



INSINÖÖRIUPSEERILIITTO RY

***Insinööriupseeri***  
***2020***



# Insinööriupseeri 2020

## Insinööriupseeriliitto ry



Tässä lehdessä:

Puheenjohtajan terveisiä.....	5
Puolustusvoimien tekoälyn tiekartasta Puolustusministeriön strategisiin linjauksiin tekoälyratkaisujen kehittämiseksi.....	8
Työnteon uudet muodot - digitalisaation vaikutukset ihmisten työntekoon, kuormitukseen ja hyvinvointiin	14
Tekoäly taistelukentällä – mahdollisuudet ja rajat .....	23
Koneautonomian esiinmarssi ja tarvittava regulaatio.....	36
Digitalisaatio, uusi haavoittuvuus, osa 1 – kyber .....	41
Digitalisaatio, uusi haavoittuvuus, osa 2 – sähkömagneettinen spektri.....	52
Digitalisaatio- ja tekoälyosaamisen kehittäminen Puolustusvoimissa - innovaatioilla tulevaisuuden informaatioympäristöön .....	56
Perspektiiviä tekoälyn Hype-käyrään.....	61
Myydään neljä kiloa tekoälyä.....	67
Vuoden 2020 insinööriupseeri.....	74
Sotalaivaprojekti nyt ja tulevaisuudessa.....	76
130 TK tornikanuunan suuntausjärjestelmä .....	81
Insinööriupseeriliitto ry:n hallitus 2020 .....	89

## Insinööriupseeriliitto ry

PL 919, 00131 Helsinki

ISSN-L 1798-3622

ISSN 1798-3622

Offset Ulonen Oy, Tampere 2020



# Puheenjohtajan terveisiä

- Insinöörieversti Jyri Kosola -



Kun vuosi sitten kirjoitin mietteitäni, päällimmäisenä olo huoli siitä, että kaikilla oli krooninen kiire: töitä tauotta tekemälläkään niitä ei ehdi tekemään niitä kunnolla. Erilaisten ohjaus- ja koordinaatioryhmien vakioasioita oli henkilöstön uupuminen.

Nykypäivänä tilanne näyttää aika lailla erilaiselta. Ihmiset eivät enää kuluta koko työpäivää kokouksissa istumalla, kokouksesta toiseen säntäilemällä tai matkustamalla julkisissa liikennevälineissä. Kokoukset tuntuvat olevan paremmin organisoituja ja ne vaikuttavat sujuvan aiempaa nopeammin. Aikaa jää nykyisin myös asioihin perehtymiselle. Työnteko ei enää häiritse perhe-elämää siinä määrin kuin aiemmin.

Muutoksen sai aikaan pakko. Korona pakotti siihen, mihin valtionhallinto ei ehtinyt. Nimitäin pienen hienosäätämisen sijaan muuttamaan

radikaalisti sitä, miten työtä tehdään, missä sitä tehdään ja jopa, milloin sitä tehdään.

Me suomalaiset olemme eteviä tekemään välttämättömyydestä hyveen. Ehkäpä kansanluonteeseemme kuuluu tyytyminen nykyyhetkeen, mihin liittyy vaikeus tehdä radikaaleja muutoksia ennakoivasti ja jopa vaikeus nähdä erilaista tulevaisuutta. Tämän hetken muotiasana on digitalisaatio, joka on kenties oman aikamme suurin yhteiskunnallinen ilmiö. Tämän lehden teemana on digitalisaatioon liittyvät puolustukselliset ja puolustusvoimalliset näkökulmat.

Digitalisaatio muuttaa radikaalisti sekä työ- että yksityiselämää. Elinkeinoelämässä liiketoiminnan pelisäännöt ja ansaintalogiikat muuttuvat. Muutos kaataa nykyisiä vahvojakin yrityksiä, mutta myös luo uudenlaisia liiketoimintamahdollisuuksia uusille yrittäjille. Kokonaisia ammattikuntia häviää ja uusia syntyy. Moniko enää muistaa sellaisia asioita kuin valokuva-kehittäjä, videovuokraamo tai kopiointiliike? Tai sellaisia ammatteja kuin kirjasinlatoja, pankkitoimihenkilö tai puhelinvaihte? YTM Anitta Hannola käsittelee artikkelissaan työntekoa uusia muotoja ja vaikutuksia ihmisten työntekoon, kuormitukseen ja hyvinvointiin.

Puolustusvoimien digitalisaatio lähtee liikkeelle hallinnosta ja etenee operatiiviseen toimintaan. Myös tekoälyn hyödyntämisessä on nähtävissä eteneminen ensin helpommin realisoitavista hallinnollisista palveluista sekä teknisesti että eettisesti haastavampiin operatiivisiin toimintoihin. Insinöörieverstiluutnantti Tero Solante kuvaa omassa artikkelissaan strategioita tekoälyn hyödyntämiseksi. Majuri Tapio Saarelainen maalaa omassa katsauksessaan maisemaa tekoälyn mahdollisuuksista ja rajoista taistelukentällä.

Digitalisaatiota ja tekoälyä voidaan hyödyntää sekä hyvään, että pahaan. Ihan niin kuin

sähköäkin: sähköpöytä on hyvä, sähkötuoli paha, vaikka itse sähkö ei itsessään ole sen paremmin hyvä kuin pahakaan. Tekoälykään ei ole hyvä eikä paha. Ei ole myöskään siviilitekoälyä eikä sotilastekoälyä. On kuitenkin selvää, että niin kuin sähkön käyttöä, myös tekoälyn hyödyntämistä pitää säädellä. Silloin hyvästä rengistä ei tule huonoa isäntää. Tekoälyn regulaatiota meille avaa tässä lehdessä professori Pekka Appelqvist.

Digitalisaation myötä kaikkia munia ei panna samaan koriin, mutta kaikki korit ovat kiinni toisissaan. Pääsy yhteen koriin voi avata pääsyn kaikkiin koreihin ja yhden korin keikuttaminen heiluttaa muitakin. Suomeksi sanottuna sekä kyber- että elektronisen sodan käynnin uhka on otettava vielä nykyistäkin vakavammin. Näitä näkökulmia tuodaan esiin insinöörieversti Janne Jokisen ja insinööri-majuri Anders Furun artikkeleissa.

Tekoälyyn liittyy paljon odotuksia, joista osa on täysin ylimitoitettuja, mutta osa hyvinkin toteuttamiskelpoisia. Tämän hype-ilmion olemusta analysoivat insinöörieversti Olli Klemola ja diplomi-insinööri Aleksi Päiväläinen.

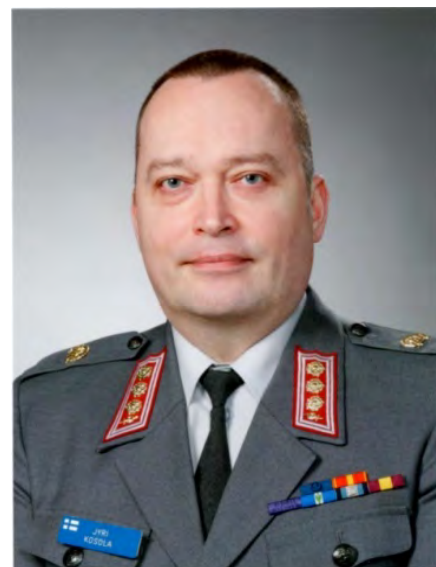
Se lehdestä. Olen toiminut Insinööriupseeriliiton puheenjohtajana seitsemän vuotta, joista viisi viimeistä yhtäjaksoisesti sääntöjen salliman maksimiajan. On siis tullut aika nuorempien astua kunniakkaan liittomme ruoriin. Kun myös liiton johdossa pitkään ja ansiokkaasti toiminut varapuheenjohtajamme Mikael Kaskelo on ilmoittanut vapauttavansa tehtävänsä nuoremmalle kohortille, on Insinööriupseeriliiton johto vaihtumassa. Nuorennusleikkaus on aina mahdollisuus kehittää toimintaa uusin silmin ja tuorein ajatuksin, vaikka saadun palautteen perusteella mitään akuuttia tarvetta muuttaa nykyisiä toimintatapoja ei olekaan.

Syksyn liittokokouksessa Tampereella Insinööriupseeriliiton puheenjohtajaksi valittiin insinöörieverstilutnantti Tero Solante ja varapuheenjohtajaksi insinöörieverstilutnantti Jouni Koivisto. Lämpimät onnittelut kummallekin, sekä menestystä tulevaan tehtävään!



Haluan tässä yhteydessä kiittää kaikkia viisivuotisen puheenjohtajuuskauteni hallituksen jäseniä hienosta työstä insinööriupseerien ammattikunnan eteen.

Yhdessä eteenpäin!



*Jyri Kosola*

# Patria

Kun kaiken on pakko toimia.



[www.patriagroup.com](http://www.patriagroup.com)

# **Puolustusvoimien tekoälyn tiekartasta Puolustusministeriön strategisiin linjauksiin tekoälyratkaisujen kehittämiseksi**

- Insinööriverstiluutnantti Tero Solante -

Koko maailma ja Suomi siinä saamalla ottaa käyttöönsä koko ajan enemmän ja enemmän sähköisiä palveluja niin työelämässä kuin vapaa-ajallakin. Informaatiota syntyy monissa tapauksissa enemmän kuin ihminen kykenee sitä järkevästi itse prosessoimaan. Tähän ongelmaan haetaan ratkaisua automatisoimalla informaation tallentamista sekä tukemalla tallennettujen tietojen käsittelyä ohjelmistorobotiikalla tai joissain tapauksissa jopa tekoälyllä avustettuna. Vaikka tällä hetkellä vain harvoja käytössä olevia sovelluksia voidaan aidosti kutsua tekoälyksi. Suurin osa on edelleen enemmän tukiälyä, jossa käytössä olevaa tietoa yhdistetään, analysoidaan tai jaetaan ennalta laadittujen ohjelmistoissa ja tietojärjestelmissä olevien sääntöjen avulla.

Puolustusvoimat, muun yhteiskunnan kanssa, on samassa tilanteessa. Erilaisilla automatisoiduilla informaation käsittelyillä pyritään vähentämään ihmisten työmäärää rutiiniluonteisissa tehtävissä ja vastaavasti kohdentamaan vapautuva työpanos varsinaisiin ydin-tehtäviin. Tämänkaltaisia ohjelmistorobotiikalla ja tekoälyllä tuettavia tarpeita on sekä hallinnollisten että operatiivisten tehtävien hoidossa. Hallinnollisia tukitarpeita, kuten esimerkiksi matkaesitysten ja -laskujen avustettu laadinta, on lukuisia ja niiden automatisoinnilla on mahdollista irrottaa työn tehostamiseen tarvittavia henkilötyöresursseja sellaisten tehtävien hoitamiseen, joissa vaaditaan ihmisen tekemiä päätöksiä. Operatiivisia tarpeita voivat olla erilaiset päätöksentekoa tukevat automaattiset toiminnot, ennustavaan kunnossapitoon liittyvät toimenpiteet sekä vastustajaan vaikuttavien asejärjestelmien automatisointi. Joskin jälkimmäisten tarpeiden toteuttamista ohjaa

vahvasti eettismoraaliset näkökulmat sekä kansainvälisessä lakivalmistelussa olevat esitykset mm. automaattisesti tappavien aseiden automatisoinnin rajoittamisesta (LAWS, Lethal Autonomous Weapon Systems)

Yleisesti tarkasteltuna tietokoneita ja ohjelmistoja on helppo hankkia eivätkä ne nykypäivänä ole enää kalliita. Uudet tekoälyratkaisut eivät kuitenkaan tule ilmaiseksi tai helpolla. Niiden rakentamiseen on investoitava sekä henkilöstövoimavaroja että taloudellisia resursseja. Henkilöitä ja erityisesti uuden tyyppistä osaamista tarvitaan omien prosessien tuntemiseen, mutta myös teknisten ratkaisuiden toteuttamiseen, jotka taas edellyttävät rahoitusta. Useassa yrityksessä, mutta erityisesti julkishallinnon organisaatioissa, rahoitusta suurempi ongelma on osaavan henkilöstön käyttöön saanti. Tekoälyratkaisuiden rakentamiseen tarvittavalle erityisosaamiselle on tällä hetkellä paljon kysyntää kaikkialla. Tämän vuoksi oman osaamisen kasvattaminen Puolustusvoimien tarpeisiin myös rekrytoimalla voi olla haastavaa.

## ***Tiedon syntymekanismin, tallentamisen ja tiedonkäsittelyn periaatteet***

Kaikki koneet tarvitsevat polttoainetta toimiakseen. Tekoälyjärjestelmien polttoaineeksi tarvitaan informaatiota, jota pitää olla tallennettuna riittävästi polttoainevarastoon. Mikä tahansa saatavilla oleva ja tallennettu informaatio ei kuitenkaan kelpaa tekoälyjärjestelmälle, vaan informaation tulee olla ennalta suunniteltua siten, että se soveltuu tekoälyllä tuettavan ja toteutettavan käyttötapauksen rakentamiseen.



// Bitwise toimittaa räätälöityjä ohjelmistoratkaisuja vaativiin toimintaympäristöihin. Osaamisemme luottavat esimerkiksi Sandvik, AGCO, Environics ja Cargotec.

# BITWISE

VALITSE BITWISE KUN TARVITSET

RAUTAISTA ASIANTUNTIJAA

*Sulautetut järjestelmät Koneenohjaus*

*Analytiikka ja AI Functional safety Mittaus*

*Autonomiset ajoneuvot ja järjestelmät*

Ota yhteyttä:  
[www.bitwise.fi](http://www.bitwise.fi)

## Laadukas ja toimintavarma ohjelmistoratkaisu ei synny sattumalta

Laadukas ohjelmisto on huomaamaton. Se toimii suunnitellusti eikä tee itsestään numeroa.

Paljon täytyy kuitenkin tapahtua ennen toimitusta. Laatu ei koskaan synny sattumalta.

Ohjelmistotoimittajan on sitouduttava laatuun työn jokaisella osa-alueella. Kehitysvaiheessa täytyy hallita esimerkiksi vaatimukset, koodauskäytännöt, riippuvuudet, testattavuus ja jäljitettävyyden aiheuttamatta kuitenkaan turhaa jäykkyyttä päivittäisessä työssä. Tässä tasapainoilussa onnistumisella on suora vaikutus projektin kaupalliseen menestymiseen.

Ohjelmistossa näkyy aina tekijöidensä kädenjälki, vähintään pinnan alla. Siksi ei

ole samantekevää, millainen tiimi sitä on tekemässä. Kehitystyötä ohjaa hallittu prosessi, mutta myös yhteistyö- ja kommunikointitaitoihin panostaminen kannattaa.

Kun ohjelmistoratkaisu on kehitetty kestävästi, muutosten tekeminen on helppoa ja niiden vaikutus koodiin hallittua ja rajoitettua. Investoiminen laadukkaasti kehitettyyn ja toimintavaraan ohjelmistoon vähentää ohjelmistovirheistä aiheutuvia kustannuksia sen koko elinkaaren ajan.

**Heikki Mäenpää**  
CTO  
Bitwise Oy

BITWISE

// Fetish for Code

Informaatiota kerätään hyvin monista eri lähteistä, kuten Puolustusvoimien omista hallinnollista tietoa käsittelevistä tietokannoista, internetin julkisista lähteistä tai erilaisista sotilaskäyttöön tarkoitetuista sensoreista. Käyttötapauksesta riippuen tieto tulee siirtää sellaiseen tietovarantoon tai -säiliöön, jossa erillisellä opetusdatalla muodostetut automatisoidut algoritmit ja komentosarjat voivat louhia tiedosta yhtäläisyyksiä ja riippuvuuksia muodostaen siitä uutta tietoa.

Jotta tämä tiedonkäsittely ja -louhinta olisi mahdollista, tekoälyjärjestelmän rakentamisessa ja käyttöönotossa tulee ottaa huomioon ainakin käytettävien tietolähteiden ja niiden sisältämän tiedon soveltavuus, tietolähteiden turvaluokka sekä niiden liittäminen tietoturvallisesti tekoälyn tietovarantoon. Mikäli tietoa on tarve siirtää eri turvaluokissa olevista tietojärjestelmistä toisiinsa, niiden välille tarvitaan yhdyskäytäväratkaisut, joiden avulla tarvittava kybersuojaus varmistetaan tietoturva-vaatimusten mukaisesti. Kaikki edellä mainitut haasteet korostuvat Puolustusvoimien tekoälyratkaisuissa, joissa informaatiota tarvitaan tekoälyjärjestelmän polttoaineeksi useista eri tietoturvaluokan lähteistä.

### ***KV-yhteistyö Puolustusvoimissa tekoälyratkaisuiden kehittämiseksi***

Tekoälyjärjestelmien kehittämiseksi ja rakentamiseksi tarvitaan uutta teknologiaa, joka ei ole vielä vakiintunut samalla tavalla kuin esimerkiksi yleisesti käytössä olevat tietojärjestelmät. Vaikka kaupallisissa siviilijärjestelmissä käytettävää teknologiaa sovelletaan sotilaskäytössä innovatiivisesti, on varsinaiseen sotilaskäytössä tarvittavan teknologian vakiinnuttamiseksi ja kehittämiseksi tehtävä yhteistyötä myös kansainvälisillä foorumeilla.

Puolustusministeriön ohjaamana Puolustusvoimat on verkottunut kansainvälisten toimijoiden kanssa tekoälyjärjestelmien käyttöönottoon liittyvien perusteiden laatimiseksi. Tällä hetkellä eettiset ja lakitekniset määrittelyt ja osin myös tulkinnat ovat työn alla useassa monikansallisessa yhteistyössä.

Tekoäly oli yksi Suomen vuoden 2019 EU-puheenjohtajakauden keskeisistä teemoista puolustuskyvyn kehittämistä koskeissa yhteisaloitteissa *'Digitalization and Artificial Intelligence in Defence'*. Puolustusvoimat oli Suomen puheenjohtajuuskauden teeman alustuksessa selkeässä pääroolissa. Perusteiden määrittämisen yhteydessä laadittiin *'food for thought paper'*, jossa digitalisaatiota sekä tekoälyn käyttöönottoa sotilaallisessa puolustuksessa käsiteltiin kolmen peruskysymyksen kautta; tekoäly sotilaallista toimintaa muuttavana teknologiana, tekoälyn vaikutukset sotilaallisiin suorituskykyihin sekä tekoälyn käyttöön liittyvä sääntely. Varsinaisessa EU:n sotilasesikunnan järjestämässä teemaseminaarissa useat maat totesivat jälkimmäisen peruskysymyksen rajaavan tekoälyn kehittämistä ja käyttöönottoa eniten juridis-eettisten haasteiden vuoksi.

Yhdysvaltojen asevoimien Joint Artificial Intelligence Center (JAIC) käynnisti vuoden 2020 elokuussa monenvälisen yhteistyöfoorumin *'AI Partnership for Defense'*. Yhteistyön tavoitteena on jakaa osallistuvien maiden kesken parhaat käytänteet tekoälyteknologian käyttöönottamiseksi puolustuksessa. Suomi osallistui käynnistävään kokoukseen 15.-16.9.12 muun maan kanssa. Tässäkin kokouksessa todettiin eettisten kysymysten ratkaisemisen olevan avainasemassa sotilaallisten tekoälysovellusten hyödyntämiseksi.

### ***Puolustusvoimien tekoälyn tiekartan suositukset***

Suomi ja Puolustusvoimat on ollut monien teknologioiden hyödyntämisessä etupainoinen moneen muuhun maahan verrattuna. Tekoälysovellusten kehittämiseksi Puolustusvoimat laati Puolustusvoimien strategiapäällikön päätöksellä vuonna 2018 tekoälyn tiekartan. Tässä tiekartassa määriteltiin perusteita tekoälyn ympärillä käytävään keskusteluun ja asioiden jatkovalmisteluun. Tarkastelu toteutettiin niin hallinnollisiin kuin operatiivisiin järjestelmiin liittyen. Tiekartassa suositeltiin käyttötapaukset, joiden kehittämisellä Puolustusvoimat kykeni ottamaan ensimmäiset askeleet tekoälyn hyödyntämiseksi. Vaikka

tarkastelu toteutettiin molemmissa toimintaympäristöissä, niin ensimmäiset sovellukset on toteutettu hallinnollisen työtaakan keventämiseksi, joilla vapautettiin henkilöstön työpanosta varsinaisten ydintehtävien hoitamiseen.

### **Puolustusministeriön strategiset linjaukset**

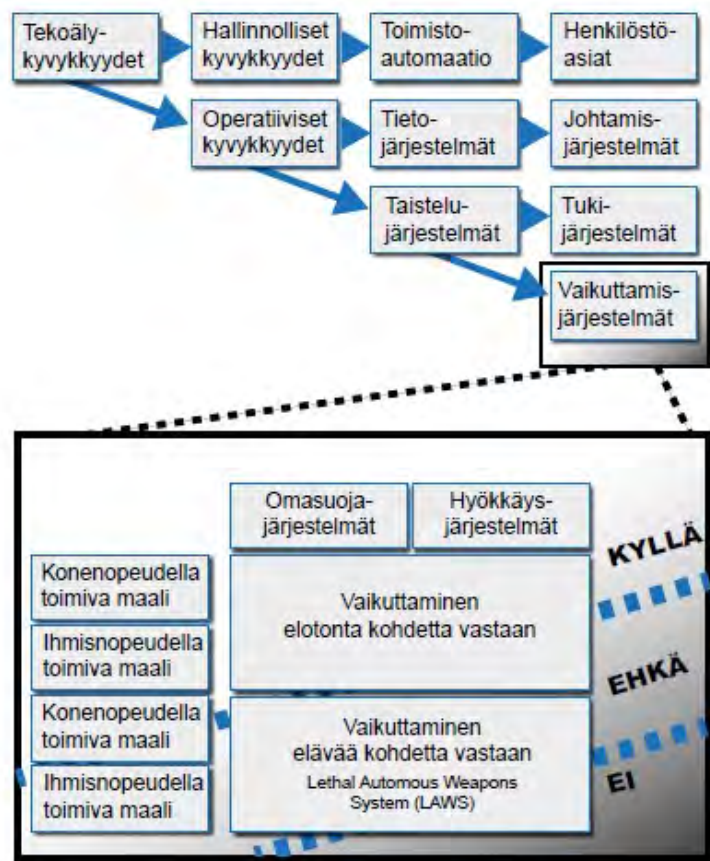
Digitalisaation ja tekoälyteknologioiden hallinnollisten perusteiden muodostamiseksi, Puolustusministeriö laati yhteistyössä Puolustusvoimien kanssa 'Strategiset linjaukset tekoälyratkaisujen kehittämiseen'. Tässä strategiassa todetaan, että Suomen on kehitettävä tekoäly- ja digitalisaatiokyvykkyksiään, jotta se voi säilyttää uskottavan puolustuskykynsä. Strategiassa todetaankin seuraavasti:

*'Perinteisesti puolustushallinto on kehittänyt suorituskykyään ostamalla valmiita ratkaisuja. Tekoäly ja digitalisaatio edellyttävät kuitenkin niin oman osaamisen kehittämistä kuin uusien kumppanien etsimistä. Tarvitaan kokonaisuutta palveleva tekninen infrastruktuuri, jonka varaan rakentuvat datan tallennus ja turvallinen jakelu sekä tekoälysovellusten kehitys ja implementointi tuotantoon. Tällaisen infrastruktuurin luominen edellyttää moderneja ja ketteriä ohjelmistonkehitysrutiineja ja -työkaluja.'*

Vaikka teknologia ja tarvittava infrastruktuuri ovat tärkeä osassa suorituskyvyn rakentamiseksi, niin strategia tunnistaa kehittämisen tärkeimmiksi teemoiksi hallintoon ja osaamiseen liittyvät osuudet. Strategian mukaisesti Puolustushallinto sitoutuu noudattamaan hallinnonalaan velvoittavia kansainvälisöikeudellisiä ja eettisiä velvoitteita kaikessa tekoälykyvykkyyskehittämässä. Tämän vuoksi myös Puolustusvoimat osallistuu aktiivisesti sekä kansallisten että kansainvälisten säätelyiden laatimiseen. Tällä työllä varmistetaan tekoälyn täysimääräinen hyödyntäminen kotimaan puolustuksessa, jottei kansallinen tai kansainvälinen lainsäädäntö

rajoita eettisesti hyväksyttävien, tarpeellisten ja tarkoituksenmukaisten tekoälyyn perustuvien ratkaisujen kehittämistä tarpeettomasti.

Yhdeksi strategian kulmakiveksi laadittiin kuva, jonka mukaisesti tekoälysovellusten käyttötapaukset ja niihin liittyvät moraaliseettiset sekä lainsäädännölliset soveltamisalueet ovat helposti hahmotettavissa.



Kuvan perusteella on helppo todeta, että suurin osa soveltamisalueista, niin hallinnollisessa kuin operatiivisessa toimintoympäristössä ovat lakiteknisesti tarkasteltuna toteuttamiskelpoisia. Ainoastaan vaikuttamisjärjestelmiin liittyvä kehittäminen on tarkasteltava tapauskohtaisesti. Vaikuttamisjärjestelmiin liittyvässä tekoälysovelluksien ja käyttötapauksien kehittämisessäkin pääosin vain autonomisesti elävää kohdetta vastaan toimivat asejärjestelmät edellyttävät huolellista pohdintaa. Näissäkin tapauksissa ihmisen tekemä päätös ennen vaikuttamista mahdollistavat tietyillä reunaehdoilla kyseisten tekoälyllä toimivien ase-

järjestelmien kehittämisen. Kuvassa ainoastaan mustalle alueelle jäävät LAW-järjestelmät vaativat syvällistä juridista ja eettistä pohdintaa.

Strategiassa on määritetty viisi selkeää linjausta; yhtenäiset strategiset linjaukset, ketteruus ja käyttötapauslähtöinen omistajuus, osaamisen aktiivinen kehittäminen, datan saatavuus ja joutavat ratkaisut sekä laillisuus, eettisyys ja avoin keskustelu.

Vaikka kaikki määritetyt linjaukset ovat tärkeitä osakokonaisuuksia tekoälyratkaisuiden kehittämiseksi, niin Puolustusvoimien kannalta tarkasteltuna osaamisen kehittäminen sekä lakitekniset ja eettiset kysymykset on ratkaistava ennen kuin varsinainen käyttöönotto voi tapahtua laajalaisemmin. Erityisesti osaamiseen liittyvät haasteet on ratkaistava kasvattamalla omaa osaamista sekä verkottamalla muun yhteiskunnan ja kumppaniverkoston kanssa. Tarvittaessa osaamista on hankittava määräaikaisella ulkoistamisella ennen kuin oma osaaminen on riittävällä tasolla.

Laillisuus- ja eettisyysnäkökulmista tarkasteltuna Puolustusvoimien tekoälysovelluksien kehittämisessä on tärkeä noudattaa kaikkia kansallisia ja kansainvälisiä säädöksiä kuitenkin siten, ettei omaehtoisella toiminnalla tai päätöksillä kiristetä tekoälysovellusten hyödyntämisen mahdollisuuksia tarpeettomasti muuta yhteiskuntaa ja kansainvälisiä yhteistyökumppaneita enemmän.

1	<b>Yhtenäiset strategiset linjaukset:</b> Puolustushallinnon strategisen tason suunnitelmat kaikille digitalisaation eri osa-alueille ovat yhteensopivia ja linjassa keskenään. Suunnitelmia päivitetään säännöllisesti.
2	<b>Ketteruus ja käyttötapauslähtöinen omistajuus:</b> Tekoälykyvykkyyksien tutkimus, kehitys ja ylläpito hankitaan ja resursoidaan ketterästi, jotta nopean teknologisen kehityksen suorituskyky potentiaali saadaan realisoitua. Ketteröittämistä tuetaan koulutuksella. Tekoälyratkaisujen ja niissä hyödynnettävän datan omistajuus on organisaatiossa toiminnan tai prosessin omistajalla.
3	<b>Osaamisen aktiivinen kehittäminen:</b> Tekoälykyvykkyyksien kehittämisessä kriittinen osaaminen turvataan rekrytoinneilla ja henkilöstön koulutuksella. Puolustushallinnolle luodaan aktiivinen yritysten, tutkimuslaitosten ja akateemisen yhteisön tekoälykumppaniverkosto, joiden kanssa osaamista kehitetään aktiivisesti.
4	<b>Datan saatavuus ja joutavat tekniset ratkaisut:</b> Puolustushallinnossa tunnistetaan, minkä datan on oltava saatavilla. Datan hallintaan tehdään tarvittavat prosessit. Puolustushallinnolle kehitetään suorituskyvyllään ajantasainen tekninen infrastruktuuri tekoälysovellusten ajamiseen. Sekä dataa, prosesseja että infrastruktuuria päivitetään iteratiivisesti.
5	<b>Laillisuus, eettisyys ja avoin keskustelu:</b> Puolustushallinto noudattaa hallinnonalaan velvoittavia kansainvälisöikeudellisiä ja eettisiä velvoitteita tekoälyn rakentamisessa ja käytössä sekä osallistuu aktiivisena toimijana niiden laatimiseen. Puolustushallinto osallistuu tekoälyn uhkista ja mahdollisuuksista käytävään julkiseen keskusteluun aktiivisesti.

## Lopuksi

Tekoälyratkaisuiden laaja-alainen käyttöönotto edellyttää vielä useiden kivien kääntämistä. Mitä enemmän automatisoituja sovelluksia otetaan käyttöön, sitä suuremmaksi muodostuu kyberuhkan muodostama hyökkäyspinta. Tämän huomioon ottaminen onkin yksi tärkeimmistä tehtävistä, jotta kokonaisuun puolustukseen kohdennettavien suorituskykyjen kybersietoisuus kyetään varmistamaan niin Puolustusvoimissa kuin myös muualla yhteiskunnassa.

Toimivaa, turvallista ja elinvoimaista  
**Suomea rakentamassa.**



CGI on globaali, Suomessa yli 3 700 asiantuntijaa työllistävä ICT-palveluyritys, joka konsultoi asiakkaitaan liiketoiminnan sekä ICT-ratkaisujen kehittämisessä ja on luotettu ulkoistuskumppani. CGI:n tavoitteena on toimialan laatujohtajuus toimittamalla palvelut ja projektit sovitun aikataulun ja budjetin mukaisesti. Lisätietoa [cgi.fi](http://cgi.fi).

# Työnteon uudet muodot - digitalisaation vaikutukset ihmisten työntekoon, kuormitukseen ja hyvinvointiin

- YTM Anitta Hannola -



## **Mitä tarkoittaa työnteon digitalisoituminen - mikä muuttuu**

Digitalisaatio työelämässä tarkoittaa toimintatapojen tai prosessien muuttamista digitaalisia välineitä (big data, mobiiliteknologia, pilvipalvelut, robotiikka, some, IoT) hyödyntä-

mällä. Asiakaspalvelua tultaneen automatisoimaan ja robotisoimaan entistä enemmän, jopa siihen pisteeseen asti, että 'virtuaalinen operaattori ei enää erotu ihmisestä'. Vaikka robottien fyysistäkin ulkonäköä voidaan muokata ihmisen kaltaiseksi, on vaikea uskoa, että robotit hyväksyttäisiin sosiaalisesti tai taitojensa puolesta kaikkiin rooleihin, esimerkiksi vanhusten hoidossa. Todennäköisesti robotit ja ihmiset tulevat työskentelemään yhteisesti, mutta länsimaissa ihmiset ovat mukana lopullisessa päätöksenteossa eettisistä syistä (etenkin miehittämättömien aseiden ja aseistuksen osalta). Robottien tullessa yhä sofistikoituneimmiksi ja ottaessa yhä enemmän vastuullisia tehtäviä, on otettava kantaa laillisuuskysymyksiin: kuka vastaa niistä toimintahäiriöiden yhteydessä - omistaja, valmistaja vai ohjelmoija? Lainsäädäntöön on tultava muu-

toksia, mutta on haasteellista saada lainsäädäntö pysymään teknisen kehityksen tahdissa.

### ***Teknologinen muutos ja sen vaikutukset yksilötasolla***

Millaisten osaamisten ja käytäntöjen ohjaamina työorganisaatiot eri aloilla ja toiminnoissa toimivat uusissa tilanteissa? Yhdistelläänkö ihmisen tekemiksi jääviä työtoimintoja entistä vaativammiksi ja monipuolisemmiksi kokonaisuuksiksi vai onko suuntana työn sisältöjen lisääntyvä sirpaleistuminen ja köyhtyminen? Teknologinen muutos sellaisenaan avaa mahdollisuuksia kumpaankin suuntaan etenevään työn muutokseen.

Erään tutkimuslaitoksen maailmanlaajuisen ennusteen mukaan automatisaatio on globaali muutosajuri, mutta sen hyödyntäminen vie kuitenkin vuosikymmeniä, ja ajallisuuden arvioinnissa on paljon epävarmuutta. Vuoteen 2040 mennessä on ennustettavissa, että teknisen automaation kehittyessä se olisi vaikuttanut korkeintaan 50 %:iin nykyisistä työtehtävistä, ja alhaisimmillaan reilusti alle 10 %:iin. Ammattien automatisoinnin sijaan on tarkasteltava ammatteihin liittyviä työtehtäviä niiden sisällä. Ammattien on todettu koostuvan hyvin monipuolisista tehtävistä, joiden automatisoinnin todennäköisyys vaihtelee suuresti. Kokonaisvaltainen automatisointi koskee vain harvoja ammatteja, mutta toisaalta osia työtoiminnoista voidaan automatisoida erittäin monissa ammateissa.

### ***Osaamisen uudet vaatimukset***

Yksilötasolla osaamisen, oppimisen ja koulutuksen ja taitojen muutokset toteutuvat joustavasti formaalin (tutkintoperusteisen) koulutuksen, non-formaalin oppimisen sekä uusien ja uudenlaisten taitojen hankkimisen ja ylläpitämisen välillä. Osaamistason riittävyys ja eri tavoin hankittujen osaamisten yhdistäminen ovat uusia haasteita niin yksilö- kuin organisaatiotasollakin. Tekoälyn tuomat uudet osaamisvaatimukset ovat aina jossain määrin

yhteen sopimattomia nykyisen osaamisen kanssa. Muuttuvat osaamisvaatimukset uusien teknologioiden käyttämisessä, sopeutuminen alituisiin muutoksiin työnteon tavoissa ja kasvavan tietomäärän hallitseminen lisäävät jo nyt psyykkisen kuormituksen kokemuksia kaikilla työntekijäryhmillä.

### ***Muutokset yhteiskunnallisesta näkökulmasta***

Kysymystä hyvästä tekoäly-yhteiskunnasta on sivuttu monissa tekoälyn soveltamista käsittelevissä raporteissa. Missään näistä ei ole kuitenkaan pyritty suoranaisesti rakentamaan kokonaisvaltaista hyvää tekoäly-yhteiskuntaa tavoitteeksi asettavaa strategiaa tai toimintaohjelmaa. Hyvän tekoäly-yhteiskunnan arvoiksi voidaan nostaa läpinäkyvyys, vastuullisuus ja laaja yhteiskunnallinen hyöty. Läpinäkyvyys tarkoittaa mm. aineiston keräämisen ja algoritmien avoimuutta, datan puhtautta ja oikeellisuutta sekä jäljitettävyyttä. Vastuullisuus tarkoittaa yhtäältä sitä, ettei tekoälyyn perustuva päätöksenteko uhkaa kenenkään terveyttä tai turvallisuutta: toisaalta sitä, että yhteiskunnallisella tasolla tekoälyratkaisujen edistämiseksi pitää huomioida työpaikkojen katoaminen. Yhteiskunnallisella hyödyllä tarkoitetaan kaikkien osaryhmien huomioonottamista sekä työelämän muotoilemista siitä näkökulmasta, että teknologia palvelee ihmistä eikä päinvastoin.

### ***Koulutuksen on muututtava***

Formaalissa koulutuksessa tulisi oppia ja harjoitella metataitojen ohella myös perusdigitaalisia taitoja tulevaisuuden lukutaitona (esim. data-analysointi ja ohjelmointi), kriittistä, analyttistä ja laajapohjaista ajattelua sekä ongelmien ratkaisutaitoja. Koulutus yksilöllistyy ja tehostuu kaikilla koulutusasteilla. Tekoälyn kehittyessä koulutusta on helpompaa yksilöidä ja tehostaa, koneen kyetessä oppimaan koko ajan lisää myös oppilaasta ja hänen taitotasostaan, sekä ohjatessa täydentämään osaamisvajeita.



## Joku Pasilassa on sinun asiallasi juuri nyt!

Vaikka liiton edunvalvontatyö voi vaikuttaa arjessasi etäiseltä, sen vaikutukset tuntuvat työelämässäsi päivittäin. Jos tietäisit, hämmästyisit siitä, miten monta ihmistä pitää tekniikan alan osaajien puolia edunvalvonnan rattaissa.



**Insinööriliitto**

Non-formaalien oppimisen taustalla ovat vaatimukset elinikäisestä oppimisesta, joka sisältää poisoppimista ja uudelleen oppimista, vastuuta oman osaamisen päivittämisestä sekä halua jatkuvaan oppimiseen ja kouluttautumiseen. Ihmisten itseohjautuvuutta sekä valmiutta muutokseen ja uuden oppimiseen tulisikin kehittää. Osaamisen kehittäminen on jatkossa tuotava vielä nykyistäkin vahvemmin työn oheen sekä osaksi työtä. Kun työ, opiskelu ja oppiminen kietoutuvat toisiinsa tulevaisuuden työurilla, on yksilötason tehtäväkuvia muokattava vastaamaan edellä mainittua kietoutuneisuutta.

Digitalisaatio tuo todennäköisesti tullessaan paljon sellaisia uusia ammatteja, joita ei ehkä tänä päivänä osata edes kuvitellakaan. Historiallisesti tarkasteltuna voidaan ajatella, että esimerkiksi 'sisällöntuottajan' ammattia ei vielä sukupolvi sitten ollut olemassa.

### Mahdollisia uusia, digitalisaatioon perustuvia ammatteja

palvelurobotin apulainen	alustamanageri
big datan syväasukeltaja	tekoälykasvattaja
personoitujen etämatkojen tuottaja	pilviturvapalvelukonsultti
kehomuunnelmiin erikoistunut eetikko	joukkoistuskoordinaattori
tekoäly - vuorovaikutuksen valmentaja	merkityksellisyysmuotoilija
jätedatan käsittelijä	priorisointivaikutusten simuloija
3D-elinten agentti	tiedonhankinnan joukkoistaja
data-panttivankitilanteiden ratkaisija	manipulointietsivä
itseohjautuvan liikenteen suunnittelija	superkykyvalmentaja
keinoliivatehtaan insinööri	tekoälyhallinnon kohtuullistaja



## Jatkuva oppiminen ja kouluttautuminen

Työpaikka on jo nyt ja tulee tulevaisuudessakin olemaan yksilön tärkein oppimisympäristö ja entistä suurempi osuus osaamisen uudistamisesta sekä kyvykkyyksien rakentamisesta tapahtuu työpaikoilla. Tähän vaikuttaa se, että aika on niukka resurssi ja täysiaikainen kouluttautuminen työn ulkopuolella on taloudellisesti haasteellista. Lisäksi tutkinto-opiskelu kestää pitkään, mikä tukee huonosti nykyistä nopea-tempoisempaa työelämälähtöistä osaamisen kehittämistä. Kun työ, opiskelu ja oppiminen kietoutuvat toisiinsa yksilöiden työurilla, on työnantajan / organisaation vastuulla päivittää tehtäväkuvia asianmukaisesti.

Vanhoista taidoista on luovuttava ja opittava ja omaksuttava uusia (*re-skilling*), mikä koskee erityisesti ikääntyviä työntekijöitä uuden teknologian hallinnan ja työurien pidentämisen ristipaineessa. Ikääntyvillä ei välttämättä ole uusien työtehtävien vaatimaa digitaalisia ja korkean teknologian taitoja, mutta kertynyt työkokemus mahdollistaa mm. johtajuutta ja asiakashallintaa vaativat tehtävät. Työntekijöiden siirtyminen uusiin työtehtäviin voi olla

hidas prosessi, mikäli uudet vaadittavat taidot ovat kovin erilaisia kuin edelliset. Työvoiman ikääntyminen ja tarve pidentää työuria tarkoittaa sitä, että työuran loppupuolelle tulee löytää joustavia käytäntöjä työuran jatkamisen tukemiseksi. Työtehtävien ja palkan tulee muuttua vastaamaan työntekijän tuottavuutta ja jaksamista, mikä edellyttää yksilöllisiä mahdollisuuksia vaihtaa tehtäviä ja sovittaa työaikoja työntekijän tilanteeseen sopivaksi.

## Työn käytännöt ja sisällöt muuttuvat

Yleisellä tasolla työn sisällöllinen muutos on ennen kaikkea siirtymistä tuottamisesta tietointensiivisyyteen ja merkityksellisyyteen; samoin työn organisointiin ja käytäntöihin liittyen siirryttäneen pysyvistä hierarkkisista organisaatioista väliaikaisiin ja itseorganisoi-tuviin yhteisöihin. Monista työntekijöistä tulee yhä itsenäisempiä ja itseohjautuvia, ja heidän työtänsä arvioidaan todennäköisemmin työn tulosten kuin siihen käytetyn ajan perusteella. Edellisen ohella ammattien sisältämät tehtävät monipuolistuvat ja kehittyvät tekoälyn myötä, ja yksittäisenkin työntekijän uusi työpanos tuottaa lisäarvoa.

**Millog**

**YHDESSÄ  
PAREMPI  
JA TURVALLINEN  
TULEVAISUUS.**

Turvaa kaluston koko elinjaksolle.

f \ \ \ in millog.fi



Tulevaisuusskenaarioissa asiantuntijatehtävät näyttäytyvät eri tavoilla: yhtäältä tehtävävetoinen asiantuntijatyö korostuu organisaatiovetoisen sijaan. Toisaalta myös tekoälyn rooli korostuu asiantuntijatyön apuna, ja asiantuntijuus keskittyy pienemmälle huippusaajien joukolle.

