU määrittä puolestaan 4G-järjestelmille vaatimukset IMT-Advanced -dokumentaatioissa. LTE-Advanced, kuten se on standardoitu Release 10:stä lähtien, sekä IEEE:n WiMAX2 täyttivät kyseiset vaatimukset, ja ne edustavat siten virallisesti matkaviestinnän neljättä sukupolvea.

ITU on sittemmin luonut kansainväliset vaatimukset 5G-järjestelmille IMT-2020 -dokumentaatioissaan. Tällä hetkellä näyttää siltä, että 3GPP on ainoa standardointitaho, joka lähettää ehdotuksensa kyseiseen ITU:n eva-

luointiprosessiin ja saa oletettavasti ”ITU-leimalla” varustetun hyväksynnän 5G-järjestelmäksi. 3GPP on kuitenkin vasta työstämässä ensimmäistä aidosti ITU-2020 -yhteensopivaa 5G:n versiota Release 16 -spesifikaatioissaan, jotka valmistuvat näillä näkymin vuoden 2020 alkupuoliskolla. Tällä välillä matkaviestintäteollisuus on edistämässä alkuvaiheen 5G-teknologian käyttöönottoa, ja olemme jo kuulleet useita ilmoituksia ensimmäisistä 5G:n palveluista. Ennen kuin 3GPP:n Release 16 on valmis, ja niiden mukaiset verkkoelementit ja päätelaitteet ovat käytettävissä, edustavat tällä hetkellä käyttöönotettavat verkot ”kevyttä versiota” 5G:stä. Ne perustuvat 3GPP:n Release 15 -spesifikaatioihin, jotka eivät vielä riitä täyttämään IMT-2020 -vaatimuksia.

Kaupallisesta näkökulmasta nähtynä alan toimijat haluavat kuitenkin edistävää 5G-aikakautta nopeammin. Kilpailu ensimmäisistä sijoista on nähtävissä operaattoreiden lehdistöilmoituksista. Yhdysvaltojen Verizon kiirehti 5G:tä tekemällä 5GTF-työryhmässä oman versionsa tuolloin vielä työn alla olevien 3GPP:n Release 15 spesifikaatioihin pohjautuen. Ennen 5G:n matkaviesintäratkaisuja, on markkinoilla ollut myös kiinteästi käytettäviä 5G-ratkaisuja (FWA, Fixed Wireless Access), joita voidaan verrata tavallaan Wi-Fi-laitteiden periaatteeseen pohjautuen 3GPP:n 5G-spesifikaatioihin. Oman standardinsa jälkeen Verizon avasi kaupallisen, nyt 3GPP-standardeihin perustuvan 5G-mobiiliverkkonsa keväällä 2019 rajoitetuilla alueilla samalla, kun muut isot yhdysvaltalaiset mobiilioperaattorit ovat avanneet omia kaupallisia 5G-verkkojaan. Tällä välillä Etelä-Korea on ollut erityisen aktiivinen, ja maan operaattorit tarjoavat vahvasti laajentuvaa 5G-peittoaluetta vuoden 2019 alusta lähtien. Muita 5G-verkkoja on avattu vähitellen Euroopassa, Australiassa ja Aasiassa, ja Release 15:n mukaiset ensimmäisen vaiheen 5G-verkot yleistyvät rauhalliseen tahtiin tämän vuoden aikana.

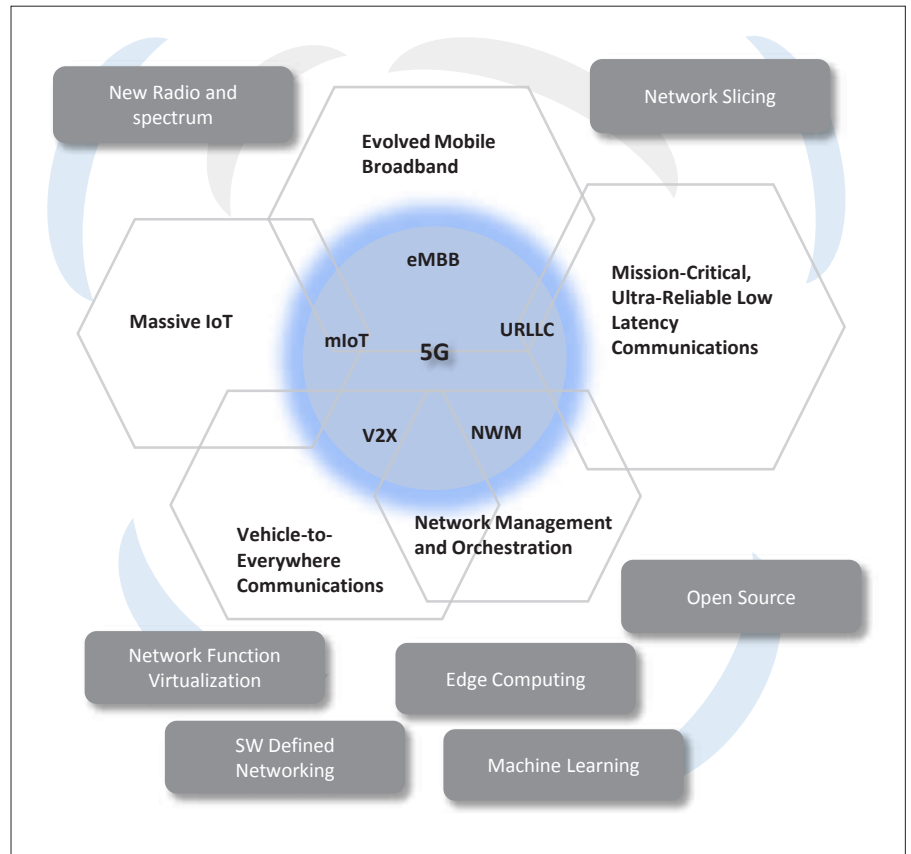
3GPP saa valmiiksi 5G:n toisen vaiheen, eli Release 16:n mukaiset tekniset spesifikaation vuoden 2020 alussa, ja niihin perustuvat laitteet ja verkot alkavat olla käytössämme vuoden 2020 paremmalla puolella. Siinä, kun tämän vuoden ensimmäinen tarjoaa lähinnä nopeampaa datansiirtoa, vaiheen kaksi 5G sisältää monia lisätoiminnallisuuksia ja edelleen parannetun suorituskyvyn.

Mikä tekee 5G:n?

Jos Release 16 on vasta työn alla, mikä sitten on riittävä toiminnallisuus ja suorituskyky ”täysveriselle” 5G:lle? Tähän vastauksen antaa parhaiten IMT-2020.

ITU:n suositus ITU-R M.2083 kuvaa IMT-2020:n yleisnäköt. Niiden mukaisesti 5G:n tulee tarjota edistysellisiä toiminnallisuksia, jotka ovat huomattavasti kehittyneempiä kuin aiempi, 4G:n kuvaava ITU-R M.1645 -vaatimussetti sisältää.

IMT-2020:n kuvaama 5G:n ekosysteemi liittyy niin käyttäjien kokemaan



5G:n peruspilarit. Lähde: J. Penttinen, *5G Simplified* (Amazon eBook, 2019).

suorituskykyyn kuin laitevalmistajien, sovelluskehittäjien, verkko-operaattoreiden kuin palvelun- ja sisällöntarjoajien rooleihin. IMT-2020 tukee siten useita eri 5G-palveluiden käyttöönotto-tilanteita eri ympäristöissä. Esimerkkinä mainittakoon massiivinen esineiden Internet (mIoT, Massive Internet of Things), joka on yksi 5G:n peruspilareista. Siitä voidaan käyttää myös nimitystä mMTC, Massive Machine-Type Communications, eli massiivinen laitteiden välinen liikennöinti. 5G:n on tuettava eräitä moodeja mahdollistaen miljoona yhtäaikaisesti viestivää IoT-laitetta neliökilometrin alueella.

Kuten on ollut tilanne 3G:n ja 4G:n osalta, ITU edustaa korkeinta auktoriteettia myös 5G:n määrittämisessä. ITU:n vision mukaisesti uusi sukupolvi toimii alustana saumattomalle, kaiken yhdistävälle yhteiskunnalle vuodesta 2020 lähtien. 5G:n korkean tason ajatuksena on yhdistää ihmisten ja esineiden viestintä, ml. datansiirto, sovellukset, siirtojärjestelmät, ja kokonaiset kaupungit toimintoihin älykkään yhteen kytketyn viestintäympäristön kautta. Tämän vi-

sion toteutukseen ITU on luonut pohjan 5G:n peruspilareista, joihin kuuluvat mIoT:n lisäksi kehittynyt mobiililaajakaista (eMBB, evolved Mobile Broadband), kriittinen viestintä (URLLC, Ultra Reliable Low Latency Communications) sekä kehittynyt verkonhallinta.

ITU:n dokumentti ITU-R M.2083 sisältää konkreettiset määrittäykset IMT-2020:n mukaisten 5G-järjestelmien suorituskyvyn vaatimuksille. Kyseiset vaatimukset on jaotettu edelleen käyttökohteiden mukaisesti. 5G:n peruspilareitten tukemat ympäristöt voivat erota huomattavasti toisistaan, joidenkin vaatiessa tukea suurelle määrälle samanaikaisesti viestittäviä sensoreita siinä, kun esimerkiksi kriittisen viestintän sovellukset vaativat luotettavaa ja nopeaa tiedonsiirtohyteyttä.

Tärkeimpiä IMT-2020:n vaatimuksia ovat seuraavat.

Huippudatanopeus (peak data rate) tarkoittaa suurinta mahdollista, hetkitäistä datansiirtonopeutta ideaalisessa, tiedonsiirrolle virheettömässä radioym-

päristössä yksittäisen päätelaitteen osalta. Tämä vaatimus on merkityksellinen eMBB-käyttöympäristölle, joka mahdollistaa alalinkkiin (DL, downlink) huippunopeuden 20 Gb/s siinä, kun ylälinkin (UL, uplink) datanopeus on maksimissaan 10 Gb/s.

Huippuspektritehokkuus (peak spectral efficiency) tarkoittaa huippu-datanopeuden normalisointia hertsia kohti (b/s/Hz), edelleen yksittäiselle päätelaitteelle ideaaliympäristössä. ITU:n vaatimus alalinkille on 30 b/s/Hz ja ylälinkille 15 b/s/Hz.

Käyttäjän kokema datanopeus (user experienced data rate) saadaan tutkimalla käyttäjän kokonaisdatanopeuden kumulatiivista jakaumaa 5%:n kohdalla. Datansiirto tapahtuu tässä tapauksessa OSI-mallin kerroksella 3, ja oletetaan virheettömäksi aktiivisen datansiirron ajan. ITU vaatii käyttäjän kokemalle datansiirrolle alalinkissä 100 Mb/s ja ylälinkissä 50 Mb/s.

Käyttäjän spektritehokkuus 5%:n kohdalla (5th percentile user spectral efficiency) tarkoittaa normalisoidun käyttäjän datansiirtonopeuden (b/s/Hz) 5%:n kiinnepistettä, ja on suhde virheettömästi vastaanotettujen OSI-kerroksen 3 datapakettien lukumäärästä aikayksikössä ja kanavan kaistanleveydestä. Tämä vaatimus on jälleen merkityksellinen eMBB-käyttökohteille. ITU:n vaatimukset on jaettu seuraaviin ympäristöihin:

- Sisätilat (hotspot): 0.3 b/s/Hz (DL) ja 0.21 b/s/Hz (UL);
- Kaupunkitihentymä: 0.225 b/s/Hz (DL) ja 0.15 b/s/Hz (UL);
- Maaseutu: 0.12 b/s/Hz (DL) ja 0.045 b/s/Hz (UL), poissulkien laajan solun hitaat päätelaitteet.

Keskiarvoinen spektritehokkuus (average spectral efficiency), eli lyhyemmin spektritehokkuus, tarkoittaa yhdistettyä tehollista datansiirtoa (throughput) ottaen huomioon kaikkien käyttäjien yhtäaikainen datansiirto. Spektritehokkuus lasketaan OSI-kerroksella 3 oikein vastaanotettujen datapakettien lukumäärällä mittaussaikana jaettuna kanavan kaistanleveydellä ja lähettimillä. ITU vaatii spektritehokkuudelle seuraavat arvot:

- Sisätilat (hotspot): 9 b/s/Hz/TRxP (DL) ja 6.75 b/s/Hz/TRxP (UL);
- Kaupunkitihentymä (Macro TRxP): 7.8 b/s/Hz/TRxP (DL) ja 5.4 b/s/Hz/TRxP (UL);

- Maaseutu, mukaan lukien laajan solun hitaat päätelaitteet: 3.3 (DL) ja 1.6 (UL).

Muuta ITU:n IMT-2020 -vaatimuksia ovat seuraavat:

- Datansiirron viive (latency) kuormittamattomassa verkossa, jonka tulee olla 4 ms eMBB-ympäristössä, ja 1 ms URLLC-käyttöympäristössä pienille paketeille.
- Merkinannon viive puolestaan tarkoittaa joutotilasta aktiivitilaan siirtymistä URLLC-käyttöympäristössä. ITU:n vaatimus tällöin on maksimissaan 20 ms, ja suositeltavana parempi kuin 10 ms.
- Yhteyksien tihentymä tarkoittaa alueella viestivien 5G-laitteiden määrittämistä lukumäärää siten, että ne vielä täyttävät tiedonsiirron laatuvaatimukset. Tämä vaatimus on relevantti mIoT-ympäristöön, ja ITU vaatii verkon tukea miljoonalle laitteelle neliökilometriä kohti.
- Energiatietäisyys on relevantti eMBB-ympäristöihin siten, että radioteknologioiden on tuettava pitkää päätelaitteen "nukkumisaikaa". Joissakin tapauksissa 5G-IoT-laitteet voivat "nukkua" esimerkiksi kuu-kauden, ja "herätä" lyhyesti lähettämään mittaustietoa. Kyseiset laitteet saattavat perustua paristoihin, joiden käyttöaika saattaa olla 5-10 vuotta.
- Tiedonsiirron luotettavuus on relevantti URLLC-kommunikointiin. ITU määrittää luotettavuuden ISO-kerroksella 2 vastaanotettujen 32-bittisten pakettien vastaanottoa 1 ms:n periodeissa siten, että niiden virhetodennäköisyys on maksimissaan 1×10^{-5} solun reuna-alueella. Tämä vaatimus on relevantti URLLC-ympäristössä.
- Päätelaitteen nopeus siten, että vaadittava palvelun laatu ei vielä täytyy. IMT-2020 määrittää useita skenaarioita laitteen nopeudelle, jotka vaihtelevat paikallaan pysyvistä laitteista aina 500 km/h etenevään laitteeseen.
- Liikkuvuuden katko aika päätelaitteen ja tukiaseman välillä on relevantti eMBB- ja URLLC-ympäristöille, ja on asetettu 0 ms:iin.
- Kaistanleveys tarkoittaa maksimia eri taajuuksien yhdistettyä kokonaisleveyttä. ITU vaatii minimissään 100 MHz:n tukea, ja 5G:n on tuettava skaalattavia kaistoja 1 GHz:iin saak-

ka korkeilla taajuuksilla kuten yli 6 GHz:llä.

