Viestimies

Viestiupseeriyhdistyksen julkaisu 71. vsk Numero 3 Syksy 2016

www.viestiupseeriyhdistys.fi

Viestimies-lehti

Päätoimittaja
Tero Palokangas
p. 050 547 8974
viestimies@viestiupseeriyhdistys.fi

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

Henkilötoimittaja
Markus Töhönen
p. 0299 510 614
henkilotoimittaja@viestiupseeriyhdistys.fi

Toiminnanjohtaja
Martti Aho
p. 040 581 7773
sihteeri@viestiupseeriyhdistys.fi

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

Toimituksen osoite
Mäntymäentie 1 A
04420 Järvenpää
www.viestiupseeriyhdistys.fi/viestimies

Pankkitili FI 21 5780 5520 017 7 44
Vuosikerta 35 Eur

Tilaukset ja osoitteenmuutokset
Martti Aho
p. 040 581 7773
sihteeri@viestiupseeriyhdistys.fi

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

Painopaikka
Newprint Oy, Raisio
p. 010 231 2600

ISSN 0357-2153

Kansikuva:Viestimies-lehden 70-vuotisjuhlaa vietettiin 3.6.2016 Riihimäen upseerikerholla. Kuvat: Joona Hakulinen.

Tässä numerossa

Seuraavan numeron aineistopäivä on 5.10.2016. Lehti ilmestyy viikolla 48.

Kokeile 2 minuuttia ja tiedät, mikä on seuraava oskilloskooppisi

Ainutlaatuinen ja vankka R&S®ScopeRider tuo laboratorio-ominaisuudet kenttäkäyttöön:

- taajuusalue 60MHz-500MHz
- erotetut mittauskanavat CAT IV 600V
- pölyltä ja vedeltä suojattu IP51
- yleismittari, dataloggeri, logiikka-analysaattori
- 7”-kosketusnäyttö
- langaton käyttö (WLAN)

Lue lisää **www.2-minutes.com/field**

2 MIN 2 be 2 sure.

2-minutes.com

Rohde & Schwarz Finland Oy
puh. 0207 600 400
asiakaspalvelu@rohde-schwarz.com

Kokeile 2 minuuttia ja tiedät, mikä on seuraava oskilloskooppisi.

ROHDE&SCHWARZ

Maratonia juoksemassa

Kainuun prikaati toimii nyt viidettä vuotta maapuolustuksen uuden johtamisjärjestelmän M18 käyttöönotosta ja kenttätestauksesta vastaavana tahona. Tehtävä on mielenkiintoinen kunnia-asia, ollaanhan taktisen tasan viestitoiminta uudistamassa Maavoimissa tietyiltä osiltaan lähes täysin. Pitkän matkan juoksussa on harjoittelulla, energiatankkauksella sekä suorituksen aikaisella vauhdin jaolla ja toimintakyvyn ylläpidolla lopputuloksen kannalta iso merkitys. Uuden järjestelmän testaaminen ja kehittäminen samalla varusmiehiä ja reserviläisiä kouluttaen on ollut prikaatille ja etenkin sen nykyisin johtamalleni Pohjois-Suomen viestipataljoonalle merkittävä fyysisten ja henkisten voimien koetus. Normaalisti maratonia juostaessa jaksamista ja voimien jakamista helpottaa tieto siitä, kuinka pitkään on juostu ja montako kilometriä on vielä edessä. M18-käyttöönoton osalta tällaista tietoa ei ole tarkalleen ollut käytettävissä: välillä on tuntunut, että loppusuora ei aukea koskaan. Nyt tuo maali on kuitenkin näkyvissä, ja maavoimien esikunnan määrätietoisessa ohjauksessa olemme siirtyneet tuota loppusuoraa juoksemaan. Kainuun prikaatissa tämä on otettu tyydytyksellä vastaan, sillä se on helpottanut vielä viimeisten käytössä olevien energiavarastojen inventointia ja jakamista loppusuoran eri koitoksia varten.

Ensi vuosi on historiallinen, sillä silloin maavoimien joukko-osastot siirtyvät vaiheittain käyttöönottamaan uutta M18-johtamisjärjestelmää. Järjestelmä onkin harjoituskokemustemme perusteella saavuttanut sellaisen kypsyysasteen ja luotettavuuden, että sitä voidaan huoletta lähteä ”ulkoiluttamaan” myös Kainuun ulkopuolella. Paljonhan toki on vielä keskeneräistä, mutta kuten nykyaikainen siviilipuolen

johtamisjärjestelmäkin, on M18 ohjelmistopohjainen useasta eri laiteperheestä ja sovelluksesta muodostuva kokonaisuus, joka päivittyy ja kehittyy koko ajan. Siinä onkin merkittävä haaste viesti- ja johtamisjärjestelmäalan osaamiselle ja sen ylläpitämiselle. Kaukana ovat ne ajat, että kouluttajan huoneessa pystyit ottamaan kainaloosi tutun ja turvallisen, useita vuosia käytetyn oppaan ja sen turvin lähteä kouluttamaan. Kokemustemme mukaan nykyaikainen johtamisjärjestelmä ei myöskään enää ole sellainen, jonka jokaisen osa-alueen, tekniikan ja sovelluksen ominaisuudet viesti- ja johtamisjärjestelmäalan henkilöstö voisi osata. Järjestelmän yleisten toimintaperiaatteiden tuntemus on mahdollista saavuttaa, mutta todelliseen syväoppimiseen ja kärkiosaajana toimimiseen edellytetään nyt ja jatkossa yhä enemmän erikoistumista.

Maratonista puheen ollen kulunut kesä onkin ollut oikea penkkiurheilijan unelma tai sitten painajainen jalkapallon Euroopan mestaruuskilpailuineen ja Rion kesäolympialaisineen. Näkökulma on riippunut siitä, kuuluuko penkkiurheilijoiden enemmistöön ja onko esimerkiksi olympialaisten aikaan ollut lomilla vai töissä. Jälkimmäisessä tapauksessa en ainakaan itse kyennyt löytämään menestyksen kaavaa aamuyön tunteihin ajoittuneiden lähetysten seuraamiseksi. Onneksi oman suosikkilajini, golfin lähetykset tulivat sentään parhaaseen katseluaikaan. Toisena jälleen kerran koukuttava lajina mieleen jäi eri ammunnat ja etenkin niiden uudistuneet finaalikilpailut. Harmi vaan, että suomalaismenestys jäi jälleen kerran osin aika vaatimattomaksi. Aina voidaan tietenkin vedota kansakuntamme pienuuteen, mutta kyllähän muut pohjoismaat osaltaan taas näyttivät, että pienelläkin maalla on menestymismahdollisuuksia. Kysymys ehkä onkin rajallisista resursseista ja niiden optimaalisesta kohdentamisesta. Ehkäpä näistäkin kisoista taas opittiin jotain jatkon ja suomalaisen huippu-urheilun kehittämisen kannalta: Tokiossa tärähtää!

Lehden 70-vuotisjuhlat saatiin menneenä kesänä asianmukaisesti juhlittua. Kiitos vielä kaikille tapahtumien järjestelyihin sekä itse juhlaan osallistuneille tahoille: teitte osaltanne päivästä ikimuistoisen. Tästä on hyvä jatkaa matkaa kohti seuraavia juhlia eli ensin Suomen ja sen jälkeen Puolustusvoimien ja samalla viestiaselajin 100-vuotisjuhlia. Hienoa, että jatkossakin riittää juhlia ja juhlimisen aiheita muuten osin synkkään ja harmaaseen arkeen. Aurinkoista syksyn jatkoa koko lukijakunnalle, tästä se Joulun ja uuden vuoden odotus jälleen kerran käynnistyy.

VM

Kirjoittajista komentajakapteeni Jari Holopainen toimii Pääesikunnan koulutusosastolla asevelvollisten informaatioprojektin projektipäällikkönä. Majuri Marko Heiskanen palvelee osastoesiupseerina Pääesikunnan johtamisjärjestelmäosastolla.

TEKSTI JA KUVAT: JARI HOLOPAINEN JA MARKO HEISKANEN

Asevelvollisten informaatioprojekti

Juttusarjan aiemmassa artikkelissa Timo Salonen ja Tommi Hermunen avasivat digitalisaation olemusta ja mahdollisuuksia. Tässä artikkelissa kerrotaan Asevelvollisten informaatioprojektin tuloksista ja miten palveluita kehitetään tulevaisuudessa. Projekti on perustettu vuonna 2012 ja se päättyy tämän vuoden lopussa.

Asevelvollisten palveluiden digitalisointi tai sähköistäminen pohjautuu kolmeen kokonaisuuteen. Suomalainen asevelvollisuus eli Siilasmaan raportti (2010) on toiminut lähtölaukauksena digitaalisten palveluiden kehittämisessä. Toiseksi Puolustusvoimien Henkilöstöstrategia 2015 osoittaa tavoitetilaa palveluiden toteuttamiselle. Kolmantena ja tuoreimpana suuntaviivana voidaan pitää valtionhallinnon ohjausta kansallisen palveluarkkitehtuurin puolelta. Kansallisen palveluarkkitehtuurin laki (KaPa-laki) eli viralliselta nimeltään laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016) astui voimaan 15.7.2016.

Lain tarkoituksena on parantaa julkisten palvelujen saatavuutta, laatua, tietoturvallisuutta, yhteen toimivuutta ja ohjausta sekä edistää julkisen hallinnon tehokkuutta ja tuottavuutta. Laissa säädetään julkisen hallinnon yhteisistä sähköisen asioinnin tukipalveluista, niitä koskevista vaatimuksista, niiden tuottamiseen liittyvistä tehtävistä sekä tuottamiseen liittyvästä henkilö- ja muiden tietojen käsittelystä. Lisäksi laissa säädetään oikeudesta ja velvollisuudesta käyttää yhteisiä sähköisen asioinnin tukipalveluja sekä tukipalvelujen käytön edellytyksistä. (esuomi.fi)

Digitalisaatio ja sen tarjoamat hyödyt asevelvolliselle eivät tällä vielä toteudu. Palvelumme ovat manuaalisia, joten uudistusta vaaditaan. Puolustusvoimien asevelvollisten informaatiopalveluprojektissa on lähdetty kehittämään toimintoja lähtökohtana asiakaslähtöisyys. Projektia voi hengeltään rinnastaa hallitusohjelman kärkihankkeiden rinnalle kokeilukulttuurin hengessä.

Uudistuksilla pyritään parantamaan tehokkuutta ja palvelua asevelvollisten erilaisten asioiden hoidossa. Uudistukset on nähtävä voimavarana, jotka lisäävät ketteryyttä Puolustusvoimien virallisten asioiden hoitamiseen ja sitä kautta asevelvollisten tyytyväisyyden ja motivaation nousemiseen. Asevelvollisuus konkretisoituu nuorille kutsunnoissa, missä jokaiselle annetaan palvelukseenastumismääräys. Elämäntilanteita on kuitenkin erilaisia, joten paljon ehtii tapahtua ennen palvelukseen astumista, jotka olisivat digitalisaatiolla ratkaistavissa. Positiivinen kokemus ensimmäisestä asioinnista Puolustusvoimien kanssa luo hyvää mielikuvaa koko organisaatiosta, jolloin kaikki osapuolet voivat hyötyä digitalisaatiosta.

Asevelvollisten informaatioprojektin laajuus.

Mitä sitten on tehty ja mitä ollaan tekemässä?

Puolustusvoimien tavoitteena on olla tavoitettavissa asevelvollisten käyttämissä kanavissa ja mahdollistaa kaksisuuntainen asiointi Puolustusvoimien kanssa. Vuoden 2016 aikana langattomat verkot ovat käytössä kaikissa perusyksiköissä, jotta tulevat palvelut voidaan mahdollistaa kaikille asevelvollisille. Sähköisiä kirjoja eli e-kirjoja on aloitettu julkaisemaan, jossa tuotteena käytetään ePUB sovellusta. Ensimmäisenä on julkaistu kesällä 2016 varusmies -kirja ja tulevaisuudessa kaikki julkiset kirjat taitetaan myös sähköiseen muotoon.

Puolustusvoimien oppimisympäristöä (PVMoodle) käytetään oppimisalustana, mutta varusmiehillä myös arjen pyörittämiseen. Varusmiehille palvelusta löytyy viikko-ohjelmat, päiväraha- ja lomatiedot, loma-anomukset ja erilaisia tiedotteita. Palvelua on kehitetty, että loma-anomusten käsittely ja muokkaaminen hoidetaan sähköisesti, mikä tehostaa merkittävästi yksikköjen henkilöstön työskentelyä. Toiminnallisuutta kutsutaan digitaaliseksi kasarmiksi. Aiemmassa artikkelissa esitelty selvitystyö digitaalisesta kasarmista on siis alkanut toteutua. Pilotointikokemukset ovat olleet positiivisia ja tavoitteena on, että digitaalinen kasarmi on käytössä kaikissa joukko-osastoissa vuoden 2016 loppuun mennessä.

Ennen palvelukseen astumista tarjotaan verkossa myös kunto-ohjelmia Marsmars-palvelussa ja palvelua kannustetaan käyttämään. Palvelua markkinoidaan aktiivisesti kutsunnoissa ja myös reserviläisille kertausharjoituskutsun mukana. Kuka tahansa kansalaisista voi ottaa oman kunto-ohjelmansa, koska palvelu ei vaadi kirjautumista.

Herätteinä Puolustusvoimat käyttää YouTubea ja Instagramia. Molempien sovellusten tavoitteena on kiinnostuksen lisääminen Puolustusvoimia kohtia. Lisäksi YouTube:ssa on julkaistu lyhyitä videoita kuvaamaan esimerkiksi varusmiesten erikoisjoukkoon hakeutumista. Näin ei yhteiskunnassa eläisi myytti sukeltajakurssin pääsykokeista. Tilaajia Instagramilla on 4600 henkilöä (#inttielämää) ja YouTube:n Puolustusvoimien kanavalla 22000 henkilöä.

Saapumiserä 2/16 Joukko-osasto	FB-ryhmien tavoittavuus Tilanne 18.8 ryhmien vahvuuksia
KAIPR	86,76%
NYBR	98,17%
KARPR	62,35%
RPR	84,64%
MAASK	70,99%
PSPR	82,37%
PORPR Säkylä	42,07%
ILMASK	57,55%
KAARTJR	75,07%
PORPR Niinisalo	43,95%
JPR	87,88%
UTJR	52,64%
UTJR/LSVJK 2016	91,32%
RJK Onttola	77,79%

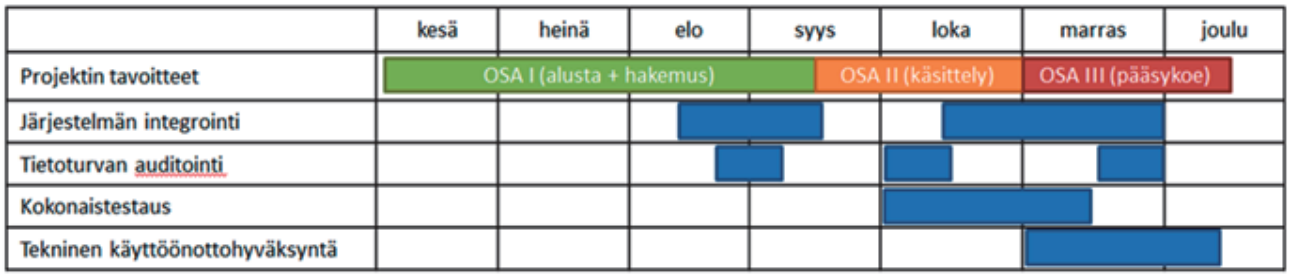
FB-ryhmien tavoittavuus 2/16 –saapumiserän ryhmissä.

Some-agentti eli Facebookin suljetut tukiryhmät avataan jokaiselle saapumiserälle ennen palvelukseenastumista, missä paikalliset Some-agentit tiedottavat aktiivisesti palvelukseen liittyvistä asioista ja vastaavat kysymyksiin. Some-agentti toiminta on käytössä kaikissa peruskoulutuskauden koulutusta antavissa varuskunnissa. Saapumiserästä 2/16 ryhmiin on liittynyt 64% palveluksessa olevista. Suurta osallistujamäärää selittänee, että kyseessä on heidän arjen väline, jolloin kynnys ottaa palvelu käyttöön on matala. Palvelussa järjestellään arjen asioita lomakuljetuksista informaation jakamiseen. Suurimpana hyötynä on esiin nostettava ryhmäytyminen, joka alkaa ennen palvelukseen astumista. Varusmiespalvelukseen astuminen on suuri muutos asevelvollisen elämässä, johon liittyy epävarmuutta ja varmasti edellisten sukupolvien disinformaatiota. Palvelua toteuttaa edellisen saapumiserän varusmies ja toimintaa valvoo nimetty kantahenkilökuntaan kuuluva ohjaaja. Varmasti skeptisimmätkin some-kriitikot myöntävät, että toiminta palvelee erinomaisesti armeijan tärkeitä arvoja.

Sähköisen asioinnin hankinta on toteutettu tänä vuonna ja tällä hetkellä projektissa on toteutusvaihe käynnissä. Hankinta sisältää palvelualustakerroksen ja käyttöliittymäkerroksen sekä ensimmäiset sähköisen asioinnin loppukäyttäjäpalvelut. Asiointiympäristöön tullaan tuottamaan palveluita asevelvollisuuden koko elinkaaren ajalle alkaen ajasta ennen kutsuntoja aina asevelvollisuuden päättymiseen saakka. Palvelu tulee olemaan osa kansallista palveluarkkitehtuuria. Asioi verkossa -palvelu aloitetaan toteuttamalla varusmiesten erikoisjoukkoihin hakeutuminen.

Sähköisen asioinnin alusta perustuu avoimen lähdekoodin ratkaisuun ja teknologiana on käytössä Liferay. Puolustusvoimien verkkosivut uudistettiin keväällä 2016 ja teknologiavalinta on yhtenevä molemmissa kokonaisuuksissa. Tulevaisuudessa asevelvollinen aloittaa asioinnin Puolustusvoimien verkkosivuilta.

Sähköisen asioinnin hankinnassa optiona on mobiilisovellus, jonka toteutuksesta ei ole vielä päätöstä. Mobiilisovellus *inttiin, intissä ja reservissä* on suunniteltu kohderyhmien mukaisesti eri sisällöillä. Mobiilisovelluksen sisällöllisiä ensiaskeleita on palvelustehtävät uusilla verkkosivuilla varusmiesten teemasivujen alla.



Sähköisen asioinnin aikataulu.

Tulevaisuus

Digitaalisten palveluiden kehittäminen ei pääty vuoden loppuun vaan alusta mahdollistaa uusien palveluiden kehittämisen. Sähköisen asioinnin kehittämistä on toteutettu ketterällä menetelmällä, joka soveltunee hyvin myös tulevien vuosien jatkokehitykseen. Tällä hetkellä on avattu digitaalinen kehityspolku, joka mahdollistaa Puolustusvoimien ja asevelvollisen sähköisen asioinnin turvallisesti. Tulevaisuudessa on tarkasteltava mitä muita sovelluksia tarvitaan digitaalisen ekosysteemin toteuttamiseksi.

Puolustusvoimilla on tunnistettu kymmeniä palveluita, joita voitaisiin digitalisoida. Tulevien vuosien kehittämisen suunnittelu ja määrittely on käynnissä, jotta kokonaisuudesta saadaan asiakkaita tukeva. Tunnistetut palvelut koskettavat koko asevelvollisen elinkaarta ja myös palveluita kansalaisille sekä organisaatioille. Näistä tutuimpia ovat varmasti erilaiset lupa-asiat, jotka ovat tällä hetkellä manuaalisia.

Tulevaisuuden ennustaminen digitalisaation suhteen on mahdotonta ja myös tarpeetonta. Digitalisaatio on valtionhallinnossa yksi kärkihanke, jolloin yhteisestä kehityksestä kannattaa ottaa hyödyt Puolustusvoimien kaikille toimijoille, ennen kaikkea meidän asiakkaille eli kansalaisille. Digitalisaatio on mahdollisuus vapauttaa aikaa merkityksellisille tapahtumille ja toimille.

VM

TEKSTI: SAKARI AHVENAINEN

Sotilas- ja siviiliteknologian eroista

– systeeminen tarkastelu, osa 2

Kirjoittaja on viestiupseeri, everstiluutnantti (evp) ja aloittanut väitöskirjan laatimisen Maanpuolustuskorkeakoulussa sodankäynnin systeemisistä, evolutiivisista ja kyberneettisistä perusteista.

Tässä kaksiosaisessa artikkelisarjassa tarkastellaan sitä, mitä voidaan sanoa sotilasteknologia ja siviiliteknologian eroista sodankäynnin pienimmän systeemikuvauksen perusteella. Sarjan ensimmäisessä osassa Viestimies 2/2016 lehdessä selvitettiin perusteet: Mikä on sodankäynnin yksikertaisin kuvaus? Mikä on sodankäynnin teknologian yksikertaisin kuvaus? Mitkä ovat sodankäynnin yleiset ominaisuudet? Mitkä ovat niiden perusteella sotilasteknologian yleiset ominaisuudet? Sarjan tässä osassa selvitetään, mitkä ovat siviili- ja sotilasteknologian erot artikkelisarjan ensimmäisen osan perusteiden mukaan ja mitä niistä seuraa ja tarkastellaan, mitä johtopäätöksiä edellisten kahden osan perusteella voidaan tehdä ja mikä on näiden johtopäätösten merkitys.

