INSINÖÖRIUPSEERILIITTO RY

Insinööriupseeri 2022

Insinööriupseeri 2022

Insinööriupseeriliitto ry

Tässä lehdessä:

Insinööriupseeriliitto ry

PL 919, 00131 Helsinki

ISSN-L 1798-3622 ISSN 1798-3622

Offset Ulonen Oy, Tampere 2023

Päätoimittajan mietteitä

- Insinöörieversti Jyri Kosola

Vuosi 2022 on ollut monilla tavoin poikkeuksellinen. Naapurimme Venäjä aloitti sodan Euroopassa hyökkäämällä Ukrainaan. Sota koskee suoraan tai välillisesti kaikkia eurooppalaisia maita. Sota lopetti NATO-option hokemisen traditiomme. Naapuri ajoi pohjoiset pikkukansat hakemaan turvaa sieltä mistä sitä on saatavissa; läntisestä arvoyhteisöstä, joka on valmis tarvittaessa asein puolustamaan jäsentensä oikeutta demokratiaan ja ihmisoikeuksiin.

Poikkeuksellista on ollut myös sodasta ja NATO-liittoutumispäätöksestä aiheutunut ylimääräinen työkuorma. Se näkyy kiireenä, toissijaisten asioiden viivästymisinä sekä pitkinä työpäivinä etenkin esikunnissa.

Toisaalta, jos asioita katsoo laajemmasta perspektiivistä, asiat eivät taida olla kovinkaan poikkeuksellisella tolalla. Venäjä on jo pitkän aikaa toiminut johdonmukaisesti kohti sysimustia tavoitteitaan. Entisen KGB-upseerin johdolla demokratia lakkautettiin ja tilalle pystytettiin diktatuureille välttämätön henkilökultti jo vuosikausia sitten. Oppositio murskattiin ja naapurimaihin hyökättiin. Sodasta länsimaiden kanssa puhuttiin, samoin oikeutuksesta sanella pienten naapureiden asioita. Narratiivin taustalla ollut valhe oli niin suuri ja toimien perustana oleva arvopohja niin absurdi, ettei sitä tavallinen Paavo tai Angela edes nähnyt. Ei sen paremmin kuin eräs Neville aikoinaan.

Venäjän hyökkäys Ukrainaan pudotti naamiot. Huomattiin, että Venäjä ei ole "ohjattu demokratia", vaan ihan oikea diktatuuri, jossa tehdään mitä elinikäinen presidentti sanoo. Huomattiin myös, että *el presidente* oli sanonut kaikenlaista. Tai paremminkin vasta nyt uskottiin tämän tarkoittaneen mitä puhui. Huomattiin myös, että hyökkäys Ukrainaan oli alkanut jo vuosia aiemmin, ja että Georgiaankin oli taidettu hyökätä. Kaikki tämä samaan aikaan kun lännessä rakennettiin energiariippuvuutta aggressiiviseen diktatuuriin.

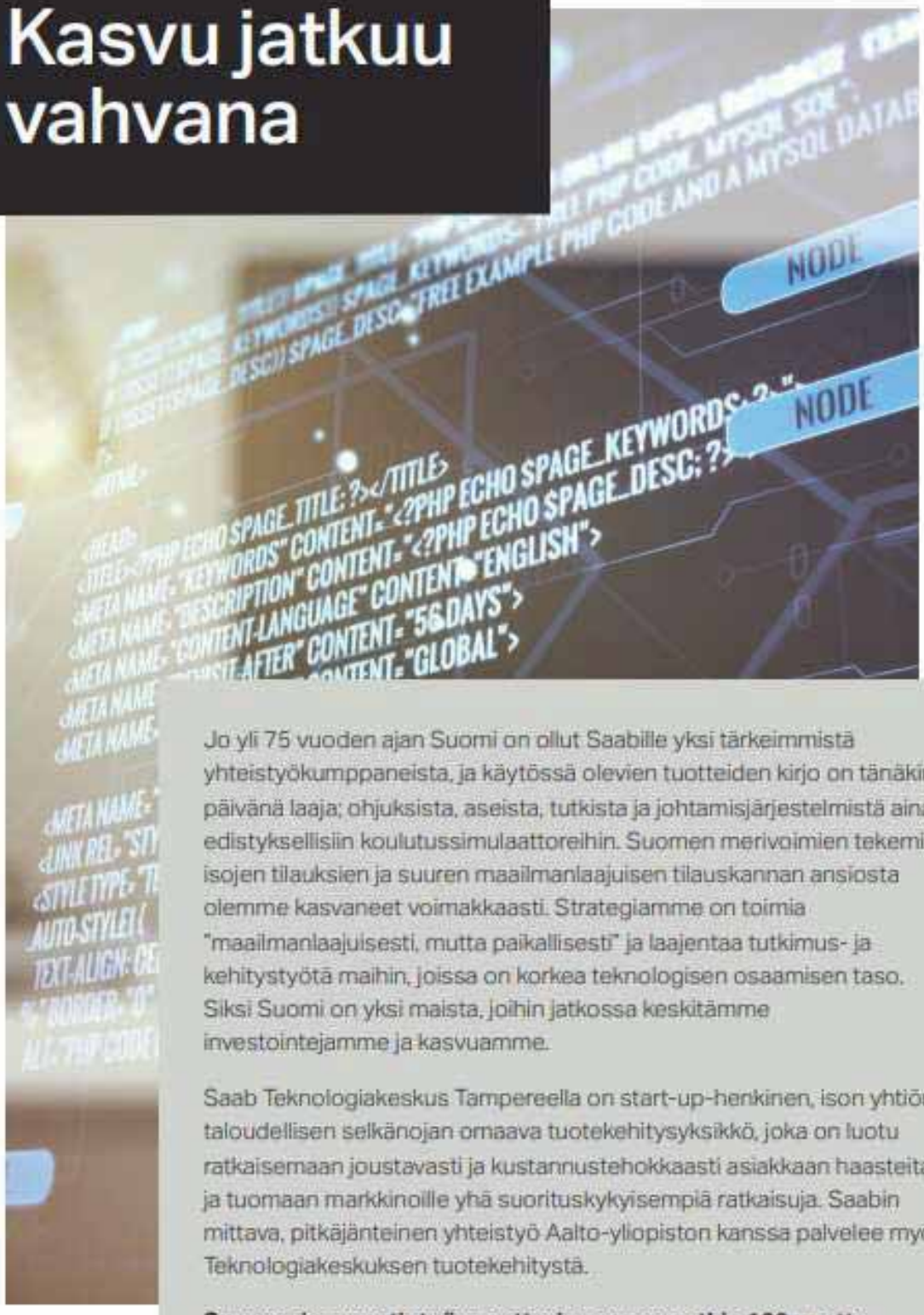
Venäjän brutaali hyökkäys lopetti löysät puheet NATO-optiosta ja EU-puolustuksesta. Kansallinen turvallisuus ei saisi perustua absurdiin ajatukseen ottaa palovakuutus vasta kun naapurustoa terrorisoinut pyromaanin on jo sytyttänyt nurkan palamaan. Samoin ei tainnut olla älyllisesti kovin rehellistä puhua EU-puolustuksesta todellisena vaihtoehtona NATO:lle. EU on kuitenkin osoittanut voimansa ja tärkeytensä Suomelle poliittisena ja taloudellisena toimijana. Se on lopettanut löysät puheet unionista eroamisesta. Suomalaisetkin ovat vihdoin ymmärtäneet, että parhaiten olemme turvassa sekä EUn, että NATOn jäseninä.

Tämän lehden teemana on sodankäynnin monet ulottuvuudet. Ikävä kyllä, sota seuraa sotaisaa ihmiskuntaa kaikkialle minne se meneekin. Siten ihmiselämän leviäminen uusiin toimintaympäristöihin tuo sodankäyntiin uusia ulottuvuuksia. Tämä asettaa laajenevia vaatimuksia Puolustusvoimien tekniselle osaamiselle ja tietysti sen keskeiselle tekijälle, insinööriupseeristolle.

Taistelumieltä!

Jyri Kosola

Kasvu jatkuu vahvana



Jo yli 75 vuoden ajan Suomi on ollut Saabille yksi tärkeimmistä yhteistyökumppaneista, ja käytössä olevien tuotteiden kirjo on tänäkin päivänä laaja; ohjuksista, aseista, tutkista ja johtamisjärjestelmistä aina edistyksellisiin koulutussimulaattoreihin. Suomen merivoimien tekemien isojen tilauksien ja suuren maailmanlaajuisen tilauskannan ansiosta olemme kasvaneet voimakkaasti. Strategiamme on toimia "maailmanlaajuisesti, mutta paikallisesti" ja laajentaa tutkimus- ja kehitystyötä maihin, joissa on korkea teknologisen osaamisen taso. Siksi Suomi on yksi maista, joihin jatkossa keskitämme investointejamme ja kasvuamme.

Saab Teknologiakeskus Tampereella on start-up-henkinen, ison yhtiön taloudellisen selkänojan omaava tuotekehitysyksikkö, joka on luotu ratkaisemaan joustavasti ja kustannustehokkaasti asiakkaan haasteita ja tuomaan markkinoille yhä suorituskykyisempiä ratkaisuja. Saabin mittava, pitkäjänteinen yhteistyö Aalto-yliopiston kanssa palvelee myös Teknologiakeskuksen tuotekehitystä.

Suomen innovaatiotyön roottorina seuraavatkin 100 vuotta.

Lue lisää osoitteessa www.saab.fi.

SAAB

Puheenjohtajan terveisiä

- Insinöörieverstiluutnantti Tero Solante -

Juuri, kun ajateltiin, että kaksi vuotta kestänyt korona-pandemia alkaa hellittämään ja voidaan siirtyä normaaliin päivärytmiin, niin kaikki muut turvallisuusympäristön premissit muuttuivat. Venäjä hyökkäsi Ukrainaan ja sota alkoi Euroopassa ensimmäisen kerran lähes sataan vuoteen. Tämä tarkoitti uutta aikaa ja uudenlaista ajateltavaa niin kaikille kansalaisille kuin myös turvallisuusviranomaisille. Uusia haasteita tilanne aiheutti erityisesti Puolustusvoimille, joka käynnisti erillisellä lisärahoituksella nopean suorituskykyjen täydennysoperaation. Yleinen turvallisuustilanteen muutos osoitti, että Puolustusvoimat on halutessaan hyvinkin ketterä organisaatio, joka kykenee toimeenpanemaan suuren mittaluokan suunnittelu- ja hankintatehtäviä nopeastikin. Tästä iso kiitos kuuluukin Puolustusvoimien materiaalisen suorituskyvyn parissa työskenteleville järjestelmäinsinööreille, projektipäälliköille ja muulle henkilöstölle.

Samalla, kun toteutettiin täydennyshankintoja niin valtion johto alkoi valmistelemaan Suomen liittymistä NATO:oon. Liittymispäätös toteutettiin ennätyksellisessä ajassa, jonka mahdollisti kansalaisten mielipiteiden muutos. Ennen Ukrainan sotaa hieman alla puolet kannatti liittoutumista. Mutta sodan alkamisen jälkeen enemmistön mielipide muuttui liittoutumista kannattavaksi, jonka seurauksena Suomi päätti lähettää jäsenanomuksen. Tämä johti työmäärän lisääntymiseen liittoutumisen valmisteluun tähtäävien työtehtävien myötä. Tällä hetkellä valmistelut ovat kiivaimmillaan. Vaikka yleisesti puhutaankin, että Suomi on jo NATO-yhteensopiva, niin paljon on vielä tekemistä jäljellä aina teknisistä ratkaisuista laki-muutoksiin asti. Puolustusvoimat ei onneksi ole tämän haasteen edessä yksin vaan tämä on koko valtiohallinnon yhteinen urakka. Joka tapauksessa teknisen yhteensopivuuden saavuttaminen edellyttää jälleen kerran Puolustusvoimissa palvelevien insinöörien työpanosta. Juuri kun täydennyshankinnat oli saatu valmisteltua, niin työkuorma kasvoi uusilla haasteilla. Onneksi insinöörikunnan osaaminen ja maanpuolustustahto on kovaa. Tästäkin urakasta tullaan selviämään kunnialla.

Viime vuonna tähän aikaan esittelimme jäsenistölle uusia ajatuksia yhdistyksen strategiamuutoksesta ja digitalisaation käyttöönotosta. Näin vuoden jälkeen on helppo todeta, että muutos on käynnistynyt pienin askelin ja digitalisaation keinoja on otettu onnistuneesti käyttöön. Paljon on työtä vielä kuitenkin tehtävänä ennen kuin voidaan sanoa, että tavoitteet on saavutettu. Toisaalta yhdistyksellä ei ole tässä mikään pakottava kiire, vaan pienin askelin on hyvä edetä.

Osana strategiamuutosta ideoitiin mahdollisuus järjestää jäsenistöä kiinnostavia webinaareja ja seminaareja. Tähän osatekijään onkin tartuttu pontevasti ja IUL tulee osallistumaan Puolustus-, ilmailu- ja

avaruusyhdistyksen (PIA) järjestämään SecD-seminaariin 8.-9.2.2023. Kyseinen tilaisuus on ensimmäinen Suomessa järjestettävä kansainvälinen turvallisuus- ja puolustusteknologian seminaari. Tilaisuus on avoin ja ilmainen kaikille viranomaisille. Tämän lisäksi IUL saa yhteistyöstä palkkioksi maksuttomia osallistumisoikeuksia niille henkilöille, jotka ovat esimerkiksi jo eläköityneet työelämästä. Toivottavasti mahdollisimman moni virkatehtävissä oleva insinööri käyttää mahdollisuuden hyväkseen ja osallistuu seminaariin.

Tuleva vuosi tulee olemaan itselleni kolmas vuosi IUL:n puheenjohtajana. Kiitos vielä kerran kaikille luottamuksesta. Kunhan SecD-seminaarista selvitään kunnialla, meidän on aika siirtää katsetta yhdistyksen 100-vuotiaan olemassa olon juhlimiseen. Tämä tulee tarkoittamaan ainakin vuosijuhlan järjestämistä sekä mahdollisen historiikin laatimista. Molempien toteuttaminen on syytä aloittaa ajoissa, jotta niistä saadaan yhdistyksemme arvoisia.

Toivon kaikille jäsenille kaikkea hyvää tulevana vuotena. Tekemistä tulee olemaan mm. NATO-liittymisen valmistelun vuoksi enemmän kuin ehditään säällisesti tekemään, jolloin on syytä pitää omasta sekä perheen hyvinvoinnista huolta. Ketju on juuri niin vahva kuin sen heikoin lenkki. Tämän vuoksi haastankin kaikki jäsenet pitämään oman lenkkinsä vahvana!

Tero Solante

Sodan monet ulottuvuudet

- Insinöörieversti Jyri Kosola -

Keskustelua siitä, mitkä ovat tunnistettuja ja tunnustettuja sotilaallisia toimintaympäristöjä, on helppo pitää akateemisena saivarteluna. On kuitenkin huomattava, että asevoimat organisoituvat ja kehittävät sekä operoivat suorituskykyjään toimintaympäristöittäin. Siten toimintaympäristöjen määrittely osaltaan määrittelee sen millaiset suorituskyvyt ja konseptit ovat mahdollisia. Jos toiminta-ympäristöä ei ole tunnistettu, siihen liittyviä investointeja ei koordinoida, suorituskyky-vaatimuksia harmonisoida, yhtenäistä doktriinia laadita ja niin edelleen. Tämän lehden teemana on esitellä sodan eri ulottu-vuuksia, sekä nykyisiä että tulevia.

Maatoimintaympäristön määrittää kiviplaneet-tamme pintakerros, merellisen ympäristön nestemolekyyli, ilmaympäristön kaasuseos, avaruusympäristön tyhjö ja kyberympäristön ihmisen luoma binäärimaailma. Sähkömag-neettisen toimintaympäristön määrittää keske-nään vuorovaikutuksessa oleva sähkö- ja mag-neettikenttien energiasäteily. Kyberympäristö on ainoa, jonka olemassaolo riippuu ihmisestä: sen voi ainakin teoriassa sammuttaa.

Toimintaympäristöt ovat erilaisia, joten sotilasoperaatiot niissä ovat luonteeltaan erilaisia vaatien erilaista toimintaa ja varustusta, henkilöstöä ja koulutusta. Tämä on huomioitu jakamalla asevoimat puolustus-haaroihin sitä mukaa kuin toiminta levisi uusiin toimintaympäristöihin.

Ihmiskunta on sotinut maalla koko olemassaolonsa ajan. Ensimmäinen tunnettu meritaistelu lienee tapahtunut 3200 vuotta sitten, jolloin heettiläiset löivät kyproslaisten laivaston. Sähkömagneettisesta spektristä tuli uusi toimintaympäristö, kun radiota ryhdyttiin hyödyntämään sodankäynnissä 1900-luvun alussa. Ilmaan sota levittäytyi 1910-luvun alussa, kun ilmaa raskaampia lentolaitteita ryhdyttiin käyttämään laivaston ja tykistön tähystykseen. Avaruus tuli mukaan 1941, kun saksalaiset laukaisivat menestyksekkäästi ensimmäisen ballistisen V2-ohjuksen. Tietokoneiden yleistyminen ja verkottuminen laajensivat sodankäynnin kyberavaruuteen 1980-luvun puolivälin jälkeen.

Teknologisen kehityksen myötä asevoimiin on syntynyt uusia puolustushaaroja: merivoimat, ilmavoimat ja avaruusvoimat. Kyber-puolustushaaran perustaminen on ainakin puheiden tasolla esillä monessa maassa. Sähkömagneettinen spektri tuskin edellyttää omaa puolustushaaraa, mutta oman kokonaisuutena hallitun toimintaympäristön tunnustamisesta olisi operatiivisia etuja.

Ympäristöt ovat keskenään niin erilaisia, että toimintaperiaatteet ja toiminnan rajat määräytyvät eri parametreista. Maaympäristöä kuvaavat esimerkiksi ihmisten läsnäolo, suuret vaihtelut säässä ja maastossa, liikkeen suhteellinen hitaus ja riippuvuus maastosta sekä operaatioiden pitkä kesto. Ilmaympäristöä kuvaavat nopeus, kantama ja vastustajan havaitseminen kaukaa. Meriympäristö on näiden välimuoto. Kyberympäristö on virtuaalinen, binaarinen, globaali ja toimii ”koneen nopeudella”. Sähkömagneettinen toimintaympäristö määrittyy valonnopeudella etenevän energian kautta.

On huomattava, että kyberavaruus ja sähkömagneettinen spektri ovat hyvin erilaisia. Kyberulottuvuus on ihmisen luoma digitaalinen pelikenttä, jossa pätevät ihmisen teknologiavalintojen määrittämät pelisäännöt. Sähkömagneettinen spektri taas on analoginen toimintaympäristö, jossa luonnonlait määrittävät pelin säännöt. Myös kamppailun syvin olemus näissä ympäristöissä on erilainen: kyberympäristössä kaksi binäärikoodia kisaa viekkaudesta, spektrissä kyse on energian kaksintaistelusta.

Teknologioiden ja yhteiskuntien kehittyessä sodankäynti levittäytyy uusiin ulottuvuuksiin, mutta mikään vanha ulottuvuus ei jää tarpeettomaksi. Siksi sodankäynti monimutkaistuu koko ajan. Seuraavissa artikkeleissa käydään läpi tätä kompleksista kokonaisuutta eri toimintaympäristöjen näkökulmasta.

Sotaa maalla

- Everstiluutnantti Janne Mäkitalo -

Janne Mäkitalo (s. 1967), on yleisesikunta-eversti ja Maasotakoulun johtaja. Mäkitalo on väitellyt Maanpuolustuskorkeakoulussa sotatieteiden tohtoriksi vuonna 2012, aiheenaan Partisaanisodasta alueelliseen puolustusjärjestelmään – Jugoslavialaisen sotataidollisen ajattelun kehittyminen toisen maailmansodan jälkeen. Hänet nimitettiin operaatiotaidon ja taktiikan dosentiksi vuonna 2016, opetusalanaan maavoimien taistelu. Mäkitalo palveli yleisen sotataidon (operaatiotaito ja taktiikka) sotilasprofessorina vuonna 2017 ja suomalaisen sotataidon (operaatiotaito ja taktiikka) sotilasprofessorina vuosina 2018–2022.

Maasodankäynti murroksessa?

