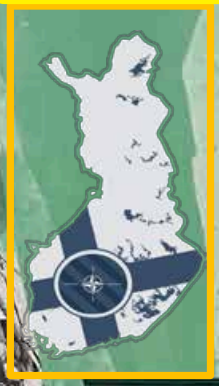
Viestimies

Viestiupseeriyhdistyksen julkaisu 78. vsk Numero 3 Syksy 2023



www.viestiupseeriyhdistys.fi

www.combitech.fi

Viestimies-lehti

Päätoimittaja
Pasi Puhakka
p 050 5290003
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Hanna Liitola
p 040 5930675
henkilotoimittaja@viestiupseeriyhdistys.fi

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

Toimituskunta
Vähätiitto Jarmo (pj)
Blomqvist Reima
Holma Harri
Hyvärinen Pertti
Isomäki Pekka
Mikkonen Mauri
Nyqvist Antti
Suokko Harri
Tunkkari Antti
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. 050 59 22722
juha.halminen@mediaosasto.fi

Painopaikka
Newprint Oy, Raisio
p 010 231 2600

ISSN 0357-2153

Kansikuva.

Tässä numerossa

Seuraavan numeron aineistopäivä on 17.10.2023. Lehti ilmestyy viikolla 49.

Loppuvuoteen Naton ensiaskelia ottaen ja uusia teknologioita tutkaillen

“DIANA Vision”

“Emerging and disruptive technologies present opportunities and threats - the NATO Alliance will continue to adapt to keep pace. Our Defence Innovation Accelerator for the North Atlantic seeks to unite the best and brightest innovators across the Alliance to ensure that we protect our one billion citizens.

DIANA provides deep tech and dual-use innovators with access to NATO resources including grant funding, acceleration services, and pathways to adapt their solutions for defence and security needs.”

Yllä kirjoitettu on suora lainaus Defence Innovation Accelerator for the North Atlantic (DIANA) sivustolta -

Vuosi on kääntynyt vääjäämättä jälkimmäiselle puoliskolleen ja Suomi sekä suomalaiset palanneet kesälomiltaan tuottamaan yhteistä hyvää yhteiskunnalle, yhteisöille ja yksilöille. Kesäkausi on perinteisesti uutismedioille hiljaiseloa ja uutisten kaivelua sieltä mistä jutun juurta sattuu löytymään. Uutisointi Suomen Natoon liittymisen jälkeen on myös ollut laantuvalla käyrällä hetkittäistä Vilnan kokouksen uutisointia lukuun ottamatta. Viesti ”Yhtä jalkaa” Ruotsin kanssa on muuttanut muotonsa, mutta strategisen viestinnän perusajatus tukee yhä vahvasti narratiivia Naton pohjoisen ulottuvuuden yhtenäisyydestä. Valoa tunnelin päähän ruotsalaisten näkökulmasta toi Vilnan kokouksesta uutisoitu Turkin myönteinen suhtautuminen Ruotsin liittymiseen. Mitä sitten ikinä tarkoittaakaan Erdoganin ”mahdollisimman pikainen ratifiointi”? Se selviää – jos ei tätä kirjoitettaessa – niin lähitulevaisuudessa. Valmistautukaamme toivottamaan Ruotsi ja ruotsalaiset Nato -perheeseen sekä samalla tiivistämään viesti- ja johtamisjärjestelmäkehitystä tulevan lähimmän kumppanimaan kanssa.

Muutama yksittäinen Nato -uutisointi nousi kesän aikana julkisuuteen koskien Suomen johtosuhdetta Naton komentorakenteessa. Lisäksi muutamassa uutisoinnissa raotettiin ovea ajatuksille Pohjoisen Euroopan komentorakenteen kehittämisestä. Suomen Nato -kumppanuus joka tapauksessa sai alkunsa johtosuhteen osalta Brunsumissa sijaitsevan esikunnan alaisuudessa. Pidemmällä tähtäimellä tarkasteltuna johtosuhteen muutokset ovat

vielä auki, sillä Naton komentorakenteen uudistamisen myötä uudet avaukset ovat mahdollisia. Vaikuttaa ainakin pohjoismaisten medioiden seurannan perusteella, että jonkinasteista keskustelua halutaan käydä mahdollisesta pohjoisen esikunnan perustamisesta. Tarkemmin sanottuna keskustelua uudelleenperustamisesta, sillä AFNORTH (Allied Forces Northern Europe) esikunta toimi vuosina 1952–1994 Norjan Kolsåsissa, kunnes johtovastuut siirtyivät Brunsumin alaisuuteen. Suomen tulee aktiivisesti vaikuttaa Nato -päämääriensä saavuttamiseksi organisaation sisältä käsin ja strategisen johdon toimesta kilpailtaessa Naton laitoksien, rakenteiden, suorituskykyjen, joukkojen ja tukeutumisen rakentumisesta parhaalla mahdollisella tavalla omalle ja lähialueellemme. Kyse on turvallisuuspoliittisesti ja kansantaloudellisesti merkittävistä asioista.

Kilpailtaessa resursseista ja täyttäessämme velvoitteitamme olemme varmasti jokainen kuulleet joskus mantraa hoettavan Naton rahoituksen järjestämisestä varaamalla 2% osuuden bruttokansantuotteesta puolustusmenoihin. Tämä hokema onkin sitten useimmiten se totuus ja koko totuus asiasta, joka julkisuudessa kerrotaan. Kehotan yleissivistämään Naton rahoitusmekanismista kiinnostuneita ja tiedonjanoisia lukemalla artikkelin Naton yhteisrahoituksen eduista ja haasteista. Samainen artikkeli johdattaa lukijan ymmärtämään Naton mukanaan tuomat mahdollisuudet uusien teknologioiden ja innovaatioiden kehittämiseksi (Diana).

Aasinsiltana Natojohdatuksesta nostan esille vähän julkisuutta saaneen nousevan teknologian. 5G teknologia on kuluttajalle tuttua kauraa vuosien takaa ja kiivaasti edetään kohti 6G-teknologoiden sisäänmarssia. Laitetoimittajat ja yhteenliittymät, kuten Nokia ja Next G Alliance ovat 6G-teknologioiden roadmapeissaan asettaneet tavoitteeksi teknologian käyttöönotolle 2030-luvun. Tavallisina teknologiakuluttajina olemme tottuneet tarkastelemaan mobiiliteknologiaa omasta perspektiivistämme, joka tavallisesti on enemmän tai vähemmän kahdessa avaruuden dimensiossa toimimista. Toisin sanoen siirrämme kuluttajabittivirtaamme maan pinnalta käsin tai hyvin rajoitetun korkeuden päässä Telluksen pinnasta.

Irtautuaksemme kuluttajanäkökulmasta viestimiehen ja -naisen on ajateltava boxin ulkopuolella olevia asioita. Mainitsemani nouseva teknologia on sanan varsinaisessa merkityksessä nouseva, sillä 5G NTN -teknologia ja siihen liittyvät suorituskyvyt tulevat kuluttaja- ja viranomaiskäyttöön nimenomaan tuosta kolmannesta dimensiosta. Sotilaallisessa viitekehyksessä puhumme avaruusdimension hyödyntämismahdollisuuksista sekä siitä, että 5G NTN voi tulevaisuudessa olla osa puolustusjärjestelmän johtamis- ja viestijärjestelmiä. Toinen syy miksi kyseessä on nouseva teknologia. Teknologiaan pohjautuvia kaupallisia ratkaisuja ei toistaiseksi ole saatavilla kuluttajakäyttöön. Läpimurtoa odotellessa kehotan jokaista viestimiestä ja -naista ottamaan teknologian seurantaan ja tutkimaan asiaa kykyjensä mukaan ollaksemme valmiita hyödyntämään teknologian, kun sovellutukset ovat riittävän kypsiä. Voihan olla, että 5G NTN -teknologia on yksi taistelukentän Game changereista tai multipliereista, kuka tietää. Tästä, ja muista nousevista teknologioista lisää lehden sivuilta.

Toivotan mukavaa syksyä ja antoisia lukuhetkiä.

Päätoimittaja

Pasi Puhakka

Digitalisoimme maailmaa

jossa panokset ovat korkeimmat, vaatimukset ovat kovimmat ja teknologia ratkaisee

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

Taistelukentän tietotekniikan numero 1

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

Ota yhteyttä saadaksesi lisätietoja mobiilituotteistamme, näytöistämme ja 19”/2 -laitteistamme.

+358 40 090 6100
salesfi@mildef.com www.mildef.com

mildef

TEKSTI: MARKO LÄHTEENMÄKI, KUVA: PUOLUSTUSVOIMAT

NATO – yhteisen rahoituksen edut ja haasteet

Suomesta tuli puolustusliitto Naton jäsen 4. huhtikuuta 2023. Millainen on muutos kumppanuuden ajan järjestelyistä täysjäsenyyden asettamiin vaatimuksiin. Ovatko jäsenyyden tuomat edut edelleen odotetun ja ajan mukaiset. Osalla jäsenmaista yhteisellä rahoituksella saavutetut edut ja niiden teknologinen muutospaine sekä jäsenmailta vaadittava lisäresurssointi voivat olla yhdenaikaista kehitystä hidastava. Naton yhteisillä ja innovatiivisilla aloitteilla voidaan luoda edellytyksiä ja mahdollisuuksia uudemman teknologian käyttöönotolle.

Uuden jäsenmaan asema ja yhteisiä muutospaineita

Suomen Nato-jäsenyyden keskeisin hyöty on liittokunnan muodostama pelote ja sen antama sotilaallinen turva. Pelotteen ja sotilaallisen turvan hyödyntäminen vaatii vastaavasi aktiivista osallistumista päätöksen tekoon. Aktiivinen Naton jäsen pystyy siten myös vaikuttamaan oman maansa puolustukseen ja edelleen liittokunnan yhteiseen ja jäsenmaiden kesken tehtäviin ratkaisuihin yhteisen edun tavoittelussa. Vaikutusmahdollisuudet ovat kuitenkin rajalliset ja niillä on tietyt reunaehdot. Suomen liittokunnan jäsenenä, huolimatta lähes kolmen vuosikymmenen mittaisesta Naton rauhankumppanuudesta, on monella tapaa omaksuttava uusia toimintatapoja ja yhteensovitettava nykyistä olemassa olevaa infrastruktuuria. Asetelman voisi kuvitella luovan hyvät lähtökohdat tulevaisuuteen katsovan teknologian käyttöönotolle ja parhaiden käytänteiden valjastamiselle organisaatiossa. Yhteisestä tavoitetilasta huolimatta ovat useat liittokunnan jäsenvaltiot eri vaiheessa uudemman teknologian valinnoissa tai haastavassa tilanteessa perinteisemmän teknologian päivittämisessä sekä elinkaaren hallinnassa.

Tämän vuosikymmenen aikana vanhentuva teknologia ja infrastruktuuri asettaa Naton ja liittokunnan jäsenvaltiot tilanteeseen, jossa joutuvat pohtimaan miten muutos toteutetaan paremman tietoturvan ja kybersietoisuuden sekä elinkaari kustannuksiltaan järkevästi hallittavilla ja uudemman teknologian mahdollistavilla järjestelmillä sekä toimintatavoilla. Naton tiedon hallintaa ohjaava toimisto Office of the Chief Information Officer (OCIO) sekä tietojärjestelmä ja palveluita ylläpitävä virasto NATO Communications and Information Agency (NCI Agency) ovat aloittaneet korvaavien ratkaisujen suunnittelun yhdessä Nato jäsenmaiden kanssa. Ratkaisut koskettavat ymmärrettävästi Naton rakenteessa olevia organisaation osia, johtoportaita ja joukkoja, mutta erityinen huomio on nousemassa liittokunnan jäsenten osuudesta. Tässä hetkessä vielä iso osa liityntä- ja tietojärjestelmäpalveluista kuuluvat katettavaksi yhteisen rahoituksen (common funding) periaatteiden mukaisesti.

NATO rahoituksen periaatteet

Naton rahoituksen resursointi on osoitettu suorasti ja osin epäsuorasti liittokunnan jäsenien vastuulle. Yhteisen rahoituksen osuus koostuu suoraan osallistumisesta kollektiiviseen budjetointiin, jolla katetaan liittouman yhteisiä kuluja. Kansallinen rahoitus on ymmärrettävästi laajin osa Naton epäsuoraa rahoitusta, joka muodostuu jokaisen maan omista tarpeista luoda uskottava puolustus ja täten myös olemaan osa Naton yhteistä pelotetta ja puolustusta sekä kykyä osallistua kriisinhallintaa ja sotilasoperaatioihin. Suoralla rahoituksella Naton budjetista ohjataan suorituskykyjen priorisointia ja toimintoja siten, että laajassa kokonaisuudessa ainakin liittokunnan yhteiset operaatiot, Naton ilmapuolustus sekä johtamisjärjestelmän toimivuus voidaan turvata. Bruttokansantuotteesta johdetun osuuden mukaisesti ohjataan kustannusten jakaantumista ja yhteisen rahoituksen jaetun taakaan kantoa. Suomen julkisen talouden suunnitelma (JTS 2024-2027) sisältää rahoitusta Natoon liittyviin suoriin kustannuksiin, tässä ovat mukana niin Naton yhteisrahoitusosuus (jäsenmaksu), henkilöstötarpeisiin kohdennettava lisärahoitus ja jäsenyyden edellyttämä johtamisjärjestelmien kehittämiseen varattua lisäpanostusta.

Naton yhteisen rahoituksen osuus jakautuu edelleen kolmeen osa-alueeseen: Naton päämajan toimintoihin liittyvä rahoitus (civil budjet), Naton komentorakenteen rahoitus (military budjet) ja sotilaallisen infrastruktuurin sekä suorituskykyjen toiminnallisuuteen liittyvä turvallisuusinvestointiohjelma (Nato Security Investment Programme, NSIP). Yhteisen rahoituksen osuudelle on vahva hallinnollinen ohjaava mekanismi eli liittolaisten kollektiivinen päätös. Ylintä päätöksen tekoa edustaa ja NATO budjetin hyväksyy poliittisella tasolla North Atlantic Council (NAC), jolle raportoinnista vastaavat resurssi ja suunnittelu johtokunta Resource Policy and Planning Board, (RPPB), määrärahaa seuraava toimikunta Budget Committee (BC) ja

sijoitus investointia ohjaava toimikunta Investment Committee (IC). Myös Naton turvallisuusinvestointi ohjelman (NSIP) toimeenpanoa valvoo IC. Suurin osa johtamisen tuen järjestelmistä ovat NSIP ohjelmalla resursoitu ja näin myös IC:n päätökselle perustuvia.

Suomen täysjäsenyyteen liittyen oli oletusarvio, että yhteisellä rahoituksella ja niin sanotusti tervetuliaisiksi saadaan riittävän kattavasti ja suhteellisen nopeasti Naton tarjoamat järjestelmät ja palvelut käyttöön. Tulevaisuuden resurssihaasteet ennakoiden ja jäsenmaiden yhteiseksi ennakkopäätöksen pohjaksi IC -rahoituspäätös oli odotettua pienempi, toisaalta ei Natollakaan olisi ollut vielä valmista teknistä ratkaisua toteuttaa uuden infrastruktuurin mukainen kokonaisuus. Päätös luo paineita myös muille jäsenmaille. Suomelle tilanne antaa mahdollisuuden täysin uuden toteutukselle, ilman vanhentuvan järjestelmän korvaamista. Ensimmäisen vaiheen palveluiden käyttöönotto on käynnissä ja toteutunee Naton nykyisen palvelutarjonnan mukaisesti ja maltillisesti toteutettuna ostopalveluina. Kansallinen toteutustapa niin sanotuille federoituville palveluille on valmisteilla ja toteutuksessa huomioidaan paitsi Naton asettamat vaatimukset ja ohjaus liittokunnan jäsenille myös resurssien kohdentuminen laajemmin kahden ja monenvälisten toimijoiden kanssa omaksi kestäväksi ratkaisuksi. Tavoitteena kustannustehokkaampi ja kybersietoisempi johtamisjärjestelmäverkko sekä palvelurakenteiden elinkaarien hallinta.

Muut rahoitusmahdollisuudet ja innovatiiviset aloitteet

Yhteisiä rahoitusjärjestelyjä (Joint funding) on myös mahdollista luoda osallistuvien jäsenmaiden omasta ja yhteisestä aloitteesta. Rahoitusohjelmasta sovitaan siten, että itse Naton organisaatiolla on siihen riittävä näkyvyys sekä poliittinen valvonta. Yhteisiä rahoitusohjelmia hyödynnetään silloin kun haetaan usein myös pidempikestoisia edelleen kehitystyötä vaatia eritysaloitteita. Usein nämä ovat liittyneet hävittäjä- ja helikopterihankkeisiin, logistisen tukitoiminnan rakentamiseen sekä ilmapuolustuksen johtamisjärjestelmiin. Tällaisia ovat olleet muun muassa NATO Airborne Early Warning and Control (NAPMA), NH90 Helicopter (NAHEMA) ja Eurofighter 2000 and Tornado (NETMA) virastojen johtamat ohjelmat. Naton eri virastoissa myös koordinoidaan tutkimus- ja kehitystyötä, joista yksi erittäin merkittävä mekanismi on ollut standardointi. Standardointiin liittyy jäsenvaltiota velvoittava ratifiointiprosessi, mutta erityisesti standardien kehitysprosessi luo mahdollisuuden vaikuttaa vaatimuksiin ja siten edelleen edesauttaa ratifioinnin edellyttämää toimeenpanoa tai käyttöönottoa.

Viimeisimpiä yhteisen rahoituksen aloitteita on vuonna 2021 käynnistynyt Defence Innovation Accelerator for the North Atlantic (DIANA). Sitä seurasi vuotta myöhemmin perustettu Nato Innovation Fund (NIF), jonka kautta investointirahoitusta on ollut mahdollista hakea tämä vuoden alusta. Toimintamalli on osa NATO 2030 ohjelmaa. Nato innovaatiot kohdentuvat tällä hetkellä yhdeksään teknologiseen alueeseen (artificial intelligence (AI), autonomy, quantum, biotechnologies and human enhancement, hypersonic systems, space, novel materials and manufacturing, energy and propulsion, next-generation communications networks). Vuoden 2021 Naton puolustusministeritapaaminen vahvisti nämä yhdeksän aluetta ajatuksella edistää ja turvata (Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies (EDT)) nousevien teknologioiden yhtenäisempi kehitys ja käyttöönotto, joita esimerkiksi on ensisijaisesti suunnattu kaupalliseen käyttöön, mutta voidaan nähdä hyvin soveltuvan puolustus- ja turvallisuusalan käyttöön (dual-use). Naton EDT strategiaa ja pyrkimyksiä on mahdollista seurata vuosittain julkaistavissa raporteissa (The NATO Advisory Group on Emerging and Disruptive Technologies Annual Report). Perinteisemmästä tiede- ja tutkimustyöstä ei Natossa (NATO Science and Technology Organization) ole luovuttu, mutta tämän rinnalla uusille teknologioille mahdollistettu malli, mukaan lukien rahoitus kannattaa taitavasti hyödyntää ja yhdistää kansallisen puolustuksen kehitykseen osana liittokuntaa.

Lopuksi

Toki jäsenyys ja sen tuomat edut ovat laajemmin ymmärrettävä kokonaisuus kuin Naton tarjoamat yhteisellä rahoituksella tarjotut johtamisjärjestelmä ratkaisut. Muuttuvassa turvallisuustilanteessa Nato edelleen tulee huolehtimaan, että riittävä muutosnopeus ja laadukkaasti hoidettu Naton yhteinen tilannekuva, päätöksen teko ja toimeenpano eivät vaarannu. Nato vastaa siitä, että liittokunnan jäsenmaat ovat riittävällä tasolla kyetty liittämään yhteiseen ja korkeasti turvattuun sekä varmennettuihin johtamisen ja tiedonvaihdon järjestelmiin. Jäsenmaat itse vastaavat siitä, että Natolle liittoutumisvelvoitteen mukaiset suorituskyvyt ovat rakentumassa ja käyttöönotetut sovitun aikataulun mukaisesti.

Marko Höyhtyä työskentelee tutkimusprofessorina Teknologian Tutkimuskeskus VTT:llä ja hänellä on dosentuuri niin Maanpuolustuskorkeakoulussa kuin Oulun yliopistossa.

Heikki Rantanen työskentelee erikoistutkijana Puolustusvoimien Tutkimuslaitoksella tutkimusalueena myös 5G/6G-verkot.

TEKSTI: MARKO HÖYHTYÄ JA HEIKKI RANTANEN

5G NTN – uusi merkittävä suorituskyky sotilasviestintäverkkoihin?

Aamulehden uutisen 27.6.2018 mukaan Tampereelta soitettiin maailman ensimmäinen puhelu 5G-verkon välityksellä Tallinnaan. Soittajana oli Suomen liikenne- ja viestintäministeri Anne Berner ja soiton vastaanottajana oli Viron kollega. Tämän jälkeen verkko on laajentunut merkittävästi ja tällä hetkellä yksi suomalaisista matkapuhelinoperaattoreista on kertonut, että jopa liki 90 % heidän asiakkaistaan tavoittaa paremman palvelunlaadun 5G-verkon asuinpaikkakunnan perusteella. Uutta suorituskykyä on tulossa jo muutamien vuosien päästä 5G:n kehityspolun kautta. Tätä tarjoaa 5G:n satelliittilaajennus eli 5G NTN (Non-Terrestrial Networking), joka mahdollistaa jopa lähes 100 % maailmanlaajuisen peittoalueen. Järjestelmänä 5G NTN, jonka yllättävän harva tänä päivänä tunnistaa lyhenteenä, on herättänyt suurta sotilaallista mielenkiintoa. Tässä artikkelissa kerrotaan mikä on 5G NTN ja miksi se olisi syytä jatkossa integroida osaksi sotilaallisia viestintäverkkoja.

Sotilaallisten viestintäjärjestelmien haasteet

Selvänä trendinä taistelukentällä on yhä harvemmat, mutta entistä suorituskykyisemmät joukot, joiden vastuualueet ovat yhä suuremmat. Tiedustelun (esimerkiksi vastapuolen joukkojen paikantaminen) kautta syntyvä verkottunut tilannetietoisuus, lähes reaaliaikainen tiedonsiirto sekä tehokkaat ja tarkat kaukovaikuttamisen asejärjestelmät ovat nykyaikaisen taistelukentän avaintekijöitä. Koska taistelukenttä on entistä tyhjempi, myös tietoliikenneyhteydet muodostuvat entistä pidemmiksi, jolloin taistelukentästä muodostuu yhteyksien katkeamisen vuoksi helposti saarekkeinen. Yhteistoiminta eri joukkojen ja verkottuneiden asejärjestelmien kesken voi muodostua haastavaksi.

Taistelukentän yksi aivan keskeinen tekijä onkin resilientti tiedonsiirtojärjestelmä, joka yhdistää kaikki taistelukentän elementit. Joukot eivät koskaan saisi olla vain yhden yhteyden varassa, pitää olla varmistavia yhteyksiä, sotilaallisten tiedonsiirtojärjestelmien pitää automaattisesti toipua verkon solmujen menettämisestä (kuten taktiset verkot tekevätkin) ja niin edelleen. Maanpäälliset radioverkot ovat aina kantamarajoitteisia (viimeistään radiohorisontti katkaisee yhteyden) varsinkin jos antennia ei voida sijoittaa korkealle ja lisäksi maastoesteet, puusto jne. voivat voimakkaasti vaimentaa radiosignaalia. Resilientin sotilasviestijärjestelmän pitääkin olla yhdistelmä verkkoja, jotka toimivat maassa, ilmassa ja avaruudessa. Drone-tukiasemat, erilaiset satelliittiyhteydet ja jatkossa mitä todennäköisemmin myös 5G NTN ovat resilientin sotilasviestijärjestelmän osajärjestelmiä.

5G: Uudet suorituskyvyt

5G-verkoissa on aiempiin sukupolviin verrattuna useita uusia ominaisuuksia, joilla on käyttöä myös kriittisissä tietoliikennejärjestelmissä ja sotilaskommunikaatiossa. Standardia kehitetään 3GPP-organisaatiossa ja sen jäsenenä toimivat aktiivisesti sotilasratkaisuja kehittävät toimijat kuten Thales (etenkin NTN-puolella), ja ryhmittymät kuten NATOn Communications and Information (NCI) Agency. Näin vaikutetaan aktiivisesti siihen, että standardin kehityksessä huomioidaan myös sotilastoiminnan tarpeet.

5G kattaa kokonaisuudessaan kolme kriittistä sovellusaluetta, jotka on nimetty seuraavasti. Enhanced Mobile Broadband (eMBB) tarkoittaa laajakaistapalveluita ja suuria datanopeuksia eli 5G eMBB pystyy tukemaan Internet-yhteyksiä myös hankalissa ympäristöolosuhteissa. Kehittyneillä moniantenniteknologioilla (MIMO, Multiple Input Multiple Output) voidaan kapasiteettia kasvattaa vielä käyttämällä tilaa ja suunnattuja lähetyksiä hyödyksi – ja samalla tehdä vastapuolen häirintä ja tiedustelu haastavammaksi. Ultra Reliable Low Latency Communications (URLLC) kattaa erittäin matalaviiveiset palvelut kriittisissä toimintaympäristöissä kuten tehtaissa ja itseohjautuvassa liikenteessä. Massive Machine Type Communications (mMTC) on koneiden väliseen kommunikaatioon ja erilaisen sensoridatan siirtoon soveltuva energiatehokas teknologia. Tämän avulla voidaan kytkeä itseajavat ajoneuvot, ympäristöä ja laitteiden tilaa seuraavat sensorit, tehdaslaitteet ja niin edelleen laitteiden Internetiin (Internet of Things, IoT). 5G:n IoT-ratkaisut mah-

dollistavat niin pienen energian kulutuksen valvontaratkaisut ja reunalaskennan avulla tehtävät nopeat tunnistukset kuin myös multimedialähetyksen kuten videon striimauksen käyttämällä viimeisintä RedCap-teknologiaa (Reduced Capability). Tällä on käyttöä esimerkiksi rajavalvonnassa.

Mobiiliverkoissa on jo pidempään ollut käytössä tuki ns. missiokriittiseen kommunikaatioon (Mission Critical Communications). Käytössä on useita teknologioita priorisoimaan kriittistä dataliikennettä ja varmistamaan näin vaikkapa tilannetietojen ja komentojen ajantasainen toimitus ohi muiden palveluiden kuten viihdekäytön. 5G-verkoissa aiempiin sukupolviin verrattuna on tullut mukaan verkkoviipalointi ja sen avulla vielä kehittyneemmät palvelun laadun ominaisuudet. Verkko on ohjelmistopohjainen (Software-Defined Networking, SDN) ja sen toiminnat ovat virtualisoituja (Network Function Virtualization, NFV), mikä mahdollistaa aiempaa monipuolisemmat palvelut. Viipaloinnin avulla voidaan varata tietty osa verkon kapasiteetista kokonaan viranomaisviestinnän käyttöön, ja näin varmistaa näiden korkean prioriteetin käyttäjien tietoliikenteen matalaviiveisyys ja jatkuva toiminta. Tämä tekee 5G:stä varsin houkuttelevan sotilaskommunikaatioratkaisun. Ja asiaa helpottaa myös kattavat verkon peitot ja suuri määrä saatavilla olevia kohtuullisen hintaisia päätelaitteita.

Sotilastoiminnan kannalta hyvin kiinnostava on mahdollisuus suoraan yhteyteen päätelaitteiden välillä silloinkin, kun yhteyttä tukiasemaan ei ole. Tätä kutsutaan nimellä Sidelink. Edellä mainitun lisäksi kehitetään runkoverkon yhteyden ketjuttamista radioteitse usealle tukiasemalle eli IAB-teknologiaa (Integrated Access and Backbone). Tätä voidaan käyttää kommunikoitaessa millimetrialueen taajuuksilla kuten 26 GHz ja toteuttaa näin tilapäisiä yhteyksiä, joita on vaikeampi havaita signaalin nopean vaimenemisen takia.

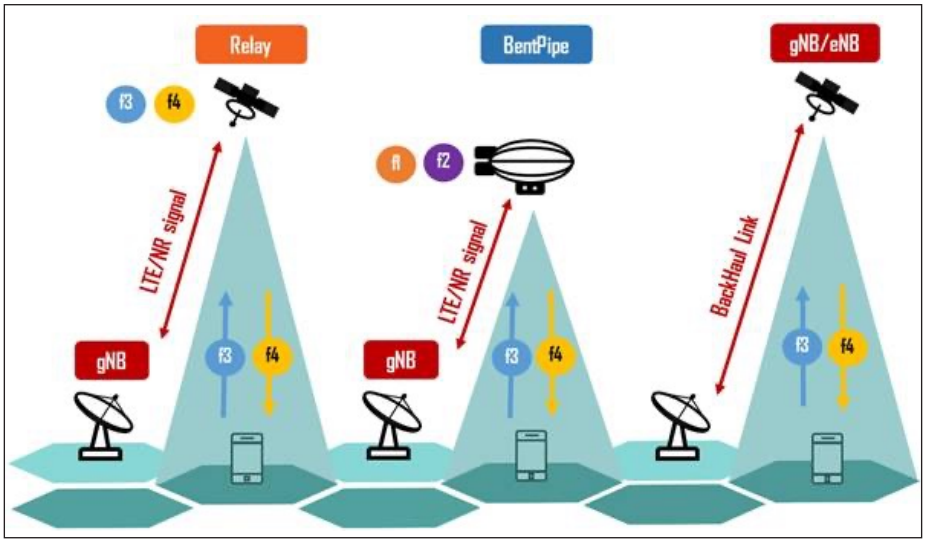
5G:n runkoverkko tai ydinverkko eli core mahdollistaa mainitut priorisoinnit ja viipaloinnit ja on koko verkkoinfrastruktuurin ydin. Sen runkoyhteydet yhdistävät eri valtiot, maanosat ja operaattoreiden verkot yhteen ja mahdollistavat näin liikkuvat palvelut. Se on useiden eri tietokoneiden joukko, joka voi olla pilvessä ja jolla toteutetaan kaikki viestintäpalvelut sekä varmistetaan tietoturvallinen toiminta. Paikallisissa verkoissa 5G Core on tukiaseman yhteydessä eli palvelut voidaan toteuttaa näin paikallisesti. Ohjelmistopohjaiset 5G-verkot käyttävät päästä-päähän orkestrointia, verkon toimintojen automatisointia ja automaattista jatkuvaa uhkien tunnistamista turvallisuuden parantamiseksi ja resurssien käytön tehokkuuden lisäämiseksi.

5G NTN – uutta merkittävää suorituskykyä

Perinteiset mobiiliverkot on suunniteltu ja optimoitu horisontaaliseen toimintaan. 5G:n evoluutiossa ja kohti 6G:tä mentäessä mukaan on tulossa vahvemmin myös vertikaalinen dimensio ja NTN-ratkaisut. Ukrainan sota on osoittanut, että avaruustoiminnalla on kriittinen merkitys paikannuksen lisäksi myös tiedustelussa, tilannekuvassa ja tiedonsiirrossa. Starlink on osoittanut matalan kiertoradan LEO-ratkaisujen (Low Earth Orbit) tuovan toimivat yhteydet niin siviileille kuin sotilaille silloinkin, kun maanpäällinen infra on tuhottu. Tämä vaatii erillisiä päätelaitteita, jotka vaikkakin ovat kohtalaisen pienikokoisia eivät silti sovellu kädessä pidettävään käyttöön.

5G NTN tekee mahdolliseksi sekä reitittää dataa tukiasemalta satelliitin kautta (backhaul) että myös suoran päätelaiteyhteyden käyttäjän päätelaitteeseen kuten älypuhelimeen, joka kulkee kätevästi taskussa mukana. Tämä voi olla käänteentekevä ratkaisu monissa viranomaiskäyttötapauksissa, tarjoten yhdessä sidelinkin kanssa yhteydet monissa muodoissaan etäisille alueille sekä ympäristöihin, joissa maanpäällinen infrastruktuuri on tuhoutunut. Kuluttajan kannalta siis päästään tilanteeseen, jossa voidaan käyttää aina mukana olevalla laitteella yhteys myös satelliitin kautta. Tämä tulee todennäköisesti olemaan pitkään niin sanottu varayhteys eli käytetään lähinnä silloin, kun maanpäällistä yhteyttä ei ole tarjolla.