Sodankäynti perustuu epävarmuuteen, siviiliteknologia varmuuteen

Sodankäynti perustuu vihollisen vapaan tahdon ja sen vastatoimien takia keskeisesti epävarmuuteen. Vihollisen vapaata tahtoa ei voida sodankäynnistä poistaa, joten epävarmuutta ei voida poistaa sodankäynnistä. Sitä ei pidä vain hyväksyä, vaan epävarmuutta on luotava tavoitteellisesti ja käytettävä omaksi eduksi.

Sotilasteknologian keskeinen ominaisuus on siis sen tavanomaisen, ”toiminnallisen” kyvyn lisäksi sen kyky tuottaa viholliselle epävarmuutta ja poistaa omaa. Toiminnallisella tasolla epävarmuutta luodaan muun muassa harhautuksella, salaamisella, reserveillä ja alueellisella, hajautetulla puolustusjärjestelmällä.

Keinoja tuottaa epävarmuutta viholliselle sotilasteknologialla ovat esimerkiksi

- sen ominaisuuksien salaaminen tai joidenkin ominaisuuksien jättäminen reserviin (war modes)
- sen ominaisuuksilla harhauttaminen
- kyky muuttaa (nopeasti) tekniikan ominaisuuksia, mm. päivittämällä laitteiden ja järjestelmien ohjelmistoja tekniikan kehityksen tai vastustajan toiminnan perusteella
- toiminnan jatkaminen vastustajan vastatoimien, esimerkiksi häirinnän jälkeen normaalina, huolimatta vastatoimien todellisesta vaikutuksesta
- järjestelmän hajauttaminen ja sen liikkuvuus (käyttö liikkeessä).

Epävarmuus on siviiliteknologiassa poistettava ominaisuus. Järjestelmät rakennetaan alun perin sellaisiksi, että haluttu varmuus saavutetaan.

Epävarmuus ja tietokoneohjelmat

Mitä ovat tietokoneohjelmat sotilasteknologiassa? Siviiliteknologiassa ne edustavat tehokkuutta. Pohjimmiltaan, huolimatta ohjelmien monimutkaisuudesta, ne edustavat varmuutta, toistettavuutta, työkalua. Sotilaallisesti tämä tarkoittaa epävarmuuden poistamista. Koska se ei ole sotilaallisesti mahdollista, tästä täytyy seurata jotain oleellista ja sotilasteknologian tietokoneohjelmille epäedullista. Tietokoneohjelmisto:

- kuvaa täysin teknisen laitteiston toiminnan tai johtamisjärjestelmän osana johtamisjärjestelmän toiminnan
- paljastaa sotilaallisen ajattelun järjestelmän takana
- paljastaa sotilaallisen järjestelmän liitynnät, seikat mistä kohdejärjestelmän toiminta on riippuvainen
- se paljastaa järjestelmän tehokkuuden ja sen rajat. Tätä tietoa voidaan käyttää muun muassa järjestelmän kyllästämiseen
- paljastaa yksityiskohtaisesti, miten järjestelmä on harhautettavissa tai miten sen tehoa voidaan laskea, jopa nollata.

Edellistä seuraa, että sotilasteknologian tärkeimmät tietokoneohjelmat

ovat erityisen tiedustelun ja suojaamisen kohde. Parhaat algoritmit ja paras suorituskyky pidetään vain itsellään ja vain harvoin myydään vieraille valtiolle sellaisenaan. Jos ohjelmistojen modifiointi ei ole mahdollista, on ulkomaille myytyyn järjestelmään käytettävä muita kontrollin keinoja.

"Tarpeeton" tekninen päällekkäisyys

"Tarpeeton" tekninen päällekkäisyys on tuhlausta siviilijärjestelmissä, mutta haluttu ominaisuus sotilasteknologisissa järjestelmissä. Jos halutun liikenteen välittämiseen tarvitaan siviilisovellutuksena kolme siltaa, siviilijärjestelmässä rakennetaan kolme siltaa. Jos sotilaalliseen sovellutukseen (joen ylitys) tarvitaan oman halutun liikenteen välittämiseen kolme siltaa, on kolmen sillan rakentamisen lisäksi ryhdyttävä moniin sotilaallisiin lisätoimiin. Näitä ovat ainakin

- siltojen suojaus eri tavoin mm. ilmavoimilta ja maahanlaskuilta
- reservisillat läheisyydessä
- neljän tai useamman sillan rakentaminen jo alun perin, jolloin tappiot on huomioitu jo rakennusvaiheessa
- liikenteen suuntaaminen jotain muuta (vaikeampaa) kautta, jos kolmea siltaa ei pystytä ylläpitämään
- operaation pysäyttäminen ja vaihtoehtoisen käynnistäminen
- toimivien siltojen salaaminen tai niiden käytöllä harhauttaminen.

Onko vihollisen vastatoimien ennakointi mahdollista?

Vihollisen vastatoimia voidaan ennakoida niin, että vastatoimien vaikutus rakennetaan teknologisiin systeemeihin etukäteen, esimerkkinä häirintäsuoja. Mitä tehokkaampi systeemi on, sitä enemmän vastatoimiin panostetaan ja sitä vaikeampi niitä on arvioida ja ennakoida. Vastustajan vastatoimien ennakointi edellyttää erittäin hyvää tiedustelua ja vastustajan tuntemista. Tämä ei ole aina ollut näin, vaan esimerkiksi ennen toista maailmansotaa vihollisten teknologian tietämys oli USA:ssa takapajuista. Lisäksi voidaan todeta, että mitä täydellisimmin vihollisen vastatoimet voidaan ennakoida, sitä vähemmän vihollisen tahtoa jää vapaaksi ja sitä vähemmän on kyse enää sodankäynnistä.

Mitä ovat sotilasteknologian vastatoimet?

Professori Edward N. Luttwak esittää teoksessaan "Strategy", että teknologian vastatoimet voivat olla taktiikkaa, uusia metodeja, uusia sotilaallisia rakenteita, jopa strategiaa ja että näiden vastatoimien ennakointi ei ole tieteellistä tai teknologista osaamista.

Teknologia on kuitenkin vain yksi sodankäynnin toiminnallisista funktioista suuremmassa, synergistisessä systeemissä. Muita sodankäynnin yleisiä toiminnallisia ulottuvuuksia ovat ihmiset, doktriini, organisaatio, logistiikka (virrat), tieto, aika, tila ja energia.

Sodankäynnin toiminnallisten ulottuvuuksien perusteella voimme täydentää Luttwakin teknologiaan kohdistuvia vastatoimia. Näitä ovat:

1. Teknologian käyttö, esimerkkinä elektronisten järjestelmien häirintä
2. Ihmisten käyttö, esimerkkinä sotilasjohtajien kouluttaminen vihollisen teknologisten järjestelmien ymmärtämiseen ja niiden tehokkuuden perusteisiin
3. Doktriinin muutokset (Luttwakin taktiikka, metodit ja strategia)
4. Logistiikan käyttö, muun muassa luomalla viholliselle liikaa maaleja, jotta kaikki voitaisiin torjua
5. Organisaation muutokset, kuten hajauttamalla omat joukot erillisiksi ja itsenäisiksi, mutta yhteistoimintakykyisiksi yksiköiksi verkostokeskeisen puolustuksen periaatteiden mukaan. Tämä olisi samalla myös doktriinin muutosta.
6. Informaation käyttö, esimerkiksi tehokkaampi tiedustelu vastustajan teknisten järjestelmien ominaisuuksien tutkimiseksi. Tämä voi sisältää myös sotasaalismateriaalin tutkimuksen tai tärkeän osajärjestelmän kaappauksen tutkittavaksi kuten saksalaisten tutkan kaappaaminen Kanaalin rannalla toisen maailmansodan aikana tai amerikkalaisten Irakin tärkeän tutkajärjestelmän kaappaus ennen vuoden 1991 sotaa.
7. Ajan käyttö, esimerkiksi hidastamalla sodankäyntiä sissisodalla tai muuttamalla epäsuoran tulen yksiköiden tuliasemia jokaisen lyhyen tuli-iskun jälkeen niin, että vastatykistötoiminnalle ei jää tarpeeksi toiminta-aikaa.
8. Tilan käyttö, kuten siirtymällä viivytykseen, ei vaihtamalla tilaa aikaan.
9. Energian käyttö, esimerkiksi käyttämällä EMP:ä tai HPM:ä elektroniikkaa vastaan.
10. Erilaiset edellä mainittujen perustapojen yhdistelmät.

Onko teknologia aina alisteinen taktiikalle?

Luttwakin mukaan sodankäynnin perustasojen vaikutussuhteet ovat seuraavat:

- teknologia on alisteinen taktiikalle
- taktiikka on alisteinen operaatiotaidolle ja
- operaatiotaito on alisteinen strategialle.

Luttwakin mukaan yksi panssarivaunu ja yksi panssarintorjuntaohjus ovat teknologisella tasolla. Kymmenen panssarivaunua ja vastaava määrä panssarintorjuntaohjuksia muodostavat uuden, taktisen tason, jolle muodostuu uusia emergenttejä piirteitä.

Tämä on esimerkki systeemien systeemistä tai olemassaolon hierarkkisesta rakenteesta, jossa ylempi taso, suurempi yksikkö muodostuu alemmista osista, kuten atomi alkeishiukkasista, molekyyli atomeista ja solu monimutkaisista biologista molekyyleistä. Tässä järjestelmässä alempi osa on osa ylempää ja siinä mielessä aina "alisteinen" ylemmälle. Mutta onko tekniikka taktiikan alempi osa?

Jos on olemassa operatiivista tai strategista teknologiaa, ne eivät ole alisteisia edellä mainitussa mielessä taktiikalle, vaan osa oman tasonsa teknologista toimintaa. Ja selvästi on olemassa operatiivista tai strategista teknologiaa. Ilmavoimien käyttö maaoperaatioissa on perinteisesti pääosin operatiivista tai strategista ja strategiset ydinaseet ovat osa strategisen tason teknologiaa. Yksittäisen strategisen ohjuksen käyttö on ydinaseiden tasolla taisteluteknistä, mutta koska ydinase on itse strategisella tasolla, myös sen käyttö on strategista.

Luttwakin periaate pitää paikkansa työkaluihin (miekka, musketti) ja (taktisiin) koneisiin liittyen, mutta ei enää

järjestelmiin ja järjestelmien järjestelmiin liittyen. Tällöinkin ”alisteisuus” ei ole oikea sana. Viesti- tai johtamisjärjestelmä, joka sitoo operatiivisen tai strategisen tason osat yhteen, ei ole taktiikalle alisteinen, vaan osa oman tasonsa teknologiaa. Tämä tarkoittaa, että on strategista, operatiivista ja taktista teknologiaa. Se taas tarkoittaa, että teknologialla voidaan vaikuttaa strategisella, operatiivisella ja taktisella tasolla. Luttwak tarkoittaa itse asiassa taistelutekniikkaa, periaatteita, joilla yksittäisen sotilaan (vast.) yksittäistä asetta käytetään. Taistelutekniikka ON alisteinen taktiikalle, sen osa.

Teknikoiden ja sotilaiden roolista

Luttwakin mukaan teknisesti suuntautuneet sotilaat ja sotilaallisesti suuntautuneet insinöörit, molemmat oman ryhmänsä vähemmistöjä, keskustelevat jatkuvasti sotilaallisten prioriteettien ja teknisten tavoitteiden välisestä jännitteestä. Mutta kun teknisen kehityksen tuotteet luovutetaan asevoimille, vaikuttavat niiden käyttöönottoon massojen teknologinen osaaminen ja käyttöönottoa edeltäneet institutionaaliset intressit.

Edellä oleva tarkoittaa ainakin sitä, että uuden sotilasteknologian käytössä tulee huomioida aina se kohderyhmä, joka lopulta tekniikkaa käyttää. Tämä on tärkeä periaate reserviläisarmeijassa. Uuden teknologian hyödyt mitataan vasta käytössä. Myös lopullisen kohderyhmän koulutus on tärkeää, erityisesti jos tekniikkaa on uutta ja vaativaa. Voidaan myös ajatella, että parhaimmillaan uuden järjestelmän käyttöönottoa seurataan ja kohdehenkilöstölle järjestetään jatkokoulutusta, jos huomataan, että teknologian mahdollisuuksien ymmärryksessä on puutteita. Tällaisella lisäkoulutuksella voidaan tietoa välittää kuitenkin vain kohderyhmän teknisen perustietämyksen puitteissa, ei enempää.

Vihollisen pakottaminen tekemään kahta vastakkaista asiaa

Vihollisen pakottaminen tekemään kahta vastakkaista asiaa yhtaikaa on ehkä tärkein yksittäinen tapa käyttää teknologiaa (tai mitä tahansa muuta keinoa) voiton saavuttamiseen sodassa. Yksi esimerkki tästä on viestitiedustelu. Yksi tehokkaimmista keinoista lisätä omaa tehokkuutta on viestiteknologian käyttö johtamisen apuna. Asejärjestelmien kantaman lisääntyessä yli näköetäisyyden, jopa yli horisontin, viestijärjestelmistä on tullut välttämättömyys.

Käyttämällä viestintäteknologiaan kohdistuvaa viestitiedustelua vihollinen pakotetaan aina tekemään kahta vastakkaista asiaa: joko tehostamaan omaa johtamista viestijärjestelmillä ja paljastamaan johtamisjärjestelmiä viestitiedustelun kautta tai tehostamaan omien johtamisjärjestelmien suojaa olemalla käyttämättä viestijärjestelmiä, mutta heikentämällä samalla omaa johtamista.

Tämä on kokonaisvaltainen ja systeeminen tapa sotia, katsoa ilmiselvän ja yksinkertaisen yli. Se on yleisen systeemiteorian mukainen tapa tarkastella kaikkia moderneja kompleksisia systeemeitä.

Sodassa jotain nyt on paljon enemmän kuin paras kuukauden päästä

Suhteellisesta edusta johtuen jotain nyt on paljon enemmän kuin paras kuukauden päästä. Jos meillä ei ole jollakin sodankäynnin alalla toivoa nykyistä paremmasta, vihollisen koko teho kohdistuu meihin täydellä teholla.

Paras ja kallein kivääri voi olla vain hieman parempi kuin tavallinen moderni kivääri, joka noudattaa samoja luonnon lakeja.

Sodankäynti on kompleksinen systeemi, eikä yksittäisen asian tehokkuus vaikuta juurikaan suureen kokonaisuuteen, kunhan kyseinen asia on minimaalisella, selvästi nollaa suuremmalla tasolla.

Pohdintaa

Tässä artikkelisarjassa on käsitelty joitain systeemiteorian ominaisuuksia, osoittamaan näiden periaatteiden mahdollisuuksia ja sovellutuksia sodankäyntiin liittyen.

Käyttämällä kirjoittajan aiemmin esittämiä sodankäynnin toiminnallisia ulottuvuuksia pystyttiin systematisoimaan Luttwakin esimerkkejä sotilasteknologian vastatoimista. Myös Luttwakin esitys teknologian yleisestä alisteisuudesta taktiikalle asetettiin kyseenalaiseksi.

Artikkelin ehkä suurin “uusi” anti oli systeemin, eli sodankäynnin ympäristön keskeisyys. Sodankäynnin yhteydessä se on liitettävä aina ympäristöönsä ja vain ympäristönsä kautta sodankäynti on ymmärrettävissä. Tästä seuraa muun muassa se, että ajallisesti kaukaisten sodankäyntitapojen ymmärtäminen on potentiaalisesti vaikeaa, koska ympäristöä ei pystytä enää useinkaan kuvaamaan ja ymmärtämään tarpeeksi tarkasti.

Systeemisesti kaikki liittyy lopulta kaikkeen ja tämä edellyttää hyvin kompleksista tarkastelua, mutta antaa tietoa muun muassa sotilasteknologian todellisista vaikutuksista ja käyttäytymisestä. Oleellista on tähän kompleksisuuden hallintaa liittyen se, että siihen on syntynyt uusia mahdollisuuksia tietokoneiden ja simulointi-järjestelmien kautta. Useat maat ovat jo perustaneet simulointilaitoksia kompleksisuuden kätkemien mahdollisuuksien hyödyntämiseen. Aihe ei ole tuntematon Suomessakaan.

Sotilasteknologia ja siviiliteknologia sillä tavalla ymmärrettynä kuin ne tässä artikkelissa on käsitelty ovat ääripäissään. Todelliset taistelut ja siviilialan kilpailu ovat aina ääripäiden välissä. Globaali media ja sen luoma globaali tietoisuus rajoittavat jo merkittävästi sotilasteknologian käyttöä ja toisaalta informaation käyttö antaa yrityksille ja jopa yksilöille uusia mahdollisuuksia vihamieliseen, sodankäynnin tyyliseen vaikuttamiseen.

Johtopäätöksiä

Artikkelissa on todettu, että yleinen systeemiteoria on käyttökelpoinen teoria sodankäynnin tarkasteluun ainakin yleisellä tasolla. Sen käyttö systematisoi ja kokonaisvaltaistaa sodankäynnin ymmärtämistä ja liittää sodankäynnin laajempiin yhteyksiin. Koska kokonaisuuksien hallinnasta on tulossa systeemikoon kasvun myötä yhä tärkeämpää,

systeemiteoria on yhä merkittävämpi keino myös sodankäynnin ymmärtämiseen, mahdollisesti jopa uudella tavalla.

Osoittautui, että tekniikka ei ole vain tekniikkaa, vaan siihen liittyy sen konteksti, muu kokonaisuus, johon tekniikka liittyy. Seuraa jatkokysymys: opetetaanko tekniikka tällä tavalla, siis siten, että kaikessa tekniikassa osa opetusajasta käytetään ensin kokonaisuuden hahmottamiseen: Missä kokonaisuudessa tekniikka on osa ja miten kyseinen kokonaisuus vaikuttaa ”varsinaiseen” tekniikkaan? Vastaava sovellutus on tehtävissä sodankäynnistä: Ilman vihollisen ja toimintaympäristön kattavaa käsittelyä sodankäynnin opetus on amatöörimäistä.

Artikkelissa on esitetty, että teknologian käyttö kilpailuintensiivisessä toimintaympäristössä, äärimmillään sodassa, asettaa ko. teknologian käytölle ”normaaliteknologiasta” poikkeavia, ko. toiminnan yleisiin ominaisuuksiin liittyviä erityisvaatimuksia.

Vihollinen on sodankäynnin ensimmäinen ja tärkein erityisvaatimus. Vihollisen kautta tärkeiksi tekijöiksi nousevat ainakin vihollisen vapaa tahto, suhteellinen etu, paradoksaalinen logiikka, yllätys, epävarmuus, oppiminen sekä salaaminen ja harhauttaminen.

Sodankäynti on systemaattisesti analysoituna äärimmäisen kompleksista toimintaa. Vaikuttavia seikkoja on liikaa analysoitavaksi perin pohjin. Tämä ei ole kuitenkaan oleellista sodankäynnissä, koska siellä ei tarvitse ymmärtää tai osata toimintaa täydellisesti, vain ratkaisevasti paremmin kuin vastustaja. Voidaan myös sanoa, että voittaja on usein se, joka tekee vähemmän virheitä.

Sotilasteknologiassa ja siviiliteknologiassa on kaksi samaa käyttöä: teknologian käyttö tehostamaan toimintaamme ja teknologian käyttö ympäristön ongelmien voittamiseen. Sotilasteknologiassa on lisäksi kaksi muuta käyttöä: teknologian käyttö teknologiaa vastaan ja teknologian käyttö teknologian puolustamiseen.

Sotilasteknologian käyttökelpoisuus on ajallisesti vastakkainen siviiliteknologian kanssa. Sotilasteknologiasta saadaan suurin hyöty alussa, yllätyksen kautta. Kun sotilasteknologia kypsyy, se menettää tehoaa, kun vastustaja oppi välttämään sen tehoa ja kehittää sille vastatoimia. Kun vastatoimilta on suojauduttava, vanhasta teknologiasta tulee myös kallista. Edellä mainitun perusteella tuleekin pyrkiä uuteen teknologiaan.

Sotilaallista (teknologista) tehokkuutta saadaan aikaiseksi luopumalla (teknologian) siviilitehokkuudesta. Yleisesti tämä periaate selittää sen, miksi sodankäynnissä on reservejä, harhauttamista ja rinnakkaisia järjestelmiä.

Sotilasteknologia on sisäisesti kompleksinen kokonaisuus, johon yksikertaisemmillaankin vaikuttaa moni asia. Lisäksi sen lopullinen synerginen kokonaisvaikutus syntyy monen ulkopuolisen asian kautta. Tästä seuraa se, että sotilasteknologian sisäiset vastatoimet ovat moninaisia ja että sotilasteknologian tehokkuuteen voidaan vaikuttaa monilla muillakin asioilla kuin pelkällä sotilasteknologialla.

Sotilasteknologian lopullinen tehokkuus on paitsi teknologian tehokkuuden funktio, myös asevoimien keskimääräisen teknologisen osaamisen funktio. Huipputeknologiasta ei ole todellista hyötyä, jos asevoimissa kokonaisuutena ei ole sitä hyödyntävää osaamista. Asevoimien teknologinen osaaminen on oltava siis sopusoinnussa muun muassa sen käyttämän teknologian kanssa.