Operaatiotaidon ja taktiikan kehittäjät ja sotilaallisten suorituskykyjen rakentajat ympäri Eurooppaa seuraavat silmä tarkkana Venäjän Ukrainaa vastaan aloittaman oikeudettoman hyökkäyssodan vaiheita ja yksityiskohtia. Sotilasasioiden vallankumousta (Revolution in Military Affairs, RMA) jo kolme vuosikymmentä povanneet ennustelijat näyttävät joutuvan jälleen pettymään. Miehittämättömien ilma-alusten ja ohjuspuolustuksen puolestapuhujat saattavat tehdä liian rohkeita tulkintoja, koska ukrainalaisten saavuttamista menestyksistä kertova lähdeaineisto ei ole vielä riittävän kattavaa ja monipuolista. Russologit ympäri maailmaa ovat hämmentyneitä aiemmista arvioinneistaan, kun ovat nyt jo kohta vuoden päässeet seuraamaan ylivertaisena pitämänsä ”punakoneen” sotilaallista alisuoriutumista. Suomalainen sotataidon tutkija ja opettaja Joose Hannula varoitti jo vuonna 1930, että oman aikakauden sotien tutkimiseen rajoittuvat teoreetikot ovat miltei säännöllisesti langenneet kaavamaisuuteen, tietyissä olosuhteissa toimineiden ratkaisujen yleistämiseen, pyrkien etsimään sotataidon ”viisasten kiveä”. Millaisia skenaarioita tulevaisuuden maasodankäynnin kehitysvaihtoehdoiksi Ukrainan sodasta tehtyjen havaintojen perusteella on muodostettavissa?

Ukrainan sodan vaikutus

Sodankäynnillä on taipumus kehittyä siten, että vaikka menestyneitä konsepteja kopioidaan, ase-vasta-ase -kilpajuoksun kaltainen liike varsin usein tavallaan neutralisoi niiden käyttöönottamisen tuoman suorituskykylisän. Sama konsepti on jo muillakin asevoimilla käytössä tai sen torjuntakeino on jo olemassa. Tämän vuoksi ei voida laskea sen varaan, että valmistautumalla esimerkiksi Ukrainan sodan kaltaiseen skenaarioon, oltaisiin vahvoilla. Uudet sodat ovat harvoin edellisen kaltaisia.

Ukrainan sotaa on kuitenkin tarkoin tutkittava, tavoitteena varmennettujen oppien hallittu jalkauttaminen. Yksittäinen havainto ei ole varmennettu oppi. Hallittu jalkauttaminen ei tarkoita sitä, että yksittäinen kouluttaja päättäisi huomaamansa havainnon ottamisesta käyttöön, vaan johto-, toimiala- ja omistajuussuhteiden mukaisesti tapahtuvaa harkittua käyttöönottoa.

Selvää on, että Ukrainan sotaa tullaan tutkimaan sotatieteellisesti meillä Suomessakin seuraavan kymmenen vuoden ajan. Lähdepohja ei ole vielä tieteelliseen tutkimukseen riittävää, mutta sodan oppien hyödyntämisessä ei ole mahdollista jäädä odottamaan luotettavan ja mahdollisimman monipuolisen lähteistön käyttöönsaamista.

Sotataidon muutostekijät

Sotataidon yleisinä muutostekijöinä on pidetty sotatekniikkaa, toimintatapoja ja organisaatioita. Sotateknisellä aspektilla tarkoitetaan sekä suoraan sotilaskäyttöön kehitettyjen teknologioiden että siviiliteknologioista johdettavien sotilassovellusten aiheuttamia vaikutuksia sodankäyntiin ja sotataitoon. Toimintatavat pitävät sisällään doktriinit eli taisteluopit ja kaikki muut sodankäyntiä ja taistelua ohjeistavat opit ja niiden vaikutukset aina yksittäisen sotilaan tasolle saakka. Organisaatioiden vaikutuksella tarkoitetaan muutostrendejä, joiden mukaan sotilasorganisaatioiden kokoonpanoja ja varustusta kehitetään.

Maasodankäynnin muutosta on mahdollista analysoida myös taistelun elementtien kautta. Perinteisten tulen, liikkeen ja suojan rinnalle on ollut perusteltua nostaa myös johtaminen. Tässä artikkelissa luodaan skenaarionkaltaisia tarkasteluja käyttäen edellä mainittuja kolmea sotataidon muutostekijäryhmää käyttäen.

Sotatekniikka

Persianlahden sodan päätyttyä eräs yhdysvaltalainen sotilasasiantuntija totesi silloiset aselavetit, kuten esimerkiksi taistelupanssarivaunut, hävittäjäpommittajat ja lentotukialukset vanhentuneiksi ja että ne katoaisivat taistelukentältä. Oleellista ei ole lavetti, vaan kohteeseen aikaansaatava vaikutus. No, totta sekin. Kolme vuosikymmentä myöhemmin mainitut järjestelmät ovat kuitenkin edelleen käytössä, eikä niiden poistuminen ole näköpiirissä. Ukrainan sota on osoittanut etenkin taistelupanssarivaunujen olevan ylivertainen offensiivinen taisteluväline. Tuli, liike, suoja ja johtaminen ovat samassa tehokkaassa paketissa. On vaikea kuvitella, että Ukrainan maavoimien vastahyökkäys olisi menestynyt ilman panssarijoukkoja.

Miehittämättömät järjestelmät saattavat osoittautua voiman moninkertaistajaksi ja voimasuhteiden tasoittajaksi etenkin sotilaallisen konfliktin alivoimaisen osapuolen kannalta. Tämän hetken näkymä ei kuitenkaan tue ajatusta, että ilmapuolustus olisi tulevaisuudessa hoidettavissa yksinomaan ohjuksin ja miehittämättömin ilma-aluksin. Jos ohjuspuolustus on tehokas, ilma-alukset laukaisevat risteilyohjuksensa ilmatorjuntaohjusten kantaman ulkopuolelta, kuten Ukrainan sota on osoittanut. Edelleenkin tarvitaan lentokoneita lentokoneiden tuhoamiseksi, tai muuta ”kättä pitempää”, jolla ulotutaan aina 500 kilometrin etäisyydelle hyökkääjän syvyyteen.

Miehittämättömien ilma-alusten aiheuttama murros näyttääkin kohdistuvan maasodankäyntiin. Monikoptereista on muodostunut 2000-luvun ”hermosaha”, joka jäytää vuorokaudenajasta riippumatta vastapuolen hermoja ja taisteluhenkeä ja aiheuttaa koko ajan merkittäviä miehistö- ja kalustotappioita. Tämä siis tilanteessa, jossa käytön kohteena oleva joukko ei noudata ilmasuojelutoimenpiteitä eikä linnoittaudu. Miehittämättömät ilma-alukset eivät ole ainoa syy, minkä vuoksi maavoimien taistelussa hakeudutaan ja tukeudutaan tulevaisuudessa yhä enenevässä määrin maanalaisiin rakenteisiin, rakennuksiin ja katettujen linnoitteiden suojaan. Aktiiviset torjuntakeinot ovat tärkeitä, mutta passiiviset menetelmät ovat usein kustannustehokkaampia ja niitä osaavat kaikki käyttää, jos joukkojen koulutustaso ja itsekuri ovat kohdallaan.

Tulenkäytön muissa osa-alueissa korostuvat nopeus, tarkkuus ja jatkuvuus. Tämä koskee erityisesti epäsuoraa tulta ja panssarintorjuntaa. Vaikka ohjautuvat ammukset ovat kalliita, niiden ansiosta on mahdollista kustannustehokkaasti tuhota vastustajan toiminnan kannalta kriittisiä maaleja. Panssarintorjunta on elinehto etenkin puolustustaistelun onnistumiselle. Panssarintorjunnalla on oltava syvyyttä, volyymiä ja kerroksettaisuutta.

Sotateknisten muutostekijöiden suuntaus näyttää viittaavan siihen, että miehittämättömiä ilma-aluksia käytetään maalittamiseen, tulenkäyttöön operaatioalueen lähisyvyydestä aina satojen kilometrien etäisyydelle sekä vaikuttamisen jälkeen vaurioarviointiin. Miehittämättömien ilma-alusten havaitsemis- ja torjuntakeinojen kehittäminen ja tuottaminen on puolustusteollisuuden 2020-luvun menestystekijä. Kaukovaikuttaminen muodostuu keskeiseksi suorituskykyvaatimukseksi myös pienempien valtioiden asevoimille. On kyettävä tuhoamaan vastustajan kriittisiä kohteita 300, jopa 500 kilometrin syvyydessä ja tarkasti. Ratkaisusotatoimissa tarvitaan raskaita asejärjestelmiä, joilla on kantamaa ja operatiivista liikkuvuutta. Kyky pitkälliseen

vastarintaan kyetään luomaan massoittamalla kannettavia panssarintorjunta-aseita ja ilmatorjuntaohjuksia, sekä kyvyllä syvään sulluttamiseen tie- ja siltahävittein sekä älymiinoin. Johtamisjärjestelmien ja asejärjestelmien vikasietokyky, resilienssi ja joukkojen kyky taistelun jatkamiseen sähköttömässä, polttoaineettomassa, digitaalista paikkatietoa vailla olevassa ja voimakkaassa sähkömagneettisessa häirintätilanteessa saattaa nousta maasodankäynnin ensi vuosikymmenen menestystekijäksi.

Toimintatavat

Maasodankäynnin taisteluoppeja tarkasteltaessa näyttää edelleenkin pätevän venäläisen generalissimus Aleksander Suvorovin yli kaksi vuosisataa sitten tokaisu ”Teoria ilman käytäntöä on kuollut”. Maasodankäynnissä ollaan heikoilla, jos suunnitellaan ja pyritään toteuttamaan sotatoimia omalle sodankäyntikulttuurille ja sotilaalliselle ajattelulle vierailla toimintamalleilla.

Venäjän hyökkäyssodan ensimmäisessä vaiheessa Ukrainassa helmi-maaliskuussa 2022 näytettiin pyrittävän yhdysvaltalaisen Schock and Awe -mallin kaltaiseen operaatioon, jossa ensisijaisesti tuli-isku-operaatiolla ja syvin, nopein, mutta rajoitetuin maasotatoimin pyrittiin vastustajan hallinnon taipumiseen omia tavoitteita palvelevaan päätöksentekoon. Tämän kaltainen pyrkimys muistuttaa myös venäläistä refleksiivisen kontrollin mallin tavoitetta ja osin myös keinovalikoimaa. Yksi merkittävä eroavuus kuitenkin ilmeni. Sotilaallisen voiman käyttö, jos ei-kineettiset keinot eivät riitä, tulee kuitenkin aloittaa vain, mikäli tietyt sodankäynnin perusedellytykset ovat voimassa. Niistä mainittakoon vain poimintoina kohdemaan sotilaspoliittinen tila ja sen asevoimien puolustuskyky, sekä oman maan kansalaisen tuki sotilaallisen voiman käytölle ja omien asevoimien suorituskyky.

Sotilaallisen voiman käytön tulee myös tapahtua omia sotateknisiä, taktisia ja operaatiotaidollisia vahvuuksia hyödyntäen ja noudattaen. Tässä suhteessa venäläisten voimaryhmittymien jakaminen jopa seitsemään operaatiosuuntaan ja eteneminen kolonnamaisissa ryhmityksissä yllätti meidät länsimaiset tarkkailijat. ”Eihän tämä voi mitenkään toimia”, saattoi nousta monien mieleen. Missä salaaminen, harhauttaminen ja voimien vaikutuksen keskittäminen? Ukrainan asevoimat ovat kyenneet nopeasti adaptoitumaan toimintamenetelmissään muuttuneen tilanteen asettamien vaatimusten mukaisesti. Vuodesta 2014 lähtien on tehty perustavaa laatua olevaa työtä entisen neuvostotaustaisen sotataidon poisoppimisen ja omiin olosuhteisiin soveltuvien ja adaptoitujen länsimaisten menetelmien käyttöönottamiseksi. Kun luotettavat lähteet ovat tutkijoidemme käytössä, on suuren kiinnostuksen kohteena, miten esimerkiksi yhtymien vastahyökkäysoperaatiot on suunniteltu, käskytetty ja toimeenpantu. Alustavat tiedot viittaavat siihen, että Ukrainan maavoimien yhtymät ja niiden yläpuolella olevat johtoportaat ovat analysoineet jokaisen operaation ja taistelun jälkeen saamiaan kokemuksia ja huomioineet opit heti seuraavia sotatoimia suunniteltaessa.

Oma kiinnostukseni kohdistuu erityisesti siihen, miten ukrainalaiset ovat onnistuneet tunkeutumaan venäläisen päätöksentekosyklin sisään, sen rikkoen ja myöhässä olevaksi turmellen. Perinteisestihän on ajateltu, että siinä missä länsimainen esikunta tai upseeri vielä pähkäilee ja suunnittelee, venäläinen jo toimii. Viimeisten kahdeksan vuoden kuluessa myös Ukrainan maavoimat ovat olleet pulpetin takana tavaamassa läntisiä operatiivisen suunnittelun prosessityökaluja GOP´ia ja COPD´tä (Guidelines for Operational Planning ja Comprehensive Operations Planning Directive), joita moni pitää nopean tilanteenmukaisen suunnittelun ja toimeenpanon vesittäjinä. Jos he ovat niitä operaatioiden suunnittelussa käyttäneet, mikä on ollut se ”ukrainalainen taikatemppu”, jolla monien länsimaisten upseereiden kammoksumat byrokraattisen ja hitaan suunnittelun karikot on vältetty?

Yhdysvaltojen asevoimien johdossa jo pitkään vaikuttanut kenraali Mark Milley totesi jo neljä vuotta sitten, että sotatekniikan monipuolistumisesta, asevaikutuksen nopeudesta ja tarkkuudesta huolimatta taistelussa menestyminen ja menestyksen varmistaminen edellyttää edelleenkin paljon jalkaväkeä, ”boots on the ground”. Miesvoiman tarve korostuu erityisesti taistelussa rakennetulla alueella, jossa hyökkääjä tarvitsee jopa yli kymmenkertaisen ylivoiman puolustajan vahvuuteen nähden.

Toimintatapojen kehittyminen vaikuttanee maasodankäyntiin lähitulevaisuudessa ”asioita yksinkertaistavasti”. Kyky nopeaan toimeenpanoon nousee avaintekijäksi, johtaen korostettuun komentajakeskeiseen tilanteen arviointiin, päätöksentekoon ja johtamiseen. Ylemmän johtoportaan jakaman tilannekuvan saamisen viive ei saa estää toimenpiteiden käynnistämistä. Tehtäväjohtamisen merkitys kasvaa entisestään. Taktisen taidon ja operatiivisen älyn korostaminen asettaa päällikkö- ja komentajatehtäviin asetettaville kovat valintakriteerit. Perustaistelumenetelmillä voitetaan aikaa tilanteenarvioinnille ja päätöksenteolle, mutta luovat ratkaisut, jotka minimoivat liian suuret riskit, ovat avain taistelun voittoon.

Organisaatiot

Länsimaissa ryhdyttiin 2010-luvulla sotatekniikan kustannuskehityksen, asevoimien vahvuuden supistustarpeiden, kriisinhallinnan tehtävätyyppien ja voiman projisoinnin kehittämistarpeiden johdosta pohtimaan, mikä raskaampien yhtymien tarve tulevaisuudessa enää olisi. Kevyiden taisteluosastojen ja joukkoyksiköiden, joiden johtoportaana olisi kymmenien upseereiden esikunnan sijaan vain tiivis komentajaa tukeva aselajimiesten suunnitteluryhmä, koettiin olevan harkinnan arvoinen ratkaisu. Tällaisella joukkoyksiköille ei toki olisi aselajien ja kauaskantoisen tulenkäytön suurempia yksiköitä sekä jatkuvuuden takaavaa omaa orgaanista huoltoa tukenaan.

Venäjä siirtyi kevyiden, keskiraskaiden ja raskaiden prikaatien kehittämisestä muodostamaan prikaatirungoista pataljoonien taisteluosastoja. Ukrainan sota on osoittanut, että kevyet ja ketterät kokoonpanot eivät menesty nykyaikaisella taistelukentällä, mikäli niiltä puuttuu aselajien välitön tuki ja jatkuvat täydennykset ja evakuoinnit. Venäläisten pataljoonien taisteluosastojen rivivahvuudet jäivät jo sodan alussa usein selvästi alle tavoitteiden, jota vaikutusta Ukrainan asevoimien aiheuttamat tappiot ovat vain kumuloineet.

Ukrainan maavoimat käytti erityisesti sodan ensimmäisissä vaiheissa alimmillaan joukkueita, useimmiten komppanioita ja tehtävän tarpeiden mukaisesti koottuja iskuosastoja (taisteluosastoja) väijytysten ja iskujen toteuttamiseen. Vaikka ne saattoivatkin kuulua maavoimien prikaateihin tai alueellisen puolustuksen yhtymiin, ne toimivat hajautetusti, joskin keskitetyssä johdossa. Sodan siirryttyä kolmanteen vaiheeseensa, Ukrainan vastahyökkäykseen, on muodostunut mielikuva, että Harkovan ja Hersonin oblastien menestyksen takana on ollut venäläisten joukkojen alhaisen suorituskyvyn lisäksi ukrainalaisten yhtymien iskukyky.

Organisaationäkymä tulevaisuuden maasodankäynnin kehittymiseen viittaa siihen, että voimakkaita, iskukykyisiä ja operatiiviseen liikkuvuuteen kykeneviä maavoimien yhtymiä tarvitaan edelleen, jos ratkaisusotatoimissa halutaan maakomponentti, joka ei ole hajanainen ja jonka voima ei ehdy vastahyökkäyksen ensimmäisen vuorokauden jälkeen.

Disclaimer

Kaiken tämän kirjoitettuani, tunnistan omassa tekstissänikin vallitsevan jatkosodassa prikaatin komentajana joukkonsa keskitysmarssia junakuljetuksessa johtaneen, yksittäisen punahävittäjän rynnäköinnissä kaatuneen eversti Joose Hannulan varoittaman pyrkimyksen ”viisasten kiven” etsimiseen oman aikakautensa sodasta tehtyjen havaintojen perusteella. Puolustusvoimien teknologiaseuranta saattaa paljastaa Ukrainan sodan kuluessa tai päätyttyä sellaisen kehitysloikan jossain aivan muualla, ”mustan joutsenen” tai jonkun jo tiedossa olevan teknologian odottamattoman jalkautumisen sotilassovelluksiin, joka aikaansaa niin mullistavia mahdollisuuksia uusien taktisten ja operatiivisten toimintamallien kehittämiselle ja edellyttää niin paljon nykykäsityksestä poikkeavia kokoonpanoja ja logistisia ratkaisuja, että yllättäen olemmekin RMA:n edessä. Siksi tarvitsemme tulevaisuuteen suuntautuneita, avarakatseisia insinööriupseereita ja logistikkoja – emme vain käynnissä olevaa sotaa tarkalla silmällä seuraavia taktikkoja ja operaatikkoja.

Sota merellä

- Insinöörikomentaja Jussi Malmberg -

Merisodankäynnin tulevaisuus – mikä muuttuu ja mikä säilyy

Artikkeli keskittyy yleisellä tasolla merisodankäynnin ja teknologian muutokseen lähitulevaisuudessa. Mikä sodankäynnissä käytännössä muuttuu, vai muuttuuko juurikaan mikään? Teknologiat kehittyvät isoin harppauksin teollisuusvetoisesti, mitkä ovat merisodankäynnille tärkeät teknologiat? Pienempien maiden merivoimilla on suurempia maita rajoitetummat tavoitteet, mutta myös vähemmän resursseja käytettävänään. Lisäksi artikkelissa tuodaan esille esimerkin kautta vedenalaisen taistelutilan monipuolistumista. Artikkelin kirjoittaja toimii Merivoimien esikunnan suunnitteluosastolla Merivoimien yli-insinöörinä. Artikkelin tausta-aineistona on käytetty Maanpuolustuskorkeakoulun Sotataidon laitoksen julkaisuja: Nykyaikainen merisodankäynti ja Tuleva sota.

Toimintaympäristö säilyy, mutta toimijat ja niiden tarkoitusperät muuttuvat

Vaikka merisodankäynti on muuttunut ja muuttuu jatkuvasti, niin sen taustalla oleva teoria on muuttunut vain vähän. Merisodankäynnin perusajatus on, että merialueita ei voi pitää, mutta niitä voi hallita. Tämä on merkittävä ero maasodankäyntiin verrattuna. Meren hallinta perustuu läsnäoloon ja kykyyn vaikuttaa merelle.

Suomen merivoimille tärkein toimintaympäristö on jatkossakin Itämeri, vaikka toimijat ja niiden tarkoitusperät merellä ovat muuttuneet vuosien saatossa. Toimintaympäristö on ainutlaatuinen ja se asettaa järjestelmille suorituskykyvaatimuksia, joita ei ole aina suoraan ostettavissa Suomen rajojen ulkopuolelta. Kansainvälisten kumppaneiden kiinnostus toimintaympäristön kautta hankkimaamme erityisosaamiseen on ilmeistä.

Konfliktien todennäköisyys toimintaympäristössä on noussut. Tämä johtuu siitä, että kylmän sodan jälkeinen maailmanjärjestys on muutoksessa. Muutoksen vaikutusta korostaa yhtäältä samaan aikaan tapahtuva globalisaatio, ilmaston lämpeneminen ja maailmanlaajuiset pandemiat sekä toisaalta polarisaation lisääntyminen demokratioiden poliittisissa, taloudellisissa ja sosiaalisissa asioissa.