Tietotekniikan mahdollistama mobiilisuus voi parhaimmillaan tuoda työhön lisää työntekijälähtöistä joustavuutta (työn ja muiden vastuiden tehokkaampaa yhteensovittamista), itseohjautuvuutta ja mahdollisuutta työn ”tuunaamiseen”. Toisaalta se voi myös jatkuvan yhteydenpidon johdosta lisätä työn kuormittavuutta ja stressiä sekä pakonomaista sitoutumista työhön ja altistumista erilaisille haitallisille työympäristötekijöille. Psykkisen ja kognitiivisen kuormituksen kokemukset ovat jo nyt lisääntyneet, sillä teknologinen kehitys on lisännyt niin sanottuja hiljaisia vaatimuksia työntekoon ajasta riippumatta. Ilmiö työn sekoittumisesta vapaa-aikaan on entisestään vahvistunut: etenkin asiantuntijatehtävissä ympärivuorokautinen tavoitettavuus vähentää työntekijän mahdollisuuksia riittävään palautumiseen ja irrottautumiseen työstä.

Lisäksi laitteiden ja järjestelmien yhteensopimattomuusongelmista ei ole vielä kukaan päästy eroon.

Kuten mobiilistyönkin osalta, on virtuaali-tiimeistä olemassa lukuisia variaatioita, mikä näkyy myös niitä koskevan tutkimuksen kohteiden ja tulosten moninaisuudessa ja hajanaisuudessa. Suuri osa tutkimuksesta on kohdistunut erilaista tieto- tai asiantuntijatyötä tekeviin ja melko perinteisiin virtuaalisissa kommunikaatioissa käytettäviin välineisiin kuten sähköpostiin, pikaviestintään, online-keskustelupalstoihin tai audio- ja videoneuvottelukokouksiin. Virtuaalitiimien toiminnan osalta vaatimuksena on ihmisten välisen luottamuksen synnyttäminen ja ylläpitäminen sekä ihmisten väliseen kommunikaatioon ja toiminnan koordinaatioon liittyvien haasteiden

### ***Johtamisen ja organisaatiokulttuurin muutos***

Tulevaisuusskenaarioissa työntekijät toteuttavat aiempaa autonomisemmin ylhäältä annettuja tehtäviä, ja johtaminen saattaa olla ensi sijassa tehtävien tehokasta jakamista.

Organisaatiokulttuuri muuttuu oman työn johtamisen suuntaan, ja (hallinnollisten) esimiehien määrä todennäköisesti laskee. Vuonna 2040 hyvä esimies on vuorovaikutuksen asiantuntija, joka kehittää ja koordinoi osaamista sen sijaan, että vain autoritäärisesti delegoisi tehtäviä alaisilleen. Robotiikan yleistyminen muuttanee eniten etenkin suuria, asiantuntijoiden tiimeihin perustuvia organisaatioita, joilla on nykyään usein paljon keskijohdollista, roboteilla suoraan korvattavaa hallinnollista esimiestoimintaa. Robotisoituminen ei johdu pelkästään koneiden tehokkaamasta ja halvemmasta työstä, vaan myös edellä mainitusta työntekijöiden itseohjautuvuuden kasvusta.

### **Riskeihin varautuminen ja hyvinvoinnista huolehtiminen**

Digitaalitekniikan kehittymisen vaikutuksia voidaan arvioida fyysisten, psyykkisten ja sosiaalisten riskitekijöiden avulla. Fyysiset riskitekijät liittyvät esimerkiksi mobiili- ja etätöihin liittyviin ergonomisiin epäkohtiin. Psyykkiset riskit voivat olla yhteydessä työn ja vapaa-ajan yhteen kietoutumiseen tai teknologisten häiriöiden tai informaatiotulvan aiheuttamaan kuormittumiseen. Sosiaaliset riskit ilmenevät esimerkiksi kasvokkaisen kommunikaation ja yhteisöllisyyden vähenemisenä.

**Digitalisaatioon liittyvät riskitekijät** (Lähde: Alasoini, T. 2019; Digitalisaatiolla työn uudelleen ajatteluun)

- uusien teknologisten ratkaisujen perinteiset kuormitus- ja altistustekijät
- ihmisten ja robottien lisääntyvään fyysiseen läheisyyteen sekä robottien lisääntyvään mobiilisuuteen sisältyvät riskit
- ihmisten epävarmuus ja lisääntyvä riippuvuus tekoälyn tuottamien ennusteiden osuvuudesta ja luotettavuudesta
- koneiden tietoturvaluutteiden synnyttämät riskit
- dataistumisen synnyttämän informaatiotulvan aiheuttama kuormitus
- dataistumisen mahdollistama työsuoritusten entistä yksityiskohtaisempi valvonta ja työntekijöiden tietosuoja
- algoritmisen ohjauksen riskit koskien esimerkiksi lisääntyvää vieraantuneisuuden tunnetta,

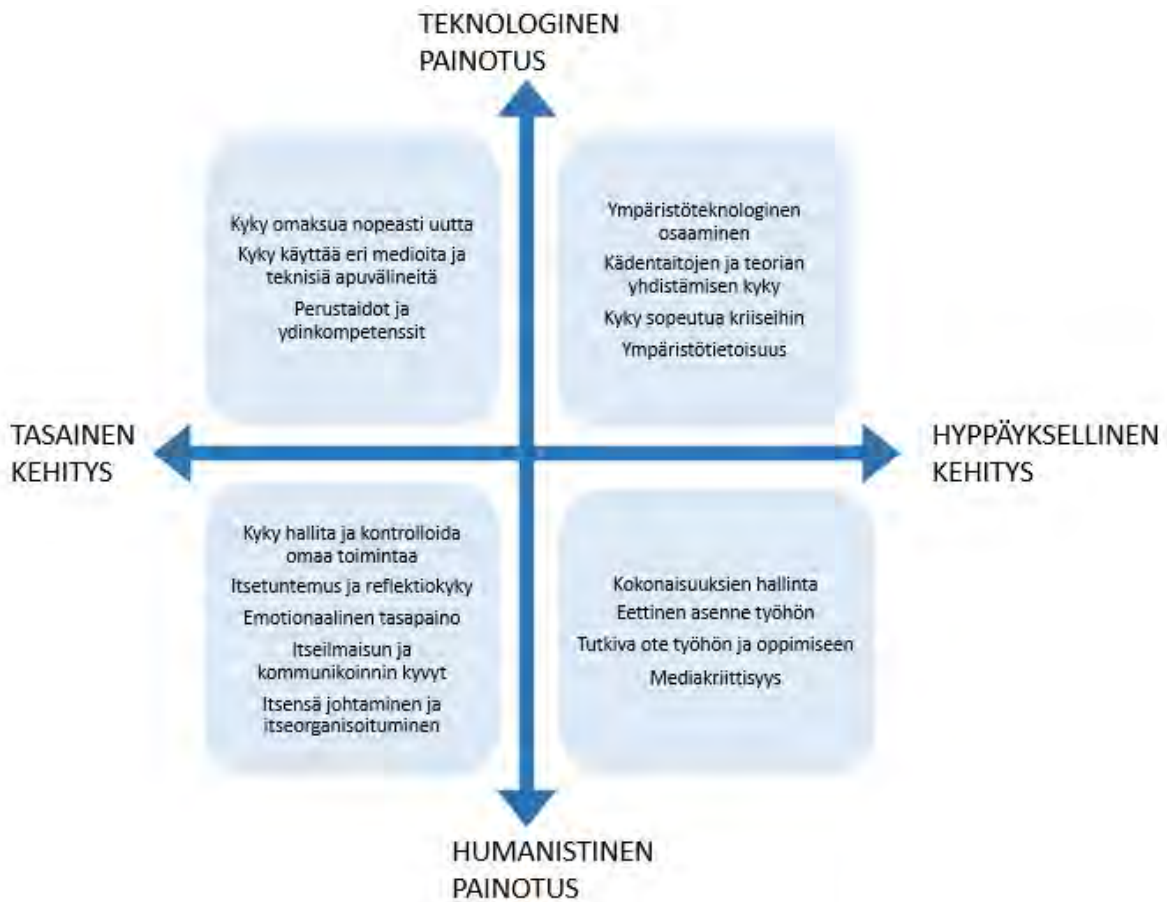
omanarvontunnon heikkenemistä ja työn mielekkyyden murenemistä
- lisääntyvään virtuaalisesti välittyvään kommunikaation sisältyvät ongelmat ja häiriöt
- lisääntyvän virtuaalisesti välittyvän kommunikaation aikaan saama kasvokkain tapahtuvan kommunikaation ja yhteisöllisyyden väheneminen
- työn läikkyminen vapaa-ajalle
- mobiilityön ergonomiset ja altistusriskit
- alustatyön tekijöiden oikeusturvan sekä turva- ja palvelujärjestelmien puutteet

SITRAn tulevaisuustyöpajojen tulevaisuusvisioissa on arvioitu, että vuonna 2040 työelämän hyvinvoinnista pidetään huolta toimeentulon, sukupuolten välisen tasa-arvon ja omaan työhön liittyvän päätäntävällän avulla. Itsejohtaminen ja siihen liittyvät taidot ovat yleistyneet positiivisena ilmiönä.

### **Miten selviän tästä yksilötasolla**

Tulevaisuuden taidot voidaan jakaa kolmeen eri kategoriaan: humanit taidot (perustaitoina havainnointi ja kommunikointi liittyen yksilöiden ja maailman väliseen suhteeseen), adaptiiviset tekniset taidot (mahdollisuuksien hyödyntämiseen) ja ennakointitaidot (epävarmuus- ja skenaarioajattelu). Humaaneista taidoista korostuvat empatia, luovuus, intuitio ja uteliaisuus taitoina, joita ei voi robotisaation tai automatisaation avulla korvata tai tuottaa. Kansainvälisten tutkijoiden mukaan teknologian syrjäyttäviltä vaikutuksilta ovat erityisesti suojattuina ne työtoiminnot ja -tehtävät, jotka edellyttävät luovaa tai sosiaalista älykkyyttä: näissä tarvitaan kyvykkyyksinä ainutlaatuisuutta, taiteellisuutta, sosiaalista havainnointia, neuvottelua, suostuttelua sekä auttamista ja välittämistä.

Koulutuksella on kuitenkin tärkeä rooli sen suhteen, että ihmisten kykyä luoda uusia ideoita, taitoa olla empaattisessa vuorovaikutuksessa ja vastuunottoa vahvistetaan. Uudet osaamiset voidaan myös asettaa typologiaan sen suhteen, onko osaamisissa teknologinen vai humanistinen painotus ja onko kehitys tasaista vai hyppäyksellistä.



*Tulevaisuuden osaamisia erilaisista näkökulmista (Lähde: Jokinen & Saarimaa 2013)*

Robotteja hyödynnetään edelleen sellaisissa työtehtävissä, jotka ovat yksinkertaisia, likaisia tai ihmiselle vaarallisia; sotilaskontekstissa esimerkiksi miinakenttien raivaamisessa. Toimitusketjut lyhenevät lisääntyvän (henkilökohtaisen) 3D -tulostuksen ja 'on-demand' -tuotannon yleistyessä - tällä on vaikutusta myös tuotannon hajauttamiseen ja siten työpaikkojen häviämiseen. Näyttää siltä, että suurin automaatiopaine kohdistuu edelleenkin matalapalkkaisiin ja vähemmän koulutusta vaativiin tehtäviin, ja työpaikan menettämisen riski on sitä suurempi, mitä matalampi on henkilön koulutustaso. Tekoälyn käytön ensimmäisessä vaiheessa on olemassa riski eriarvoisuuden kasvamiseen ja työmarkki-

noiden polarisaatioon. Robotiikka korvatesa tiettyjä tehtäviä, niissä tarvittavien taitojen markkina-arvo laskee ja vastaavasti uusien työtehtävien vaatimien taitojen kysyntä kasvaa - äärimmillään tätä polarisoitumista kuvataan 'supertähdet vastaan muut' -työmarkkinoina.

Yksilön koulutustason nousu mahdollistuu muun muassa sillä, että yhä suurempi määrä koulutuksesta on helpommin saavutettavissa on-line opiskelun avulla - erityisesti yliopistotasolla. Digitaalitekniikan kehitys vaikuttaa myös osaamisen kehittämisen tapoihin, sillä se mahdollistaa uudenlaisia virtuaalisesti välittyviä, verkko-oppimiseen, simulaatioon ja pelillistämiseen perustuvia oppimisen tapoja.



### ***Vaikutukset oppimiselle***

Tulevaisuudessa entistä tärkeämpänä ja välttämättömänä kyvykkyytenä on hallita ja hyödyntää sosiaalista verkkoa (social networks); näitä taitoja voikin luontevasti kehittää jo koulussa reaaliaikaisilla keskusteluilla ja virtuaalisilla luokkahuoneilla. Jos ja kun tekoälyä käytetään laajasti ihmistyötä korvaten ja täydentäen, on työntekijän edelleen ymmärrettävä, mitä tehtävää tekoäly tekee hänen puolestaan ja opittava hyödyntämään tekoälyä. Tähän liittyy myös opettaminen osana oppivien järjestelmien käyttöä.

### ***Epävarmuuden sietäminen***

Työn automatisaation vaikutus työntekijän toimintakykyyn on kuitenkin kaksijakoista: yhtäältä toimintakyky voi parantua tehtävien vaativuuden sekä oppimis- ja kehittämismahdollisuuksien lisääntyessä. Toisaalta toimintakyky voi heikentyä sopeutumistarpeen ja teknologiamuutoksen tuoman stressin ja epävarmuuden myötä. Uuden työn tekemiseen

liittyvää epävarmuutta voidaan tarkastella erilaisten sosioteknisten järjestelmien avulla. Nämä järjestelmät koskevat esimerkiksi sitä, kuinka työtä johdetaan ja organisoidaan (johtamis- ja organisointijärjestelmä), kuinka työsuhteen ehdot muotoutuvat (työsuhtejärjestelmä), kuinka työntekijöiden osaamista kehitetään (osaamisen kehittämisjärjestelmä) tai kuinka työntekijöiden terveydestä, turvallisuudesta ja hyvinvoinnista työssä huolehditaan (terveys- ja turvallisuusjärjestelmä).

### ***Mitä tämä tarkoittaa Puolustusvoimille***

Organisaatiolla on oltava valmiutta uudistamiseen sekä toimintakulttuurin ja toimintatapojen uudistamiseen, mikä edellyttää samanaikaisesti vanhoista käytännöistä luopumista. Esimerkiksi toimialan muuttuminen tai kokonaan uuden syntyminen edellyttävät samaan aikaan uusien teknologioiden luomista, ajattelutapojen uudistumista, suurten henkilöstöryhmien osaamisen ja ammattitunteiden päivittämistä. Tämä voi olla haasteellista Puolustusvoimien kaltaiselle organisaatiolle, jolla on byrokraattinen ja jäykkä maine.

Organisaation, Puolustusvoimien, on kyettävä sisäisesti ennakoimaan osaamistarpeita sekä osaamisen johtamista ja kehittämistä. Ennakoinnin on ulotuttava yhteistyöhön korkeakoulujen kanssa tulevien koulutus-tarpeiden suhteen. Muiden isojen organisaatioiden joukossa myös Puolustusvoimien tulee investoida elinikäiseen koulutukseen ja harjoitteluun pysyäkseen kilpailukykyisenä. Entistä laajemmalle joukolle voidaan tekoälyn ja digitalisaation avulla tarjota yksilöllistä opetusta ja koulutusta matalammin kustannuksin.

Työnantajalla / organisaatiolla on - yhdessä työntekijöiden kanssa - paras tietämys osaamisvaatimuksen muutoksista ja uusien osaamisten täsmällisten tarpeiden määrittelyssä. Osaamisen kehittämisen ja päivittämisen tulee-kin olla menestyvän organisaation strategisen johtamisen keskiössä: tällä varmistetaan korkea ja ajanmukainen osaaminen. Organisaation tulisi tarjota joustavaa ja kontekstisidonnaista oppimista, mikä toteutunee jo nyt Puolustusvoimissa. Koulutuksen ja osaamisen lisäämistä digitaalisista koneista, laitteista ja järjestelmistä, muuttuvista prosesseista ja työtoiminnoista esitetään yleisesti ratkaisuna työmarkkinakelpoisuuden säilyttämiseen - on kuitenkin tärkeää muodostaa kuva siitä, millaista luovaa ja sosiaalista älykkyyttä tarvitaan tulevaisuudessa. Onkin kysyttävä: millaisia koulutuksen sisältöjä, oppimisen tapoja, osaamisen yhdistelmiä ja organisatorisia innovaatioita ”koneen ja ihmisen” välinen vuorovaikutteisuus ja työ tarvitsevat.

Digitalisaation myötä entistä tärkeämpänä nousee esille kysymys tietoturvasta, sillä puutteellinen tietoturva altistaa ohjelmoitavia, älykkäitä ja oppivia koneita, laitteita ja järjestelmiä ulkopuolelta aiheutetuille häiriöille. Tällaiset riskit ja vaarat voivat aiheuttaa haittaa sekä organisaation toiminnalle, että ihmisten terveydelle ja turvallisuudelle.

Myös Puolustusvoimissa työn paikkariippumattomuuden ja monipaikkaisuuden vähentää

mahdollisuuksia ja tarvetta kontrolloida työ-aikaa. Työn tuloksia mitataan tällöin sisällöillä ja syntyneillä tuotteilla. Keskeinen haaste on, että työn ajan ja paikan joustot toteutetaan tavalla, jonka työntekijät kokevat tasa-arvoisena ja oikeudenmukaisena. Mikäli tässä ei onnistuta, voivat työmotivaatio ja sitoutuminen työnantajaan (tässä Puolustusvoimiin) heikentyä.

Voimankäytön hajaantuessa ja uusien turvallisuutta tuottavien toimijoiden ilmaantuessa, valtiojohtoisille puolustusvoimille tulee erityisiä haasteita rekrytointiin. Tulevaisuudessa jouduttaneen työnantajakohtaisiin, räätälöityihin rekrytointitesteihin, joissa on kyvykkyyss-testejä ja simulaatioita. Tällaisia toteutetaan jo nyt Puolustusvoimissa osana korkeimpiin asiantuntija- ja sotilastehtäviin hakeutuvien osalta. Lisäksi rekrytoinneissa painotetaan yhä enemmän taitoja ja kokemusta kuin akateemisia tietoja ja formaalista koulusta. Vuoteen 2045 mennessä saattaa DCDC:n (Development, Concepts & Doctrine Center, MoD, Britannia) arvioiden mukaan olla mahdollista, että rekrytointipäätökset tehdään yksinomaan kognitiivisten testien perusteella.

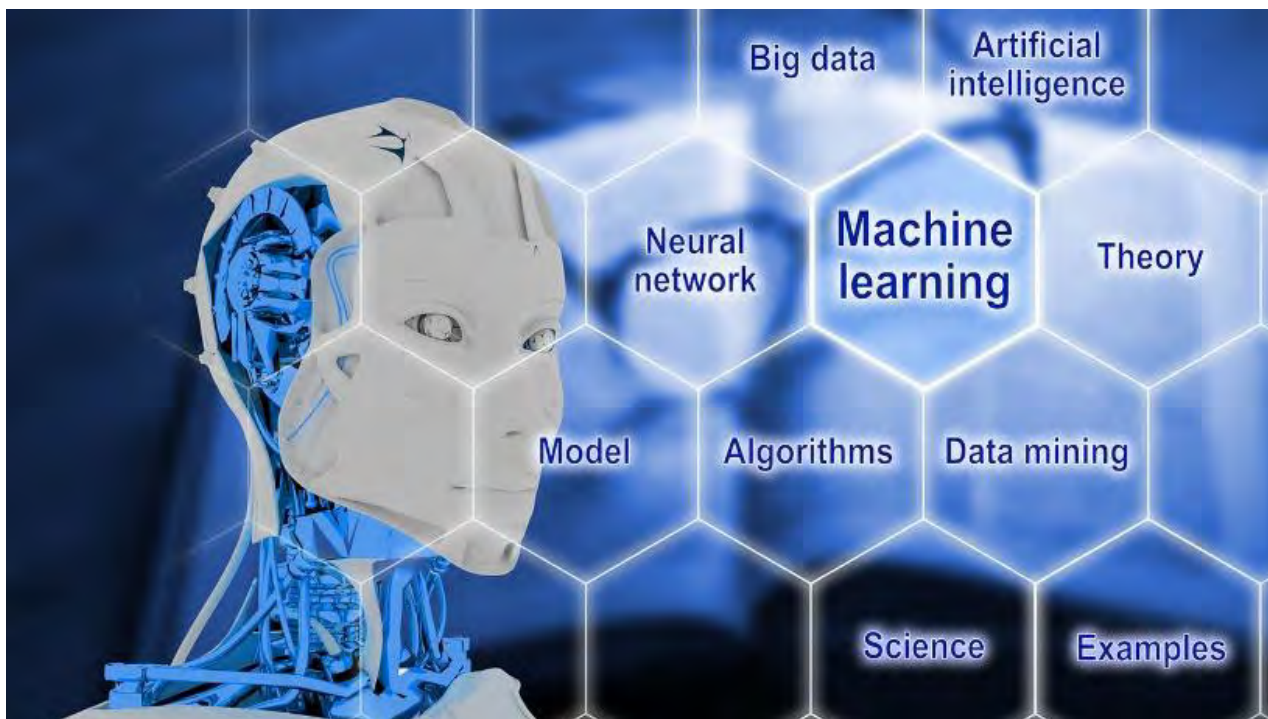
*Artikkelin taustalla tietopohja, jota on koottu tutkimushankkeeseen:*

### ***Työelämän ja yhteiskunnan muutosten vaikutus työn tekemiseen Puolustusvoimissa***

*Tutkimuksen tavoitteena on tarkastella, millä tavoin työelämässä ja yhteiskunnassa tapahtuvat muutokset vaikuttavat työn tekemisen tapoihin, rekrytointiin, sitoutumiseen ja sitouttamiseen sekä johtamis- ja organisaatiomalleihin Puolustusvoimissa. Tavoitteena on, että Puolustusvoimat pystyy ennakoimaan työelämässä tapahtuvia muutoksia sekä varautumaan niihin. Tutkimuksen aikajänne ulottuu 2040-luvulle, strategisen suunnittelurytmin mukaisesti. Tutkimus tarjoaa taustatietoja ja synteesejä henkilöstöjärjestelmän tueksi.*

# Tekoäly taistelukentällä – mahdollisuudet ja rajat

- Majuri (evp), dosentti Tapio Saarelainen -



[https://www.google.com/search?client=firefox-b-ab&biw=1280&bih=570&tbn=isch&sa=1&ei=OTSbXM2OEeyrgTR44\\_gBA&q=machine+learning+major+models&ogq=machine+learning+major+models&gs\\_l=img.3...11093.13688..13915...0.0.0.187.714.4j3.....0...1.gws-wiz-img.GYCNA-ipSvg#imgrc=3yH1p\\_PZlv\\_6oM](https://www.google.com/search?client=firefox-b-ab&biw=1280&bih=570&tbn=isch&sa=1&ei=OTSbXM2OEeyrgTR44_gBA&q=machine+learning+major+models&ogq=machine+learning+major+models&gs_l=img.3...11093.13688..13915...0.0.0.187.714.4j3.....0...1.gws-wiz-img.GYCNA-ipSvg#imgrc=3yH1p_PZlv_6oM)

*Artikkeli keskittyy tekoälyn mahdollisuuksiin ja rajoihin taistelukentällä. Tarkastelukulma on kriittinen. Tarkastelijan tausta on maavoimissa, joten artikkelin tulokulma on maavoimakeskainen, taistelukentän digitaalisuus ja tekoälyn mahdollisuudet ja rajat ovat artikkelin keskiössä. Lähdemateriaalina olen käyttänyt oman väitöskirjani materiaalia siltä osin, kuin se on ollut soveliaista, jolloin en ole lähdeä erikseen merkinnyt. Muiden kuvien osalta lähteet on aina mainittu kuvan yhteydessä.*

Tekoälyn halutaan taistelukentällä tehostavan sotilaallisia operaatioita. Tekoälyn saaminen osaksi taistelujärjestelmiä on välttämätöntä, koska taisteluiden tempo kiihtyy jatkuvasti. Samanaikaisesti sotilaallisten operaatioiden tavoitteet on saavutettava nopeammin. Tämän lisäksi kaiken taistelutoiminnan on oltava kustannustehokkaampaa kuin edellisellä kerralla. Lopuksi, tekoäly halutaan varmistamaan se, ettemme ammu vahingossa omia taistelijoitamme. Kaikissa näissä tavoitteissa

riittää tekemistä. Vaatimusten yhteensovittaminen tekoälyn avulla se vasta temppu onkin!

Artikkeli on rakennettu siten, että selvitän ensi nykyaikaisen taistelukentän luonnetta ja rakennetta. Seuraavaksi esitän tekoälyn suomia mahdollisuuksia taistelukentällä luvussa kaksi. Sen jälkeen keskityn tekoälyn tuomiin mahdollisuuksiin taistelukentällä, sitten tekoälyn rajoihin ja lopuksi arvioin tekoälyn tulevaisuuden mahdollisuuksia. Näkemykset ja mielipiteet artikkelissa ovat omia, ne eivät edusta Puolustusvoimien tai Lappeenrannan–Lahden teknillisen yliopiston mielipiteitä tai näkökantoja.

## **Taistelukenttä vuonna 2020**

Ennen kuin edes haaveillaan tekoälyn käyttämisestä taistelukentän operaatioihin, tulee suunnittelun lähtökohtana olla realismi. Pienellä ”sotavaltiolla” on pienet resurssit. Kaiken toiminnan perustana tulee olla realistiset suunnitelmat suorituskykyjen hankinnasta

ja toteuttamisesta. Suorituskykyjen hankkimisen jälkeen on vuorossa suorituskykyjen käyttöönotto, suorituskykyjen hyödyntäminen ja ylläpito sekä erilaisiin yllätyksiin varautuminen. Yleisellä tasolla voidaan lyhyesti todeta seuraavaa: Tosiasia on se, että nykyaikaisella monimutkaisella ja varsin nopeasti muuttuvalla taistelukentällä tulee ottaa huomioon ainakin seuraavat asiat: Energian tuottaminen, energian jakelu, energian jakelun turvaaminen sekä varajärjestelmät energian tuottamisen turvaamiseksi.



#### ***Taistelukenttää jalkaväkitaistelijan silmin kolmannella vuosituhatuulla.***

Nykyaikainen taistelukenttä on edelleen lihaa, verta ja ampumatarvikkeita sekä tulta ja liikettä. Edellisten lisäksi ovat tulleet erilaiset sähköiset järjestelmät. Analogisista sähköjärjestelmistä on tultu digitaalisiin sähköjärjestelmiin. Digitaaliset järjestelmät mahdollistavat suuremman laskentatehon ja ainakin teoriassa suuremman suorituskyvyn kaikissa sotilasoperaatioissa. Tämä edellyttää kuitenkin seuraavien asioiden toteutumista:

1) Operaatioita suorittavan tahon tulee ymmärtää sähkömagneettisen taistelukentän mahdollisuudet ja rajoitukset. Operoivan tahon tulee luoda digitaalisen sodankäynnin järjestelmille toimiva ja luotettava topologia, jota se kykenee hallitsemaan. Taajuushallinta, käytettävät aaltomuodot sekä käytetyt lähetystehot tulee osata optimoida, jotta signaalit etenevät sähköisessä taistelutilassa halutulla tavalla. Operoivan tahon tulee hallita vähintään se osa sähkömagneettista spektristä, jolla operoiva taho suorittaa digitaalisia toimia.

2) Energiansaanti on kyettävä turvaamaan kaikille järjestelmille saumattomasti ja luotettavasti. Toimivat digitaaliset järjestelmät voivat sijaita kaukana toisistaan, yhteydessä toisiinsa tai saarekkeisina järjestelminä. Energiansaanti on turvattava järjestelmän topologiasta riippumatta.

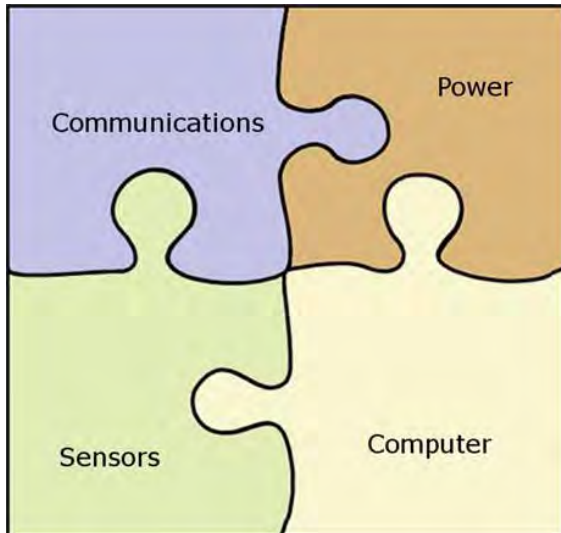
3) Omiin sensori- ja viestijärjestelmiin on ylläpidettävä reaaliaikainen luotettava ja turvallinen (OPSEC) yhteys. Omista sensoreista saatavaan tietoon on kyettävä luottamaan. Sensorijärjestelmät voivat olla yhteydessä toisiinsa kuituoptyksillä kaapeleilla tai erilaisten linkkien avulla. Sensoreiden tuottama tieto on oltava saatavissa jatkuvasti (24/7/365) huolimatta digitaalisen sodankäynnin vaikutuksista.

4) Viestiyhteyksien on toimittava kaikkiin sensoreihin, kaikkien järjestelmien ja laskentakeskusten (data-mining center) välillä, jotta tekoälyn hyödyntämisedellytykset taistelukentällä ovat olemassa.

Keskeistä on muistaa se, että mitä kauempana suurista taistelunjohtopaikoista- tai komento- paikoista ollaan, sitä enemmän tietoa siirretään ilmateitse. Ilmatie on haavoittuvin tapa siirtää tietoa. Tyypillisimmillään mikroaaltoratkaisut tarjoavat tiedonsiirtonopeutta tasoilla 10 Mbps – 100 Mbps aina 1 Gbps tasolle saakka, joista viimeksi mainittu tiedonsiirtonopeus on tyypillisesti toteutettavissa ainoastaan 1500 metrin etäisyydelle saakka. Jalkaväkikomppanioilla ei ole käytössään mikroaaltolinkkejä, joten niiden tiedonsiirtonopeus on varsin vaatimattomalla tasolla.

Kun nämä neljä lueteltua kokonaisuutta toimivat luotettavasti kaikissa taistelukentän olosuhteissa, voidaan tekoälyä alkaa hyödyntää taistelukentällä. Alla oleva kuva kiteyttää nykyaikaisen taistelukentän eri elementtien nivoutumisen toisiinsa. Nelikenttä on vaikea hallita taistelukentän muuttuvissa olosuhteissa.



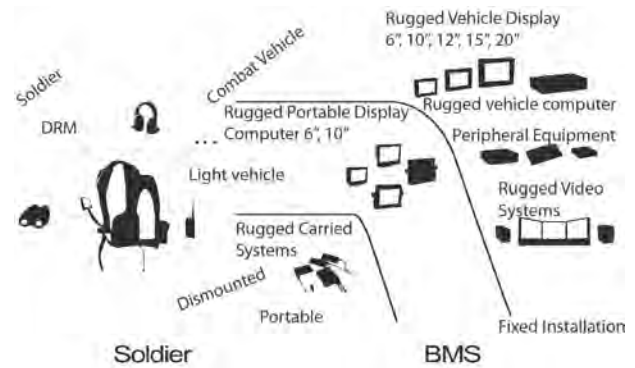


### ***Digitaalisen taistelukentän elementit.***

Edellisten neljän ”vanhan” vaatimuksen lisäksi viidentenä vaateena tekoälyn optimoinnin kannalta on paikkatieto. Paikkatiedon on oltava toimivien joukkojen ja materiaalin osalta luotettava ja jatkuvasti ajan tasalla. Tämä on kova vaade, joka sisältää vaateen niin jatkuvien viestiyhteyksien ylläpidosta energiankulutuksen hallintaan aina ruohonjuuritasolta, jalkaväkitaistelijasta, aina prikaati- ja taisteluosastojen tasolle saakka. Nämä suorituskyvyt puuttuvat edelleen. Nelikenttä –kuvasta puuttuvan paikkatietovaatimuksen merkitys on uusi ja samalla oleellinen vaade tekoälyä vaativissa sovelluksissa, jotka ohjaavat asejärjestelmien käyttöä.

Digitaalinen taistelukenttä on rakenteeltaan viereisten kuvien kaltainen. Digitaalinen taistelukenttä sekä tarvitsee sensoridatan jokaiselta sensorilta erilaisten taistelunjohtokeskusten ja tiedonlouhintakeskusten toimittamana sopivassa ja jo osin analysoidussa muodossa, jotta tiedon päätyessä aikanaan tekoälyä hyödyntäviin laskentakeskuksiin, se voidaan täysimääräisesti ja luotettavasti hyödyntää. Digitaalisen tiedon tulee kulkea ja siirtyä erilaisten rajapintojen kautta luotettavasti, ehyenä ja muuttumattomana, jotta erilaiset tekoälyyn perustuvat järjestelmät voivat saatua tietoa hyödyntää. Taistelukentän ruohonjuuritasolta tieto saapuu yleensä vihollisen vastatoimille edullisten matalatehoisten radioyhteyksien välityksellä. Alla olevissa

kuvissa kuvattuina alemman tason viesti- ja taistelunjohtojärjestelmiä.

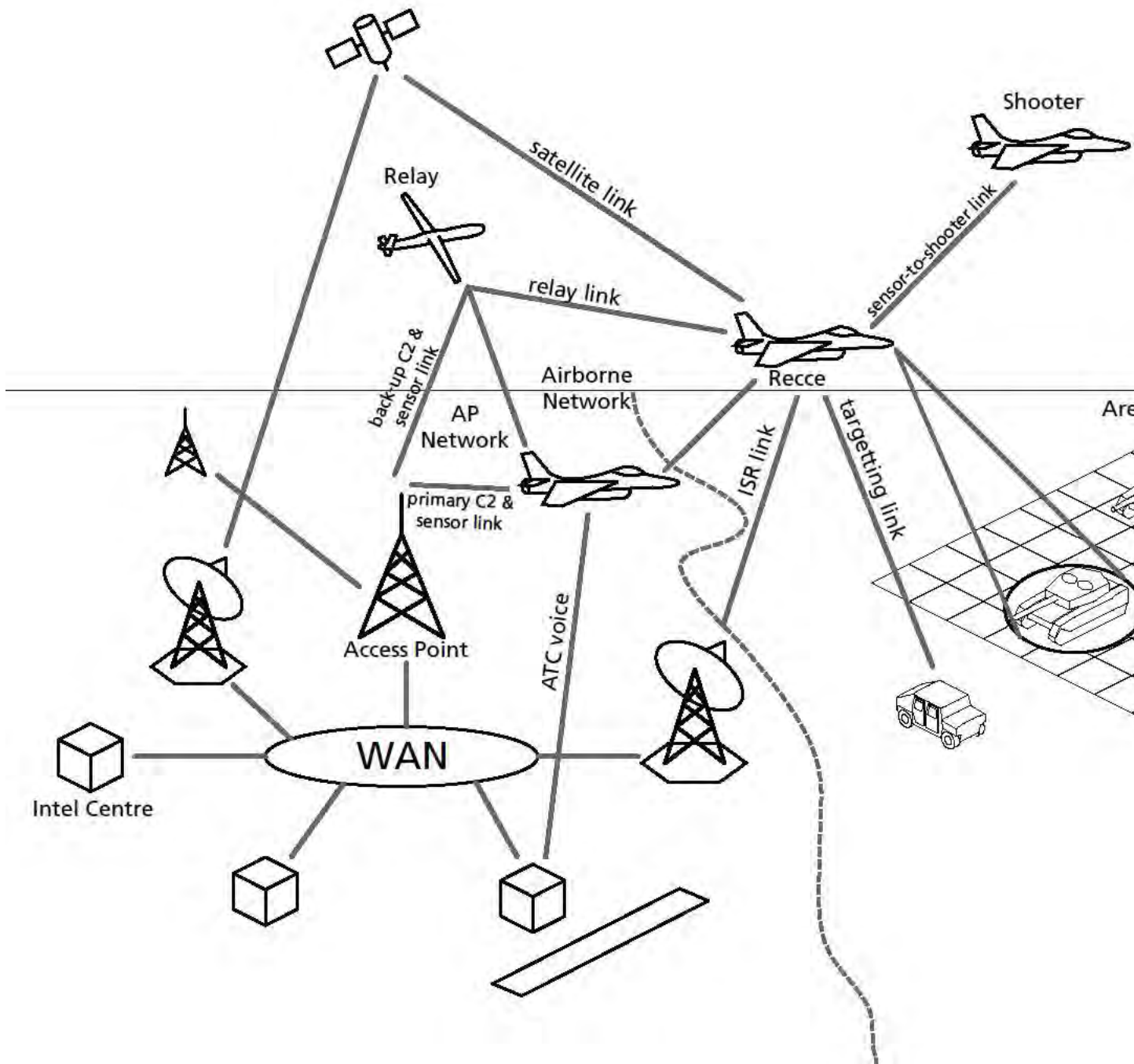


***Erilaisia järjestelmiä rajapintoiheen yksittäisen jalkaväkitaistelijan taistelunjohtojärjestelmän sekä taistelunjohtojärjestelmien välillä, päätyen taistelunjohtokeskukseen.***



### ***Erään taistelunjohtokeskuksen viestiyhteydet.***

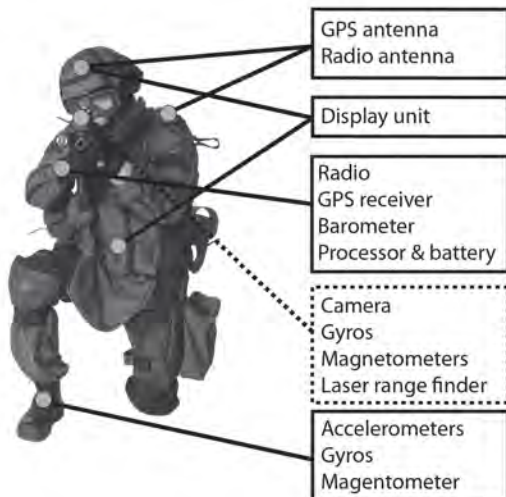
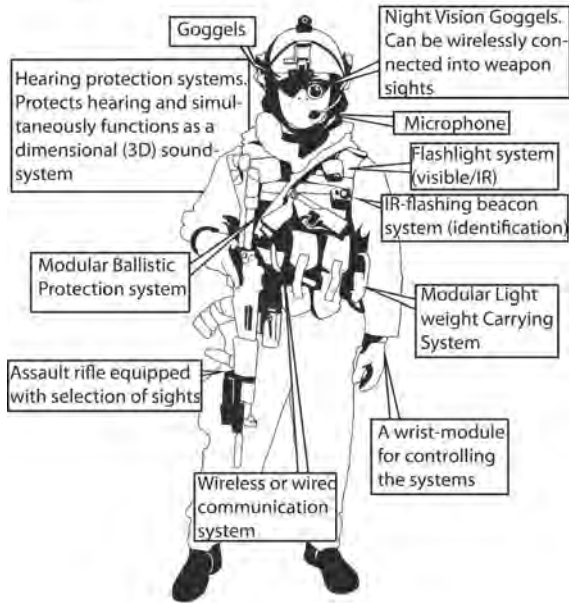
Seuraavissa on kuvattu taistelukentän digitaalista järjestelmää laajemmassa mittakaavassa. Digitaalisten viestijärjestelmien tulee luotettavasti toimia, jotta taistelukentällä toimiva tekoäly saa reaaliaikaista tilannetietoa. Tämä reaaliaikainen tilannetieto on tekoälylle välttämätöntä, jotta sen tekemiä suosituksia päätöksenteon tueksi kyetään jatkuvasti hyödyntämään eritasoisissa tilannekeskuksissa ja komentopaikoilla hyödyntämään. Tekoäly ei välttämättä pääte itsenäisesti vielä mitään, vaan päätöksen tekee toistaiseksi vielä ihminen. Kohti automatisoituja taisteluaita siirrytään, mutta tällä hetkellä tekoäly ei kykene kaikilla tasoilla tekemään järkeviä päätöksiä.



***Digitaalinen taistelukenttä pelkistetysti***

Tekoälylle tuotetaan tietoa muun muassa jalkaväkitaistelijan sensoripakettien avulla. Kukin jalkaväkitaistelija on eräänlainen sensoripaketti, joka tuottaa omalla taistelunjohtokeskukselleen tilannetietoa automaattisesti. Kukin jalkaväkitaistelija on eräänlainen liikkuva sensorilavetti.