Nyt kehitettävänä oleva 5G NTN-ratkaisu pohjautuu ns. bent pipe -arkkitehtuuriin eli satelliitti vastaanottaa maasta tulevan signaalin, vahvistaa sen ja lähettää kauempana maassa olevaan tukiasemaan, tukien niin 4G- kuin 5G-yhteyksiä. Tulevaisuudessa tavoitellaan tilannetta, jossa osa toiminnallisuuksista jaetaan satelliitin ja sen maassa olevan gatewayn kesken tai jopa kaikki 5G-tukiaseman toiminnot olisivat taivaalla ns. regeneratiivisessa satelliitissa. Tämä tarjoaisi paremman tuen viivesensitiivisille palveluille ja mahdollistaisi satelliittien välisen reitityksen. Regeneratiivinen satelliitti voi purkaa datan ja käyttää eri teknologiaa uudelleen lähetykseen. LEO-radat ovat juuri viivesyistä pääasiallinen koh-



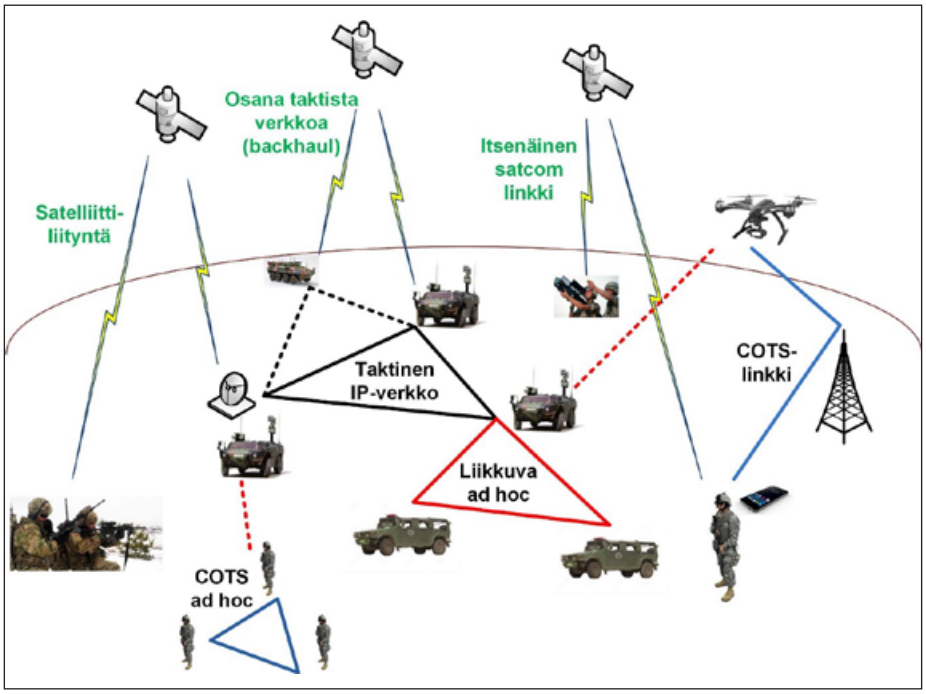
Kuva 1. NTN-ratkaisun toimintamallit. Kuvassa voi yhtä hyvin olla HAPS tai satelliitti.

de suorille 5G-yhteyksille eli satelliitti vaikkapa 600 km korkeudessa tarkoittaa vain muutamien millisekuntien etenemisviivettä, kun taas ylemmät GEO-radat vievät viiveen satojen millisekuntien luokkaan.

5G standardisointia tekevän 3GPP terminologiassa sana NTN kattaa myös ilmassa noin 20 km korkeudella lentävät alustat (High Altitude Pseudo Satellites, HAPS) ja alla olevassa kuvassa on kuvattuna eri toimintamallit. Oikealla on tilanne, jossa tukiasema on nostettu taivaalle (joko satelliittiin tai HAPS-alustaan). Keskellä on bentpipe-arkkitehtuuri, jossa uplink- ja downlink-taajuudet toimivat eri kaistoilla nykyisten järjestelmien kaltaisesti. Relay-vaihtoehdossa lisätään peittoa samaa taajuutta hyödyntäen eli voidaan vaikkapa viedä tukiaseman sijasta ilmassa oleva relay-asema peittoa halutulle alueelle tuomaan niin, että relay-asemasta on näköyhteys kaukana olevaan tukiasemaan.

Tällä hetkellä ei vielä ole olemassa kiertoradalla toimivaa standardiin perustuvaa 5G NTN-satelliittia. On kuitenkin testattu kaupasta ostetuilla päätelaitteilla jo onnistuneesti viestintää Lynk-järjestelmän satelliittien avulla, soitettu onnistuneesti puhelu kahden puhelimen välillä edistyneellä ASTSpaceMobilen LEO-satelliitilla, jossa on 64 neliömetrin antenni riittävän signaalitehon aikaan saamiseksi ja Nokiakin mukana kehitystyössä. Lisäksi valmistajat kuten Apple ja Huawei ovat lisänneet muutamaan puhelinmalliin jo hätäviestintäpalvelut olemassa olevien satelliittipalveluiden kuten Globalstar ja Beidou varaan.

Tällä hetkellä 3GPP:n ensimmäiset standardiversiot NTN:ää koskien ovat valmiina ja sen myötä esim. Ericsson on esitellyt Qualcommin kanssa toteutettua päätelaitetta. On odotettavissa, että jo parin vuoden sisään saadaan ensimmäisiä kaupallisia laitteita ja vuosikymmenen loppuun mennessä on kaupallisia palveluita myös satelliiteista tarjolla. On myös huomioitava, että nykyiset satelliittijärjestelmät rakennetaan jo ohjelmistopohjaisiksi eli niihin voidaan päivittää standardin mukaisia ominaisuuksia myös laukaisun jälkeen. Myös Starlink voi tulevaisuudessa päivittää kehittämäänsä proprietary-teknologiaa NTN:n suuntaan. Heillä on jo suuri toimiva järjestelmä ja teknologiassakin on paljon samoja piirteitä, kuten OFDM-kaltainen aaltomuoto



Kuva 2. Satelliitit osana taktista verkkoa. Satelliitti voi olla liityntä taktiseen verkkoon tai osa itse taktista runkoverkkoa.Tai sitä voidaan käyttää rinnalla itsenäisenä linkkinä.

(Orthogonal Frequency Division Multiplexing). Muita merkittäviä uusia toimijoita ovat esimerkiksi OneWeb ja Amazon omalla Kuiper-järjestelmällään.

Tällä hetkellä satelliittiviestintä kasvaa nopeasti liiketoimintana ja koko avaruusliiketoiminnan koko kasvanee 1000 miljardiin dollariin vuosittain 2040 mennessä. Tässä suurimpana ajurina ja mahdollisuutena ovat etenkin suorat yhteydet standardoituihin päätelaitteisiin sekä laajakaistapalvelut ja IoT-toiminta. Palveluita tulevat tarjoamaan niin perinteiset satelliittioperaattorit kuin nousevat uudet toimijat. Nykyisessä maailmantilanteessa myös geopolitiikalla on sanansa sanottavana ja esimerkiksi Euroopassa panostetaan oman IRIS2-järjestelmän kehitykseen. Siinä tavoitteena on monikerroksisella ratkaisulla (satelliitteja niin LEO kuin GEO-radoilla) ja 5G-verkkoon integroitumalla tarjota kriittisille eurooppalaisille toimijoilla luotettavat yhteydet niin kriisin kuin rauhan aikana.

5G NTN ja MIL-yhteisöt

NTN-ratkaisut ovat suuren mielenkiinnon kohteena eri sotilasyhteisöissä. Esittelemme tässä tiiviisti nykytilannetta NATOn toiminnan ja Euroopan puolustustutkimuksen näkökulmasta sekä tarkastelemme lyhyesti tilannetta niin USA:ssa kuin muualla maailmassa.

NATO: Perustetussa työryhmässä IST-187 työssä yhtenä alueena on Extreme long range coverage, joka kattaa niin satelliittien, HAPSien kuin matalammallakin lentävien dronejen käytön pitkän kantaman viestinnässä. Lisäksi NATO rahoittaa tutkimushankkeita, joissa perehdytään erityisesti 5G NTN:n tuomiin sotilaallisiin mahdollisuuksiin niin sotilaiden kuin koneiden näkökulmasta.

EDA (European Defence Agency) / EDF (European Defence Fund): Euroopan tutkimusstrategiassa puolustus ja avaruus nivoutuvat olennaisesti yhteen ja niinpä avaruuden sotilaallista käyttöä tutkitaan ja kehitetään sekä EDAn hankkeissa, että myös EDF:n puolella. Kohteina ovat muun muassa ajantasainen tilannekuva ja kaupallisen 5G:n käyttö osana taktista verkkoa. Esimerkiksi EDF:n 5G COMPAD (5G Communications for Peacekeeping and Defence) tutkimuksessa on mukana Suomesta Bittium sekä Nokia. Johtuen suuresta osallistujamäärästä ja mielenkiinnosta sitä kohtaan jo ennakkoon, 5G COMPAD:sta odotetaan muodostuvan yksi EDF:n kärkihankkeista.

USA ja muu maailma:

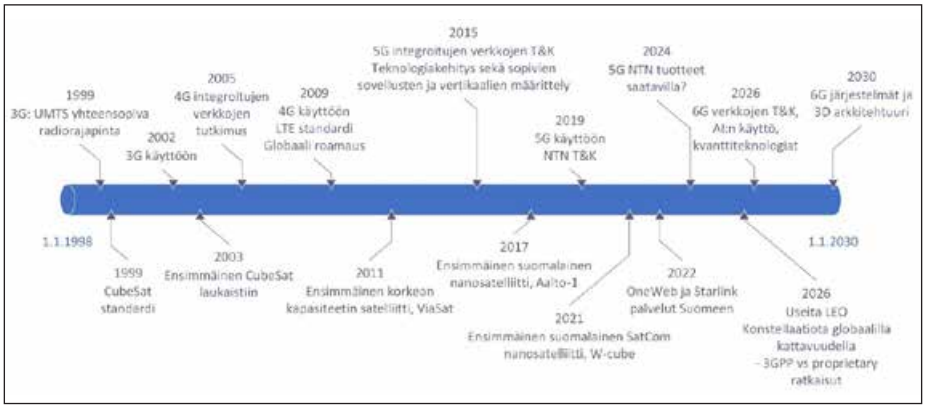
USA ei ole ollut merkittävä toimija 5G-markkinoilla ja niinpä se nyt panostaa 5G-standardin jatkokehitykseen lopullisena tavoitteena merkittävä rooli 6G-markkinoilla. USA:ssa on myös todella suuri mielenkiinto 5G-tekniikan käyttöön sotilaallisissa viestintäjärjestelmissä. Lockheed Martin on yhdessä Omnispacen kanssa tutkinut maailmanlaajuisen 5G-standardien mukaisen satelliittiverkon rakentamista palvelemaan niin kaupallisia kuin viranomaistoimijoita kaikkialla maailmassa.

Kiinassa GalaxySpace väittää rakentavansa 5G-standardeja mukailevan satelliittiverkon ja kilpailevansa jatkossa jopa SpaceX:n kanssa. On arveltu, että tämä verkko on suunnattu lähinnä ei-kiinalaisille tilaajille sekä Kiinan hallitukselle ja armeijalle – Kiinassa kun kansalaisille on tarjolla suuren nopeuden 5G verkko erinomaisella maanlaajuisella peitolla.

5G NTN osaksi PV tietoliikenneverkkoa?

Suomen toimintaympäristö on haastava ja elektroniikan on toimittava niin kovassa pakkasessa ja lumessa kuin etäisillä alueilla toimittaessa. 5G-teknologia ja NTN ovat lupaavia ratkaisuja moniin tilanteisiin, tarjoten myös kyvykkyyksiä massiiviseen tiedonsiirtoon ja monipuoliseen priorisointiin. Täydellistä maanpäällistä 5G-peittoa ei pystytä saavuttamaan ja maan päällä ollaan asemassa, jossa olosuhteet ovat haastavat ja häirintä ja tuhoaminen helpompaa. Sen sijaan NTN-ratkaisut voivat tarjota yhteydet mihin tahansa ja niiden tuhoaminen ja häirintä on vaikeampaa. Vaikkakin satelliitteja voidaan tuhota myös kiertoradalle, se on sekä kallista että voi aiheuttaa suuren määrän avaruusromua, joka vaarantaa myös tuhoajan omien satelliittien ja liittolaisten satelliittien toiminnan. Siksi tätä vältetään viimeiseen asti. Kuvassa 2 esitetään, kuinka satelliitit voidaan liittää taktiseen tiedonsiirtoverkkoon ja käytössä voi olla muitakin kaupallisia COTS-linkkejä.

Puolustusvoimat seuraa aktiivisesti mobiiliverkkojen kehittymistä mukaan lukien 5G NTN. Kenttäkokeissa on demonstroitu taktisilla 4/5G tukiasemilla (Tactical Bubble) saavutettavaa uutta



Kuva 3. Aikajana satelliittitietoliikennetoiminnan kehityksestä 1999–2030.

suorituskykyä. PVTUTKL osallistuu NATO IST-187 tutkimukseen, jonka vuoden 2024 loppuraportissa tullaan esittämään 5G mahdollistamat käyttöskenaariot huomioiden tieto- ja kyberturvallisuus sekä muut kaupallisten järjestelmien rajoitteet. Aikaisemmin mainittu 5G COMPAD tulee määrittelemään referenssiarkkitehtuurin, jossa 5G integroidaan osaksi taktisia verkkoja.

Matalan kiertoradan satelliitteja ammutaan tällä hetkellä taivaalle yli tuhannen satelliitin vuosivauhtia ja suunnitteilla on Starlinkin lisäksi useita satojen tai tuhansien satelliittien järjestelmiä. Esimerkiksi Kiina on esitellyt yli 12 000 satelliitin Guowang-suunnitelmaa. Satelliittien lukumäärän kasvaessa tarvitaan koko ajan kehittyneempää avaruusliikenteen hallintaa ja törmäyksien aktiivista välttämistä. Avaruuden ruuhkautuminen hankaloittaa uusien toimijoiden tulemista ja vaarantaa myös miehitettyjen lentojen turvallisuutta.

5G NTN on ominaisuuksineen hyvä tekninen lisä sotilastoimintaan. NTN tekee kokonaisjärjestelmästä resilientimmän sekä peittoalueeltaan kattavan ja siksi puolustusvoimat eri maissa ovat aktiivisesti mukana kehitys- ja tutkimustyössä

Yhteenveto

Avaruusjärjestelmät ovat pitkään olleet tärkeä osa sotilastoimintaa. Tulevaisuudessa niiden rooli voi kasvaa merkittävästi 5G NTN:n mahdollistamien suorien päätelaiteyhteyksien ja tuettavien palveluiden takia. 3GPP kehityspolun myötä 5G NTN on 10 vuoden päästä 6G NTN yhä kehittynein ominaisuuksin.

Kuvassa 3 on lyhyesti summeerattuna kehitys 90-luvun lopulta kohti vuotta 2030 sisältäen niin satelliittitoiminnan standardoinnin 3GPP:ssä kuin piensatelliittitoiminnan kehittymisen. Suomalaista VTT:n kehittämää radioteknologiaa lentää mm. W-Cube -nanosatelliitissa, jolla tutkitaan 75 GHz:n kaistan soveltuvuutta 6G-käyttöön.

Patria

Kun kaiken on pakko toimia.

Patria tarjoaa huippuluokan suorituskykyä

Patria on moderni ja kansainvälinen puolustus- ja teknologiayritys, jonka kokemus ulottuu yli 100 vuoden päähän. Järkevästi käytetyt resurssit, innovatiiviset ratkaisut ja älykkäät järjestelmät varmistavat, että voimme tarjota asiakkaillemme suorituskykyä, johon voi luottaa kaikissa olosuhteissa. Patrian tarjooma on NATO-yhteensopivaa.

Patrian laaja tarjooma on jaettu kolmeen päähaaraan, jotka ovat **Through Life Capability**, **Protected Mobility and Defence Systems** ja **Battlefield and Critical Systems**.

Toimimme asiakkaidemme kanssa yhteistyössä tuotteidemme koko elinkaaren ajan, jotta tuotteiden hyöty saadaan varmasti maksimoitua. Rakennamme kumppanuuksia, jotka toimivat myös kriittisissä olosuhteissa.

Niklas Collin *työskentelee Cinia Oy:n johtavana konsulttina ja Team Leadina. Hänellä on lähes kahden vuosikymmenen kokemus haastavista ohjelmistokehitysprojekteista. Erityisen kiinnostunut hän on siitä, miten ohjelmistot voivat tuoda käyttäjilleen arvoa kehitystyön alkumetreiltä alkaen.*

Tommi Harakkamäki *on työskennellyt asiantuntijana vaativissa sovelluskehityshankkeissa vuosituhannen alusta alkaen. Työssään Cinia Oy:n ratkaisuarkkitehtina hän etsii tehokkaimmat keinot siihen, miten vaativaan ammattikäyttöön tehtyjen ohjelmistojen kokonaisuuksista tehdään turvallisia, moderneja ja joustavia.*

TEKSTI: NIKLAS COLLIN, TOMMI HARAKKAMÄKI

Tekoälyn mahdollisuudet turvallisuuskriittisissä ympäristöissä

Ohjelmistokehityksen tuottavuudessa otetaan tällä hetkellä valtavia harppauksia uusien, älykkäiden teknologioiden ansiosta. Moni uusista työkaluista kytkeytyy julkipilvipalveluihin tai avoimen lähdekoodin hankkeisiin. Miten tekoälyn etuja voi tuoda myös suljettuihin, korkean turvatason ympäristöihin – tietoturvasta tinkimättä?

Artikkeli aloittaa sarjan, jossa tarkastellaan nousevien teknologioiden hyödyntämistä vaativissa, korkean turvatason IT-ympäristöissä. Tämä osa keskittyy ammattikäyttöön rakennettujen ohjelmistojen kehittämiseen. Sarjan seuraavissa osissa näkökulmina ovat tietoliikenteen turvaaminen sekä kyberturvallisuuden jatkuva valvonta.

Kielimallit, kuvantunnistustyökalut ja koneoppivat vahvistusalgoritmit: siinä muutama esimerkki nousevista teknologioista, joiden hyödyntäminen kiinnostaa järjestelmien kehityksen vastuuhenkilöitä tällä hetkellä organisaatiossa kuin organisaatiossa. Uusia teknologioita yhdistämällä ja ketjuttamalla markkinoille on tuotu työkaluja, joita arkisessa puheessa kutsutaan tekoälyksi.

Älyä ja tehoa voidaan tuoda vaativan ammattikäytön sovelluksiin monella tavalla, esimerkiksi matemaattisilla malleilla, jotka optimoivat resurssien tai välineistön käyttöä. Viime aikoina erityisen paljon pinnalla ovat olleet generatiiviset LLM-kielimallit (Large Language Model). Näistä ChatGPT lienee tunnetuin. Oheisessa taulukossa olemme listanneet käyttötapauksista muutamia esimerkkejä.

Opetatko tekoälymallia salaisuuksilla?

Tänä keväänä maailmalla uutisoitiin tapauksesta, jossa Samsungin työntekijät olivat epähuomiossa vuotaneet huippusalaisia tietoja ChatGPT:tä käyttäessään. Insinöörit syöttivät koodin lisäksi sovellukseen muun muassa laitteistoon liittyviä muistiinpanoja. Liikesalaisuudet päätyivät osaksi sitä aineistomassaa, josta työkalun muut käyttäjät louhivat vastauksia.

Uusimmissa päivityksissä ChatGPT on tuonut käyttäjille laajemmat mahdollisuudet vaikuttaa asetuksiin, mutta uusiin teknologioihin sisältyvät riskit pitää siitä huolimatta tiedostaa.

Sopivan työkalun valinnassa saa olla tarkkana. Salaisen datan vuotaminen on ilmeinen tietoturvariski, mutta tuo riski on mahdollista eliminoida vertailemalla samaan tarkoitukseen kehitettyjä, vaihtoehtoisia sovelluksia keskenään. Tarjokkaita on tullut lyhyessä ajassa saataville runsaasti. Niitä kehitetään etenkin suurten pilvipalveluntarjoajien, kuten Amazonin, Microsoftin ja Googlen siipien suojissa, mutta myös avoimen lähdekoodin yhteisöllisinä projekteina.

Yksinkertaistettuna riittää, että ammattikäyttöön ohjelmistoa kehittävä tiimi etsii vaihtoehtojen joukosta turvallisuus- ja saatavuuskriteerit täyttävän palvelun, kuten kielimallin, joka ei sieppaa sille syö-

Teknologia	Toimintaperiaate ja hyödyt	Esimerkkejä käyttökohteista	Erityistä huomioitavaa, kun työkaluja tuodaan turvaluokiteltuun ympäristöön
Luonnollisen kielen käsittely (NLP, Natural Language Processing)	Algoritmiperhe, joka muuntaa ihmisen tuottamaa tekstiä tietokoneen ymmärtämään muotoon. Mahdollistaa mm. puheen muuntamisen tekstiksi ja analyysin.	Aihealueiden tunnistaminen laajoista datamassoista. Automaattisten lyhennelmien luominen. Puhutun viestiliikenteen litterointi.	Mistä opetusdata on peräisin? Miten sovellus kerää käyttäjien dataa? Miten mallin opettaminen ja käyttäminen onnistuu suomeksi?
Vahvistusoppiminen (Reinforcement Learning)	Jatkuvasti oppiva päätöksentekojärjestelmä, joka adaptoituu muutoksiin nopeasti ja etsii optimaalisen tavan toimia. Mahdollistaa rationaaliset päätökset myös tilanteissa, joissa eri muuttujia olisi liikaa ihmisen käsiteltäväksi.	Itseohjautuva liikenne, asiantuntijajärjestelmät (eng. expert system).	Kun koneelle annetaan valta tehdä päätöksiä, millaiset ovat mahdolliset seuraukset turvallisuuden näkökulmasta?
Ennakoiva analyysi (Predictive Analysis)	Tekoäly ymmärtää historiallisen datan avulla, mihin tämän hetken indikaattorit johtavat tulevaisuudessa. Ennustemallit antavat ihmistä luotettavampia arvauksia siitä, mitä on tapahtumassa.	Ajoneuvojen moottorivahinkojen ennustaminen etukäteen. Ennakoivilla huolloilla maksimoidaan hyötyajon määrä.	Miten tuoda kaikki luotettaviin analyyseihin tarvittava data varsinkin korkeamman turvaluokan järjestelmiin (TL I, II ja III) turvallisesti?
Resurssioptimointi (Resource Optimization)	Resursseja on rajatusti, ja niitä tulisi hyödyntää mahdollisimman tehokkaasti. Matemaattinen optimointimalli laskee suunnitelman nopeasti ja aina oikein.	Asiantuntijaresurssien allokaatioasteen optimointi. Kaluston tai tilojen maksimaalisen käyttöasteen löytäminen.	Algoritmi ei tarvitse historiallista dataa, mutta riittävän määrän syötedataa toimiakseen. Miten tuoda se turvallisesti varsinkin korkeamman turvaluokan järjestelmiin (TL I, II ja III)?
Konenäkö (Computer Vision)	Tunnistetaan valokuvista tai videokuvasta esineitä, henkilöitä, tekstiä tai muita asioita, joilla on merkitystä käyttökontekstissa	Rakennusten tunnistaminen ilmakuvasta. Ihmisen erottaminen koirasta osana liiketunnistusta	Mallin opetusvaiheessa on tärkeää pohtia, miten voidaan tehokkaasti hyödyntää avointa dataa.

Taulukko:Viisi ajankohtaista tapaa hyödyntää tekoälyä sovelluskehityksessä. Monet työkalut ovat näiden teknologioiden yhdistelmiä.

tettyä informaatiota käytön aikana, vaan hyödyntää muiden mallien keräämää tietoa. Sen jälkeen malli voidaan liittää osaksi järjestelmää. Korkean turvaluokituksen ympäristöissä lähtökohta on kuitenkin hieman monimutkaisempi.

Suljetut ympäristöt tuottavuuden kannalta eri asemassa

Valtiotason turvallisuuskriittiset ja suljetut ympäristöt ovat murroksen äärellä eri viivalla kuin esimerkiksi yksityisen sektorin yritykset, joiden kaupallisiin tuotteisiin ei kohdistu yhtä tiukkoja vaatimuksia tietojen turvaamisesta. Molemmilla areenoilla on siitä huolimatta yhtä suuri halu tehostaa toimintaa ja saada hyöty irti uusista teknologioista.

Helposti saatavilla olevat, edulliset tekoälymallit ovat usein osa julkipilvialustojen palvelutarjontaa, tai niitä voi hankkia käyttöön erillisinä palveluina SaaS-mallilla. Turvallisuusluokitelluissa järjestelmäkehityksen projekteissa – erityisesti maanpuolustuksen kontekstissa – näiden julkisesti saatavilla olevien valmisratkaisujen käyttö ei kuitenkaan ole aina mahdollista.

Työn alla oleva järjestelmä saattaa sisältää tietoa, joka ei missään oloissa saa joutua vieraan vallan käsiin. Siksi vaatimuksissa edellytetään datan säilytystä tiukasti omissa käsissä. Äärimmäisissä oloissa järjestelmän on toimittava esimerkiksi metsään sijoitetusta serverikontista käsin, ulkopuolisista internetyhteyksistä riippumatta. Silloin omiin, fyysisiin palvelimiin nojaava on-premise -ratkaisu voi olla ainoa vaihtoehto.

On työläämpää rakentaa älykkäitä teknologioita – oppivien algoritmien ja mallien monimutkaisia yhdistelmiä – suljettuihin sovelluksiin alusta asti itse, verrattuna siihen, että ottaisi käyttöön valmiita, edullisia komponentteja julkipilvikirjaston hyllystä. Toimiviksi todettujen mallien takana on laaja, globaali opetusdata ja paljon hajautettua laskentatehoa. Jos samaa tasoa tavoitellaan turvaluokitellussa ympäristössä täysin omin voimin, hankkeiden tuottavuusero repeää hallitsemattoman suureksi.

Tekoälyn ketterään hyödyntämiseen on kuitenkin paljon mahdollisuuksia myös turvallisuuskriittisissä ympäristöissä.

Ota teknologia avuksi tietoturvallisen koodin tuottamiseen

Nousevat teknologiat tuovat mukanaan uusia toiminnallisuuksia, jotka näkyvät järjestelmien loppukäyttäjille. Näkymättömämpi, mutta vähintään yhtä merkittävä hyöty on se, miten paljon ohjelmistojen kehitystyö ja jatkuva ylläpito tehostuu. Älykkäät työkalut auttavat ohjelmistokehittäjiä esimerkiksi 1) ottamaan olemassaolevan koodin nopeammin haltuun, 2) luomaan proof of concept -kokeiluja, joihin oma osaaminen ei muutoin riittäisi, 3) nopeuttamaan uusien ohjelmointikielien oppimista ja 4) pääsemään eteenpäin arkisista ongelmanratkaisun umpikujista.

Olennaista on jälleen osata valita kehittäjän työkalupakkiin ne sovellukset, joiden käyttö on kyseisessä hankkeessa turvallista ja vaatimusten mukaista.

Tietoturvan analysointi on yksi tapa käyttää tekoälysovelluksia entistä kestävämpien järjestelmien rakentamiseen. Kone tunnistaa virheet väsymättä ja käsittelee suuriakin koodimassoja nopeasti. Myös ohjelmistojen testauksen ammattilaiset seuraavat koneoppimisen työkalujen kehitystä tarkasti. Tietoturvaan ja testaamiseen liittyvät tekoälyn hyödyt pätevät yhtä lailla avoimien kuin suljettujen ympäristöjen järjestelmäkehitykseen.

Hyödynnä valmisratkaisuja siellä, missä se on mahdollista

Oletetaan tilanne, jossa koko organisaatio joutuu huomioimaan tarkat turvallisuusmääräykset kaikessa toiminnassaan. Laajan organisaation sisältä voi silti löytyä yksiköitä tai toimintoja, joissa järjestelmät tai niihin liittyvä data eivät edellytä samankaltaisia turvatoimenpiteitä kuin jonkin toisen toiminnon kohdalla.

Esimerkiksi sotilassoittokunnan nuotit on ehkä mahdollista säilyttää tietoturvallisesti julkipilvessä, vaikka se tarkoittaisi että palvelimet ovat toisen valtion alueella. Tai jos tarkoituksena on kerätä tiedustelutietoa avoimista, julkisista lähteistä kuten Facebook- tai Telegram-keskusteluista, voi olla mielekästä yhdistää tiedonkeruuvaiheeseen avoimesti saatavilla olevia algoritmeja ja julkipilvessä toimivia koneoppimismalleja. Se tuo tehoa tiedonkeruuseen, vaikka myöhemmässä tietojen käsittelyn vaiheessa julkipilven resurssien käyttö ei olisikaan enää mahdollista.

Tietojen säilytys saattaa näyttäytyä uudessa valossa myös Suomen NATO-jäsenyyden myötä. Eteen saattaa tulla tilanteita, joissa tietyn sovelluksen pyörittäminen yhdysvaltalaisten yritysten palvelinkeskuksilta käsin olisi aiemmin ollut tietoturvanäkökulmasta mahdoton ajatus. Nyt vaihtoehto voikin olla harkitsemisen arvoinen.

Tunnista, milloin datan käsittely muuttuu arkaluontoiseksi

Ohjelmistokehitykseen liittyy aina geneerisiä ongelmia, jotka toistuvat lukuisissa muissa projekteissa ympäri maailman. Kun kehittäjä etsii vastausta geneeriseen ongelmaan, hän voi ajatella tekoälymalleja osana tiedonhaun evoluutiota. Tänä päivänä tärkeä osa arkipäivän tietoturvaa onkin, että asiantuntija osaa erottaa, mitkä kysymykset ovat yleisiä, millaiset ongelmat taas sisältävät jo kysymyksenasettelun tasolla arkaluontoista tietoa.

Valmiita algoritmeja voi hyödyntää erityisesti uusien sovellusten ideointivaiheessa. Esimerkiksi salatun, ajoneuvoista kerätyn datan käsittelyä maastotietoihin yhdistettynä voisi ensin mallintaa vastaavan tyyppisellä julkisella datalla ja julkisilla karttatyökaluilla. Rautalankamallin pohjalta on helpompaa rakentaa vaatimuksia varsinaiselle järjestelmälle.

Seuraava vaihe, eli omien mallien rakentaminen, on Data Scientist -asiantuntijoille tuttua työtä. On silti syytä tietää tarkasti, mitä aikoo tehdä, ennen kuin polkaisee oman projektin käyntiin. Jos verrataan tekoälytoteutusta liikennevälineisiin: rakennatko potkulautaa standardisoiduista komponenteista vai teetkö scifi-alusta, jollaista ei ole vielä nähty?

Valmiin sovelluksen sisälläkin arkkitehtuureja voi olla useita erilaisia. Aiemmin mainittua julkista, sosiaalisen median tiedustelutietoa voisi aluksi luokitella julkipilveen nojaavilla sovelluksilla. Tai julkisista lähteistä kerättyjä maastokuvia voisi analysoida julkisesti saatavilla olevilla kuvantunnistuksen työkaluilla.

Kriteerit muuttuvat siinä vaiheessa, kun kerätystä tiedosta tehdään havaintoja, analyyseja, yhteenvetoja ja toimintasuunnitelmia. Tulkintoja ja johtopäätöksiä sisältävä data muuttuu valtion kannalta turvallisuuskriittiseksi, eikä sen joutumisesta vääriin käsiin voi ottaa riskejä. On siirryttävä suljettuun ympäristöön ja täysin omissa käsissä oleviin älykkäisiin malleihin.

Nivelkohtiin järjestelmien sisällä täytyy kiinnittää erityistä huomiota. Uuden sovelluksen rakennusvaiheessa tarvitaan syvällistä osaamista IT-arkkitehtuureista. Tarvitaan kykyä tehdä turvallisia siltoja avointen ja suljettujen ympäristöjen välille.

Etsi yhteistyön mahdollisuuksia omien mallien kehittämiseen

On siis tilanteita, joissa data on käsiteltävä tiukasti suljetussa ympäristössä, ja työtä helpottavat tekoälykyvykkyydet täytyy rakentaa itse. Kuten sanottua, työmaa ei ole aivan pieni. Haluaisimmekin nähdä tulevaisuudessa entistä enemmän ennakkoluulotonta yhteistyötä julkisen sektorin eri yksiköiden välillä.

Esimerkki NLP-toteutuksen näkökulmasta: suomi on pieni kielialue, ja valmista opetusdataa on siksi saatavilla niukasti. Toisaalta varsinkaan julkisella sektorilla ei ole realistista ajatella, että työkieli vaihtuisi sormia napsauttamalla englanniksi vain, koska tekoälytyökalut vaatisivat niin.

Kuvitellaan nyt tilanne, jossa terveydenhuolto ja maanpuolustus huomaavat yhtä aikaa tarpeen sovellukselle, joka litteroisi puhuttua suomen kieltä tekstiksi ja tekisi siitä yhteenvetoja. Silloin on optimaalista resurssien käyttöä lähteä kehittämään mallia yhdessä eri organisaatioiden ja tutkimuslaitosten, kuten yliopistojen kanssa. Tämän tyyppisiä hankkeita onkin parhaillaan käynnissä.

Voinko hyödyntää pilvipalveluja ja niiden älykkäitä ominaisuuksia turvallisuuskriittisten ratkaisujen kehittämisessä?

Selvitä rationaalisesti, mikä on oikeasti kriittistä tietoa ja mikä ei. Saatat todeta esimerkiksi, että:

- Järjestelmä ei ole salainen, eikä datakaan ole
- Järjestelmä ei ole salainen, mutta sen data on
- Järjestelmä ja data ovat salaisia, mutta prosessin alkuvaiheessa, kuten koodin generoinnissa, voi hyödyntää julkisia työkaluja, tai järjestelmän sisällä voi olla kokonaisuuksia joissa luokittelu on toisenlainen
- Järjestelmä ja data ovat salaisia, mutta tarvittavien algoritmien kouluttamiseen voi käyttää julkista dataa

Huolellisesti suunniteltuna ja oikeilla teknologioilla, lopputulos on resurssitehokas ja täyttää korkeat turvallisuusvaatimukset.]

Mitä teknologiaan ja osaamiseen tulee, omien algoritmien kehittämiseen on Suomessa hyvät olosuhteet. Onhan valtion hallussa Euroopan nopein ja energiatehokkain supertietokone Lumi. Sen arvokasta laskentatehoa pääsee tällä hetkellä käyttämään vain rajatuissa aikaikkunoissa – jälleen hyvä peruste organisaatiorajat ylittävälle yhteistyölle.

Onnistuuko järjestelmän siirtäminen poikkeustilanteessa?

Turvallisuuskriittiset järjestelmät on viisainta tehdä arkkitehtuureiltaan siirrettäviksi, ja mahdollisuuksien mukaan myös harjoitella siirtoja erilaisiin ympäristöihin. Se on osa uhkiin varautumista.

Rauhan aikana on perusteltua vaatia esimerkiksi tiedon säilyttämistä konesaleissa valtion rajojen sisäpuolella. Varmuuskopioista huolehditaan kahdentamalla tai kolmentamalla data eri konesaleihin.