Itämeri ei ole tärkeä vain Suomen huoltovarmuuden ja tietoliikenneyhteyksien kannalta, vaan myös Euroopan energiantuotannon ja raaka-aineiden kuljettamisen kannalta. Suomeen tuotavista ja Suomesta vietävistä tarvikkeista 90 % kulkee meritse. Kilpailun kiristyessä teollisuuden ja kaupan maavarastoinnin osuus on vähentynyt merkittävästi. Käytännössä suuri osuus varastoista on merellä aluksissa menossa jonnekin tai tulossa jostain. Meriyhteyksien katkeaminen tarkoittaisi kansallista katastrofia, ja siksi niiden säilyttäminen on suomalaisen merisodankäynnin keskiössä. Mereltä tulevien materiaalivirtojen siirtäminen rauta- tai maantiekuljetuksiin on kuljetuskapasiteetista johtuen käytännössä mahdotonta.

Sodankäynnin peruselementit säilyvät, mutta suojan merkitys korostuu

Tutkimus ei tarjoa lopullisia ratkaisuja, eikä sen tuottama tieto ole täysin varmaa. Varmojen vastausten sijaan on vain todennäköisyyksiä. Siten tulevaisuuden sodankäynnin ennustaminen, tai kauaskantoisten teknologiapainotteisten arvioiden tekeminen kaiken ratkaisevana hopealuotina, on osin hyödytöntä. Sodankäynnin perusluonne ei ole kuitenkaan muuttunut, vaan ainoastaan sodankäynnin olemus on muuttunut. Sodankäynnin peruselementit tuli ja liike säilyvät, mutta merisodankäynnin osalta suojan merkitys korostuu.

Itämeren pinnan päällinen alue on melko kattavasti ja lähes reaaliaikaisesti valvottu. Sensoriverkosto on myös hyvin verkottunut. Meritorjuntaohjusten kantama on kasvanut ja tulta kyetään käyttämään tarkasti, laajasti ja nopeasti. Avaruuden hyödyntäminen yhdessä kehittyvän sensoriverkoston kanssa tarkoittaa sitä, että tulevaisuudessa meri ei itsessään tarjoa suojaa ilma- ja pinta-aluksille. AESA-tutka pystyy havaitsemaan suuren määrän kohteita ja seuramaan niitä. HF- tutka taas näkee horisontin yli. Satelliittien paikannus- navigaatio- ja aikapalvelut ovat helposti häirittävissä ja pilvipeitto estää elektro-optisen kuvaustiedustelun, mutta SAR-kuvaus ja ELINT -suorituskyvyt toimivat edelleen. Kaikki tämä edelle sanottu tarkoittaa, että pinnalla olevat kohteet eivät pysy piilossa ilman aktiivista häirintää, häivettä tai harhauttamista yhdistettynä liikkeeseen.

Vaikka taistelutilan läpinäkyvyys kasvaa pinta- ja ilmatilan osalta, niin toisaalta vedenalaisessa valvonnassa ei ole nähtävissä merkittävää kehitystä, mikä tarkoittaa, että vedenalainen tila tarjoaa jatkossakin osittaista suojaa havaituksi tulemiselta.

Taistelutila monipuolistuu etenkin vedenalaisen sodankäynnin osalta

Meriyhteydet, satamat ja vedenalainen infrastruktuuri ovat osa yhteiskunnan kriittistä infrastruktuuria, jota on kyettävä suojaamaan niin normaali kuin poikkeusoloissa. Miinat ja torpedot sekä tulevaisuudessa niiden yhdistelmät korostuvat vedenalaisen sodankäynnin vaikuttamisen elementteinä. Vaikuttamisjärjestelmät on integroitu kiintomerkkialueen ulkopuolella toimintakykyisten alusten taistelunjohtojärjestelmään. Pinta- ja vedenalaisen valvonnan osalta kiinteä valvonta on jatkossakin kustannustehokkain tekninen ratkaisu jatkuvaan valvontaan. Kiinteällä valvontaverkolla on kuitenkin heikko taistelunkestävyys ja siksi niitä pitää täydentää siirrettävällä ja liikkuvalla valvontakyvyllä.

Vedenalaisille äänihavainnoille on tyypillistä, että ne ilmestyvät yllättäen, ja että kohde häviää nopeasti. Mikäli ei olla valmiiksi saadun havainnon valvonta-alueella, niin sinne pitää päästä nopeasti. Nopean reagointiajan varmistamiseksi kyvykkyyksien pitää olla orgaaninen osa valvontaa ja vaikuttamista tekevää joukkoa, jotta se on käytettävissä, kun sitä tarvitaan.

NH90 SUTO-helikopteri

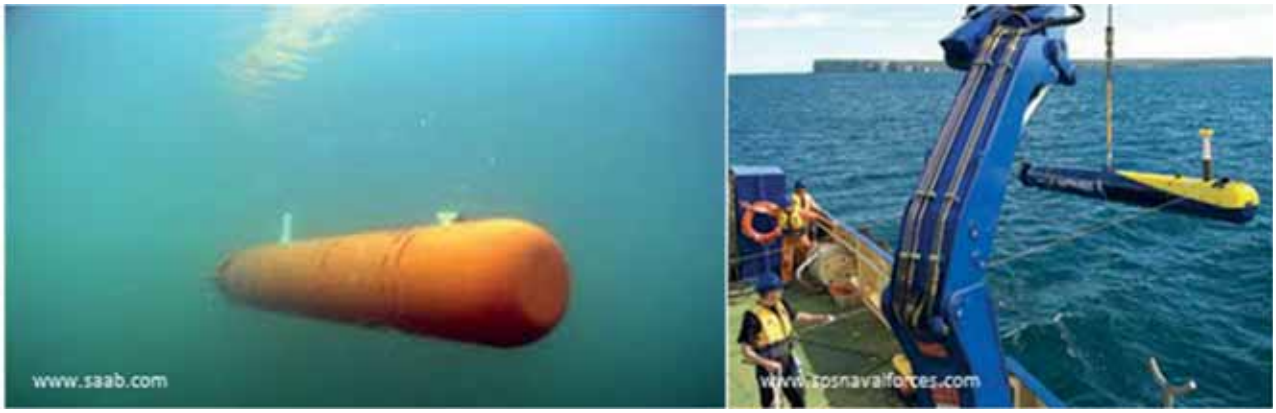
Helikopterit soveltuvat hyvin vedenalaisen sodankäynnin kyvykkyyden täydentäjäksi, ja siksi ne ovat laajasti käytössä eri maiden merivoimissa. Valvonta- ja vaikuttamiskykyinen miehitetty helikopteri kykenee siirtymään kiintomerkkialueen ulkopuolella havaittuun kohteeseen nopeasti ilman, että vedenalainen kohde havaitsisi sitä ajoissa ja ehtisi poistua valvonta-alueelta. Pyöriväsiipisten teknisten ratkaisujen haittapuolena on se, että niillä on huono kyky jatkuvaan valvontaan. Lisäksi hankintahinta ja kunnossapitokustannukset voivat muodostua ylipääsemättömäksi haasteeksi pienemmille asevoimille.

Elbit Seagul SUTO-USV

Tarvittava hyötykuorma muodostuu 3D-tutkasta, syvyytettävästä sonarista tai kertakäyttöisistä sonopoijuista sekä kiinnikkeisiin asennettavista torpedoista, mikä asettaa lentävän laiteen koolle vaatimuksia. Tällä hetkellä sukellusveneentorjuntahelikopteri on käytännössä ainoa järjestelmä, jolla vaikeasti seurattava havainto saadaan nopeasti varmennettua, ja johon päästään riittävän nopeasti vaikuttamaan. Lisäksi meritoimintahelikopterilla on merkittävä määrä myös muita rooleja mm. meripelastus, materiaali- ja henkilöstökuljetukset, valvonnan täydentäminen.

USV-järjestelmät soveltuvat hyvin vedenalaisen valvonnan- ja vaikuttamisen kyvykkyyden täydentäjäksi, ja siksi sellaisia kehitetään voimakkaasti puolustusteollisuudessa. Valvonta- ja vaikuttamiskykyisellä USV-parvella siirtyminen kohteeseen kestää kuitenkin reilusti helikopteria pidempään, mutta sillä on kykyä jatkuvaan valvontaan ainakin kiintomerkkialueen sisäpuolella. Haittapuolena on se, että vedenalainen kohde kuulee pinnalla nopeasti lähestyvän aluksen kaukaa ja kykenee reagoimaa sen lähestymiseen. Pienen tai keskisuuren USV-järjestelmän hankintahinta on varustelusta riippuen matalahko, mutta niitä tarvitaan valvottavan alueen koosta riippuen useampia, mikä nostaa hankinta- ja kunnossapitokustannuksia. Hankintahintaa toisaalta laskee miehistötilojen puuttuminen ja käyttöaikaa nostaa, kun miehistöä ei tarvitse vaihtaa aika ajoin.

Hyötykuorma voi vaihdella parven jäsenissä siten, että yhdellä parven jäsenellä on liikkeessä hinattava TLA sensori (kuvassa 2 vasemmalla) tai paikalla syvyytettävä sonari. Toisella parven jäsenellä voi olla torpedonlaukaisujärjestelmä.



Saab UAV62

UUV-järjestelmät soveltuvat hyvin kiinteän ja siirrettävän vedenalaisen valvonnan kyvykkyyden täydentäjäksi, ja siksi sellaisia kehitetään voimakkaasti puolustusteollisuudessa. Valvontakykyisellä UUV-parvella siirtyminen kohteeseen on hidasta, mutta sen toimintaan ei vaikeuta merenkäynti, jolloin se voi toimia myös kiintomerkkialueen ulkopuolella. Vedenalainen kohde ei havaitse hitaasti kulkevaa UUV-järjestelmää kuin lähietäisyydellä passiivijärjestelmillä. Pienen alle 7 metrisen UUV-järjestelmän hankintahintaa voinee varustelutasosta riippumatta pitää kohtuullisena. Valvottavan alueen koko vaikuttaa suoraan parven kokoon samalla tavalla kuin USV-parvessa.

Hyötykuormana tulisi kysymykseen TLA ja aktiivinen sonar. Lisäksi mahdollinen pitkäaikainen valvontakyky edellyttää vedenalaisia latauspisteitä tai pinnan päällistä tukialusta, mikä nostaa hankinta- ja kunnossapitokustannuksia. Tällä hetkellä propulsiolla varustettuja UUV-järjestelmiä käytetään lähinnä sukellusveneentorjunnan maaleina ja Glider-tyyppisiä UUV-järjestelmiä vedenalaisen toimintaympäristön kartoittamiseen sekä olosuhteiden seurantaan. Loitering-tyyppisiä vedenalaisen valvonnan ja vaikuttamisen kyvykkyyksiä yhdistäviä UUV-järjestelmiä ollaan vasta tutkimassa. UUV-järjestelmät liikkuvat hitaasti ja ne pitää viedä operaatioalueelle tukialuksella. Oman haasteensa järjestelmien käytölle avomerellä tuo merenkäynnistä johtuen järjestelmien lasku ja nosto. Yleisimmin käytetty tekninen ratkaisu on tukialuksen nosto- ja laskulaite eli taavetti.

Merisodankäynnin muutostekijänä laatu korvaa määrän

90-luvulla alkanut Kiinan nopea teollistuminen ja kilpailu Yhdysvaltojen talouden kanssa, on korostanut suurten teollisuusmaiden merivoimien tarvetta projisoida sotilaallista voimaa tai painostusta globaalisti. Teollistumisen ja globalisaation seurauksena suurten maiden merivoimat ovat jo pitkään perustuneet lentotukialusten ympärille rakennetuista taisteluosastoista. Pienempien maiden merivoimilla on rajoitetummat tavoitteet ja toimintaympäristö, mutta myös vähemmän resursseja käytettävänään. Kaiken kokoisille merivoimille on yhteistä teknologisten innovaatioiden löytäminen ja nopea käyttöönotto.

Nykyisin suurvaltojenkin merisodankäynnissä painotetaan kykyä toimia rannikon lähellä ja kapeilla merialueilla sekä puolustushaarojen välistä yhteistoimintaa. Merisodankäynnin muutostekijänä on, että joukkojen koko ja määrä pienenevät, mutta ne ovat aikaisempaa tulivoimaisempia. Merisodankäynnissä halutaan hyödyntää vaikuttamisjärjestelmien kantaman kasvun täysimääräisesti, mikä edellyttää vaikuttamista tukevia toimia, jotka ylittävät kiinteän valvonnan kantaman ja kattavuuden. Joukkoja käytetään hajautetusti koko taistelutilan alueella, mutta ne ovat liikkuvampia ja verkottuneita. Merisodankäynnissä halutaan käyttää järjestelmiä koko operaatioalueella. Tämä edellyttää, että valvontakykyä voidaan kasvattaa lennokeilla, pitkäaikaista valvontaa kyetään tehostamaan rannikolla ja saaristossa

miehittämättömillä pinta-aluksilla ja miinan- ja sukellusveneentorjunnan kerroksellisuutta on mahdollista lisätä vedenalaisilla miehittämättömillä ja autonomisilla järjestelmillä. Vedenalainen langaton tietoliikenne mahdollistaa valvonta- ja vaikuttamiselementtien operoinnin. Sensoritiedon yhdistäminen miehittämättömiin järjestelmiin avaa uusia mahdollisuuksia jatkuvaan valvontaan kykenevien järjestelmien kehittämiselle myös kiintomerkkialueen ulkopuolelle.

Suomen Merivoimien osalta on huomioin arvoista, että toiminta perustuu kahteen hyvin erityyppiseen joukkokokonaisuuteen. Yhtäältä operoidaan teknisesti kehittyneillä, mutta vähälukuisilla laivastojoukoilla ja toisaalta määrällisesti suuremmilla rannikkojoukoilla. Suuressa kuvassa rannikkojoukkojen operointi on pitkälti Maavoimien kanssa yhdenmukaista ja lähtökohtaisesti kulutussodankäyntiä, kun taas laivastojoukkoja operoidaan enemmän liikesodankäynnin periaatteiden mukaisesti.

Merisodankäynnille tärkeät teknologiat

Luonnontieteellinen tutkimus ei ainoastaan kuvaa todellisuutta, vaan se myös rakentaa sitä. Nopeasti kehittyvä informaatioteknologia tarjoaa uusia ulottuvuuksia sodankäyntiin ja muokkaa varmuudella sodan kuvaa. Uudet mullistavat teknologiat voivat tuoda sodankäyntiin yllättävän ja nopean muutoksen, joka muuttaa perinteiset doktriinit vanhentuneiksi. Teknologisesti ylivoimainen osapuoli on usein selviytynyt voittajana. Toisaalta tekoälyn kyky vastata odottamattomiin siirtoihin, voi tarjota mahdollisuuksia kertaluonteisiin pikavoittoihon. Koneoppiminen on kuitenkin laskentatehon kasvaessa yhä nopeampaa eikä pikavoittoa ole luvassa pitkässä juoksussa.

Meripuolustuksessa tekoälyn soveltamismahdollisuudet ovat ensisijaisesti ihmisen toimintakykyä parantavissa ja tukevissa toiminoissa. Esimerkiksi valvonnassa, tekoäly voi antaa hälytyksen tunnistamattomista tai poikkeuksellisesti liikehtivistä kohteista. Sama pätee tulenkäytön tilanteissa, joissa tekoäly vastaisi datan reaaliaikaisesta analysoinnista ja tukisi operaattoria nopealla ehdotuksella tulenkäytön optimoinnista.

Teknologisesta näkökulmasta merisodankäynnissä korostuvat sensoriverkoston kyvykkyyden kasvu, miehittämättömien ja autonomisten järjestelmien yleistyminen sekä aseiden kantaman, tarkkuuden ja nopeuden kasvu. Suomen Merivoimille tärkeät teknologiat painottuvat Itämeren rannikkoalueiden ruskeille ajoittain osin jäisille vesille soveltuvien johtamis-, valvonta- ja vaikuttamisjärjestelmien sekä niiden sensoreiden ja sensorifuusion teknologioihin.

Reaktor

Cross-Domain API Guard -yhdyskäytävä.

Traficomin hyväksymä yhdyskäytävätuote tiedon hallittuun ja turvalliseen siirtoon verkkojen välillä alkiotason sisällönsuodatuksella varustettuna.

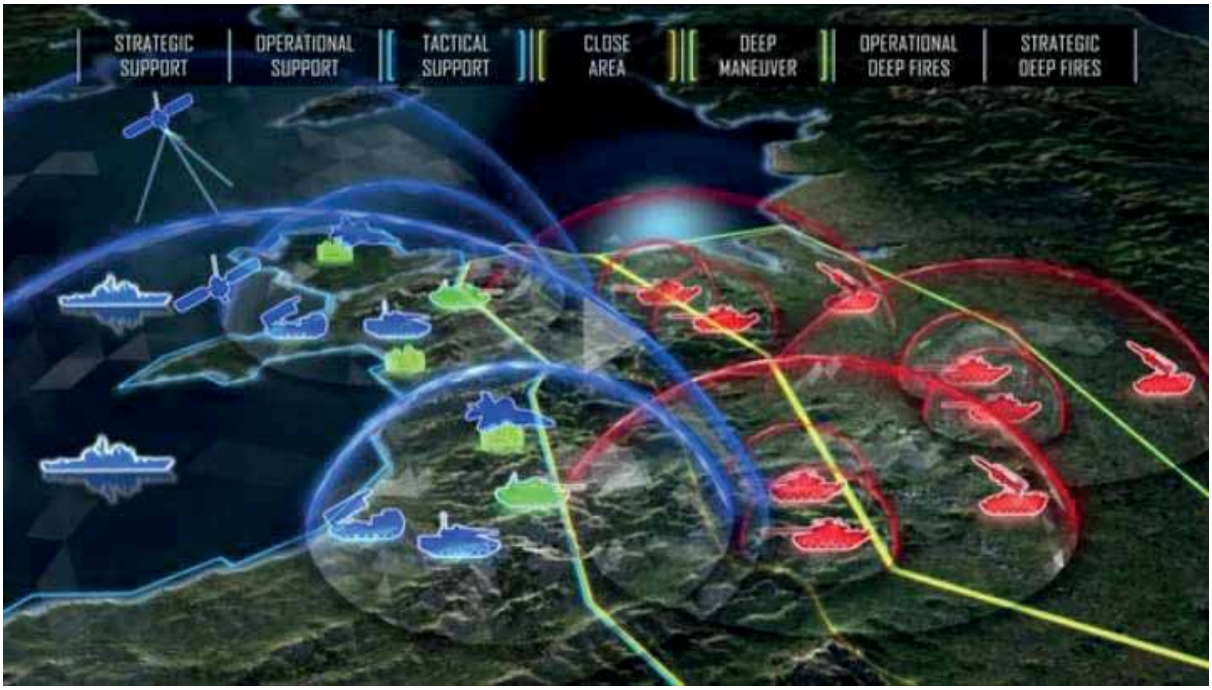
Tiedonsiirto toisistaan eristettyjen verkkojen välillä on haastavaa. Reaktor Cross-Domain API Guard (CDG) toteuttaa määritetyn politiikan mukaisen tiedonsiirtomekanismin verkkojen välillä. Se tarjoaa selkeän REST-pohjaisen lähestymistaavan tiedon lähettämiseen ja vastaanottamiseen, sekä yksisuuntaiseen optiseen linkkiin perustuvan datadiodin turvalliseen tiedonsiirtoon.

Reaktor Defence & Security

Ota yhteyttä: defsec@reaktor.com

Joint All Domain Operaatio

- Everstiluutnantti Tommi Pyöriä- -



Kirjoittaja palvelee Ilmasotakoulun koulutuskeskuksen johtajana. Hänellä on kokemusta ilmavoimien esikunnasta operatiiviselta osastolta sekä ilmaoperaatiokeskuksesta. Kirjoittaja on toiminut Suomen Bold Quest osaston vanhimpana kahdessa harjoituksessa. Kirjoitus heijastaa kirjoittajan mielipiteitä eikä ilma- tai Puolustusvoimien virallista kantaa.

”Vastustaja on perustanut A2AD (Anti Access – Area Denial) alueen ja uhkaa sillä vapaata kauttakulkua niin maalla, merellä kuin ilmassa. Liittouma päättää mahdollistaa vapaan liikkumisen sekä kauttakulun poistamalla A2AD uhkan alueelta. Operaatio toteutetaan yhden johdon johtamana Multi- tai Joint All Domain operaationa. Avaruutta käytetään alueen maalittamiseen sekä alueen yleiseen valvontaan. Kyber valvoo maalitetun alueen tietoverkkoja ja valmistautuu vaikuttamaan esimerkiksi alueen sähkö- ja vesi-infraan. Kun kyber on pimentänyt verkot, toteutetaan iskut ilmasta ja mereltä ennalta valittuihin kriittisiin maalipisteisiin ja niiden tuho varmistetaan maajoukkojen (esim. panssarit, raketinheittimet ja tykistö) aktiivisella hyökkäystoiminnalla. Näin joint all domain operaatiolla on saavutettu haluttu vaikutus eli vapaa kauttakulku kyseiselle alueelle, joka mahdollistaa niin kauppa-yhteyksien kuin mahdollisen humanitaarisen avun toimittamisen alueelle.”