Vihollisen vapaa tahto nousi sodankäynnin määrittelyssä keskeiseksi edellytykseksi monissa kohdissa. Jos sota on yksipuolista teurastusta, se ei ole sotaa vaan yksipuolista teurastusta. Todellinen sotilasteknologia perustuu epävarmuuteen, vihollisen vapaaseen tahtoon ja siviiliteknologia varmuuteen, vapaan tahdon puuttumiseen.

Ensimmäinen suuri ero siviili- ja sotilasteknologian välillä on niiden ympäristö. Ja koska ympäristö on erityisen tärkeä kaikille järjestelmille, tulee tästä ympäristöerosta erityisen tärkeä. Sotilasteknologian ympäristö on sodankäynti, taistelu kahden vastakkaisen ja vapaan tahdon välillä. Siviiliteknologian ympäristö on laitteiden ja järjestelmien rauhanomainen käyttö edistämään kyseisen käyttäjän tai ryhmän tavoitteita. Tärkein ero on vihollinen, joka sotilasteknologiassa pyrkii aktiivisesti tuhoamaan vastapuolen teknologiaa tai vaikeuttamaan sen käyttöä.

Siviiliteknologian tehokkuus on ennustettavissa ja varmaa. Sotilasteknologian tehokkuus ei ole ennustettavissa ja on epävarmaa. Sotilasteknologian tulee jopa luoda epävarmuutta. Yksi aivan keskeinen tapa siihen on pakottaa vihollinen tekemään kahta vastakkaista asiaa yhtaikaa.

Siviiliteknologian logiikka on lineaarista ja sotilasteknologian paradoksaalista. Siksi tässä artikkelisarjassa esitetyn logiikan mukaan yksikertaisin ja selkein ratkaisu ei ole oikea valinta sodassa, toisin kuin yleisesti sanotaan. Siviiliteknologissa paras on aina paras. Sotilasteknologiassa toiseksi paras on usein lopulta paras, kun vastustajan vastatoimet parhaasta järjestelmää vastaan huomioidaan. Tästä seuraa ainakin se, että siviilimäisesti vanhanaikaiseksi tuomittu teknologia onkin sotilaallisesti tehokasta, kun oivalletaan, että vanhaa teknologiaa ei käytetä uusinta teknologiaa vastaan, vaan sitä käytetään vasta, kuin huipputeknologiset järjestelmät ovat pitkälti tuhonneet toisensa.

Ylimääräinen tekninen päällekkäisyys on tuhlausta siviiliteknologiassa, mutta tavoiteltava järjestelmäominaisuus sotilasteknologiassa.

Monet esitetyt johtopäätökset ovat sinänsä triviaaleja, yleisesti tunnettuja. Oleellista tässä artikkelisarjassa on kuitenkin niiden syiden esittäminen ja ymmärtäminen. Vain ymmärtäminen mahdollistaa tunkeutumisen näiden triviaalien johtopäätösten taakse, syvemmälle. Ja vain ymmärtämällä sodankäyntiä ja sen teknologiaa, niitä voidaan hallita. Ei täydellisesti, mutta vastustajaa paremmin. VM

Insinööri AMK Aimo Pellinen toimii T&K –päällikkönä Jyväskylän ammattikorkeakoulun IT-instituutissa.

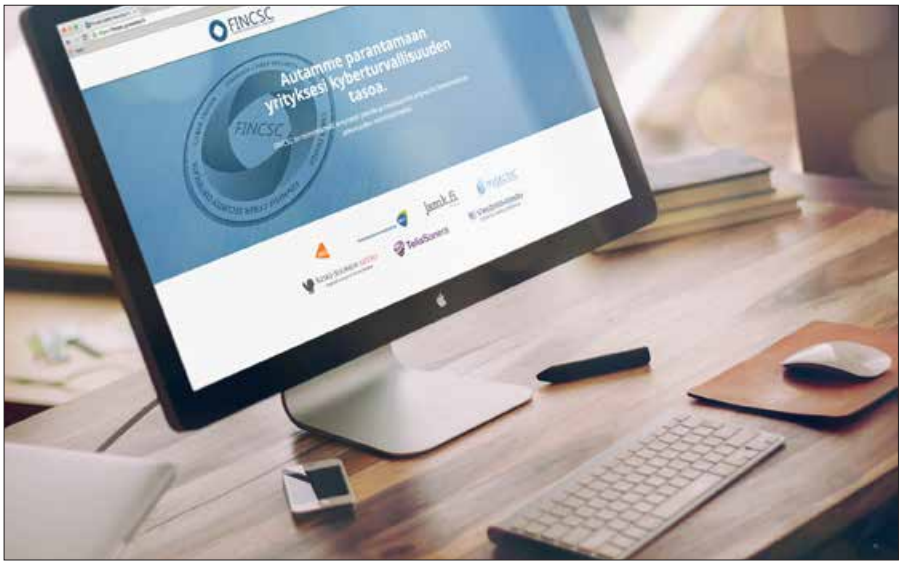
TEKSTI: AIMO PELLINEN
KUVAT: HELI SUTINEN

Kyberturvallisuuden tason arviointi pk-yrityksissä

Digitalisoitumisen myötä informaatioteknologiasta ja sen turvallisuudesta on tullut lähes poikkeuksetta elementti, joka vaikuttaa vähintäänkin epäsuorasti lähes kaikkien yritysten liiketoimintaan ja sen jatkuvuuteen. Tieto ja sen käsittelyssä ja tallentamisessa käytettävä informaatioteknologia ovat useimpien yritysten kriittisiä menestystekijöitä. Henkinen pääoma, tuotteiden suunnitteluun, valmistusprosessiin tai strategiaan liittyvät luottamukselliset tai arkaluontoiset tiedot muodostavat usein suurimman osan yritysten kilpailuedusta. Samalla tarve käyttää ja jakaa tietoa entistä laajemmin ja tehokkaammin uusia tieto- ja viestintätekniikoita käyttäen lisää yrityksen tietopääomaan liittyviä riskejä.

Nykyaikainen tieto- ja viestintätekniikka mahdollistaa kaikenkokoisille yrityksille innovoinnin, uusien markkinoiden sekä asiakkaita ja yhteiskuntaa hyödyttävien tehokkuusetujen saavuttamisen. Lisääntyvässä määrin liiketoiminnan käytäntöjä joudutaan suoraan tai välillisesti sopeuttamaan niihin viestinnällisiin ympäristöihin ja tietoverkkoihin, joita vaaditaan tavaroiden ja palvelujen toimittamiseen. Monet yritykset hyväksyvät modernien tieto- ja viestintätekniikoiden käytön ymmärtämättä täysin niiden mukanaan tuomia uudentyyppisiä riskejä ja uhkakuvia. Digitaalisuuden näin mukanaan tuoma haavoittuvuuksien määrän eksponentiaalinen kasvu ja kyberturvallisuusuhkien lisääntyminen on käytännössä tarkoittanut lisääntyvää tarvetta yritysten liiketoiminnan jatkuvuuden turvaamiseen. Yritykset ovatkin entistä aktiivisemmin alkaneet havainnoida omassa toiminnassaan kyberkontekstin tuomia uusia uhkavektoreita, mutta toisaalta myös uusia liiketoimintamahdollisuuksia. Kyberkontekstin huomioon ottaminen organisaatioiden toiminnassa on kuitenkin edelleen liiaksi perinteiseen tietoturvaan keskittyvää riskienhallintaa ja teknisten suojausmallien kehittämistä.

Uutiset tietomurroista ja palvelunestohyökkäyksistä ovat jo arkipäivää lehdistössä. Niin suuret kuin pienet yritykset ovat nyt alttiina yhä kasvavalle tietoverkkorikollisuudelle, jossa toimijoita ovat hakkerit, valtiolliset toimijat ja mahdollisesti myös kilpailijat. Yrityksiin kohdistuvat tietoverkkorikokset ovat yhä hienostuneempia ja niissä hyödynnetään uuden tieto- ja viestintätekniikan teknologioissa ja ohjelmistoissa esiintyviä tietoturvaheikkouksia ja -haavoittuvuuksia. Yhä useammista ulkoisista laitteista koostuvat tietojärjestelmät lisäävät vaativuustasoa ja uhkia yritysten tietojärjestelmiä kohtaan. Ulkoisten uhkien lisäksi yritysten on kyettävä hallitsemaan myös sisäisiä tietojärjestelmiin kohdistuvia uhkia, joissa esimerkiksi yrityksen henkilöstö kykenee vioittamaan tietoverkon dataa tai käyttämään sitä haitallisesti yrityksen ulkopuolella. Liiketoiminnan näkökulmasta on tärkeää, että yritys - suuri tai pieni - kykenee tunnistamaan tietoverkkojensa turvallisuusuhkia ja arvioimaan turvallisuusriskejä. Samaan aikaan yritysjohtajien on tunnistettava, että kyberturvallisuusriskien hallinta on kokonaisvaltainen ja jatkuva prosessi.



FINCSC kyberturvallisuuden arviointimallia käytetään verkkopohjaisen käyttöliittymän (portaalin) avulla (www.fincsc.fi).

Pk-yritysten haasteita

Toisin kuin monet muut liiketoiminnan haasteet, tietoverkkojen ja muun digitaalisen toimintaympäristön turvallisuuden riskienhallinta on edelleen haaste, johon ei ole saatavissa helppoa ratkaisua. Riittävän tietoisuuden hankkiminen toimintaympäristöön sisältyvistä uhkista ja niiden vaikutuksista liiketoimintaan on ensimmäinen askel tällä tiellä. Vaikka monet palveluntuottajat tarjoavatkin selvityksiä tietoverkkojen uhkista, on pk-yrityksille sopivaa materiaalia auttamaan liiketoiminnan hallintaa suhteessa tietoverkkoturvallisuuteen kuitenkin vain vähän olemassa.
Yrityksissä on olemassa lukuisia mahdollisia haavoittuvuuksia, kuten organisatoriset, tekniset, inhimilliset ja fyysiset tekijät. Ilman oikeanlaista käsitystä haavoittuvuuksista, uhkista ja niihin liittyvistä riskeistä voivat yritykset tuhlata voimavarojaan pyrkimyksissään lieventää kyberturvallisuusriskejään. Koska teknologiaympäristö ja uhkien vektorit muuttuvat jatkuvasti, on tiedostettava, ettei absoluuttista turvallisuutta voida ponnisteluista huolimatta koskaan saavuttaa.
Suomessa oli vuonna 2013 yhteensä lähes 300 000 yritystä, joista yli 98 % oli alle 50 henkilöä työllistäviä yrityksiä. Näihin lukuihin ei sisälly maa-, metsä- ja kalatalouden aloilla toimivat yritykset. Pk-yritysten osuus kaikkien yritysten kokonaisliikevaihdosta oli samana vuonna lähes 55 %. Kun otetaan lisäksi huomioon, että pk-yritykset muodostavat merkittävän osan suuryritysten toimittajaverkostosta, on pk-yritysten kyberturvallisuudella kriittinen merkitys paitsi pk-yritysten itsensä kannalta, myös kansallisen kyberturvallisuuden kannalta tarkasteltuna.
Tällä hetkellä käytettävissä olevia tapoja tason osoittamiseen ovat esimerkiksi kansainväliseen ISO/IEC 27001 -standardiin perustuva sertifiointi tai Kansallinen turvallisuusauditointikriteeristö KATAKRI:n mukainen auditointi. Molemmat näistä ovat kuitenkin pienen yrityksen näkökulmasta aikaa vieviä, raskaita ja kalliita prosesseja, joihin monellakaan yrityksellä ei yksinkertaisesti ole mahdollisuutta eikä varaa. Tästä johtuen pk-yritysten käyttöön tarvitaan yleisesti hyväksytty kyberturvallisuuden viitekehys ja toimintamalli, jonka mukaan kyberturvallisuuden tasoa voidaan arvioida ja edelleen kehittää kattavasti ja luotettavasti. Suomessa ei tällaista arviointimallia ole vielä käytössä, mutta esimerkiksi Iso-Britanniassa on käytössä tähän tarkoitukseen soveltuva malli.

FINCSC – Finnish Cyber Security Certificate on erityisesti pienten ja keskisuurten yritysten käyttöön kehitetty malli kyberturvallisuuden tason arviointiin ja sertifiointiin.

FINCSC arviointimallin kehittäminen

FINCSC – Finnish Cyber Security Certificate on erityisesti pienten ja keskisuurten yritysten käyttöön kehitetty malli kyberturvallisuuden tason arviointiin ja sertifiointiin. Kyberturvallisuuden arviointimallin kehittäminen on perustunut tavoitteeseen, että sen kriteereihin vastaamalla yritys kykenee arvioimaan oman tieto- ja kyberturvallisuuden tasonsa sekä osoittamaan tämän luotettavasti myös asiakkailleen ja liikekumppaneilleen. Keskeiset arvot arviointimallin käytössä piilevät siinä käytettävän kriteeristön vaatimusasettelussa ja sekä koko arviointimallin kustannustehokkuudessa. Vaatimusasettelu on rakennettu vastaamaan pk-yritysten liiketoiminnan haasteisiin siten, että arviointimallin asettamien vaatimusten mukaisella toiminnalla voidaan varmistua siitä, että kyberturvallisuuteen liittyvät perusasiat ovat yrityksessä kunnossa.
Arviointimalli sekä siihen liittyvät työkalut ja toimintaprosessit on kehitetty Cyber Scheme Finland -pilottihankkeessa, joka alkoi syksyllä 2015 Keski-Suomen liiton, Teollisuuden ja Työnantajain Keskusliiton (TT) -säätiön ja Jyväskylän ammattikorkeakoulun rahoittamana. Mallin ovat yhdessä laatineet Elinkeinoelämän keskusliitto, Jyväskylän ammattikorkeakoulun IT-instituutti, TeliaSonera Finland, Viestintäviraston Kyberturvallisuuskeskus sekä 3SDL Ltd Iso-Britanniasta.
Hankkeessa tehtyyn arviointimallin pilotointiin on osallistunut parikymmentä pk-yritystä kattavasti eri toimialoilta pääasiassa Keski-Suomen alueelta. Yrityksiä on ollut edustettuina muun muassa terveys- ja sosiaalipalvelujen, metalliteollisuuden, tietotekniikan ja energiahuollon aloilta. Näillä kaikilla aloilla pilotoinnin yhteydessä saadut tulokset ovat olleet saatuun palautteeseen perustuen kaiken kaikkiaan positiivisia. Ne ovat tukeneet tavoitetta aikaansaada erityisesti pk-yrityksille suunnattu yhtenäinen kansallinen kyberturvallisuuden arviointimalli, jota FINCSC pilottihankkeen päättyessä elokuun 2016 lopussa edustaa.
FINCSC kyberturvallisuuden arviointimallia ylläpitää ja edelleen kehittää Jyväskylän ammattikorkeakoulun IT-instituutin osana toimiva, puolueeton kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTEC – Jyväskylä Security Technology. Se toimii FINCSC –arviointimallissa akkreditoivana tahona ja myös ylläpitää

ajantasaista rekisteriä FINCSC –kriteeristön mukaan sertifioiduista yrityksistä ja akkreditoiduista FINCSC -arvioijatahoista. Akkreditoiduilla FINCSC -arvioijatahoilla tarkoitetaan kaikkia niitä yrityksiä, jotka voivat hyväksyttävästi suorittaa pk-yritysten tieto- ja kyberturvallisuuden tason FINCSC -sertifiointiin liittyviä arviointitehtäviä. Pilottihankkeessa arvioijatahona toimi teleoperaattori TeliaSonera Finland Oyj, joka hankkeen päätyttyä tulee toimimaan yhtenä akkreditoituna arvioijatahona.

FINCSC -arviointimallin käyttö

Ollakseen myös pienimpien pk-yritysten saavutettavissa, tulee kyberturvallisuuden arviointimallin olla rakenteeltaan riittävän yksikertainen, sen tulee pitää sisällään kyberturvallisuuden perusulottuvuudet ja sen tulee kansainvälisesti hyödynnettävissä ja kustannuksiltaan riittävän alhainen. Näistä lähtökohdista rakennettua FINCSC kyberturvallisuuden arviointimallia käytetään verkkopohjaisen käyttöliittymän (portaalin) avulla (www.fincsc.fi). Halutessaan hankkia FINCSC -sertifikaatin, yritys lähettää portaalin välityksellä hakemuksen ja samalla sitoutuu suorittamaan arvioinnista ja sertifikaatista määritellyn maksun akkreditoidulle arvioijataholle. Yritykselle myönnetään hakemuksen perusteella portaaliin käyttäjätunnukset, joilla se saa pääsyn portaalissa olevaan kysymysaineistoon. Aineisto sisältää yrityksen perustietojen lisäksi yli 50 tieto- ja kyberturvallisuustasoa mittaavaa kysymystä. Kysymyksiin vastataan sisäisenä itsearvioinnin periaatteiden mukaan, jolloin yritys tarkastelee tieto- ja kyberturvallisuustasoaan omista lähtökohdistaan käsin. Kaikkiin kysymyksiin vastattuaan yritys lähettää kysymysaineiston akkreditoidulle FINCSC -arvioijataholle portaalin välityksellä.
Akkreditoitu FINCSC -arvioijataho käy läpi yrityksen laatimat vastaukset kullekin kysymykselle määriteltyjen kriteerien mukaisesti ja lähettää antamansa palautteen sisältävän arviointiraportin portaalin välityksellä yritykselle. Palaute antaa yritykselle suuntaviivoja kyberturvallisuuden edelleen kehittämistä varten. Mikäli yrityksen toiminta on FINCSC -arviointimallin kriteeristön mukaisella tasolla, saa yritys määräajan voimassa olevan FINCSC -sertifiointitodistuksen sekä FINCSC -sertifiointia osoittavan ”leiman”, jota yritys saa käyttää sähköisessä viestinnässään sertifikaatin voimassaoloaikana. Sertifikaatti toimii sekä asiakkaille, viranomaisille että muille yhteistyökumppaneille osoituksena kyberturvallisuuden tasosta yrityksessä.

FINCSC -arviointimallin kansainvälinen yhteensopivuus ja jatkokehittäminen

Yhtenä lähtökohtana FINCSC kyberturvallisuuden arviointimallin kehittämistyössä on ollut tukea suomalaisten pk-yritysten kansainvälistä liiketoimintaa. Tämän vuoksi mallia on alusta lähtien rakennettu tavoitteena kansainvälinen yhteensopivuus. Kehittämistyössä on hyödynnetty Iso-Britanniassa toukokuusta 2014 lähtien käytössä olleesta Cyber Essentials -arviointimallista saatuja kokemuksia. Cyber Essentials -mallia on kehitetty osana Iso-Britannian kansallista kyberturvallisuusohjelmaa yhteistyössä teollisuuden kanssa. Arviointimallin kehittäminen on ollut Iso-Britannian hallituksen vastine kasvaneelle kyberrikollisuudelle. Cyber Essentials -arviointimalli on suunnattu sekä pienille ja suurille yrityksille toimialasta katsomatta.
Arviointimallin käyttö Iso-Britanniassa perustuu lähtökohtaisesti vapaaehtoisuuteen, mutta sen mukainen sertifiointi on edellytyksenä 1.10.2014 jälkeen julkaistuissa valtion keskushallinnon järjestämissä kilpailutuksissa. Sertifiointia vaaditaan, mikäli toimitussopimukseen sisältyy joko henkilötietojen tai sensitiivisten tietojen käsittelyä taikka tiettyjä ICT -tuotteita ja palveluja. Iso-Britanniassa Cyber Essentials ja Cyber Essentials Plus -sertifikaatteja on arviointimallin heinäkuun 2016 puoleen väliin mennessä myönnetty jo lähes 1900 yritykselle. Yritysten sertifioinneista Iso-Britanniassa vastaavat akkreditoidut arvioijatahot (Assessor Bodies). Yksi näistä tahoista on Cyber Scheme Finland -pilottihankkeen toteutukseen osallistunut brittiläinen turvallisuus- ja puolustusalan konsultointiyritys 3SDL Ltd, joka on ollut omalla kokemuksellaan ja panoksellaan edesauttamassa arviointimallin rakentamista Suomeen. Suuryrityksen tai julkisen organisaation alihankkijana toimivan yrityksen tekemä itsearviointi ei välttämättä ole riittävä tae yrityksen kyberturvallisuuden tasosta, mikäli kyse on esimerkiksi huoltovarmuuskriittisestä toimialasta. Tämän vuoksi tarvitaan jo rakennetun FINCSC perustason arviointimallin lisäksi arviointimalli, jossa yrityksen kyberturvallisuuden taso todennetaan auditointikäynnin avulla. Tämä luonnollisesti nostaa sertifioinnista yritykselle aiheutuvia kustannuksia, mutta niiden tulee jäädä huomattavasti edellä mainitun ISO/IEC 27001 -standardiin perustuvan sertifioinnin tai KATAKRI:n mukaisen auditoinnin kustannustason alapuolelle. Tämän niin sanotun FINCSC PLUS -tason arviointimallin kehittämistyö käynnistyy syyskuun 2016 alussa alkavassa hankkeessa Jyväskylän ammattikorkeakoulun IT-instituutin ja sen yhteistyökumppaneiden voimin. Mallin kehittämisen lisäksi hankkeessa varmistetaan Cyber Essentials/Cyber Essentials Plus ja FINCSC/FINCSC PLUS -arviointimallien keskinäinen yhteensopivuus, vahvistetaan arviointimallia sen kaikilla toiminnallisilla tasoilla sekä levitetään tietoisuutta arviointimalleista erityisesti pk-yrityksille mutta myös suuremmille yrityksille. Tavoitteena on, että Suomessa myönnetty tieto- ja kyberturvallisuuden tason FINCSC -sertifiointi on pätevä myös kansainvälisillä markkinoilla ja tunnustetaan muun muassa Iso-Britanniassa.

