Viestimies

Viestiupseeriyhdistyksen julkaisu 75. vsk Numero 3 Syksy 2020

Teema: ”Arjen välineet - hyödyt sotilaallisessa toiminnassa”

5-G tietoturvallisuuden haasteet, sivu 6

Potilaskortit sähköisiksi, sivu 10

Tietotulvaa ja tietoturvaa arjen ehdoilla, sivu 16

www.viestiupseeriyhdistys.fi

www.combitech.fi

Viestimies-lehti

Päätoimittaja
Samuli Terämä
p 050 3399038
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Hanna Liitola
p 040 5930675
henkilotoimittaja@viestiupseeriyhdistys.fi

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

Toimituskunta
Heiskanen Mikko (pj)
Blomqvist Reima
Isomäki Pekka
Mikkonen Mauri
Petäjäinen Juha
Putkonen Jyri
Ståhlberg Mika
Suokko Harri
Valkola Eero
Wirman Kari
Yli-Äyhö Janne

Toimituksen osoite:
Päivölänrinne 7 A 1
04220 Kerava

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

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

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

Painopaikka
Newprint Oy, Raisio
p 010 231 2600

ISSN 0357-2153

Kansikuva: Arjenvälineitä, kuva: Viestimies

Tässä numerossa

5 Pääkirjoitus: Maskilla vai ilman?

6 5-G tietoturvallisuuden haasteet.

10 Potilaskortit sähköisiksi.

16 Tietotulvaa ja tietoturvaa arjen ehdoilla.

21 Matrix-protokolla ja arjen ratkaisuista koottujen viestijärjestelmien mahdollisuuksia.

25 Jääkärieversti Birger Homén - viestikoulutuksen uranuurtaja.

27 Kybernetiikka: Informaatioaikakauden ja kybersodankäynnin ajattelumalli? (osa 2/2)

33 Lyhyesti.

35 Analysaattori.

36 Henkilöasiat.

37 Viestimies 50 vuotta sitten.

38 Vuoden viestiupseeri: Raija Pihlainen.

Seuraavan numeron aineistopäivä on 16.10.2020. Lehti ilmestyy viikolla 49.

Fujitsu luo osallistavaa, kestävää ja luotettavaa tulevaisuutta

Turvallisuus syntyy luottamuksesta, osaamisesta ja vastuun kantamisesta. Fujitsu on sitoutunut edistämään ict-ratkaisuja, jotka auttavat organisaatioita ja yrityksiä rakentamaan tulevaisuutta turvallisesti ja kestävästi. Monipuolisen teknologia- ja palveluosaamisemme avulla autamme asiakkaitamme pysymään kehityksen kärjessä.

Teemme kaikkemme, jotta asiakkaamme saavat meiltä aina erinomaista palvelua riippumatta teknologiasta, hankkeen koosta tai asiakkaan tilanteesta. Tarjoamme asiakkaan luottokumppanin roolissa ict-ratkaisut tiedon saatavuuteen, integrointiin, jalostamiseen ja hyödyntämiseen, jotta yhteiskunta toimii aina – vaativissakin tilanteissa.

Lue lisää: **www.fujitsu.com/fi**

FUJITSU

Maskilla vai ilman?

Koronakeväästä selvittiin vaihtelevalla menestyksellä ja yhteiskuntaa avattiin vähitellen tartuntalukujen hiipuessa. Nyt syksyn saapuessa pandemia näyttäisi nostavan taas päätään. Suomalaiset ovat kurinalaista kansaa – noin lähtökohtaisesti. Käsiä on pesty, on yskitty hihaan ja niin edelleen. Epävarmuus leijuu kuitenkin ilmassa, miten tilanne kehittyy syksyn aikana. Voidaanko rajoituksia purkaa vai tuleeko kiristyksiä taas kevään malliin. Mahdollisilla kiristyksillä on vaikutuksia koko yhteiskuntaan ja sen toimintakykyyn. Keväällä lanseerattu ”Korona-appi” eli Koronavilkku julkaistiin 31.8.2020. Kahden ensimmäisen päivän aikana sovellusta ladattiin jo miljoona kertaa. Tätä kirjoittaessa konkreettisia tuloksia sovelluksen toimivuudesta tartuntaketjujen jäljittämisessä ei vielä ole, mutta toivottavasti se tuo merkittävän lisän potentiaalisten altistuneiden jäljittämisessä sekä lisätartuntojen ehkäisemisessä. Toisin sanoen perus arjen väline hyödynnettäväksi koko kansan kriisinsiedon parantamiseksi.

Tämän lehden teemana on arjen välineiden hyödyntäminen. Paneudumme aihepiiriin kolmessa eri artikkelissa. Arjen välineet, kuten kaikki muukin tietotekniikkaan liittyvä, koskettelee aina myös tietoturvaa. Miten suojaudumme kaikilta niiltä mahdollisilta hyökkäysvektoreilta, joita käyttämämme palvelut ja laitteet käyttävät? Tähän tuskin löytyy aukotonta vastausta, mutta jo maalaisjärjen käyttö ja sopiva ennakkoluuloisuus sähköpostiin kilahteleviin tarjouksiin auttaa pitkälle. Lisäksi on syytä huolehtia perusvirustorjunnasta ja ehkä hyödyntää saatavilla olevia VPN-ratkaisuja sekä salasanageneraattoreita ja taltioita. Jokaiseen käytettävään tiliin tai palveluun ei ole syytä käyttää samaa salasanaa tai sen varianttia.

Jyväskylän yliopistossa elokuun lopussa julkaistussa väitöskirjassa Jouni Pöyhönen (insinöörieversti evp) käsitteli kyberturvallisuuden johtamista kriittisen infrastruktuurin yrityksissä ja organisaatioissa. Pöyhönen tutkii väitöksessään, miten organisaatiokohtaisilla toimenpiteillä kyetään lisäämään kriittisen infrastruktuurin suojaamista ja

sitä kautta muun muassa kokonaisturvallisuutta, huoltovarmuutta ja kilpailuetua. Tutkimuksessa korostetaan ihmisten eli organisaatioiden työntekijöiden osuutta kyberturvallisuuden rakentamisessa. Yhteistyötä ja kumppanoitumista unohtamatta. Ihmiset ovat usein heikoin lenkki kyberturvallisuuden varmistamisessa.

Turvallisuudesta puhuttaessa on hyvä muistaa myös terveyteen liittyvät asiat osana kokonaisturvallisuutta. Edellisessä numerossa kerroin ilmiöstä, jossa esitettiin väitteitä 5G-verkon tukiasemien kytköksestä koronaviruksen leviämiseen. Asioilla ei liene yhteyttä, mutta huoli elää edelleen 5G:n turvallisuudesta ja terveysvaikutuksista. Tutkimustietoa on vielä varsin vähän tarjolla käytännön ympäristöistä. Asian tiimoilta on vireillä kansalaisaloite. Aika näyttää eteneekö asia eduskuntakäsittelyyn asti.

Riskit lisääntyvät, kun 5G vähitellen yleistyy ja sen hyödyntämän tekniikan sovellutukset kehittyvät. IoT (Internet of Things) eli esineiden internet lisääntyy kodeissa ja yhteiskunnassa. Turvallisuuskysymykset puhuttavat enenevissä määrin. Tietoturvayhtiöt tutkivat jatkuvasti sovelluksia mahdollisten tietoturva-aukkojen varalta. Mitä enemmän tutkitaan, sitä enemmän aukkoja löytyy. Tämä lienee luonnollinen seuraus. Esimerkkinä voidaan mainita puheohjattavat älykaiuttimet ja niiden ohjelmistot, kuten Alexa-virtuaaliavustajaohjelmisto. Ohjelmistoa voidaan käyttää muun muassa kodin automaatiojärjestelmien ohjaamiseen. Murtauduttuaan järjestelmään hyökkääjän olisi mahdollista käyttää uhrinsa henkilökohtaisia tietoja, kuten pankkitietoja, käyttäjätunnuksia, puhelinnumeroita ja niin edelleen. Kyseiset laitteet yleistyvät hiljalleen, ja mitä enemmän annamme tekniikalle valtaa ohjata kaikkea kodin elektroniikkaa, sitä suuremmaksi riskit niiden väärinkäytöksestä kasvavat. Suojautuminen vaatii paneutumista riskeihin ja niiden ennaltaehkäisyyn. 5G:n turvallisuudesta olemme saaneet lukea lehden palstoilla aiemmin ja aihepiiristä tulemme varmasti kuulemaan jatkossakin. Kokonaisuus on otettava haltuun, ettei yksi osa vaaranna kaikkea muuta hyödyllistä.

Uudelle polulle astuttiin myös Vuoden Viestiupseerin valinnassa. Vuoden Viestiupseeri on valittu vuodesta 2004 asti, ja olemme tottuneet siihen, että palkittu henkilö on toiminut sotilasvirassa. Nyt palkittu henkilö on siviili. Tehtävässään hän on edistänyt merkittävästi johtamisjärjestelmäalan kehitystä kaupallisen toiminnan kautta. Hankintapäällikkö Raija Pihlaisen haastattelu on luettavissa tämän lehden sivuilla.

Päätoimittaja

Samuli Terämä

TEKSTI JA KUVAT: RONNY BACKMAN, SILKE HOLTMANNS JA AAPO KALLIOLA

Ronny Backman on opinnäytetyöntekijä Nokia Bell Labsilla aiheesta "Luotettavien rautatieturvalaitteiden simulointi". Hän on siirtymässä Rejlersille jatkamaan rautatieturvallisuuden parissa. Hän on aiemmin palvellut Utin Jääkärirykmentissä noin 14 vuotta erikoisjoukko-operaattorina, kouluttajana ja esikunta-aliupseerina.

TkT Silke Holtmanns on toiminut pitkään tietoturvatutkijana Nokia Bell Labsilla, ja on nykyään 5G-turvallisuuden johtava tutkija AdaptiveMobile Securityllä. Hän on tutkinut kattavasti SS7, Diameter ja GTP -protokolliin kohdistuvia hyökkäyksiä ja niiden torjumista. Vuonna 2019 hänelle annettiin Suomen Leijonan ritarimerkki.

DI Aapo Kalliola on työskennellyt 2015 alkaen Nokia Bell Labsilla tietoturvatutkijana. Hänen tutkimusaiheensa keskittyvät IP-verkkojen liikenteeseen liittyviin hyökkäyksiin ja puolustusmekanismeihin sekä tunkeutumistestaamiseen.

5G-tietoturvallisuuden haasteet

Yleistä

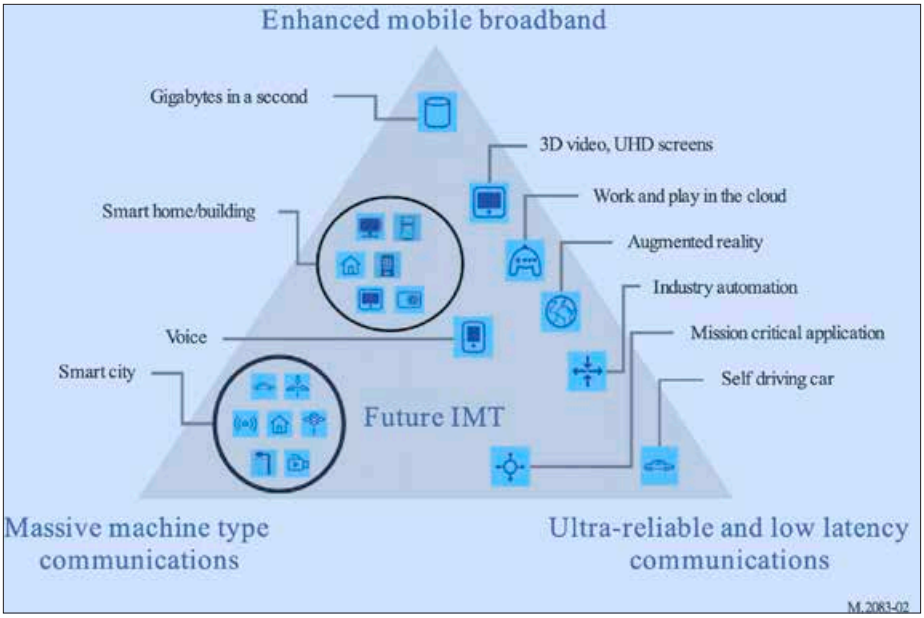
5G on mobiiliteknologian kehityksessä enemmän kuin vähäinen askel eteenpäin 4G-teknologiasta. 4G:n pääasiallinen tehtävä on ollut puhe- ja viestipalvelujen ohella kohtuullisen datasiirtonopeuden tarjoaminen lankaverkkoja suuremmalla viiveellä. 5G ei ole pelkästään nopeampi versio 4G:stä, vaan sekä käyttötarkoitusten kirjoltaan että verkon toteutustavoiltaan 5G laajenee kokonaan uusille alueille.

Kuva 1 havainnollistaa 5G:n palvelemia käyttötapauksia. 5G:n on tarkoitus tarjota päätelaitteelle tarvittaessa yli 10Gbps kaistanleveys alle 1 millisekunnin viiveellä ympäristössä, jossa laitteiden vaatima kaistanleveys on pinta-alayksikköä kohden äärimmäisillään tuhatkertainen nykyiseen verrattuna. Nämä laajennetut ominaisuudet mahdollistavat monia uusia käyttötarkoituksia, mm. itseajavien autojen, älykkäiden tehtaiden, täydennetyn todellisuuden sekä älykkäiden kaupunkiympäristöjen toteuttamisen mobiiliverkkoja hyödyntäen.

Verkkototeutuksessa 5G etenee aiemmasta pääosin diskreettejä verkkolaitteita sisältävästä verkosta virtualisoituun ympäristöön, joka muistuttaa enemmän pilvipalveluita kuin aiempia mobiiliverkkoja. Tämän muutoksen seurauksena esimerkiksi verkon loogisten osien erottaminen toisistaan fyysisesti riippumattomiksi komponenteiksi ei enää tapahdu itsestään, vaan vaatii erillisiä mekanismeja.

Hyökkäyspinta ja turvallisuusominaisuudet

Skaalautuvuus sekä käyttötarkoitusten laajuuden että suorituskyvyn osalta on 5G:n määrittävä piirre. Verkon toteutuk-



Kuva 1: 5G:n käyttötarkoitukset. lähde: ITU-R M.2083-02.

selta tämä vaatii uusien teknologioiden ja arkkitehtuurien hyödyntämistä, mikä aiheuttaa suuria muutoksia aiempaan 4G:n tässä vaiheessa hyvin tunnettuun turvallisuusympäristöön. 5G-verkkojärjestelmän hyökkäyspinta on järjestelmän monipuolisuuden vuoksi jo lähtökohtaisesti laajempi, ja lisäksi uudet lähestymistavat toteutuksessa muuttavat aiemmin tunnistettuja turvallisuusriskejä.

Eräs 5G-arkkitehtuuria määrittävä muutos aiempaan verrattuna on verkon toiminnallisten komponenttien virtualisoinnin lisääntyminen: Erillisten fyysisten laitteiden sijasta verkon sisäiset toiminnot ovat virtualisoituja palveluita, jotka viestivät keskenään standardoitujen rajapintojen välityksellä. Näiden palveluiden toteuttamisessa hyödynnetään Network Function Virtualization (NFV) ja Software Defined Networking (SDN) teknologioita, jotka ovat tuttuja nykyisistä pilviympäristöistä. Verkon palvelujen toteutustapojen muuttuessa näin joustavammiksi sisällytetään mobiiliverkkojen laajenevaan hyökkäyspintaan pilvipalvelujen tietoturvallisuusriskejä.

Olennainen ominaisuus 5G:ssä on tietoliikenteen käyttäjä- ja kontrollitasojen eriyttäminen (CUPS, Control and User Plane Separation). CUPS mahdollistaa käyttäjätason verkkotoimintojen hajauttamisen verkon ytimestä aivan verkon rajalle esimerkiksi tukiaseman läheisyydessä olevalle Edge-pilvipalvelimelle. Tämä osaltaan mahdollistaa Multi-access Edge Computing (MEC) -ratkaisut, joissa kolmansien osapuolien palveluita voidaan tarjota käyttäjille pienimmällä mahdollisella tiedonsiirtoviiveellä suoraan verkon laidalla sijaitsevilta palvelimilta. MEC:in toteuttaminen johtaa myös kriittisten palveluiden sijoittamiseen fyysisesti ja verkkotopologisesti hajautetusti, mikä lisää palveluiden sekä fyysisen ympäristön että datan koskemattomuuden ja verkko-/hallintayhteyksien turvaamisen kriittisyyttä. Jo nykytilanteessa on mahdollista aiheuttaa haittaa esimerkiksi kytkeytymällä heikosti lukitun tukiaseman sisäisiin portteihin, mutta ongelma laajenee vielä paljon merkittävämmäksi, jos samassa fyysisessä ympäristössä toimii alueen käyttäjille kriittisiä palveluita tarjoava pieni palvelinkeskus, joka sisältää arkaluontoista dataa.

5G-ympäristön myötä osa verkon toimintaan liittyvistä uhkista on kasvanut ja osa muuntunut. Yksittäisten laitteiden käytössä oleva kaistanleveys kasvaa dramaattisesti 5G:n myötä, ja lisäksi massiivinen esineiden internet (MIoT, Massive Internet of Things) lisää laitteiden lukumäärää, tiheyttä ja monimuotoisuutta valtavasti. Tämä luo riskin verkon kapasiteetin väärinkäytöstä esim. palvelunestohyökkäysten suorittamiseen kolmansia osapuolia, itse verkkoa tai verkkoon kytkettyjä esimerkiksi patterikapasiteetiltaan rajallisia laitteita vastaan.

Yhden fyysisen verkon ”viipalointi” (Network Slicing) useisiin loogisiin verkkoihin, jotka voivat olla eri käyttötarkoituksiin suunnattuja ja eri tahojen hallitsemia. Näin ollen on mahdollista, että yhden verkon palveluita tarjoavat useat virtuaaliset verkko-operaattorit samanaikaisesti. Koska nämä käyttäjille näkyvät verkot pohjimmiltaan jakavat saman fyysisen laitteiston on riskinä, että turvallisuusongelmat yhdessä viipaleessa vaikuttavat negatiivisesti myös muihin verkkoviipaleisiin. Yksinkertaisena esimerkkinä yhden viipaleen aiheuttama ylikuormitus jaetun fyysisen palvelimen laskentakapasiteetissa altistaa muiden viipaleiden palvelut alentuneelle suorituskyvylle, ellei kapasiteetin reiluun jakoon ole vankkoja mekanismeja. Verkkoviipaleiden välille voi myös muodostua ei-toivottuja yhteyksiä jos päätelaite voi ottaa yhteyden samanaikaisesti kahteen tai useampaan viipaleeseen ja välittää liikennettä näiden välillä.

IP-pohjainen osoitteistus saattaa altistaa verkon komponentit aiempaa helpommalle näkyvyydelle mahdollisten hyökkääjien suuntaan, etenkin jos verkon osoitteistus toteutetaan IPv6:lla. Myös verkkopinon komponenttien lisääntyvä yhteneväisyys laajemman IT-maailman kanssa altistaa mobiiliverkon toteutukset laajemmalti yleisessä käytössä olevien ohjelmistojen tietoturvaongelmille.

Havaittujen uusien turvallisuusuhkien torjumiseksi 5G-ympäristössä on käytössä muunmuassa uusia turvallisuusominaisuuksia. Verkkoliikenteen kontrollitaso on aiempaa paremmin suojattu: verkon komponenttien välinen sertifikaatteja hyödyntävä Transport Layer Security (TLS) -pohjainen salaus ja tunnistautuminen tarjoaa varmuuden kontrolliviestinnän luottamuksellisuudesta ja eheydestä. Aiemmin avoimemmin toteutetut operaattoriverkkojen väliset verkkovierailujen kontrolliyhteydet kulkevat Security Edge Protection Proxyn (SEPP) kautta, mikä vähentää muunmuassa käyttäjiin kohdistuvan urkinnan riskiä. 5G:n järjestelmätason suojausarkkitehtuuria on tarkemmin eritelty Viestimies-lehden 4/2019 artikkelissa ”5G:n tietoturvallisuus”.

5G-teknologian määrittelyssä suoraan huomioitujen turvallisuusominaisuuksien lisäksi turvallinen mobiiliverkko vaatii verkkojen valmistajilta paljon turvallisuusosaamista ja lisäominaisuuksien toteuttamista. Kyberhyökkäykset kehittyvät ja monipuolistuvat jatkuvasti, eikä staattisilla turvallisuusratkaisuilla voida enää turvata verkkojen tai niihin kytkeytyneiden laitteiden toimintavarmuutta. Turvallisuusriskien hallinta vaatii käytännössä verkossa jatkuvaa verkon tapahtumien seurantaa ja analysointia, jotta hyökkäyksiä voidaan tunnistaa, torjua ja parhaassa tapauksessa myös ennustaa ja ennaltaehkäistä. Valtavan datamäärän hallitseminen vaatii pitkälti automatisoituja turvallisuusratkaisuja, joissa useat yhteensopivat turvallisuuskomponentit keskitetysti johdettuina tunnistavat uhkia ja toteuttavat torjuntatoimenpiteitä.

Teknologioiden konvergenssi

Mobiiliverkkojen kehityksessä sukupolvesta seuraavaan trendinä on ollut verkon protokollapinojen konvergoituminen laajemman informaatioteknologia-alan suuntaan. Kuvassa 2 on nähtävissä tästä esimerkki verkkoytimeen liittyvien hallintaliikenteen protokollien yhteydessä. Noin 40-vuotias Signaling System 7 (SS7) on käytössä pääasiassa 2G/GSM -operaattoreiden välisen roaming-yhteyden luomiseen, minkä lisäksi se mahdollistaa mm. SMS-viestinnän. SS7-protokollapinossa alemmat kerrokset on toteutettu Message Transfer Part (MTP) -protokollalla, joka on määritelty SS7:aa varten. SIGTRAN on SS7:n laajennus, jossa protokollapinon pohjimmaiset kerrokset käyttävät jo Ethernet/IP-pohjaista viestintää, ja verkkokerrokseen määriteltiin uusi laajempaankin käyttöön päätynyt Stream Control Transmission Protocol (SCTP). Kehitys on jatkunut 4G/LTE-sukupolveen, jossa SS7:aa vastaavat toiminnot toteutetaan paremmin suojatulla Diameter-protokollalla, jonka viestiliikenne kulkee täysin IP-pohjaisessa verkossa ilman MTP-protokollan osia. Kattava yhdistyminen jokapäiväisten IT-palveluiden teknologioihin on nähtävissä 5G:n Service Based Interface (SBI) -viestirajapinnassa, jota käyttäen verkon ytimen Service Based Architecture (SBA) -komponentit viestivät keskenään. Tämä viestintä tapahtuu Representational State Transfer (REST)-rajapinnan kautta HTTP/2-protokollaa käyttäen.

Laajalti IT-maailmassa käytössä olevien protokollien ja arkkitehtuuriratkaisujen hyödyntäminen mobiiliverkkojen toteutuksessa on hyödyllistä: ei ole tarvetta kehittää uusia ratkaisuja, mikäli tarpeeseen löytyy olemassa oleva ratkaisu. Kääntöpuolena helppouteen sisältyy kuitenkin riski toteutusvirheiden uusimisesta ja uusiutumisesta siirrettäessä ratkaisuja

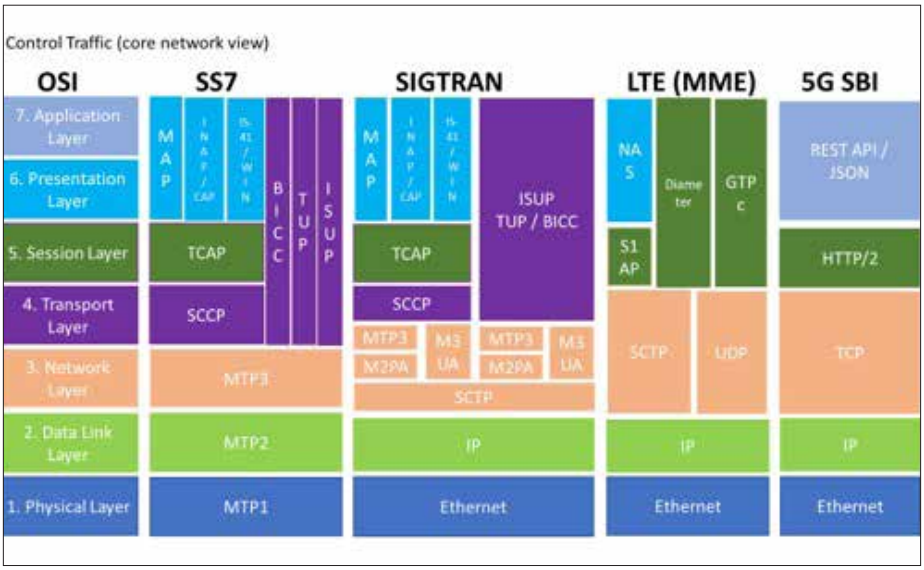
telekommunikaatioympäristöön. Täysin uusien teknologioiden kohdalla riskiä lisäävät myös toteutusten turvallisuuteen vaikuttavat lastentaudit. Esimerkiksi REST-rajapintojen turvallisesta toteuttamisesta on IT-maailmassa yli vuosikymmenen kokemus ja tämän kokemuksen täysimittainen hyödyntäminen on olennaista rajapintojen toteutuksessa mobiiliverkkojen ytimessä. Toteutettaessa tuoreita teknologioita vastaavaa kokemuspohjaa ei vielä ole olemassa ja siten niiden käyttöönottoon sisältyy korkeampi riski. Käytännön esimerkkinä HTTP/2-protokollan toteutukset yleisissä kuormanhallinta- ja palvelinohjelmistoissa ovat hiljattain kärsineet suorituskykyongelmista ja suoranaisista haavoittuvuuksista palvelunestohyökkäyksiä vastaan.