Yllä oleva on kuvitteellinen esimerkki siitä, mitä Joint All Domain operaatio voisi olla, mutta onko tuo jo olemassa vai vasta haaveena – sitä voidaan miettiä.

Viisi sodankäynnin domainia

2020- luvulla sodankäynti on yleismaailmallisen järjestelmien sekä verkostoituneen ja digitaalisuuteen nojaavan yhteiskunnan kehittymisen myötä on myös sota ja sodankäynti muutoksessa. Ennen ensimmäistä maailmansotaa sodankäynnissä oli vain kaksi domainia Maa ja Meri. Ensimmäisessä maailmansodassa näiden yläpuolelle tuli uusi domain - Ilma. Ja pitkään sodankäynnissä pysyttiin näissä kolmessa selkeässä ja välillä keskenään kilpailevassa domainissa. Siirryttäessä uudelle vuosituhannelle tekninen kehitys aiheutti vaateita Yhdysvalloissa uusien domainien hyväksynnälle. Hyväksytyiksi tulivat ensin Avaruus ja myöhemmin Kyber. Nämä viisi ovat virallisia domaineja Näiden lisäksi esimerkiksi elektronista sodankäyntiä tai informaatioympäristöä on yritetty saada omaksi domainiksi, mutta toistaiseksi ei ole tullut virallisia muutoksia edellä mainittuihin.

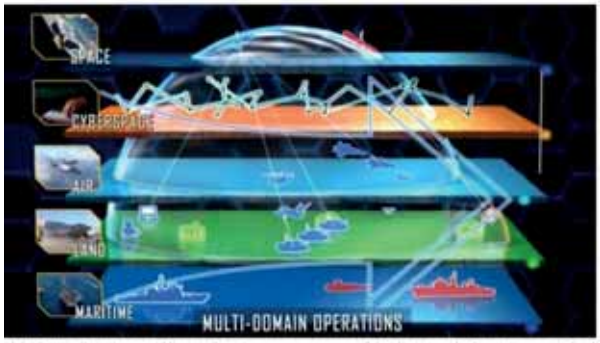
JADO ja MDO

Joint All Domain Operations (JADO) ja Multi Domain Operations (MDO) esiintyvät monissa julkaisuissa lähes synonyymeina. Minä en osaa sanoa mikä on niiden todellinen ero, jos mikään. Joint Air Power Competence Center:n (JAPCC) mukaan NATO JADO on uusi evoluutio NATO MDO:sta. Määritelmiä katsomalla asia on ehkä hieman erinäköinen. Naton MDO määritelmä on seuraava:

"Multi-Domain Operations aim to orchestrate and synchronise military activities with non-military activities, across all domains and environments, to enable commanders to deliver converging effects."

Natossa JADO on määritelty taas seuraavasti:

"Actions taken by the joint forces of two or more NATO nations, comprised of all available domains, integrated in planning and synchronized in execution, at a pace sufficient to effectively accomplish the mission."



Kuva US Army

Kun vertailee määritelmiä, niin MDO vaikuttaa laajemmalta, joka ottaa huomioon myös ei-sotilaalliset toimijat. JADO taas on suoraviivaisempi ja sotilaalle, varsinkin operaatikolle, helpommin ymmärrettävässä muodossa. Yhtä kaikki, käyttää kumpaa termiä hyvänsä on päämäärä kuitenkin sama. Väkisin tuleekin mieleen, että halutaan ”kikkailla” terminologialla, kun ei vielä ole eväitä todella toteuttaa kuvatun laisia operaatioita.

JADO Command&Control (JADC2)

Tehokas Joint All Domain operaatio vaatii sitä, että tieto on kaikkien operaatioon osallistuvien käytettävissä. Yhdysvaltojen asevoimia, ja samaa on havaittavissa myös Suomessa, on pitkään vaivannut se, että jokainen domain on kehitellyt omia johtamisjärjestelmiään ottamatta huomioon sitä, mitä joku muu domain on tehnyt tai miten tieto liikkuu eri domainien välillä. US Joint Staff vetää JADC2 kokonaisuutta, jossa pyritään tuottamaan alusta JADO-toiminnoille. Siinä pyritään saamaan tieto liikkumaan helposti ja tehokkaasti kerääjältä tarvitsijalle ja päätöksentekijälle. Kuvainnollisesti siirrytään ”savupiipuista” ”altaaseen”, josta kaikki tarvitsijat saavat tietoa omien tarpeidensa mukaisesti. Tämä ei kuitenkaan tarkoita sitä, että kaikki tieto olisi kaikkien käytössä vaan jokainen saa sitä oman luokituksensa ja roolinsa mukaan. JADC2 ei ole yksi ainoa ”crossdomain – one size fit all”- johtamisjärjestelmä, vaan jokaisella domainilla on oma, sen tarpeet täyttävä työkalu. Tämän työkalun vaatimuksena

on se, että se pystyy ottamaan vastaan ja tuottamaan sellaista dataa, jota muiden doimainien johtamisjärjestelmätyökalut pystyvät hyödyntämään. Applikaatioiden tulee olla teknisesti ”joustavia” samoin alustan tulee ottaa joustavasti vastaan uudet applikaatiot. Tällöin toimintojen kehittäminen on helpompaa, kevyempää ja edullisempaa. Tieto- ja operaatioturvallisuus pysyvät parempina, koska operaattorilla on käytössä juuri oikeat työkalut, mikä vähentää tarvetta omien viritysten tekemiselle.

Lopuksi

JADO tai MDO tai miksi tahansa tämä kokonaisuus tulee olemaan merkittävä osa länsimaista sodankäyntiä ainakin 2030 luvun puoliväliin saakka, ellei kauemmin. Näin operaatikon silmin tässä ei ole mitään ihmeellistä, mutta JOJÄ- tai TRS-henkilön silmin tämä ei välttämättä ole yksinkertaista. JOJÄ kauhistelee sitä, miten kaikki tuo kokonaisuus rakennetaan, että se toimii, mutta jokainen operaattori saa työskennellä juuri hänelle räätälöidyllä työkalulla. TRS henkilö taas pelkää sitä, että häneltä viedään resursseja, koska joku muu domain on jakamassa samaa kakkua. Tätä kirjoittaessani luin yhden artikkelin, jossa kritisoitiin koko domain ajattelua ja toivottiin US asevoimien siirtyvän domain-valtaisesta ajattelusta vaikutus-ajatteluun, eli käytetään eri asejärjestelmiä siten, mikä tuottaa parhaan vaikutuksen. Eli kaikessa olemme noidan kehässä, ei ole pitkä aika, kun meilläkin oli muodissa EBAO eli Effects Based Approach to Operations. Onko olemassakaan oikeaa tapaa määrittää asioita – en osaa sanoa. Minun näkemykseni ja operaattorikokemukseni mukaan olemme tuossa tietoallaskokonaisuudessa menossa oikeaan suuntaan, kun ajattelemme tulevia suorituskykyjä ja niiden mahdollisimman tehokasta käyttöä. Toivotaan vaan, että myös johtamisjärjestelmät ja -työkalut saadaan vastaamaan uusien suorituskykyjen sekä liittouman vaatimuksia niin käytettävyyden kuin operaatio- ja tietoturvallisuuden osalta. Ja niitä kehitettäessä tulee olla itselleen rehellinen, varsikin jos emme pysty jotakin asetettua tavoitetta saavuttamaan.

Kuva Lockheed Martin

Sotaa sähkömagneettisessa spektrissä

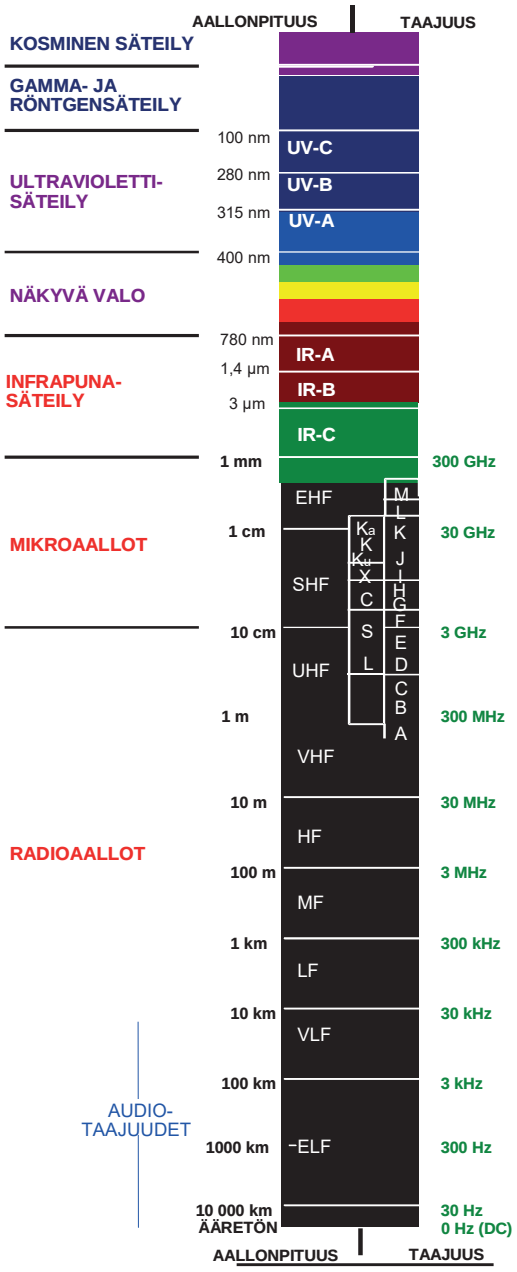
- Insinöörieversti Jyri Kosola -

i5D, unohtuiko jotakin?

I5D multidimension operations on nykypäivän muotitermi, johon ei voi välttyä törmäämästä. Kyseessä on amerikkalainen ajatus laajentaa maa-, meri-, ilma- ja avaruusympäristöt sisältävään taistelutilaan liittyviä analyysejä, tilannekuvia ja päätöksiä koskemaan myös informaatioulottuvuus. 1990-luvun puolivälissä viidennellä ulottuvuudella tarkoitettiin nimenomaisesti informaatio-operaatioita, mutta ajan mittaan viides ulottuvuus alkoi tarkoittaa kybertoimintaympäristöä, siis tietokoneita ja tietoverkkoja.

I5D:hen liittyy valuvika. Sen kautta maailmaa tarkasteltuna jää huomaamatta yksi sodankäynnin keskeinen ulottuvuus: sähkömagneettinen spektri. Se on itse asiassa kaikista ulottuvuuksista vanhin: ollut olemassa jo alkuräjähdyksestä alkaen, miljardeja vuosia ennen maapallollisia toimintaympäristöjä.

Toisinaan kuulee puhuttavan, että elektroninen sodankäynti on osa kybersodankäyntiä näiden fuusioituessa ja että tämän johdosta i5D:n viides D sisältää sekä kyber- että ELSO-ulottuvuudet. Perustelen seuraavassa miksi tämä Cyber Electromagnetic Activities (CEMA) ei ole kovinkaan järkevä.



Sähkömagneettisen spektrin osat.

Taistelu sähkömagneettisessa spektrissä ei ole pelkkää ELSOa

Moni mieltää taistelun sähkömagneettisessa spektrissä tarkoittavan elektronista sodankäyntiä. Mielikuva on väärä. Nimitys elektroninen sodankäynti (Electronic Warfare)

juontuu toisesta maailmansodasta, jolloin elektronisten laitteiden, erityisesti tutkien ja radioiden sotilaallinen käyttö motivoi kehittämään niihin vastamenetelmiä (Electronic Counter-Measures, ECM) ja edelleen suojautumiseksi vastamenetelmien vastamenetelmiä (Electronic Counter-Counter-Measures, ECCM). ELSO on siis ainakin alun perin tarkoittanut sotaa elektronisia laitteita vastaan. Vastaavasti ilmasotaa voitaisiin kutsua hävittäjäsodaksi ja merisotaa korvettisodaksi. Toimintaympäristön näkökulmasta tulisi puhua sähkömagneettisesta sodankäynnistä (Electro-Magnetic Warfare, EMW), jossa keskeistä on operointi sähkömagneettisessa toimintaympäristössä. Operoinnin kohde voi olla esimerkiksi myös ihmisen kyky hyödyntää sähkömagneettista spektriä näköhavaintoihin tai ihon tuntoaistin alttius sähkömagneettiselle vaikuttamiselle.

Operoinnin kannalta sähkömagneettinen sodankäynti ei eroa maa-, meri-, ja ilmasodankäynnistä. Kaikissa näissä on määritetty operaatioalue (taajuusalueet), jolla toiminta on sallittua ja jossa operoi myös vastustaja, joka on havaittava, paikannettava ja tunnistettava. Tehtävän ja tilanteen mukaan vastustajaan on vaikutettava tai sitä on vältettävä ja tarpeen mukaan väistettävä. Vastustajan lisäksi myös toimintaympäristössä olevien omien joukkojen sekä sivullisten huomioiminen edellyttää kykyä säätää suunnitelmia ja liikkua ketterästi toimintaympäristössä.

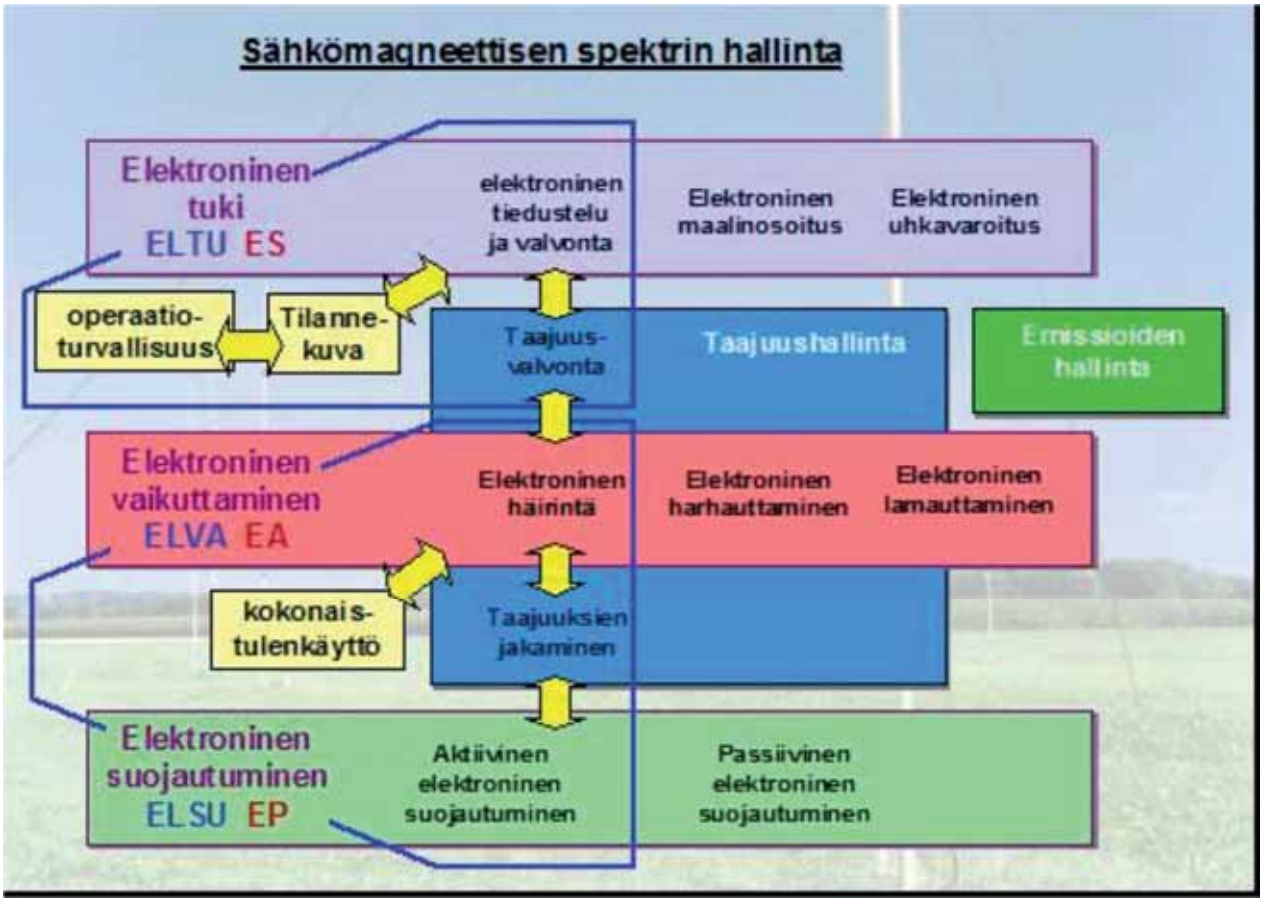
Kuten fyysisissä ympäristöissä, myös spektrissä on vältettävä ruuhkautumista ja kyettävä dekonfliktoimaan tilanteita. Toisinaan paras keino suojautua vastustajan tulenkäytöltä on ryhmittyä riittävän lähelle sitä, tai soluttautua sen ryhmitykseen. Tämä pätee niin fyysiseen kuin sähkömagneettiseen ulottuvuuteen.

Siinä missä maasodankäynnissä kyse on tuntiluokasta, merisodankäynnissä minuuteista ja ilmasodassa sekunneista, kybersodankäynti tapahtuu ohjelmakoodin suoritusnopeudella. Sähkömagneettisessa sodankäynnissä toiminnan on tapahduttava tarvittaessa millisekunneissa, esimerkiksi lähetettäessä harhatoistolähete tai seurattaessa taajuushypintäjärjestelmiä. Tämän vuoksi teknologian ja ihmisen rooli on erilainen kuin fyysisissä toimintaympäristöissä: koneiden on pääsääntöisesti operoitava spektrissä ilman ihmisen välitöntä ohjausta. Toimintaympäristössä saattaa olla 10.000 ystävällismielistä, vihamielistä tai sivullista tahoa, joiden toimintaedellytyksiä on ylläpidettävä, tuettava tai heikennettävä ohjaamalla spektrin käyttöä. Päätökset taisteluliikkeestä ja voimankäytöstä on tehtävä millisekunneissa. Ihminen ei tähän kykene, joten koneen on johdettava toimenpiteitä ja ihmisen tulee keskittyä tehtävän tavoitteiden määrittämiseen sekä toteutuksen reunaehtojen asettamiseen.

Toimintaympäristön tunnustaminen on tärkeää

Puolustusjärjestelmät perustuvat koko ajan enenevässä määrin ohjelmistoihin, jolloin niistä tulee yleiskäyttöisempiä. Ohjelmistopohjaisuuden myötä järjestelmät osaavat sovittaa toimintansa tilanteeseen. Kognitiiviset radioverkot ja tutkajärjestelmät tietävät mitä, milloin ja mihin suuntaan niiden pitää tai ei kannata säteillä oma tehtävä ja elektronisen tiedustelun ja häirinnän uhka huomioiden. Kognitiivitutkien verkko voi toimia passiivisensorin tai liftaritutkan tavoin ja valaista vain kulloinkin tarvittavaan suuntaan. Jokin sensori voi jäädä passiivisesti seuraamaan tilannetta, kun jokin toinen sensori valaisee sen puolesta maalialuetta. Tämä edellyttää kuitenkin sitä, että joku heiluttaa tahtipuikkoa sähkömagneettisessa orkesterissa.

Kognitiivisten järjestelmien myötä toiminta spektrissä kehittyy aktiiviseksi kamppailuksi, jossa tapahtuvaa tiedustelua valvontaa, maalinosoitusta, suojautumista, liikettä ja vaikuttamista koordinoidaan yli muiden ympäristöjen rajojen. Siksi sähkömagneettinen toimintaympäristö tulisi tunnustaa omaksi kokonaisuudekseen ja huomioida sähkömagneettinen sodankäynti maa-, meri-, ilma-, avaruus- ja kybersodankäynnin rinnalla yhtenä sodan ulottuvuutena, sillä sodankäynti sähkömagneettisessa spektrissä edellyttää kokonaisvaltaista spektri hallintaa.