Lisätietoja
Lisää pk-yritysten kyberturvallisuudesta ja kyberturvallisuuden FINCSC -arviointimallista voi esimerkiksi kuulla Jyväskylässä 2. – 3.11.2016 järjestettävillä Kyberturvallisuusmessuilla. Messuilla aiheista ovat kertomassa yritysturvallisuusasiantuntija Mika Susi Elinkeinoelämän keskusliitosta ja Cyber Scheme Finland –pilottihankkeen ja FINCSC PLUS –hankkeiden projektipäällikkö, kyberturvallisuuden lehtori Mika Karjalainen Jyväskylän ammattikorkeakoulun IT-instituutista. Lisätietoa messujen ohjelmasta ja näytteilleasettajista on löydettävissä kyberturvallisuusmessujen kotisivuilta osoitteesta http://www.kyberturvallisuusmessut.fi/.

Analysaattori

Peliä ja politiikkaa

Nämä syyskuun Viestimiehen jutut ovat siinäkin mielessä kiehtovia kirjoitettavia, että näitä naputellaan juuri heinäkuussa, joka on tyypillisesti hiljaista uutisaikaa. Tänä kuluneena kesänä ei kuitenkaan ole ollut yhtään hiljaista hetkeä. Englannin EU-ero, USA:n presidenttiehdokkaiden valinnat, Istanbulin, Nizzan ja Saksan terrori-iskut ja Turkin vähintäänkin erikoinen vallankaappausyritys ovat olleet otsikoissa ja mielissä kesän mittaan. Positiivisia uutisia on ollut ehkä vain yksi, jos sellaiseksi lasketaan Venäjän järjestelmällisen doping-ohjelma, joka aiheutti niin paljon positiivisia tuloksia että itänaapurin urheilijat suljettiin pääosin pois Rion Olympialaisista. Eurooppaa ja sen yhtenäisyyttä on tänä kesänä koeteltu tosissaan eikä loppua ole näkyvissä. Ennustan että samanlaisena tämä jatkuu vaikka tällä kertaa olisin kyllä mielelläni väärässä. Tässä jutussa tarkastellaan kuitenkin näihin surullisiin tapahtumiin ja muihinkin tämän kesän ilmiöihin liittyviä osatekijöitä, jotka liittyvät jotenkin sähköiseen tiedonvälitykseen.

Tietoyhteiskunta eri muodoissaan on näytellyt isoa osaa kesän tapahtumissa. Hakkerit pääsivät käsiksi USA:n demokraattipuolueen rahankeruujärjestön aineistoihin ja puolueelta väitettiin jo aikaisemmin kadonneen läjäpäin sähköposteja. Molemmista tempuista syytetään Venäjää ja Donald Trump pyysikin jo Venäjää ”löytämään” ne Hillary Clintonilta kadonnet postit. Tuntuukin siltä että Putin pyrkisi vaikuttamaan USA:n presidentin valintaan. Ei liene yllätys, että Putinin suosikki näissä karkeloissa on juuri Trump, näillä herroilla kun on muutenkin samaa suuruusluokkaa oleva testosteronin tuotanto ja todennäköisesti sama mediakonsultti.

Sosiaalisen median rooli puolestaan on nykyään iso kaikissa tapahtumissa. Esimerkkinä mainittakoon Brysselin terrori-iskut ja niitä seurannut ajojahti, jonka aikana Belgian viranomaiset pyysivät, etteivät ihmiset raportoisi jokaisesta hälytysajoneuvosta tai poliisiyksiköiden liikkeistä, jotta jahdin kohteena olleet terroristit eivät saisi liikaa tietoja tilanteesta. Näin siis Belgiassa, Turkissa toimittiin hiukan toisin. Heti vallankaappausyrityksen alkuvaiheessa sosiaalinen media suljettiin kokonaan. Tai ainakin yritettiin, sillä täysin se ei onnistunut, joka kertoo myös jotain siitä miten monimuotoisesti tieto liikkuu verkoissa. Hieman myöhemmin Turkki blokkasi myös Wikileaksin sivuston jossa oli juuri julkaistu noin 300 000 sähköpostia jotka kuuluivat AKP-puolueelle, joka on siis preidentti Erdoganin puolue. Tästäkin uutisoitiin laajasti ja vastavetona Turkin viranomaiset sitten sulkivat 16 televisiokanavaa, 23 radiokanavaa ja 45 sanomalehteä.

Näissä USA:n ja Turkin tapahtumissa on se matemaattinen eroavaisuus, että USA:ssa tehdään jakolaskua ja Turkissa yhteenlaskua. USA:n aikaisempi kaksipuoluejärjestelmä näyttää jakaantuvan neljään osaan kun taas Turkissa ei tämän vallankaappausnäytelmän jälkeen ole jäljellä kuin yksi isäntä.

Ranskassa otettiin kesän Jalkapallon EM-kisojen yhteydessä käyttöön SAIP-järjestelmä, jonka tarkoituksena on antaa varoitus matkapuhelimeen jos käyttäjän lähistöllä on menossa jotain vaarallista tai epäilyttävää. Nizzan iskun yhteydessä tämä hälytys aktivoitiin, mutta se saavutti käyttäjät vasta kolme tuntia myöhemmin. Vika ei ollut Hardwaressa eikä Softwaressa vaan sovelluksen kehittäjäyhtiö Deverywaressa. Virallinen selitys on tietysti tekninen vika, ja todellinen syy huonolaatuinen koodi tai riittämätön testaus, nämä molemmat tunnetusti Analysaattorin lempiaiheita. Onhan toki mahdollista että viiveen aiheutti myös inhimillinen virhe. Joku ei vaan osunut hiirellä ihan kohdalleen eli vika olisikin ollut siis Humanwaressa.

Näin voisi kyllä sattua myös meillä täällä Suomessa. Onnettomuustutkimuskeskus suoritti laajan tutkinnan junaliikenteen turvallisuudesta joka koski erityisesti ”virheellisten kulkuteiden syntymiseen vaikuttavia tekijöitä”. On muuten hieno kiertoilmaisu, jolla tarkoitetaan siis sitä, että tutkitaan miksi junia kulkee väärillä raiteilla. Tutkimuksen mukaan yksistään viime vuonna Suomessa näin tapahtui yli sata kertaa ja suurin osa johtui käsiohjauksessa tapahtuneesta virheestä. ”Pääsääntöisesti kyse on hiirellä klikkaamisesta ja silloin saattaa sattua sellainen lipsahdus, että painetaan väärää kohtaa. Tai ei muisteta, että tällä kertaa pitikin tehdä näin”, johtava tutkija Esko Värttiö selittää. Tutkimus jäi myös hieman vajavaiseksi, sillä sen aikana voimassa ollut Liikenneviraston rautatieliikenteen ohjauksen käsikirja oli luokiteltu salassa pidettäväksi, mikä rajoitti sen hyödyntämistä tutkinnassa.

Kuluneen kesän merkittävin ilmiö monessakin mielessä ja ihan maailmanlaajuisesti lienee ollut Pokémon Go-pelin valtava suosio. Siinä kun pelaajat kulkevat ihan oikeasti ulkona ja metsästävät näitä Pokémon-hahmoja älypäätelaitteellaan aidolla karttapohjalla. Kukaan ei ole voinut välttyä huomaamasta tätä liikehdintää ja onhan sillä merkittäviä vaikutuksia jos se on saanut nämä ex-sohvaperunat kävelemään kilometrikaupalla. Törmäilyä, kompurointia ja erilaisia onnettomuuksia on tapahtunut paljon. Baltimoressa eräs pelaaja jahtasi autoillessaan haluttua Pikachu-hahmoa ja onnistui törmäämään suoraan poliisiauton kylkeen. Tarina ei kerro olivatko konstaapelit juuri siinä kohdassa suorittamassa virkatehtäviään

vai olivatko he mahdollisesti itsekin jäljittämässä Pikachua. Ihmisiä on kävellyt mereen ja tullut ryöstetyksi, Pokémon-hahmoja on etsitty sairaaloista, kirkoista ja yksityisalueilta kuten Floridassa, jossa talonomistaja yritti ampua pihalleen ilmestyneet pelaajat. Epäilen että tämä kaikki on kuitenkin vasta alkua, joten jäädään odottelemaan onnistuuko joku järjestämään itsensä hengiltä niin komeasti, että pääsisi kisailemaan vuotuisesta Darwin Awards -palkinnosta. Pelistä uutisointi onkin ollut usein huumorilla sävyttynyttä. Aina ei välttämättä ole ollut aihetta naureskeluun, sillä esimerkiksi Bosniassa pelaajia on kulkenut merkityillä ja aidatuilla miinakentillä. Israelin armeija puolestaan kielsi pelin pelaamisen tukikohdissaan tietoturvasyistä johtuen siitä, että sen pelätään aiheuttavan tietojen vuotamista luokitelluista kohteista. Pelatessaan joutuu käyttämään puhelimen kameraa ja ottamaan kuvia joihin tallentuu myös paikkatietoa. Vastaavien sovellusten ja palveluiden käyttöä varuskunnissa on samoista syistä rajoitettu myös Suomessakin Puolustusvoimien toimesta.

Tästä Pokémon Go-pelistä ollaan jo hyvää vauhtia tekemässä erilaisia versioita. Harry Potter Go on tulossa ja itänaapurissa elokuun aikana julkaistaan uusi versio Pokémon Go-pelistä, jossa näiden nykyisten hahmojen sijasta pyydystetäänkin kuuluisia venäläisiä hahmoja. Listalla ovat ainakin Juri Gagarin, Venäjän tsaarit, Aleksander Pushkin, Pjotr Tsaikovski ja Napoleon Bonaparte. Analysaattorin käsityksen mukaan Napoleon ei ole venäläinen, mutta ottaen huomioon itänaapurin voimapolitiikan lienee kuitenkin viisainta tarkentaa, että Napoleon ei ole venäläinen, ainakaan vielä, vaikka hän ponnekkaasti sinne aikoinaan pyrkikin. Analysaattorikin tulee julkaisemaan oman versionsa tästä menestysformaatista ja sen nimeksi tulee Äly Go. Arvaattekohan mitä siinä jahdataan?

Pokémon Go:n tietoturvasta on muutenkin noussut kohu, sillä Google-tilin kautta kirjautuva pelaaja on joutunut antamaan melko laajat oikeudet sähköpostiensa ja Googlen hakuhistoriansa käyttöön. Koskapa pelin kehittäjäyhtiö Niantic väittää, ettei sitä kiinnosta pelaajan henkilökohtainen aineisto, jäljet johtavat tutulle sylttypurkille, eli Googleen. Jännityksellä jäämme odottamaan kuinka tämä soppa kehittyy ja koska joku vuotaja taas kertoo kuinka noita tietoja on käytetty.

Ja kun nyt tuli puheeksi niin olenkin tässä hämmästellyt erästä Googlen uusinta liikenneturvallisuuteen liittyvää keksintöä. Google on patentoinut keksinnön, jonka ansiosta auton konepellistä purskahtaa jotain tökättiä onnettomuustilanteessa, ja sen ansiosta jalankulkija, jonka yli on siis juuri ajettu, liimautuu siihen auton konepeltiin eikä lennä katuun kuten siinä yleensä tuppaa tapahtumaan. Periaatteessa tämä kuulostaa aika hyvältä, joskin Analysaattori haluaisi huomauttaa parista yksityiskohdasta. Ensimmäiseksi tietysti tulee mieleen, että kai se kuitenkin vähän sattuu, kun siihen konepellille mätkähtää, joten ei tällä keksinnöllä ihan mullistavia vaikutuksia jalankulkijan turvallisuudelle ole. Toinen juttu joka tulee mieleen että mitähän mahtaisi tapahtua hirvikolarissa? Ettäkö se 700 kiloinen hirvisonni ihan oikeasti jämähtää konepeltiin kiinni sillä liimalla? Ja jos jämähtää, niin onko se hyvä asia? Ja kysyn vaan, että miten se joka/mikä on siihen konepellille liimautunut, saadaan siitä sitten irti. Sehän se kai kuitenkin on tarkoitus, ja jos se liima kestää onnettomuudesta syntyvän kiihtyvyyden niin ei se vissiin sitten ihan vaan nyppäämällä irtoa. Epäilen, että keksinnöllä pyritäänkin vain pönkittämään itse itseään ajavan Google-auton kehitystä. Jos vaikka kävisi niin onnettomasti, että joku jäisi sellaisen auton yliajamaksi.

Kesän mittaan olemme saaneet lukea useitakin suru-uutisia, sillä moni tuttu asia on tullut tiensä päähän. VHS-videonauhureiden valmistus lopetetaan ja painettujen puhelinluetteloiden julkaiseminen lopetetaan. Näistä molemmista takaiskuista olen jo melkein päässyt yli mutta tieto viimeisimmästä vainajasta on vavisuttanut rajusti suomalaisia, etupäässä miehiä. Armeija nimittäin luopuu yhdestä peruskoulutuksen kulmakivistään. Tulevassa palvelusohjesäännössä ei enää ole mainintaa varusmiesten sängyissä olevan päiväpeitteen taittamisesta, eli pinkan tekemisestä: R.I.P. Pinkka. Kukaan ei jää sinua kaipaamaan, mutta olisihan tulevienkin saapumiserien pitänyt saada sinuun tutustua. Analysaattori puolestaan odottaa uutta yleistä palvelusohjesääntöä mielenkiinnolla, sillä onhan siinä varmaan jotain todettu päiväpeiton säilytyksestä, eli juuri siitä miten pinkka korvataan.

Todella huonojen uutisten sävyttämä kesä kääntyy loppuaan kohti ja yllättäen tämän synkän uutisvirran seasta löytyi lähes hyväksi tulkittava uutinen. Uutinen Venäjältä kertoo että turvallisuuspalvelu FSB toimitti oikeuteen tutkintaviranomaisia joita syytettiin miljoonan dollarin katoamisesta. Mikähän tässä nyt sitten oli se hyvä uutinen? No, sehän on tulkinta, jonka on tehnyt venäjän tuntija Mark Galeotti. Hänen mukaansa uutinen osoittaa, että Venäjälläkään ei enää suvaita ihan mitä tahansa ja varastamiselle ja epäpätevyydelle on lopultakin asetettu rajat. Ja jos se ei ole hyvä uutinen, niin on se ainakin pieni ele oikeaan suuntaan. VM

TEKSTI JA KUVAT: JYRKI PENTTINEN

Kyberin jäljillä

TkT, ins-ltn (res.) Jyrki Penttinen on työskennellyt operaattoreiden ja laitevalmistajien palveluksessa Suomessa, Espanjassa, Meksikossa ja Yhdysvalloissa, ja on vapaa-ajallaan aktiivinen tietokirjailija. Penttinen toimii nykyään matkaviestinnän tietoturva-asioiden parissa USA:ssa. Lisätietoa artikkelin aihepiiristä löytyy Penttisen uusimmasta kirjasta "Wireless Communications Security", joka julkaistaan tämän vuoden aikana.

Kyber on jo vakiintunut sanastoomme sen verran aktiivisesti, että siitä kuulee lähes päivittäin. Terminä se on kuitenkin varsin moniselitteinen. Artikkelin tavoitteena on selvittää, mitä kyber on erityisesti maanpuolustuksen näkökulmasta.

Johdanto

Olemme siirtymässä määrätietoisesti kohti pysyvästi tietoliikennetekniikoilla kytkettyä yhteiskuntaa, joka tarjoaa meille pääsyn lähes äärettömän laajoihin tietosisältöihin ajasta ja paikasta riippumatta. Yksi merkittävistä digitaalisen maailman virstanpylväistä on langattomien tietoliikennetekniikoiden ja -verkkojen kehittyminen, mikä on mahdollistanut matkaviestinnän muuttumisen entisaikojen harvojen luksuksesta meidän kaikkien päivittäispalveluksi. Mobiilidataviestinnän suosio on kasvanut eksponentiaalisesti tiedon hakuun ja jakoon. Samalla uusien tekniikoiden myötä on kasvanut täysin uusi käyttäjäsukupolvi, joka ei tyypillisesti edes halua suojata henkilökohtaista viestintäänsä, vaan kaikenlaista tietoa jaetaan avoimesti. Kehittyneet tekniikat ja niiden ennakkoluulottomat käyttäjät ovat itse asiassa muokanneet yhteiskuntia ja kulttuureita varsin merkittävällä tavalla, ja uudet viestintätavat kuten kansalaisten sosiaalisten medioitten ex tempore -viestit riippumatta lukijoiden sosiaalisesta taustasta aina valtiopäämiestasolle saakka ovat nykyään melkein sääntö kuin poikkeus.

Laaja, edistyneiden palveluiden käyttöönotto ja niiden innovatiiviset käyttöliittymät ovat avanneet uusia tapoja jakaa viestejä ja uutisia joka maailman kolkkaan käytännössä reaaliaikaisesti. Samalla yhä avoimempi käyttöympäristö voi myös paljastaa merkittäviä turvallisuuspuutteita, jotka vaarantavat luottamuksellisia tietoja ja käyttäjien profiileita.

Ei pelkästään henkilöiden välinen liikennöinti ole muuttumassa, mutta myös informaatioyhteiskunta kokonaisuudessaan on merkittävän uudistuksen kohteena. Esineiden Internet (IoT, Internet of Things) on kehittymässä vahvasti ja tulee tarjoamaan uusia ja automaattisia tapoja kytkeä tietoliikenneverkkojen kautta laitteita, palveluita ja henkilöitä ennennäkemättömällä tavalla.

IoT on yhtä laaja käsite kuin termi antaa ymmärtää. Se sisältää suuren joukon kaikenlaisia tietoverkkojen kuten julkisen Internetin kautta kytkettyjä laitteita. Niiden joukossa on valvontakameroita, kodinkoneita, tulostimia, sensoreita, itseohjaavia ajoneuvoja ja telematiikkalaitteita, jotka kommunikoivat joko toistensa tai niihin liittyvien järjestelmien kanssa ja voivat tehdä itsenäisesti mittauksia, päätelmiä ja toimintoja. IoT:n perusidea on mahdollistaa aktiivisena toimivien ja kytkettynä olevien laitteiden saumaton liikennöinti, joka puolestaan tekee meidän kansalaisten elämän nautittavammaksi ja tehokkaammaksi. Laitteiden Internetissä on kyse siis tietoyhteiskunnan murroksesta ja siirtymisestä kohti aina verkkoihin kytkettynä olevaa yhteiskuntaa.

IoT tarjoaa uusia mahdollisuuksia erityisesti koneiden väliseen liikennöintiin (M2M, Machine to Machine), jolla voidaan paremmin hallita ja koordinoida niiden tehtäviä ilman ihmisen toimia. On huomattavaa, että M2M on IoT:n osajoukko. IoT voidaan puolestaan määritellä joukoksi *objekteja, jotka voivat edustaa itseään digitaalisesti ympäristölleen ja tulevat niin ollen osaksi laajempaa kokonaisuutta*. Tarkemmin sanottuna, IoT-objekti kytkeytyy muihin lähiobjekteihin ja tietokantoihin siten, että siitä tulee osa kokonaisuutta lisäten sen yhteisarvoa enemmän kuin mitä pelkkä summa erillisistä objekteista tarjoaisi. Tämä on kiehtovaa, sillä kun tällainen joukko kehittyneitä IoT-laitteita sensoreineen toimii koordinoidusti ja tietoisesti lähiseudun tapahtumista, ne muodostavat samalla eräänlaista *ympäristöälykkyyttä*.