Luotettavuuden haasteet

5G:n myötä perinteinen suljettu rajapinta teleoperaattoriverkkoon on avautumassa ja protokollatasolla siirrytään lähemmäs julkista internetiä, mikä luo uusia turvallisuushaasteita. Yleinen tietämättömyys aiheesta on suojannut verkkoja tähän asti, mutta 5G:n myötä tämä muuttuu niin hyvässä kuin pahassa. Televerkon infrastruktuurin osalta siirrytään enemmän pilvipalvelu-ajattelumalliin, jossa eri toimijat voivat hyödyntää infrastruktuuria luomalla omia verkkoja virtualisoinnin avulla. Myös laskentatehoa vaativien toimintojen siirtämistä osaksi infrastruktuuria on suunniteltu, mikä edellyttää luotettavuuden osalta yhteneväisyyttä datakeskustoiminnan kanssa: luotettavuus on pystyttävä todentamaan rautatasolta asti.

Millä tekniikalla luotettavuutta voidaan todentaa? Perinteisesti tämä on toteutettu varmistamalla, että laiteajurin tai sovelluksen tiiviste vastaa allekirjoitetun sertifikaatin tiivistettä. Epäonnistunut varmistus pysäyttää järjestelmän käynnistymisen tai siirtää sen rajoitettuun toimintatilaan turvallisuuskäytännön mukaisesti. Tämän tekniikan rajallisuutta ja sertifikaatinhallinnan vaativuutta on kierretty yhä enenevässä määrin vanhalla tekniikalla: Trusted Platform Module (TPM) on uuden 2.0 spesifikaation myötä saavuttanut jalansijaa niin datakeskuksissa kuin käyttäjälaitteissakin, mikä luo uusia mahdollisuuksia luotettavuuden todentamiselle.

Moduulin tärkeimpiä ominaisuuksia ovat laiteidentiteetti, avainhallinta ja suojatut alustarekisterit. Alustarekisteriin tallennetaan käynnistyksen yhteydessä merkintä turvallisuuden kannalta olennaisista laiteajureista ja -sovelluksista. Lisäksi



Kuva 2: Protokollapinojen evoluutio.

alustarekisteriin luodaan lokitiedosto, jonka eheyttä voidaan myöhemmin kontrolloida alustarekisterin ja avaininfrastruktuurin avulla. Laiteidentiteetti on toteutettu sisäänrakennetulla epäsymmetrisellä avaimella, jonka yksityistä osaa voi käyttää ainoastaan moduuliin sisällä. Moduulin avainhallinnalla on mahdollista luoda myös uusia avaimia, joilla on samoja ominaisuuksia kuin edellä mainitulla avaimella.

Hyödynnettäessä rajoitettua avainta on mahdollista luotettavasti raportoida laitteen käynnistyksestä siteeraamalla alustarekisteriä; sitaatti vastaanotetaan todennuspalvelussa, joka voi seurata laitteen tilaa käynnistyksestä toiseen. Huomionarvoista on, että sitaattia voidaan jakaa turvallisesti laiteomistajan organisaation ulkopuolelle, mikä mahdollistaa luotettavuuden todentamisen joustavan valvonnan. Etuna on, ettei enää tarvitse pelkästään luottaa siihen, että laite on luotettava, mikäli verifiointi on onnistunut käynnistyksen yhteydessä. Tämän seurauksena loppukäyttäjällä on työkalu alustan ja sovelluskuormaa ajavan sovelluspinon todentamiseen.

Edellisten vuosikymmenien aikana sovellusturvallisuus on ottanut ison harppauksen eteenpäin. Kehitys on lähtenyt liikkeellä kysynnän mukaan: ylimmät sovelluskerrokset ovat olleet jatkuvan hyökkäyksen kohteena ja siten myös jatkuvan turvallisuuskehityksen piirissä. Ylimmän kerroksen vahvistumisen seurauksena on pienin askelin siirrytty sovelluspinokerroksissa alaspäin hyökkäyksien osalta, kuten kuvassa 3 näkyy. Tämä vaatii hyökkääjältä tyypillisesti korkeatasoisempaa osaamista, mutta voi olla investointina hyökkääjän näkökulmasta järkevä koska ylempi taso on yleensä vaarassa alemman tason pettäessä. Alemmalla tasolla vaikutus on myös potentiaalisesti laajempi, koska eristysteknologiat ovat kehittyneet varsin hyvin ja siten vaikuttavuus ylemmällä sovellustasolla on rajallisempi.

Sovellustason jälkeen myös käyttöjärjestelmien turvallisuus on jo parantunut, ja parhaillaan seuraavana on vuorossa laiteajuritaso. Turvallisuuden parantaminen vaatii työkaluja, joista yksi on laiteajurien eheyden valvonta. On nähtävissä, että tulevaisuudessa myös viimeinen taso, rautataso, tulee olemaan vahvasti turvallisuus kehityksen kohteena. Luotettavuuden ankkurointi sovellustasolla ei riitä, vaan sen tulee olla toteutettu rautatasolla. Tällä hetkellä todentaminen tehdään varmistamalla, että Trusted Platform Moduuli on sertifioitu Trusted Computing Groupin (TCG) toimesta sekä alustavalmistaja on implementoinut moduulin TCG:n spesifikaation mukaisesti.

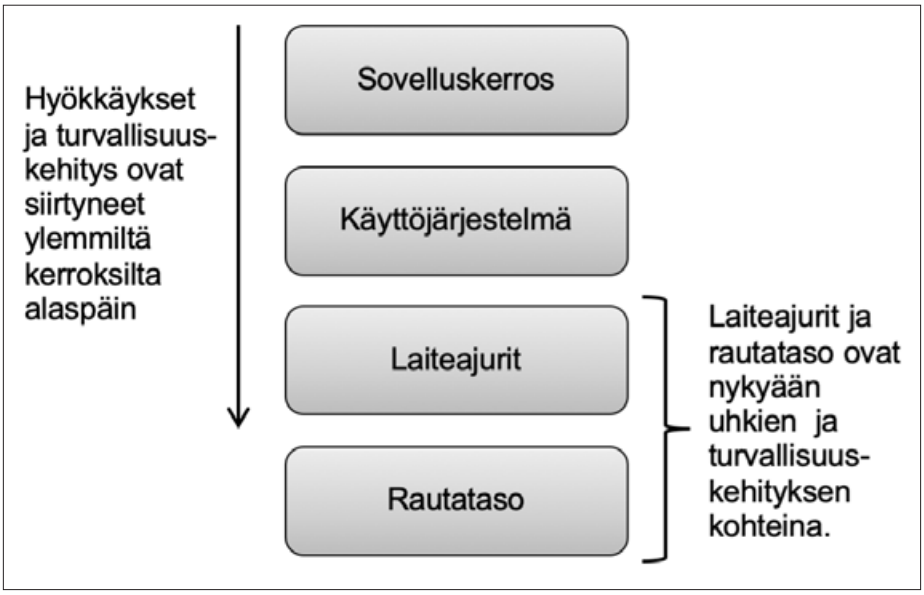
Eheyden valvonta vaatii kehittämistä vielä pitkään, jotta valvontaprosessissa tapahtunut poikkeus tunnistetaan oikein ongelmaksi ja ongelman syy-seuraussuhteet pystytään selvittämään tarkasti. Eri rauta- sekä sovelluskomponenttien eheyttä voidaan seurata melko tarkasti käynnistyslokin kautta, mutta pureutuminen komponentin sovellusmuutoksiin vaatii yleensä valmistajan tukea, ellei kyseessä ole avoimen lähdekoodin ohjelmiston osa. Käytännön ympäristöissä toivottavaa kehitystä on nähtävissä esimerkiksi UEFI alusta-sovelluspohjan osalta TianoCore -yhteisön ja EDK II -ympäristön kautta. Mitä yhteneväisempi alustasovellus, sitä helpompaa syy-seuraussuhteita on seurata, mutta toisaalta alusta myös muodostaa yhtenäisemmän kohteen hyökkääjille.

Turvallisuusimplementoinnit eivät ole valmistajalle oletusarvoisia, vaan riippuvat suoraan ostajien ja käyttäjien vaatimuksista. Verkkoinfrastruktuurin uusiutumisen myötä siirrytään lähemmäs palvelinkeskusajattelua ja –virtualisointia. Tässä yhteydessä toteutettavien uusien ympäristöjen tulee tarjota kattavat työkalut järjestelmän osien luotettavuuden varmistamiseksi, mikä on todennäköisesti olennaista esimerkiksi uuden Tetra-verkkoa korvaavan kommunikointikanavan luomisen yhteydessä. Verkon infrastruktuurin varmennettava eheys on verkko-operaattoreiden ja käyttäjien yhteinen etu.

Luotettavassa prosessoinnissa hieman ristiriitaisesti juuri luottamuksen määrää pyritään vähentämään - luottamus on käytäntö, jossa odotetaan toisen osapuolen tai tässä tapauksessa laitteen tekevän asioita omien odotustemme mukaisesti. Luottamuksen tarve vähenee varmistamalla ja rajoittamalla lopputuloksia lähemmäs odotuksiamme. Avoimen lähdekoodin osalta voidaan periaatteessa varmistua toteutuksen laadusta, mutta kustannussyistä varmistusta ei kuitenkaan yleensä tehdä, vaan luotetaan jonkun muun varmistaneen lopputuloksen laadun. Usein tästä syystä ostetaan sovelluksia, joissa lähdekoodi on suljettu ja luottamus on käytännössä ulkoistettu myyjätaholle. On toivottavaa että tulevaisuudessa voidaan siirtyä koko sovelluspinon varmistukseen sokean luottamuksen sijasta. Parhaassa tapauksessa tämä tavoite toteutuu myös rautatasolla.

Yhteenveto

5G:n myötä mobiiliverkon tarjoamat käyttömahdollisuudet ovat monipuolistuneet dramaattisesti. Nämä uudet ominaisuudet vaativat verkolta skaalautuvuutta sekä suorituskyvyn että monipuolisuuden osalta. Verkon arkkitehtuurin ja sisäisen toteutuksen osalta tämä vaatii erittäin suuria muutoksia 4G:hen verrattuna, mikä yhdistettynä yleisten IT-teknologioiden käyttöönottoon mobiiliverkossa laajentaa verkon hyökkäyspintaa merkittävästi. Tämän riskin hallitsemiseksi 5G-verkossa on määritelty uusia turvallisuusominaisuuksia, joiden lisäksi tarvitaan valmistajakohtaisia lisäominaisuuksia alati muuttuvien tietoturvauhkien torjumiseksi. Myös ohjelmisto- ja laitteistoalustojen ja konfiguraatioiden luotettavuuden todentaminen on tulevaisuudessa kriittinen teknologia. Verkon arkkitehtuurin ja toteutuksen turvaaminen on silti jatkuvaa työtä vaativa haaste.



Kuva 3: Luotettavuuden todentamisen tasot.

Kirjoittaja kapteeni Otto Saarenvirta palvelee tätä kirjoittaessa Kainuun prikaatin Kuopion Huoltopataljoonan esikunnassa ja tutki omassa pro gradu -tutkielmassaan 2018 arjen välineiden käyttöä joukkoyksikön kenttähuoltojärjestelmän johtamisessa. Kirjoittaja pääsi osallistumaan sähköisten potilastietokorttien käyttöön liittyvään kenttäkokeeseen kesällä 2020.

TEKSTI: OTTO SAARENVIRTA

Potilaskortit sähköisiksi - Pakkodigitalisointia vai kehitystä tarpeesta?

Terveydenhoitoala on digitalisoitunut muun yhteiskunnan myötä ja lähes kaikki potilastiedot säilytetään nykyään sähköisessä muodossa. Kenttähuollon lääkintäketju on jäänyt toistaiseksi kehityskulun ulkopuolelle ja nojaa edelleen vain käsin kirjoitettaviin SMART TAG -potilaskortteihin. Riittävätkö arjen välineiden ominaisuudet uuteen valloitukseen?

Kuva 1: Sovellusta ja NFC-kortteja on tarkoitus käyttää vanhan kortin rinnalla. LÄHDE: Ari Kosonen

Ideointia ja innovointia

Kenttäkokeessa testatun sovelluksen ja toimintatapamallin juuret johtavat edellä mainittuun pro gradu -tutkielmaan. Tutkielma tehtiin osana Arjen välineiden suurempaa tutkimuskokonaisuutta ja sen aiheena oli joukkoyksikön kenttähuoltojärjestelmän johtaminen arjen ratkaisuilla. Tutkielmassa tarkasteltiin yllämainittua toimintaympäristöä ja sen asettamia vaatimuksia arjen ratkaisuille. Vaatimuksien määrittelyn jälkeen innovoitiin asiantuntijaryhmien kanssa erilaisia sovelluksia, palveluita ja toimintatapamalleja, joiden kautta vaatimuksiin voitaisiin vastata. Yksi näistä oli potilastietosovellus.

Potilastietosovelluksen tarkoitus oli lyhyesti sanottuna digitalisoida nykyisin käytössä oleva, jokaisen taistelijan varustukseen kuuluva potilastietokortti (SMART TAG). Korttiin kirjataan taistelijan omat perustiedot (nimi, henkilötunnus, perussairaudet, lääkeallergiat, veriryhmä jne.) ja haavoittumisen tapahtuessa kirjataan mm. potilaaseen kohdistettu hoitotoimenpiteet sekä elintoimintojen seuranta. Lisäksi kortti toimii muistilistana hoitohenkilöstölle erilaisista tarkastuksista sekä toimenpiteistä, jotka haavoittuneelle on aina perustaistelumenetelmän mukaan tehtävä. Potilastietokortin rooli osana tiedonvälitystä eri hoitotasojen välillä on ilmeinen. Kortti kertoo seuraavan hoitopaikan henkilöstölle potilaan hoitohistorian ja hoidossa tarvittavat tiedot. Ensihoitoaseman leikkausryhmä on todennäköisesti hyvin kiinnostunut saapuvan potilaan mahdollisesta opiaattiallergiasta tai tekonivelestä.

Kortti itsessään on lääkinnällisessä mielessä hiottu kokonaisuus ja kehitystyön haasteista on luoda digitaalinen versio, joka vastaa fyysistä korttia. Digitalisointi ei saa olla itsetarkoitus, vaan sillä on saavutettava jotain konkreettista hyötyä. Kun potilastietosovellusta ideoitiin tutkimustyötä tehdessä, ilmeni hyvin varhaisessa vaiheessa, että kortit eivät voisi olla puhelimeen tallennettavia tiedostoja, vaan tiedot olisi kyettävä tallentamaan kohteeseen, joka ei olisi virransaannista riippuvainen ja kykenisi säilyttämään tiedon olosuhteista riippumatta. Puhelinta käytettäisiin vain luku- ja kirjoituslaitteena.

Vaatimukset täyttävä vaihtoehto löytyi RFID-tekniikkaa hyödyntävistä korteista, joita käytetään esimerkiksi hotelleissa huoneavaimina. Kortti ei tarvitse akkua, on pahvista korttia kestävämpi ja uudelleen käytettävissä. Tietojen lukeminen ja kirjaaminen kortille voidaan tehdä millä tahansa NFC-antennin sisältävällä

puhelimella, johon on asennettu kortin lukemiseen kehitetty sovellus.

Suurin osa älypuhelimista käyttää nykyään NFC-tiedonsiirtoa. Vaikka ominaisuus puuttuu vanhemmista malleista, on potilastoiminnan kannalta riittävää, jos edes osa taistelijoista kykenee käsittelemään kortteja. Potilastietokortin täyttöä ei kouluteta kaikille taistelijoille nykyoloissakaan, joten mitään ei sinänsä menetetä.

RFID-kortteja ei ole mielekästä hankkia satoja tuhansia varastoon sodanajan varalle. Kuten älypuhelimet, nämäkin kortit kehittyvät nopeassa tahdissa ja nyt hankittavat kortit ovat todennäköisesti teknisesti vanhentuneita muutamien vuosien kuluttua. Varteenotettava vaihtoehto olisi ostaa kortteja koulutuskäyttöön joitakin tuhansia jaettavaksi joukko-osastoille, ja lopuista sodanajantarpeista tehtäisiin hankintasopimus yhteistyökumppanin kanssa. Materiaali ei ole ainakaan nykytiedon valossa sellaista, että se vietäisiin kriisin aattona käsistä kansainvälisillä markkinoilla nykyisten kasvomaskien tapaan.

Kuva 2: Kuten kuvassa näkyy korttia ei tarvitse pitää kiinni laitteessa kirjoittamisen aikana. LÄHDE: Ari Kosonen

Korttien käyttämiseen olisi siis kehitettävä oma sovellus. Tämä vaatimus on ristiriidassa koko Arjen välineet -kehitystyön kanssa, jonka perusratkaisuna on ottaa markkinoilla oleva valmis, kaupallinen sovellus ja käyttää sitä sellaisenaan. Potilastietosovellus on kuitenkin siinä mielessä erityistapaus, että tässä asiassa ratkaisun on oltava valtakunnallisesti sama: Potilastietoja on kyettävä käsittelemään samalla tavalla jokaisella hoitopaikalla, koska on mahdotonta ennustaa, onko haavoittumisen sattuessa lähimpänä oleva hoitopaikka oman vai jonkin muun joukon. Mahdolliset rajapinnat siviilijärjestelmien, esimerkiksi uusien sote-alueiden tietokantojen tai valtakunnallisen kanta-arkiston kanssa edellyttävät teknisesti yhdenmukaista ratkaisua. Siksi sovelluksen tulisi olla PV:n omistama. Inarista Meilahteen leikkaukseen lennätettävän rajasissin potilastietojen pitää olla käytettävissä sekä lähettävässä että vastaanottavassa päässä.

Tutkielman sivuilta kentälle

Tutkielma valmistui ja kirjoittaja sen mukana. Opinnäytetyön puitteissa on harvoin mahdollisuuksia luoda ja testata ideoituja sovelluksia eikä tämä työ ollut poikkeus. Valmistumisen jälkeen kirjoittaja piti kuitenkin yhteyttä tutkimusryhmään ja osallistui muutamaan kehitystyöhön liittyvään työpajaan. Yhteistyön seurauksena päätettiin testata potilastietosovellusta kenttäkokeella. Kokeen johti opinnäytetyön ohjaaja eversti evp. Mika Hyytiäinen, yhteistyökumppani kehitti sovelluksesta kevennetyn demoversion nykyisen potilastietokortin pohjalta, ja kirjoittaja vastasi käytännön järjestelyistä kenttäkokeen toteuttavassa varuskunnassa sekä teki tarvittavat yhteydenotot paikalliselle terveysasemalle ja kokeeseen osallistuviin joukkoihin. Yhteistyön järjestelyt Nälkämaassa on aina parempi jättää paikallisille intiaanioppaille.

Suunnitelma käytännön toteutuksesta oli seuraava: Kenttäkoe päätettiin toteuttaa osana Kainuun prikaatin aselajiharjoitusta, joka on saapumiserän pääsotaharjoitusta edeltävä, viiden päivän mittainen sotaharjoitus, johon osallistuvat kaikki prikaatin joukkoyksiköt. Ennen koetta oli tarkoitus esitellä demoversio lääkinnän kenttätyön ammattilaisille, tässä tapauksessa Kajaanin terveysaseman kenttäsairaanhoitajille, jotka arvioivat sovelluksen käytettävyyttä ensimmäisen version pohjalta. Annetun palautteen perusteella muokattiin sovellus muotoon, jossa sitä tultaisiin testaamaan. Kokeen rakenteeksi suunniteltiin seuraavaa: Koe käynnistyy harjoituksessa jääkärikomppanian etulinjan taisteluista, jossa kuvataan 4-5 taistelijan haavoittuminen ja evakuointi komppanian ensihoitopaikalle. Jääkärikomppanian tasalla ryhmien taistelupelastajat sekä joukkueen lääkintämiehet perehdytetään pikakoulutuksella sovelluksen käyttöön ja se saavat kirjata tarvittavat tiedot korteille ennen potilaiden siirtymistä ensihoitopaikalle. Ensihoitopaikalle lääkintäryhmä vastaanottaa potilaat, lukee potilastiedot heidän korteistaan, kirjaa tekemänsä hoitotoimenpiteet ja lähettää potilaat eteenpäin huoltokomppanian ensihoitoasemalle, jossa prosessi toistetaan. Jokaisella tasolla tilanne keskeytetään ennen potilaiden siirtoa ja hoitohenkilöstön kokemukset sovelluksen käytöstä kerätään haastatteluilla. Testiin osallistuva lääkintähenkilöstö ei saa tutustua sovellukseen kuin hieman ennen testitapahtumaa. Sovelluksen on oltava niin yksinkertainen ja toimiva, että se pystytään kouluttamaan tarvittaessa perustamispaikalle palvelukseen kutsutulle reserviläiselle, joka syöttää sovelluksella omat tietonsa kortilleen, ja soittaa todennäköisesti äidilleen, koska ei muista mitä lääkeaineallergioita hänellä onkaan, veriryhmästä puhumattakaan. Onneksi kirjoituslaite on myös puhelin.

Kuva 3: Hoitopaikalla, jossa on enemmän henkilöstöä, muutamat taistelijat valikoituvat kirjureiksi. LÄHDE: Mika Hyytiäinen

Alkuperäinen suunnitelma kenttäkokeen järjestämiseksi kaatui monen muun projektin lailla maaliskuussa. Pandemiat eivät ole kiinnostuneita yksittäisten armeijoiden kehitystyöstä. Hetken aikaa näytti siltä, että projektin olisi tyydyttävä toteuttamaan luodun sovelluksen arviointi puhtaasti teoriapohjalta. Koe päästiin kuitenkin järjestämään Kainuun prikaatin osasto C:n pääsotaharjoituksen yhteydessä. Kenttäkokeeseen osallistuivat pioneerikomppanian huoltojoukkue, jolla korvattiin aiemmin mainittu jääkärikomppanian huoltojoukkue. Pioneerikomppanian huoltojoukkueella ei ollut varsinaista omaa ensihoitopaikkaa, mutta komppanian lääkintämiehet kerättiin sen komentopaikan yhteyteen kuvaamaan ensihoitopaikan suorituskykyä. Lääkintämiehiä osallistui pioneerikomppaniasta loppujen lopuksi vain kaksi, mutta tämä antoi toisaalta mielenkiintoista dataa sovelluksen käytöstä tilanteessa, jossa yhdellä hoitohenkilöllä on useita hoidettavia potilaita yhtä aikaa. Lääkintämiehet suorittivat potilaslajittelun eli triagen kenttäsairaanhoitajan valvonnassa ja tekivät alustavan potilasarvion maskeeratun potilaan käytöksen ja ulkoisten vammojen perusteella. Kun arviot oli tehty ja potilaat asetettu prioriteettijärjestykseen, tekivät lääkintämiehet potilaille tarvittavat hoitotoimenpiteet ja kirjasivat ne potilaiden korteille.

Tilanteen päätyttyä pioneerikomppanian lääkintähenkilöstö antoi sovellukselle positiivista palautetta ja piti sen käyttöönottoa entisen potilasluokittelukortin rinnalle järkevänä. Lääkintämiehet pitivät sovelluksen käyttöä jopa perinteistä kynä-paperi -menetelmää miellyttävämpänä kirjaamismenetelmänä. Toisaalta todettiin, että esimerkin kortin säilytyspaikan varusteissa on oltava vakioitu, koska potilaslajittelua hidasti eri paikkaan sijoitettujen haavoittuneiden korttien etsintä.

Seuraavassa vaiheessa maskipotilaat, joiden korteille oli nyt kirjattu pioneerikomppaniassa tehdyt hoitotoimenpiteet, siirrettiin evakuointikuljetuksena huoltokomppanian ensihoitoasemalle. Ensihoitoasemalle saapumisen jälkeen koulutettiin sovelluksen käyttö aseman kahdelle ensihoitoryhmälle. Ensihoitoryhmä oli harjoitellut potilastoimintaa ja triagea osana normaalia koulutustaan edeltävänä päivänä, joten sovelluksen käytön yhdistäminen osaksi normaalia potilastoimintaa oli suhteellisen helppoa. Hoitohenkilöitä oli tällä tasolla enemmän kuin potilaita, ja ilman erillistä ohjeistusta ensihoitoryhmistä vakiintui kaksi kirjuria, jotka vastasivat korttien lukemisesta, tietojen ilmoittamisesta ja tallentamisesta takaisin korteille. Potilaiden lajittelu ja siirtäminen hoitotilaan priorisoteettijärjestyksessä sujui melko nopeasti ja pian tarvittavat hoitotoimenpiteet oli tehty kenttäsairaanhoitajan valvonnassa. Viimeisenä haastateltiin potilastoimintaa harjoitelleet kaksi ensihoitoryhmää sekä testiin osallistunut kenttäsairaanhoitaja. Arviot sovelluksesta olivat niin ikään positiivisia.

Kuva 4: Sovelluksen on oltava niin helppokäyttöinen, että käyttäjä oppii sen perustamispaikalla. LÄHDE: Mika Hyytiäinen.

Kehitystyössä mukana ollut lääkintähenkilöstö näki heti alusta alkaen sovelluksen käytössä uhan: Hoitohenkilöstön huomio keskittyy vain sovelluksen käyttöön ja itse potilastoiminta jää toissijaiseksi. Tästä nähtiin jonkin verran merkkejä pioneerikomppaniassa, jossa molemmat lääkintämiehet joutuivat käsittelemään useita potilaita ja kirjaamaan kaikki tiedot itse. Vain jatkotutkimuksella voidaan todeta, että eroaako sovelluksen käyttö tässä asiassa perinteisestä pahvikortista. Huoltokomppanian ensihoitoasemalla oli tarpeeksi henkilöstöä, jotta voitiin asettaa ”kokopäiväinen” kirjuri, joka vastasi potilaskirjanpidosta. Pitkällinen palvelus huoltoaselajissa on osoittanut kirjoittajalle, että kirjureiksi kannattaa asettaa sen työn osaavat. Kirjoittajan oma käsiala painii todennäköisesti samassa sarjassa ”lääkärien” kanssa, näppäilynopeudesta puhumattakaan.

Kenttäkokeen tulokset olivat lupaavia, mutta on silti hyvä muistaa tosiasiat: käytössä oleva SMART TAG-kortti on suhteellisen kestävä, eikä tarvitse käyttöä varten itsensä lisäksi kuin kynän. Sen käytöstä ei tule luopua, vaan vanhat kortit säilytettäisiin uusien rinnalla käytössä niin kauan kuin niitä varastoissa riittää. Kortin kehittämiseen on laitettu huomattava määrä resursseja, mutta se on suhteellisen kallis, kun ottaa huomioon vuosittaisen kulutuksen henkilöstön koulutuksessa.

