Viestimies

Viestiupseeriyhdistyksen julkaisu 79. vsk Numero 3 Syksy 2024

www.viestiupseeriyhdistys.fi

COMBITECH

Kovaa softaa

Nopeampaa päätöksentekoa
suorituskykyisillä ohjelmistoilla.

Combitech Finland

www.combitech.fi

Viestimies-lehti

Päätoimittaja
Kimmo Kaipainen
p 040 7222646
viestimies@viestiupseeriyhdistys.fi

Toimitussihteeri
Kyösti Saarenheimo
p 040 5536182
toimitussihteeri@viestiupseeriyhdistys.fi

Henkilötoimittaja
Hanna Liitola
p 040 5930675
henkilotoimittaja@viestiupseeriyhdistys.fi

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

Toimituskunta
Vähätiitto Jarmo (pj)
Blomqvist Reima
Hyvärinen Pertti
Isomäki Pekka
Koski Harri
Nyqvist Antti
Pellikka Jarkko
Puhakka Pasi
Sipilä Olli
Suokko Harri
Tunkkari Antti
Wirman Kari

Toimituksen osoite:
Päivölänrinne 7 A 1
04220 Kerava

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

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

Ilmoitusmyynti
Juha Halminen
p. 050 59 22722
juha.halminen@mediaosasto.fi

Painopaikka
Newprint Oy, Raisio
p 010 231 2600

ISSN 0357-2153

Kansikuva: ChatGPT:n näkemys Kiinasta kybervoimana

Tässä numerossa

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

Mukana lehdessä
–
Mukana päätöksiä tehdessä!

Seuraavan numeron aineistopäivä on 1.11.2024. Lehti ilmestyy viikolla 49.

Uhka

Jatkosodan päättymisestä tulee tänä syksynä kuluneeksi 80 vuotta. Itsenäisyytemme oli Neuvostoliiton kesällä 1944 aloittaman suurhyökkäyksen seurauksena vaakalaudalla. Torjuntataisteluita seurannut jatkosodan päättänyt tulitauko alkoi virallisesti 4. syyskuuta 1944. Välirauhan ehtojen mukaisesti saksalaiset joukot oli pakotettava pois maasta ja Lapin sota alkoikin 15. syyskuuta 1944. Sota Neuvostoliiton kanssa loppui lähes päivälleen 80 vuotta ennen tämän lehden ilmestymistä 19. syyskuuta allekirjoitettuun Moskovan välirauhaan.

Veteraanien perintönä säilytimme itsenäisyytemme. Kansakuntien tarinoiden lisäksi sodista kertovat myös yksilöt. Yhdistyksemme entinen toiminnanjohtaja Martti Aho vie meidät artikkelissaan seuraamaan isänsä sotapolkua Jatkosodan aikaisen päiväkirjan perusteella.

Nykyhetkessä sodan kaiut ovat kuultavissa joka hetki. Nyt on Ukrainan vuoro kamppailla selviytymisestä. Nykyaikaisen taistelukentän todellisuus ja vaatimukset esimerkiksi viestijoukoille ja johtamiselle ovat sodan usvasta huolimatta ainakin osin tavoitettavissamme. Majuri Matti Ruotsalainen antaa meille tästä esimerkin tarkastelemalla artikkelissaan elektronisen sodankäynnin havaintoja Ukrainasta julkisiin lähteisiin pohjautuen.

Suomessakin maailman turbulenssi tuntuu, myös konkreettisina tapahtumina arjessamme. Venäjän toteuttama GNSS-häirintä on ollut kesän ja syksyn mittaan uutisissa. Joensuun lentokentälle suuntautuneita lentoja on jouduttu uudelleen reitittämään. Kesällä uutisoitiin myös Janakkalassa kaadetusta tukiasemamastosta. Maston harukset oli katkaistu tahallisesti. Myös vesilaitosmurtoja on havaittu vuoden kuluessa useampia. Se onko tapahtumissa kyse sodan heijasteista, laaja-alaisesta vaikuttamisesta vaiko sattumista on toki arvioitava erikseen. Turvallisuutemme muodostuu osaltaan tämän kaltaisten tapahtumien tunnistamisesta ja torjumisesta.

Yhteiskunnan turvallisuutta voidaan rakentaa tai vähentää omin toimin, ihan ilman ulkopuolista puuttumista. Paikkatietojen turvallisuus on ajoittain keskusteluissa esiin nouseva kysymys. Valtiovarainministeriön työryhmä julkaisi 12.6. paikkatiedon kansallisen riskiarvion. Avoimen datan tuomat rahalliset hyödyt johtivat valtavan kartta- ja paikkatietoaineiston avaamiseen julkiseksi dataksi vuonna 2012. Paikkatietojen avoimuus tuo hyötyjä, mutta lisää myös riskejä aineiston väärinkäytölle. Ehkäpä tässäkin asiassa sinisilmäisyyden aika on ohi.

Suomi asemoi itseään liittoutuneena valtiona myös virallisesti. Valtioneuvosto antoi 20.6. uuden Valtioneuvoston ulko- ja turvallisuuspoliittisen selonteon. Selonteossa todetaan, että Suomen ulko- ja turvallisuuspolitiikkaa tehdään vakavassa ja vaikeasti ennakoitavassa toimintaympäristössä. Suomen turvallisuusympäristön mainitaan myös muuttuneen perustavanlaatuisesti ja pitkäkestoisesti.