An example of current Future Force Warrior System

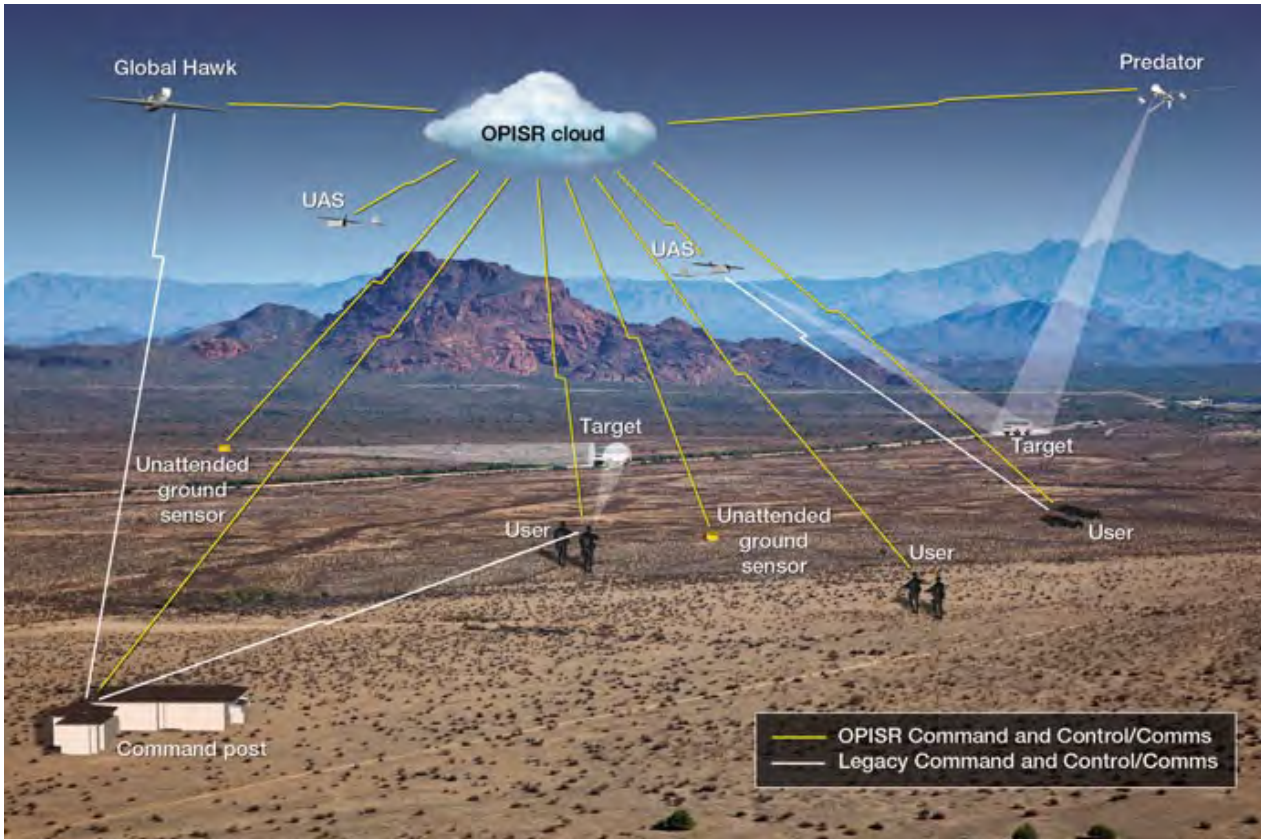


### ***Digitalisoitu jalkaväentaistelija sensoreineen.***

Sama tiedonkeruun mekanismi toistuu miehitettyjen ja miehittämättömien maa-, meri- ja ilmailulaitteiden osalta. Tiedonkeräämiseen tarkoitettujen sensoreiden on oltava tarkoituksenmukaisia, ja tiedonvälityksen tulee olla reaaliaikaista ja luotettavaa sensorista aina tekoälyä hyödyntävään tietojärjestelmään. Erilaisilta laveteilta kerätty tieto voidaan välittää pilveen, jossa on laskentatehoa ja joka voi esikäsitellä ja luokitella kerätyn tiedustelutiedon siihen muotoon, jossa tekoälyyn perustuvat järjestelmät voivat kerättyä tietoa hyödyntää. Aikoinaan tällainen käytössä ollut merkintäkielien standardi oli Extensible Markup Language (XML), joka toimi varsin hyvin käyttötarkoituksessaan.

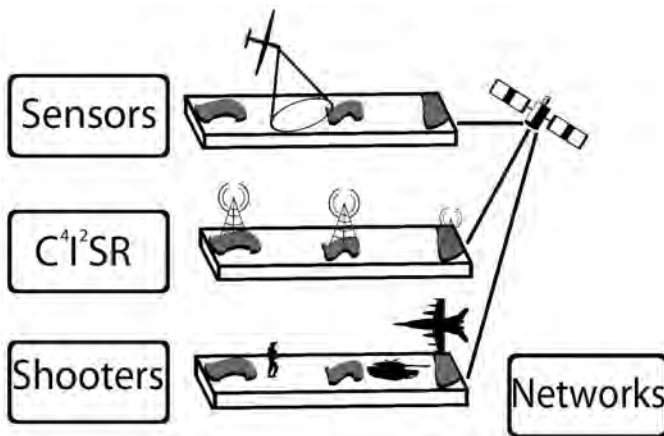
### **Tekoälyn mahdollisuudet taistelukentällä**

Tekoälyn mahdollisuuksia pyritään hyödyntämään taistelukentällä aloitteen tempaamiseksi sekä saavutetun edun ylläpitämiseksi. Alla olevassa kuvassa kokonaisuus on pelkistetyssä muodossa. Mikäli kaikki edellä, kohdissa 1 -4 luetellut ehdot sekä viidentenä vaateena esitetty paikkatietovaade toteutuvat, voidaan siirtyä tekoälyn hyödyntämiseen taistelukentällä. Pienen maan Puolustusvoimien kannattaa ottaa kaikki hyöty irti tekoälyn suomista suorituskyvyistä, mikäli se suinkin on kustannustehokasta ja taloudellisesti mahdollista.



**Tilannetiedon keräämiseen suunniteltu kokonaisjärjestelmä kuvana.**

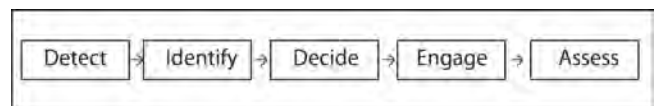
Lähde: [http://techdigest.jhuapl.edu/TD/td3102/31\\_02-Scheidt.pdf](http://techdigest.jhuapl.edu/TD/td3102/31_02-Scheidt.pdf)



asejärjestelmän käytön vaikutusten arviointi. Mikäli maali ei käyttäytymisellään osoita haluttua vaikutusta, ampumista jatketaan valitulla asejärjestelmällä, mahdollisesti vaihtaen tai muuttaen asejärjestelmän vaikuttavia aseita sekä niiden käyttämiä ampumatarvikkeita. Ampumista jatketaan niin kauan, että kohde toimii ampujan haluamalla tavalla, yleensä kohde lamautetaan toimintakyvyttömäksi tai tuhoetaan, jolloin siitä ei ole enää häiriöksi taistelukentällä. Sama vaikutus voidaan kohteessa joskus aikaansaada myös hybridi- ja kyber-vaikuttamisen menetelmin.

**Tiedonkeruu sensoreilta asejärjestelmälle.**

Taistelukentällä tapahtuvalle asejärjestelmien käytölle on tyypillistä, että maali tulee ensin havaita, tämän jälkeen se tulee tunnistaa ja luokitella, tämän jälkeen asejärjestelmän käyttävä taho päättää käytettävä asejärjestelmä sekä maalin suhteen optimaaliset ampumatarvikkeet ja tulimuodot. Tämän jälkeen tehdään ampumispäätös, jonka jälkeen asejärjestelmällä ammutaan, jonka jälkeen tehdään



**Detect, Identify, Decide, Engage and Assess – toimintaketju.**

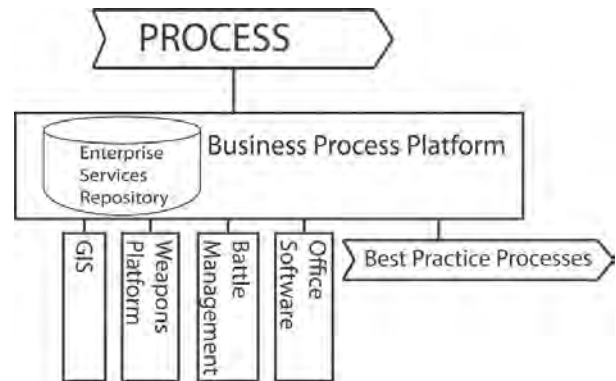
Tämä päätäntäketju voidaan ulkoistaa tekoälylle. Siinä ei ole teknisesti mitään ongelmaa, mikäli kaikki järjestelmän toimivuudelle välttämättömät, edellä jo

useastikin luetellut, komponentit toimivat. Ongelmia saattaa tulla eettisten asioiden osalta, mikäli koko toimintaketju annetaan tekoälylle.

Tarkastelemme tekoälyä alla olevan esimerkin kautta, jotta tekoälyä voidaan ymmärtää sen potentiaalisen suorituskyvyn kautta. Esimerkki perustuu aikaisempiin tutkimuksiini.

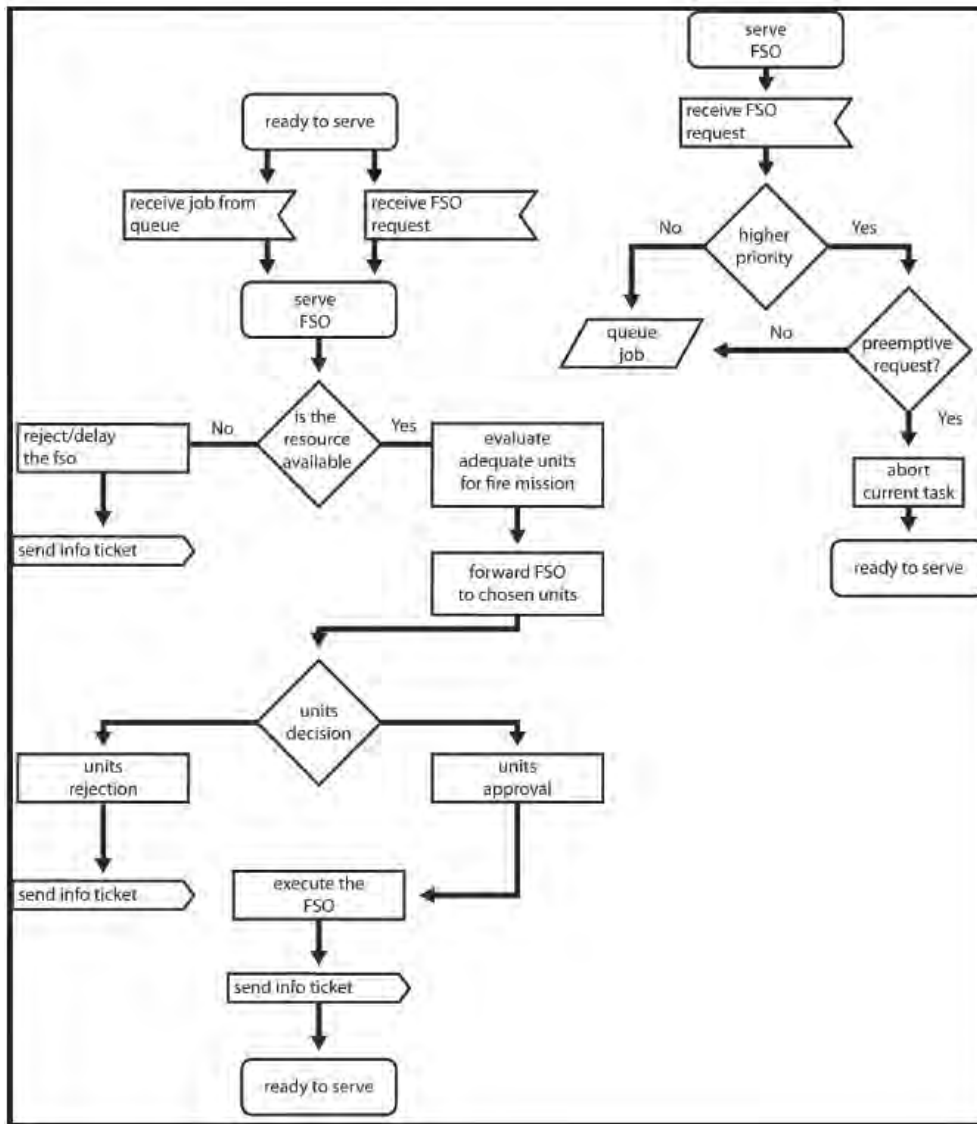
Tekoälyä voidaan käyttää erilaisten palveluiden tarjoajana taistelukentällä. Tämä onnistuu, mikäli tekoälyllä on tarkka paikkatieto (GIS) omista joukoista sekä vihollisen joukkojen ja rakenteiden sijainnista. Taistelu voidaan mallintaa tekoälylle eräänlaisina liiketoimintaprosesseina (Business Process). Näissä prosesseissa tekoäly on jatkuvasti, mieluiten myös varmennettujen yhteyksien kautta, yhteydessä paikkatieto-; asejärjestelmä-, taistelunjohtokeskuksiin sekä erilaisten signaali- ja järjestelmäkirjastoihin sekä tietokoneohjelmiin. Kun asia on tällä tavalla, tekoäly voi tuottaa halutun palvelun joko automaattisesti. Yleensä tekoällyn taso ei ole vielä nykyaikana kaikilla taistelukentän asejärjestelmien osalta niin valmis, että tekoälyllä voidaan antaa

automaattisesti lupa suorittaa jokin prosessi, esimerkiksi tulenkäyttöön liittyen.



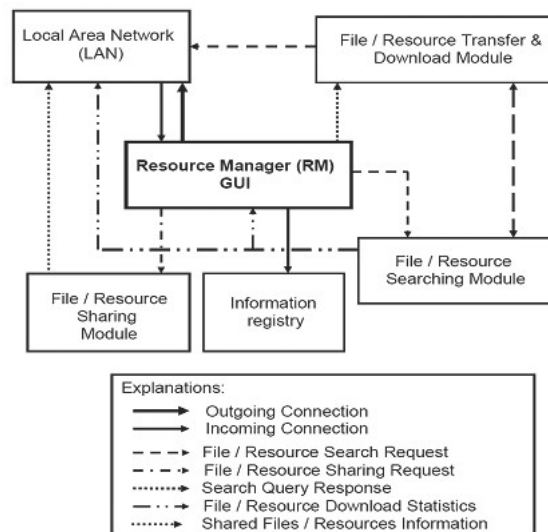
### *Liiketoimintaprosessi taistelukentällä.*

Otetaan käytännön esimerkki. Seuraava esimerkki perustuu tutkittuun tietoon. Seuraavassa kuvassa oleva esimerkki selvittää tulikomentopyyntöä SDL-diagrammin muodossa eräässä kokeellisessa järjestelmässä, jossa on mukana resursoija (Resource Manager).



*Tulipyynnö SDL –diagrammina.*

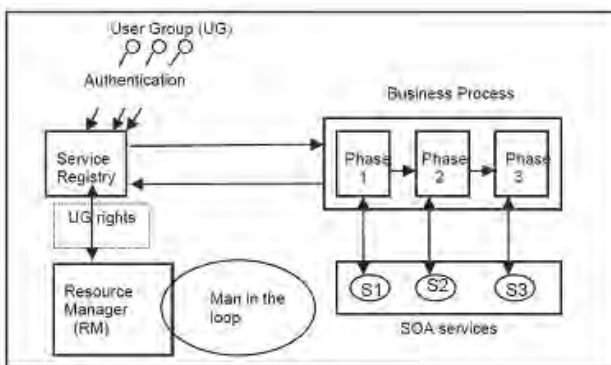
Oikealla esitetään resursoijan (Resource Managerin) toiminnallinen kuvaus. Resursoija on yhteydessä tietoverkkoihin ja erilaisiin tietokantoihin. Resursoija järjestee tekoälylle resursseja taistelukentän operaatioiden toteuttamiseksi. Resursoijan avulla taistelukentän tulipyynnöt, tukipyynnöt, huollon toiminnot (täydennykset, evakuoinnit, korjaustoiminta) sekä operatiivisten joukkojen liikuttelu voidaan toteuttaa, mikäli järjestelmä toimii aukottomasti ja aiemmin luetellut kohdat 1 – 5 toteutuvat jatkuvasti ja luotettavasti.



*Resursoija.*

Edellä selvitetty toiminnallisuudet vaativat toteutukseen vielä erään toiminnallisuuden. Tämä toiminnallisuus on palvelukeskeinen arkkitehtuuri, Service Oriented Architecture (SOA). Palvelukeskeinen arkkitehtuuri on ohjelmistotekniikassa käytetty arkkitehtuuritasen suunnittelutapa, jolla eri tietojärjestelmien toiminnot ja prosessit on suunniteltu toimimaan itsenäisinä, avoimina ja joustavina palveluina. Kun palvelukeskeinen arkkitehtuuri sekä liiketoimintaprosessi sulautetaan yhteen, voidaan luoda alla olevassa kuvassa näkyvä toiminnallinen kokonaisuus.

Tekoäly kykenee käsittelemään eri käyttäjäryhmien lähettämiä pyyntöjä koskien erilaisten resurssien (tulipyyntö, huollon toiminnot, joukkojen siirto) käyttöön saamista. Tämä pyyntö käsitellään tekoälyn mahdollistamana siten, että tekoäly hyödyntää tiedonkäsittelyssä resurssienresursoijaa sekä liiketoimintaprosesseja. Kuvassa tarkistetaan (Authentication) myös pyynnön lähettäjän oikeudet (UG Rights) (komppanianpäällikkö, pataljoonan komentaja, taisteluosaston komentaja) pyynnön esittämiseksi. Mikäli käyttäjän oikeudet pyyntöön eivät riitä, pyyntö evätään automaattisesti. Mikäli pyyntö on oikeutettu, resursoija tarkistaa pyydetyn suorituksen osalta kyseisen palvelun (tulipyyntö, joukkojen siirto, täydennys) tilan (vapaa, käytössä, huollossa) ja mahdollisuuksien mukaan toteuttaa pyynnön.



**Liiketoimintaprosessi ja palvelukeskeinen arkkitehtuuri kuvattuna yhdessä resursoijan ja erilaisten palveluiden (S1-S3) kera.**

Tekoäly ei tee itsenäistä päätöstä palvelun toimittamisesta tilaajalle, vaan mukana on ihminen (Man in the loop). Kun tekoälyn luotettavuus kasvaa riittävästi, ihminen tullaan

poistamaan edellä olevan kuvan mukaisesta toiminnallisuudesta.

## Rajat

Yllä olevan esimerkin kautta tarkastelin mahdollisuuksia hyödyntää tekoälyä taistelukentällä. Se on ainoastaan yksi esimerkki. Maalta, mereltä ja vedenalaisista toiminnoista voi kirjoittaa kukin alansa asiantuntija omansa. Kuvaamani esimerkki on sovellettavissa ja skaalattavissa ylös- ja alaspäin sekä kuhunkin toimintaympäristöön räätälöitynä sovellettavissa muiden aselajien ja puolustushaarojen käyttöön.

Siirrymme kirjoitukseni kriittiseen osioon. Mikäli luvussa yksi luetellut kohdat 1 – 5 eivät toteudu, tekoälyn käyttäminen vaikeutuu merkittävästi. Samassa tekoälyn käyttöön liittyvät riskit kasvavat suuressa määrin. Mikäli emme voi luottaa siihen, että tekoäly on jatkuvasti ”iskukunnossa” ja käytettävissä, emme myöskään luota siihen. Tällöin emme voi hyödyntää tekoälyn suomia mahdollisuuksia taistelukentällä. Luottamus tekoälyä sisältäviin päätöksentekojärjestelmiin on oltava aukoton, jotta tekoälyä voidaan täysimääräisesti hyödyntää taistelutilassa.

Sähkömagneettisen spektrin hallinta on erittäin vaikea asia jo rauhan aikana. Tästä olemme saaneet esimakua erilaisten hybridi- ja kyberhyökkäysten muodossa kokea. Milloin ovat palvelunestohyökkäykset ja muut ”madot” iskeneet valtiollisiin toimijoihin, milloin siviilikäytössä oleviin taajuuksiin. Myös pankkien ja vakuutuslaitosten palvelinten toimintaa on vakavasti häiritty vuoden 2020 aikana. Viestintäverkkojen aukottoman toiminnallisuuden turvaaminen on jo yksistään rauhanaikana mahdoton tehtävä. Erilaisia ”häiriöitä” esiintyy tämän tästä.

Mikäli paikkatietosovellukset ja niiden tukena olevat sensorit eivät tuota riittävän reaaliaikaista ja tarkkaa paikkatietoa, tekoälyn soveltaminen taisteluissa tuottaa aivan varmasti omia tappioita. Tekoälyn käyttöönoton eräs keskeinen suorituskyky on juuri se, että vältetään omien joukkojen ampuminen omalla

tulella. Tämä vaatii onnistuakseen luotettavan ja reaaliaikaisen paikkatiedon. Alla olevassa kuvassa on erään harjoituksen satoa, jossa paikkatietoa hyödynnettiin tilannetietoisuuden lisäämiseksi komentopaikalla. Kokeilu oli menestys, paikkatiedon keräämisen osalta.



### **Tracker-järjestelmällä tuotettu paikkatieto.**

Seuraava pulmatilanne: Signaali ei liiku sensorilta tekoälylle saakka, mikäli viestiyhteys sensorilta ”pääkallopaikalle” ei toimi reaaliaikaisesti ja luotettavasti. Erilaisia viestiliikenteen häiriöitä on rauhanaikanakin koettu sekä luonnollisten toimijoiden kautta, kuten myrskyt ja metsurit maasto-olosuhteissa sekä erilaiset ”kaapelinkaivajat” rakennetulla alueella. Sodassa häiriöiden määrä viestiverkoissa lienee erityisen suuri.

Digitaalisten laitteiden tarvitsema energia on ongelma. Samoin on energian tuottaminen, tuotetun energian siirtäminen kohteelle sekä energian varastointi tulevat sodassa olemaan se kaikkein suurin ongelma. Jo yksistään jalkaväkitaistelijaan suunniteltujen antureiden tarvitseman energiavarannon ylläpito vaatii huikean määrän erityyppisiä virtalähteitä, joita taistelija on kuljetettava mukanaan. Jo yksistään virtalähteiden kirjo on valtava tälläkin hetkellä. Sensoreiden virtalähteitä ei

ole vielä kukaan kyettä standardoimaan. Kaikilla laitevalmistajilla ovat omat ”mantransa” siitä, miksi juuri CR2032 paristo on ainoa oikea virtalähde juurikin tälle laitteelle. Jokin muu laitevalmistaja vannoo puolestaan CR123A virtalähteen nimeen. Sen lisäksi, että virtalähteen tyyppi muuttuu, virtalähteen tuotetun jännitteen säilyessä samana, joissain tapauksissa 3 Volttia, muuttuu virtalähteen tuottamien ampeerien määrä. Vaikka paristojen jännitteet ovat tasajännitteitä sekä arvoltaan yleensä välillä 1,5–9 V, näidenkin osalta voi olla laitekohtaista vaihtelua. Tämä tilanne vallitsee siellä ruohonjuuritasolla, jalkaväkitaistelijaan taisteluympäristössä.

Tilanne muuttuu sitä vaikeammaksi energia-asioissa, mitä ylempää siirrytään eri organisaatioissa ruohonjuuritasolta ylöspäin. Sähköä tuottavien aggregaattien lukumäärä on niiden tarpeeseen nähden voimakkaasti alimitoitettu. Aggregaattien tarvitseman polttoaineen kuljettaminen korpeen on sekin oma lukunsa. Valtakunnan sähköverkon toimivuus lienee ensimmäisiä asioita, jotka vihollinen Suomeen hyökätessään tuhoaa, mikäli se kuuluu hyökkääjän taistelusuunnitelmaan. Vihollisen toimintaa helpottaa avoimen yhteiskunnan tuottama Suomen sähköjärjestelmän verkkokartta, joka löytyy tyhmemmällekkin internetin käyttäjälle minuutissa.

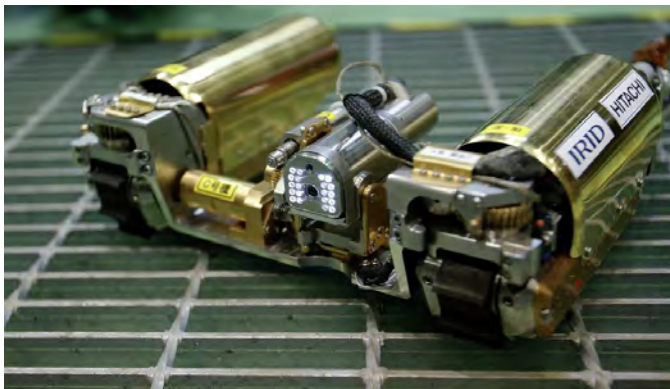
Tekoäly perustuu sarjaan algoritmeja. Ihminen on suunnitellut nuo algoritmit. Algoritmit tulee testata ja niiden toiminnallisuus ja luotettavuus tulee verifioida ennen tekoälysovellusten käyttöönottoa.

Venäläinen taisteluohje on: Harjoittele kuten taistelet. Tämän lauseen myötä voidaan siirtyä tekoälyn kanssa harjoitteluun. Kun tekoälyn kanssa toimitaan taistelukentällä, tekoälyn



tekemiin ratkaisuihin tulee kyetä luottamaan. Jotta näin tapahtuu, tulee toimintaa – päätöksentekoa ja resurssien käyttöä – harjoitella tekoälyn kanssa yhdessä. Tämä operaatio tulee suorittaa ennen taistelukentälle siirtymistä, oikeilla joukoilla, oikeilla resursseilla. Turvallisuudesta ei voida tinkiä. Harjoitukset tulee osittain simuloida, jotta voidaan järjestelmän vikaantumistilanteessa välttyä omilta tappioilta.

Taistelunkestävyys on vaade, joka koskee myös tekoälyä. Kuinka paljon digitaalista asevaikutusta tekoälyn on kestävä, jotta se edelleen toimii? Alla olevassa kuvassa on Fukushimaassa käytetty robotti, joka mittasi tuhoutuneen ydinvoimalan tuhoja. Laite tuhoutui käyttökelvottomaksi altistuttuaan voimakkaalle säteilylle työskentelyympäristössään kolmen tunnin aikana.



**Fukushiman ydinvoimalassa tuhoutunut robotti, joka työskenteli reaktorirakennuksessa.**

[https://www.google.com/search?q=fukushima+robots&client=firefox-b-ab&tbm=isch&tbs=rimq:CX4L1U\\_1JTnqIjhyCNP0uK1gEoPvSDG\\_14FbzjgLnViJaKbsk922EP5BMldyziWjh5BKVwFqib2LpwIRhY1XTJMHWJyoSCXII0\\_1S4rWoSEazyllEerARRKhJg-9IMb\\_1gVvMRcFJ5Sz6jAWAgEgmOoudWlllopuxE59q05al-BNC0SCST3bYQ\\_1kEwhEW0FzEpA0IDXKhJ3LOJaOHkEpURHCwbh5k0tkqEgnAWqJvYunAhBHBWYA--ZuPCyoSCWFjVdOMwdYnEaeMiDDk\\_1V8C&tbo=u&sa=X&ved=2ahUKEwjYw7SI56HhAhWxyKYKHcROABkQ9C96BAqBEBg&biw=1164&bih=553&dpr=1.65#imgrc=mDQ5IYu3RMNVYM:&spf=1553672071761](https://www.google.com/search?q=fukushima+robots&client=firefox-b-ab&tbm=isch&tbs=rimq:CX4L1U_1JTnqIjhyCNP0uK1gEoPvSDG_14FbzjgLnViJaKbsk922EP5BMldyziWjh5BKVwFqib2LpwIRhY1XTJMHWJyoSCXII0_1S4rWoSEazyllEerARRKhJg-9IMb_1gVvMRcFJ5Sz6jAWAgEgmOoudWlllopuxE59q05al-BNC0SCST3bYQ_1kEwhEW0FzEpA0IDXKhJ3LOJaOHkEpURHCwbh5k0tkqEgnAWqJvYunAhBHBWYA--ZuPCyoSCWFjVdOMwdYnEaeMiDDk_1V8C&tbo=u&sa=X&ved=2ahUKEwjYw7SI56HhAhWxyKYKHcROABkQ9C96BAqBEBg&biw=1164&bih=553&dpr=1.65#imgrc=mDQ5IYu3RMNVYM:&spf=1553672071761)

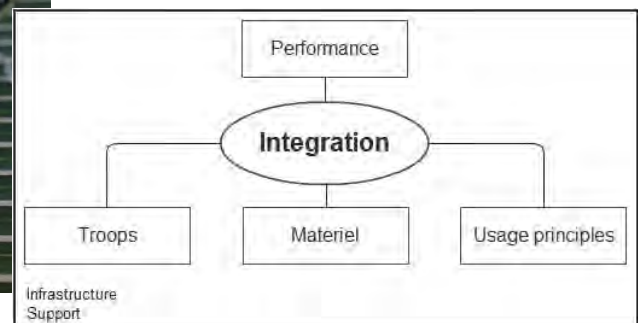
Lopuksi muutama inhottava kysymys: Mitäs sitten tehdään, kun tekoäly ei toimikaan? Kuinka tekoälyn toimivuus ja toimimattomuus voidaan havaita? Mitkä ovat työkalut, jotta voimme varmistua tekoälyn toimivuudesta ja tekoälyn tekemien ratkaisuiden järkevyydestä omaan taisteluamme liittyen? Mitä jos vihollinen onkin ottanut haltuunsa meidän tekoälyn suorituskyvyt käyttäen niitä omiin

tarkoituksiinsa? Kuka koodaa tulevaisuudessa ihmisen käyttämät algoritmit? Onko se robotti?

## **Tekoälyn tulevaisuus**

Varmaankin jossain vaiheessa tulevaisuudessa tekoäly voidaan ottaa osaksi taistelutoimintoja. Onhan tietokone voittanut ihmisen shakissa jo yli kaksi vuosikymmentä sitten. Kyseisessä pelissä oli maailman paras shakinpelaaja Garri Kasparov Deep Blue –tietokonetta vastassa. Toukokuussa 1997 Deep Blue voitti hallitsevan maailmanmestarin tuloksella 3,5 – 2,5. Lisäksi, heinäkuussa 2020 tietokone voitti ihmisen ilmataistelussa; onneksi kyse oli peliympäristössä toteutetusta kokeesta.

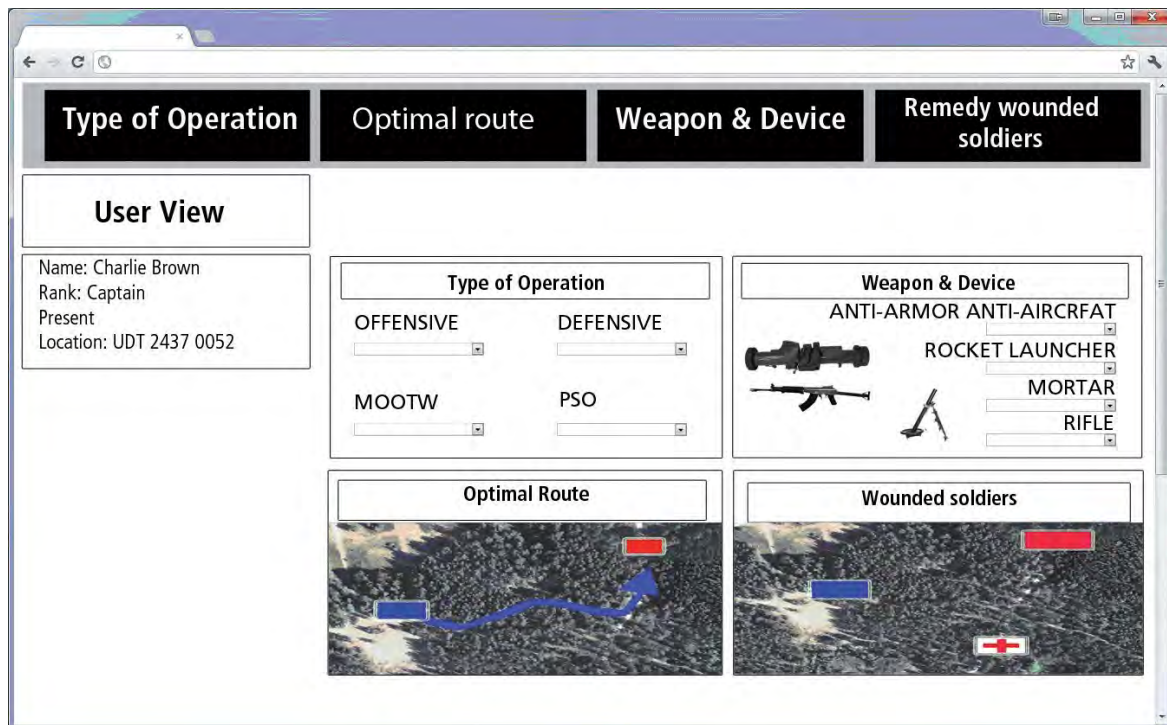
Järjestelmän suorituskyky rakentuu alla olevan kaavion mukaisesti. Kyse on siis myös integraatiosta, eli tässä artikkelissa siitä, kuinka tekoäly voidaan sijoittaa kyseiseen kuvaan. Tämän lisäksi tekoäly on saatava tuottamaan haluttuja tuloksia taistelussa.



## **Suorituskyvyn rakentuminen.**

Varmaa on se, että digitalisaation myötä taistelukentällä käytettävät koneet ja laitteet kallistuvat ja monimutkaistuvat jatkuvasti. Kysymys kuuluu: ”Millaisiin järjestelmiin meillä on varaa?” Vastausta ei tämän artikkelin kirjoittaja tiedä. Kysymys vastauksineen on siksi oleellinen, että meidän tulee mitoittaa omat resurssimme jollain tavoin. Kaikkeen ei pienen maan ”sotavoimilla” ole varaa nyt eikä varsinkaan tulevaisuudessa.

Jossain vaiheessa tekoäly saadaan osaksi taistelija järjestelmiä. Tavoitteena voi olla seuraavassa kuvassa esitetyn kaltainen näkymä taistelijan tietokoneesta, vaikka joukkueenjohtajan tasolla, aluksi.

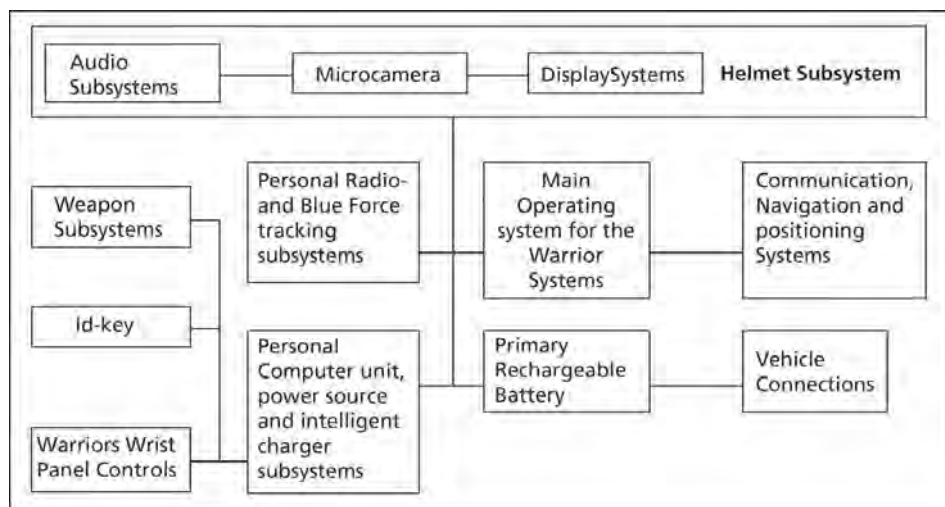


*Kuva tulevaisuuden taistelijan päätelaitteesta.*

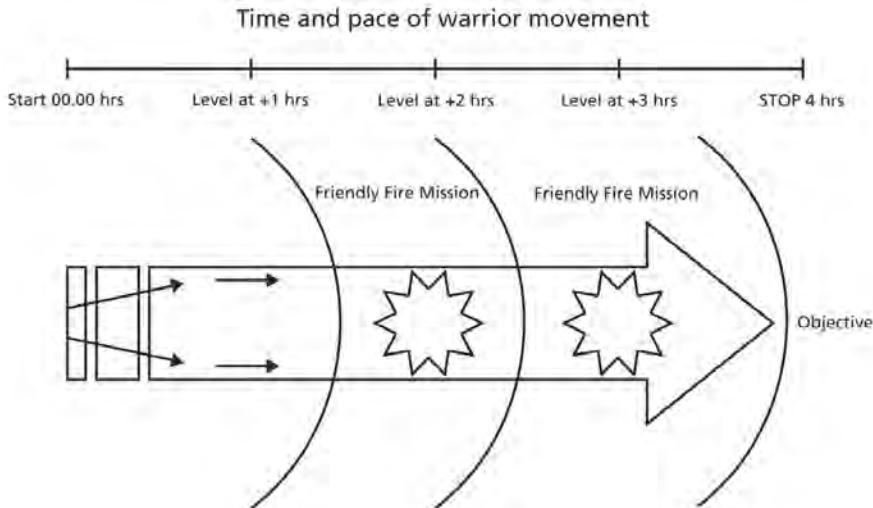
Viestiverkkojen hallinta tulee osata, jotta voimme valita oikeanlaiset tavat kommunikoida. Tämä vaatii sähkömagneettisen spektrin hallitsemista yhdessä erilaisten varajärjestelmien käyttöönoton myötä.

Koska järjestelmät monimutkaistuvat ja kallistuvat jatkuvasti, tulee tarkoin harkita mihin meillä on varaa. Alla olevassa kuvassa on kuvattu yksittäisen jalkaväkitaistelijan mahdollinen järjestelmä, aikaa tästä on liki kymmenen vuotta. Kuvassa oleva näkymä ei ole toteutunut vielä kotimaisessa jalkaväkitaistelijassa.

Tekoälylle on toki annettava mahdollisuus. Tietokoneavusteisesti voimme mallintaa esimerkiksi jalkaväkikomppanian hyökkäyksen alla olevan kuvan mukaisesti. Järjestelmä tarvitsee luvussa 3 kerrotun esimerkin mukaiset toiminnallisuudet. Kun esitetyt toiminnallisuudet otetaan menestyksekkäästi käyttöön ja saatetaan toiminnallisiksi, voidaan hyökkäys toteuttaa optimaalisesti.



**Taistelijan sähköinen luuranko.**



***Tekoälyllä avustettuna toteutettu optimaalinen hyökkäys resurssienkäytön osalta.***

Tulevaisuuden ennustaminen on vaikea laji. Voidaan kuitenkin hyvällä syyllä olettaa, että automaatio taistelukentällä kasvaa. Samoin sensorien määrä kasvaa yhdessä lisääntyvän tiedonsiirtotarpeen kera. Taistelukentän nopeuden oletetaan myös kasvavan, samoin kuin erilaisten taistelumenetelmien kirjo lisääntyä. Erilaiset hybridi-operaatiot muuttavat muotoaan, vaikuttaen yhä ennakoimattomalla tavalla, jo rauhan aikana.



***Vuonna 2018 esitelty taistelurobotti.***

Konearmeijoiden esillemarssia saamme vielä kuitenkin hetken odottaa. Tekoäly odottaa nurkan takana, mutta sen ilmestymisvuodesta ei ole tietoa. Koska sodissa halutaan välttää

ihmisuhreja, erilaiset ennalta ohjelmoitavat ja etäkäytettävät taisteluvälineet lisääntyvät maalla, merellä ja erityisesti ilmassa, vedenalaisia toimintoja tai avaruutta unohtamatta.

Lopuksi totean, että Suomessa taistelukentän olosuhteet ovat erittäin haastavat, kaikilla mittareilla mitattuina. Mikäli jokin taisteluväline toimii Suomessa, se toimii missä tahansa. Pitkät viestiysetäisyydet toteutuvat varmasti, samoin vaikeat maasto-olosuhteet yhdessä reippaiden lämpötilavaihteluiden kera, jotka Suomen Lapissa voivat olla helposti kahdenkymmen asteen tasolla niin kesällä kuin talvellakin.



***Tekoälylle pohdittavaa.***

<http://www.goodnewsfinland.com/feature/finland-paves-the-way-for-robotic-vehicles/>

Taajuuksien hallinta on jatkuva haaste yhdessä sähkömagneettisen spektrin ”orkestroinnin kanssa”.

Toivottavasti kriittinen artikkelini herättää ajatuksia tekoälystä, sen mahdollisuuksista ja rajoista.

# Koneautonomian esiinmarssi ja tarvittava regulaatio

- TKT, Professori Pekka Appelqvist -

## ***Teknologinen tilannekuva - missä menemme?***

Tietotekniikan kehitys on edennyt tietojenkäsittelyn abstraktiotason jatkuvan nousun myötä vaiheeseen, jossa laitteiden ja järjestelmien omatoimisuuden edellytykset laajenevat kohti monimutkaisempia kokonaisuuksia, myös dynaamisissa ja strukturoimattomissa tehtävissä ja toimintaympäristöissä. Yhä useammat tehtävätyypit mahdollistuvat täysin uusilla sovellusalueilla. Samaan aikaan saatavilla olevan datan määrä lisääntyy eksponentiaalisesti. Algoritmipohjainen päätöksenteko, tekoälyteknologiat, ohjelmistorobotiikka tai fyysisen robotiikan ilmentymät sekoittuvat usein merkityksiltään ja mielikuviltaan. Isossa kuvassa kehitys etenee yläkäsitteisesti kohti lisääntyvää koneautonomiaa. Ehkä näkyvin esimerkki tästä kehityksestä ovat autot, joissa erilaiset ajamisen apujärjestelmät avustavat kuljettajaa. Jossain vaiheessa kuljettajan rooli muuttuu aktiivisesta järjestelmäoperaattorista passiiviseksi prosessin valvojaksi, ja myöhemmin pääprosessin sivuosaan matkustajaksi.

Terminologisesti on siten perusteltua puhua järjestelmistä, joissa on autonomisia ominaisuuksia tai piirteitä. Tällöin ei tarvitse ottaa kantaa järjestelmän autonomian tasoon, joka voi joiltain osin olla hyvinkin korkea, kun taas jotkin ominaisuudet ovat täysin ihmisen hallinnassa. Esimerkiksi käy myös vaikkapa lennokkijärjestelmä, jonka alusta suorittaa annetun lentotehtävänsä täysin omatoimisesti, mutta jonka hyötykuormia ihminen käyttää. Edelleen on tärkeä ymmärtää, että eri toimintojen autonomia-aste voi muuttua eri tekijöistä johtuen dynaamisesti, jolloin järjestelmän autonomisuuden astetta on vaikea ilmaista yksikäsitteisesti.