Yksi esimerkki tästä on IoT-sensoriverkon omatoimisesti havaitseva auto-onnettomuus, joka johtaa kulkuväylän tukkimiseen. Sensori saattaa ensin tehdä paikallisesti alustavan analyysin keräämänsä tiedon perusteella ja lähettää viestin edelleen muiden osapuolien tiedoksi sen perusteella, miten oleellisiksi sensori toteaa vastaanottajat kyseiseen tapahtumaan. Siten sensori voi tiedottaa lähiseudun lentokenttiä potentiaalisista matkustajien viivästyksistä, jotta lentoyhtiöt voivat varata ajoissa varareittejä. Samoin sensori voi varoittaa lähiseudun hotelleja, jotka voivat varautua lisääntyneisiin asiakasmääriin. Maanpuolustuksen näkökulmasta taistelijoiden varustukseen kuuluvat ja kentällä sijaitsevat älykkäät IoT-sensorit voivat mahdollistaa tilannekuvan lisäksi arvokasta lisäarvoa reaaliaikaisessa tuessa joukkojensiirtopäätöksille. Sensoreiden ja muiden IoT-laitteiden mahdollistaman tietomäärän ansiosta IoT liittyy läheisesti myös datalouhintaan, pilvipalveluihin ja ison datan tekniikoihin. IoT-laitteiden datavirtojen

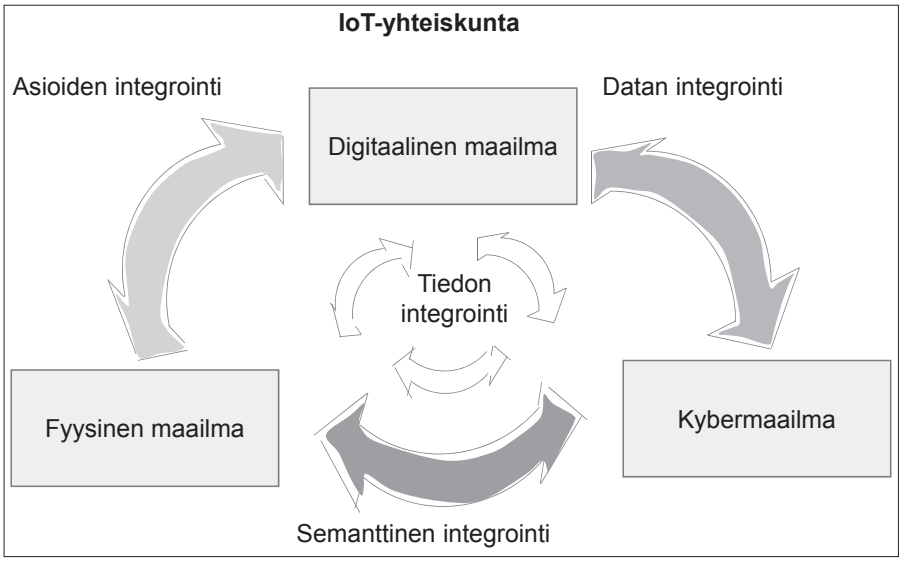
suodatuksella ja analysoinnilla voi olla merkittäviä tulevaisuuden etuja monessa ympäristössä niin puolustusvoimissa kuin siviilissä.

Parhaillaan tapahtuvan tuotekehityksen tuloksena saatamme nähdä pian täysin uudentyyppisiä koneita, sensoreita ja muita laitteita niin kuluttajamarkkinoilla kuin laitteiden ja palveluiden välisessä viestinnässä. Uusien laitetekniikoiden myötä on oletettavaa, että myös innovatiiviset tietoturvauhkat lisääntyvät. Uhkat voivat johtaa käyttäjän identiteetin paljastumiseen, mikä puolestaan vaarantaa luottamuksellisen tietosisällön ja voi vahingoittaa yksittäisiä käyttäjiä tai kokonaisia yhteiskuntia taloudellisesti, poliittisesti tai muulla tavoin. Yksilön kannalta uhkakuva voi olla pahimmillaan terveyteen tai jopa henkeen liittyvä, esimerkiksi lääketieteellisten, elintoimintoja ylläpitävien laitteiden vaurioittamisen kautta. Yksi tyyppiesimerkki hengenvaarallisista riskeistä liittyy itseohjaaviin ajoneuvoihin niihin kohdistuvien kyberhyökkäyksien tuloksena.

Kansalaisten suojaaminen tällaisilta vaaroilta on haastavaa uusien kehittyneiden kyberhyökkäystekniikoiden myötä. Vastatoimiin voivat kuulua jatkuva kybervalvonta yhteistyökumppaneiden ollessa yksittäisiä kansalaisia, hallituksia tai kokonaisia pankkilaitosten ekosysteemejä, tuoteketjuja, puolustusvoimia sekä opetuslaitoksia. IoT:n roolin muuttuessa yhä tärkeämmäksi, se voidaan mieltää sensoriverkkoineen perustavaa laatua olevaksi kybermaailman elementiksi, ja siten siihen liittyvän tietotaidon ylläpitäminen sekä sen suojaaminen kaikilla tasoilla on yhä oleellisempaa.

Mitä kyber on?

Kyber (eng. cyber) on erittäin laaja käsite, ja se voi liittyä moneen ympäristöön esimerkiksi tekniikan ja kulttuurin aloilla. Kyber voi sisältää tuttuja elementtejä päivittäisestä elinympäristöstämme mukaan lukien tietoverkot kuten Internet, matkaviestintä ja langalliset telejärjestelmät, ja se voi liittyä myös tietokonemaailmaan sekä sen sisäisiin ja ulkoisiin dataverkkoihin. Toisaalta näiden tuttujen ja näkyvien ympäristöjen lisäksi kyber voi liittyä oleellisesti



Kybermaailma on osa IoT-yhteiskuntaa, jonka muina komponentteina ovat fyysinen ja digitaalinen maailma.

salaisuuksiin, niiden suojaukseen sekä niiden hyökkäys- ja paljastusyrityksiin. Kyber voi myös liittyä keinoälyyn, joka on pohjana itsenäisesti toimiville ja ajatteleville koneille kuten autonomisesti liikkuville roboteille. Kyber on siten läsnä oikeastaan kaikilla yhteiskunnan tasoilla ml. henkilökohtainen elämämme, hallitukset, yritykset, pankit ja puolustusvoimat.

Nykyinen IoT-ympäristö voidaan tulkita joukoksi sekä passiivisia että aktiivisia fyysisiä objekteja, jotka ovat osa tietoverkkoja joustavalla ja huomaamattomalla tavalla. Nämä objektit osallistuvat osaltaan kokonaisten järjestelmien toimintaan ja auttavat monissa jokapäiväisissä toiminnoissa kuten oppimisessa, terveydenhuollossa, telematiikassa ja yritysmaailmassa. IoT raivaa tietä kohti täysin uutta yhteiskuntaa joka yhdistää perinteisen, fyysisen maailman siten kun me sen koemme ja näemme sekä digitaalisen maailman, jossa tietoa varastoidaan ja siirretään, ja virtuaalisen kybermaailman.

Yhtä lailla kuin kyber yleisesti ottaen, myös termi *kyberturvallisuus* on hyvin laaja ja sisältää monenlaisia tietoturvaan liittyviä riskejä kuten kyberhyökkäyksen ja siltä suojautumisen. Kyberturvallisuuden yksiselitteinen määritys on siten haastavaa. Yksi monista yritelmistä koostaa se kompaktiin muotoon löytyy dokumentista *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Se kuvaa kyberoperaation maanpuolustusnäkökulmasta. Lähteen mukaan yksi kybersodankäynnin tärkeimpiä näkökohtia on se, että sillä voidaan aiheuttaa henkilövahinkoja ja hengenmenetyksiä, tai sillä voidaan vaurioittaa ja tuhota fyysisiä kohteita eli objekteja. Lisäksi, laaja kyberhyökkäysten valikoima voi sisältää tietosisältöön tunkeutumisen, tietojen keruun ja tallentamisen, vakoilun, tiedon poiston, tuhoamisen, varastamisen ja manipuloinnin, laitteiden ja järjestelmien kontrollin ja haltuunoton sekä niitä käyttäen esimerkiksi kineettisen kontrollin käytön, laitteiden, omaisuuden ja kriittisen infrastruktuurin tuhoamisen, sekä yleisesti yksilön ja yhteiskunnan vahingoittamisen. Näihin toimiin tarjoaa vastatoimia kyberturvallisuus.

Kyberhyökkäys voidaan kategorisoida kolmeen komponenttiin, jotka ovat **tiedon keruu** (jolla saavutetaan looginen tai fyysinen pääsy, ajetaan koodia ja ymmärretään kohteen ympäristötekijät), **kyberaseet** (jotka tyypillisesti ovat kohdespesifisiä ja aktivoidaan erityisesti suunniteltujen personoitujen kriteerien perusteella) ja laskelmoitu **inhimillinen päätös**. Näiden kolmen tekijän yhdistelmää voidaan kutsua kybervoimaksi, joka on nykyään oleellinen osa moderneja asevoimia.

Inhimillisesti ajateltuna, kyberhyökkäyksellä voi olla kahdenlaisia seurauksia: niitä, joilla on väkivallaton vaikutus yhteiskunnan toimintaan (eli toisin sanoen kyseessä on eräänlainen virtu-

aalinen tuho), ja niitä, jotka johtavat fyysiseen tuhoon ja henkilövahinkoihin. Klassinen esimerkki kyberhyökkäyksestä on vuonna 2010 toteutettu ydinlaitosonnettomuus Stuxnet-viruksen avulla siten, että se kohdisti vaikutuksen spesifisiin sentrifugeihin, mikä johti niiden hallitsemattomaan (tai hyökkääjän näkökulmasta suunniteltuun) kiihtymiseen ja tuhoon tartunnan saaneissa tuotantolaitoksissa. Tämä esimerkki antaa kuvaa hyökkäysten potentiaalista ja tuhovoimasta fyysisessä maailmassa. Fyysisen vaikutuksen lisäksi hyökkäys voi johtaa myös laajoihin ja pysyviin digitaalisen maailman tietovarastojen tuhoihin.

Suojausmotivaatio

Kyberhyökkäykset ovat realiteetti ja niiden merkitys tulee kasvamaan lähivuosien kuluessa. Ne eivät ole ainoastaan puolustusvoimien näkökohta, vaan ne vaikuttavat myös kaikilla siviiliyhteiskunnan tasoilla, ml. henkilökohtainen turvallisuus. Suojaamaton ympäristö voi johtaa katastrofaalisiin seuraamuksiin niin yksilötasolla kuin organisaatioissa, ja voi vavisuttaa jopa yhteiskuntien taloudellista perustaa. Siksi kaikkien tasojen on syytä olla riittävän hyvin suojattu kyberhyökkäyksiä vastaan, ml. kotiympäristön tavanomaiset IoT-laitteet (jotka usein ovat vaarallisimpia heikon suojatason vuoksi), ja toisessa ääripäässä kaikkein kehittyneimmät ammattimaisten kyberarmeijoiden laitteet.

Standardointi

Kyberuhkat edustavat niin kehittynyttä ympäristöä verrattuna "perinteisiin" krakkerimenetelmiin, että niitä on otettu erityisesti huomioon myös kansainvälisessä standardointityössä ja kansallisissa regulaattoriympäristöissä.

Esimerkiksi ISO (International Standardization Organisation) on todennut, että kyberuhkat ovat olleet todellisuutta ja ovat edelleen vaara niin hallituksille ja talousjärjestelmille kansainvälisellä tasolla. Uhkakuvat kasvavat edelleen kyberrikollisten tietotaidon ja työkalujen kehittyessä sekä hyökkäysten keskittyessä. Siksi ISO on muiden mukana kehittämässä kansainvälisiä suojausperiaatteita. Esimerkkinä ISO/IEC 27001 kuvaa hallintakehyksen riskien evaluointiin ja suojaukseen, ml. kyberorientoituneet hyökkäykset, jotka vaarantavat liiketaloutta, poliittisia järjestelmiä, hallituksia ja kansallisia infrastruktuureita. ISO tuottaa myös muita kyberiin liittyviä standardeja, joista esimerkkinä on ISO 15408 (Common Criteria) suojaustasojen evaluoinnin kuvaamiseen.

Toinen merkittävä standardointielin, joka on ottanut kyberin huomioon, on ETSI (European Telecommunications Standards Institute). Konkreettisena esimerkkinä ETSI on perustanut työryhmän Cyber Security Technical Committee (TC CYBER) vuonna 2014. Sen päämääränä on mahdollistaa suojausmenetelmiä ja –ratkaisuja lisääntyvien Internet-kyberhyökkäysten varalle. Työryhmä myös tarjoaa keskitetyn asiantuntijuuden muille standardointielimille.

Myös monissa muissa standardointityöryhmissä on kyber otettu huomioon yhtenä tärkeänä osana televiestinnän ja IT-maailman kehittyessä. Eräitä esimerkkejä ovat NERC (North American Electric Reliability Corporation) kriittisen infrastruktuurin suojaamiseen, ja NIST (National Institute of Standards and Technology), joka keskittyy suojauksen hallintaan. Myös IETF (Internet Engineering Task Force) on oleellisessa roolissa, ja on julkaissut esimerkiksi Site Security Handbook –dokumentin (RFC 2196). ISA/IEC (International Society for Automation / International Electrotechnical Commission) on puolestaan julkaissut 62443-sarjan standardit, jotka kuvaavat teollisten automaatio- ja kontrollijärjestelmien suojatun käyttöönoton (Industrial Automation and Control System, IACS).

Kyber on siis otettu huomioon varsin monessa standardointiorganisaatiossa. Varsinaista kyberin määritystä haettaessa, jatketaan vielä hetki termin historiassa.

Kyberin juuret ja kehitys

Julkisuudessa esiintyvien moninaisten kyberiin liittyvien uutisten vilistessä silmissä voidaan miettiä, mistä termi yleensä juontaa juurensa. Tilanne on hämmentävä, koska kyberiä on käytetty etuliitteenä mitä mielikuvituksellisimmissa yhteyksissä, mukaan lukien "kyberpunk", "kyberavaruus" ja "kybersota".

> *"Mikä sinä olet?"*
> *"Johan vastasin kysymykseesi," tuhahti kone, selvästi ärsyyntyneenä.*
> *"Tarkoitan, oletko sinä ihminen vai robotti?" Klapaucius selvensi.*
> *"Ja mikähän, sinun mukaasi, onkaan niiden ero?" totesi kone.*
> *(Stanislaw Lem, Kyberias)*

Kyberin juuret juontavat antiikin Kreikkaan, missä siitä käytettiin termiä "". Sana kuvasi niihin aikoihin johtamista ja hallintaa. Niiden aikojen poliittisissa yhteyksissä käytetty termi on sittemmin kokenut uusrenessanssin, ja sen merkitys muuttui varsin radikaalisti 20. vuosisadan puolivälin kieppeillä, jolloin sitä käytettiin perustana muodolle *kybernetiikka* (cybernetics). Termillä pyrittiin kuvaamaan sen aikaisia yhdistelmätutkimuksia liittyen elävien olentojen ja koneiden kommunikointiin ja kontrollijärjestelmiin. Kyseiset tutkimukset sisälsivät varsin poikkitieteellisiä tutkimusaiheita niin insinööritieteiden kuin biologian ja sosiaalitieteiden saralla, joten termi yhdisti loogisesti yhteistyön idean.

Pian sen jälkeen, kyber herätti terminä mielenkiintoa laajemmin, ja sitä alettiin käyttää kaikenlaisen teknisen edistyksen kuvaamiseen painottaen erityisesti kehittynyttä tulevaisuutta, mutta kuitenkin siten, että sitä ei määritetty sen tarkemmin. Joitakin aktiivisimpia osapuolia terin käyttöönotossa olivat populaarikulttuurin tieteiselokuvat ja –kirjallisuus. Monien sen aikaisten klassisten teosten ohella erinomainen esimerkki on Stanislaw Lemin "Kyberias", joka sisältää kiehtovia tarinoita roboteista ja keinoälystä. Toinen esimerkki on Star Trek –elokuvien Borgin hahmo, joka esittää kyberneettistä, orgaanista pseudo-oliota, tai kyborgia. Siispä kyber-termiä on käytetty perustana kuvaamaan ihmisen kaltaisesti toimivia robotteja tai androideja, jotka ovat kykeneviä kommunikoimaan, ajattelemaan, tekemään päätöksiä ja toimimaan sen mukaisesti – eli keinoälyllä varustettuja koneita.

Koneiden keinoälyyn liittyvä kehitys on sittemmin ollut sen verran vauhdi-

kasta, että se on herättänyt jopa vakavaa henkilöturvallisuuteen liittyvää huolta monella tasolla, kuten professori Steven Hawking on indikoinut mahdollisten vikatapausten esiintymisestä meitä viisaampien koneiden kontrollin pettäessä.

Vaikka kybernetiikan saralla on varmasti huolenaiheita, olemme vielä varsin alkeellisella tasolla vakavimpien riskien realisoitumiseen. Siitä huolimatta on varmasti tärkeää sopia kansainvälisesti pelisäännöistä keinoälyn edelleen kehittämisessä, jotta elokuvien pessimistisimmät kauhukuvat eivät toteutuisi koneiden alkaessa hyökkäilemään ihmisten kimppuun. Toisaalta, aihe avaa valtavasti positiivisia mahdollisuuksia, joilla ihmisten elämää helpotetaan, joten vielä meidän Viestimies-lehden lukijoiden elinaikana ei olisi mikään ihme nähdä robotteja vaeltelemassa itsenäisesti kaduilla vaikkapa lähipuodin ostoskasseja kantamassa perustuen kodin IoT-jääkaapin kommunikoimiin elintarvikeanalyyseihin.

Määrityksiin palattaessa, kyber oli terminä erityisessä suosiossa 80- ja 90-luvuilla, ja koki jo eräänlaisen inflaationkin. Kyberiä käytettiin synonyymina monenlaisiin asioihin, vaikka termi olisi voitu loogisemmin korvata etuliitteillä “digitaalinen”, “kehittynyt” tai “tulevaisuuden”. Esimerkkinä tästä voisi olla “kyberpunk”, joka kuvasi jokseenkin futuristista otetta kyseisestä musiikkigenrestä. Käytännössä kaikkien yritysten jälkeen, termi jäi elämään ehkä voimakkaimmin asevoimissa ja kansallisissa regulaattoriorganisaatioissa kuvaamaan ICT-teknologioiden uhkakuvia ja suojausta.

Virtuaalisen maailman lisäksi kehittynyt robotiikka kuuluu siis oleellisena osana kyberiin. Joitakin todellisen elämän esimerkkejä tästä ympäristöstä ovat eläinten ja ihmisten hahmoihin suunnitellut, itsenäisesti toimivat Boston Dynamicsin ja Googlen robotit. Niiden keinoälyn ja autonomisen toimintasäteen edelleen kehittyessä, ne voivat edustaa tulevaisuudessa perustavaa laatua olevaa kyberin fyysistä muotoa esimerkiksi asevoimien kyberjoukkojen osana.

Vaikka monet standardointiorganisaatiot käyttävät kyberiä terminä, on vielä hiukan epäselvää, mitä sillä lopulta tarkoitetaan. Tutkitaanpa siis, mitä tietokirjallisuus toteaa. Oxford-sanakirjan mukaan kyber liittyy tietokoneiden kulttuuriin, informaatioteknologioihin ja virtuaalitodellisuuteen. Sanakirja toteaa edelleen, että se on johdannainen kybernetiikasta, joka on yhdistelmätiedettä koneiden ja elävien olentojen kommunikointiin ja automaattiseen kontrolliin. Espanjalainen Real Academia Española puolestaan toteaa, että kyber kuvaa etuliitettä, joka on lyhennelmä kybernetiikasta, ja se muodostaa omalta osaltaan termejä, jotka liittyvät tietokoneiden maailmaan ja virtuaalitodellisuuteen.

“Menestys keinoälyn luomisessa olisi suurin saavutus ihmisen historiassa. Valitettavasti, se saattaa jäädä myös viimeiseksi.”
(Steven Hawking, Huffington Post, 5.5.2014)

Johtopäätös

Kyberiä on yritetty määrittää monenlaisista näkökulmista, ja korkealla tasolla voidaan sen idea koostaa siten, että se liittyy tietokoneisiin, virtuaalitodellisuuteen, mekaanisiin koneisiin ja/tai eläviin olentoihin täydentäen ”perinteistä” fyysistä ja digitaalista maailmaa. Kaikkien kyber-termien yritelmien jälkeen se on etuliitteenä jäänyt sanastoon hiukan systemaattisemmin sellaisiin ympäristöihin kuten kyberturvallisuus ja kyberrikollisuus.

Kyber – kuinka epämääräinen terminä se onkaan – on jo nyt todellisuutta, ja luo parhaillaan täysin uudenlaisen aikakauden mahdollisuuksineen, uhkakuvineen ja puolustusmenetelmineen. Puolustusvoimien näkökulmasta kyber on yhä merkittävämpi osa toimintaa niin viestinnässä kuin kaikissa muissakin joukko-osastoissa. Alan kehittyessä kiihtyvään tahtiin, on kyberjoukkojen koulutus ja varustaminen ensisijaisen tärkeää yhtenä rakennuselementeistä informaatiosodan aikakaudella. VM

KUTSU SONERAN KERHON SYYSKOKOUKSEEN

Viestiupseeriyhdistyksen Soneran kerhon hallitus kutsuu kerhon jäsenet sääntömääräiseen syyskokoukseen 20.10.2016 klo 15:00 alkaen.

Kokous järjestetään Helsingissä Soneran tiloissa, Teollisuuskatu 15 (nh. ”1-2-3” 7 krs. aulasta lisätietoja).

Kokouksessa käsitellään säännöissä mainitut asiat: mm.toimintasuunnitelma, talousarvio sekä hallituksen kokoonpano. Kahvitarjoilu alkaa klo 14:30 .

Pyydämme ilmoittautumaan kerhon sihteerille viimeistään 12.10. sähköpostitse (toivottava tapa) tai puhelimitse / tekstiviestillä.

Sihteeri: Ismo Siimelä, ismo.siimela@teliacompany.com, p. 040 5062330

Lisätietoja antaa myös kerhon puheenjohtaja:

Olli Welin, olli.welin@teliacompany.com, p. 0400 502054 Tervetuloa Kerhon hallitus

DI Karri-Tuomas Salli vastaa Insta DefSec Oy:n Defence Solutions -liiketoiminta-alueen Yhteiset johtamisjärjestelmät -liiketoimintayksiköstä, jonka asiakas on Puolustusvoimat. Hänellä on yli 15 vuoden kokemus kriittisten tietojärjestelmien kehittämisestä vaativiin ympäristöihin.