Selonteossa todetaan, että ”*Teknologian kehitys nostaa esiin uusia kansainvälisen oikeuden kysymyksiä liittyen muun muassa kyberympäristöön, tekoälyn käyttöön, uusiin aseteknologioihin ja kriittisten raaka-aineiden hyödyntämiseen.*” Erinomaisen ajankohtaista ja mielenkiintoista tekoälyn käytettävyyteen liittyvää oikeudellista pohdintaa meille tarjoavat Aarne Klemetti ja Janne-Matti Peltola tekoälyn sotilassovellusta käsittelevässä artikkelissaan.

Selonteossa linjataan myös Suomen asemaa kybertilassa. Suomen mainitaan kehittävän kansalliset suuntaviivat tavoitteelliselle ja johdonmukaiselle kyberattribuutiotoiminnalle, huomioiden keskeiset liittolaiset ja kumppanit. Vihamieliseen vaikuttamiseen valmistaudutaan siis nykyistä selkeämmin valmistautumalla osoittamaan syyllisiä sormella. Suurista kybertoimijoista Venäjä ja Kiina ovat käsittelyssä apulaissotilasprofessori Juha Kukkolan ja erikoistutkija Matti Purasen erinomaisissa artikkeleissa.

Mainittu selonteko on ensimmäinen uuden aikakauden ulko- ja turvallisuuspolitiikan linjapaperi, jossa on huomioitu niin Nato-jäsenyys kuin muuttunut turvallisuusympäristö. Rakennamme vastavoimaa uhalle sanoittamalla Suomena itse paikkamme maailmassa. Tämä Suomen asemoitumisen määrittely saa vuoden lopulla jatkoa uuden Yhteiskunnan turvallisuusstrategian sekä myöhemmässä vaiheessa uuden Valtioneuvoston puolustusselonteon myötä.

Olemme vähän kerrallaan löytämässä paikkamme liittouman osana myös käytännössä. Suomi on nimittäin saanut ensimmäisen komentorakenteessa palvelevan kenraalinsa Jarkko Karsikkaan aloitettua Belgian Monsissa sijaitsevan johtamis- ja tietojärjestelmäportaan (Nato Communication & Information Systems Group, NCISG) esikuntapäällikön tehtävässä. Viestimies-lehti onnittelee lämpimästi prikaatikenraali Karsikasta historiallisen tehtävän johdosta!

Tervetuloa uusimman Viestimies-lehden pariin. Antoisia lukuhetkiä ja mukavaa syksyn jatkoa!

Kimmo Kaipainen

Päätoimittaja

WE ARMOR IT.™

Letters. Words. Codes. Coordinates. Orders.

Every moment vital information is transmitted around us and at risk. Enter MilDef. We create rugged IT solutions for the harshest conditions and most challenging environments, which prevent your information from being interrupted, intercepted or disrupted.

Put simply; we armor your IT, when and where the stakes are the highest.

MILDEF

TEKSTI: MATTI PURANEN, KUVAT:CHATGPT.

Kiinalaisen kybersodankäynnin monimuotoinen maailma

Matti Puranen (matti.puranen@mil.fi) toimii strategian erikoistutkijana Maanpuolustuskorkeakoulun Sotataidon laitoksella. Hänen tutkimuksensa keskittyy Kiinan ja Yhdysvaltojen väliseen dynamiikkaan.

Taloudellisen ja sotilaallisen suurvalta-asemansa ohessa Kiina on kohonnut nopeasti yhdeksi maailman merkittävimmistä kybervalloista. Kiina on internetteknologian jättiläinen, jonka verkkolaiteyhtiöt rakentavat kasvavan osan globaalista internet-infrastruktuurista, ja jonka internetpalveluilla on satoja miljoonia käyttäjiä. Kiina on myös merkittävä offensiivinen kybertoimija: maailmalla uutisoidaan jatkuvasti suurista ja edistyksellisistä kyberhyökkäyksistä, joiden jäljet johtavat tavalla tai toisella juurensa Kiinaan.

Tässä artikkelissa pyritään luomaan kokonaisvaltainen yleissilmäys kiinalaisen kybertoiminnan suureen kuvaan: Kiinassa vallitsevaan ”kybersuvereniteetin” ajatteluun, Kiinan siviilitiedustelupalveluiden suorittamaan strategiseen tiedusteluun sekä Kiinan asevoimien kyberoperaatioihin.

Puoluevaltion kyberkoneisto

Kiinan valtavaa kyberkoneistoa tulee tarkastella osana Kiinan autoritaarista poliittista järjestelmää, jossa yksinvaltainen Kiinan kommunistinen puolue näyttelee keskeistä roolia. Kiinan ”leninistiseksi puoluevaltioksi” kuvaillussa järjestelmässä kommunistinen puolue johtaa suoraan kaikkein tärkeimpiä hallinnonaloja talous-, ulko- ja turvallisuuspolitiikasta sotilasstrategiaan, kun taas valtiolliset organisaatiot, kuten ministeriöt toimivat lähinnä puolueen linjausten toteuttajina. Valtiollisten rakenteiden johtamisen lisäksi puolue pyrkii ohjailemaan ja vähintään valvomaan myös kaikkia yksityisiä toimijoita kansalaisyhteiskunnasta Kiinassa toimiviin ulkomaisiin yrityksiin.