Teknologisesti tarkastellen kehitys kohti koneautonomiaa vaikuttaa selkeältä ja

loogiselta jatkumolta –vaikkakin etenemisvauhdiltaan kehitys on epälineaarista ja toteutusteknologioiden osalta vaikeasti ennakoitavassa. Sen sijaan, kun tarkastellaan tilannetta ihmiskeskeisesti, on tultu suuren paradigmaattisen murroksen äärelle. Lisääntyvän koneautonomian myötä ihmisen suhde koneisiin on vähitellen muuttumassa työvälineestä omatoimiseksi apulaiseksi tai työkaveriksi. Kun ihmisten toimintajärjestelmään ilmestyy uusi aktiivinen entiteetti, on pelisäännöistä, hyödyntämisen etiikasta ja tarvittavasta sääntelystä sovittava oikeuksien ja vastuiden selkiyttämiseksi. Ihminen-kone – vuorovaikutuksen hallinta on keskeinen tekoälyn hyödyntämisen edellytys. Kyse on paitsi osaamisesta, myös menettelytapojen sopimisesta eri tasoilla; oman organisaation sisällä, kansallisesti ja kansainvälisesti.

Koneella ei ole omaa tahtoa tai kontekstuaalista ymmärrystä, jonka pohjalta se voisi itse arvottaa toimintansa perimmäiset motiivit ja määrittellä tavoitteet. Myöskään mitkään tunnetut koneoppimisen muodot eivät muuta tätä perusasetelmaa. Kaikesta koneautonomian tai tekoälyn edistyksestä huolimatta ei ole syytä hämärtää sitä tosiseikkaa, että **kehittyneinkin kone suorittaa pohjimmiltaan vain ihmisen sille määrittämiä tehtäviä**. Voiko koneelle joskus kehittyä tietoisuutta singulariteetin tuolla puolen, on sitten jo täysin eri keskustelu.

## ***Moraalista etiikan kautta regulaatioon***

Käsitehierarkiassa moraalit edustaa kulttuurisidonnaista arvopohjaa, siis yleisesti yhteisössä tavoiteltavia toimintaperiaatteita ja hyviksi koettuja käytäntöjä. Etiikka on puolestaan moraalipohjalle rakentuvaa teoretisointia ja formalisointia, tavoiteltavien arvojen systematisointia. Siirryttäessä edelleen kohti käytännön tekemistä, eettisten periaatteiden toimeenpanoa sekä toteutumista voidaan edistää ja valvoa regulaation kautta - regulaatio voi olla

esimerkiksi sopimuksia, sääntöjä, standardeja, tai lakeja.

Koska etiikka on vahvasti kontekstuaalista, eikä jokaista tapausta ole mahdollista ennakkoon normittaa, eettinen ohjeistus ilmenee tyypillisesti yleisinä periaatteina, jotka voivat olla vaikeasti toteutettavissa ja todennettavissa käytännön insinööriyössä. Kun ajatellaan monimutkaista teknistä järjestelmäsuunnittelua, joko kertaluonteisena suunnitteluhaasteena tai vähittäin rakentuvana kokonaisuutena, mahdollinen eettinen regulaatio määrittelee osaltaan vaatimusten minimitaso. Käytännön suunnittelukysymykset liittyvät paitsi teknisen toteutuksen oikeellisuuteen ja luotettavaan toimintaan, niin myös toisaalta arvovalintoihin, mitä ylipäättään katsotaan soveliaaksi koneen voivan tehdä tai päättää, tiedossa oleva koneen kognitiivinen suorituskyky huomioiden.

Eettisestä regulaatiosta tai sen puuttumisesta huolimatta on tarpeen tiedostaa, että lopputulokseen vaikuttavat vahvasti kaikkien järjestelmän suunnitteluun ja ohjelmointiin osallistuvien asiantuntijoiden sekä organisaatioiden arvot, käsitykset ja ammattietiikka. Yksittäinen algoritmi tai laajempi tietojärjestelmä heijastelevat suunnittelun ja toteutuksen kautta väistämättä myös tekijöidensä tapaa hahmottaa ja arvottaa tehtävää ja sen toimintaympäristöä. Koneautonomian suorituskyvyn kehittyessä ymmärrystä eettisten näkökohtien huomioimiseksi tulisikin lisätä koulutuksessa ja perehdytyksessä kaikilla tasoilla. Kuten järjestelmän kyberturvallisuus, myöskään etiikka ei ole erillinen toiminto, vaan läpäisee sisäänrakennettuna kaikki toiminnan tasot ja osa-alueet.

### ***Eettiset periaatteet***

Suomen AI-strategiassa (Suomen tekoälyaika, 2017) eettiset kysymykset mainitaan ”jatkokysymyksinä”, joita koskevia toimenpidesuosituksia ollaan vasta muodostamassa. Aiheesta on sittemmin laadittu useita tutkimus- ja selvitysraportteja, ja mm. yrityksiä on kannustettu eettiseen periaatteidensa kirkastamiseen. Nykyisin perusarvopohjaisen ihmis-

keskeisyyden korostaminen tekoälyn hyödyntämisen lähtökohtana on vakiintunut Suomen virallisiin kannanottoihin ja ohjaaviin periaatteisiin.



Osana EU:n AI-strategiaa vuonna 2018 julkaistiin geneeriset luotettavan tekoälyn eettiset periaatteet (Ethics Guidelines for Trustworthy AI), nämä ovat: Human agency and oversight; Technical robustness and safety; Privacy and data governance; Transparency; Diversity, non-discrimination and fairness; Societal and environmental wellbeing; Accountability. EU:n piirissä ja Suomessakin on vahvistunut näkemys, että eurooppalaisen tekoälyn hyödyntämisen ja sovellusten tulisi olla niin arvopohjaltaan kuin kilpailutekijänä eettisesti korkeampitasoista kuin USA:lla ja Kiinalla, jotka ovat muilta osin markkina-johtajia tekoälyn alustataloudessa, teknologisesti ja datan hallinnassa.

Eri organisaatiot, valtiolliset ja yksityiset, ovat julkaisseet tekoälyn soveltamiseen liittyviä eettisiä periaatteitaan. Kirjoittajan havaintojen mukaan yleensä näissä toistuu jokin valikoima seuraavassa luetelluista teemoista, suluissa mainittuna useimmin käytettyä käsitteistöä. Käsittekokoelma kuvastaa haasteen laajuutta, kun ihmisen tai ihmisorganisaation toimintaa lähdetään koneellisesti auttamaan tai korvaamaan:

- Vastuullisuus (responsibility, accountability)
- Oikeudenmukaisuus (fairness, lawfulness, equitability, inclusiveness)
- Todennettavuus (transparency, traceability, explainability, interpretability, auditability)
- Luotettavuus (reliability, trustworthiness, integrity, robustness)
- Turvallisuus (safety, security)
- Hallittavuus (governability, controllability, privacy)
- Ihmiskeskeisyys (human-centeredness, human agency, non-discrimination)



Esimerkiksi Pentagon päätyi omaksumaan Defense Innovation Boardin suosituksesta alkuvuodesta 2020 oman tekoälykehityksensä eettiseksi ohjenuoraksi seuraavat arvot: Responsible, Equitable, Traceable, Reliable, Governable. Suomessa puolustusministeriön Tekoälyratkaisujen kehittämisen strategiset linjaukset (2020) –ohjausasiakirjassa yksi viidestä kehittämisen pääperiaatteesta käsittelee etiikkaa: ”Laillisuus, eettisyys ja avoin keskustelu: Puolustushallinto noudattaa hallinnonalaa velvoittavia kansainvälis-oikeudellisia ja eettisiä velvoitteita tekoälyn rakentamisessa ja käytössä sekä osallistuu aktiivisena toimijana niiden laatimiseen. Puolustushallinto osallistuu tekoälyn uhkista ja mahdollisuuksista käytävään julkiseen keskusteluun aktiivisesti.”

Selkeän ja ohjaavan arvopohjan tulisi tarjota perusteet tekemiselle, ja toimia myös viestintänä sidosryhmien suuntaan. Vielä olennaisempaa on kuitenkin lopulta se, **miten periaatteet viedään käytäntöön**; mitä jokin eettinen periaate tarkoittaa teknisen suorituskyvyn vaatimuksina tai jonkin standardin mukaisena toimintana. Tällä hetkellä moni organisaatio onkin saanut jo määriteltyä arvonsa suhteessa näköpiirissä olevaan tekoölyyn, mutta kaikkialla tuskaillaan puuttuvien käytäntöjen kanssa jotka koskevat mm. datan järjestämistä ja jakamista, tekoälyn testausta ja validointia, rajapintoja ja arkkitehtuuriratkaisuja. Siviilitoimijat tarvitsevat näitä mm. tehokkaan ja skaalautuvan liiketoiminnan mahdollistamiseksi; sotilaallisissa sovelluksissa korostuu yhteistoimintakyvyn (interoperability) rakentuminen eri tasoilla.

### Vastuun toteutuminen

Tekoälyn ja koneautonomian teknologiapohja on täysin yhteinen niin siviili- kuin sotilas-sovelluksillekin. Vastaavasti edellä mainitut yleiset eettiset periaatteet tuntuvat rationaalisilta ja perustelluilta, vaikka sovellettavat oikeudelliset kehikot poikkeavatkin toisistaan merkittävästi siviilitoiminnassa ja sodankäynnissä. Oikeusregiimistä riippumatta, perimmäiseksi kysymykseksi muodostuu lopulta varmistuminen siitä, että vastuu

koneelle annetusta tehtävästä ja koneen toiminnasta seurauksineen säilyy aina ihmisellä; ihminen ei voi ulkoistaa vastuutaan koneelle.

Kuten tuotevastuussa yleensäkin, myös tekoälyn osalta vastuullisuuden voidaan ajatella jakautuvan valmistajan vastuuseen, sekä toisaalta käyttäjän vastuuseen. Järjestelmän on lähtökohtaisesti täytettävä kaikki määräykset, mutta tämä ei vapauta käyttäjää vastuullisen toiminnan vaatimuksesta. Toisin sanoen, laillis-takin järjestelmää on silti aina mahdollista käyttää väärin tai lainvastaisesti.

Tarkasteltaessa tekoälyn soveltamista ja siihen liittyviä eettisiä kysymyksiä sotilaallisen toiminnan näkökulmasta, tarkastelu jakautuu selvästi kahteen päälinjaan: 1. tukitoimintoihin ja ns. toimistojärjestelmiin liittyvä tekoäly, jolla voi olla myös merkittäviä implikaatioita sotilaalliseen suorituskäyttöön (esim. logistiikka, kunnossapito, tilannekuva), ja 2. varsinaisiin asejärjestelmiin. Vaikka rajanveto mainittujen kategorioiden välillä vaikeutuu mm. IoT-kehityksen myötä, koskee asejärjestelmiä ja taistelumenetelmiä (means and methods of warfare) kuitenkin omat erityiset eettiset säännökset, kun humanitaarinen laki pätee (IHL, International Humanitarian Law, ns. sodan oikeussäännöt).

Luonnollisesti mitä monimutkaisemmasta ja potentiaalisesti vaarallisemmasta järjestelmästä on kyse, sitä kattavammasi valmistajan vastuu yleensä muodostuu. Kuten todettua, yleisesti tekoälyn osalta nämä käytännöt ja normit ovat vasta muotoutumassa. Vastaavasti autonomisten asejärjestelmien osalta (LAWS, Lethal Autonomous Weapons Systems) aiheutta on työstetty YK:n tavanomaisten aseiden CCW-asevalvontakonventissa Genevessä epävirallisella statuksella vuosina 2014-16, ja prosessi virallistettiin (GGE, Group of Governmental Experts) vuodesta 2017 lukien. Toistaiseksi tuloksina on saatu hyväksytyä 11 ns. ohjaavaa pääperiaatetta sekä ohut konsensus jatkotyön tavoiteasetannasta ”normative and operative frameworks”, eli käytännön työssä tarvittavaa konkretiaa kolmessa toisiinsa nivoutuvassa dimensiossa: teknologinen-, sotilaallinen- ja lainsäädännöllinen ulottuvuus. Vaikka työ on

hidasta, aikaansaannoksia ja niiden merkitystä ei pidä silti väheksyä, sillä kaikesta päätettävästä vaaditaan täysi konsensus valtioiden kesken. CCW-sopimukseen kuuluu 125 maata, jossa ovat mukana kaikki asian kannalta merkittävät valtiot, joten tehtävä ei ole helppo.

Maat ovat yksimielisiä siitä, että täysin vailla ihmisen kontrollia toimivia asejärjestelmiä ei tule sallia eikä rakentaa. Mutta kun kysytään mikä on riittävä taso ihmisen ja koneen väliseksi vuorovaikutukseksi vastuun varmistamiseksi, päädytään jo asian ytimeen, jossa yhteisen ymmärryksen saavuttaminen on vaikeaa. On kuitenkin selvää, että pohjalle tarvitaan aina ihmisen tietoinen päätös tappavan voiman käyttämisestä. Kuinka paljon koneelle voidaan antaa vapauksia tehtävän suorittamiseksi, riippuu mm. sovellettavista säännöksistä, tehtävästä, tilanteesta, olosuhteista ja koneen suorituskäytöstä.

Ihmisen vastuu autonomisen asejärjestelmän eettisesti kestävästä ja laillisesta käytöstä toteutuisi käytännössä kahden raiteen kautta:

1. Varmistaudutaan järjestelmän laillisuudesta, käsittäen koko järjestelmän elinkaaren: konsepti- ja doktriinis suunnittelun; ohjelmistosuunnittelun ja koodauksen, muun toteutuksen ja testauksen; hyväksynnät; koulutuksen ja käyttöönoton; päivitykset ja lopulta käytöstä poistamisen. Asejärjestelmien yhteydessä Geneven sopimusten lisäpöytäkirjan Artikla 36 mukainen Weapons Review -prosessi korostuu, jossa tarkastetaan käyttötapauskohtaisesti laillisuuden edellytykset.
2. Varmistutaan käytön laillisuudesta; komentajan vastuu operaatiosta ja sen menetelmistä pätee jatkossakin, päätös sisältää myös tapauskohtaisen eettisen arvion käytettävien asejärjestelmien soveltuvuudesta ja lainmukaisuudesta. Keskeinen osa käyttöä on tehtävän määrittely autonomiselle järjestelmälle sisältäen mm. tehtävän reunaehdot, toiminnan rajat ja varotoimet. Operatiivisen henkilöstön syvälinen koulutus järjestelmän toiminnan, ominaisuuksien ja rajoitteiden ymmärtämiseksi korostuu.


## Miten etiikassa edetään?

Tekoälyn ja koneautonomian laajassa sovellusalueiden kentässä asejärjestelmät edustavat ns. altaan syvää päätä, jossa perustavaa laatua olevat vaikeat moraaliset kysymykset ihmisyydestä ja ihmisoikeuksista suhteessa koneisiin korostuvat, ja hyvästä syystä näitä onkin punnittava huolella. Kuitenkin sotilaallisen toiminnan ja puolustuksen alalla on erittäin paljon potentiaalia tekoälyn tehokkaaseen ja innovatiiviseen hyödyntämiseen lukusissa sovelluksissa ilman että törmätään edellä kuvattuihin haastaviin pohdintoihin. Toki on huolehdittava etiikasta ja turvallisuudesta näissäkin sovelluksissa.

Hyvien periaatteiden jälkeen monet käytännön kysymykset vaikkapa luotettavuudessa ja testauksessa aukeavat vasta omakohtaisen tekemisen kautta, vastaan tulevia ongelmia ratkottaessa. Koska kompleksisten järjestelmien testaus on tunnetusti jo itsessään haastavaa, suurimmat turvallisuusuhat koituvat varmasti eri järjestelmien yhteensopivuudesta sekä kyber-ulottuvuudesta. Tekoäly ei sentään muuta kaikkea, vaan hyväksi havaittuja käytänteitä löytyy runsaasti kaikilta turvallisuuskriittisiltä aloilta (esim. avioniikka, ydinvoima, lääketieteen tekniikka) jo ennes-

tään, mutta niiden soveltaminen esimerkiksi itseoppivia piirteitä sisältäviin tekoälyjärjestelmiin tulee arvioida erikseen ja täydentää muuttuneiden vaatimusten mukaisesti. Ohjelmistoteollisuudella on vahva intressi kehittää tekoälyn läpinäkyvyyttä ja validointimenetelmiä, joten tilanne kehittyy varmasti näiltäkin osin vauhdilla.

Puolustushallinnon omien tekoälyresurssien ollessa varsin vaatimattomat, pitkäjärteinen yhteistyö niin yritysten kuin valtiollisten toimijoiden kanssa on ratkaisevan tärkeää. Pentagonin alaisuudessa toimiva Joint Artificial Intelligence Center (JAIC) on kutsunut Suomen tekoäly-yhteistyöhön (AI Partnership for Defense) yhdessä 11 muun maan kanssa, joukossa NATO-maita ja muita kumppaneita, myös Ruotsi. Asialistalla on mm. edistää tekoälyn vastuullista käyttöä ja jakaa parhaita käytäntöjä tekoälyn liittyvien eettisten periaatteiden käyttöönotossa. Työ käynnistyi syyskuussa 2020. Käytännön puolustusyhteistyössä rakennetaan tekoälypohjaisille järjestelmille yhteistoimintakyvyn edellytyksiä. Tekoälyn maailmassa etiikka näyttäytyy strategisen tason kysymyksenä, josta on samalla yllättävän lyhyt matka käytäntöön.




**COJOT**  
MORE THAN ONE WAVELENGTH

## SWITCHED BEAM ANTENNAS

Improved performance for tactical communication networks and C-UAS Detection and Jamming.

- Different beam modes configurable (wide and omni)
- Improved coverage and LPI/LPD
- Low (10W) and high power (100W) antennas for various frequency ranges
- Simple field-proven control protocol
- No moving parts within the product



COJOT Switched Beam Antennas (SBAs) combine the outputs of multiple antennas in such a way that narrow beams are steered with an increased sensitivity and gain - configurable to "point" in single or multiple directions concurrently. Its default mode can be configured to be in omni or sweep mode to monitor the area around the location of the sensor, automatically switching to a narrow beam when required for tracking or jamming operation. [www.cojot.com](http://www.cojot.com)



# Digitalisaatio, uusi haavoittuvuus, osa 1 – kyber

- Insinöörieversti, dosentti Janne Jokinen -

Koska en korona-aikaan halua koskettaa sormellani maksupäätettä edes yli 50 euron ostoksilla, halusin ottaa käyttöni omena-ekosysteemin maksujärjestelmän. Oman pankkini maksukorttia en saanut siihen kytkettyä, joten ryhdyin käyttämään välissä englantilaista virtuaalimaksukorttia. Nyt kun ostan Pääesikunnan lounasravintolasta lounaan, hipaisen maksupäätettä älykellollani – rahastus kiertää kai Amerikassa omena-palvelun kautta, Englannin virtuaalikorttifirman ja kahden amerikkalaisen luottokorttibrandin palvelimilta edelleen omaan pankkiini Suomessa. Ja kuinka monta eri palvelua maksupäätteoperaattori tai nämä eri rahalaitokset käyttävätkään eri maissa, kukapa tietää. Nykyaikaisesta läntisestä elämänmuodosta on tullut valtavan kompleksi kudelma atk:ta, mitä monimutkaisuutta on äärimmäisen hankala hallita. Kuka pystyy hallitsemaan näihin liittyvät haavoittuvuudet? Kuka haluaa käyttää haavoittuvuuksia hyväkseen?

*Julkisuudessa on varoitettu ylenpalttisesta kyberalarmismista<sup>1</sup>, minkä inspiroimana provosoin keskustelua:*

*Täytyisikö peruskoulussa opettaa kansalaistaidon tunneilla nuotion tekemistä kirjahyllystä olohuoneen lattialle – tilanteeseen, kun sähkö ei virtaa talvipakkasilla?*

*Pitäisikö kirkoissa rukoilla, että kun väistämätön kyber-Pearl-Harbor tulee, olkoon se kansakunnallemme armollinen ja tuokoon riittävän opetuksen riittävän vähin vaurioin?*

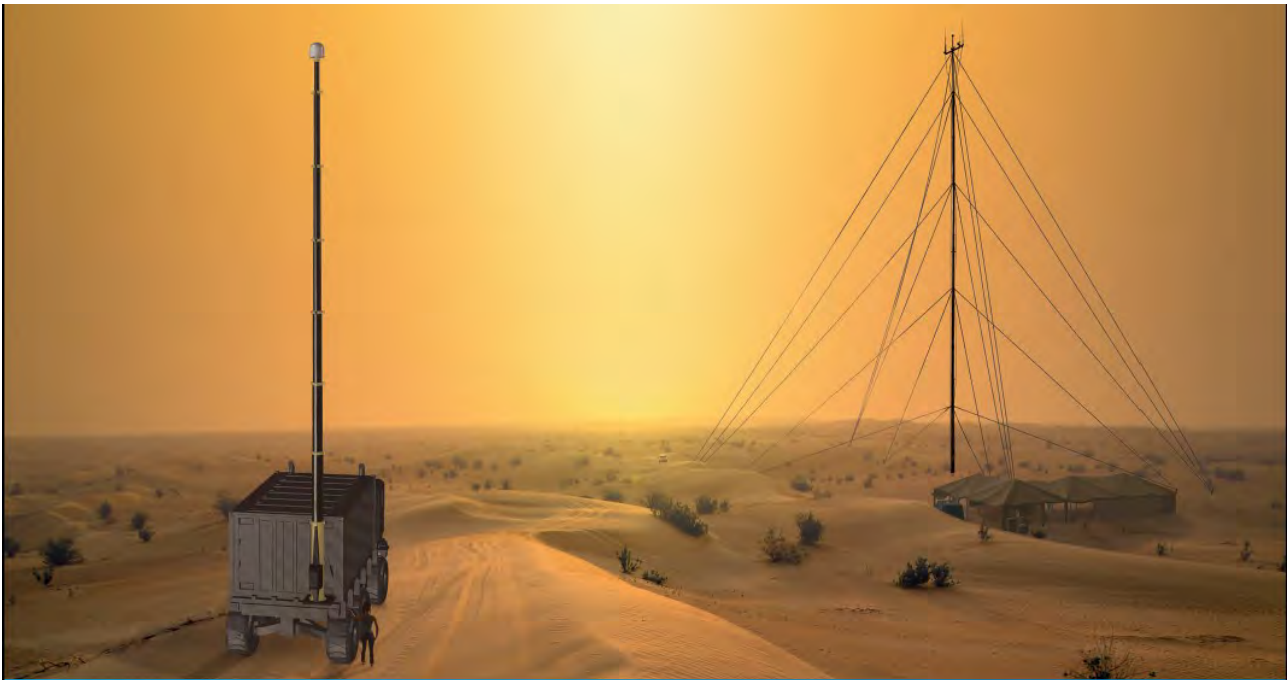
*Puolustaako Suomea yhteiskuntana kukaan kybertoimintaympäristössä, riittävän kattavasti? Pitäisikö jonkun, ja kuka se olisi?*

<sup>1</sup> Puolustusministeri Antti Kaikkosen puhe 231. Maanpuolustuskurssin avajaisissa 11.11.2019. [https://www.defmin.fi/ajankohtaista/puheet/puolustusministeri\\_antti\\_kaikkosen\\_puhe\\_231.\\_maanpuolustuskurssin\\_avajaisissa.10066.news](https://www.defmin.fi/ajankohtaista/puheet/puolustusministeri_antti_kaikkosen_puhe_231._maanpuolustuskurssin_avajaisissa.10066.news)

## Digitalisaatio

Yhteiskuntamme digitalisoituu yhä kiihtyvää vauhtia. Kansalaisten kannalta lähes kaikki merkittävät toiminnot vaativat verkottunutta tietotekniikkaa. Koteihimme tuleva sähkö, lämpö, vesi – viihteestä tai korona-ajan sosiaalisesta elämästä ja etätöistä puhumatta – on kaikki riippuvaista teollisuusautomaatiosta, tietoverkoista, pilvipalvelimista, verkottuneista palveluista. Terveyspalvelut hallinnoidaan yhä enemmän Kanta-tyyppisten keskitettyjen palveluiden ja yksityisten lääkäri-asemien kännykkäsovellusten kautta, ja moderni lääketiede perustuu erilaisiin kuvantamis- yms. laitteisiin. Raha liikkuu verkossa, eikä marketin kassalla auta enää päässä lasku, vaikka käteistä olisikin. Pian autot haluavat jutella älykkään tien kanssa, ja ovet avautuvat automaattisesti kasvontunnistuksella.

Tämä kehitys tulee jatkumaan intensiivisesti. Internet-of-Things (IoT) ja 5G-teknologiat (ei se lentokone) levittävät tietoverkot yhä laajemmalle arkeen, kaikkiin käyttämiimme laitteisiin. Nyt internet on tavaroissamme ja sensorit sormuksissamme, pian tietotekniikka integroidaan halukkaiden elimistöihin. Nyt voimme vielä riisua elektroniikan kokoushuoneen ulkopuolelle, mutta saammeko kohta palkattua nuoria osaajia, jotka eivät olisi augmentoineet elektroniikkaa elimistöönsä? Vähintään tämä hiipii insuliinipumppujen, sydämentahdistimien, perhesuunnittelun yms. sovellusten kautta – sitten kuntoilusovelluksiin ja muuhun elimistön tarkkailuun, viihteeseen, sosiaaliseen mediaan ja vastaavaan (vaikkapa Elon Muskin kultin kautta, joka on noussut Steve Jobsin seuraajaksi wow-tekniikassa). Nyt saan some-viesteistä värinän ranteeseeni ja viestit kellooni, näppärämpää olisi kuulla nämä suoraan korvaan myös saunassa.



## Cobham Mast Systems

Cobham Mast Systems is the world leader  
in high performance composite telescopic masts

The most important thing we build is trust

**COBHAM**

[www.cobham.com/mastsystems](http://www.cobham.com/mastsystems)

Ja jo ennen näitä IoT-tekniikan visioita tietoverkkojen ja -järjestelmien kompleksisuus on kasvanut valtavasti ja tasolle, mitä ihmisen on mahdotonta hallita. Tietokoneiden mikropiirien, käyttöjärjestelmien ja ohjelmistojen suuriin koodirivimääriin jää virheitä, mitä tilannetta järjestelmien väliset lukemattomat yhteydet monimutkaistavat. Nämä altistavat tietojärjestelmät haavoittuvuudelle, joita rikolliset ja tiedustelupalvelut systemaattisesti etsivät ja hyödyntävät tarpeisiinsa – tietojärjestelmiin syntyy tahtomattomia tai suunniteltuja reikiä, joita pitkin vastapuolel pääsevät ottamaan järjestelmiä haltuunsa tai niitä lamauttamaan. Käyttöjärjestelmä- ja ohjelmistotoimittajat pyrkivät paikkaamaan ja tiedottamaan näistä haavoittuvuuksista, joita käyttäjät ehtiessään päivittävät tai eri syistä jättävät päivittämättä, ja päivitykset usein synnyttävät uusia haavoittuvuuksia. Monista syistä järjestelmien päivittäminen saattaa osoittautua riskialttiiksi tai mahdottomaksi, ja vanhojen järjestelmien käyttöä on pakko jatkaa.

Valtakunnan sähköverkkokokonaisuus, suuri sairaala tai vaikkapa puolustusjärjestelmämme on hyvin laaja kokonaisuus Windows-tietokoneita, Linux-palvelimia, älypuhelimia, vanhoja legacy-laitteita, tietoverkkokomponentteja, teollisuusautomaatiota, sulautettuja järjestelmiä, räätälöityjä ohjelmistoja, yms. Yritämme suojata tällaisia kokonaisuuksia monin tietoteknisin ja myös fyysisen turvallisuuden keinoin, mutta järjestelmien yhteydet suljettujen ympäristöjen ulkopuolelle synnyttävät väistämättä riskejä. Vanhan viisauden mukaan: mikäli se on mitenkään kiinni internetissä, siihen voi tunkeutua. Usein muutenkin.

Digitalisaatioon liittyvä kyberuhka nousee vielä huomattavasti, kun tiedustelupalvelut ja kyberrikolliset ryhtyvät hyödyntämään kehittyneitä tekoälyalgoritmeja etsiessään haavoittuvia järjestelmiä ja tunkeutuessaan niihin sisään millisekunneissa. Siinä vaiheessa myös kyberturvallisuuden täytyy kyetä vastaamaan nopeuteen ja adaptiivisuuteen uhkiin reagoidessaan.

# Merellistä vaikutusvaltaa



Advanced Solutions from Seabed to Space  
[www.da-group.fi](http://www.da-group.fi)

## **Puolustusjärjestelmän haavoittuvuus**

Myös puolustusjärjestelmämme kompleksisuus kasvaa. Asejärjestelmien alati lisääntyvä tietoteknistyminen ja vuosikymmeniä pitkät elinkaaret synnyttävät suuria ylläpito-ongelmia: jättääkö vanhentunut käyttöjärjestelmä ja ohjelmisto käyttöön, täytyykö se pyrkiä eristämään laajemmista tietoverkoista, vai varautuako säännöllisiin suuriin päivityskustannuksiin ja mahdollisiin yllättäviin yhteensopivuusongelmiin? Sama ongelma liittyy myös esim. lääketieteelliseen tekniikkaan, mutta puolustusvoimien järjestelmät kiinnostavat erityisesti muiden maiden tiedustelupalveluita ja asevoimia.

Moderneissa järjestelmissä puolestaan digitalisaation ja verkottumisen edut pyritään hyödyntämään usein täysimääräisesti. Järjestelmiä on järkevää ylläpitää ja säätää valmistajan tehtaalta tai alihankkijalta käsin, mutta kuinka mahdollistaa tämä puolustus-

voimien järjestelmissä? Haluammeko avata ulkopuolisille tätä mahdollisuutta, vai paljonko vaihtoehtoisesti maksaa järjestää kaikki ylläpito itsenäisesti? Pystymmekö edes jatkossa eristämään järjestelmiämme, mikäli niiden logiikka perustuu esim. Big Datan hyödyntämiseen tai pilvipalveluissa toimiviin tekoälyalgoritmeihin?

Ihminen ei pysty hallitsemaan nykyisiä komplekseja järjestelmiä. Mikäli järjestelmä pyrittäisiinkin tarkastamaan huolellisesti, tarvittaessa jokaista ohjelmakoodiriviä myöten, jo huomenna seuraavan päivityksen myötä ohjelmistopohjainen järjestelmä voi olla täysin erilainen. Viime kädessä kyse on uskosta toimittajaan, sen alihankintaketjuun ja ekosysteemiin, toimittajien kotivaltioiden oikeusvaltioperusteisiin. Tästä on kyse myös keskustelussa 5G-tietoliikennetekniikkaan ja ylipäänsä esim. kiinalaiseen tekniikkaan liittyen: vaikka juuri nyt emme löytäisikään vakoilua mahdollistavia takaportteja, mitä tapahtuu seuraavien päivitysten myötä? Sama

haaste tulee olemaan myös mm. HX-hankkeen lentokoneiden kanssa: valtaosa modernin hävittäjän järjestelmästä on ohjelmistoja; voimme saada suorituskykyjä ohjelmistopäivitysten kautta, ja toimittajamaiden policy-muutosten myötä myös niitä menettää. Ohjelmistopohjainen järjestelmä synnyttää pitkissä elinkaarissa suuria riskejä ja on tietyllä tasolla uskonvarainen ratkaisu, mutta muutakaan polkua ei ole digitalisoituvassa maailmassa ja aseteknologian kehitystä seurattaessa.

Omien järjestelmiensä lisäksi Puolustusvoimat on riippuvainen myös ympäröivästä yhteiskunnasta. Emme sodi pitkään ilman valtakunnanverkon sähköä ja siviiliyhteiskunnan logistiikkaa tai sairaanhoitoa. Vaikka Puolustusvoimien tulee kanta huolta erityisesti omien ase-, sensori- ja johtamisjärjestelmiensä kyberturvallisuudesta, seisomme tai kaadumme muun yhteiskunnan mukana.

### **Kyberuhkat**

Tietoverkoissa vaativat kyberuhkat ovat moninaisia. Yleisessä keskustelussa on tarpeen korostaa esim. yritystoimintaa lamauttavia uhkia: palvelunestohyökkäyksiä, kiristyshaitto-ohjelmia, teollisuusvakoilua yms. Nämä kaikki voivat vaikuttaa myös maanpuolustukseen vähintään kriittisen infrastruktuurin kautta.

Puolustusvoimien kannalta merkittävimmän uhkajoukon muodostavat kuitenkin edistyneet (tyypillisesti) valtiolliset organisaatiot, joita kyberturvallisuuden slangissa kutsutaan APT-toimijoiksi (Advanced Persistent Threat – kehittynyt pitkäkestoinen uhkatoimija). Nämä ovat tyypillisesti eri valtioiden tiedustelupalveluita tai valtioiden käyttämiä joukkioita, ja eri ryhmien toiminnan jäljittäminen ja tunnistaminen on keskeistä tietoturvayritysten, länsimaiden tiedustelupalveluiden ja kyberpuolustusjoukkojen toimintaa.

Valtiollisten kyberuhkatoimijoiden keskeinen intressi on valtiollinen vakoilu, mistä klassisena esimerkkinä toimii Ulkoministeriön vuonna 2013 paljastunut vuosia jatkunut kybervakoilutapaus. Tämän lisäksi valtiolliset

toimijat pyrkivät tunkeutumaan kriittisen infrastruktuurin järjestelmiin, todennäköisesti valmistukseen jalansijaa myöhempiä mahdollisia vaikuttamisoperaatioita ja jopa täysipainoista kyberhyökkäystä varten. Operaatioita pyritään piilottamaan toimimalla näennäisesti viattomien palvelimien kautta, minkä vuoksi valtiolliset toimijat valtaavat ja piiloutuvat mihin tahansa huonosti päivitettyihin ja suojattuihin järjestelmiin myöhempää käyttöä varten.

Viime vuosien ilmiönä valtiot ovat ryhtyneet vaikuttamaan aggressiivisemmin myös toistensa politiikkaan kybermenetelmiä käyttäen. Etenkin Yhdysvaltojen vaaleissa tämä ilmiö on noussut esille, ja muutenkin uhkana on länsimaisen demokratian rapauttaminen esim. yhteiskuntien sisäisiä jakolinjoja vahvistamalla. Tätä voidaan tehdä kybermenetelmin, mutta myös osana laajempia hybridioperaatioita.

Yhdysvaltojen viranomaiset ovat julkaisseet mielenkiintoisia syytekirjelmia ja muita dokumentteja, joilla osoittavat mm. Venäjän sotilastiedustelupalvelu GRU:n kyberoperaatioita Yhdysvalloissa. Nämä julkistukset toimivat hyvänä julkisena oppimateriaalina nykyiseen valtiollisen kybervakoilun ja -operaatioiden kenttään.<sup>2</sup> Suomessa Suojelupoliisi on ottanut kantaa mm. kybervakoiluun ja kriittiseen infrastruktuuriin tunkeutumiseen esim. vuosikirjassaan<sup>3</sup>.

### **Kyberpuolustus**

Vuoden 2013 kansallinen kyberturvallisuusstrategia<sup>4</sup> asetti edelleen ajankohtaiset suunta- viivat sille, kuinka puolustusvoimat kehittää kyberpuolustusta:

<sup>2</sup> Ks. esim. <https://www.justice.gov> -> hakuun esim. "GRU".

<sup>3</sup> Suojelupoliisi, Vuosikirja 2019. <https://www.supo.fi/julkaisut/esitteet> -> "Vuosikirja 2019".

<sup>4</sup> Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013. <https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/>

# MILCON

Valmis vaativien kumppaneiden haasteisiin

Viesti- ja johtamisvälineet koviin olosuhteisiin sekä vaativien sovellusten kaapelointi- ja sähköistysratkaisut. Toimitukset yksittäisistä komponenteista aina kokonaisjärjestelmiin saakka yhteistyössä alan johtavien komponenttivalmistajien kanssa.

- Liittimet
- Kenttävalokaapelit Pro Beam Jr. liittimin
- Viestilaitteiden erikoisvaraosat ja varusteet
- Puhelulaitteet ja audioliitännät
- Kaapelisarjat
- Antennit ja teholähteet
- Ruggeroidut tietokoneet, kytkimet, näytöt ja EMP/EMI-Filtrit vaativiin olosuhteisiin.



**MILCON OY**

Kolmionkatu 5D, 33900 Tampere  
010 239 2170 | info@milcon.fi

[milcon.fi](http://milcon.fi)

*”Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisäätteisissä tehtävissään.*

*Sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyyvistä. Puolustusvoimat suojaa omat järjestelmänsä siten, että se kykenee suoriutumaan lakisäätteisistä tehtävistään huolimatta kybertoimintaympäristön uhkista. Suorituskyyvyn varmistamiseksi kehitetään tiedustelu- ja vaikuttamiskykyä kybertoimintaympäristössä osana muun sotilaallisen voimankäytön kehittämistä.*

*Edellä mainittujen tehtävien täyttämiseksi laaditaan puolustusministeriön johdolla puolustusvoimille tarvittava toimivaltuussäädös-tö. Tunnistetut puutteet toimivaltuussäädöksis-sä korjataan lainsäädäntötoimenpitein.*

*Kyberpuolustusta harjoitellaan ja kehitetään yhdessä keskeisten viranomaisten, järjestöjen ja elinkeinoelämän toimijoiden kanssa kansallisesti ja kansainvälisesti. Puolustusvoimat antaa virka-apua lainsäädännön salliessa.”*

Strategiatyö on edennyt strategian toimeenpano-ohjelmien kautta vuoden 2019 kyberstrategiaan, jonka anti kyberpuolustuksen kehittämiseen oli aiempaa strategiaa geneerisempi. Strategian myötä valtionhallintoon on perustettu valtion kyberturvallisuusjohtajan virka, jonka johdolla parhaillaan laaditaan kyberstrategian kehittämisohjelmaa.

Vuonna 2019 Puolustusministeriö julkaisi kyberpuolustuksen kehittämisen strategiset linjaukset.<sup>5</sup> Kyseinen asiakirja asettaa selkeitä vaatimuksia siinä käsitellyille kyberpuolustuksen kehittämisen osa-alueille: osaaminen, teknologia, yritystoiminta, tutkimus, kansainvälinen yhteistoiminta ja kyberpuolustus osana kansallista kyberturvallisuutta. Esimerkiksi ”keskeisimmiksi kyberpuolustuksen osaamis-alueiksi on tällä hetkellä tunnistettu mm.

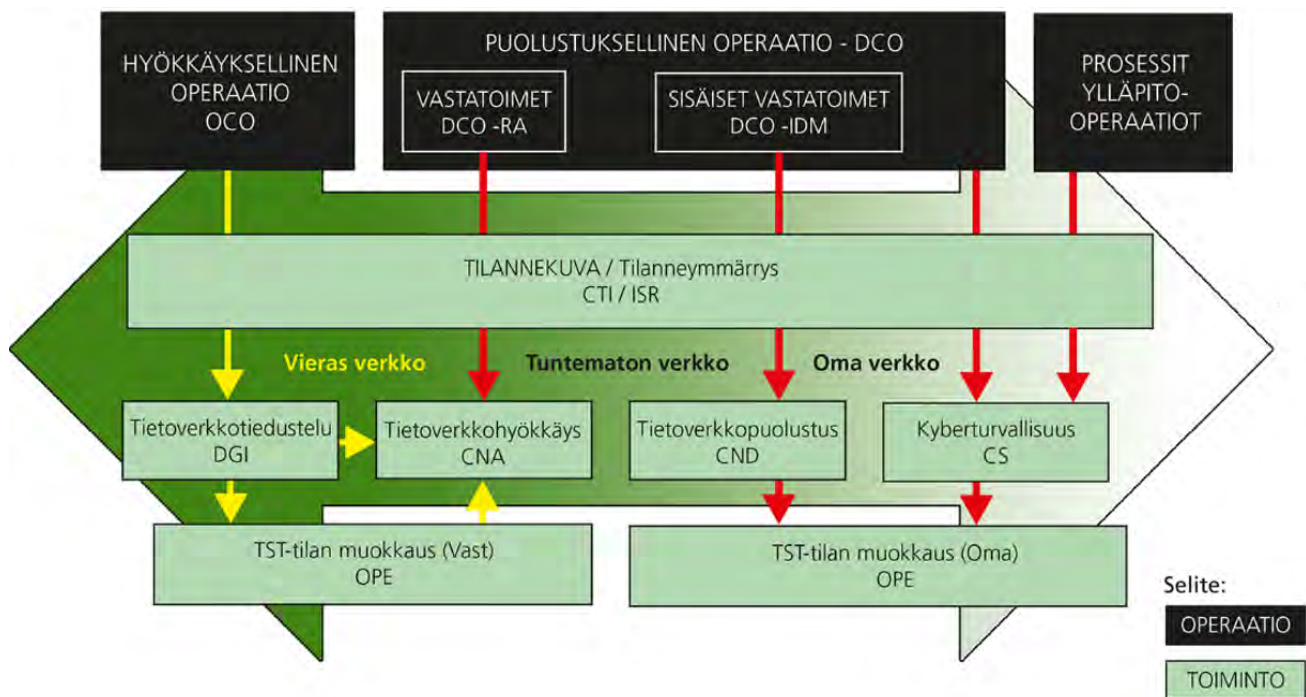
<sup>5</sup> Puolustusministeriö, Kyberpuolustuksen kehittämisen strategiset linjaukset.  
<http://urn.fi/URN:ISBN:978-951-663-069-7>

tietoturvallisuus, havainnointi, kyberforensiikka ja haittaohjelma-analyysi, tiedonsiirtotekniikka, ohjelmistokehitys, suurten tietomäärien käsittely, kryptologia, tekoäly ja kvanttilaskenta.” ”Kyberpuolustuksen kriittiseksi tunnistettu osaaminen puolustushallinnossa turvataan rekrytoinneilla ja henkilöstön koulutuksella.” ”Keskeisimmiksi teknologia-alueiksi on tunnistettu mm. haavoittuvuustutkimus, tunkeutumisen havaitsemis- ja estojärjestelmät, salausteknologia, suuren ja strukturoimattoman tietomäärän käsittely ja tekoälyteknologiat.” ”Kybersuorituskykyjä ja niihin liittyviä kriittisiä teknologia-alueita koskeva osaaminen ja kehittämiskyky turvataan Suomessa valtioneuvoston periaatepäätöksen (VnP 7.4.2016) linjausten mukaisesti.” Tällaisen kokonaisuuden hallitseminen Puolustusvoimissa tai edes kansallisesti vaatii erittäin määrätietoisia toimia, jottei asiakirja jäisi vain haaveiluksi.