Yhteenvedona ITU:n IMT-2020 -dokumentin vaatimuksista voidaan todeta, että ne ovat kokonaisuudessaan huomattavasti tiukempia kuin aiemmil- le sukupolville. 3GPP:n Release 15 ei vielä sisällä vaadittavia toimintoja kaikkien vaatimusten täyttämiseen, mutta on oletettavaa, että Release 16 tukee tarvittavat toiminnallisuudet kyseisten vaatimusten täyttämiseksi.

5G-arkkitehtuuri

5G jatkaa 4G-LTE:n peruseriaatetta täysin IP-pohjaisesta tiedonsiirrosta. Siten 5G:ssä ei ole piirikytkentäisiä puheluita, vaan puhepuhelut välitetään pakettimuotoisesti joko erillisen sovel-luksen avulla, tai verkkoon integroituna VoNR-palveluna (Voice over New Radio).

5G muuttaa kuitenkin aiempien matkaviestintäverkkojen periaatteita merkittävästi. Perinteisen referenssi-arkkitehtuurin sijaan 5G toimii palvelupohjaisen arkkitehtuurimallin mukaisesti. Tämä on mahdollista verkon toimintojen virtualisoinnin myötä (NFV, Network Functions Virtualization) ja ohjelmistopohjaiseen toimintaan perustuen (SDN, Software Defined Networking). Niiden ansiosta 5G-verkon suorituskykyä voidaan parantaa merkittävästi. Siinä, kun aiemmissa verkkoarkkitehtuureissa käytetään tehtäväkohtaisia elementtejä kuhunkin verkon toimintoon, 5G käyttää yhteistä laitekapasiteettia, ja verkkotoimintojen prosessointi tapahtuu instansseina.

5G mahdollistaa myös entistä paremmin datansiirto- ja merkinantotasojen erittelyn, jolla voidaan edelleen optimoida verkon suorituskykyä. Yhtenä esimerkkinä, 5G:n datansiirto voidaan ohjata nopeana eMBB-palveluna 5G-infrastruktuurin kautta, ja aiempaa 4G-verkkoa voidaan käyttää merkinantoliikenteen välittämiseen.

Samoin, 5G:n myötä prosessointia ja sisältöä voidaan suorittaa entistä tehokkaammin verkon reunalla edge-tekniikan mukaisesti. Yhtenä esimerkkinä edgen hyödyistä on virtuaalitodellisuussovellusten (VR, Virtual Reality) toteuttaminen siten, että 5G-päätelaitetta voidaan käyttää lähinnä edullisena näyttöpäätteenä siinä, kun 5G:n edge prosessoi VR-sisällön. 5G:n mahdol-

listamat minimilattenssijat puolestaan mahdollistavat VR-sovelluksen vaatimat lähes reaaliaikaiset vasteajat.

5G avaa täysin uusia teknisiä ja kaupallisia malleja. Koska 5G perustuu verkon virtualisointiin, kytkentäverkon asennus onnistuu luontevimmin tukeutuen datakeskusten tarjoamiin palveluihin ja kapasiteettiin. Koska kaikki operaattorit eivät välttämättä halua rakentaa omaa pilvi-infrastruktuuriaan, avaa se uusia liiketoiminnan mahdollisuuksia pilvipalveluntarjoajille.

5G poikkeusoloissa

5G perustuu nk. verkkopaloitteluun (network slicing). Se tarkoittaa toiminnallisuutta, jolla fyysinen radio- ja kytkentäverkko voidaan toteuttaa luomalla yksi tai useampia virtuaaliverkkoja, joista kunkin suorituskyky voidaan optimoida tietyille käyttöympäristöille.

Siten yksi ”verkkopala” voi tarjota nopeaa datansiirtoa, vaikka videopuheluihin, kun toinen verkkopala voi palvella pienikapasiteettisia, yhtäaikaan viestiviä sensoreita. Hyötynä tästä on verkkokapasiteetin ja -suorituskyvyn optimointia siten, että käyttäjien kokema laatu voidaan samalla maksimoida. Lisäksi, verkkopaloja voidaan luoda ja poistaa dynaamisesti tarpeen mukaan. Siten esimerkiksi pelastuslaitoksen tapahtumapaikan kenttäviestikeskus voi tukeutua poikkeustilan aikana erityiseen viranomaisverkkopalaan, joka mahdollistaa prioriteettipuhelut ja nopean, drooniin perustuvan videonsiirron korkeimmalla prioriteetilla tapahtumapaikalta.

5G on myös uudistanut verkon turvallisuusnäkökohdat täysin, mikä hyödyntää verkon käyttäjiä. Eräs vaihtoehto on siten käyttää 5G-infrastruktuuria varmentavana erillisverkkona maanpuolustuksen ja viranomaisten tarpeisiin.



MILCON

Valmis vaativien kumppaneiden haasteisiin

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



MILCON OY

Kolmionkatu 5 D
33900 Tampere.

Puh. 010 239 2170
info@milcon.fi

www.milcon.fi

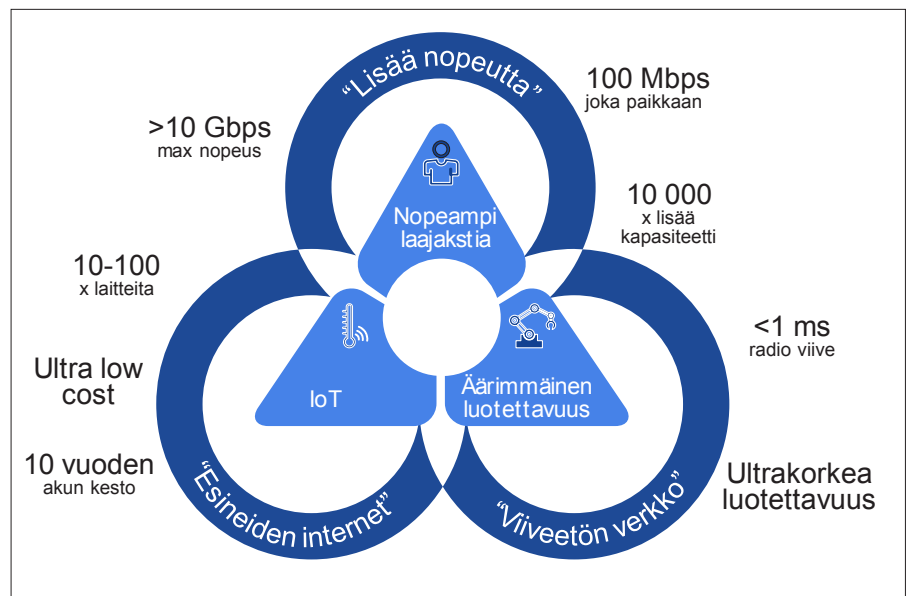
TEKSTI JA KUVAT: HARRI HOLMA¹, MIKA RAITOLA², PEKKA ISOMÄKI², JYRI PUTKONEN¹
¹NOKIA BELL LABS, FINLAND, ²TELIA FINLAND

5G-teknologia tuo nopeata datasiirtoa, suurta luotettavuutta ja pientä viivettä

5G-tavoitteet

5G-radioteknologia on iso harppaus eteenpäin langattomien verkkojen kyvykkyudessa. 4G/LTE-verkot oli suunniteltu tarjoamaan yhteyksiä älypuhelimiin, tietokoneisiin ja tabletteihin kuluttajille. 5G-verkot tarjoavat lisää siirtonopeutta ja kapasiteettia kuluttaja-asiakkaille mutta sen lisäksi 5G on suunniteltu mahdollistamaan suurta luotettavuutta ja lyhyttä viivettä vaativien sovellusten toteuttamisen langattomien verkkojen yli. 5G-verkkoja voidaan siten hyödyntää esimerkiksi tehtaiden sisällä paikallisesti tai koneiden etäohjaukseen koko maan alueella. 5G-verkot tulevat mahdollistamaan tuotantoprosessien ja logistiikan automatisoinnin ja digitalisoinnin, ja sitä kautta parantamaan tuottavuutta. 5G-verkoista tulee merkittävä osa tulevaisuuden turvallisuuden kannalta kriittistä infrastruktuuria. 4G-verkot yhdistivät ihmiset internetiin ja toisiinsa. 5G-verkot yhdistävät lisäksi koneet, esineet ja laitteet internettiin.

Kuva 1 esittää 5G:n pää tavoitteet: lisää siirtonopeutta ja kapasiteettia, esineiden internetin (IoT, Internet of Things) sekä pienen viiveen ja suuren luotettavuuden radioyhteyden. Tavoitteena on mahdollistaa jopa 10 Gbps siirtonopeus, alle 1 millisekunnin viive ja 99.9999% luotettavuus. Ensimmäinen vaihe siirtymisessä kohti 5G-kyvykkyksiä on tapahtumassa jo 4G-verkkojen päälle, kun Suomen viranomaisvies-tintä (Virve) siirtyy vähitellen omasta Tetra-standardin verkostaan käyttämään julkisia 4G/5G verkkoja alkaen 2020.



Kuva 1. 5G:n tärkeimmät tavoitteet.

5G-teknologiaratkaisut

5G:n tavoitteet on asetettu korkealle ja niiden saavuttaminen vaatii uudenlaisia teknologioita, joita ei ollut käytössä vielä 4G-verkoissa. Kuva 2 esittää viisi tärkeintä uutta teknologiaa.

Uudet taajuudet. 5G on suunniteltu käyttämään 400 MHz ja 90 GHz välisiä taajuuksia eli 5G voi hyödyntää monenlaisia taajuusalueita. Yhdistämällä eri taajuuksia voidaan mahdollistaa suuria siirtonopeuksia ja laajoja peittoalueita.

Keilanmuodostus. 5G on suunniteltu hyödyntämään keilanmuodostusta heti alusta lähtien. Keilanmuodostus parantaa taajuustehokkuutta ja lisää peitto- aluetta.

Verkon viipalointi. 5G-verkot tukevat viipalointia, missä luodaan virtuaalisesti dedikoituja verkkoja 5G-verkon sisälle eli dynaamisesti allokoidaan verkon resursseja takaamaan haluttu viive- ja luotettavuustaso.

Yhteistoiminta LTE kanssa. 5G-verkot on suunniteltu toimimaan yhdessä LTE:n kanssa. Päätelaitte voi vastaanottaa LTE- ja 5G-signaalia yhtä aikaa. LTE ja 5G voivat myös käyttää samaa taajuuskaista yhtä aikaa, jolloin siirtymä LTE:sta 5G:hen tulee olemaan joustavaa.

Pilvioptimointi. 5G-verkkojen arkkitehtuuri on rakennettu mahdollistamaan toimintojen virtualisointi pilveen.

5G-taajuuudet

5G on ensimmäinen radiojärjestelmä, joka pystyy hyödyntämään laajasti erilaisia taajuuksia. Alkuvaiheen 5G-verkot Suomessa ja monessa muussakin maassa käyttävät 3.5 GHz taajuutta, missä on tyypillisesti 100 MHz kaista käytössä operaattoria kohti. Suomessa tilanne on vielä parempi eli kaistaa on 130 MHz per operaattori. Tämä mahdollistaa jopa 2 Gbps teoreettisen siirtonopeuden. Hyödyntämällä keilanmuodostusta 3.5 GHz kaistalla saadaan käytännössä samanlainen verkon peittoalue kuin 2 GHz kaistalla 4G-verkoissa. 5G voi siten suoraan hyödyntää olemassa olevia tukiasemapaikkoja ja mastoja. 5G-verkot käyttävät myös vuodesta 2020 lähtien alempia taajuuksia 700 – 2600 MHz alueilta. Näillä taajuuksilla voidaan rakentaa tehokkaasti koko maan kattava verkko. Käyttämällä korkeampia, niin sanottuja millimetri-alueen taajuuksia 24 – 39 GHz, saadaan paikallisesti hyvin suuria datanopeuksia ja kapasiteetteja. 5G:n tyypilliset taajuuudet, peittoalueet ja siirtonopeudet on esitetty kuva 3:ssa.

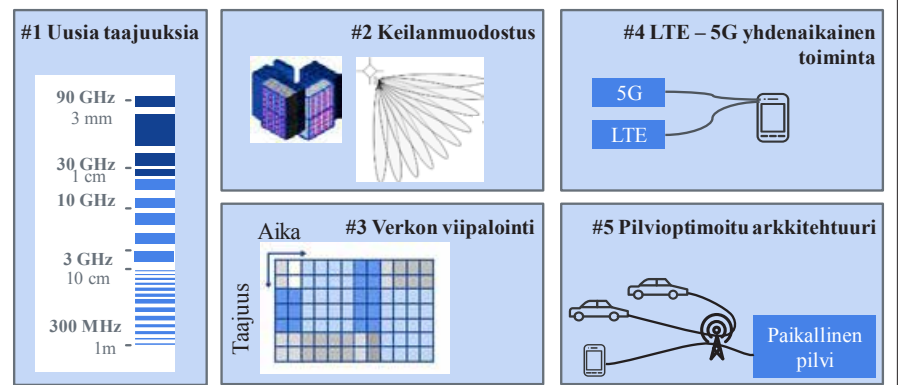
5G – Mitä se tarjoaa palveluille

Yksi menneen kesän trendi oli sähköpotkulautojen vuokrauspalvelut, jotka herättivät sekä innostusta, että myös vihaustunutta keskustelua. Se mikä jäi vähemmälle näissä palveluissa on kuinka kokonaisvaltaisesti niiden kokemus hyödyntää langatonta teknologiaa. Niin niiden vuokraamiseen tarvittava sovelus, kuin lauta itsessään hyödyntävät jatkuvaa langatonta teknologiaa, eli 4G-verkkoja.