Yksinkertaisimmillaan kommunistisen puolueen päätavoitteena on oman valta-asemansa ylläpitäminen ja sitä uhkaavien haasteiden tukahduttaminen. Tämän vuoksi informaation ja siten myös kybertoimintaympäristön hallinta on puolueen näkökulmasta kriittinen asia. Puoluejohtoa on internetin alkuajoista lähtien huolettanut internetin informaation vapaata liikkuvuutta ja liberaalia ideologiaa heijasteleva perusolemus. Lisäksi koko internet-infrastruktuuri verkkolaitteita, valokuitukaapeleita ja ohjelmistoja myöten koostui pitkälle 2000-luvulle miltei yksinomaan länsimaisten yhtiöiden valmistamista järjestelmistä. Vapaa internet näyttäytyi Kiinan johdolle siten lännen, ennen kaikkea Yhdysvaltojen, vallankäytön välineenä, mitä Edward Snowdenin paljastukset Yhdysvaltojen tiedusteluyhteisön kyvyistä hyödyntää internetiä huomattavasti alleviivasivat.

Näistä syistä kommunistinen puolue katsoo kybertilan kuuluvan valtiollisen suvereniteetin piiriin, minkä seurauksena kaikilla valtioilla tulisi olla oikeus valvoa ja hallita rajojensa sisäistä verkkoliikennettä. Integroituessaan osaksi globaalia internettiä Kiina on rakentanut pienin askelin tehokkaan valvontainfrastruktuurin, jolla se kykenee seuraamaan tietoliikennettä Kiinan sisällä, sekä eristämään kiinalaisen internetin ”Kiinan suurena palomuurina” tunnetun järjestelmän taakse. Suuri palomuuri estää pääsyn Facebookin tai entisen Twitterin (X:n) kaltaisille sosiaalisen median alustoille, mutta myös esimerkiksi kansainvälisille uutissivustoille, jotka ovat joutuneet Kiinan sensuuriviranomaisten kynsiin.

Samaan aikaan Kiina on pyrkinyt systemaattisesti irtautumaan riippuvuudestaan länsimaiseen internet-infrastruktuuriin. Kiinalaiset verkkolaitevalmistajat, kuten Huawei ja ZTE, ovat pitkälti savustaneet kansainväliset kilpailijansa Kiinan kotimarkkinoilta, ja ”suuren palomuurin” sisäpuolisessa verkossa on kehittynyt kiinalaisten palveluntuottajien ekosysteemi, jossa Weibon ja WeChatin kaltaiset sovellukset ovat korvanneet läntiset vastinparinsa. Lopputulosta voi hyvällä syyllä kuvata kiinalaiseksi internetiksi, jolla oli vuonna 2023 tehdyn arvion mukaan jo yli miljardi käyttäjää.

Kiinalainen internet laajenee nopeasti Kiinan rajojen ulkopuolelle presidentti Xi Jinpingin lanseeraamaan ”digitaalinen silkkitie” -hankkeen myötä. Varsinkin kehittyvässä maailmassa, jossa verkkoon kytkeytyminen painaa usein turvallisuushuolia enemmän, kiinalaisten yhtiöiden kilpailukyky on ollut länsimaisia huomattavasti parempi. Esimerkiksi Huawein arvioidaan rakentaneen yli 70 % Afrikan 4G-verkoista ja valtaavan tehokkaasti myös tulevien 5G-verkkojen markkinoita.

Tietoliikenneinfran sivutuotteena leviää myös kommunistisen puolueen vaalima näkemys kybersuvereniteetista, minkä nähdään synkimmissä tulevaisuudenkuvissa ajavan maailmaa kohti internetin kahtiajakoa demokratioiden edustamaan vapaaseen internettiin sekä sen kiinalaiseen infrastruktuuriin pohjautuvaan

autoritaariseen kilpailijaan. Toisaalta, vaikka kiinalaiset verkkoyhtiöt valtaavat markkinaosuuksia, eivät kiinalaiset internetpalvelut ole muutamaa verkkokauppaa ja TikTokia lukuun ottamatta juurikaan onnistuneet levittäytymään Kiinan ulkopuolelle.

Kybersodankäyntiä kiinalaisin erityispiirtein

Kaikkia Kiinan kyberasioita kiinalaisen internetin hallinnoimisesta kybertiedusteluun ja kybersodankäyntiin johtaa kommunistisen puolueen kyberasioiden keskuskomissio. Komissio perustettiin vuonna 2014 osana presidentti Xi Jinpingin uudistuksia puolueen valta-aseman keskittämiseksi ja lujittamiseksi.

