

Viestimies

Viestiupseeriyhdistyksen julkaisu 77. vsk Numero 3 Syksy 2022

Keskittämisen ja hajauttamisen historia ja tulevaisuus, sivu 6

Huoltovarmuuden digitaalinen ulottuvuus, sivu 9

Viestikoulun kansainvälinen toiminta, sivu 13

www.viestiupseeriyhdistys.fi



COMBITECH

Experts in Digitalizing Defence

Viestimies-lehti

Päätoimittaja
Samuli Terämä
p 050 3399038
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Hanna Liitola
p 040 5930675
henkilotoimittaja@viestiupseeriyhdistys.fi

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

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

Toimituksen osoite:
Päivölärinne 7 A 1
04220 Kerava

www.viestiupseeriyhdistys.fi/viestimies
Pankkitili FI21 5780 5520 0177 44
Vuosikerta 35 €

Tilaukset ja osoitteenmuutokset
Harri Reini
p 040 514 2497
toiminnanjohtaja@viestiupseeriyhdistys.fi

Ilmoitusmyynti
Juha Halminen
p 09 873 6944, 050 592 2722
juha.halminen@kolumbus.fi

Painopaikka
Newprint Oy, Raisio
p 010 231 2600

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



Kansikuva. Pohjoismaista yhteistoimintaa
VIGILANT KNIFE-harjoituksessa Rovajärvellä.
Kuva: Samuli Terämä

Tässä numerossa

- 4 Pääkirjoitus: Paluu tulevaisuuteen
- 6 Keskittämisen ja hajauttamisen historia ja tulevaisuus
- 9 Huoltovarmuuden digitaalinen ulottuvuus
- 13 Viestikoulun kansainvälinen toiminta – missä mennään Suomen ja Ruotsin välillä nyt?
- 17 Järjestelmäintegroitumisen tulevaisuudesta
- 21 Valokuitukytkentöjen rajapintojen puhtaus varmistaa kriittiset verkkoyhteydet
- 25 Viestimiespäivät 2022
- 27 Analysaattori
- 29 Viestimies 50 vuotta sitten
- 30 Viestiupseeriyhdistyksen seminaari-ilmoitus
- 31 Kadonneen radiovastaanottimen metsästys
- 31 Viestiupseeriyhdistyksen seminaari-ilmoitus

Seuraavan numeron aineistopäivä on 17.10.2022. Lehti ilmestyy viikolla 49.

Paluu tulevaisuuteen

Syyskelit vyöryvät päälle sateineen, tuuliseen ja viileine ilmoineen. Koronavirus on piinannut meitä lähes kolmen vuoden ajan, mutta se vihdoinkin näyttää hellittävän otettaan. Venäjän hyökkäyssotakin Ukrainassa on kestänyt jo yli puoli vuotta. Viime viikkoina Ukraina on aloittanut vastahyökkäykset omien alueidensa takaisin valtaamiseksi ja toistaiseksi joukot ovatkin saaneet vallattua takaisin miehittyjä alueita Harkovan alueella. Ukrainan ja Venäjän välisen sodan vaikutukset ovat olleet varsin mittavia ja dramaattisia. Maailman markkinat ovat kokeneet ennakoimattoman suuria muutoksia esimerkiksi vilja- ja sähkömarkkinoiden saralla. Ukrainan asema merkittävänä vehnän viejämaana on vaikuttanut maailman laajuisesti vehnän hintaan. Myös sähkömarkkinat ovat olleet sekaisin viime talvesta lähtien. Hinta on noussut Suomessakin moninkertaisesti. Vaikka sota ei olekaan välittömästi Suomen naapurissa, sen vaikutukset ulottuvat niin yksityisiin henkilöihin kuin yrityksiinkin. Yleinen kustannustason nousu vaikuttaa kaikkeen ja kaikkiin. Inflaatio on noussut jo 9% tietämille ja myös viitekorot ovat nousussa. Sekä yksityistalouksien että yritysten talouden tasapainottaminen tulee olemaan haastavaa.

Eri tuotantolaitokset ovat saaneet palautettua tuotantoansa koronatilanteen helpotuttua. Komponenttien tuotanto on vähitellen elpymässä, mikä helpottaa pitkään jatkuneita laitetoimituksien viivästymisiä ja saatavuutta. Vaikka nykyinen maailman tilanne vaikuttaaakin monessa mielessä hyvin epävakaalta, maailma ei silti pysähdy. Epävakaassakin tilanteessa meidän on katsottava tulevaisuuteen. Työ- ja elinkeinoministeriön on julkaissut juuri huoltovarmuuden selonteon, jossa määritetään suuntaviivoja aina 2030 vuoteen asti. Selonteossa peräänkuulutetaan entistä kokonaisvaltaisempaa huoltovarmuutta ja toimintamallien kehittämistä. Sen keskeisin sisältö liittyy huoltovarmuuden taloudellisiin resursseihin, sääntelyyn, osaamisen varmistamiseen ja yhteistyön tiivistämiseen. Selonteon tuominen käytäntöön on tärkeämpää nyt kuin koskaan.

Suomen Nato-jäsenyys edistyy pienin askelin. Tätä kirjoittaessa enää kolme maata on ratifioimatta Suomen jäsenyyden. Vaikka Suomi on ollut ePPF-maa (Enhanced Partnership for Peace) Ruotsin kanssa jo pitkään, nyt tarkkailijajäsenyyden myötä on avautunut monia mahdollisuuksia ja yhteistyöohjelmia Naton



sisällä. Aiemmin Suomella ei ole ollut näihin asiaa. Tämä vaikuttaa luonnollisesti siihen, ettei aiemman yhteistyön mukaisesti määritetty henkilöstö enää riittä osallistumaan kaikkiin tilaisuuksiin, joihin Suomella olisi intressejä. Esimerkiksi Upseeriliitto on esittänyt merkittävää henkilöstölisäystä Nato-tehtäviin. Tulevaisuus näyttää, kaikki ne yhteistyöfoorumit ja työryhmät, joihin Suomi katsoo tarpeelliseksi osallistua ja kuinka paljon niihin henkilöstöä tarvitaan.

Suomi ja Ruotsi ovat olleet hyvin esillä kansainvälisillä foorumeilla puolustuksen suorituskykyjen osalta. Suomessa on järjestetty viime kuukausien kuluessa useita, nopeallakin aikataululla toteutettuja harjoituksia. Näillä harjoituksella on osoitettu kaikille kiinnostuneille tahoille kykyä vastata nopeastikin muuttuvan turvallisuusympäristön vaikutuksiin. Kesän aikana Suomen maaperällä on ollut yhdysvaltalaisia, brittejä, norjalaisia ja ruotsalaisia sotilaita harjoittelemassa yhdessä suomalaisten kanssa. Näissä harjoituksissa on harjoiteltu erityisesti yhteisoperointia ja kykyä toimia yhden, suomalaisen johdon alaisuudessa. Samaa yhteisoperointia on toki tehty ennenkin, mutta suomalaiset joukot ovat olleet silloin muun maan johdossa.

Yhteisoperointi vaatii joukoilta ja järjestelmiltä paljon. Yhteinen kieli, toimintatavat, johtaminen ja johtamisjärjestelmät sekä huolto ovat merkittävimpiä operoinnin edellytyksiä. Vaikka Suomi onkin ollut jo pitkään Nato-yhteensopiva, eivät kaikki suomalaisetkaan joukot ole tottuneet toimimaan yhdessä ulkomaiden joukkojen kanssa. Viime aikojen harjoitukset ovat lisänneet merkittävästi varmuutta ja osaamista yhteisoperoinnista kaikilla tasoilla. Vaikka joukkoja saattaa aluksi arveluttaa toimiminen vieralla kielellä, ei suomalaisilla ole yhtään hävettävää osaamistasossa. Taktinen, taistelutekninen ja tekninen osaaminen ovat huippuluokkaa, eikä kielitaitokaan ole este. Jos heti ei löydy oikeita sanoja, niin keskustelemalla löytyy oikeat termit ja yhteinen ymmärrys mitä ollaan tekemässä. Kansainvälinen toiminta ei eroa paljoakaan toiminnasta kotimaassa. Siinä tulee vain huomioida erilaiset lähestymistavat ja terminologia. Toki väärinymmärryksen mahdollisuus on aina olemassa, mutta yhteistyöllä ja yhdessä tekemällä nämäkin sudenkuopat ovat väistettävissä. Se edellyttää opettelua ja yhdessä tekemistä, mutta luotan suomalaiseen sotilaaseen. Suomalainen sotilas on ennenkin mennyt läpi harmaan kiven saavuttaakseen päämäärän ja täyttääkseen annetun tehtävän.

Hyvää syksyn jatkoa kaikille!

Päätoimittaja

Samuli Terämä



Digitalisoimme taistelukenttää

**jossa panokset ovat korkeimmat,
vaatimukset ovat kovimmat ja teknologia ratkaisee**

MilDefin tarjonta käsittää ruggeroitua elektroniikkaa, ohjelmistoja ja palveluita. Tuotteitamme käytetään maalla, merellä ja ilmassa niin kansallisissa kuin kansainvälisissä operaatioissa maailmanlaajuisesti, äärimmäisissä ja vaativissa ympäristöissä.



Taistelukentän tietotekniikan numero 1

MilDef on jo 25 vuotta kehittänyt ja toimittanut ruggeroitua tietotekniikkaa ja erikoiselektroniikkaa puolustusvoimien ja muiden turvallisuusviranomaisten käyttöön. Olemme pohjoismainen toimittaja, joka tarjoaa integroituja ja räätälöityjä laitteistoratkaisuja myös kyberpuolustuksen tarpeisiin.

Ota yhteyttä saadaksesi lisätietoja mobiilituotteistamme, näyttöistämme ja 19"/2 -laitteistamme.



Tero Maaniemi toimii Teliällä Suomen verkkojen ja Infran pääarkkitehtinä.

Teksti: Tero Maaniemi

Kuvat: Tero Maaniemi, internet

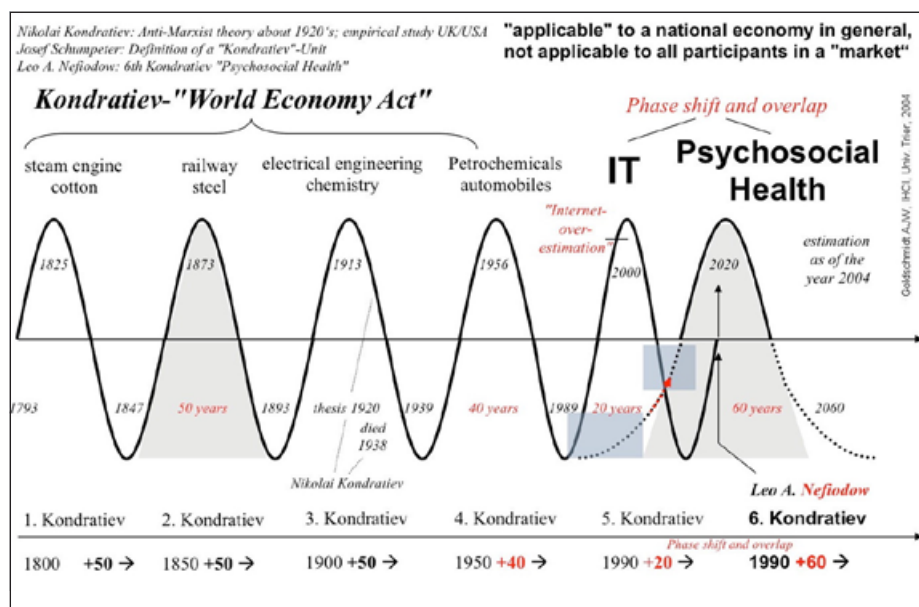
Keskittämisen ja hajauttamisen historia ja tulevaisuus

Informaatioteknologia on käynyt vuosien saatossa aaltoliikettä hajauttamisen ja keskittämisen välillä. Tämä aaltoliike ei ole pysähtynyt vaan korkeintaan lähtenyt kohti uutta suuntaa. Tällä kertaa vuorossa on hajauttamisen aalto. Tässä artikkelissa pyritään luomaan kuvaa siitä miten aiemmat aallot ovat vaikuttaneet seuraaviin, ja mitä on mahdollisesti odotettavissa viimeiseltä hajauttamisen aalloilta. Valmiita vastauksia tai teknologisia ratkaisuja ei ole tarjolla, sen sijaan pureudun pohtimaan syitä ja seurauksia ja mahdollista tulevaisuutta.

Moni asia maailmassa seuraa aaltoliikkeitä. Yksi merkittävimmistä nyt nähtävistä poliittisista aaltoliikkeistä on globalisaatio. Maailmamme on nähnyt useita kertoja liikkeitä tiiviimpiin riippuvuussuhteisiin vaan valuakseen pois noista riippuvuussuhteista. Talouden osalta on esitetty useita erilaisia syklejä, joista ehkä tunnetuin on Kondratjevin aallot. Kondratjevin aallot kuvaavat teollistumisen aaltoja. Aallot katkeavat suuriin lamoihin ja syntyvät katoja seuraavista nousukaudesta. Näitä aaltoja on ollut tähän mennessä viisi, ja kuudes on juuri alkanut. Yhteistä näille sykleille tai aalloille on se, että ne seuraavat ihmisen elinkaarta. Pidemmät syklit ovat ihmisen eliniän mittaisia ja lyhyemmät taas liittyvät usein ihmisten työuriin. Pörssisykleissä on useasti kyse siitä, että ihmiset eivät joko enää pelkää tai eivät enää muista. Vanha totuttu toimintatapa ei olekaan enää uudessa tilanteessa yhtä toimiva. On muutettava suuntaa. Sama ajattelu pätee sähköiseen tietojenkäsittelyyn.

Nykymallin mukaisen tietojen käsitteelyn voi tulkita lyöneen läpi aikaisintaan toisen maailmansodan aikana, kun britit purkivat saksalaisten enigma-koodin.

Koodi tuotettiin mekaanisella laitteella, jossa salaus perustui laitteen sisällä pyöriviin salauskiekkoihin. Laite patentointiin 1918 ja toiseen maailmansotaan



Kuva 1. Kondratjevin aallot.

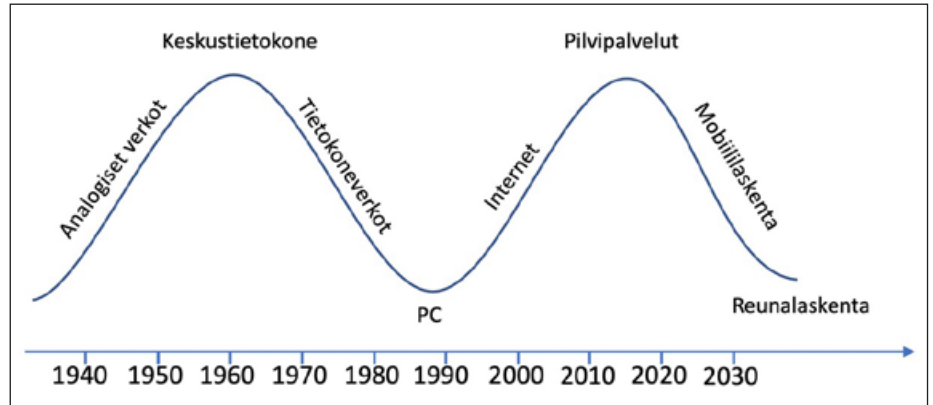
mennessä tuota mekaanisiin kiekkoihin perustuvaa salausta ei ollut kyetty purkamaan. Koodauslaite ei siis ollut nykyisen kaltainen tietokone, mutta koodin purkuun käytetty laite oli. Laite sijaitsi ja se kehitettiin Englannissa Bletchley Parkin kartanossa. Tätä laitetta englantilaiseen kartanoon rakennettua konetta voitaneen pitää ensimmäisen modernina tietokoneena ja sen ollessa yksi, oli se myös hyvin keskitetty. Tästä kohdin voidaan ajatella lähteneen liikkeelle aaltoliike keskitetyn ja hajautetun laskennan välillä.

Keskustietokoneet ja matka kohti tietokoneverkkoja

Toisen maailmansodan aikana huomattiin tietotekniikan merkitys sotilaallisessa toiminnassa, mikä mahdollisti merkittäviä investointeja suurille yrityksille, kuten IBM. Yhdysvaltain puolustusvoimien DARPA (Defense Advanced Research Projects Agency) ja yliopistot olivat tiiviissä yhteistyössä kehittämässä tietoteknisiä kyvykkyksiä. Alkuvaiheessa laskentakyky oli paikallista ja itsenäistä. Ajan myötä DARPA:n ja yliopistojen yhdessä kehittämän verkkoteknologian yleistyessä tuli mahdolliseksi jakaa tietoa yksittäisten laskentapisteen välillä verkon yli. Syntyi ensimmäiset tietokoneverkot ja internetin esiaste. Keskustietokoneiden ilmeinen ongelma oli niiden valtava koko ja koon mukainen hinta. Laskentakyky ei ollut kuitenkin hyvin harvojen saatavilla ja yhä useampi olisi halunnut päästä osaksi tietokonevallankumousta.