Jos ulkopuoliset uhkat realisoituvat poikkeusoloiksi, voikin äkisti olla turvallisempi vaihtoehto hajauttaa tietyt järjestelmät säilytettäviksi maan rajojen ulkopuolelle, esimerkiksi NATO-kumppanimaissa sijaitseviin konesaleihin. Kahdennuksesta tai kolmennuksesta huolimatta vihollisella olisi liian korkeat mahdollisuudet tuhota fyysisiä palvelimia.

Kriittisimmät järjestelmät pitäisi voida siirtää ketterästi kahteen suuntaan. Toisaalta on-premisesta virtuaalipalvelimille, toisaalta virtuaaliresursseilta tarvittaessa paikallisille servereille, juuri sinne metsässä sijaitsevaan fyysiseen palvelinkonttiin.

Mitä enemmän järjestelmään on liitetty älykkäitä ominaisuuksia ja uutta teknologiaa, sitä enemmän erityisasiantuntemusta tarvitaan jo arkkitehtuurien suunnitteluvaiheessa. Vain siten voidaan varmistua siitä, että siirtymät ovat joustavia, ja operationaalinen toiminta ja älykkäiden teknologioiden hyödyntäminen voi jatkua ilman katkoksia kaikissa olosuhteissa.

Tekoälyn arvausten validointiin tarvitaan edelleen ihminen

Paljon pinnalla olleet generatiiviset kielimallit muodostavat kysyjälle vastauksia, jotka ovat kyllä vakuuttavan näköisiä, mutta silti vain aineistomassaan perustuvia arvauksia. Arvausten validointiin tarvitaan edelleen ihmistä. Oppivat, optimaalisia ehdotuksia tarjoavat matemaattiset algoritmit taas tarjoavat väsymättä rationaalisimman mahdollisimman vaihtoehdon, ilman inhimillisten tekijöiden vaikutusta. Se on sekä teknologian vahvuus että heikkous.

Tekoäly kehittyy valtavaa vauhtia. Turvallisuusvaatimukset sanelevat reunaehdot sille, millaisia kokeiluja omassa organisaatiossa on mahdollista tehdä, mutta kokeilevaa ja uteliasta asennetta tarvitaan myös korkean kriittisyystason suljetuissa ympäristöissä. Vain siten voimme rakentaa tulevaisuudenkestäviä, vahvoja ja kilpailukykyisiä ohjelmistoja.

Kirjoittaja toimii IBM:n konsultointi-organisaatiossa johtavana arkkitehtina.

TEKSTI: TUOMAS VANHANEN

Alustariippumattomat ratkaisut taktisessa käytössä - konttiteknologia mahdollistajana

Erilaisten sensorien tuottaman datan määrä on sotilaskäytössä kasvanut viime vuosina räjähdysmäisesti ja datan määrän kasvulle ei näy loppua. Tuotettua tietoa käsitellään sekä päätelaitteissa että palvelinympäristöissä ja tekoäly tulee avustamaan sotilaita yhä moninaisimmilla tavoilla. Kehitettäviä uusia kyvykkyyksiä halutaan usein hyödyntää mahdollisimman laajasti myös muissa, jopa hyvin erilaisissa, käyttöympäristöissä. Alustariippumattomuus edesauttaa sovellusten laajempaa käyttöä.

Asevoimat rakentavat ratkaisujaan yhä enemmän siviilipuolelle kehitetyn teknologian päälle, koska ne haluavat hyötyä siellä tehdystä tuotekehityksestä ja innovaatioista. Taistelukentän vaativissa oloissa tulee teknologian olla käytettävissä esimerkiksi ajoneuvoissa, miehittämättömissä aluksissa tai puettuna teknologiana osana taistelijan varusteita. Alustariippumattomat ratkaisut voivat auttaa myös siirtymisessä normaalioloista poikkeusoloihin, koska ne tukevat sovellusten kapasiteetin lisäämistä tarpeen mukaiseksi. Lisäksi ne voivat helpottaa myös arjen välineiden hyödyntämisessä poikkeusoloissa.

Alustariippumattomuus

Alustariippumattomat sovellusohjelmat määritellään ohjelmistoiksi, jotka eivät ole sidoksissa tiettyyn alustaan (tietokonelaitteistoon tai käyttöjärjestelmään). Alustariippumattomien sovelluksien käyttökohteet voidaan karkeasti jakaa kahteen ryhmään: päätelaitteisiin ja palvelinohjelmistoihin. Molemmista sovellustyypeistä on käyttötapauksia asevoimien taktisessa käytössä. Useimmat tietojärjestelmät vaativat toimiakseen sekä päätelaitteessa toimivan käyttöliittymän että sille palveluita tarjoavan palvelinohjelmiston.

Alustariippumattomia sovelluksia kehitettäessä tavoitteena on, että sama sovellus voidaan tarjota sellaisenaan käyttöön laajemmalle käyttäjäkunnalle eikä samoja toiminnallisuuksia tarvitse kehittää eri alustoille. Näin sovelluksen kehitys ja ylläpito on tehokkaampaa. Alustariippumattomuus voi kuitenkin myös rajoittaa sovelluksen kyvykkyyksiä, koska sovelluksen käytössä ei välttämättä ole kaikki sen alla olevan alustaohjelmiston kyvykkyydet.

Kehitettäessä alustariippumattomia sovelluksia päätelaitteille on tavoitteena usein, että samaa ohjelmistoa voidaan ajaa sekä iOS että Android-laitteissa ja myös tietokoneella. Päätelaitteelle alustariippumattomuus voidaan toteuttaa monella eri tavalla, joista useimmat käyttävät web-tekniikoita. Tekniikan valinnassa on syytä huomioida mm. sen soveltuvuus suunniteltuun käyttötarkoitukseen, sen turvallisuus ja miten se tukee esim. tekoälyn tai lisätyn todellisuuden hyödyntämistä.

Web-tekniikoiden lisäksi sovelluksia voidaan ohjelmoida myös muilla kuin iOS:n ja Androidin tukemilla ohjelmointikielillä. Eri kielellä kehitetty sovellus voidaan kääntää sitten eri käyttöjärjestelmille, esimerkiksi Flutter- käyttöliittymäkehitystyökalun tapaan. Eri ohjelmointikielellä toteutettua ohjelmistoa tulkataan päätelaitteelle sopivaksi ja ajettavaksi. Tästä käy esimerkkinä React Native, joka on tällä hetkellä hyvin suosittu tapa toteuttaa päätelaiteriippumattomia ohjelmistoja.

Web-tekniikoilla tehtyjä alustariippumattomia sovelluksia on kritisoitu niiden huonommasta suorituskyvystä, käyttökokemuksen poikkeavuudesta käyttöjärjestelmän omilla tekniikoilla tehtyihin sovelluksiin verrattuna ja heikommasta tuesta käyttöjärjestelmän edistyneiden kyvykkyyksien – kuten lisätty todellisuus – käytölle. Erot suosituimpien kehikkojen ja natiivien sovellusten kyvykkyyksien välillä ovat kuitenkin kaventuneet ja alustan kyvykkyydet ovat hybridisovelluksissa hyvin käytössä, vaikkakin käyttökokemus poikkeaa natiivista sovelluksesta.

Oheinen taulukko esittelee eri mobiilisovellusten tyyppejä ja niissä käytettyjä sovelluskehityskehikkoja ja ohjelmointikieliä. Lista ei ole kattava.

Päätelaiteriippumattomuudesta esimerkiksi käy Ukrainan käyttämä Delta-tilannekuvajärjestelmä, joka koostaa tietoa useista eri siviili- ja sotilaslähteistä. Sen käyttöliittymä on selainpohjainen ja se toimii eri päätelaitteissa kannettavasta tietokoneesta niin tablettiin kuin puhelimeenkin.

Konttiteknologia mahdollistajana

Palvelinohjelmistoissa suosituin tapa ajaa ohjelmistoja alustariippumattomasti on nykyään ns. kontitus. Kontituksessa sovellus paketoidaan standardoidulla tavalla, joka mahdollistaa sen ajamisen hyvin erityyppisissä ympäristöissä. Kontitetut sovellukset voivat olla hyvin erilaisia ja kehitetty eri ohjelmointikieliä ja teknologioita hyödyntäen. Tämä mahdollistaa iäkkäämpienkin sovellusten modernisoinnin ja siirron konttimaailmaan.

Sovellustyyppi	Kuvaus	Sovelluskehitys-kehikko	Ohjelmointikielet
Natiivi-sovellus	Käyttöjärjestelmälle kehitetty sovellus, joka ei ole alustariippumaton.		Kotlin, Java, Swift, Objective-C
Web-sovellus	Sovellus, jota ajetaan selaimessa		HTML, CSS, JavaScript
Progressiivinen web-sovellus (PWA)	Sovellus hyödyntää selaimen toteuttamia rajapintoja ja mahdollistaa mm. offline -toiminnallisuudet sekä push -notifikaatiot		HTML, CSS, JavaScript
Hybridisovellus	Web-tekniikalla toteutettu sovellus ajetaan natiivin säiliön sisällä WebView:ssä	Apache Cordova, Ionic	JavaScript
Tulkattava sovellus	Alustariippumaton koodi (esim. JavaScript) tulkataan sovelluksessa. Voidaan hyödyntää natiiveja rajapintoja.	React Native, Xamarin, Qt	JavaScript, C#, QML
Käännettävä sovellus	Sovellus kehitetään omalla kielellään ja käännetään natiiviksi-ohjelmaksi	Flutter	Dart

Taulukko 1. Erityyppisiä tapoja toteuttaa käyttöliittymäsovellus.

Samaa kontitettua ohjelmistoa voi siis ajaa vaikka Windows tai Linux -käyttöjärjestelmässä, mutta myös kooltaan hyvin erikokoisissa ympäristöissä: esim. drooneissa tai useita palvelimia vaativissa klustereissa. Suurissa ympäristöissä sovellus voi koostua useista erikseen kontitetuista komponenteista ja ajoympäristö (esim. Kubernetes) huolehtii siitä, että sovellus on saatavilla ja sen kapasiteetti skaalautuu käytön mukaan. Nämä kontitetut sovellukset toimivat usein taustajärjestelminä, jotka palvelevat käyttöliittymiä varastoimalla tietoa, käsittelemällä sitä eri tavoin ja välittämällä tietoa muille järjestelmille. Konttien ajoympäristöt mahdollistavat sovellusten skaalautumisen ja vikasietoisuuden perinteisiä tapoja tehokkaammin. Kubernetes mm. käynnistää uudestaan kontin, joka ei enää vastaa pyyntöihin. Jo olemassa olevaan Kubernetes-klusteriin voidaan lisätä uusia palvelimia ja sen kokoa kasvattaa käytön kasvaessa tai esim. siirtyessä normaalioloista poikkeusoloihin.

Myös Java-ohjelmointikieli on ollut suosittu tapa toteuttaa palvelinohjelmistoja siten, että niitä voidaan ajaa eri käyttöjärjestelmillä. Java-ohjelmisto on käännetty jakelua varten välivaiheen tavukoodiksi ja ohjelma ajetaan kullekin käyttöjärjestelmälle tehdyllä versiolla Javan virtuaalikoneesta. Lisäksi laitteistoriippumattomia palvelinohjelmistoja voidaan kehittää myös komentokielillä (skriptikielillä), jotka tulkataan lennossa sen sijaan, että ohjelmisto käännettäisiin Javan tapaan etukäteen. Tämän tyyppisiä kieliä ovat mm. Perl, Python ja PHP. Tavoitteena kaikissa on se, että jaeltava ohjelmisto on sama, vaikka sen ajoympäristö onkin erilainen.

Nykyisin valloillaan on trendi jatkaa vanhojen Java-sovellusten käyttöaikaa modernisoimalla ja kontittamalla näitä sovelluksia. Tällöin voidaan vaihtoehtoisesti käyttää GraalVm-virtuaalikonetta, joka kykenee Javan lisäksi myös muiden ohjelmointikielien ajoon, mutta on Javan virtuaalikonetta tehokkaampi ja turvallisempi. Java-sovellusten modernisoinnissa ja kehityksessä voidaan käyttää myös Quarkus-kehystä, joka on kehitetty nimenomaan Java-sovellusten ajoon Kubernetes-ympäristössä ja on optimoitu esimerkiksi sovellusten nopeaan käynnistymiseen.

Tietokone- ja palvelinympäristöissä on käytetty pitkään pääosin x86/x64-suoritinarkkitehtuuria. ARM-arkkitehtuurin mukaiset palvelimet, jotka kuluttavat vähemmän energiaa, ovat kuitenkin yleistymässä ja niitä voidaan käyttää esim. drooneissa ja puettavassa teknologiassa. ARM-suorittimien käytön lisääntyminen on syytä huomioida alustariippumattomia ratkaisuja toteutettaessa. Java-sovelluksia voidaan ajaa sellaisenaan ARM:ia tukevalla virtuaalikoneella, mutta sovelluskontit pitää erikseen kääntää ARM-prosessoreille. Komentokielillä toteutetut sovellukset ovat usein ajettavissa sellaisenaan, mikäli niiden riippuvuudet muihin komponentteihin täyttyvät.

Kuva 1. Erityyppisiä alustariippumattomia tapoja ajaa ohjelmia.

Taktinen käyttöympäristö

Taktisessa käytössä olevia ratkaisuja käytetään sotatoimi- tai kriisinhallinta-alueilla. Taktiset järjestelmät ovat käytössä pääosin prikaatissa ja sitä alemmilla tasoilla ja niitä hyödynnetään ajoneuvoissa ja muissa liikkuvissa järjestelmissä.

Taktisia järjestelmiä yhdistää se, että tehtävän onnistuminen ja käyttäjien selviytyminen alueella voi olla riippuvainen järjestelmien ja yhteyksien toimivuudesta. Käyttäjät toimivat kovan kuormituksen ja paineen alla ja niin käyttäjät, järjestelmien yhteydet kuin niiden infrastruktuuri ovat uhattuina. Ympäristö edellyttää täten järjestelmiltä vikasietoisuutta, liikkeen ja tärinän sietoa ja ohjelmistojen kykyä toipua erilaisista vika- ja häiriötilanteista. Alustariippumattomia sovelluksia voidaan taktisessa ympäristössä käyttää hyvin moninaisiin tarpeisiin, kuten logistiikka, huolto, tilannekuva ja viestintä.

Järjestelmien eri käyttöympäristöt taktisessa ympäristössä voidaan luokitella esimerkiksi näihin ympäristöihin:

1. Ylemmät johtoportaat ja ennalta valmistellut komentopaikat

2. Liikkuvat komentopaikat

3. Taistelijan tai autonomisen järjestelmän taso

Nämä ympäristöt eroavat toisistaan käytettävissä olevien verkkoyhteyksien ja teknisen ympäristön resurssien osalta ja niissä voidaan suojata järjestelmiä ja tietoa eri tavoin. Myös käyttäjille tarjottavissa olevat käyttöliittymät voivat olla hyvin erilaisia sisältäen kunkin käyttäjäryhmän toiminnassaan tarvitsemat ominaisuudet.

Taktisessa käyttöympäristössä 5G tulee olemaan yksi kasvava tapa tuottaa tarvittavat yhteydet järjestelmille. 5G-verkkoja voidaan käyttää niin yksityisinä (private) kuin julkisina (public) sekä yhdistellä näitä hybridiverkoksi. Ylipäätään 5G tarjoaa monia hyötyjä sotilaskäyttöön, kuten mahdollisuus viranomaisliikenteen priorisoinnille, 5G-verkon korkeampi nopeus, IoT-yhteydet yhdistettynä reunalaskennalla (Mobile Edge Computing) ja päätelaitteiden suorat keskinäiset yhteydet (Sidelink). 5G mahdollistaa myös tukiaseman kytkeytymisen verkkoon radioteitse (IAB, Integrated Access Backhaul), jota voidaan käyttää esimerkiksi ennalta valmistelemattoman johtopaikan yhteyksien muodostamiseen.

Ylemmät johtoportaat ja ennalta valmistellut komentopaikat sijaitsevat paikoissa, joissa on yleensä saatavilla hyvät valmiiksi rakennetut verkkoyhteydet ja sinne voidaan viedä isompia palvelinklustereita, joilla on paljon tallennus- ja laskentakapasiteettia. Ne mahdollistavat saarekkeisen toiminnan yhteyksien katketessa. Päätelaitteet ovat tuttuja toimistotyöstä ja käyttöliittymätkin voivat olla laajempia ja monimutkaisempia. Järjestelmiä voidaan suojata samoin periaattein kuin perinteisissä palvelinkeskuksissa. Tiedot ovat kryptattuina levyillä, liikenne salataan VPN-ratkaisuilla ja se kulkee erilaisten yhdyskäytävien kautta. Järjestelmien käyttäjät tunnistetaan käyttäen vahvaa tunnistamista ja heidän käyttöoikeutensa eri järjestelmissä ovat roolipohjaiset, vastaten sen hetkistä tehtävää.

Kuva 2. Järjestelmien käyttöympäristöt ja niiden laitteistoa.

Liikkuvissa komentopaikoissa tai ajoneuvoissa käytössä voi olla pieni akkuvirrallakin toimiva palvelinklusteri, joka tarjoaa vikasietoisuutta, mutta on liikuteltavissa. Verkkoyhteydet ovat todennäköisesti pääosin käytettävissä, vaikka katkoksia ja saarekkeista toimintaa voi ilmentyä. Yhteyksissä voidaan hyödyntää 5G:tä, satelliitteja, radio- tai kuituyhteyksiä. Palvelinympäristöön kytkeytyvät laitteet ovat ajoneuvoasenteisia tai kannettavia laitteita, joko tablettilaitteita tai tietokoneita. Järjestelmässä on riittävästi kapasiteettia käsitellä ja tallentaa myös paikallisesti kohtuullisen suuria tietomassoja ja toimia taustajärjestelmänä useille sovelluksille. Palvelinympäristön tiedon suojausmahdollisuudet ovat samankaltaiset kuin ylemmän johtoportaan järjestelmissä. Tiedot säilytetään kryptattuna ja liikenne on salattua. Käyttäjillä on roolipohjaiset käyttöoikeudet, kirjautumisen toimiessa myös ilman verkkoyhteyksiä. Mobiilipäätelaitteiden turvallisuuden varmistamiseksi niitä hallitaan keskitetysti. Järjestelmiin kohdistuu elektronisen sodankäynnin toimia ja tiedustelua.

Taistelijan tai autonomisen järjestelmän tasolla toimitaan pääosin ilman verkkoyhteyksiä. Yhteyksiä käytetään, kun niitä tarvitaan. Käyttäjät käyttävät pääosin mobiilipäätelaitteita ja niiden sovelluksia. Näiden lisäksi voi olla hyvin pieniä palvelinympäristön kaltaisia ratkaisuja esimerkiksi drooneissa tai osana puettavaa teknologiaa. Koska käyttötilanne on stressaava, on käyttöliittymien oltava yksinkertaisia ja laitteiden kovennettuja. Käyttöliittymänä voi olla kosketusnäyttö, mutta laitetta voi ohjata myös puheella. Uhkana on laitteiden päätyminen viholliselle, niiden vaurioituminen ja viestiyhteyksien estäminen sekä paikantaminen tiedustelun avulla. Paikallisesti tallennetaan vain tarpeellinen tieto ja tiedot salataan, ja päätelaitteita hallitaan keskitetysti tietoturvan varmistamiseksi.

Käyttöympäristöt rajoittavat sekä varsinaista sovellusta että sen käyttöä usealla eri tavalla. MITRE:n julkaisema viitekehys (Tactical Edge Characterization Framework) erottelee taktisen käytön järjestelmiä verkkoyhteyksien, operoinnin, teknisen ympäristön resurssien, fyysisen ympäristön ja turvallisuuden perusteella. Taulukossa 2 on koostettu keskeisiä eroja eri taktisten käyttöympäristöjen välillä viitekehykseen pohjautuen, tiivistäen ja ajantasaistamalla luokittelua.

Yksi keskeinen rajoittava tekijä on verkkoyhteyksien haavoittuvuus. Sovellukset on suunniteltava toimimaan myös ilman yhteyksiä ja esimerkiksi tarvittavan tiedon osalta laitteessa on oltava ne tiedot mukana, joita tehtävän suorittamiseen tarvitaan. Tehtävän aikana on varauduttava siihen, että verkkoyhteyksiä ei ole käytettävissä tai niitä ei haluta käyttää.

	Ylemmät johtoportaat ja ennalta valmistellut komentopaikat	Liikkuvat komentopaikat	Taistelijan ja autonomisen järjestelmän taso
Verkkoyhteydet	Hyvät yhteydet	Kohtuulliset yhteydet	Pääosin ilman yhteyksiä
Päätelaitetyyppi	Tietokone	Liikuteltava palvelinympäristö	Mobiilipäätelaite
Palvelinympäristön tyyppi	Palvelinklusterit	Tietokone, mobiilipäätelaite	Puettavat laitteet Droonit
Laitteiston kapasiteetti	Suuri	Kohtuullinen	Kohtuullinen/Pieni
Käyttöliittymän laajuus	Kompleksi	Kohtuullinen	Yksinkertainen

Taulukko 2. Kooste taktisen ympäristön luokittelusta.

Taktinen käyttötarkoitus

Sensorien välittämää tietoa (esim. kuvaa, ääntä tai signaalitietoja) voidaan käsitellä joko laitteessa, jonka sensori kerää tietoa, tai tieto voidaan välittää tilannearvion ja päätöksen teon tekemiseksi eteenpäin. Kun sensoridatan määrä kasvaa, tarve käyttää kehittynyttä analytiikkaa, tekoälyä ja oppivia malleja taktisessa ympäristössä kasvaa, jotta isoa tietomassaa ei tarvitse siirtää jonnekin toisaalle käsiteltäväksi. Esimerkiksi, tekoäly voi kuvan perusteella tunnistaa mielenkiintoisen kohteen ja välittää vain tiedon kohteesta eteenpäin tilannearviota varten. Samoja tekoälymalleja kohteen tunnistamiseen haluttanee jatkossa käyttää hyvin erilaisissa ympäristöissä ja siksi sovellusten siirrettävyys on tärkeää, jotta vältetään tarve sovellusten mukauttamiseen kuhunkin käyttöympäristöön erikseen. Palvelinympäristössä kehitettyjä malleja voidaan ajaa esimerkiksi riittävällä prosessorikapasiteetilla varustetuissa drooneissa, jotka valvovat joukkoja, johtoportaita tai komentopaikkoja. Samaa mallia voidaan myös hyödyntää 5G-verkkoon liitetyn sensorin tiedonkäsittelyyn 5G-verkon reunalaskentakyvykkyyksiä hyödyntäen.

Esimerkkinä toteutetusta siirrettävästä sovelluksesta havainnointitarkoituksessa käy Lockheed Martinin esittelemä miehittämätön ilma-alus ’Stalker’. Lockheed käyttää aluksessa Red Hat:n pieniin ympäristöihin, kuten robotteihin, julkiseen liikenteeseen ja IoT-ympäristöihin suunniteltua konttien ajoalustaa (MicroShift) ajamaan tekoälysovelluksia, joilla tulkitaan sensorien välittämää tietoa. Alusta mahdollistaa paitsi sovellusten ajamisen, myös tekoälymallien päivittämisen etänä käytön aikana.

Sensoritiedon määrän kasvaessa tarve sensorifuusiolle kasvaa. Sensorifuusiossa yhdistetään erilaista ja eri lähteistä kerättyä tietoa ja sitä jalostetaan päätöksenteon tueksi. Sensorifuusio voidaan tehdä jatkossa automaattisesti ja lähempänä tietoa tarvitsevaa joukkoa. Joukkojen käytössä olevat laitteistot sensorifuusiolle voivat erota merkittävästi (vrt. pinta-alus, ajoneuvo tai komentopaikka), mutta tarve tehdä sensorifuusiota tilannekuvan saamiseksi voi edellyttää kykyä ajaa sovelluksia näissä erilaisissa ympäristöissä.

Turvallinen nopeus on valttia

Taktisen ympäristön ratkaisujen kehittäminen on nopeutunut huimasti. Olemme nähneet, miten ukrainalaiset ovat kehittäneet nopeasti erilaisia ratkaisuja sitä mukaa, kun tarpeita on noussut. Tarve ketterämpään reagointiin on havaittu myös perinteisessä aseteollisuudessa. Yhdysvaltain ilmavoimat testasi sovellusten päivittämistä F-35-hävittäjässä. Nämä ohjelmistot eivät toki olleet lennon turvallisuudelle kriittisiä, vaan liittyivät uhkien tunnistamiseen. Testilennon jälkeen ohjelmistoa päivitettiin sovelluskehitystiimin toimesta ja seuraava testilento tehtiin jo 24 tuntia myöhemmin.

Taktisten ympäristöjen ohjelmistoja täytyy pystyä kehittämään ja jakelemaan nopeasti. Jakeleminen päätelaitteisiin ja palvelinympäristöihin pitää olla automatisoitua, koska taistelukentällä ei ole aikaa asennella ohjelmistopäivityksiä - eikä siellä välttämättä ole siihen osaamistakaan.

Nopea kehittäminen puolestaan asettaa vaatimuksia laadunvarmistukselle ja tietoturvalle. Vaikka pyydetty ominaisuus halutaan nopeasti käyttöön, se ei saa rikkoa mitään käytössä olevaa toimintoa. Vikaantunut tai väärin toimiva ohjelmisto taktisessa ympäristössä voi aiheuttaa tappioita tai pilata operaation.

Ohjelmistokehityksen parhaita käytänteitä seuraamalla voidaan tuottaa turvallista ja toimivaa ohjelmistoa nopeastikin. Joissakin tilanteissa ei kuukausien testaus- ja hyväksymisprosesseille ole aikaa, mutta riittävät menetelmät ja prosessit on oltava käytössä, joilla ohjelmistopäivitysten toimivuus varmistetaan ennen kuin päivitys jaetaan laajempaan käyttöön.

Mitä tulevaisuus tuo tullessaan?

Suomessa on perinteisesti valmistauduttu siihen, että sodan syttyessä vihollinen katkaisee-merikaapelit ja viestiyhteydet ulkomaille. Uhka merikaapelien katkomisesta on aito, mutta jäämmekö kokonaan ilman ulkomaan yhteyksiä? Ukrainassa olemme nähneet, että Ukraina on kyennyt tarjoamaan verkkoyhteyksiä kriisin aikana niin siviileille kuin sotilaillekin. Internetiä käyttävät sovellukset ovat Ukrainassa olleet saatavilla. Karttaja tykistön tulenjohtosovellus Kropivan käyttäjillä on Starlinkin kautta yhteydet ”kaikkialla” ja olemme nähneet miten ukrainalaisen kranaatinheitinryhmän tulta johdetaan selainkäyttöisessä Google Meets -videokonferenssissa, jossa jaetaan droonin välittämää videokuvaa. Ukraina on onnistunut operaatioturvallisuudessaan ja sotilaita on ohjeistettu olemaan käyttämättä puhelimiaan, jotta Venäjän tiedustelu ei ole voinut paikantaa heitä. Voidaanko jatkossa taistelukentällä olettaa, että data liikkuu, jos vain haluamme sen liikkuvan?

Alustariippumattomuus kehittynee samaan suuntaan kuin tietoliikenneverkot ja kotonakin tuttu mesh-verkko. Kotona langatonta verkko käyttävä laite juttelee lähimmän mesh-tukiaseman kanssa tarjoten parhaan yhteyden riippumatta siitä, missä kerroksessa tai huoneessa laitetta käytetään. Samalla tavalla alustariippumattomat palvelut tulevat olemaan käytössä taktisessa ympäristössä. Jos jokin palvelinympäristö vioittuu tai tuhoutuu, tarjotaan palvelut toisesta ympäristöstä. Kapasiteetin ollessa riittämätön vähemmän tärkeitä kyvykkyyksiä ajetaan alas ja käyttäjille tarjotaan vain ne kriittiset kyvykkyydet, joita välttämättä tarvitaan. Tämän tyyppinen ympäristö rakennetaan hyödyntäen pilvipalveluissa käytetty-

Kuva 3. Ukrainassa käytössä oleva Kropiva-sovellus (Kuva:Army SOS)

ja teknologioita ja muodostamalla taistelukentän pilvipalvelu (Multi-Domain Combat Cloud), joka on hajautettu ja kybersietoinen alusta, jossa tieto ja sen jakaminen eri toimijoiden välillä on keskiössä.

Laajat kielimallit ovat olleet viime aikoina paljon uutisissa. Laajat kielimallit tulevat käyttöön asevoimissakin ja niitä tullaan käyttämään sekä turvaluokitelluissa ympäristöissä kuin taktisessakin käytössä ja näidenkin pitää toimia alustasta riippumatta. Esimerkiksi Palantir on esitellyt tekoälyalustansa käyttöä tehtävän suunnittelussa. Tulevaisuudessa voidaan tekoälyltä kyselemällä arvioida eri vaihtoehtoja tehtävän suorittamiseen ja tekoälyä komentamalla voidaan koostaa käskyt. Jos tulevaisuuden työntekijän taito on muotoilla tekoälylle kysymyksiä ja tehtäviä (ns. prompt engineering), niin ehkä tulevaisuuden sotilaallekin tämä on tärkeä taito.

TEKSTI JA KUVAT: JUKKA-PEKKA VIRTANEN

Ilmavoimien tiedustelua ja viestijärjestelmien kansainvälistymistä

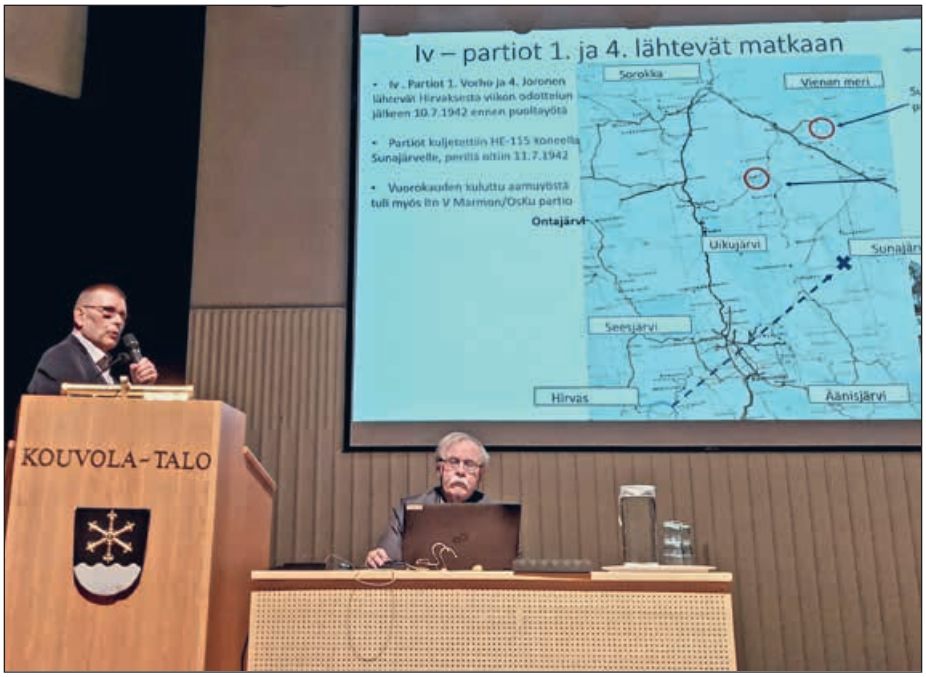
Sotilasradiopäivä 2023

Kouvolan Sotilasradiomuseon ja Kymen Viestikillan järjestämä kymmenes Sotilasradiopäivä toimeenpantiin Kouvola-talolla 22.4.2023. Tasokkaista sisällöistään ja erinomaisista esitelmöitsijöistä tunnettu seminaari tarjosi tällä kertaa paikalla olleelle noin 200-päiselle yleisölle rautaisannoksen Ilmavoimien radiotiedustelua osasto Hartikaisen edesottamuksiin peilaten. Ohjelmassa oli myös tarinaa hävittäjäradion sodanaikaisesta kehityksestä. Nykyaikaan – ehkäpä hieman tulevaisuuteenkin kuulijat vei majuri Paavo Kaivonurmen esitys Nato-jäsenyyden vaikutuksista maanpuolustuksen johtamisjärjestelmään. Tapahtuman päätti Päämajan viestikeskus Lokista kertova dokumenttifilmin televisioversio, joka oli vastikään voittanut toisen palkinnon Filmi- ja videokuvaajien liiton SM-kilpailujen dokumenttisarjassa.

Ilmavoimien radiotiedustelu-valmistelut muuttuivat kaukopartioinniksi

Kapteeni evp Jorma Risku oli otsikoinut esitelmänsä ”Osasto Hartikaisen ilmavalvontapartiot vihollisen lentokentille jatkosodassa 1942”. Ilmavoimien oman radiotiedustelun tarve nousi esille vuonna 1941, koska ilmapuolustus tarvitsi tietoa vihollisen lentokoneista vasta- ja suojelutoimenpiteitä varten. Ajatuksen radiotiedustelusta esitti LeR2 komentaja eversti Richard Lorenz. Asiaa edisti myös ilmavoimien viestikomentaja majuri Matti Virva. Marraskuussa 1941 luutnantti Mauri Hartikainen lähetettiin perehtymään Päämajan Radiopataljoona, ’Moton’ toimintaan Itä-Karjalassa ja Sortavalassa sijainneeseen radiotiedustelukeskukseen. Tämän perusteella Hartikainen ja Virva laativat esityksen ilmavoimien radiotiedustelujärjestelyistä ja -kalustosta.