Kyberkomissio muistuttaa muita samankaltaisia puoluejohdon pienryhmiä, jotka ohjaavat esimerkiksi ulkopolitiikkaa tai asevoimia. Ne laativat pienissä ja suljetuissa piireissään toimialojensa

tärkeimmät strategiset suuntaviivat, joita valtiolliset organisaatiot lähtevät mukisematta noudattamaan. Kyberkomission kautta puolueen ylin johto, ja tarvittaessa Xi Jinping henkilökohtaisesti, kykenee ohjaamaan koko Kiinan valtiollisen kyberkoneiston toimintaa. Se asettaa myös Kiinan kybertiedustelun ja kybersodankäynnin painopisteet.

Kiinan kybersodankäynnistä ja kybertiedustelusta vastaavat organisaatiot voidaan jakaa karkeasti kahteen kokonaisuuteen: siviilitiedustelupalveluihin sekä asevoimiin, eli Kansan vapautusarmeijaan (People's Liberation Army, PLA). Tiedustelupalvelut keskittyvät strategiseen kybertiedusteluun ja teollisuusvakoiluun, kun taas asevoimien päätehtävänä on valmistautuminen sodanajan operaatioihin ennen kaikkea Taiwania ja Yhdysvaltoja vastaan. Vaikka molempien toiminnassa ja tavoitteissa on paljon päällekkäisyyttä, on työnjako suhteellisen selvä.

Puolueen suoraan komentamien organisaatioiden lisäksi kyberoperaatioita suorittavat myös valtio-omisteiset ja yksityiset yritykset sekä lukemattomat erilaiset vapaaehtoisryhmät ja kyberrikolliset, joita puolue pyrkii mahdollisuuksiensa mukaan ohjailemaan ja hyödyntämään. Tunnetuimpiin ja vanhempiin aktivistiryhmiin lukeutuu ”punaisten hakkereiden unioni” (Honker Union), jonka juuret juontavat jo vuoteen 1999, jolloin Yhdysvallat pommitti vahingossa Kiinan Belgradin suurlähetystöä osana Kosovon operaatiotaan.

Kiinalaisten kybertoimijoiden kenttä on kokonaisuudessaan valtava ja monimuotoinen. Vaikka kommunistinen puolue pyrkii Xi Jinpingin toteamuksen mukaisesti ”johtamaan kaikkea”, on epäselvää, kuinka hyvin se kykenee orwellilaisesta kontrollikoneistostaan huolimatta ohjailemaan luomustaan. Kommunistista puoluetta huomattavasti vanhemman kiinalaisen sananlaskun mukaan ”vuoret ovat korkeita, keisari kaukana”, ja iso osa Kiinaan jäljitettävistä kyberoperaatioista voi hyvin olla puolueen kontrollin ulkopuolista oma-aloitteisuutta.

Siviilipuolen kybertoimijat

Kiinan tärkeimmät siviilipuolen kybertoimijat ovat Kansallisen turvallisuuden ministeriö (Ministry of State Security, MSS) sekä poliisitoimintaa johtava Julkisen turvallisuuden ministeriö (Ministry of Public Security, MPS). MSS on Kiinan tärkein ulkomaantiedusteluviranomainen, jonka tehtäväkenttään kuuluu myös vastavakoilu ja signaalitiedustelu. Käytännössä MSS on siten eräänlainen CIA:n ja NSA:n amalgaami samassa organisaatiossa.

MPS johtaa puolestaan Kiinan poliisivoimia, mutta sen vastuulle kuuluu myös kommunistisen puolueen hallinnon turvaaminen ja sisäisen vakauden ylläpito – kiinalaisin termein ”poliittinen turvallisuus”. Olennaisesti MPS:n vastuulla on myös Kiinan sisäisen verkkosensuurin sekä Kiinan palomuurin ylläpitäminen.

Vuonna 2017 hyväksytyn tiedustelulain myötä MSS ja MPS saivat hyvin laajat valtuudet erilaisten kybertiedusteluoperaatioiden suorittamiseen sekä Kiinassa että Kiinan ulkopuolella. Lisäksi laki käytännössä velvoittaa kaikki kiinalaiset toimijat ja jopa ulkomaiset yksitysyritykset tukemaan tiedustelupalveluita niiden näin pyytäessä. Kiinan kaltaisessa autoritaarisessa maassa oikeudellista siunausta ei tietenkään sinänsä tarvita, mutta lain allekirjoittaminen kuvaa itsessään kommunistisen puolueen sisällä vallitsevia prioriteetteja. Tiedusteluoperaatioissaan molemmat palvelut voivat myös tukeutua kasvavaan määrään kiinalaisten yhtiöiden rakentamaa verkkoinfrastruktuuria sekä Kiinan sisällä että yhä laajemmin myös ulkomailla, erityisesti kehittyvässä maailmassa.

Tiedustelu- ja turvallisuuspalveluiden offensiiviset kyberoperaatiot, joista vastaa pääasiassa MSS, voidaan jakaa karkeasti strategiseen tiedusteluun ja teollisuusvakoiluun. Kolmantena päätehtävänä tiedustelupalvelut valvovat kiinalaisten toisinajattelijoiden, kuten demokratia-aktivistien tai tiibetiläisten ja uiguurien vähemmistöjen toimintaa niin Kiinassa kuin sen ulkopuolellakin.