Sähkömagneettinen spektri strategisena toimintaympäristönä

Vuosia sotaa matala-asteisempiin kriiseihin keskittynyt ja sotiakin vain alivoimaisia puolikehittyneitä valtioita vastaan sotinut USA on voinut nauttia ilma- ja tuliylivoiman ohella täydellisestä spektrinkäytön ylivoimasta. Nykyisin Amerikassakin on herätty siihen, ettei spektri aina olekaan käytettävissä tai siellä ei ole syytä loistaa majakan lailla. Vertaisvastustajat, kuten Kiina, ja wannabe-vertaisvastustajat, kuten Venäjä, kykenevät kiistämään amerikkalaisten toiminnanvapauden sähkömagneettisessa ulottuvuudessa. Se johtaa riskiin toiminnanvapauksien suhteen myös muissa ulottuvuuksissa. Kyetäkseen varmistamaan kokonaisvaltaisen ylivoiman myös tulevaisuudessa USAn puolustushallinto on laatinut strategian "Electromagnetic Spectrum Superiority Strategy" spektriylivoiman saavuttamiseksi.

Spektristrategian keskiössä on teknologioiden sijaan sähkömagneettisen spektrin näkeminen kokonaisvaltaisena ja koordinoidusti hallittuna kokonaisuutena. Esimerkiksi elektroninen sodankäynti, taajuushallinta ja muut spektrin käyttöön liittyvät toiminnot integroidaan sähkömagneettisten operaatioiden (Electromagnetic Spectrum Operations, EMSO) alle. Tavoitteena on varmistaa koko ajan ahtaammaksi käyvän sähkömagneettisen spektrin tehokas käyttö sekä taata asevoimille riittävät operointivapaudet tässä sodankäynnin keskeisessä ulottuvuudessa. Vastustajien lisäksi asevoimien spektrin käyttöä rajoittaa koko ajan kasvava kaupallinen käyttö sekä viranomaisrajoitukset. Nämä vaarantavat asevoimien kyvyn nähdä, johtaa, liikkua, suojautua ja käyttää voimaa. Toiminnanvapauden luominen edellyttää uudenlaista ajattelutapaa sen suhteen, miten sähkömagneettista spektriä käytetään ja sen rajallista tilaa jaetaan sekä eri käyttäjien, että eri käyttötarkoitusten kesken.

Sähkömagneettinen spektri on kiistetty, ruuhkainen ja rajoitettu (contested, congested, constrained), Vastustaja pyrkii kiistämään omaa spektrin käyttöämme tiedustelemalla, valvomalla ja paikantamalla järjestelmiä käyttäviä joukkojamme sekä heikentämään, estämään ja tuhoamaan niiden toimintakykyä. Spektriä hyödyntävien järjestelmien runsauden vuoksi järjestelmät aiheuttavat toisilleen myös tahattomia häiriöitä. Spektrin ahtautta lisäävät sekä kansainväliset että kansalliset määräykset, jotka rajaavat asevoimien oikeutta käyttää spektrin eri alueita.

Yhdysvalloissa sähkömagneettinen spektri nähdään nykyisin tilaksi, jossa sotaa käydään. Siis ympäristöksi, jossa asevoimat ovat läsnä, liikkuvat, havaitsevat, suojautuvat ja vaikuttavat niin kuin fyysisessäkin tilassa. Ja samoin kuin maalla, merellä ja ilmassa, myös spektrissä on omien joukkojen lisäksi vastustajan joukkoja, liittolaisia ja siviilejä, jotka on otettava huomioon omassa suunnittelussa ja tilanteen mukaisessa johtamisessa.

Miten elektronisen sodankäynnin käy?

Elektroninen sodankäynti on ratkaissut monen taistelun tuloksen siitä asti kuin sodassa on hyödynnetty elektronisia laitteita ja sähkömagneettista spektriä. Ensimmäisenä merkittävänä ELSOn kontribuutiona taistelun, operaation ja lopulta koko sodan lopputulemaan pidetään Tsushiman meritaistelua vuonna 1905. Se joka päätyi Venäjän Itämeren laivaston tuhoon. Tappio aiheutti tyytymättömyyttä ja osoitti tsaarin asevoimien haavoittuvuuden. Se johti osaltaan vallankaappaukseen ja mahdollisti Suomen itsenäistymisen. Japanilaiset olivat paikantaneet venäläisten alukset ja paljastaneet operaatioajatuksen venäläisten heikon radiokurin vuoksi. Japani hallitsi ELSOn ja voitti sodan.

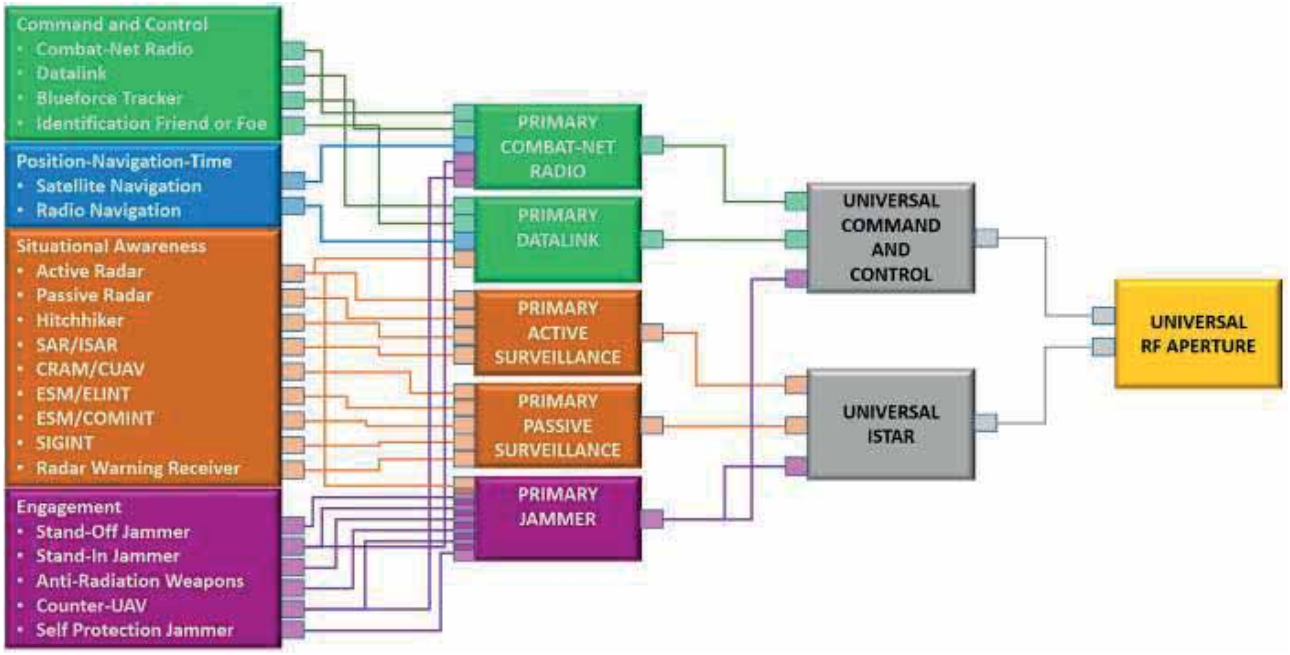
Sama asetelma toistui vuosikymmen myöhemmin, kun saksalaisten radiotiedustelu kykeni Tannenbergissä selvittämään venäläisten kahden armeijan ryhmityksen ja etenemisaikataulun. Radioliikennettä seuraamalla oli saatu tieto venäläisten armeijoiden komentajien äärimmäisen heikoista keskinäisistä väleistä. Saksalaiset kykenivät laskemaan sen varaan, että toinen komentaja ei tulisi toisen avuksi. Tämä mahdollisti sen, että saksalaiset kykenivät lyömään ensin toisen ja sitten toisen armeijan ennen kuin venäläisvoimat ehtivät yhtyä.

Toisessa maailmansodassa Midwayn meritaistelu käänsi Tyynenmeren sodan kulun lopullisesti amerikkalaisten hyväksi. Amiraali Nimiz tiesi USA:n signaalitiedustelun perusteella japanilaisten hyökkäyksen ajankohdan sekä hyökkäyksessä käytettävät joukot. Hän kykeni näillä tiedoilla ryhmittämään joukkonsa oikeaan aikaan japanilaisten todennäköisintä toimintavaihtoehtoa vastaan. Operaation lopputuloksena Japanin laivasto menetti neljä lentotukialustaan. Menetysten vuoksi Japani joutui luopumaan hyökkäyksestä Midwaylle, ja aloite Tyynenmeren sodassa siirtyi lopullisesti amerikkalaisille.

Elektronista sodankäyntiä on menestyksekkäästi hyödynnetty maailmansotien jälkeenkin. Elektronisen tiedustelun ja valvonnan keinoin on havaittu ja paikannettu vastustajan joukot sekä selvitetty niiden aikeita. Elektronisella häirinnällä on estetty vastustajaa hyödyntämästä omia elektronisia järjestelmiään ennen kaikkea ilmapuolustuksessa.

Sähkömagneettinen spektri on ilmaa, avaruutta ja kyberiä vanhempi toimintaympäristö, jossa käytävällä taistelulla on saavutettu merkittäviä voittoja. On kuitenkin nähtävissä, että teknologisen kehityksen myötä jotkut elektronisen sodankäynnin muodot tulevat tiensä päähän tai ne on ainakin toteutettava täysin eri tavoin kuin nykyisin.

Ensimmäinen muutokseen johtava tekijä on ELSOn kohdejärjestelmien digitalisoituminen. Siirtyminen analogiakalustosta digitaaliseen mahdollistaa sekä radiosignaalin että sen sisältämän datan suojaamisen niin, ettei viestintää ole mahdollista salakuunnella. Siten perinteinen viestitiedustelu (COMINT, communications Intelligence) marginalisoituu ja lopulta häviää. Vastaavasti digitaalisten lähetteiden yleistyminen johtaa signaalin piirteiden havainnointiin ja tunnistamiseen



perustuvan elektronisen tiedustelun (ELINT, Electronic Intelligence) ja sen taktisen pikkusisaren elektronisen tuen (ES, Electronic Support) merkityksen kasvuun, ainakin joksikin aikaa. Elektronisen tuen kyky tunnistaa havaitsemiaan järjestelmiä perustuu pitkälti signaalikirjastoihin, joiden avulla tietynlaisten piirteiden yhdistelmän omaava järjestelmä tunnistetaan oikeaksi kohteeksi. Kehityksen myötä tiedusteltavat järjestelmät ovat tulevaisuudessa ohjelmistopohjaisia, eli niiden lähettämät signaalit eivät ole "kovakoodattuja", vaan ohjelmistolla luotuja. Ohjelmistollinen toteutus mahdollistaa signaalin piirteiden muokkaamisen niin, että signaalikirjastot eivät pysy perässä.

Teknologinen kehitys ja potentiaalisen vastustajan kyky hyödyntää sitä vievät edellytykset nykyisen kaltaiselta taktiselta elektroniselta tiedustelulta ja valvonnalta. Yhtään sen paremmin ei käyne elektroniselle vaikuttamiselle. Signaalin piilottaminen hajaspektritekniikoilla estää häirinnän tarkan kohdistamisen, jolloin häirinnän teho laskee. Tilanteen mukaan muotoaan muuttavat ohjelmistopohjaiset signaalit estävät älykkään häirinnän ja pakottavat käymään tehotasokilpailua vastustajan järjestelmien kanssa. Siinä häiritsijän on turvauduttava laajakaistaiseen kohinahäirintään, joka on älykästä häirintää tehottomampaa pakottaen lyhentämään häirintäetäisyyttä.

Ennen pitkää tullaan siis tilanteeseen, jossa omien joukkojen selustassa toimivat sensori- ja häirintäjärjestelmät menettävät merkityksenä. Loppuuko ELSOn menestystarina siihen? Voi hyvinkin loppua, jos elektroninen sodankäynti ei saa uusia muotoja. Ratkaisu voisi löytyä ajatuksesta, että jos kalliit ja harvalukuiset etulinjan takana toimivat järjestelmät eivät ole oikea ratkaisu, siirrytään halvempiin, runsaslukuisempiin ja etulinjassa tai sen edessä vastustajan syvyydessä operoiviin ratkaisuihin.

Konvergenssin myötä yhä suuremmalla joukolla erilaisia viesti- ja sensorijärjestelmiä on kyky toimia myös elektronisen sodankäynnin roolissa. Jos esimerkiksi kenttäradio kykenee havaitsemaan ja paikantamaan vastustajan radiolähetteitä sekä häiritsemään niitä, käytettävissä on elektronisen sodankäynnin kyvykkyyksiä ilman ELSO-järjestelmiä. Jos kehitys kulkee tähän suuntaan, ELSO joukkoistuu ja arkipäiväistyy. Tämän myötä ELSOn toiminnallisuuksilla ja alan osaamisella on suurempi merkitys, vaikka alan erikoisvälineistö saattaakin hävitä. Keskeiseksi muodostuu elektronisen sodankäynnin yhteisön kyky ennakoida tulevaa ja mukautua muutokseen. Tämän johdosta sähkömagneettinen ulottuvuus

tulisi nähdä strategisena asiana, jossa resursointi-, priorisointi-, koordinointi- ja dekonfliktointipäätökset on tehtävä konsernitasolla.

Nykykäytäntö, jossa spektrin käyttöä ohjataan ja koordinoidaan jakamalla eri toimijoiden käyttöön taajuusalueita hallinnollisina päätöksinä, ei ole ollut järkevää enää moniin vuosiin. Taajuuksienjakobyrokratiasta tulee siirtyä dynaamiseen aikaan ja paikkaan sijoittuvaan spektrin yhteiskäyttöön (spectrum sharing), jossa epätoivottavat keskinäishäiriötilanteet hallitaan tapauskohtaisesti. Tätä varten on paitsi kehitettävä protokollat ja prosessit, myös luotava johtamis- ja koordinointirakenteet ja toimintatavat. Koneiden kognitiivisten kykyjen kehittymisen myötä niin radio kuin tutkakin tietävät ihmistä paremmin ja ennen kaikkea nopeammin millä taajuudella ja teholla, milloin ja mihin suuntaan niiden kannattaa lähettää oma tehtävä, uhka ja sivulliset huomioiden. Tällöin ihmisen rooli muuttuu taajuustaulukon lukijasta ja käyttötaajuuksien veivaajasta tehtävän päättäjäksi ja pelisääntöjen asettajaksi.

Pentagonin spektristrategia sisältää viisi strategista tavoitetta: 1) havainnointiin, tilannekuvan muodostamiseen, spektrin yhteiskäyttöön ja toimintavapauksien varmistamiseen tarvittavien teknologioiden kehittäminen. Tämä käsittää sekä siviiliteknologioiden ketterän hyödyntämisen, että vallankumouksellisten sotilasteknologioiden kehittämisen. 2) sähkömagneettisen spektrin integroiminen operatiiviseen suunnitteluun ja johtamiseen, sekä tähän liittyvä tiedustelutuki ja arkkitehtuurien hallinta. 3) henkilöstön osaamisen ja joukkojen valmiuden kehittäminen integroimalla sähkömagneettinen ulottuvuus muuhun koulutukseen ja harjoitteluun sekä varmistamalla alan henkilöstölle kilpailukykyiset urakehitysmahdollisuudet. 4) kumppanimaiden kykyjen kehittäminen, hyödyntäminen ja yhteensopivuuden varmistaminen, 5) hallinnonlaajuisen ohjausmekanismin luominen. On selvää, että näin merkittävän ja puolustushaararajat ylittävän asian läpivienti edellyttää riittävää senioriteettia keskushallinnossa sekä konkreettisen kehittämisen tiekartan laadintaa.

Sota avaruudessa

- sotilasvirkamies 3.lk Mathias Fontell -

Kirjoittaja palvelee Ilmavoimien esikunnan suunnitteluosastolla avaruussuorituskykyjen teknisenä asiantuntijana ja avaruustilannekuvan hankevalmistelijana.

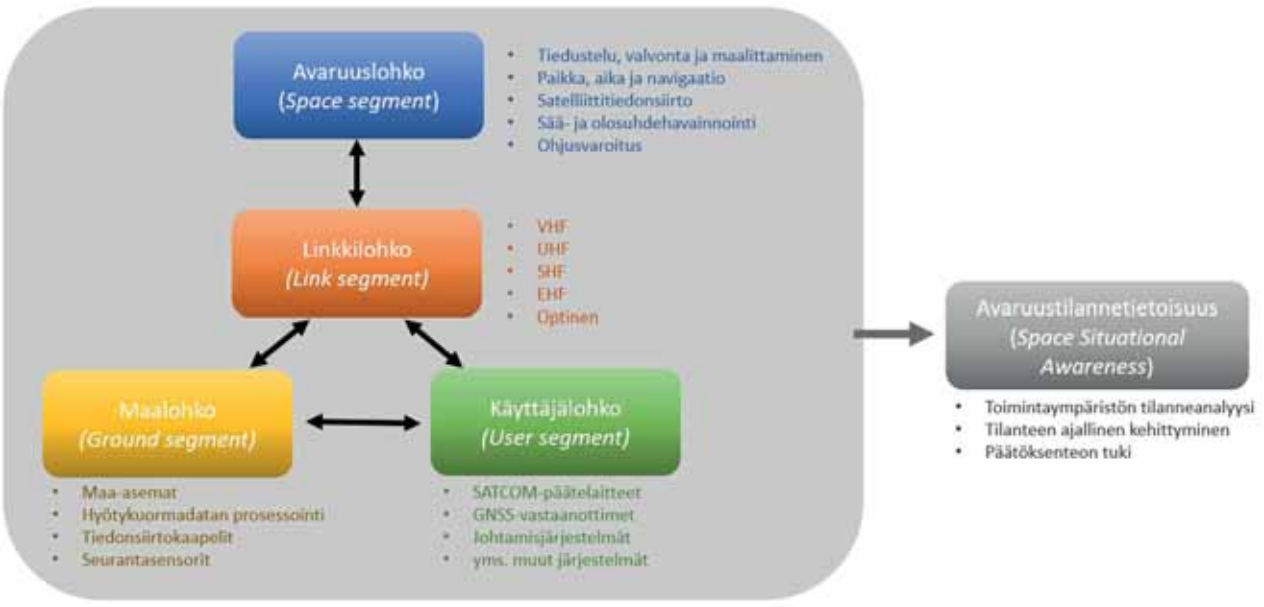
Avaruudesta kuulee usein puhuttavan sodan uutena ulottuvuutena. Toisaalta mikäli avaruuden kuuluminen sodan yhdeksi toimintaympäristöksi määritellään alkavan siitä, kun avaruuteen sijoitetut järjestelmät ensimmäisen kerran tulivat osaksi jonkin puolustusjärjestelmän suorituskykyä, voidaan avaruuden nähdä kuuluneen osaksi sodankäyntiä ainakin vuodesta 1959 lähtien kun Yhdysvallat laukaisi ensimmäiset CORONA--sotilastiedustelusatelliitit. Sotilaallisen avaruustoimintaympäristön voidaan myös nähdä saaneen alkunsa jo 1940-luvulla pian toisen maailmansodan jälkeen, kun Neuvostoliitto ja Yhdysvallat aloittivat kantorakettien kehittämisohjelmansa ja laativat ensimmäiset konseptinsa avaruuteen sijoitetuille, sotilaalliseen käyttöön tarkoitetuille laitteille. Riippuen siis hieman määritelmästä, on avaruus ollut yksi sodan ulottuvuuksista jo yli 60 vuotta eli heti avaruusajan alusta alkaen.

Avaruuden sotilaallinen ulottuvuus onkin ollut etenkin suurvalloille hyvin merkittävä ensimmäisistä satelliiteista alkaen, jotka suunniteltiin ensisijaisesti tiedustelemaan vastustajan ydinohjusten ja pommikoneiden lukumäärää ja sijoituspaikkoja sekä paikantamaan omien pintaan nousevien ydinsukellusveneiden sijainnit ennen ohjuslaukaisua. Teknologian kehittyessä satelliiteille löydettiin käyttöä muihinkin käyttötarkoituksiin, kuten satelliittitiedonsiirtoon, säähavainnointiin, ohjusvaroitukseen, ja ydinräjähdysten valvontaan. Vaikka satelliittien käyttö on paljon aiempaa laajempaa, kaikki nämä käyttötarkoitukset ovat edelleen myös nykyään tärkeitä.

Avaruuden kaupallistuminen – määrä korvaa laadun?

1990-luvun alkupuolelle asti valtaosa satelliiteista laukaistiin Yhdysvaltojen ja Neuvostoliiton viranomais- ja sotilaskäyttöön. Nykyään tilanne on erilainen, sillä muun muassa laukaisujen ja satelliittitekniikan halpeneminen, teknologian miniatyrisointi ja satelliittipalvelujen lähes räjähdysmäinen kaupallistuminen on avannut ovet pienemmille valtioille sekä yrityksille joko hyödyntää omia satelliitteja tai satelliittien tuottamaa kykyä ostopalveluina.