Henkilökohtainen tietokone ja internetin synty

Laskentakyvyn saatavuuden laajentaminen ei ollut mahdollista keskustietokoneiden ja siihen kytkettyjen päätteiden lisäämisellä, vaikka useissa 1970-luvun scifitarinoissa näin annettiinkin ymmärtää. Merkittävin este oli tietoverkkojen puutteellinen kyky kuljettaa tietoa päätteen ja keskustietokoneen välillä pitkiä matkoja. 1970- ja 1980-luvun vaihteessa toimineen Homebrew Computer Clubin piirissä valmistettiin nimensä mukaisesti ensimmäisiä kotikutoisia mikrotietokoneita, jotka pystyivät IBM:n kauhuksi vastaamaan tietotekniikan demokratisointiin verkkojen rajoitteista huolimatta. Laskenta oli löytänyt paikkansa kodeista ja pienistä toimistoista eikä ollut enää suurien valtiollisten ja yksityisten konsernien ulottuvilla. Vaikka verkot eivät mahdollistaneetkaan edellä kuvattua



Kuva 2. Hajauttamisen ja keskittämisen aaltoliike.

päätelaitekäyttöä, ne mahdollistivat näiden uusien koteja valtaavien tietokoneiden kytkemisen toisiinsa ja myös suuriin keskustietokoneisiin. Kyvykkyys oli alkuvaiheessa hyvin rajallinen eikä mahdollistanut kuin erityisen yksinkertaisia verkkotoimintoja kuten verkkopankin. 1991 muutti tilanteen, kun Tim Berners-Leen johdolla käynnistettiin ensimmäinen HTML-koodia tukeva WWW-palvelin. Internet oli syntynyt, ja laskenta saattoi jälleen keskittyä.

Pilvitoimijat ja mobiiliverkkojen nousu

Internetin nousun myötä syntyi iso liuta uusia yhtiöitä 1990-luvun lopulla. Pörssi-markkinat uskoivat uuden runsauden sarven löytyneen, eikä mikään voisi lopettaa kasvua. Todellisuudessa tietoliikenneverkkojen kehityksen valtaisa vauhtikaan ei riittänyt lunastamaan alkuvaiheen hurjia vaatimuksia. Ns. Dotcom-kuplan puhjettua päästiin kehityksessä terveelle pohjalle ja romahduksen pohjilta nousi aluksi useita keskitettyjä verkkopalveluita (verkkokauppa, videopalvelut, kuvapalvelut jne). Alkuvaiheen verkkopalveluilla ei ollut sosiaalisen median ulottuvuutta, mutta niitä ja tulevia sosiaalisen median palveluita yhdisti ja yhdistää edelleen palveluiden keskittäminen harvoin globaalisti saatavilla oleviin datakeskuksiin. Keskustietokone teki pa-luun ja henkilökohtainen tietokone alkoi vähitellen muistuttamaan yhä enemmän päätelaitetta, jolla kytkeydyttiin pilvessä oleviin palveluihin. Päätelaitteistumista edistivät mobiiliverkkojen vahva nousu ja merkittävästi lisääntynyt kapasiteetti. Nykyään on mahdollista kantaa taskussa tupakka-askia pienempää laitetta, jossa on tarjolla kaikki maailman musiikki, elokuvat, taide ja kirjallisuus. Sisältö on

löytynyt tiensä ehkä lopullisesti julkiseen pilveen ja kaikkien saataville. Historia ei ole kuitenkaan tullut loppuun.

Reunalaskenta ja tuntematon tulevaisuus

On edelleen asioita, mitä ei voi tehdä harvaan sijoitetuissa julkipilvitoimijoiden datakeskuksissa. Tämä ei tarkoita sitä, että julkipilvi olisi tulossa tiensä päähän. Kirjoitanhan minäkin tätä artikkelia parhaillaan henkilökohtaisella tietokoneella, jossa on paikallista laskentatehoa, ja sekään ei tullut tiensä päähän. Julkipilven vahvuudet ovat helppo, nopea ja kustannustehokas skaalautuminen ja ääretön redundanssi. Nykyisen kaltaisella julkipilvellä on kuitenkin yksi heikkous, mikä oli tuttu jo keskustietokoneiden aikana. Valonnopeudelle ei voi mitään eikä sen suhteen voi neuvotella. Viive tulee olemaan rajoittava tekijä sille, mitä palveluita voidaan nykyisen mallisiin julkipilvipalveluihin siirtää. Mitä ei voi tehdä kaukana, on tehtävä lähellä.

Aikaisemmissa aalloissa pääosassa on ollut perinteisiin tietokoneisiin verrattavissa olevat laitteet. Hajautuvasta laskennasta tulevat hyötymään selkeästi laajimmin palvelut, jotka vaativat lyhyttä viivettä. Näistä yhtenä esimerkkinä voidaan pitää automaatiojärjestelmiä, missä antureiden tuottamaan syötteeseen reagoidaan ja tuotetaan järjestelmien ohjausta ilman ihmisen väliintuloa. Laajemmin voidaan puhua korkealentoisista termeistä, kuten kaiken internet (internet of everything). Myös yhden laitteen tai vieläpä itsenäisten laitteiden ajattelusta on jo siirrytty vahvemmin ekosysteemiä ajatteluun vuosia sitten. Laskennan hajauttaminen mahdollistaa näiden ekosysteemien laajentamisen sekä laitteiden

määrässä että koko ekosysteemien kyvykkyyksissä tuottaa hyödyllistä informaatiota käyttäjilleen.

Miksi tällä on merkitystä?

Tietotekniikka on toiminut pitkään omalla ajurinaan siirryttäessä aallonharjoista kuoppiin ja takaisin. Nyt edessä olevan hajauttamisen tarpeen luo ensisijaisesti perinteinen laskenta, mitä edustaa mm. teollisuusautomaatio. Se on alue, jossa ei ole perinteisesti ollut halukkuutta tehdä ensimmäisenä uusia asioita tietoliikenteen tai tietotekniikan suhteen. Virtuaalisoitujen ympäristöjen laajeneminen teollisuuteen voisi mahdollisesti tuoda merkittäviä hyötyjä joustavuudessa ja varmuudessa. Toinen merkittävä hyötyjä on alueelliseen itsenäisyyteen tukeutuvat toimijat. Viive on ohjaava tekijä mentäessä kohti reunalaskentaa. Reunalaskenta mahdollistaa vahvemmin saarekkeisen toiminnan. Tämä tulee ikään kuin ”kaupan päälle”.

Aaltojen perintö

Aaltojen harjoista ja pohjista peritään tietoa seuraavaan harjaan ja seuraavaan pohjaan. Aallonharjalta laskeudutaan alas pohjaan, koska edellinen harja ei ole tyydyttänyt kaikkia tarpeita. Keskustietokoneiden puutteellisuus loi pohjan henkilökohtaiselle tietokoneelle, henkilökohtaisen tietokoneen puutteet taas pilvipalveluille. Harjat ovat kuitenkin sukua toisilleen siinä, missä pohjatkin ovat toisilleen. Keskustietokoneilla on paljon yhteistä tämän päivän pilveistymisen kanssa. Uskon myös, että henkilökohtaisilla tietokoneilla on paljon yhteistä tulevan reunalaskennan kanssa.

Merkitys kansalliselle turvallisuudelle ja jatkuvuudelle

Tänään tuntemiemme tietoverkkojen pohjimmainen periaate on ollut aina se, että minkä tahansa noodin voi poistaa verkosta ja verkko toimii edelleen.

Julkipilvitoimijoiden verkosto on kansallisesta näkökulmasta harmillisen keskittynyt. Tämä johtaa siihen, että jo yhden kohteen menettäminen saattaa olla haitallista. Hajauttaminen tuottaa mahdollisuuden tarjota pientä viivettä laajasti, tämä ei kuitenkaan ole ainoa etu. Etuna on myös se, että verkko on hajautettuna pilkottavissa pienempiin osiin myös maiden sisällä, ja nämä osat voivat toimia itsenäisesti. Palveluiden ja verkkojen rakenteet tulevat tulevaisuudessa johtamaan kohti tilannetta, missä yksi osa kokonaisuutta voi toimia ilman muita osia ja vastaavasti kokonaisuus voi toimia vailla sen yksittäisiä osia. Kun kaikki on lähellä, kaikki on hajautettu ja sitä myötä kestävämpää. Ukrainan sota on tehnyt selväksi sen, että vain toimimalla joustavasti ja paikallisesti, voidaan varmistaa tiedon kulku kriisitilanteessa. Ukrainassa tämä oli osittain mahdollista useiden pienten operaattoreiden olemassaolon vuoksi. Suomessa tuota kehitystä tulee ajamaan viivevaateet uusissa teknologioissa.

Kaikkiin viestiliikennehaasteisiin ei aina löydy valmista ratkaisua kaupan hyllyltä. Silloin tarvitaan asiantuntemusta, kokemusta ja ammattitaitoa.

Tämä parikaapelin kantorinkka ja monet muut räätälöidyt ratkaisut vaativien kumppaneiden haasteisiin löydät Milconista.

MILCON

Valmis vaativien kumppaneiden haasteisiin



LÖYDÄT MEIDÄT:

Kolmionkatu 5 D
33900 Tampere

Puh. 010 239 2170
info@milcon.fi



www.milcon.fi



Teksti: Antti Nyqvist

Kuvat: Huoltovarmuuskeskus

Huoltovarmuuden digitaalinen ulottuvuus

Kirjoittaja on valmiuspäällikkö, huoltovarmuusorganisaation Digipoolin poolisihteeri Teknologiaoteollisuus ry:ssä. HVO Digipooli on ICT alan yritysten verkosto, joka toiminnallaan tukee yritysten kokonaisturvallisuuden kehitystä erityisesti digitaalisen turvallisuuden aiheissa. Kirjoittajalla on pitkä yritysmaailman kokemus ohjelmistoprojektien ja palveluliiketoiminnan parista, projekteista sekä liiketoimintayksikön johtotehtävistä.

Huoltovarmuus on perunoita, viljaa, pahan päivän varalle varautumista – on se niitäkin, mutta myös paljon muuta. Mitä huoltovarmuus oikeastaan tarkoittaa modernissa maailmassa?

Suomen valtion toiminnalle ja niille elintärkeille kriittisille toimintoille kaikille on yhteistä se, että ne ovat pitkälti riippuvaisia digitaalisista järjestelmistä ja yhteyksistä, joiden avulla tietoa välitetään ja toimintaa ohjataan.

Yritysten merkitys - arvontuotanto/toimitusketjut – sopimussuhteet

Huoltovarmuus tänään tarkoittaa niiden kotimaamme toiminnan kannalta kriittisten toimintojen varmistamista monessa ulottuvuudessa. Useimmat kriittiset toiminnot, kuten energiatuotanto ja jakelu, on täysin riippuvaista kotimaisista yrityksistä ja siksi on tärkeää, että yritykset huolehtivat kokonaisturvallisuudestaan varsinkin ollessaan osana jotain kriittistä toimitus tai arvontuotantoketjua. Huoltovarmuutta tehdään siis yritysten kanssa heidän turvallisuuttaan kehittämällä. Huoltovarmuusorganisaatio keskittyykin yritysten sparraamiseen näissä toimitusketjuissa.

Kriittisissä arvontuotantoketjuissa korostuu viranomaisten ja yritysten välinen toiminta ja tiedonvaihto, keskinäisriippuvuus – asioita, jotka useimmiten tapahtuu sopimussuhteissa ja siksi sopimussuhteiden sisältökin on merkittävässä roolissa kun huoltovarmuutta turvataan. Keski-

näisriippuvuus on hyvin ajankohtainen aihe kun pohditaan Venäjän hyökkäyssodan vaikutuksia energiamarkkinaan ja sen moninaisia vaikutuksia esim. ICT alan toimijoiden vastuulla oleviin tietoliikenneverkkoihin, niiden verkkolaitteisiin, konesaleihin tai näiden toimintaan toistuvissa sähkökatkotilanteissa.

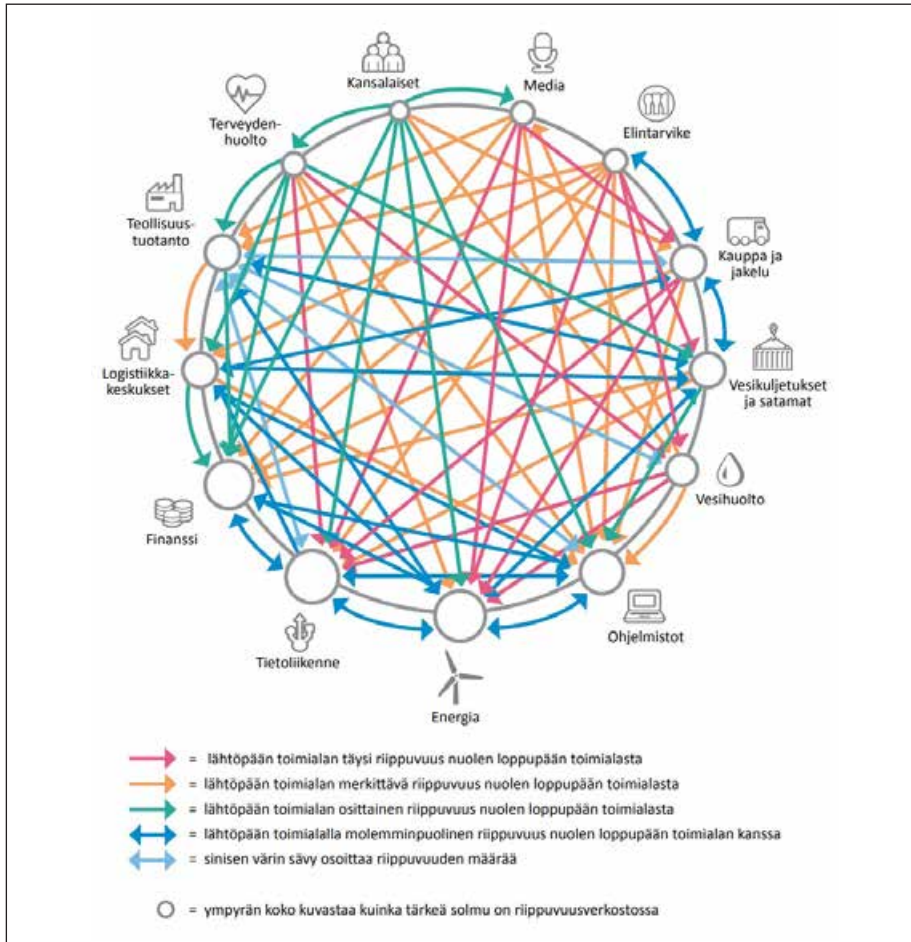
Huoltovarmuuden kannalta tulee siis tuntea, mitkä toimijat ovat näissä ketjuissa mukana ja mikä heidän kypsytyksensä on turvallisuuden aiheissa. Huoltovarmuusorganisaation Digipooli tekee töitä ICT alan yritysten ja muiden organisaatioiden kanssa tukien niiden kokonaisturvallisuuden kehitystä sekä tarjoaa tukea muulle huoltovarmuusorganisaatiolle ICT aiheeseen varautumiseen liittyen.

Digitalisaation turvallisuus

Yritysten toiminnassa ollaan Suomessa saavutettu yksi maailman korkeimmista digitalisaation asteista, joka tarkoittaa myös korkeaa riippuvuuden astetta digitaalisista ratkaisuista ja digitalisoinnin tahti vaan kiihtyy ja uusia riippuvuuksia

syntyy. Ja yrityksillä sekä muilla organisaatioilla onkin syntynyt myös Digitalisoinnin turvallisuuden suhteen velkaa. Ja tätä velkaa nyt pyritään kuromaan ja rakentamaan Digitaalisen turvallisuuden suhteen toimintamalleja, joissa turvallisuus olisi sisäänleivottuna.

Huoltovarmuuskeskuksen DT2030 (Digitaalinen turvallisuus 2030) kehitysohjelma on julkishallinnon suurin rahallinen panostus kyberturvallisuuteen ja toisin kuin euromääräisesti merkittävästi pienempi hallitusohjelman rahoitus kyberaiheisiin on se tarkoitettu elinkeinoelämän digitaalisen turvallisuuden kohtamiseen. Kehitysohjelman rahoitus suunnataan elinkeinoelämän toiminnassa haasteelliseksi tunnistettuihin aiheisiin. Aiheita tunnistetaan muun muassa yhteistoiminnalla yritysten kanssa – Digipoolin TIETO-harjoitukset sekä Selviytykset toimialojen kyberturvallisuuden tilasta ovat nostaneet esiin aiheita, joihin tulee tuottaa tukea niiden turvallisuuden ja varautumisen kehittämiseksi – varmistaksemme jatkuvuuden.