Kyberpuolustukseen liittyen lainsäädäntötyötä on tehty tiedustelulakien osalta, minkä myötä puolustusvoimat on saanut mm. oikeudet tietoverkoissa tietoliikenne- ja ulkomaan tietojärjestelmätiedusteluun. Muuta kyberpuolustuksen säädöspohjaan liittyvää keskustelua on käyty valtionhallinnon sisäisesti mm. kyber-toimintaympäristön kansainvälisoikeudellisiin tulkintoihin liittyen, esim. mitä mieltä olemme

kansallisesti suvereniteetista, valtion vastuusta rajat ylittävissä vahingoissa, itsepuolustuksesta, vastatoimista, yms. Kyberpuolustukseen liittyvä juridiikka ei ole kokonaisuutena vielä täysin selkeää, ja väistämättä tullaan näkemään kansallisia kannanottoja valmiuslakiin, aluevalvontalakiin, lakiin puolustusvoimista, lakiin sähköisen viestinnän palveluista yms. liittyen, ja lisäksi valtioiden kansainvälisoikeudellisia neuvotteluja ja julistuksia.

Kyberpuolustus jakautuu strategian mukaisesti suojaan, tiedusteluun ja vaikuttamiseen. Tämän kokonaisuuden sisällä voidaan eritellä erilaisia operaatiotyyppisiä, joista yksi jaottelu on esitelty seuraavassa kuvassa. Ylläpito- tai johtamisjärjestelmäoperaatioilla pyritään jatkuvasti pitämään omat verkot suojattuina, mutta kun omaan tietojärjestelmään on tunkeuduttu tai uhka on ilmeinen, käynnistetään tähän liittyvät sisäiset suojatoimet. Toisaalta saatetaan puolustuksellisesti joutua tekemään myös vastatoimia, jotka toteutetaan oman verkon ulkopuolella ja jopa suoraan hyökännyttä osapuolta tai sen käyttämiä järjestelmiä vastaan hyökkäyksen pysäyttämiseksi. Viime kädessä valmius on myös hyökkäyksellisiin operaatioihin, jotka Puolustusvoimien viitekehyksessä kytetään osaksi muuta operaatioiden ja vaikuttamisen kokonaisuutta.



**Eräs kyberoperaatioiden jaottelu. Aiheesta tarkemmin ja lyhenteiden selitys #kyberpuolustus-kirjassa.**

(Kuva: #kyberpuolustus-kirja)

Maanpuolustuskorkeakoulun julkaisema #kyberpuolustus-kirja<sup>6</sup> avaa tätä kotimaista kyberpuolustukseen liittyvää terminologiaa ja ajattelua tarkemmin.

Ajattelua laajentavat myös Naton<sup>7</sup> ja Yhdysvaltojen asevoimien<sup>8</sup> kyberoperaatioita käsittelevät ohjekirjat, sekä julkista keskustelua aktiivisesti ylläpitäneen Yhdysvaltojen asevoimien kyberpuolustuksen johtoportaan USCYBERCOM:in julkaisut<sup>9</sup>. Yhdysvalloissa

kehitetty ajattelu leviää etenkin Nato-maissa: Nato julisti vuoden 2016 Varsovan huippukokouksessa kybertoimintaympäristön yhdeksi operatiivisista toimintaympäristöistä fyysisten toimintaympäristöjen (maa, meri, ilma, avaruus) rinnalle, ja Nato-maissa on käynnissä kehitys perustaa CYBERCOM-tyyppisiä johtoportaita ja muutenkin ottaa kyberpuolustukseen liittyvä haaste vakavasti. On syytä olettaa, että myös Yhdysvaltojen tuoreempi ajattelu leviää viiteryhmämme maissa, esim. Yhdysvaltojen kyberpuolustusstrategiassa<sup>10</sup> vuonna 2018 ja sittemmin laajasti erilaisissa kannanotoissa ja artikkeleissa korostettu ns. ”Defend Forward” -konsepti, jonka mukaan puolustajan operointi pelkästään omista verkoistaan ei mahdollista tehokasta puolustusta. Tämä johtaa vähintään lisääntyvään yhteistyöhön kansallisessa kyberpuolustuksessa ja myös valtioiden välillä, mahdollisesti muihinkin toimiin.

<sup>6</sup> Tommi Laari et al., #kyberpuolustus: kyberkäsikirja Puolustusvoimien henkilöstölle, MPKK 2019. <http://urn.fi/URN:ISBN:978-951-25-3120-2>

<sup>7</sup> NATO Standard AJP 3-20: Allied Joint Doctrine for Cyberspace Operations, 2020. [https://nso.nato.int/nso/->hakuun “AJP-3.20”](https://nso.nato.int/nso/->hakuun%20AJP-3.20).

<sup>8</sup> US DOD, Joint Publication 3-12: Cyberspace Operations, 2018.

[https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf)

<sup>9</sup> Ks. esim. The George Washington Universityn ylläpitämä kooste UCSYBERCOM:in julkaisemista dokumenteista:

<https://nsarchive.gwu.edu/news/cyber-vault/2020-05-11/uscycbercom-documents-timeline>

<sup>10</sup> US DOD, Summary, Department of Defense Cyber Strategy 2018.

[https://media.defense.gov/2018/Sep/18/2002041658/1-1-1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/1-1-1/CYBER_STRATEGY_SUMMARY_FINAL.PDF)



**Teknologia on työväline. Sen kuuluu toimia.**

**IntoWorks turvaa hankintakumppanina järjestelmäsi toimivuuden.**

<p>IntoWorks Oy Liitintie 14, 90630 Oulu www.intoworks.fi</p>	<p>Lisätietoja Mika Koskela puh. +358 40 2164 132 info@intoworks.fi</p>	
---	---	---

## **Kansallinen kyberpuolustus**

Suomessa on tehty kyberturvallisuuteen liittyen paljon strategiatyötä, ja strategista johtamista on korostettu. Olemme ylpeitä kokonaisturvallisuuden yhteistoimintamallistamme, jossa ”yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä”. Kokonaisturvallisuus ja kaikkien toimijoiden vastuuttaminen on elintärkeää, ja esim. Kyberturvallisuuskeskus, Huoltovarmuuskeskus ja Digi- ja väestötietovirasto – mutta myös Maanpuolustuskoulutus ry:n, yritysten yhteenliittymien ja jopa erilaisten vapaaehtois-yhdistysten kaltaiset toimijat – tekevät tässä erinomaista työtä. Kokonaisturvallisuus toimii rauhallisesti kehittyvissä tai hyvin harjoitelluissa kriiseissä, mutta korona-kevät on toiminut monessakin mielessä opetuksena, kuinka viranomaisten yhteistyö käytännössä toimii kansallisessa mallissamme. Viranomaisilta kesti kauan löytää vastuulliset toimijat esim. Helsinki-Vantaan lentokentällä altistuneiden

den tai sairastuneiden matkustajien käsittelyyn, ja lukuisten eri viranomaisten parasta tarkoittavista toimita on kaiveltu moitittavuutta ja niitä jopa tullaan käsittelemään oikeudessa. Puolustusvoimissa olemme eläneet systeemiharhassa, että ”sitten kun pilliin puhalletaan”, asioita on mahdollisuus tehdä jotenkin oikoen. Nykyaikojen ensimmäinen poikkeustila osoitti, että toimivaltuuksien ja viranomaisten yhteistoimintamallien täytyy olla kunnossa kriisin ensihetkestä lähtien – kybertoimintaympäristön osalta sen luonteen vuoksi käytännössä jo normaalioloissa.

Valtiontalouden tarkastusvirasto on arvioinut kybersuojauksen järjestämistä kansallisesti: VTV:n raportin<sup>11</sup> mukaan mm. ”kyberturvallisuuden operatiivisen tilannekuvan muodostamista on syytä parantaa” ja ”laajavaikutteisen

<sup>11</sup> Valtiontalouden tarkastusvirasto, Tuloksellisuustarkastuskertomus: Kybersuojauksen järjestäminen, 16/2017 ja sen jälkiseurantaraportti 16.1.2020 Dnro 185/54/2016.



kyberloukkaustilanteen operatiivista johtamista ei ole määritelty”. Nykyinen hajautettu malli johtaa hajanaisiin vastuisiin ja siiloutumiseen, jopa viranomaisten reviiiririitoihin. Suomen leppoisosessa elämässä juhannus- tai etenkin kylmänä jouluaattona alkava laaja ja hankalasti hahmottuva kyberhäiriö voisi johtaa suuren mittakaavan ongelmiin.

Tällainen laaja kyberhäiriö voisi olla vieraan valtion yritys horjuttaa suomalaista yhteiskuntaa ja pakottaa poliittista johtoa konsultaatioihin. Tarvitseeko Suomeen enää hurruutella panssarivaunuilla, vai pystytäänkö yhteiskuntaamme lamauttamaan kriittisillä ajanhetkillä riittävästi ilman perinteistä asevaikutusta? Yhteiskuntamme on erittäin riippuvainen sähköverkoista, vesihuollon automaatiosta, sähköisistä maksujärjestelmistä, terveydenhuollon tietojärjestelmistä ja sairaanhoidon lääketieteellisistä järjestelmistä, satamien ja logistiikkayritysten tietojärjestelmistä, ynnä muista vastaavista kriittisen infrastruktuurin osista. Moni viranomaisjärjestelmä, yksityisen sektorin järjestelmistä puhumattakaan, ei toimi ilman jatkuvaa

yhteyttä ulkomaisiin palvelimiin. Tämän kriittisen infrastruktuurin riittävä puolustaminen on tärkeää yhteiskunnan kannalta, mutta myös puolustusvoimien toiminta on siitä riippuvaista.

Operatiivista viranomaistoimintaa on syytä kehittää kohti dynaamista, välittömästi käynnistyvää, tarvittaessa nopeatempoista, korkean turvallisuusluokituksen ja eri viranomaisten toimivaltuuksia joustavasti käyttävää reaaliaikaista yhteistoimintaa. Yhtenä esimerkkinä tällaisesta toimii Yhdysvaltojen signaalitiedusteluvirasto NSA:n ja USCYBERCOM:in yhteinen integroitu kyberkeskus (Integrated Cyber Center, ICC), missä myös muut keskeiset viranomaiset ovat edustettuina. Vastaavaa viranomaisyhteistyön keskusta ollaan perustamassa Ruotsiin, missä ainakin puolustusvoimat, signaalitiedustelulaitos FRA, huoltovarmuusviranomaisen MSB ja turvallisuuspoliisi Säpo ovat osoittamassa, että aikaa ei tuhlata diskuteeraukseen. Suomessa vastaavaan reaaliaikaiseen moniviranomaistoimintaan kyetään esim. meripelastuksessa, toivottavasti pian myös kansallisessa kyberpuolustuksessa.



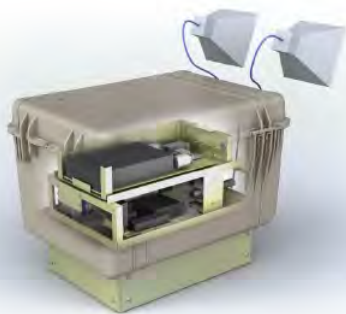
***Yhdysvaltojen signaalitiedusteluviranomaisen NSA:n ja asevoimien kyberpuolustuksen johtoportaan USCYBERCOM:in yhteinen Integrated Cyber Center (ICC) Fort Meadessa Marylandissa. Samassa keskuksessa on läsnä myös monia muita viranomaisia. (Kuva: NSA)***

Todennäköisesti myöskään viranomaisten toimivaltuudet eivät ole riittävät laajojen valtiollisten kyberoperaatioiden torjuntaan, etenkin mikäli vastustaja pystyy pitämään toimintansa aseellisen voimankäytön kynnyksen alapuolella ja muutenkin operoimaan ovelasti ja lainsäädäntöömme adaptoituen. Esim. aluevalvontaan verrattavaa toimintoa kyberulottuvuudessa ei ole vielä olemassa – aihe on vaikeasti määriteltävissä ja muutenkin sisältää ongelmia, mutta kyberulottuvuuteen liittyvistä viranomaisten tiedonsaantioikeuksista on kyettävä käymään kansallista keskustelua. Lisäksi keskustelua täytyy käydä vaikuttamismenetelmistä ja voimankäytöstä esim. Suomeen kohdistuvan laajan kyberhyökkäyksen tilanteessa: vastatoimien paletin täytyy olla laaja, sisältäen

mm. diplomaattisia toimia, pakotteita ja CERT-viranomaisten välisiä kansainvälisiä toimia, mutta tarvittaessa myös kybervastatoimia – deterrenssin avulla voimme nostaa pidäkekynnystä, mistä on keskusteltu mm. EU:n piirissä.

Näihin aiheisiin sisältyy runsaasti intohimoja, ja monenlaisia erilaisia kansallisia ratkaisumalleja olisi mahdollista hahmotella meidänkin hallintokulttuurissamme, mutta väistämättä joudumme vielä kehittämään kansallisen tason kyberpuolustustamme. Toivottavasti tämä ei tapahdu vasta jonkun uuden skandaalimaisen kybervakoilutapauksen tai fataalin kriittisen infrastruktuurin häiriön myötä.

*Tämä artikkeli on kirjoitettu ennen Vastaamotietomurron tuloa julkisuuteen syksyllä 2020.*



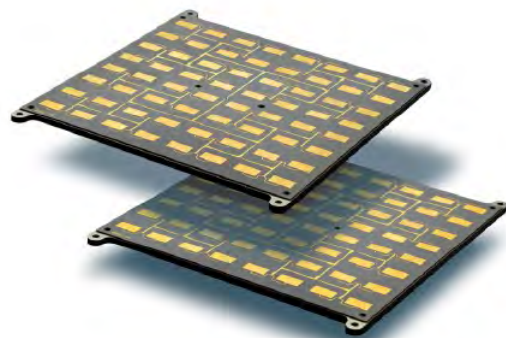
Tekniikantie 14, 02150 Espoo  
Puh. +358 50 300 2625  
[www.harptechnologies.com](http://www.harptechnologies.com)  
[contactharp@harptechnologies.com](mailto:contactharp@harptechnologies.com)

### Harp Technologies Oy

Tarjoamme laadukkaita RF- ja mikroaaltotekniikan suunnittelu- ja tuotekehityspalveluja. Olemme luotettava kumppani T&K-hankkeissanne.

Tutkatekniikka, passiivisensorit, RF-etupäät, antennit ja sovituspierit, jne.

Soveltuvuustutkimukset, EM-simulaatiot, komponentit, alijärjestelmät ja laitteet, myös vaativiin olosuhteisiin avaruus- ja puolustussektoreille.



JYVÄSKYLÄ SECURITY TECHNOLOGY:



# Kybersietokkyä varmistamassa

JYVSECTEC on Jyväskylän ammattikorkeakoulussa toimiva kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus, joka palvelee turvallisuusviranomaisia, valtionhallintoa sekä kriittisen infrastruktuurin yrityksiä.

Missiomme on parantaa suomalaisen yhteiskunnan resilienssiä kyberturvallisuuden avulla.

Tuotamme palveluita käyttäen hyväksi itse kehittämäämme, edistyksellistä ja maailmanlaajuisesti uniikkia, RGCE (Realistic Global Cyber Environment) Cyber Range -ekosysteemiä.

## Palvelumme

-  FINCSC-sertifiointi
-  Kyberturvallisuusharjoitukset
-  Koulutuspalvelut
-  Testauspalvelut
-  Tutkimustoiminta
-  Konsultointipalvelut

**JYVSECTEC**  
by jamk

Lisätietoa meistä ja palveluistamme,  
tutustu [www.jyvsectec.fi](http://www.jyvsectec.fi)

# Digitalisaatio, uusi haavoittuvuus, osa 2 – sähkömagneettinen spektri

- Insinöörimajuri Anders Furu -

Digitalisaatio näkyy sähkömagneettisessa spektrissä lupavapaiden lähettimien määrän valtavana kasvuna. Suurina kasvun tuojina ovat erilaiset IoT (Internet of Things) -ratkaisut sekä 5G- ja 6G-verkkoihin tulevat uudet palvelut. Vanhentunut ajattelutapa spektristä elää vahvasti, ajatellaan että on olemassa siviilitaajuuksia ja sotilastaajuuksia. Kuitenkin esimerkiksi riippuvuus muuhun yhteiskuntaan on erityisesti logistiikkaketjussa erittäin vahva. Kasvun vaaranpaikkoja ei ole kuitenkaan täysin analysoitu. Kenelläkään ei ole kokonaiskuvaa, kuinka monta lähetintä on käytössä ja miten kuormitettuja taajuudet lupavapailla taajuusalueilla ovat. Ei ole olemassa edes arvioita missä lähettimiä on tai paljonko niitä on.

Radioliikenne oli 1980-luvulla perinteistä luvanvaraista toimintaa, jota valvoi Posti- ja telehallitus. Telehallintokeskus perustettiin vuonna 1988, perustehtävänään radio- ja televiestinnän lupa- ja valvontaviranomaistehtävät. Vuosien mittaan tehtävät ovat lisääntyneet, ja nimikin on muuttunut ensin Viestintävirastoksi ja nykyään nimenä on TRAFICOM – Liikenne- ja viestintävirasto. Radiotaajuuksien valvonta on vähentynyt minimiin ja on nykypäivänä lähinnä häiriöselvitystyötä.

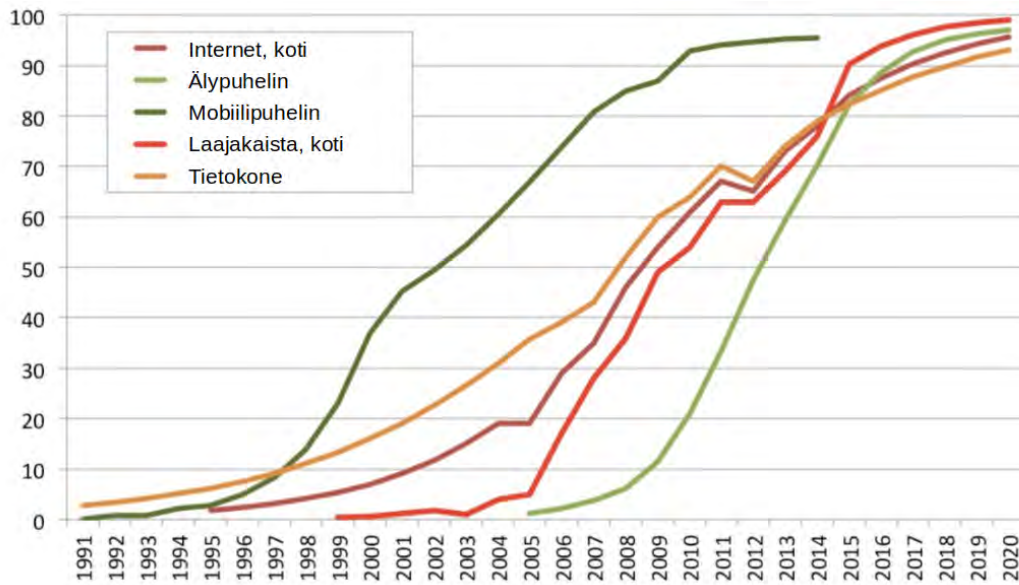
Ennen 1990-lukua suurin osa radioliikenteestä oli luvanvaraista, esimerkiksi radiolinkit, yleisradiolähettimet ja tutkat tarvitsivat aina luvan. Lupavapaata liikennettä ei juurikaan ollut. Tänä päivänä suurin osa radiotaajuisesta liikenteestä on lupavapaata, arvion mukaan noin 90–95 %. Traficomien määräyksessä ”Luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä” näitä laiteluokkia on lueteltu 32 kappaletta. Lupavapaata liikennettä ovat esimerkiksi Wi-Fi, matkapuhelinverkon

päätelaitteet, lyhyen kantaman laitteet ja satelliittitietoliikenteen päätelaitteet. Päätelaitteilta vaaditaan vain vaatimustenmukaisuuden täyttymistä. Radiolupia vaaditaan edelleen lähinnä suuritehoisille lähettimille, joilla häiriöiden aiheuttamisen vaara on suuri.

Arvioita radiotaajuisen spektrin käyttöasteesta ei ole. Radiolaitteiden määrästäkään ei ole arvioita. Arvion tekemistä vaikeuttaa se, ettei lupavapaiden lähettimien määrää tiedä kukaan. Vaikeusastetta tuo vielä lisää, ettei ole oikein varmuutta edes lähettimen määritelmästä; onko älypuhelin yksi lähetin vai useampi? Esimerkiksi voidaan ottaa Googlen tuore Pixel 4a 5G älypuhelin. Puhelimessa on lähetimet neljälle matkapuhelinsukupolvelle, kahdelle WiFi-taajuusalueelle sekä Bluetoothille, taajuuksien ollessa välillä 850 MHz–6 GHz. Käytössä voi yhtäaikaaisesti olla kolme eri lähetintä. Onko puhelin siis yksi lähetin vai useampi?

Jonkinlaisen tuntuman radiolähettimien määrän kasvusta saa seuraavasta kuvasta Vuodesta 2010 lähtien kaikki kuvassa olevat laitteet ovat yhä useammin langattomia ja toimivat usealla taajuusalueella. EUn jäsenmaissa on tällä hetkellä noin 250 miljoonaa kotitaloutta. Euroopan komission vuoden 2014 arvion mukaan vuonna 2015 EU-28 -maissa olisi 1,5 miljardia radiolaitetta ja vuonna 2025 jo 46 miljardia radiolaitetta. Kasvua tuovat IoT ja laajakaistainen tiedonsiirto.

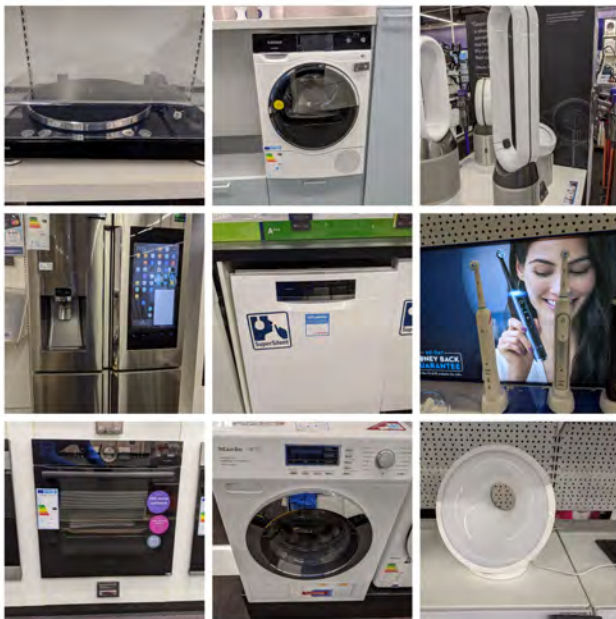
Teollisen internetin puolella on nähtävissä taajuuksien ruuhkautumista, minkä vuoksi tutkitaan dynaamisia ja kognitiivisia piirteitä. Tämä sotii IoT:n perusajatuksiin kuuluvaa laitteiden halpuutta vastaan, koska kybersietoisuus ja spektrinkäytön monimutkaistuminen nostavat hintoja. [4]



**Kotitalouksien elektroniikan käyttöönoton aste EU-28 -maissa.** [Estimation of the number of RLNs deployed in Europe in 2025. Euroopan komissio. 2015]

Esineiden internet (IoT) on kovassa kasvussa. Suurin osa laitteista tulee olemaan yhteydessä taustajärjestelmään langattoman tiedonsiirron kautta. Varsinkin logistiikka-alalla ja teollisuudessa internetiin kytkeytyneet sensorit ja ohjaukset tulevat lisääntymään 5G:n myötä, kun yritykset voivat helposti hankkia itselleen yksityisen 5G-verkon. Automaatio-ohjauksessa 5G:n tuomat edut ovat yhteyksien hyvä laatu,

lyhyet viiveet ja turvallisuus. Langattomat sensorit ja ohjaukset tuovat yrityksille joustavuutta tuotantoon ja sen järjestämiseen. Tulevaisuuden 5G tuo tullessaan vielä eimaanpäällisen verkon (non-terrestrial network), jota voidaan käyttää esimerkiksi satelliitin kautta. Tämä tuo IoT:n edut myös syrjäisille seuduille, joihin oman 5G-verkon rakentaminen ei ole taloudellisesti kannattavaa.



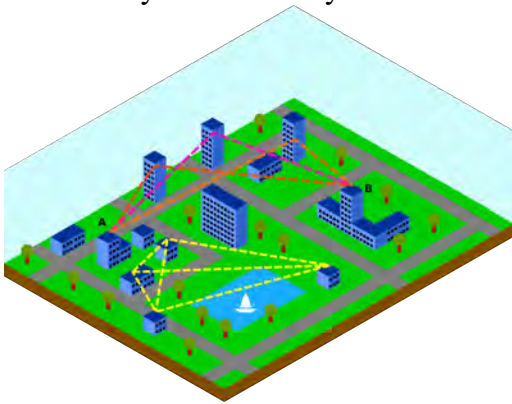
**Esimerkkejä kodin IoT-laitteista. Vinyylilevysoitin, kuivausrumpu, tuuletin, jääkaappi, tiskikone, hammasharja, uuni, pyykinpesukone ja kirkasvalo.**

Euroopan komission vuoden 2015 arvion mukaan vuonna 2020 kotitalouksissa olisi 50 IoT-laitetta. Toisen arvion mukaan teollisen

IoT:n laitteita on vuonna 2025 kaksinkertainen määrä verrattuna kotitalouksien IoT-laitteisiin. Teollinen internet on suurimmaksi osaksi

siirtynyt langattomaksi, ja älykaupungin sovellukset ja sensorit on myös rakennettu langattomiksi. Nämä verkot ovat usein pienitehoisia ja suhteellisen lähellä toisiaan, mutta suurta redundanssia, kuten vaihtoehtoisia reitityksiä tai menetelmiä, niihin ei ole suunniteltu tai rakennettu. Tämä voi johtaa siihen, että häiriö- tai häirintätilanteissa vaikutukset ovat suuret.

5G:ssä käytettävän MIMO (Multiple Input – Multiple Output) -antennitekniikan avulla samalla taajuudella voidaan lähettää eri informaatioita eri paikkaan tai vahvistaa lähetettä käyttämällä hyväksi monitie-



***Punasävyiset katkoviivat kuvaavat MIMO-monitieyhteyttä, joka muodostuu pisteiden A ja B välillä. Saman aikaisesti samalla taajuudella voi toimia esimerkiksi erillinen lyhyenkantaman ad hoc-verkko.***

Koska taajuuksia on rajallisesti ja nähtävissä on jo joidenkin taajuusalueiden ruuhkaantuminen, erilaiset kognitiiviset tietoliikennejärjestelmät ja muut dynaamisesti spektriä käyttävät järjestelmät ovat tulossa lähitulevaisuudessa käyttöön. Yksinkertaistaen dynaamisen ja kognitiivisen järjestelmän ero on, että kognitiivinen järjestelmä havainnoi sille sallittua taajuusaluetta ja käyttää taajuuksia tarpeen mukaan, kun ne ovat vapaina. Dynaaminen järjestelmä käyttää puolestaan sille osoitettua spektriä aikataulutettuna tai alueellisesti kun sen on hallinnollisesti sovittu olevan vapaana. Liikenne- ja viestintävirasto on vuoden 2019 alusta myöntänyt kokeilulupia, joilla samaa taajuutta voidaan dynaamisesti käyttää joko ajallisesti tai alueellisesti silloin, kun toisella käyttäjällä ei ole taajuudelle käyttöä.

etenemistä. Lisäksi sähköisesti keilaavan antennin avulla voidaan muodostaa lähetelle keila, joka palvelee vastaanottajaa parhaiten. Nämä järjestelmien edut aiheuttavat valvonnalle haasteita, koska edullisin paikka vastaanottaa lähetettä on juurikin lähetys- tai vastaanottopäässä. Geometriasta riippuen voi olla, ettei valvonta huomaa kaikkea liikennettä. Tätä voi myös kolmas osapuoli käyttää hyväkseen piilottamalla oman liikenteensä muun liikenteen sekaan. Edistyneen MIMO-tekniikan vuoksi voi olla, ettei alkuperäinen hyötyliikenne edes häiriinny, eikä kukaan huomaa ylimääräistä liikennettä.

Edellä mainitut kehityskulut johtavat siihen, että sähkömagneettinen spektri tulee olemaan hyvin erilainen eri paikoissa. Maaseudulla se pysyy hyvin perinteisen kaltaisena, mutta satelliittitietoliikennejärjestelmät tuovat omat mausteensa. Rakennetuilla ja kaupunkialueilla IoT ja lupavapaat lähettimet muodostavat tulevaisuudessa paikallisesti hyvinkin erilaiset ympäristöt, jotka myös muuttuvat päivittäin eri kellonaikoina. Viikon eri päivinä ja viikonloppuisin spektriympäristö vaihtelee suurestikin. Normaalin erottaminen epänormaalista voi olla hyvinkin vaikeaa. Onko kyseessä häiriö vai häirintä? Selvittäminen voi olla vaikeaa, kun ei tiedetä mikä on spektrin normaali tila.

Perinteisesti Puolustusvoimat on valvonut sotilastaajuuksia, mutta tulisiko koko taajuusalueen olla normaaliolojen aikana tarkemmin valvottu? Ilmannormaali-olojen valvontaa normaalin tunteminen ja sitä kautta poikkeuksien tunnistaminen on vaikeaa. Historiatiedostakin on hyötyä. Mikä on spektrissä normaalia? Miltä spektrin tulisi näyttää maanantaina kello 0900? Entä sunnuntaina kello 1400?

Taajuushallintaa ei tehdä yhdessä/yhteistyössä vastustajan kanssa. Vastustaja voi käyttää muita kuin perinteisiä sotilastaajuuksia tai omaa siviili-infrastruktuuriamme sen mukaan, missä vaiheessa kriisiä ollaan. Valvonnalla ei tarkoiteta viestintäsalaisuuden rikkomista. Tarkoituksena voisi olla esimerkiksi koneoppimisen menetelmien avulla selvittää

aaltomuodon parametrejä ja tunnistaa kuuluuko lähetteen olla spektrissä tai siinä spektrin osassa missä se on.

Millaista valvonnan tulisi olla? Varsinkin ruuhkaisessa ja kiistetyssä (congested and contested) spektrissä lyhyen matkan lähettimillä varustetut sensoriverkot pystyvät piiloutumaan muun liikenteen sekaan. Tällaisten verkkojen löytämiseen ei käy perinteinen valvontajärjestelmä, joka valvoo useamman kilometrin päästä. Taajaan rakennetulla alueella tarvitaan ehkä vastaavanlainen pienistä halvoista verkottuneista sensoreista koostuva valvontaverkko, joka pystyy tunnistamaan lähetteen ja ilmoittamaan havainnosta eteenpäin. Pitäisikö älykaupungilla olla kyky valvoa taajuuksien käyttöä?

Sotilaallisesta näkökulmasta näistä havainnoista on voitava muodostaa tunnistettu spektritilannekuva koko radiotaajuisesta spektristä. Tunnistettu spektritilannekuva täydentää muita tunnistettuja tilannekuvia (maa, meri, ilma, avaruus ja kyber) sekä toimii

operaatioiden suunnittelun ja toteuttamisen apuna.

Lupavapaan liikenteen säätelyssä perusajatuk-  
sena on ollut, että markkinat hoitavat itsensä ja  
laitteiden vaatimuskaisuus takaa häiriöttö-  
myyden. Lupavapaiden lähettimien ollessa  
kyseessä päävastuuta ei ole kenelläkään.  
Jonkinlainen ymmärrys spektristä ja siellä  
vaikuttavaista laitteista tulisi olla jo normaali-  
olojen aikana. Miten nykymalli toimii  
poikkeusoloissa, jos valvonta on häiriöiden  
poistoa ja reaktiivista?

[1] Hallituksen esitys Eduskunnalle laiksi viestintähallinnosta HE 52/2001, <https://finlex.fi/fi/esitykset/he/2001/20010052>

[2] <https://www.traficom.fi/fi/viestinta/viestintaverkot/radiohairioiden-ehkaisy-ja-selvittaminen>

[3] Määräys lupavapaiden radiolähettimien yhteistaajuuksista ja käytöstä, Liikenne ja viestintävirasto, 15 AQ/2020 M, [https://www.finlex.fi/data/normit/46168/Maarays\\_15\\_AQ.pdf](https://www.finlex.fi/data/normit/46168/Maarays_15_AQ.pdf)

[4] Identification of the market for radio equipment operating in licence-exempt frequency bands to assess medium and long-term spectrum usage densities, Euroopan komissio, doi:10.2759/743336

[5] 3GPP nonterrestrial networks Anttonen, Antti; Ruuska, Pekka; Kiviranta, Markku, <https://cris.vtt.fi>

**TELVA**  
1936

**Puolustusvoimien  
luotettava kumppani  
vuodesta 1952**

WWW.TELVA.FI

**RHEINMETALL**  
GROUP

**IAI**

**RH**  
**MARINE**

**ANDRITZ**  
Hydro

**JENOPTIK**

**RENK**

**mtu**

# **Digitalisaatio- ja tekoälyosaamisen kehittäminen Puolustusvoimissa - innovaatioilla tulevaisuuden informaatioympäristöön**

- Kommodori, DI Petteri Kuosmanen -



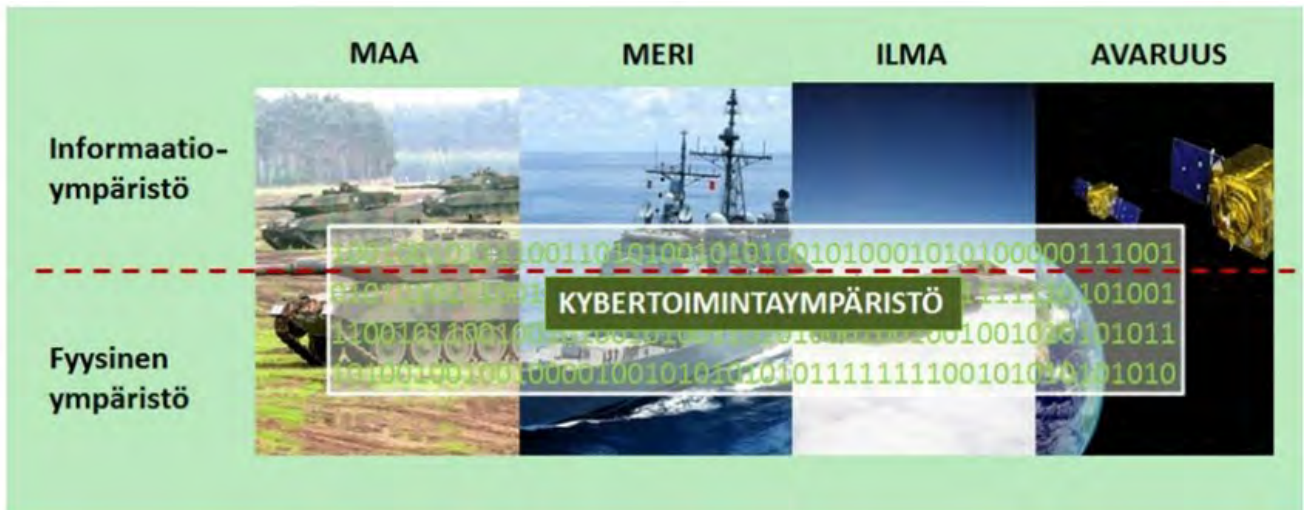
*Artikkelin kirjoittaja on toiminut Puolustusvoimissa yli 25 vuoden ajan koulutuksen, opetuksen sekä erilaisten operatiivisten ja teknisten tehtävien parissa. Puolustusvoimien osaamisen kehittäminen sekä osaamisen innovatiivinen hyödyntäminen on ollut kirjoittajan yksi pääteema nykyisessä tehtävässä.*

1990-luvun lopussa ja 2000-luvun alussa sodankäynnin mullistajina tunnistettiin useita teknologioita ja ratkaisuita. Kuten taktinen internet ja sen osana ohjelmistoradio, täsmäaseet, uudet tutkatekniikat, häivetekniikka sekä suunnatun energian aseet. Näistä mainituista lienee kaikki muut paitsi suunnatun energia aseet ovat edenneet kohti tuotantoa ja käyttöönottoa. Muutoksen suunta ja osittain nopeuskin tunnistettiin tuolloin noin 25 vuotta sitten kohtuullisen hyvin. Kovin radiaalia muutosta ei sotatekniikassa tai sodankäynnissä ole siis tapahtunut viimeisen 25 vuoden kuluessa. Evoluutiota kylläkin ja järjestelmien

tehon kasvua erityisesti niiden verkottumisen myötä. Bitit ovat alkaneet liikkua taistelukentällä lähes yhtä ripeästi kuin siviilisovelluksissakin. Toki myös muussakin kuin elektroniikassa on edistystä tapahtunut. Materiaalit ovat paremmin suojaavia ja ehkä kevyempiä, ajoneuvot kyvykkäämpiä ja tehokkaampia. Mutta iso osa tästäkin kehityksestä voidaan laskea tietokonetekniikan kehityksen lukuun. Mooren laki on näyttänyt voimansa, ja välillä Mr. Murphykin on ollut oikeassa.

2020-luvulle tultaessa teknologinen kehitys on jatkunut kiihtyvällä tahdilla. On alettu yhä useammin puhua odotettavissa olevasta sodankäynnin disruptiivisesta muutoksesta. Tämän muutoksen on arvioitu aiheutuvan yhden tai useamman teknologian seurauksena sekä usein näiden teknologioiden yhteisvaikutuksena. Kun teknologia muuttuu, se mahdollistaa uusia sodankäynnin tapoja. Perinteisten maa-, meri- ja ilmaoperaatioympäristöjen rinnalle ovat nousseet avaruus-, informaatio- ja kybertoimintaympäristöt. Sodankäynti ja varsinkin hybridisodankäynti voi toteutua missä tahansa näistä ympäristöistä tai yhtä aikaa näissä kaikissa. Fyysisessä ulottuvuudessa teknologia mahdollistaa toiminnan laajemmalla alueella, syvemmillä vastustajan maaperällä ja huimalla tarkkuudella. Kehittyneet asejärjestelmät voivat vaikuttaa kauas, nopeasti ja tarkasti. Ajalla ja tilalla on erilainen olemus tämän päivän kriiseissä kuin se oli vielä reilut 30 vuotta sitten.





*Maa- meri- ja ilmatoimintaympäristön rinnalle viime vuosina ovat nousseet avaruus- ja kybertoimintaympäristöt. Kullakin näistä on fyysisen ja informaatioympäristön ulottuvuus. Kyky ymmärtää informaatioympäristön ilmiöitä korostuu tulevaisuudessa.*

Informaatioulottuvuudessa on tehty vielä suurempi loikka. Eikä tämä koske vain sodankäyntiä vaan normaalia arkeakin. Kerätyn informaation määrä on suurempi ja sen laatu on parempaa. Informaatio liikkuu verkottuneissa järjestelmissä Shannonin teoreeman rajoja viistäen. Yhteys saadaan lähes minne tahansa ja lähes kenen tahansa kanssa. Ennen sanomalaiteen 600 bit/s nopeus oli huimaava ja hyvin käyttökelpoinen. Tänä odotamme saavamme suoratoistopalvelun videot näkyviin missä tahansa. Lisäksi yhä pienemmät laitteet kommunikoivat keskenään. Esineiden internet on jo ihmisten arjessa. Tietoa muodostetaan, sitä kerätään ja siirretään yhä kiihtyvällä tahdilla ja sitä hyödynnetään mitä mielikuvituksellisimpiin tarkoituksiin.

Teknisen kehityksen seurauksena tiedosta on tullut entistäkin tärkeämpi voimavara. Vaikka tieto on aina ollut voimavara ja hyödyke, niin nykypäivänä oikean, riittävän ja tarkan tiedon merkitystä ei voi liioitella. Yksikään tavara ei liiku ilman siihen liitettyä tietoa ja tiedon vaihtoa. Kaikki toiminta perustuu yhä suuremmassa määrin tietoon. Mikäli toiminta perustuisi satunnaiseen tai väärään tietoon, niin toiminnasta tulisi päämäärätöntä. Liike säilyisi, mutta suunta puuttuisi. Näin ollen tiedon tai sen yläkäsitteenä informaation sekä fyysisen maailman yhteys on välttämätön.