Vuonna 2011 laukaistuista satelliiteista vain noin 20 % oli kaupallisiin tarkoituksiin rekisteröityjä, kun vuonna 2021 vastaava luku oli yli 90 %. Vastaavasti vuonna 2011 yksi laukaisu vei keskimäärin vain hieman alle kaksi hyötykuormaa kiertoradalle, kun nykyään mm. satelliittien miniatyrisoitumisen ja laukaisujen kilohinnan alenemisen johdosta yksi laukaisu vie kiertoradalla keskimäärin noin 13 hyötykuormaa. Joissakin asioissa määrä korvaa laadun, ja sotilaskäytössäkin tiettyihin käyttötarkoituksiin voi olla nykyään merkittävästi kustannustehokkaampaa ostaa kapasiteettia olemassa olevasta kaupallisesta konstellaatiosta kuin rakentaa, laukaista ja operoida itse omia satelliitteja.



Kuluneen parin vuosikymmenen aikana tapahtuneet muutokset avaruudessa toiminta-ympäristönä ovat niin merkittäviä, että muutokset aiheuttavat perusteellisia muutoksia avaruussuorituskykyjen arkkitehtuureissa ja niiden käyttöperiaatteissa. Menneen aikakauden isot, kalliit, ja lukumäärällisesti pienet konstellaatiot korvataan osittain suuremmilla konstellaatioilla, jotka koostuvat pienemmistä ja halvemmista yksiköistä. Yksittäiset satelliitit ovat haavoittuvaisia, mutta hajauttamalla ja käyttämällä monimuotoisia hyötykuormia sekä nopeuttamalla käyttöönottoa parannetaan järjestelmän häiriönsietokykyä. Näin järjestelmän suorituskyky ei romahda, vaikka sen yksittäiset solmut vikaantuisivat tai tuhoutuisivat. Sadoista tai tuhansista satelliiteista koostuvat verkottuneet, matalalle kiertoradalle sijoitetut isot konstellaatiot tunnetaan nykyään uudella termillä PLEO eli Proliferated Low Earth Orbit. Ukrainan sodassakin paljon julkisuutta saanut SpaceX:n Starlink-konstellaatio (joka muuten muodostaa tätä artikkelia kirjoittaessani noin 45 % kaikista kiertoradalla sijaitsevista aktiivisista satelliiteista) on malliesimerkki PLEO-konseptista.

Toisena esimerkkinä voidaan mainita Yhdysvaltojen avaruusvoimien tulevat suunnitelmat korvata korkeilla (GEO) radoilla sijaitsevat ohjusvaroitussatelliitit suuremmalla matalan (LEO) kiertoradan konstellaatiolla, parantaen järjestelmän resilienssiä entiseen verrattuna. Ajattelutapa ”määrä korvaa laadun” näkyy myös avaruusteollisuuden tuotanto-ketjuissa, joissa pyritään nopeisiin kehitys-sykleihin ja suuriin tuotantovolyymeihin laadunvarmistuksen kustannuksella. Palvelun-tarjoajaa (eikä loppuasiakasta) haittaa välttämät-tä, jos yksi satelliitti vikaantuu kymmenien tai satojen joukossa – erityisesti jos suhteellisen halvalla voidaan rakentaa ja laukaista uusi vastaava tai jopa suorituskykyisempi satelliitti teknologian nopean kehityksen johdosta.

Avaruusjärjestelmä on muutakin kuin satelliitteja

Mitä oikeastaan tarkoitetaan termillä avaruus-sijoitteinen suorituskyky? Olipa määritelmä mikä tahansa, on tärkeää ymmärtää, että suorituskyvyn tuottava järjestelmä ei koskaan koostu pelkästään satelliiteista. Avaruussijoit-teinen suorituskyky (space-based capability) voidaan jakaa avaruuslohkoon (space segment), linkkilohkoon (link segment), maalohkoon (ground segment), ja lisäksi vielä käyttäjä-lohkoon (user segment). Avaruuslohko koostuu satelliiteista ja näiden osajärjestelmistä – ennen kaikkea hyötykuormista (payload), joilla suorituskyky (esimerkiksi tiedonsiirto- tai kaukokartoituspalvelu) tuotetaan. Maalohko

koostuu pääsääntöisesti satelliittien operointiin ja seurantaan käytettävistä maa-asemista, hyötykuormadataa prosessoivista konesaleista, tiedonsiirtokaapeleista, ja satelliittien seurantaan käytettävistä sensoreista (kuten tutkista). Linkkilohkolla tarkoitetaan kaikkea sähkömagneettista säteilyä, jolla avaruus-, maa- ja käyttäjälohkot yhdistetään toisiinsa. Käyttäjälohko sisältää käyttäjät ja järjestelmät, jotka hyödyntävät avaruussijoitteista suorituskykyä, esimerkiksi vastaanottamalla GNSS-satelliittien paikannussignaalia, analysoimalla kuvaussatelliiteilla muodostettua tiedustelutietoa, tai liittymällä satelliittitiedonsiirtoverkkoon omalla päätelaitteellaan.

Sodan moniulotteisuus näkyy hyvin selkeästi yllä esitetyssä avaruussuorituskyvyn toiminnallisessa jaottelussa. Avaruussijoitteinen suorituskyky sisältää aina maa- ja linkkilohkojen kautta keskeisiä palasia kaikissa muissa toimintaympäristöissä (maa, meri, ilma, kyber, spektri), ja näiden toimintaympäristöjen lainalaisuudet ja keskinäisvaikutukset tulee ymmärtää osana isompaa kokonaisuutta.

Kyberhaavoittuvuus maalohkon maa-asemassa tai häirintä linkkilohkon kriittisessä osassa spektriä voi kiistää avaruussuorituskyvyn käytön samalla vaikutuksella kuin jos avaruuslohkoon kuuluviin satelliitteihin vaikutettaisiin kineettisesti. Kyberin ja elektronisen sodankäynnin avulla vaikuttaminen voi olla jopa merkittävästi kustannustehokkaampaa, helpompaa toteuttaa, ja ennen kaikkea hyökkääjän osoittaminen voi olla vaikeampaa. Esimerkkinä tästä on helmikuussa 2022 tapahtunut laaja kyberhyökkäys Ukrainan asevoimien ja viranomaisten käyttämään kaupalliseen Viasat-satelliittilaajakaistapalveluun, jonka uutisoitiin lamaannuttaneen tuhansia päätelaitteita Ukrainassa ja Keski-Euroopassa asti. Hyökkääjän ei tarvinnut vaikuttaa satelliitteihin itsessään, ja Venäjän on ollut helppoa (vaikka ei kovin uskottavaa) kieltää osallisuutensa kyberhyökkäykseen.

Mihin satelliitteja käytetään?

Avaruussijoitteisilla suorituskyvyillä voidaan merkittävästi tehostaa suorituskykyä maassa, merellä, ja ilmassa, ja tästä syystä satelliitit ovat tärkeä osa moderneja taistelujärjestelmiä. Sotilaallisesta näkökulmasta satelliittipalvelut voidaan jakaa käyttötarkoituksen perusteella viiteen kategoriaan:

1. Tiedustelu, valvonta, ja maalittaminen (Intelligence, Surveillance and Reconnaissance eli ISR)
2. Paikka, aika, ja navigaatio (Position, Navigation and Timing eli PNT)
3. Satelliittitiedonsiirto (Satellite Communications eli SATCOM)
4. Sää- ja olosuhdehavainnointi (Environmental Monitoring)
5. Ohjusvaroitus (Missile Warning)

Monet eivät välttämättä tajua, kuinka tärkeässä asemassa erityisesti paikka-, aika- ja navigaatiopalvelut (PNT) ovat nykyään koko yhteiskunnan toiminnan kannalta. GNSS-vastaanotin (Global Navigation Satellite System) joka kykenee vastaanottamaan signaalin vähintään neljästä satelliitista, kykenee määrittämään oman sijaintinsa ja kellonajan tarkasti. Sijainnin määrittäminen älypuhelimen GNSS-navigaattorin ruudulta on kaikille tuttua, mutta harvempi tiedostaa, että tämä määrittää samalla puhelimen kelloajan. Tarkkaa aikasynkronointia vaativat järjestelmät, kuten matkapuhelinverkkojen tukiasemat ja sähkönjakeluverkot, käyttävät nykyään paljon GNSS-vastaanottimia aikasynkronointiin. Vuonna 2021 arvioitiin, että maailmanlaajuisesti lähes seitsemään miljardiin laitteeseen on integroitu GNSS-vastaanotin. On edes vaikea kuvitella, kuinka suuria seurannaisvaikutuksia olisi, jos kaikki GNSS-konstellaatiot lakkaisivat yhtäkkiä toimimasta (vaikka epätodennäköinen skenaario onkin). Sotilaille tämä tarkoittaisi muun muassa kaukovaikutteisten täsmäaseiden tarkkuuden huonontumista ja langattomien johtamisjärjestelmien tiedonsiirtonopeuksen heikentymistä, ellei järjestelmiä ole varmennettu muilla ratkaisuilla. Siviiliyhteiskuntaan vaikutukset olisivat vielä merkittävämpiä, mikäli navigaattorit, matkapuhelinverkot, pankkisiirrot ja sähkönjakeluverkot lakkaisivat toimimasta.

Avaruustilannetietoisuus mahdollistaa avaruuspuolustuksen

Avaruudesta kohdistuvilta uhkilta puolustautuminen ja omien avaruussuorituskykyjen optimaalinen käyttö edellyttää avaruustilannekuvaa. Avaruustilannekuva käsittää muun muassa tiedon:

- Satelliittien käyttäjistä, käyttötarkoituksista, toimintakunnosta ja radasta
- Avaruussäästä, kuten säteilytasoista, ionosfäärin tilasta, ja avaruusmyrkyistä
- Avaruusromusta ja törmäysuhkasta omiin satelliitteihin
- Ennusteet satelliittien paluusta ilmakehään ja sirpaloitumiset avaruudessa

Avaruustilannekuva muodostetaan sekä maa- että avaruussijoitteisilla sensoreilla, kuten tutkilla, teleskoopeilla, laseretäisyysmittareilla, elektronisen tiedustelun avulla ja avaruussääinstrumenteilla. Avaruustilannekuvan pohjalta tehdyllä tilanneanalyysillä ja arviolla tilanteen kehittymisestä muodostetaan avaruustilannetietoisuus (SSA, Space Situational Awareness), joka käsittää arvion sekä omista että vihollisen avaruusjärjestelmistä menneisyydessä, nykyhetkessä, että tulevaisuudessa. Avaruustilannetietoisuus mahdollistaa avaruuden huomioimisen omien operaatioiden suunnittelussa ja toimeenpanossa muissa toimintaympäristöissä. Se sisältää tiedon sekä omien että vastustajan avaruudellisten suorituskykyjen käytettävyydestä ajallisesti ja paikallisesti, ja mahdollistaa puolustautumisen uhkia vastaan kompleksisessa ja dynaamisessa toimintaympäristössä.

Avaruustilannetietoisuuden muodostaminen on nykyään hyvin haastavaa. Esimerkiksi Yhdysvalloissa asevoimien avaruusesikunta (USSPACECOM) on tähän asti ylläpitänyt maailman kattavinta julkista satelliittikatalogia ja tarjonnut ilmaista törmäyksenestopalvelua yksityisille satelliittioperaattoreille kansainvälisesti, mutta monimutkaistuva toimintaympäristö ja nopeasti kasvava satelliittien lukumäärä kuormittaa enenevissä määrin asevoimien henkilöstöä ja sensorikapasiteettia. Seurauksena perinteisesti asevoimien ylläpitämiä avaruusliikenteen hallintatoimintoja (STM, Space Traffic Management) ollaan siirtämässä siviiliviranomaisille, jotta asevoimien kapasiteettia voidaan vapauttaa sotilaallisen avaruustilannetietoisuuden muodostamiseen.

Myös Suomessa sotilas- ja siviiliviranomaisten yhteistyötä avaruustilannetietoisuuden muodostamisessa on odotettavissa. Valtioneuvoston vuoden 2021 puolustusselonteossa mainitaankin, että ”Puolustusvoimat kehittää kykyään ympärivuorokautisen avaruustilannekuvan ylläpitämiseen yhteistyössä muiden viranomaisten ja kansainvälisten kumppanien kanssa”. Puolustusvoimat on ollut vuodesta 2020 lähtien tiiviisti mukana poikkihallinnollisen avaruustilannekuvan kehittämisessä. Lokakuussa 2022

liikenne- ja viestintäministeriö perusti avaruustilannekeskuksen ohjausryhmän, jonka tehtävänä on selvittää poikkihallinnollisesti kansallisen avaruustilannekeskuksen perustamista.

Oma toimintaympäristö vaatii sille omistautumista

Avaruus on oma sodankäynnin toimintaympäristö lainalaisuuksineen ja erityispiirteineen, joiden hallitseminen vaatii henkilöstön koulutusta ja organisoitumista. Puolustusvoimat eivät välttämättä tarvitse omaa avaruuspuolustushaaraa, mutta suorituskyvyn kehittäjän näkökulmasta on nykyinen avaruuteen vihkiytyneen henkilöstön määrä liian vähäinen ja kokonaisuuden koordinointi pirstaloitunutta. Kyetäksemme vastaamaan uhkaympäristön vaatimuksiin tulee uhkaympäristö ensin ymmärtää, mutta avaruuden tekniset, operatiiviset ja poliittiset ulottuvuudet ovat muuttuneet niin monimuotoisiksi, että toimintaympäristön hallitseminen ei ole mahdollista Puolustusvoimien henkilöstön omien tehtävien ohella.

Tästä huolimatta minulla on täysi luottamus ammattitovereideni, insinööriupseerien sekä koko Puolustusvoimien henkilöstön oppimiskykyyn ja ammattitaitoon sen osalta, että avaruus saadaan haltuun puolustusvoimallisesti. Avaruus on toimintaympäristönä muuttunut merkittävästi ensimmäisistä avaruuslennoista 60 vuotta sitten, ja tulee muuttumaan paljon seuraavienkin vuosikymmenien aikana. Puolustuksen vuorovaikutussuhteet avaruusjärjestelmiin tulevat vain lisääntymään entisestään, ja uuteen uhkaympäristöön vastaaminen vaatii, että avaruus tunnistetaan omana toimintaympäristönään samalla vakavuudella kuin nykyään maa, meri, ilma, ja kyber.

Sota tietoverkoissa

- Insinöörieversti Janne Jokinen -

Alkuprovokaatio: Keskiajalla Suomi kuulemma kuului Ruotsin alaisuuteen, mutta alussa valtio oli läsnä vain herrain linnoissa. Kansalaisten tärkeisiin asioihin periferiassa valtio ei juurikaan sotkeutunut. Aina välillä kulkutauti tappoi ja vainulainen hätyytteli, mutta valtio ei näissä ehtinyt tai osannut auttaa. Pystyi vain toteamaan, että oho. Oho, Kiina varasti taas keskeistä kansallista osaamispääomaamme. Oho, Venäjä härkki taas kriittisen infrastruktuurin kontrolleissa. Olemmeko ajautuneet digitaaliselle keskiajalle?

Kybersota Ukrainassa

Venäjän hyökättyä Ukrainaan helmikuussa 2022 ei tullutkaan manattua kyber-Pearl-Harboria, vaan Ukrainan tietoverkot jatkoivat toimintaansa hämmästyttävän hyvin. Jotkut ovat vetäneet tästä johtopäätöksiä kybersodankäynnin vähäisestä merkityksestä, mutta fiksuimmat sentään tajusivat, että ei Venäjän hyökkäyssodasta pidä vetää liikaa johtopäätöksiä myöskään ilmasodankäynnin tulevaisuudesta.

Ukraina on ollut vähintään vuodesta 2014 Venäjän jatkuvien kyberhyökkäysten kohde ja oli Venäjän viimeisimmän hyökkäyksen alkaessa Euroopan johtava kyberturvallisuusmaa. Ukraina oli valmistautunut kybersotaan määrätietoisesti, läntisten kumppaneidensa avustamana, ja on kyennyt taitavasti suojautumaan Venäjän hyökkäyksiltä. Näistä Venäjän kyberhyökkäyksistä ei ole ollut pulaa, ja ne ovat osin levinneet myös muihin maihin

Ukraina on ollut myös mallimaa uusimpien teknologioiden hyödyntämisessä sodankäynnissä. Tätä on ollut miehittämättömien taistelulavettien kehittäminen, mutta myös mm. mobiili- ja satelliittiverkkojen sekä kännykkäsovellusten hyödyntäminen moneen. Ukraina on myös kyennyt mobilisoimaan vapaaehtoisia ”kyberpartisaaneja” venäläisiä kohteita vastaan ja maalittamaan näitä toimia.

Keskeinen Ukrainan demonstroima opetus kyberpuolustukselle on ollut läntisten teknologiayritysten rooli Venäjän operaatioiden selvittämisessä ja Ukrainan suojaamisessa. Microsoftin ja Googlen kaltaisilla yrityksillä on ainutlaatuinen näkymä globaaliin internetin rakenteeseen ja eri toimijoiden askareisiin, jota tietoa hyödyntämällä voidaan myös valtiollisista kyberoperaatioista saada tarkkaa tietoa. Samoin suuret kyberturvallisuusyritykset keräävät valtavasti telemetriaa. Yksittäisten valtioiden on vaikeaa kyetä vastaavaan sensorointiin, ja tulevaisuudessa yhä enenevissä määrin yritysten ja länsimaiden täytyy yhdessä liittoutua kyberpuolustukseen pahuutta vastaan.

Ukrainan kokemuksista tulisi ottaa opiksi myös Suomessa. Tietoverkkojen ja tietojärjestelmien operointia tulee kehittää varautuminen prioriteettina, ja kyberpuolustuksen dynaamisuuteen täytyy panostaa. Koko kansallisen potentiaalin tulee tarvittaessa olla nopeasti mobilisoitavissa kansakunnan puolustamiseen.

Valitettavasti syksyä kohti Venäjä siirtyi fyysisesti tuhoamaan sähköverkkoja ja muuta Ukrainan kriittistä infrastruktuuria. Sähkön merkitys korostuu tietoverkoissa, ja resilienssi sähköverkkojen suhteen onkin kriittistä. Myös kyberissä, kuten elektronisessa sodankäynnissä, ”hard kill” tuottaa pidemmän vaikutuksen.

Digitalisaatio

Suomi on digitalisaation kärkimaita. Koronapandemian aikainen nopea siirtymä etätöihin kouluissa ja työpaikoilla osoitti edistystämme tietoteknisissä valmiuksissa ja ratkaisuissa. Pahin rangaistus teineille on WLAN-salasanan muuttaminen, etenkin kun samalla klikkaa kännykkäliittymien hallintasovelluksesta

Jonnen mobiilidatan pois päältä. Elämämme siirtyy kännykkäsovelluksilla hallituksi, ja samoin yhteiskuntamme toimintoja ohjataan digitaalisin ratkaisuin – valtaosin julkisiin tietoverkkoihin kytkeytyen. Kotivarana kehotetaan pitämään käteistä, mutta Prisman kassa ei hevin säntäile katsomaan hintoja hyllynreunasta, mikäli kassapääte ei toimi. Mikäli tietojärjestelmät lamautuvat, yhteiskuntamme lamaantuu ja etenkin talvella ihmisiä alkaa kuolla.

Digitalisaation hyödyt ovat tietenkin valtavat. Monet klassiset ammatit ovat tehostuneet tai jopa poistuneet, ja tulevaisuudessa Suuren Datan käsittely tuottaa paljon lisäarvoa. Kun kaikkea sensoroidaan, tekoäly louhii sellaistakin tietoa jota ihmissilmä ei havaitse. Kybersodankäynnin lisäksi tämä synnyttää uusia sodankäynnin muotoja, kuten hyökkäykset itse tekoälyä vastaan saastutetulla opetusdatalla tai ovelasti valitulla harhauttavalla hyötydatalla. Siihen on vielä matkaa, mutta itse ohjautuvien autojen jekuttaminen on jo lähellä.

Puolustusvoimissa velmuilijat ovat esittäneet, että siinä sitä olisikin ensimmäinen askel sotilaalliselle tekoälylle, kun löytäisimme asiakirjan asianhallintajärjestelmästä asiakirjan diaarionumerolla. Puolustusvoimien tietojärjestelmiä luonnehtii valtava kompleksisuus; kyseessä on valtakunnan monimutkaisin tietojärjestelmäkokonaisuus, jota on kunnianhimoisesti kehitetty yhä laajemmaksi rajallisin resurssein.