Vuodenvaihteen 1942 taitteessa kehittyi Ilmavoimien esikunnassa uusi ajatus tiedustelun toteuttamisesta lähettämällä ilmavalvontakaukopartioita vihollisen lentokentille. Partiot viestittäisivät reaaliaikaisesti lentokenttätoiminnoista; nousuista, laskuista, konetyypeistä jne. Päämaja hyväksyi eversti Lorenzin helmikuussa 1942 tekemän esityksen, henkilöstöä ja materiaalia koskevin reu-



Kapteeni evp Jorma Risku esitelmöi ilmavoimien jatkosodanaikaisesta ilmavalvontapartiotoiminnasta. Kuvassa myös Sotilasradiopäivien monivuotinen puuhamies Kouvolan Putkiradiomuseosäätiö hallituksen puheenjohtaja Kari Taskinen.

naehdoin, lähettää Ilmavoimien kaukopartioita vihollisen lentokentille alkukesästä 1942. Käytännön toteuttajaksi ja osaston päälliköksi määrättiin Hartikainen.

Ennen operaation toimeenpanoa toteutettiin Naarajärvellä Ilmavoimien Viestivarikolla Lentokenttäpartioiden Ilmavalvontakurssi. Yli kahden kuukauden mittaiselle käytännön harjoitteluun painottuneelle kurssille osallistui nelisenkymmentä vapaaehtoista. Kaukopartiotaitojen lisäksi ohjelma sisälsi Kyynel-viestitystä, viestisalausta, venäjän kieltä, laskuvarjohyppyjä, lentokoneiden tunnistusta, ammuntaa ja fyysisiä harjoitteita. Toiminta oli salaista, eikä lomia ollut.

Tehtävän toteuttamiseksi perustettiin Osasto Hartikainen (OsH) Tiiksjärvellä 1.6.1942. Osaston vahvuus oli 1 upseeri, 18 aliupseeria ja 30 miehistön jäsentä, joista muodostettiin viisi nelihenkistä kaukopartiota. Osaston johtajaksi määrättiin kapteeni Mauri Hartikainen. Tehtävänä oli lähettää lento- ja säätulokset kiireysjärjestyksessä lähimmälle kuuntelupisteelle ja lentoyksikölle. ’Tavalliset’ tiedustelutulokset oli lähetettävä lähimmälle kaukopartio-osastolle ja Ilmavoimien Esikunnalle. Osaston toiminta-alue Vienan Karjalassa oli kooltaan noin 200 km x 200 km ollen yksi Euroopan suurimmista erämaista. Alueelle leimansa antoi myös Sorokassa haarautuva Muurmannin rautatie sekä Vienanmeren ja Äänisen yhdistävä Stalinin kanava.

Partiot ryhmittyivät moninaisten vaiheiden jälkeen lentokenttien läheisyyteen, joita olivat Sumskij-Posad (Vorho), Letnjaja (Kemppainen), Sosnovitsa (Myllyniemi), Jendoguba (Joronen) ja Sekee (Valkeinen). Siirtymiset olivat kymmeniä kilometrejä kestäen useita vuorokausia. Ilmavalvontasanomien vasta-asema toimi Tiiksjärven partiotukikohdassa. ’Normaalisanomien’ vasta-asema sijaitsi Äänislinnassa. Kalustona käytettiin venäläistä 70 watin tehoista RSB lähetintä ja amerikkalaista NC 100-XA vastaanotinta. Lisäksi käytettiin Hellschreiber kaukokirjoittimia. Jokaisella partiolla oli käytössään ’Kyynel’ M4/M7 partioradio ja ’Töpö’ yleisradiovastaanotin.

Partioiden viestiliikennejärjestelyt oli toteutettu siten, että molemmilla vasta-asemilla oli sama kuuntelutaajuus

Tapahtumassa oli esillä hävittäjäradioteemaan liittyvää esineistöä.

(4600 kHz), jonne partioasemat lähettivät havaintonsa. Kyynel-partioasemat vastaanottivat 4100 kHz:n taajuudella. Partioiden käyttöön kehitettiin ilmavalvontasanomille soveltuva salauskoodisto. Sähkötysnopeus oli 30-40 merkkiä sekunnissa. Partioiden yleishuolto oli ilmavoimien vastuulla. Se toteutettiin tavarapudotuksina Dornier 17- ja Blenheim-pommikoneista. Materiaaliin kuului myös Kyynel-radion paristoja, radioputkia, antenneja ja muita varaosia.

Osasto Hartikaisen toiminta-alueella arvioitiin olevan noin 10 000 venäläistä sotilasta muodostuen kuudesta rajavartiorykmenttistä, NKVD rykmentistä ja muutamasta pataljoonasta. Vihollisen joukot olivat erinomaisesti koulutettuja ja varustettuja. Niiden yksi päätehtävistä oli Muurmanskin radan ja Stalinin kanavan turvaaminen. Tämä vaikeutti merkittävästi suomalaisten partiotoimintaa ja paluuta omalle puolelle. Esimerkiksi Vorhon johtama partio lähetti ilmavalvonta- ja sääsanomia 22.7. - 3.8.1942 Sumskij Posadista, jossa oli lentotoimintaa runsaasti. 3.8. - 3.9.1942 partio oli nälkäkuoleman partaalla, mutta pääsi omalle puolelle huonossa kunnossa. Matkaa kertyi kaikkiaan noin 500 km.

Osasto Hartikaisen loppuraportissa todettiin, ettei lentokenttien ilmavalvontatoiminta toiminut halutulla tavalla. Heinäkuun 1942 sateista johtuen vihollinen lensi vähän. Lentokentät olivat hyvin valvottuja, eikä niiden lähelle päässyt, mistä johtuen toimintaa jouduttiin seuraamaan kauempaa. Vain yksi kotiasema päivysti ympäri vuorokauden, joten ilmavalvontasanomia ei kyetty vastaanottamaan. Ilmavalvontasanomista meni perille vain 30-40 prosenttia, vaatimuksen ollessa 70 prosenttia. ’Normaalisanomat’ saatiin viestitettyä lähes 100 prosenttisesti molempiin suuntiin. Lentolaivueiden ja Ilmavoimien johto eivät olleet tyytyväisiä tuloksiin. Laivueet moittivat viestien hitautta, joka aiheutti torjunnan myöhästymisiä. Myös nelihenkisen partio vahvuus todettiin liian pieneksi. Osasto Hartikainen lakkautettiin 14.9.1942 ja kapteeni Hartikainen sai 21.10.1942 tehtävän perustaa Ilmavoimien radiotiedusteluyksikön.

Sodanaikainen hävittäjäradiokehitys

Seuraava esitelmöitsijä, Jussi Harola on keskittynyt tutkimuksissaan ilmavoimien viestikalustoon ja sen taktisiin käyttöperiaatteisiin. Häneltä ovat ilmestyneet mm. kirjat ’Yhteys! - Tiedonanto- ja viestivälineitä Suomen puolustusvoimissa’ ja uusimpana ’Ilmavoimien taktinen viestitoiminta talvi- ja jatkosodassa - Menomatkalla radiohiljaisuus’, jossa käsitellään hävittäjä-, kaukotoiminta- ja yhteistoimintakoneiden tärkein radiokalusto sekä maaradio- ja suuntimoasemat. Kirja perehdyttää lukijan myös ilmavoimien viestitoiminnan kehittymiseen ja siihen liittyviin keskeisimpiin sotatapah-

tumiin laivue- ja rykmenttitasolla. Harolan tämän kertainen esitys keskittyi edellisiin kiinteästi linkittyen hävittäjäradion sotien aikaiseen kehittymiseen.

Ensimmäinen kotimainen hävittäjäasema oli P-12-17, jonka ensimmäinen koekappale valmistui vuonna 1934. Radion lähettimessä oli kolme kidekanavaa ja jatkuvasäätöinen vastaanotin. Radiolla oli merkittävä rooli talvisodassa. Sodan jälkeen vastaanottimen mekaaninen kauko-ohjain korvattiin viidellä kidekanavalla ja sähköisellä kauko-ohjauksella.

Positiiviset kokemukset Morane Saulnier -hävittäjän ultralyhytaaltoisesta radioasemasta johtivat siihen, että Puolustusministeriön sähkölaboratorio aloitti vuoden 1940 vaihteessa 4-8 m (37,5-75 MHz) aseman suunnittelutyön. Käyttäjävaatimuksissa yhteysetäisyys ilmassa piti olla vähintään 50-75 km ja ilmasta maahan 150-250 km. Kanavia tuli olla 2-3 ja mahdollisuus dublex-puheliikenteeseen. Säätimet haluttiin ohjaamon vasemmalle puolelle ja lennonaikainen viritystarve poistaa. Vaatimuksina oli myös panssarointi ja yhteysmahdollisuus ilmatorjuntatykistön komentopaikkaan. Koekappaleen tilaus tehtiin 18.4.1941. Asemaa suunnitellut insinööri vaihtoi kuitenkin työnantajaa toukokuussa 1941, mistä johtuen sähkölaboratorio ilmoitti seuraavan vuoden helmikuussa, ettei voi valmistaa koekappaletta työvoimapuutteen vuoksi. Tilaus peruttiin 22.10.1942.

Uusi hävittäjäradiohanke P-12-100 käynnistettiin syksyllä 1942. Suunnittelupöydällä oli alkuaan kolme erityyppistä radiota: P-12-100/A (3,9-6 MHz, AM), P-12-100/B (50-55 MHz, AM) ja P-12-100/C (43-67 MHz, FM). Näistä ainoastaan P-12-100A-hanke eteni. Sopimuksessa Helvar toimittaa kolme mallikappaletta 16.1.1943 mennessä. Hankkeeseen tuli heti alkuun kahden kuukauden viive. Sarjatuotanto käynnistyisi mahdollisesta vasta loppuvuodesta. Välitön tarve uusiin Myrsky-hävittäjiin oli 50 kappaletta ja pohdintoihin nousikin luottamus Helvarin mallin valmistumiseen, vanhemman P-12-17-radion käytettävyyden parantaminen ja ulkomaiset hankintamahdollisuudet.

Helvarin mallikappale valmistui vuoden 1944 alussa ja siihen liittyneet koelento-ohjelmat Junkers W34:llä toteutettiin maaliskuussa ja Curtissilla kesäkuun alussa. Neuvostoliiton suurhyökkäys kuitenkin keskeytti koeohjelman ja maakalusto sekä hävittäjät lähetettiin rintamalle. Hankkeesta luovuttiin heinäkuussa. Junkers Ju 88 -syöksypommittajat saapuivat huhtikuussa 1943 ja Messerschmitt Bf 109 G-6 -hävittäjät maaliskuussa 1944, jolloin ultralyhytaaltoisen radioaseman kehittämistä päätettiin jatkaa ja esitys ultralyhytaaltoisesta radiosta tehtiin kesäkuun alussa 1944.

Ilmavoimien viestikalustoon ja taktisiin käyttöperiaatteisiin perehtynyt Jussi Harola (vas) ennätti esitysten välillä tutustua myös Kaakkois-Suomen Viestikillan esittelyständiin. Pöydän ääressä Seppo Kiiski (oik) ja Martti Susitaival.

Ensimmäisessä kotimaisessa hävittäjäasemassa P-12-17 oli kolme kidekanavaa ja jatkuvasäätöinen vastaanotin. Koekappale valmistui vuonna 1934.

Johtamisjärjestelmiltä edellytetään Nato-yhteensopivuutta

Majuri Paavo Kaivonurmi esitelmöi tilaisuuden pääteeksi Naton vaikutuksista kansallisiin johtamisjärjestelmiin. Hänen mukaansa jäsenyys ei muuta Puolustusvoimien lakisääteisiä tehtäviä ja tärkein tehtävä on jatkossakin oman maan puolustaminen. Toki puolustusliiton jäsenenä

valmistaudumme puolustamaan myös liittolaisia. Varusmiespalvelukseen ja suureen reserviin perustuva sodan ajan suorituskyky säilyy. Jäsenyys vie meidän turvatakuiden piiriin, tarjoten kyvykkyyksiä, joihin pienellä maalla ei ole varaa, eikä edes järkevää hankkia itse.

Maapuolustuksen johtamisjärjestelmäkokonaisuus muodostuu Puolustusvoimien yhteisestä järjestelmästä, maavoimien omista M18- ja Maaleijona-järjestelmistä sekä arjen välineistä. Keskeisinä Nato-jäsenyyden vaikutuksina Kaivonurmi listasi liittymisen Naton tietojärjestelmiin ja palveluihin, kansallisesti toteutettavan verkkolaajennuksen ja oman palvelutuotannon, Naton salausratkaisut, lainsäädännön, sopimuksien ja normien muutokset, integraatiossa tarvittavan henkilöstöresurssin varmistamisen sekä viranomaisten yhteiset ratkaisut.

Majuri Paavo Kaivonurmi esitelmöimässä 'Nato-jäsenyyden vaikutuksia maapuolustuksen johtamisjärjestelmään'.

Johtopäätöksissä hän totesi, että M18 ja arjen välineet jäävät kansalliseen käyttöön. Maaleijona-tietojärjestelmältä edellytetään FMN-yhteensopivuutta (Federated Mission Networking). Tarkasteltaessa eri järjestelmiä johtamis- ja organisaatiotasoja vasten voidaan todeta, että ylimpänä on strategisen tason Nato secret (NS) -järjestelmä, seuraavalle tasolle sijoittuu operaation johtamisen mahdollistava FMN-yhteensopiva kansallinen järjestelmä ja prikaatitasolta alkaen tukeudutaan lähtökohtaisesti kansallisiin järjestelmiin, joilta ei edellytetä välttämättä kansainvälistä yhteensopivuutta.

Antti Nyqvist
Valmiuspäällikkö, Huoltovarmuusorganisaation Digipoolin pääsihteeri Teknologiateollisuus ry:ssä.

TEKSTI: ANTTI NYQVIST

Pilvipalvelut ja huoltovarmuus - järkeviä päätöksiä

Johdanto

Yritysten liiketoiminnan jatkuvuus ja huoltovarmuus ovat pitkälti riippuvaisia häiriöttömästä ICT järjestelmien toiminnasta. Yhä useampi siis panostaa järjestelmien jatkuvuuteen ja tekee siihen liittyviä päätöksiä tiedostaen tai valitettavan usein tiedostamattaan. Huoltovarmuuden kannalta onkin koettu tarpeelliseksi nostaa esiin eri näkökohdat huomioiva päätöksentekoprosessi, jonka läpikäytyään yrityksessä tai muussa organisaatiossa voidaan varsin vakain mielin lähteä etenemään tiedonhallinnan kehityspoluilla.

Päätöksentekoprosessi on syytä miettiä yritykseen sopivaksi ja sellaiseksi, että se huomioi ne organisaation yksilölliset tarpeet ja aiheet, jotka arvioidaan olevan sille olennaisia. Hallitun päätöksentekoprosessin läpikäynyt toimija on todennäköisesti varmistanut liiketoimintansa jatkuvuuden ja samalla edistänyt huoltovarmuutta osaltaan.

Kun puhutaan tiedonhallinnasta ja siihen liittyvistä päätöksistä on yksi suurimmista asioista kysymys siitä, miten ja missä tietoamme hallitaan ja yksinkertaistettuna puhutaankin hyvin pian siitä, ollaanko konesalissa suomessa vai kansainvälisissä pilvipalveluissa. Molempiin liittyvät riskinsä ja toisaalta molemmissa on omat hyötynsä ja molemmissa tapauksissa ratkaisun kanssa tulee pystyä elämään pidempiä aikoja ja näin tulee miettiä myös esim. se mitä osaamista se vaatii pitkällä aikavälillä.

Julkista keskustelua pilvipalveluista värittää monet jopa väärinkäsityksistä kumpuavat ajatukset siitä, että jotain tietynlaista tietoa tulisi käsitellä vain paikallisissa konesaleissa. Lainsäädäntö ei kuitenkaan tähän suoraan ota kantaa ja siksi tiedostavalla (ja dokumentoidulla) päätöksentekoprosessilla suuri merkitys sille onko tehty järkeviä päätöksiä.

Keskusteluilmapiiri on myös pilvipalveluiden käytölle myönteinen ja Valtionvarainministeriötä myöden onkin käynnissä hankkeita, jotka selkiyttävät edellytyksiä pilvipalveluiden käytölle julkishallinnossa. Myönteiseen ilmapiiriin on vaikuttanut myös Venäjän hyökkäyssodan kokemukset ukrainasta, missä kansallinen infrastruktuuri ministeriöitä ja yliopistolaitoksia myöden on viety pilvipalveluiden varaan fyysisen tuhoutumisen uhan jaloista.

TOP3 aiheita, jotka tuntuvat aiheuttavan päänvaivaa tai joihin liittyy vaikeasti täytettävien edellytysten tähden vääriä loppupäätelmiä, ovat henkilötietojen käsittely ja tiedon sijainti tai siirto. Näiden lisäksi vaakakupissa tuntuu usein olevan se mitä osataan nyt vs. mitä pitäisi osata - eli henkilöstön osaaminen. Näidenkin kanssa oppii elämään, kunhan päätöksentekoprosessi osaa ottaa oikeat asiat huomioon.

Pilvipalveluista jatkuvuudenhallinnan välineenä

Pilvipalvelut yleistyvät ja useita yrityksille välttämättömiä ohjelmistoja ei enää saakaan muuten kuin pilvipalveluina, joten monet ovat pakotettuja niitä käyttämään - monien ohjelmistojen osalta kuitenkin on olemassa vielä muitakin vaihtoehtoja. Niissä tapauksissa, kun ei ole muuta mahdollisuutta kuin käyttää pilvipalvelua tulee tuntea sen turvallisuusominaisuudet ja pyrkiä se konfiguroimaan omaan tarpeeseen turvalliseksi - tulee miettiä mm., että voidaanko sitä käyttää oman infran osana vai erikseen siitä erotettuna.

Usein törmää kysymykseen siitä, että mitä jos yhteydet pilvipalveluihin katkeavat - tulisiko kuitenkin viedä tiedot omaan konesaliin? Nykyinen suomessa voittava ajattelumalli on, että katkoksia voi tulla, mutta useimmiten kuitenkin yhteydet saadaan palautettua ja pilvessä kun ollaan, on se palvelu siellä edelleen hengissä ja käytettävissä yhteyksien palautuksen jälkeen. Ja samoin ne yhteydet sinne konesaliin voivat katketa ja paikallisessa konesali-infrassa tai pienessä privaattipilvessä riski laitteiden hajoamiselle/tuhoutumiselle tai tiedon katoamiselle on ehkä kuitenkin suurempi. Eli puntaroidaan riskejä yhteyksien katkeamisesta fyysisten konesalien tai laitteiden rikkoutumiseen ja pistetään näitä vaakakuppiin.

Pilvipalveluiden eduksi tiedonhallinnan ja liiketoiminnan jatkuvuudenhallinnan välineenä on laskettava monia asioita. Näitä etuja ei voi ohittaa, kun palveluita verrataan muihin vaihtoehtoihin. Päätösprosessin on huomioitava näitä etuja ja verrattava niitä muihin vaihtoehtoihin sekä huomioitava vaihtoehtoihin liittyvät riskit. Esimerkkeinä pilvipalvelluiden eduista mainittakoon:

- Palveluiden ylivertainen skaalautuminen

- Ketterästi käyttöön mukautuvat resurssit (ja niiden myötä kustannukset)- - Resilienssi ja vikasietoisuus on toteutettavissa ilman merkittäviä lisäkustannuksia (Pilvipalveluiden tietoturvan kehittämiseen investoidaan valtavasti - pelkästään Microsoft investoi pilvipalvelujensa kehittämiseen enemmän kuin Suomen valtio kaikkeen digitalisaation kehittämiseen.)

- Pilvipalvelut mahdollistavat nopean ja kustannustehokkaan palautumisen.

Päätöksentekoprosessista

Jokaisen organisaation tulisi siis kiinnittää huomiota prosessiin, jolla päätöksiä tehdään tiedonhallintaan liittyen. Ja hyvän prosessin voikin tiivistää 4 oleelliseen aiheeseen, jotka toimenpiteinä istuvat hyvin esim. turvallisuuden vuosikelloon yrityksen toiminnassa:

- Tietojen ja toimintojen tunteminen, arvon arviointi ja priorisointi

- Toimintaan kohdistuvien vaatimusten tuntemus

- Päätöksenteko prosessin tai hallintamallin määrittely ja organisaation sitouttaminen

- Toimintaan ja toimintoihin kohdistuvien uhkien ja riskien arviointi ja toimenpidesuunnittelu

Yritykset tarvitsevat päätöksentekoa varten ymmärryksen oman liiketoimintansa kriittisistä toiminnoista ja datasta, lainsäädännön ja toimialan vaatimuksista sekä yritystoimintaan kohdistuvista uhkista ja riskeistä. Tämän lisäksi on huomioitava muut mahdolliset liiketoiminnan erityispiirteet, jotka asettavat vaatimuksia eri vaihtoehdoille.

Kaikki lähtee tässäkin aiheessa siitä, että organisaatio on läpikäynyt toimintonsa ja arvioinut sen tärkeyden omalle liiketoiminalleen sekä esim. huoltovarmuudelle tai yhteiskuntavastuulle. Priorisoinnin tulee ohjata mm. turvallisuuteen käytettäviä investointeja sekä muita tiedonhallintaan liittyviä päätöksiä - esim. se mitä palveluita hankitaan ja minkälaisilla vaatimuksilla - alemmalla prioriteetilla voi luonnollisesti olla höllemmät vaatimuksetkin ja korkeammalla tietysti tiukemmat. Kaupallisesti toiminnon kriittisyyden kommunikointi toimitusketjuun on välistä haastava aihe, sillä se tuppaa kasvattamaan kustannuksia, mutta hyvin arvioitu kriittisyys kannattaa kuitenkin kommunikoida ketjussa eteenpäin, jotta toiminto saa ansaitsemansa suojauksen toiminnassa.

Toimintojen arvioinnin lisäksi tulee nykyisellään tuntea sen omassa omistuksessa olevan tiedon arvo. Organisaation hallussa olevan tiedon arvo tulee ohjata siihen liittyviä päätöksiä. Suomessa vaikuttaisi olevan vähän lapsenkengissä ajattelu tieto-omaisuuden arvon vaikutuksista. Sen lisäksi että tieto tulee luokitella luottamuksellisuuden mukaisesti, tulee arvioida sen arvoa yrityksen liiketoiminnalle. Ja vastikään on alettu nähdä se, että yrityksen hallussa olevan tiedon, eli datan arvoa on alettu arvioimaan ja sen mukaan mitoittamaan sen suojaukseen tms. liittyviä investointeja. Turhan usein tiedon arvo nähdään vasta kun tieto on jo vaarantunut, varastettu, vääristynyt tai sitä ei pystytäkään käyttämään. Nykyisin yhä useampi toimija miettii uusia dataan perustuvia liiketoimintamalleja ja sen myötä hallussa olevan tiedon arvo onkin merkittävässä nousussa ja sen pitäisi tietysti merkitä myös sen suojaamiseen ja saatavuuteen liittyviin toimiin panostamista.

Päätösprosessi yksinkertaistettuna.

Toisena tulee tuntea omaan toimintaan kohdistuvat vaatimukset - jotka voivat olla ihan lakisääteisiä tai niillä voi olla muuten velvoittava luonne, kuten vastuullisuusaiheet tai yhteiskuntavastuu. Pelkästään lakisääteisiä vaatimuksia voi olla niin paljon, että viidakosta ei selviä ilman juristia ja vaatimusten läpikäynti voi olla oma projektinsa. EU myös nykyisellään asettaa odotusarvoja lisääntyvässä määrin ja näiden tuloon onkin jo hyvä varautua. Asiaan on siis kiinnitettävä huomiota ja verkostoista on tässä hyötyä - useinkaan ei siis tarvitse jäädä yksin miettimään mikä meitä velvoittaa.

Organisaation oman prosessin miettiminen myös kannattaa. Se kuinka asiat käsitellään niiden noustessa sekä se, kuinka niitä ylläpidetään. Prosessin tulee huolehtia vastuista ja valtuuksista, joita organisaation rooleilla on ja tätä tietoa pitää myös ylläpitää velvoitteiden tai organisaation muuttuessa. Myös monet aihealueen standardit kiinnittävät tähän huomiota - eli useinkin standardien mukaan toimiminen auttaa pitämään asiat hallussa ja tukevat järkevien päätösten teossa.

Ja luonnollisesti päätöksentekoprosessiin tulee kuulua uhka ja riskikartoitus. Pitää miettiä se mitä uhkia ja riskejä meihin tai meille tärkeisiin aiheisiin liittyy ja kuinka niiden mahdollista vaikutusta pienennetään tai kuinka niistä päästään eroon. Ja tässä kannustetaan laaja-alaiseen katsantoon, jotta huomioidaan esim. teknisiä riskejä laajemmin vaikuttimet. Digipoolin selvitysten perusteella suomessa onkin parannettavaa siinä, kuinka kyberriskit tai niiden mahdolliset vaikutukset otettaisiin paremmin huomioon yrityksen liiketoiminnan riskienhallinnassa - toisin sanoen tekniset riskit tulee käsitellä liiketoimintavaikutuksiksi, jotta ne tulevat huomioiduksi. Ja toinen riskienhallintaa koskeva havainto on se, että aivan turhan harvoin sopimussuhteissa tehdään yhteistä uhkien tai riskien käsittelyä - vaikka molemmat pyrkivät tekemään parhaansa sen tärkeän toiminnon eteen - näin ainakin niissä kriittisimmissä toiminnoissa tulisi tehdä yhteistä riskienhallintaa ja sitä vaikka sopimuksilla edellyttää.

Selvitystemme perusteella päätöksiin vaikuttavat lopulta hyvin rajallinen joukko aiheita ja näihin kannattaakin päätösprosessissa kiinnittää huomiota. Yritysten toimintaan kohdistuvista ja pilvipalveluidenkin käyttöön vaikuttavista aiheista löytyy paljon lainsäädännöllisiä edellytyksiä, joista seuraavissa kappaleissa kerrotaan lisää. Mutta yksi suurimmista hidasteista pilvipalveluihin siirtymiselle on osaamisen puute. Pilvipalvelujen käyttö vaatii omanlaista osaamista, jota ei välttämättä löydy perinteisen IT-ympäristön ammattilaisilta. Pilviympäristöön siirtyminen vaatiikin uudenlaisen

osaamisen hankkimista ja usein uusien IT-kumppanien etsimistä. Toisaalta tämä tarkoittaa sitä, että asiakkaat voivat tehdä epähuomiossa tai tietämättään tyhmyyksiä, koska pilvipalveluissa sen jokainen komponentti on yhteydessä internetiin. Pilvipalvelujen tietoturvallinen käyttö vaatiikin kovan luokan osaamista joko yritykseltä itseltään tai sen IT-kumppanilta sekä omaa riskienhallinnan prosessia. Pilvipalveluihin siirtyminen onkin iso teknologiamurros. Selvityksessä huomattiin, että pilvipalveluiden hallinnan osalta osaaminen ei ole riittävän korkealla tasolla.

Järkevän päätösprosessin lopputuloksista

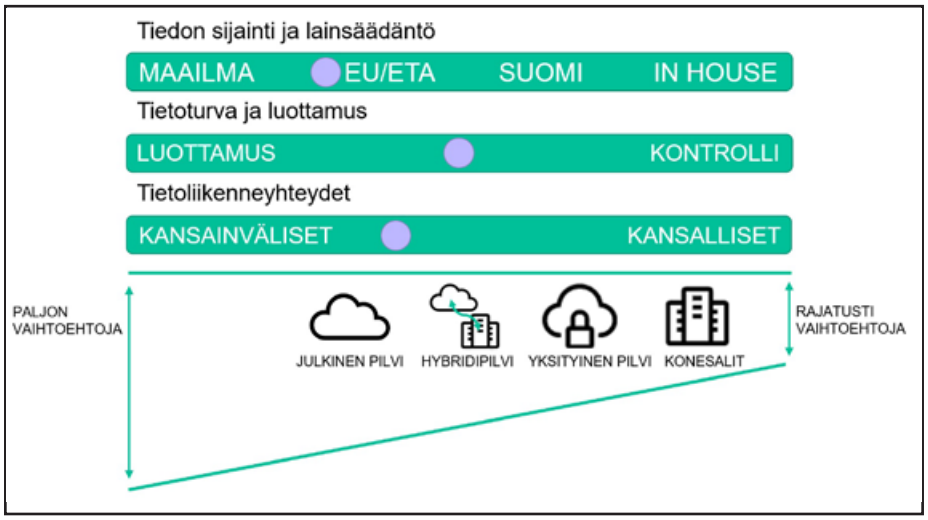
Suunnitellun ja hallitun päätösprosessin läpikäytyään voi organisaatio toimia rauhallisemmin mielin ja lähteä toteuttamaan toimenpiteitä, joista se tietää olevan mahdollisimman hyviä ja kohdistuvan tärkeisiin aiheisiin. Päätösprosessin lopputuloksena voi olla hyvinkin erilaisia päätöksiä esim. siitä kuinka tietoa hallitaan ja mitkä ovat ne ratkaisut, jotka juuri omaan toimintaan soveltuvat.

Kuvassa 2 on havainnollistettu sitä kenttää, minne päätökset järkevän prosessin myötä osuvat. Huoltovarmuusorganisaation käsitellessä tietojensa hallintaa voi päätökset johtaa julkipilven käyttöön tai oman kovan konesali-infran rakentamiseen tai jonnekin näiden välille riippuen siitä mitä edellytyksiä tiedon käsittelylle on tai asetetaan.

Jos äärimmilleen haluaa varautua (Mahdollisiin tietoliikennekatkoksiin tai konesalien tuhoutumiseen) ja varmistaa pääsyn tietoon kaikissa tilanteissa on todennäköisesti paras (ja kallein) ratkaisu se että toimitaan jonkun tiedon tai järjestelmien osalta sekä kv pilvipalveluissa että kotimaan kamaralla olevissa konesaleissa. Kokonaisuuden ylläpito perustamiskustannusten lisäksi on tietysti sitten myös korkeampi. Päätösprosessin pitää kuitenkin vastata siihen paljonko kunkin toiminnon turvallisuus saa maksaa.

Juridisen selvityksen huomioita pilvipalveluiden käyttöön liittyen

Digipoolin teettämän pilvipalveluiden käyttöön liittyvän lainsäädännön selvityksen perusteella kotimainen lainsäädäntö ei ole niin määräävä tai rajaava kuin julkisesta keskustelusta voisi ymmärtää. Kansallinen lainsäädäntö tai EU-lainsäädäntö asettavat usein edellytyksiä pilvipalveluiden käytölle, jotka valitettavan usein koetaan esteiksi pilvipalveluiden hyödyntämiselle. Edellytykset tulee siis täyttää, jotta tietynlaista tietoa voidaan käsitellä pilvipalveluissa.



Päätösprosessin lopputuloksia.

Merkittävimmät aiheet, jotka aiheuttavat harmaita hiuksia päätöksentekoprosessissa ovat niitä, joihin liittyy eniten lainsäädäntöä ja erilaista (joskus jopa ristiriitaista) ohjausta. Ehdottomasti eniten tiedonhallinnan päätöksiin vaikuttaa henkilötietojen käsittelyyn liittyvä lainsäädäntö ja GDPR asetus. Toisena vaikuttaa eri alojen oma erityissäätelynsä. Kolmantena on huomioitava julkishallinnon lainsäädäntöä - joka usein ohjaa myös palvelutuottajia, jos ja kun palveluita tuotetaan julkishallinnolle edes jostain yrityksen kulmasta. (Palvelutuottajan kun ei kannata tuottaa palveluitaan kovin monella tavalla vaan tehokkuuden tähden sille yhdelle vaativalle asiakkaalle tuotettu palvelu on hyvää palvelua myös muille ja samalla turvallisuuden kustannuskin kohtuullistuu per asiakas.)

Henkilötietojen käsittelyyn liittyy GDPR asetuksen ohjaus säilyttää sellaisen tiedon käsittely tai säilytys EU/ETA alueella. Tämä onkin konkreettisin vaade pilvipalveluiden käyttöön liittyen. Tulee siis voida osoittaa se, että tällaista tietoa käsitellään tietyllä maantieteellisellä alueella. Ja toisaalta tiedon siirtäminen tältä alueelta muualle ei pitäisi tapahtua ilman täällä olevaa toimijaa ja EU tuomioistuinten päätösten (Schrems 2) perusteella ei esim. amer. lainsäädäntö (saati kiinalainen tai venäläinen) tarjoa tarpeen hyvää tietosuojaa ja siksi tällaista tietoa ei pitäisi sinne siirtää. Merkittävää on, että EU parlamentin asetuksen mukaan jäsenvaltiot eivät voi vaatia muuta kuin henkilötietoa säilytettäväksi tietyllä maantieteellisellä alueella.

Kotimainen lainsäädäntö ja alakohtaiset erityisvaatimukset ottavat kantaa myös monin paikoin henkilötiedon säilytysaikoihin ja niitä tulee tietysti noudattaa ratkaisusta huolimatta. Henkilötietoja käsiteltäessä on myös syytä kiinnittää huomiota käytännesääntöihin, ja EU onkin julkaissut omat ohjeistuksensa pilvipalveluiden käytänteisiin liittyen.

Kuten EU on myös kotimainen julkishallinto luonut kirjavan kokoelman erilaista ohjeistusta pilvipalveluihin liittyen. Yhteisenä teemana voi kuitenkin nimetä sen, että pilvipalveluiden käytölle esitellään edellytyksiä, jotka on syytä täyttää. Edellytetään mm. vaikutustenarviointia, Roolien ja vastuiden dokumentointia sekä mahdollista kolmansien maiden lainsäädännön vaikutusten analysointia. Pääasiassa siis edellytetään järkeviä toimenpiteitä, joita on syytä miettiä osana päätösprosessia - muutenkin kuin vain julkishallinnossa. Turvaluokiteltujen asiakirjojen käsittelykin on mahdollista pilvipalveluissa tietyin reunaehdoin (Lähinnä alimmat turvaluokat).