TEKSTI JA KUVAT: KARRI-TUOMAS SALLI

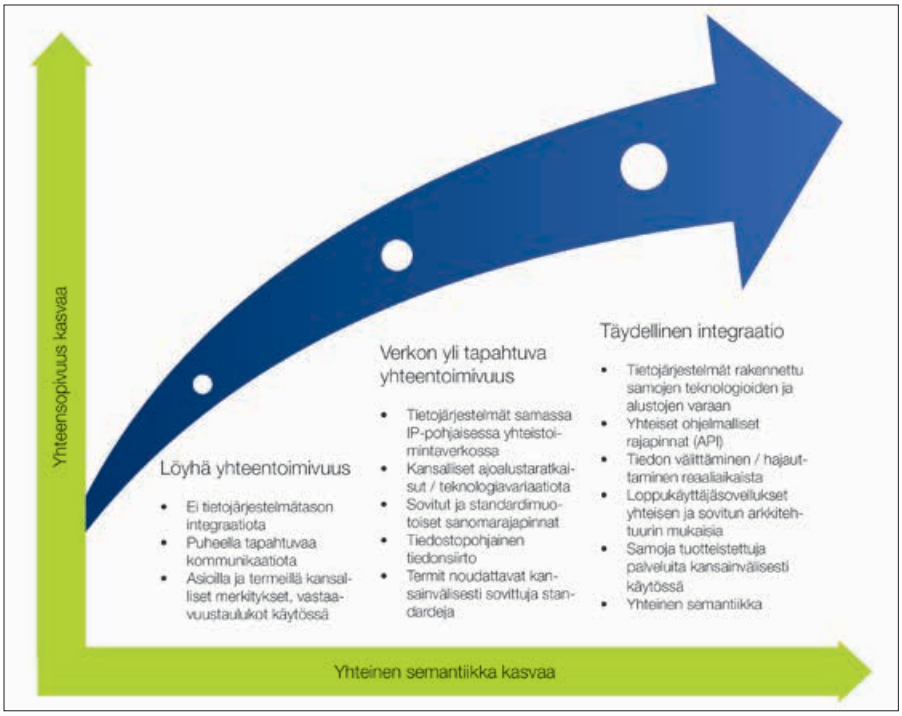
Johtamisjärjestelmien kansainvälinen yhteensopivuus Puolustusvoimien ja teollisuuden yhteistyöllä

Suomen Puolustusvoimien johtamisjärjestelmien kansainvälinen yhteensopivuus on tänä päivänä välttämättömyys. Ennen hankintojen käynnistämistä tulee tavoiteltava yhteensopivuuden taso määritellä. Sen lisäksi yhteensopivuus on huomioitava myös järjestelmän koko elinkaaren ajan. Kansainvälinen harjoitustoiminta on keskeisessä roolissa yhteensopivuuden varmistamisessa ja siinä Puolustusvoimien sekä teollisuuden yhteistyöllä on iso merkitys.

Tavoitteena yhteensopivat järjestelmät

Termistä "kansainvälinen yhteensopivuus" tulee usein ensimmäisenä mieleen kansainväliset sotilas- ja NATO-standardit, joita noudattamalla järjestelmät pystyvät välittämään toisilleen dataa ja tulkitsemaan sitä. Puhuttaessa yhteensopivuudesta tarkoitetaan yleensä yhteentoimivuutta (engl. interoperability). IEEE määrittelee yhteentoimivuuden järjestelmän kyvykkyydeksi toimia toisten järjestelmien kanssa ilman merkittäviä loppukäyttäjän toimenpiteitä. Yhteentoimivuuden mahdollistaa standardinmukaiset toteutukset. NATO:n näkökulmasta yhteentoimivuus tarkoittaa monikansallisten joukkojen kykyä toimia yhdessä. Tämä muodostaa perustan kaikille NATO-operaatioille.

Tietojärjestelmien yhteensopivuuden tavoitetiloihin ja -tasoihin löytyy monia vaihtoehtoisia määritelmiä ja malleja. Kansainvälistä yhteensopivuutta voidaan tarkastella johtamisjärjestelmien



Johtamisjärjestelmien yhteensopivuuden eri tasoja sekä niitä kuvaavia piirteitä.

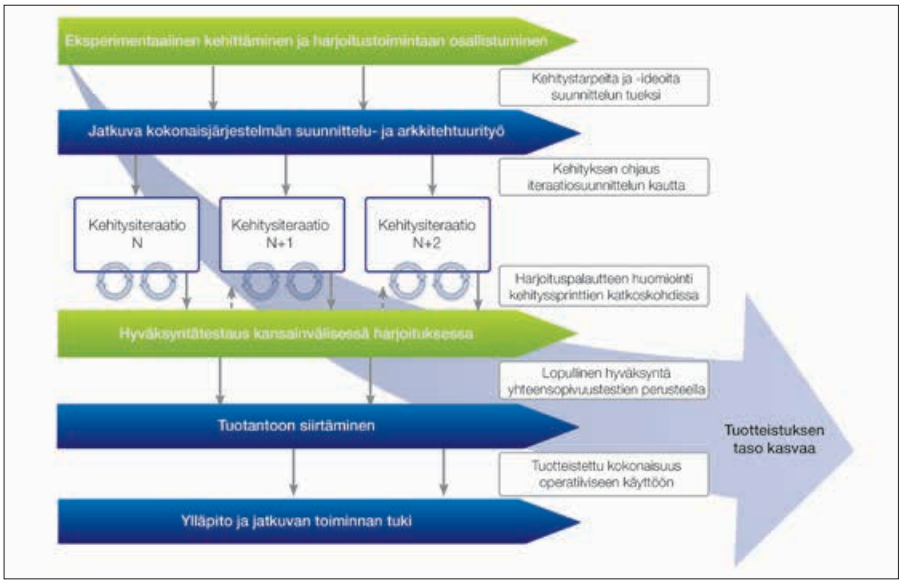
näkökulmasta muutaman eri tavoitetilan kautta. Viereisen sivun kuva esittää kolmen tason määritelmän, jossa painottuu yhteisen semantiikan kasvaminen yhteensopivuuden kasvaessa.

Yhteentoimivuuden näkökulmasta yhteensopivuutta ei käytännössä ole, jos johtamisjärjestelmät eivät voi välittää toisilleen tietoa jollain tiedonsiirtomedialla. Tässä tilanteessa yhteistoiminta hoidetaan puheella ja tilannekuva muodostetaan tulkitsemalla sekä sovittamalla vastaanotettu informaatio vastaaviin kansallisiin käsitteisiin nähden (engl. data mapping). Tällä tavalla saadaan aikaiseksi auttava yhteinen ymmärrys ja tiedonjako.

Nykyisin kansainvälinen yhteensopivuus perustuu aina tietojärjestelmien jollain mekanismilla vaihtamaan tietoon. Järjestelmien välillä voi olla esimerkiksi sanomapohjainen tiedonsiirtokanava tai jaettu tietokantayhteys. Tyypillisesti eri kansalliset järjestelmät ovat samassa IP-verkossa ja keskustelevat toistensa kanssa NATO-standardien mukaisten sanomien avulla. Esimerkki tästä on Link16 -järjestelmä ja sen IP-pohjainen JREAP-C -protokolla. Link16 sisältää sanomamääritysten lisäksi myös toimintatavan määrittelyn. Kotimaiset johtamisjärjestelmät on rakennettu noudattamaan pääosin omaa kansallista toimintatapaa ja tietomallia.

Esimerkkinä yhteensopivuuden kehittyneistä konsepteista on NATO:n Federated Mission Networking (FMN) -kokonaisjärjestelmä, joka mahdollistaa kansainvälisiin yhteisoperaatioihin osallistuvien maiden tehokkaan tiedonvaihdon operaation aikana. Yhteensopivuuden näkökulmasta FMN määrittelee kokonaisjärjestelmän, joka koostuu sidostahoista eli toimijoista, prosesseista sekä määritellyistä toiminnallisista ja teknisistä vaatimuksista. FMN-järjestelmän määrittely- ja kehitystyötä tehdään konseptissa määritellyissä spiraaleissa eli kehitysvaiheissa.

Yhteensopivuuden saavuttamisen kannalta tehokkainta olisi rakentaa johtamisjärjestelmät alusta alkaen yhteisen alustan ja rajapintojen päälle. Tässä yhteydessä alusta tarkoittaa kokonaisuutta, joka koostuu kehitysympäristöstä, ajoalustasta, ohjelmistoalustasta ja



Kansainvälisten harjoitusten rooli kehityshankkeessa.

mahdollisimman suuresta joukosta yhteisiä palveluita. Mikäli lisäksi prosessit ja tietomallit olisivat samat, myös semanttinen ymmärrys olisi yhteinen eri toimijoiden kesken. Toki tässä asiassa on paljon muita ratkaistavia haasteita – eikä yhteinen johtamisjärjestelmäalusta ole myöskään kansainvälisessä mittapuussa tällä hetkellä realistinen tavoite.

Yhteensopivuuden huomiointi järjestelmän koko elinkaaren ajan

Yhteensopivuuden vaatimuksiin pureudutaan jo järjestelmien hankintavaiheessa. Karkeasti hankinnat voidaan jakaa johtamisjärjestelmien näkökulmasta kahteen tapaukseen:

1. Kehitetään kotimainen johtamisjärjestelmä, joka sovitetaan kansainvälisesti yhteensopivaksi.
2. Hankitaan ulkomailta vaikuttamisjärjestelmä (asejärjestelmä), joka integroidaan osaksi kotimaista johtamisjärjestelmää.

Järjestelmähankinnoissa yhteensopivuuteen liittyviä asioita hallitaan erilaisten sopimusten ja yhteistyömallien kautta. Keskeisin asia järjestelmähankinnassa on varmistaa riittävän ja oikean tiedon saaminen järjestelmäintegraattorille integroitavan järjestelmän toimittajalta. Technical Assistance Agreement -sopimusmallia on tyypillisesti käytetty kaikkien hankintaan osallistuvien tahojen kesken määrittelemään yhteistoiminnan ja keskinäisen informaation jakamisen sisällön ja aikataulun vastuut. Kotimaisen teollisuuden rooli onkin usein toimia tulkkina järjestelmätoimittajan ja hankinnan vaatimusten välillä.

Toinen keskeinen asia on saada kotimaiselle järjestelmäintegraattorille käyttöön tarvittavat standardit ja spesifikaatiot mahdollisimman varhain hankinnan käynnistysvaiheessa. Näillä varmistetaan perusta järjestelmien keskinäiselle yhteensopivuudelle.

Kolmas tärkeä asia on järjestelmän testaaminen todellisia rajapintoja vasten mahdollisimman varhaisessa vaiheessa. Näin saadaan varmuus todellisesta yhteistoiminnan kyvykkyydestä kehittämisen aikana ja mahdollisiin ongelmakohtiin voidaan reagoida riittävän varhain aktiivisen rakentamisvaiheen aikana.

Yhteensopivuuden varmistaminen täytyy huomioida koko järjestelmän elinkaaren ajan – myös ylläpitovaiheessa aktiivisen kehittämisen jälkeen. Tyypillisesti ylläpitovaiheessa johtamisjärjestelmien osalta tehdään pienimuotoista kehittävää ylläpitoa, jolloin järjestelmään kuuluvien osajärjestelmien toiminnallisuudet ja rajapinnat saattavat muuttua.

Varsinkin järjestelmäintegraattorin työssä korostuvat useista osajärjestelmistä muodostuvan kokonaisjärjestelmän (System of Systems) hallinta sekä toimialaosaaminen ja -kokemus. Hankinnoissa tulisikin varmistaa, että aktiivisen järjestelmän kehitystyön aikana kotimaiselle teollisuudelle syntyy kokonaisjärjestelmästä tulevien vuosien ylläpidon näkökulmasta riittävä toiminnallinen ja tekninen osaaminen.

Kansainvälisten harjoitusten rooli yhteensopivuuden varmistamisessa

Hankkeen rakentamis- ja kehitysvaiheen aikana kansainvälisillä harjoituksilla on merkittävä rooli yhteensopivuuden varmistamisessa. Sivun 23 kuva esittää periaatteellisella tasolla hanketta, jonka läpivientimalli noudattaa iteratiivisen kehittämisen mallia. Kyseisessä hankinnassa hyödynnetään kansainvälisiä harjoituksia muun muassa eksperimentaalisen kehityksen alustana sekä kansainvälisiin rajapintoihin ja toiminnallisuuksiin liittyvien osuuksien hyväksyntätestausympäristönä.

Eksperimentaaliseen kehittämiseen viedään sellaisia osuuksia, joita halutaan tarkemmin tutkia esimerkiksi teknologiavalintojen tai ylipäätään ratkaisun tai konseptin toimivuuden suhteen sopivassa testiympäristössä. Eksperimentaalisesta kehittämisestä saadaan palautetta varsinaisen hankkeen ohjaamisen ja suunnittelun tueksi. Eksperimentaalisessa kehittämisessä hyväksytään se tosiasia, että kirjoitettua koodia ei välttämättä voida hyödyntää operatiivisen järjestelmän osana ollenkaan.

Toinen ääripää on lähes tuotantokelpoisen ohjelmiston hyväksyntätestaaminen kansainvälisessä harjoituksessa. Tämä on tehokasta, koska harjoitusympäristössä on helposti järjestettävissä hyväksyntätestaus osana muuta harjoitustoimintaa. Sinne tulevat joka tapauksessa eri toimijat ja tahot mukanaan ne järjestelmät, joita hyväksyntätestauksessa tarvitaan.

Keskeisimmät järjestelmien kehittämiselle ja testaukselle saatavat hyödyt kansainvälisistä harjoituksista:
- eksperimentaalisen ja tutkivan kehittämisen ympäristö ja tuki
- tuotteiden yhteensopivuuden kustannustehokkaan testaamisen ympäristö
- järjestelmien määrittelyjen tarkentaminen (esimerkiksi rajapintojen osalta)
- kontaktien ja yhteistyön edistäminen.

Joint Forces Training Centre Puolan Bydgoszcz:ssä.

CWIX – johtamisjärjestelmäalan keskeisin NATO-harjoitus

Vuosittain kesäkuussa Puolan Bydgoszcz:ssä ja siellä NATO:n JFTC-harjoituskeskuksessa (Joint Forces Training Centre) pidettävä CWIX-harjoitus on yksi merkittävimmistä NATO:n johtamisjärjestelmäalan harjoituksia. CWIX tulee sanoista The Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise.

Nimensä mukaisesti harjoituksessa eri tahot – mukaan lukien rauhankumppanimaat – testaavat järjestelmiään yhteisessä verkottuneessa monitoimittajaympäristössä.

CWIX-harjoituksessa
- kehitetään yhteensopivuuden standardeja ja ratkaisuja
- tehdään kokeilevaa (eksperimentaalista) testaamista uusien yhteensopivuuden ratkaisuiden osalta
- testataan järjestelmien teknistä yhteensopivuutta testikumppanien välillä
- tehdään loppukäyttäjien toimesta järjestelmien operatiivisen käytön testausta erilaisiin yhteisiin skenaarioihin pohjautuen.

Insta DefSec Oy on osallistunut Puolustusvoimien kumppanina jo useana vuonna peräkkäin CWIX-harjoitukseen tukien omalta osaltaan harjoituksen onnistumista Puolustusvoimien tavoitteiden mukaisesti. Käytännössä Instasta on ollut mukana asiantuntijoita tekemässä käytännön työtä osana varsinaista harjoitusorganisaatiota Puolustusvoimien henkilöiden lisäksi.

CWIX-harjoitus on erittäin tärkeä osa järjestelmien kehittämisen vuosikelloa yhdessä muun järjestelmien kehittämiseen ja yhteensopivuuteen tähtäävän harjoitustoiminnan kanssa. Vuosittain säännöllinen harjoitustoiminta kotimaassa ja ulkomailla tukee erinomaisesti johtamisjärjestelmäkehitystä. Harjoitusten kokemukset ja niistä kerättävä palaute pystytään ottamaan suunnitelmallisesti osaksi kehittämissuunnitelmaa iteratiivisen toimintatavan luonteen mukaisesti. Tässä Puolustusvoimien ja teollisuuden saumaton yhteistyö on avainasemassa.

Instan kehittämien järjestelmien osalta CWIX-harjoituksessa on
- testattu eksperimentaalisia toteutuksia testikumppanien kanssa

- tehty lähellä tuotantoa oleville järjestelmille yhteensopivuustestejä valittujen testikumppanien kanssa
- tehty hyväksyntätestejä kansainvälisiä standardeja vasten
- kerätty arvokasta kokemusta kansainvälisistä NATO-järjestelmistä ja niiden kyvykkyyksistä.

Yhteenveto

Tietojärjestelmien keskinäinen yhteensopivuus kansainvälisissä operaatioissa on ollut jo vuosia keskeinen tavoite ja kehittämiskohde. Vastaavasti kansainvälinen yhteensopivuus korostuu jatkossa myös kotimaassa pidettävien yhteistyöharjoitusten näkökulmasta.

Hankinnan kannalta kotimainen teollisuus on hyvä saada mukaan riittävän varhaisessa vaiheessa, jolloin kansainvälinen yhteensopivuus ja siihen liittyvä osaaminen ehtii syntyä aktiivisen kehittämisen aikana.

Kansainvälisellä harjoitustoiminnalla on tässä keskeinen rooli. Varsinaisen testaamisen lisäksi paikan päällä tapahtuvan vuorovaikutuksen ja kokemusten vaihtamisen merkitystä ei voi liikaa korostaa. Tässä teollisuuden mukana olo koko järjestelmän elinkaaren ja huoltovarmuuden varmistamisen näkökulmasta on erittäin tärkeää. Puolustusvoimien ja teollisuuden osallistuminen yhdessä kansainvälisiin harjoituksiin on merkittävä asia järjestelmien kokonaissuorituskyvyn varmistamisen ja koko elinkaaren aikaisen hallinnan ja ylläpidon näkökulmista.

VM

TEKSTI: SEPPO URO
KUVAT: SEPPO URO JA BEN NYBERG

Kiveen hakattua viestihistoriaa

Kirjoittaja on eversti evp, joka on pitkään harrastanut viestialan historian tutkimusta. Hän on kirjoittanut säännöllisesti Viestimies-lehteen ja vastannut osaltaan usean viestialan historiateoksen laatimisesta.

Kirjallisten historiikkien ja alan museoiden lisäksi suomalaista viestihistoriaa on tallennettu myös lukuisiin muistomerkkeihin ja muistolaattoihin eri puolilla Suomea. Sellaisia on pystytetty pääasiassa 1960-luvulta alkaen ja useimmat ovat viestialan vapaaehtoisten maanpuolustusjärjestöjen aikaansaannoksia. Kuuluuhan viestiperinteiden vaaliminen sekä Viestiupseeriyhdistyksen että viestikiltojen sääntöjen mukaisiin tehtäviin.

Kouvolan vanhan varuskuntasairaalan seinässä oleva laatta kertoo, että rakennuksessa perustettiin 3.Erillinen Viestikomppania toukokuussa 1961.

Lähes kaikkien Suomessa toimineiden viestijoukko-osastojen kotivaruskuntiin on pystytetty muistomerkki tai muistolaatta kertomaan joukon perustamisesta ja toiminnasta. Mikkelin työväentalon seinään kiinnitettiin vuonna 1989 muistolaatta ensimmäisen viestijoukkomme Kenttälennätinpataljoonan muistoksi. Joukko-osasto perustettiin rakennuksessa 5.3.1918. Laatan hankki Kaakkois-Suomen Viestikilta ry. Riihimäen etukasarmilla olevaan Kasakkakallioon kiinnitettiin vuonna 1982 laatta sen muistoksi, että uudelleen perustetun Kenttälennätinpataljoonan toiminta käynnistyi siellä vuonna 1920. Pataljoona toimi vuosina 1930-34 nimellä Viestipataljoona 2. Laatan hankki Viestikilta ry. Santahaminassa olevan vanhan tiilikasarmin seinään kiinnitettiin vuonna 2010 muistolaatta rakennuksessa vuosina 1918-34 toimineiden viestijoukkojen, kuten muun muassa Kipinälennätinlaitoksen, Radiopataljoonan ja Viestipataljoona 1:n muistoksi. Laatan hankki Uudenmaan Viestikilta ry.

Myös useimmat sotien jälkeen perustetut viestijoukot ovat saaneet oman laattansa tai muistokivensä. Oulun vanhalla kasarmialueella vuosina 1953-89 toiminut 1. Erillinen Viestikomppania on saanut laatan entisen kasarminsa seinään. Sen lisäksi komppanian nimi on hakattu myös muistokiveen, jossa on mainittu kaikki alueella toimineet joukko-osastot. Turun Pääskyvuoren kasarmialueelle kiinnitettiin vuonna 1996 laatta siellä vuosina 1963-94 toimineen 2. Erillisen Viestikomppanian muistoksi. Laatan hankki Varsinais-Suomen Viestikilta ry. Kouvolan kasarmialueella vuosina 1961-79 toiminut 3. Erillinen Viestikomppania sai muistolaatan vanhan varuskuntasairaalan seinään vuonna 2001. Laatan hankki Kymen Viestikilta ry. 4. ja 5. ErVK:lle ei muistolaattoja tiettävästi ole hankittu. Komppaniat yhdistettiin Keuruulla vuonna 1976 Keski-Suomen Viestipataljoonaksi, joka lakkautettiin organisaatiouudistuksessa vuonna 1998. Tässä yhteydessä

pataljoonan kasarmialueelle kiinnitettiin laatta joukko-osaston muistoksi. Viestikoulun perustamisesta kertoo Hämeenlinnan Linnankasarmille nykyisen Museo Militarian ovenpieleen vuonna 2001 kiinnitetty laatta. Viestirykmentille pystytettiin kookas muistokivi Riihimäen varuskunnan portinpieleen vuonna 1999. Kun joukko-osasto lakkautettiin vuoden 2014 lopussa, kivi siirrettiin takakasarmille niin sanottuun rykmentinpuistoon. Varuskunnan etukasarmille on kiinnitetty laatta myös sen muistoksi, että viestijoukkojen yhteinen aliupseerikoulu toimi siellä vuosina 1968-94. Riihimäellä sijaitsee myös valtakunnallinen viestimuistomerkki, jossa on teksti "Viestitoiminnoissa uurastaneiden ja heidän saavutustensa kunnioittamiseksi Viestikilta ry 5.3.1968".