Tässä kirjoituksessa esitetty järjestelmä on suhteellisen ”huoltovapaa”, mutta kirjoituslaitteet tarvitsevat virtansa. Lisäksi nopeassa tilanteessa, missä potilaat lajitellaan prioriteettijärjestykseen puhtaasti kortin värin perusteella, on vanha kortti käytännöllisempi. Uusi sovellus pitää kuitenkin nähdä ensisijaisesti mahdollisuutena: Sähköisessä muodossa olevien korttien datan käsittely antaa aivan uudenlaisia vaihtoehtoja. Haavoittuneiden tiedot voidaan lähettää etukäteen vastaanottavalle hoitopaikalle, jolloin esim. leikkausryhmän kirurgi voi tehdä jo alustavan arvion saapuvasta potilaasta ja suorittaa tarvittavat valmistelut, kun potilaskuljetus on vielä matkalla. Hoitopaikan potilaspäiväkirjat on mahdollista automatisoida täysin käyttämällä jokaisen potilaan korttia lukulaitteessa, joka tallentaa tiedot ja arkistointia varten. Perustamispaikalla voidaan ladata valmiiksi kortille sotilaan hoitohistoria.

Kortti voi olla teknisenä ratkaisuna täysin erilainen kymmenen vuoden päästä. Tämän takia käyttöliittymän pitää olla niin yksinkertainen, että sen koodaamiseen kuluu kymmenen työtuntia muutamalta osaavalta reserviläiseltä.

Kuva 5: Kenttäkokeen jokaisen vaiheen jälkeen kerättiin palaute kokeeseen osallistuneilta. LÄHDE: Mika Hyytiäinen.

Projektissa käytetty demosovellus syntyi suunnilleen tämän suuruisella työsuoritteella. Samaten muokkaaminen kriisin pitkittyessä on mahdollista. Kun sovellus ei ole teknisesti lopullisessa muodossaan käytössä rauhan aikana, kuluu vihollisen koodareilta pari kuormalavallista energiajuomaa ennen kuin järjestelmään päästään sisälle kriisin käynnistyessä. Lisähyötynä koulutuskäytössä olevan sovelluksen uudistaminen muutaman vuoden välein suhteellisen pienillä kustannuksilla testaa mallin toimivuutta kriisiaikaa silmällä pitäen. Vaikka arjen välineet eivät ole operatiivisten joukkojen pääjohtamisjärjestelmä, ei mikään estä niitä käyttämästä myös kuvattua järjestelmää. Puhelintahan voidaan käyttää täysin ilman verkkoa, kuten kynääkin Järjestelmä on kenttäkokeeseen osallistuneen yhteistyökumppanin edustajan mukaan muokattavissa suhteellisen helposti yhteensopivaksi M18-järjestelmän kanssa, mutta tämän varmistaminen vaatisi erillisen jatkoselvityksen.

Korttien valmistelu tehdään perustamispaikalla, ei verkon yli. Mahdolliset kannoista saatavat potilashistoriat toimitetaan sinne niin ikään fyysisesti. Kun käyttäjä tarkastaa perustettaessa oman korttinsa tiedot hän tekee samalla tietoturvatyötä: Hän tarkastaa inhimillisten näppivirheiden lisäksi, onko vihollisen hakkeri päässyt väliin. Seuraavalle hoitopaikalle etukäteen lähetetyt tiedot varmennetaan uudelleen potilaiden saapuessa. Tietoturvallisuus rakentuu, kuten usein arjen välineiden kohdalla, käyttäjän ja tekniikan yhteistyöstä.

Kehitys ponnistaa nurmen tasalta

Kenttäkokeen tavoite oli selvittää edellytyksiä potilastietosovellukselle ja arvioida sen mahdollista käytettävyyttä. Tämä oli kuitenkin vain osa tutkimuksen tarkoitusta ja sivutavoitteena oli löytää samalla prosessi, jolla arjen välineitä tuodaan osaksi johtamisjärjestelmää. Puolustusvoimien johtamisjärjestelmäpäällikkö prikaatikenraali Mikko Heiskasen Twitterissä julkaisema Puolustusvoimien johtamisen tuen konsepti 2030-luvulla ilmoitti alueellisten ja paikallisjoukkojen pääjohtamisjärjestelmän rakentuvan pääsääntöisesti arjen välineiden varaan. Suunniteltu muutos on poikinut useita opinnäytetöitä ja tutkimuksia, mutta toistaiseksi kentällä muutosta ei ole nähty ja joukot pelaavat edelleen ”vihreillä” radioilla. 2030-luvulle on vielä matkaa vajaa vuosikymmen, mutta arjen välineet muuttuvat niin nopeasti, että meidän on pakko ”hypätä kelkkaan”, jotta tiedämme miten pysyä kyydissä kymmenenkin vuoden päästä.

Arjen välineet eroavat järjestelmänä merkittävästi edeltävistä Puolustusvoimien käytössä olleista sähköisistä johtamisvälineistä. Merkittävä osa hardwarea ei ole enää kiinteää, tunnettua ja jatkuvasti

Puolustusvoimien hallussa, vaan potentiaalisten johtamislaitteiden massa on jatkuvan ja Puolustusvoimista riippumattoman muutoksen alla. Puolustusvoimat ei voi sanella minkälaisia laitteita markkinoilla liikkuu ja minkälaisia puhelimia ihmiset käyttävät. Pitkän aikavälin tarkka suunnittelu on sula mahdottomuus ja voimme vain pyrkiä ennakoimaan muutoksia ja reagoimaan niihin. Organisaatiokulttuurimme taipuu muuttuneeseen ympäristöön heikosti, koska olemme tottuneet siihen, että kaikki käyttämämme välineet ovat tiukasti keskitetyn johdon hallinnassa. Tämä pätee erityisesti johtamisjärjestelmään.

Dosentti Hyytiäinen keksi varsin hyvän analogian arjen välineistä kirjoittajan tehdessä opinnäytetyötään. Arjen välineet ovat kuin savolaisen kirves. Sama väline on käytössä vuosikymmeniä. Varsi on vaihdettu kymmenen kertaa ja terä viisi, mutta kyseessä on silti sama kirves. Myös yksittäiset laitteet ja sovellukset tulevat vaihtumaan ajan kuluessa, mutta käyttöperiaatteet ovat samoja. Kirvestä heilutetaan samalla tavalla, oli varsi sitten muovia tai puuta. Kirvestä on vain osattava käyttää, samoin arjen välineitä. Ja sotilashan oppii parhaiten tekemällä. Jos emme ala vähitellen siirtyä teorian tasolta käytännön kokeiluihin löydämme polvestamme kirveen vuonna 2030.

Arjen välineillä luotu johtamisjärjestelmä ei voi olla massiivinen, keskenään integroitu tekninen kokonaisuus, jossa kaikki tarvittavat tiedot siirtyvät kryptattuna automaattisesti järjestelmässä valtakunnan laidalta toiselle. Sellainen järjestelmä olisi ehkä mahdollista kehittää, mutta se maksaisi pienen valtion vuosibudjetin verran ja olisi käyttöönotettaessa jo kymmenen vuotta vanhentunut. Arjen välineissä kehitystyön on lähdettävä ruohonjuuritasolta ja pala kerrallaan. Yksittäinen ihminen voi keksiä hyvinkin merkittävän tavan hyödyntää olemassa olevaa kaupallista sovellusta. Kuka sanoo, ettei Oma Riista -sovelluksella voi tehdä jänis-havainnon lisäksi panssarivaunuhavaintoja? Kun toimintatapamalli tai sovellus nousee joukosta itsestään, on se varmasti sen omaan ympäristöön sopiva. Idea voi olla myös sovellettavissa valtakunnallisesti, jolloin levitetään sen käyttö kaikille joukoille. Malli voi myös jäädä paikalliseksi malliksi ja esimerkiksi viereisen sotilasalueen joukot käyttävät eri ratkaisua. Vaikka sovellukset eivät voisikaan keskustella keskenään, käyttäjät voivat sen tehdä. Arjen välineiden johtamisjärjestelmässä ihmisen rooli nousee entistä merkittävämmäksi. Sovelluksia, palveluita tai tietokantoja ei saa yleensä keskustelemaan keskenään ainakaan ilman merkittävää rajapintojen kehittämistyötä. Teknisen rajapinnan puuttuessa ihminen täyttää aukon. Ja Suomen Puolustusvoimissa ei ole pulaa osaavista reserviläisistä.

Edellä esitetty malli voi kuulostaa villiltä länneltä, mutta keskusjohtoinen, vanha malli ei pysy arjen teknologian perässä. Uudet tavat käyttää arjen teknologiaa nousevat pääsääntöisesti jokapäiväisestä elämästä ja palveluksesta, eivätkä tutkijoiden kammioista. Innovoimista on tuettava ja kannustettava, mutta sille on myös annettava pelisäännöt. Keskusjohto ei tietenkään voi ulkoistaa itseään kehitystyössä tai jättää sitä valvomatta. Villi länsi tarvitsee sheriffinsä tai rosvot ryöstävät pankin. Päätettäviä asioita ainakin on, mille tasolle asti ulotetaan oikeus valita omat sovellukset, toimintamallit ja applikaatiot. Perusyksiköiden tasalle asti tilanne on varmasti selvä. Jos samoissa teltoissa majoittuvat soturit eivät pääse sopuun applikaatioiden käytöstä on sota jo hävitty. Muita päätettäviä asioita ovat: Mitä arjen välineillä saa ilmaista ja miten tieto peitetään tai suojataan siten, että vihollinen ei pysty murtamaan ajallisesti kriittistä tietoa ennen sen vanhentumista. Lopuksi innovoinnille on luotava uusia helpottavia kanavia. Niitä on jo olemassa, mutta ongelma niiden käytölle ei ole organisaatiorakenteessa vaan -kulttuurissa ja toimintaympäristössä. Innovointikanavista tiedotetaan heikosti ja perusyksiköiden jatkuva kiire kaventaa jo ennestään innovaatioiden kehittämismahdollisuuksia. Keräämme palautetta olemassa olevista järjestelmistä lähes tukehtumiseen asti, mutta emme kysy mitä uutta voisi kehittää?

Organisaatiokulttuuri muuttuu hitaasti ja kirjoittajan oman, toki rajallisen kokemuksen mukaan perusyksiköiden henkilökunta suhtautuu sotilaiden omien puhelimien käyttöön nuivasti ymmärrettävistä syistä. Henkilökunta ei halua hämärtää rajaa taistelijoiden henkilökohtaisen ja Puolustusvoimien omaisuuden välillä. Lisäksi epäilyksiä herättävät ilmeiset tietoturvariskit ja kaupallisten verkkojen luotettavuus kriisitilanteissa. Tosiasiat ovat kuitenkin armottomia: Mikäli aiomme pitää kiinni yleisestä asevelvollisuudesta ja nykyisen vahvuisista sodanajan joukoista, on näiden joukkojen valtaosille järjestettävä johtamisjärjestelmä jotain muuta kautta kuin Puolustusvoimien hankkimalla kalustolla. Rahaa ei yksinkertaisesti ole varustaa kaikkia joukkoja sotilasradioilla tai muilla vastaavilla johtamisvälineillä. Vastarannankiiski nurkasta huutaa tässä vaiheessa, että onhan ennenkin pärjätty ilman. Kenties näin on, mutta muiden valtioiden asevoimat kehittävät johtamisjärjestelmiään jatkuvasti. Jos päätämme alueellisten ja paikallisjoukkojen pääjohtamisjärjestelmän perustuvan nopeaan pariin Nokian 42 -koon kumikenkiä ja kirjekyyhkyihin vastapuolen käyttäessä tämän vuosituhannen tekniikkaa, on meidän sama todeta sodanajan suunnitelmien perustuvan näiden joukkojen kohdalla aikaan ennen radioiden keksimistä.

Sami Rautén on 2. vuosikurssin kadetti ja opiskelee Maanpuolustuskorkeakoulussa 105. Kadettikurssilla ja aloittaa syksyllä 2020 opinnot johtamisjärjestelmä- ja viestilinjalla.

TEKSTI: SAMI RAUTÉN

Tietotulvaa ja tietoturvaa arjen ehdoilla

Arjen ratkaisujen ekosysteemi mahdollistaa johtamisen aivan uudella tavalla. Verkottuneisuus ja reaaliaikainen tilannekuva ovat olleet jo vuosikymmeniä johtamisjärjestelmien tavoitteena. Uudet ratkaisut vaativat uudenlaista ajattelutapaa, niin tietoturvan kuin johtamisen rakenteiden osalta. Vastapainona arjen ratkaisujen saatavuus ja käyttöönoton nopeus vapauttavat sekä taloudellisia että henkilöstöresursseja ja näin parantavat kustannustehokkuutta. Tässä artikkelissa käsitellään tietotulvan ja tietoturvan käsitteitä ja merkitystä sovellettaessa arjen ratkaisuja sotilaalliseen viitekehykseen.

Informaatiota kerätään aikaisempaa tehokkaammin ja välitetään mittavia määriä joukolta toiselle. Sen kokoamiseksi tai yhdistelemiseksi ei kuitenkaan ole kehitetty vielä edistyneempiä menetelmiä, jotka samalla parantavat saatavuutta sekä yhteensopivuutta. Tietoturvan matala taso on noussut useasti keskustelun aiheeksi, syystäkin. Tulevaisuuden teknologiat kuten 5G ja esineiden internet eivät ainakaan helpota tietoverkkojen hallintaa, kun aikaisempiakaan tietoturvaongelmia ei ole vielä ratkaistu. Yhtenä ratkaisuna tietoturvan ja sekä arjen välineiden eri sovellusten viestiliikenteen yhdistämiseksi sekä tilannekuvan parantamiseksi on Matrix protokolla. [1]

Arjen ratkaisujen tutkimus on lisääntynyt merkittävästi kahden viimeisen vuoden aikana. Puolustusvoimien tutkimuslaitoksen ja Maanpuolustuskorkeakoulun tutkimuksen painopiste on siirtymässä käsitteistä ja teoriasta tekniikan ja taktiikan soveltamiseen. Aktiivisten reserviläisten merkitystä nykytilanteessa ei voi olla korostamatta liikaa. Heidän laatikon ulkopuolelta tyyppinen ajattelutapansa on ollut tärkeässä roolissa kehitettäessä arjen ratkaisuihin perustuvaa johtamisjärjestelmää.

Tietoa turvallisesti oikeaan osoitteeseen

Useat arjen välineitä käsittelevät tutkimukset nostavat laitteiden ja sovellusten matalan tietoturvan esille. Tietoturva ja siihen liittyvät uhat eivät ole keksittyjä, niitä ei kuitenkaan tule korostaa liikaa. Operaatioturvallisuus termiä käytetään joskus synonyyminä tietoturvallisuudelle. Operaatioturvallisuudella tarkoitetaan sotilaiden ja sotilaallisen toiminnan kannalta tärkeän tiedon turvaamista ja sen vastustajalle paljastumisen estämistä. Tietoturva taas on yksi tiedon suojaamisen keino, tarkoituksena suojata tietoaineisto ja tietojärjestelmät sisältäen kaikki toimenpiteet aina yksittäisen henkilön viestin peittämisestä teknisiin suojausratkaisuihin.

Arjen ratkaisujen näkökulmasta matala tietoturva on normi ja hyväksyttävä asiantila. Se vaatii ajattelumaailman muuttamista tilanteesta, jossa kaiken viestiliikenteen on kuljettava vihreäksi maalattujen laatikoiden läpi salattuna, varmennettuna ja eristettynä muusta verkkoliikenteestä. Jokainen viesti ei ole merkityksellinen oman joukon operaatioturvallisuuden näkökulmasta. On ymmärrettävä, milloin ja missä tilanteessa tietoturvan korottaminen on tarpeellista. Tieto vanhenee nopeasti nykypäivänä, esimerkiksi joukkueen sijainnin paljastuminen vastustajalle viikkoa myöhemmin ei välttämättä ole kovinkaan arvokasta tietoa.

Tietoturvaa parantavien ratkaisujen käyttö tulisi optimoida tilanteesta riippuen, eikä pyritä automaattisesti maksimoimaan sitä joka tilanteessa. Johtamisjärjestelmän tarkoituksenahan on yksinkertaisesti mahdollistaa joukon johtaminen tehokkaasti tehtävän ja tavoitteen täyttämiseksi. Arjen ratkaisut tarjoavat mahdollisuuden saavuttaa korkea saatavuus, helppo käyttöönottoprosessi ja järjestelmien nopea perustaminen kustannustehokkaasti. On pyrittävä hyödyntämään nämä edut, huomioiden pahamaineinen tietoturva ja keskityttävä ainoastaan siihen millä on loppujen lopuksi merkitystä: viesti vain perille vietynä ratkaisee.

Tekniikkaa ja taktiikkaa vai käskyjä ja koulutusta?

Tietoturvaa voidaan parantaa monin eri

Kuva 1. Arjen välineiltä halutaan yhä enemmän suorituskykyä ja ominaisuuksia. Pikaviestisovelluksia, karttapalveluita, puhepalveluita, seurantapalveluita ja VPN palveluita.

keinoin. Nämä voidaan karkeasti jakaa vaikkapa teknisiin, koulutuksellisiin ja hallinnollisiin, sekä toiminnallisiin menetelmiin. Tekniset ratkaisut parantavat tietoturvaa esimerkiksi salaamalla viestiliikenteen tai eristämällä sen palomuureja käyttäen tai tunneloimalla ja eristäen sen muusta verkosta siten, että ainoastaan valtuutetuilla käyttäjillä on oikeus lukea ja lähettää viestejä. Koulutukselliset ja hallinnolliset ratkaisut pyrkivät parantamaan tietoturvaa ohjeistamalla ja kouluttamalla käyttäjiä minimoimaan tietoturvariskit omassa toimintaympäristössään. Se kattaa kaikki toimenpiteet matkapuhelimen asetuksista kuten paikkatiedon jakamisesta aina ohjeisiin toiminnasta sosiaalisessa mediassa.

Toiminnallisina ratkaisuina voidaan pitää toimenpiteitä, joihin vaikutamme joukkona aktiivisesti kuten esimerkiksi omien joukkojen sijainnilla ja laitteiden käyttöpolitiikalla, harhauttamisella sekä peitteistön käytöllä. Kaikissa ratkaisuissa on omat hyvät ja huonot puolensa eikä varmasti oikeaa tai väärää vastausta ole.

Tietoturvallisuus on ennen kaikkea riskienhallintaa. Onnistuneen tietoturvamallin rakentamisen pohjana toimii uhkien ja haavoittuvuuksien tunnistaminen, jonka analyysin lopputulokseen vaikutetaan aikaisemmin mainituilla keinoilla. Meillä kaikilla on oma mielikuvamme siitä, millainen oma täydellinen johtamisjärjestelmämme on ja mitä ominaisuuksia siihen kuuluu. Arjen järjestelmän palikat eli kaikki sovellukset, laitteet ja toimintamallit joita hyödynnämme arjen välineillä vaikeuttavat tietoturvakokonaisuuden hallintaa. Olemme tilanteessa, jossa joukolla on niin monia työkaluja ja eri ratkaisuja kommunikoida, että kaikkia riskejä ei ole edes mahdollista tunnistaa käyttöönottoprosessin alkumetreillä.

Tietotulvan hallintaa

Arjen välineiden pääkäyttäjillä eli paikallisjoukoilla on useita yhteistyötahoja toiminta-alueellaan aina viranomaisista yksityisyrittäjiin ja yksittäisiin kansalaisiin. Viestien tulee tavoittaa ne osapuolet, joille viestit on osoitettu ja työskentelyn tulee olla mutkatonta ja selkeää. Tästä syystä tilannekuvan koostaminen ja suodattaminen ylä- ja alajohtoportaiden välillä on erityisen tärkeää pohdittaessa ratkaisuja arjen välineillä.

Tämä on havaittu ongelmana tutkimuksissa ja kentällä. Arjen ratkaisujen saatavuus lisää viestiliikenteen määrää joukoilla huomattavasti. Joukot tavoittavat aikaisempaa helpommin toisensa ja informaatiota oman ja vihollisen joukoista on saatavilla enemmän kuin aikaisemmin – jopa liikaakin. Tätä kutsutaan tietotulvaksi, siinä vastaanottaja saa enemmän tietoa eri informaatiolähteistä kuin on kykyä käsitellä ja hyödyntää sitä. Sotilas saa tiedon omien joukkojen liikkeestä yhdellä sovelluksella, karttapalvelut toisella, puhetta hyödyntävän komentoverkon kolmannella ja kuvien välittämisen neljännellä.

Arjen toimintaympäristössä viestiliikenne on jo monesti valmiiksi hajautettua ilman, että sitä tarvitsee suunnitelmallisesti toteuttaa esimerkiksi tietoturvan parantamista varten. Pikaviestisovellukset ja muut alustat mahdollistavat tiedon välittämisen, mutta keinoja koota tieto yhteen paikkaan on vähemmän saatavilla. Jos tietoa ei pystytä kokoamaan useista eri lähteistä yhteen paikkaan, vaikeuttaa se tiedon käsittelyä ja hyödyntämistä. Havainnot vihollisen liikkeestä ja omien joukkojen sijainnista saattavat jäädä huomaamatta, tuottaen virheellistä tilannekuvaa.

Yhtä lailla joukon vastaanottaessa liikaa tietoa kerralla, emme kykene suodattamaan ja prosessoimaan tietoa riittävästi jolloin tuotetaan puutteellista tilannekuvaa. Tietotulva voidaan nähdä epäonnistuneena suodattimien hyödyntämisenä. Käsittelemättä jäänyt tieto saattaa sisältää tärkeää informaatiota oman tehtävän ja tavoitteen kannalta. Tiedon pitää siirtyä oikealle vastaanottajalle ja saada vain tieto, jota hän tarvitsee tehtävänsä toteuttamiseksi. Tietotulvaan voidaan vaikuttaa kouluttamalla ja ohjeistamalla millaista tietoa, missä muodossa ja kenelle tieto tulee välittää.

Jokainen uudelleenlähetetty tai välitetty viesti lisää verkon kuormittavuutta. Se on sotilasorganisaatiomme hierarkkisen tietojenvälittämisen rakenteen ja esikuntakeskeisen johtamisen kannalta kuitenkin tarpeellista. Tietotulvaa vahvistaa entisestään disinformaation eli tarkoituksellisesti harhaanjohtavan tiedon tai misinformaation eli tahallisesti tai tahattomasti levitetyn väärän tiedon jakaminen verkossa, joka sekoittaa tilannekuvaa entisestään.

Tilannekuvan koostamisessa sensorien,

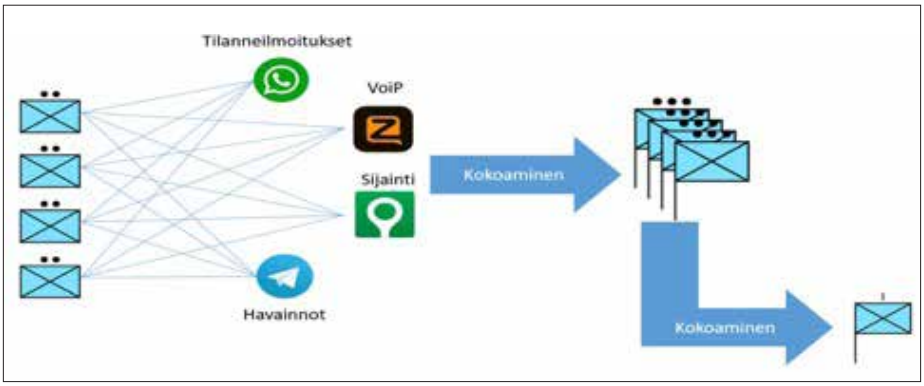
eli yksittäisten sotilaiden tai teknisten valvontaratkaisujen tuottaman tiedon siirtyminen joukkueelta komppanian komentopaikalle on kriittinen yhteysväli arjen ratkaisujen parissa. Yläjohtoportaiden välillä tieto kulkee suhteellisen hyvin, suurempi ongelma on saada riittävästi tietoa alajohtoportaalta ylös ja ylhäältä alaspäin muodossa, jossa siitä on joukolle hyötyä.

Taistelutehtävissä arjen ratkaisuilla toteutetun viestiliikenteen tulee ottaa kaikki hyöty irti saatavuudesta. Yksinkertaiset, lyhyet ja selkeät viestit toistettuna eri kanavia pitkin mahdollistavat viestin perille pääsyn. Tätä menetelmää ei kuitenkaan voida hyödyntää staattisimmissa aluevalvonta- ja kohteensuojaustehtäviä hyödyntävien joukkojen kanssa. Tällöin kriittisempää on tiedon koostaminen joukkueiden johtamispaikoille ja komppanioiden komentopaikoille. Tiedon välittämistä voidaan helpottaa esimerkiksi ohjaamalla kriittinen viestiliikenne eri ryhmiltä tiettyihin yhteiskanaviin tarvitsijoille ja luomalla perustaistelumenetelmät tilanneilmoituksista.

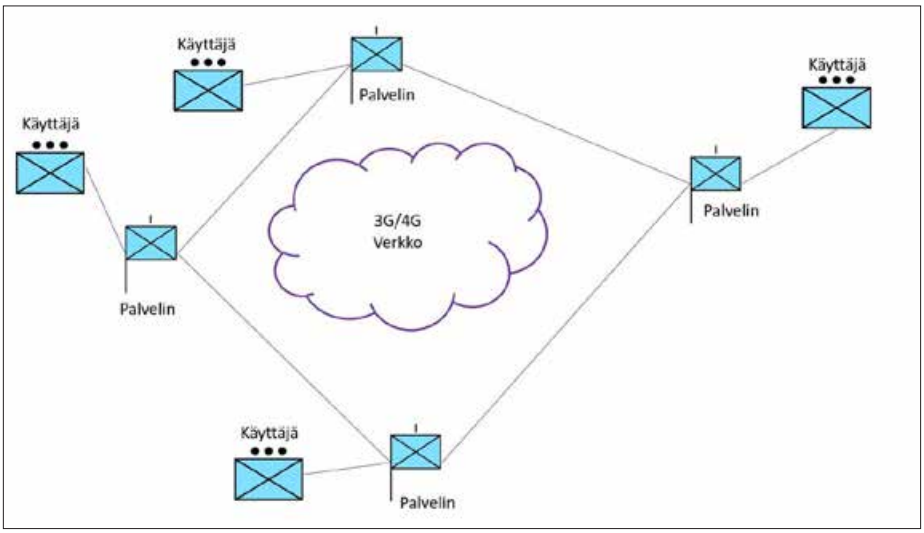
Kaikki yhden katon alle

Matrix on avoimeen lähdekoodiin perustuva avoin standardi ja protokolla reaaliaikaiseen hajautettuun kommunikaatioon IP verkon yli. Se on suunniteltu mahdollistamaan kommunikaatio eri palveluiden käyttäjien välillä tekstiä, puhetta ja videoita käyttäen. Matrix voidaan ajatella SMTP (Simple Mail Transfer Protocol) protokollana, joka itsessään toimii standardina sähköpostin välityksessä nykypäivänä.