Erilaisia arviointikriteeristöjä on olemassa turvallisuuden arviointia tukemaan - näistä on hyvä muistaa se että ne eivät ole suoraan velvoittavia, vaan ajatuksena on se että niistä valitaan ne kohdat, joita kulloinkin tulee noudattaa - velvoittavia

niistä tulee vasta kun sopimuksilla tietyn kriteerin täyttymisestä sovitaan.

EU:n alati kehittyvä ohjaus ja sitä myötä viiveellä kehittyvä kotimainen lainsäädäntö tulee myös myllertämään kenttää lähitulevaisuudessa. Tässä kirjoituksessa on siis huomioitu nykyistä tilannetta. Ja on mahdollista, että esim. EU:n suvereniteettipyrkimykset tuottavat entistä rajaavampaa ohjausta - siitä huolimatta eurooppalainen tai kotimainen pilvi ovat varmasti varteenotettavia vaihtoehtoja, jos vakavasti otettavia sellaisia saadaan tarjolle amerikkalaisten jo vakiintuneiden rinnalle/sijaan.

Summa summarum

Liiketoiminnan jatkuvuudesta huolehtimisen, kriiseihin varautumisen ja huoltovarmuuden näkökulmasta suunnitellulla päätöksentekoprosessilla on paikkansa, jotta tehdään kestävää liiketoimintaa joka osaltaan edistää huoltovarmuutta. Tiedonhallinnassa pilvipalveluilla on selkeitä etuja verrattuna perinteisiin konesaleihin. Organisaatioiden päätöksenteko siitä, millaisiin pilvipalveluihin siirtyä ja miten, ja laajentaako pilvipalvelujen käyttöä kriittisiin toimintoihin, ei kuitenkaan ole helppoa.

Päätöksenteon tueksi Huoltovarmuusorganisaation Digipooli on julkaissut ohjeistuksen, joka sisältää “Tunnista ja turvaa” -korttipakan, joka auttaa pilvipalveluihin siirtymisen päätöksenteossa ja ohjaa prosessissa huomioimaan oleellisia aiheita, joita tämäkin kirjoitus avaa. Korttipakan käytön avulla voidaan varmistua siitä, että päätökset pohjautuvat tietoon ja että jatkuvuudenhallinnan sekä huoltovarmuuden tekijät on huomioitu.

Oppaassa ja korttipakassa on hyvät ja perusteelliset ohjeet ja vinkit niiden käytölle. Ne kuvaavat pilvipalveluihin siirtymisen päätösprosessin vaiheet ja kussakin vaiheessa tarvittavat tiedot, tehtävät ja roolit. Niitä käyttämällä yritys tai muu organisaatio pystyy huomioimaan jatkuvuudenhallinnan ja huoltovarmuuden päätöksenteossaan riippumatta siitä, päätyykö se pilvipalveluihin vai ei.

Usein yrityksissä päädytään hybridimalliin, jossa on käytössä niin pilvipalveluita kuin oma IT-ympäristö sen tukena. Ja yhä useammin omassa konesalissa käytetään pilviteknologioita perinteisten teknologioiden sijaan

Tutustu lisää aiheeseen ja em. materiaaliin päätöksenteon tukevoittamiseksi vaikka www.digipooli.fi verkkosivun kautta.

Jani Isohanni on Digian Defence-liiketoiminnan pääarkkitehti. Hänellä on pitkä kokemus ICT-teknologista, kokonaisarkkitehtuurista ja tutkimustyöstä. Isohanni on koulutukseltaan tekniikan lisensiaatti.

TEKSTI: JANI ISOHANNI

Kvanttilaskenta

Artikkelissa käydään lyhyesti läpi kvanttilaskennan luonne sekä pohditaan sen tuomia mahdollisuuksia ja uhkia. Näkökulma on tietoturvassa sekä sodankäynnin kehittymisen visiossa.

Teoriataustaa

Nykyisten digitaalisten tietokoneiden perusta on luotu jo 1900-luvun alkupuolella. Tuolloin formaalin matematiikan kehittyessä kehiteltiin erilaisia laskennan malleja, jotka toimivat nykyisten transistoripohjaisten koneiden arkkitehtuurin perusteina. Tietokonehan oli tuohon aikaan tuntematon käsite ja kyseessä oli enemmän laskennan mekaanisen tekemisen automatisointi, sekä osaltaan myös formaalin matematiikan luonti, joka palautuu tietyiltä osin pitkälti edelliseen.

Tuolloisista laskennan formalisoinneista ehkä tunnetuimmat ovat Markovin algoritmit, Lambda-kalkyyli sekä ehkä eniten tunnettuutta kerännyt Turingin kehittämä Turingin kone. Myöhemmin on osoitettu, että ilmaisuvoimaltaan nämä kaikki ovat sinänsä yhteneviä eli kaikilla voidaan laskea samat asiat. Eli kun rakennetaan Turingin kone mihin tahansa tarkoitukseen, voidaan se toteuttaa myös Lambda-kalkyylissä sekä Markovin algoritmeilla, sekä toisin päin.

Monesti mielenkiinnon kohde on kuitenkin enemmän siinä, miten nopeasti haluttu asia voidaan laskea. Nykyiset erilaiset mallit ovat siinä mielessä kaikki samanlaisia, ettei niistä yksikään voi tarjota oleellisesti nopeampaa tapaa tehdä laskentaa kuin muut. Käytännössä kaikki kutakuinkin järjellisesti rakennetut koneistot voidaan palauttaa toisiin vastaaviin korkeintaan ns. polynomiaikaisella palautuksella eli ilman merkittävää hidastumista (tai nopeutumista).

Kvanttitietokoneet ovat kuitenkin haastamassa tilanteen ennennäkemättömällä tavalla.

Kvanttikoneet

Perinteisessä tietokoneessa kaikki laskenta palautuu lopulta pienen pieniin bitti-tason operaatioihin, joita nykyiset prosessorit jauhavat käsittämättömällä nopeudella. Tietokoneiden prosessori, eli laskennan juhta, sekä muisti on rakennettu takomaan yksinkertaisia operaatioita. Niiden todellisuudessa yksittäinen bitti on joko 1 tai 0, ja jokaisen laskutoimituksen tulos on bittejä/tavuja, jotka määräytyvät täysin syötteistä.

Kvanttikoneissa bitti korvautuu käsitteellä kubitti. Kun perinteinen bitti on joko 1 tai 0 eikä mitään muuta, niin kubitti voi olla 1 tai 0 tai niiden superpositio. Tässä superposition voi ajatella olevan tietynlainen todennäköisyys sille, luetaanko kubitti ykköseksi vai nollaksi. Erityistä on, että yksittäisen kubitin superpositio voi vaikuttaa toisen kubitin superpositioon välittömästi. Taustalla oleva fysiikka on siis hyvin erilaista kuin mihin perinteisessä tietokonemaailmassa on totuttu ja laskennan formalisointi vaatii uuden lähestymistavan.

Yksinkertaistamalla kokonaisuutta, voidaan ajatella, että kvanttikoneiden tehokkuus nousee pitkälti niiden kyvystä tehdä laskentaa tietyssä mielessä rinnakkaisesti mainittujen vuorovaikutusten kautta. Jos ajatellaan perinteistä tietokonetta, niin jokainen ohjelmointia tehnyt tiedostaa prosessin käsitteen ja miten prosessia ajetaan aina lähtökohtaisesti yhdellä prosessorilla. Suoritus on puhtaasti sekventiaalista eli jonomaista, ja yhdestä tilasta mennään laskennan kautta toiseen tilaan. Kvanttikoneiden sisäinen maailma on erilaista ja niiden voi ajatella laskevan useita tiloja ”samaan aikaan”. Tämä kyvykkyys tuo nopeusetua.

Algoritmien aikavaativuudesta

Näyttäisi, että kvanttitietokoneet tulevat ainakin alkuun olemaan ylivertaisia sellaisten ongelmien kanssa, joissa on selvä maltillisen kokoinen syöte ja siitä laskettava vastaus, jossa laskenta vie aikaa eli laskettava ongelma on vaikea.

Jotta saisimme kiinni konkreettisista tapauksista, on määriteltävä laskennan ”vaikeus”. Laskennan vaativuusteoriassa on luotu koneisto, jolla voidaan arvioida varsin hyvin, minkälaiset ongelmat ovat tietokoneille vaikeita ratkaista eli mihin ongelmiin menee laskenta-aikaa paljon.

Laskentaa ajatellaan mallina, jossa tietokone ottaa vastaan luvun ja tulostaa vastauksena luvun. Koneen (oikeastaan algoritmin) laskennasta seurataan laskutoimitusten lukumäärää suhteessa

syötteen pituuteen. Ei siis arvoon vaan merkkijonon eli luvun pituuteen. Tällä määritelmällä voidaan luokitella ongelmia erilaisiin vaativuusluokkiin.

Tässä yhteydessä riittää tieto, että jos ongelma voidaan perinteisillä laskennan keinoilla (footnote: Kvanttimaailmassa määritelmät ovat erilaiset, mutta ajattelutapa on vastaava.) ratkaista ajassa, joka on polynominen suhteessa syötteen pituuteen, niin se on käytännössä laskettavissa. Tällöin sanotaan, että ongelman aikavaativuusluokka on P. Jos ongelma ratkeaisi lineaarisessa ajassa (eli todella nopeasti), se kuuluisi luokkaan LIN. Koska lineaarisessa ajassa ratkeavat ongelmat ratkeavat nopeammin kuin polynomisessa ajassa, niin huomataan, että jokainen LIN-luokan ongelma on itse asiassa myös luokassa P ja vastaavasti kaikissa muissakin luokissa, jotka ovat LIN-luokkaa vaikeammin laskettavia.

Monesti on verrattain suoraviivaista löytää ongelmalle aikavaativuusluokka, jossa se on. Haaste onkin, että on hankalaa osoittaa, etteikö sitä voisi ratkaista nopeamminkin. Haaste seuraa sinänsä määritelmää, koska aikavaativuus määritellään ongelman ratkaisevalle algoritmille eikä itse ongelmalle. Joten jos halutaan osoittaa, etteikö nopeampaa toteutusta ole olemassa, joudutaan pureutumaan itse ongelman luonteeseen hyvin syvällisesti.

Tämä tilanne tulee kiusallisen vahvasti esiin aikavaativuusluokan NP tapauksessa. NP koostuu karkeasti ottaen ongelmista, joihin olemassa oleva vastauskandidaatin oikeellisuus voidaan tarkistaa polynomisessa ajassa, mutta tuon kandidaatin löytymiseen ei tunneta polynomista menetelmää, vaan algoritmit ovat käytännössä aikavaativuudeltaan eksponentiaalisia tai ainakin lähellä sitä. Ratkaisun löytäminen on siis vaikeaa. Suoraan määritelmistä tiedetään, että P kuuluu NP:hen, mutta yksi kuumista perunoista on ollut jo vuosikymmeniä onko P=NP.

Luokka NP on mielenkiintoinen, koska nykyinen käsitys on, ettei siihen kuuluviin ongelmiin voida kehittää nykyisillä tietokoneilla nopeita algoritmeja. Tosin kukaan ei ole voinut osoittaa asiaa suuntaan tai toiseen. NP sisältää monia ongelmia, joihin haluttaisiin löytää nopea algoritmi, mutta siinä ei siis ole onnistuttu.

Kvanttitietokoneiden suorituskyky

Kvanttitietokoneiden vahvuus on (karkeasti yleistäen) ”arvata” oikea vastaus, minkä jälkeen jäljelle jää vain vastauksen todentaminen. Tämä tarkoittaa, että kvanttialgoritmit ovat ainakin tietyissä ongelmissa lähestulkoon eksponentiaalisesti nopeampia kuin nykyiset algoritmit.

Tilanne on herkullinen, koska tämä mahdollistaisi monen käytännön ongelman ratkaisemisen nopeasti. Yhtenä yleisenä esimerkkinä on ns. kauppamatkustajan ongelma, jossa pyritän etsimään kauppamatkustajalle nopein reitti annetussa ympäristössä. Ongelma on kuuluisa NP-luokan ns. täydellinen ongelma ja se yleistyy varsin suoraviivaisesti esimerkiksi logistiikan ketjujen optimointiin.

Toinen jokapäiväinen esimerkki on luentokalenterin järjestäminen niin, että opiskelijoille tulee annetuilla esiehdoilla mahdollisimman vähän konflikteja. Tämäkin yleistyy aika suoraviivaisesti muihin vastaaviin optimointiongelmiin.

Suorituskyvyn nousu tuo myös ongelmia. Esimerkiksi monen salausalgoritmin turvallisuus perustuu olettamukseen, että niiden pohjalla olevat algoritmit ovat sellaisia, ettei niitä voi murtaa polynomisessa ajassa. Konkreettisemmin moni salausalgoritmi perustuu olettamukseen, että esim. diskreettiä logaritmia tai kokonaisluvun tekijöitä ei voitaisi laskea polynomisessa ajassa eli tehokkaasti suurilla syötteillä. Tämä olettama on pitänyt paikkansa vuosikymmeniä, mutta kvanttitietokoneiden myötä tilanne saattaa muuttua.

Eri yhteisöt ovat kuitenkin hereillä ja esim. kevään 2023 NATO ACT:n TIDE-sprintissä(footnote: ACT (Allied Command Transformation) on NATO:n elin, joka vastaa osaltaan jatkuvasta kehittämisestä. TIDE (Think-Tank for Information Decision and Execution) on ACT:n organisoima think-tank konferenssi, jossa kehitystyön suuntia luodaan ja määritellään.) mm. DCS-track (Data Centric Security) mietti, milloin aletaan vaatia kvanttikestäviä algoritmeja. Myös itse algoritmeja on kehitteillä jo useampaankin tarkoitukseen. Lisätietoja löytyy post-quantum cryptography hakusanoilla.

Yhdysvalloissa NIST julkaisi syksyllä 2022 kuusivuotisen kilpailun jälkeen valitsemansa algoritmit, joihin nojaten kvanttikestävää salausta kehitetään. Yleiskäyttöiseksi algoritmiksi valikoitui CRYSTALS-Kyber ja digitaaliseen allekirjoittamiseen kolmikko CRYSTALS-Dilithium, FALCON ja SPHINCS+. Algoritmit ovat perusideoiltaan hyvin erilaisia kuin nykyiset ja tämä työ onkin osaltaan kesken. Aihepiiri on kiivaan tutkimuksen kohteena.

Myös NIST on perehtynyt asiaan ja on julkaissut taulukon (footnote: NIST Internal Report (NISTIR) 8105, Report on Post-Quantum Cryptography), jossa arvioidaan erilaisten kryptografisten algoritmien kohtaloa, jos kvanttilaskenta mahdollistuu.

Perinteiset laskentamallit

On hyvä myös tiedostaa, että on tilanteita, joissa kvanttitietokoneiden ei uskota olevan haastajia nykyisille teknologioille. Yhtenä esimerkkinä on isojen datamassojen läpikäynti ja analysointi. Tämä johtuu siitä, että tiedon vieminen kvanttikoneeseen on ainakin tällä hetkellä sekin operaatio itsessään. Näyttäisi siis, että mitä pienempi syöte ja mitä vaikeampi laskutoimitus, niin sitä paremmin kvanttilaskennan hyödyt tulevat esiin, ja päinvastoin. Ainakin teknologian kehityksen alkuvaiheessa.

Hieman ehkä yllättäväkin suunta on, että kvanttilaskennan algoritmien kehittämisen yhteydessä on jouduttu ajattelemaan ja mallintamaan asioita täysin uudella tavalla. Tämä älyllinen haastaminen on tuonut mukanaan uusia oivalluksia myös nykyisten algoritmien kehittämiseen. Puhutaan ”quantum-inspired”- algoritmeista, joissa toteutukseen on saatu uusia ideoita pohtimalla toteutusta kvanttilaskennan kautta.

Kvanttisoftaa ja -rautaa

Ensimmäiset ajatukset kvanttilaskennasta syntyivät luultavasti samoihin aikoihin, kun kvanttimekaniikka ja laskennan teoria alkoivat löytää toisensa. 1980-luvun alkupuolella Paul Beinoff esitteli ajatuksen kvanttilaskennan mekaanisesta toteutuksesta ja hieman myöhemmin Richard Feynmann esitteli ajatuksia fysiikan simuloinnista kvanttikoneilla.

Peter Shor esitteli 1994 ensimmäisen konkreettisen kvanttilaskennan algoritmin kokonaisluvun jakamiseksi tekijöihinsä, joka tunnetaankin Shorin algoritmina. Algoritmi esittää periaatteen, miten kokonaisluvun voi jakaa tekijöihin ja se tarjoaa merkittävästi nopeamman tavan kuin perinteiset menetelmät eli siinä kvanttimaailman tehokkuushyöty todentuu. Tämä aiheutti tuolloin pientä kuohuntaa tiedepiireissä ja antoi buustia alalle, mutta tieteelle tyypillisesti kehitys jatkui hiljalleen ilman suurelle yleisölle tuotuja läpimurtoja.

Perinteisiä algoritmeja oleellisesti tehokkaampia kvanttialgoritmeja ei ole

juurikaan julkaistu intensiivisestä tutkimuksesta huolimatta. Aiemmin mainitun Shorin algoritmin ohella Groverin algoritmi, vuonna 1996 julkaistu hakualgoritmi, on yksi verrattain harvoja, joka tarjoaa aidon nopeushyödyn. Joskin senkin tuoma hyöty on maltillinen eikä sen uskota tarjoava varsinaista läpimurtoa nykyisiin vaikeisiin ongelmiin tai esim. salausjärjestelmiin, koska nopeutus on matalaa polynomista tasoa.

Viime vuosina rautapuolen kehitys näyttää ottaneen isohkoja askelia. Esimerkkeinä Googlen 72-kubittinen Bristlecone, IBM:n 52-kubittinen IBM Q3 ja Rigettin 80-kubittinen Aspen-M-3. Ohjelmistopuolella Microsoft on kehittänyt Q#-kielen, joka on luotu kvanttialgoritmien kehittämiseen. Näiden teknologiajättien rinnalla on ilo huomata, että meillä on myös kotimaista yrittäjyyttä kuten viime aikoina julkisuutta saanut IQM sekä hieman tuoreempi ohjelmistopuolen toimija Quanscient.

Tiedon salaus

Turvallinen ja toimiva viestintä on yksi sodankäynnin peruspilareita. Viestin pitää paitsi olla oikeasisältöinen, niin myös saavuttaa oikea vastaanottaja turvallisesti. Turvallisuuden yksi oleellinen tekijä on viestin salaaminen siirtokerroksessa. Kvanttilaskennan myötä siirtokerroksen salausalgoritmien vaihtaminen kvanttikestäväksi tulee ajankohtaiseksi ennemmin tai myöhemmin. Nykyinen kehitys kvanttikestävien algoritmien kanssa onneksi tarjoaa jokseenkin varmasti tähän ratkaisut. Koska salausratkaisut ovat usein varsin läpinäkyviä loppukäyttäjälle, on teknisesti oletettavaa, että osaava ylläpito huolehtii itsenäisesti teknologian asianmukaisesta päivittämisestä kestäväksi.

Viestiliikenteen salaaminen on kuitenkin siinä mielessä erityinen käyttötapaus, että viestin sisällön turvaluokitus voi laskea ja usein laskeekin varsin nopeasti ajan myötä. Tänään salainen operaation aloitustieto saattaa muuttua julkiseksi sillä hetkellä, kun lähtökäskyt on jaettu. Tämä tarkoittaa, että viestiliikenteen salauksen pitää olla sellaista, jonka purkaminen reaaliajassa ei ole mahdollista ja toisaalta liikenne itsessään on pääsääntöisesti sellaista, että sen purkaminen viiveellä ei tuo enää lisäarvoa.

Tilanne on kuitenkin tyystin eri sellaisen datan kanssa, jonka turvaluokitus on korkea huomattavasti pidemmällä aikajänteellä. Nykypäivänä parhaimmilla mahdollisille keinoilla salattu materiaali voi olla avattavissa kvanttiajan myötä varsin helposti. Jos informaatio on sellaista, jolla on korkea turvaluokitus myös tulevaisuudessa, niin sen salaaminen tänään toimivalla algoritmilla ei siis välttämättä varmista sen salauksen kestoa huomenna.

Tilanne onkin johtanut siihen, että on tahoja, jotka keräävät salattua dataa, jota nykyisellään ei saada purettua. Ajatus on, että teknologian kehitys on niin nopeaa, kohta salaus onkin purettavissa. Tämä ilmiötä kutsutaan monessa yhteydessä ”Harvest now – decrypt later” (”HNDL”)-teoriaksi. Tilanne on ainakin jossain määrin ongelmallinen, koska se heikentää yhtä tietoturvan kerrosta kohtalaisen paljon ja siihen ei ole tänä päivänä suoraa ratkaisua tarjolla.

Positiivisena puolena on, että hyvä tietoturva on kerrosteista ja ylipäätään paikalla olevaan salattuun tietoon pääseminen on tehty muilla arkkitehtuurillisilla ratkaisuilla monesti todella vaikeaksi. Liikkuvan datan kanssa tilanne on kuitenkin eri. Esimerkiksi internetissä liikkuva salattu tieto on kohtalaisella vaivalla vihamielisen tahon tallennettavissa ja sitä kautta myös kerättävissä. Tämän takia voi olla aiheellista muun jatkuvan riskiarvioinnin kyljessä pohtia, minkälaista tietoa missäkin verkossa halutaan liikutella.

Sodankäynnin nopeus

Edellä mainittiin kvanttikoneiden mahdolliseksi sovellutuskohteeksi tiettyjen optimointiongelmien nopea suorittaminen. Jos tämä toteutuu, moni logistinen ongelma muuttuu siinä mielessä helpoksi, että niihin voidaan löytää nopeasti paras mahdollinen ratkaisu. Käytännön elämässä tämä tarkoittaa, että esimerkiksi moni logistinen järjestely voidaan optimoida paremmin kuin nykyään. Jos tätä optimointia päästään toteuttamaan läpi koko toiminnan, tuo se parhaimmillaan nopeusetua varsin moneen asiaan ja sitä kautta mahdollistaa mahdollisesti huomattavastikin nopeamman operoinnin kuin nykyisellään on mahdollista.

Vastaavasti hetkessä tehtäviin päätöksiin voidaan muotoilla etukäteen ratkaisusapluunoita tai malleja, joiden avulla voidaan laskea ja arvioida tilanne ja päätösten vaikutus huomattavasti nykyistä nopeammin ja tarkemmin. Tämä helpottaa päätöksentekoa ja vähentää johdon kognitiivista kuormaa.

Edelliset kohdat yhdessä tarjoavat työkalut, joilla voidaan nopeuttaa OODA-luuppia kokonaisuudessaan ja tuoda sitä kautta parempi tilannetieto päätöksenteon tueksi sekä mahdollistaa nopeampi reagointi muuttuneeseen tilanteeseen. Nämä visiot yhdistettynä tekoälyn mahdollisuuksiin päätöksenteon tukena saattavat luoda sotakoneiston, jossa päätöksenteon taajuus voi jopa nousta ihmiselle hallitsemattomaksi. Tilanne voi haastaa sodankäynnin perusparadigmoja moninaisilla tavoilla.

OODA-luuppi.

Lopuksi

Tulevaisuuden ennustaminen on vaikeaa ja artikkelia varten tehdyn selvittelyn jälkeen näyttäisi, ettei suuriin läpimurtoihin ainakaan lähivuosina uskota. Teknologiassa on vielä valtavasti ratkottavia asioita ja myös ohjelmistokerros tulee luultavasti elämään ja kehittymään useammankin kerran ennen varsinaista maailmanvalloitusta. Tämä tuo sinänsä levollisen mielen uhkakuvien osalta, mutta jättää samalla useita hyödyllisiä sovellutuskohteita odottamaan tulevia läpimurtoja.

Joka tapauksessa hereillä on oltava, ja ollaankin.

Kirjoittaja palvelee Puolustusvoimien johtamisjärjestelmäkeskuksessa Johtamisjärjestelmäkoululla täydennyskoulutusosaston johtajana. Artikkelin kirjoittamiseen ja rakentamiseen on osallistunut myös muita koulun henkilökuntaan kuuluvia, jotka eivät tässä halua esiintyä nimellään.

TEKSTI: JUHA LEPPÄNEN

Kyberpuolustus täydennyskoulutuksen näkökulmasta

Kyberpuolustus on ajankohtainen ja näkyvä aihe niin Puolustusvoimissa sisäisesti kuin mediassakin. Kyberin koulutus on kehittynyt viime vuosina Suomessa ja kansainvälisestikin. Kyberopetusta tarjoaa jo yhä useampi oppilaitos sekä palveluntuottaja koulutusohjelmissaan. Tässä artikkelissa tarkastellaan Puolustusvoimien johtamisjärjestelmäkeskuksen johtamisjärjestelmäkoulun tarjoamaa kyberpuolustuksen täydennyskoulutusta ja sen tavoitetilaa sekä askelia toiminnan kehittymisestä tähän päivään. Samassa yhteydessä avataan myös hiukan Johtamisjärjestelmäkoulun täydennyskoulutuksen filosofiaa, pedagogisia ratkaisuja ja -ajatuksia, koko koulutustarjontaa ja sen tavoitetilaa. Johtamisjärjestelmä- ja informaatiopuolustuksen ulottuvuudet toimivat samassa kybertoimintaympäristössä omaten vahvoja liitoksia keskenään. Huomioitavaa on, että esitelty koulutuksen tavoitetila on suunnitelma, joka on jo koulun aloittamisesta 2022 vuoden alusta päivittynyt sekä kehittynyt useampaan kertaan.

Koulutustoiminnan käynnistäminen ja kehittyminen

Kyberpuolustuksen täydennyskoulutus voidaan katsoa alkaneen Maasotakoulun Viestikoululla ennen vuotta 2010. Tällöin terminologiassa käytettiin toki enemmän ”tietoturva” termiä aiheesta. Samoihin aikoihin järjestettiin verkkosodankäynti -nimettyjä sotaharjoituksia. Tietoturva-termillä koulutusta tarjottiin koko puolustusvoimallisesti täydennyskoulutuksen osalta ja verkkosodankäynti-termiä taas käytettiin enemmän henkilökunnan virkaurakursseilla järjestetyissä koulutuksissa sekä sotaharjoituksissa. Voidaan siis todeta, että vaikkakin ”kyber” terminä on trendinä koulutuspuolellakin, samaa aihepiiriä ja toimintaympäristöä on koulutettu jo noin 15 vuoden ajan Puolustusvoimissa. Tilanne on siis sama kuin muualla yhteiskunnassa, jossa myös opetuksessa ilmentynyt tietoturva-termi on ajan kuluessa useassa opetustapahtumassa tai ohjelmassa muutettu kyber-termiksi. Tietoturvallisuutta ja sen koulutusta tietysti tehdään edelleen, mutta sen rinnalle on voimakkaasti noussut kyberturvallisuus ja -puolustus osana tietoturvallisuuden kenttää. Koulutuksen näkökulmasta tarkasteltunakin pelikenttä on laaja ja välillä näkemykset ja käsitykset tietoturvallisuuden sekä kyberturvallisuuden määritelmistäkin ovat erilaisia.

Kybereksperimenttiympäristön hankinta aloitettiin Viestikoululla vuonna 2018 opetustoiminnan tarpeisiin. Tarkoitus oli, että ympäristö tukisi täydennyskoulutusta ja se poistaisi tarpeen rakentaa erillinen koulutusympäristö aina erikseen jokaiseen koulutustapahtumaan. Henkilöresurssit tämän työn edistämiseksi olivat aluksi rajalliset. Kyberkoulutusympäristön kehittämiseen erikseen korvamerkittyä henkilöstöresurssia ei ollut, vaan määrittely- ja kehitystyö tapahtui projektiin osallistuvien henkilöiden muiden tehtävien ohella. Vuosien saatossa ”kyber” nimikkeellä olevia tehtäviä perustettiin ja henkilöitä saatiin rekrytoitua, jolloin koulutusympäristön kehittäminen ja täydennyskoulutustapahtumien suunnittelu lähti etenemään vauhdilla. Viestikoululla järjestettiin ensimmäiset valtakunnalliset ”Kyberpuolustuksen perusteet” -opetustilaisuudet. Tilaisuuksien tarkoitus oli lisätä ymmärrystä kyberpuolustuksesta.

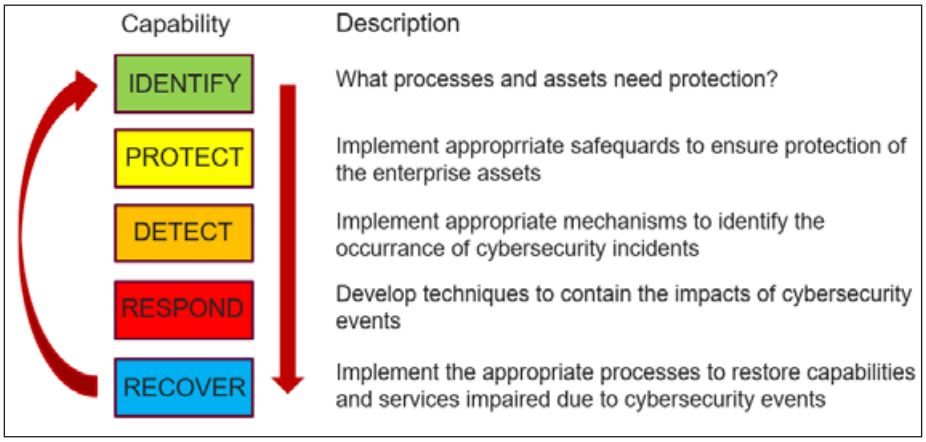
Vuosina 2019 ja 2020 Puolustusvoimien kybertoiminta kehittyi edelleen ja alkoi muodostua konkretiaksi. Tällöin toiminnalle alkoi muodostua selkeitä vaatimuksia ja nykyinen täydennyskoulutuksen kehitys sai alkunsa. Vuonna 2021 järjestettiin ensimmäiset kyberin täydennyskoulutustapahtumat Viestikoulun ja Johtamisjärjestelmäkoulun rungon henkilöstön voimin. Osassa opetustilaisuuksia käytössä oli kehitystyön tuloksena ollut kybereksperimentti- ja koulutusympäristö. Tilaisuuksista saatiin arvokkaat ensimmäiset kokemukset ja ennen kaikkea hyvää palautetta opiskelijoiden suunnasta. Tämä ei tullut ilmaiseksi. Toiminnan kehittämiseen ja eksperimentointiin osallistunut henkilöstö joutui työskentelemään lujasti, jotta uudet, myös opettajia haastavat opetustilaisuudet opetusmateriaaleineen ja -ympäristöineen saatiin ”opetuskelpoiselle” tasolle.

Kyberpuolustuksen täydennyskoulutus Johtamisjärjestelmäkoululla

Johtamisjärjestelmäkoulu perustettiin vuoden 2022 alusta, jolloin myös kyberpuolustuksen täydennyskoulutusvastuu siirtyi koululle. Haasteena heti alkuun osoittautui, että osa koulun rungon aikaisesta henkilöstöstä siirtyi toisiin tehtäviin. Rekrytointihaasteista johtuen tilaisuuksia jouduttiin siirtämään ja perumaan. Kehitystyö ja yhteistoiminta verkostojen kanssa lähti etenemään verkkaisesti, toki tätä työtä oli tehty jo paljon vuoden 2021 aikana osana koulun rungon valmistelua. Haasteista huolimatta toiminta kehittyi ja kyberopetuskokonaisuuden jäsentäminen edistyi.

Kyberin täydennyskoulutuksen kohderyhmänä on pääosin Puolustusvoimien henkilöstö. Myös Rajavartiolaitoksen ja yhteistyökumppaneiden opiskelijoita valitaan tilaisuuksiin tapauskohtaisesti. Opetustilaisuudet ja verkkokurssit muodostavat opintopolkuja, joilla pyritään tukemaan eri tehtävissä vaadittavaa osaamista. Toki opinnot myös itsenäisinä suoritteina tukevat osaamisen kehittymistä (kts. kuva 2).

NIST (National Institute of Standards and Technology) Cybersecurity framework (kuva 1 alla) valikoitui kyberpuolustuksen täydennyskoulutuksen opetustilaisuuksien näkökulman ja rakenteiden lähtökohdaksi. NIST Frameworkin avulla jäsennettiin tilaisuuksien aiheet, rajaus, sisällöt ja tavoitteet.



NIST Cybersecurity framework (tunnista, suojaa, havainnoi, reagoi/vastaa, palaudu)

Pedagoginen näkökulma

Kyberpuolustuksen täydennyskoulutuksessa huomioidaan täysin samat nykyaikaiset pedagogiset ratkaisut kuin minkä tahansa muun aihealueen opetuksessa. Johtamisjärjestelmäkoululla on pyritty sen perustamisesta asti ajattelemaan koulutuksesta innovoivasti ja uusia nykyaikaisia ratkaisuja sekä teknologioita opetuksessa mahdollisuuksien mukaan hyödyntäen.

Ajasta ja paikasta riippumaton verkossa tapahtuva itseopiskelu on nykyaikaa ja vastaa erityisesti kiireisten aikuisopiskelijoiden tarpeisiin. Kuitenkaan kaikkia aiheita ei pysty eikä ole järkevää tuottaa verkkokursseina. Sisällöllisesti laadukkaitten verkkokurssien tuottaminen pedagoginen näkökulma huomioiden on hyvin työlästä ja pitkäjänteistä työtä, mutta tämän onnistuessa säästetään opettajien työaikaa muihin aiheisiin ja samalla tuetaan suuremman opiskelijajoukon osaamisen kehittymistä. Opiskelijamäärä on myös yksi laadun mittari arvioitaessa toimintaa.

Johtamisjärjestelmäkoulun aloittamisesta asti on ollut selvää, että verkkokurssien tuottamisella mahdollistetaan perustason osaamisen kehittämistä. Vaaditut perusteet -tason verkkokurssit suorittanut opiskelija myös varmistaa niin itselleen kuin koululle, että esitietovaatimukset muihin täydennyskoulutustapahtumiin täyttyvät. Verkkokursseilla pyritään osaltaan myös varmistamaan pohjatietojen ja osaamisen taso, jonka johdosta lähiopetustapahtumaan saapuva opiskelijajoukko on osaamiseltaan ja lähtökohdiltaan suhteellisen tasainen ja näin ollen mahdollistaa laadukkaan ja sujuvan lähiopetuksen.