Viime sotien viestijoukoille on pystytetty varsin niukasti muistomerkkejä. Talvisodan Viestipataljoona 8:n perusyksiköistä muistuttaa vuonna 2009 kiinnitetty laatta Seinäjoella ja jatkosodan Viestipataljoona 5:stä vuonna 2012 kiinnitetty laatta Ilmajoella. Molempien hankinnasta vastasi Pohjanmaan Viestikilta ry. Muille viestipataljoonille ja koulutuskeskuksille muistolaattoja ei tiettävästi ole pystytetty. Vuonna 1966 kiinnitettiin laatta Mikkelin Naisvuoren kupeeseen kertomaan kallioluolassa sijainneesta Päämajan viestikeskus Lokista. Laatta poistettiin myöhemmin ja vuodesta 1995 asiasta muistuttaakin Lokki-viestikeskusmuseo. Suomalaisen radiotiedustelun historiaa on muistettu useallakin laatalla ja muistomerkillä. Laattoja on muun muassa Päämajan Radiopataljoonan koulutus- ja toimintapaikoilla Säämingin Rauhanlinnassa, Tuusulan Lottamuseolla, Munkkiniemen Kaartintorpalla sekä Kauniaisissa "Klostretin" kohdalla. Päämajan radiotiedustelun muistomerkki on Tikkakosken Kuikassa sekä Stella Polariksen muistomerkki Närpiön Nämpnäsin kylässä ja Uudenkaupungin Seikowin koululla. Monet edellä mainituista muistomerkeistä on hankkinut Viestikoelaitoksen Kilta ry. Ilmavoimien Viestikoulun ja Viestipataljoonan historiasta kertovat muistolaatat Naarajärvellä ja Parolassa. Suomen ensimmäisen ilmavalvontatutkan muistoksi on kiinnitetty laatta Malmin lentoasemalle. Pääkaupunkiseudun ilmavalvonnasta muistuttavat laatat entisten ilmavalvonta-aluekeskusten seinissä Korkeavuorenkadulla ja Suomenlinnassa.

Yleisen viestitoiminnankin kehityksestä kertovat lukuisat muistomerkit tai muut sen luonteiset kohteet. Hangossa ja tiettävästi eräillä muillakin paikkakunnilla on muistolaatta Krimin sodan aikaisen optisen lennätinaseman paikalla. Kotkassa muistolaatta kertoo Suomen ensimmäisestä radioyhteydestä Kotkan ja Suursaaren välillä vuonna 1900. Laatan hankkivat yhteistoiminnassa Viestiupseeriyhdistys ja Viestikilta vuonna 1988. Kotkassa on myös edellä mainitun yhteyden rakentajan, Aleksandr Popovin patsas. Yleisradiotoiminnan historiasta muistuttavat Lahdessa olevat yleisradiomastot, Pasilan radiokeskuksessa sijaitseva vanha lähetyskeskus sekä Fabianinkadun vanha radiotalo. Maamme ensimmäisestä automaattikeskuksesta kertoo Helsingin Töölössä sijaitseva komea keskusrakennus. Valtion rautateiden viestihistoriasta

Viestirykmentin muistokivi sijaitsee nykyisin takakasarmin rykmentinpuistossa. Patsaan laatassa kerrotaan rykmentin perustamisesta Riihimäelle 4.12.1944 ja sen lakkauttamisesta 31.12.2014.

Stella Polaris -operaation muistomerkki sijaitsee Närpiön Nämpnäsin kylässä, josta eräs radiotiedustelijoita kuljettanut alus lähti matkaan syksyllä 1944. Laatassa on teksti "Frihet är det bästa ting som sökas kan all världen kring".

muistuttaa pronssilaatta Riihimäen veturitallien kupeessa.

Viestihistoriassamme on kuitenkin edelleen lukuisia joukkoja, kohteita ja tapahtumia, jotka ansaitsisivat tulla muistetuiksi myös tulevina vuosikymmeninä. Itsenäinen Suomi täyttää sata vuotta vuoden 2017 lopulla ja viestijoukkojen perustamisesta tulee kuluneeksi samat sata vuotta 5.3.2018. Viestiaselajin vapaaehtoisille järjestöille tarjoutuukin nyt erinomainen mahdollisuus muistaa viestitoiminnan parissa tehtyä työtä uusia muistomerkkejä ja muistolaattoja kiinnittämällä sekä vanhoja kunnostamalla.

VM

Kotkan ortodoksisen kirkon puistossa oleva laatta muistuttaa Aleksandr Popovin vuonna 1900 rakentamasta Kotkan ja Suursaaren välisestä radioyhteydestä, jota pidetään maailman ensimmäisenä meripelastusta auttaneena radioyhteytenä.

Viestimies

MEDIA KORTTI 2016

Viestiupseeriyhdistys ry:n julkaisema viesti-, johtamisjärjestelmä- ja ICT-alojen sekä kyberturvallisuuden päättäjien ja asiantuntijoiden lehti.
Esillä lehdessä – mukana päätöksiä tehtäessä!

ILMOITUSHINNAT (ALV 0%)

1/1 s	800 €
1/2 s	500 €
1/4 s	350 €
Takakansi	1000 €

Määräpaikkalisä 20 %.

ILMOITUSTEN KOOT

1/1 s A4	210 x 297 mm bleed 3 mm	
1/1 s	180 x 260 mm	
1/2 s	180 x 130 mm	vaaka
1/2 s	90 x 260 mm	pysty
1/4 s	90 x 130 mm	pysty
1/4 s	180 x 65 mm	vaaka

Aineistot:
PDF, CMYK Fogra Coated 27
Kuvien resoluutio: 300 dpi

AINEISTO-OSOITE:
juha.halminen@kolumbus.fi

AIKATAULU VUONNA 2016
Valmiin mainosmateriaalin toimitus

N:o	Aineistot viim.	Ilmestyy
1	05.02.2016	04.03.2016
2	09.05.2016	03.06.2016
3	26.08.2016	23.09.2016
4	04.11.2016	05.12.2016

ILMOITUSMYYNTI
Juha Halminen
Puhelin 09 873 6944
Gsm 050 592 2722
Sähköposti:
juha.halminen@kolumbus.fi

PÄÄTOIMITTAJA
Tero Palokangas
Gsm 050 547 8974
Sähköposti: viestimies@viestiupseeriyhdistys.fi

PAINOPAIKKA
Newprint Oy
Tuijussuontie 1
21280 RAISIO
Puhelin 010 231 2600
Faksi 010 231 2699

JULKAISIJA
Viestiupseeriyhdistys ry
HELSINKI
Y-tunnus 0223897-9
ISSN 0357-2153

TEKSTI: TERO PALOKANGAS
KUVAT: JOONA HAKULINEN

Viestimies-lehti miehen ikään

4.6.1946 näki päivänvalonsa Viestimies-lehden ensimmäinen näytenumero. Lehti oli vain 13-sivuinen ja huonolle paperille painettu moniste, mutta siitä käynnistyi katkeamaton lehdenteon perinne Viestiupseeriyhdistyksen piirissä. Viestimies-lehteä on vuosien saatossa talkoilla tai pienen korvauksen tukemana pääsääntöisesti toimitettu harrastelijavoimin. Kovalla työllä, tahdolla ja sitoutumisella tekemiseen on lehti saatu kuitenkin pidettyä hengissä ja samalla elämään myös ajassaan. 3.6.2016 oli aika kokoontua arvovaltaisten kutsuvieraiden läsnä ollessa Riihimäen varuskunnan upseerikerholle juhlimaan 70-vuotista lehteämme.

Arvovaltainen kutsuvierasjoukko oli saapunut juhlistamaan lehden 70-vuotista taivalta.

Tilaisuuden aloitti varusmiessoittokunnan taitava jousiorkesteri johtajanaan yliluutnantti Tommi Suutarinen, joka esitti Sibeliuksen jääkärimarssin. Tämän jälkeen lehden päätoimittaja majuri Tero Palokangas avasi tilaisuuden ja johdatteli juhlayleisön aiheeseen lehden historian, nykytilan ja tulevaisuuden näkymien kautta. Sotatieteiden tohtori, eversti evp Martti Lehdon juhlapuheessa pohdittiin puolestaan ansiokkaan monipuolisesti maanpuolustuslehtien tulevaisuutta digitalisoituvassa maailmassa. Puhe löytyy kokonaisuudessaan tämän artikkelin liitteenä. Puheen jälkeen varusmiessoittokunnan jousiorkesteri soitti kaksi Piazzolan tangoa, joista jälkimmäisessä hienon

Reima Tahvanainen vastaanotti lehden toimituskunnan puheenjohtajalta, prikaatikenraali Mikko Heiskaselta yhdistyksen pronssisen levykkeen.

Varusmiessoittokunnan jousiorkesteri johtajanaan yliluutnantti Tommi Suutarinen piti osaltaan huolen siitä, että juhlaväki viihtyi.

Majuri Mikko Rasimus palkittiin vuoden 2015 kirjoittajastipendillä.

soolon esitti haitarillaan jääkäri Sami Salonen. Esityksen jälkeen johtamisjärjestelmä-päällikkö, prikaatikenraali Mikko Heiskanen toi tilaisuuteen Puolustusvoimien ja johtamisjärjestelmäalan tervehdyksen.

Everstiluutnantti Jukka-Pekka Virtanen palkittiin merkittävästä panoksestaan lehden ja yhdistyksen toiminnan hyväksi VUY:n standaarilla. Samoin pitkäaikainen lehden yhteistyökumppani Newprint Oy palkittiin yhdistyksen standaarilla. Reima Tahvanainen, Milla Nummenpää ja Olavi Waljakka palkittiin puolestaan ansioistaan yhdistyksen pronssisella levykkeellä. Lehden kirjoittajina vuodelta 2015 palkittiin majuri Mikko Rasimus sekä tekniikan tohtori Jyrki Penttinen. Rasimus kirjoitti lehden numeroon 4/2015 erittäin mielenkiintoisen artikkelin "Kaupallisten tiedonsiirtotekniikoiden hyödyntäminen sotilaallisessa toimintaympäristössä". Artikkeli pohjautui Rasimuksen YE-diplomityöhön, ja oli erinomaisesti tiivistetty ja sovitettu lehtiartikkeliksi. Penttinen kirjoitti puolestaan säännöllisen ahkerasti useaan vuoden 2015 numeroon mielenkiintoisista aiheista, jotka oli ilo julkaista lehdessä. Lopuksi muistettiin vielä Riihimäkeläisellä taidelasilla lehden nykyistä toimitusta ja vakituisia avustajia pyyteettömän ansiokkaasta työstään lehden eteen.

Everstiluutnantti Jukka-Pekka Virtanen palkittiin merkittävistä ansioistaan viestiupseeriyhdistyksen standaarilla.

Paikalla olevien yhdistysten (esimerkkeinä logistiikkaupseeriyhdistys ja viestikiltojen liitto) edustajat toivat tervehdyksensä juhlivalle lehdelle. Samoin lehden palveluksessa aikoinaan toimineet henkilöt toivat tervehdyksensä lehdelle ja samalla valottivat juhlayleisölle heidän aikaisen lehden toimintaa ja osin hauskojakin sattumuksia. Lopuksi varusmiessoittokunta esitti vielä Maasalon juhlamarssin. Juhlan jälkeen nautittiin upseerikerhon maittavasta coctail-illallisesta ja paikalle saapuneiden vieraiden seurasta. Voi varmaan sanoa, että lehti ja sen eteen töitä tehneet ihmiset saivat arvoisensa ja näköisensä juhlan. Tästä on hyvä jatkaa lehden toimittamista ja kehittämistä seuraavatkin 70 vuotta.

VM

TEKSTI: MARTTI LEHTO

Maanpuolustuslehtien tulevaisuus digitalisoituvassa maailmassa

Herra kenraali, arvoisat kutsuvieraat

ST, eversti evp Martti Lehto toimii muun muassa Jyväskylän yliopiston kyberturvallisuuden professorina sekä sotilasaikauslehden päätoimittajana. Hän piti alla olevan juhlapuheen viestimies-lehden 70-vuotisjuhlissa Riihimäellä 3.6.2016.

Hyvin usein kuulee, että printtimedia tekee kuolemaa ja että painetut lehdet katoavat yksi toisensa jälkeen. Aikakausmedian mukaan uusien, painettujen aikakauslehtien määrä vuonna 2015 nousi ennätysvuosien lukemiin. Markkinoille tuli 30 uutta aikakauslehteä - kymmenen enemmän kuin vuonna 2014. Kansalliskirjaston vapaakappalekokoelman mukaan Suomessa julkaistavien aikakauslehtinimikkeiden määrä vuonna 2014 oli 4106. Suomi on siis edelleen kärkimaa aikakauslehtien määrässä suhteessa väestömäärään.

Vuonna 2014 tehdyssä median käyttöä koskevassa tutkimuksessa selvisi, että painettua sanoma- ja aikakauslehteä luetaan yhä todella paljon samalla, kun verkko- ja mobiilisisältöä on jatkuvasti enemmän tarjolla. Aikakauslehti tavoittaa lukijansa parhaiten printillä, kun sanomalehden lukijat taas ovat siirtyneet selkeästi myös verkkoon ja mobiiliin. Molempien medioiden lukeminen mobiilissa ja tabletissa on kasvanut, etenkin nuorten keskuudessa. Haaste onkin tulevaisuudessa, sillä merkittävä osa 17–35-vuotiaista karttaa painettua mediaa.

Talouden näkymät ovat mediataloille edelleen epävarmat. Lehtitoimialojen liikevaihdot ja tulokset heikkenevät tai pysyvät parhaimmillaankin aikaisempien vuosien tasolla. Sanomalehtien Liiton puheenjohtaja **Vesa-Pekka Kangaskorven mukaan** keinot levikki- ja mainostulojen laskun pysäyttämiseen ovat vähissä. Mainonnan volyymi laskee ja kilpailu kovenee. Printtimedian levikit laskevat, eikä digitaalisella puolella ole löydetty vielä toimivia ansaintamalleja.

Kuluttajakäyttäytyminen on muuttunut pysyvästi. Viihteestä on aina maksettu, joten siitä halutaan maksaa myös netissä, ainakin osa haluaa. Muun muassa musiikin kuuntelu eri palveluiden kautta kasvaa, mutta alan talous pysyy ennallaan – kuuntelusta ei haluta maksaa. Wikipedia hemmottelee meitä ilmaisella tiedolla ja mediatalot ovat opettaneet meidät ilmaisen uutisvirran käyttäjiksi. Kuinka käyttäjät saadaan maksamaan digitaalisesta tiedosta?

Digitalisaatio on tehnyt mediasta ja median käyttämisestä globaalia. Me kilpailemme nyt lehtiemme sisällöillä kuluttajien huomiosta ja rahoista kansainvälisiä digijättejä, kuten Facebookia, Microsoftia ja Googlea, vastaan.

Lähitulevaisuudessa mainonnan kokonaismäärä ei Suomessa kasva. Digitalisaatio antaa mainostajille mahdollisuuden jakaa mainoseurot moniin kohteisiin kuluttajaprofiilien mukaan. Mainonnalla haetaan täsmävaikutusta ja siksi monelle lehdelle tulee olemaan haaste vakuuttaa mainostaja printtilehden vetovoimasta mainospaikkana.

Mainonnan kasvu edellyttäisi vähintään kahden prosentin talouskasvua, mitä ei ole valitettavasti näköpiirissä. Siksi hengissä selviävät ne, jotka onnistuvat löytämään uudenlaisia ansaintamalleja tasokkaalle sisällölle. Tämän kokevat ensin sanomalehdet, joiden on löydettävä malli periä kuluttajilta tilausmaksuja verkkopalveluistaan.

Ainoa ratkaisu on laadukas sisältö. Laadukas journalistinen tiedon jakaminen saa kuluttajat maksamaan sekä printtilehdestä että digitaalisista sisällöistä. Tässä on myös maanpuolustuslehtien mahdollisuus.

Millainen on median tulevaisuus?

Median tulevaisuus on eri asia kuin journalismin tulevaisuus. Tasokkaan journalismin ja objektiivisen tiedon tuottaminen tulee olemaan järjestöissä kuten Viestiupseeriyhdistys, kriittiseen journalismiin uskovissa voittoa tavoittelemattomissa organisaatioissa. Viestimies-lehden vahvuus on ja samalla tulevaisuus on sen laadukkaassa sisällössä.

Media taas keskittyy kaupallisiin ja globaaleihin mediayrityksiin – mediatavarataloihin - ja informaatioteknologiayrityksiin, jotka hakevat ansaintamahdollisuuksia uusilla alustaratkaisuilla. Isot mediatavaratalot eivät lähtökohtaisesti ole tiedonvälityksen kannalta huono asia. Kuluttajat ovat ongelman ytimessä. Kuluttajat suosivat yhä enemmän viihteellistä, nopeaa, dramaattista uutisointia, jolloin objektiivinen tieto jää taustalle. Kukaan ei halua miettiä eri uutisten ja ilmiöiden taustoja, otsikot riittävät. Tätä kulut-

tajakäyttäytymistä suuret mediatalot vahvistavat.

Sosiaalisesta mediasta on tullut tiedon valtavirtaa, paikka jossa väärä tieto leviää nopeasti ja jota on vaikea hallita. Ollaan jo vakavissa ongelmissa, kun poliitikot pikaistuksissaan ottavat kantaa sosiaalisessa mediassa esiin tulleisiin vääriin uutisiin, joista osa on tahallisesti tuotettu.

Pikaviesteistä (Whatsapp) on tullut tärkein ja käytetyin älypuhelimen sovellus. Sitä käyttää lähes 2 miljoonaa suomalaista. Nopeasta lähipiirin saavuttamisesta on tullut hyve, jossa tiedon objektiivisuus jää taustalle. Tärkeintä on saada informaatio ensimmäisenä jakeluun, aikaa taustan tarkistamiselle ei ole.

Toinen merkittävä trendi on seuraaminen. Twitterin käyttäjät arvotetaan sen mukaan, kuinka suuri heidän seuraaja-armeijansa on ja sama on tapahtunut YouTubessa. Arvokasta on viestin tai videon klikkausten määrä ei niiden sisältö. Merkityksettömistä viesteistä tai videoista tulee siis merkityksellisiä määrän, ei laadun perusteella. Tämä viestinnän viihteellistyminen hautaa alleen tiedonvälityksen. YouTubessa on yli 2 miljoonaa kissavideota, parhaimpia on katsottu 100 miljoonaa kertaa ja kokonaisuudessa näitä videoita on katsottu yli 25 miljardia kertaa. Twiittaaminen ja tubettaminen ovat vallanneet tiedonvälityksen itselleen, jossa informaation viihdearvo on merkittävämpi kuin sen tietoarvo. Viihde on voittanut tiedon.

Median tulevaisuuteen vaikuttavat ainakin seuraavat trendit:

1. Uudet sukupolvet ovat haluttomia maksamaan mediasta. Kehitys supistaa kaupallisen median tulorahoitusta.

2. Perinteinen media selviytyykin lähitulevaisuuden minun kaltaisten vanhenevien ikäluokkien avulla.

3. Mediakulutus viihteellistyy ja siirtyy uusiin alustoihin. Mainostajat seuraavat perässä näihin uusiin digitaalisiin ja mobiileihin kanaviin.

4. Mainostajat eivät enää tarvitse perinteisiä kanavia kommunikoidessaan asiakkaidensa kanssa. Mainostajat voivat tavoittaa kohdeyleisönsä medialaitteet suoraan omien medioidensa ja kanaviensa kautta.

5. Informaatioteknologinen kehitys voimistaa em. trendejä. Teknologia poistaa perinteisiä media-alalle tulon esteitä, mutta samalla luo uusia. Näistä merkittävin on suurien mediakonsernien dominanssi.

6. Teknologinen kehitys (mm. automaatio ja keinoäly) merkitsee sitä, että mediakulutuksen ja mediakäyttäytymisen muutos jatkuvat edelleen voimakkaana.

Mitä tulevaisuus tuo maanpuolustuslehdille?

Viestimies ja Sotilasaikakauslehti ovat olleet toimintansa alkuvaiheessa keskeisiä ja tärkeitä tiedon jakajia. Ne olivat lehtiä, jotka tarvittiin jakamaan tietoa, jota ei ollut muualta saatavissa. Nyt digitaalinen maailma on haastanut perinteiset aikakauslehdet tiedon jakajina.