Tämä on alku pohdinnalle, kuinka seuraavan sukupolven 5G-verkot vaikuttavat palveluihin, joita kuluttajat ja yritykset saattavat kokea.

Lisää kapasiteettia ja nopeutta, vähemmän ruuhkaa

5G-verkot ovat selvästi nopeampia kuin 4G-verkot. Tämä tarkoittaa sekä nopeampia palveluita, että enemmän kapasiteettia, joka vähentää verkon hektisyyttä ruuhkatilanteita.



Kuva 2. 5G:n uudet teknologiat.

Taajuus-kaista	Taajuus per operaattori	Maksimi datanopeus	
20-90 GHz	1 GHz	5-20 Gbps	
1 – 6 GHz	100 MHz	2 Gbps	
Alle 1 GHz	10 MHz	0.2 Gbps	

Kuva 3. 5G:n käyttämät taajuuudet.

Miten kuluttaja sitten hyötyy 5G-laitteista? Videosovelluksia ainakin tulee lisää – puhelinhan on nykyään yksi kanava katsoa TV:tä tai yhä useammin Netflixin kaltaisia streaming-palveluita. Tulemme lisäksi näkemään lisätyn ja virtuaalitodellisuuden sovelluksia kasvavassa määrin. Samoin verkkopelaamisen kokemus mobiililaitteilla paranee huomattavasti. Verkkopelaamista on kokeiltu jo useasti 5G:n yli. Ensimmäisen kerran tämä tapahtui Nokian, Telian ja ENCE e-urheilutiimin toimesta Espoossa talvella 2018. Kokemukset ovat olleet hyvin rohkaisevia, ja 5G on selvästi sopiva yhteys tähän käyttöön.

Yksittäisen pelaajan tarpeiden lisäksi, 5G on myös erittäin hyvä yhteys erilaisiin tapahtumiin, joissa on tarve suurelle tiedonsiirtokapasiteetille. Hiljattain Summer Assembly tapahtumassa testattiin 5G-yhteyksiä. Tapahtumassa, jossa on tuhansittain tietokoneita, kaikki tietoliikenneyhteydet ovat kuormitettuna. 5G tuo tällöin lisää kapasiteettia,

ja antaa käyttäjilleen suurinopeuksisen vaihtoehdon.

Myös yrityksille jo 5G:n suuremmasta nopeudesta on paljon hyötyjä. Esimerkiksi yrityksen pilvipalvelut voidaan mobilisoida paremmin. Ensimmäiset selvästi 5G:stä hyötyvät yritykset liittyvät videoon. Esimerkiksi korkealaatuisia videokuvia voidaan siirtää tehtaalta datakeskukseen analysoitavaksi. 5G:n kapasiteettia hyödynnetään muun muassa Helsingissä ABB:n taajuusmuuttajatehtaalla, jossa 5G-tekoälysovellus parantaa työhyvintä ja tehostaa tuottavuutta.

Samaan aikaan on hyvä huomata, että ensimmäiset 5G-päätelaitteet eivät ole pelkästään puhelimia vaan reitittimiä eli hotspot-laitteita tai modeemeita. Eli laitteita, jotka vastaanottavat 5G-radionäköalaa ja jakavat sitä eteenpäin Ethernet-kaapelilla tai WiFillä. Näitä löytyy koodista esimerkiksi langattoman laajakaistan reitittiminä. Keväällä esimerkiksi Telia kertoi aloittavansa Nokian FastMile reitittimen pilotoinnin.

Lyhyestä viiveestä hyötty muun muassa älyliikenne

5G-verkon viive on pienempi kuin 4G:ssä. Lyhyt vasteaika mahdollistaa täysin uusien teknologisten ratkaisujen hyödyntämisen muun muassa yrityskäytössä.

Lyhyt viive helpottaa ja nopeuttaa teollisuuden prosesseja. Etäohjattavilla koneilla kuten droneilla päästään paikkoihin, jotka ovat ihmisten ulottumattomissa. Itseohjautuvia ajoneuvoja ja koneita taas voidaan hyödyntää vain, jos ne voivat viestiä keskenään viiveettä ja reagoida välittömästi virhetilanteisiin. 5G tekee näistä scifi-elokuvien kuvitelmista totta.

Kuten alun sähköpotkulautaesimerkki osoitti, uusia liikennevaihtoehtoja kehittää nyt aktiivisesti. Käynnissä on myös monia itseohjautuvan tai etäohjattavan liikenteen kokeiluja. Itseohjautuvan liikenteen startup-yritys Sensible 4 kokeili syksyllä 2018 yhdessä Nokian ja Telian kanssa itseajavaa autoa, jonka tietoliikennettä hoiti 5G-verkko. Kesällä 2019 älyliikenneyritys Roboride aloitti itse ajavan liikenteen kokeilun teollisuusalueella Porissa.

5G teollisuuden kriittiseen käyttöön

Lyhyestä verkon viiveestä tulevat myös hyötymään monet teolliset prosessit, jotka vaativat nopeaa ja automaattista seurantaa tai säätöä. Näitä kokeiluja on jo aloitettu, mutta kehitys tulee jatkumaan pitkään. Erityisesti tässä kohtaa tullaan hyötymään vasta standardoinnin alla olevista 5G-ominaisuuksista, jotka tulevat käyttöön tulevina vuosina. Jo tähän mennessä asioita on kokeiltu esimerkiksi Nokian Oulun tukiasematehtaalla, jossa reaali-aikainen videoanalytiikka opasti työntekijää asennustyössä. Teollisuuden 5G-sovelluksien tutkimusta vauhdittaa myös 5G Viima -projekti, jonka yksi testialue on Oulun sataman ja paperitehtaan ympäristö.

Erityisesti teollisuuden kohdalla nousevana trendinä on yrityskohtaiset verkot. Näillä toteutetaan sekä uusia käyttötapauksia sekä aikaisemmin yrityskohtaisten WLAN-verkkojen käyttötapauksia. On useita tapoja tuoda 5G teollisuusalueille. Se voi olla osa julkis-



Kuva 4. Joona Leppanen eli 'natu' ENCE tiimistä testaamassa 5G-yhteyttä pelamiseen.



Kuva 5. 5G-tekoälysovellus avustaa ABB:n taajuusmuuttajatehtaalla kokoonpanotyössä.



Kuva 6. Nokia FastMile 5G-reititin, jolla voidaan esimerkiksi toteuttaa kotien laajakaistayhteydet 5G-verkkoa hyödyntäen.

ta mobiiliverkkoa, kuten on aikaisemmin tehty 4G:n osalta. Tai 5G-verkosta voidaan tarjota yrityksille parempaa laatua ja taattua kaistanleveyttä verkon viipalointiominaisuuksien (slicing) avulla. Yrityksille voidaan myös rakentaa oma dedikoitu 4G/5G-verkko (private network).

5G:ssä on useita ominaisuuksia, jotka mahdollistavat hyvinkin kriittisten sovellusten käytön. Verkon viipaloinnilla voidaan taata kaistaa tai viivettä esimerkiksi viranomaisten käyttöön tai teollisiin tarpeisiin. Tällöin haluttu käyttötarkoitus saa enemmän verkon resursseja kuin muut käyttötarkoitukset. Yritystai paikkakohtaiset verkot voivat olla paljon 'vahvemmin' rakennettuja kuin julkiset verkot. Esimerkiksi redundanssia voidaan moninkertaistaa tai vastavasti verkko voi olla täysin eristetty. Lisäksi 5G-teknologia on hiljattain standardoitua, joten siinä on kyetty varautumaan uusimpiin tietoturvauxkiin. Samoin pilvipohjainen verkkoteknologia mahdollistaa ratkaisun päivityksen, jos uusia uhkakuvia syntyy.

Internet of Things ottaa harppauksen eteenpäin

5G:llä on iso rooli myös esineiden internetin kehityksessä, sillä 5G-verkoon voidaan liittää erilaisia laitteita massiivisia määriä. Antureiden avulla voidaan kerätä dataa periaatteessa mistä tahansa ja hyödyntää sitä muun muassa ennakoivassa huollossa, päätöksenteossa ja uudenlaisten, dataan pohjautuvien liiketoimintamallien kehittämisessä.

IoT-anturit eivät sinänsä ole mullistus, sillä erilaista tilannetietoa kerätään ja hyödynnetään jo nyt. 5G:n myötä dataa voidaan kuitenkin kerätä entistäkin useammasta paikasta ja muodostaa siten kattavampi kokonaiskuva.

5G-aikataulu

5G-teknologia on määritelty 3GPP-organisaatiossa, missä suurimman työn ovat tehneet verkko- ja päätelaitevalmistajat mukaan lukien Nokia. Ensimmäinen 5G-speksiversio valmistui vuoden 2018 lopussa. Ensimmäiset kaupalliset verkot on avattu keväällä 2019. Laajimmat 5G-verkot löytyvät Etelä-Koreasta, missä on jo lähes 200.000 5G-tukiasemasektoria



Kuva 7. Sensible4 yrityksen autonominen ajoneuvo kokeilemassa 5G-yhteyksiä tiedonsiirtoon.



Kuva 8. Roboride yrityksen 'Robo' huolehtii vierailijoiden kuljetuksista teollisuusalueella, jossa vieraat eivät saa liikkua itsenäisesti ilman saattajaa.



Kuva 9. Oulun Nuottasaaren teollisuusalue. 5G-sovelluksia kehitetään mm. Telian ja Stora Enson yhteistyössä. 5G Viima -projekti tutkii ja kehittää teollisia 5G-sovelluksia. Projektissa on mukana esimerkiksi Oulun satama, joka näkyy myös kuvassa.

käytössä ja vuoden 2019 loppuun mennessä jo lähes 10% asukkaista käyttää 5G-päätelaitetta. Myös Suomessa ensimmäiset 5G-verkot on avattu 2019 ja peittoalue laajenee vähitellen vuoden 2019 ja 2020 aikana. Ensimmäinen vaihe tarjoaa käyttäjille lisää siirtonopeutta: maksiminopeudet yli 1 Gbps ja käytännön nopeudet satoja Mbps. Nämä nopeudet ovat jo niin korkeita, että 5G yhteyttä voidaan tehokkaasti käyttää korvaamaan myös kodin laajakaistaliittymä ja tarjoamaan lähes kuituyhteyden veroista palvelua. Seuraavassa vaiheessa 5G mahdollistaa myös uusia viivekriittisiä palveluita alkaen vuodesta 2020. Samalla 5G tuodaan myös

2018	2019	2020
3GPP spesifikaation valmistuminen	5G verkkojen avaus. Lisää datanopeutta.	5G vaihe 2. Uusia 5G palveluita.

Kuva 10. 5G:n aikataulut.

alemmille taajuuskaistoille. Suomi on 5G:n kehityksessä yksi maailman johtavia maita: Suomessa käytetään nykyisin enemmän mobiilidataa kuin missään muualla maailmassa eli yli 1 gigatavu per asukas per päivä. Tarve 5G:n kapasiteetille on siis selkeä. Suomessa on

myös allokoitu oleelliset 5G- taajuudet – 3.5 GHz ja 700 MHz – operaattoreille, mikä mahdollistaa 5G-verkkojen rakentamisen. Suomessa tehdään myös merkittävää 5G-tutkimus- ja tuotekehitystyötä Nokialla ja yliopistoilla. 5G:n aikataulu on esitetty 10:ssä.

TELIA CYGATE TAKAA TURVALLISUUDEN 24/7

Varmistamme ehdottoman luottamuksen ympäristösi toimijoiden tiedonsiirron välillä parhaalla mahdollisella tavalla.

Takaamme juuri tarpeisiisi optimoidut ratkaisumallit vahvalla tietoturvaosaamisellamme ja lohkoketjuteknologian asiantuntijuudellamme.

www.teliacygate.fi





SISÄRADIOVERKOT

VIRVE- ja monioperaattoriverkkojen
toteutus luottamuksellisesti
avaimet käteen -periaatteella.

EMP/HPM-SUOJAUS

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

FITELNET OY, JOUKONTIE 42 A, VANTAA

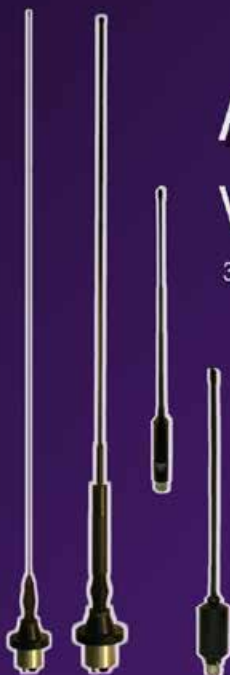
Fitelnet



ADAPTIIVISET VHF / UHF ANTENNIT

30 - 90 MHz / 30 - 520 MHz

- Linkkipituuden tuplaus
- Neljä kertaa isompi solukoko
- Signaali-kohinasuhteen parannus
- Pienemmät antennit
- Matalampi tehonkulutus kannettaville radioille



COJOT
MORE THAN ONE WAVELENGTH

COJOT OY on innovatiivinen, RF-teknologiaan erikoistunut yritys, jonka tuotevalikoimaan kuuluvat laajakaistaiset erikoisantennit VHF-, UHF- ja SHF-taajuuksalueille. COJOT OY:llä on yli 30 vuoden kokemus toimimisesta avainasiakkaidensa kanssa, joista tärkeimpiä ovat RF-laittevalmistajat (OEM) ja järjestelmäintegraattorit sekä puolustusvoimat. www.cojot.com

COJOT on osa Alaris Holdings konsernia, www.alarisholdings.com



Marko Koukka



Pasi Mäkinen

TEKSTI: MARKO KOUKKA JA PASI MÄKINEN
KUVAT: TELIA

Digitalisoinnin työkalupakki – Lohkoketjuteknologia ja Arvon internet

Tämän juttusarjan aikaisemmissa osissa olemme käsitelleet digitalisaation murrosta ja siihen liittyviä työkaluja kuten indentiteetin hallintaa ja tulossa olevien mobiiliverkkojen suomia mahdollisuuksia. Digitalisaatio on todettu johtamisen välineeksi ja teknologia on tässä muutoksessa vain työkalu, ei itse tarkoitus. Tämänkertainen artikkelimme keskittyy yhden uuden ja hieman kohutunkin teknologian mahdollisuuksiin ja mahdottomuuksiin. Kyseessä on lohkoketju- eli blockchain teknologia. Useat tutkimukset sekä globaalit konsulttitalot hehkuttavat seuraavan sukupolven Arvon internetin mullistavan digitaalisen liiketoiminnan arvon tuotannon. Hajautetut teknologiat, kuten lohkoketjut ovat peruste Arvon internetille.