Tavanomaisen toimisto-ATK:n lisäksi Puolustusvoimissa tietotekniikka on integroitu taistelujärjestelmiin ja moninaisiin liikkuviin lavetteihin, tietoa täytyy suojata lukuisissa eri tietoturvaluokissa, asejärjestelmät vaativat tarkkoja navigaatiolähetteitä, valvonta- ja muuta sensoridataa on valtavasti, toiminta täytyy skaalata 280 000 hengen kokonaisvahvuuteen, jne. Käytössä on monenlaista ”vaikeaa-ATK:ta”, johon ei löydy osaamista juurikaan siviilistä. Tästä eri puolustushaarojen ja yhteisen johtamisen kudelmasta muodostuu kokonaisuus, jota ei hallitse kokonaisuutena kukaan. Silti Puolustusvoimien johtamisjärjestelmät täytyy kyetä suojaamaan; pitämään toiminnassa ja suojattuina kaikissa olosuhteissa, pommien räjähtäessä yllä, sähköpulassa, ja vastustajan kyberhyökkäysten alaisena.

Puolustusratkaisussamme maanpuolustus on integroitu tiiviisti siviiliyhteiskuntaan. Sähköhuolto, tietoliikenne, logistiikka, kenttäsairaanhoito ja monet muut vastaavat toiminnot on rakennettu pääosin siviiliyhteiskunnan ratkaisuja hyödyntäen. Tämä on kustannustehokasta ja pienelle kansalle viisasta, mutta altistaa puolustusjärjestelmää sen siviilikomponentin kyberturvallisuus- ja muille riskeille. Mikäli sähkö loppuu yhteiskunnasta, varavoima ehkä puksuttaa, mutta loputtomiin sekään ei pidä 2020-luvun Puolustusvoimia toiminnassa.

Puolustaako Puolustusvoimia?

Suomen ensimmäinen kyberturvallisuusstrategia laadittiin vuonna 2013. Strategian kirjaukset olivat niin aikaansa kestäviä, että ne on syytä kaivaa esiin vielä kymmenisen vuotta myöhemmin:

Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.

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

Edellä mainittujen tehtävien täyttämiseksi laaditaan puolustusministeriön johdolla Puolustusvoimille tarvittava toimivaltuussäännöstö. Tunnistetut puutteet toimivaltuussäädöksissä korjataan lainsäädäntötoimenpitein.

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

Kyberpuolustuksen kehittäminen alkoi systemaattisesti näiden kirjausten jälkeen, ja Puolustusvoimissa onkin käynnissä pitkä kehittämisohjelma kyberpuolustuksen henkilöstön ja järjestelmien kehittämiseksi. Suorituskykyjä on rakennettu tiedustelun, vaikuttamisen ja suojautumisen osa-alueilla. Kaikkea ei kuitenkaan ole saatu kattavasti syntymään; useita vuosia valmisteltu sotilastiedustelulainsäädäntö oli kriittistä myös kyberpuolustuksen kannalta, mutta riittävän laajaa lainsäädäntötyötä ei kyetty tunnistamaan ja käynnistämään heti strategiatyön jälkeen. Monia muitakin haasteita on edelleen ratkottavaksi.

Kyberpuolustuksen ymmärtäminen on mahdotonta pääkaupungissa vain juristerian tai muun generalian kautta. Tekninen syväsukellus on välttämätöntä. On helppoa hokea tilannekuvan tärkeyttä, kehua että tietoahan vaihdetaan tai että senkun vaan kyberissä ”ammutaan gigabitin tykillä” kun käsky tulee – mutta mikäli edes kohtuullista ymmärrystä ei ole varsinaisesta kyberpuolustuksen aseenkäytöstä, ei voi ymmärtää missä yksityiskohdissa paholainen todellisuudessa asuu. Lisäksi kohdeympäristö muuttuu ja monipuolistuu jatkuvasti: Sen enempää kuin sotilaslääkäri ei osaa tehdä sodassa ampumahaavoille leikkauksia, jos vain normaalioloissa jakaa saikkua, ei myöskään kyberpuolustaja kykene toimiin, mikäli ei ole koko ajan kädet rasvassa taistelukosketuksessa haastavimpiin vastustajiin.

Ensimmäisestä kyberturvallisuusstrategiasta jäi elämään hokema, että ”Puolustusvoimat suojaa omat järjestelmänsä”. Tämä on kriittinen arvo, mutta puolustusjärjestelmän ollessa riippuvainen myös sen siviilikomponentista – yhteiskunnan kriittisestä infrastruktuurista – omaa toimintaa on mahdotonta suojella vain omassa hallussa olevia järjestelmien nurkkia suojaamalla.

Tämän vuoksi syyskuussa 2021 Puolustusselontekoon tuli seuraavia kirjauksia:

Kyberpuolustusta kehitetään niin, että sen avulla voidaan turvata paremmin paitsi Puolustusvoimien omat myös muut puolustuskykyyn suoraan vaikuttavat järjestelmät.

Puolustusvoimat on kehittänyt kybertilannekuvan muodostamista, omien järjestelmien suojaamista ja valvontaa sekä puolustuksellisten kyberoperaatioiden suunnittelua ja toimeenpanoa. Kyberpuolustuksen integrointia osaksi operatiivista toimintaa on jatkettava ja se on sisällytettävä myös kaikkien eri toimialojen, viranomaisten ja muun yhteiskunnan väliseen tiiviiseen yhteistyöhön.

Suomen sotilaallinen puolustus on riippuvainen yhteiskunnan infrastruktuurista ja Suomen puolustus hyödyntää kumppaneiden palveluita kaikissa turvallisuustilanteissa. Tästä syystä niiden toiminnan jatkuvuus on turvattava.

Puolustuksen kehittämisessä varmistetaan kyky valvoa kaikkia toimintaympäristöjä – maa, meri, ilma, kyber- ja informaatioympäristö sekä avaruus – ja tarvittaessa käynnistää puolustuksen edellyttämät toimenpiteet.

Puolustusvoimat vastaa Suomen sotilaallisesta kyberpuolustuksesta osana kansallista kyberturvallisuutta. Kyberpuolustukseen kuuluvien suojautumisen, tiedustelun ja vaikuttamisen tavoitteena on turvata sekä Puolustusvoimien omat että muut puolustuskykyyn suoraan vaikuttavat järjestelmät erityisesti valtiollisilta uhkatoimijoilta ja niiden edustajilta, siten, että Puolustusvoimat kykenee suoriutumaan lakisääteisistä tehtävistään. Puolustusvoimilla on velvollisuus torjua maanpuolustukseen ja puolustusjärjestelmään kohdistuva tietoverkkotiedustelu sekä kyberhyökkäykset etenkin silloin, kun kyseessä on valtiollinen toimija. Kyberpuolustus toteutetaan yhteistoiminnassa kansallisten ja kansainvälisten turvallisuusviranomaisten kanssa, ja Puolustusvoimat tukee kyberturvallisuudessa muita viranomaisia antamalla virka-apua.

Selonteossa linjattiin lisäksi seuraavasta selvitystyöstä, joka on tätä kirjoitettaessa vielä kesken:

Kybertoimintaympäristön uhkia ja niihin liittyviä kansallisia kehittämistoimia arvioidaan

kyberturvallisuusstrategian kehittämisohjelmassa sekä käynnistettävässä selvitystyössä, jossa arvioidaan viranomaisten toiminta-edellytykset kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, ja kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa. Selvitystyön perusteella käynnistetään kyberpuolustuksen kehittämistoimenpiteet, mukaan lukien tarvittava säädösvalmistelu. Toimenpiteiden tavoitteena on varmistaa turvallisuusympäristön edellyttämät kyberpuolustuksen toimivaltuudet, osaaminen ja riittävät tiedonsaantioikeudet.

Tavoitteena siten on, että ”suojaa omat järjestelmänsä” -ajattelusta kehitytään ”turvaamaan myös muut puolustuskykyyn suoraan vaikuttavat järjestelmät”. Kaltaisessamme yhteiskunnassa ja puolustusjärjestelmässä tästä syntyy kuitenkin vuorovaikutusketju, jolle ei ole loppua. Niinpä Puolustusvoimat ei viime kädessä voi suojata koko puolustusjärjestelmää, vaan toiminnan täytyy perustua eri viranomaisten, yksityisten yritysten ja jopa kolmannen sektorin tiiviiseen yhteistoimintaan. Kriittistä on kuitenkin kehittää ja velvoittaa tämä yhteistoiminta sellaiselle riittävän teknisen ja yksityiskohtaisen toiminnan tasolle, jolla on todellista vaikuttavuutta.

Mikäli tässä onnistutaan, kyetään samalla kehittämään myös koko Suomen kyberpuolustamisen ideaalia.

Venäjä ja Nato

Tätä kirjoitettaessa talven pakkanen vasta kerää voimiaan, ja sähkön riittävyyttä arvuutellaan. Venäjä on aggressiivisesti tuhonnut Ukrainan kriittistä infrastruktuuria, ja länsimaissa on jännätty, millaisiin hybridivaikuttamisen toimiin Venäjällä on intoa länsimaita vastaan. Venäjän tiedustelupalvelut ovat viime vuosina kyenneet erittäin taitaviin operaatioihin länsimaissa, mutta toisaalta etenkin Yhdysvallat on kyennyt nimeämään syyllisiä jopa yksittäisten nörttejä myöten – he tuskin koskaan enää matkustavat länsimaihin. Venäjän aktiivisuus näytti keväällä kohdistuneen nimenomaan Ukrainaan, mutta sittemmin on ollut merkkejä valmistautumisesta toimintaan myös muissa länsimaissa.

Tätä luettaessa on ehkä selvinnyt, kuinka olemme selviämässä mahdollisesta sähköpulasta ja jopa aktiivisesta kyber- ja hybridihäirinnästä. Josko Venäjä laittaa kaiken peliin, vai onko hallinnolla tai elämästään huolehtivilla nörteillä pidäkkeitä länsimaita kohtaan.

Olemme tietenkin itse vastuussa oman kyberalueemme puolustamisesta, mutta kybertoimintaympäristö on globaali eikä juuri tunne rajoja. Tämän vuoksi Nato-liittoutuminen tuo välttämätöntä yhteistoimintaa myös kybertoimintaympäristöön.

Natolla on laaja eri instituutioista koostuva oma tietojärjestelmäkokonaisuus suojattavanaan, mutta myös komentorakenteissaan kyberpuolustuksen organisaatioita. Tällainen on mm. SHAPE:ssa sijaitseva Cyberspace Operations Center (CyOC). Naton sisällä on kuitenkin ollut pohdintaa selkeämmästä CYBERCOM-tyyppisestä johtamisrakenteesta tai uudesta siviili-, sotilas- ja yritystoimijoiden tietoa yhdistävästä keskuksesta. Meitä lähellä Tallinnassa oleva The Nato Cooperative Cyber Defence Centre of Excellence (CCD-COE) on tärkeä keskus harjoitustoiminnassa ja käsitteenmuodostuksessa, mutta ennen kaikkea ajatushautomo irti komentorakenteista.

Nato näkee kyberpuolustuksen suomalaista määritelmää laajempana resilienssikysymyksenä. Esim. ”Cyber Defence Pledge” sitouttaa ja jopa mittaa ulkopuolisen silmin maita kehittämään kriittisen infrastruktuurin kyberturvallisuuteen liittyvää resilienssiä, varautumista ja vastetta. Naton viitekehys on tuonut suomalaiseen keskusteluun mielenkiintoisia sävyjä: kun aiemmin ”kansallista turvallisuutta ja maanpuolustusta” vieroksuttiin monessa kyberturvallisuuteen liittyvässä keskustelussa, nyt Naton myötä kyberpuolustus on leviämässä eri hallinnonaloilla kiinnostavaksi yläkäsitteeksi.

Matkalla kohti Naton kesän 2023 Vilnan huippukokousta ymmärrys Naton tulevista

kyberrakenteista kirkastunee. Rakenteista riippumatta on kuitenkin selvää, että myös kyberhyökkäys voi laukaista kollektiivisen puolustuksen viidennen artiklan. Ja on myös selvää, että Venäjän toiminta on herättänyt Naton – liittoutuneiden kyberpuolustus ja resilienssi ovat vahvassa nosteessa.

Loppuprovokaatio: Myös Suomen on syytä olla hereillä kyberuhkien äärellä – kuten kybertoimintaympäristön tarvitseman tieto- ja sähköverkkojen laajemmankin suojaamisen äärellä. Keskeinen Naton hyötymme tulee olemaan ”benchmarkkauksessa” – kun muutkin näkevät tekemisemme, omaan bluffiin (eli pidäkeviestintään) itse uskominen ei ole niin helppoa. Toivottavasti emme joudu heräämään liittolaistemme nauruun, mutta parempi sekin kuin herätä kasakan nauruun.

Toimintaympäristön digitalisoituminen Ukrainan sodassa

- Sotilasprofessori Aki-Mauri Huhtinen -

Digitaalisuus voi olla kansallisena brändinä

Ennen Venäjän tunkeutumista asevoimillaan Ukrainaan helmikuussa 2022 Ukrainan strategisena visiona oli tulla yhdeksi Euroopan johtavaksi digitalisoiduksi valtioksi. Ukraina ei ole luopunut tavoitteestaan tarjota laajenevasti digitaalisia palveluita kansalaisilleen. Oikeastaan viimeisen yhdeksän kuukauden aikana sota on vain vahvistanut tätä kansallista visiota.

Presidentti Zelenskyin strategisen kommunikoinnin tempo sekä henkilökohtaisesti että hallinnon ja kansalaisyhteiskunnan laajojen kerroksien kanssa kertoo tarinaa siitä, että digitaalisuus voi olla paitsi kansakunnan visio myös strategia selvitä sodasta ja kriiseistä. Parhaimmillaan digitalisaatio lisää osallistuvuutta, aktivoi kansalaiset ja tekee hallinnosta päätöksentekijöille ja sen kohteille läpinäkyvää ja oikeudenmukaista.

Vuoden 2022 aikana Ukraina on saanut kerättyä ennennäkemättömän paljon dataa sodankäynnistä. Sitä on kyetty jakamaan ja hyödyntämään myös länsimaisten suurvaltojen tiedustelun kanssa Ukrainan sotatoimien menestyksen takaamiseksi. Viimeiset 10–15 vuotta Venäjän vihamielisyys on ollut selvää sekä Ukrainan hallinnolle että kansalaisyhteiskunnalle. Siksi virallisen hallinnon on ollut helppo luottaa kansalaisyhteiskuntaan ja antaa sen improvisoida digitaalisuutta käytännön arjen ratkaisuiksi sodankäyntiin. Tulosta on syntynyt: tähän mennessä Venäjä on jäänyt sekä teknisellä että psykologisella rintamalla altavastaajaksi sodassa.

Ukrainan taistelun menestystekijöitä on monia, mutta digitaalisuus ja sen johtaminen ovat keskeisiä. Keskellä sotaa Ukraina on kutsunut ulkomaisia teknologiayrityksiä ja innovaatioyhteisöjä ideoimaan ja testaamaan erilaisia digitaalisia ratkaisuja paitsi sodankäynnin tukemiseksi myös yhteiskunnan rakentamiseksi. Tästä toimintatavasta on esimerkiksi meillä Suomessa paljon opittavaa. Voisiko Suomen tulevaisuuden visiona olla jotakin vastaavaa, esimerkiksi avaruudellisten ilmiöiden ja toiminnallisuuksien kärkimaa maailmassa?

Sodan päämääränä vastapuolen käyttäytymisen muuttaminen

Kun katsotaan Naton julkisia tulevaisuuden sodankäynnin ilmiöihin liittyviä ulostuloja, keskiössä on ajatus muun muassa kognitiivisesta sodankäynnistä. Tämä tarkoittaa sitä, että kaikki sotilaalliset vaikutukset integroidaan tavoittelemaan vastapuolen ja kilpailijoiden käyttäytymisen muuttamista. Uudet teknologiat mahdollistavat tämän yhä tehokkaammin.

Yli puolet maapallon väestöstä käyttää jonkinlaista sosiaalisen median sovellutusta, ja yleensä ihmisten globaali vuorovaikutus on virtuaalista. Oleellista on siis olla mukana tässä vuorovaikutuksessa, mikäli pyrkimyksenä on saada oma tarina lävitse laajoissa ihmismassoissa.

Lisäksi ihmisten käyttämistä sovellutuksista havaitaan, että tekstipohjaisuus tekee tilaa audiovisuaaliselle kommunikaatiolle. Kun mukaan astuu teknologia, jossa pöytätietokoneista, läppäreistä ja älypuhelimista siirrytään suoraan aisteihin, kuten iholle, silmiin ja kuuloon, tuleviin langattomiin sensoreihin, vaikuttaa informaatiokuormitus räjähdysmäisesti suoraan ihmisen kognitiiviseen toimintakykyyn. Toimintaympäristön merkitysten luominen syntyy tulevaisuudessa yhä enemmän meemien, kuvien, äänen ja symbolien kautta. Tällä hetkellä tästä muutoksesta kertoo se, että globaalisti nuoret lukevat tekstejä vähemmän kuin ennen.

Kilpailu ja taistelu informaatiosta on jatkuvaa ja globaalia. Vaikka fyysinen sota Ukrainassa on paikallista, siihen liittyvä informaatiovaikuttaminen palvelunestohyökkäyksineen, haittaohjelmineen, identiteettivarkauksineen ja psykologisen vaikuttamisen keinoineen on globaalia ja mahdollista kaikkialla verkoissa.

Vaikka Venäjän informaatiosotakoneisto onkin altavastaajana läntisissä demokratioissa, disinformaation levittäminen. internetin sekä sen palveluiden tekninen häirintä ja sabotointi jatkuvat erityisesti Intian, Kiinan, Iranin, Afrikan ja Etelä-Amerikan alueilla. Näissä maapallon osissa valtiot ovat kontrolloineet ja rajoittaneet internetin perusrakennetta ja medialukutaito on heikkoa. Vahvat ennakkoluulot länttä kohtaan kolonialistisen historiakokemuksen vuoksi helpottavat Kremlin informaatiovaikuttamista.

Mitä voimme oppia Ukrainan sodan digitaalisuudesta?

Mikäli kansakunnan päätöksentekijöiden ja kansalaisyhteiskunnan välillä on vahva luottamuksen kulttuuri, digitalisaatiota tulisi käyttää asioiden helpottamiseen ja kontrollin purkamiseen – eikä päinvastoin. Erityisesti pienten valtioiden tulisi hyödyntää digitalisaation mahdollistama joukkoistaminen ja toimintavapauksien delegoiminen. Lisäksi jos kansalaisyhteiskunta on hyvin koulutettua ja digitaalisesti osaavaa, ei digitaalisuuden hallintoa kannata byrokratisoida.

Suomessa monet esimerkit julkisen hallinnon tietojärjestelmähankkeista kertovat huolestuttavia uutisia siitä, etteivät kalliit järjestelmät toimi eivätkä ne tuota toivottua tehokkuutta loppukäyttäjälle. Lisäksi monet hallinnon järjestelmät ovat irtaantuneet yksityisen ihmisen arjen järjestelmistä käyttömukavuudessaan. Jos digitaalinen visio ei ole integroituna osana kansallista visiota tai jos kansallista tulevaisuuden tilaa ei selkeästi ole, digitalisointi ei tuo toivottuja tehoja sen enempää hallinnolliseen päätöksentekoon kuin kansalaisten arkeenkaan.

Toinen kysymys on se, miten tieto ja informaatio saadaan tarvitsijoille. Ukrainan esimerkit osoittavat, kuinka normaaliolojen sovellutukset on koodattu auttamaan helposti sodan tarpeita ja kansalaiset toimivat sensoreina sodan avuksi. Informaatio kulkeutuu nopeasti ruohonjuuritasolta hallintoon ja takaisin.

Perinteinen ”johtamisen nyrkki” -malli on toimiva nopeassa päätöksentekotilanteessa. Tutut ja saman mieliset avaintoimijat pääsevät konsensukseen nopeasti ja voivat päätöksellään ohittaa laajan hallintokoneiston byrokraattisen hitauden. Nyrkkimallin haasteena on se, että ajan kuluessa sen käyttö rapautuu vaihtoehtoisten signaalien kulkeutuessa informaatiorihmastoista päätöksentekoon. Se rämettää hallintokanavat, jotka eivät ole nyrkin toiminnan sisällä. Lisäksi toimintatapakulttuurina nyrkkimalli luo epävirallisia siiloja tiedonvälityksen kanaviin, lisää läpinäkymättömyyttä hallintoon ja samalla rapauttaa luottamusta.

Esimerkiksi Suomessa on viime aikoina keskusteltu eri medioissa siitä, kuinka vaihtoehtoista tietoa Venäjän taloudellisista hankkeista, esimerkiksi Nord Stream -kaasuputkien turvallisuusuhkista, oli saatavilla, mutta ne sivuutettiin. Yksi keskeisistä

informaatioyhteiskunnan haavoittuvuuksista onkin inhimillisen päätöksenteon rajallisuus ja ihmisen informaationkäsittelyn kapeus.