Matrixia hyödyntäviä käyttöliittymiä on saatavilla Androidille, iOS, Windowsille, Linuxille ja se toimii tarvittaessa myös selaimessa. Matrixissa käyttäjät yhdistävät omaan palvelimeensa ja osallistuvat huoneisiin, jotka luodaan palvelimille. Palvelimet ovat yhteydessä toisiin palvelimiin, jonka ansiosta käyttäjät voivat keskustella eri palvelimilla sijaitsevien käyttäjien kanssa. Palvelimet voidaan ylläpitää kaupallisilla pilvipalveluilla tai omalta kotitietokoneelta tarvittaessa. Myös liikkuvat palvelimet (esim. Viestimies 4/19 lehden sivulla 25 esitelty mobiilipalvelin) soveltuvat tarkoitukseen hyvin.



Kuva 2. Viestiliikenteen hajauttaminen eri sovelluksiin lisää tietoturvaa. sen uudelleenkokoaminen on kuitenkin raskas prosessi.



Kuva 3. Toisiinsa yhteydessä olevat Matrix palvelimet replikoivat viestit IP verkon yli palvelimelta toiselle.

Viestit replikoidaan Matrix verkossa kaikilla palvelimilla jotka osallistuvat keskusteluun. Näin ollen toisiinsa kytketyt palvelut eivät lakkaa toimimasta, mikäli yksi palvelimista kaatuu vaan muut palvelimet voivat tarvittaessa korvata sen. Käyttäjät voivat käyttää joko valmiiksi luotuja palvelimia tai perustaa oman. Luomalla oman palvelimen, on mahdollista hyödyntää Matrixin tilannekuvan kokoamisen kannalta merkittävintä ominaisuutta eli siltaus ominaisuutta.

Matrixissa voidaan käyttää pelkästään matrix protokollaa hyödyntävää verkkoa, mutta siltauksen avulla voidaan yhdistää muiden viestintäsovellusten viestiliikenne osaksi Matrix ekosysteemiä. Käytännössä se tarkoittaa sitä, että eri

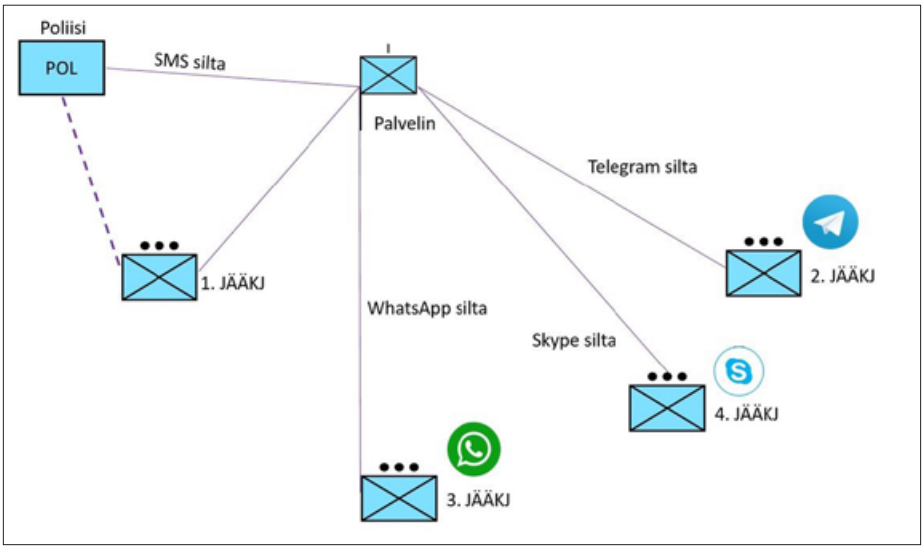
viestintäpalveluja hyödyntävien käyttäjien viestit voidaan koota siltojen avulla yhteen paikkaan. Siltaa voidaan käyttää kahdella tavalla, ensimmäisessä vaihtoehdossa ainoastaan kokoava osapuoli voi keskustella eri osapuolten kanssa. Samalla viestit voidaan ohjata kootusti yhteen huoneeseen Matrix palvelimessa.

Toinen vaihtoehto on, että luodaan välityssilta, joka mahdollistaa liikenteen välittämisen palvelusta toiseen edestakaisin. Tällöin kuvan 3. mukaisesti viestit replikoituvat palvelinten välillä. Kirjoitushetkellä Matrix tukee virallisesti 19 erilaisen viestintäsovelluksen ja ratkaisun liittämistä toisiinsa, kuten esimerkiksi Skypen, WhatsAppin, Telegramin, tekstiviestit, sähköpostin. Viestit voivat sisältää tekstiä, kuvia ja tällä hetkellä kokeellinen VoiP ominaisuus on myös mahdollinen. Samalla Matrix säilyttää viestiliikenteessä muiden sovellusten omat salausominaisuudet ja lisää oman E2EE salauksensa tarvittaessa Matrixin kautta liikkuville viesteille. [2]

Hajautettu ja keskitetty

Kyky suodattaa, järjestellä ja koota useista palasista kokonainen tilannekuva toimintaympäristöstä on jokaisen joukon tavoite. Vaikka nykyaikaiset johtamisjärjestelmäkokonaisuudet mahdollistavat luonnollisesti tämän tavoitteen toteutumisen, kaikille ei kuitenkaan ole tarjolla uusinta M18 kenttäviestijärjestelmää eikä sen kouluttaminen kaikille ole edes mahdollista. Arjen välineillä toteutettavan viestijärjestelmän etuna on paitsi resurssien vapautuminen, myös koulutusvaatimusten laskeminen.

Matrix soveltuu erityisen hyvin tilanteisiin, jossa käytettävien sovellusten ja ratkaisujen määrä on suuri kuten esimerkiksi yhteistoimintaa sovitettaessa. Peruskäyttäjän näkökulmasta koulutusta ei tarvita enempää, sillä käyttäjälle riittää oman pikaviestipalvelun osaaminen. Tekniikka ja logiikka Matrixin takana kuitenkin vaatii verkon rakentamiseksi ja ylläpitämiseksi huomattavasti enemmän koulutusta. Matrix ilman siltaus ominaisuutta on nopea ottaa käyttöön, kuitenkin yhdistettäessä palveluja toisiinsa lisää valtava määrä erilaisia asetuksia voi lisätä viivettä verkon perustamiseen huomattavasti.



Kuva 4. Joukkueet ovat yhteydessä komentopaikkaan omien siltojen avulla. Yhteistoiminta viranomaisten, kuten poliisin ja joukkueen välillä voidaan toteuttaa esimerkiksi tekstiviestillä tai tulevaisuudessa poliisin kenttäjohtosovelluksen kanssa yhteensopivan rajapinnan ylitse.

Hitaasta perustamisesta riippumatta joukoilla saattaa olla useita eri arjen ratkaisuja käytössä. Valmiiden siltauksien avulla voidaan joukko liittää verkkoon vaikkapa yksittäisellä puhelinnumerolla ilman salausavaimien tai viestiperusteiden asentamista. Viestiliikennettä voidaan suodattaa ja jakaa vain tarvittavalle henkilöstölle, esimerkiksi ainoastaan kokoamalla eri palveluista viestit johtamispaikalle. Tällöin muille joukoille ei replikoida viestejä. Tällä menettelyllä voidaan vähentää kaapatun laitteen viestiliikenteen paljastumisen vaikutusta. Joukon päätettäväksi näin rauhan aikana jääkin, kuinka paljon halutaan ja voidaan tehdä etukäteen, jotta ratkaisusta saadaan mahdollisimman paljon irti.

Tietoturva(tonko?)

Arjen välineiden ja niillä käytettävien sovellusten kanssa tulee olla tarkkana. Yhä useampi sovelluksista kerää luonnostaan jotain informaatiota käyttäjistään ja mahdollisesti myy sitä mainostajille tai muille kolmannen osapuolen kumppaneille. Avoin lähdekoodi ja tietoturva-auditoinnit eivät ole tae tietoturvallisuudesta. Matrixin kryptograafiset ominaisuudet, kuten sen päästä-päähän salaus ovat esimerkiksi auditoitu NCC Groupin toimesta.

Se ei kuitenkaan estänyt tietoturvatestaajaa läpäisemästä Ranskan valtion eri ministeriöiden käyttämää omaa versiota Matrix-verkkoa hyödyntävästä käyttöliittymästä nimeltään Tchap huhtikuussa 2019. Samassa kuussa hakkeri onnistui pääsemään Matrixin julkiselle pääpalvelimelle ja sai pääsyn kaikkiin salaamattomiin viesteihin ja salasanoihin.

Avoimeen lähdekoodiin perustuvat ohjelmistot ja protokollat tarjoavat läpinäkyvyyttä käyttäjille sekä toisaalta paljastavat myös heikkoudet hakkereille ja valveutuneille käyttäjille. Kuten aikaisemmin mainitsin, tärkeintä arjen välineiden kannalta on löytää keskitie, jossa eri ratkaisujen yhdistelmällä voidaan saavuttaa niin tieto- ja operaatioturvallinen kokonaisuus kuin mahdollista. Matrixin aikaisemmat heikkoudet ovat hyvä muistutus siitä, että nykypäivänä mikään sovellus ei ole sataprosenttisesti tietoturvallinen. On vain ajan kysymys, kunnes seuraava tietoturva-aukko löydetään puhumattakaan 5G-verkkojen ja esineiden internetin tuomista haasteista suomalaisessa toimintaympäristössä.

Arjen ratkaisuista kohti tulevaisuuden arjen järjestelmää

Arjen ratkaisuja joukkojen eri tarpeiden täyttämiseksi on eri joukko-osastoissa keksitty useita viime vuosina ja kaikilla on ollut hyvät ja huonot puolensa. Tämän lisäksi niitä on enemmän tai vähemmän onnistuneesti hyödynnetty oikeassa toimintaympäristössä ja kerätty kokemuksia arjen soveltuvuu desta sotilaalliseen toimintaympäristöön. Ensimmäinen askel kohti arjen järjestelmää on jo otettu.

Yksittäisen pikaviestisovelluksen käyttöönotto älypuhelimella tiedustelutiedon välittämiseksi, paikkatiedon välittäminen tai tietoverkon eristäminen julkisesta verkosta VPN tunnelilla ovat olleet hedelmällisiä ja tarpeellisia arjen ekosysteemin hahmottamiseksi. Yhteensopivuutta ja verkottuneisuutta edistävien sovellusten kuten Matrixin käyttöönotto ei kuitenkaan ole välttämättä ainoa seuraava askel. Toimintatavat, mallit, ohjeistukset ja hyvien käytänteiden jakaminen ovat jääneet taka-alalle viime aikoina.

RESTIKU ja Pahkis-harjoituksissa nähdyt erilaiset arjen järjestelmien prototyypit sekä monet muut ratkaisut ovat olleet luomassa hyvää pohjaa arjen ratkaisujen tulevaisuudelle. Avoimeen lähdekoodin perustuvat ohjelmistot ovat varmasti myös tulevaisuudessa merkittävä roolissa arjen ratkaisuissa. Kuitenkaan yksittäiset välineet tai ratkaisut eivät ole kokonaiskuvassa riittäviä. Ne ovat hyvä alku, mutta hyödyntääksemme arjen ratkaisujen koko spektrin, tulisi meidän rakentaa yhdessä yhteinen toimintatapamalli.

Malli joka tarjoaa perusteet arjen ratkaisujen ekosysteemin ja käsitteistön ymmärtämiseen. Malli joka määrittää selkeästi arjen välineiden käyttöönottoprosessin aina joukkojen perustamisesta taistelutilanteeseen ja yhteistoimintaan muiden joukkojen kanssa. Malli joka tukee joukon oman järjestelmän ja ratkaisujen kehittämistä ja suunnittelua.

Arjen ratkaisuihin liittyen meidän täytyy parantaa raportointia kentältä ja tutkimustuloksien jakamista suuntaan ja toiseen. Meidän täytyy olla myös valmiita siirtymään seuraavaan monipuolisempaan ja tehokkaampaan ratkaisuun eikä lukkiutua vain yhteen vaihtoehtoon. Arjesta saadaan enemmän irti sen monipuolisuuden ja muokkaantuvuuden ansiosta, eikä yksittäisen loppuun hiotun ratkaisun avulla.

Tuotteliasta syksyä.

Linkkejä:

[1] Virallinen sivusto - https://matrix.org/

[2] Salauksesta - https://matrix.org/docs/guides/end-to-end-encryption-implementation-guide

[3] Github ja lähdekoodi - https://github.com/matrix-org

TEKSTI JA KUVAT: LTN RES BENJAM GRÖNMARK

Matrix-protokolla ja arjen ratkaisuista koottujen viestijärjestelmien mahdollisuuksia

Grönmark on pääkaupunkiseudulla toimiva johtamisjärjestelmäalan vapaaehtoinen kouluttaja (ESMPP/MPK, KAARTJR). Siviilissä hän on teologian kandidaatti ja maisteriopiskelija. Artikkeli on kirjoitettu keskustelussa kad Sami Rauténinin ja Jyri Genralin kanssa.

Rakennettaessa arjen välineistä pääasiallisia yhtä hyvin kuin täydentäviäkin järjestelmiä määrittävät onnistumista samat asiat kuin kenttäviestijärjestelmissäkin.

Keskiössä on loppukäyttäjän, tilaajan, kyky liittyä ja hyödyntää järjestelmää oman ja johtoportaansa tehtävän toteuttamiseksi. Merkittävää sivuroolia esittävät myös operaatioturvallisuus ja järjestelmän ylläpidon vaatimat resurssit – riittävän merkittävää, että pääosanesittäjän osuus voi sivuosien huonon näyttelyn tai ohjauksen myötä muuttua kokonaisuuden kannalta harmilliseksi farssiksi. Saako alainen ja esimies toisiltaan tilannekuvan ratkaisujensa perusteeksi – riittävän ajoissa, riittävän todenmukaisena, riittävän helposti? Mahdollistaako järjestelmän ylläpitovaatimukset ja operaatioturvallisuus sen käyttöönoton ja luotettavuuden?

Seuraavassa artikkelissa tarkoitukseni on, Rauténinin edellisen artikkelin kanssa keskustellen, ensinnäkin hahmotella Matrix-protokollan mahdollisuuksia arjen ratkaisuna. Toiseksi esittelen erään Matrix-pohjaisen ratkaisun, jonka parissa olen syksystä 2019 työskennellyt kehitysryhmäni kanssa. Kolmanneksi pohdin haasteita arjen viestijärjestelmissä sekä loppukäyttäjän ja toteuttamisen että järjestelmien kehittämisen kannalta.

Näkökulmani aiheeseen tulee paikallisjoukkojen koulutustoiminnasta pääkaupunkiseudulla sekä palveluksesta viestivälineistä ja tilannekuvasta vastanneen joukon johtajana kriisinhallintapalveluksessa.

Arjen välineet tarjoavat mahdollisuuksia, joiden rajana on ideointivaiheessa **lähinnä viestimiehen mielikuvitus**. Jäsentelen mahdollisuuksien kenttää välineiden käyttötarkoitusten perusteella seuraavasti kolmeen. **Ensinnäkin** arjen välineet mahdollistavat kykyjä, mitä kenttäviestijärjestelmin ei ole ajateltu toteutettavaksi. **Toiseksi** COTS-kalustosta ja ohjelmistoista on mahdollista tuottaa viestijärjestelmäksi rakennettu suorituskyky. **Kolmanneksi** kenttäviestijärjestelmän rinnalle, esimerkiksi joukkoyksikön **käyttöön valjastettu** täydentävä arjen järjestelmä tarjoaa varayhteyden ja liikkuvuutta. Yhtäaikaisesti desentralisaatiota ja sähköpostin kaltaista riippumattomuutta lähettäjän, vastaanottajan ja siirrettävän datan tyypeistä tavoitteleva Matrix-ekosysteemi tarjoaa mielenkiintoisia mahdollisuuksia arjen välineet -tyyppisen sotilaskäytön näkökulmasta.

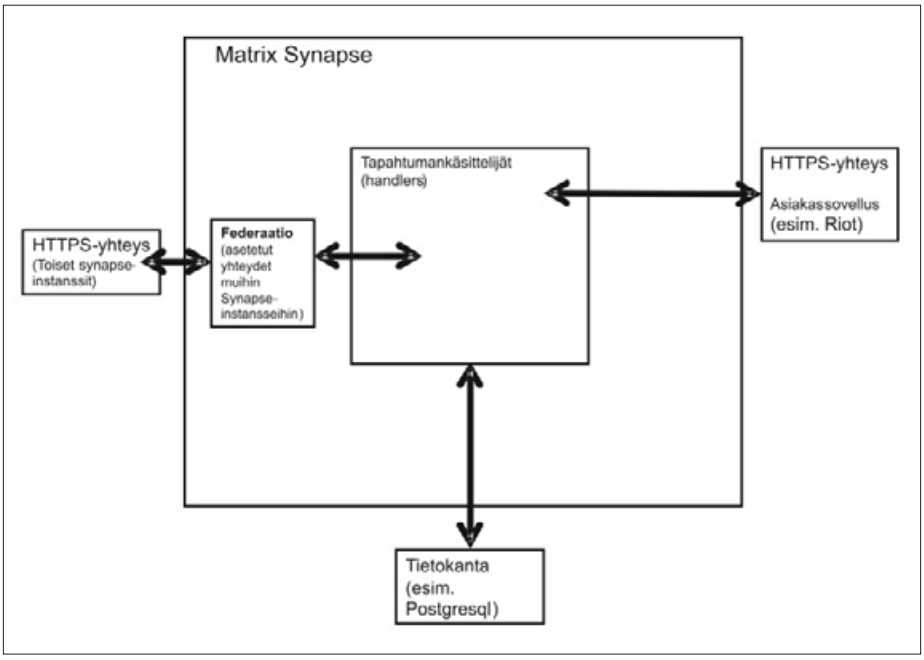
1.1. Kolmen kehityssuunnan mahdollisuuksia

Ensimmäiseen, uudentyyppisten kykyjen ryhmään lukeutuu edellä Rauténinin esittämä Matrixin hyödyntäminen eri kanaviin hajautetun viestiliikenteen koostamiseen. Protokollan siltausominaisuus voi villeimmillään mahdollistaa sen digitalisoinnin, mikä on epäsäännöllisistä konflikteista tuttu puolustajan kotikenttäetu: paikallisten ja viranomaisten havaintoja on mahdollista saada keskitetyksi ja ryhmitellyksi hyödynnettävään muotoon jo perusyksikkötasolle. Vähintään ominaisuuden avulla voidaan Rauténinin esittämällä tavalla hajauttaa perusyksikön viestiliikennettä eri sovelluksiin johdetusti niin, että liikenteestä tulee useiden sovellusten vuoksi tarkoitukseensa nähden liian työlästä ja huomiotavievää.

Itse olen toistaiseksi työskennellyt lähinnä toisen ja kolmannen sovellutustyypin – joukon pääasialliseksi tai täydentäväksi viestijärjestelmäksi suunnatun arjen ratkaisun – parissa. Näihin rooleihin istutettu arjen ratkaisu voi tarjota, kenttäviestijärjestelmiin verrattuna, monenlaisia etuja. Keskeisimpiä lienee kaksi: ensinäkin signaalin maastoutuminen siviililiikenteeseen ja siten – luonteeltaan ratkaiseva – passiivinen suojautuminen signaalitiedustelulta. Toisaalta – siinä tapauksessa, että käytettävä arjen ratkaisu on luonteeltaan sellainen, että sen käyttöönotto ja ylläpito on toteutettavissa ilman suurta ammattitaitoa – kaupallisten verkkojen sekä enemmän tai vähemmän

COTS-sovellusten käyttö siirtotienä tarjoaa ketteryyttä: viesti kulkee vähällä miesvoimalla, millä on arvonsa erityisesti nopeassa tilannekehityksessä.

Edelleen jaotellessa eritasoisten joukkojen tarpeita arjen ratkaisuille arvioisin, että toiseen, p**ääasiallisen** viestijärjestelmän rooliin arjen ratkaisuille lienee suurin tilaus perusyksikön tarpeisiin. Kolmannessa, kenttäviestijärjestelmää täydentävässä arjen ratkaisut lienevät tulevan kyseeseen lähinnä joukkoyksikkötasolla, perusyksiköiden ja esikunnan välisessä liikenteessä. Periaatteellisena vahvuutena näen tässä sen, että arjen ratkaisuista koottu järjestelmä olisi tässä mielessä potentiaalinen varajärjestelmä – vähällä miesvoimalla ja erikoiskoulutuksella ylläpidetty, hallittu tai tuotettu kyky, jota voi käyttää silloin, kun kenttäviestijärjestelmän käytölle on logistiikasta, EMCONista tai niukkuudesta johtuen esteitä.



Kuva 1. Yksinkertaistettu kaavio Matrix Synapse –palvelimen arkkitehtuurista.

1.2. Matrix-protokollan toimintaperiaate

Näihin kehitystoiveisiin Matrix tarjoaa mielenkiintoisia vastauksia. Matrix-protokollan desentralisoitu luonne tarkoittaa, että itse ylläpidettyjen palvelinten (Matrix home server) verkkotopologiasta ja käyttäjienhallinnasta voi luoda melkeinpä minkälaisen vain. Palvelimelle tai palvelinverkolle voidaan muun muassa esiluoda **käyttäjätunnukset, jotka sitten jaetaan loppukäyttäjille kenttäviestijärjestelmien tapaan.** Vaihtoehtoisesti käyttäjät voivat rekisteröityä itse käyttäen – niin ikään itse ylläpidettyä – identiteettipalvelinta, johon voi asettaa esimerkiksi tietyt sähköpostiosoitteet oikeudellisiksi luomaan matrix-osoite palvelimelle. Verkonkuvan näkökulmasta yksittäistä palvelinta voi ajaa yksinään tai niitä voi konfiguroida keskustelemaan keskenään ennalta määritellysti tai sen mukaan, miltä palvelimilta käyttäjät tavoittelevat toisiaan matrix-osoitteella menetelmällä, mitä Matrixin Synapse-referenssipalvelimessa kutsutaan federaatioksi (Matrix Federation).

Itse Matrix-palvelin (esimerkiksi referenssipalvelin Synapse) on oikeastaan – karkeasti sanottuna – toisaalta luettelo matrix-tunnuksista, jotka voivat kirjautua palvelimeen asiakasohjelmilla (esim. Element/Riot tai Ranskan valtion Riot-fork Tchap), viestiä ja perustaa palvelimen sisään viestihuoneita. Toisaalta Matrix-palvelin keskustelee isäntäjärjestelmässään olevan tietokannan (esimerkiksi Postgresql) kanssa, minne palvelimeen rekisteröityneiden käyttämien viestihuoneiden ja yksityisviestien data säilötään ja noudetaan tietokannasta. Kolmanneksi palvelin keskustelee muiden Matrix-palvelimien kanssa ylläpitäjän asettamalla tavalla (Matrix Federation). Viestihuoneet ovat toisistaan itsenäisiä siten, että jos niitä ei erikseen aseta avoimiksi tai mainostuviksi kaikille palvelimen jäsentunnuksille, ei niistä välity tietoa palvelimen jäsenelle, ellei häntä ole kutsuttu kyseisiin viestihuoneisiin. Mikäli federaatiotoiminto on asetettu, palvelin replikoi viestit ja viestihuoneet niille palvelimille, joista kutakin ketjua käyttävät matrix-tunnukset ovat peräisin. Palvelin itse ei ota kantaa viestien tai viestihuoneiden salaukseen; tästä huolehtii käytettävä asiakasohjelma, joista esimerkiksi Matrix.org:in omassa referenssiklientissä Element (kesäkuuhun 2020 asti Riot, nimenmuutos tavaramerkkisyistä) on avainten vuotamisen kannalta varsin huolellisesti suunniteltu E2EE. **Näin palvelimen tai sen tietokannan ”korkkaus” ei E2EE:tä käytettäessä johda** välittömään tietovuotoon – haasteena on yksinomaan avainten päätyminen vääriin käsiin.

2.1. Projekti ”Backroom” – Matrix-ekosysteemi päävestijärjestelmänä

Kuvauksesta voi päätellä, että protokollasta olisi moneksi sotilaallisiin tarkoitusperiinkin. Oma kehitysryhmäni, jonka tavoitteena on ollut täydentävän tai pääasiallisen viestijärjestelmän rooliin sopivan arjen ratkaisun kehittäminen, on lähtenyt liikkeelle siitä johtavasta ajatuksesta, että näissä rooleissa ratkaisun on loppukäytt**äjän ja ylläpitäjän kannalta** edullista muistuttaa peruskäyttömenetelmiltään kenttäviestijärjestelmiä. Matrix-ekosysteemistä on sen joustavuuden vuoksi helppo rakentaa järjestelmä, joka käyttöönotoltaan, verkkotopologialtaan ja ennen kaikkea sille sovellettavan perustaistelumenetelm**än puolesta** muistuttaa kenttäviestijärjestelmiä, millä esimerkiksi jääkärijoukko nyt käyttää liikkuvia tilaajiaan, kuitenkin niin, että alustan edut ja Rauténin kuvailemat käyttöpotentiaalit, joihin aiemmin ei ollut mahdollisuutta, säilytetään.