Kuva 1. Toimialojen kyberturvallisuuden tilanneselvitys 2020 nosti esiin myös alojen välisissä suhteissa korostuvia aiheita ja kertoo mm. siitä mihin kannattaa näiden toimijoiden välillä kiinnittää huomiota.

Elinkeinoelämän Toimialojen kyberturvallisuuden tila

Huoltovarmuustoiminnassa pyritään muodostamaan ymmärrystä yritysten tilanteesta niin liiketoiminnan kuin turvallisuudenkin aiheissa ja tätä on tehty mm. itsearviointeja tukemalla sekä erillisillä selvityksillä. Digipooli vastaa toimialojen kyberturvallisuuden tilaa selvittävän, toistuvan, kartoituksen järjestämisestä (Selvitys). Vuonna 2022 selvitystä tehdään taas ja tuloksia sadaankin pian julkaistavaksi ja toimialoilla käsiteltäväksi. Vuonna 2020 tehdyn selvityksen tulosten pohjalta on tunnistettu useita yrityksille yhteisiä haasteita, joissa pyritään löytämään keinoja kiihdyttää kehitystä. Näistä kehityskohteista kerrotaan seuraavissa kappaleissa.

Tilanneymmärrys ja tilannekuva

Koronapandemian myötä Huoltovarmuuskeskus sai Huoltovarmuusorganisaation kanssa tehtäväksi muodostaa

elinkeinoelämän tilannekuvaa ja tätä on määriteltäessä lähdetty kehittämään tässä luontaisessa verkostossa. Digitaalisen turvallisuuden ja kyberturvallisuuden osalta tätä tehdään vahvassa yhteistyössä viranomaisten ja elinkeinoelämän kanssa. Kyberturvallisuuskeskus vastaa kyberturvallisuuden tilannekuvasta ja pääpiirteissään se koostuu heille raportoiduista häiriöistä, HAVARO järjestelmän tuottamista havainnoista sekä tiedonvaihtoverkoston (I. ISAC ryhmät) välittämästä tiedosta.

Kyberturvallisuuden tilannekuvaa koostetaan ja jaetaan säännöllisesti ja sitä myös välitetään huoltovarmuuskeskukseen.

Huoltovarmuusorganisaatio taas kerää liiketoiminnan tilaan liittyvää tietoa – sillä jos se on uhattuna on useimmat kriittiset toiminnotkin uhattuna. Huoltovarmuuskeskus välittää heille näin kertyneet tiedot eteenpäin valtioneuvostolle ja toisaalta myös jakaa sitä yrityksille omassa toiminnassa hyödynnettäväksi.

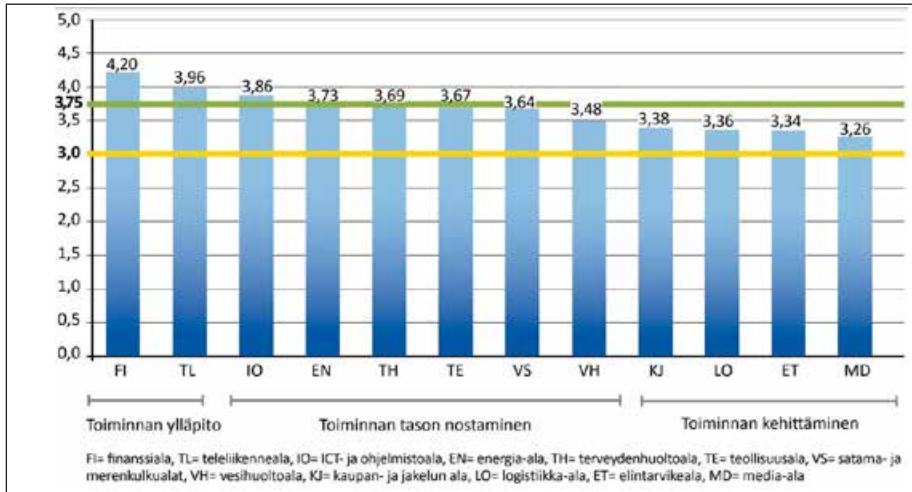
Nyt muodostettu tilannekuva ja ymmärrys on jo varsin hyvä otos kokonaisuudesta ja havainnoita sekä selviytymiskeinoja saadaan jaettua, mutta parannettavaakin löytyy. Esim. Kyberturvallisuuden tilannekuvan ei voi väittää olevan kaikenkattava ja siksi HAVARO järjestelmän käyttöä pitää pystyä laajentamaan kotimaisissa yrityksissä sekä ISAC ryhmiä perustaa aloille, missä niitä vielä uupuu.

Digipoolin 2020 selvityksen perusteella kehitettävää on myös siinä, että organisaatiot määriteltäessä muodostaisivat tilannekuvaa tai kun organisaatiot saavat tilannetietoa tai muodostavat sitä itse, ei se leviä organisaatioissa tarpeeksi hyvin tai että sitä osattaisiin kommunikoida hyvin myös sopimussuhteissa alihankkijoille tai asiakkaille. Nyt pyritäänkin löytämään toimenpiteitä, joilla voidaan tukea yrityksiä tätä tekemään ja jakamaan tilannekuvaa rakenteellisesti sitä tarvitseville. Esimerkkinä voidaan kysyä, että moniko taloushallinto on tietoinen käyttämiensä järjestelmien tilanteesta tai niihin kohdistuvista riskeistä?

Strategia

2020 Selvityksen havainnoista ehkä tärkein oli se, että kaikille yrityksille yhteinen haaste oli se, että Kyber- tai Digitaalisen turvallisuuden aiheet eivät näkyneet yritysten strategioissa. Ja tällä voi nähdä olevan vaikutusta siihen kuinka turvallisuus toteutuu yritysten arjessa. Nyt onkin tärkeää tehdä toimenpiteitä, jotka saavat yritykset lähtökohtaisesti käsittelemään aihetta liiketoimintatavoitteena – eikä vain osana riskienhallintaa. Nyt vedotaankin yritysten vastuullisuuteen digitaalisessa ulottuvuudessa sekä pyritään siihen, että yritykset tekevät arvolupauksia asiakkailleen siitä, että Digitaalinen turvallisuus ja asiakkaiden tiedot on turvattu vakuuttavasti. Tietosuoja onkin reguloituna aiheena tässä edellä muuta turvallisuutta.

Selvityksen myötä on perehdytty myös kotimaiselle yritysjohdolle tarjolla oleviin koulutuksiin ja todettu aiheen sieltä myös uupuvan. Käynnissä onkin nyt toimenpiteitä, joilla yritysjohdolle suunnatut koulutukset huomioisikin aiheen sisällöissään. Yliopistokoulutusta aiheesta jo löytyykin, mutta sielläkin aihe vaatii erikoistumista sen sijaan, että se olisi osana yleisopintoja.



Kuva 2. 2020 toimialojen suhteellinen kypsyys kartoituksen perusteella.

Se täytyy kuitenkin todeta, että pandemia ja käynnissä oleva sota ukrainassa ovat saaneet aiheen johtajienkin agendalle ja sikäli muutosta tapahtuu kiihtyvään tahtiin.

Liiketoimintojen priorisointi

Edelliseen liittyen ja tarvittavan investoinnin rajaamiseksi lähtee varautumistoiminta siitä, että organisaatiot kävisivät läpi toimintonsa ja priorisoisivat ne – niin oman liiketoiminnan kannalta tärkeiden kuin huoltovarmuuskriittisten toimintojen osalta. Priorisointi on tärkeää sikäli, että harvalla on resursseja suojata kaikki toiminnot saatavilla olevin keinoin, mutta ainakin ne tärkeimmät tulisi varmistaa ja niiden jatkuvuus taata. Yritysten strategian tulee vastata niihin kysymyksiin, että mitkä aiheet ovat näitä varmistettavia ja missä aiheissa on mahdollista ottaa tunnistettu ja harkittu riski. Digitaalisen turvallisuuden kannalta priorisointi tulee johtaa ICT järjestelmätasolle ja tunnistaa ne yhteydet ja järjestelmät, joista priorisoidut aiheet ovat riippuvaisia ja varmistaa ne tarvittavalla tasolla.

Tiedonvaihto ja kommunikaatio

Varautumiselle, jatkuvuudenhallinnalle ja huoltovarmuudelle oleellinen osa on jatkuva dialogi – tiedonvaihto niin yritysten sisällä, asiakkaiden ja alihankkijoiden sekä kumppanien kanssa unohtamatta viranomaisia. Aktiivisella tiedonvaihdolla selvittää erilaisista häiriötilanteista ja sillä on usein vaikutusta nopeaan palautumiseen.

Tiedonvaihtoon ja kommunikaatioon kuuluu tilannekuvan muodostaminen ja sen jakaminen eri tavoin verkostossa. Havaintojemme perusteella tässäkin toiminnassa on yhteiskunnassamme parannettavaa. Parhaillaan onkin käynnissä lainsäädäntöhankkeet, jotka edesauttavat eri tiedonvaihtoa niiden viranomaisten kesken, joilla on erilaiset toimivaltuudet normaaliolojen häiriötilanteissa tai valmiuslain pykälää käyttöön otettaessa. Puolustuseläntöön hengessä Digipoolissakin toivomme, että normaaliolojen tiedonvaihto ottaa huomioon kaikki viranomaiset tasapuolisesti, jotta ollaan liikkeellä oikeilla pohjatiedoilla siirryttäessä tiukempaan tilanteeseen ja uusiin toimivaltuuksiin eri viranomaisilla.

Elinkeinoelämän tiedonvaihdossa haasteita tuottaa sopimussuhteissa sen kohteen kriittisyyden oikea kommunikaatio. Yritysten toimintojen priorisoinnin myötä tulisi myös prioriteetti kommunikoida myös esim. alihankintasuhteissa ja se tehdään laatimalla sopimus. Usein on kuitenkin niin, että asian tärkeys tai sen ansaitsema turvallisuusinvestointi, eli asian kriittisyys, ei sopimukseen mallinnu. Kriittisyys tulee kuitenkin pysyä kommunikoidaan ja siitä pitää olla valmis myös maksamaan, jotta toiminto on sen ansaitsemalla tasolla turvattu. Pitkissä sopimussuhteissa tämä vaatii jatkuvaa dialogia ja aktiivista sopimuksen päivitystä esim. vastuumuutosten hallitsemiseksi.

Harjoitustoiminnan tärkeys ja TIETO22 harjoitus

Hyvät varautumissuunitelmat eivät yksinään riitä ja ne myös helposti vanhentuvat tai unohtuvat – eli niitä tulee aktiivisesti ylläpitää ja kehittää. Paras tapa

kehittää jatkuvuudenhallintaa ja varautumista on ehdottomasti harjoitustoiminta. Huoltovarmuusorganisaatio kannustaakin yrityksiä harjoittelemaan monin tavoin, jotta mahdolliset haasteenpaikat saadaan esiin ja niihin kehitetään keinoja selvittää niistä.

Digipoolin mallien mukaan yrityksiä ja organisaatioita kannustetaan harjoittelemaan useilla eri tavoin – niin teknisesti kuin hallinnollisestikin. Kaiken perustana on organisaation oma harjoittelu – Backupit pitää pystyä palauttamaan ja torjuntakykyä pitää löytyä, mutta pitää myös tietää mitä ja kenelle viestitään, kun jotain tapahtuu. Oman harjoittelun lisäksi omaa kehitystä suositellaan tehtäväksi esim. harjoitteleamalla saman kaltaisen toisen yrityksen kanssa – vertaistukea häiriötilanteisiin ja ratkaisuehdotusten jakoa. Näiden lisäksi pyritään järjestämään kriittisten toimintojen tuottamiseen harjoituksia, missä kohtaavat asiakkaat ja palveluita tuottavat toimijat ja voidaan keskittyä juuri sen toimitusketjun toimintaan.

Näiden lisäksi on tarjolla laajoja tiedonvaihtoharjoituksia, jotka toimivat tavallan loppusotana, missä hiotaan vielä kansallisissa kontekstissa kulmat pois tiedonvaihdosta, jotta sekin toimisi laajoissa kyberhäiriötilanteissa. Digipoolilla onkin kunnia järjestää joka toinen vuosi TIETO harjoituksia, missä päästään tätä tekemään modernissa mediaympäristössä yritysten ja viranomaisten läsnäollessa. TIETO22 harjoituksessa on mukana yli 160 organisaatiota 13 toimialan yrityksistä ministeriöihin ja intensiivivaiheen tiedonvaihtopeliä pelaamaan on tulossa yli 400 henkilöä. TIETO harjoitusten havaintoihin pyritään myös tuomaan tukea yrityksille. Esim. tieto harjoituksissa toistuva havainto ja em. selvityksemme havainto on, että teknistä jäljitettävyyttä tulee kehittää yrityksissä.

Järjestelmät ja verkot – verkkojen toiminta ja varmistukset

Viestimies lehteen kirjoitettaessa ei voi olla sanomatta jotain kotimaisten verkkojen tilasta.

Suomessa teleoperaattoreiden ja viranomaisten välinen yhteistyö on hyvin vahvaa ja juontaa juurensa osin regulaatiosta, joka alaan kohdistuu ja toisaalta siihen, että toimintaa on kehitetty jo hyvin pitkään. Tietoverkot on useissa kansainvälisissä vertailuissa todettu toistuvasti olevan maailman puhtaimpien joukossa. Ja se johtuu mm. siitä, että teleoperaattorit aktiivisesti puhdistavat

verkoistamme haitallista liikennettä ja tunnistavat/poistavat häiriölähteitä. Verkoissamme kuitenkin on jatkuvasti lisääntyvissä määrin häiriöitä, jotka on onnistuttu siivoamaan pois. Tätä aihetta turhan vähän päästään julkisuudessa kehumään – tähän tulee myös jatkossa löytyä resursseja entistä enemmän.

Tietoverkkojen osalta ajankohtaisena on kaikkia koskeva murros uusiin teknologiageneraatioihin, kuten 5G siirtymisessä ja niiden tuomiin uusiin uhkavektoreihin ja toisaalta energian saanti ja hallinta jos saanti on jossain tilanteessa rajattu. Yhteysiemme tulee kuitenkin toimia kaikissa tilanteissa edes jollain tasolla.

Loppusanat

Lopulta digitaalinen huoltovarmuus on ennenkaikkea sitä, että varmistetaan arjessa toimivien yhteyksien, järjestelmien ja muiden ratkaisuiden toiminta niin että ne toimivat myös häiriötilanteissa (häiriöitä tulee sietää, olla resilientti) ja varmistetaan toiminnan nopea palautuminen negatiivisten vaikutusten minimoimiseksi.

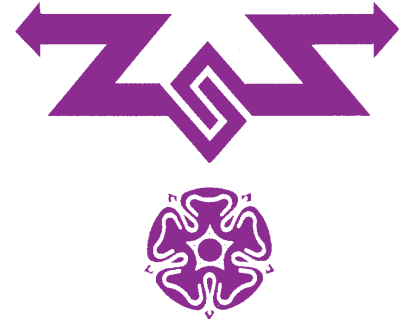
Lue lisää Digipoolin aiheista: www.digipooli.fi, mistä löydät tietoa esim. TIETO22- harjoituksesta sekä Toimialojen kyberturvallisuuden tilannekuva selvityksestä.

Antti Nyqvist

+358408619446

@Digipooli

digipooli@teknologiateollisuus.fi



Laadukkaat mittalaitteet puolustusteollisuuden erityisvaatimuksiin

Anritsu
Advancing beyond



MS2090A Field Master Pro™
kannettava vektoriverkko- ja spektrianalysaattori



MS2026C VNA Master™
kannettava spektrianalysaattori

LUOTETTAVAA TIEDONSIIRTOA JO VUODESTA 1949

Orbis Oy | Vanha Kaarelantie 9, 01610 Vantaa | www.orbis.fi | p. 020 478 8600





Kirjoittaja Evt Harry Kantola toimi Viestikoulun johtajana 1.1.2019-31.5.2022 sekä oli aktiivisesti mukana kehittämässä koulujen välistä yhteistoimintaa.

Teksti: Harry Kantola

Kuvat: Linda Säveros, Mika Toppinen

Viestikoulun kansainvälinen toiminta – missä mennään Suomen ja Ruotsin välillä nyt?

Pitkän hiljaiselon jälkeen on kansainvälinen toiminta taas nousussa. Kansainvälistä yhteistoimintaa aloitettiin tiivistämään jo ennen kuin Suomi anoi pääsyä NATO:n jäseneksi. Toki yhteistoimintaa on harjoitettu pitkään Suomen ja eri maiden sekä kansainvälisten organisaatioiden välillä. Viestiaselajin ja Viestikoulun osalta tosin yhteistoiminta oli hieman vähäisempää jokunen vuosi sopivien yhteistoimintatahojen puuttuessa. Ehkä yhtenä tekijänä on ollut koulutuksessa käytettävä kieli tai kurssien tiivis ohjelma, joka ei ole oikein mahdollistanut kansainvälisten vierailujen toteuttamista, puhumattakaan monikansallisten opetustapahtumien järjestämisestä.