Kuten alussa mainitsin, uusia aikakauslehtiä on tullut edelleen markkinoille. Ne profiloituvat hyvinkin kapeille segmenteille, jossa ne tarjoavat korkealuokkaista sisältöä. Tasokas ulkoasu ja laadukas sisältö mahdollistavat niiden menestymisen. Osa aikakauslehdistä myös panostaa digitaaliseen formaattiin. Ei vain digitaalisiin näköispainoksiin vaan vuorovaikutteiseen verkkopalveluun, josta kuluttaja voida saada haluamaansa palvelua ja tietoa printtilehtien ilmestymisen väliaikoina

Viestimiehellä kuten muillakin maanpuolustuslehdillä on ollut ja tulee olemaan asema maanpuolustushengen ylläpitäjinä. Jokaiselle järjestölle jäsenten yhteenkuuluvuuden ja jäsenpidon kannalta viestintä on merkittävässä asemassa. Jokainen yhdistys on tavalla tai toisella yhteydessä jäsenistöönsä. Jäsenlehti on yksi tapa yhteydenpitoon, mutta digitaalinen viestintä antaa uusia tapoja hoitaa yhteydenpitoa ja tiedottamista yhdistyksen jäsenistöön. Tässä suhteessa printtilehti tiedotusvälineenä on jäämässä taustalle. Esimerkkeinä yhdistyksen verkkosivut ja postituslistat hoitavat hyvin tiedottamisen. Lehden rooli korostuu erityistiedon välittäjänä, sellaisen tiedon, jota ei digitaalisesta maailmasta ole löydettävissä ainakaan helposti. Informaation tulee lukijan kannalta olla mielenkiintoista, arvokasta ja ymmärrettävää. Lukukokemuksen tulee antaa merkityksellinen kokemus – mitään sanomattomuus ei kanna lehteä pitkälle.

Lehti tuo myös lisäarvoa maanpuolustushengen vaalijana ja kohottajana. Lehti yksinään ei voi kantaa maanpuolustushenkeä, se lähteen yhdistyksen kokonaistoiminnasta. Kuitenkin oma lehti vahvistaa yhdistyksen maanpuolustusaatteellista toimintaa ja lisää kokemusta yhteenkuuluvuudesta.

Pitääkö tiedollisesti korkeatasoisen ja maanpuolustusaatetta vahvistavan lehden olla printtiversio vai ajaako digiversio saman asian? Kaikki edellä sanottu sisällön korkealaatuisuudesta ja yhteenkuuluvuuden vahvistamisesta pätevät niin printti- kuin digiversioon. Kysymys on lukukokemuksesta. Minä kuulun siihen sukupolveen, joka haluaa lukea aamun sanomalehden printtiversiona ja Viestimiehen nykymuotoisena sohvalla istuen.

Uutiskirjeet 1400- ja 1500-lukujen taitteessa ovat nykyisten sanomalehtien esi-isiä. Niiden keskeinen tavoite oli tiedonjakaminen. 1700-luvun vallankumousten aikoina lehdistä tuli myös aatteen levittäjiä, olihan keskiluokka jo tuolloin luku- ja kirjoitustaitoista. 1800-luvulta lähtien lehdistöstä muodostui poliittisen vaikuttamisen väline. 2000-luvulle saakka fyysinen versio lehdestä on ollut ainoa mahdollisuus, nyt tiedon jakamisen, aatteen levittämisen ja vaikuttamisen voidaan tehdä myös digitaalisilla välineillä.

Enemmän kuin pohdintaa printtimedian tulevaisuudesta tarvitaan analyysiä median sisällöistä. Minusta oleellisempaa on keskittyä korkeatasoiseen sisältötuotantoon, tiedon jakamiseen ja aatteen vahvistamiseen, kuin keskittyä vain jakelukanavan analogisuus-digitaalisuuspohdintaan. Teknologian kehitys osoittaa, että disruptiiviset teknologiat ovat syrjäyttäneet vanhoja teknologioita, kun aika muutokselle on kypsä. Tuskin kovin moni meistä haluaa palata vanhoihin numerolevypuhelimiin ja käsivälitteiseen puheluliikenteeseen nykyisen mobiiliviestinnän aikana.

Maanpuolustuslehdillä tulee seurata näitä muutostrendejä ja lukijakuntansa odotuksia. Kyky seurata aikaansa on yhdistysten ja niiden julkaisuiden selviytymisen perusehto.

Samalla, kun omasta puolestani onnittelen 70-vuotiasta Viestimiestä, uskon Viestimiehen laadukkaaseen ja korkeatasoiseen sisältötuotantoon myös tulevaisuudessa.

VM

Kenraalimajuri Leo Ekberg

Näinä päivinä kaksi vuotta sitten päättyneet sodat veivät viestiaselajia eteenpäin. Ihannoimatta sotaa sinänsä on meidän kuitenkin tunnustettava, että nämä sodat antoivat meille joukon arvokkaita kokemuksia. Nämä kokemukset ovat aselajillemme ja varsinkin viestivälineistön kehittämiselle suorastaan perustavaa laatua olevia. Varmaa on, että ilman näitä sotia olisimme tuskin paremmassa asemassa kuin vuonna 1939, käytännöllisesti katsoen vailla omakohtaisia kokemuksia ja vailla riittäviä, nykyajan vaatimukset jotakuinkin täyttäviä viestivälineitä.

Maamme taloudellisesti vaikean tilanteen vuoksi ja meistä itsestämme riippumattomista tekijöistä johtuen emme lähivuosina voi jatkaa hyvälle alulle saatua aselajimme kehitystä. Pienen armeijan mahdollisuudet ovat aina rajoitetummat kuin suurvaltojen armeijoiden, joten emme voi seurata kehitystä niin kiinteästi kuin se olisi aselajimme kannalta, ei ainoastaan suotavaa, vaan jopa välttämätöntä. Jokaisen viestiupseerinasianharrastuksella on siksi mitä suurin merkitys ja sen turvin voidaan korjata ja korvata paljon sellaista, joka muuten jäisi toteutumatta. Oma apu on paras apu. Viestiupseerikerholla on tässä suuret mahdollisuudet. Vetämällä toimintaansa mukaan reservissä olevat viestiupseerit ja insinöörit, jotka sota-aikana epäitsekkäällä ja määrätietoisella työllään monissa suhteissa vei viestipuolta eteenpäin, voi kerho suoriutua varsin vaativistakin tehtävistä. Olen vakuutettu, että reservissä olevat edelleenkin auliisti asettavat tietonsa ja taitonsa aselajimme käytettäväksi ja ilomielin ovat mukana kehittämässä omaa aselajiansa.

VIESTIMIES

70 vuotta sitten
nro 3 / 1946

Toinen tärkeä ja laaja työsarka, joka on kuin luotu Viestiupseerikerhoa varten, on sotakokemustemme kerääminen, seulominen ja järjestäminen. Toistuvista kehotuksista ja käskyistä huolimatta eivät viestikomentajat tai vastaavassa asemassa toimineet sodan kestäessä tuoreeltaan, sen enempää kuin sodan päätyttyäkään, lähettäneet sotakokemuksiaan Puolustusministeriöön. Näin ollen suurin osa näistä kokemuksista on edelleenkin kokemusten saavuttajien omana tietonaan ja poissa meidän ulottuviltamme. Upseeripulasta ja runsaista jokapäiväistä päiväjärjestystä täysin sekoittavista odottamattomista tehtävistä johtuen, ei PE:n viestiosasto ole saanut asiaa järjestettyä eikä erityistä upseeria saada tätä laajaa työtä johtamaan. Sotakokemusten kerääminen lähitulevaisuudessa, ennen kuin aselajimme kehitykselle välttämättömät tiedot ovat täydellisesti häipyneet kokemusten saavuttajien aivoista, on siksi mitä tärkeintä. Koottu ja käyttökelpoiseen muotoon saatettu aineisto palvelee paitsi aselajimme järjestystä myös välittömästi jokaista viestiupseeria, toimikoon hän sitten kouluttaja, johtajana tai kasvattajana.

Varsin tärkeitä ja kehittyviä tehtäviä on Viestiupseerikerholla siis kylliksi edessään. Hyvät saavutukset kannustakoot aina uusiin ja älkäämme antako muualla kehitettyjen viimeisten saavutusten luisua ulottuviltamme. Toivon, että kerhosta muodostuisi aselajimme kaikkien upseerien luja yhteenliittymä, joka jäseniensä kehittäjänä ja kouluttajana on lähitulevaisuudessa varsin varteenotettava tekijä. Toivotan kerholle parhainta menestystä tärkeiden tehtäviensä suorittamisessa ja uskon tulevaisuudessa voivani viettää monta innoittavaa ja antoisaa hetkeä kerhon keskuudessa.

Artikkelin toimittaja: Veli-Matti Pesola

VM

Henkilöasiat:

Siirrot ja tehtävään määräämiset

Siirrot ja tehtävään määräämiset

- eversti **Pasi Välimäki** (PEKANSLIA) Pääesikunnan operatiiviselle osastolle erityistehtävään 1.7.2016 lukien

- kapteeni **Marko Saarela** (PORPR) Puolustusvoimien palvelukeskukseen määräajaksi 1.8.2016-31.12.2017

- majuri **Jani Liitola** (MPKK) Pääesikunnan johtamisjärjestelmäosastolle osastoesiupseeriksi 1.9.2016 lukien

- majuri **Risto Linsuri** (PVJJK) Puolustusvoimien johtamisjärjestelmäkeskuksessa suunnitteluosaston apulaisosastopäälliköksi 1.11.2016 lukien

- kapteeni **Jukka Heinänen** (PEKANSLIA) Maasotakouluun 1.12.2016 lukien

Ylennykset 4.6.2016

Everstiksi
- everstiluutnantti **Harri Suni**

Everstiluutnantiksi
- majuri **Tapani Keskitalo**
- majuri **Tero Palokangas**

Majuriksi
- kapteeni **Heikki Lantto**
- kapteeni res. **Jari Vanhatapio**

Insinöörimajuriksi
- insinöörikapteeni **Marko Saarela**

Kapteeniksi
- yliluutnantti **Kalle Hyvönen**

Yliluutnantiksi
- luutnantti res. **Ossi Ikonen**
- luutnantti res. **Lauri Tolvas**

Luutnantiksi
- vänrikki res. **Eino Jauhiainen**
- vänrikki res. **Pentti Launonen**

Reserviin

- everstiluutnantti **Jari Rantapelkonen** 1.6.2016

Onnittelemme merkkipäivänä

Everstiluutnantti Jukka-Pekka Virtanen 50 vuotta

Kotkassa syntynyt everstiluutnantti Jukka-Pekka Virtanen täyttää 50 vuotta 16.9.2016. Kadettikurssin 74 viestilinjalta vuonna 1990 valmistuttuaan hän on toiminut monissa viesti- ja johtamisjärjestelmäalan tehtävissä. Tutuksi ovat tulleet monet joukko-osastot ja eritasoiset esikunnat kuin myös muu valtionhallinto. Vapaa-aika kuluu veneilyn, musiikin ja vapaaehtoisen maanpuolustustyön parissa.

Jukka-Pekka Virtanen syntyi 16.9.1966 Kotkassa. Hän kirjoitti ylioppilaaksi vuonna 1985 Langinkosken lukiosta ja suoritti varusmiespalveluksen Viestirykmentissä 1986-87. Varusmiespalveluksen jälkeen hän haki kadettikouluun ja aloitti samana vuonna kadettikurssi 74:llä. Virtanen valmistui viestilinjalta vuonna 1990. Ensimmäinen palveluspaikka oli Reserviupseerikoulun Viestikomppania ja siellä joukkueen johtajan tehtävä, jossa hän toimi vuoteen 1993 saakka. Vuonna 1994 suoritetun viimeisen viestikapteenikurssin jälkeen hän siirtyi samaisen komppanian varapäälliköksi. Esiupseerikurssin Virtanen kävi vuonna 1998 ja heti sen jälkeen yleisesikuntaupseerikurssin. Kurssin jälkeen hän toimi osastoesiupseerina Pääesikunnan viestiosastolla vuosina 1999-2000. Pääesikunnasta hän siirtyi viestiopettajaksi Maanpuolustuskorkeakoululle, josta edelleen vuonna 2004 Riihimäelle Viesti- ja sähköteknisen koulun (VSK) apulaisjohtajaksi. Samana vuonna Virtanen palveli kansainvälisissä tehtävissä ja toimi viestipäällikkönä monikansallisessa prikaatissa Kosovossa. Hän palasi kansainvälisistä tehtävistä takaisin VSK:lle. Vuonna 2006 alkoi toinen kierros Pääesikunnassa ja Virtanen toimi Pääesikunnan johtamisjärjestelmäosastolla Liikenne- ja viestintäministeriön yhteysupseerina. Pääesikunnasta hän

siirtyi Itä-Suomen viestipataljoonan komentajaksi Karjalan prikaatiin vuosiksi 2009-12. Komentajan tehtävästä seurasi siirto Mikkeliin Maavoimien esikuntaan, jossa hän toimi useassa eri tehtävässä - viimeiseksi johtamisjärjestelmäosastolla palvelupäällikkönä. Virtanen aloitti vuoden 2016 alusta Puolustusvoimien johtamisjärjestelmäkeskuksen esikuntapäällikkönä, jossa tehtävässä edelleen toimii.

Virtanen pitää mielenkiintoisimpana tehtävänä LVM:n yhteysupseerin tehtävää, jossa sai tutustua läheisesti muun valtionhallinnon toimintaan. Haastavin tehtävistä on ollut pataljoonan komentajuus. Tehtävässä tuli eteen monipuolisia johtamis- ja suunnittelutehtäviä sekä käytännönläheistä toimintaa valmiusprikaatin kehyksessä.

Vapaa-ajalla Virtanen rentoutuu harrastusten parissa. Lähellä sydäntä ovat veneily, musiikki ja vapaaehtoinen maanpuolustustyö. Veneilijän kausi alkaa varhain keväällä veneen kunnostamisella. Puuvene vaatii jokavuotista huolenpitoa. Veneilykausi jatkuu pitkään syksyyn. Ajotunteja voi kaudessa tulla jopa 180 ja yöpymisiä veneessä jopa kuukauden verran. Muusikin osalta harrastuksiin on kuulunut rocklaulanta 80-luvun alusta lähtien. Viimeiset parikymmentä vuotta hän on laulanut vuonna 1994 perustetussa southern rockille omistautuneessa Rising sun -yhtyeessä. Musiikki on hyvä vastapaino työlle sekä pysyvä yhdysside kavereihin. Keikkoja tehdään noin kerran kuussa. Vapaaehtoinen maanpuolustustyö lähti käyntiin vuonna 2003, kun Virtanen aloitti Viestimies-lehden henkilötoimittajana ja Viestiupseeriyhdistyksen henkilösihteerinä. Vuosina 2007-12 hän toimi Viestimies-lehden päätoimittajana ja samaan aikaan myös VUY:n hallituksessa. Hän oli Viestikiltojen liiton valtuuskunnan jäsen vuosina 2010-14, Viestikiltojen liiton hallituksen varapuheenjohtaja vuosina 2014-15 ja puheenjohtaja vuodesta 2016 alkaen.

Ansioistaan Virtaselle on myönnetty SVR R1, SL R1, Sam, Mpm, Viestir sk ja NATOm Kosovo.

Merkkipäivää Virtanen viettää läheistensä seurassa.

Viestimies-lehti esittää lämpimät onnittelut entiselle päätoimittajalleen merkkipäivän johdosta.

VM

MUSEO **MILITARIA**
THE ARTILLERY, ENGINEER AND SIGNALS MUSEUM OF FINLAND

Teemaseminaari

Vapaus valita vai pakko sitoutua –

Suomen mahdollisuudet Venäjän – EU:n – Naton – USA:n ristiaallokossa?

Museo Mliitariassa 29.10.2016 klo 12.30–16.00

Vanhankaupunginkatu 19, Hämeenlinna

www.museomilitaria.fi

0. Tilaisuuden avaus:
juontaja ja puheenjohtaja kenraalimajuri **Pertti Salminen**

1. Ensimmäinen alustus:
Suomen turvallisuus- ja puolustuspolitiikan kulmakivet II maailman sodan jälkeen
YYA-sopimus
Neuvostoliiton hajoaminen / Saksojen yhdistyminen
EU-sopimus
Nato-kumppanuussopimus
Haetaan vastausta kysymykseen, mitkä asiat ovat menneitä ja mitkä ovat vielä voimissaan. Miten aikaisemmat toimet voivat vaikuttaa tulevaan. Taustalla ajatus, jos et tunne historiaa, et voi arvioida tulevaa.Lähestymiskulma historiasta. Alustuksen pituus 30–40 minuuttia muutamine kysymyksineen.
Alustaja: ministeri **Jaakko Iloniemi.**

2. Toinen alustus:
Muuttuva turvallisuuspoliittinen ympäristö –
muutokset ja vaikutus Suomen valinnan vapauteen
EU:n tavoitteet ja toiminta
Venäjän tavoitteet ja toiminta
USA tavoitteet ja toiminta
Muuttuva Nato
Mitä meidän suomalaisten pitäisi tästä ymmärtää
Lähestymiskulma kansainvälisestä ja lähiympäristöstä – syvempää sisältöä sille, mitä päivittäin tv:stä katsotaan ja lehdistä luetaan. Alustuksen pituus 30–40 minuuttia muutamine kysymyksineen.
Alustaja: vanhempi tutkija **Kristi Raik,** Ulkopoliittinen Instituutti.

3. Kolmas alustus:
Muuttuva Suomen talouspoliittinen ympäristö – talouden monet kytkökset
Suomen taloudellisen ympäristön muutokset
Suomen talouspolitiikan liikkumavara
Mistä kasvun edellytykset?
Kansainvälisten kriisien kytkökset talouspolitiikkaan
Lyhyt katsaus Suomen talouspoliittisen ympäristön muutoksiin – miten monin tavoin Suomen talous kytkeytyy kansainväliseen talouteen ja talouspolitiikkaan. Miten taloudelliset ja poliittiset kriisit heijastuvat Suomen talouteen. Alustuksen pituus 30–40 minuuttia muutamine kysymyksineen.
Alustaja: neuvonantaja **Juuso Vanhanen**, Suomen Pankki.

KAHVITAUKO (30 min)

4. Paneelikeskustelu ja yleisökysymykset *(30–40 min)*
a. kommenttipuheenvuoro kenraalimajuri Pertti Salminen b. alustajat
Yhteenveto ja päättäminen: kenraalimajuri **Pertti Salminen**

***5. Seminaarin hinta:* 50 €.** Seminaariin **ilmoittaudutaan 26.10.2016 mennessä**
maksamalla 50€ Museo Militarian tilille: Etelä-Hämeen Osuuspankki **FI35 5680 0020 3056 25.**
Maksuviite: Teemaseminaari 2016. Viitteeseen myös seminaariin osallistujan nimi ja sähköposti tai puhelinnumero.

Tykkihallissa on käytettävissä 150 paikkaa, jotka täytetään ilmoittautumisjärjestyksessä.

Järjestäjät:
Suomen Tykistö-, Pioneeri- ja Viestimuseoyhdistys ry Suomen Sotatieteellinen Seura ry:n avustuksella.
Lisätietoja:
Esko Hasila, Suomen Tykistö-, Pioneeri- ja Viestimuseoyhdistys ry:n hallituksen puheenjohtaja, *esko.hasila@kolumbus.fi*
Lasse Otranen, Suomen Tykistö-, Pioneeri- ja Viestimuseoyhdistys ry:n hallituksen varapuheenjohtaja, *lasse.otranen@skal.fi*
Sirkka Ojala, Museo Militaria, museosihteeri, *sirkka.ojala@museomilitaria.fi*, puh 050 3688 460

Koskee nykyisiä ja uusia asiakkaita. *Puheaika/viestietu norm.hintaisiin puheluihin teksti- ja multimediaviesteihin kotimaassa. Liittymän kuukausimaksu sisältää 500 Mt/kk tiedonsiirtoa EU-vyöhykkeellä. 500 Mt ylittävä datakäyttö EU-vyöhykkeelle veloitetaan roaminghinnaston mukaisesti. Tilatessasi liittymän annat sähköisen suoramarkkinointiluvan (liittymä ilman markkinointilupaa +1 €/kk). Tiedonsiirtonopeus vaihtelee riippuen päätelaitteen ominaisuuksista, sijainnista ja verkon kuormituksesta. Nopeuden vaihteluväli 3G-verkossa 0,4–25 Mbit/s ja 4G-verkossa 5–80 Mbit/s. Tarkista verkon peittoalue: elisa.fi/kuuluvuus. Ei määräaikaisuutta. Liittymien avausmaksu 3,90 €.

L2
Posti Oy

Posti Green

Draka

Kautta kiven ja kannon

Drakan optinen kenttäviestikaapeli taipuu hankalaankin maastoon. Ainutlaatuisen BendBright^{XS} -kuidun ansiosta kaapelilla on poikkeuksellisen hyvä taivutussietoisuus ja se säilyttää toimintavarmuutensa tiukoissakin mutkissa. Liikuteltavilla valokaapeleilla on mahdollista rakentaa luotettava viestintäjärjestelmä nopeasti ja vaivattomasti juuri sinne, missä yhteyksiä tarvitaan. Maalla, vesistössä ja ilmassa. Vaativissa olosuhteissa turvallinen laajakaista rakennetaan kustannustehokkaasti Drakan yksimuoto- ja monimuotokaapeleilla.

Prysmian Group

www.draka.fi