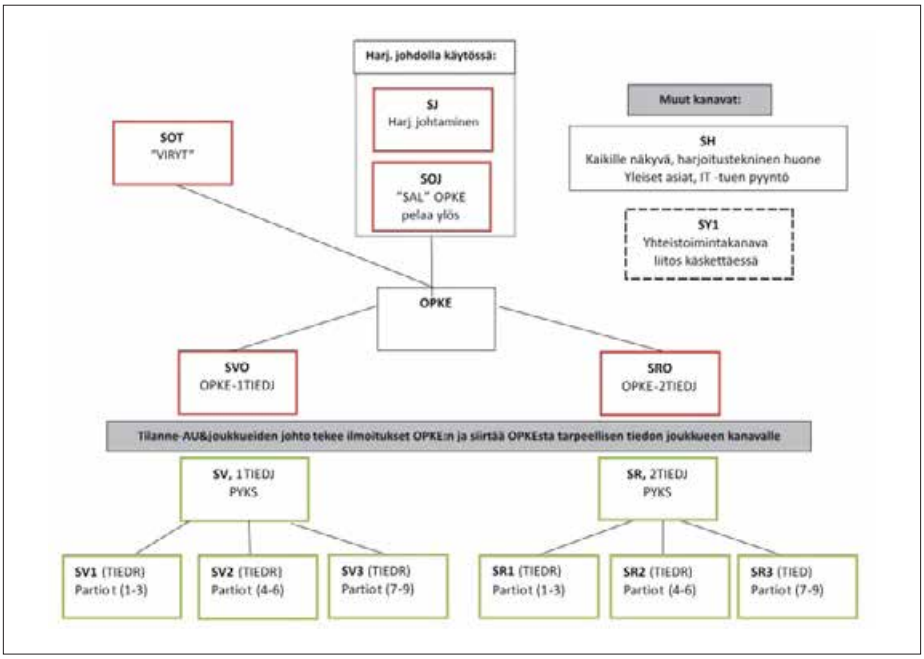
Elokuun 2019 lopusta olemmekin työstäneet työnimellä ”Backroom” arjen viestijärjestelmää, jonka ydin loppukäyttäjän kannalta on Matrix-protokolla, tärkeimpänä tavoitteenamme ratkaisutyypit 2 ja 3, täydentävä ja pääasiallinen viestitaktinen suorituskyky. Kehitysryhm**ämme kanssa, missä** käytön suunnittelijoina toimii allekirjoittanut ja tämän entisen rauhanturvaajaryhmän jäseniä sekä teknisenä toteuttajana **Jyri Genral**, tavoitteemme on ollut vastata näkemyksemme mukaan geneerisen joukkoyksikön ja perusyksikön viestiaselajille asettamiin vaatimuksiin – sekä toisaalta havainnoida, mitä siviilisuorituskyvyn mahdollisuuksien maailmasta näihin tarpeisiin tarvitaan.

Itse tiivistän nämä taktiset vaatimukset lyhyesti kolmeen yleiseen iskulauseeseen, tärkeysjärjestyksessä: viestitoiminnan on 1) mahdollistettava tulenkäyttöyhtedet, 2) tuettava joukon

johtamista ja 3) mahdollistettava nopea tilannekuvan tuotto. Viestitaktiikka on yhtä kuin vastaus **näihin tarpeisiin siten, että** huomioidaan joukon tyypistä, tehtävästä ja olosuhteista muodostuvat toteutuksen taktiset reunaehdot. Arjen ratkaisujen ja järjestelmien tapauksessa selkeitä reunaehtoja joukolle kuin joukolle ovat 1) riittävä tietoturva vs. riittävä yksinkertaisuus ja käytettävyys sekä 2) ”orgaaninen” kyky arjen järjestelmän perustamiseen ja ylläpitoon on suppea. Muut reunaehdot arjen järjestelmien käytölle muodostuvat muun muassa joukon kenttäviestijärjestelmästä – kyky ja tarve käyttää sitä. Tältä kannalta on lähtökohtaista, että epäilemättä joukon kuin joukon viestitaktiikassa arjen välineet tulisivat näyttelemään osaa nimenomaan ja erityisesti vaatimuksen 3) nopea tilannekuvan tuotto täyttämisessä, siinä missä kahden edellisen kannalta nämä voivat täydentää kenttäviestijärjestelmiä.

Näiden taktisten vaatimusten ja reunaehtojen täyttämiseen pyrkivä, Matrixia hyödyntävä perusideamme on järjestelmä, joka olisi itse perustettavissa esivalmistelluin viestiperustein ja konfiguraatioin, siten, että järjestelmän käyttöönotto ja käyttö olisi kenttäviestijärjestelmien tyyliin ennalta suunniteltua ja johdettavissa olevaa – yksinkertaista – mutta toisaalta järjestelmä itse olisi ajettavissa vuokra-, pilvi tai jopa kotipalvelimille ilman etukäteisvalmistelua niin, että perustamis- ja ylläpitoprosessi olisi mahdollisimman helppoa eikä vaatisi ”orgaanista” eli ennalta koulutettua henkilöstöä – orgaanisen kyvyn kannalta mahdollista ja toisaalta riittävästi tietoturvallista.

Näillä perustein ”Backroom”-projektin tekninen ydin, Matrixin ohella, on linux-jakelu, joka mahdollistaa järjestelmän esikonfiguroinnin yhtä tekstitiedostoa ja geneeristä asennuslevykuvaa käyttäen. Siten pelkän konfiguraation avulla on teoriassa mahdollista asettaa mikä tahansa laite tai verkkopalvelin etukäteen räätälöidyksi ”Backroom” –järjestelmän palvelimeksi sisältäen kaikki ajatellut sovellukset, kuten Matrix Synapse-palvelimen ja Mumblen perusasetuksineen. Tällöin joukolle voi teoriassa varata Backroom-palvelinverkon käyttöön varastoimalla muutaman konfiguraatiotiedoston – ja johtuen jakelun paketinhallintatavasta, konfiguraation perusteella käyttöönotossa asennettavat ohjelmaversiot ovat, ellei toisin määritetä, aina ajantasaisia, milloin järjestelmän pitäminen ajan tasalla on tavoitellusti yksinkertaista. Samoin operaatioturvallisuuden kannalta mielenkiintoisesti palvelua ei ole havaittavissa tai vuodettavissa ennen sen käyttöönottoa. Toistaiseksi



Kuva 2. P19-harjoituksen ”verkonkuva.” Kukin laatikko on Riot-huone. Lisäksi kutakin Riot-huonetta vastasi Mumble-huone, esim. ITIEDJ:n huone ”SV” -> Mumble-huone ”PV.”

tosin loppukäyttäjän käyttö**liittymä** – **viestiperusteet ja** Element (Riot)-sovelluksen käyttäjätunnukset ja huoneet – on laadittava etukäteen. Tarkoituksemme on koestaa myös tämän työvaiheen automatisointia esimerkiksi niin, että järjestelmän käyttöönottava henkilöstö tuottaa viestiperusteet ja käyttäjätunnukset skriptillä ja luo viestihuoneet Elementillä skriptin tuottamien viestiperusteiden avulla manuaalisesti.

2.2. Käyttökokeilu – P19:n sissit koekaniineina

Työ ”Backroomin” parissa on tähän asti sisältänyt yhden käyttökokeilun Stadin Sissien ja ESMPP:n KARPR:ssä syyskuussa 2019 järjestämässä Pahkis 19-tiedusteluharjoituksessa. P19:ssa noin 70 hengen vahvuinen joukko jaettuna kahteen tiedustelujoukkueeseen ja operaatiokeskukseen käytti ainoana viestijärjestelmänään Matrix-pohjaista järjestelmäämme. Järjestelmän näkökulmasta tiedustelujoukkueet itsenäisesti toimivine ryhmineen muodostivat kaksi perusyksikköä – operaatiokeskuksen sekä tiedustelujoukkueiden tilannepaikkojen tuottaessa käyttökokeiluun joukkoyksikkötason näkökulman. Joukkoa varten esiluotiin tunnukset ja keskeiset Matrix-palvelimen viestiketjut ”huoneet”, joita tuotetussa viestikäskyssä kutsuttiin ”AR-kanaviksi.” Käyttökoulutuksessa joukolle luovutettiin tunnukset ja joukon android- ja iOS-puhelimiin haettiin käytettävät sovellukset – Riot ja lisäksi Tahkokallion (Viestimies 4/19) mallin mukaisesti PTT-sovellus Mumble –, koulutettiin sovellusten perusominaisuudet sekä viestiperusteiden mukainen käyttö.

Siinä missä palvelua ylläpitävän joukon kannalta Matrix-ideamme on yksinkertaisuus ja kenttäviestijärjestelmissä muistuttava käyttöönotto, niin loppukäyttäjien kannalta pyrimme laatimaan käyttökokemuksesta ja viestiperusteista kenttäviestijärjestelmän kaltaisen –”kuin sanomalaitetta tai FINACCISta käyttäisi – paitsi että tällä voidaan lähettää kuvia.” Siten viestiperusteet laadittiin harjoitukseen tavanomaisuutta mukaillen, siten, että kullakin ”ryhmällä” – tässä tiedustelupartiolla – oli yksi liikkuva tilaaja, johon on asetettu tiedusteluryhmän (”joukkueen”) ja tiedustelujoukkueen (”perusyksikön”) kanavat kuunteluun. Joukkueiden tilannepaikoilla vastaavasti oli ryhmien (”joukkueiden”) kanavat kuuntelussa sekä lisäksi operaatiokeskus-joukkue (”joukkoyksikkö”) kanava, niin että tilannepaikan tehtävänä oli arjen viestijärjestelmää käyttäen rakentaa oman joukon tilannekuvaa ja välittää sitä ylös operaatiokeskukselle, joka puolestaan rakensi ”joukkoyksikön” tilannekuvaa kahden joukkueen elävän ja käsikirjoituksen valmiin tilanteen perusteella, välittäen tätä alaspäin sekä ”perusyksiköille” että harjoituksen johdolle. Näin kenttäviestijärjestelmän

tijärjestelmän kaltaisuus ideana toteutui myös loppukäyttäjille.

3.1. Pohdintaa – haasteena tietotulva (ja -turva)

Pohdinta, joka johti kenttäviestijärjestelmän kaltaisuuden tavoitteluun, on seuraava. Huolenaihe on Rauténin mainitsemalla tavalla tietoturva ja tietotulva. Tässä käsittelen tilan vuoksi vain tietotulvaa. On vaarana, että laitteesta ja palvelusta itsessään voi tulla loppukäyttäjälle valikkojen, vastaanottajien ja mahdollisuuksien tietotulva, sen lisäksi, että taistelukenttä itsessään on tietotulva.

Arjen välinein kyseessä on sama haaste kuin kenttäviestijärjestelminkin toimiessa. Yleisesti ottaen tarkan ja ajantasaisen tiedon saanti taistelukentältä ylös on vaikeaa, niin perusyksikön sisällä joukkueista komentopaikalle kuin perusyksiköstä joukkoyksikköönkin. Tilannekuvaa tuottavilla taistelukentän toimijoilla, ”tuntosarvilla” on paljon ärsykkeitä ja lisäksi potentiaalinen taistelutilanne. Hyvän tilanneymmärryksen saavuttaminen taistelussa tai vaikkapa partiossa on jo itsessään vaikeaa, jolloin viestikapula kädessä tulee helposti jo tämän haasteen vuoksi ajatelleeksi niin, että lähetän tämän eteenpäin, kun on aikaa. Jos viestivälineen käytössä on vähääkään epäselvyyttä – ”pitikö tämä asia ilmoittaa nyt heti, ja kenelle, ja mikä nappi se nyt oli?”, tämänkaltainen päätös vahvistuu. Vaikka tekniikka mahdollistaa, ajatus ei kulje – ja tilannekuva ensisijaisesti on juuri ajatuksen muodostamista, toissijaisesti välittämistä eteenpäin teknisellä apuvälineellä.

Jotta ”tuntosarvet” kykenevät siirtämään kokemaansa ja ymmärtämäänsä tietoa kokonaisuutta ja toiminnan jatkoa pohtiviin ”aivoihin” asti, on välittäjänä toimivan viestijärjestelmän oltava äärimmäisen selkeä, jopa ohjaava, siten että taistelija ottaessaan viestivälineen käteensä suunnilleen tietää, mitä tällä laitteella tulee lähettää ja minne, samoin kun hän tietää saadessaan käteensä telamiinoja, että nyt rakennetaan varamiinoite – minkä hän hallitsee, sillä hän osaa kuvitella toiminnan lopputuloksen mielessään. Samoin tilannekuvan apuvälineen on tuettava korvienvälystä siten, että se intuitiivisesti ohjaa käskettyyn ja toivottuun käyttöön.

Matrix-ideamme käytännöllinen, sotilaspedagoginen ydin onkin, että protokollan monipuolisten sovellusmahdollisuuksien avulla vältetään loppukäyttäjälle laitteesta johtuvaa tietotulva-kokemusta. Tämä siten, että tavat käyttää viestimiä siviilissä, eivät tulisi sotilaalle mieleen kohdatessa ”Backroom”, vaan mieleen tulevatkin tavat, joilla sotilas käyttää viestintä: ymmärrys siitä, että järjestelmään on ilmoitettava täsmällistä tietoa käskyn avulla hallituilla ”kanavilla”, jotka on ylhäältä päin rakennettu ja joita viestiperusteiden mukaan kuunnellaan. Samoin järjestelmän käyttöä johtavan ja ylläpitävän joukon näkökulmasta järjestelmä itse luodaan ex nihilo, jotta se ei olisi etukäteen vuotava, ja toisaalta, jotta sen käyttö olisi siirtotietä lukuun ottamatta keskeisesti omassa johdossa ja hallinnassa. Kun arjen järjestelmä muistuttaa tällä tavoin kenttäviestijärjestelmää, voidaan nojata taistelijoiden – niin tuntosarvien, aivojen kuin hermoston osaa näyttelevien viestimiestenkin – vanhaan koulutukseen: heillä on mielikuva valmiina, vain kapula vaihtuu tekstiviestejä lähettävästä vihreästä laatikosta tai ruggeroidusta tietokoneesta älypuhelimeen.

3.2. Käyttökokeilun ja pohdinnan yhteenveto

P19-käyttökokeessa ajatus onnistui. Alle 45 minuutin rastikoulutuksella harjoitusjoukon viestiliikenne järjestelmällä oli kurinalaista, kuin olisimme käyttäneet sanomalaitteita, mahdollistaen luotettavan tilannekuvan rakentumisen perusyksikkötasolla. Arjen välineen hyödyt realisoituvat: jakotavaraa viestivarastolta ei harjoituksessa tarvittu, ja tiedusteluhavainnoista saattoi lähettää kuvia yhtä hyvin kuin tekstiä, kuten pikaviestisovelluksilla yleensä. Ongelmat, jotka tulivat ilmi palautteessa, liittyivät siviililaitteiden käyttöön vaativissa olosuhteissa. Etenkin jos periaate on käyttää COTS-laitteita mielessä ”omat laitteet” tai ”tyhjennetään Gigantti”, laitteiden sähkönkulutus, vedenkestävyys ja näyttövalon aiheuttama pimeänäön kato tulevat konkreettisiksi haasteiksi maastossa toimivalle joukolle.

Käyttökokeilun perusteella voimme todeta Matrix-protokollan mielenkiintoisen puolen olevan se, että siitä on mahdollista rakentaa johdettu ja valvottu arjen järjestelmä, joka on helppo räätälöidä tarkoituksenmukaiseksi teknisesti palvelimeen kuin pedagogisesti taistelijoiden ajatuksiin. Toisaalta – protokolla mahdollistaa Rauténin kuvaamalla tavalla mielenkiintoisia kokonaan uudentyyppisiä sovellutuksia. Näistä mielenkiintoisimpina voi pitää viranomaisyhteistyötä ja yhteyttä paikalliseen väestöön.

Kolmanneksi, niin ikään Rauténin esitykseen verraten, Matrix-protokolla mahdollistaa myös teknisesti hyvin toisenlaisen lähestymistavan arjen viestijärjestelmän toteuttamiseen, kuin mitä omassa käyttökokeilussamme koestimme, kuitenkin niin, että loppukäyttäjän näkökulmasta – ”korvien välistä” puheenollen – tuo tärkein eli käyttöprosessi on samankaltainen. Siltausominaisuuden avulla voidaan itse viestiliikenteessä käyttää edeltä rakennetun ja itse kokonaan hallitun järjestelmän sijaan tavanomaisia pikaviestisovelluksia siten, että käyttäjille käsketään vastapäät, mutta tilannekuvaa rakentavalla tasolla Matrix-siltaus kokoaa eri kanavilta tulleet viestit tarkoituksenmukaisella tavalla yhteen.

Näin ollen jo yhden protokollan ääressä huomattavan vaihtoehtojen moninaisuuden johdosta onkin lopuksi todettava, että tärkein askel arjen ratkaisujen hyödyntämisen tutkimuksessa ei ole kuitenkaan ole protokollan tai tietyn ratkaisumallin, kuten Matrixin, ajaminen eteenpäin – vaan Rauténin sanoin ”täytyy parantaa raportointia kentältä ja tutkimuksesta suuntaan ja toiseen.” Vaihtoehtojen ja tehtävien moninaisuuden hahmotteluun, toteuttamiseen ja koestamiseen tarvitaan ihmisiä, ympäristöjä, joissa tutkimusta tehdään ja arvioidaan – yksi tai muutama pää yhden järjestelmän kimpussa kykenee tähän jo ajankäyttösyistä heikommin kuin useampi pää, jotka vertailevat useampia ideoita samassa ympäristössä. Yliopistomaailmassa käyn parhaillaan viikoittain graduseminaarissa keskustelemassa siitä, kuinka uskottavaa tutkimustyötä tehdään. Lopputuloksena on graduja erilaisista aiheista, mutta kuitenkin graduja, jotka täyttävät tieteelliseltä kirjoittamiselta vaaditut asiat ja siten kykenevät toteuttamaan yliopiston opinnäytetyöprosessille määrittämät tehtävät. Vastaavasti on syytä rakentaa arjen välineiden kehitykselle jonkinlaista johdettua yhteyttä, esimerkiksi alueellisesti joukko-osastoittain, jotta ideanikkarien – niin aktiivisten reserviläisten kuin sotilashenkilöiden ja yritysten – ajatusten koestamiselle ja kehittämiselle teoriassa ja käytännössä olisi väylä.

TEKSTI: SEPPO URO

Jääkärieversti Birger Homén - viestikoulutuksen uranuurtaja

Jääkärieversti, diplomi-insinööri Birger Homén kuului siihen pieneen jääkäriupseerien joukkoon, jonka johdolla juuri perustettuihin Suomen puolustusvoimiin luotiin viestijoukot ja uusi aselaji. Homén ilmoittautui jääkärikoulutukseen Lockstedtin leirille ensimmäisten tulevien viestiupseereiden joukossa. Ennen häntä leirille olivat saapuneet vain Eric Heimbürger ja Väinö Pasanen. Hyvän viestialan tuntemuksensa ja saksan kielen taitonsa johdosta Homén sai pian keskeisen aseman jääkäreiden kouluttajana ja saksalaisten upseerien ja aliupseerien apulaisena. Hänen syntymästään tulee marraskuussa kuluneeksi 140 vuotta.

Lars Birger Homén syntyi säätyläisperheeseen Helsingissä 11.11.1880. Hänen vanhempansa olivat hovioikeudenneuvos, senaattori Lars Homén ja hänen puolisonsa Anna Ulrika Baarman. Homén kirjoitti ylioppilaaksi Helsingin uudesta ruotsalaisesta yhteiskoulusta vuonna 1901 ja liittyi Uusimaalaiseen osakuntaan. Tämän jälkeen hän suoritti vapaaehtoisena vuoden mittaisen asepalveluksen Suomen Rakuunarykmentissä Lappeenrannassa. Asepalveluksen jälkeen vuonna 1902 hän aloitti opinnot Hannoverin teknillisessä korkeakoulussa valmistuen sieltä insinööriksi vuonna 1906. Valmistuttuaan korkeakoulusta hän toimi koneinsinöörinä ja teknillisenä johtajana useissa eri tehtaissa Suomessa, Ruotsissa ja Saksassa vuosina 1906-14. Työtehtäviensä ohessa hän teki opintomatkoja Saksaan ja Englantiin vuonna 1907.

Ensimmäisen maailmansodan sytyttyä loppukesällä 1914 rajat sulkeutuivat ja ulkomailla opiskelevien ja työskentelevien suomalaisten mahdollisuudet palata kotimaahansa olivat heikot. Työskennellessään Saksassa Homén sai tiedon jääkäriliikkeestä ja päätti liittyä maanmiestensä joukkoon heti kun se kävi mahdolliseksi. Hän ilmoittautui Lockstedtin leirillä jo noin kolme viikkoa

koulutuksen aloittamisesta 18.3.1915. Homén määrättiin palvelukseen aluksi Pfadfinder-kurssin 1.Komppaniaan, josta hän siirtyi saman vuoden syyskuussa konekivääriKomppaniaan ja toukokuun lopulla 1916 3.Komppaniaan. Jalkaväkikoulutuksen ohessa jääkäreille ryhdyttiin antamaan myös puhelin- ja viittoilulippukoulutusta, jota johti saksalainen luutnantti Lindner. Tämä valitsi apukouluttajakseen jääkäri Homénin, joka koulutuksensa puolesta soveltui tehtävään hyvin. 34-vuotiaana hän kuului joukon vanhimpiin ja oli ainoana jääkäreistä saanut myös sotilaskoulutusta Suomen "vanhassa väessä". Homén menestyi tehtävässä ja ylennettiin Gruppenführeriksi jo syyskuussa 1915. Keväästä 1916 alkaen viestikoulutusta laajennettiin järjestämällä jääkäreille useita viestikursseja, joiden kouluttajana Homén yleensä toimi. Toukokuussa 1916 jääkäreistä muodostettiin Kuninkaallinen Preussin Jääkäripataljoona 27, joka määrättiin rintamapalvelukseen Saksan itärintamalle Missejoelle ja Riianlahdelle. Homén toimi rintamapalveluksen aikana viestitehtävissä ja osallistui myös Aajoen talvitaisteluihin.

Pataljoonan palattua jatkokoulutukseen Tuckumiin ja Libauhun Homén jatkoi viestimiesten kouluttajana ja joukon suomalaisena esimiehenä. Hänet ylennettiin Zugführeriksi 9.8.1917. Kun viestikoulutetuista jääkäreistä muodostettiin pataljoonan tiedonanto-osasto 2.10.1917 Homén määrättiin sen johtajaksi ja ylennettiin 24.12.1917 Oberzugführeriksi eli samaan arvoon, joka oli kaikilla muillakin komppanianpäälliköillä. Jääkärikauden lopulla Homén osallistui myös johtajatehtävissä toimineille jääkäreille tarkoitetulle lyhyelle sotakoulukurssille. Muiden komppanianpäälliköiden tavoin hänet ylennettiin majuriksi juuri ennen jääkäreiden kotiinpaluuta 11.2.1918. Varsinaisen sotilaskoulutuksen ohessa jääkäripataljoonassa tehtiin myös muita valmisteluja Suomessa eteen tulevia tehtäviä ajatellen. Saksalaisia ohjesääntöjä suomentamalla ja Suomen oloihin sovittamalla jääkärit kirjoittivat laajan ohjesääntö- ja oppikirjakokoelman, joka sai nimen Suomalainen sotilaskäsikirja. Pataljoonassa kehitettiin sotaväelle myös suomenkieliset komentosanat. Kerrotaan, että äidinkieleltään ruotsinkieliselle Homénille nämä teettivät aluksi jonkin verran ongelmia. Eräs tiedonanto-osaston marssiharjoitus Libaussa päättyi komentoihin "Halt, seis, stopsis, eller va fan ä de på finska!"

Homén saapui Vaasaan jääkäripataljoonan pääjoukon mukana 25.2.1918. Jo 3.3. hän sai ylipäälliköltä tehtäväksi perustaa valkoiselle armeijalle sen ensimmäisen viestijoukko-osaston, Kenttälennätinpataljoonan. Pataljoonaan määrätyt upseerit ja aliupseerit ilmoittautuivat Mikkelin työväentalossa 5.3.1918, mikä päivä määrättiin myöhemmin Viestirykmentin ja viestiaselajin vuosipäiväksi. Kenttälennätinpataljoonan toiminta osoittautui kuitenkin vaikeaksi. Koulutettaviksi ei saatu miehiä, joilla olisi jo ollut sotilaan perustaidot ja ehkä vähän viestialankin tuntemusta. Myös viestikalustosta oli huutava puute. Lisäksi pataljoonan henkilökunta halusi rintamalle peläten, että

joukosta tulee vain rintamantakainen koulutuskeskus. Edellä mainituista syistä Kenttälennätinpataljoona päätettiin jo maaliskuun lopulla muuttaa jalkaväkijoukoksi. Se sai nimen 5.Jääkärirykmentin XV Jääkäripataljoona. Joukko-osaston kokoonpanoa laajennettiin siten, että siihen kuului kolme kivääriKomppaniaa ja konekivääriKomppania. Majuri Homén jatkoi pataljoonan komentajana. Vähäisestä viestikoulutetusta henkilöstöstä muodostettiin kaksi noin parikymmentä miestä käsittävää osastoa, jotka lähetettiin rintamalle viestitehtäviin. XV Jääkäripataljoona siirrettiin huhtikuun lopulla Karjalankannakselle Rautuun ja sieltä edelleen Kuokkalan ja Terijoen seudulle, jossa se osallistui Vapaussodan lopputaisteluihin. Sodan päätyttyä pataljoona jäi Vammelsuun ja Raivolan alueelle linnoitustöihin ja rajojen valvontaan. Syksyllä 1918 5.Jääkärirykmentti nimettiin Kuopion Jalkaväkirykmentiksi n:o 4 ja majuri Homén palveli sen III Pataljoonan komentajana loppuvuoteen 1918.