Kansallisessa turvallisuuspoliittisessa selonteossa ja Puolustusvoimien sisäisissä ohjeistuksissa on useampaan otteeseen määritetty, että yhteistyötä tiivistetään Suomen ja Ruotsin välillä. Vastaavia vaatimuksia on myös Ruotsissa kirjattu heidän tavoitteisiinsa ja tätä on myös tuotu esille toimintaa ohjaavissa dokumenteissa. Nämä selkeät ohjenuorat ovat olleet hyvänä tukena ja luoneet oikean ja vasemman rajan yhteistoiminnan kehittämiselle.

Yhteistoiminnan aloitteen tempaaminen

Puuttuvaan yhteistoimintaan ja samalla englannin kielen harjaantumisen mah-

dollistamiseksi pohdittiin Viestikoulun johtoryhmässä vaihtoehtoja ja ratkaisuja. Perinteinen yhteistoimintataho oli tietenkin Ruotsin Viestikoulu, jonka kanssa Suomen Viestikoulu on aiemminkin pitänyt yhteyttä eri otteisiin ja jopa järjestänyt yhteisiä opetustapahtumia kansainvälisen kommunikaation ja viestitoiminnan ympärillä.

Pohdinnan tuloksena Viestikoululla temmattiin aloite vuonna 2019. Koululta otettiin yhteyttä Ruotsiin ja siellä koulun lähimpään vastineeseen, eli Ledningsstridsskolaniin (LedSS). Toiminta aloitettiin näin ollen siis hyvissä ajoin ennen suomen NATO-prosessin aloittamista. Koronaepidemia keskeytti valitettavasti lähes välittömästi yhteistoiminnan kehittämisen ensimmäiseen yhteydenottoon.

Koronarajoitusten aikana pidettiin kuitenkin Viestikoulujen johtajien välillä yhteyttä ja kaavailtiin useampaan otteeseen tapaamisia, yhteistoiminnan viemisestä uudelle tiiviimmälle tasolle. Jo heti alusta alkaen oli selvää, että tavoitteena ei ole pelkästään ystävyystoimintaa ja kohteliaisuusvierailuja, vaan toiminnan pitää tukea koulujen ja puolustusvoimien operatiivisia tavoitteita. Selkeitä hyötyjä pitää siis saada aikaiseksi puolin ja toisin.

Koronan rauhoittumisen jälkeen

Rajoitusten aikana ylläpidettiin ajatusta ja valmiutta kehittää aselajikoulujen välistä yhteistoimintaa maavoimien muun Suomi-Ruotsi yhteistoiminnan yhteydessä. Koulujen välillä vaihdettiin kuulumisia ja tiedusteltiin tilannetta puolin ja toisin. Keväällä 2022 päästiin kuitenkin ottamaan seuraava askel, kun koronatilanne helpotti ja Ruotsin Ledningsstridsskolaniin johtaja kutsui Viestikoulun johtajan suunnittelulilaisuuteen Ruotsiin.

Suomessa oltiin jo tässä vaiheessa ehditty kehittää puolustusvoimien sisäistä toimintaa muun muassa organisaatiomuutoksilla. Vuodenvaihteessa 2021-2022 oli ehditty perustaa Puolustusvoimien johtamisjärjestelmäkeskuksen (PVJJK) alainen Johtamisjärjestelmäkoulu (JOJÄK). Uuden koulun perustamiseen liittyen oltiin määritetty vastuualueet uudelleen Maasotakoulun Viestikoulun ja PVJJK:n Johtamisjärjestelmäkoulun välillä. Viestikoulu keskittyy jatkossa enemmän kenttäviestijärjestelmien koulutukseen, kun taas Johtamisjärjestelmäkoulu johtamisjärjestelmäläns tekniikan ja kyberpuolustuksen kouluttamiseen.

Viestikoulu oli siis jo luovuttanut osan vastuualueestaan uudelle koululle ja toimintoja oltiin jaettu uudella tavoin koulujen välillä, eikä aiempien valmistelujen



Kuva 1. Kuvassa eversti Anders Edholm ja kommodori Juha Ravanti.

perusteella voitu yhteistoimintaa Ruotsin vastineen kanssa jatkaa. Kun vielä kutsun yhteydessä saatiin päivitetty organisaatiokaavio Ruotsin koulusta tehtävien, todettiin Viestikoululla, että Suomessa on syytä miettiä yhteistoimintatahojen ja toiminnan osalta asiaa jälleen kerran uudelleen.

Ledningsstridsskolanin kokoonpano ja tehtävät vastaavat koulutuksen osalta pitkälti niitä tehtäviä mitä Suomessa on jaettu Maasotakoulun Viestikoulun, Puolustusvoimien johtamisjärjestelmäkeskuksen Johtamisjärjestelmäkoulun ja Maavoimien elektronisen sodankäynnin keskuksen tehtäviin. Viimeksi mainitun osalta tosin vain henkilökunnan kursituksen ja opetuksen osalta. Laaditun analyysin perusteella kutsui silloinen Viestikoulun johtaja muut osapuolet neuvonpitoon ja päätettiin yhdessä käydä Ruotsissa valmistelemissa tulevia yhteistoimintatavoitteita ja toimintatapoja.

Yhteisen koulutuksen valmistelu

Suomesta päästiin toukokuussa 2022 Viestikoulun, Johtamisjärjestelmäkoulun ja Elektronisen sodankäynnin keskuksen delegaation kanssa käymään Ruotsissa sopimassa tavoitteita koulutustapahtu-

mien järjestämisestä. Delegaatiota johti Puolustusvoimien johtamisjärjestelmäkeskuksen johtaja.

Tiiviin ja määrätietoisien tapaamisen yhteydessä löydettiin koulujen eroavaisuuksista huolimatta yhteisiä tavoitteita ja toimintamalleja. Näistä alustavista tapahtumista rakennetaan parhaillaan yksityiskohtaisempaa kokonaisuutta, jolla vastataan Suomen ja Ruotsin kansallisiin sekä monikansallisiin tarpeisiin.

Esimerkkejä identifioiduista yhteistoimintamalleista

Koulujen välillä löydettiin useita eri malleja ja toimintatapoja harjoittaa kansainvälistä yhteistoimintaa riippuen koulusta, koulutettavien tasosta ja asiasisällöstä. Näitä havaittuja malleja hiotaan vielä tarkemmin kuntoon vuoden 2022 aikana ja tavoitteena on aloittaa pienin askelin toiminta jo vuonna 2023 kaikkien osapuolten osalta.

Mahdollisuuksista harjoittaa kansainvälistä yhteistoimintaa Viestikoulun osalta on esimerkiksi kadettikoulutuksen (Sotatieteiden kandidaatin) osalta opettajavaihto, jossa Suomen tai Ruotsin koululta kouluttaja käy pitämässä opetusta toisen koululla. Tällä tavoin vastataan

tarpeeseen kehittää nuorten upseereiden kielitaitoa ja ”pakotetaan” heitä käyttämään englantia sekä opiskelussa että käytännössä. Samalla päästään harjaantumaan englanniksi ammattikielen sanastoon aivan uudella tavoin.

Toisena esimerkkinä löydettiin sotatieteiden maisterien opetuksen osalta taktiikan opettamisessa. Tällä tasolla käsitellään maiden välillä saman tasoisia joukkoja ja taktiikan opetuksessakin löytyikin nopeasti yhteinen sävel. Tällä hetkellä on suunniteltu, että opiskelijat käyvät vuoroin toisen maan koulussa, jolloin harjoitellaan soveltuvan taktiikan harjoituksen aikana yhteistoimintaa, pohditaan järjestelmien rajapintoja, tiedonkulkua kenttäviestijärjestelmissä ja johtamistoimintaa. Jopa vaihtoehtoisia skenaarioita löytyi valmiiksi, joihin taktiikan opetus soveltuu hienosti.

Johtamisjärjestelmäkoulun tarkastelussa todettiin, että Viestikoulun aloittama kyberpuolustuksen koulutus, joka uuden koulun perustamisen yhteydessä siirrettiin JOJÄK:lle, oli myös yksi sopiva yhteinen tekijä. Kyberpuolustuksen osalta on maiden välillä ollut jo aiemmin tiivistä yhteistoimintaa. Näistä voi esimerkkinä mainita Suomen ja Ruotsin osallistuminen NATO Cooperative Cyber Defence Center of Excellence (NATO CCD CoE) järjestämään joka vuotiseen kyberpuolustuskilpailuun. Näihin kilpailuihin on Suomi ja Ruotsi osallistunut yhdessä jo vuodesta 2017 alkaen lähes joka vuosi. Kyberpuolustuskoulutuksen tiivistäminen ja yhteisten toimintatapamallien opettaminen parantavat selkeästi toimintaa alalla, jossa muutenkin rajat ovat osin epäselkeitä ja eivätkä aktiviteetit noudata valtakunnan rajoja.

Way ahead – eli miten tästä eteenpäin

Yhteistoiminnan käyntiin saamiseen on panostettu sekä maavoimissa Maasotakoulun Viestikoulun että johtamisjärjestelmälalla Johtamisjärjestelmäkoulun osalta tänä vuonna huomattavasti. Syksyn ja loppuvuoden tarkentavat suunnitelmat luovat varman pohjan tulevien vuosien yhteisen koulutuksen kehittämiseen. Tarkoitus ei ole, että koulutus yhteinäistetään täysin, vaan poimitaan sopivia kokonaisuuksia, josta molemmat maat



Kuva 2.
Plakaatti

hyötyvät ja joka parantaa sekä yhteisten että kansallisten tavoitteiden saavuttamista.

Tätä koulutuksen kehittämistä on tehtävä pienin askelin ja tarkasteltava koko ajan siten, että maiden puolustusvoimien kokonaistavoitteet saavutetaan. Panostuksesta on myös oltava oikeasti hyötyä molemmille maille, kaikille opiskelijoille ja jopa opettajille.

Tarkastelua on tehtävä koko ajan, varsinkin nyt muuttuvassa toimintaympäristössä sekä aloitetun NATO-hakeutumisprosessin yhteydessä. Nyt luodut askeleet ovat vielä linjassa näiden vaatimusten mukaisesti, mutta mahdolliset uudet tarpeet ja vaatimukset pitää herkästi huomioida toiminnan kansainvälistyessä. Valittu polku tulee vaatimaan yhä enemmän koulutusta kansainväliseen toimintaan liittyen. Tästä on hyvä lähteä liikkeelle.

FITELNET.FI | MYynti@FITELNET.FI

SISÄRADIOVERKOT

VIRVE- ja monioperaattoriverkkojen toteutus luottamuksellisesti avaimet käteen -periaatteella.

EMP/HPM-SUOJAUS

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

FITELNET OY, JOUKONTIE 42 A, VANTAA

Fitelnet





TURVALLISEN DIGITALISAATION EDELLÄKÄVIJÄ

PUOLUSTUSVOIMIEN STRATEGINEN KUMPPANI

Kyber- ja tietoturvaratkaisut | Tiedustelu-, valvonta- ja johtamisjärjestelmät
Harjoittelu-, koulutus- ja simulointiratkaisut | Datakeskeiset ratkaisut ja edistynyt analytiikka
Kokonaisarkkitehtuurin ja hankejohtamisen palvelut | Rikostorjunnan ratkaisut
Avioniikan elinkaaren tukipalvelut ja tuotteet | Autonomiset järjestelmät

insta.fi



Teksti: Jose Malmberg, Product Owner, Integration and interoperability, Combitech Oy

Kuvat: Saab AB, Combitech Oy

Järjestelmäintegroitumisen tulevaisuudesta

Tietojärjestelmien integraatio on kaikille tärkeää. Suomen kaltaiselle pienelle toimijalle se on elinehto. Epäonnistunut tai muutoin puutteellinen integraatio moninkertaistaa ylläpidon ja toiminnan kitkaa, mutta onnistuessaan integraatio on todellinen suorituskyvyn moninkertaistaja järjestelmien koko elinkaarten ajan, saarekkeisuus kun vaikuttaa suoraan järjestelmän kokonaissuorituskykyyn.

Tässä artikkelissa tarkastellaan sitä, kuinka järjestelmäintegraatioita tulisi suunnitella ja toteuttaa eräitä tulevaisuuden kehityssuuntia ennakoiden. Mainittavat kehityssuunnat ja ratkaisut koskevat samalla tavalla sekä asejärjestelmätasanteegroimista että eri tasojen johtamisjärjestelmien yhteensopivuutta olemassa olevaan infrastruktuuriin ja muiden johtamisjärjestelmien kanssa. Aihetta tarkastellaan ohjelmistoalan näkökulmasta, joten fokus on pääasiassa teknisessä järjestelmien liittämisenä toisiinsa rajapintoja hyödyntäen. Tämän artikkelin ulkopuolelle jäävät mm. infrastruktuuriin ja prosesseihin liittyvät integraation osat.

Järjestelmäintegraatioiden kehityskaari ja nykytila

Ensimmäiset tietotekniset integraatiot järjestelmien välillä olivat yksittäisten järjestelmien liittämistä toisiinsa yksi-yhteen -periaatteella, käyttäen jotakin yhdessä sovittua sovellusspesifiä metodia. Yleisesti sovittuja tapoja, standardeja tai protokollia ei käytännössä ollut. Lisäksi käsitteelliset erot eri järjestelmien välillä olivat suuria ja siksi siirrettävät tiedotkin monin paikoin vajavaista tai jopa puutteellista. Näiden syiden vuoksi uuden

järjestelmän liittäminen toiseen täytyi aina aloittaa puhtaalta pöydältä.

Koska eri tehtäviä suorittavien järjestelmien yhteen liittämisen edut olivat kuitenkin ilmeiset, suhteellisen pian syntyivät ensimmäiset edelleenkin käytössä olevat rajapintastandardit, mm. 70-luvulla alkunsa saaneet datalinkki ja JREAP määrittelyt. Standardien synty ei tietenkään ongelmaa suoraan ratkaissut: monet jo puolen vuosisadan ikäiset standardit eivät vielä ole kaikilta osin laajalti tuettuja. Ylipäänsä minkäänlainen laajamittainen tiedonsiirron standardien käyttöönotto kesti 90-luvun lopulle, internetin yleistymiseen ja XML-standardin syntymiseen saakka. Siitä eteenpäin eri tasoisten standardien käyttöönotto ja käyttö onkin laajentunut merkittävästi.

Integraation näkökulmasta nykypäivän järjestelmien suurin ero muutaman vuosikymmenen takaisin järjestelmiin on se, että järjestelmät ylipäänsä ovat laajasti integroituja muiden järjestelmien kanssa. Kaikki järjestelmät ovat jo lähtökohtaisesti luotu osaksi järjestelmäkonaisuutta, jolloin yhden olemassaolo sekä edellyttää että mahdollistaa muiden järjestelmien toimintaa.

Vaikka kaikenlaisia standardeja onkin siis käytössä yhä enemmän, alkuperäisen kaltaiset täysin räätälöityinä tuotetut integraatiot eivät ole täysin kadonneet. Entiset jo olemassa olevat integroitumistavat eivät ole kokonaisuudessaan korvautuneet uusilla, vaan monimuotoisuus standardeista räätälöityihin ratkaisuihin on vain lisääntynyt.



Tulevaisuuden kehityssuunnat

Tulevaa ennakoiden kehityssuunta tullee jatkumaan samanlaisena, mutta kiihtyvässä tahdissa. Standardeja tullaan ottamaan käyttöön entistä laajemmin sekä uusien liitoksien tuottamisessa että aiempien epästandardien ratkaisujen korvaamisessa. Olennaisena osana tähän liittyy niin sanottu toimintaympäristön integraatio. Hyvänä esimerkkinä ovat FMN-viitekehys ja NATO, joiden osalta teknisten rajapintojen ja standardien käyttöönotto tai edes niihin käsiksi pääseminen edellyttää jopa poliittisen tason päätöksiä ja ”integraatiota” organisaatioiden välillä. Viimeaikaisten ja käynnissä olevien kansainvälisen politiikan prosessien myötä lienee kaikille selvää, että puolustustoimialan yhteydessä kansainvälisten (NATO) standardien lisääntyminen on integraatioiden tulevaisuus myös kansallisesti.