Verkkokurssit ymmärretään usein terminologisesti rajattuna itseopiskelukursseina. Näin ei välttämättä tarvitse olla, vaan verkkokurssi voi sisältää myös ”live” verkko-opetusta, ryhmätöitä tai opetuskeskusteluita. Verkkokurssi voidaan liittää myös osaksi lähiopetusta. Verkko-opetus taas on verkon yli tai verkossa tapahtuvaa opetusta, johon voidaan liittää esimerkiksi itseopiskelua tai ryhmätöitä. Verkko-opetuksella on myös sijansa kyberpuolustuksen täydennyskoulutuksessa, varsinkin seminaari- tai luentotyyppisten lyhyiden opetustilaisuuksien tai ajankohtaiskatsausten osalta.

Verkkokurssit tai verkko-opetus ei kuitenkaan sinällään korvaa laadukasta lähiopetusta, jossa opettajan ja oppilaan välinen vuorovaikutus sekä oppilasjoukon verkostoituminen nousee arvoonsa. Verkossa tapahtuvalla opiskelulla on paikkansa, mutta kaikkiin aiheisiin ja osaamisen tavoitetasoihin se ei sovellu. Lähiopetus fyysisessä tuotannon kaltaisessa koulutusympäristössä käsinkosketeltavissa olevilla laitteilla on optimitilanne pedagogisesta näkökulmasta ja työtehtäviin tuotettavan osaamisen kannalta. Kuitenkin virtualisoinnin ja simuloinnin hyödyntäminen myös opetuksessa on nykyaikaa ja se tulee huomioida mahdollisuutena, kun koulutusympäristöjä kehitetään. Fyysisten ympäristöjen osalta tulee aina mietittäväksi elinkaari, ylläpito ja rahoitus. Virtualisoinnilla ja simuloinnilla luodaan edullisempia, ketterämpiä ja dynaamisempia koulutusympäristöjä. Osaltaan kyberpuolustuksen kehittämisessä tulisi tarkastella kokeilu- ja kehittämisympäristöjen yhteensopivuus sekä mahdollisuudet myös koulutukseen.

Koulutussisällöt

Ajallisesti Johtamisjärjestelmäkoulun kyberpuolustuksen täydennyskoulutustapahtumat kestävät noin 2-5 työpäivää, verkkokurssien osalta tietysti opiskelijan ehdoilla. Täydennyskoulutuksessa jaetaan osaamispisteitä ja viikon opetustilaisuudesta ansaitsee noin yhden osaamispisteen (OSP).

Seuraavissa kappaleissa on esitelty kuvan 2 mukainen koulutuskokonaisuus ja opintopolut. Huomioitavaa on, että myös kuvan 3 mukaisen opetustarjonnan kokonaisuus tukee kyberopintoja suorittavan opiskelijan osaamistarpeita.

Kyberpuolustuksen perusteet -verkkokurssi suoritetaan Moodle-alustalla.

Verkkokurssi koostuu Jyväskylän yliopiston ”Kansalaisen kyberturvallisuus” -osiosta ja Puolustusvoimien näkökulmaa sekä toimintaa käsittelevästä osiosta. Kurssilla käsitellään kybertoimintaympäristöä, kyberturvallisuutta, kyberpuolustusta osana kansallista kyberturvallisuutta sekä kyberpuolustuksen eri osa-alueita (tiedustelu, suojautuminen ja vaikuttaminen). Verkkokurssi on tarkoitettu kaikille Puolustusvoimien työntekijöille. Kurssin avulla on mahdollisuus ottaa ”startti” ja perusteet haltuun kyberin maailmaan. Kurssin tavoitteena on, että opiskelija ymmärtää perusteet kybertoimintaympäristön rakenteista ja ilmiöistä, ymmärtää kyberpuolustuksen merkityksen osana kansallista kyberturvallisuutta sekä tuntee kyberpuolustuksen osana sotilaallisen suorituskyvyn rakentamista ja käyttöä.

Teknisen kyberpuolustuksen perusteet -verkkokurssilla tuetaan opiskelijoita, jotka tarvitsevat syvällisempää ymmärrystä muun muassa verkkojen tietoturvallisuudesta ja suojaamisesta. Verkkokurssi antaa perusteita kybertoimintaympäristöön teknisestä näkökulmasta NIST Cybersecurity framework -taustaan peilaten. Verkkokurssin tuottaminen on vielä käynnissä, eikä se ole vielä koulutustarjonnassa.

Kybersietoisuuden huomioiminen hankkeissa -opetustilaisuudessa tunnistetaan kehitettävän suorituskyvyn ja sen tunnistettujen uhkien kautta suorituskyvyn kybertoimintaympäristö ja tehdään ympäristölle uhkamallinnus sekä riskiarvio. Näin tunnistetaan suorituskykyyn kohdistetut kybersietoisuuden vaatimukset suuremmasta vaatimusmassasta ja opetetaan niiden asettaminen.

Tekninen kyberpuolustus -opetustilaisuudessa kuvataan konkreettisesti kybertoimintaympäristöä, käsitellään siellä tapahtuvia ilmiöitä, verkon aktiivilaitteita ja ohjelmistoja. Lisäksi tilaisuudessa käsitellään, mitä teknisiä ratkaisuja tulee ottaa huomioon verkkoympäristöjä suojatessa kybervaikuttamiselta tai -tiedustelulta. Tietoverkkojen tietoturva on opetustilaisuuden keskeistä sisältöä. Tavoitteena on, että opiskelija tuntee tietojärjestelmien ja verkkojen kybertapahtumien valvonnan perusteet, tuntee tietoverkon turvallisuuden parantamiseen liittyvät keskeiset turvallisuuskontrollit ja tietää perustoimenpiteet tietoverkon turvallisuuden parantamiseksi. Lisäksi tavoitteena on ymmärtää, kuinka erilaisia haavoittuvuuksia on mahdollista käyttää hyväksi tietoverkkoihin tunkeuduttaessa ja miten tietoverkon aktiivilaitteet ja palvelut on mahdollista selvittää ja kartoittaa.

Kuva 2: Johtamisjärjestelmäkoulun kyberkoulutustarjonta tavoitetilassa (vrt. kuva 3)

Lokienhallintaopetustilaisuus tarjoaa osaltaan perusteita valvomotoimintaan. Opetustilaisuudessa käsitellään, miten lokienhallinta voidaan toteuttaa sekä miten sitä ylläpidetään ja edelleen kehitetään. Kybervalvomo-opetustilaisuudessa taas käsitellään valvomon eri toiminteita niin käytäntöjen kuin tekniikankin näkökulmasta. Aiheina ovat kybervalvontaan liittyvät yleiset prosessit ja työkalut teknisestä sekä toiminnallisesta näkökulmasta. Tavoitteena on, että opiskelijat tuntevat kybervalvonnan, lainsäädännön, toiminnallisuuksien, työkalujen ja organisoitumisen periaatteet.

Haasteita kyberpuolustuksen täydennyskoulutuksessa

Minkä tahansa organisaation kyberturvallisuuteen liittyvää täydennyskoulutusjärjestelmää tai -ohjelmaa rakennettaessa, edessä on kaksi suurta haastetta. Ensimmäinen haaste on ymmärtää organisaatiossa tarvittava osaaminen. Organisaation kybertoimintaympäristö, toiminnot ja toimintatavat muuttuvat jatkuvasti teknisten muutosten, uusien hankintojen (tekniset ratkaisut, palvelut jne.) sekä teknologisen ja vastustajan kehityksen takia. Tämä aiheuttaa organisaatioille haasteita määrittää miten kyberpuolustusta tai -turvallisuutta tulee tehdä, millaisia tehtäviä ja rooleja organisaatiossa tähän liittyen tulee olla ja mitä osaamista eri tehtävissä ja rooleissa tarvitaan.

Toisena haasteena on pula osaajista. International Information System Security Certification Consortiumin (ISC2) tekemän tutkimuksen (viite (ISC2) CYBERSECURITY WORKFORCE STUDY 2022) mukaan kansainvälinen kyberturvallisuusalan henkilöstö oli vuonna 2022 kaikkien aikojen suurimmillaan (4.7 milj. ammattilaista). Siitä huolimatta, että alalle oli tullut vuodessa 464 000 uutta työntekijää, tutkimuksen mukaan alalle tarvitaan vielä 3.4 miljoonaa lisää. Yrityksistä 70% ilmoitti, että heillä ei ole tarpeeksi alan työntekijöitä.

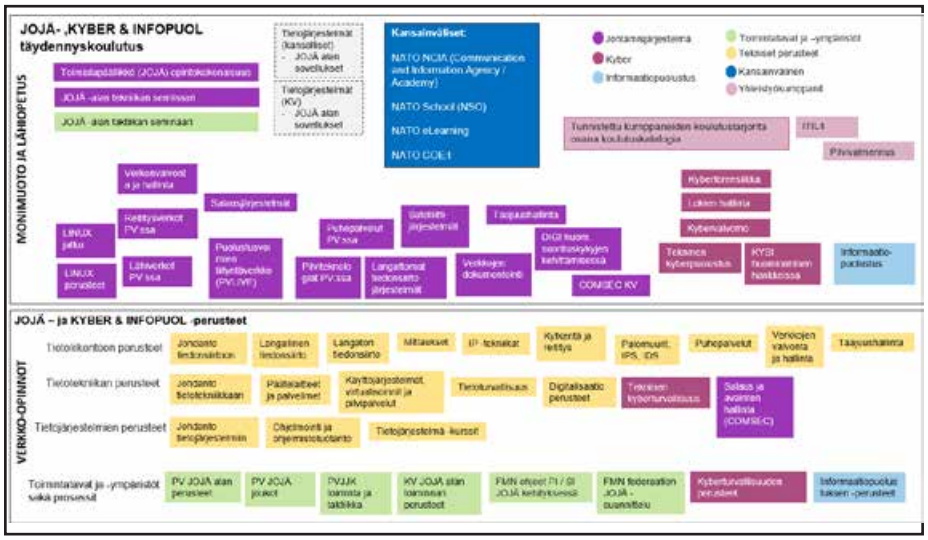
Tämä tarkoittaa sitä, että alalle pyrkii ja alalla on hyvin eri taustoilla ja osaamisella varustettua henkilöstöä. Miten luodaan koulutusohjelma tai yksilölle opintopolku, jos erilaisia osaamisprofiileja on paljon ja henkilöstö vaihtuu usein? Miten nämä eri osaamisprofiilit ylipäätään tunnistetaan ja huomioidaan luotaessa järjestelmää tai yksittäistä opetustilaisuutta?

Johtamisjärjestelmäkoulu pyrkii vastaamaan näihin haasteisiin kyberkoulutuksen osalta toiminnallisesta näkökulmasta. Täydennyskoulutuksen tuottama osaaminen liittyy kyberpuolustuksen suorituskykyjen rakentamiseen tai käyttöön. Opiskelijan ymmärtäessä suorituskykyjen toiminnallisuuksia ja toiminnan tavoitteita organisaatiossa paremmin, hän kykenee itsenäisesti hankkimaan- ja kehittämään osaamistaan tehtävänsä sekä roolinsa mukaisesti.

Täydennyskoulutuksen tavoitetila

Tavoitetilassa täydennyskoulutus tuottaa oppilaille tietoja, taitoja, kykyjä ja ymmärryksen kyberpuolustuksen toiminnallisuuksista ja sen tavoitteista. Osa koulttautumismahdollisuuksista tuotetaan itse ja osa hankintaan ulkopuolelta. Johtamisjärjestelmäkoulu voidaan nähdä tavoitetilassa alustana, jolla on itse tuotettuja palveluita sekä sen kautta käytettäviä tai rakennettuja palveluita.

Varsinaiset kyberpuolustuksen opetustapahtumat ovat ylläolevassa kuvassa vaaraimen punaisella värillä. Huomioitavaa on kuitenkin, kuten jo aiemminkin mainittu, että myös ”perusteet” opintojen verkkokurssit ja myös muut johtamisjärjestelmäalan opetustilaisuudet ilman ”kyber” termiäkin muodostavat osaltaan esitietovaatimuksia ja ovat näin ollen kiinteä osa ”kyberistinkin” opintopolkuja. Kybertoimintaympäristön tuntemus on yhtä kuin johtamisjärjestelmän tunteminen. Yllä olevassa kuvassa esitetyn koulutustarjonnan sisällössä on jo muutostarpeita, esimerkiksi kansainväliseen toimintaan liittyvien koulutusten osalta. Muutoksia ja päivityksiä on jo tehtykin koulun lyhyen historian aikana.



Kuva 3: Johtamisjärjestelmäkoulun koulutustarjonta tavoitetilassa.

Tulevaisuuden näkymiä ja mahdollisuuksia

Johtamisjärjestelmäkoulun toiminnassa on alusta alkaen korostunut verkostoituminen. Täydennyskoulutuksen näkökulmasta on yritetty tunnistaa yhteistyökumppanit, muut viranomaiset ja palveluntuottajat, joiden kanssa yhteistoiminta olisi kannattavaa, tarpeellista sekä kustannustehokasta. Kaikkea ei kannata ja pidä tehdä itse tai yksin, jos valmista tai yhteisiä intressejä on jo olemassa. Tähän yhteistoimintaan liittyy myös vahvasti koulutusympäristöt ja niiden kehittäminen.

Kansainväliset koulut, muun muassa Nato School Saksassa ja Nato Communications & Information Agency (NCIA) Portugalissa tarjoavat laajasti myös kyberiin liittyvää täydennyskoulutusta. Kansainvälinen koulutus ja verkostoituminen on myös isossa roolissa koulun henkilöstön kybertaitojen kehittämisessä. Koulun henkilökuntaa on koulutettu jo useilla edellä mainittujen Naton koulutusorganisaatioiden kursseilla ja hyväksi havaitut kurssit pyritään sisällyttämään jatkossakin osaksi uusien työntekijöiden perehdyttämistä sekä osaamisen kehittämistä. Näiden kurssien sisältö nähdään myös osana Johtamisjärjestelmäkoulun kyberpuolustuksen täydennyskoulutus mahdollisuuksien markkinointia.

Esimerkiksi Nato School -kurssi ”Network Vulnerability Assessment & Risk Mitigation” -kurssin kesto on 10 viikkoa sisältäen lähi- ja etäopintoja. Opetustapahtuma on Nato School Oberammergaussa olevan neljän kyberturvallisuuskurssin muodostaman kokonaisuuden toinen kurssi. Kaikki neljä kurssia ovat 10 viikkoa kestoltaan. Kurssi keskittyy tietoliikenteeseen ja tietotekniikkaan liittyvien haavoittuvuuksien esittelyyn, niiden tunnistamiseen ja arviointiin sekä niiden käytön estämiseen tai vaikutuksien lieventämiseen. Käytännössä siis aiemmin esitetyn NIST frameworkin vaiheisiin. Kurssilla hyödynnetään useita erillisiä sähköisiä ympäristöjä, -kirjoja ja -palveluita. Opiskelijat, jotka pääsevät läpi kurssista, saavat vielä mahdollisuuden osallistua Certified Ethical Hacker -kokeeseen ja näin saavuttaa kansainvälisesti tunnistetun sertifikaatin. Koko laajan kokonaisuuden neljä kurssia suorittaneet opiskelijat saavat mahdollisuuden ”Cyber Security Professional Programme” -sertifikaattiin. Kokemusten perusteella kurssit ovat osoittautuneet erittäin laadukkaiksi ja myös opiskelijaa haastaviksi.

Kurssissa on samoja elementtejä, kuin esimerkiksi kansallisessa täydennyskoulutuksessa tai Suomessa tarjolla olevissa kyberaihepiiriin liittyvissä sertifikaattikoulutuksissa. Vaikka edellä kuvattu koulutuskokonaisuus ei olekaan täysin verrattavissa kansalliseen täydennyskoulutukseen lähtökohdiltaan, kohderyhmältään ja tavoitteiltaan, herättää se kuitenkin paljon ajatuksia ja huomioita myös kansalliseen koulutukseen. Joka tapauksessa esimerkiksi kyseinen Nato School kyber-kurssikokonaisuus tulee nähdä osana kyberpuolustuksen täydennyskoulutustarjontaa. Johtamisjärjestelmäkoulun henkilöstö, joka näitä kursseja on käynyt, pystyy jo siirtämään ja jalkauttamaan osaamista koulun täydennyskoulutustilaisuuksissa edelleen eteenpäin.

Mahdollisuudet verkossa itseopiskeluna Naton eLearning (JADL) alustalla tai esimerkiksi TryHackMe.com -sivustolla tarjoavat laadukasta itseopiskelumateriaalia ja -kursseja moneen osaamistarpeeseen. Koulutuksen pelillistäminen on nykypäivää kaikilla opetustasoilla peruskoulusta aikuiskoulutukseen, TryHackMe.com -alusta on tästä hyvä esimerkki verkossa toteutettuna.

Tietyt koulutustarpeet, kuten esimerkiksi kyberanalyysi ja -forensiikka, ovat melko rajattua opiskelijajoukkoa koskeva aihe. Näin ollen olisikin mahdollisesti järkevää ja kustannustehokasta, että forensiikan parissa työskentelevät asiantuntijat eri hallinnon aloilta kootaan yhteen ja samaan tilaisuuteen jakamaan asiantuntijuuttaan toisilleen. Se, että kategorisoidaanko tämä enää täydennyskoulutukseen, on kysymys erikseen. Kyberanalyysi ja -forensiikka on vielä jäsentymätön kokonaisuus täydennyskoulutuksen näkökulmasta ja sen toteu-

tustapoja tulee vielä jatkossa pohtia sekä miettiä yhdessä eri toimijoiden kanssa.

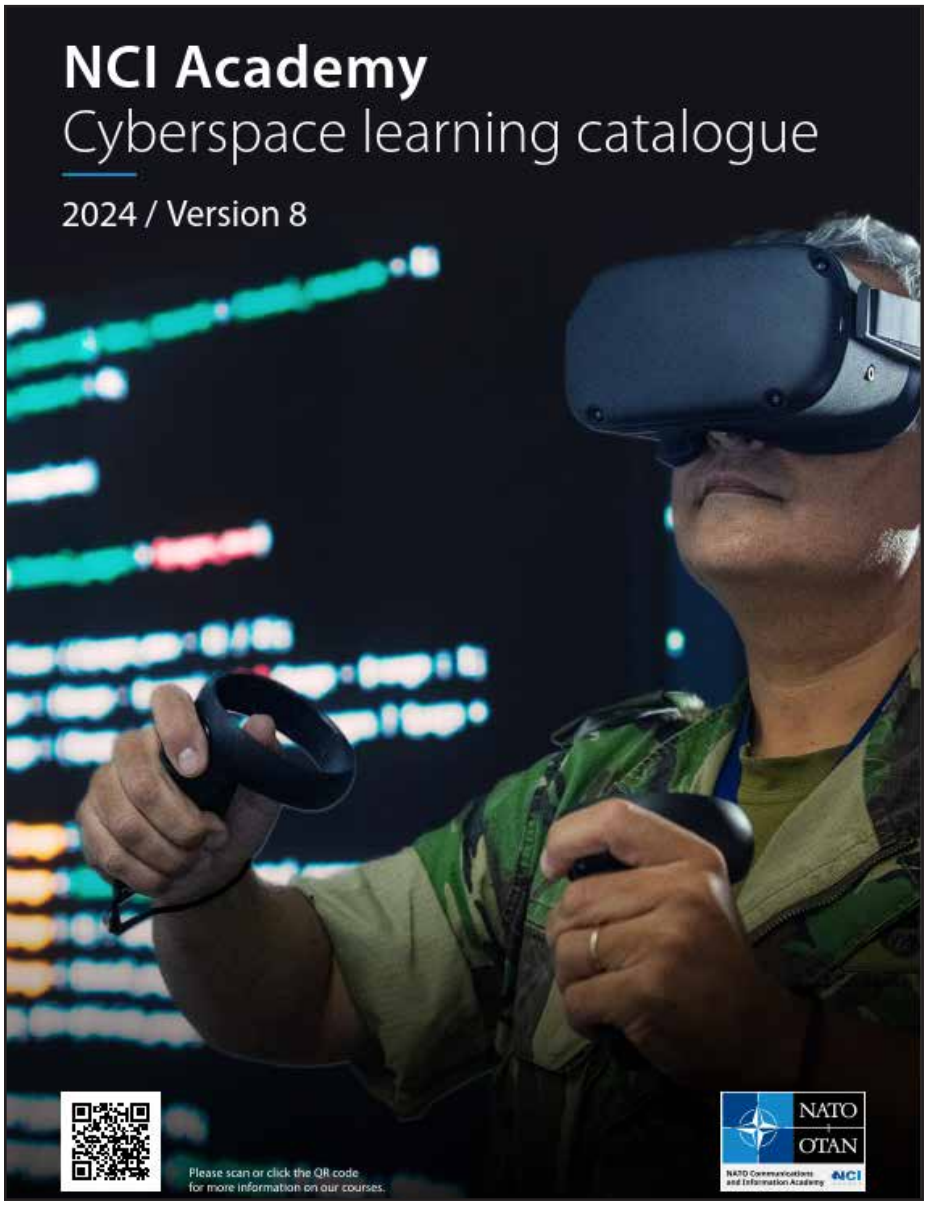
Johtamisjärjestelmäkoulun täydennyskoulutuksen yhtenä päätavoitteena on luoda selkeä ”opetustarjotin” opiskelijoille, jossa on kuvattu laadukas kyberkoulutustarjonta niin kansallisesti kuin kansainvälisestikin. Opetustarjotin, josta voidaan puhua myös koulutuskatalogina (kuten NCIA -koulutuskatalogi kuvassa), kokoaa Johtamisjärjestelmäkoulun oman koulutustarjonnan lisäksi verkostoitumisen ”hedelmät”, johon kuuluu palveluntuottajien ja yhteistyökumppaneiden koulutusmahdollisuudet kotimaassa, ulkomailla sekä verkossa. Opiskelijoille pyritään kuvaamaan lähtötasosta alkaen selkeitä opintopolkuja, joiden avulla voi kehittää osaamistaan aina huippuosaajaksi asti.

Yhteenvetona voisi todeta, että työtä on vielä paljon laadukkaan kyberkoulutustarjonnan mahdollistamiseksi ja jäsentämiseksi opiskelijalle selkeäksi kokonaisuudeksi. Opetustilaisuuksien järjestämisen toteutustavoissa riittää jatkuvasti arvioitavaa, mitä kannattaa kustannustehokkaasti tehdä itse ja mitä hankkia mahdollisesti muualta. Myös kyberpuolustuksen toiminnan- ja kyberkoulutusympäristöjen kehittyminen vaikuttaa suoraan täydennyskoulutuksen sisältöihin sekä opetustapoihin. Tärkeää onkin, että opetustehtävissä toimiva henkilöstö tekee koko ajan tiivistä yhteistyötä kehittämis- ja tutkimushenkilöstön kanssa opetusympäristöjen kehittämisen saralla. Varmaa on se, että kyberpuolustuksen teknisten ratkaisujen ja toimintatapojen kehittymisen myötä vaikutukset sekä kehittämistarpeet koulutuksessakin ovat jatkuvia.

Lopuksi voidaan todeta, että haasteista huolimatta kyberpuolustuksen täydennyskoulutustoiminta Johtamisjärjestelmäkoululla on käynnistetty ja pidetyistä opetustilaisuuksista on saatu erittäin hyvää palautetta. Verkostoituminen on jo tuottanut tuloksellista yhteistoimintaa ja yhteisiä intressejä eri toimijoiden kanssa on tunnistettu. Toiminta kehittyy vauhdilla suunnitelman mukaisesti kohti tavoitetilaansa.

VIITE artikkelissa mainittuun tutkimukseen:

https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196&hash=11E2B28C57ED8BC721CA3DC26A6C1A74



NCIA-koulutuskatalogin kansilehti (lähde: NCIA internetsivut)

FICEC johtaja FT Mika Karjalainen toimii vararehtorina Jyväskylän ammattikorkeakoulussa.

ST Martti Lehto toimii Jyväskylän yliopiston IT-tiedekunnassa kyberturvallisuuden työelämäprofessorina ja FICEC koordinaattorina.

TEKSTI: MIKA KARJALAINEN JA MARTTI LEHTO

Kyberturvallisuuden osaamiskeskittymä Jyväskylään

Jyväskylän yliopisto ja Jyväskylän ammattikorkeakoulu muodostivat maaliskuussa 2023 Suomen kyberosaamiskeskuksen (Finnish Center of Expertise for Cybersecurity, FICEC), jonka tarkoituksena on kyberturvallisuuden huippututkimuksen ja -osaamisen vahvistaminen sekä alueellisen elinvoiman lisääminen erityisesti Jyväskylässä ja Keski-Suomessa sekä laajemmin valtakunnallisesti.

Yhteiskunnan yksityiset ja julkiset palvelut perustuvat yhä laajemmin ihmisten, eri toimijoiden ja älykkäiden systeemien keskinäisriippuvaan digitaaliseen toimintaympäristöön. Digitaalitalouden kehitystä edistävät erilaisten palveluiden ja käytäntöjen digitalisoituminen ja siirtyminen verkkoon. Yhteiskunnan digitalisaatio on luonut kybertilan, jossa kriittinen infrastruktuuri tuottaa yhteiskunnan elintärkeät palvelut yhä laajemmin digitaalisesti. Tämä digitaalinen murros muuttaa tapaa, jolla palveluita ja hyvinvointia tuotetaan eli koko yhteiskunnan toimintalogiikka on muuttunut – kyber on kaikkialla.

Digitalisaatiokehitys lisää valtiollisten ja valtiosta riippumattomien toimijoiden mahdollisuuksia toteuttaa yhä kehittyneempiä kyberoperaatioita, joilla on sotilaallisia, poliittisia ja taloudellisia tavoitteita. Äärimmillään yhteiskunnan haavoittuvuuksia hyödynnetään kyberoperaatioissa kriittisen infrastruktuurin sabotoimiseen, lamauttamiseen ja tuhoamiseen.

Valtion kyberturvallisuusjohtajan johdolla laaditussa kyberturvallisuuden kehittämisohjelmassa (2021) määritetään keskeiset toimenpiteet kyberturvallisuuden parantamiseksi koko yhteiskunnassa. Siinä kuvataan kyberturvallisuuden kehittämisen lyhyen ja pitkän aikavälin tavoitteita (2021–2030) ja painopistealueita. Se vastuuttaa eri hallinnonaloja kyberturvallisuuden varautumisessa ja resilienssin vahvistamisessa. Periaatepäätöksen mukaan vahva kansallinen kyberturvallisuus edellyttää tarvittavaa osaamista ja laajaa osallistumista yhteiskunnan kaikilla eri tasoilla, tiivistä yhteistyötä erityisesti julkishallinnon ja elinkeinoelämän välillä, vahvaa kotimaista kyberturvallisuusteollisuutta, joka luo kyvykkyyksiä digitaalisen yhteiskunnan palveluiden turvaamiselle ja viranomaisten kyberturvallisuuskyvykkyyksiä, jotka luovat pohjaa koko yhteiskunnan turvalliselle toiminnalle.

Kyberturvallisuuden koulutustarpeita tutkittiin 2022

Osana kyberturvallisuuden kehittämisohjelmaa Jyväskylän yliopisto, Jyväskylän ammattikorkeakoulu ja Turun ammattikorkeakoulu selvittivät vuonna 2022 laaja-alaisesti kyberturvallisuuteen liittyvän osaamisen määrällistä ja laadullista kehittämistä perusopetuksessa, II asteen koulutuksessa sekä yliopistoissa ja ammattikorkeakouluissa. Tutkimuksessa tehtiin merkittäviä havaintoja ja esitettiin kehittämislinjauksia eri koulutusasteille.

Osaamisen määrätietoisen vahvistamisen avulla eri ikäluokat ja kansanosat luovat vankan perustan kyberturvallisuudelle. Lisäksi osaaminen mahdollistaa tarvittavien teknologisten kyberkyvykkyyksien rakentamisen niin viranomaisten kuin yritystenkin tarpeisiin. Siksi on syytä varmistaa, että tutkimuksen, kyberturvallisuutta valmistavan teollisuuden ja kyberturvallisuuden käyttäjäorganisaatioiden osaamistarpeet huomioidaan kaikilla osa-alueilla. Jatkuva vuoropuhelu työelämän kanssa osaamistarpeista on keino viestiä sisältötarpeista.

Tutkintoon johtava koulutus ei tuota riittävää osaamista alalla ja siksi on turvauduttava työssä oppimiseen ja täydennyskoulutukseen työvoiman osaamisen turvaamiseksi. On aivan selvää, että työelämässä on opittava uutta aiempaa no-

peammin, eikä kaikkia työelämätarpeita voida toteuttaa osana tutkintoon johtavaa koulutusta. Koulutusohjelmien kestot ovat pitkiä ja niiden muutostahti hidas. Jatkuvan oppimisen joustavat toteutusmuodot tulevat joka tapauksessa yleistymään kaikilla aloilla työelämän tarvitseman osaamisen tueksi.

Kansalaisten kybertaitojen parantaminen koulutuksen kautta on tärkeä tavoite, joka vahvistaa Suomea korkean koulutuksen ja osaamisen maana ja luo pohjan tulevaisuuden yhteiskunnalle. Elinkeinoelämää ja yhteiskuntaa tukevan tutkintopohjaisen koulutustarjonnan lisäksi tulee panostaa joustavaan täydennyskoulutukseen ja elinikäistä oppimista tukevaan kurssi- ja koulutustarjontaan.

Osaamispohjan vahvistaminen ja kyberturvallisuusteollisuuden toimintaedellytysten parantaminen ovat ensiarvoisen tärkeitä paitsi elinkeinopoliittisesti, myös kansallisen turvallisuuden näkökulmasta. Se tarkoittaa, että Suomessa tulee tehdä huomattavia lisäpanostuksia alan koulutuksen lisäämiseen, investointeihin sekä tutkimus- ja tuotekehityshankkeiden käynnistämiseen ja niiden tulosten markkinoille saamiseen. Osaajapula haittaa jo nykyisellään alan kehitystä ja yritysten menestymismahdollisuuksia. Isot teknologiamurrokset ja digitalisaatio tulevat entisestään kasvattamaan kyberturvallisuusalan osaamispulaa. Koulutusmahdollisuuksia tulee lisätä niin työelämässä kuin eri koulutusasteillakin.

Koulutukseen tehtävät muutokset ovat erittäin tärkeitä. Tarvetta on kyberturvallisuuden ammateissa toimiville, mutta yhtä tärkeää on varhaiskasvatuksesta lähtevän koulutuksen kautta varmistua siitä, että kaikki kansalaiset ymmärtävät kyberturvallisuuden perusteet ja työelämään siirtyvät tai työelämässä olevat kykenevät ymmärtämään kyberturvallisuuden vaatimukset oman työnsä kannalta - esim. palvelu- ja tuotekehitystehtävissä toimivan on tiedettävä, miten kyberturvallisuus tulee huomioida näissä kehitystehtävissä.

Tutkimus päätyi näkemykseen, jonka mukaan kansallisen kyberturvallisuuden huippuosaamisen kehittäminen edellyttää riittävän osaamiskeskittymän muodostumista. Tällaisen osaamiskeskittymän luominen edellyttää esitettyä laajaa kansallista ja kansainvälistä yhteistyötä. Kansainvälisen kilpailukyvyn saavuttaminen edellyttää, että saamme Suomeen korkeatasoisia opiskelijoita, tutkijoita ja alan asiantuntijoita. Kyberturvallisuuden kehittämisen kannalta on välttämätöntä, että Suomi on houkutteleva kohde kansainvälisille asiantuntijoille.

Vasemmalta:FICEC johtaja FT Mika Karjalainen, JAMK vararehtori,Työelämäprofessori ST Martti Lehto, FICEC JYU koordinaattori, Keski-Suomen maakuntajohtaja Pekka Hokkanen puhumassa, JYU vararehtori Henrik Kunttu, JAMK rehtori Vesa Saarikoski.

Osaamiskeskuksen taustalla vahva kyberturvallisuusosaaminen Jyväskylässä

Jyväskylä on ollut pitkään kyberturvallisuuden tutkimuksen ja koulutuksen edelläkävijä Suomessa.

Jyväskylän yliopiston kyberturvallisuuden profiloituminen aloitettiin vuonna 2009 ja alan opetus alkoi 2011. Vuodesta 2015 käynnistyneestä kyberturvallisuuden maisteriohjelmasta valmistuu vuosittain 25–30 maisteria ja kyberturvallisuuden tohtoreita valmistuu vuosittain 5–10. Yliopiston laaja-alaisen ja monitieteisen kyberturvallisuuden huippututkimuksen aloja ovat mm. kriittisen infrastruktuurin suojaaminen, kyberturvallisuuden johtaminen, kyberturvallisuuskäyttäytyminen, kyberturvallisuuden teknologiset ratkaisut sekä kyberrikollisuus ja kyberpuolustus.

Jyväskylän ammattikorkeakoulussa voi suorittaa kyberturvallisuuden AMK-insinöörin ja YAMK-insinöörin tutkinnon. AMK-tutkinto-ohjelmissa on tarjolla 200 ja YAMK-tutkinto-ohjelmissa 70 aloituspaikkaa. Lisäksi avoimessa ammattikorkeakoulussa tarjotaan kyberturvallisuuden opintokokonaisuutta. JYVSECTEC (Jyväskylä Security Technology) on JAMK:iin kuuluva kyberturvallisuuteen ja tekoälykehitykseen keskittynyt tutkimus-, koulutus- ja kehityskeskus ja se tarjoaa kyberturvallisuuskoulutuksia ja -harjoituksia yrityksille ja julkisille toimijoille. JYVSECTEC on kehittänyt Suomen kansallisen Cyber Range -kyberharjoitusympäristön ja on järjestänyt vuodesta 2013 kansallisia kyberturvallisuusharjoituksia (turvallisuusviranomaiset, valtionhallinto, terveydenhuolto sekä kuntasektori ja kriittinen infrastruktuuri).