Vuoden 1919 alusta lukien Homén määrättiin I Pataljoonan komentajaksi Itämeren Jalkaväkirykmenttiin n:o 1, joka oli muodostettu Helsingissä Vapaussodan aikana toimineista joukoista ja siirretty syksyllä 1918 Turkuun. Rykmentin pääosat toimivat Venäjän vallan aikaisella Vähä-Heikkilän kasarmialueella, mutta esikunta ja I Pataljoona Turun vanhoilla puukasarmeilla. Maaliskuussa 1919 joukko-osaston nimi vaihtui Porin Rykmentiksi. Majuri Homén toimi joukko-osastossa pataljoonan komentajan tehtävän ohessa myös rykmentin komentajan sijaisena useassa eri jaksossa yhteensä noin 2,5 vuoden ajan. Vuonna 1919 I Pataljoona osallistui koulutuksen ja tavanomaisen varuskuntapalveluksen lisäksi noin puolen vuoden ajan myös itärajan vartiointiin Karjalankannaksella. Samana vuonna Suomeen hankittiin Ranskasta vähäinen määrä panssarivaunuja, joita ajateltiin käytettävän ensisijaisesti jalkaväen tulitukena. Joukko jalkaväkijohtajia perehdytettiin uuden aseen käyttöön Hämeenlinnassa järjestetyillä hyökkäysvaunukursseilla. Homén osallistui tällaiselle kurssille vuonna 1922. Helmikuussa 1926 majuri Homén sai siirron Helsingin liepeille Santahaminaan, jossa hän toimi Uudenmaan Rykmentin III Pataljoonan komentajana runsaan kahden vuoden ajan. Kesällä 1928 hänet ylennettiin everstiluutnantiksi ja määrättiin Vaasan kutsuntapiirin päälliköksi. Kun kutsuntapiirit muuttuivat sotilaspiireiksi vuonna 1932 hän jatkoi Vaasan sotilaspiirin päällikkönä lakisääteiseen eroonsa saakka 11.11.1935. Hänet ylennettiin everstiksi vuonna 1941. Erottuaan vakinaisesta palveluksesta Homén toimi Tammisaaren kaupungin maistraatissa raastuvanoikeuden arvostettuna kunnallisneuvosmiehenä kuolemaansa saakka 13.5.1947.

Jääkärieversti Birger Homénilla oli merkittävä osuus puolustusvoimien viestiaselajin syntyvaiheissa, mutta hänen myöhempi sotilasuransa itsenäisen Suomen puolustusvoimissa keskittyi ensisijaisesti komentajatehtäviin jalkaväkijoukoissa. Tämä lienee johtunut siitä, että toimintaansa aloittelevissa viestijoukoissa ei vielä tuolloin ollut riittävästi tehtäviä ja vakansseja jo majurin arvoon ylennetylle upseerille. Tästä huolimatta eversti Homén ansaitsee tulla muistetuksi eräänä nuoren aselajin tärkeistä johtajista ja kehittäjistä.

TEKSTI JA KUVAT: SAKARI AHVENAINEN

Kybernetiikka: Informaatio-aikakauden ja kybersodankäynnin ajattelumalli? (osa 2/2)

Tiivistelmä: Tämä kaksiosainen artikkelisarja käsittelee kybersodankäynnin yleisiä perusteita. Lähtökohta on sanan *kyber* tausta ja historia. Informaatioaikamme tarvitsee myös oppia tai teoriaa, joka käsittelee tietoa kokonaisuutena kuten teollisuuden aika käsitteli energiaa termodynamiikan kautta. Kybernetiikka on yksi tällainen kokonaisvaltainen malli tai -teoria. Se on laaja yläkäsite ja sellaisena edelleen paljolti filosofinen, strateginen ja ”vain” ajattelun apuväline.
Artikkelisarja käsittelee kybernetiikkaa sen perusilmiöiden, erityisesti kyberneettisen systeemikäsityksen kautta. Yksi tästä näkökulmasta tuleva johtopäätös on, että kybersodankäyntiä on ollut olemassa yhtä kauan kuin ihmiskunnassa on ollut sotia. Kybernetiikka on muutenkin, hypestä huolimatta, luonnollinen jatkumo osana paljon laajempaa evoluutiota (ks. osa 1, Viestimies 2/2020).
Kybernetiikka selventää (?) myös tietoturvallisuuden suhdetta kyberturvallisuuteen ja luo niistä kokonaisvaltaisen systeemin. Sama koskee informaatiosodankäynnin ja kybersodankäynnin suhdetta.

Artikkelisarjasta

Tämän artikkelisarjan ensimmäisessä osassa, Viestimies lehden numerossa 2/2020 esiteltiin kybersodankäyntiin liittyen kybernetiikan yleisiä perusteita, ensin mitä kybernetiikka on ja mitä se ei ole. Näiden lisäksi käsiteltiin muutamia kybernetiikan uusia sovellutuksia, kybernetiikan perusilmiöitä sekä valikoituja kohtia kyber-sanan ainakin kaksi tuhatta vuotta vanhasta historiasta. Lopuksi esiteltiin lyhyesti kolme kyberneettistä järjestelmää - elävä solu, ihminen ja tietokone - sekä niiden evolutiivinen systeemiriippuvuus toisistaan. Myös tietokoneiden merkitys kasvavan kompleksisuuden hallinnassa oli yksi käsiteltyjä aiheita. Artikkelin lisäksi kyseisen lehden Lyhyesti – palstalla esiteltiin muutamia artikkelin ja kybernetiikan kannalta keskeisiä teoksia, joukossa myös useita suomalaisia teoksia.

Tässä artikkelisarjan osassa 2/2 jatketaan kybernetiikan perusilmiöiden käsittelyä. Vuorossa ovat yleisen kyberneettisen järjestelmän perusosat, kyberneettisen järjestelmän tiedonkäsittelyn perusteita sekä se, miten kybernetiikka liittyy yleisellä tasolla (nykyaikaiseen) sodankäyntiin.

Lopuksi esitellään artikkelisarjan kootut johtopäätökset. Ne jakautuvat neljään osaan: Ensin, mitä kybersodankäynti on *tämän artikkelisarjan perusteella*, mikä on uutta kybersodankäynnissä, mikä on vanhaa kybersodankäynnissä ja lopuksi mitä muuta voidaan sanoa yleisesti kyberin ja tiedon suhteesta.

Artikkelisarjan yhtenä mottona voisi pitää evoluutiobiologi Richard Dawkinsin ajatusta siitä, että aina silloin tällöin on hyvä katsoa vanhoja teorioita ja faktoja uusin silmin.

Kyberneettisen järjestelmän perusosat

Tietoa käsitteleviä, eli kybernettisiä järjestelmiä ovat ensin elävä solu ja sen emergenttinä tasona, täysin uutena ilmiönä elämä, toiseksi ihminen ja ihmisen emergenttinä tasona (olemassaolon) tietoisuus ja lopuksi kolmantena tietokone. Mutta mikä on tietokoneen luoma emergentti taso? Tähän palataan johtopäätöksissä.

Tässä artikkelissa käytetyn tulkinnan mukaan kyberneettisen järjestelmän pohja on aina järjestelmän fyysinen rakenne, esimerkiksi ihmisen solut sekä tietokoneen hardware, esimerkiksi mikropiirit ja piirilevyt. Alkuperäinen, Wienerin 1940-luvun (matemaattinen) kybernetiikka ei ollut kiinnostunut kyberneettisen järjestelmän fyysisestä rakenteesta, tiedon alustasta. Tässä mielessä tämän artikkelisarjan näkökulma on osin erityinen.

Fyysisen rakenteen lisäksi kyberneetti-

sessä järjestelmässä on abstraktia tietoa, joka on pohjimmiltaan ero. Kybernettisessä järjestelmässä ei siis ole abstraktia tietoa ilman fyysistä todellisuutta, atomeja. Voidaan myös sanoa, että tieto on tällä tavalla nähtynä aineellisen todellisuuden emergentti, uusi ominaisuus. Koskeeko tämä tiedon riippuvuus aineellisesta alustasta myös yleisemmin kaikkea tietoa?

Tiedonsiirtotekniikan OSI-malli - Open Systems Interconnection Reference Model - noudattaa pitkälti yllä mainittua logiikkaa. Alin, ”yhden bitin siirtävä” kerros on siinäkin fyysinen. Muut tasot ovat emergenttejä ja abstrakteja tiedon tasoja, jotka muodostuvat periaatteessa alatasonsa osista tai palveluista.

Kybernettinen järjestelmä pystyy säätöön, eli tavoitteen saavuttamiseen kyberneettiseen järjestelmään sisältyvän säätö- ja tilaprosessin kautta. Kyberneettisen järjestelmän kyberneettiset perusosat ovat *sensori, päätöksentekoelin, toimielin, tavoitearvo, palautekytkennät, rajat, tilaprosessi* ja nämä kaikki yhteen liittävä *viestintäjärjestelmä*. Toinen vastaava ryhmittely perusosille on syöttöarvo (input), ulostuloarvo (output) ja musta laatikko.

Sensori muuttaa ympäristöstä tai kyberneettisestä järjestelmästä itsestään saatavan tiedon kyberneettisen järjestelmän ymmärtämään muotoon, esimerkiksi valon fotonit silmässä sähkökemialliseksi hermosignaaliksi. Periaatteessa kyberneettinen systeemi, esimerkiksi ihminen, voi saada todellisuudesta vain sellaista tietoa, jonka saamisen hänen sensorinsa mahdollistava. Ihmisellä sensorit voivat olla biologisia tai esimerkiksi teknologisia. Esimerkkejä ihmisen tietoa laajentavista teknisistä sensoreista ovat kaukoputki ja mikroskooppi ja tämän artikkelin kannalta keskeinen tietokone. Tutkimusvälineenä se tekee kompleksisuuden ”näkyväksi” ihmiselle. Tämä liittyy muun muassa kaaosteorian syntyyn ja fraktaalien löytymiseen.

Päätöksentekoelin muuttaa sensoritiedon valinnaksi, eroksi, joka ohjaa toimielintä. Päätöksentekoelin on yksinkertaisemmillaan fyysistä rakennetta, esimerkiksi refleksi, nollavalinta, mutta sensorin ja vaikutuksen yhteen kytkemistä, eli vaikutusta todellisuuteen silti. Kyberneettisen systeemin fyysinen rakenne on jo määritelmänkin mukaan kokonaisuus ja todellisuuden malli, joka pystyy oman tietonsa havaitsemiseen, tulkintaan, käsittelyyn ja sen mukaiseen toimintaan. Ylemmillä ja kompleksisimmilla tasoilla valinta sisältää myös muistia, tietoa sekä tiedollisia malleja todellisuudesta ja tietoa käsitteleviä tilaprosesseja.

Todellisuuden mallien ohjelmoinnissa kieli on tärkeä, sekä ihmisten että tietokoneiden osalta. Kielen merkitystä kuvaa myös noin 50.000 vuotta sitten syntynyt ihmiskunnan aivan uudenlainen, nopeasti muuttuva ja uusia komponentteja sisältänyt kulttuuri. Sen perustaksi on esitetty modernin, rajattomasti koodaavan kielen syntymistä. Uusia ihmisyhteisön elementtejä olivat muun muassa uusi suurempi organisaatio (klaanista heimoksi), suurriistan metsästys, kauppa, taide sekä nopeasti kehittyvä ja yhä kompleksisempi teknologia.

Ihmisen kannalta päätöksentekojärjestelmän, eli lähinnä aivojen rakentuminen yksilön historiallisten kokemusten ja elinikäisen oppimisen summana tarkoittaa, että jokainen on yksilö ja jokaisen tulkintatausta todellisuuden ilmiöille eroaa aina enemmän tai vähemmän muiden tulkinnasta. Tieto, sen tulkinta ja laajempi ymmärrys ovat siis ihmisen osalta aina subjektiivista. Tässä kybernetiikan tulkinta poikkeaa perinteisestä länsimaisesta tietokäsityksestä, jossa tieto oli objektiivista, tarkkailijasta riippumatonta.

Malleihin liittyen uusi ja merkittävä asia on tietokoneiden ja tietokonepohjaisten todellisuuden mallien asema ihmisen yhä kompleksisemman, globaalin toiminnan ymmärtämisessä, organisoinnissa ja kontrollissa. Tietokone ja oikea data mahdollistaa massamaisen vaikuttamisen (lehdistö, radio, TV) sijasta täsmävaikuttamisen. Siinä kohdeyleisö on segmentoitu ja kuhunkin segmenttiin vaikuttamisessa tarvittava täsmädata löytyy (globaalin) sosiaalisen median eri kanavista. Muun muassa USA:n vuoden 2016 presidentinvaaleihin liittyvä Cambridge Analytica - yrityksen toiminta oli juuri tätä. Mallintaminen ja siihen liittyen laskennallinen tiede yleisemmin pitäisi olla yhä keskeisempi uuden tieteen tutkimus- ja sovellutusalue.

Toimielin muuttaa lopuksi päätöksentekoelimen valinnan vaikutukseksi todellisuuteen, esimerkiksi päätöksen kahvin juomisesta käden toiminnaksi, kahvikuppiin tarttumiseksi ja kahvin juomiseksi. Tämä tarkoittaa, että (kyberneettisen) tiedon lopullinen tavoite on yleensä toiminta, todellisuuteen vaikuttaminen, todellisuuden muuttaminen. Tässä mielessä kyberneettinen systeemi edustaa joksikin tulemista jonain olemisen sijasta. Tämäkin poikkeaa perinteisestä länsimaisesta tieteestä, jossa teleologia, tutkittavien ilmiöiden tavoitteellisuus ei ole tieteen valtavirtaa. Tässä mielessä aika ennen kyberneettisiä järjestelmiä oli pitkälti ”epätavoitteellista”, fysiikkaa ja kemiaa. Uusi kybernetiikan aika on kyberneettisten systeemien osalta tavoitteellista, eli biologiaa ja ihmisten osalta myös psykologiaa, sosiologiaa ja politiikkaa. Tässäkin, kuten yleensä evoluutiossa, mikään vanha ei poistu lopullisesti. Vaikka elämme nyt tavoitteellisten kyberneettisten järjestelmien aikaa, niitä edeltäneet ei-tavoitteelliset järjestelemät, esimerkiksi atomit ja molekyylit, ovat edelleen olemassa ja vaikuttavat.

Tavoite- tai säätöarvokin palvelee todellisuuteen vaikuttamista. Se on kyberneettiseen järjestelmään ”ohjelmoitunut” ja kyberneettistä järjestelmää ”ylätasolla” ohjaava loppu- tai tavoitetila, johon se rakenteensa tai tietojensa perusteella ”pyrkii”. Näitä voivat olla esimerkiksi elämän voima (vitalismi!?), vaistot, säätöarvo tai sotilaallisen operaation tavoitetila, operaation loppuasetelma.

Palautekytkennät luovat silmukan muun muassa säätöarvon ja kyberneettisen tilaprosessin saavuttaman tilan välille. Tämä mahdollistaa säädön, tavoitteen saavuttamisen, joksikin tulemisen. Perussäätöjä on kaksi, negatiivinen ja positiivinen säätö. Negatiivinen on rajoittava ja positiivinen on vahvistava säätö.

Kyberneettisen systeemin rajat suojaavat systeemiä ulkoisilta häiriöiltä. Rajat myös rajoittavat systeemin toimintaan vaikuttavia tekijöitä ja yksinkertaistavat systeemiä ja mahdollistavat näin muun muassa sen sisäisen häiriöttömän säädön. Tästä on helppo tunnistaa muun muassa valtio kyberneettisenä systeeminä, historiallisena ja myös uudempana kyberajan organisaationa. Kyse on nyt erityisesti siitä, onko valtio ”liian” avoin (globaalille tiedolle) ja sen seurauksena epäsysteeminen, kaoottinen.

Kyberneettinen systeemi on keskeisesti tilakone, jolla on tiloja ja joka pystyy muuttamaan tilaansa ulkoisen ja sisäisen tiedon ja sen prosessoinnin ja siihen perustuvan toiminnan perusteella. Ihmisen suurempia tiloja voisivat olla esimerkiksi hedelmöittynyt munasolu, vastasyntynyt, lapsi, aikuinen ja vanhus. Pienempiä tiloja voisivat olla esimerkiksi nälkäinen, janoinen, suuttunut, …

Viestintäjärjestelmä liittää edellä mainitut kyberneettisen systeemin osat yhteen. Se on systeemin *kokonaisuuden* keino osiensa koordinaatioon, yhteistoimintaan, mutta myös niiden kontrolliin. Viestintä ja säätö tekevät kyberneettisestä systeemistä älykkään, suuremman kuin osiensa summa. Sama koskee esimerkiksi muurahaisista ja mehiläisistä (osista) koostuvia muurahais- tai mehiläispesiä (kokonaisuus) sekä ihmisen organisaatioita perheistä (parisuhteista) globaaliin

ihmiskuntaan. Oleellista on, että erilaisilla kyberneettisillä systeemeillä on erilaiset, kyseessä olevaan tasoon optimoidut viestintäjärjestelmät. Ihmisen sisällä kokonaisuuden kontrollin keinoina toimivat hormonit ja hermosto ja ihmisten välillä esimerkiksi ilmeet, eleet ja erityisesti kieli ja sen laajennukset kuten kirjoitus- ja kirjapainotaito päätyen aina globaaliin tietokoneteknologiaan ja internetiin. Viestimiehille taktisten, operatiivisten ja strategisten viestijärjestelmien erilaisuus ja erillisuus on itsestään selvää.

Tieto ja kyberneettinen järjestelmä

Tieto liittyy kybernetiikkaan kahdella perustavaa laatua olevalla tavalla ja molemmat eron kautta. Ensin vähintään kahden erilaisen asian, viestin tai valinnan abstraktina erona se on tiedon ja päätöksenteon pohja. Tieto liittyy, verkottuu jo aivan perustasolla vähintään kahteen eron pohjalla olevaan asiaa. Esimerkkinä komentajalle pidettävä operaatiovaihtoehtojen vertailu tai nolla ja ykkönen tietokoneteknologian tiedon pohjana. Toiseksi saman asian kahden ajantilan erona tieto on säädön pohja, esimerkiksi termostaatissa huoneen olevan lämpötilan ja ”tulevaisuuden” tavoitearvoksi asetetun lämpötilan ero.

Tieto esiintyy kyberneettisessä järjestelmässä neljällä periaatteellisella tasolla. Ne ovat alimmasta ylimpään (1) sensoritieto todellisuudesta, (2) päätöksentekoelimen rakenne ja tietomallit todellisuudesta ja (3) tavoitearvo, johon systeemi omassa todellisuudessaan, toimintaympäristössään rakenteensa perusteella ”pyrkii”. Ja lopuksi (4) kybernettisen järjestelmän rakenne kokonaisuutena on erityinen ”valinta”, joka pystyy kokonaisuutena käsittelemään kyseessä olevan kyberneettisen systeemin tietoa. Näitä kaikkia ja niiden välisiä takaisinkytkentöjä tarvitaan säätöprosessin osana.

Sensoritieto todellisuudesta ja kyberneettisen järjestelmän osien välillä on alimpana tietorakenteena kyberneettisen systeemin tietoa itsestään ja etenkin toimintaympäristöstään. Se on siirrettävää tietoa, dataa. Oleellista on, että tietoa saadaan todellisuudesta vain sensorien kautta, ihmisillä aisteilla. Kybernetiikassa ei siis ole filosofista ”suoraa todellisuustietoa”. Kyberneettinen sensoritieto on aina sensoreiden välittämää ja päätöksentekoelimen rakenteen ja sen todellisuusmallien tulkitsemaa ja tällä tavalla tulkittuna ainakin kahdella tavalla rajoittunutta. Tästä voi saada jopa filosofista pohjaa ihmisen ymmärryksen rajoille.

Todellisuuden malleilla päätöksentekoelimessä tulkitaan todellisuudesta saatua sensoritietoa aivoissa tai tietokoneessa. Mallit sisältävät ihmisellä geneettisesti ja kulttuurisesti perityt ja kokemuksen kautta opitut tai ohjelmoidut todellisuuden mallit, mukaan luettuna muun muassa tieteelliset teoriat, geenit, meemit, tarinat, myytit, huhut ja luulot. On siis olemassa kyberneettisen järjestelmän ulkopuolinen fyysinen todellisuus, se ”todellinen todellisuus” ja kyberneettisen järjestelmän sisäiset, ulkopuolista todellisuutta kuvaavat mallit, virtuaalinen todellisuus, se kyberavaruus. Näiden kahden *erilaisen* todellisuuden riittävän suuri yhteneväisyys on evoluutiossa eloonjäännin keskeinen pohja muun muassa yksilöillä, lajeilla, sotilaallisilla yksiköillä ja valtioilla.

Sensoritieto ja sen tulkintamallit näkyvät muun muassa ihmisen näköaistissa. Näkeminen ei ole ”kameramaista”, silmistä tulevaa signaalia. Näkeminen on 90 prosenttisesti tulkintaa muun muassa sillä perusteella, että aivojen näkökeskuksen yhteyksistä vain 10 prosenttia tulee silmistä. Myös näkemiseen liittyvät väärät *tulkinnat* kertovat samasta.

Sensoritiedon ominaisuuksia ja yleensäkin systeemin ja sen toimintaympäristön keskeisyyttä kuvaa edelleen esimerkiksi se, että ihmisen näköalue on tietyllä kapealla sähkömagneettisen spektrin alueella, jota kutsumme valoksi. Miksi? Koska auringon säteilymaksimi on kyseessä olevalla alueella. Tämä liittyy luonnon tehokkuusperiaatteeseen.

Tavoite- tai säätöarvo on kolmas kyberneettisen systeemin tietolaji, johon systeemi ”pyrkii” tai pyrkii. Se on kyberneettisen järjestelmän pohja, esimerkiksi solussa sen ”pyrkimys” itsensä kopiointiin, siis elämän säilyttämiseen ja jatkumiseen tai sotilaallisella yksiköllä sen pyrkimys sille tehtävänä annettuun tavoitteeseen.

Kyberneettisen järjestelmän rakenne kokonaisuutena on erityinen ”valinta”. Se pystyy kokonaisuutena käsittelemään kyseessä olevan kyberneettisen systeemin tietoa muun muassa sen datan peruseroja.

Puhuttaessa tiedon kontekstista, merkityksestä, siitä mihin tieto liittyy, löydetään edellisen perusteella kolme eri tasoista merkitystä: Ensin sen fyysinen konteksti (Vrt. OSI-malli), toiseksi sen tulkinta, todellisuuden malli mihin se liittyy ja kolmanneksi minkä kyberneettisen systeemin tiedosta on kokonaisuutena kyse.

Sodankäynti ja kybernetiikka

Tässä luvussa ei puututa tarkemmin siihen, mitä sodankäynti on. Sinänsä sodankäynnin määritelmä ja määrittely olisi nykyisen suuren ja nopean muutoksen aikana aivan keskeistä. Esimerkiksi kysymys siitä, onko sodankäynti vain ja aina väkivallan käyttöä vai toimiiko myös tieto sodankäynnin välineenä väkivallan tapaan tai sen rinnalla?

Alla olevassa kuvassa on vertailtu ihmisen, tietokoneen ja sodankäynnin perusominaisuuksia kyberneettisenä järjestelmänä. Kuten kuvasta on pääteltävissä, sodankäynti on yleisellä tasolla kyberneettinen, tietoa käsittelevä ja säätöä sisältävä järjestelmä.

Kybernetiikka on ollut sodan taustalla aina tiedon ja säädön, tavoitteen kautta, aluksi ihmisiin ja myöhemmin myös tietokoneisiin liittyen. Jälkimmäisissä kybernetiikka on ollut osa sodankäyntiä ensimmäisestä tietokoneteknologian sovellutuksesta asti, eli toisesta maailmansodasta alkaen.

COLOSSUS oli toisen maailmansodan aikana erityistarkoitukseen rakennettu tietokonesarja murtamaan Saksan ylimmän sodanjohdon käyttämä salaamisjärjestelmä, Geheimschreiber. Kuuluisampaa Enigma-salakirjoituskonetta käytettiin alemmilla tasoilla. Yksi ensimmäisiä todellisia monikäyttöisiä tietokoneita, 1940-luvun ENIAC (Electronic Numerical Integrator And Computer), oli strateginen tuote ja maailmanhallinnan väline. Strategisella tasolla sitä sovellettiin muun muassa atomipommia kompleksisemman vetypommin suunnitteluun. Siihen tarvittiin noin miljoona reikäkorttia useammassa vaiheessa. Ja strategisena tuotteena ja maailmanhallinnan välineenä tietokone on säilynyt koko historiansa ajan ja sellainen se on kybersodankäynnissä edelleen. Laskennallisen tieteen kannalta ENIAC:n lyhenteen avaus yllä on vähintään mielenkiintoinen, erityisesti kun muistetaan, että ”computer” tarkoitti alun perin (naispuolista) laskijaa, joka käytti lähinnä paperia ja kynää.

USA:n 1960-luvun loppupuolen Arpanet-viestintäverkkoa pidetään yleensä internetin esiasteena. USA:ssa oli kuitenkin jo 1950-luvun lopulla koko valtakunnan laajuinen tietokonepohjainen kyberneettinen järjestelmä, Semi-Automatic Ground Environment (SAGE), USA:n ilmapuolustusjärjestelmä Neuvostoliiton ydinpommittajia vastaan. Se sisälsi sensoreita (tutkat), päätöksentekoelimiä (tietokoneet ja ihmiset), laajan viestintäjärjestelmän sekä toimielimiä (torjun-

Kybernetiikka, ihminen, tietokone ja sodankäynti

Kyberneettisen systeemin osat	Ihmisessä	Tietokoneessa	Sodankäynnissä
Sensori (tieto todellisuudesta)	Mm. aistit	Mm. näppäimistö, hiiri, …	Alayksiköt, oma tiedustelu, ylempi johtoporras, …
Päätöksenteko-yksikkö	Aivot, todellisuuden mallit, (kyber-avaruus1!)	Mikroprosessori, todellisuuden mallit, (kyberavaruus2)	Komentaja ja esikunta, kasvavasti tietokoneet, todellisuuden mallit (kyberavatuus1 ja 2)
Toimielin (todellisuuteen vaikuttaminen)	Kädet, jalat, muut lihakset, …	Näyttö, kovaääniset, ohjattavat prosessit	Alayksiköt, epäsuora tuli, elso, pioneerit, …
Rajat	Iho	Kotelo	Vastuualueen rajat, …
Takaisinkytkentä, palaute	Aivot – käsi – silmä – aivot - …	IF …THEN … ELSE	Käsky – raportti – tarkastus – käsky,
Tavoite	Tavoitteet elämässä, päivässä, …	Asetusarvo, tavoitetila, …	Tavoite, operaation loppuasetelma, …
Tilat	Hedelmöittynyt munasolu, vasta-syntynyt, lapsi, …	Ohjelmoitavana, ohjelmaa tai aliohjelmaa suorittava, ohjelmaa odottava, virraton, …	Koulutuksessa, valmiudessa, taistelussa, reservissä tai huollossa oleva, tuhoutunut, …
Viestintäjärjestelmä	Hermosto, hormonit, …	Väylät, emolevy, tiedonsiirron stradardit, modemit, …	Puhe, merkit, radiot, tiedonsiirtojärjestelmät, …

Taulukko: Onko sodankäynti kyberneettinen järjestelmä?

tahävittäjä). Projektina se oli jopa suurempi ja kalliimpi kuin USA:lle toisessa maailmansodassa ydinaseen tuottanut Manhattan – projekti.