Strategisen tiedustelun tavoitteena on poliittisesti ja strategisesti arvokkaan tiedon hankinta. Kiinan tiedustelupalvelut (erityisesti MSS) on yhdistetty useisiin ”kohdistettuihin haittaohjelmahyökkäyksiin” (APT, advanced persistent threat) kaikkialla maailmassa. Tunnetuimpiin MSS:n yhdistettyihin operaatioihin lukeutuu Yhdysvaltojen henkilöstöhallintoon vuonna 2015 suoritettu hyökkäys, jonka seurauksena kymmenien miljoonien liittovaltion työntekijöiden henkilötiedot päätyivät hyökkääjien käsiin. Myös Suomen eduskuntaan vuonna 2020 kohdistettu hyökkäys on yhdistetty kiinalaiseen APT-ryhmään (APT31), joka puolestaan on yhdistetty kansallisen turvallisuuden ministeriöön. Tutkijat ovat arvelleet, että kyberoperaatioilla hankittua henkilötietojen big dataa on voitu hyödyntää mm. CIA:n peitetehtävissä toimivien tiedustelu-upseerien paljastamiseen.

Toinen Kiinan tiedustelupalveluiden keskeinen tehtävä on teollisuusvakoilu. Kylmän sodan päätyttyä Kiinan johto havahtui maan teknologisesta takapajuisuudesta etenkin sotilasteknologian kohdalla, ja tiedustelupalveluiden toiseksi painopistealueeksi asetettiin teollisuusvakoilu. Kyberoperaatiot alkoivat viimeistään 2000-luvun alusta lähtien näytellä yhä keskeisempää roolia kiinalaisessa teollisuusvakoilussa. Erityisesti MSS on yhdistetty maailmalla lukemattomiin kaupallisesti motivoituneisiin hyökkäyksiin, ja myös esimerkiksi yllä mainittu APT31 on nimetty amerikkalaisiin it- ja finanssialan yrityksiin kohdistuneiden tietomurtojen toteuttajaksi. Sekä NSA:n että Yhdysvaltojen kybervoimien komentaja Keith Alexander kuvaili vuonna 2012 kiinalaista kybervakoilua peräti ”historian suurimmaksi varallisuuden siirroksi”, jossa amerikkalaiset yritykset tekevät yli 250 miljardin dollarin vuotuiset tappiot menetettyjen immateriaalioikeuksien seurauksena.

Sekä strategisessa tiedustelussa että teollisuusvakoilussa kommunistisen puolueen tai virallisen Kiinan attribuointi on kuitenkin hankalaa. Etenkin teollisuusvakoilun kentällä operoi paljon kiinalaisia kaupallisia toimijoita, jotka tavoittelevat omia etujaan ilman minkäänlaista siunausta kommunistiselta puolueelta. Siviilitiedustelupalvelut hyödyntävät myös paljon kyberrikollisia ja alihankkijoita, kuten keväällä 2024 paljastuneet iS00N-vuodot hyvin osoittivat: iS00N on Kiinan Chengudsta käsin operoinut tiedustelun alihankkija, joka suoritti vuodettujen asiakirjojen valossa monentyyppisiä kyberoperaatioita MPS:n ja MSS:n aluetoimistoille sekä Kansan vapautusarmeijalle.

Asevoimien kyberoperaatiot

Kansan vapautusarmeija on Kiinan toinen merkittävä kybertoimija siviilitiedustelupalveluiden rinnalla. Se on keskittynyt ennen kaikkea kyberpuolustukseen ja sodan olosuhteiden kyberoperaatioihin Kiinan lähiympäristössä. Vaikka Kiinalla on aktiivisia aluekiistoja mm. Etelä-Kiinan merellä ja Intian vastaisella rajalla, on Kansan vapautusarmeijan kyberjoukkojen päätehtävänä valmistautua Taiwanin vastaiseen laajempaan konfliktiin, johon osallistuisi myös Yhdysvallat. Osana päätehtäväänsä Kiinan asevoimat valmistautuu käymään myös strategisempaa kybersotaa iskemällä vastustajien kriittiseen infrastruktuuriin sekä harjoittaa kybertiedustelua osin päällekkäisesti MSS:n ja MPS:n portfolioiden kanssa.

Kansan vapautusarmeijan kyberajattelu juontaa juurensa ensimmäiseen Persianlahden sotaan vuonna 1991. Kuten muuallakin maailmassa, Persianlahden sota osoitti Kiinan sotilasjohdolle täsmäaseiden ja edistyneiden johtamisjärjestelmien merkityksen, ja ajoi Kiinan modernisoimaan asevoimansa Yhdysvalloissa vallinnutta ”sodankäynnin vallankumouksen” -ajattelua (Revolution in Military Affairs) mukaillen. Uudistusten seurauksena Kiina on 2000-luvun alkuvuosista lähtien kuvaillut vallitsevaa sodan olomuotoa ”informatisoituneeksi sodankäynniksi”, jossa informaatiovirtojen hallinta nähdään kineettistä tulivoimaa tärkeämpänä ulottuvuutena. Informatisoituneen sodankäynnin tavoitteena on ”informaatioherruus”, millä Kiinassa

tarkoitetaan vastustajaa ajankohtaisempaa ja tarkempaa tilannekuvaa, ja siitä seuraavaa kykyä nopeampaan päätöksentekosykliin ja taistelukentän hallintaan.