Toisaalta samaan aikaan myös standardeista poikkeavien integraatioiden lisääntyminen on vääjäämätöntä, muidenkin kuin ns. legacy-järjestelmien osalta. Tämä johtuu kahdesta standardien ominaisuudesta: standardi on ”aina vanhentunut” ja ”liian geneerinen”. Laajalti käytetyn standardin on oman yleiskäytettävyytensä nimissä oltava jonkin verran terävintä kärkeä jäljessä, jotta riittävän suuri osa käyttäjistä kykene sen käyttöön ottamaan. Lisäksi standardien käyttöönotossa itsessään kestää yleensä niin pitkään, että kehitys on senkin vuoksi karannut vähintään aavistuksen verran edemmäs. Samoin standardin on sisällössään oltava ”riittävän summittainen” mahdollisimman suuren yleisön palvelemiseksi riittävällä tasolla. Kaikkia mahdollisia nyansseja erilaisten käsitteiden ja järjestelmien välillä on yksinkertaisesti mahdotonta kuvata yhdessä muodossa täydellisesti.

Ongelmallisiksi nämä ominaisuudet muodostuvat siksi, että innovaatio tuottaa kaiken aikaa uusia toiminnallisuuksia ja suorituskykyjä, jotka eivät kokonaisuudessaan sovellu jo olemassa oleviin standardeihin. Koska erityisesti matalan tason suorituskykykriittisissä järjestelmissä uudet suorituskyvyt halutaan ottaa käyttöön siellä missä se vain on mahdollista, kaikille muille yleispätevään standardiin on pakko tehdä kansallisia/vast. laajennoksia: kukaan ei ole valmis priorisoimaan yhteensopivuutta teknisen etulyöntiasemansa kustannuksella. Tämä johtaa siihen, ettei vain ja ainoastaan standardeihin perustuva viestinvaihto ja integraatio ole kaikkialla realismia.



Koska täysin standardien mukainen yhteensopivuus taas täytyy olla olemassa ylemmän tason tiedonvaihdon ja KV-kontekstin vuoksi, monimuotoisuus erilaisten ei-standardien rajapintojen ja integraatioiden välillä tulee jopa lisääntymään.

”Yllä mainitun pohjalta on pienen ja ketterän hyvä kuitenkin pohtia kuinka rakennetaan kansalliset tahtotilat täyttävä kansainvälisesti yhteensopiva johtamisjärjestelmäkokonaisuus. KV-kontekstissa vastuut eri standardirajapintojen osalta on jaettu domainien/puolustushaarojen välillä, joiden intressit ohjaavat kyseisen standardin kehittymistä. Voitaaisiinko kansallinen, operatiivisten tasojen 1 ja 2, johtamisjärjestelmien yhteensopivuus luoda esimerkiksi Land domain:n vastuulla olevan MIP4- standardin perusteella hyödyntäen MIP:n tietomallia (MIM)? On myös hyvä kysyä, parantuuko vai heikentyykö suorituskyky täysin standardien mukaisella integraatiolla? Olisiko ratkaisuna laajentaa standardien sisältöä kansallisten tarpeiden mukaan?”

Toinen järjestelmien tulevaisuutta määrittävä kehityslinja on ohjelmiston merkityksen korostuminen suhteessa fyysiseen laitteistoon. Arkielämässä tämän kehityssuunta lienee selkeimmin nähtävissä autoissa. Siinä missä 80-luvun autoissa ainoa elektroninen toiminnallisuus oli radio, tämän päivän autoissa tietotekniset järjestelmät vastaavat kaikesta polttoaineen syötöstä jarrujen toimintaan ja navigaatiopalveluihin. Monella muulla sovelusalueella esimerkit ohjelmiston roolin kasvusta eivät toki ole yhtä äärimmäisiä, mutta sama ilmiö toistuu lähes kaikkialla. (kts. esimerkiksi Viestimies 3/2021, Timo Mustonen: ”Joustavaa ELSO-suorituskykyä ohjelmistovastaanottimilla”) Fyysisellä laitteistolla tulee edelleen säilymään ehdottoman tärkeä roolinsa

kaiken mahdollistajana, mutta ohjelmisto nousee suorituskyvyn kannalta yhtä tärkeään rooliin, ellei jopa tärkeämmäksi.

Kuinka kehityssuunnat vaikuttavat

Se mitä seuraa näistä molemmista kehityssuunnista – integroitumistapojen monimuotoistumisesta ja ohjelmiston osuuden kasvulla – on tarve jatkuvalla muutoksella järjestelmäintegraatioidenkin suhteen.

Vaikka tässä ajanhetkessä yhteensopivuuden lisääminen ja uusiin standardeihin siirtyminen näyttääkin kertaluontoiselta, kyse on jo aiemmin liikkeelle lähteneestä prosessista, joka myös tulee jatkumaan hamaan tulevaisuuteen. Esimerkiksi läntisen puolustusyhteisön kontekstissa tämä tarkoittaa FMN:ää spiraaleineen, joiden tavoitteena on alati syvenevä ja kehittyvä integraatio. Kun vielä tämän lisäksi tulee jo mainittu suorituskykyjen teknisestä kehityksestä johtuva kansallinen tarve standardien laajentamiselle, integraatioita täytyy päivittää toistuvasti myös tulevaisuudessa.

Se kuinka ohjelmiston roolin muutos suhteessa laitteistoon vaikuttaa integraatioon, johtuu yleisestä päivittämisen helppoudesta: Kun järjestelmän toiminta perustuu olennaisimmilta osiltaan ohjelmistoon, järjestelmien paranteleminen ja jopa uusien suorituskykyjen tuottaminen on mahdollista yksinomaan ohjelmistopäivityksillä ilman laitteiston uusimista. Siellä missä tämä on mahdollista, tilaisuutta ei todennäköisesti jätetä käyttämättä. Ohjelmiston päivittäminen on joka tapauksessa merkittävästi helpompaa ja edullisempaa kuin kokonaisten lait-



teistojen päivittäminen, jolloin kynnys päivitykseen on huomattavasti matalampi ja sen suorittaminen vastustamattoman houkuttelevaa.

Eri järjestelmien ohjelmistojen päivittämisen syklin ja toimintaympäristön tarpeiden muuttumisen nopeutuessa seuraa, että eräässä mielessä kaikki ohjelmistot ja integraatiot ovat aina rikki – vanhentuneita, vanhenemassa tai muuten muutosten tarpeessa. Tästä syystä järjestelmien integraatiota keskenään tulisi ajatella jatkuvana prosessina, ei kertaluontoisena tai vain elinkaaripäivitysten myötä 10 vuoden välein tapahtuvana projektina.

Kuinka varautua tähän?

Mikäli integraatio on rakennettu suoraan järjestelmiin, niin että jokainen yksittäinen järjestelmä on räätälöity itsessään ymmärtämään jokaista siihen liittyvää järjestelmää, integraatio jatkuvana prosessina on erittäin työlästä. Muutoksenhallinta ei kohdistu vain yksittäiseen järjestelmään ja järjestelmätoimittajaan, vaan myös kaikkiin liittyviin järjestelmiin ja toimittajiin. Tällöin suuri haaste on muutosten aikatauluttaminen, koordinoiminen ja resursointi. Pahimmillaan yksi tai useampi integraatio on kaiken aikaa epäkunnossa.

Yhtenä ratkaisuna tähän ohjelmistoista johtuvaan jatkuvaan muutostarpeeseen onkin myös integraation ulkoistaminen itse järjestelmistä ja toteuttaminen omana ohjelmistonaan. Tämä lähestymistapa mahdollistaa sen, että missä tahansa järjestelmäkokonaisuuden osassa tapahtuvat

muutokset tarvitsee implementoida, itse päivittyvän järjestelmän lisäksi, vain tässä erillisessä integraatio-ohjelmistossa. Työn kohteiden määrän supistumisesta seuraavat hyödyt ovat luonnollisesti moninaiset. Tämän lisäksi integraation erillisuus mahdollistaa sellaisten uusien integraatioiden liittyvien ominaisuuksien mukaan tuomisen, joita itse järjestelmässä ei välttämättä lainkaan ole.

Hyvänä esimerkkinä tästä ovat tiedon jakamiseen ja suodattamiseen liittyvät toiminnot. Riippumatta tietoja lähettävän järjestelmän tarjoamista toiminnallisuuksista, tietoja voidaan vielä järjestelmän ulkopuolellakin reitittää ja suodattaa muille järjestelmille tiedon itsensä sisältämien parametrien perusteella. Tällaisia parametreja voivat olla esimerkiksi arvoväleihin, luokitteluun tai maantieteelliseen sijaintiin liittyvät arvot.

Syyt, miksi tällaista haluttaisiin tehdä ja jälkeensäkin lisätä, liittyvät ennen kaikkea tiedon määrän rajoittamiseen ja operaatioturvallisuuteen. Mikäli tiedon määrää voidaan perustellusti rajata, tämä palvelee sekä verkkoyhteyksiä että tiedon käsittelyn tarvetta, niin ohjelmallisen suorituskyvyn kuin käyttäjän kognitiivisestakin näkökulmasta. Operaatioturvallisuuden näkökulmasta on aina edullista, mikäli tiedon jakamista voidaan tehdä need-to-know-perusteella ja jopa datan itsensä määrittämänä (data centric security). Ohjelmallisen integraation avulla tällaisia toiminnallisuuksia voidaan hallinnoida ja muokata dynaamisesti tarpeen mukaan.

Soveltamalla tätä integrointiratkaisua ja ottamalla se huomioon jo materiaallisen suorituskyvyn rakentamisen suunnittelu-

ja kehittämisvaiheessa, voidaan varautua ja ehkäistä nekin tulevaisuudessa vaativat epämieluisat yllätystilanteet, joita vielä ei ole edes mahdollista kokonaan ennakoita. Parhaimmillaan integraation siirtäminen erilliselle ohjelmistolle konkretisoituu yllätystilanteiden sijaan huoltovarmuutena ja kustannustehokkuutena.

Integraation jatkuvan kehittämisen prosessin toteuttamiseen ei luonnollisesti riitä pelkkä tuote. Jotta tarvittava kehitys olisi riittävän kiinni ajassaan, integraation ylläpidon täytyy olla palvelu ja yhteistyötä, jossa molempipuolinen ymmärrys takaa tuotteenkin palvelevan todellista tarvetta. Jokainen ohjelmisto on ihmisen tekemä ja sellaisenaan representaatio tekijänsä aiheen ymmärryksestä ja asiantuntemuksesta. Mikäli tekijä ei täsmälleen tiedä mitä ongelmaa teke- misellään on ratkaisemassa, seuraukset ilmenevät itse ohjelmistossa. Käytännön toteutuksen kannalta asiantuntemus ja kokonaisvaltainen yhteistyö ovatkin olennaisempaa kuin tiettyä nimeä kantava tuote.

Kuinka yhteistyön tulisi tapahtua?

Kuten hyvissä tietojärjestelmissäkin, myös järjestelmien tuottamisen ja ylläpidon yhteistyössä olennaista on, että kunkin osapuolen tehtävät, roolit ja vastuut ovat selkeästi määritetty. Karkeasti yleistettynä ohjelmistoihin liittyvässä palvelussa tilaajan tehtävänä on keksiä tarpeita ja toimittajan tehtävänä keksiä niihin ratkaisu. Mikäli näin ei ole, tilaaja voi kyllä saada sen mitä halusi, muttei välttämättä sitä mitä olisi tarvinnut.

Ohjelmiston käyttäjänä tilaajalla on vääjäämättä paras ymmärrys siitä minkä takia ja mihin tuotettavaa kokonaisuutta ollaan käyttämässä. Usein taustalla onkin jo kokemusta vastaavasta toimintaympäristöstä ja järjestelmistä. Kokemus menneisyyden ratkaisuksista voi kuitenkin olla taakaksi silloin, kun ratkaistava ongelma on joko merkittävästi muuttunut aiemmasta tai silloin kun samaan ongelmaan olisi olemassa parempia ratkaisumalleja.

Ohjelmiston toimittajalla taas ei lähtökohtaisesti ole samankaltaista ymmärrystä ongelmakentästä, mutta muiden sovelluskohteiden ja ohjelmistokehityskokemuksen kautta laajempi käsitys mahdollisista ratkaisumalleista erilaisiin tarpeisiin. Toimittajien haaste taas on aidosti ymmärtää mikä on projektin perimmäinen tarve ja tavoite, ja vasta sitten



tarjota soveltuvia ratkaisuja. Aina on kiusaus oman vielä hataran käsityksensä perusteella tehdä asioista joko liian yksinkertaisia tai liian kompleksisia.

Ratkaisuna tähän dynamiikkaan erityisesti tilaajan näkökulmasta on se, että pyrittäisiin määrittämään ensisijaisesti tarve ja ongelma: käyttötapaus siitä mil-

laista toiminnallisuutta kokonaisuudessaan ollaan tavoittelemassa. Itse tarpeeseen tai käyttötapaukseen keskittyminen valmiiksi mietittyjen ratkaisujen sijaan korostuu erityisesti silloin kun projektiin liittyy useampia osapuolia. Tällöin vain tietystä näkökulmasta sinänsä oikea ja hyvä ratkaisu saattaakin olla paras vain ja ainoastaan kyseisestä näkökulmasta ja

aiheuttaa muille osapuolille merkittäviä haasteita toisaalla. Mikäli pelkkä ratkaisu-ongelma tai tavoittele sellaisenaan esitettäisiin kaikille osapuolille, mahdollisia ratkaisuja voitaisiin löytää myös sellaisista suunnista, joista niitä ei muuten kenties etsittäisi. Yhdessä suunniteltaessa myös käyttäjän edustajalla on tärkeä rooli omien mahdollisten ratkaisuehdotuksiensa esittäjänä, mutta silloinkin niiden asema on rakentavampi, kuin jos niiden toteuttamista oltaisiin suoraan vaatimassa esimerkiksi sitovan listan muodossa.

Edellä kuvattu tilaaja-toimittaja -dynamiikka koskee integraatioiden lisäksi kaikkia muitakin erityisesti ohjelmistoon liittyviä projekteja. Suurin haaste tällaisessa yleensä on se, ettei kiireen, resurssien ja yleisen projektimallin suhteen tällaista voida jokaisen hankinnan ja mahdollisen toimittajan kanssa järjestää. Riittävän integraalissa yhteistyö- ja kumppanuussuhteessa tällaiseen olisi kuitenkin hyvä pyrkiä, ja mahdollisuuksien mukaan hyödyntää ohjelmistoasiantuntijoiden osaamista kaikissa projekteissa mahdollisimman aikaisin ratkaisujen määrittämiseen. Näin tilaajakin voi keskittyä ennen kaikkea todellisen tarpeen ja käytön suunnitteluun ja kuvaamiseen.

VARMISTAMME LIIKETOIMINTASI JATKUVUUDEN DIGITAALISESSA MURROKSESSA

**Huolehdimme koko
digitaalisesta ekosysteemistäsi,
ja yksinkertaistamme prosessisi
kustannustehokkaasti, skaalautuvasti
ja tietoturvallisesti.**

www.teliacygate.fi



Teksti: Orbis Oy

Kuvat: Orbis Oy ja Sähköinfo oy:n ST-kortisto

Valokuitukytkentöjen rajapintojen puhtaus varmistaa kriittiset verkkoyhteydet

Suomalainen perheomisteinen Orbis Oy on jo vuodesta 1949 alkaen toiminut teknologian kehitystrendien kärjessä. Tänä päivänä yritys kehittää digitaaliselle yhteiskunnalle uuden sukupolven mobiiliverkkojen sekä älykautupunkien ratkaisuja. Orbis Oy tarjoaa tiedonsiirtoverkkoihin RF- ja valokuituteknologioiden tuotteita ja osaamista, jota tarvitaan varmistamaan datan luotettava liikkuminen kiinteistöissä, datakeskuksissa, laitteissa ja teollisuudessa sekä kaupunkien ja tietoliikenneoperaattoreiden infraassa. Lue lisää: www.orbis.fi.

Puolustusvoimien johtamisjärjestelmäkeskus (PVJJK) mahdollistaa Puolustusvoimien johtamisen ja sen tehokkaan toiminnan. Johtamisjärjestelmälän ammattilaiset turvaavat järjestelmien toimivuuden ja suorituskyvyn, ja sen kannalta valokuituverkko sekä sen rakentaminen ja ylläpito ovat isossa roolissa.

Valokuituverkon toiminnassa on tärkeää verkossa olevien liittimien ja liitettävien pintojen puhtaus. Suuri osa järjestelmissä ilmeneistä vioista ja ongelmista aiheutuukin juuri kytkennöistä ja kytkentöjen yhteydessä liitinpintoihin jääneistä epäpuhtauksista. Pahimmillaan tietoliikenneyhteydet voivat katketa kokonaan. Liittimien tarkistaminen ja niiden puhdistaminen onkin ensiarvoisen tärkeää joka kerta, kun kytkentöjä tehdään.

Vaativissa kenttäolosuhteissa puhdistamisen tärkeys korostuu, sillä olosuhteet voivat olla helteisistä 30 asteen paah-teesta aina -40 asteen pakkasiin saakka. Harjoitustoiminnassa harjoittelevien joukkojen johtamisjärjestelmät ovat taisteluharjoituksissa suuressa roolissa ja kuitupuhdistamisen tärkeys korostuu.