Mitä se on

Lohkoketjuteknologia on tiedon tallennusmekanismi, jossa tietoa tallennetaan hajautetusti eri paikkoihin ja jokaiselle tällaiselle tallennuspaikalle, eli lohkolle, annetaan yksilöllinen tunnistus. Lohkoketjuteknologiaa on myös kuvattu digitaalseksi rekisteriksi, jota ei voi väärentää. Lohkoketjutietorakenteessa kaikki muokkaukset lisätään tietokantaan kryptografisesti ketjutettuina lohkoina. Lohkon hajautustiiviste aina kyseisen lohkon hyötykuormasta ja edellisen lohkon hajautustiivisteestä eli hashista.

Vaikka tämä edelleen melko tuntematon teknologia onkin kehittynyt virtuaalivaluutan kyljessä, sen hyödyntäminen on mahdollista minkä tahansa arvon välittämässä ja tallentamisessa. Lohkoketjuteknologian perusteet ovat peräisin jo vuodelta 1991, jolloin tutkijat kehittivät digitaalisen dokumentin aikaleimaukseen perustuvan toiminteen. Tämän keksinnön patentti vanheni käyttämättömänä jo 2004 eli neljä vuotta ennen Bitcoinin keksimistä.

Ominaispiirteitä lohkoketjuteknologialle ovat tiedon eheys, alkuperäisyys, kiistämättömyys ja muokkaushistorian pysyvyys. Näiden lisäksi voidaan todeta, että tiedon varmennettavuus ja vikasietokyky ovat ominaisuuksia, jotka tukevat erityisesti toimia, jossa liikutellaan arvoja. Huomion arvoista on se, että osapuolien välillä ei välttämättä tarvita luottamusta.

Merkittävä tekijä lohkoketjuissa on tiedon omistajuus. Kuten tiedämme mm. Facebook ja Google omistavat tietosi, joita heidän palveluissaan käytät. Lohkoketjuissa tiedon luoja omistaa ja päättää omalla salauksellaan kenelle tietoja haluaa antaa. Yksityisyyden kannalta katsottuna kyseessä on merkittävä ominaisuus.

Mitä Lohkoketju ei ole?

Lohkoketju ei ole kryptovaluuttaa, se ei ole ohjelmointikieli, se ei ole sala-

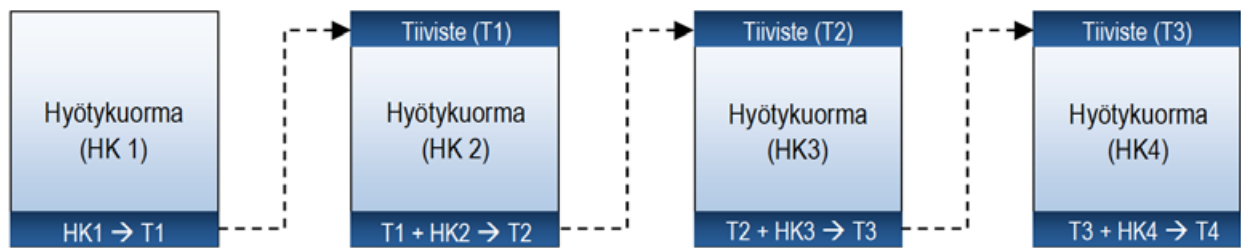
ustekniikkaa, eikä se ole keinoälyä tai koneoppimista. Tämä teknologia myös jakaa mielipiteitä. Osa näkee lohkoketjun kaikkein suurimpana teknologisena mullistuksena sitten Internetin ja osa taas on sitä mieltä, että mahdollisuudet ovat hieman liioiteltuja. Lohkoketjun on myös sanottu olevan ratkaisu, joka yhä etsii ongelmaansa.

Case Bitcoin

Kun puhutaan lohkoketjuteknologiasta, kääntyy keskustelu herkästi virtuaalivaluutta Bitcoinin. Lohkoketjuteknologia onkin alun perin kehitetty Bitcoinin yhteydessä varmentamaan, ettei käytettyjä Bitcoineja voisi käyttää uudelleen.

Bitcoin on ensimmäinen ”kryptovaluutta” joka perustuu hajautettuun lohkoketjuteknologiaan. Periaatteessa kuka vaan voi omistaa Bitcoineja ja sitä voi käyttää maksuvälineenä, eikä sen käyttöön tai omistamiseen tarvita mitään lupia. Bitcoinin eräs ominaisuus on myös se, että sen teknologinen toteutus pudottaa perinteiset pankit välistä pois, sillä niitä säilytetään virtuaalisissa lompakoissa eikä välittämiseen tarvita erillisiä rahalaitoksia, sillä kuten aiemmin mainittiin, luottamus ei ole tarpeen transaktion toteuttamiseksi.

Negatiivisena puolena mainittakoon Bitcoinin louhinnan kuluttama energia.



Lohkoketjutietorakenne.

Louhiminen on siis se operaatio, joka tapahtuu, kun Bitcoinia siirretään ja sehän on eräänlainen arvauskilpailu, jossa kaikki louhijat pyrkivät olemaan seuraavan numeron ensimmäisiä arvanneita ja saamaan siitä sitten palkinnoksi juuri Bitcoinia. Vain yksi voi voittaa ja siitä tietenkin syntyy tämä valtava energian kulutus, kun yrittäjiä on paljon. Louhinnasta syntyvä hiilijalanjälki on kooltaan samaa luokkaa kuin esim. Las Vegasin kaupungin tai Sri Lankan koko valtion vastaava, eli noin 22Mt hiilidioksidia vuodessa.

Arvon internet, älyraha ja älysopimukset

Nykyään on paljon esillä termi arvon internet. Termillä tarkoitetaan maailmanlaajuisia verkkoja, jossa ihmiset, koneet ja tekoälyt voivat käydä kauppaa ja tehdä sopimuksia keskenään ohjelmallisesti, ilman välikäsiä. Samaan kontekstiin liitetään myös termit älyraha ja erityisesti älysopimukset ja näissä molemmissa käytetään juuri lohkoketjuteknologiaa.

Älysopimukset ovat nimestään huolimatta kuitenkin ohjelmia, jotka tuottavat ihmisten ja tekoälyjen välisiä sopimuksia, jotka tallentuvat lohkoketjuihin. Älyraha puolestaan sekään ei ole pelkästään varsinaista valuuttaa vaan sen arvo muodostuu em. älysopimuksen myötä tuotetusta resurssista, joten se voi edustaa mitä tahansa arvoa. Esimerkkinä mainittakoon tästä vaikka yrityksen osakkeet, kiinteistöjen osakekirjat tai tekijänoikeudet. Kokonaisuutena älysopimukset ja niiden resurssit

eli älyrahat mahdollistavat kokonaan uuden tyyppistä taloutta, jossa osapuolet eivät tunne toisiaan mutta voivat käydä luotettavasti kauppaa keskenään tietämättä onko toinen osapuoli kone vai ihminen. Kaiken perustana on hajautettu luotettu verkko.

Lohkoketjuliiketoimintamahdollisuudet

Varmuudella voimme sanoa, että lohkoketjuilla on jatkossa merkittävä rooli liiketoiminnan digitalisoinnissa. Lohkoketjut pitää nähdä yhtenä mahdollistavana teknologiana. 5G sekä Iot tulevat räjäyttämään verkkoihin liitettävien laitteiden määrän ja luovat entisestään tarvetta resurssien ja tiedon hallinnalle. Tekoäly ja robotiikka ovat tulevaisuudessa hyvin tiivistä osa lohkoketjuja toimintojen automatisoinnissa.

Lohkoketjujen perusolettamukset tukevat hyvin digitalisoinnin ja digitaalisen ekosysteemin hallintaa. Teknologia ei yksin ratkaise haasteita, myös toimintaa pitää muuttaa. Liiketoiminnan digitalisoinnissa verkostojen kompleksisuuteen lohkoketjut tarjoavat parhaillaan joustavan, luotettavan ja kustannustehokkaan ratkaisun liiketoiminta-arvoketjun luomiseksi. Liiketoiminnan edellyttämät sopimus- ja korvauskäytänteet voidaan toteuttaa erittäin kustannustehokkaasti ja innovatiivisesti ilman välikäsiä, kunhan verkon luottamuksellisuus saadaan varmistettua. Älysopimukset ja Älyraha ovat verkoston sisällä sovittavia asioita.

On hyvä myös huomioida myöhemmin esitettävät lohkoketjujen tuomat

mahdollisuudet liiketoimintaketjujen tehostamisen kautta saavutettavaan ekologisiin säästöihin. Vaikka Bitcoin louhintaa energiaa kuluttaakin, tyypillisesti liiketoimintalohkoketjut eivät edellytä energiasyöppöä louhimista.

Tyypillisiä esimerkkejä lohkoketjutoteutuksista.

Käytännön sovelluksia, joissa on käytetty lohkoketjuteknologiaa, on kyllä jo olemassa paljonkin. Viihteen jakelussa ja tuottamisessa erityisesti musiikin alalla on jo useita toteutuksia. Viihdealan kiinnostus tähän teknologiaan johtuukin juuri tekijänoikeuksien eli viihteen arvojen tuottamisesta ja välittämisestä. Toinen yleisesti käytetty kokonaisuus on logistiikkaketjun hallintaan liittyvät toteutukset. Logistiikan osana lohkoketjuja käytetään todentamaan yksittäisten tavaroiden aitoutta ja alkuperää.

Vähän villimpi lohkoketjutoteutus löytyy lounaisosasta Kiinaa, jossa kanafarmit on valjastettu hyödyntämään uusinta teknologiaa. Kananpoikien jalokoihin asennetaan anturit jotka seuraavat niiden liikkeitä ja toimintaa ympäri vuorokauden. Kaikki data, joka kanoista saadaan, ladataan pilveen ja varmennetaan lohkoketjuteknologialla. Näin saadaan aikaiseksi kanan elinkaaren historia, jonka sitten lopullinen asiakas voi tarkastaa skannaamalla QR-koodin, joka tulee ostetun kanan mukana. Näin loppuasiakas saa selville kanan syntymästä asti kaikki tapahtumat, jopa sen ottamat askeleet aina teurastamispäivään asti. Kaikki tämä on siis tallen-

nettuna lohkoketjun historiaan. Kiinan keskiluokkaistuu kuluttajat haluavat panostaa ruokansa laatuun. Tuottaja ja tuotantoketju saavat tuotteestaan paremman hinnan, ja tämä toteutus onkin osa köyhyyden poistamisen hanketta maaseudulla.

Digitalisoinnin ja alustatalouden haasteena on nähty vallan siirtyminen globaaleille alustatalouden yrityksille. Maailmanlaajuisessa kuvassa oikeudenmukaisuuden ja hyvän hallinnon periaatteet eivät välttämättä ole linjassa meillä totuttuihin käytäntöihin. Tähän haasteeseen lohkoketjut voivat tarjota mielenkiintoisen mahdollisuuden esimerkiksi kansallisten ratkaisujen toteutukseen ja demokratian varmistamiseen esimerkiksi äänestämässä. Suomessa julkishallinto on tehnyt useita selvityksiä lohkoketjujen mahdollisuuksista. Yhtenä selkeänä haasteena on noussut esille regulaation keskeneräisyys, mikä toisaalta antaa tilaa pilotoineille.

Teoriasta käytäntöön, osaamisen puute rajoittaa

Lohkoketjuteknologiaan asetetut odotukset eivät ehkä ole toteutuneet siinä mittakaavassa, kuin mitä voisi olettaa. Odotukset ovat paisuneet lähes suhteettomiksi ja siten kohdistuneet myös väärin. Se ei kuitenkaan tarkoita, etteikö meneillään olisi merkittäviä toteutushankkeita ja tutkimuksia.

Myös valtionhallinto on ottanut askeleita käytännön toteutusten tutkimiseen. Valtioneuvoston kanslia rahoitti ja julkaisi tutkimuksen ”*Lohkoketjuteknologian hyödyntämismahdollisuudet palkkatulojen verotuksessa*” joka julkaistiin huhtikuussa 2019. Siinä tarkasteltiin, voitaisiinko lohkoketjuteknologiaan perustuvia älykkäitä sopimuksia hyödyntää palkkatulojen verotuksen prosessin automatisoinnissa. Lopputulos ei ainaakaan kovin nopeasti johda tässä käytäntöihin, sillä teknologian katsottiin soveltuvan vielä heikosti tähän tarkoitukseen. Haasteina nähtiin toteutusten kypsyysasteen keskeneräisyys ja erityisesti tarvittavan osaamisen rajallinen olemassaolo. Lohkoketjuteknologioiden käyttöön niinkin vaativassa tehtävässä kuin verotuksessa liittyy myös lainsäädännön kehittämistä ja sääntelyä.

Huolestuttavaa tässä tutkimuksessa



oli erityisesti havaittu osaamisen puute, sillä siihen ei meillä kansainvälisesti ajatellen ole varaa. Globaali digitalisaation murros vaatii tekijänsä ja on selvää, että siihen on syytä panostaa juuri nyt.

Seuraavassa lehdessä tämän juttuarjan viimeisessä osassa tuomme esiin

näkemyksiä, miten esiteltyjen digitalisaation työkalupakin työkalut sekä digitaalisen ekosysteemien kompleksiset palveluketjut ja prosessit saadaan yhtenäistettyä yhdeksi saumattomaksi palvelukokonaisuudeksi. Lähestymme asiaa SIAM (Service Integration and Management) viitekehyksen kautta.

VIESTIALAN AMMATTILAINEN!

Oletko kiinnostunut Maanpuolustuksesta?
Ammatillisen osaamisesi kehittämisestä?
Kansainvälisestä yhteistyöstä?
Perinteistä ja historiasta?

LIITY JÄSENEKSI!

Vuosimaksu vain 20 EUR. Sisältää mm. laadukkaan Viestimies-lehden. Sinun ei tarvitse olla viestiupseeri liittyäksesi. Lue lisää toiminnastamme ja jäseneduista verkkosivuiltamme.

VIESTIUPSEERIYHDISTYS RY

www.viestiupseeriyhdistys.fi



Kommodori Juha Ravanti toimii Merivoimien johtamisjärjestelmäpäällikkönä.