Amerikkalainen sotilaallista johtamista vastaava termi on ”Command and Control” (C2), siis ”käskeä ja valvoa”, säätää, pyrkiä tavoitteeseen. Alun perin termi oli vain ”Command”, käskeä. Ennen taistelua annettiin omille johtajille ohjeet (taistelun tavoite, lopputila) ja taistelun alettua mahdollisuudet ”säätöön” olivat pienet. Termi on kehittynyt useamman välivaiheen kautta niin, että nyt puhutaan jopa C4ISTAR:sta, eli termistä ”Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, Reconnaissance”. Siitä löytyy johtaminen (säätö), tietokoneet, viestintä, useanlaiset sensorit (tiedustelu) sekä maalittaminen (vaikutus).

Ensimmäisen postmodernin strategin ja sodankäynnin filosofin John Boydin OODA-loop (Observation, Orientation, Decision and Action) on melko puhdas kyberneettinen säätö- ja informaatiojärjestelmä. Observation viittaa sensoriin, Orientation ja todellisuuden malleihin ja Decision päätöksentekoelimeen ja Action toimielimeen ja toimintaympäristöön (viholliseen) vaikuttamiseen.

Johtopäätöksiä

Tässä artikkelisarjassa on esitelty yksi ja erityinen näkemys kybernetiikkaan. Tavoitteena oli saada sitä kautta perusnäkemystä kybersodankäyntiin. Näkemyksen pohja ovat hyvin yleiset, ylätason lähtökohdat kybernetiikkaan, lähinnä vielä erityisesti kyberneettiseen järjestelmään liittyen. Osoittautui, että näistäkin lähtökohdista päästään mielenkiintoisiin ja merkittäviin, joskin yleisiin johtopäätöksiin, *ymmärtämiseen periaatteessa*. Erityisen merkittävää oli pitkän aikavälin tarkastelu, tässä kolme kyberneettistä systeemiä osana olemassaolon suurempaa evoluutiota. Tämä tarkastelu toi mukanaan pitkän aikavälin johtopäätöksiä, joita voidaan pitää merkittävinä. Näillä johtopäätöksillä on merkitystä, kun tulevaisuuden sodankäyntiä pyritään hahmottamaan kyberneettisestä näkökulmasta.

Ensimmäisenä merkittävänä johtopäätöksenä todetaan, että tietokoneteknologian kehitys on vailla vertailukohtaa ihmiskunnan teknologian historiassa. Tästä ja tietokoneen yleiskäyttöisyydestä seuraa ennen näkemätön ihmiskunnan evoluution nopeus ja muutoksen laajuus. Se on informaatioteknologinen ja valon nopeuteen perustuva evoluutiovaihe, kun edellinen vaihe oli ihmiseen, paperiin ja fyysiseen tiedonsiirtoon (ihminen, hevonen) perustuva kulttuurinen evoluution vaihe.

Toiseksi todetaan, että kybernetiikka on yksi kokonaisvaltainen malli tai teoria informaation ja säädön käsittelyyn. Se on sellaisena edelleen säätötekniikan perusta, mutta muuten lähinnä laaja yläkäsite ja paljolti filosofinen, strateginen ja ”vain” ajattelun apuväline. Tähän liittyen pitää kuitenkin aina kysyä, mitä muita vastaavia tietoa käsitteleviä kokonaisvaltaisia teorioita on olemassa? Kybernetiikka antaa kuitenkin mahdollisuuden ymmärtämiseen *periaatteessa*.

Kolmanneksi todetaan, että vaikka kybernetiikka korostaa sen abstraktia, tiedollista tasoa, kyberneettinen systeemi perustuu tässä artikkelissa esitetyssä mallissa aina ensin fyysiseen todellisuuteen, kyberneettisen systeemin atomeihin. Pilvipalvelu voi olla palvelun käyttäjän kannalta pitkälti abstrakti, ”mielenkiinnoton” asia, mutta palvelun tarjoajan kannalta pilvipalvelun käytännössä toteuttavat kovalevyt, tietokoneet ja niiden yhteydet ovat hyvinkin mielenkiintoisia ja konkreettisia asioita ja ne sijaitsevat aina jossain, osana fyysistä todellisuutta. Kyberneettisen systeemin (ihminen /

tietokone) fyysinen, sen pohjana oleva osa, voidaan siis valloittaa tai miehittää maavoimilla, tappaa myrkyllä tai hermokaasulla, se voidaan tuhota tulenkäytöllä tai ohjuksilla ilmavoimilla, sen viestintäjärjestelmän yhteydet voidaan katkaista esimerkiksi elektronisen sodankäynnin häirinnällä tai se voidaan tuhota korkeäjähdyksen EMP-pulssilla. Kybersodankäynti on ylätason kokonaisuus ja kokoisuuden tulisi hallita osia, jotta tehokkuutta ja synergiaa syntyisi. Tämä perusteella informaatiosodankäynti ei voi olla asevoimien kyberajan ylimmän tason doktriini.

Seuraavana käydään läpi artikkelisarjan yksityiskohtaisemmat johtopäätökset niin, että ensin esitellään (1) mitä kybersodankäynti on, sitten mitkä ovat (2) uusia asioita kybersodankäynnissä, mitä ovat (3) vanhoja asioita kybersodankäynnissä ja (4) mitkä liittyvät muuten tietoon, kyberiin tai kyberneettisiin järjestelemiin yleisemmin.

Mitä kybersodankäynti on?

Mitä kybersodankäynti on tämän artikkelisarjan, eli kybernetiikan ja kyberneettisen systeemin näkökulmasta? Kybersodankäynnin pohjalla ja esiasteena on perinteinen ihmiskeskeinen ja fyysinen, väkivaltaan perustuva clausewitziläinen sodankäynti. Kybersodankäynti oli tässä esivaiheessa vain osa sodankäynnin luonnollista evoluutioprosessia ja pitkää jatkumoa. Kyberiin, eli säätöön ja informaatioon liittyvät asiat olivat paljolti vielä ”heikkoja signaaleja”. Myös valon nopeuden käyttöönotto tiedon siirrossa lennättimessä 1800-luvun puolivälissä oli vielä uuden kyberaikakauden heikko signaali.

Kybersodankäynnistä voidaan alkaa puhua uutena ja merkittävämpänä asiana, kun globaalin tietokoneteknologian ja globaalien tietokoneverkkojen merkitys nousee sodankäynnin ytimeen *ihmisen rinnalle*. Me elämme jo tätä aikakautta. Mutta kuten yleisemmin evoluutiossa, mitään vanhaa ei poistu lopullisesti. Uuden tietokonepohjaisen ja globaalin kybersodankäynnin osana on edelleen sen vanha, ihmiseen ja väkivaltaan perustuva valtiollinen pohja, tosin muuttuneena, eli muokkautuneena uuden megatrendin mukaisesti. Seuraavana käydään tarkemmin läpi, mikä on uutta ja mikä on vanhaa kybersodankäynnissä.

Mikä on uutta kybersodankäynnissä?

Onko kybersodankäynti tämän artikkelisarjan käyttämän näkökulman ja määritelmien mukaan uusi ilmiö? On ja ei. Uutta kybersodankäynnissä on ensin se, että *ihmisen rinnalle* nousee toiseksi tietotoimijaksi tietokone monine seurannaisvaikutuksineen. Tämän toimijan merkitys on kasvanut koko ajan ja kasvaa edelleen. Tietokoneen kautta muun muassa täsmäaseet, keinoäly ja vihamieliset ohjelmistot sekä vihamieliset mikropiirit tulevat tärkeiksi sodankäynnissä. Tämä on niin merkittävä ja pysyvä muutos, että se edellyttää myös asevoimien rakenteiden muuttamista. Yksi ilmeinen muutostarve on kyberpuolustushaaran luominen.

Yksi tietokoneen luomista monista seurannaisvaikutuksista on globaalien tietokoneverkkojen muodostaman kyberavaruus. Tässä tietokoneiden kyberavaruudessa erityistä on se, että tämä kyberavaruus on ensimmäinen keinotekoinen, ihmisen luoma sodankäynnin ulottuvuus verrattuna esimerkiksi alkuräjähdyksen luomiin tilaan ja aikaan. Tämä taas kertoo paljon teknologian ja sen mukana muun muassa teknisen infrastruktuurin roolista nyky-yhteiskunnassa ja sen sodankäynnissä. Viittaan tässä esimerkiksi teknologiseen huoltovarmuuteen perinteisen öljyn ja viljan *lisäksi*.

Uutta kybersodankäynnissä on myös sen globaali luonne, eli se on kaksi tasoa valtiotason yläpuolella. Välissä on kulttuurinen taso, kuten Länsi tai Kiina. Sen ydin oli yleinen tiede ja teknologia. Huomionarvoista tässä on, että esimerkiksi sotilasfilosofit Clausewitz ja Sunzi käsittelevät lähinnä vain sodankäynnin valtiollista tasoa. Globaali toiminta on sinänsä vanha asia ainakin löytöretkistä alkaen, mutta globaalin tietokoneteknologian kautta sen vaikutus on monella tavalla ennen näkemättömällä tasolla, kuten tietokoneet yleisestikin.

Uutena tasona globaali ihmiskunta on lisäksi systeeminä emergentti, eli omaa uusia ominaisuuksia, joita emme voi ennustaa etukäteen, ainakaan täsmällisesti. Hyviä esimerkkejä ovat sosiaalisen median palvelut kuten Google, Facebook, Instagram ja Twitter ja miten ne ovat muuttaneet maailmaamme viimeisen *kymmenen* vuoden aikana. Ne syntyivät uuden globaalin systeemin eri osien, uusien ja vanhojen, yhteisvaikutuksesta, verkostosta. Muutosvaihe tarkoittaa kaaosta ja korostaa nopeaa uusien systeemien havaitsemista ja yleensäkin oppimista. Globaali toiminta on myös osa uutta laajempaa tiedon avoimutta, joka on koko ajan kasvanut jo aiemmissa vastaavissa informaatioteknologian megamuutoksissa. Näitä ovat olleet protokieli, kieli, kirjoitustaito, kirjapainotaito.

Globaalin tason mukana muun muassa strateginen viestintä globaaleissa tietoverkoissa nousee valtioiden merkittäväksi toiminnaksi ja muuttaa niiden toimintaa. Tämä liittyy siihen, että suuressa systeemimuutoksessa (globaali ihmiskunta) suuremman ja uuden systeemitason uudet ominaisuudet muokkaavat aiempia tasoja, esimerkiksi valtioita. Onko tässä ideassa osa Venäjän uutta vaikutusvaltaa?

Uutta on myös uuden vaiheen uusi ylivoiman lähde suhteessa vanhoihin vaiheisiin: Edellisen kulttuurisen vaiheen aikana 1800-luvun lopun siirtomaaupseeri saattoi levollisena todeta joutuessaan lukumääräisesti pahasti alivoimaisena taisteluun Afrikan alkuasukkaiden kanssa: ”Meillä on Maxim (konekivääri), heillä ei”. Mikä on tämän uuden kybervaiheen Maxim? Kyky vaikuttaa suoraan vastustajan päätöksentekoon ja tietojärjestelmiin, siis ihmisiin ja tietokoneisiin ja niihin perustuviin systeemeihin. Erityisesti kyse on täsmävaikuttamisesta johtajiin ja kansan erilaisiin osakokonaisuuksiin. Antaako tämä myös viitteitä siitä mitä tapahtuu, kun uuden vaiheen ylivoiman lähde on useamman toimijan hallussa? Viittaan tässä konekivääriin osalta ensimmäiseen maailmansotaan ja nyt siis muun muassa Venäjään ja Kiinaan.

Uutta on edelleen kybersodankäyntiin liittyvä uusi nopeus ja uuden ulottuvuuden uudet ominaisuudet. Lentokone avasi 1900-luvun alussa sodankäynnille aivan uusia mahdollisuuksia. Niitä olivat lentokoneen suuri nopeus ja kyky ohittaa kaikki pinnan esteet. Vastaavasti kybersodankäynti mahdollistaa valon nopeuden hyväksikäytön ja muun muassa asevoimien ja monenlaisen muun puolustuksen ohittamisen ja iskemisen suoraan vastustajan *kansan ja johdon tahtoon*. Tässä on oleellista, että ihminen on edelleen sodankäynnin merkittävin tekijä ja tahto edustaa sodankäynnissä sen korkeinta tasoa.

Mikä on vanhaa kybersodankäynnissä?

Vanhaa kybersodankäynnissä on ensin sodankäynti, eli se, että sota on ”vain” evolutiivinen väline ratkaista isojen ihmisyhteisöiden välisiä eturistiriitoja ja sitä, mitkä suuret organisaatiot jäävät henkiin. Tässä mielessä kyber on tieto-

koneiden osalta ”vain” yksi uusi väline sodankäynnin, vihamielisten eturistiriitojen ratkaisussa.

Edellisen perusteella kaikki sodankäynnin perusilmiöistä johtuvat asiat toimivat myös kybersodankäynnissä. Sodankäynnin perustavaa laatuisin ilmiö on oman tahdon omaavan vastustajan olemassaolo ja siitä seuraavat asiat. Tärkeiksi tulee tällöin muun muassa kyberneettinen (K) suhteellinen etu, K-yllätys, K-salaaminen, K-harhauttaminen ja K-operaatioturvallisuus. Sodankäynti on edelleen vihamielistä vaikuttamista, mutta nyt yhä enemmän (globaalilla) tiedolla, ei pelkästään asevoimien väkivallalla. Kiinalaisittain voidaan yleistää, että kaikki vaikuttamisen keinot ovat aina olleet mukana suurstrategiassa, jonka yksi ja vain yksi elementti on sotilasstrategia, asevoimien käyttö valtion poliittisten tavoitteiden välineenä.

Vanha ilmiö kybersodankäynnissä on myös ihmisen osuus, eli ihminen tietotoimijana. Tämän perusteella ihmisen aivoissa ja erityisesti kielen kehittymisen jälkeen laajemmin myös aivojen verkostoissa on aina ollut kyberavaruudeksi kutsuttavissa oleva tiedon ensimmäinen ulottuvuus. Tietokoneverkkojen globaali kyberavaruus ja sen pienemmät osat ovat ihmiseen liittyen vasta toinen abstraktin tiedon ulottuvuus, kyberavaruus.

Vanha ilmiö on myös se, että mikään vanha ei poistu kybersodankäynninkään mukana, vaan muokkautuu uuden systeemin ja sen ominaisuuksien mukaisesti. Perusesimerkki on aseiden muuttuminen täsmäaseiksi, aseiksi, jotka sisältävät tiedon käsittelyä ja säätöä ilman ihmistä. Tämä koskee myös esimerkiksi fyysistä väkivaltaa ja valtiota, joista kumpikaan ei tämä periaatteen perusteella poistu. Tämä lohduttanee ns. perinteisen sodankäynnin kannattajia ja on varoitus niille, jotka uskovat suurempaan sodankäynnin vallankumoukseen tai peräti sodankäynnin loppumiseen. Mutta *kaikki* on muutettava kybersodankäynnin mukaisiksi ja tämä korostaa erityisesti kyberpuolustushaaran tarvetta.

Kybernetiikasta ja tiedosta

Kybernetiikka ja sen mukana tieto ja säätö perustuvat tässä artikkelisarjassa esitetyn tulkinnan mukaan aina ensin fyysiseen todellisuuteen (hardware) ja vasta sitten abstraktiin tietoon (software). Tämän kyberneettisen tulkinnan mukaan ei ole olemassa itsenäistä, atomeista riippumatonta ”ideoiden maailmaa”.

Kybernetiikka on integroiva, kokonaisvaltainen teoria tai ajattelumalli tiedosta. Ensin se yhdistää fyysisen todellisuuden ja abstraktin tiedon kokonaisuudeksi. Tämä kokonaisuus on kyberneettinen järjestelmä. Onko tässä pohjimmiltaan kyse jopa ikiaikaisen ruumiin ja mielen ongelman periaatteellisesta ratkaisusta? Ja se mikä on jäänyt muun muassa Descartesilta huomaamatta on *emergenssi*, miten (ruumiin) osista muodostuu uusi kokonaisuus, tiedon käsittelykyky ja siihen liittyvä tietoisuus. Toiseksi kybernetiikka yhdistää kolmen tasoisen tiedon yhteen järjestelmään: systeemin tavoitteen toimintaympäristössään, systeemin todellisuudessa, systeemin mallit todellisuudesta ja systeemin sensoritiedot todellisuudesta. Esimerkiksi Shannonin tiedon*siirto*teoria käsittelee vain tätä viimeistä, siirrettävää sensoritietoa. Shannonin teoria ei ole (yleinen) informaatioteoria, kuten hän itsekin kirjassaan toteaa.

Mielenkiintoinen johtopäätös saadaan siitä näkökulmasta, että viestijärjestelmä on kyberneettisen järjestelmän koordinaation ja kontrollin välttämätön väline, kyseisen kokonaisuuden toiminnan mahdollistaja. Jos globaali tietokoneteknologia on globaalin ihmiskunnan uusi viestijärjestelmä, se mahdollistaa siis paitsi yhteistoiminnan, myös kontrollin. 2010-luvulla tästä on saatu useita uusia havaintoja, esimerkiksi Snowdenin paljastusten ja vaalien ja muiden poliittisten ilmiöiden manipuloinnin osalta. Onko tässä myös Venäjän tämän hetken vaikuttamisen pohjaa, eli keskittymistä osaltaan uuden ajan vaikuttamisen ytimeen, globaaliin tietoon?

Esitetty kybernettisen systeemin malli antaa myös selkeyttä (?) paljon keskustelua ja mielipahaa herättäneeseen tietoturvallisuuden ja kyberturvallisuuden suhteeseen. Tietoturva on osa ja kyberturvallisuus on kokonaisuus. Kyberturvallisuus on fyysisen turvallisuuden (hardware) ja informaatioturvallisuuden (software) summa. Tietoturva on (vain) abstraktiin tietoon liittyvää turvallisuutta. Fyysiseen turvallisuuteen kuuluu muun muassa tietokoneiden ja mikropiirien fyysinen rakenteellinen turvallisuus ja suoja muun muassa varkauksia vastaan. Jos pyrimme hallitsemaan kokonaisuuksia ja samalla siis kompleksisuutta, on aloitettava kyberturvallisuudesta. Tässä voidaan taas viitata kyberpuolustushaaran tarpeeseen ja siihen, miten uusi taso muuttaa kaikkea aiemmin ollutta. Abstrakti tietoturva liittyy sekä ihmisiin että tietokoneisiin, periaatteessa jopa soluihin ja siis biologiseen ja kemialliseen sodankäyntiin. Sivuhuomautuksena todettakoon, että solua, ensimmäistä kyberneettistä järjestelmää, ei ole käsitelty mainintaa enemmän tässä artikkelisarjassa.

Erityisen tärkeää tässä on, että kyberturvallisuus ja tietoturva, eli systeemi ja sen tieto ovat tässä esitetyn tulkinnan mukaan eri tason ilmiötä, kokonaisuus ja osa. Tasojen sekoittamisesta seuraa aina tehottomuutta, virheitä, epäloogisuuksia, paradokseja ja vaikeuksia.

Kyberneettisen tiedon kolme tasoa, (1) sensoritieto (data), (2) todellisuuden mallit sen tulkintaan ja (3) kyberneettisen systeemin säätöarvo kyberneettisen systeemin tiedon korkeimpana tasona, sen kokonaistavoitteena, antaa myös perusteita tiedon käytölle (kyber-)sodankäynnissä. Se antaa muun muassa vastauksen datan keräämisen tärkeyteen. Sillä ei ole merkitystä, jos ei ole dataa tulkitsevaa mallia. Jos taas on tiedossa dataa tulkitseva malli, tiedetään jo etukäteen ja tarkasti millaista tietoa pitää kerätä. Säätöarvo, systeemin tavoite tiedon korkeimpana tasona on kuitenkin merkittävin. Sunzi sanoo tämän asian niin, että sodankäynnissä tärkeintä on hyökätä vihollisen suunnitelmaa, strategiaa, kybernetiikan kielellä sodan kokonaistavoitetta vastaan. Seuraavaksi tärkeimpiä hyökkäyskohteita ovat liittoumat (vrt. Suomen NATO-kysymys!), vasta sitten sotilaat ja huonoin vaihtoehto on hyökätä linnoitettuihin kaupunkeihin (vrt. Helsinki ja Kaartin jääkärirykmentti).

Informaatio ja tieto ovat materian uusi ja emergentti taso osana kyberneettisiä systeemejä. Mikä on informaation emergentti taso? (Ihmisen ja olemassaolon) tietoisuus? Mikä on ihmisen tietoisuuden emergentti taso? Globaali tietoisuus globaaleissa tietoverkoissa, noosphere, järjen ulottuvuus?

Kun ihmiskunta on yhä enemmän organisoitunut globaaliksi yksiköksi, hyvässä ja pahassa, seurauksena ovat globaalit ongelmat, hyödyt ja yhteistoimintatarpeet. Niiden uudella tasolla oleva kompleksisuus edellyttää uusia asioita, ensin ajattelua ja toiseksi muun muassa välineitä. Uudenlaista ajattelua ja sen välineitä edustavat muun muassa systeemianalyysi, operaatioanalyysi, kompleksisuusteoria, kaaosteoria, kybernetiikka, tietokonesimulointi, peliteoria ja laskennallinen tiede. Niissä tietokone on välineenä kasvavasti välttämätön. Se on ihmisen aivojen ja siis ymmärryksen laajennus kompleksisuuden ymmärtämisen ja hallinnan (?) suuntaan. Näiden ongelmien ja yhteistoimintatarpeiden dynaamisuus, verkottuneisuus ja takaisinkytkennät taas johtavat siihen, että ihmisen peräkkäisyyteen, evoluutiossa syy-seuraus suh-

teeseen rakentunut ajattelun logiikka ei yleisesti ole enää riittävä.

Tietokone edustaa myös tärkeää ajattelun muutosta muun muassa laskennallinen tieteen ja keinoälyn kautta. Ajattelun muutos on kaikkien suurien muutosten pohjalla, niiden juurisyy. Aiemmat ajattelun muutokset ovat olleet usko useammalla tasolla ja sitten perinteinen, paperiin perustuva tiede. Uskon vaiheita edustavat luonnon uskonto, esi-isien palvonta, kaupunkijumalat ja modernit, globaalit uskonnot. Tieteen vaiheita edustavat muun muassa astronomia tieteen esiasteena, sitten tieteellisen, aakkosiin ja paperiin perustuvan mielen synty noin 3000 vuotta sitten antiikin Kreikassa sekä myöhemmin perinteinen länsimainen, matematiikkaan, reduktionismiin, teorioihin ja kokeisiin perustuva tiede. Tietokone edustaa uudenlaista, laskennallista tiedettä. Mutta mitään vanhaa ei poistu tästäkään. Tämä pitää paikkansa perinteisen tieteen, mutta myös eritasoisten uskontojen ja uskomusten osalta.

Lopuksi ja yleisesti: Kybernetiikka on perinteisen länsimaisen newtonilaisen tieteen haastaja, monella tapaa. Sillä on periaatteellisesti hyvinkin erilainen tulkinta muun muassa tiedon objektiivisuuteen, (evoluution) tavoitteellisuuteen (teleologia) ja reduktionismiin, eli suuren ongelman hallitsemiseen pilkkomalla se yhä pienempiin ja ”paremmin” hallittaviin osiin. Osana tätä laajempaa muutosta tieteessä on myös determinismin tuho. Sen tuhosivat kvanttimekaniikka ja kaaosteoria.

Lopuksi ja sodankäyntiin liittyen: Clausewitzin mukaan vastustaja tulee tehdä puolustuskyvyttömäksi ja tämä on sotilaallisen toiminnan *käsitteellinen* tavoite. Perinteinen, joskin erityisesti länsimaalainen keino siihen on ollut fyysinen väkivalta, vastustajan asevoimien tuhoaminen. Voiko informaatio tehdä vastustajan puolustuskyvyttömäksi? Voi, jos sen tietokonejärjestelmiä ja uskomusjärjestelmiä, tavoitteita ja todellisuuden malleja voidaan hallita. Onko tämä tapahtunut jo? Useamminkin?

Vastaan mielelläni artikkeliin liittyviin kysymyksiin ja perustelen tarvittaessa asioita tarkemmin ja lähteillä. Olen enemmän kuin kiinnostunut jatkamaan keskustelua aiheesta: sakari.ahvenainen@kolumbus.fi

TEKSTI: SAKARI AHVENAINEN

Lyhyesti

– aineistoa artikkeliin liittyen

Tämän Viestimies lehden numeron Lyhyesti – palstalla esitetään kybernetiikkaan liittyviä kirjoja. Aihe liittyy lehdessä muualla olevaan artikkeliin ”Kybernetiikka, informaatioaikakauden ja kybersodankäynnin ajattelumalli?”. Kybernetiikkaan liittyviä kirjoja esiteltiin myös Viestimies-lehden edellisen numeron Lyhyesti-palstalla.

Artikkelisarjan pohjana on kaksi kirjoittajan kybersodankäyntiin liittyvää konferenssiesitystä: ”What Systems Theory and Evolution Can Tell Us About Cyberwar?” *European Conference on Cyber Warfare and Security* (ECCWS) (Dublin 2017) ja “Cybernetics: Theory of General Information Influence? - Information, Computers and Humans as an Essence of Postmodern Warfare” *International Society of Military Sciences* (ISMS) (Varsova 2016). Linkit kyseisiin esityksiin:

https://ln2.sync.com/dl/d951f6640/bxndub94-g5kd2hbq-6ryv8d6g-vfenspdb

https://ln2.sync.com/dl/ac027b6f0/bjkzw6zp-z94uwvyr-u7djqtnj-xccphr63

Turchin, V. F. (1977): *The Phenomenon of Science - a cybernetic approach to human evolution*, Abode Reader pdf Edition, New York, Principia Cybernetica Project. Tämä USA:han vuonna 1977 muuttaneen venäläisen fyysikon, kyberneetikon ja tietojenkäsittelyn tiedemiehen teos käsittelee evoluutiota ja tiedettä kybernetiikan näkökulmasta. Näihin liittyen Turchinin keskeinen tutkimuskohde oli metasysteemimuutos (metasystem transitions). Turchin työskenteli kuuluisan neuvostoliittolaisen toisinajattelijan Andrei Sakharov kanssa. Linkki: http://pespmc1.vub.ac.be/POSBOOK.html

Reed, Thomas. C. (2004). *At the Abyss - An Insider's History of the Cold War*. New York: Ballantine Books. Kirja on USA:n apulaispuolustusministerin muistelmateos siitä, miten Kylmä Sota hänen mielestä voitettiin. Kybernetiikan kannalta kirjassa on tärkeää, miten Neuvostoliittoon salakuljetettiin vihamielisiksi manipuloituja mikropiirejä ja ohjelmistoja, joiden kautta niitä käyttävät NL:n järjestelmät olivat USA:n hallittavissa, kontrollissa.