Jyväskylään on muodostunut 10 vuoden aikana kansallisesti ainutlaatuinen ja kansainvälisesti merkittävä kyberturvallisuuden ekosysteemi, johon kuuluu korkeakoulujen lisäksi lukuisa joukko alan yrityksiä ja julkisia toimijoita. Viime vuosien aikana usea yritys on perustanut toimipaikan Jyvässeudulle. Julkisia toimijoita ovat mm. Puolustusvoimien johtamisjärjestelmäkeskuksen kyberosasto, Puolustusvoimien tiedustelulaitoksen yksikkö, Ilmavoimien esikunta, Ilmasotakoulu sekä Erillisverkot ja Valtori.

Osaamiskeskus vahvistaa kansallisia tavoitteita

Suomen kyberosaamiskeskuksen visiona on kehittyä huippuluokan kansainväliseksi kyberturvallisuuden tutkimus- ja koulutuskeskukseksi, joka vahvistaa alueen ja koko Suomen kyberturvallisuusbrändiä. Jyväskylän yliopiston ja Jyväskylän ammattikorkeakoulun perustama osaamiskeskus ei ole itsenäinen oikeushenkilö, vaan se on sopijapuolten ja toimintaan mahdollisesti myöhemmin mukaan liittyvien organisaatioiden muodostama vapaaehtoinen yhteistyömuoto.

Osaamiskeskuksen tehtävä on kyberturvallisuuden huippututkimuksen ja -osaamisen vahvistaminen sekä alueellisen elinvoiman lisääminen Jyväskylässä ja Keski-Suomessa. Osaamiskeskuksessa

yhdistyy vahva yhteistyö elinkeinoelämän ja muun yhteiskunnan kanssa, kyky uusimman teknologian soveltamiseen sekä organisaatioiden vahva sitoutuminen toimintaan. Osaamiskeskuksen toiminnalla luodaan tulevaisuuden osaamista ja kestäviä ratkaisuja yhteiskunnan kyberturvallisuuden haasteisiin niin julkisella kuin yksityisellä sektorilla sekä edistetään alueen taloudellista kasvua kehittämällä uusia liiketoimintamahdollisuuksia.

Osaamiskeskus tuottaa monenlaisia asiakaslähtöisiä koulutus- ja kehittämispalveluja (jatkuvaan oppimiseen MOOC-verkkokoulutusta, lyhytkursseja, seminaareja/webinaareja, Round Table -tilaisuuksia, Studia generalia -luentoja) kansallisille ja kansainvälisille yleisölle. Se yhdistää monialaista tutkimusosaamista aivan uudella ja innovatiivisella tavalla, jonka avulla voidaan tehokkaasti ja nopeasti tuottaa yrityksille ja julkisille toimijoille niiden tarvitsemaa tietoa ja osaamista.

Akateemisen verkostoitumisen avulla järjestetään alan kansainvälisten huippuosaajien vierailuja, seminaareja ja tieteellisiä konferensseja, sekä kiinteä yhteistoiminta tutkija- ja opiskelijavaihtoineen tärkeimpiin alan kansainvälisiin yliopistoihin ja korkeakouluihin. Tämä kytkee Suomen alan parhaaseen osaamisen maailmalla ja hankittu osaaminen ankkuroidaan Suomeen. Näin osaamiskeskus luo edellytyksiä vahvan ja vetovoimaisen kansallisen kyberturvallisuuden ekosysteemin vahvistumiselle Jyväskylän seudulle.

Kyberosaamiskeskuksen road-map 2023–2024

Koulutus

Kyberosaamisen tarjonnan kartoitus kytketään OKM:n rahoittamaan kyberosaamisverkostohankkeeseen, joissa kehitetään sekä yliopistojen että ammattikorkeakoulujen tarjontaan soveltuvia kyberturvallisuuden osaamisen kehittämisen sisältöjä.

Yritysverkoston tarpeiden kartoittaminen ja yhteistyömuotojen määrittely.

Tutkimus ja tieteelliset konferenssit

Vuonna 2024 toteutetaan Digiturvallisuuden messut yhteistyössä Jyväskylän messujen kanssa ja kaksi kyberturvallisuuteen liittyvä akateemista konferenssia.

Tutkimusohjelman rakentaminen ja tutkimusjulkaisujen alustan kehittäminen omalle julkaisusarjalle.

Yhteiskunnallinen vaikuttaminen

Osaamiskeskuksen viestintäsuunnitelman laatiminen ja oman kotisivun rakentaminen.

Vaikuttajaverkoston luominen.

Osaamiskeskuksen podcast-ohjelmakonseptin edelleen kehittäminen.

Kumppanuustoiminta

Ohjaus- ja sidosryhmätoiminnan luominen ja vakiinnuttaminen osaksi osaamiskeskuksen toimintaa.

Kumppanuusverkoston luominen ja sen toiminnan etablointi osaksi osaamiskeskuksen toimintaa.

Osaamiskeskuksen kehitystoiminnassa on tunnistettu, että kyberturvallisuuteen tähtäävän tutkimuksen, kehittämisen ja koulutuksen toteuttaminen eri tasoilla vahvistaa kansallista osaamista ja Suomea tietoyhteiskuntana. EU-tasolla ja kansallisesti on julkaistu useita strategioita, joiden tavoitteena on parantaa kyberturvallisuuden osaamista sekä luoda edellytyksiä alan tutkimukselle, koulutukselle ja innovaatiotoiminnalle.

Jyväskylä koordinoi kansallisen kyberturvallisuuskoulutusverkoston kehittämistä

Merkittävä askel kyberturvallisuuden kehitystyössä otettiin loppuvuodesta 2022, kun tiede- ja kulttuuriministeri Petri Honkonen päätti myöntää Jyväskylän yliopistolle ja Jyväskylän ammattikorkeakoululle noin 3,4 miljoonan euron rahoituksen kyberturvallisuusalan koulutuksen kehittämiseen sekä informaatiopsykologisen turvallisuuden tutkimuksen ja opetuksen lisäämiseen.

Aikaisemmat tutkimuksen ovat osoittaneet, että kyberturvallisuusalan osaajapula on merkittävä. Erityisosaajien määrää voidaan tehokkaasti lisätä kehittämällä olemassa olevaa opetusta, luomalla niistä opintokokonaisuuksia yli korkeakoulurajojen ja avaamalla opetussisällöt mahdollisimman laajaan käyttöön.

Käynnissä oleva OKM:n rahoittama hanke edistää Valtioneuvoston koulutuspoliittisen selonteon tavoitteita, jonka mukaan “Suomen yhteiskunnan ja hyvinvoinnin kehittyminen edellyttää, että osaamistaso nousee ja erityisesti huippuosaaminen vahvistuu.” Lisäksi OKM:n Korkeakoulutuksen ja tutkimuksen visio 2030 -työssä linjattiin, että Suomi tarvitsee nykyistä enemmän osaajia, korkealaatuista korkeakoulutusta sekä tutkimus- ja innovaatiotoimintaa, ja myös vahvaa kytkeytymistä muualla tuotettuun uuteen tietoon.

Hankkeessa kootaan kyberturvallisuusalan korkeakoulutusta tutkimusperusteisesti kehittävä, koordinoiva ja tarjoava verkosto, jonka avulla pystytään vahvistamaan ja laajentamaan Suomessa tarjottavaa kyberturvallisuuden koulutusta. Ensisijaisena tavoitteena on varmistaa laaja-alainen ja jatkuva kyberturvallisuuden erityisosaamisen koulutus. Jyväskylän yliopisto koordinoi yhdeksän yliopiston verkostoa ja Jyväskylän ammattikorkeakoulu vastaavasti 11 ammattikorkeakoulun verkostoa. Kehittämistyössä on vahvasti mukana tekniikan alan verkostoyliopisto FITech (Finnish Institute of Technology).

Hankkeessa tuotetaan ja jaetaan kyberturvallisuuden opetusta verkoston kautta. Kehittämisen painopiste on kyberturvallisuuden erityisosaamisen vahvistamisessa. Lisäksi pyritään varmistamaan riittävä taso kyberturvallisuuden perusosaamisessa laaja-alaisesti korkeakouluopiskelijoille.

Hanke vastaa kyberturvallisuuden osaajapulaan ja nostaa koulutustasoa kehittämällä alan opetusta, tekemällä yhteistyötä korkeakoulujen välillä sekä tuottamalla kyberturvallisuutta laajasti kattavia opintokokonaisuuksia. Opetusta avataan myös työelämässä jo oleville.

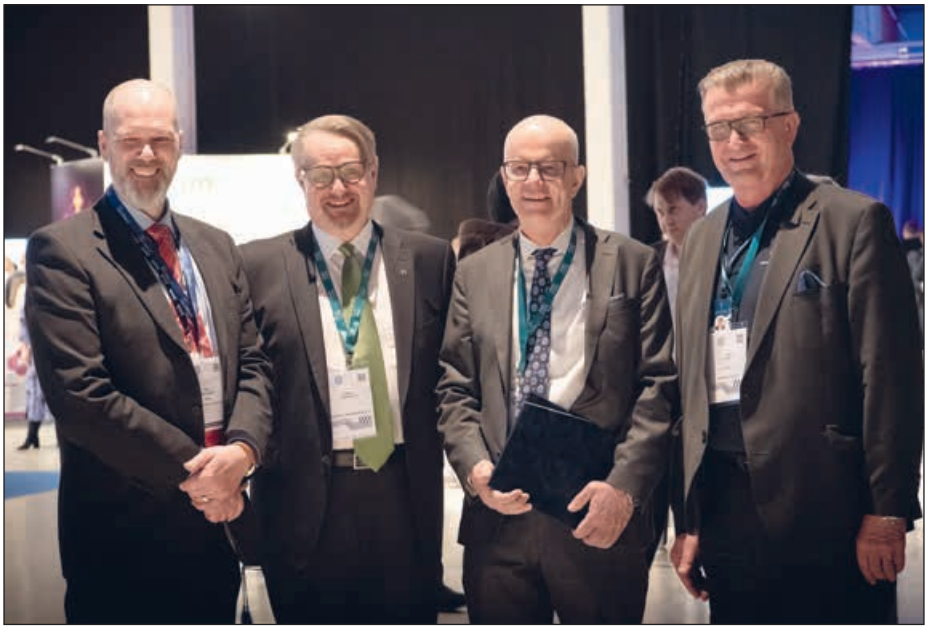
Opetusta kehitetään muodostettavan koulutusverkoston yhteistyönä. Työssä painotetaan kyberturvallisuuden alueita, joilla on kriittistä koulutuskysyntää ja työllistytään hyvin, keskeisenä tavoitteena erityisosaajien lisääminen. Hanke tuottaa perusosaamista lisääviä alempaan korkeakoulututkintoon sopivia kursseja ja erityisosaamista palvelevia ylempään korkeakoulututkinnon kursseja. Avointen verkkokurssien avulla tavoitetaan laaja-alaisesti eri opiskelijaryhmiä yli yliopistorajojen sekä työelämässä jo työskenteleviä.

Lisäksi hankkeessa vahvistetaan yliopistojen opetusyhteistyötä ja vuorovaikutusta teollisuuden ja julkisen sektorin kanssa, jotta voidaan kehittää alan tutkinto-opetusta ja jo työelämässä olevien kyberturvallisuusosaamista.

Hanke tuottaa kyberturvallisuuden perusosaamista suurelle määrälle opiskelijoita sekä lisää valmistuvien erityisosaajien määrää. Tähän päästään lisäämällä koulutustarjontaa sekä määrällisesti että laadullisesti. Perusosaamista parannetaan luomalla opetusta, joka skaalautuu suu-

relle määrälle opiskelijoita ja jota jaetaan verkossa tai kampuksella useille korkeakouluille sekä elinikäisille oppijoille. Kyberturvallisuuden erityisosaajien määrää yhteiskunnassa lisätään tarjoamalla opintokokonaisuuksia, jotka koostuvat usean yliopiston ja ammattikorkeakoulun kursseista. Opetusresursseja käytetään tehokkaasti selvittämällä todelliset koulutustarpeet ja koordinoimalla opetustarjontaa yhdessä korkeakoulujen välillä.

Hankkeessa kehitetty opetus ja menetelmät vakiinnutetaan osaksi korkeakoulujen normaalia toimintaa ja opiskelijoiden arkea. Kyberturvallisuuden koulutusverkostoa ylläpidetään jatkossa hankkeessa kehitetyn mallin mukaisesti. Hankkeessa syntyy pysyviä opetusyhteistyön muotoja.



Yhdessä enemmän

Kyberturvallisuuden osaamiselle ja opetukselle on nykyistä enemmän tarvetta, eikä opetuksessa ole riittävästi korkeakoulujen välistä yhteistyötä. Opetuksessa on nykyisellään mahdollisia päällekkäisyyksiä. Vaikka yliopistot ja ammattikorkeakoulut ovat rekrytoineet alan opettajia ja tutkijoita, yksittäisillä toimijoilla ei ole riittäviä resursseja kasvattaa merkittävästi kyberturvallisuuden opetusta. Osaamiskeskus vahvistaa kansallista kyberturvallisuuden osaamispääomaa ja tukee omalta osaltaan pääministeri Petteri Orpon hallitusohjelman tavoitetta, jonka mukaa suomalainen kyber- ja informaatioturvallisuusosaaminen varmistetaan panostamalla alan koulutukseen.

Pääministeri Sanna Marinin asettaman parlamentaarisen TKI-työryhmän raportin mukaisesti Suomen tavoitteena on nostaa T&K- menot neljään prosenttiin suhteessa bruttokansantuotteeseen vuoteen 2030 mennessä. Aikaisempi kehitys on pudottanut T&K- menot vuodesta 2009 vuoteen 2019 3,7 prosentista 2,8 prosenttiin. Asetettu tavoite on siis merkittävä käännös kansallisessa T&K panostuksessa, ja tarkoittaa käytännössä valtiolta noin 200 M€, sekä yrityksiltä noin 400 M€ vuosittaista lisäystä T&K-menoihin 2030 vuoteen saakka. Parlamentaarinen TKI- työryhmä on lisäksi esittänyt tohtorikoulutettujen vuosittaisen koulutusmäärien nostamista. Mahdollisen tohtorien koulutusmäärien noston yhteydessä tulisi erityisesti pohtia työ-/elinkeinoelämälähtöisen tohtorikoulutuksen kehittämistä, jolla vastattaisiin erityisesti teknologia-alan yhä nopeampaan teknologian kehitykseen, korkeampiin osaamistavoitteisiin ja tuettaisiin yrityksissä tapahtuvaa T&K- työtä. Näiden mahdollisuuksien toteuttamiseksi FICEC yhdistää Jyväskylän yliopiston ja Jyväskylän ammattikorkeakoulun voimavaroja erityisesti kyberturvallisuuden T&K- työn volyymin ja tulosten nostamiseksi. Yhdessä toimien osaamiskeskittymällä on myös nykyistä parempia mahdollisuuksia kotiuttaa T&K- rahoitusta mm. Eurooppalaisista tutkimusohjelmista, kuten Horizon-, European Defence Fund- ohjelmat. Huomioitavaa on, että myös NATO-jäsenyys avaa uusia ovia tutkimusyhteistyössä.

Käynnissä oleva korkeakoulujen Digivisio 2030 –hankkeessa kaikki suomalaiset korkeakoulut rakentavat yhdessä oppimiselle tulevaisuutta. Tavoitteena on oppimisen uusi aikakausi, jonka ytimessä on digipedagogiikan jatkuva kehittäminen ja jossa jokainen meistä voi helpommin oppia ja kerryttää osaamistaan muuttuvassa maailmassa. Huippuosaamista ylläpidetään kansainvälisen tason tutkimuksella.

Suomen kyberosaamiskeskus vahvistaa kansallista kyberturvallisuutta tuomalla laajasti yhteen eri toimijoita korkeakoulusektorilta, julkishallinnosta ja yrityssektorilta. Yhteistyön avulla voidaan tarjota innovatiivisia kyberturvallisuusratkaisuja alan teollisuudelle, joka vahvistaa niiden kyberturvallisuusvalmiuksia.

Osaamiskeskus yhdistää Jyväskylän yliopiston ja Jyväskylän ammattikorkeakoulun laaja-alaista kyberturvallisuusosaamista uudella tavalla, mikä vahvistaa kansallista kyberturvallisuusresilienssiä. FICEC yhdessä verkostonsa kanssa luo vahvan kansallisen kyberturvallisuusyhteisön.

Kapteeni (res.) Seppo Simola tutkii, kerää ja tallentaa kokoelmaansa suomalaista sotilasperinnettä, kuten kauluslaattoja, arvomerkkejä ja muita sotilaspuvun tunnuksia sekä sotilaspukuja. Simola on kirjoittanut artikkeleja ja kirja-arvosteluja etenkin sotilasalan lehtiin jatkuvasti vuodesta 2008 alkaen.

TEKSTI JA KUVAT: SEPPO SIMOLA

Aselajivärien vaiheita Suomessa

Violetti on ollut viestijoukkojen väri Suomessa jo 100 vuotta

Aselajivärit ovat kansainvälinen ilmiö ja ne periytyvät ajalta, jolloin sotilaspuvut olivat värikkäitä. Housujen ja takkien sekä takinkäänteiden ja käännettyjen hihansuiden värit vaihtelivat joukon mukaan. Tietyt väriyhdistelmät liittyivät esimerkiksi tiettyyn rykmenttiin.

Värikkäät asut jäivät 1800-luvulle, ja seuraavalle vuosisadalle tultaessa kenttävärit valtasivat yhä enemmän alaa etenkin taisteluasuissa. Paraatiunivormut saattoivat edelleen olla värikkäämpiä. Vaikka pukujen väriskaalasta tuli maanläheisempi, niin vanhoja rykmenttivärejä ei suinkaan unohdettu.

Eräs selitysmalli aselajivärien synnyksi nimittäin on, että vanhoista puvuista saatettiin ihan konkreettisesti leikata muutama kangassuikale talteen ja kiinnittää ne neulalla kenttäpuvun kauluskäänteeseen. Epävirallinen käytäntö muovautui lopulta aselajiväreiksi. Aselajien tunnusvärit vaihtelevat eri maissa, mutta kansainvälisiä yhtäläisyyksiäkin ilmenee.

Itsenäisen Suomen sotaväessä pukua m/22 koskeva normisto oli ensimmäinen laaja ja kattava ohjeistus myös aselajiväreistä. Kauluslaattoja puvuissa ei vielä tuolloin ollut, vaan aselajivärit ilmenivät lähinnä olkapolettien pohjan ja reunuksen väreinä. Teknillisten joukkojen olkapoletti oli harmaa ja sitä kiersi violetti reunus. Selvästi erottuva aselajin ilmaisutapa olivat myös housujen reunusnauhat eli reväärit. Teknillisillä joukoilla ne olivat violetit.

Puku ilmaisi joskus aselajin

Suomessa sotilaspuvut ovat olleet itsenäisyyden alusta asti lähinnä kenttävärisiä, yleensä harmaita. Pukumalliston m/27 väriskaala oli ruskea ja puvun omaksuivat käyttöönsä erityisesti suojeluskunnat. Ruskeita pukuja oli myös kokeilukäytössä 1950-luvulla.

Näkyvänä poikkeuksena kenttäväreihin olivat monille tutut ratsuväen punaiset housut. Vaan olipa oman värisiä pukineita muillakin joukoilla. Rannikkotykistön puvun m/22 housut olivat tummansiniset. Tankkimiehet on puolestaan tunnettu mustasta päähineestään jo ennen puvun m/22 vahvistamista. Tankki- ja automiehet ovat käyttäneet myös mustia nahkapukuja.

Aselajivärisiä pukineita edustavat Suomessa nykyään tavallaan baretit. Värillisiä elementtejä on myös soittokuntien edustusasuissa sekä Kaartin jääkärirykmentille suunnitellussa edustusasussa m/10, jossa on vihreä kaulus, olkapoletit ja hihansuut sekä näitä rajaamassa hopeanvärinen nauha. Asussa siis toistuvat KAARTJR:n kauluslaattojen vihreä ja hopea.

Violetti väri esiintyy aselajivärin ohella myös teknillisen toimialan värinä. Yleisimmin tämän voi havaita teknikko- ja insinööriupseerien hihakaluunoiden välissä olevina violetteina verkasuikaleina. Violetti on tekniikan toimialaväri myös Ilma- ja Merivoimissa.

Ilma- ja Merivoimat ovat olleet ja ovat yhä asujen värien suhteen asia erikseen. Siinä missä maavoimamme ovat suosineet harmaita pukuja, niin Ilmavoimat sekä Merivoimat ovat suosineet sinistä. Rajavartiolaitos puolestaan siirtyi pääasiassa vihreisiin asuihin 1990-luvulla.

Kauluslaatat pukuihin m/36

Kauluslaatat tulivat suomalaisiin sotilaspukuihin puvun m/36 myötä. Kauluslaattoja käyttöön otettaessa monet silloiset aselajivärit siirtyivät olkapoleteista kauluslaattoihin joko sinällään tai muunneltuina. Kauluslaatat ovat säilyneet hyvin pitkään suomalaisen sotilaspuvun elementtinä, vaikka kauluslaatallisten pukujen käyttö on selvästi vähentynyt.

Varusmiehillä kauluslaatallisia pukuja näkee enää aniharvoin erikoistilanteissa, eikä kantahenkilökuntakaan arkioloissa juuri kauluslaatallisia pukuja käytä paitsi ehkä esikuntapalvelussa. Maastopuvun vallatessa alaa kevyt palveluspuku m/83 on käynyt ammattisotilailla varsin harvinaiseksi ainakin omien havaintojeni perusteella, mutta pukua m/58 näkee sentään virallisissa tilaisuuksissa ja paraateissa.

Yksinkertaistamista ja karsintaa

Suomalaisia sotilaspukuja ja niiden tunnuksia on jo vuosikymmenien ajan systemaattisesti yksinkertaistettu ja karsittu. Pataljoonatason joukoilta ovat käytännössä kadonneet omat joukko-osastotunnukset, ja pukujen värielementtejä – kuten housujen saumanauhat eli reväärit – on vähennetty. Ero sota-ajan puvun m/36 ja nykyisen m/58:n välillä on melkoinen.

Esimerkiksi kenttätykistön upseerin erotti puvussa m/36 jo kaukaa – punaista oli niin lakin terenauhassa, kauluslaatoissa kuin saapashousujen reunusnauhoissakin. No, toisaaltahan tämä erottuvuus oli myös työturvallisuuskysymys. Kun kaikki käyttävät demokraattisesti samanlaista maastopukua eikä rähinäremmiäkään enää ole, niin vihollisen tarkka-ampujan on hankala valita parasta maalia.

Erityisen pahaa jälkeä kauluslaattojen kannalta teki vuoden 2010 suuri karsinta, jolloin moni joukko menetti oman perinteisen aselajivärinsä. Oman värinsä menettivät tuolloin esimerkiksi topografikunta, panssarintorjunta, Urheilukoulu, sähköteknillinen ala, eläinlääkintä ja farmasia.

Mistä tulee viestin violetti?

Violetti on kansainvälisesti tieteen ja tekniikan väri. Tämä yhteys lienee taustana sille, että Suomen viesti- ja pioneerijoukot käyttävät violettipohjaisia kauluslaattoja teknillisten joukkojen luoman perinteen mukaan.

Kun kauluslaatat tulivat käyttöön puvun m/36 myötä, niin viestimiehillä ja pioneereilla ei vielä ollut omia laattoja vaan he käyttivät violettipohjaisia ja mustareunaisia teknillisten joukkojen laattoja vuoteen 1939 saakka. Silloin pioneerit saivat nykyiset harmaareunaiset laattansa ja viestimiehet keltareunaiset laatat.

Harmaan reunusvärin lienee tarkoitus sitoa pioneerijoukot lähemmäs jalkaväkeä, onhan jalkaväen vihreän laatan reunus harmaa. Keltainen puolestaan symboloi nopeutta sekä ratsuväen kautta että jääkärijoukkojen vihreiden laattojen keltaisten reunusten mukaan. Viestijoukkojen kauluslaattojen keltaisen reunusvärin voi hyvinkin mieltää merkitsevän nopeutta viestien kulussa.

Mahdollisesti vuosina 1939–1941 myös viestimiehet käyttivät pioneerien tapaan violettia laattaa harmain reunuksin, jolloin kyseinen väri vaihteittain korvasi teknillisten joukkojen

aiemman violetti-mustan laatan. Pioneerit jatkoivat violetti-harmaalla kauluslaatalla, mutta viestimiehet siirtyivät viimeistään jatkosodan aikana violetti-keltaiseen laattaan.

Violetti esiintyi myös Ratsuväkiprikaatiin kuuluneen Viestieskadroonan kauluslaatoissa ilmeisesti vuosina 1937–1942. Itse laatta oli ratsuväen tapaan keltainen, mutta violetti reunus kertoi kyseessä olevan viestimiesten laatan.

Violetti kirkollisessa käytössä

Violetti on myös yksi kirkon liturgisista väreistä – se on katumuksen ja syntien tunnustamisen väri, ja sitä käytetään esimerkiksi pääsiäistä edeltävän paaston aikana. Sotilaspapisto käytti violettia, harmaareunaista kauluslaattaa vuosina 1936–1941. Väriyhdistelmä oli periaatteessa sama kuin pioneerien, mutta violetti – eli ohjesäännössä punasinervä – oli sävyltään selvästi vaaleampi.

Papisto sai mustan harmaareunaisen laatan – eli panssarijoukkojen aiemman värin – kesällä 1941, jolloin panssarijoukkojen oli määrä siirtyä käyttämään oranssireunaisia laattoja. Tankkimiehille palautettiin perinteinen aselajiväri vuonna 1948, jolloin papit saivat nykyiset mustat violettireunaiset laattansa.

Linnoitusjoukoille tekniikan väri

Tarpeettomaksi käynyt alkuperäinen teknillisten joukkojen violetti-musta kauluslaatta annettiin vuonna 1944 linnoitusjoukoille. Tiedossani ei ole, pitkäänkö laatta oli silloin käytössä. Tuskin kovin pitkään, koska sotien jälkeen ei isommin nähty tarvetta erillisille linnoitusjoukoillekaan. Pioneerit hoitivat tarvittaessa linnoittamisen. Ainakaan vuoden 1958 kauluslaattakuvastossa linnoitusjoukkojen laattaa ei enää näy.

Niinpä violetti-musta kauluslaatta painui vuosikymmeniksi unhon yöhön. Uusi tuleminen tapahtui ensi kerran vuonna 1982, jolloin kauluslaatan otti käyttöön Sähköteknillinen koulu. Violetti-musta laajeni myöhemmin koko sähköteknillisen toimialan väriksi. Laatta pysyi käytössä lähes 30 vuotta kunnes se vuoden 2010 karsinnassa poistettiin.

Violetti-mustan neljäs tuleminen

Mutta violetti-musta laattapa ei suostunut kuolemaan, vaan se nousi sotilasperinteiden haudasta vielä kerran, jolloin siitä tuli vuonna 2007 perustetun Elektronisen sodankäynnin keskuksen (ELSOK) kauluslaatta.

ELSOK kuuluu nykyään Panssariprikaatiin, ja sen toiminnot sijaitsevat osaksi Parolannummella ja osaksi Riihimäellä. Oli ilahduttavaa nähdä harvinainen ja monet käänteet kokenut aselajiväri jälleen käytössä viime vuonna eräässä panssarialaan liittyneessä tilaisuudessa.

Violetti laatta mustin reunuksin on eräiden lähteiden mukaan ollut aivan kauluslaattojen käyttöön oton alkuvaiheessa sotakoirakomppanialla ja jatkosodan loppupuolella – nähtävästi juuri ennen siirtymistä linnoitusjoukkojen väriksi – myös Ilmavoimien viestijoukoilla. Tutkimukseni näiden tietojen vahvistamiseksi tai kumoamiseksi jatkuvat.

Kaikki lisätiedot tässä artikkelissa käsiteltyihin asioihin sekä muut kiinnostavat tiedot ovat erittäin tervetulleita. Allekirjoittaneen yhteystiedot saa lehden toimituksesta.

Lähteitä:

Pekka Aarniaho: Kaluunat ja rähinäremmit – Itsenäisen Suomen virkapuvut ja arvomerkit 1918–1945 (1996)

Juhani U.E. Lehtonen: Sotilaselämän perinnekirja (2003)

Petteri Leino: Asepuku m/36 (1998)

Marko Palokangas: Itsenäisen Suomen sotilasarvot ja -arvomerkit (2000)

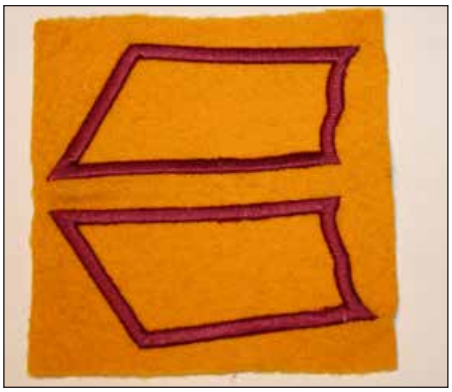
Marko Palokangas: Suomen Puolustusvoimien joukko-osastoperineet (2008)

Puolustusvoimien ohjesäännöt

Nykyään violeteilla kauluslaatoilla on kolme käyttäjää: ylhäältä lukien viestijoukot, Elektronisen sodankäynnin keskus ja pioneerit.

Violetti näkyy edelleen teknillisen alan toimialavärinä erikoisupseerien kaluunoiden välissä. Kuvassa ylempänä on insinöörikommodorin olkapoletit ja alempana insinööri- tai teknikkoluutnantin päällystakin hihakaluunat.

Teknillisten joukkojen kauluslaatto- ja m/36. Tämä oli viesti- ja pioneerijoukkojen yhteinen kauluslaatta ennen kummankin aselajin oman aselajivärin käyttöönottoa vuoden 1939 kauluslaattauudistuksen jälkeen.



Ratsuväkiprikaatiin kuulunut Viestieskadroona käytti violetteja reunuksia ratsuväen keltaisissa laatoissa.

Kuvassa on Puolustusvoimien pääinsinöörinä vuosina 1994–2003 palvelleen insinöörikenraalimajuri Kalle Ukkolan kauluslaatat. Violetti väri tarkoittaa tässä yhteydessä teknillistä toimialaa, vaikka kenraalien kauluslaattoihin kuuluva keltainen reunusväri saa laatat näyttämään viestijoukkojen kauluslaatoilta.

Kapteeni palvelee tutkijaesiupseerina Puolustusvoimien tutkimuslaitoksella.

TEKSTI: ALEXANDER GRANDIN

Software Engineering Management

Tom Gilb's principle on fuzzy targets: "Projects without clear goals will not achieve their goals clearly."

"Tehokasta ohjelmistoprojektien johtamista ja ohjelmistojen elinkaaren hallintaa hankaloittavat niiden eräät erityispiirteet." todetaan IEEE:n julkaisemassa ohjelmistotuotantoa käsittelevässä SWEBOK käsikirjassa. Suurin osa ohjelmistotuotannon projekteista epäonnistuvat maailmanlaajuisesti vieläkin, joko ylittäen aikataulun, budjetin tai jättämällä vaatimuksia täyttämättä. Näitä ongelmia voi liennyttää hyvällä johtamisella, mutta ei täysin hallita. Samanaikaisesti sotatarvikkeiden hinta nousee inflaatiota nopeammin. Onko päivitettävillä ohjelmistolla varustetuilla sotatarvikkeilla, kuten "software-defined" laitteilla, löydettävissä ratkaisu tähän hintojen nousuun, vai onko se osittain syypää siihen?

Ongelma

The Standish Group on vuodesta 1994 alkaen julkaissut CHAOS tutkimuksen, joka selvittää ohjelmistotuotannon tilannetta maailmanlaajuisesti vuosittain. Raportissa arvioidaan vuodesta 2015 eteenpäin ohjelmistoprojekteja kolmella mittarilla – 1) asetetussa aikataulussa, 2) määritetyssä budjetissa sekä 3) täyttäen asiakkaan vaatimukset. Kuten alla olevasta taulukosta näkyy, niin vuoden 2015 raportin tulokset ovat linjassa aikaisempien vuosien tulosten kanssa.

Asetetut vaatimukset täyttäviä onnistuneita ohjelmistoprojekteja on alle kolmasosa kaikista projekteista. Vähintään kyseenalaisesti toteutetut projektit kattavat yli puolet kaikista, ja suoraan epäonnistuneita projekteja on noin viidesosa. Kyseenalainen projekti alittaa jonkun määritetyistä laatumittareista ja epäonnistunut projekti joko päätetään keskeneräisenä tai tuotetta ei oteta käyttöön. Vuonna 2018 luvut ovat hieman paremmat, mutta silloinkin vain 33% projekteista määritettiin onnistuneiksi. Pitkän aikavälin tarkastelulla voidaan todeta, että ohjelmistotuotannon haasteita ei ole ratkaistu. Kannattaako toteutustapoja kehittämällä yrittää lieventää näitä ongelmia? Onneksi raportti valaisee myös mitkä projektit onnistuvat parhaiten.

	2011	2012	2013	2014	2015
SUCCESSFUL	29%	27%	31%	28%	29%
CHALLENGED	49%	56%	50%	55%	52%
FAILED	22%	17%	19%	17%	19%

Ohjelmistoprojektien onnistumisprosentti CHAOS rap ortin mukaisesti.