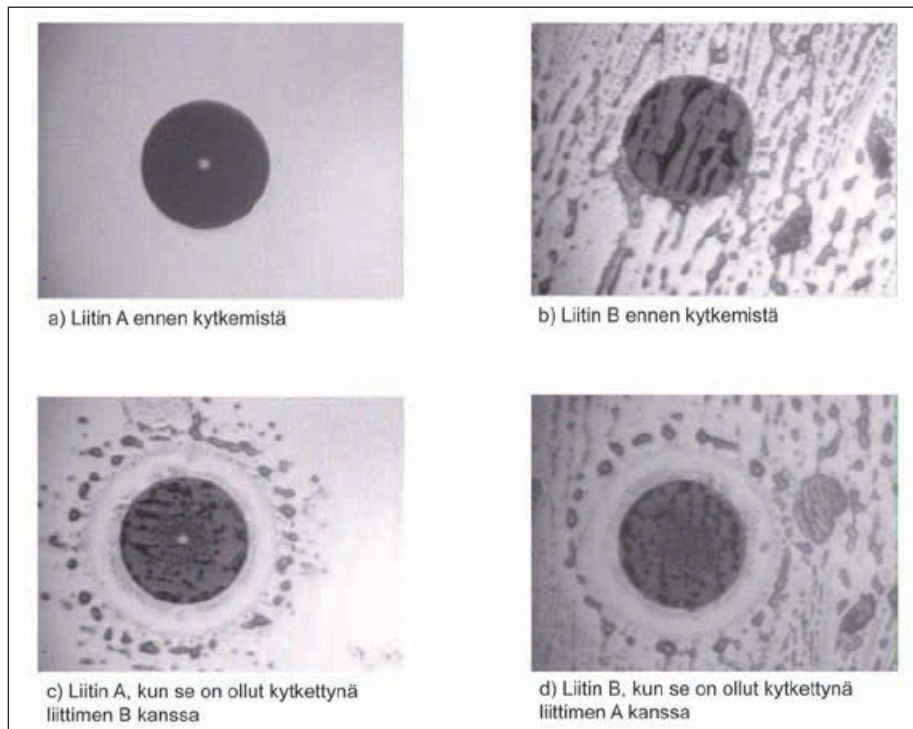
Käytännönläheistä koulutusta

Orbis Oy:ssä puolustusteollisuuden ja kiinteistöjen tiedonsiirron asiakkuuksista vastaavalla asiakkuuspäällikkö Harri Mutasella on lähes 40 vuoden kokemus tiedonsiirrosta, etenkin valokuituteknologian ratkaisuista. Mutanen osallistuu aktiivisesti mm. SANT ry:n ja Traficom:n sisäverkkotyöryhmän M65:n työskentelyyn. ”Olen seurannut Suomessa vuodesta 2011 lähtien valokuituverkkojen rakentamista ja näiden yhteydessä valokuitujen käsittelyä moninaisissa

ympäristöolosuhteissa, ja todennut, että valokuidun puhdistamisella on erittäin suuri merkitys valokuituverkon toimivuudelle”, Mutanen kertoo. ”Puhdistaminen on ymmärrettävä teoriassa, mutta se on osattava toteuttaa myös käytännössä”, hän summaa.

Osaamista täytyy siis myös harjoitella erilaisten kuitujen, liittimien sekä puhdistamisen osalta. Kuituja, liittintyyppä ja adaptoreita on tuotantokäytössä useanlaisia, kuten myös kuitumikroskooppeja ja kuitupuhdistusvälineitä. Viime vuoden lopulla ja kuluvan vuoden aikana Orbis Oy on järjestänyt kuitupuhdistuskoulutusta Puolustusvoimissa, ja palaute siitä on ollut hyvää. Koulutettava henkilökunta on päässyt tutustumaan erilaisiin liittintyyppäihin, mikroskooppeihin ja kuitupuhdistusvälineisiin. ”Tämän tyyppinen käytäntöön perustuva koulutus takaa sen, että valokuituverkon ympärillä tapahtuva asennustyö on tehty oikein ja Puolustusvoimilla on toimiva valokuituverkko johtamisjärjestelmiä varten”, toteaa PVJJK:n ICT-erityisasiantuntija Maire Kössö.

Mutanen kertoo kokevansa innostavaksi keskustella valokuidun puhdistamisesta niin koulutuksissa, asiakastapaamisissa kuin messuilla: ”Näistä kaikista mahdollisuuksista aina oppii ja samalla myös haluan jakaa tätä tärkeää viestiäni niin vanhoille konkareille kuin uusillekin ICT-asentajille. Kehityssuunta on ollut hyvä ja rohkaiseva, mutta työtä riittää edelleen.” Mutanen kolmen P:n sääntö kuuluukin: PUHDISTA, PUHDISTA ja PUHDISTA.



Kuva 1. Videomikroskoopilla otettuja kuvia, joissa näkyy lian siirtyminen liittimestä toiseen.

Liittimien käsittely ja likaisten liittimien vaikutus

Jatkuvasti lisääntyvä valokuitukaapeleiden käyttö on jo pitkälti syrjäyttänyt kupariset telekaapelit niin videovalvonta- kuin tieto- ja kaapeliverkoissakin. Käytännössä tämä merkitsee kuitukytkentöjen tekemistä laitteisiin sekä päätepaneeliin ja liitinrasioihin. Kun liittimiä kytketään päätepaneeliin, -koteloihin tai ulkona maastossa suoraan adapterin kautta kriittiseen kenttäkaapeliverkkoon, jää liitinpintojen puhdistaminen usein liian vähälle huomiolle. Tai se jää kokonaan tekemättä. Tämä johtaa lähes aina tilanteeseen, että verkkoyhteydessä havaitaan vikoja, yhteydet ptkivät tai toimivat satunnaisesti, ja syyksi paljastuvat likaiset liitinpäät tai adapterit. Valokuidun kenttälinsiliittimet ovat oma lukunsa, mutta niissäkin puhtauden merkitys on yhtä lailla tärkeää. Paitsi pölyä ja muuta likaa, liitinpäässä voi olla myös naarmuja, säröjä, lohkeamia tai muita vikoja. Jos puhdistaminen ei auta ja liitin on viallinen, tulee se aina vaihtaa.

Nyrkkisääntönä kytkemättömien liittimien osalta on, että niiden tulee aina olla suojattuina mukana tulevilla omilla suojatulpillaan ja jokainen liitin tulee aina puhdistaa ennen kytkentää. Suojamattomina liittimet likaantuvat ja osuessaan johonkin helposti naarmuuntuvat. Näkyvän valon tai laser-valon kytkeytminen liitännästä kuituun tai päinvastoin

ei onnistu lainkaan, jos liitännät ovat likaisia tai pölyisiä. Puhdistuksen lisäksi liittimien kunnon voi ennen kytkentää varmistaa kenttäkäyttöisellä videomikroskoopilla. Huomioitavaa on myös se, että likainen liitin likaa myös vastakkaisen liitinpään ja adapterin.

Suurempiin siirtonopeuksiin siirryttäessä

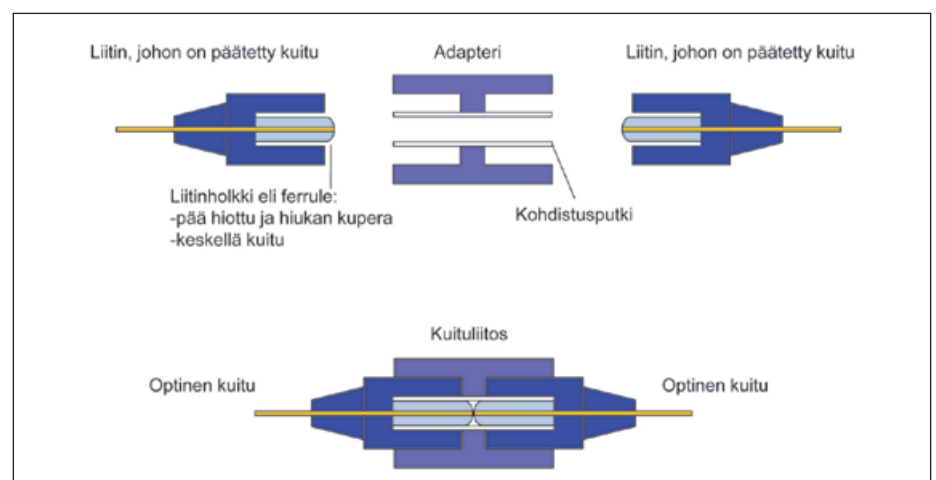
Likaiset tai huonokuntoiset liittimet voivat aiheuttaa ikäviä yllätyksiä myös silloin, kun järjestelmiä päivitetään nopeampiin, esimerkiksi siirryttäessä

100 Mbit/s Ethernet-verkoista 1 Gbit/s Ethernet-verkkoihin. Tämä johtuu siitä, että siirtonopeuksien kasvaessa laitteiden LED-lähtetimet vaihtuvat laser- tai VCEL-lähtetimiin, joiden lähettämä valoteho keskittyy kuidun ytimen koko poikkipinnan sijasta ytimen keskiakselin läheisyyteen. Tällöin pienikin lian määrä sopivassa kohtaa liittimen päässä voi aiheuttaa järjestelmän toimimattomuuden. Toimintahäiriöt voivat ilmentyä järjestelmiin joko välittömästi tai joskus vasta aikojen päästä.

Järjestelmien siirtonopeuksien kasvaessa kasvavat myös niiden lähetintehot. Lähetintehot voivat olla joissain siirtojärjestelmissä jopa useita milliwatteja, tällöin liittimen päähän kuidun ytimen kohdalle kohdistuva energiatiheys saattaa olla hyvinkin suuri. Valotehojen kasvu tuo siis mukanaan lisävaatimuksia myös liittimien puhtaudelle. Likaiset liittimien päät voivat aiheuttaa vaurioita lähettimille valon heijastuessa likaisesta liittimestä takaisin lähettimelle tai itse liitin voi rikkoutua valotehon ”räjäyttäessä” liittimen päässä olevan lian. Tällaisista tapauksista on Suomessakin kokemuksia ja siksi liittimien puhtauteen ja laadun tarkastukseen kiinnitetään yhä enemmän huomiota.

Kuituliittimien rakenne ja kytkentä

Nykyiset liittimet on pyritty tekemään sellaisiksi, että ne olisivat mahdollisimman helppoja ja varmoja kytkeä. Kun ensimmäisen sukupolven kuituliittimet, kuten SMA, olivat mutterikiinnitteisiä ja kiristysvoima vaikutti liitosvaimennukseen, niin nykyiset liittimet ovat ”napsahavia” ns. push-pull- eli pistokeliittimiä.



Kuva 2. Holkki- eli häntäkuituliittimessä optinen kuitu on liimattu kiinni holkkiin eli ferruleen. Liitos syntyy, kun kaksi holkkiin kiinnitettyä kuidun päätä kohdistetaan toisiinsa naarasliittimessä liitinadapterissa olevan kohdistusputken avulla.

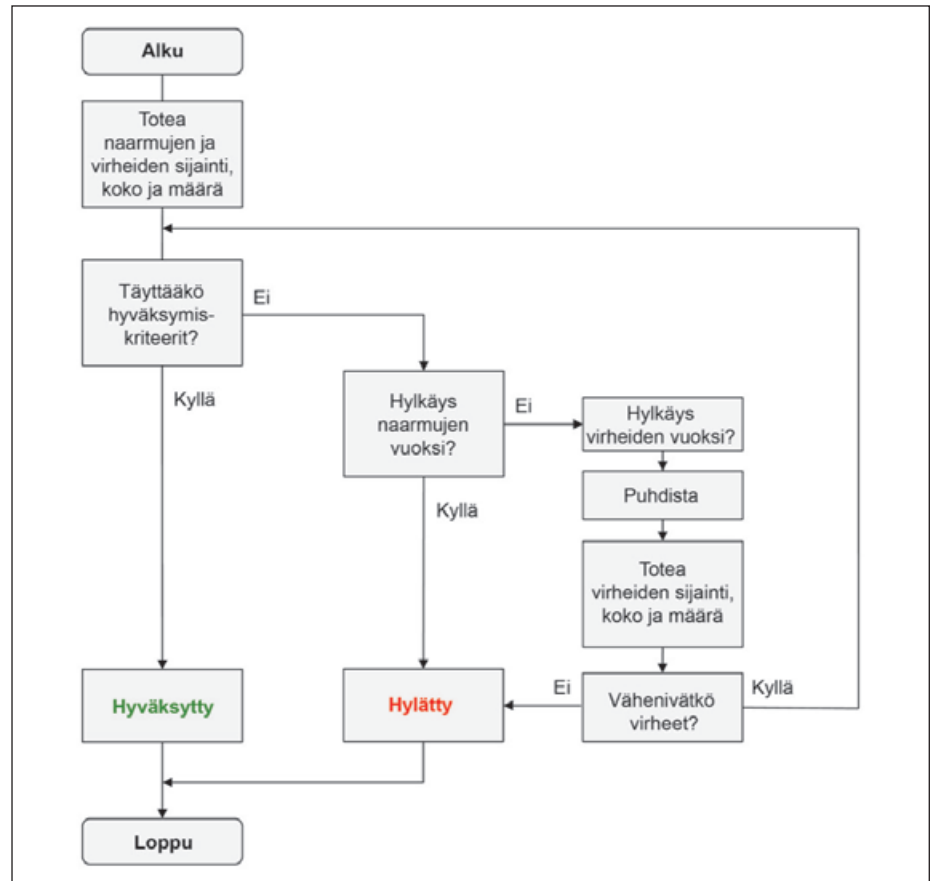
Nykyisin yleisimmin käytetyt kuituliittimet ovat niin sanottuja holkkiliittimiä (kutsutaan myös häntäkuituliittimiksi). Holkkiliittimiä on useita eri tyyppisiä, uusissa asennuksissa käytetään tällä hetkellä yleisimmin LC- ja SC-liittimiä. Holkkiliittimissä optinen kuitu on liimattu holkin eli ferrulen sisälle, minkä jälkeen holkin ja kuidun pää on hiottu kuperaksi tai kulmahioitu (APC). Liitos syntyy, kun kaksi tällaista holkkiin kiinnitettyä kuidun päätä kohdistetaan toisiinsa naarasliittimessä liitinadapterissa olevan kohdistusputken avulla. Adapteri lukitsee liitinnat paikoilleen ja liittimien jousivoimat pitävät liittinpäiden kosketusta yllä. Holkkiliittimen periaate on esitetty kuvassa 2.

Liitinpäiden tarkastusperiaatteet sekä hyväksymis- ja hylkäysperusteet

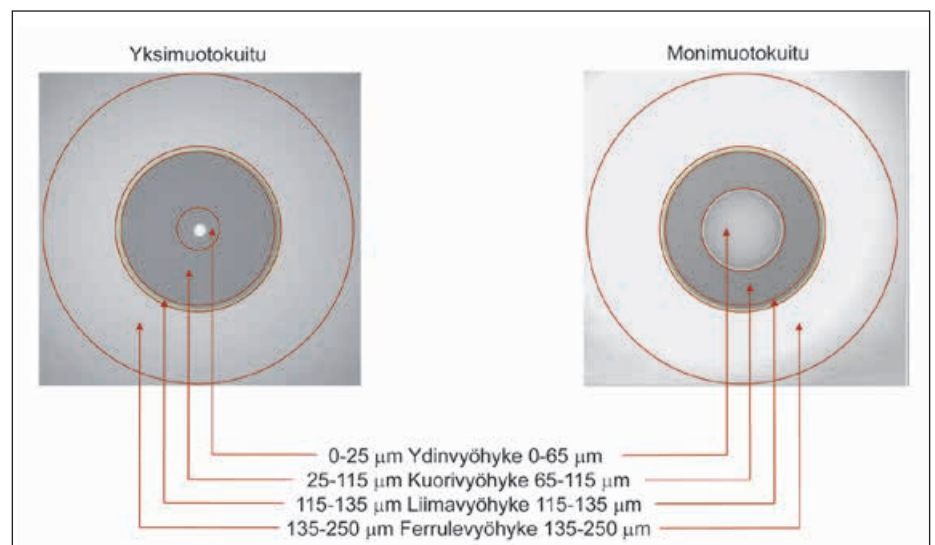
Standardissa SFS-EN 61300-3-35 on määritelty liitinpäiden tarkastusperiaatteet sekä hyväksymis- ja hylkäysperusteet optisella videomikroskoopilla tarkastettaessa. Yleiskaapeloinnin asennusta koskevassa standardissa EN 50174-2 on vaatimus, jonka mukaan optisen kaapeloinnin päätteiden liitinpäät tulee tarkastaa ja tarvittaessa puhdistaa vikojen estämiseksi. Asennuksen yhteydessä tilaajalla on oikeus vaatia tarkastusta ja kirjallista raporttia. Ennen kytkentää tehtävä tarkastusprosessi on esitetty kuvassa 3.