TEKSTI: JUHA RAVANTI
KUVAT: PUOLUSTUSVOIMAT

Merivoimien johtamisjärjestelmä 2025

Johdanto

Merivoimien johtamisjärjestelmä on muutoksessa, jota kuvaavina trendeinä ovat ensisijaisesti muutokset teknologiassa, vaatimuksessa ajasta ja paikasta riippumattomaan johtamiskykyyn sekä yhteensopivuus kansallisten ja kansainvälisten kumppanien kanssa. Samanaikaisesti kyberuhka kasvaa ja tiedustelu-uhka asettaa kokonaan uusia vaatimuksia oman toiminnan suojaamiselle vastustajan toiminnalta.

Merivoimien johtamisjärjestelmää kehitetään osana Puolustusvoimien johtamiskykyä. Monissa kohdissa siirrytään käyttämään joko Puolustusvoimien yhteistä tai muun puolustushaaran järjestelmää myös Merivoimien päätöksämisena. Tällä ratkaisulla vastataan paitsi yhteensopivuuden, myös ylläpidon ja kustannustehokkuuden sekä ennen kaikkea osaamisen laajuuden asettamaan haasteeseen.

Johtamisjärjestelmällä mahdollistetaan ajasta ja paikasta riippumaton johtaminen. Liikkuvalla ja hajautetulla johtamiskyvyllä parannetaan valmiutta sekä mahdollistetaan tuli-iskusta selviytyminen. Tietojärjestelmäpalveluilla tarjotaan kyky johtaa verkostokeskeisesti ja johtamista tuetaan kyvyllä käyttää tietoa paikallisilla, joukon omassa hallussa olevilla palveluilla.

Järjestelmistä palveluiksi - mikä muuttuu

Keskeisin muutos vuosien 2019 ja 2025 välillä on siirtyminen järjestelmien rakentamisesta palveluiden tuottamiseen. *Palveluilla* tarkoitetaan esimerkiksi sanoma-, puhe- ja tilannekuvapalvelua. *Palveluiden tuottamisella*



tarkoitetaan prosessia, jossa palveluiden käyttö pyritään optimoimaan mahdollisimman tehokkaasti. Ohjaavina tekijöinä ovat toimintamallit/-ohjeet sekä ns. *palveluajattelu*. Palveluajattelussa johtamisjärjestelmää lähestytään loppukäyttäjän näkökulmasta. Palvelutuotanto rakennetaan niin, että loppukäyttäjän on mahdollisimman helppo ymmärtää se. Mitkä palvelut hänelle kuuluvat orgaanisesti (kuten aseet), kuinka niitä käytetään ja miten ne saadaan käyttöön eri paikoissa.

Loppukäyttäjien koulutusta ja osaamisvaatimusta lisätään; tavoitetilassa loppukäyttäjän tulee osata liittää oma johtamisjärjestelmänsä valmisteltuun johtamispaikkaan. Palvelutuotannolle itselleen osoitetaan uusia vaatimuksia ja johtamisen tuen toimintatapoja muutetaan tukemaan palveluajattelua ja joukkojen suurempaa vastuuta omasta liittymisestäään. Joukon tulee siis itse kyetä

liittymään valmisteltuun johtamisyyhteeseen. Kuulostaa ehkä helpolta, mutta osaatko liittää kotona uuden television Internetiin ja ottaa käyttöön kanavapaketit ja muut mahdolliset palvelut. Entä jos on ongelmia wifin kanssa? Peli alkaa 15 minuutin päästä...

Tietoliikennealusta on osa itse palvelua

Merivoimien johtamisjärjestelmä tukeutuu jatkossakin Suomen turvallisuusverkon (STUVEn) runkoverkkoon ja Puolustusvoimien liityntäverkkoon, jotka mahdollistavat joukkojen, järjestelmien ja sensorien liittämisen. Puolustusvoimien liityntäverkko-hankkeessa (PVLIVE) uudistetaan verkon rakenteita ja rannikon liityntäverkon tekniikka tullaan korvaamaan PVLIVEN tekniikan mukaisilla ratkaisuilla.

Samalla mahdollistetaan entistä paremmin ajasta ja paikasta riippumaton johtaminen tukemalla langatonta liittytään aina STIII-tasolle saakka. Kaikkien puolustushaarojen ja Puolustusvoimien eri toimialojen toimintaa kyetään tukemaan rannikon liittytäväverkon palveluilla.

Merivoimien radiotukiasemaverkko suunnitellaan ja rakennetaan uudestaan tukemaan sanomalaiteverkon jälkeistä aikaa. Mitoitusperusteena käytetään operatiivista tarvetta ajatuksella ”missä minun tulee kyetä johtamaan” sen sijaan, että pyrittäisiin kattamaan koko rannikko mahdollisimman peittävästi. Tukiasemaverkon skaalautumista ja kykyä muodostaa painopisteitä parannetaan tukemaan sekä laivasto- että rannikkojoukkojen toimintaa.

Langattomassa tiedonsiirrossa siirrytään kerroksittaiseen liittytämalliin. Langaton liittytäkyky rakennetaan rannikolta ulospäin siten, että kullekin vyöhykkeelle (aluemeri-AKV-alue-Itämeri-Kaukoliikenne) optimoidaan oma tietoliikennekapasiteettinsa. Mitä lähempänä rannikkoa toimitaan, sitä useampia ja nopeampia mahdollisuuksia joukolla on toteuttaa liittytminen. Mitä kauemmas rannikosta siirrytään, sitä harvempia ja hitaampia, mutta taitelunkestävämpiä ratkaisuja liittytään tarjotaan. Langattomassa liittytynässä hyödynnetään Puolustusvoimien satelliittijärjestelmiä varmentavana ja nopeutta tarjoavana ratkaisuna.

Tietojärjestelmä täydentää palvelun

Merileijona tulee jatkossakin toimimaan Merivoimien taktisen johtamisen pääjärjestelmänä. Merileijonaa tuetaan organisaatiotasojen ja puolustushaarojen välillä Puolustusvoimien yhteisillä ratkaisulla sekä muiden puolustushaarojen ja toimialojen ratkaisulla. Vuoteen 2025 mennessä kehitetään Merileijonan ja Alueellisen johtamisen tukipalvelun (ATU) yhteensopivuutta ja yhdistetään niiden palveluita siten, että tietojärjestelmäalusta ja osa Merileijonan palveluista ovat Puolustusvoimien yhteisesti käyttämiä. Yhteensopivuutta Maavoimien johtamisjärjestelmän kanssa kehitetään ATUn avulla; ATU nähdään Merivoimien kannalta ennen kaikkea integraatorajapintana muiden



puolustushaarojen tilannekuva- ja johtamisinformaation suhteen.

Merivoimien tilannekuva muodostetaan, ylläpidetään ja jaetaan Merileijonassa. Merivoimien tilannekuvaa tuetaan toimialojen tilannekuvilla, joista osa ylläpidetään Merileijonassa ja osa muissa järjestelmissä.

Yhteensopivuutta niin kansallisiin kuin kansainvälisiinkin tarpeisiin rakennetaan Federated Mission Network (FMN)-hankkeen kehitysspiraalien mukaisesti. Tällä hetkellä taktisen tason merivoimapalveluiden kuvauksia ei ole laadittu, mutta työ on käynnissä ja suorituskyky rakentuu eri yhteistöiden kautta. Johtamisen tietojärjestelmäkokonaisuus liitetään kansainvälisten toimijoiden palveluihin operaatioverkkojen välityksellä. Tärkeimmät Itämeren alueen operaatioverkot rakennetaan pysyviksi ja jatkuvasti käytössä oleviksi ratkaisuksiksi.

Muiden puolustushaarojen kohdearkkitehtuurijärjestelmiä käytetään siirtymävaiheen aikana pääosin Puolustusvoimien yhteisten suorituskykyjen (Logistiikka, Ilmapuolustus) johtamiseen. Tavoitetilassa 2025 tarvittavat rajapinnat on integroitu ja toiminnallisuudet rakennettu Merileijonaan joko osana ATU-palveluita tai Merivoimien omana toteutuksena.

Tulenkäytön johtamisen toiminnallisuudet rakennetaan perustumaan Link-järjestelmiin ja niiden mukaisiin teknisiin rakenteisiin. Tulenkäytön ratkaisut toteutetaan Link-järjestelmien

(Link16, Link22) avulla; Merivoimat käyttää molempia sekä aluksilla että maajärjestelmissä.

Vain suojattu palvelu hyödyttää loppukäyttäjää

Salausratkaisuisa tukeudutaan kansallisiin Puolustusvoimien yhteisiin ratkaisuihin ja kansainvälisiin ratkaisuihin. Kansallisia ratkaisuja käytetään rannikon liittytäverkossa ja puhtaasti kansallisissa yhteyksissä. Kansainväliset salausratkaisut puolestaan mahdollistavat yhteensopivuuden kumppanien kanssa.

Merivoimat tukeutuu kybersuojauksessa PVJJK:n tuottamaan PV:n yhteiseen suorituskykyyn ja valvoo oman kohdearkkitehtuurinsa ja sen suorat liittynät ulos PV:n rakenteista (METO, operaatioverkot tms.). Kybersuojauksessa noudatetaan PV:n yleisiä periaatteita ja Merivoimilla on kyky tehdä tarkastuksia aluksiin, aselavetteihin ja joukkojen järjestelmiin.

Merivoimat siirtyy vuoteen 2025 mennessä toimintaan, jossa johtamisjärjestelmä on kiinteä osa informaatio-osodankäyntiä. Tämä edellyttää kykyä säädellä käsiteltävän tiedon määrää ja laatua eri tiedonsiirron medioilla sekä ohjata liikennettä toimiville palveluille. Informaation hallinta on kiinteä osa johtamista ja sitä säädellään osana kybertilannekuvaa ja -ennustetta.



Kirjoittaja on reservin kapteeni sekä Pirkanmaan Viestikillan puheenjohtaja ja työskentelee Milcon Oy:ssä projektipäällikkönä. Milcon Oy toteuttaa vaativien sovellusten ja haastavien olosuhteiden kaapelointi- ja johtamisjärjestelmät asiakkaidemme vaatimusten mukaisesti.

Lyly on perinteinen Viestiaselajin paikkakunta

Lyly valikoitui päivien pitopaikaksi pitkien Viestiperinteidensä siivittämänä. Viestivarikon toiminta Suomen Puolustusvoimissa alkoi 22. lokakuuta 1939 Espoon Leppävaarassa. Syksyllä 1940 varikko siirtyi Juupajoen Korkeakoskelle, josta se siirtyi uudelleen nykyiselle paikalleen Juupajoen Lylyyn 22. marraskuuta 1940.

Lylyn Viestivarikkona toiminut Puolustusvoimien viestijoukkojen kalustoa varastoinut, huoltanut ja ylläpitänyt laitos lakkautettiin vuoden 2008 lopussa, jolloin sen toiminnot siirtyivät maavoimien kunnossapidon ulkoistuksen myötä Millog Oy:lle. Millogin Lylyn toimipiste tuottaa nykyisin samat elektroniikka-alan materiaalipalvelut puolustusvoimille.

Avauspäivä – Herrasmieskilpailu ja leppoisaa yhdessäoloa

Päivät aloitettiin ilmoittautumisella, tervetulokahveilla ja aloitus- sekä järjestelypuheenvuorolla. Osallistujat esittelivät itsensä ja kertoivat lyhyesti viestiaselajitustansa.

TEKSTI: TOMMI VALKEEJÄRVI

KUVAT: TAPIO TEITTINEN, TOMMI VALKEEJÄRVI JA JUKKA-PEKKA VIRTANEN

Viestimiespäivillä Lylyssä 10.-11.8.2019

Pirkanmaan Viestikillan isännöimät Viestikiltojen Liiton valtakunnalliset viestimiespäivät pidettiin aurinkoisessa säässä nykyisellä Millog Oy:n Lylyn toimipisteellä - entisellä Viestivarikolla Juupajoen Lylyssä. Päiville osallistui parisenkymmentä osallistujaa paikallisista viestikilloista eripuolelta Suomea.



Viestimuseo. Kuva Tapio Teittinen



Viestikorsu. Kuva Tapio Teittinen

Tämän jälkeen Viestikiltojen Liiton puheenjohtaja Jukka-Pekka Virtanen piti oman avauspuheenpuoronsa ja julisti Viestimiespäivät 2019 avatuiksi.

Seuraavana oli vuorossa erityisesti pitkämatkalaisten kaipaama maittava lounas, jonka jälkeen osallistujat siirtyivät Millog Oy:n vierasmajoitukseen.

Majoittumisen jälkeen oli vuorossa päivien ohjelmaan kuuluva erittäin perinteinen Viestimieskilpailu.

Herrashenkilökilpailussa testattiin moninaisia tietoja ja taitoja huumorin pilke silmäkulmassa. Kilpailu aloitettiin Lylyn ja Varikon historiaa sekä yleistietoa tenttaavilla kysymyksillä. Kysymyksistä ja niihin myöhemmin annetuista vastauksista osallistujille piirrettiin kuva piskuisesta Pirkanmaalaiskylästä, jonka arkeen ja historiaan olivat jättäneet merkittävällä tavalla jälkensä Isänmaamme historian käännekohtat: Vuoden 1918 tapahtumat sekä talvi- ja jatkosota.

Tätä seuraavilla rasteilla testattiin käytännössä kaapelijatkoksen tekoa, arjen välineitä HF- radorastilla laitteen toimintakuntoon laittona ja yhteyskokeiluna. Lämpimään säähän suunnitellulla nestehukan torjuntarastilla kokeiltiin hiiren heittoa laatikkoon ja heitettiin frisbeetä. Sotilaallisimpana rastina oli pistoolilla laseraseammuntaa. Laserammuntarastin onnistumiseen vaikutti ratkaisevasti Juupajoen Reserviläisiltä lainaan saatu eko-pistooli. Viestikiltojen Liiton koulutusteemojen mukaisesti aiemman arjen välineet rastin lisäksi harjoiteltiin toiseen painopistealueeseen Kyber-uhkiin varautumiseen humoristisesti foliohatun rakennuskilpailussa. Kaiken tämän lisäksi kisassa mukana olivat perinteiset arviointirastit, erikoisten laitteiden tai komponenttien tunnistusta sekä sotilaallisen musiikin tunnistusrasti.

Tiukan kisailun jälkeen siirryttiin jälkipeliin saunan lauteille keskustelemaan kisasta, mutta ennen kaikkea vaihtamaan kuulumisia eripuolilta Suomea saapuneiden kiltaveljien kanssa.