Toffler, Alvin ja Toffler, Heidi (1994). *Sodan ja rauhan futurologia – Miten selviydymme hengissä 2000-luvulla*. Otava. Tofflereiden vuoden 1994 ennustus tulevaisuuden sodankäynnistä keskittyy informaatioon. Teoksen ennustukset pitävät hyvin paikkansa edelleen siltä osin kuin niitä esitetään teoksessa. Merkittävin puute teoksessa on tiettyjen asioiden puuttuminen, muun muassa sosiaalisen media osuus. Se syntyikin vasta 2000-luvulla. Internet esiintyy kirjassa, mutta sen keskeisyyttä tulevaisuudelle ei ole arvioitu oikein.

1990-luvulla USA:n tiedusteluyhteisö kartoitti tiedustelun tulevaisuuden haasteita julkisessa kirjassa useamman skenaarion voimalla. Yksi kirjan johtopäätös oli, että internet oli keskeinen kaikissa skenaarioissa. Jos sitä ei olisi jo keksitty, se olisi pitänyt keksiä!

Fyysikko Heinz Pagelsin jo yli 30 vuotta vanha kirja ”*Dream of Reason – The Computer and the Rise of Sciences of Complexity*” vuodelta 1989 käsittelee tieteen paradigman muutosta Valistuksen aikana syntyneestä paperilla tehtävästä tieteestä tietokoneella tehtävään ja sen mahdollistavaan tieteeseen. Tämä on laskennallista tiedettä ja sen ydin on kompleksisuuden hallinta. Tietokone on samanlainen kompleksisuuden tutkinnan väline kuin kaukoputki suuren (kosmos) ja mikroskooppi pienen (bakteerit ym.).

Analysaattori

SOME:n nopeudella

Se on se vauhti, jolla uutiset nykyään leviävät. Nopeutena tämä lienee vain vähän valon nopeutta suurempi. Eipä mene silmänräpäystäkään siitä, kun Dannyllä on uusi nuorikko kierroksessa tai kasvomaskien hyödyllisyydestä on uusi hurja teoria, kun kaikki sen jo tietävät. Näinä vaikeina aikoina erityisesti huonot uutiset leviävät hurjaa vauhtia. Viestimies ilmestyy kuitenkin entiseen vakaaseen tahtiinsa ja niinpä mekin taas suoritamme tässä katsauksen ajankohtaisiin asioihin, niiden viereen ja vähän taaksekin. Ja erityisesti juuri sinne.

Syynä tiedonvälityksen nykyvauhtiin on luonnollisesti (toistaiseksi) ilmainen Internet. Johtava hakukonepalveluita tuottava Google kertoo, että sillä on joka sekunti noin 40000 hakua. Googlella on kuitenkin hakukonemarkkinoista enää vain 65% markkinaosuus. Markkinaosuus on ollut aika paljon suurempikin vielä muutama vuosi sitten. Analysaattori ainakin hieman yllättyi tuosta lukemasta ja syyhän on se, että nousevat palvelut Yandex ja Baidu vastaavat yhdessä jopa yli 10% markkinaosuuksista. Yandex on venäläisten ja Baidu kiinalaisten hakupalvelu. Jopa vanha kunnon Yahoo nauttii yhä 4,9% osuudesta. Noita molempia itäisiä haastajia vähän testailin mutta Baidun käyttö ei oikein sujunut, sillä Kiina on edelleen vähän marginaalikieli meidän VHS-miesten keskuudessa. Yandex oli periaatteessa aika miellyttävä kokemus, sillä se ei tyrkyttänyt mainoksia. Kokeilu loppui kuitenkin lyhyeen sillä asettaessani hauksi ”*Russians like Donald Trump*” toimintani keskeytyi ja sain englanniksi ilmoituksen ”*ip osoitteestasi tulevat haut vaikuttavat automatisoiduilta*”. Elämme mielenkiintoisia aikoja, sillä venäläiset luulevat Analysaattoria robotiksi.

Päällimmäisenä suomalaisessa mediassa tätä kirjoitettaessa on juuri piakkoin julkaistava älypuhelinsovellus Koronavilkku. Valtion puolelta toivotaan, että jopa miljoona suomalaista lataisi sen jo syyskuun aikana. Ideahan on sinänsä hieno. Sen tyylilaji on ”ammu ja unohda”. Lataat vain sovelluksen ja annat sille luvan tutkia samassa tilassa olevia vastaavia sovelluksia. Jos joku sitten saa tartunnan ja ilmoittaa sen sillä sovelluksella, tulee sinullekin hälytys, jos olet ollut sopivaan aikaan tarpeeksi kauan ja lähellä. Valtio tilasi sovelluksen kehittämisen Solitalta kilpailutuksen jälkeen. Hieman erikoinen on kuitenkin tämä polku, jota tähän asti on tultu. Keväällä hallitus ilmoitti, että kännykkäsovellus tulee syksyllä. Samoihin aikoihin uutisoitiin, että kyseessä on Ketju-niminen suomalaista työtä oleva sovellus, jonka toteuttavat Reaktor ja Futurice. Yhtiöt olivat kehittäneet sovellusta omilla rahoillaan jo ennakoiden tuleavn tilanteen. Nämä kaksi eivät lopulta sitten edes osallistuneet kilpailutukseen joidenkin teknologisten reunaehtojen vuoksi. Kelakin on mainittu tässä reunaehtojen yhteydessä.

Tässäkään ei vielä ole sinänsä mitään uutta, sillä julkiset hankinnat ja kilpailutukset saattavat päättyä aivan miten vaan riippumatta hyvästäkin tarkoituksesta. Eräs jo edesmennyt kollega kuvasi tätä efektiä sanomalla että ”*sitä saa mitä sattuu tulemaan*”. Mutta kun tutkii tätä jäljityssovelluksen toimintaa, käy ilmi, että se varsinainen työhän on tehty jo aiemmin Googlen ja Applen toimesta. Hieman pelkistäen voidaan siis sanoa, että nyt vaan räätälöidään kansallisia käyttöliittymiä laitteissa jo olemassa oleviin rajapintoihin.

Tämän tietäen, aika kallista käyttöliittymää suomessa toteutetaan. Jotenkin olisi tuntunut hyvältä idealta, jos EU olisi pystynyt tämän toteuttamaan yhdessä. Sovelluksessa on merkittävä osuus juuri tietosuojan säilyttämisellä ja meillä kun olisi jo valmiina EU-tasoinen tietosuoja-asetuskin. Mutta eipäs nyt kuitenkaan tuomita sovellusta, kun ei ole vielä sitä nähtykään. Kolmella miljoonalla saa varmasti hienon ja toimivan käyttöliittymän.

Tuossa Googlen ja Applen yhteistyönä toteuttamassa projektissa on jotenkin tälle poikkeukselliselle ajalle ominainen yhteishengen tuoksu. Että nämä pahimmat kilpakumppanit siis pystyivät jo huhtikuussa julkaisemaan tämän ”*conventional contact tracing*” yhteistyön, joka tuottaa bluetoothia hyödyntäen rajapinnat älylaitteisiin hallitusten ja terveydenhuollon korona-jäljitystarpeisiin. Huawein puhelimiin toteutus ei vielä yllä, mutta politiikalla tuskin on mitään tekemistä tässä asiassa. Taitaakin olla niin että siinä tuoksussa on kyse vain erittäin tarkasti suunnatusta bisneksestä, jossa Android ja iOS käyttöjärjestelmien yhteistyöllä iskетään kiinalaisia kilpailijoita molemmille puolille maskia, eli korville.

Tuossa huhtikuussa ilmestyneessä teknisessä selosteessa, jossa Google ja Apple tätä toteutusta kuvaavat, käytetään esimerkkihenkilöinä Alicea ja Bobia. Tämähän ei ole mikään sattuma, sillä Alice ja Bob ovat jo ikään kuin esimerkkiveteraaneja. Näitä söpöläisiä on käytetty mm. tietoturvan, kryptologian, fysiikan ja monissa muissakin tieteellisissä julkaisuissa. En tunne tarkkaan heidän syntyhistoriaansa mutta ilmeisesti esimerkkinä aikaisemmin käytetyt A, B ja C olivat amerikkalaisille liian tylsiä. Keskittyminen hajosi ja vastavetona piti alkaa piirtämään esimerkit, sillä visuaalisuus toimii aina. C:nä on käytetty ainakin Chuckia, Charlesia ja Carolia mutta he eivät ole näissä piireissä yhtä kuuluisia kuin Alice ja Bob. Ehkä se sitten taas johtuukin siitä, että jos esimerkki on piirrettävä, että sen ymmärtäisi, pitäisi Charlien osallistumisen perusteena olla myös kyky laskea kolmeen asti.

Meillä, jotka teemme työtämme tekniikan ympärillä ja sen avulla, ei ole tapana ihan ensimmäisenä ryntäillä salaliittoteorioiden etulinjassa. Jostain näitä tyyppejä kuitenkin sikiää ja tällainen poikkeusaika tietenkin heittää bensaa liekkeihin. Aikaisemmin koronaviruksesta on syytetty USA:n ja Kiinan laboratoroita, 5G-verkkoja ja myös Bill Gatesia. Bill sai syyt niskoilleen, kun oli jo ennen korona-aikaa vaatinut presidentti Trumpia panostamaan juuri pandemioiden torjuntaan ja nyt hän kuulemma tekee sitten miljardeja rahoittaessaan rokotetutkimuksia. Henkilökohtaisesti olen hänelle edelleen katkera Windows 95-julkaisusta, mutta mies laittaa nykyään niin paljon rahaa kehittymättömien alueiden tukemiseen, että pystyn lähes antamaan anteeksi. Ainakin lupaan harkita sitä. Uusin virallinen ja faktantarkistuksen läpi käynyt syy koronaviruksen syntymiselle on sitten taas nähnyt päivänvalon. Pahiten viruksesta kärsineet alueet sijaitsevat teorian mukaan juuri leveysasteella 40. Kuten Kiinan Wuhan, Ranska, Italia, Iran Japani, Seattle ja New York. Hieno teoria mutta vesittyy jonkin verran, kun ihan karttaa tarkastelemalla havaitaan mm. että Ruotsi, Brasilia ja Meksiko eivät osu mainittuun alueeseen.

En tiedä kuvittelenko vain, mutta olisiko niin että epävarmoina aikoina myös korruptio kukoistaa. Tai miten sen nyt määrittelee, että mikä on korruptiota ja mikä vain suhteiden ja vallan hyväksi käyttöä. Suosikkipöljäkkeeni Trumpilla on mennyt taas jotain soraa snorkkeliinsa, sillä hän oli mennyt valittelemaan, että hiusten pesu on vaikeaa, kun vesijohtoverkon paine ei riitä. Tässä on hieman totuuttakin lipsahtanut mukaan, sillä USA:ssa on itse asiassa säädös vuodelta 1992 jolla veden painetta suihkussa rajoitetaan. Tähän Donald nyt haluaisi muutoksen, sillä omien sanojensa mukaan ”*Hiusteni tulee olla täydelliset*”. Nyt sitten kaikista ympäristöpaineista huolimatta USA:n energiavirasto esittää veden paineen kasvattamista. Hiukan huolestuttavaa jos tuollainen muutos Amerikoissa todella syntyy tällaisen keskustelun ja noin vähien hiusten pohjalta. Aikamoista menoa. Onhan noita vahvoja johtajia toki meilläkin Suomessa ollut. Johtajia, jotka ovat ohjanneet yhteiskuntaa rautaisella otteella, kuten nyt vaikka Kekkonen, mutta eivät nuo ole muistaakseni paljon hiustensa pesusta valitelleet.

Koronan aiheuttamat matkustuskiellot ja lentoliikenteen pysäyttäminen ajoi suomalaiset tunnetuin seurauksin metsään. Kansallis- ja luonnonpuistot ja kaikki retkeilykohteet ruuhkautuivat ennen näkemättömällä tavalla. Pienellä Karhunkierroksella Myllykosken riippusillalla on kuulemma ollut porukkaa kuin Ilveksen maalilla. Retkeily, patikointi, vaeltaminen, jne. ovat upea harrastus mutta sinnekin on teknologia tullut kaveriksi. Itsekin käytän Polarin ranneketta, josta saa hyvää informaatiota siitä, kuinka setämiehen patikointi on sujunut. Eräs johtava aktiivirannekkeiden, urheilu- ja älykellojen valmistaja koki tämän kesän kuitenkin hieman mollivoittoisena. Garmin joutui kyberhyökkäyksen kohteeksi ja väitetään että kyseessä oli ransomware eli kiristysohjelma. Hevosmiesten tietotoimiston mukaan yhtiö maksoi mehevät lunnaat, että sai liiketoimintansa palautettua ennalleen. Tarina ei kerro kuinka paljon kilpailijat ottivat tässä yhteydessä haltuun heidän markkinoistaan. Paikka- ja henkilötietoa käsittelevät sovellukset ovat varmuudella haluttuja kohteita niin valtiollisille tahoille kuin tavallisillekin roistoille. Toivoa sopii, että siinä Koronavilkussa säilyy yksityisyyden suoja, sillä se on sen käytölle ja sitä kautta koko yhteiskunnalle sen toiminnan edellytys.

Ja vielä lopuksi, pidetään kädet puhtaina ja turvavälit kunnossa. Kyllä se siitä.

Henkilöasiat:

Viestimies lehti ei julkaise jatkossa puolustusvoimien henkilökunnan siirtoja ja tehtävään määräämisiä henkilösuojalain rajoitusten vuoksi.

Ylennykset 4.6.2020

Everstiksi

- everstiluutnantti **Mika Seppä**
- everstiluutnantti **Jari Seppälä**

Everstiluutnantiksi

- majuri **Jarno Tyyskä**

Majuriksi

- kapteeni **Jussi Eronen**

Eversti Pentti Myyryläinen

Viestitarkastajan tervehdys

Viestialan kehitysilmiöitä tarkkailtaessa todetaan, että elektroniikka on kehittynyt edelleenkin voimakkaasti aiheuttaen muutoksia viesti- ja sähköteknillisiin järjestelmiin sekä parannuksia kalustoon. Viime vuosien kuvaan kuuluvat tyypillisinä kanavamäärien ja tehojen kasvu, laitteiden koon pienentyminen, datasiirron alkaminen sekä laitejärjestelmien ja sähköisten laskimien käyttöönotto. Elektronisen puolustuksen toimiala on suuresti laajentunut ja sen merkitys lisääntynyt.

Meidän sotilasviestitoimintamme muutosnopeus on ollut verkkaista, mutta sen kehittämistarve ei ole lakannut. Viestitoiminnan merkitys kasvaa sitä mukaa kuin joukkojen liikkuvuutta ja hajauttamista lisätään. Tutka-alan osuus koko puolustuskoneistossa voimistuu jatkuvasti.

Viestialan kehittämistoimenpiteillä on nähtävissä neljä päätavoitetta. Ensinnäkin viestiverkon aikaansaaminen nopeammin kuin ennen. Tähän pääsemiseksi löytyy monia keinoja, joista muutamia mainittakoon: Pystytettävät ja siirryttäessä purettavat viestiasemat korvataan kiinteästi ajoneuvoihin asennetuilla. Määrätilanteessa luovutaan kokonaan kaapeliyhteyksien hitaasta rakentamisesta ja jättäydytään radioyhteyksien varaan. Sanomaviestitytystä kehitetään siten, että joukot käyttävät radiokaukokirjoittimia automaattisin salaamislaittein. Automatisoituja viestivälineitä otetaan sotilaskäyttöön nykyistä enemmän.

Toinen tavoite sisältää sen, että viestiyhteyksien rungon on säilyttävä, vaikka vastustaja käyttäisi massatuhoaseitakin. Tässä tarkoituksessa kantaviestiverkon monitahoisia varmistustoimenpiteitä on syytä jatkaa samalla kun varaudutaan verkon täydentämiseen kenttäradiolaitteilla. Viimeksi mainittujen sotilaallinen käyttö suunnitellaan niin, että suuntaradioyhteydet ulottuvat ylimmistä johtoportaista prikaateihin saakka.

Kolmantena tavoitteena on pyrkimys kaluston standardisointiin koko puolustuslaitoksessa. Kun oman teollisuutemme osuus kalustotoimituksissa on ollut rajoitettua ja hankintojen toteuttaminen on ollut useiden viranomaisten tehtävänä, on syntynyt viesti- ja sähköteknillisessä varustuksessamme valitettava tyyppikirjavuus, josta aiheutuu vaikeuksia varsinkin kriisiaikoina. Järkevämpää on sellainen menettely, jossa samaa perusratkaisua sovelletaan useammille puolustushaaroille, aselajeille ja johtoportaille pitämällä erikoisvaatimukset kohtuullisissa rajoissa.

Neljäntenä on kotimaisen tutkimus-, kehittämis- ja tuotantotoiminnan kasvattaminen. Elektroniikkateollisuutemme on ilahduttavassa nousussa, mikä merkitsee samalla maanpuolustusvalmiuden lisääntymistä. Meillä on hyvin koulutettua työvoimaa ja tuontikomponenttien edustamasta haitasta huolimatta edullinen lähtöasema tälle teollisuudelle, jota puolustusvälineiden tilauksin pitäisi työllistää. Välineistön ja menetelmien kehittämisessä ei haluta jättäytyä vieraan varaan. Puolustuslaitos odottaakin vain tilaisuutta antaakseen useita kehittämistehtäviä omille tutkimus- ja tuotantolaitoksillemme.

Näiden päätavoitteiden saavuttamisessa viestiupseeristolla on runsaasti tehtävää. Voimakas ja aktiivinen Viestiupseeriyhdistys parantaa sotilaiden ja siviilien yhteistyön mahdollisuuksia ja siten auttaa saavuttamaan tuloksia sotilaallisen viestitoiminnan kehittämisessä. Kiitollisin mielin totean, että Viestiupseeriyhdistys ry on täyttänyt tehtävänsä. Toivon, että yhdistyksen myönteinen vaikutus säilyy.

Onnea 25 -vuotiaalle Viestiupseeriyhdistykselle!

Artikkelin kirjoittaja Veli-Matti Pesola

Vuoden Viestiupseeri 2020 - Raija Pihlainen

Vuoden 2020 viestiupseeriksi on valittu Puolustusvoimien johisjärjestelmäkeskuksessa hankintapäällikkönä työskentelevä KTM Raija Pihlainen. Raija on valmistunut Jyväskylän kauppaoppilaitoksesta vuonna 1984 ja Jyväskylän yliopistosta kauppatieteiden maisteriksi (ekonomiksi) vuonna 1989. Jo ennen opiskeluja ja niiden aikana hän työskenteli liike-elämän palveluksessa kaupan alalla, posti- ja pankkipalveluissa sekä tilitoimistossa eri tehtävissä.

Raija oli valmistumassa Jyväskylän yliopistosta, kun Ilmavoimien esikunta rekrytoi kaupallista sihteeriä Kaukovalvontatutka -projektiin. Hän haki kyseistä tehtävää ja tuli siihen valituksi – tästä alkoi Raijan työura Puolustusvoimissa. Raija on työskennellyt koko uransa ajan hankinnan tehtävissä ja tehnyt pääsääntöisesti johtamisjärjestelmäalan hankintoja koko tämän ajan. Lisäksi Raija on ollut mukana eri projekteissa, joissa hän on ollut kehittämässä muun muassa tietojärjestelmiä ja toiminut myös muutaman järjestelmän pääkäyttäjänä. Ilmavoimissa hän työskenteli lähes 18 vuotta.

Vuonna 2007 perustettiin Puolustusvoimien johtamisjärjestelmäkeskus, johon Raija hakeutui hankintapäällikön virkaan ja hän aloitti tässä tehtävässä uudessa organisaatiossa kyseisen vuoden alusta. Hankintapäällikkönä hän toimii edelleen, joskin tehtävät ovat puolustusvoimauudistuksen ja Suomen Turvallisuusverkko Oy:lle tapahtuneen liikkeenluovutuksen jälkeen muuttuneet sisällöltään erilaisiksi. Aikaisemmin Raijan johtamalla sektorilla oli vastuulla pelkästään hankinnat, mutta nykyisin tehtäväkenttään kuuluvat hankintojen lisäksi myös talousasiat sekä tietyt sovellusvastuu -tehtävät.

Raija on viihtynyt Puolustusvoimissa erinomaisesti. Isänmaallisena ihmisenä työpaikan maanpuolustuksellisella statuksella on hänelle suuri merkitys. Hän on kokenut, että työnantajana Puolustusvoimat arvostaa työntekijöidensä osaamista ja tehtävässä on voinut kasvaa ajan myötä. Matkan varrella myöskin tehtäväkuvaa on laajennettu vastaamaan osaamista. Työ on ollut lisäksi sopivan haasteellista ja monipuolista. Vuosien varrella on tullut eteen paljon erilaisia projekteja, joista Raija mainitsee muun muassa PVSAP-projektin, jossa hän oli mukana

aivan sen alku metreistä käyttöönottoon asti. TUVE-projekti oli työmäärältään massiivinen ja vaati siksi paljon, kuten myös Suomen Turvallisuusverkko Oy:lle tehty liikkeenluovutus, mikä ajoittui osin päällekkäin puolustusvoimauudistuksen kanssa tehden kokonaisuudesta siinäkin suhteessa haastavan.

Raija toteaa, että työtehtävät tulevat eteen sellaisina kuin ovat ja työt pitää hoitaa samalla tavalla olivatpa ne enemmän tai vähemmän mieluisia. Parhaimpina Raija kokee sellaiset tehtävät, joista voi antaa kiitosta toisille yhteisen tuloksen aikaansaamisesta. Nykyisen työn tekee mielekkääksi myös siihen liittyvä vuorovaikutus ja yhteistyö oman organisaation, kaikkien joukko-osastojen/vastaavien sekä ulkoisten toimijoiden kanssa. Samalla on muodostunut tukiverkko, jonka avulla löytyy vastaus lähes ”kaikkeen”.

Jokaisesta työuran varrelle osuneesta työpaikasta on jäänyt paljon hyviä muistoja, ihmissuhteita ja ”eväitä” tulevaisuuteen. Etenkin Puolustusvoimista muistoja on niin paljon, että on vaikeaa nimetä yhtä yksittäistä asiaa ylitse muiden. Raija on työskennellyt Puolustusvoimissa yli 30 vuotta, joten hän on vuosien saatossa nähnyt monta muutosta. Hän tuli PV:n palvelukseen aikakautena, jolloin käytössä olivat kaukokirjoittimet ja telexit ja konekirjoittajat kirjoittivat puhtaaksi käsin kirjoitetut asiakirjojen luonnokset. Aloittaessaan työuraansa Puolustusvoimissa Raija sai kuitenkin toisen henkilön kanssa yhteisen tietokoneen, koska hän oli suorittanut myös tietotekniikan opintoja ja oli kirjoittanut gradunsa Tekoplus -tekstinkäsittelyohjelmalla. Jo tuohon aikaan Raija kirjoittikin kaikki asiakirjansa itse tietokoneella. Tietotekniikka sekä tietoliikenne ovat monessa suhteessa muuttuneet paljon kolmessa vuosikymmenessä – nykypäivänä kehitetään robotiikkaa ja tekoälyä. Raijan mielestä varuskuntien yhteisöllisyys on myös vuosikymmenten aikana muuttunut huomattavasti. Aikoinaan varuskunnissa ja joukko-osastoissa/vastaavissa järjestettiin paljon vapaa-ajan toimintaa ja hauskanpitoa kuten tanssiaisia, laskiaismäen laskua ym. Nyt lähes kaikki PV:n työntekijät asuvat varuskuntien ulkopuolella eikä tuosta yhteisöllisyydestä ole kovin paljoa jäljellä.

Raija on kotoisin Uuraisilta, jossa hän asuu myös nykyisin miehensä kanssa. Perheeseen kuuluvat lisäksi omassa taloudessa asuva poika sekä pojanpoika. Harrastuksista Raija mainitsee päivittäisen liikunnan, josta pitää huolen suomenpystykorva. Koiralenkkien lisäksi hän käy kuntosalilla ja uimassa. Yhdistystoiminta ”kotien ja perheiden hyväksi” muun muassa Martoissa ja Mannerheimin lastensuojeluliitossa on myös lähellä Raijan sydäntä. Raija harrastaa lisäksi lukemista, käsitöitä ja kulttuurinautintoja eri muodoissa.

Raija toteaa, että ei aluksi ollut uskoa korviaan kuultuaan huomionosoituksesta. ”Olin siitä yllättynyt ja tietenkin hyvin otettu. Olen hyvin kiitollinen valinnasta, sillä siviilinä ja naisena en osannut tällaisen tulevan kohdalleni, kun ottaa huomioon, että ikäluokkani naisilla ei aikoinaan ollut mahdollisuutta valita sotilasuraa”. Valintaa juhlistettiin perhepiirissä nostamalla maljat ja syömällä ”juhlalounas”.

Viestimieslehden toimitus onnittelee Raijaa valinnasta vuoden 2020 viestiupseeriksi!


KIIHDYTÄ
5G
-NOPEUTEEN
JOYLI
35 PAIKKAKUNNALLA
KYSY LISÄÄ TAI OSTA:
Soita 0800 939393
Käy Elisan myymälässä
Klikkaa elisa.fi/5G
elisa 5G

Yhteydet maastoon Nestorin tuotteilla

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

nestor cables

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

Mittarikuja 5,
90620 Oulu
PL 276, 90101 Oulu