Apuvälineenä tarkastamisessa käytetään mikroskooppia. Laite voi olla optinen mikroskooppi tai videomikroskooppi. Suositus on, että optinen mikroskooppi on varustettu infrapunasuodattimella, jotta silmään ei osu kuidusta tulevaa valoa siinä tapauksessa, että tarkastaja on unohtanut huolehtia lähettimen sammuttamisesta tai irrottamisesta kuidun toisessa päässä. Mikroskoopin suurenuksen tulisi olla vähintään 100-kertainen monimuotokuiduille ja 200-kertainen yksimuotokuiduille.

Suurennoksessa tärkeää on se, että liittimen pää näkyy riittävän suurelta alueelta myös kuidun ulkopuolelta. Näkökentän laajuuden tulisi olla vähintään 250 mikrometriä eli 250 μm ja erottelevyyden sellainen, että halkaisijaltaan 2 μm levyiset hiukkaset tai viat erottuvat. Kuva 4 havainnollistaa liitinpäiden neljä eri vyöhykettä. Kullekin vyöhykkeelle on määritelty vikojen sallitut koot ja lukumäärät standardissa EN 50174-2. Mitä lähemmäs ydintä mennään, sitä kriittisempää on lian poistaminen. Yksi- ja monimuotokuitujen ferruleissa alueet ovat erikokoiset.



Kuva 3. Liitinpäiden tarkastusprosessi ennen kytkemistä.



Kuva 4. Liitinpäässä on neljä vyöhykettä, joista jokaiselle on määritelty vikojen sallitut koot ja lukumäärät standardissa EN 50174-2. Mitä lähemmäs ydintä mennään, sitä kriittisempää on lian poistaminen.

Ytimen koko on yksimuotokuidussa (SM) 9 μm ja monimuotokuidussa (MM) 50 μm (OM3/OM4) tai 62,5 μm (OM1). Vertailun vuoksi, ihmisen hiuksen paksuus on 80 μm , hiekk- ja pölyhiukkasten 20...200 μm . Valokuidusta puhuttaessa voidaan puhua käytännössä ”näkymättömästä” liasta ja epäpuhtauksista liittimen ferrulen ytimien päällä.

”Tämä ”näkymättömyys” luo meille todella suuria haasteita, mikäli emme oikein ymmärrä valokuitujen puhtauden merkitystä ja kuinka näitä oikeilla tavalla ja välineistöllä saadaan puhdistettua”, sanoo Mutanen.

Muista työturvallisuus

Optisiin mittauksiin liittyy tiettyjä turvallisuusriskejä, jotka tulee tunnistaa ja joita tulee välttää. Yksi tällainen riski on laser-valo. Valonlähettimet toimivat aallonpituudella, jolla niiden lähettämä valo on näkymätöntä. Valokuidun tai liittimen päähän ei saa katsoa suoraan edestä, sillä varsinkin laservalo on silmälle vaarallista ja voi vahingoittaa verkkokalvoa.

Toisen turvallisuusrisikin muodostavat kemikaalit. Kuitujen ja liittimien puhdistuksessa käytettävät kemikaalit ovat useimmiten palavia, huumaita ja ärsy-tysoireita aiheuttavia. Tuuletuksesta ja suojakäsineiden käytöstä on siksi syytä huolehtia tarpeen mukaan. Puhdistus-tenneiden mukana tuleva valmistajan käyttö-turvallisuustiedote kannattaa aina lukea.

Myös optisten kaapeleiden rakenneosat saattavat sisältää ärsytysoireita aiheutta-via materiaaleja. Esimerkkeinä tällaisista mainittakoon aramidi- tai lasikuituvah-vikkeet sekä täyterasvat ja niiden puhdis-tusaineet. Vastuullinen valmistaja huo-lehtii, että turvallisuusriskejä sisältävissä tuotteissa on tarvittavat varoitusmerkit.



Kuva 5. Valokuidun puhdistusvälineet ja videomikroskooppi ovat asentajan päivittäi-siä käyttövälineitä kriittisten verkkoyhteyksien toiminnan varmistamisessa.

Lopuksi

Markkinoilla on saatavilla laajasti laa-dukaita valokuidun puhdistusvälineitä ja -laitteita, kuten puhdistuskasetit, -pui-kot, -kynät, -liinat ja -nesteet. Orbis Oy:n järjestämissä koulutuksissa Harri Muta-nen on esitellyt erilaisia puhdistusväli-neitä ja niiden käyttöä, ja myös asentajat ovat itse saaneet kokeilla näitä. ”Monesti olen saanut palautetta siitä, että asentajal-la ei ole ollut tiedossaan, kuinka ja miksi pitää puhdistaa ja että välineitä on näin monenlaisia, myös sellaisia, joita olisi jo aiemmin tarvinnut”, kertoo Mutanen.

Puhdistusvälineiden kustannuksista Mu-tanen toteaa, että tuotteiden hinnat vaih-televat muutamista euroista useampiin kymppeihin. Hinnakkaammat tuotteet riittävät jopa useisiin satoihin käyttöker-toihin per tuote. ”Nämä ovat jokaisen asentajan päivittäisiä käyttömateriaaleja ja niiden merkitystä ei voi liikaa korostaa kriittisten verkkoyhteyksien toiminnan varmistamisessa”, sanoo Mutanen ja jatkaa ”Panostus tietoliikenneverkon aktiivilaitteisiin, reitittimiin ja muihin komponentteihin ei yksistään riitä, mikäli kytkentöjen rajapintojen puhtaudesta ei samalla pidetä huolta.”



Tervetuloa Museo Militariaan!

Laaja tykistö-, pioneeri- ja viestiaselajeja esittelevä perusnäyttely.

Uusi vaihtuva näyttely:

”Viihtykää hyvin, pojat” – Varusmieselämää 1920- ja 1930-luvuilla.

Avoimna talvikaudella 30.4. asti ti-su klo 11–17 (sulj. 16.12.2022–1.1.2023).

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



Viestimiespäivät 2022

Viestimiespäivät 20.-21.8.2022 järjestettiin Turussa Forum Marinumissa, joka on merenkulun valtakunnallinen vastuumuseo ja meripuolustuksen museo sekä toiminnallinen merikeskus.

Kolmisenkymmentä osallistujaa saapui lauantai aamulla paikalle, mukana myös neljä naista.

Viestimiespäivät avasi Viestikiltojen liiton puheenjohtaja Jukka-Pekka Virtanen ja tapahtuman suojelija, puolustusvoimien johtamisjärjestelmakeskuksen (PVJJK) johtaja kommodori Juha Ravanti kertoi PVJJK:n toiminnasta. Näin päivät saatiin käyntiin ja päästiin tutustumaan eri museokohteisiin. Forum Marinumin alueella on useita museolaivoja, kuten tykkivene Karjala, miinalaiva Keihäsalmi, Bore I, fregatti Suomen Joutsen ja parkki Sigyn. Väillä nautittiin lounas ja ilta-päivällä jatkettiin tutustumista laivoihin ja Forum Marinumin näyttelyihin. Bore I:n hytteihin majoittumisen jälkeen syötiin päivällinen. Päivän päätteeksi saunottiin Boren saunatiloissa. Ilta kului vapaan seurustelun merkeissä.

Sunnuntaina 21.8. siirryimme yhteiskuljetuksella Ruissalon saarelle ja tutustuimme Krimin sodan aikaisiin varustuksiin. Lopuksi kävimme ihas-telemassa Honkapirttiä, jonka JR14 sotilaat rakensivat sodan aikana Uhtuan seudulla. Honkapirtissä söimme myös keitolounaan, kala- tai hernekeittoa sekä pannaria hillon kera. Ruokailun jälkeen julkaistiin vielä Erkki Renbergin laatiman viestimieskisan tulokset, maksimi pisteet oli 23.



Joukkokuva Krimin sodan varustuksilla.

Tässä kolmen kärki:

1. Kastemaa Pekka ja Liisa, 19 pistettä
2. jaettu 2. sija, Vainio Esko ja Liisa, 18 pistettä, Pitkänen Esko ja Savander Susanna, 18 pistettä
3. jaettu 3. sija, Salminen Esa ja Järvinen Jarkko, 17,5 pistettä, Tuhkanen Marko, 17,5 pistettä

Viestimiespäivien järjestelyvastuu lankesi tänä vuonna Varsinais-Suomen Viestikillalle. Killan työryhmässä olivat Erkki Renberg, Juhani Pilpola, Topi Mellanen ja Seppo Halminen sekä autokillan Kauko Kaskinen.

Maanpuolustuksen Viestisäätiö ja Viestikiltojen liitto tukivat myös merkittävästi tapahtumaa taaten näin onnistuneet Viestimiespäivät. Myös sään haltija suosi meitä koko viikonlopun, lämmintä poutasäätä.

Suuret kiitokset kaikille tapahtumaan osallistuneille ja tukea sekä neuvoja antaneille.



Varsinais-Suomen Viestikillan edustajat pj. Erkki Renberg ja hallituksen jäsen Seppo Halminen ojentavat yhdistyksen viirin kommodori Juha Ravantille.

Turvallinen tulevaisuus

Tehokas tiedonhallinta, analytiikka, tiedolla johtaminen ja tiedon jalostaminen ovat modernin organisaation tunnuksia. Yhdessä ne voitelevat yhteiskunnan rattaita, helpottavat arkea, synnyttävät uusia palveluita ja lisäävät kansalaisten luottamusta tulevaisuuteen.

Me Fujitsussa olemme sitoutuneet edistämään ict-palveluja ja -ratkaisuja, jotka auttavat organisaatioita ja yrityksiä rakentamaan tulevaisuutta turvallisesti ja kestävästi.

Monipuolisen teknologia- ja palveluosaamisemme avulla autamme asiakkaitamme pysymään kehityksen kärjessä.

Rakennetaan turvallista yhteiskuntaa yhdessä.

www.fujitsu.com/fi

Analysaattori



Kotikonsteja ja luovaa ajattelua

Analysaattorin harhaiset ajatukset jäivät julkaisematta Viestimiehen kesäkuun numerosta. Jokin painotekninen ongelma ilmeisesti. Tai sitten vaan klassinen taustatekniikan aiheuttama tilanne. Tässä se nyt kuitenkin on, mutta hiukan päivitettyinä. Melko staattinen tilanne siis vallitsee, kun kolme kuukautta ei juurikaan muuta tekstiä. Päivitykset on helppo havaita tekstistä, ne on luonnollisesti merkitty sanalla PÄIVITYS.

Venäjän hyökkäys Ukrainaan helmi-kuussa pääsi sitten yllättämään lähes kaikki. Siinä menivät naapurisopu ja YYA-sopimus katolleen kerrasta ja tämän hyökkäyksen ja muutaman puhelun seurauksena Suomi jättikin juuri tätä kirjoitettaessa Ruotsin kanssa liittymishakemuksensa Natoon. Jotka sitten Turkki on jo ehtinyt kieltämään ja sanoo estävänsä liittymiset. Paljon puhutaan, että Turkki on iltalypsyllä ja hakee jotain muita poliittisia myönnytyksiä. Analysaattorilla on tähän(kin) oma näkemyksensä, joka johtaa vuonna 2012 Puolassa NATOn Joint Force Training Centerissä järjestettyyn CWIX harjoitukseen, johon sain myös kunnian osallistua. Sieltä asti saattavat olla siis peräisin todelliset syyt tähän Turkin uhoamiseen. Delegaatiomme testaustila oli iso jaettu luokka, jossa oli keskellä kevyt väliseinäsermi. Puolan Bydgoszczissa (yrityksessä itse lausua tuo) oli kesäkuussa jo melko lämmin ja sen tilan ilmastoinnin säätimet olivat onnekkaisesti meidän puolellamme sitä väliseinää. Joten helpotimme hellettä viilentämällä tilaa ihan kunnolla. Sen väliseinän takana piti majaan juurikin Turkin delegaatio, jolle se ilmastointi oli hieman liikaa. Turkkilaiset kävivät siinä huovat harteillaan niiskuttamassa, että heillä on liian kylmä. Ajattelen tässä tietenkin nyt vaan sitä, että jos tuosta vaikka jäi jotain hampaankoloon, joka

purkautuu nyt sitten poliittisena kiukuteluksi. PÄIVITYS: Sama jarrutus jatkuu, mutta 23/30 on jo ratifioinnin status, viimeisimpänä USA.

Venäjän sotilaallinen suoritus yleisesti ottaen Ukrainassa on ollut vähintäänkin heikkoa. Kuka tahansa suomalainen jalkaväkisotilas olisi osannut kertoa heille, miten ei kannata toimia. Esim. että alkua ajelko 60 km pitkässä letkassa ilman turvavälejä. Voisi jopa näsäviisaasti sanoa, että tähän ei ollut edes ensimmäinen kerta. Eikä toinen. Raatteen tien kokemukset ovat ainakin selkeästi venäläisiltä unohtuneet. Tai sitten ne eivät ole koskaan oikein kiinnostaneetkaan, kun siellähän itse asiassa tuhottiin mm. juuri Ukrainasta kotoisin ollut Neuvostoliiton 44. divisioona. Toisen kerran samaan vipuun venäläiset menivät Tsetsenian sodassa Groznyin valloituksessa. Venäläiset panssarit päästettiin tunkeutumaan sisään kaupunkiin melkein ilman vastarintaa, jossa ne sitten käytännössä tuhottiin.

Länsimainen aseapu Ukrainalle on merkittävässä, jopa ratkaisevassa roolissa, mutta on pakko myös arvostaa ukrainalaisten maanpuolustustahtoa ja kykyä soveltaa ja toteuttaa erilaisia kotikonsteja taistelussaan. Siviilit rakentavat panssariesteitä ja Molotovin cocktailleja ja aseet jaetaan käytännössä kaikille halukkaille. He myös poistavat katukylttejä hyökkääjien reiteiltä tai kääntävät ne väärin suuntiin eksyttääkseen vihollista. Paikallinen sosiaalinen media toimii myös Ukrainan armeijan tukena kuvaamalla venäläisiä joukkoja ja jakamalla tietoa heidän liikkeistään. Kansalaisia kehoitettiin hyökkäyksen alkuvaiheessa myös poimimaan risteyskististä sinne pudotettuja laitteita ja tuhoamaan ne. Laitteet näytti-

vät vähän sellaisilta punaisilta vanhusten Doro-puhelimilta. Kyse oli venäläisten tykistön maalituslaitteista joilla he merkitsivät tärkeitä kohtia. Mutta saattoi ne toki olla niitä Dorojakin, kun ottaa huomioon millä vehkeillä hyökkääjä muutenkin kommunikoi. PÄIVITYS: Länsiapua virtaa edelleen, Himars-raketinheittimet, joita USA on toimittanut ovat osoittautuneet merkittäväksi Ukrainan suorituskyvyille.

Hyvä esimerkki innovaatioiden tuloksista on myös tuo mainittu ajoneuvosaattue, joka mutkitteli Valko-Venäjältä Kiovaan kohti heti sodan alkupäivinä. Kolonnahan ensin pysäytettiin ja sitten pitkälti tuhottiin. Pysähtymisen syyksi on paljastunut Ukrainan armeijan Ilmailu-IT-yksikkö, joka n. 30 nörtin voimalla ja itse tuunatuilla droneillaan tuhosi yksitellen ajoneuvo kerrallaan noita hyökkääjiä, pysäyttäen ensin saattueen alkupään. He ajelivat mönkijöillä yön pimeydessä lähelle ja pudottelivat droneistaan kranaatteja ja räjähteitä venäläisten niskaan. Analysaattori itekin harrastelijadroneilijana arvostaa etenkin heidän keksintöään, jota voisi kutsua vaikka hilloyllätykseksi. Käsikranaatti sijoitetaan lasipurkkiin, sokka irrotettuna ja kiilataan sinne purkkiin siten että kahva pysyy vielä paikoillaan aukeamatta. Tässä lieene viisainta käyttää halkaisijaltaan juuri oikean kokoista hillopurkkiä. Sitten se ripustetaan itse kehitettyyn pudotuslaitteeseen dronen alle ja lähdetään lentämään kohti vihollista. Pudotettu lasipurkki sitten hajotessaan aiheuttaa sen halutun vaikutuksen kohteelleen. Itse toki vain kierrätän hillopurkkini seuraavan vuoden hilloille mutta arvostan innovaatiota.