Tieto on myös ongelmallista. Varsinkin silloin kun tietoa on liikaa ja sen käsittelyyn on aivan liian vähän aikaa. Tässä tilanteessa tietotekniikan tai kuten ennen puhuttiin automaattisen tietojen käsittelyn, eli retrohenkisesti ATK:n, roolilla on merkitystä. Kone prosessoi tietoa ja murskaa numeroita nopeammin sekä tarkemmin kuin yksikään ihminen. Kone jalostaa tietoa ihmiselle sopivaan muotoon ja mahdollistaa sen, että ihminen voi tehdä tämän tiedon perusteella nopeampia ja parempia päätöksiä. Tiedon käsittely digitaalisesti mahdollistaa myös toiminnan kehittämisen - digitalisaation. Digitalisaatiolla käsitetäänkin juuri **toiminnan muuttamista** tai uuteen mahdollistamista. Ilman digitalisaatiota toimintatapamme olisivat varmastikin toimivia, mutta eivät tehokkaita. Oikealla tavalla digitalisaatiota hyödyntävä toiminta tekee asioita nopeammin ja paremmin sekä vähemmällä käsipareilla. Näille käsipareille jää sitten muuta ja mielekkäämpää tekemistä. Digitalisaatiota voinee verrata ojan kaivamiseen kaivinkoneella sen sijaan, että oja kaivettaisiin perinteiseen tapaan lapiolla, kuokalla ja rautakangella. Näinkin oja syntyy, mutta ei sitä nopeasti kaiveta, eikä siitä tule yhtä hyvä (tai syvä) kuin koneella kaivettaessa. Digitalisaatio vie toimintaa fyysisestä ympäristöstä informaatioympäristöön, jossa käsiparien sijasta annetaan koneen hoitaa työläätiä rutiinit.

**Polartherm MIL** THE HEAT IS ON™

Photo courtesy of USAF

**HDU-43**  
Lentokonelämmitin  
NSN 4520-58-000-0441

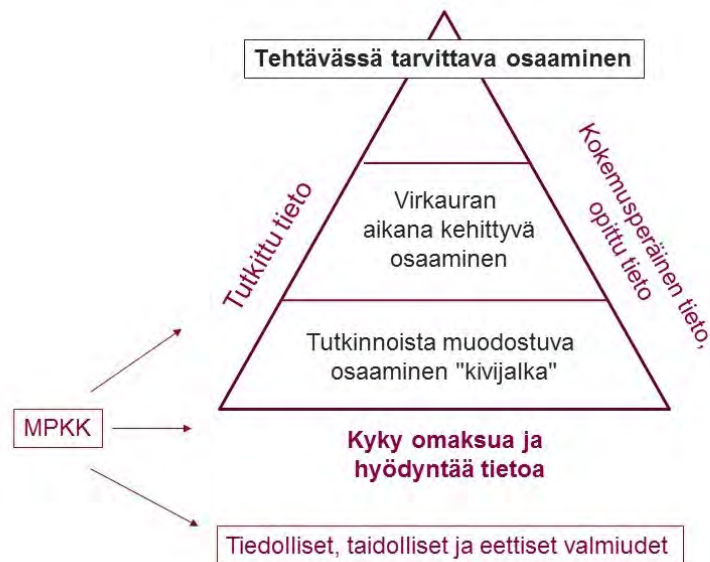
Skannaa QR-koodi ja käy lukemassa tarina: "Story of two water bottles"

[www.polartherm.fi](http://www.polartherm.fi)

Digitalisaation kehitys on linkittynyt erittäin vahvasti tietotekniikan edistykseen. Mitä nopeammin voidaan laskea (eli ajaa tietokoneohjelmia), niin sitä nopeammin rutiinitemppuja voidaan tehdä. Tietotekniikan kehitykseen on alkuajoista saakka liittynyt ajatus älykkästä koneesta - keinotekoisesta älystä - tekoälystä. Eräiden määritelmien mukaan elämme parhaillamme tekoälyn kolmatta tulemistä. Kaksi edellistä tekoälyn esiintuloa ovat päättyneet tekoälyn takatalveen, kun ylioptimistiset kuvitelmat tekoälyn kyvykkyydestä ovat

osoittautuneet virheellisiksi. Nyt tekoälyn kolmanteen tulemiseen onkin lähdetty jossain määrin paremmista asemista. Määritelmistä riippuen meillä on jo käytössä kapeaa tekoälyä useissa arkipäivän sovelluksissa. Sovellus voi olla älypuhelimien kameran toiminnallisuus tai vaikkapa internetin hakukoneen koneoppimista hyödyntävä ominaisuus. Jos digitalisaatio vie toimintaa fyysisestä ympäristöstä informaatioympäristöön, niin tekoäly mahdollistaa informaatioympäristössä entistäkin tehokkaamman toiminnan. Tekoäly on digitalisaation työkalu ja mahdollistaja.

Digitalisaation ja sen työkaluna toimivan



tekoälyn kehitys vie myös sodankäyntiä entistä enemmän fyysisestä ympäristöstä kohti informaatioympäristöä. Tai ehkä oikeamminkin niin, että fyysistä ulottuvuutta ei voi hallita ilman informaatioulottuvuuden hallintaa. Näiden kahden ympäristön keskinäinen sidos ja vuorovaikutus muodostuvat vahvoiksi ja erottamattomiksi. Sodan ja taistelunkuva muuttuu. **Enää ei riitä ainoastaan fyysisen maailman tapahtumien ymmärtäminen. Tarvitaan myös kykyä ymmärtää asioita, jotka tapahtuvat informaatioympäristössä.** Osana tätä ymmärrystä tarvitaan digitalisaatio- ja tekoälyosaamista. Mutta mitä tämä edellyttää sotilasjohtajalta? Tai mitä tämä edellyttää asiantuntijalta, joka suunnittelee tai rakentaa suorituskykyjä, joilla varaudutaan käymään sotaa?

Digitalisaatio- ja tekoälyosaamisen kehittämisen viitekehyksenä on hyödyllistä käyttää Puolustusvoimien palkatun henkilökunnan koko työuran aikana tarvittavan osaamisen muodostumista. Esitän kuvassa 1 näkemykseni osaamisen kehittymisestä erityisesti upseerin virkauran aikana sekä Maanpuolustuskorkeakoulun (MPKK) roolia tämän osaamisen muodostamisessa. Lähtökohtana tarkastelussa on upseerien virkauran aikaisen osaamisen muodostuminen. Sama tarkastelutapa on toki soveltuva muidenkin johto-, suunnittelu- ja asiantuntijatehtävien osaamisen rakentumiseen. Pääajatus on, että työtehtävässä tarvittava osaaminen muodostuu tutkintojen antaman muodollisen osaamisen sekä työuran aikana kehittyvän osaamisen varaan. Tutkinnoissa korostuu opittu tieto, kun taas työuran aikaisessa osaamisen kehittämisessä korostuu kokemusperäinen tieto. Sekä tutkinnoista ammennettava tieto, että kokemusperäinen tieto perustuvat parhaassa tapauksessa tutkimukseen, jolloin osaamisen kehittymisen perustana on tutkitun tiedon omaksuminen.

*Maanpuolustuskorkeakoulu tuottaa tiedollisia, taidollisia ja eettisiä valmiuksia sekä tukee osaamisen kehittymistä tuottamalla tutkittua tietoa. Kyky omaksua ja hyödyntää tietoa on olennaista koko virkauran aikana tarvittavan osaamisen kehittämisessä.*

Olennaisinta on **kyky omaksua ja hyödyntää tietoa sekä soveltaa sitä**. Tällöin puhutaan tiedollisista, taidollisista ja eettisistä valmiuksista. Valmiudet antavat mahdollisuuden varautua tässä hetkessä vielä tuntemattomaan tulevaisuuteen. Näin ollen osaamisvaatimusten rinnalla on järkevää tunnistaa myös laajemmat osaamisvalmiudet. Kovin tarkkoja digitalisaatio- ja tekoälyosaamisen osaamisvaatimuksia upseerin koko virkauralle ei ole edes mielekästä määrittää. Vaikeaksi tämän tekee se, että kyseessä on kehittyvän teknologian aiheuttama jatkuva ja kiivas muutos. Mahdollista sen sijaan on asettaa **vaatimus valmiudesta arvioida muutoksen suuntaa ja sen seurannaisvaikutuksia omaan toimintaan sekä kyky löytää uusia tapoja toimia muuttuneessa toimintaympäristössä**. Tämän

valmiuden luominen vaatii tiedonjanon sekä innovatiivisuuden syöttämistä valmiiksi mietittyjen mallien ja prosessien ulkoa opetteluun rinnalle. Erään sanonnan mukaan köyhän tulee olla kekseliäs. Ottamatta kantaa tulevien vuosien puolustusbudjettiin niin toteaisiin kuitenkin, että innovatiivisuudella ja kekseliäisyydellä olemme ennenkin pärjänneet ja vain sillä pärjäämme tulevaisuudessa. Näin ollen innovatiivinen ja avoin mieli yhdistettynä valmiuteen omaksua uutta tietoa on menestystekijä tulevaisuuden informaatioympäristössä toimittaessa.

Digitalisaatio ja sen yhtenä työkaluna tekoäly linkittävät yhteen tekniikan ja toiminnan. Toisin termein ilmaistuna teorian ja käytännön. Koulutuksen yhtenä kulmakivenä tulisikin olla teorian sitominen käytäntöön konkreettisin esimerkein. Vielä parempi tapa oppia olisi oppia tekemällä ja kokeilemalla. Tunnetusti tekeminen jättää vahvemman muistijäljen kuin saman asian pänttäminen kirjaa lukemalla tai videota katsomalla. Myös valmiuksien kehittämisen kannalta teorian sitominen käytäntöön on mielekästä. Tällöin uudessa tilanteessa hahmotetaan uusi ongelma aiemmin koetun ratkaisun perusteella ja mahdollisesti osataan analysoida ongelmaa myös teoriaan perustuen. Ratkaisu ongelmaan syntyy näin luultavasti nopeammin ja ratkaisu on yhtä iteraatio-kierrosta parempi heti alkuunsa. Koska upseereista ei ole tarkoituksenmukaista tehdä insinööritieteiden osaajia, niin painopiste koulutuksessa on toki enemmän toiminnassa kuin tekniikassa. Toisaalta tekniikan opetuksessa on tärkeää ymmärtää tietyt peruslainalaisuudet sekä erityisesti teknologian mahdollisuudet ja rajoitukset. Tämä tekniikan osaaminen asettaa realistiset reunaehdot toiminnan kehittämiseksi sekä toisaalta myös mahdollistaa toiminnalliset innovaatiot. Innovaatiohan on aika harvoin pelkkää tekniikkaa vaan onnistuminen perustuu usein tekniikan soveltamiseen uudella tavalla.



*Autonomisen järjestelmän demonstraattori, Laykka versio 1.1, © Christian Andersson. Demonstraattoria on ajateltu hyödynnettäväksi tekoälyn mahdollisuuksien havainnollistamisessa opetettaessa teknisiä peruseriaatteita, käyttökonsepteja sekä sodan kuvan muutosta. Kyseinen demonstraattori on hyvä esimerkki fyysisen ja informaatiotoimintaympäristön yhdistymisestä ja informaation merkityksen kasvusta kaikilla tasoilla.*

Puolustusvoimien digitalisaatio- ja tekoälyosaamisen kehittämisessä kenttä on laaja ja tuulinen. Tuulinen siinä mielessä, että asiat liikkuvat jatkuvasti ja tyventä aikaa jäädä miettimään ei ole. On valmistauduttava ja toimeenpantava. Osaamisen kehittämisessä paikalleen jääminen ei ole vaihtoehto, jos ohjaketket halutaan pitää omilla käsissä. Älyn ja osaamisen ostaminen on myös vaihtoehto. Digitalisaatio- ja tekoälyosaamisen kaupallinen tarjonta on laaja ja monipuolinen. Tämän osaamisen ostamiseen on siis hyvinkin mielenkiintoa. Toisaalta pitää muistaa se, että osaamista on eri tasoilla. Insinööriosaamista voidaan ja kannattaakin ostaa, toiminnan kehittämisen osaamistakin on tarjolla. Mutta oman ydintehtävän vaatimaa osaamista ei ole muualla tarjolla. Tai sitten emme ole oikean ydinosaamisen kanssa tekemisissä. Ydintehtävän osaamisen lisäksi suotavaa olisi, että omassa hallussa on riittävässä määrin osaamista kokonaisuuden hallinnasta sekä siitä, että miten tähän kokonaisuuteen voidaan integroida uusia toiminnallisuksia. Toiminnallisten innovaatioiden kehittämisen tulee olla omassa hallussamme, näin toimintaa voidaan kehittää Puolustusvoimien tarpeista lähtien eikä

tekniikka edellä. Tulevaisuuteen tulee mennä osaaminen edellä ja osaaminen varmistaa. Vain ajantasaisella osaamisella on merkitystä.

**Kyberturvan  
asiantuntijat valmiina  
palvelukseen**

Pidämme digitaalisen  
yhteiskunnan toiminnassa.  
Lue lisää palveluistamme [nixu.com](http://nixu.com)

**nixu**  
cybersecurity.

# Perspektiiviä tekoälyn Hype-käyrään

- Insinöörieversti Olli Klemola -

*Digitalisaatio, koneoppiminen, tekoäly, Big Data, Internet of Things, analytiikka...viime vuosina on saatu sanastoomme taas uusia termejä opittaviksi. Melkein kaikki niistä puhuvat, mutta kuinka moni tuntee niihin liittyvän teknologian, mahdollisuudet ja mahdolliset vaarat? Tässä artikkelissa luodaan vapaamuotoinen ja subjektiivinen katsaus teknologian kehittymiseen ja sen hyödyntämiseen lähinnä Puolustusvoimien näkökulmasta.*

## **Perspektiiviä kehittämiseen**

Hieman mahtipontisesta ingressistä huolimatta tässä artikkelissa ei ole tarkoitus pureutua teknologian kehittymisen historiaan kokonaisvaltaisella otteella. Esitetyt ajatukset ja näkemykset perustuvat yksinomaan kirjoittajan omiin kokemuksiin, joihin luonnollisesti on ollut vaikuttamassa verraten pitkä ura Puolustusvoimissa ja ylipäätään teknologian parissa tavalla tai toisella. Niinpä kirjoittajan omakohtainen satunnaisotanta yhteiskunnan ja Puolustusvoimien kyvystä ja halusta omaksua uutta teknologiaa käyttöön edustaa ajallisesti varsin lyhyttä jaksoa, jos sitä verrataan vaikkapa teollisen yhteiskunnan syntymisen ajoista lähtien tapahtuneeseen teknologiakehitykseen.

Elektroniikkateollisuus nousi maailmanlaajuisesti merkittäväksi teollisuudenalaksi vähitellen, kun 1800-luvun lopulla kehitetyn elektroniputken ympärille alkoi kehittyä ihmisten elämää helpottavia ja osin myös viihdyttäviä sovelluksia. Keksittiin ”kipinä-lennätin”, sittemmin radiovastaanotin ja edelleen radiolähetysverkko, gramofoni, puhelin ja paljon muuta. Niin uskomattomalta kuin asia kuulostaakin, niin maailman ensimmäinen väritelevisioon liittyvä patentti haettiin jo vuonna 1897 puolalaisen keksijän

Jan Szczepanikin toimesta. Toki varsinaiset televisiolähetykset aloitettiin Iso-Britanniassa ja Saksassa vasta 1930-luvulla ja nekin aluksi mustavalkoisina, mutta suunta oli kuitenkin selvä: kuluttajien hyödyksi ja viihdykkeeksi tuotettiin alati uusia hyödykkeitä. Maailmansodat kiihdyttivät teknologiakehitystä eritoten sotilaallisten tarpeiden nuotittamana. Sotilajärjestelmien kehitys heijasteli myös kuluttajapuolelle: massiivinen tuotanto ja uudet innovaatiot toivat uusia keksintöjä kuluttajien ulottuville ja ajan mittaan myös hinnat laskivat kasvavien volyymien myötä.

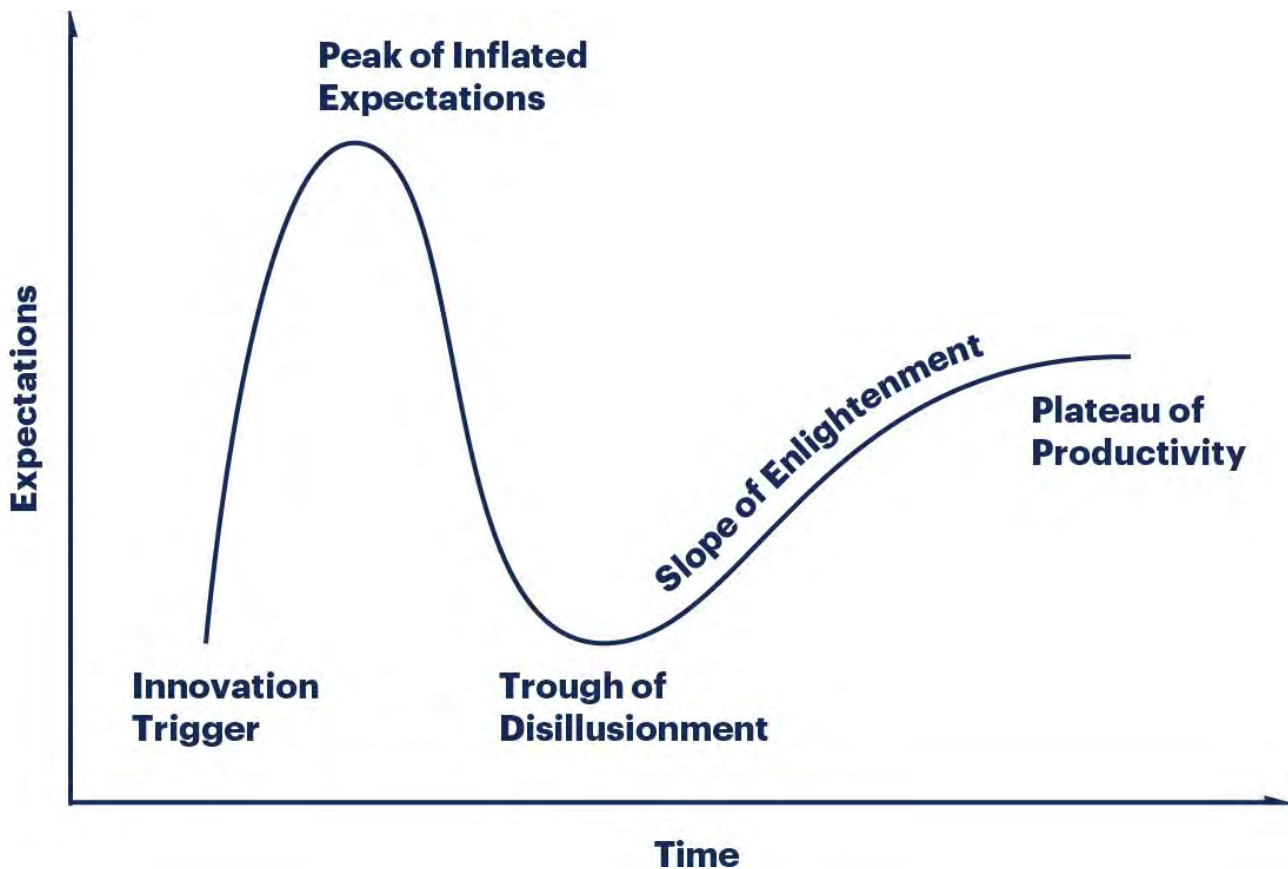
Transistorin keksiminen v. 1947 aloitti omanlaisensa teollisen vallankumouksen puolijohdetekniikan vähitellen korvatessa elektroniputken useissa sovelluksissa. Vähintään sama ja usein myös monin verroin parempi suorituskyky oli mahdollista saavuttaa edullisemmin, vähemmällä teholla ja fyysisesti pienemmillä laitteilla. Puolijohdetekniikan kehitys on ollut ja on edelleen huimaa: Gordon Mooren kehittämän ns. Mooren lain mukaan mikropiirien komponenttitiheys kasvaa kaksinkertaiseksi aina kahden vuoden välein. Tämä ”laki” on pitänyt paikkansa vuodesta 1975 lähtien aina tähän päivään saakka. Verrokiksi voidaan ottaa vaikkapa Suomen ensimmäisiin tietokoneisiin lukeutuva, Teknillisessä korkeakoulussa v. 1954-1960 kehitetty ESKO (Elektroninen Sarjakomputaattori). ESKO perustui elektroniputkiin, diskreetteihin komponentteihin ja ferriittirenkaisiin ja sen suorituskyky oli huimat 20 yhteenlaskua sekunnissa. Nykypäivän kannettavilla tietokoneilla päästään yli sadan gigaflopsin (FLOPS = Floating Point Operations per Second) laskunopeuksiin. Laskentakapasiteetin megalomaaninen kehitys yhdistettynä laitteiden fyysisen koon kutistumiseen on luonut ja luo koko ajan täysin uusia käyttömahdollisuuksia teknologian

hyödyntämisessä niin sotilas- kuin siviili-sovelluksissakin.

### **Alkohämmennyksestä innostukseen – mitä sen jälkeen?**

Edellä kuvattu teknologiakehitys toi kuluttaja-elektroniikan lähes kaikkien arkipäivään. Kehitys oli erityisen voimakasta 70- ja 80-luvuilla. Esimerkiksi 80-luvulla monen yrityksen ja tuotteen nimessä näkyi liite ”tronics”, vaikka yrityksen toimenkuva saatiikka itse tuote ei välttämättä liittynyt

elektroniikkaan millään tavalla. Yhteiskunta oli kuitenkin omaksunut elektroniikan vallankumouksen hedelmät monin tavoin ja näin ollen elektroniikkaan liittyvä positiivinen mielikuva haluttiin välittää kuluttajalle tavalla tai toisella. Voidaan perustellusti väittää, että yhtä lailla yhteiskunta ja me kuluttajat siinä mukana *hypetimme* elektroniikkaa ja sen merkitystä jokapäiväisessä elämässämme. Noudattelipa suhtautumisemme asiaan sitten Gartnerin tunnettua Hype-käyrää tai ei, niin kukaan ei voi kuitenkaan kiistää elektroniikan merkityksen rajua vaikutusta lähes kaikkeen.



**Gartnerin Hype-käyrä (Gartner Hype Cycle, <https://www.gartner.com/en/research/methodologies/gartner-hype-cycle>).**

Puolijohdetekniikan kehitystahti vaikutti 1980- ja etenkin 1990-luvulla teknologian transformointiin diskreetistä analogiaelektroniikasta kohti digitaalelektroniikkaa ja sulautettuja järjestelmiä. Toisin sanoen moni toiminto voitiin toteuttaa yleisillä ”digitaalialustoilla” ohjelmallisesti sen sijaan, että jokaiselle erillistoiminnolle olisi tarvittu oma laitteensa tai piirikorttinsa. Tämä suunnanmuutos avasi luonnollisesti järjestelmäsunnittelussa aivan

uusia mahdollisuuksia samalla lyhentäen huomattavasti suunnitteluajoja. Uusia suorituskäykyisiä tuotteita oli siis mahdollista saada markkinoille aiempaa nopeammin ja paremmilla katteilla.

Mobiiliteknologian kehittyminen on monella tavoin vaikuttanut myös muiden teknologia-alojen kehitykseen ja toimintamalleihin joko suoraan tai välillisesti. Voidaan myös todeta,

että koko yhteiskuntamme on rakentunut nyky-  
muodossaan mobiiliteknologian ja erilaisten  
verkkojen varaan. Paluuta puhelinkoppien ja  
pyöritettävillä valintalevyillä varustettujen  
lankapuhelimien aikakauteen ei ole nähtävissä.  
Olemme oppineet omaksuma kiihtyvällä  
tahdilla uutta teknologiaa ja samalla rakennam-  
me toimintamme ja perusrakenteemme sen  
varaan.

Tämän päivän yhteiskunnassamme yhtenä  
muotisanana on digitalisaatio. Sanalla ei enää  
ihan tarkkaan ottaen viitata enää analogia-  
elektroniikan korvaamiseen digitaalielektroni-  
kalla, vaan merkitykseen on liitetty paljon  
muutakin. Isommassa mitassa kyse on nyky-  
teknologian mahdollistamista palveluista, joista  
näkyvimpanä ilmentymänä voidaan pitää  
internetin varaan rakennettuja palveluita eri  
muodoissaan. Esimerkiksi monet sähköllä  
toimivat laitteet voidaan liittää internetin kautta  
verkkoon, mikä puolestaan mahdollistaa älyn  
lisäämisen aiemmin ”tyhmiltä” vaikuttaviin  
laitteisiin. Puhutaan siis esineiden internetistä  
(Internet of Things) ja niiden tuottamasta  
massiivisesta datamäärästä (Big Data), jota  
voidaan puolestaan käyttää hyväksi vaikkapa  
laitteiden kunnonvalvonnassa ja etäohjelmoin-  
nissa. Hyvänä esimerkkinä olkoon vaikkapa  
kodin lämmitysjärjestelmän ohjelmointi verkon  
ylitse.

Verkottumisen kautta muodostuu myös  
mahdollisuus järjestelmien ja tiedon  
väärinkäyttöön. Järjestelmien ”häkkeröinti” ja  
toiminta-arvojen tahallinen muuttaminen, sala-  
kuuntelu eri muodoissaan, identiteetti-  
varkaudet, kiristäminen ja muu rikollinen tai  
yhteiskunnalle haitallinen toiminta on saanut  
uusia muotoja. Emme aina tule innostuksissam-  
me ajatelleeksi uuteen teknologiaan liittyviä  
uhkia, vaikka varmaankin sopiva balanssi  
elämäämme helpottavien ja viihdyttävien digi-  
palveluiden ja turvallisuuden välillä olisikin  
löydettävissä.

Yhtä kaikki, digitalisaatio-termi on kovassa  
nousussa yhteiskunnassamme Hype-käyrän  
mukaisesti. Digiä käytetään mainosmielessä  
samaa tapaan kuin 80-luvulla aiemmin  
mainittua tronics-liitettä.



*Järjestelmäkeskuksen ikioma robotti ”Oiva”. Kuva:  
Mikael Grundström/Järjestelmäkeskus.*

### **Tekoälyä halvalla, paljonko laitetaan?**

Jos kohta yhteiskunnassa on innostuttu  
hyppäämään melko vaivattomasti uuden  
teknologian tahdittamiin ratkaisuihin, niin  
Puolustusvoimatkaan ei tässä suhteessa ole  
poikkeus. Päinvastoin, joskus vaikuttaa siltä,  
että Puolustusvoimissa lähdetään usein  
rytinällä kehittämään uusia ratkaisuita, mikä  
sinällään tietysti osoittaa ennakkoluulotto-  
muutta ja halua kulkea kehityksen etunenässä.  
Vaarana on kuitenkin monesti se, että rahoitus  
ei riitä uuden kehittämiseen laajassa mitassa  
samalla, kun pitäisi huolehtia ns. legacy-  
kaluston käyttökunnosta. Malti on hyvä valtti  
uuden kehittämisessä. Hypetykseen hyppää-  
minen voi olla turmion tie, jos ei tiedä mihin on  
hyppäämässä. Tämän vuoksi tulevan  
ennakointi nimenomaan tutkimustoiminnan  
kautta on varmempi tapa luoda hyvät perusteet  
kehitettävälle suorituskyvyille.

Yhteiskunnan digihuumassa on saatu populari-  
soitua myös tekoäly ali AI (Artificial  
Intelligence). Lehtien otsikoiden pohjalta tulee  
helposti mielikuva jostakin uudesta ja  
käänteentekevästä teknologiasta: ikään kuin  
kyseessä olisi hopealuoti, joka ratkaisee kaiken.  
Laitetaan järjestelmiin vain vähän tekoälyä,  
niin kyllä se siitä.

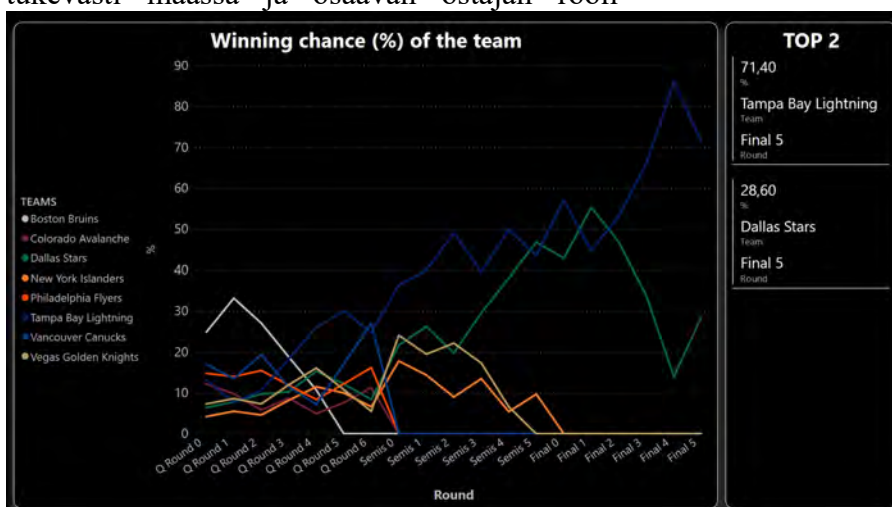
Kuten arvata saattaa, niin tekoäly teknologiana  
ei ole mikään uusi keksintö. Vaikka tekoälyn  
juuria etsittäessä ei nyt ihan antiikin ajan  
filosofointiin mentäisikään, niin toisen

maailmansodan aikoihin sentään. Brittiläinen matemaatikko Alan Turing loi pohjaa koneoppimiselle Church-Turing -väittämässään, jonka mukaan tietokoneilla voidaan simuloida formaalia päättelykykyä. Varsinaisena tekoälytieteen syntyhetkenä pidetään lähteestä riippuen vuotta 1943, jolloin tutkijat Warren McCullough ja Walter Pitts sovelsivat Turingin teoriaa neuronitutkimuksissaan. Varsin pian tähän kontekstiin liitettiin englanninkielinen termi ”electronic brain”. Muistettakoon samassa yhteydessä, että kotimaisen ESKO-tietokoneen eli *sarjakomputaattorin* yhteydessä puhuttiin sähköaivoista, koska tietokone-termiä ei vielä ollut keksitty.

Samaan tapaan kuin kuluttajaelektronikan osalta on käynyt, niin tekoälyn vähittäinen arkipäiväistyminen perustuu paljolti puolijohdetekniikan mahdollistaman laskentakapasiteetin kasvuun. Tavallinen ihminen ei lähtökohtaisesti ole kovin hyvin perillä saatikka edes kiinnostunut tieteen saralla tapahtuvasta kehityksestä. Kun sitten jollakin tieteen alueella saavutetaan läpimurto, paketoidaan tulos suurelle yleisölle maailman suurimpana ihmeenä ja ”galaksit räjäyttävänä” tapahtumana. Tällaisten ilmiöiden ympärille syntyy helposti uutta liiketoimintaa, josta suurin osa on lähtökohdiltaan asiallista. Joukkoon mahtuu myös uusia trendikkäitä termejä hyödyntäviä yritelmiä, joiden hyöty kuluttajalle voi olla kyseenalaista. Sopii toivoa, että valtion hallinnonaloilla osataan pitää jalat tukevasti maassa ja osaavan ostajan rooli

kirkkaana mielessä. Pitää tietää mitä hankitaan ja mihin tarpeeseen: mikä on ongelma, mikä halutaan esim. nimenomaan tekoälyllä ratkaista. Samaan aikaan on syytä miettiä vaihtoehtoisia ja mahdollisesti kustannustehokkaampia ratkaisuja: aina ei ole tarvetta uudelle ja trendikkäälle toimintatavalle, jos vanhalla päästään samaan lopputulokseen.

Tekoälysovellusten määrä on kasvanut huikasti parin viime vuoden aikana. Vaikka kirjoittaja onkin tässä käsillä olevassa artikkelissaan nimellisesti vetänyt hieman suitsista tässä asiassa, ei teknologiakehitystä voi eikä kannata yrittääkään pysäyttää. Kunhan tekoälyn Hype-käyrällä päästään vähitellen tasaiselle alueelle, voidaan todeta yhteiskuntamme ja jokapäiväisen toimintaympäristömme muuttuvan todella nopeasti. Tekoäly ujuttautuu käytännössä kaikille elämänalueille terveydenhuollosta perushyödykkeisiin ja kaikkeen siltä väliltä. Suurena jääkiekon ystävänä kirjoittaja oli erityisen ilahtunut suomalaisen Digia-yhtiön tekemään simulaatioon, jossa koneoppimiseen perustuvalla simulaatiolla kyettiin ennustamaan 71,40 % todennäköisyydellä Tampa Bay Lightningin voitto tämän vuoden Stanley Cup -finaalissa. Tässä simulaatiossa hyödynnettiin otteluvoittojen ennakointiin liittyviä runkosarjan ja pudotuspelien tilastotietoja. Turnaussimulaatio ajettiin läpi 100 000 kertaa, jolloin lopputuloksena saatiin laskettua jokaiselle joukkueelle voittotodennäköisyydet.



Stanley Cup -simulaatio. Kuva: Digia Oy.



## **Puolustusvoimien näkökulma – digistä ja tekoälystä vääntöä hankintoihin**

Digitalisaatiosta ja tekoälystä on käyty kohtuullisen kattavaa keskustelua Puolustusvoimissa. Hype-käyrän nouseva osa oli keskustelun alkuvaiheessa selkeästi tunnistettavissa, mutta melko pian suunta kääntyi alkunnostuksesta pragmaattisuuteen. Puolustusvoimissa on julkaistu tekoälyn tiekartta, joka sisältää kohtuullisen hyvän kattauksen tekoälyn määrittelyistä, kehitysnäkymistä ja sen käytön mahdollisuuksista. Myös digitalisaatiosta on julkaistu oma strategiansa, joskaan se ei ole kattavuudeltaan läheskään samalla tasolla kuin tekoälyn tiekartta. Sen sijaan Pääesikunnan logistiikkaosaston julkaisemassa logistiikan digitalisoinnin tiekartassa määritellään tavoite-tilan visio, strategiset tavoitteet ja selkeät kehittämiskohteet. On huojentavaa havaita Puolustusvoimien yhtäältä riittävän kunnianhimoisen, mutta toisaalta selkeä jalat maassa - lähestymistapaan perustuva suhtautuminen tähän kokonaisuuteen. Esimerkkeinä logistiikan digitalisoinnin pilottiprojekteista mainittakoon mm. logistiikkaan liittyvien palveluiden liittäminen mobiilipalveluun, varusmiesten vaatetushuollon järjestelyt (ml. palvelurobotin hyödyntäminen varusteiden vaihdossa) sekä materiaalilogistiikan digitalisaation kehittäminen.

Digitalisaatiolla ja tekoälyllä on valtavaa potentiaalia sekä ihmisten arjen helpottamisessa, että myös vaativissa päätöksentekoon liittyvissä asioissa. Siinä missä sodankäynnin operaatioiden tempo on kasvanut, on sama ilmiö havaittavissa myös miltei kaikilla elämän aloilla (ken ei usko, palauttakoon mieliinsä vaikkapa Rintamäkeläiset tai Tankki täyteen - TV-sarjat). Vaikeistakin asioista pitäisi saada selkeitä päätöksiä entistä nopeammin ja tarkemmin. Hyvänä esimerkkinä edellisestä käyköön vaikkapa Puolustusvoimien hankintatoiminta. Yksistään HX-hankkeeseen liittyy valtava määrä informaatiota, joka pitäisi omaksua mahdollisimman syvällisesti analyttisen ja tasapuolisen vaihtoehtovertailun toteuttamiseksi. Toimittajaverkostot huomioiden tämän tiedon tuottamiseen ja analysoi-

miseen sitoutuu satoja ihmisiä useiksi vuosiksi. Kuinka hienoa olisikaan, jos vertailukriteeristö ja kaikki siihen liittyvä olennainen informaatio voitaisiin syöttää ”tekoälykoneeseen” ja napin painalluksen jälkeen odotella lopputulosta?

Edellä kuvattu skenaario saattaa hyvinkin olla tulevaisuuden realismia. On kuitenkin selvää, että tällaiseen tavoitelaan mennään lähtökohtaisesti ennalta määriteltyä kehityspolkua pitkin – ellei sitten jokin yksittäinen disruptiivinen läpimurto mahdollista nopeampaa kehitystä. Puolustusvoimien logistiikkastrategiassa todetaan hankintatoiminnan digitalisoinnin tulevaisuuskuvasta seuraavaa: ”Hankinnoissa käytetään robotiikkaa ja automatiikkaa käyttäjän tukena. Ennen kaikkea yksinkertaiset päivittäistavarahankinnat ja kotiinkutsutilaukset tehdään ohjelmistorobottivälineillä. Hankinnan järjestelmien käyttäjäkokemusta parantamalla ja helpottamalla lisätään digitaalisia tapahtumamääriä ja näin edesautetaan prosessien kokonaisdigitalisointia. Automatiikka mahdollistaa automaattiset hankintaehdotukset sekä rajattujen hankintasopimusten kohdalla automaattiset ostotilaukset, hankinnan käynnistää mm. varastosaldojen lasku tai esimerkiksi puheavusteinen toimeksianto eTUVE-mobiililaitteella. Pitkän tähtäimen kehityksessä tekoäly tukee hankintojen johtamista, raportointia ja tilannekuvaa. Tekoäly seuraa mm. Puolustusvoimien ja valtion sopimustilanteita, markkinoita, hintojen kehittymistä ja ostokäyttäytymistä.”

Tekoälyllä on taatusti paikkansa Puolustusvoimien tulevaisuuden hankintatoiminnassa – ei ainoastaan itse hankintaprosessia helpottavana ja avustavana toimintona – vaan myös itse hankinnan kohteena muodossa tai toisessa. Rutiinitehtävät, eri formaateissa olevien tiedonmurusten kerääminen eri paikoista esim. kilpailutuksen kohteiden ominaisuuksien vertailemiseksi ja päätöksentekosyklin nopeuttaminen ovat kaikki asioita, joissa tekoälyllä on hyvin todennäköisesti oma roolinsa lähitulevaisuudessa. Jos taas hankinnan kohteena on järjestelmä, jossa hyödynnetään tekoälyä, pitää teknologia ja sen heijastevaikutukset tuntea todella hyvin. Millä tavalla esimerkiksi

autonomisten järjestelmien muodostaman parven ryhmäkäyttäytymistä (parveilua) hallitaan? Voiko sitä opettaa? Minkälaisella säännöstöllä se jakautuu osaparviin? Minkälaisia voimankäytön sääntöjä (VOKS) hankittavaan järjestelmään liittyy? Minkälaista dataa tekoäly vaatii toimiakseen? Miten taataan datan turvallinen käsittely? Kysymyslistaa voisi jatkaa loputtomiin. Johtopäätöksenä voidaan kuitenkin todeta, että tekoälysovelluksiin varautuminen vaatii rautaista ammattitaitoa eli osaavaa ostajaa. Puolustusvoimien pitää varautua tähän teknologiamurrokseen ennakoimalla asiaan liittyvät osaamistarpeet ja osoittamalla avaintehtäviin osaamistarpeita vastaavaa henkilöstöä.

### ***Tavoitteet korkealle, mutta jalat maassa***

Huolimatta tämän kirjoituksen alkuosan ironis-kseptisestä vireestä kirjoittaja on kuitenkin teknologiamyönteinen perusinsinööri, jolle uuden omaksuminen ei ole periaatteellisesti

vastahakoista. Pitkähkön työhistorian aikana on usein tullut törmättyä tapauksiin, jossa uuden kehittämiseen tunnutaan lähettävän liian innokkaasti, unohtaen samalla monta asia-kokonaisuuteen vaikuttavaa perusasiaa. Yritysten markkinointikoneisto pystyy kyllä perustelemaan asiakkaalle tarpeen, miksi jokin uusi tuote pitäisi saada käyttöön. Tarpeen pitäisi allekirjoittaneen järjen mukaan lähteä kuitenkin itse asiakkaasta. Toki markkinoinnilla on tärkeä sijansa myös uuden tiedon levittämisessä, mutta liika aggressiivisuus voi sotia itseään vastaan. Uuden teknologian ostajan pitäisi myös muistaa, että moni asia perustuu itse asiassa yllättävän vanhoihin innovaatioihin ja teorioihin, jotka ovat saaneet työntövoimaa asialle suotuisten kehityspolkujen kautta. Hyvänä esimerkkinä olkoon vaikkapa jo aiemmin esillä ollut puolijohde-tekniikan kehitys laskentakapasiteetin kasvun mahdollistajana. Mentäköön siis ennakkoluulottomasti eteenpäin, mutta jalat maassa.



# Myydään neljä kiloa tekoälyä

- DI, KTM Alekski Päiväläinen -

*Kirjoittaja työskentelee projektipäällikkönä Atlas Elektronik Finland Oy:ssä. Kirjoituksessa esitetyt näkemykset ovat kirjoittajan omia eivätkä edusta työnantajan kantaa.*

Lapsuus- ja nuoruusvuosinani 1980–1990-lukujen taitteessa kouluun ilmestyi luokka, jonka ovea koristi komealta kalskahtava kirjainyhdistelmä *ATK*. Samoihin aikoihin isäni hankki kotiimme ensimmäisen modeemin, jonka nopeus taisi olla jossain muutaman tuhannen bitin luokassa. Muistan vieläkin elävästi sen telefaksimaisen äänen, jonka modeemi päästi yhdistäessään verkkopankkiin. Muutamaa vuotta myöhemmin perheeseen hankittiin semmoinen ihme kuin matkapuhelin. Ei tarvinnut enää mennä mökillä naapuriin pyytämään lupaa käyttää lankapuhelinta.

Nyt, kolmisenkymmentä vuotta myöhemmin tuo aika tuntuu jopa nostalgisen muinaiselta. Minä ja kanssaihminen olemme itse nähneet ja kokeneet tietoverkkojen, mobiililaitteiden, pilvipalveluiden ja Googlen kautta digitalisaation hitaan mutta varman murroksen. Päivittäisessä kiireessä murrosta ei huomaa, mutta pidemmällä perspektiivillä tarkasteltuna moni asia on mullistunut. Niin yksityis- kuin työelämässä. Mitä tämä murros voi merkitä puolustusteollisuudelle?