Saunomisen päälle siirryttiin vanhalle Viestivarikon kerholle Viestimies-illalliselle, jossa viihdyttiinkin hyvän ruuan, seuran ja ruokajuomien ryydittämänä puolille öin. Erityisesti Secja:n pitopalvelun loihittimat taivaalliset jälkiruokakakut syötiin loppuun viimeistä murua ja tuorejuuston palaa myöden.



Kyber-uhkarastin foliohatut. Kuva Tapio Teittinen



Perinteinen Viestijoneuvo sai osallistujien jakamattoman kiinnostuksen. Kuva Tommi Valkeejärvi



Palkitsemisia illallisella. Kuva Tommi Valkeejärvi

Ruokailun ohessa julistettiin viestimieskilpailun tulokset, kerrottiin oikeita vastauksia, keskusteltiin hiltitysti vastausten tulkinnoista protestien välttämiseksi sekä palkittiin kaikki osallistujat kirja- ja muilla palkinnoilla. Palkintoja oli saatu kasaan niin, että mukavaa kotiin viemistä tuli kaikille.

Tärkeä osa illallista olivat pääruuan jälkeen esitetyt Pirkanmaan ja Kaakkois-Suomen Viestikiltojen viestiaselajin historiaan liittyvät alustukset. Alustuksissa pohdittiin mm. viestiaselajin alkutaipaleeseen liittyviä avoimia kysymyksiä ja niistä käytiin vilkasta ja syvällisen asiantuntevaa keskustelua - jokainen oppi taas jotain uutta toisiltaan. Illallisella oli myös oivallinen hetki palkita ansioituneita kiltatoimijoita.

Väki viihtyi hyvin illallis-pöydässä ja tasainen puheensorina täytti Kerhon tilat illan loppuun saakka.

Toinen päivä – Lylyn Viestimuseo ja Lylyn viestivarikon radiokerho OI3V

Aamunherätyksen jälkeen nautittiin maittava vahvennettu aamupala ja valmistauduttiin tutustumaan Lylyn viestimuseoon sekä Lylyn viestivarikon radiokerhoon.

Lylyn Viestimuseo – ja uudelleen vuonna 2000 perustettu Lylyn Viestivarikon radiokerho, toimivat edelleen vaalien Lylyn Viestivarikon historiaa ja perinteitä, radioviestinnän historiaa sekä ylläpitäen viestimiestaitoja ja -perinteitä. Lylyn Viestivarikon henkilöstön vahvalla myötävaikutuksella on ollut suuri merkitys museon ja radiokerhon toiminnassa.

Lylyn varikon museo tarjosi nähtävää ja kuultavaa monipuolisesti ja niitä esiteltiin 40-vuoden syvällisellä viestikokemuksella. Eri-tyisesti ensimmäistä kertaa tässä museossa vierailuille riitti nähtävää ja kuultavaa yli kahdeksi tunniksi. Kuulijoita kiinnostivat ensimmäisen Viestikomentajan Leo Ekberg:n asepuke Jääkäripataljoona 27 merkkeineen, Kyynel-radio, vanhat kenttäpuhelimet, joita yksi oli aikaa ennen kuin puhelimissa oli luuri. Museosta löytyvä pieni viestikorsu sai ansaitsemansa huomion. Vilkasta keskustelua aiheuttivat museosta löytyvät sekä idän että lännen maiden vakoilijoiden ja desanttien Suomessa aikanaan käyttävät vakoilijadiot kuten Severi-radio sekä Amerikkalainen matkalaukuun rakennettu AN/PRC-1/RT-30-radio.

Sunnuntain toisena ohjelmanumerona oli Lylyn viestivarikon radiokerhon esitely. Vuodesta 2008 lukien Lylyn Viestivarikon radiokerho on toiminut Juupajoen Reserviläiset ry:n alaisena



viestijaoksena. Kansainvälisissä yhteyksissä radiokerho tunnetaan myös nimellä Radio Club of Lyly Signals Depot. Radioamatööriyhteyksissä kerhon perinteinen radiokutsu on OI3V (Otto Iivari Kolme Vihtori). Radiokerho ylläpitää myös muita radioamatööriasemia, kuten Suomen ensimmäistä OI -etuliitettä käyttävää APRS -paikkatietotoistinta kutsulla OI3RDV. Kerhon toimintamuotoina esiteltiin radiokilpailu- ja perinneradiotoiminta, museo- ja kerhoaseman aktivoinnit sekä

radioamatööri- ja reserviläisviestitoimintaan liittyvä rakentelu. Lylyn Viestivarikon radiokerho on aktiivisimpia Puolustusvoimien OI -alkuisia kutsutunnuksia käyttäviä radioamatööriasemista.

Museo- ja radioasemakäynnin jälkeen siirryttiin päätöskahveille ja Kiltujen Liiton puheenjohtaja julisti Viestimiespäivät päättyneiksi sekä toivotti Pirkanmaan Viestikillan puheenjohtajan kanssa turvallista kotimatkaa.



Museo Militarian teemaseminaari "TURVASSA"

24.10.2019 klo 18.00-20.15

Hallintopolitiikan alivaltiosihteeri **Päivi Nerg** (VM): *"Suomi, maailman turvallisin maa ja sellaisena haluamme sen pysyvän - luottamusyhteiskuntamme koetuksella"*

Erikoistutkija, dos. **Kari Laitinen** (POLAMK): *"Kansallinen turvallisuus"*

Akatemiatutkija **Teija Norri-Sederholm** (MPKK): *"Some ja nuoret- kokonaisturvallisuuden näkökulmaa"*

Seminaari järjestetään Tykkihallissa.

Osallistumismaksu 10 € sisältää kahvituksen ja pääsylipun näyttelyyn.

Opiskelijat ja alle 18-vuotiaat ilmaiseksi.

Tervetuloa!

www.museomilitaria.fi

Vanhankaupunginkatu 19, 13100 HÄMEENLINNA
Puh. 040 450 7479, asiakaspalvelu@museomilitaria.fi



Analysaattori



Houston, meillä on tietokone!

Ihmiskunnan ensimmäisestä kuuhun laskeutumisesta tuli juuri heinäkuussa kuluneeksi 50 vuotta. Edelleen aika kiehtova tarina on koko tämä Apollo-ohjelma ja tulin sitä taas tarkkaan seuranneeksi. Muistan nimittäin vielä sen varsinaisenkin kesän -69 kun juoksentelimme naapurin poikien kanssa innoissamme Apollo 11-paidoissa pitkin pihvoja ja katselimme kuun valloitusta mustavalkoisesta televisiosta. Tänä kesänä seurasin myös Twitteristä tiliä Apollo 50th (@apollo_50th), joka livetwiittasi ”reaaliajassa” Houstonin operaatiokeskuksen ja Apollo 11 astronauttien välisen radioliikenteen kesältä 1969. Siinä yhteydessä kiinnitin huomioni myös asiaan, jota en silloin vielä ymmärtänyt, mutta nyt se iski lujaa tajuntaani. Siinä kuuhun laskeutumisessa käytettiin vahvasti apuna tietokonetta. Tämä innoittikin sitten tutustumaan siihen laitteeseen vähän tarkemmin.

Kyseinen tietokone kulki nimellä AGC (Apollo Guidance Computer) ja se oli suunniteltu ihan nimensä mukaisesti ohjausta ja navigointia varten. Kuusikymmenluvun alussa NASA:ssa tajuttiin, että jotain tällaista tarvitaan, jotta lentäminen ja laskeutuminen kuuhun ja erityisesti paluu maahan olisi mahdollista. Tässä oli avainasemassa Charles Stark “Doc” Draper, joka oli uranuurtaja instrumentoinnissa ja kehityksessä jo toisen maailmansodan asejärjestelmissä ja 50-luvulla ohjusten ohjausjärjestelmissä. Hän johti MIT:n (Massachusetts Institute of Technology) laboratoriota ja ryhmää, joka kehitti ohjaus- navigointi ja kontrollijärjestelmän Apollo-ohjelmalle ja ilman häntä ei kuussa olisi presidentti Kennedyn lupauksen mukaan vielä 60-luvulla kä-

velty. Hänen ryhmänsä sai NASA:lta tämän sopimuksen kehittää tarvittava järjestelmä jo niinkin varhain kuin 1961. Kerrotaan, että parikin isoa ilmailuteknologian yritystä vetivät vähän soraa venttiilinsä tästä sopimuksen menettämisestä, mutta se ei Doc Draperia haitannut. Kun hänen ja hänen tiiminsä kyvykkyyttä kehittää tarvittava järjestelmä epäiltiin ja kysyttiin, pystyttekö siihen, vastasi Draper itsevarmasti: *”Kyllä. Mistäkö tiedän, että pystymme siihen? Minä vaikka lennän sitä itse”*. Kuten tunnettua Draperia ei valittu avaruusohjelman lentäjien joukkoon, mutta kyllähän ne raketit sitten lensivät. Tuo mainittu sopimus sinänsä tuntuu kantavan hyvin, sillä MIT on edelleen mukana NASA:n avaruusohjelmissa ja tuli keväällä 2019 toiseksi innovaatiokisassa, jossa kehiteltiin ravinnon kasvatamista MARS:iin matkaaville astro- tai mahdollisesti jopa joillekin muillekin nauteille.

Kuualuksen ohjaukseen tarvittiin tietokoneita ja olihan niitä jo olemassa, mutta ne olivat tuolloin keskimäärin huoneen kokoisia, joten jotain pientä säätöä pitäisi tehdä, että se mahtuisi mukaan. Avaruustietokoneita oli toki jo käytetty Gemini-ohjelmassakin, jossa sen rooli oli kuitenkin vain astronautteja opastava, kun taas Apollon AGC:llä oli elintärkeä rooli aluksen ohjaamisessa ja kontrolloinnissa. Apollo 11 laskeutui kuuhun AGC:n avulla ja tunnetusti myös palasi takaisin maahan aivan suunnitellusti. MIT sen tietokoneen suunnitteli, mutta Raytheon sen lopulta rakensi. AGC:n suorituskyky ei nykymittapuussa ollut mikään huimaa. Laitteessa oli 36KT ROM-muistia ja 2 KT RAM-muistia ja tavun pituus 16 bittia.

Tietokone tarvitsee toimiakseen raudan lisäksi ohjelmistoa. AGC:n ohjelmiston kehittämisestä vastasi Margaret Hamilton tiimeineen. Hänen sanotaan ensimmäisenä käyttäneen itsestään nimitystä ohjelmistoinsinööri. Jokainen, joka tarkkaavaisesti on seurannut dokumenttiohjelmaa tai elokuvia kuuhun laskeutumisesta muistaa virheilmoitukset 1201, 1202 jotka olivat AGC:n ylikuormittumisesta johtuvia virheilmoituksia. Nämä tupsahtivat näyttöön juuri kuuhun laskeuduttaessa. Tietokone ei kuitenkaan ”kipannut” tällä kriittisellä hetkellä vaan priorisoi tärkeämmät tehtävät etusijalle. Virheilmoitukset johtuivat siitä, että lähestymistutkan kytkimet oli asetettu manuaalisesti väärään asentoon eikä AGC:llä ollut kapasiteettia käsitellä tätä tilannetta. Tarina kertoo, että ohjelmistoa paranneltiin siksi, että Hamiltonin 4-vuotias tytär oli vahingossa näpytellyt laboratoriossa AGC:tä ja aiheuttanut koneen kaatumisen. Hamilton alkoi pohtia voisiko astronautti tehdä samanlaisen virheen avaruudessa, mutta ei saanut lupaa keskittyä ohjelmiston parantamiseen, sillä hänelle vakuutettiin että *”astronautit nyt eivät vaan tee tuollaisia virheitä”*. Kunnes Apollo 8 astronautit sitten nimenomaan onnistuivat vähän sössimään ollessaan kuun kiertoradalla. Hamilton pääsi sitten tekemään koodista vikasietoisempaa, joka siis tunnetuin seurauksin pelasti ensimmäisen kuuhun laskeutumisen.

Hienoa tässä softassa on sekin, että tämä AGC:n ohjelmisto, jolla Apollo-ohjelmat lennettiin, on ladattavissa sivustolta <http://www.ibiblio.org/apollo/index.html>. Ohjelmistoa voi ajaa useilla eri alustoilla, jopa Windows-koneella, joka sinänsä kuulostaa aika vaaralliselta

yhdistelmältä. Ketään ei varmaan yllätä sekään, että tämän havaittuani latasin välittömästi ohjelmiston koneelleni, mutta testaus on vielä tätä kirjoitellessa vähän kesken.

Jos 60-luvulla kyettiin pitämään avaruusalus kurssissaan ohjelmoinnin avulla, on nykypäivän tilanne yllättäen hieman toisenlainen. Tällä viittaa tietenkin Boeingin 737 Max 8-koneen ohjelmiston ongelmiin, joiden ansiosta on jo n. 350 ihmistä menettänyt henkensä kahdessa lento-onnettomuudessa. Ongelmat johtuvat siitä, että tämän uuden konetyypin moottoreita siirrettiin eteenpäin ja ylemmäksi polttoainesäätöjä tavoitellen. Lentämiseen tämä vaikutti siten, että myös sakkauksenesto-ohjelmistoa MCAS:ia jouduttiin vähän ”tuunaamaan”. Lentäjille tästä ei ollut annettu tarpeeksi lisätietoja ja seuraukset ovat nyt tiedossa. Konetyppi on lentokiellossa ja vahvat huhut syyttävät mm. huonoa koodaamista. Sen lisäksi on nyt tullut julkisuuteen muitakin seikkoja, joilla on ollut vaikutusta tähän katastrofaaliseen munaukseen. Eräs vahva huhu kertoo, että Boeing on ulkoistanut koodaamistaan halvoille alihankkijoille, joilla keskimääräinen palkka koodajalle olisi vain 9 taalaa tunnilta. Tarina ei kerro mistä näitä halpiskoodaajia hankitaan, mutta arvaan kyllä, että aika moni heistä on kasvatettu Naan-leivällä. Todella huolestuttavaa on sitten se, että Yhdysvaltain ilmailuviranominen FAA, joka myöntää tarvittavat sertifioinnit, on päästänyt Boeingin painostuksesta juuri tämän konetyypin ”ohituskaistalle” luokituksia tehtäessä. Tämähän ei sinänsä ole ainutkertaista, kun aika on rahaa ja suuryritykset pystyvät siihen. Mutta kun on käynyt ilmi, että merkittävä osa itse validointiprosessista on ulkoistettu viranomaisilta juuri Boeingille itselleen, ovat puurot ja vellit todella pahasti sekaisin. Boeingin liiketoimintaan siis sisältyy ikään kuin itsepalveluna konetyypin viranomaissertifiointi. Syyt ovat kuulemma FAA:n resurssipulassa ja osaamisvajeessa, sillä valtion palkoilla ei meinaa löytyä tarpeeksi kovia osajia. Joita sitten on tietenkin ilmailuteollisuudessa tarjolla. Hieman etäämmältä tarkasteltuna kyse on tietenkin protektionismista ja kilpailun rajoittamisesta, joten tästä sotkusta saavat kyllä Yhdysvalloissa syyttää vain itseään.