Keskikokoinen ihme lieene sekin, että Ukrainassa on säilynyt tietoliikenneinfra edes jossain muodossa. Osittain se

johtuu varmasti siitä, että Elon Musk lahjoitti Ukrainaan Starlink satelliittiterminaalejaan, joita on käytetty siellä, missä venäjän hyökkäys on tuhonnut tietoliikennekapasiteettia. Näitä samoja Starlink-yhteyksiä hyödynsivät myös nuo nörtit, jotka pommittivat sitä saatuetta. Sosiaalisessa mediassa on nähty myös tietoliikenneasentajia, jotka siellä kranaattikeskitysten lomassa ovat korjaamassa kuituyhteyksiä. Reaaliaikaisen tiedon välityksen rooli korostuu niin paljon nykyaikaisessa sotimisessa, että sen ylläpitämiseksi on otettava riskejäkin. PÄIVITYS: Ilmeisesti tätä kaistaa tarjotaan myös sinne etulinjan itäpuolelle, sillä venäläisten sotilaiden sometamista seurataan käytännössä reaaliaikaisesti Ukrainan puolella.

Viestimiehenä ei voi kuitenkaan kuin huokailla venäläisten aloskasmaisia munauksia viestiliikenteessä. Taktisten salattujen yhteyksien sijaan sotilailla on paljon käytössä halpoja kiinalaisia käsi-radioita ja omia matkaviestimiä. Tämä sekoilu vaikuttaa erikoiselta siinäkin valossa, että jo 2009 Venäjän sotilasjohto ilmoitti silloisen presidentti Medvedevin käskystä kehittävänsä radiojärjestelmän joka vuoden 2011 loppuun mennessä tuodaan jokaiseen taistelujoukkoeseen ja jokaiselle sotilaille. Tätä järjestelmää kutsuttiin nimellä Akveduk. Nimi viitane muinaisten roomalaisten vesijohtoverkostoon. Tämä suunnitelma ilmeisesti sitten ”vesittyi” ja tilalle kehitettiin ns. kuudennen sukupolven radiojärjestelmä, jonka nimi on Azart. Projektin toimittajaksi valittiin yritys nimeltä Angstrom. Eräs yrityksen johtajista oli ollut Medvedevin neuvonantaja, mutta tuskin sillä nyt oli merkitystä tässä valinnassa.

Nämä radiot antoivat sitten odottaa itseään todella pitkään. Sotshin olympialaisissa 2014 niitä sitten nähtiin armeijan suojajoukoilla ja ne saivat nimityksen ”vihreä krokotiili” pitkien vihreiden antenniensä johdosta. Joko näitä laitteita ei sitten ole Venäjän armeijalla vieläkaan tarpeeksi tai sitten ne toimivat vaan huonosti. Näin voisi nimittäin päätellä hyökkääjän varjo-it:n ratkaisuiden pohjalta.

PÄIVITYS: Sama teknologiasekoilu jatkuu. Alasammattu venäläinen lentäjä oli kertonut käyttäneensä navigointiin Garminin gps-navigaattoria sekä jotain Pronebo-sovellusta. Hän kertoi sen olevan tarkempi kuin lentokoneen omat

varusteet. PÄIVITYS: Kyseinen lentäjä on onnekas, ja ilmeisesti käyttänyt myös omaa siviililaskuvarjoaan, sillä useat laskuvarjoa käyttäneet lentäjät ovat tulleet tonttiin varjon petettyä. Venäläiset ovat nimittäin itse sabotoineet lentäjiensä laskuvarjoja, etteivät nämä jäisi elävinä vangeiksi.

Venäjän kyberhyökkäykset ovat jääneet hieman laajamittaisen konventionaalisen sodan varjoon. Nämä hyökkäykset alkoivat jo ennen varsinaista sotaa ja olivat vaikutukseltaan merkittäviä. Microsoftin rooli Ukrainan kybertorjunnassa on hieman hämärä mutta vaikuttaa melko suurelta. CIA ja FBI ovat olleet aktiivisia Ukrainassa jo vuodesta 2014 mutta suuren amerikkalaisen yrityksen osallistuminen lähes sotatoimiin on melko ainutlaatuisia. Microsoft on globaalina toimijana jo niin suuri, että sen toiminta on luokiteltavissa jo poliittiseksi.

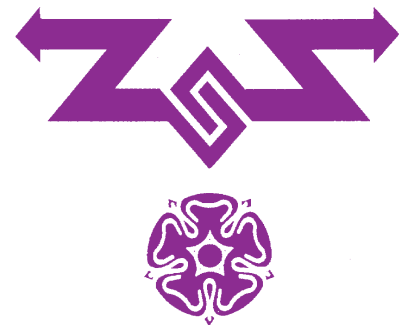
Läntisen maailman pakotteet ovat ajaneet Venäjän tilanteeseen, jossa sen on pakko kehittää omavaraisuuttaan myös ohjelmistojen osalta. Presidentti Putin onkin jo antanut määräyksen, että Venäjän valtion kriittisen infrastruktuurin toimijat eivät voi enää jatkossa hankkia tai käyttää ulkomaisia ohjelmistoja, jos vastaava kotimainen tuote on olemassa. Tuota vastaavuutta ei ole julkisesti tarkemmin määritelty, mutta se kyllä kiinnostaisi. Tavoite on siis vähentää riippuvuutta ulkomaisista tuotteista. Parin vuoden siirtymäajan jälkeen on tarkoitus luopua kokonaan ulkomaisista ohjelmistoista. Ulkomaisista elektronikan komponenteistahan Venäjä pääsikin jo näppärästi eroon juuri mainittujen pakotteiden ansiosta.

Jos hiukan käyttää mielikuvitustaan on helppo kuvitella millaisia ne tulevat kotimaiset ohjelmistoratkaisut ovat, käskytys-metodilla synnytettyinä. Kun Microsoftin tuotteisiin tottunut loppukäyttäjä saa käsiinsä Pjower Pjoint-ohjelmiston, on ilo varmasti ylimmillään. Eikä tarvitse enää kärvistellä Tiimsissäkään. Tosin korvaava versio toimii todennäköisesti vieläkin arvaamattomammin kuin esikuvansa. PÄIVITYS: Tältä osin Tiimssi on kyllä ihan ennallaan.

Pasi Mäkinen

Oikaisu:

Edellisessä numerossa etusivun kuvan ottaja oli virheellinen. Kuvan oli ottanut Jukka-Pekka Virtanen ja sivun 23 kuvasta kuvaaja oli jäänyt pois. Toimitus pahoittelee tapahtunutta.



Kirjoittanut: DI P S Leino ja DI Pauli R U Lallo

Armeijakunnan esikunnan yhteyksien automatisointi



Sotilasviestiyhteydet toimivat perinteisesti manuaalivälitteisinä. Asiasta on viime aikoina kirjoitettu Viestimiehesäkin ja näyttää siltä, että käsivälitys koetaan armeijan kantahenkilökunnan piirissä parhaaksi ratkaisuksi. Tässä kirjoituksessa pyritään tuomaan esiin kirjoittajien käsitys siitä, mikä olisi tällä hetkellä oikea ratkaisu, lähinnä armeijakunnan kokaisen joukon esikunnan viestiyhteyksiksi. Lähtökohtana on vaatimus, että puolustusvoimien on osattava soveltaa nykyaikaista tekniikkaa parhaalla mahdollisella tavalla maanpuolustuksen hyväksi.

Puhelinvaihteen käyttö on sopiva suurrehkon joukon esikunnan tarpeita varten. Koska automaattivaihte liitetään yleisen keskuksen tilaajaksi (tai tilaajiksi), ei tarvita mitään sovituselimiä siirryttäessä paikasta toiseen ja keskustekniikasta toiseen. Tukeudutaan siis markkinoilla saatavilla olevaan standardivaihdetekniikkaan ja kantaviestiverkoon, joita Posti- ja lennätinlaitos sekä toimilupalaitokset jatkuvasti ylläpitävät. LB- ja CB-keskukset tarvitsisivat automaattiliikenteen lisälaitteet keskuksen liittyessään. Kantaverkkoon tukeutuminen merkitsee, ettei yleisten keskustusten välittimiin tarvita mitään muutoksia. Näin ei menetetä aikaa muutoskytöjen tekemisen tai teettämisen vuoksi. Puhelinvaihteen käyttöön avautuu koko valtakunnan kunnossa oleva verkko, eikä vaihteen käyttäjä tarvitse tietää verkon rakenteesta tai suunnista mitään, niin kuin käsivälitteisessä liikenteessä.

Vihollinenkin pyrkii suurella todennäköisyydellä käyttämään kantaviestiverkkoa hyväkseen, joten senkin intresseissä on verkon säilyttäminen ehjänä, vaikkei tähän voi luottaa kaikissa olosuhteissa.

Suomen kantaverkko on suunniteltu kokonaan automatisoitavan vuoteen 1980 mennessä ja tätäkin aikataulua valtioneuvosto on kiirehtinyt. Tässä verkossa käsikeskustoja jää toiminnan varmistamista varten varalle suurimpien kaukokeskusten yhteyteen. Tällä varajärjestelyllä pystytäänkin hoitamaan vain murto-osa automaattisten kaukokeskusten kapasiteetista.

Automaattivaihteilla ovat etuoikeutetut puhelut mahdollisia. Automaattiliikenteessä on yhteyden saanti käsivälitteiseen liikenteeseen verrattuna huomattavan nopeaa ja varmaa. Välittäjän inhimilliset tekijät (hermostuneisuus jne.) eivät vaikuta asiaan. Sisäisessä liikenteessä komentaja pääsee antamaan aina käskynsä päällekytkeytymällä yhteydelle kuten välittäjä. Ajan tasalla olevat verkkokuvat ovat tarpeettomia, koska voidaan aina liittyä mihin tahansa tilaajajohtoon (pakko-otto) aina joukon liikkeen mukaisesti. Vikatapaus verkkoryhmäjohtolla ei sotke toimintaa, sillä ehjän johdon valinta tapahtuu automaattisesti vikaantuneen estovarautuessa. Kaukojohtokimpun vikaantuessa toiminta siirtyy automaattisesti vaihtoehdoiselle kimpulle. Automaattinen vian

eliminointi puuttuu käsikeskustekniikan yhteyksiltä.

Todettakoon, että aikajaksoisella PCM-tekniikalla saataisiin edullisesti automaattiset viestiyhteydet pataljoonatasolle saakka. Tämä tekniikka tekee laitteet pienikokoisiksi ja kenttäkelpoisiksi. Yhteyksien laatuvaatimuksia voidaan jopa alentaa nykyisestä. Tällöin salaaminen pataljoonaportaasta ylöspäin voidaan tehdä erittäin tehokkaaksi satunnaisperiaatetta sovellettaessa. PCM-keskustekniikkaa on sotilaallisiin tarkoituksiin kehitetty ranskalais-saksalaisena yhteistyönä ja tekniikka on jo jonkin aikaa ollut kokeilukäytössä. Erityisesti on huomattava aseman kohtuullinen koko: 2m³ ja 600 kg. Kotimaisen teollisuuden kanssa yhteistyössä olisi selvitettävä ja tutkittava kyseisen tekniikan käyttökelpoisuutta Suomen oloihin. Tämä merkitsee sitä, että Puolustuslaitoksen viestipuolelle olisi saatava lisää insinööriävoimaa ja perustettava varsinaisia tutkijan virkoja.

Artikkelin kirjoittaja: Veli-Matti Pesola

SAVE THE DATE



Viestiupseeriyhdistyksen seminaari 14.2.2023

DIGITAALINEN TURVALLISUUS UUDESSA MAAILMANTILANTEESSA

Miltä näyttävät digitaalisen turvallisuuden uhkat uudessa maailmantilanteessa?
Ja miten niihin voimme kansallisesti sekä NATO-jäsenenä vastata?

Viestiupseeriyhdistys järjestää digitaalisen turvallisuuden ajankohtaisseminaarin
pääkaupunkiseudulla tiistaina **14.2.2023**.

Tilaisuuden järjestelyissä on mukana Nixu Oyj. Alustajina toimivat jälleen maan
parhaimmat asiantuntijat.

Seminaarin ohjelma ja kutsu julkaistaan Viestimies-lehdessä ja
verkkosivuillamme www.viestiupseeriyhdistys.fi joulukuussa 2022.

Varaa aika jo kalenteristasi ja tule mukaan kuuntelemaan ja osallistumaan
keskusteluun!

SAVE THE DATE



TEKSTI: SEPPO URO

Kadonneen radiovastaanottimen metsästys

Monilla viime sotiimme osallistuneilla upseereilla oli rintamalla myös jonkin verran erilaista henkilökohtaista omaisuutta. Erityisesti kesällä 1944 Karjalankannakselta kiireesti vetäydyttäessä tällaista materiaalia jäi sodan jalkoihin. Jo vuonna 1943 valtioneuvosto antoi määräykset siitä, kuinka tällainen sodan johdosta vahingoittunut, tuhoutunut tai hävinnyt yksityisomaisuus korvataan.

Kaukainen sukulaiseni majuri Ilmari Halme toimi vuonna 1944 JR 57:n huoltopäällikkönä Lempäälässä Karjalankannaksella. Hänellä oli siellä kotoaan Viipurista mukaan otettu uusi yleisradiovastaanotin, jonka hän vasta edellisellä vuonna oli ostanut. Radiota kerrottiin käytetyn yleisradio-ohjelmien kuunteleluun joukko-osaston esikunnassa. Radio oli tyypiltään AEG Super 421 GW. Sen hankintahinta oli ollut 4300 mk (tämän päivän rahassa noin 750 euroa). Kesäkuun alussa Halme vei radion tarkistettavaksi 15.D:n radiokorjaamolle Rautuun, jonne se jäi kiireisen vetäytymisen alkaessa. Taistelujen tauottua omistaja alkoi kysellä radionsa perään, jolloin hänelle ilmoitettiin, että radio on evakuoitu 15.D:n viestikenttämakasiiniin Piekämäelle. Sieltä asiaa kysyttäessä laitetta ei kuitenkaan löytynyt. Jatkosodan päätyttyä Halme koetti löytää radionsa vielä

mm. Puolustusvoimien Pääesikunnan viihdytysvälinevarastosta Helsingin Mesuhallista, mutta tuloksetta.

Koska radiota ei etsiskelyistä huolimatta löytynyt Halme teki vuonna 1945 Puolustusvoimain Pääesikunnan varainhoito-toimistolle anomuksen laitteen korvaamisesta. Anomus siirtyi sieltä Pääesikunnan koulutusosastolle, jossa asiaa hoiti toimistoupseeri, kapteeni Niilo Tarvajärvi, myöhemmin koko kansan tuntema ”Tarva”. Hän lähetti Pääesikunnan hallinnolliselle osastolle kirjeen, jossa hän esitti, että Halmeelle joko korvattaisiin radio rahalla tai vaihtoehtoisesti hankittaisiin vastaava kone tilalle. Radioliik-keestä saadun tiedon mukaan kadonnutta vastaanotinta ei ollut myynissä, mutta vastaavana pidettiin esimerkiksi Telefunkenin mallia 2B 54 GMK. Halmeelle lähetettiin kirje, jossa pyydettiin valitsemaan mieluisampi esitetyistä vaihtoehtoista. Koska sotien jälkeen radioista oli huutava pula, valinta kallistui uuteen radioon. Ja jo syyskuussa 1946 majuri Halme sai Pääesikunnasta kirjeen, jossa todettiin, että ”koska omistamaanne ja sittemmin kadonnutta yleisradiovastaanotintanne, AEG Super 421 GW, ei etsiskelyistä huolimatta ole löytynyt, on teille tänään rahtitavarana Helsingin asemalta lähetetty kadonneen vastaanottimenne

korvaukseksi yleisvirtavastaanotin Telefunken Super 2B 54 GWK N:o 40624, joka Kotimainen Radio Oy:n antaman asiantuntijalausunnon perusteella vastaa kadonnutta vastaanotintanne”. Allekirjoituksena jälleen kapteeni Niilo Tarvajärvi. Yli kaksi vuotta kestänyt odotus palkittiin ja Viipurista evakkoon joutunut Halmeen perhe sai uuden radion. Elämä jatkui uusilla asuinsijoilla.

Kapteeni Niilo Tarvajärvi valmistui Kadettikoulusta vuonna 1939. Hän sai tykistöupseerin koulutuksen ja toimi sodissamme mm patterin päällikkönä ja patteristoupseerina. Sotien jälkeen vuosina 1945-50 hän palveli toimistoupseerina Pääesikunnan koulutusosastossa sekä puolustusvoimain komentajan adjutantina. Vuonna 1950 hän erosi puolustusvoimista ja ryhtyi radio- ja televisiotuottajaksi. Myöhemmin hän kertoi lupaavasti alkaneen sotilasuransa katkenneen siihen, kun Pekka Tiilikainen pyysi häntä selostajaksi Lontoon olympialaisiin. Toimittajana Tarva oli idearikas. Hän organisoi useita erilaisia keräyksiä ja tempauksia, joilla hankittiin mm pelastushelikopteri, liikkuvalla poliisille yli 50 partioautoa ja useille sotainvalideille omakotitalo. Tarva ylennettiin majuriksi vuonna 1967 ja Tasavallan presidentti myönsi hänelle kamarineuvoksen arvonimen vuonna 1989.



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