Ensinnäkin pienet projektit onnistuvat huomattavasti paremmin kuin isot, kuten taulukosta 2 voidaan lukea. Raportissa todetaan jopa, että "useimmat, jollei kaikki, isot, monimutkaiset, ylivuotiset projektit ovat tarpeettomia". Yksinkertaisin tapa onnistua ohjelmistoprojekteissa on siis pilkkomalla kokonaisuus osiin ja toteuttamalla nämä erikseen.

Toinen selkeä tapa parantaa ohjelmistotuotantoaan, on käyttää iteratiiviseen kehitykseen perustuvia Agile-menetelmiä. Suomeksi tämä on käännetty ketteräksi ohjelmistokehitysmalliksi, mutta koska alkuperäinen termi on laajalle levinnyt, niin käytän tässä Agile kuvaamaan tätä. Taulukosta 3 voimme nähdä, että kautta linjan Agile-periaatteita noudattavat projektit onnistuvat lähes 350% paremmin kuin vesiputousmenetelmää käyttävät projektit. Pienempien projektien osalta ero on pienempi, mutta isompien projektien osalta ero on jo varsin merkittävät. Agile sopii paremmin pienempien projektien toteuttamiseen kuin isojen. Agile on kuitenkin parempi tapa toteuttaa myös isoja projekteja kuin vesiputousmalli. Agile-mallia ja sen kehitystä käsittelen laajemmin alla.

Muutoksen taustat

Ohjelmistotuotannon prosesseja on kehitetty voimakkaasti ohjelmistojen yleistyessä. Ohjelmistotuotantoa varten kehitettiin erityisesti 1980-luvun jälkeen omia johtamismalleja. Silloin huomattiin, että tekniikan alan yleiset laatu- ja prosessikuvaukset sopivat tähän yleisesti huonosti. Ohjelmistokehityksen alkuaikoina käytettiin samoja johtamismalleja kuin muissakin teknisissä projekteissa. Ne perustuvat suoraviivaisesti etenevään (linear) suunnitteluun, jossa projekti nähdään sarjana päätettyjä työosioita. Kuuluisimpana esimerkkinä tästä on vesiputousmalli. Näiden perusteella tehty ohjelmistosuunnittelu ja -tuottaminen ei kuitenkaan johtanut parantuneeseen laatuun, vaan lisääntyneeseen dokumentaatioon. Tämän ongelman ratkaisemiseksi kehitettiin Lean- ja Agile-mallit. Työ keskittyi siten enemmän tekemiseen kuin työn (uudelleen)suunnittelemiseen.

Erityisesti vaatimusten hallinta asettaa haasteita ohjelmistotuotannolle; ohjelma ei ole ikinä valmis, vaan vaatimukset muuttuvat, kehittyvät ja ymmärretään väärin. Koska vaatimukset ohjelmistotuotannossa useimmiten muuttuvat työn aikana, tuottamistyö toteutetaan useimmiten nykyisin iteratiivisilla prosesseilla ennalta määrättyjen yksittäisten tehtävien sarjan sijaan.

Agile ja sen lukuisat versiot ovat muuttaneet ohjelmistotuotantoa merkittävästi, mutta metodina se on osittain ristiriitainen esimerkiksi Systems engineering lähestymistapaan. Agile on ketterä ja painottaa tekemistä suunnittelemisen sijaan. Agile-mallin lähtökohtana on työn aikana muuttuvat vaatimukset. Tämän lisäksi ohjelmisto ei ikinä ole valmis, vaan sitä käytetään ja kehitetään sen koko elinkaaren aikana. Tämä erottaa ohjelmistotuotantoa fyysisistä tuotteista. Agilen yhtenä edellytyksenä on kuitenkin osaavan ja kokeneen kehittäjätiimin muodostaminen – vähällä suunnittelulla aiheutetaan haasteita, jos tekijät eivät tarkasti tiedä mitä tehdä. CHAOS raportissa todetaankin, että osaava Agile-tiimi onnistuu projekteissaan lähes 220% useammin kuin osaamaton tiimi. Osaamisvaatimuksen lisäksi Agilen skaalautuvuus suuriin järjestelmiin on haastavaa.

	SUCCESSFUL	CHALLENGED	FAILED
Grand	2%	7%	17%
Large	6%	17%	24%
Medium	9%	26%	31%
Moderate	21%	32%	17%
Small	62%	16%	11%
TOTAL	100%	100%	100%

Pienet ohjelmistoprojektit onnistuvat huomattavasti useammin kuin isot projektit CHAOS raportin mukaan.

Agile ja suunnittelun yhteensovittaminen

Agilen ja suunnitteluun perustuvien metodien yhteensovittamista sekä organisaation arvioimista on esimerkiksi Barry Boem käsitellyt artikkelissaan "*Observations on Balancing Discipline and Agility*". Boemin mallin mukaan organisaation tulee ensin arvioida nykyisiä projektejaan viidellä mittarilla, joilla voidaan määrittää ovatko organisaation kyvykkyydet ja projektit enemmän Agile vai suoraviivaisen suunnitteluun perustuvia.

Jos tulosten perusteella organisaatio on selkeämmin yhtä kuin toista, niin tätä osaamista tulee kehittää määrätietoisesti. Kehittämistä tulee tehdä yhdessä tärkeimpien sidosryhmien edustajien kanssa. Analyysin perusteella havaitut yleismalliin kuulumattomat osat tulee käsitellä poikkeuksina. Nämä poikkeukset voidaan hallita riskienhallintamenetelmien avulla. Jos taas tulos näyttää organisaation olevan selkeästi sekoitus molempia malleja, tulee inkrementaaliseen kehittämiseen perustuva sekastrategia kehittää asetettujen tavoitteiden saavuttamiseksi. Oli tulos mikä tahansa, tulee päätöstä tukea jatkuvalla henkilöstön

SIZE	METHOD	SUCCESSFUL	CHALLENGED	FAILED
All Size Projects	Agile	39%	52%	9%
	Waterfall	11%	60%	29%
Large Size Projects	Agile	18%	59%	23%
	Waterfall	3%	55%	42%
Medium Size Projects	Agile	27%	62%	11%
	Waterfall	7%	68%	25%
Small Size Projects	Agile	58%	38%	4%
	Waterfall	44%	45%	11%

TaAgileprojektit onnistuvat merkittävästi paremmin kuin vesiputousmalliin perustuvat CHAOS raportin mukaan.

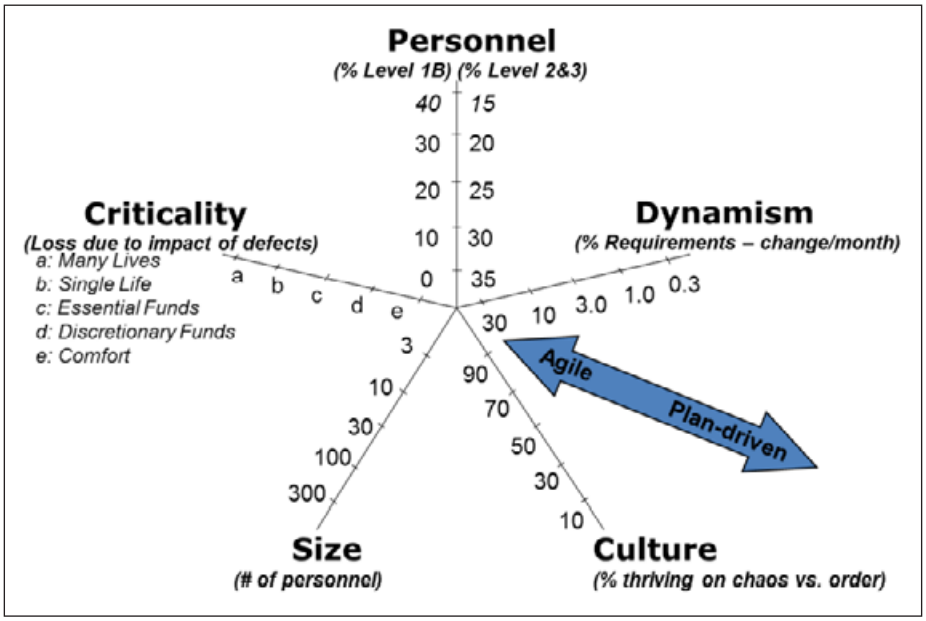
koulutuksella, niin osaamisen, viestinnän kuin arvojenkin osalta. Unohtamatta kehityksen seuraamista asetetuilla mittareilla.

Pohdinta

Ohjelmistopohjaiset tuotteet näyttäytyvät helposti halpana ja tehokkaana tapana hillitä yleistä kustannusten nousua. Olisi mielenkiintoista arvioida kustannusten sekä käyttäjien näkökulmasta, kuinka hyvin Puolustusvoimien sisäiset ohjelmistoprojektit tai valmiiksi ostetut ratkaisut laadunhallinnan näkökulmasta näyttäytyvät esitettyyn materiaaliin perustuen. Yksittäisiä ratkaisuja hyödyntämällä ei hallita ohjelmistotuotannon lopputulosta. Mahdollisia haasteita voidaan kuitenkin liennyttää hyödyntämällä hyväksi todettuja menetelmiä, vaikka nämä voivat olla raskaasti implementoitavia.

Agile menetelmien käyttäminen edellyttää asiakkaalta sitoutumista. Asiakkaan edustajat tulee kouluttaa tehtävään ja sitouttaa pitkäjänteisesti kehitystyöhön osaksi ohjelmistokehitystiimiä. Ketkäköhän nämä henkilöt olisivat Puolustusvoimissa? Lisäksi jatkuvasti muuttuvat vaatimukset aiheuttavat haasteita suunnitteluun perustuvassa ympäristössä. Millä projektin tai hankkeen tasolla Systems engineering päättyy ja antaa tilaa mukautuville, ketterille menetelmille? Tärkeintä on tietenkin tietää mitä ohjelmistokehityksellä halutaan – mikä on haluttu lopputulos ohjelman kehitykselle tai muokkaukselle?

Artikkeli perustuu Tampereen yliopiston Porin Johtamisen ja Tietotekniikan yksikön järjestämään samannimiseen kurssiin, jonka kirjoittaja suoritti osana opintojaan vuona 2021.



Kuva 4. Barry Boemin artikkelin mukainen arviointiasteikko.

TEKSTI:ESA TIILIKAINEN, HEAD OF PRODUCTION, COMBITECH OY

Ohjelmistoyrityksen näkökulma vesiputous-mallin ja ketterän ohjelmistokehitysmallin vertailussa

Esa Tiilikainen on Combitechin tuotantojohtaja, joka on urallaan kohdannut sekä asiakkaan, että yrityksen ketteröitymisen haasteita ja mahdollistanut menestyksekkäitä muutoksia. Combitechilla Esa huolehtii tuotannon kokonaisuudesta auttaen organisaatiota, johdettaviaan ja asiakkaitaan kasvamaan ja menestymään.

Työelämään siirtyvälle nuorelle vesiputous terminä voi parhaimmillaankin herättää vain nostalgisia ajatuksia lapsuuden perhelomasta Yhdysvaltojen ja Kanadan rajalle. Perinteisen ohjelmistotuotantoprosessin sijaan nykypäivän IT-koulutuksessa pääpaino on ketterien työskentelymenetelmien rooleihin ja prosesseihin perehtyminen sekä käytännön harjoittelu ryhmätyöskentelynä. Ketterät ohjelmistokehityksen menetelmät ja tämän mukainen organisaatio rooleineen ovat nykyään itsestäänselvyys työnhakijalle. Alati haastavammaksi käyvässä IT-osaajien rekrytointimarkkinassa yrityksen on pystyttävä tarjoamaan työnhakijalle merkityksellisten projektien ja tuotteiden lisäksi modernit toimintatavat sekä ketteryyden arvomaailman sisäistänyt työyhteisö. Ketterien toimintatapojen omaksuminen ja niissä harjaantuminen onkin menestyvälle ohjelmistoyritykselle elinehto. Yleensä tämä on edellyttänyt organisaation kyvykkyyttä ja sitoutumista kokonaisvaltaiseen muutokseen, esimerkiksi ketterien menetelmien kouluttamista koko henkilöstölle sekä yrityksen prosessien ja työkalujen uudistamista.

Puolustustoimialalle tyypillisiä ovat laajat ja pitkäkestoiset suorituskykyhankkeet, joissa pyritään hahmottamaan tuotettavan järjestelmän elinkaari aina esiselvityksistä suorituskyvyn rakentamiseen, käyttöönottoon ja ylläpitoon saakka. Usein tämä näyttäytyy suunnitelmaohjautuvina hankkeina, joissa on paljon vesiputousmallin piirteitä. Pitkän elinkaaren mahdollistamiseksi tarvitaan uskottava ratkaisu myös huoltovarmuudellisiin kysymyksiin. Miten ketteriin menetelmiin ohjelmistokehityksessään tukeutuva ohjelmistoyritys pystyy menestymään tällaisessa toimintaympäristössä?

Hyvin suunniteltu = puoliksi tehty

Vesiputousprojektien parissa työskennelleet tietävät sen ylivertaisen hallinnan tunteen, kun projekti on viimein ositettu loogisiin kokonaisuuksiin, jossa eri vaiheet seuraavat toisiaan ja kriittinen polku tuo ryhtiä projektin useisiin riippuvuuksiin ja aikataulutukseen. Projektin kick-off on pidetty ja juuri tätä projektia varten kasattu kokenut projektiryhmä suuntaa katseensa parin vuoden päästä juhannuksena tehtävään ensimmäiseen toimitukseen. Ensin on toki selvitettävä, määritettävä ja katselmoitava tarkasti projektin vaatimukset, suunniteltava rajapinnat, integraatiot ja muutenkin tuotettava kaikenkattava suunnittelumateriaali, joka osaltaan varmistaa tuotettavan ratkaisun vaatimuksenmukaisuuden samalla mahdollistaen muutoksenhallinnan.

Erityisesti laajojen uusien ratkaisujen tuottamisessa on kuitenkin kaikesta suunnittelusta huolimatta paljon myös tuntemattomia asioita ja muuttuvia vaatimuksia. Käyttötarpeeseensa hyvin soveltuvan ratkaisun tuottamisessa vaatimustenmukaisuuden ohella keskeistä onkin kyetä vastaamaan muutoksiin ja ymmärtää ne osana normaalia yhteistyötä. Ketterien ohjelmistokehitysmallien tunnuspiirteenä voidaan pitää juuri tätä muutosohjautuvuutta.

Ketterä ohjelmistokehitys itsessään ei tuo suurta eroa onnistuneen lopputuloksen kannalta välttämättömiin työvaiheisiin. Samat päävaiheet ovat edelleen käytössä määrittelystä suunnitteluun, toteutukseen, testaukseen ja toimitukseen, mutta nämä vaiheet toistuvat jokaisessa iteraatiossa tai vähintäänkin inkrementaalisesti. Ketterälle kehitykselle ominaista ovat toteutustyön edetessä tarkentuvat kehityssyklit, työn läpinäkyvyys saavutusten esittelyn kautta sekä valmius nopeiden muutosten tekemiseen. Toimiakseen tämä edellyttää kehitystiimin ja asiakkaan tiivistä yhteistyötä. Asiakkaan aktiivinen rooli korostuu, koska pienissä erin tehtävässä kehityksessä avainroolissa on jatkuva asiakaspalaute ja päätösten tekeminen. Asiakkaalta tarvitaan kyvykkyyttä arvioida asetettujen tarpeiden täyttymistä ja mahdollisesti tarvittavia muutoksia. Isojen hankkeiden tapauksessa haasteeksi voi kuitenkin muodostua se, että pienin palasin edetessä hukataan ajatus järjestelmäkokonaisuudesta ja yhtenäisestä toimintalogiikasta. Yleisesti isommissa hankkeissa myös muutokset ovat todennäköisempiä.

Olipa käytetty projektityön menetelmä mikä tahansa, on tuotettavan ratkaisun omistajalla oltava selkeä ajatus rakennettavasta kokonaisuudesta. Tavoite on oltava kirkas ja konkreettinen. Toimittajan näkökulmasta ketterän kehityksen etuihin kuuluu nimenomaan parempi läpinäkyvyys, jolloin ongelmat tulevat useammin ja aiemmin esille. Tämä tarjoaa mahdollisuuden löytää ratkaisuja ja hallita tekemisen riskejä.

Mitä edellytyksiä ketterä malli vaatii eri osapuolilta?

Yksi ketterän kehityksen merkittävistä eduista on asiakkaalle arvoa tuottavien työn tuloksien toimittaminen sitä mukaa, kun ne ovat toimitusvalmiina. Tällaiset iteratiiviset julkaisut tarjoavat paremman näkyvyyden toteutuksen valmiusasteeseen ja mahdollisuuden suunnitelmien mukauttamiseen tarvittaessa. Jotta tähän päästään, täytyy toiminnan kuitenkin olla ketterän ohjelmistokehityksen periaatteiden mukaista koko toimintaympäristössä. Yrityksen ohjelmistotuotannon tulee perustua hyvin hallittuihin prosesseihin, korkeasti automatisoituun testaukseen sekä jatkuvaan julkaisuvalmiuteen.

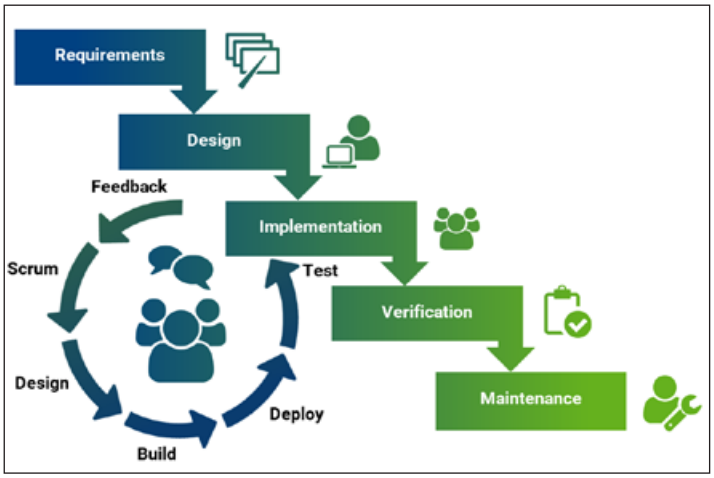
Asiakkaalla puolestaan on oltava varhaiseen koekäyttöön soveltuvia ylläpidettyjä testausympäristöjä sekä käytettävissä riittävät toiminnan edellyttämät henkilöresurssit. Säännöllisesti ja kohtuullisen lyhyin väliajoin tehtävät yhteiset verifiointi- ja validointitilaisuudet projektin aikana tarjoavat parhaimmillaan kaikille osapuolille kaivattua kokonaisjärjestelmätasoista näkyvyyttä tuotosten soveltuvuudesta käyttötarkoitukseensa.

Kuten aiemmin todettiin, ketterä kehitys vaatii ympärilleen myös ketteryyden arvomaailman sisäistäneen organisaation. Luonnollisesti tämä pätee sekä toimittajan että asiakkaan puolella, kaikilla hankkeen kannalta keskeisillä organisaatioiden tasoilla. Olennaista on, että kaikki puhuvat samaa kieltä. Työssä tarvittavien roolien ja erityisesti niihin soveltuvien henkilöiden tunnistaminen on keskeistä. Tämä tiedostaen on samalla kuitenkin pyrittävä minimoimaan henkilöriskejä. Perinteisten ohjelmistokehitysmenetelmien tapauksessa on tyypillistä, että pitkien toteutusvaiheiden myötä avainhenkilöille kertyy kriittistä osaamista. Kun jokaisella kehitystiimin jäsenellä on oma iso kokonaisuutensa vastuullaan, usein monessa eri projektissa, avainhenkilön poistuminen voi luoda ongelmia jatkuvuudenhallinnan osalta. Ketterässä ohjelmistokehitysmallissa, edellä mainittu tiedostaen, pyritään luomaan puitteet säännölliseen tiedon jakamiseen ja ominaisuuksien toteuttamiseen yhteistyössä koko tiimin voimin. Osaltaan tämä parantaa yrityksen kyvykkyyttä tuottamansa ratkaisun uskottavan huoltovarmuuden turvaamiseen.

Mielekäs organisoituminen ja osaavat henkilöt rooleissaan eivät kuitenkaan vielä takaa sujuvaa ketterää ohjelmistokehitystä. Tarvitaan valtuudet tiimille ja tukirooleille tehdä päätöksiä nopeasti ja itsenäisesti. Kehitystiimi tarvitsee myös säännöllistä ohjausta asiakkaalta prioriteettien ja toteutuksen laajuuden osalta. Joskus voi kuitenkin tulla tilanteita, joissa asiakkaan asianhoitajan laaja-alainen toimialakokemus ei suoraan välity kehitystiimille riittävän selvinä tarpeina. Asiakkaan käyttämä kieli voi olla kehitystiimille vierasta. Tästä syystä tuoteomistajalla on kriittisen tärkeä rooli osana yrityksen kehitystiimiä. Hänen tehtävänään on ymmärtää asiakkaan tarpeita ja sanoittaa ne tiimin työlistoille konkreettisiksi ominaisuuksiksi. Tuoteomistaja hyödyntää tiimin suunnitteluosaamista, kerää lisäselvitystä kaipaavat asiat ja tuottaa asiakkaalle ratkaisuesityksiä mahdollisesta etenemistavasta. Tämä edesauttaa ratkaisukeskeistä etenemistapaa, avoimuutta ja päätösten tekemistä tarveperusteisesti.

Yhdistelmämallit - kultainen keskitie?

Perinteisen vesiputousmallin sijaan erilaiset yhdistelmämallit ovat nykyään varsin yleisiä. Näissä pyritään hyödyntämään eri ohjelmistokehitysmallien soveltuvia osuuksia, pyrkimyksenä vähentää painetta ja riskien realisoitumista projektin loppupäästä.



Erilaisissa yhdistelmämalleissa voidaan hyödyntää ketteriä menetelmiä osana suurempaa hankekokonaisuutta.

Vesiputousmallin heikkoutena voidaankin pitää juuri sitä, että projektit painottuvat loppupäähän. Tämä tarkoittaa yleensä päätöksenteon ja tuotosten tarpeenmukaisuuden arvioimista erilaisissa testausvaiheissa, jolloin toimittajan tuotos on jo kokonaisuudessaan määritelty, toteutettu ja toimitettu. Hyväksymistestausvaiheessa tunnistetut puutteet, virhetulkinnat, ohjelmistovirheet ja uudelleensuunnittelutarpeet saattavat käynnistää uuden kehitysvaiheen, jolloin kaikki siitä riippuvat vaiheet on myös suunniteltava uudelleen ja voivat viivästyä vastaavasti. Ketterien menetelmien yhtenä etuna tästä näkökulmasta voidaan pitää sitä, että varhain tehdyillä toimituksilla pyritään havaitsemaan tarvittavat muutokset aiemmin. Tämä ei poissulje sitä, etteikö hankkeessa edelleen olisi kaikki testaus- ja hyväksyntämenettelyt kuin aiemminkin.

Puolustustoimialalla toimivan ohjelmistoyrityksen tulee hallita sekä ketterä ohjelmistokehitys että laajojen hankkeiden vaiheittainen läpivienti. Tämä edellyttää yritykseltä kykyä sopeutua kulloisenkin työmaan tunnuspiirteisiin sekä sovittaa työskentelymenetelmät tarpeiden mukaisesti. Usein tämä voi tarkoittaa suunnitelmaohjatun projektin tiettyjen työvaiheiden toteutusta ketterin menetelmin. Esimerkiksi päähanke voi edetä vesiputousmallin kaltaisesti vaiheittain, mutta ohjelmistoon liittyvä toteutusvaihe saatetaan tehdä hyödyntäen ketterien menetelmien nopeaa palaute- ja kehityssykliä. Tällöin korostuu hankkeen hyvän kokonaistilannekuvan tärkeys sekä sopeutumiskyvykkyys. Vesiputousmalli puolestaan voi olla hyvinkin resurssitehokasta erityisesti silloin, kun vaatimuksien ei oleteta muuttuvan kesken työn eikä asiakkaalta tarvita palautetta työn aikana. Tällainen voi olla esimerkiksi kahden järjestelmän välisen rajapinnan toteutus kypsän ja muuttumattoman rajapintamäärittelyn mukaisesti.

Lopetus

Kuten todettua, ohjelmistokehityksen ja rakennettavien järjestelmien karikot ovat moninaiset. Välillä ketterää kehitystä saatetaan pitää hopealuotina laajan ongelmakirjon ratkaisemisessa. Olennaista on kuitenkin tiedostaa, ettei olemassa ole yhtä oikeaoppista tapaa tehdä ketterää ohjelmistokehitystä. Vastaavasti vesiputousmallia on lähdetty tarveperustaisesti muokkaamaan, jotta hankkeiden joustava läpivienti olisi mahdollista. Kumpikaan malli ei ole toisiaan poissulkevia. Huolellisesti tehty esiselvitystyö harvoin heikentää ketteränkään ohjelmistoprojektin lähtöasetelmaa. Suunnitelmaohjatuissa projekteissa kaikille osapuolille hyödyllistä on puolestaan tunnistaa ja hyödyntää keinovalikoimaa toteutuksen aikaisten vaatimusmuutosten ja muuttuvien tarpeiden käsittelyssä palvelemaan lopputuloksen onnistumista.

Siksi onkin tärkeää, heti kehitystyön alussa, luoda osapuolten yhteinen ymmärrys käytetyistä menetelmistä ja mitä ne tarkoittavat - ja eivät tarkoita - kulloinkin aktiivisen yhteistyön osalta. Rehellisesti ja realistisesti tunnistetut toiminnan rajoitteet ja tunnuspiirteet luovat edellytykset sopia toimivat yhteistyön käytänteet. Usein myös aiemmat yhteistyön kokemukset, parhaat käytännöt ja näitä tukevat valmiit sopimusmallit tuovat kaivattua selkeyttä uusiin yhteisiin kehitysponnistuksiin. Mitä ikinä käytännöt ovatkaan, lopulta osapuolten keskinäinen arvostus, avoimuus ja yhteinen päämäärä luovat puitteet onnistuneelle lopputulokselle.

Ins A. Rajaniemi

Rovaniemen puhelinpiiri esittäytyy

Rovaniemen puhelinpiiri muodostuu Lapin läänistä ja Kuivaniemen kunnasta Oulun lääniä. Piirin pinta-ala (ilman vesialueita) on 94.000km^2 eli 31 % koko Suomen ”kuivasta” pinta-alasta. Eteläisen Suomen ”päälle” asetettuna tämä pohjoinen alueemme peittäisi puolet muusta manner-Suomesta. Väkilukumme piirimme alueella on kuitenkin vain vajaa 210.000 henkeä eli 4,5 % koko maan väkiluvusta. Nämä erikoisolosuhteet – suuri alue ja harva asutus – ovat ne seikat, jotka muuttavat pohjoisen piirimme puhelintoimen hoidon eräin osin toisenlaiseksi, kuin mitä on laita eteläisessä puhelinlaitoksessa. Viime vuoden päättyessä piirissä oli 353 keskusta, niissä 33.501 tilaajaliittymää ja niillä käytössään 43.795 liikennöivää puhelinta. Edellä mainitulla asiakasluvullaan piirimme on puhelinpiireistä kolmanneksi suurin ja kaikista paikallispuhelintointa hoitavista ”yrityksistä” se sijoittuu seitsemännelle sijalle.

Kaukoverkon rakentamissuunnitelma Lapissa rakentuu lähes kokonaan radiolinkkien varaan. Tähän laajakaistaiseen linkkiverkostoon kytkeytyy aikanaan myös kalottialueen Ruotsin puoleisen osan puhelinverkko Haaparannan – Kemin välisellä linkillä. Kaukokaapelointia Lapissa ei ole lainkaan. Koaksiaalirakenne tunnettaan täällä vain ”sisäänottoina” linkkien radiolaiteasemilta keskuksen ka-laiteasemille.

Lapin eräät erikoisolosuhteet kuvastuvat selvemmin laajojen haja-asutusalueiden, poronhoidon, metsätyömaiden yms. tilaajapalvelussa. Pienet erilliset asutusryhmät ja ”nauhamaiset” jokivarsiasutukset tilaajajohdon yhteiskäytön varsin yleiseksi. Tämä tarkoittaa kyläkytkimiä, rivikytkimiä ja myös useamman yhteisen johdon järjestelmiä. Kaukana olevia etäispuhelimia joudutaan liittämään keskukseensa tilaajalinkein. Etäisasutuksiin liittyvät ”suurpuhujat” kuten metsätyömaat, joita ei voida yhteisjohtoihin kytkeä, tarvitsevat tilaajajärjestelmiä. Ennen kuin poronhoitoa ja kalastusta harjoittavat saamelaisasukkaat saataisiin tilaajapalvelun piiriin, olisi myös muita teletekniikan luomia mahdollisuuksia voitava käyttää hyväksi tilaajapuhelimien liittämiseen.

Piirimme autopuhelinverkko käsittää tällä hetkellä 13 tukiasemaa, mutta jos saisimme nykyisten lisäksi eräisiin kriittisiin katvepaikkoihin neljä tukiasemaa lisää, olisi lähes koko tieverkostomme jo tämän palvelun kattava. Kaukokirjoitinverkko eli Telex-palvelu on pääosassa Lappia tyystin järjestämättä. Koko maakunnan saattaminen tuon palvelun piiriin ei onnistune ilman omaa telex-solmukeskusta, joka meiltä nyt puuttuu. Se olisi myös edellytyksenä Lapin liittämiselle muissa osissa Pohjois-Kalottia oleviin telex -verkkoihin. Rovaniemellä on nyt 100-numeroinen telex -päätekeskus ja Kemissä 50 -numeroinen tilapäinen telex- päätekeskus. Lähin tavoitteemme olisi saada Kemiin niin suuri uusi Telex-keskus, johon mahtuisivat kaikki talousalueen asiakkaat, jolloin Kemin nykyinen keskus olisi siirrettävissä esim. Sodankylään. Tällä voisimme käynnistää pohjoisten verkkoryhmien Telex-palvelun.

Piirimme organisaatio muodostuu Rovaniemellä olevasta piirikonttorista, muutamista piirin yhteisistä työryhmistä sekä tällä hetkellä kuudesta puhelinalueesta, joille tekninen suoritustehtävä on delegoitu. Lisäksi piirin alueella on telehenkilöstöä eräissä postiorganisaatioon kuuluvissa posti- ja lennätinkonttoreissa. Yhteensä teletoimen palveluksessa väkeä on täällä n. 1.300 henkeä, joista ylivoimaisesti suurimman ryhmän (noin 630 henkeä) muodostaa puhelinvälittäjäkunta. Toiseksi eniten on puhelinasentajia (noin 500 henkeä). Teknisiä toimihenkilöitä on 110. Muut ovat toimisto-, auto- ja kiinteistöhenkilökuntaa. Maakunta, jonka hyväksi Rovaniemen puhelinpiiri toimialallaan ponnistelee, kuuluu ns. kehitysalueeseen.

Artikkelin kirjoittaja: Veli-Matti Pesola

Viestiupseeriyhdistys ry:n tulevia tapahtumia

Webinaari marraskuussa 2023

Digitaalisen turvallisuuden webinaarin aamupäivällä 1.11.2023. Teemana on muun muassa avaruuden käyttö viestiyhteyksien muodostamisessa huomioiden kyberin aiheuttamat haasteet.
Webinaarin ohjelma ja kutsu julkaistaan verkkosivuillamme www.viestiupseeriyhdistys.fi piakkoin. Varaa aika jo kalenteristasi ja tule mukaan kuuntelemaan ja osallistumaan keskusteluun!

Seminaari helmikuussa 2024

VUY:n perinteinen kaksipäiväinen seminaari 13.-14.2.2024 teemalla ”Digitaalinen turvallisuus muuttuu – vai muuttuuko?” Miltä näyttävät digitaalisen turvallisuuden uhkat nykyisessä maailmantilanteessa? Kuinka EU/NATO-regulaatio vastaa ajan haasteisiin?
Tilaisuus aloitetaan 13.2. maaosuudella Helsingissä ja jatkuu Tallinnan laivalla/Tallinnassa 14.2. Alustajina toimivat jälleen maan parhaimmat asiantuntijat.
Seminaarin ohjelma ja kutsu julkaistaan Viestimies-lehdessä ja verkkosivuillamme www.viestiupseeriyhdistys.fi joulukuussa 2023. Varaa aika jo kalenteristasi ja tule mukaan kuuntelemaan ja osallistumaan keskusteluun!

SAVE THE DATE

Viestimies

MEDIAKORTTI 2023

ILMOITUSHINNAT (ALV 0%)

1/1 s	950 €
1/2 s	600 €
1/4 s	400 €
Takakansi	1200 €
Määräpaikkalisä	20 %.

ILMOITUSTEN KOOT

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

Aineistot:

PDF, CMYK Fogra Coated 27
Kuvien resoluutio: 300 dpi

AINEISTO-OSOITE:

juha.halminen@mediaosasto.fi

Viestiupseeriyhdistys ry:n julkaisema viesti-, johtamisjärjestelmä- ja ICT-alojen sekä kyberturvallisuuden päättäjien ja asiantuntijoiden lehti.

Esillä lehdessä – mukana päätöksiä tehtäessä!

AIKATAULU VUONNA 2023

Valmiin mainosmateriaalin toimitus

N:o	Aineistot	Ilmestyy
1:	8.2.	1.3.
2:	11.5.	5.6.
3:	31.8.	20.9.
4:	17.11.	4.12.

ILMOITUSMYYNTI

Juha Halminen
Gsm 050 592 2722
Sähköposti:
juha.halminen@mediaosasto.fi

PÄÄTOIMITTAJA

Pasi Puhakka
Gsm 050 529 0003
Sähköposti: viestimies@viestiupseeriyhdistys.fi

PAINOPAIKKA

Newprint Oy
Tuijussuontie 1
21280 RAISIO
Puhelin 010 231 2600
www.newprint.fi

JULKAISIJA

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

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