Tarpeeksi kun mennään ajassa taaksepäin, löytyy täältä kotinurkiltakin

ainakin etäisesti tätä Boeingin tapausta muistuttava liikennevälineen standardointi- ja sertifiointivirhe, joista myös aiheutui ihmishenkien menetyksiä. Vaasa-laivan rakentamisen yhteydessä 1600-luvun alussa nimittäin Ruotsin kuningas sekaantui kesken laivan rakentamisen sen arkkitehtuuriin ja vaati rakennettavaksi yhden ylimääräisen tykkikannen. Tämän ansiosta laivasta tuli erittäin kiikkerä. Lisäksi on tutkimuksissa todettu, että ruotsalaisten ja hollantilaisten laivanrakentajien käyttämät tuuma- ja jalkamitat eivät olleet täysin samoja mittoja, jonka johdosta laivan runko oli hieman kierossa.

Vaasa-laivan käyttöönottestin valvojaksi kutsuttiin suomalainen amiraali Fleming. Kyseessä oli ns. juoksutesti jossa 30 merimiestä juoksi ryhmänä laivan reunalta toiselle. Laiva oli kaatumaisillaan jo testin aikana, joten Flemingin käskystä testi keskeytettiin. Epäonnistuminen olisi ollut ilmeisesti pahaksi urakehitykselle, joten testien tulokset jotenkin unohdettiin ilmoittaa eteenpäin ja laivalle annettiin ”ajolupa”. Ja niinhän siinä sitten kävi, että Vaasa-laiva lähti satamasta Flemingin käskystä neitsytmatkalleen ja selvisi jotenkuten ensimmäisestä tuulenpuuskasta, mutta ei sitten enää toisesta. Laiva vei mennessään 50 merimiestä ja aiheutti pysyvän mainehaitan Ruotsin laivanrakennusteollisuudelle. ATK:n käyttö olisi tässäkin tapauksessa pelastanut tuotteen, mutta se ei ollut vielä noihin aikoihin edes laivateollisuuden pitkän tähtäimen roadmapissa.

Ja viimeiseksi vaan ei vähäisimmäksi, katsaus tietoturvapuolelle. On nimittäin käynyt ilmi, että sekä Applen Siri-sovellus että Googlen Home-kaiuttimet välittävät saamiaan äänikomentoja ”johonkin” ja niitä sitten kuunnellaan palveluiden kehittämisen varjolla. Ilmeisesti tämä tietojen luovutus on jossain ehdoissa mainittu oikein pienellä ja epäselvästi. Analysaattorin mielestä kyseessä on kuitenkin törkeä yksityisyyden loukkaus. Tahtoisin myös ehdottomasti tietää, miten nämä sala kuuntelijat olivat luokitelleet sen, mitä tulin tälle Sirille täryttäneeksi pari vuotta sitten. Tämä tapahtui talvella, kun olin luistelemassa järvelle auratulla retkiluisteluradalla. Fokukseni karkasi jossain vaiheessa hetkeksi ja suoritin tahtoni vastaisen suunnittelemtoman sukelluksen rataa reunustavaan lumi-

valliin. Komeasti, pää edellä. Siinä sitten keräilin itsetuntoani ja varustetani, kun takkini taskusta kuului Sirin huomautus selkeällä äänellä ”*Sorry, I didn't quite get that*”. Siihen sitten annoin välittömästi suoran palautteeni täysin tietämättömänä siitä, että se lähti johonkin maailman toiselle puolelle kuunneltavaksi. Epäilen muuten, että ei taida ihan Google-kääntäjällä aueta sen viestin sisältö.



Insinööri K Merentausta.

Posti- ja lennätinlaitoksen autoradiopuhelinverkko

Useiden vuosien aikana on ilmennyt tarvetta yhtenäisen koko valtakunnan alueelle ulottuvan, lähinnä autoliikennettä palvelevan radiotoiminnan aloittamiseen. Useilla tahoilla, eikä vähiten posti- ja lennätinlaitoksen piirissä on osoitettu lukuisia toivomuksia yleisen radiopuhelinverkon luomiseksi. Viime vuoden lopulla valmistui yleissuunnitelma ja posti- ja lennätinhallitus teki istunossaan 22.11.1968 periaatepäätöksen perustaa yleiseen puhelinverkkoon liittyvän ja koko valtakunnan alueelle ulottuvan siirtyvän maaradioliikenteen hoitamista varten tarpeellisen määrän radioasemia ja radiotoimipaikkoja joko olemassa olevien puhelin- ja lennätintuomipaikkojen yhteyteen tai tarvittaessa uusina toimipaikkoina. Yleissuunnitelman pohjalta jatkettiin yksityiskohtaisia suunnitelmia ja ensimmäisten tukiasemien rakentaminen päästiin aloittamaan kuluvan kesän aikana. Verkon käyttäjinä voivat olla valtion ja kuntien erielimet, teollisuus- ja liikelaitokset sekä yksityiset henkilöt.

Verkko on tarkoitettu pääasiassa siirtyvää liikennettä varten, mutta poikkeustapauksissa sitä voidaan käyttää myös kiinteään liikenteeseen. Autoradioverkko ja yleinen puhelinverkko liitetään toisiinsa siten, että puhelut radiopuhelintilaajien ja puhelintilaajien kesken ovat mahdollisia. Radiopuhelinverkon tilaajilla on mahdollisuus myös keskinäisiin puheluihin. Tukiasemien yhteinen lukumäärä koko maassa on noin 140. Tukiasemien kautta ohjautuvan liikenteen välitys tapahtuu aluekeskuksessa, jossa autoradiopuhelinverkko liitetään puhelinverkkoon kaukotasolla.



Verkon perustustyöskentelytavaksi on valittu puoliduplex, jolloin liikkuvalla asemalta puhuttaessa on käytettävä puhepainiketta (tangenttia), kun taas kiinteän puhelinverkon tilaaja käyttää puhelintaan normaaliin tapaan. Tämän käyttäjältä hieman tottumusta vaativan työskentelytavan etuina duplexiin (käyttö kuten tavallisen puhelimen) nähden ovat esim. yksinkertaisemmat ja halvemmat ajoneuvoaseman laitteet sekä taajuuksien tehokkaampi käyttö ajoneuvojen keskinäisissä puheluissa.

Yhteydenotto kumpaankin suuntaan (ajoneuvosta tai ajoneuvoon) tapahtuu aina kutsukanavalla. Soitto ajoneuvosta keskukseen annetaan joko kutsupainikkeen avulla tai se tapahtuu automaattisesti nostettaessa kuulopuhelin pidikkeestä. Soitto keskuksesta ajoneuvoon avaa ajoneuvoasemien kovaääniset, jolloin puhelu tulee kuultavaksi. Myöhemmin otetaan käyttöön selektiivikutsu, jolloin soiton saa kulloinkin ainoastaan se ajoneuvo, johon puhelu on tarkoitettu yhdistää. Kun selektiivinen kutsujärjestelmä saadaan myöhemmin käyttöön, niin voidaan turvata puhelusalaisuus järjestelmän sisällä. Toisin sanoen muiden järjestelmään kuuluvien asemien kuuntelu tulee olemaan estetty.

Puhelujen tilaus ajoneuvoihin tapahtuu samojen periaatteiden mukaisesti kuin käsivälitteisessä kaukoliikenteessäkin joko numerosta 09 tai jostain erikoisnumerosta. Puhelumaksut koostuvat linjamaksusta ja erityisestä radiomaksusta. Niitä ei ole vielä vahvistettu, mutta tullevat perusmaksuineen olemaan luokkaa 50-80 penniä minuutilta. Radiopuhelintilaajien on yleensä itse hankittava omien asemiansa laitteet ja heidän tulee anoa laitteilleen käyttöluupa posti- ja lennätinhallituksen radio-osastolta. Radiopuhelimeen tulee sisältyä puhekanavalla toimivat signaalintilaajien ajoneuvosta annettavaa kutsu- ja loppusoittoa varten (2000Hz) ja keskuksesta annettavaa avaussoittoa (1800Hz) varten.

Posti- ja lennätinhallituksen radio-osastossa on arvioitu, että radiopuhelinverkossa kyetään rakentamaan jo noin kolmessa vuodessa sellaiseen laajuuteen, että sen vaikutuspiiriin kuuluu alue, jolla tapahtuu yli 80% koko maan autoliikenteestä ja se käsittää mm. kaikki tärkeimmät päätiet Etelä-Suomesta aina Muonioon ja Ivaloon saakka. Seuraavina vuosina rakennettavien tukiasemien asennusjärjestys määräytyy lähinnä liikenteellisten seikkojen perusteella.

Artikkelin kirjoittaja Veli-Matti Pesola



VM

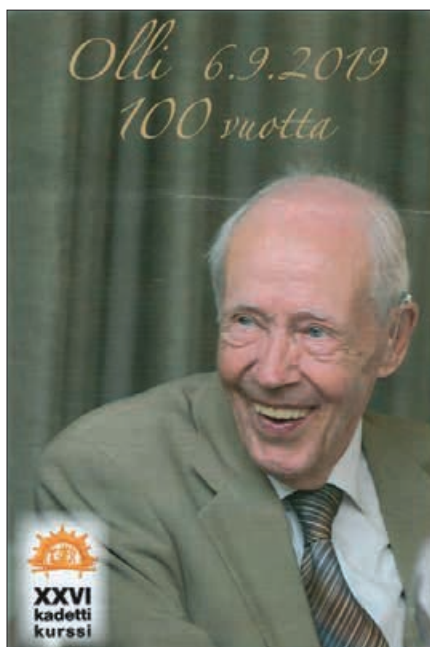
Onnittelemme

Viestiupseeriyhdistyksen kunniajäsenen Olli Vuorio täyttää 100-vuotta

Viestimieslehdellä oli kunnia päästä haastattelemaan yhdistyksemme kunniajäsentä 100-vuotta 6.9.2019 täyttäneitä Ikikaa-deria majuri Olli Vuoriota hänen kotoaan. Vuorion olohuoneessa huokui historiallinen tunnelma ja haastattelu venyi suunniteltua pidemmäksi. Vuorion kanssa käyty keskustelu herätti haastattelijassa runsaasti ajatuksia ja soisin samaisen keskusteluhetken myös nuoremalle sukupolvelle. Jokainen eletty hetki on kokemisen arvoinen ja sen voi ikuistaa, vaikka valokuvin, joiden pohjalta elettyyn elämään on helppo palata myöhemminkin.

Vuorio on tällä hetkellä Suomen vanhin kadettiupseeri. Hän syntyi vuonna 1919 Suomen Turussa, josta perhe muutti kuitenkin hyvin pian Helsinkiin, kun Vuorion isä sai työpaikan Uudesta Suomesta. Turun ajasta Vuoriolla ei ole muistikuvia, sillä muutto Helsinkiin tapahtui vuonna 1922 Vuorion ollessa kolmevuotias. Asunto, johon muutettiin, oli Vuorion isän työpaikalta saama työsuhdeasunto ja se sijaitsi pihan perällä ullakolla, jonne ei johtanut hissiä vain jyrkät portaat.

Vuosi 1935 on Vuoriolle merkittävä, sillä silloin hän sai ensimmäisen kameransa Baby Boxin, pikkuserkultaan, joka toimi Uuden Suomen valokuvaajana. Noista vuosista lähtien erilaiset kamerat ovat kulkeneet Vuorion mukana jokaisessa paikassa, minne hän on mennyt. Vuoriolla oli kamera mukana myös rintamalla ja yhdestä hänen lukuisista kuvakansioistaan löytyy edelleen esikuntapäällikön eversti Inkan Vuoriolle myöntämä lupa valokuvaukseen



hallussapitoon ja käyttöön rintamalla. Vuorio muisteli, että kyseistä lupaa ei häneltä kuitenkaan ikinä kysytty.

Koulutaipaaleensa Vuorio aloitti seitsenvuotiaana Punavuoren kansakoulussa. Vuorio muisteli koulunkäynnin olleen tahmeaa, se ei oikein maistunut nuorelle Ollille. Koulutaipale jatkui oppikoulun merkeissä Koulukujan yhteislyseossa. Vuonna 1938 koulu sai uudet tilat Arkadiankadulta ja sen nimeksi tuli Arkadian yhteislyseo. Arkadian yhteislyseon nimi on säilynyt ja koulu toimii edelleen, mutta ei enää Arkadiankadulla vaan Nurmijärjen Klaukkalassa. Kun koulua perustettiin Klaukkalaan 1990-luvulla, niin Vuorio oli paikalla yhtenä kutsuttujen senioreiden joukossa. Koulussa Vuorio harrasti liikunnan lisäksi toverikunta- ja suojeluskuntatoimintaa. Liikunta piti sisällään pyöräilyä

ja hiihtämistä. Ensimmäisen pyörän Vuorio sai noin 10-vuotiaana ja oppi heti ajamaan. Siitä todisteena on Vuorion isän valokuvakansiossa oleva kuva, jossa todetaan ”Olli ookaa”. Samat liikuntaharrastukset ovat jatkuneet aina viime vuosiin asti.

Kouluaikana Vuoriolla oli myös heila Kaisa, jonka isä oli yksi niistä jääkäreistä, joka tuli UC-57:llä Suomeen vuonna 1917. Kiinnostus sotilasuraa kohtaan alkoi Kaisan isän kautta. Tytön isä ohjasi myös nuorta Ollia, sillä RUK:n päättymisen jälkeen Vuorion olisi pitänyt mennä jatkamaan kahdeksatta luokkaa. Tosin Vuorion omissa ajatuksissa ei ollut koulun jatkaminen, koska seitsemännän luokan todistuksella olisi jo päässyt Kadettikouluun. Kun Kaisan isä kuuli tästä, niin yhtenä päivänä hän oli ilmoittanut tyttärelle, ”mikäli Olli ei ole huomenna koulussa, niin minä tulen ja talutan pojan niskasta kouluun”. Vaihtoehtoja ei siis ollut ja Olli lähti kiltisti kouluun. Näin Vuorio suoritti kahdeksannen luokan koulussa ainoana reservin vänrikkinä ja muiden oppilaiden esimiehenä.