## **Tekoälyn historiaa ja hypeä**

Aluksi pieni määritelmällinen täsmennys: Tässä kirjoituksessa tekoäly ymmärretään laajasti yhtenä digitalisaation haarana, jossa korostuvat sellaiset teknologian osa-alueet kuin koneoppiminen, neuroverkot sekä autonomisia piirteitä omaavat järjestelmät. Se on käsitteenä laaja sateenvarjoa, jota ei ole tarkkarajaisesti määritelty.

Ennen digi-innostuksen puuskaa on ehkä paikallaan vetää hetki henkeä ja luoda silmäys

taaksepäin. Hypettävän mediatulvan ja Elon Muskin kaltaisten lennokkaiden visionäärien puheiden perusteella voi syntyä käsitys, että tekoäly ja sen monet sovellukset kuten autonomiset autot olisivat syntyneet äskettäin Googlen, Teslan ja muiden vastaavien yritysten kehityksen tuloksena. Näinhän ei tietenkään ole, sillä urauurtavan kehityksen siemenet kylvettiin jo 1950-luvulla. Yhtenä merkki-paaluna voidaan pitää vuotta 1957, jolloin yhdysvaltalainen psykologi Frank Rosenblatt esitteli neuroverkkojen perusidean. Kiihkeän alun jälkeen innostus laantui ja painui pohjalukemiin suorastaan niin voimakkaasti, että alettiin puhua 1970–80-lukujen ”tekoäly-talvesta”. Tänä aikana nähtiin esimerkiksi puheentunnistuksen epäonnistuminen, DARPA:n AI-tutkimuksen leikkaukset sekä niin sanottujen asiantuntijajärjestelmien nousu ja tuho.

Vasta 2010-luvulla nähtiin neuroverkkojen uusi tuleminen ja sittemmin kehitys onkin ollut huimaa. Skeptisissä puheenvuoroissa muistutellaan edelleen tekoälytalven kompuroinneista ja varoitellaan yliampuista odotuksista. Aiempiin vuosikymmeniin verrattuna tilanne on kuitenkin muuttunut merkittävästi erityisesti laskentatehon eksponentiaalisen kasvun ja keskeisten komponenttien pienentymisen ja halventumisen myötä. Siinä missä 1960-luvun tutkijat joutuivat operoimaan huoneen kokoisilla reikäkorttitietokoneilla, 2020-luvun tutkijalle on tarjolla monituhatkertainen laskentateho omalla kotikonttorilla. Lisäksi tutkimusyhteisöt pyrkivät nyt kaikki mahdolliset ongelmat ratkaisevan yleisen tekoälyn (General AI) sijaan kehittämään huomattavasti rajatumpia tekoälysovelluksia kapeaan ongelmanratkaisuun.

Toki edelleen Gartnerin hype-käyrällä esimerkiksi luonnollisen kielen AI-prosessointi-

teknologiat (NLP) sekä puheohjattavat käyttöliittymät ovat 5–10 vuoden päässä, autonomiset ajoneuvot puolestaan siirtävät edelleen yli 10 vuoden horisontissa. Muutos on kuitenkin todellinen ja oikeastaan ensimmäistä kertaa historiassa on nähtävissä, että tietokoneet kykenevät lähivuosina automaattiseen, merkityksiä ja kontekstia sisältävien tietojen käsittelyyn. Ehkäpä ATK on muutaman vuoden sisällä vihdoin todellisuutta!

### ***Evoluutio evoluution kautta***

Tieto- ja laskentateknologiat – joihin tekoäly tässäkin kirjoituksessa lasketaan – ovat luonteeltaan niin sanottuja yleiskäyttöisiä teknologioita. Tämä lieneekin osin syynä siihen, että ICT- ja AI-teknologioita on usein verrattu merkitykseltään sähköön. Sähkö ja siihen perustuvat laitteet olivat aikanaan 1870-luvulla mullistavia uutuuksia, joita ei suinkaan otettu käyttöön sormia napsauttamalla vaan useiden vuosikymmenien mittaan. Ihmisiltä ja organisaatioilta kesti pitkään oppia, miten uusia keksintöjä kannatti hyödyntää. Esimerkiksi höyryvoimalla toimineet konepajat oli suunniteltu siten, että voimansiirtoakselit saatiin kytkettyä höyrykoneeseen parhaalla tavalla. Sähköllä toimivat koneet toivat aivan uutta toimintavapautta ja joustavuutta tehtaiden suunnitteluun. Aikansa se kuitenkin otti; Joidenkin arvioiden mukaan kesti noin 70 vuotta ennen kuin uuden teknologian tuottavuushyödyistä päästiin nauttimaan täysimääräisesti yrityksissä ja yhteiskunnassa. Omalle sukupolvelleni arkisempi esimerkki on toimistopaperi ja tulostus. Paperitonta toimistoa on odotettu kuin kuuta nousevaa aina ensimmäisestä PC:stä lähtien 1980-luvun alkupuolelta, mutta vasta nyt se alkaa olla todellisuutta. Kotimaassamme tämä näkyy esimerkiksi graafisen paperin kysynnän laskuna ja metsäteollisuuden ahdinkona.

Mitä edellä esitetystä voidaan oppia? Laajat teknologiset murrokset ovat hitaita mutta syvällisiä. Evoluution sijaan ympärillämme tapahtuu kaiken aikaa evoluutiota, jota ei päivittäisessä tai edes vuotuisessa elämäntymisissä huomaa. Sen sijaan useamman

vuosikymmenen perspektiivillä muutos saattaa olla huima.

Toisaalta on hyvä huomata, että ympärillämme on myös paljon pysyvää. Suuri osa meistä esimerkiksi ajaa päivittäin autolla, jonka toiminta perustuu 1870-luvulla kehitettyyn polttomoottoriin. Suomen Ilmavoimat lentää 1970-luvulla suunnitellulla hävittäjällä, ja USA:ssa B-52-pommikoneet ovat edelleen operatiivisessa käytössä.

### ***Sota ja teknologiamurros***

Huolimatta kaikista harhapoluista, viiveistä ja mutkista matkan varrella muutos on todellisuutta. Se toki etenee eri elämänalueilla ei tahtia. Puolustusvoimat kautta maailman ja sitä kautta myös alan teollisuus ovat todennäköisesti luonteeltaan konservatiivisimpien toimialojen joukossa. Sotahistoriasta muistetaan esimerkiksi ne ensimmäisen maailmansodan kenraalit, jotka johtivat joukkonsa ratsuväen opeilla tykistö- ja konekivääri-taisteluun. Kahden maailmansodan välissä sotavarusteiden kehitys oli suhteellisen vaatimatonta verrattuna siviilimaailmassa tapahtuneisiin luonnontieteellisiin ja teknisiin edistysaskeliin. Toisen maailmansodan alkupuolella monet maat huomasivat merkittäviä puutteita järjestelmässään suhteessa uuden sodan luonteeseen. Esimerkiksi Kuninkaallisilla ilmavoimilla ei ollut kykyä suojata Pohjois-Atlantin yli kulkevia saattueita Saksan sukellusvenehyökkäyksiltä sen enempää kuin Luftwaffella oli edellytyksiä tukea omaa sukellusvenelaivastoaan hyökkäyksissä näitä saattueita vastaan. Sodan aikana tilanne kuitenkin muuttui nopeasti, jopa räjähdysmäisesti. Teollisen aikakauden totaalinen sota saavutti massiiviset mittasuhteet.

Viimeisen vuosikymmenen aikana edellä kuvattu digitaalinen evoluutio on siviilipuolella edennyt hyvinkin pitkälle. Esimerkiksi palvelimien vuokraaminen pilvestä on ollut valtavirtaa jo pitkään, kun taas omien palvelimien ylläpitäjät ovat käyneet harvinaisiksi. Eräät turvallisuuskriittiset alat kuten puolustusväline-teollisuus ovat toki edelleen jossain määrin poikkeus.



Siviilipuolella digimurros on luonut myös valtavasti uusia mahdollisuuksia uusille toimijoille. Vanhat ja vakiintuneet toimijat ovat saaneet uusia haastajia sellaisillakin vakiintuneina pidetyillä aloilla kuin auto- tai avaruusteollisuus. Puolustusvälineteollisuus on perinteisesti ollut melko suojattua osin kansallisen turvallisuuden ja poliittisten intressienkin takia. Mutta miten on tulevaisuudessa?

### ***Puolustusvälineteollisuus ja luova tuho***

Luova tuho on taloustieteissä usein käytetty termi, jolla viitataan teknistaloudelliseen kehitykseen, jonka seurauksena uudet ja paremmat teknologiat ja toimintatavat syrjäyttävät vanhat siten, että tietyn toimialan tuottavuus kohoaa. Saadaan siis aikaan aiempaa parempaa halvemmalla hinnalla. Kääntäen samalla rahalla saa enemmän. Puolustusvälineteollisuudessa asian voi ajatella esimerkiksi niin, että viranomaisasiakas saa samalla rahalla entistä enemmän suorituskykyä.

Mitä sitten voivat olla puolustusvälineteollisuudessa luovan tuhon elementit?

Jo kuluneen sanonnan mukaan data on digiajan uusi öljy. Taistelukentällä tämä voi tarkoittaa esimerkiksi sitä, että datasta ja siitä jalostetusta tiedosta tulee ase tai vasta-ase. Datalla yritetään vaikuttaa ja siihen yritetään vaikuttaa. Sitä jalostetaan, muokataan ja manipuloidaan niin

ihmisten kuin yhä enenevässä määrin algoritmien toimesta. Operaatiotempon kasvu edellyttää nopeata päätöksentekoa, jonka puolestaan mahdollistaa aiempaa parempi tilannetietoisuus. Kognitiivisia kykyjä omaavista autonomisista järjestelmistä tulee ihmisten taistelupareja. Mitä ovat ne tuotteet tai ratkaisut, joita yrityksillä on tarjota tähän tarpeeseen? Tai ehkäpä oikeammin sanottuna mikä on se tiekartta, jota seuraamalla tarvittavat ratkaisut kyetään kehittämään?

Esimerkkinä voisi pohtia vaikkapa datan jalostamista neuroverkkojen opetuskäyttöön. Voisiko tiettyyn käyttötarkoitukseen opetettu neuroverkko olla myytävä tuote? Potentiaalisia käyttökohteita ei ole vaikea keksiä, mutta opetusdatan saatavuus ja laatu ovat ilmeisiä ratkaistavia kysymyksiä. Iso kysymys on myös tietoturva, joka tähän asti on voitu monissa tapauksissa ratkaista yksinkertaisesti pitämällä sensori, laite tai muu järjestelmä poissa verkosta. Mutta entäpä jos tulevaisuuden taistelukenttä edellyttää (lähes) täydellistä verkottuneisuutta? Vähintäänkin on odotettavissa, että perinteinen, jäykähkö tiedon luokittelu eri tasoihin etukäteen tulee haastetuksi tämän seurauksena. Jokaisen yrityksen puolestaan olisi hyvä miettiä miten omat tuotteet istuvat tähän kehityskulkuun. Taipuvatko esimerkiksi järjestelmäarkkitehtuurit siihen tietoturvan tasoon, jota hyperverkottunut taistelukenttä saattaisi edellyttää?

## Ero on tuntuva

Kun työelämässä sattuu, me turvaamme selustasi.

724  
€/kk\*

**Kelan myöntämä  
peruspäiväraha**

1868,35  
€/kk\*

**Työttömyyskassan  
myöntämä ansiopäiväraha**

\* jos palkka 3500 €/kk

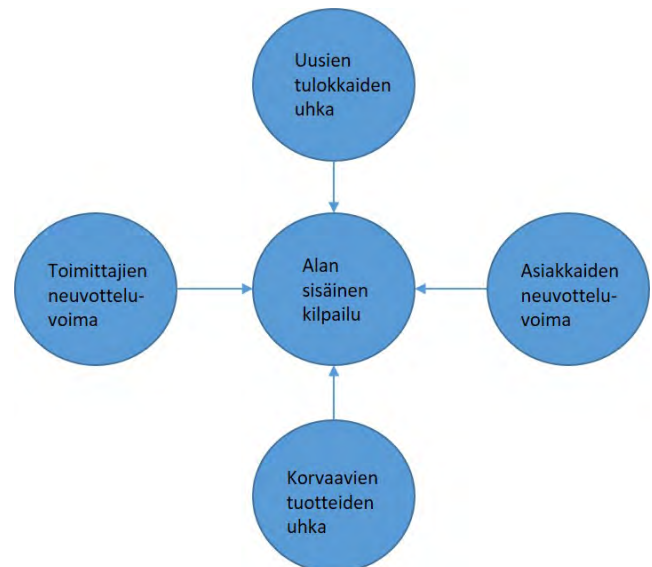
Oma mielenkiintoinen kysymyksensä on kuka nämä uudet ratkaisut kehittää ja toimittaa? Löytyvätkö innovatiivisimmat tulevaisuuden tekijät edelleen perinteisistä puolustusteollisuuden yrityksistä vai ehkäpä Helsingin Maria01-start-up-puistosta? Ovatko toimialan yritykset kiinnostavia työnantajia myös korkeakoulujen penkillä valmistuvien tulevaisuuden huippulupausten silmissä? Luovan tuhon yksi tyypillinen ilmentymä ovat uudet, joskus yllättävätkin haastajat, joita vakiintuneet toimijat eivät ota vakavasti.

### **Kilpailuympäristö á la Porter**

Michael Porterin vuonna 1979 julkaistu viiden kilpailuvoiman malli ("Porter five forces") on yksi yritysstrategian klassikoista ja edelleen yksi käytetyimmistä yritysten strategisista analyysiviitekehikoista. Perusajatus on toimialan kilpailuasetelman ymmärtäminen ja oman yrityksen asemointi tässä kilpailussa. Yrityksen menestys riippuu olennaisesti siitä, miten se tässä onnistuu. Toimintaympäristö muodostuu tekijöistä, joiden pääelementit on esitetty seuraavassa kuvassa. Jos hieman vedetään mutkia suoriksi, niillä tarkoitetaan seuraavaa:

*Uusien tulokkaiden uhka:* Onko toimialalla merkittäviä esteitä, jotka hidastavat tai jopa

estävät uusien toimijoiden tuloa? Tyypillisiä esteitä ovat esimerkiksi liiketoiminnan skaalaedut, tuotedifferointi (eli erottuminen kilpailevista tuotteista esimerkiksi paremmilla ominaisuuksilla), vaadittu pääoma, julkisen vallan politiikka (esimerkiksi regulaatio) tai erityinen osaaminen.



**Porterin viiden kilpailuvoiman malli** (Porter 1979).

*Toimittajien ja asiakkaiden neuvotteluvoima:* Millaiset ovat asiakkaan ja toimittajan väliset

voimasuhteet kaupankäynnissä? Kumpi on alisteisessa asemassa suhteessa toiseen?

*Korvaavien tuotteiden uhka:* Miten paljon asiakkaille on tarjolla korvaavia tuotteita, jotka täyttävät asiakkaan tarpeen?

Miltä puolustustoimialan teknologiamurros voisi näyttää Porterin silmälasien läpi tarkasteltuna?

Edellä mainittiin, että viime vuosina sellaisillakin vakiintuneina pidetyillä aloilla kuten auto- tai avaruusteollisuudessa on nähty uusia tulokkaita. Kiinnostavaa kyllä, klassikko-artikkelissaan Porter (1979) esitti autoteollisuuden esimerkkinä toimialasta, jolla tuotannon automaatio ja voimallinen vertikaalinen integraatio aikanaan lähes poistivat uusien tulokkaiden uhan: ”In the auto industry economies of scale increased enormously with post-World War II automation and vertical integration – virtually stopping successful new entry.” Yksinkertaistaen voidaan sanoa, että tämä on muuttunut vasta Teslan myötä. Vaikka Teslan pitkän aikavälin menestystä ei voida vielä pitää kirkossa kuulutettuna, yritys on jo ravistellut vakiintuneena pidettyä pelikenttää – samoin kuin Elon Muskin toinen voimannäyttö SpaceX. Porterilaisittain automaailman ”häirikön” voi asemoida ainakin substituuttien sekä tuotedifferoinnin kautta. Hyödyntämällä uusia teknologioita (akut, ohjelmistot) Tesla on sekä kyennyt tuomaan markkinoille uskottavia vaihtoehtoja perinteisten autojen rinnalle että pystynyt ylittämään tuotedifferoinnin avulla markkinoille tulon esteet.

Ronskisti yksinkertaistaen niin sanottua perinteistä puolustusvälineteollisuutta voisi luonnehtia esimerkiksi seuraavilla piirteillä:

- Markkinoille pääsyn esteet ovat perinteisesti olleet korkeat johtuen muun muassa tuotannon edellyttämistä mittavista pääomatarpeista, pitkälle erikoistuneista milspeksatuista tuotteista sekä julkisen vallan politiikasta. Markkinoille on vaikea päästä, mutta toisaalta myös vaikea päästä pois (Porterin käsitteistössä niin sanottu ”exit

barrier”), mikäli tuotteet on räätälöity täsmälleen tietynlaisiin tarkoituksiin.

- Potentiaalisten asiakkaiden määrä on pieni, mikä vahvistaa varsinkin isojen ostajien asemaa. Toisaalta samaan aikaan tarjoajien määrä on melko pieni, tuotteet ovat erikoistuneita ja niihin liittyy merkittäviä vaihtamiskustannuksia (switching costs). Nämä piirteet ovat omiaan vahvistamaan myyjän asemaa.
- Substituuttien määrä on rajallinen, mikä osaltaan vähentää asiakkaan valinnanvaraa ja siten laskee kilpailun intensiteettiä.

Noptel LRX etäisyysmittausmoduuli

## Mahtava suorituskyky pienessä koossa

Paino vain 136 grammaa ja mittausetäisyys jopa yli 30 km!



**Noptel** [www.noptel.fi](http://www.noptel.fi)



SYSTEMATIC  
**SITAWARE**

**SYSTEMATIC**

Ei ole mitenkään selvää millä tavoin edellä kuvattu teknologiamurros muuttaa toimintaympäristöä. Joitakin arvioita tai akateemisia arvauksia voidaan kuitenkin tehdä. Hyvin todennäköinen – oikeastaan jo tapahtunut – muutos on toimialan laajeneminen ja sitä kautta sisääntuloesteiden madaltuminen. Kybersodankäynti on tästä konkreettinen esimerkki, jonka myötä markkina on auennut uusille tulokkaille. Älykkään kyberpuolustuksen kehittäminen ei vaadi mittavia alkuinvestointeja tuotantolaitteisiin tai raaka-aineisiin. Samalla ero siviili- ja sotilastuotteen välillä hämärtyy, jolloin mahdollisten substituuttien kirjo kasvaa. ICT-pohjaisten tuotteiden elinkaaret lyhenevät ja sitä kautta myös toimialan kilpailuasetelmat voivat muuttua huomattavasti totuttua nopeammin. Toisaalta kehityksen myötä teknologioista voi tulla niin monimutkaisia, että niiden kehittäminen ja perusteellinen hallinta vaativat erittäin syvää erikoisosaamista, mikä puolestaan saattaa nostaa uusia pääsyn esteitä – ainakin siinä vaiheessa, kun uudet toimijat alkavat vakiinnuttaa asemaansa.

### ***Toimialan pysyviä (?) piirteitä***

On myös huomattava, että puolustustoimialaan liittyy tiettyjä erityispiirteitä, jotka ainakin keskipitkällä ja todennäköisesti myös pitkällä aikavälillä jarruttavat muutosta. Ensinnäkin asiakkaiden määrä ja laatu pysyvät enemmän tai vähemmän vakiona. Toisekseen monet kansalliset ja reaali poliittiset intressit yhdistyvät sodankäynnin melko muuttumattomaan perusluonteeseen, jossa fyysisen maailman *voimankäyttö* tai sen uhka ovat aina läsnä. Tämä edellyttää puolustajalta kykyä vastustaa hyökkääjää kineettiseen tai ei-kineettiseen vaikuttamiseen perustuvilla aseilla kuten ohjuksilla tai tykistöillä. Näiden järjestelmien kehittäminen ja ylläpito lienevät nyt ja tulevaisuudessa niin sanotun raskaan puolustusteollisuuden heiniä. Kolmanneksi taistelukenttä asettaa ainakin operatiivisen toiminnan ytimessä käytettäville tuotteille sellaisia erityisvaatimuksia, joita ei niin sanotuilta kuluttajamarkkinoilta sellaisenaan löydy. Sitä kautta toimialaan erikoistuville yrityksille löytynee tulevaisuudessakin oma ”niche”



(mutta tuoko se tarpeeksi liikevaihtoa?). Neljäntenä toimialan erityispiirteenä voisi nostaa *luottamuksen* merkityksen ympäristössä, jossa lähtökohtana on konflikti viekkaan vastustajan kanssa. *Luottamus* korostuu entisestään digitaalisella taistelulentällä, jossa datan pysyviä attribuutteja lienevät luottamuksellisuus, eheys ja saatavuus. Luottamus rakentuu pitkällä aikavälillä ja siinä auttavat esimerkiksi yhteinen kieli, kulttuuri ja arvopohja.

### **Lopuksi**

Jarruttavista hitausmomenteista huolimatta kenenkään ei kannata kuvitella olevansa immuuni muutoksen edessä. Jokaisen liiketoimintaa harjoittavan olisi syytä viimeistään nyt kysyä itseltään mitä kaikki edellä mainittu merkitsee omalla kohdalla. Onko yrityksessämme oikea tahtotila, kyvykkyudet,

sekä osaaminen? Ymmärrämmekö mitä teknologiamurros tarkoittaa meidän kohdallamme? Mitä ovat uusien teknologioiden tuomat liiketoimintamahdollisuudet? Jos ensimmäinen mieleen juolahtava vastaus näihin on edelleen ”Ei koske minua”, on todennäköisesti jo hävinnyt pelin.

Suomessa on paljon sellaista korkean tason osaamista, jota muutoksessa pärjääminen edellyttää. On elävä start-up-kenttä, korkeatasoista akateemista tutkimusta ja osin Nokian jäljiltä elinvoimainen ICT-klusteri. Monilla puolustusteollisuuden yrityksillä on varmasti erinomaiset edellytykset ja lähtökohdat pärjätä muutoksessa. Onnistuminen on kuitenkin pitkäjännitteistä työtä, pikavoittoja ei ole luvassa. Maraton on vasta alkanut.

*Lähteet: Porter, M.E., (1979). How Competitive Forces Shape Strategy. Harvard Business Review, March Issue.*

## ***Maanpuolustuksen Insinöörit MPI ry***



***Akavalaista edunvalvontaa  
puolustusvoimissa ja -hallinnossa  
vuodesta 1967***

***--- turvallista tulevaisuutta jäsenelle***

***[www.mpiry.fi](http://www.mpiry.fi)***

## Vuoden 2020 insinööriupseeri

- Insinöörieversti Jyri Kosola -



### **Annetaan Andersin kertoa**

Tekniikan kiinnostus heräsi jo aikaisin. Varhaisia muistoja on kuinka viikonloppu-aamuisin ennen vanhempien heräämistä olin jo, kielloista huolimatta, ottamassa esiin ruuvimeisseleitä ja purkamassa eri laitteita. Taitaa yksi vaarilta saamani takkakello olla savuhormin alaosassa vieläkin piilossa, kun en saanut sitä kasaan. Kiinnostus luonnontieteisiinkin heräsi aika varhain, pienen von Däniken ja ufoiluharhailun jälkeen. Tietokoneet tulivat kuvioon Commodore 64 muodossa, pelaaminen ei ollutkaan yhtä hauskaa kuin ohjelmointi. Radioharrastus alkoi SWL-kuuntelulla ja Berliinin muurin murtumista ja Romanian vallankumousta tuli seurattua suorana radioaalloilta.

Tietokoneharrastus vei lukion sijaan kauppaopistoon, siellä kun oli ATK-linja, mutta nuorisosteemien kokeilun koekanina kirjoitin kuitenkin ylioppilaaksi. Varusmiespalveluksen aikana Keski-Suomen Viestipataljoonassa sain koulutuksen keskussanomalaitteelle. Palveluk-

sen aikana suoritin radioamatööritutkinnon, josta on ollut iloa ja hyötyä myöhemmin.

Seuraava askel olikin 1994 UNPROFOR/FYROM rauhanturvaoperaatio Makedoniassa. Tehtävä oli radioryhmässä, joka hoiti HF kaukokirjoitinyhteyttä Suomeen ja pataljoonan HF koulutusta ja radioiden asentamista. Uutena laitteena oli keskussanomalaite, jolla hoidettiin yhteydet kaukaisille tarkkailuasemille ja Suomen vartiojoukkueeseen Kroatiaan.

Kauppaopiston aikana innostuin talousmaantiedosta, jota menin opiskelemaan Åbo Akademiin, mutta puolen vuoden opiskelun jälkeen veri veti IFOR operaatioon Bosniaan. Tehtävä oli viestiryhmän johtaja. Vuoden pataljoonassa olon jälkeen pääsin uuteen tehtävään Pohjoismais-Puolalaisen Prikaatin esikuntaan, pioneirimateriaali-aliupseeriksi.

Porin Prikaatissa oli samaan aikaan aloitettu Kansainvälisen Valmiusjoukon koulutus. Sinne haettiin kessuja kouluttamaan varusmiehiä. Hain ja pääsin kouluttamaan panssaritiedustelujoukkuetta ja komento- ja huoltojoukkuetta. Samaan aikaan olin mukana kehittämässä englanninkielisen viestiliikenteen koulutuspakettia. Vuoden jälkeen oli taas aika vaihtaa maisemia ja palata opiskelemaan, mutta maailmanrauha halusi muuta. Löysin itseni taas Bosniasta tällä kertaa taas radioryhmästä, neljässä vuodessa oli sentään nauhakaukokirjoitin vaihtunut päätteeseen.

Kahdeksan kuukauden jälkeen oli paluu Suomeen, tällä kertaa Suomenlahden Meripuolustusalueelle, ensin sanomaviestittäjäksi. Syksyn radistikurssin jälkeen olisi ollut meno radistiksi jollekin alukselle, mutta hakeuduinkin syksyksi Maanpuolustusopistolle, tarkoituksena opiskella viestilinjalla. Opistolla tulikin mahdollisuus muutamille maavoimien kiintiössä olleille opiskella elsoa ilmavoimien

viestikoululla. Opistoupseeriksi valmistuttuani siirryin Viestikoululle Maavoimien elso-osastolle josta myöhemmin muodostettiin ensimmäinen elso-yksikkö. Riihimäellä aloitin AMK-opinnot ja valmistuin muutaman vuoden jälkeen AMK-insinööriksi.

Taas 2004 oli tarkoitus mennä Bosniaan rauhanturvaajaksi, mutta koulutuksen aikana sain tiedon että minut oli valittu osasto-insinöörin virkaan Pääesikunnan Tutkintaosastolle, joten Bosnia sai jäädä. Tutkintaosastolla sain tehdä mielenkiintoisia insinöörin hommia tekniikan parissa ja vuoden verran toimin osaston tietohallintopäällikkönä. Jaksoon kuului myös vuosi EU-taisteluosastossa (Nordic Battlegroup) elso-osaston järjestelmäinsinöörinä. Saman aikaisesti opiskelin YAMK-tutkinnon.

Vuonna 2012 onni potkaisi ja pääsin Defence Academy UK/Cranfield yliopistoon opiskelemaan Military Electronics Systems Engineering linjalle (linja on perustettu ja nimetty kylmän sodan aikana, opintojen aiheet liittyvät elsoon). Vuoden jälkeen paluu oli yllättäen Pääesikunnan Materiaaliosastolle. Ilmeisesti sanat system ja engineering peräkkäin takasivat paikan vaatimustenhallinnan ja hanketoiminnan parissa. Työ kuitenkin tekijäänsä opettaa, opin paljon systems engineeringistä, menetelmistä, prosesseista ja hankkeista. Logistiikkaosasto yhdistettiin materiaaliosastoon ja nimettiin logistiikkaosastoksi, josta löysin itseni samoista hommissa edelleen. Kansainvälistä makua sain FISE-yhteistyöstä, NATO:n Life-cycle management groupista ja EDA:n CODABA työstä.

Pääesikunnan suunnitteluosasto oli vuorossa 2016, tutkimus ja kehittämisselktorilla oli tarjolla T&K rahoituksen järjestelyä ja seuranta sekä Puolustusvoimien Tutkimuslaitoksen ohjaamiseen osallistuminen. Odottamatta 2018 tarjoutui elso-tutkimusalojohtajan tehtävä Tutkimuslaitoksella, johon lähdin mielelläni.

Minulla on ollut onni mukana ja olen saanut työskennellä mielenkiintoisissa ja hyvinkin erilaisissa tehtävissä. Esimiehet ovat kannustaneet opiskelemaan ja antaneet siihen aikaa.

Työkaverit ja alaiset ovat sopivasti haastaneet ja auttaneet. Omalta osalta voin vain kiittää Puolustusvoimia opiskelun mahdollistamisesta ja tehtävä kirjosta mitä olen saanut tehdä. Itse olen yrittänyt pitää yllä sotilasinsinöörin molempia osia, olla sotilas ja insinööri, vaikka välillä on tunne että on "Jack of all trades, master of none".

Opinnot:

2012-2013 Defence Academy UK/Cranfield University, MSc, Military Electronic Systems Engineering  
2010-2011 Metropolia ammattikorkeakoulu, YAMK-insinööri, Industrial Management  
2002-2004 Hämeen ammattikorkeakoulu, AMK-insinööri, Tietoliikenne  
1999-2002 Maasotakoulu/Ilmavoimien Viestikoulu, Opistoupseeri elso-opintosuunta

Palvelus Puolustusvoimissa

2018- Puolustusvoimien Tutkimuslaitos  
2016-2018 Pääesikunta, Suunnitteluosasto  
2014-2016 Pääesikunta, Materiaaliosasto  
2012-2013 Maanpuolustuskorkeakoulu  
2007-2008 EU-taisteluosasto  
2005-2012 Pääesikunta, Tutkintaosasto  
2002-2004 Etelä-Suomen Viestipataljoona  
2002 Viestikoulu  
1999-2002 Maasotakoulu/Ilmavoimien Viestikoulu  
1999 Suomenlahden Meripuolustusalue, Operatiivinen osasto  
1998-1999 SFOR, Bosnia  
1997-1998 Porin Prikaati  
1996-1997 IFOR, Bosnia  
1994-1995 UNPROFOR/FYROM Command, Makedonia  
1992-1993 Keski-Suomen viestipataljoona



Sähköjärjestelmien suunnittelu ja valmistus: johtosarjat, kaapeloinnit ja kojeistot

# Sotalaivaprojekti nyt ja tulevaisuudessa

- DI, Eero Järvenpää -



*DI Eero Järvenpää toimii projektipäällikkönä DA-Groupin Defence-yksikössä.*

Merivoimien tähän asti suurin alushanke porskuttaa eteenpäin, minkä seurauksena Merivoimat saa tämän vuosikymmenen toisella puoliskolla maailman mittapuussa ainutlaatuiset Pohjanmaa-luokan korvettinsa käyttöönsä. Mutta mitä modernin sotalaivan suunnittelu on ja minkälaiset tekijät ovat vaikuttaneet ja tulevat vaikuttamaan suunnitteluprosessiin?

Luomme tässä katsauksen keskeisiin tekijöihin, jotka ovat muuttaneet sotalaivaprojektin luonteen monilta osin lähes kokonaan viimeisten vuosikymmenten aikana ja pohdimme myös tulevaisuuden näkymiä.

## **Taistelunkestävyys – elintärkeä osa modernia sotalaivaa**

Sotalaivahistoriaan katsoessa on selvää, että valmistusteollisuuden läpimurrot sekä aseiden ja uhkakuvien monipuolistuminen ovat kiihdyttäneet sotalaivalle asetettavia vaatimuksia, mistä on seurannut laivojen kasvu niin mitoitetaan kuin hintalapultaan. Siinä missä muinaiset foinikialaiset paransivat ja hioivat laivastoaan vuosisatojen ajan peruskonseptin suhteellisen samanlaisena, on pelkästään 1900-luvulla nähty valtava muutos nopeista laivoista panssarilaitoihin, joista nopeampien ketterien alusten kautta nykyaikaisiin häivefokusoituneisiin laivoihin. Näistä tunnetuimmat esimerkit ovat ruotsalainen Visby-luokan korvetti sekä yhdysvaltalainen Zumwalt-luokan hävittäjä, jotka eivät välttämättä miellytä perinteisempää tyyliä arvostavan silmää.



*Pieni, taktinen miehittämätön ilma-alus RQ-21A Blackjack juuri laukaistuna San Antonio-luokan maihinnousutukialukselta USS San Diegolta (LPD 22). Lähde: U.S. Marine Corps photo by Cpl. Jeremy Laboy/Released*

Koska kukaan meistä ei ole häppöinen ennustaja, niin yhden spesifin oletuksen tai ennustuksen varaan sotalaivan suunnitteleminen ei ole järkevää, vaan on syytä tutkia epätodennäköisimpiäkin tulevaisuuden skenaarioita ja tutkia, miten ehdotettu konsepti pärjäisi myös näissä tilanteissa, mukaan lukien erilaiset asevaikutukset. Tässä työssä oleellisissa roolissa ovat kokeneet eri alojen asiantuntijat, joiden verkottunut asiantuntijatiimi pystyy analysoimaan ja esittämään perustellut johtopäätökset päätöksentekijöille jo hyvin varhaisessa projektin vaiheessa eri konseptien hyvistä ja huonoista puolista. On päivänselvää, että vaillinaisesti tai vaarallisiin oletuksiin perustuvat vaatimukset voivat tehdä vielä valmisteilla olevasta sotalaivasta vanhentuneen jo ennen valmistumistaan.

Menneisyydessä ovat ajat, kun esimerkiksi taistelunkestävyysanalyysi tehtiin vasta

valmiille laivalle kuukausien työnä, jolloin juuri mitään ei ole enää tehtävissä – ainakaan järkevin kustannuksin. Nyykään sama syntyy oleellisin osin, vaikka useamman kerran saman päivän aikana jo projektin ensimetreiltä lähtien.

### **Modulaarisuus**

Sotalaivojen kyvykkyyksiin kohdistuu yhä suuremmat, monipuolisemmat ja usein myös keskenään ristiriitaiset odotukset ja vaatimukset, minkä seurauksena selvä trendi maailmalla on kohti modulaarisuutta aseistuksen sekä muiden tehtäväjärjestelmien osalta.

Yleisin tehtävämoduulialusta on standardimerikontin kokoinen, vaikkakin monesti varta vasten tarkoitukseen rakennettu. Tehtävämoduuli voi sisältää täydellisen miinoitusjärjestelmän, nopean toiminnan veneyksikön tai esimerkiksi syvyytettävän kaikuluotaimen kaikkine järjestelmineen. Näin modulaarisuus mahdollistaa operointiprofiilin vaihtamisen tunneissa täysiverisestä miinoittajasta kriisinhallinta- tai öljyntorjunta-alukseksi.



***Tulenjohtaja ohjushävittäjä USS Chung-Hoonin (DDG 93) taistelukeskuksessa RIMPAC 2020 – harjoituksessa. Lähde: (U.S. Navy photo by Mass Communication Specialist 1st Class Devin M. Langer)***

Modulaari-ajattelu myös mahdollistaa ja helpottaa reagoimista alati muuttuvan maailman uhkakuviin. On oleellisesti helpompaa ja nopeampaa hankkia ja asentaa muutama uusi tehtävämoduuli tiettyyn tarpeeseen kuin asentaa kiinteitä järjestelmiä olemassa olevaan ja yleensä hyvin täyteen ahdettuun laivaan. Lisäksi perinteisten raskaampien miehitettyjen ratkaisujen tilalle ja rinnalle on vahvasti tulossa kevyemmät, joustavammät ja erityisesti miehittämättömät ratkaisut niin pinnan päälle kuin pinnan alle, joiden avulla voidaan pitää suurempi ja arvokkaampi tukialus sekä ihmiset kauempana mahdollisesta uhasta. Erityisesti miehittämättömien alusten nopea kehitys tukee modulaarisuutta, jolloin vältetään kovin tiukka ja usein kallis sitoutuminen tiettyyn teknologi-asukupolveen. Niin sanottu konttiratkaisu on myös helppo siirtää maihin huollettavaksi ja päivitettäväksi ilman laivan seisottamista satamassa tai telakassa.

Modulaarisuus helpottaa ja sujuvoittaa myös elinkaaripäivitystä, jolloin hieman kärjistäen voisi ajatella, että vaihdetaan uudet moduulit vanhojen tilalle. Näin helppo elinkaaripäivitys on tosin vielä toistaiseksi utopiaa, mutta nähtäväksi jää, ladataanko jotain päivänä laivan kyljestä valmiiksi kalustettu taistelukeskus vanhan tilalle.

### ***Digitaalinen kaksonen***

Nykyään laiva – oli kyseessä sota- tai kauppalaiva – aloittaa elämänsä digitaalimaailmassa vuosia ennen ensimmäistäkään hitsisaumaa tai laitehankintaa erilaisina konsepteina, tutkimuksina ja selvityksinä. Näistä erilaisten vaatimusmäärittelyjen, tarkasteluiden ja hyväksyntäprosessien kautta jokin versio jatkaa elämäänsä kehittyen lopulta yksityiskohtaiseksi 3D-malliksi, josta syntyy nykyään puoliautomaattisesti rakennuspiirustuksetkin laiva- ja taisteluteknisten analyysien sekä hienojen grafiikoiden lisäksi. Laivan valmistuttuakin digikaksonen jatkaa tyyppillisesti elämäänsä reaalisiskonsa rinnalla niin vauriontorjuntasimulaatioiden, lastauslaskimen kuin elinjaksopäivityksen suunnittelun pohjana.



T&G Nordic Oy,  
Verkkorinte 2,  
03100 Nummi  
p. 020 753 9750

## PUOLUSTUS JA TURVALLISUUS

Kytentäjäjärjestelmät meren pohjasta avaruuteen ja kaikkeen siltä väliltä.  
Suunnittelun tuki, komponenttien hankinnat, kokoonpano, testaus ja dokumentointi



KATAKRI FSOC LEVEL III



## TEOLLISUUSAUTOMAATIO

Automaatio sovellukset HW- ja SW-tuella. Suunnittelun tuki, komponenttien hankinnat, kokoonpano ja testaus



## KOMPONENTIT

Tehdassopimuksilla suoraan alkuperäisiltä valmistajilta. Myös asiakaskohtaisesti räätälöidyt



## Laskentakyvyn räjähdysmäinen kasvu

Jo vuonna 1965 Gordon Moore kuuluisasti ennusti transistoreiden määrän tuplaantumisen ensiksi vuosittain ja 1975 päivituksen myötä joka toinen vuosi, mikä on pitänyt tähän päivään asti kutinsa. Laskentakyky onkin triljoonakertaistunut vuodesta 1956 vuoteen 2015, mistä yhtenä konkreettisenä ja arkisempaan käytännön esimerkkinä on jo pelkästään vanhentuvan pelikonsolisukupolven yli satatuhatkertainen laskentakyky verrattuna Apollo 11:n ohjaustietokoneeseen.

Laivanrakennuksen kannalta käyttökelpoisen laskentakyvyn ja siten käytettävissä olevien työkalujen räjähdysmäinen kasvu on realisoitunut erityisesti viimeisen parin vuosikymmenen aikana, kun esimerkiksi virtausmekaniikan Navier-Stokes-yhtälöiden ratkaiseminen laivamittakaavassa numeerisin menetelmin on tullut ensiksi yliopistojen ja isojen toimijoiden, mutta viimeisinä vuosina kenen tahansa ulottuville. Tämä totta kai mahdollistaa entistä suurempien

ja yksityiskohtaisempien mallien ja ilmiöiden tutkimisen sekä pidemmälle menevän monimuuttujaoptimoinnin pienillekin toimijoille. Tämä on lisännyt kilpailua ja siirtänyt kehityksen kärkeä yliopistoilta ja tutkimuskeskuksilta enemmässä määrin yrityksiin.

Laivaprojektin kannalta tämä tarkoittaa käytännössä, että tilavarausten, erilaisten asevaikutusten, häiveominaisuuksien ja laivateknisen suorituskyvyn suunnittelu ja testaaminen digimaailmassa on helpompaa ja ennen kaikkea nopeampaa kuin koskaan, joissain ääritapauksissa jopa ensi kertaa mahdollista.

## Ajantasainen tieto – turvallisesti

Laskentakyvyn kasvaminen ja entistä helppokäyttöisemmät työkalut mahdollistavat entistä monimutkaisimpien ongelmien ratkaisemisen niin omalla kuin vastapuolellakin. Tämän seurauksena laivat, laivajärjestelmät ja puolustuksen kokonaisratkaisut kasvavat jatkuvasti monimutkaisemmiksi ja laajemmiksi kokonaisuuksiksi, jotka ovat myös kalliimpia

hankkia ja ylläpitää. Tästä seuraa myös entistä suurempi vastuu hankkeiden suunnittelijoille ja vaatimuksenasettajille, joiden tarvitsee hallita yhä suurempia ja abstraktimpia kokonaisuuksia niin reaali- kuin kybermaailmassa sekä vastata ratkaisuilleen niin tiedossa oleviin nykyisiin kuin myös odotettuihin ja odottamattomiin tulevaisuuden skenaarioihin.

Kokonaisuuksien kasvaessa harva yksittäinen taho tai henkilö pystyy enää hallitsemaan koko pakettia, vaan hankkeeseen osallistuu verkottunut asiantuntijatiimi, jonka eri osa-alueiden erikoisosaamiset mahdollistavat osiensa summaa paremman lopputuloksen. Tässä tosin törmätään hyvin nopeasti realiteetteihin ihmisten asuessa ja toimiessa eri paikkakunnilla ja monesti myös eri maissa. Tästä seuraa myös tarve turvalliseen kommunikointiin ja tiedonsiirtoon: Julkisessa verkossa ei arkaluontoisia asioita käsitellä millään tasolla, vaan tarvitaan tarkoituksenmukainen turvallisen tiedonsiirron ja –hallinnan ratkaisu.