Täsmällisemmin Kiina kuvaa nykypäivän sodankäyntiä ”järjestelmien konfliktiksi”, jonka voi nähdä Yhdysvaltojen ”verkostokeskeisen sodankäynnin” (network-centric warfare) kiinalaisena peilikuvana. Järjestelmien konfliktissa tavoitteena on vastustajan koko sotapotentiaalin tuhoamisen sijaan sen ase-, tiedustelu- ja johtamisjärjestelmistä koostuvan ”operaatiojärjestelmän” halvaannuttaminen. Tämä voidaan saavuttaa iskemällä vastustajan järjestelmän avainkykyihin ja kriittisiin solmukohtiin, päävastustaja Yhdysvaltojen kohdalla esimerkiksi satelliittiyhteyksiin tai ilmavalvonta- ja taistelunjohtokoneisiin. Samaan aikaan omaa operaatiojärjestelmää on luonnollisesti kyettävä suojelemaan vastustajan iskuilta.

Solmukohtia vastaan voidaan iskeä monilla tavoin (kineettisesti, elektronisesti, psykologisesti jne.), mutta kybersodankäynnin merkitys on kiinalaisessa ajattelussa vuosi vuodelta korostunut. Suuressa kuvassa kybersodankäynti nähdään siten informatisoituneen sodan ja järjestelmien konfliktin alalajina, ja keskeisenä työkaluna vastustajan operaatiojärjestelmän häiritsemisessä.

Kansan vapautusarmeijan kybertoiminnot ovat parhaillaan perustavanlaatuisten uudistusten alla. Vuonna 2015 käynnistetyissä uudistuksissa perustettiin uusi joukko-osasto, Strategiset tukijoukot (Strategic Support Force, SSF), jonka alaisuuteen keskitettiin sekä avaruus-, kyber- että psykologiset operaatiot. Keväällä 2024 strategiset tukijoukot kuitenkin yllättäen lakkautettiin ja jaettiin kolmeen uuteen joukko-osastoon: informaatiotukijoukkoihin, avaruusjoukkoihin sekä kyberavaruusjoukkoihin. Vastaperustettujen joukkojen työnjako on toistaiseksi varsin epäselvä, mutta informaatiotukijoukkojen arvellaan keskittyvän Kiinan oman operaatioverkon ylläpitoon, kun taas kyberavaruusjoukot ovat päävastuussa asevoimien kyberoperaatioista. Monet asiantuntijat näkevät uudistusten kuvaavan Kansan vapautusarmeijan keskuudessa vallitsevaa epävarmuutta asevoimien kyvystä menestyä visioimassaan informatisoituneessa konfliktissa Yhdysvaltoja vastaan.

Riippumatta Kansan vapautusarmeijan kyberjoukkojen organisaatiosta asevoimien päätehtävänä on kyberpuolustus sekä kybersodan käyminen erityisesti Kiinan lähiympäristössä. Kyberjoukot tähtäävät informatisoituneen sodan kuvan mukaisesti vastustajan operaatioverkon lamauttamiseen ja oman operaatioverkon ja kybertilan suojelemiseen, sekä saavuttamaan informaatioherruuden jo konfliktin ensihetkinä, ennen kineettisten iskujen käynnistymistä. Kyetäkseen tähän kyberavaruusjoukot suorittavat jatkuvaa tiedustelua ja matalan tason kyberoperaatioita omilla vastuualueillaan erityisesti Intian, Koreoiden, Japanin ja Taiwanin vastaisilla alueilla.

Lähialueiden lisäksi Kansan vapautusarmeijan kyberjoukot valmistautuvat käymään myös strategista kybersotaa, jossa isketään esimerkiksi vastustajan kriittistä infrastruktuuria vastaan kaukana taistelujen eturintamasta. Keväällä 2024 Yhdysvaltojen tiedusteluviranomaiset varoittivat kiinalaisten toimijoiden pyrkivän iskemään sopivalla hetkellä tietoverkkoja, vedenjakelua tai energiainfrastruktuuria vastaan. Tavoitteena olisi pyrkiä konfliktitilanteessa estämään Yhdysvaltoja keskittämästä joukkojaan Taiwania puolustukseksi sekä horjuttamaan maan yhteiskunnallista vakautta.

Kiinan asevoimien kyberjoukoilla on ollut ainakin lähihistoriassa merkittävä rooli myös strategisen tason kybertiedustelussa. Kansan vapautusarmeija on osallistunut laajasti MSS-tyylisiin tiedusteluoperaatioihin sekä teollisuusvakoiluun, ja etenkin yksiköt, kuten PLA Unit 61398 ja PLA Unit 61486, ovat tulleet tutuiksi iskuista länsimaisia kaupallisia toimijoita kohtaan. Erityisenä kohteena asevoimien kybervakoilussa ovat olleet sotilasteknologiaa kehittävät yritykset, eikä työ ole valunut hukkaan. Kiinan ilmavoimien uusinta viidennen sukupolven J-31-hävittäjää pidetään laajan tiedusteluohjelman lopputuotteena ja erityisesti Yhdysvaltojen F-35- ja F-22-hävittäjien jäljitelmänä. Kiinalaishävittäjän kehitystyö juontaa juurensa Yhdysvalloissa 2000-luvun alussa tapahtuneisiin ”Byzantine Hades” -hyökkäyksiin, joiden takana oli Kansan vapautusarmeijaan kytkeytyviä yksiköitä, ja joiden myötä hyökkääjät pääsivät käsiksi valtavaan määrään häivehävittäjiä koskevia dokumentteja.