Kaikkialla yhteiskunnassa tarvitaan yksittäisiä toimijoita varten vapaan datan algoritmipohjaista apua ja tekoälysovellutusten käyttöä, jotta työkalut ja toiminnot helpottuvat, yksinkertaistuvat ja demokratisoituvat. Organisaatioilla ei ole varaa perustaa päätöksentekoa heraldiseen induktioon tai manuaaliseen tiedonsiirtoon, vaan datan keräämisen ja analysoinnin ammattilaisia on koulutettava ja rekrytoitava päätöksenteon tueksi.

Strateginen kommunikaatio integroi informaatiovaikuttamisen suorituskyvyt

Strateginen kommunikaatio ei ole vain viestintää, vaan ennen kaikkea koko organisaation käytännön toimintaa ja tekoja, joiden avulla kommunikoidaan valittujen yleisöjen ja maalien kanssa. Sotilasorganisaatioissa strategisen kommunikaation onnistumisen edellytys on kansallisen turvallisuuden poliittisen tahdon ja turvallisuustoimijoiden saumaton yhteen pelaaminen, jolloin kilpailijat ja vastustajat eivät pääse iskemään omalla informaatiovaikuttamisella kiilaa ristiriitaisten tarinoiden ja teemojen väliin. Yhä tärkeämmäksi perinteisen salatun ja ns. ”kovan” tiedustelutiedon rinnalle on nousemassa koko organisaation kyky hyödyntää informaatioympäristön tarjoamaa avointa dataa ja osaaminen tekoälyn ja algoritmien käytössä on tullut osaksi myös sotilasorganisaatioiden rutiinioperointia. Sensoreiden kasvu taistelutilassa ja informaatioverkostojen ja kytkentöjen tihentyminen antaa juuri informaatiojohtamiselle etulyöntiaseman suunnata oikeaa vaikuttamista oikea-aikaisesti sekä kustannustehokkaasti sekä turvallistaa oman operoinnin tavoitteet. Pääsy erilaiseen informaatioon on avainasemassa mm. informaatioympäristön analysoinnissa ja sen tilannekuvaan ja päätöksentekoon tarvittavassa tiedossa. Yhä enemmän myös teknisen puolen kybersuorituskykyjen ja vastaavasti ”pehmeämpien” ei-kineettisten suorituskykyjen integrointi ja yhteensovittaminen tapahtuu juuri strategisen kommunikaation toiminnallisuuden alla.

Sota tietoisuudesta

- Insinöörieversti Jyri Kosola -

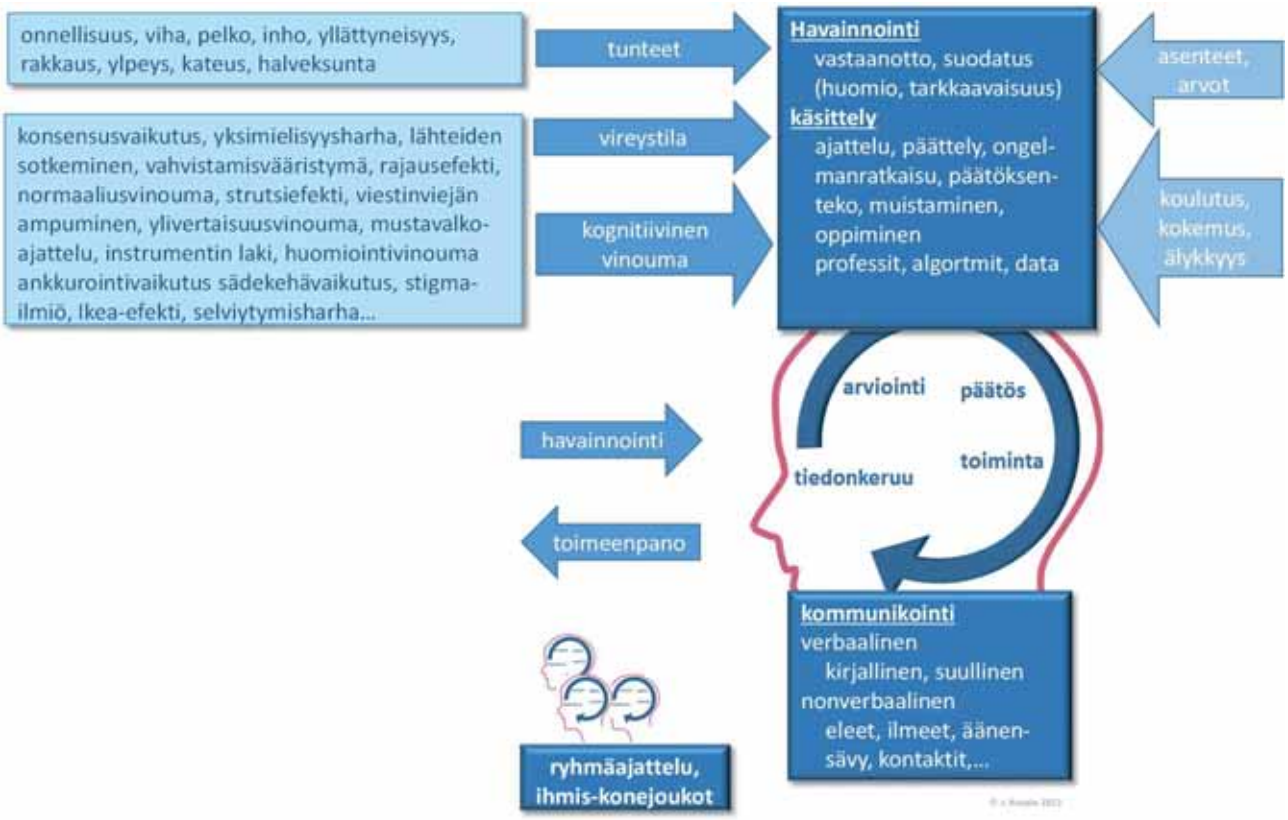
Kognitio, sodan seitsemäs ulottuvuus?

Kognitiivisiin toimintoihin kuuluu havainnointi, tiedon käsittely ja päätöksenteko sekä näihin liittyvä muistaminen, oppiminen ja uuden informaation, esimerkiksi puheen ja tekstin tuottaminen. Kognitiivinen sodankäynti on vielä olemustaan hakeva psykologis-sosiaalisteknologinen sodankäynnin muoto, jossa yhdistyy sekalainen joukko jo vakiintuneita sodankäynnin aloja joukkoon uusia, osin liike-elämässäkin hyödynnettäviä, menetelmiä.

Kognitiivinen prosessi on pääosin aisteilla havaitun ja kokemusten sekä oppimisen perusteella muistiin tallennetun tiedon käsittelyä. Tiedonkäsittelyyn voidaan vaikuttaa vaikuttamalla aistihavaintojen lisäksi tunteisiin ja vireystilaan. Varmistamalla tai estämällä uni ja lepo sekä kemiallisin ja biologisin keinoin voidaan nostaa tai laskea vireystilaa. Tunteita nostattamalla on mahdollista ohittaa loogisen prosessoinnin järkeily. Asenteita ja arvoja muokkaamalla sekä kokemuksia tarjoamalla on mahdollista valmistella henkistä taistelutilaa.

Nykykäsitys sodasta perustuu pitkälti olettamukseen siitä, että se on aseellinen konflikti, jota käydään maalla, merellä ja ilmassa operoivilla sotajoukoilla, avaruuteen sijoitetuilla järjestelmillä, tietoverkoissa sekä sähkömagneettisessa spektrissä. Käsitettä aseellinen konflikti on teknologioiden kehityksen myötä yhä vaikeampi määritellä. Operointi maalla, merellä ja ilmassa edellyttää joukkojen tai järjestelmien lähettämistä operointialueelle. Tavoitteeseen pääseminen vaatii sotilaallisen voiman käyttöä operaatioalueella, tai ainakin sillä uhkaamista. Informaatioteknologian kehittymisen ja yhteiskunnan digitalisoitumisen myötä kaikilla ihmisillä on pääsy kaikkeen tietoon, ainakin periaatteessa. Asetelma on käännettävissä myös toisin päin; kaikkialta päästään käsiksi ihmisten tietoisuuteen. Tällöin ihmisten ajatteluun ja päätöksentekoon voidaan vaikuttaa olematta fyysisesti läsnä. Samoin tiedustelu, valvonta ja maalitus voidaan tehdä tunkeutumatta operaatioalueelle joukoin tai järjestelmin.

Sodankäynnin äärimmäisenä onnistumisena pidetään voittoa ampumatta laukaustakaan. Tämä on mahdollista, jos yhteisöjen ja niiden avainhenkilöiden tilanneymmärrykseen, ajatteluun ja päätöksentekoon voidaan vaikuttaa. Vaikuttamisen tavoitteena on tukea diplomaattista, sotilaallista tai taloudellista operaatiota kohdentamalla vastustajan päätöksiä haluttuun suuntaan tai hidastamalla päätöksentekoa riittävästi. Päätöksentekoa voidaan hidastaa kiinnittämällä vastustajan huomio muualle, luomalla epävarmuutta, synnyttämällä ristiriitoja ja vaikeuttamalla kompromissien aikaansaamista. Tämä voidaan toteuttaa esimerkiksi luomalla vaihtoehtoisia narratiiveja, polarisoimalla keskustelua, synnyttämällä mustavalkoajattelua ja radikalisoimalla yksilöitä ja yhteisöjä.

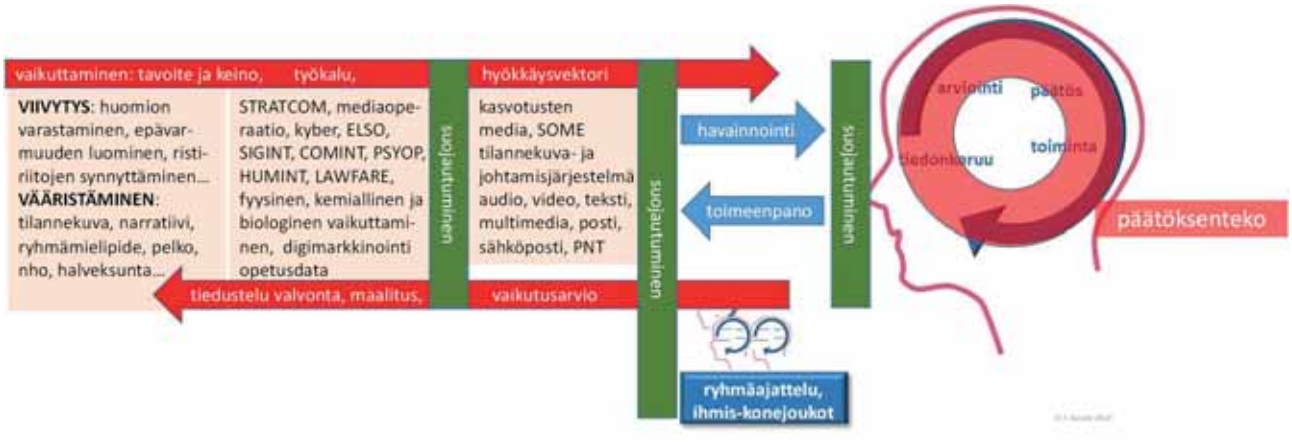


Päätösten suuntaamisessa pyritään hyödyntämään ihmisen kognitiivisten prosessien heikkouksia ja erilaisia ihmiselle luontaisia ajatteluvääristymiä, eli kognitiivisia vinoumia.

kognitiiviset vinoumat vääristävät ajattelua

Konsensusvaikutuksessa ihminen mukauttaa ajattelunsa siihen, mitä muut ihmiset asiasta sanovat. Rajaamalla pääsyä informaatioon ja luomalla keinotekoista informaatiota voidaan synnyttää illuusio, että jostakin asiasta on laaja konsensus. Yksimielisyysharha puolestaan on valheellinen konsensusvaikutus, jossa ihminen ajattelee muiden ihmisten jakavan hänen näkemyksensä. Tällä voidaan sekä radikalisoida yksilöitä, että saada ihminen tekemään huonoja päätöksiä. Lähteiden sotkeminen on epätietoisuutta informaation alkuperästä. Varsinkin digitaaliavaruudessa voi olla vaikea hahmottaa mihin jokin väite tai argumentti perustuu. Tämä vaikeuttaa informaation arviointia. Vahvistamis-vääristymässä ihminen huomioi ja muistaa kaiken, mikä vahvistaa hänen ennakkoluulojaan ja oletuksiaan, mutta jätättää huomioimatta ja muistaa huonommin seikat, jotka voisivat kumota oletuksen. Rajausefekti on taipumus tehdä eri johtopäätöksiä samasta tiedosta sen perusteella, onko asia esitetty positiiviseen vai negatiiviseen sävyyn. Tuntemalla kumminpäin ihminen ajattelee, negatiivisen vai positiivisen kautta, asia on esitettävissä tavalla, joka todennäköisemmin menee läpi.

Normaaliusvinouma estää ennakoimasta tai reagoimasta asiaan, jota ei ole tapahtunut koskaan aiemmin. Strutsiefekti on taipumus jättää huomioimatta negatiiviset asiat. Lähellä tätä on viestinviejän ampuminen, eli negatiivisen asian projisoiminen sen syyksi, joka asian tuo ilmi. Nämä vinoumat estävät kyvyn käsitellä negatiivisia asioita ja tehdä ennakoivia tai korjaavia päätöksiä. Ne myös ruokkivat ylivertaisuusvinoumaa, jossa henkilö yliarvioi tietämyksensä, osaamisensa tai taitonsa. Mitä huonompi yksilö on kyseisessä asiassa, sitä enemmän hän tyypillisesti yliarvioi itseään: kun yksilö ei hallitse asiaa, hän ei osaa myöskään arvioida osaamistasoaan.



Mustavalkoajattelu estää näkemästä vaihtoehtoja ääripäiden välillä, jolloin ei kyetä yhdistämään asian hyviä ja huonoja puolia järkeväksi kokonaisuudeksi. Instrumentin laki on vahva luottamus tuttua toimintatapaa kohtaan ja uusien vaihtoehtoisten tapojen ia menetelmien vierastaminen. Huomiointivinouma on taipumus tehdä havaintoja sen hetkisen olotilan tai valloillaan olevien ajatusten mukaisesti. Esimerkiksi väsyneenä, verensokeritason ollessa matala ja ihmisen ollessa ärtynyt tai huonolla tuulella, hän huomioi ympäristöään normaalia negatiivisemmin. Ankkurointivaikutus tarkoittaa sitä, että ihminen asemoi ajattelunsa asiasta saamansa ensimmäisen tiedon mukaan. Kaikki myöhempi tieto tulkitaan tämän "mentaalisen ankkurin" suhteen. Sädekehävaikutus on kognitiivinen vinouma, jossa huomiota herättävän myönteisen ominaisuuden omaavaan kohteeseen liitetään muitakin positiivisia piirteitä. Stigmailmiö on sädekehäilmiötä vastaavaa negatiivinen konnotaatio. Ikea-efekti on ilmiö, jossa ihminen antaa suhteettoman paljon painoarvoa asialle, jonka kehittämiseen hän on itse osallistunut. Selviytymisharha on looginen virhe, jossa keskitytään asioihin, jotka ”selviytyivät" jostain prosessista, vaikka huomion pitäisi olla niissä, jotka eivät selviytyneet.

Yhdistelmä vanhoja ja uusia keinoja

Kognitiivinen sodankäynti lienee parasta jäsentää niin kuin muutkin immateriaaliset sodankäynnin muodot kyber ja ELSO: tiedusteluun ja vaikuttamiseen sekä niiltä suojautumiseen. Näihin on syytä lisätä taistelutilan preparointi, eli varautuminen operaatioihin luomalla suotuisia asetelmia jo etukäteen.

Ajatteluun vaikuttaminen edellyttää psykologisen, sosiaalisen ja informaatioympäristön manipulointia yksilö- ja joukkotasoilla; miten ihmiset hahmottavat tilanteen, muodostavat kantansa ja tekevät päätöksensä yksilöinä ja sosiaalisena ryhmänä sekä miten yksilöt ovat vuorovaikutuksessa keskenään.

Kognitiivisen sodankäynnin keinovalikoima käsittää laajan joukon jo vakiintuneita tiedustelun ja vaikuttamisen menetelmiä, kuten avointen lähteiden tiedustelu, signaali- ja asiamiestiedustelu, kyber- ja elektroninen sodankäynti, psykologiset operaatiot, informaatiomanipulointi ja social engineering. Avointen lähteiden tiedustelulla sekä digimarkkinoinnin keinoin ja työvälinein on mahdollista päästä käsiksi laajojen ihmisjoukkojen arvoihin, asenteisiin, ajatuksiin ja päätöksentekoprosesseihin.

On syytä huomata, että vaikka kognitio laajentaa sodankäynnin ulottuvuutta, se ei tee vanhoja ulottuvuuksia tarpeettomiksi. Ilmasodankäyntikään ei aikoinaan tehnyt maa- ja merisodankäyntiä tarpeettomiksi. Toisaalta maalla ja merellä operointi edellyttää myös ilmassa operointia. Aivan samoin toimintakyky maalla, merellä ja ilmassa edellyttää

toimintakykyä ja aktiivista toimintaa myös kognitiivisessa ulottuvuudessa.

Tekoälyä hyödyntävien ohjelmistorobottien ja deep fake -tekniikoiden avulla on jo nykyteknologialla mahdollista luoda sodankäyntiin uusi ulottuvuus, joka voi olla näkymätön perinteisissä ulottuvuuksissa toimiville asevoimille, joiden toimenkuvaan ja toimivaltuuksiin kognitio ei sisälly ja joiden organisaatiorakenteeseen se ei istu.

'

Vuoden insinööriupseeri 2022

Insinööriupseeriliitto valitsee vuosittain Vuoden insinööriupseerin. Valintaperusteena on palkinnon saajan osoittama erinomainen kyky sotateknillisen kehittämistehtävän tai ongelman ratkaisussa tai edellä mainittuja tehtäviä suorittavan joukon vetäjänä, innostavana ja tuloksellisena johtajana. Lisäksi Vuoden insinööriupseerin tulee nauttia työyhteisönsä arvostusta maapuolustustahtoisena ja puolustusvoimien tavoitteisiin sitoutuneena tekniikan ammattilaisena.

Vuoden insinööriupseeriksi on aiemmin valittu
2002 inskom Jari Junttila (MERIVTL)
2003 inskaptl Seppo Lahti (PVMATLE)
2004 insmaj Kari Renko (ILMAVE)
2005 inskomkapt Risto Hellgren (MERIVTL)
2006 insmaj Risto Lehtomäki (HELSLE)
2007 insevl Jyri Kosola (PVMATLE)
2008 inskapt Timo Pulkkinen (PVTT)
2009 insevl Raimo Siltanen (LSHRE)
2010 inskaptl Björn Ehnroth (MERIVE)
2011 insmaj Jaakko Jurvelin (PVTT)
2012 insmaj Riku Lahtinen (ILMAVMATL)
2013 insevl Matti Rantanen (PE)
2014 insevl Antti Karva (MAAVMATLE)
2015 insev Hannu Kihlman (JÄRJK)
2016 insev Juha Hakulinen (JÄRJK
2017 insevl Jouni Koivisto PVTUTKL
2018 insevl Markus Mecklin ILMASK
2019 inskom Jari Hörkkö, JÄRJK
2020 insevl Anders Furu, PVTUTKL
2021 insevl Esko Kaleva, JÄRJK

Vuoden 2022 insinööriupseeriksi valittiin Järjestelmäkeskuksen apulaisjohtaja insinöörieversti Olli Klemola. Hän vastaa materiaalisen suorituskyvyn rakentamisen ja ylläpidon prosessiohjauksesta. Tehtävällä on huomattavaa puolustusvoimien laajuista vaikuttavuutta Järjestelmäkeskuksen keskittyessä puolustusvoimien suorituskyvyn rakentamisen ja teknisen elinjakson hallinnan projekteihin. Klemolan ohjauksessa on yli puolet puolustusbudjetin rahoituksesta.

Klemola on aktiivisella ja työtä pelkäämättömällä otteellaan kehittänyt merkittävästi hankehallinnan tärkeintä rajapintaa, toimeksiantokatselmointia, jolla kehittämisohjelma antaa rakennettavan suorituskyvyn Logistiikkalaitoksen hankittavaksi. Hänen sitoutumisensa aste ja työmoraalinsa on poikkeuksellisen korkeaa. Klemola nauttii esimiestensä, kollegoidensa ja alaistensa varauksetonta arvostusta. Ihmisenä Klemola on avoin, helposti lähestyttävä ja kannustava

Klemola on myös palvelusuransa aiemmissa tehtävissä osoittanut kykenevänsä yhdistämään korkean teknisen osaamisensa, ihmisten johtamisen ja asioiden aikaan saamisen. Muutamina nostoina aiemmista onnistumisista mainitaan Puolustusvoimien tutkimuslaitoksen tutkimusjohtajan tehtävä ja Elektroniikkalaitoksen johtajuus.

Insinööriupseeriliitto onnittelee insinöörieversti Olli Klemolaa ja toivottaa kaikkea hyvää vuodelle 2023.