Tätäkin osaamista ja ratkaisuja löytyy onneksi kotimaasta nykyisiin ja tuleviin tarpeisiin. Aika näyttää tosin, mitä kvanttilaskennan aikakausi tuo mukanaan, ja koska.

### ***Katse tulevaan***

Moni asia maailmassa ja Suomessa on muuttunut siitä, kun Laivue 2020-hanke käynnistettiin, saati sitten Laivue 2000. Kuitenkin tietyt perustarpeet näyttävät pysyvän muuttumattomina, ja ovat ajankohtaisia vielä silloinkin, kun seuraavia alushankkeita käynnistetään: tarve kommunikoida projektin sisällä sujuvasti, tarve ajantasaiseen tietoon läpi projektin sekä ehkä tärkeimpänä rohkeus yhdistää vanhaa kokemusta uusiin näkemyksiin ja ratkaisuihin, jotta lopputulos vastaa asiakkaan tarpeita myös siinä tapauksessa, kun tulevaisuus näyttääkin kovin erilaiselta kuin mistä kaikki mukana olleet olivat yhtä mieltä silloin 15 vuotta sitten.



Lue lisää: [www.rmcf Finland.fi](http://www.rmcf Finland.fi)



# 130 TK tornikanuunan suuntausjärjestelmä

## prototyypeistä sarjalaitteeksi 1975 – 1985

- DI Jorma Pesonen -

### Johdanto

Tornikanuunahankinta teknisen asiahoidon, vaatimustenhallinnan ja tekniikan kehityksen näkökulmasta tarkasteltuna, sekä yhteistyö eri toimijoiden kanssa huomioiden. Asejärjestelmissäkin oltiin siirtymässä ”mikroprosessori-aikaan”, rannikkotyökistö yhtenä ensimmäisistä.

### Prototyypin hankintasopimus

Raskaan tornikanuunan kehittäminen alkoi 1970-luvun alkupuolella toimineiden parlamentaaristen puolustuskomiteoiden suosituksesta. Kaukosuunnatun raskaan tornikanuunan prototyypin hankintasopimus n:o 522/Hank-75 allekirjoitettiin 6.8.1975 Tampellan ja Pääesikunnan välillä. Sopimuksen kaupallinen osio oli 3-sivuinen. Prototyypin toimituksella asetettiin vaiheittaiset luovutusaikataulut siten, että viimeinen vaihe, dokumentointi oli tammi-kuussa 1978.

Sopimuksen tekninen osio ”130 TK-prototyypin suunnittelulle ja valmistukselle asetetut vaatimukset” oli 9-sivuinen asiakirja, jossa määriteltiin suuntausjärjestelmälle mm seuraavat vaatimukset:

- tykki on suunnattavissa vapaasti ympäri kumpaankin suuntaan (sivusuuntaus)
- tykin putken korotuskulma on suunnattavissa vapaasti ylös ja alas määrättyllä alueella (korkeussuuntaus)
- suuntausnopeuksille, kiihtyvyyksille ja hidastuksille on määritetty vaatimukset, samoin kuin seurantatarkkuudet automaattisuuntauksessa myös erittäin hitaat maalit huomioiden
- maalivaihdolle (askelmuutokset) on asetettu asettumisajat sekä seurantatarkkuudet automaattisuuntauksessa

- pääsuuntaustapa on tutkan/keskuslaskimen (RAVAL) ohjaama automaattinen kaukosuuntaus, muita suuntaustapoja ovat käsi-suuntaus moottoreita ja käsisuuntaus käsipyöriä käyttäen

Lisäksi oli periaatteellisia vaatimuksia mm. hallinta- ja turvalaitteille, dokumentoinnille sekä ympäristöolosuhteille.

Aloitin Pääesikunnan sähkötekniillisellä osastolla 1.10.1975 tehtävinä mm. 130 TK-hankinnan suuntausjärjestelmän tekninen asianhoito ja 100 56 TK-tornikanuunan sähkölaitteiden kunnossapidon suunnittelu ja koulutus. Olin juuri kotiutunut varusmiespalveluksesta, Karjalan Prikaatin Viestikomppania, ts. jalkaväen viestimiehenä. Varusmiespalvelukseen menin opiskelujen valmistumisen, Oulun Yliopisto Sähkötekniikan osasto 30.5.1974, jälkeen. Teknisenä asianhoitajana, sellaista ei kuulunut opinto-ohjelmaan, aloittelin täysin nollasta.

### Suunnittelu

Tornikanuunan suunnittelu alkoi yhteistyössä Tampellan ja Pääesikunnan Asetekniillisen osaston (asejärjestelmä ja hankkeen johto), Sähkötekniillisen osaston (suuntausjärjestelmä) sekä Rannikkotyökistötoimiston (toimeksianto ja käyttäjävaatimukset) kesken noin kuukauden välein pidetyillä kokouksilla ja katselmuksilla. Välillä edettiin hyvin, välillä soudettiin ja huovattiin. Pääesikunnan hanke/projektiryhmä kokoontui myös noin kuukauden välein tarkastelemaan hankinnan edistymistä. Pääesikunnan Hankintaosasto vastasi hankinnan kaupallisista asioista.

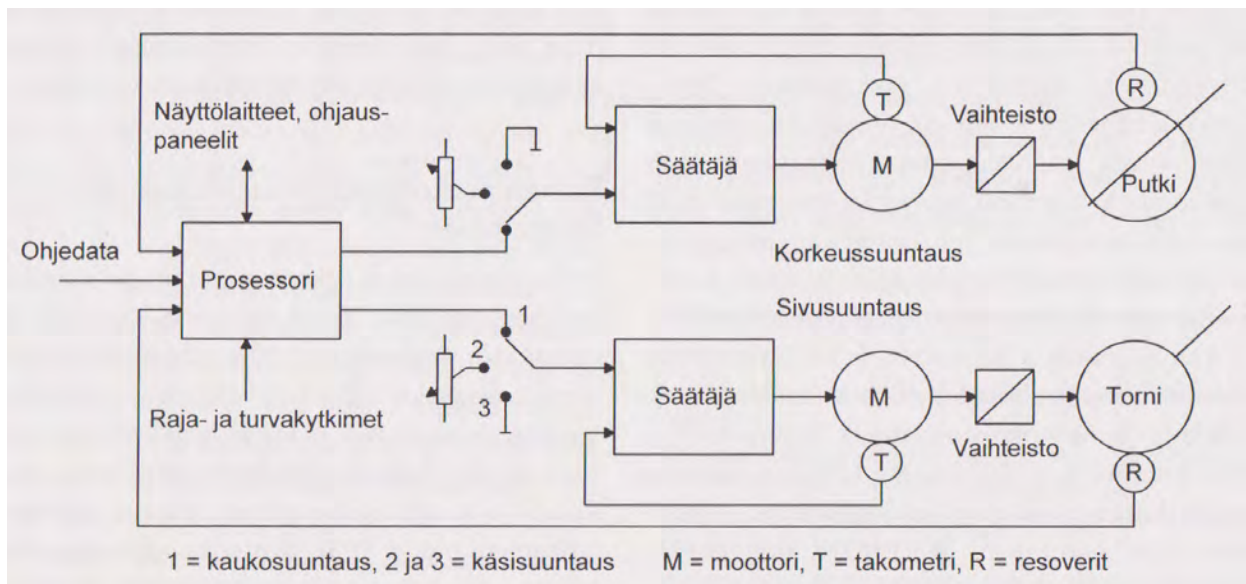
Suunnittelutyön alkuvaiheessa tutkittiin moottorisuuntausta kahden eri vaihtoehdon hydraulikkamoottoreiden ja sähkömoottoreiden välillä. Suuntausmoottoreiksi valittiin tasavirtamoottorit koska jo käytössä olevissa järjestelmissä oli sähkömoottorisuuntaus.

Huollettavuuden arvioitiin olevan teknistaloudellisemmin toteutettavissa niillä vaadituissa käyttö- ja huolto-olosuhteissa.

Hanke oli salainen tai vähintään ETS-luokkaa, joten asioiden hoito oli osin hankalaakin. Kesällä 1976 hankinta ”julkistettiin”, asiasta oli mm. Helsingin sanomissa 7.7.1976 lyhyt uutinen ”Tampellalta tilattu tornitykki”. Ilta-Sanomien julkaisi 15.7.1976 Bisquit kirjoittaman pakinan ”RTYKIN aikaan”. Tykistä ei tullut ihan sellainen kuin pakinnassa värikkäästi kuvailtiin edellisen kesän 1975 ETYK-hengessä.

johdolla) kanssa, Tampella ei osallistunut pyynnöstä huolimatta tähän työhön. Tampella hyväksyi tarkennukset ja lisähintaa tuli vain testausjärjestelmän liittynälle, joka ostettiin erillishankintana.

Alkuvaiheen kangertelujen jälkeen prototyypin suunnittelu ja lopulta valmistuskin alkoi edetä vaiheittain myös suuntausjärjestelmän osalta. Nopeusohjaussilmukka toteutettiin säätäjämoottori-takometriyhdistelmällä, johon ohje-arvo tuli käsisuuntauksessa suuntauslaitteelta (kaksikahvainen joystick, jossa laukaisupainikkeet ja suuntausvarmistimet) ja kaukosuuntauksessa prosessorilta.



Kun alkoi näyttää siltä, ettei prototyyppi tule valmistumaan määräaikaan mennessä ja etteivät sopimuksessa asetetut vaatimukset ole riittävän kattavia tulevia vastaanotto-tarkastuksia ja testauksia silmällä pitäen, päätimme tarkentaa asetettuja vaatimuksia. Laadimme esimieheni insmaj. Martti Korvolan kanssa tarkennetun vaatimusrungon. Se pohjautui PMK 5.2 (pysyväismääräyskokoelma) Hankinnan tekniset vaatimukset 12:ta pääkohtaan. Täsmennettiin mm. käyttäjärajapintoja, dokumentointia ja testausmenettelyä. Määrittely viimeisteltiin yhteistyössä Aseteknillisen osaston, Rannikkotykistöimiston ja Rannikkotykistökoulun (käyttäjävaihtimukset, käyttötestaus kapt. Pertti Malmbergin

**Kuva 1 Suuntausjärjestelmän periaatekaavio** (J Pesonen 2003).

Moottoreissa roottori on valmistettu painopiiriteknikalla, jolloin hitausmomentti on pieni ja siten kiihtyvyyssominaisuudet perinteistä ratkaisua paremmat. Moottoreiden ohjaus – säätäjät – toteutettiin kolmivaiheverkkoon kytkettävillä BBC:n tyristorisuuntaajilla. Sivusuuntausmoottori kääntää tornia planeettavaihteiston välityksellä. Korkeussuuntausmoottorien pyöriä liike muutetaan planeettavaihteiston jälkeen lineaariseksi liikkeeksi, jolla suunnataan putken korotusta.

## Image Soft Oy: suomalaista huippuosaamista vedenalaisen valvonnan kokonaistoimituksiin

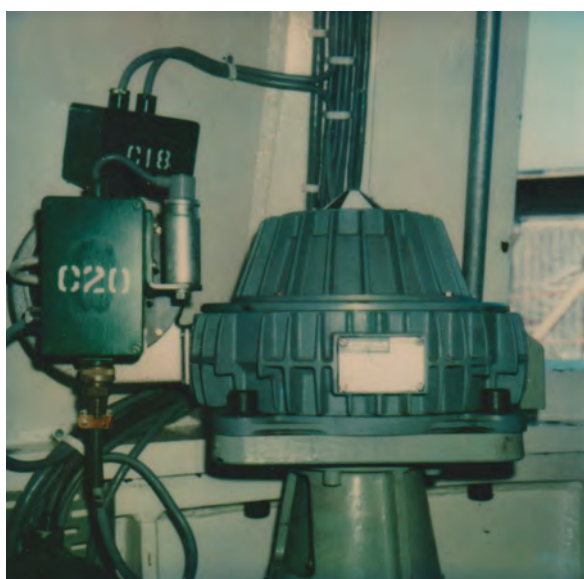
- *Vedenalaisen valvonnan kokonaisjärjestelmät: testattua tarkkuutta vedenalaisten aluksien ja jopa yksittäisten sukeltajien havaitsemiseen.*
- *Operatiivisen toiminnan tueksi koulutussimulaattorit vedenalaiseen valvontaan ja sertifioituun merenkulun opetukseen.*

[www.imagesoft.fi](http://www.imagesoft.fi)



**IMAGE SOFT**  
*Underwater surveillance technology*

**Suunniteltu ja  
valmistettu Suomessa.  
Järjestelmätoimituksia  
maailmanlaajuisesti  
jo vuodesta 1990.**



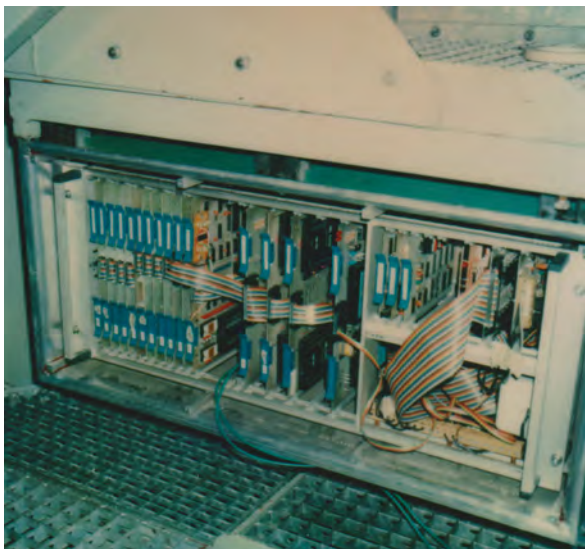
**Kuva 2 Sivusuuntausmoottori tykkiin asennettuna**  
(J Pesonen 1980).

Suuntausjärjestelmän alustavat testaukset suoritettiin koepenissä simuloitusti koska todellista tykkiasemaa kaikkine järjestelmän osineen ei ollut tarkoituksen mukaista ja mahdollista rakentaa tehtaalle. Koepenki oli inskomdri Aaro Wiion (PE Sähkötekniillinen osasto) suunnittelema, se valmistettiin Santahaminan korjaamolla ja lainattiin Tampellalle. Tykin pyörivän osan massa, noin 16 tonnia, mallinnettiin Wiion laskelmien mukaisesti suuntausmoottorin akselille asennetulla teräksestä sorvatulla ”vauhtipyörällä” vaihteiston välityssuhde huomioiden.

Asemaohjaussilmukka toteutettiin prosessori – säätäjä – moottori – vaihteisto –vaihteisto/resolverit-yhdistelmällä. Pääsuuntaustavassa, automaattinen kaukosuuntaus, tykki vastaanottaa ohjeavot, maalin ennakkopisteen sivu- ja korkeussuuntauslukemat piiruina tutka/laskinyhdistelmästä (RAVAL) kaapeliyhteyden (modeemi-) välityksellä. Ohjeavosanomia,

joka sisältää muutakin tykin toimintaa ohjaavaa mm suuntaajien näyttölaitteissa esitettävää tietoa, lähetetään määrätyn välein. Sanomarakenne oli alun perin Nokia suunnittelema RAVALin ja Nokian valmistaman tykkipäätteen välille (käyttö 100 56 TK:ssa). Jonkin verran oli jopa ylemmän tahon kädenvääntöä, että sanomarakenne saatiin myös Tampellan käyttöön. Tykin sivu- ja korkeussuunta (kulmatieto piiruna) mitataan karkea/hienoresolveripareilla (välyksettömät vaihteistot 1:1 ja 1:15) riittävän tarkkuuden ja erottelukyvyn saavuttamiseksi.

Prossessori toteutettiin Motorolan 8-bittisellä mikroprosessoriperheellä. Ohjelmointikielenä oli assembler. Laitteistoon sisältyi mm. emolevy/väylä, keskusyksikkö (CPU), muistit, modeemi, resolveri/digitaalimuuntimet, analogia/digitaalimuuntimet ja muut I/O-yksiköt sekä rinnakkaisliityntä testausta varten.



**Kuva 3** *Prossessori tykkiin asennettuna (J Pesonen 1980).*

Asemaohjaussilmukkaa kehitettiin ja testattiin myös em. koepenissä, johon lisättiin em. prosessori ja vaihteiston välityksellä suuntakulman (asematiedon) mittausta varten resolverit. Koska tutkat/laskimet (RAVAL) sijaitsivat linnakesaarilla, oli ohjausdata lähettäminen tehtaalte testauksia varten puhelinverkonvälityksellä varsin hankalaa 70-luvun tekniikalla. Kehitystyötä tukemaan ja testauksia varten hankimme PC-kautta edeltä-

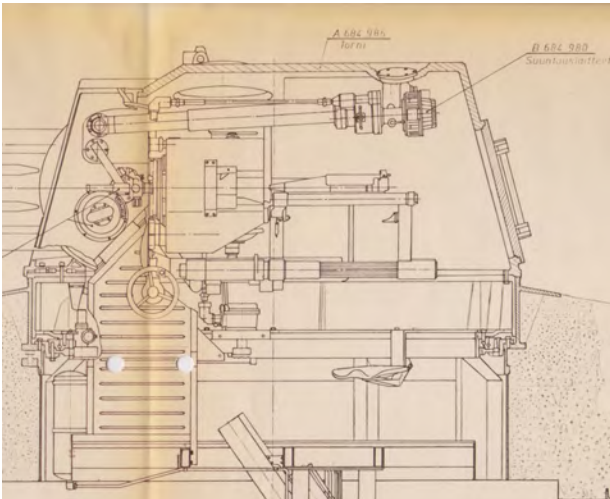
neen HP:n siirrettävän pöytätietokoneen HP9825. Siinä oli 64 merkin rivinäyttö, massamuistina minikasetit ja tulostimena rivikirjoitin. Laitetta täydennettiin sarjaliitynnällä datan lähetystä varten ja rinnakkaisliitynnällä datan lukemiseksi prosessorilta. Wiio opetti oman toimensa ohella säätötekniikkaa TKK:ssa ja teetti tykin servotekniikkaa sivuavan diplomityön. Diplomityön tekijän kanssa, palveli myös erikoisupseerikokelaana, kehitimme pöytätietokoneelle ohjelmiston, jolla voitiin tuottaa ohjearvodataa (RAVAL-sanomaa) ja jonka kaikkia parametreja voitiin ”lennosta” muuttaa. Näin muodostetulla simulaattorilla ohjearvodatan lähettämisen lisäksi voitiin rinnakkaisliitynnällä tallettaa tykin prosessorilta sen vastaanottama ohjearvo ja tykin sivun ja korotuksen oloarvot sekä laskea em. erotukset. Alkuvaiheessa mittausdata tulostettiin tietokoneen paperitulostimella. Myöhemmin hankittiin neliväripiirturi ja testausohjelmistoa kehitettiin erikoisupseeritöinä. Näin toteutettuna testausjärjestelmästä tuli erittäin hyödyllinen väline koko hankkeen, protosta sarjaan, ajaksi säätöparametrien virittämisessä ja testaamisessa. Testauslaitteistoa käytettiin myös sarjalaitteiden loppu-testauksissa ja modernisoituna sellaiset luovutettiin joukko-osastotojen käyttöön huoltovälineeksi.

### **Uutta tekniikkaa - mikroprosessorit**

Mikroprosessorien kehitystahti ja soveltaminen kiihtyi 70-luvun puolivälissä ja tähän saumaan sattui myös prototykin suunnittelu. Mikroprosessoritekniikan opetusta aloitettiin Oulussa siinä vaiheessa, kun olin jo päättämässä opintoja, joten se oli siten myös minulle uutta ja tuntematonta työtehtävääni aloitellessa. Perusteita piti opiskella työn ohessa mm. INSKOn peruskursseilla, maahantuojojen opetustilaisuuksissa sekä ”takapenkkiopiskelijana” Teknillisessä Korkeakoulussa. Asia tuli tutuksi vähitellen myös itseopiskelun kautta. Telmac-mikroprosessorikerhon perustajajäsenenä rakentelin ensimmäisen kotitietokoneen (perustui RCA:n tuoteperheeseen) keväällä 1977. Lahjoitin sen 2015 Tekniikan museolle ja se on esillä Etäunelmia-näyttelyssä. Proto-

hankkeen loppuvaiheessa ja sarjahankintaa aloitellessa hankittiin asennus- testaus- ja kunnossapitohenkilöstölle peruskoulutusta mikroprosessoritekniikkaan mm Ammattien-edistämislaitoksen kursseilla. Järjestimme uuden tekniikan peruskoulutusta myös Sähköteknisellä koululla.

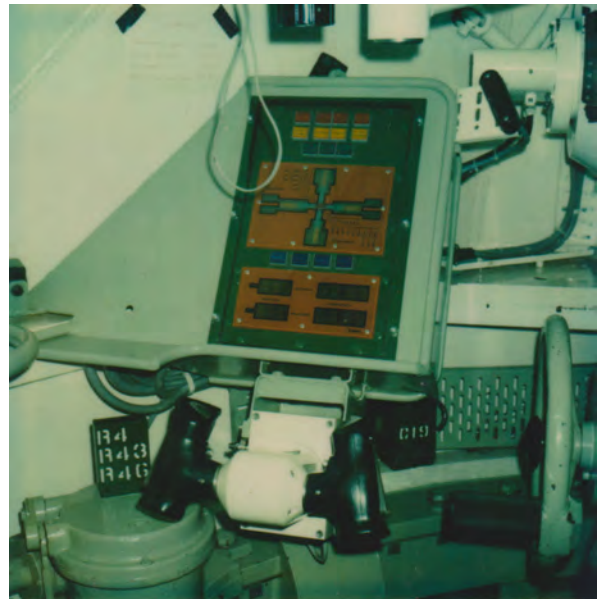
Rannikkotyökistön kalustoon, menetelmiin jne. perehdyttiin mm. ampumaleireillä.



*kuva 4 Tykkitorni korkeussuuntaajan puoli (Tampella 1980)*

### **Prototyypitykin asennus tykkiasemaan, testaukset ja hyväksyminen**

PE Pioneeriosasto rakensi yhteistyössä PLM Rakennusosaston kanssa linnakesaareen kallioon tykkiaseman, jossa oli varusteltuna tilat: tykkipiha, laitehuone ja ammushuone. Tykin sekä suuntausjärjestelmän tehdasvaiheen vastaanottotarkastuksen jälkeen järjestelmä asennettiin tykkiasemaan. Tykkitorniin asennettiin suuntausmoottorit ja anturit, prosessori, ohjaus- ja näyttölaitteet, rajakytkimet jne.



*Kuva 5 Korkeussuuntaajan hallintalaitteet (J Pesonen 1980).*

Tykkiaseman laitettiin asennettiin tyristorisäättäjät, tasavirtakeskus ja akustot jne. Laitetilasta data-, puhelin-, ohjaus- ja muut yhteydet pyörivään tykkitorniin toteutettiin liukurengas-yksikön välityksellä.

Asennusvaihetta seurasivat koko järjestelmän testaukset todellisissa olosuhteissa ja todellisella laitteistokokoonpanolla. Testaukset etenivät toiminnan/käytön turvallisuuteen liittyvistä laitteista (rajakytkimet, rajoittimet, relelogiikka jne.) sähköiseen käsinohjaukseen ja kaukosuuntaukseen. Kaukosuuntauksen toimintoihin liittyen jouduttiin tässä vaiheessa vielä tekemään ohjelmiston kehitystyötä ja säätämään parametreja.

Liikkuvan maalin seurantatarkkuusvaatimukset koko nopeus- ja kiihtyvyyalueella täytyivät hyvin testausten edistyessä. Maalinvaihdot ts. askelmuutokset teettivät eniten työtä, koska asettumisajoissa ja tarkkuuksissa ei välittömästi päästy asetettuihin vaatimuksiin (ylitykset, alitukset, värähtely). Säättöjen ja testauksen alkuvaiheessa käytettiin ohjedataa edellä mainitusta simulaattorista ja testien edetessä todellista RAVALilta tulevaa dataa. Testausmaalina käytettiin mm. hinaajan vetämää maalilauttaa. Koska testauslaitteemme liityntä prosessorilta oli rinnakkaismuotoinen, piti sitä käyttää tornista käsin, mikä hieman

hankaloitti tulosten käsittelyä piirturilla (tykkitornissa ei ollut turhaa tilaa).



**Kuva 6 Testaussimulaattori korkeussuuntaajan istuimella (J Pesonen 1980).**

Edellä kuvattujen monivaiheisten testausten jälkeen käyttöönotto/testaukset jatkuivat kova-panosammunnoilla kaukosuunnattuna erilaisissa tilanteissa. Ammunnoissa liikkuvaan maaliin suuntausjärjestelmä piti tykin suunnassa erittäin hyvin. Suuntausjärjestelmän vastaanottotarkastus ja hyväksyminen suoritettiin kolmessa vaiheessa 29.7. – 12.8.1980 eli muutaman vuoden myöhästyneenä hankintasopimukseen verrattuna.

Linnakesaarella tapahtuneella järjestelmän lopullisella kokoonpanolla oli hyvät ja huonot puolensa. Hyvinä puolina oli mm. todellinen asennus-, testaus- ja käyttöympäristö ja olosuhteet. Huonoina puolina oli mm. ohjelmiston kehitystyön loppuunsaattamisympäristö. Varsinaiset ohjelmiston kehittämis-, kääntämisen jne. välineet olivat tuotantokäytössä Tampereella Tampellan alihankkijalla. 1970-luvun varsin kookkaiden kehityslaitteiden siirtäminen lähes kenttäolosuhteisiin ja käyttäminen siellä ei ollut käytännöllistä. Ohjelmiston korjaus/muutosvaiheita varten piti useita kertoja matkustaa linnake – Tampere väliä mikä aiheutti viivettä toimitukseen. Syysolosuhteiden lähestyessä ja valmistumista nopeuttaaksemme annoimme hieman periksi ja vuokrasimme maahantuojalta kehityslaitteiston linnakkeelle Tampellan käyttöön (käyttöympäristö taisi jäädä kertomatta maahantuojalle).

Hankintasopimuksen kohdassa 9: ”Hankkija (Tampella) asettaa vastaanotossa tarvittavat mittavälineet ja –laitteet sekä tarvittavan apuhenkilöstö veloitusetta tilaajan (Pääesikunta) käyttöön”. Niin kuin edellä kuvailusta käy ilmi niin tässä asiassa joustettiin yhteisen edun nimissä, koska molemmin puolin toimittiin mm. minimi henkilöstöresursseilla ...ja koko ajan opittiin uutta.

### **Sarjahankintaan**

Käyttökokeiden ja hyväksytyjen vastaanotto-tarkastusten jälkeen prototyypitykki esiteltiin hankkeen johtoryhmälle sarjahankintalupaa varten. Ko. tilaisuudessa esitin, että sarjahankintaa varten pitäisi käyttökokemusten pohjalta tarkentaa suuntausjärjestelmän teknisiä vaatimuksia. Tähän eräs johtoryhmän jäsen totesi ”mihin sellaista tarvitaan, ostetaan toimivia tykkejä”. Sarjahankintalupa saatiin, tarkennettiin hieman teknisiä vaatimuksia. Kaikkien yllätykseksi Tampella tarjosi vain varsinaisen tykkien valmistuksen ja vetäytyi toistaiseksi tarjoamasta suuntausjärjestelmää. Koska kokonaisuutelle oli asetettu tavoite-aikataulut, päädyttiin ratkaisuun: suuntausjärjestelmän teknisiä vaatimuksia vielä tarkennettiin ja 1981 tarjouspyynnöt lähetettiin useampaan yritykseen. Tarjousten perusteella suuntausjärjestelmän toimittajaksi valittiin Altim Control Ky (myöhemmin Ahlström Automation) Varkaudesta.

### **Toinen prototyyppi**

Tässä vaiheessa oltiin uudessa tilanteessa hankinnan kannalta, koska kukin yritys tarjosi omaa tekniikkaansa suuntausjärjestelmän toteutukseen, niin myös Altim Control. Eli aloitettiin toisen prototyypivaiheen suunnittelu ja toteutus sekä yhteistyössä säännölliset katselmuskokoukset. Linnakesaarikokemusten perusteella oli päätetty purkaa prototyypitykki ja asentaa se mantereen puolelle. Rannikkotykkikoulun yhteyteen, 100 56 TK-koulutusaseman viereen, rakennettiin täydellinen tykkiasema, johon prototyyppi siirrettiin.



**Kuva 7 koulutustykkiasema** (J Pesonen 2012).

Ensimmäisen prototyypin suuntausjärjestelmä, pl. suuntausmoottorit ja anturit vaihteistoinen, purettiin ja romutettiin. Tykkiaseman tarkoituksena oli toimia toisen protovaiheen testauspaikkana ja jatkossa Rannikkotykkistökoulun koulutustykkinä.

Toisessa prototyypivaiheessa suuntausmoottorit, anturit, liukurengasyksikkö samoin kuin raja- ja turvakytkinratkaisut säilyivät ennallaan. Samoin säilyivät hallinta- ja valvontalaitteiden periaateratkaisut ennallaan, toteutettuna 4 ... 6 vuotta uudemmalla tekniikalla. Koulutustykki- asemassa tehtyjen testausten perusteella tyristorisäätäjiksi valittiin kotimaisen valmistajan, Intertrafo Oy:n, laitteet. Prosessori, moniprosessorijärjestelmänä, toteutettiin Altimin teollisuusautomaation tuoteperheellä (toteutus Intel 8086/80186 16-bittisellä mikroprosessoriperheellä) sovellettuna vaativampiin ympäristöolosuhteisiin. Uusina I/O-tuotteina suunniteltiin mm. resolveri/digitaali- ja digitaali/analogiamuunnin- ja modeemikortit. Testausliityntä toteutettiin nyt sarjaliitynnällä, joten simulaattoriamme voitiin käyttää laitetilasta käsin. Ensimmäisessä prototyypissä ollut relelogiikka toteutettiin ohjelmallisesti.

Tehdasvaiheen tuotekehitys ja viritys toteutettiin pääosin simuloituna, lainaamalla laitteistolla, kuten ensimmäisessäkin prototyypissä. Tehdastarkastusten jälkeen suuntausjärjestelmä asennettiin 1983 koulutustykkiin ja aloitettiin sen lopullinen testaus sekä säätöparametrien viritys. Viritys/parametrien säätö tehtiin ensisijaisesti simulaattoriamme käyttäen. Niin kuin ensimmäisessä protovaiheessa

myös tässäkin vaiheessa maalinvaihdot (eli askelmuutokset) olivat ongelmallisempia. Askelmuutosten säätömenetelmäksi valittiin adaptiivinen säätö, missä parametrit valitaan automaattisesti askeleen suuruuden mukaan. Näin saatiin sopiva kiihdytys ja hidastus, ei syntynyt ylityksiä ja alituksia eikä ryömintää. Vasteaika ja seurantarkkuus täyttivät asetetut vaatimukset ja voitiin aloittaa testaukset todellisilla, RAVALin lähettämällä, ampumarvoilla. Aivan vieressä Rannikkotykkistökoululla oli RAVAL-laitteisto, jonka asiantuntijaksi oli PE Sähkötekniliseltä osastolta siirtynyt DI Pentti Ylinen. Suuntauslaitteiston pääsuunnittelijana ja testaajana toimi PE Sähkötekniliseltä osastolta Altimille siirtynyt DI Aimo Hakulinen. Yhteistyö oli saumatonta, kun selviteltiin ja ratkaistiin muutamia RAVAL-datan ongelmia.

Asiointi asennus-, testaus- ja koekäyttö- vaiheessa mantereella sijaitsevaan tykki- asemaan oli huomattavasti helpompaa kuin linnakesaarelle. Koska myös Altimin ohjelmiston olivat tuotantokäytössä Varkaudessa, tykkiasemassa testatut viritysparametri- ja ohjelmistokorjausdata siirrettiin kehittyneempien puhelinyhteyksien myötä modeemiyhteydellä tehtaalle. Korjatut ohjelmistopakettit siirrettiin tehtaalta tykille modeemiyhteydellä ja poltettiin asennuspaikalla prosessorin muistikorteille (EPROM). Kovapanosammuntoja lukuun ottamatta kaikki muu toiminnallinen testaus voitiin suorittaa koulutustykissä. Tämän kakkosproton hyväksytyn vastaanottotarkastuksen jälkeen voitiin aloittaa sarjavalmistus. Vastaanottotarkastukset suoritettiin tehtaalla siltä osin kuin oli mahdollista ennen tykkeihin asentamista.

### **Sarjalaitteasennukset**

Myös varsinaisten tornitykkien valmistus oli käynnistynyt Tampellassa. Kävin siellä suorittamassa vastaanottotarkastukset tykkien ja suuntausjärjestelmän rajapintaosuuksiin. Myös tykkiasemien rakentaminen linnakesaariin oli käynnistetty.

Kun ensimmäinen sarjatykki valmistajien tuke- mana suuntausjärjestelmiseen oli asennettu,

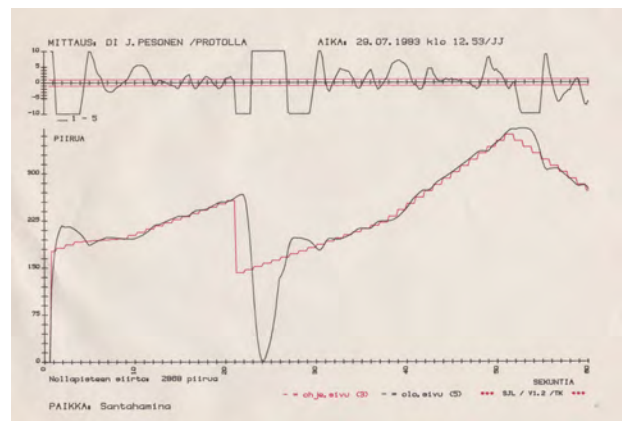
testattu ja koeammuttu linnakesaaren tykkiasemassa, jatkettiin muiden tykkien asentamista. Tykkien ja suuntauslaitteiden asentamisen, testaamisen, koeammunnat ja luovuttamisen joukko-osastoille suorittivat Pääesikunnan ja Asevarikon asennusryhmät vahvennettuna kunkin joukko-osaston henkilöstöllä. Suuntauslaiteryhmään kuului PESähkö-osaston teknikko, AseV5:n teknikko ja asentaja sekä ao. joukko-osaston asesähköteknikko. Tehdasvastaanottotarkastusten ohella osallistuivat kunkin tykin asennusten loppu-testaukseen ja luovutukseen joukko-osastoille. Niin proto- kuin sarjavaiheen testit ja käyttöönotot etenivät turvallisesti muutamaa läheltä piti -tapausta lukuun ottamatta. Prototyypivaiheen ja ensimmäisen linnakkeen asennusten ajaksi työryhmille oli varattu huoneisto henkilökunnan asunnoista. Seuraavilla linnakkeilla asuntolina olivat talviaikaan jokseenkin ankeat työmaaparikit, niinpä tehtiin pitkää työpäivää oleskeluajan lyhentämiseksi. Kelirikkoaikaan matkustamien asennustyömaille oli aikaa vievää. Ensimmäisen hankinatavaiheen viimeisen patterin luovutukseen meidät kuljettiin helikopterilla. Asennusten jälkeen käyttö- ja huoltokoulutus toteutettiin Rannikkotyökistökoululla. Tykkihankkeen tehtävien vähetessä siirryin 1986 esimieheni insev. Max Nybeghin ohjaamana tekniseksi asianhoitajaksi ilmatorjunnan johtamisjärjestelmä-, asemodernisointi- ja simulaattorihankkeisiin. Tuleviin rannikkotyökistöhankkeisiin palkattiin DI Johnny Heikell.

Työnjako, jossa Tampella Oy valmisti tykit ja Altim Control ky suuntausjärjestelmät, osoittautui alkukangertelujen jälkeen onnistuneeksi ratkaisuksi. Proto – ja sarjavaiheessa kaikki osapuolet perehtyivät käytännön kautta mm. tekniseen asianhoitoon, vaatimustenhallintaan, testaukseen ja tarkastuksiin. Varsinaista koulutusta ei ollut vielä saatavilla em. asioihin. 90-luvun alkupuolella pääinsinöörin asettama työryhmä uusi vaatimustenhallintaohjeistuksen (entinen PMK 5.2) ja aloitti koulutuksen vuosikymmen puolivälissä. Hieman raskaaksi muodostunut

ohjeistus uusittiin sitten useampaan kertaan Jyri Kosolan toimesta.

## Lopuksi

Prototyypin ja ensimmäisen linnakkeen patterin käyttöönottovaiheissa sekä koulutustykkiasemassa kävi paljon tutustujia, uusi asejärjestelmä ja tekniikka kiinnostivat. Yhtenä esittelymuotona vierailija sai suunnata tykkiä sähköisellä käsisuuntauksella seuraamalla simulaattorin lähettämän ohjearvon ja tykin oloarvon erotusta suuntaajan näyttölaiteella sekä pitämällä erotuksen minimissään. Suoritteestaan vierailija sai sitten piirtutulosteen.



**Kuva 8 Suuntausharjoittelua (J Pesonen 1983), oma varsin kehno suoritukseni, tasaisesti liikkuva maali ja yksi maalinvaihto sekä suunnanmuutos.**

Kun Aaro Wiio ehdotti 2003 minulle että kirjoittaisin jutun tykin suuntausjärjestelmästä Suomen Automaatioseura ry:n kirjaan ”Teollisuusautomaation vuosikymmeniltä osa 2”, Rannikkotyökistöimiston ohjaus oli ”kirjoita kohteliaasti”. Olivathan hankkeen eri vaiheet ajoittain aika ”värikkäitäkin”. Noudatin samaani ohjetta ja Rannikkotyökistöimisto tarkasti käsikirjoituksen ennen julkaisemista. Tämä tarina perustuu kirjoittamiini em. kirjan ja Rannikon Puolustaja-lehden 2/2005 artikkeleihin hieman laajennettuna.

100 56 TK-tornitykit on purettu ja romutettu, 130 TK lienee edelleen käytössä. Viimeksi olen vierailut linnakesaaren 130 TK:lla vuonna 1988.



## Insinööriupseeriliitto ry:n hallitus 2020



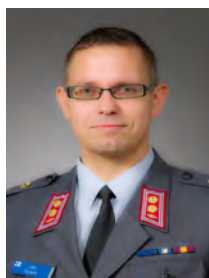
Puheenjohtaja  
Insinöörieversti  
**Jyri Kosola**  
0299 510 504  
[jyri.kosola@mil.fi](mailto:jyri.kosola@mil.fi)



Insinööriylliluutnantti res  
**Hannu Saarikangas**  
0400 838 008  
[<hannu.h.saarikangas@gmail.com>](mailto:hannu.h.saarikangas@gmail.com)



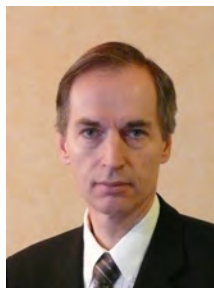
Varapuheenjohtaja  
Insinöörikommentajakapteeni  
**Mikael Kaskelo**  
työ 0299 578 623  
koti 040 522 2840  
[kaskelo01@gmail.com](mailto:kaskelo01@gmail.com)



Insinöörieverstiluutnantti  
**Tero Solante**  
0299 510 602  
[tero.solante@mil.fi](mailto:tero.solante@mil.fi)



Taloudenhoitaja, sihteeri  
insinöörieverstiluutnantti  
evp  
**Eino Laiho**  
0400 933 837  
[eino.laiho@kotikone.fi](mailto:eino.laiho@kotikone.fi)



Diplomi-insinööri  
**Harri Tilvis**  
0299 577 114  
[harri.tilvis@pp.inet.fi](mailto:harri.tilvis@pp.inet.fi)



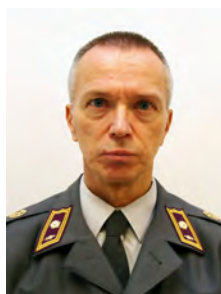
Varainhankinta  
Insinöörikommentajakapteeni  
evp  
**Raimo Kaipiainen**  
050 4343 308  
[raimo.k.kaipiainen@gmail.com](mailto:raimo.k.kaipiainen@gmail.com)



Insinöörikommentaja  
**Jari Vainio**  
0299 341 730  
[jari.vainio@mil.fi](mailto:jari.vainio@mil.fi)



Insinöörieverstiluutnantti  
**Jouni Koivisto**  
0299 550 120  
[jouni.koivisto@mil.fi](mailto:jouni.koivisto@mil.fi)



Insinöörimajuri  
**Jari Viuhon**  
0299 578 430  
[jari.viuhon@mil.fi](mailto:jari.viuhon@mil.fi)



**INSINÖÖRIUPSEERILIITTO ry JÄSENYYSKEMUS** **OSOITEMUUTOS** **VARSINANEN JÄSEN**c/o ~~Mikael~~ Kaskelo Särkän rantatie 4 as 4 21160 Merimasku **KANNATTAJAJÄSEN**

Sukunimi		Etunimet (kutsumanimi alleviivattuna)		
Postinumero	Pos titoimipaikka	Lähiosoite		
Saako jäsentiedotteet tulla vain sähköpostilla? (lu-lehti tulee kantopostina)		Sähköpostiosite		
Sotilasarvo		Ylennysvuosi	Syntymäaika	
Palvelu Puolustusvoimissa		( aika / joukko-osasto, vast / tehtävä )		
Sotilaskoulutus (vuosi)				
RUK	POI / PK / KadK	Erikupsk	Insupsk	SOJO-kurssi
YPK	YE-kurssi	YJK		
Siviilitutkinnot	( loppututkinto / opinto suunta / vuosi )		(mainittava tekninen tai matemaattis-luonnontiet.)	
Siviilityöpaikka				
Päiväys		Allekirjoitus		

**IUL ei anna yllämainittuja tietoja ilman asianomaisen lupaa IUL:n ulkopuolisiin tarkoituksiin.**