Talvisodan aikana Vuorio oli koulutuskeskuksessa ja välirauhan aikana RUK:ssa kurssilla 47, jossa oli noin 1500 oppilasta. Kurssin päättymisen 6.9.1940 Vuorio muistaa erinomaisesti, sillä sehän oli sama kuin hänen syntymäpäivänsä. Lukion päättymisen jälkeen Vuorio ilmoittautui 4.6.1941 Sulkavalla 6. Prikaatissa reservin vänrikkinä jatkamaan varusmiespalvelua. 10.6.1941 prikaati muuttui Jalkaväkirykmentti 6:ksi ja he marssivat kaksi vuorokautta Ruokolahteen suojajoukoksi. Tästä Vuorio totesi, ”että silloin

vänrikkiä hirvitti”. Hän kykeni edelleen palauttamaan mieleensä ne vahvat tuntemukset, jotka nuorella sotilaalla oli tuolloin. RUK:n aikainen koulutus oli ollut olematonta, edes yhtä kunnollista junailutehtävää ei ollut sattunut kohdalle, kurssin suuresta koosta johtuen. Vuorio ei muistanut myöskään, että heillä olisi ollut ainuttakaan ampumaharjoitusta RUK:ssa. Nuoren vänrikin koulutus oli ollut puutteellista. Joukko, johon Vuorio kuului, oli varusmiespataljoona, jonka varusmiehet olivat olleet tuolloin palveluksessa jo noin kaksi vuotta. He olivat valiojoukko, johon nuori joukkueenjohtaja pystyi luottamaan ja turvautumaan.

JR 6 oli yksi Karjalan kannaksella 18. Divisioonan rykmenteistä. Heinäkuun viimeisenä päivänä alkoi hyökkäys, jonka kärjessä JR 6 oli koko ajan. Hyökkäys päättyi Valkeasaaren syyskuun alkupäivinä. Vuorio oli ainut joukkueenjohtaja, joka tuli perille. Muut kaatuivat tai haavoittuivat - ”minulla kävi hyvä onni, vaikka läheltä piti-tilanteita oli monia”, Vuorio toteaa. Tappioita tuli paljon, Valkeasaaren saavuttaessa puolet joukkueesta oli täydennysmiehiä. Keskusteltaessa siitä, miten tappioita käsiteltiin, Vuorio vastasi, ”ei oikeastaan mitenkään”. Kaikille oli varmasti ankarin paikka se, kun kohdalle tuli ensimmäisen miehen kaatuminen. Tällöin tajusi, että täällä voi ihan oikeasti mennä henki. Vähitellen tähän kaikkeen kuitenkin tottui.

Vuoden 1942 keväällä tuli tieto Kadettikoulun alkamisesta ja Vuorio ilmoittautui halukkaaksi. Koulu alkoi 1.7.1942. Joukkue oli JV 1 I, johtajanaan kapteeni Olavi Larkas. Kahden viikon kohdalla joukkueelle valkeni, että kyseessä oli viestijoukkue. Joukkueessa oli toistakymmentä henkilöä, joilla ei ollut mitään kokemusta viestistä. Valintaa ei tehty osaamisen tai halukkuuden kautta, vaan joukkuejako tehtiin aakkosten perusteella. Tämä poikkeaa suhteellisen paljon nykyisen Kadettikoulun aselajivalinnoista. Koulun päätyttyä Vuorio ei tuntenut osaavansa viestistä oikeastaan yhtään mitään, sillä koulussa ollut opetus oli hyvin puutteellista. Onneksi kaksi viikkoa koulun päättymisen jälkeen oli Mikkeliissä kirkasjohtokurssi, joka paransi huomattavasti Vuorion osaamista viestiasioista.



Viestijoukkue jaettiin kahtia, jonka toinen puoli lähti koulutuskeskukseen ja toinen rintamalle. Vuorion paikaksi tuli koulutuskeskus Miehikkälässä ja Taavetissa. Koulutuskeskuksen alueella tehtiin linjatoita ja kaapelointeja. Syksyllä tuli siirto Viestipataljoona 5:een (VP 5) Aunukseen.

VP 5 komentajana toimi jääkärimajuri Seppä ja Vuorio oli joukon ainut kadettiupseeri. Joukkueen varajohtajana hänellä oli kersantti Ranta, joka oli palvellut Riihimäellä Viestirykmentissä ja osasi asiansa. Tekemällä opittiin ja kokemusta karttui koko ajan lisää. Ihan loppu vaiheessa Aunuksella Vuorio siirrettiin pataljoonan esikuntaan kalustoupseeriksi. 1943 syksyllä pataljoona kuormattiin junaan Lappeenrannassa ja koska miehet olivat kotoisin pääosin pohjanmaalta, niin kuviteltiin, että päästään Ilmajoelle ja pataljoona kotiutetaan. Matkalla kuitenkin kerrottiin, että ollaan menossa lappiin. Lapissa jouduttiin siirtymään laivalla ilman ilmasuojaa Tornioon, josta matkaa jatkettiin Rovaniemelle. Rovaniemellä oli tarkoitus jatkaa tutuksi tulleita linjatoita. Tarvikkeita ei kuitenkaan ollut ja ilma sekä olosuhteet olivat ankeita. Marraskuun puolivälissä tuli puhelu, jossa todettiin, että luutnantti Olli Vuorio siirretään Mikkeliin Päämajaan.

Kahden viikon jälkeen Vuorio kuitenkin komennettiin Mikkelistä viestiosasto kolmeen Helsinkiin. Vuorion ollessa viestiosastolla elettiin aikaa, jolloin

valvontakomissio oli Suomessa. Vuorio laati tuolloin yhteenvetoja valvontakomissiolle viestijoukkojen tilanneilmoituksista. Nämä ilmoitukset laadittiin kynällä kirjoittaen.

Välirauhan tultua Vuorio pyrki Hämeenlinnaan, koska morsian, johon hän oli tutustunut Aunuksella, asui paikkakunnalla. Vuonna 1946 Vuorio sai siirron Hämeenlinnaan, Suomen kasarmeille Viestikouluun adjutantiksi. Koulun johtajana oli tuolloin everstiluutnantti Risto Kare. Kare kuitenkin hävisi koululta muutaman kuukauden kuluttua ja everstiluutnantti Matti Virva tuli hänen tilalleen koulun johtajaksi. Taas kului aikaa ja yhtäkkiä Kare palasi. Hänen poissaolostaan ei puhuttu missään vaiheessa yhtään mitään. Poissaolon syy selvisi Vuorion vastasta Matti Lukkarin kirjan (Asekätkentä 1984) ilmestymisen kautta. Kare oli toiminut Viestialan kätkenä johtajana.

Viestikoulusta Vuorion tie vei pakosiirtojen kautta Viestirykmentistä Ouluun ja sieltä huoltoupseerikurssille Santahaminaan. Kurssin jälkeen Vuorio siirrettiin Riihimäelle huoltopäällikön apulaiseksi. Aikaa Riihimäellä kului noin 10-vuotta, jonka jälkeen Vuorio siirrettiin jälleen pakosiirtona Huoltokouluun Santahaminaan perheen jäädessä Riihimäelle. Perhe asui tuolloin omakotitalossa, jossa vesi jäätynä talvella keittiössä. Myöhemmin Vuorio sai hankittua perheelle pankin suosiollisella avustuksella aravatalosta pienen kaksion, jolloin asuinolosuhteet muuttuivat huomattavasti paremmiksi. Koska palveluspaikkana oli Helsinki, niin Vuorio pyrki muuttamaan koko perheen pääkaupunkiin. Vaikka he olivat olleet asuntojonossa pisimpään, niin asuntoa ei saatu. Vuorion mitta tuli täyteen tästä toiminnasta ja hän pyysi siirtoa, minne tahansa. Siirto Pääesikunnan taloushuolto-osastolle tuli pyynnöstä parin kuukauden kuluttua. PE:ssä palvelusaikaa kertyi parisen vuotta, jolloin Vuorio huomasi, että moni nuorempi kapteeni ylennettiin majuriksi, anoi eroa, osaeläkettä ja erosin palveluksesta.

Siviilissä Vuorio pääsi häntä Mikkeliin opettaneen Simo Laurilan johtamaan Maaseudun Autoliittoon. Maaseudun Autoliitossa toimiessaan hänelle tarjottiin Tehokalusteen varastopääl-

likön paikkaa, jonka hän otti vastaan. Tätä työtä kesti vain hetken, sillä laman saapuessa hänet irtisanottiin. Vuorio pääsi onnekseen muutaman kuukauden kuluttua harjoittelijaksi rouva Autin agentuuriliikkeeseen. Agentuuriliikkeen asioissa Vuorio meni myymään Pääesikuntaan kivisahaa, jota ei ollut koskaan nähnyt. Tällä käynnillä Vuorio tapasi entisen esimiehensä eversti Simo Liikkasen. Eversti Liikanen tarjosi mahdollisuutta palata palvelukseen ja Vuorio tarttui tähän tilaisuuteen päivän harkinta-ajan jälkeen. Työt jatkuivat hetken aikaa kapteenina Pääesikunnan muonitustoimistossa ennen ylennystä majuriksi. Ura jatkui vielä tämän jälkeen Kaartin pataljoonassa huoltopäällikkönä. Vuorio alkoi epäillä, että kohta on taas tulossa aika, jolloin todennäköisyys pakkosiirrolle lähenee ja hän alkoi kartoittamaan mahdollisia työpaikkoja siviilissä. Hän haki ja sai töitä Kappakeskuksesta ja erosi Puolustusvoimien palveluksesta.

Vuorio toimi tarkastajana Pukimon Kauppakeskuksessa (sittemmin Pukeva) vuoteen 1982 saakka, jolloin siirtyi virallisesti eläkkeelle. Tänä aikana häntä kosketti avioero ensimmäisestä

puolisosta, liitosta, jonka piti kestää koko elämä. Onnekseen Vuorio löysi itselleen kuitenkin uuden vaimon Aunen, joka työskenteli myös Pukimon palveluksessa.

Viestiupseeriyhdistys perustettiin Riihimäellä vuonna 1945 ja ensimmäiseksi puheenjohtajaksi valittiin everstiluutnantti Virva. Vuorio on yksi yhdistyksen perustajajäsenistä ja tätä kautta hän on ollut mukana yhdistyksen toiminnassa aina sen alkua ajoista lähtien aktiivijäsenenä. Viestimieslehteä perustettaessa Virva soitti ja pyysi Vuoriota viestimieslehden toimitussihteeriksi. Vuorio kieltäytyi jyrkästi kyseisestä tehtävästä ja on myöhemmin monesti harmitellut tuota päätöstä. Vuorio on kirjoittanut elämänsä aikana yhden maillisen juttuja Viestimieslehteen.

Vaikka ikää on kertynyt näinkin paljon, ei Vuorio ole jäänyt paikoilleen, vaan hän on osallistunut monenlaiseen yhdistystoimintaan ja käynyt puhumassa lukemattomia kertoja nuorille kouluissa. Hän käyttää päivittäin tietokonetta, älylaitteita ja kirjoittaa artikkeleita sekä lukee ja lähettää sähköposteja. Arjen välineet ovat osa Ikikaaderin

päivittäistä elämää. Valokuvaaminen, jonka Vuorio aloitti vuonna 1935 ja kuvakirjojen tekeminen ovat edelleen se tärkein yksittäinen harrastus Vuoriolle. Kirjoja valmistuu tasaiseen tahtiin ja nyt niitä on kertynyt jo 70 kappaletta. Haastattelun jälkeen Vuoriolla oli tarkoitus lähteä valmistelevaan tulevia syntymäpäiviään ja kamera lähtee tietysti matkalle mukaan.

Tämä haastattelu on vain pieni osa Ikikaaderi Vuorion tarinaa. Mikäli haluat tutustua häneen, kadettikurssiin 26 ja joukkoihin, joissa Vuoriokin on palvellut, niin tietoa löytyy runsaasti. Voit aloittaa tutustumisen lukemalla esimerkiksi artikkelin Helsingin Sanomista 19.3.2019, joka käsittelee kurssia 26 tai Ikikaaderin oman kirjoituksen (Ikikaaderin taipaleelle) Kylkiraudasta 4/2018.

Merkkipäiväänsä 6.9.2019 Vuorio vietti tekemällä kunnianosoituksen Sankariristille ja Suomen marsalkka Mannerheimin hautapaadelle. Tämän jälkeen juhlaa jatkettiin lähipiirin ja kutsuvieraiden kanssa juhlatilaisuudessa.

Viestimies-lehti esittää lämpimät onnittelut Olli Vuoriolle.

Henkilöasiat:

Siirrot ja tehtävään määräämiset

- everstiluutnantti **Mika Huttunen** (PVTUTKL) tutkimusalojohtajaksi doktriiniosastolla Puolustusvoimien tutkimuslaitoksessa 1.7.2019 lukien enintään siihen saakka, kunnes tehtävään määrätään varsinainen tehtävänhoitaja
- komentaja **Sami Vesterinen** (PV-TIEDL) keskuksen johtajaksi operatiokeskukseen Merivoimien esikuntaan 1.9.2019 lukien
- everstiluutnantti **Juhapekka Lötjönen** (MAAVE) erityistehtävään (hanketohtaja) johtamisjärjestelmäosastolle Pääesikuntaan 1.12.2019 lukien
- everstiluutnantti **Juha Peltomäki** (MAASK) apulaisosastopäälliköksi johtamisjärjestelmäosastolle Maavoimien esikuntaan 1.12.2019 lukien

Ylennykset 4.6.2019

Everstiluutnantiksi

- majuri **Tuomas Arajuri**

Ylennykset reservissä 4.6.2019

Majuriksi

- kapteeni **Antti Laurila**

Insinöörimajuriksi

- insinöörikapteeni **Mika Seppänen**

Luutnantiksi

- vänrikki **Juha Nyholm**



elisa^{5G}

Nouse uudelle tasolle

elisa.fi/5G



Yhteydet maastoon Nestorin tuotteilla

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

nestor
cables

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

Mittarikuja 5,
90620 Oulu
PL 276, 90101 Oulu