Kohti älyllistynyttä kybersodankäyntiä

Kiinan offensiivisen kybertoiminnan, niin siviilitiedustelupalveluiden kuin asevoimienkin, polttopisteessä on Taiwan. Kiinan näkökulmasta Taiwan on osa Kiinaa, ja Taiwanin palauttaminen Pekingin keskushallinnon alaisuuteen on kommunistiselle puolueelle sekä ideologisesti että pragmaattisesti olennainen prioriteetti. Maiden välillä vallitsee käytännössä intensiivinen hybridisota, jossa kybertoimintaympäristö näyttelee keskeistä roolia.

Kiinan kyberhyökkäykset Taiwania vastaan ovat lisääntyneet merkittävästi koronapandemian alkamisen jälkeen, ja taiwanilaisten hallintolähteiden mukaan hallitusta vastaan kohdistuu viisi miljoonaa eritasoista kyberhyökkäystä tai tunnustelua päivässä. Kulunut vuosi 2024 on ollut erityisen aktiivinen, sillä Taiwanissa järjestettiin tammikuussa presidentinvaalit, joiden lopputulokseen Kiina pyrki puuttumaan laajamittaisilla kyber- ja psykologisilla operaatioilla.

Valmistautuessaan mahdolliseen Taiwanin konfliktiin Kiina pitää kybersuorituskykyjään merkittävänä valttikorttina, mitä vasten Kiinassa on seurattu tarkasti myös Ukrainan sodan tarjoamia kybersodankäynnin oppeja. Yleisesti ottaen kiinalaiset tutkijat ovat olleet yllättyneitä Ukrainan kyberpuolustuksen lujuudesta sekä länsimaisten suuryritysten halukkuudesta tukea Ukrainaa esimerkiksi pilvipalveluita tarjoamalla. Venäjän kybersodan heikkouden saatetaan siten Kiinassa tulkita kasaavan epävarmuutta myös Kiinan Taiwanin ja Yhdysvaltojen vastaisiin suunnitelmiin.

Tulevaisuudessa Kiina uskoo kuitenkin kykenevänsä haastamaan Yhdysvallat tukeutumalla vahvemmin tekoälyn sovelluksiin. Kiinassa uskotaan informatisoituneen sodankäynnin olevan kehittymässä kohti ”älyllistynyttä” sodankäyntiä, jossa tekoäly ja ”älyn herruus” korvaisivat informaation sodankäynnin painopisteenä. Älyllistymisen arvellaan mullistavan myös kybersodankäynnin, ja mikäli Kiina onnistuisi nousemaan tekoälykilvassa Yhdysvaltojen ohi, uskoo se kykenevänsä harppaamaan Yhdysvaltojen ohi myös sotataidollisesti. Tämä tekisi kiinalaisista kybertoimijoista vielä nykyistäkin vaarallisempia.

Majuri, dosentti Juha Kukkola palvelee Maanpuolustuskorkeakoulun Sotataidon laitoksen Venäjä-ryhmässä apulaissotilasprofessorina.

TEKSTI: JUHA KUKKOLA, KUVAT:CHATGPT.

Venäjän kybersodankäyntiä Ukrainassa: Informaatiotuli-iskusta kulutussodankäyntiin

Venäjän helmikuussa 2022 aloittama strateginen hyökkäysoperaatio Ukrainassa olisi voinut olla ohi viikossa. Tämä oli Venäjän asevoimien tavoite. Jos tähän tavoitteeseen olisi päästy, Ukrainan sotaa tutkittaisiin kiihkeästi ensimmäisenä sotana, jossa kyberoperaatiot olivat ratkaisevassa asemassa, ja Venäjän kybersuorituskykyjä varmastikin arvioitaisiin varsin myönteisessä valossa. Näin ei kuitenkaan käynyt.

Venäläinen ajattelu

Ennen Ukrainan operaatiota venäläiset sotilaat ja sotilasakateemikot olivat jo usean vuosikymmenen ajan pohtineet hyökkäyksellisten kybertoimien luonnetta ja mahdollisuuksia. Nämä vaikuttivat, psykologiseen vaikuttamiseen yhdistettyinä, erittäin lupaavilta. Jopa siinä määrin, että konfliktin alussa hankitun informaatioylivoiman nähtiin lähes ratkaisevan tulevaisuuden konfliktit. Kybertoimilla, venäläisittäin informaatioteknologisilla keinoilla, piti olla strategisia vaikutuksia. Niiden itsessään piti mahdollistaa vastustajan taivuttaminen hyökkääjän tahtoon eli sodan voittaminen.

Venäläisten optimismi kybertoimien suhteen kumpusi ajatuksesta, jonka mukaan informaatiovaikuttaminen on luonteeltaan asymmetristä ja epäsuoraa. Sillä voidaan muuttaa merkittävästi materiaalisia voimasuhteita, lamauttaa vastustaja ja saavuttaa yllätys. Kaiken lisäksi informaatiovaikuttamisen piti olla halpaa. Venäläiset eivät olleet yksin ajatustensa kanssa. Esimerkiksi Kiinasta oli jo pitkään kuulunut samanlaisia pohdintoja. Vuosien 2022–2024 tapahtumien valossa näyttäisi siltä, että nämä visiot ovat olleet ainakin osittain harhanäkyjä.

Toimet Ukrainassa

Venäjä pyrki osana helmikuun 2022 hyökkäysoperaatiota toteuttamaan informaatiotuli-iskun. Siinä kineettinen, sähkömagneettinen, psykologinen ja kybervaikuttaminen yhdistettiin muihin epäsuoriin toimiin Ukrainan valtiojohdon, asevoimien ja yhteiskunnan lamauttamiseen riittävässä määrin maan miehittämiseksi. Hyökkäyksellisiä kyberoperaatioita oli valmisteltu noin vuosi. Niitä käytettiin Ukrainan painostamiseksi ja harhauttamiseksi sekä sen liittolaisten tuen rapauttamiseksi ja informaatioylivoiman hankkimiseksi jo ennen sotatoimien alkua. Psykologinen ja kybervaikuttaminen olivat tiiviisti yhteen kietoutuneita.

Varsinaisen hyökkäyksen alkuun liittyi ennen näkemätön tuhoavien kyberhyökkäysten sarja, joka kohdistui Ukrainan asevoimien järjestelmien sekä tietoliikennepalvelujen lisäksi valtiohallintoon, energia-alaan, maataloussektoriin ja finanssialaan. GPS-häirintä aloitettiin välittömästi. Ensimmäisen viikon jälkeen hyökkäysten vakavuus, tosin ei intensiteetti, laski nopeasti. Venäjä kohdisti hyökkäyksiä enenevässä määrin Ukrainan valtiohallinnon viestintää ja mediaa sekä energia-alan kohteita vastaan. Ilma- ja maaoperaation epäonnistuessa kybertoimet eivät kuitenkaan riittäneet horjuttamaan Ukrainan puolustustahtoa.

Informaatiotuli-isku epäonnistui yhtäältä ”tuli” -osuuden, eli ohjusiskujen, jäädessä tavoitteestaan, toisaalta Ukrainan kyberpuolustuksen ja varautumisen johdosta, ja kolmanneksi maa-, meri- ja ilmaoperaatioiden epäonnistuessa. Etenkin muiden epäsuorien toimien, kuten Ukrainan valtiojohdon salamurhien, epäonnistuminen heikensi kyberhyökkäysten kerrannaisvaikutuksia. Eri toimintaympäristöjen, tai domainien, vaikutukset eivät synkronoituneet, eikä Ukraina, ajateltuna järjestelmänä, romahtanut.

Vuoden 2022 kevään jälkeen Venäjä on jatkanut kyberhyökkäyksiä, mutta ne ovat painottuneet ennen kaikkea tiedonhankintaan ja toiseksi psykologisen vaikuttamisen tukemiseen. Tietojen kalastelu, tietomurrot ja -vuodot, palvelunestohyökkäykset, verkkosivujen sotkemiset ja väärennetyn sisällön syöttäminen mediapalveluihin on arkipäiväistynyt. Hyökkäykset ovat kohdistuneet myös Ukrainan tukijoihin ja liittolaisiin. On siirrytty eräänlaisen kyberkulutussodankäynnin vaiheeseen. Hyökkäyksillä ei haeta nopeita vaikutuksia, vaan Ukrainan ja sen tukijoiden tahdon hidasta rapauttamista.

Sodan jatkuessa haktivistien kyberhyökkäyksistä on tullut normaalia. Erilaiset riippumattomat, rikolliset ja tiedustelupalveluiden ohjaamat ryhmät toteuttavat kyberhyökkäyksiä melko sumeilematta valtiollisia, talouselämän ja yhteiskunnallisia kohteita vastaan. Venäjän turvallisuuspalvelu FSB ja sotilastiedustelun päähallinto GRU yhtäältä piiloutuvat näiden toimijoiden taakse ja toisaalta käyttävät niitä omien operaatioidensa julkistamiseen. Ukrainakin käyttää vapaaehtoisia ja aktivisteja omien operaatioidensa toteuttamiseen. Yksityisten, rikollisten ja valtiollisten intressien sekaantuessa, kybertaistelijoiden status sodan oikeussääntöjen puitteissa hämärtyy. Venäjän ja Ukrainan välinen kybertaistelu on käytännössä muuttanut globaalisti kybertoiminnan sallittavuuden rajoja. Se mikä ennen olisi tulkittu äärimmäisen aggressiiviseksi toiminnaksi, on tätä nykyä arkipäivää, eikä yksityisten toimijoiden osallistumista sotatoimiin nähdä ongelmana.

Venäjän epäonnistumisten rinnalla tarkasteltuna Ukrainan onnistunut kyberpuolustus näyttää tarjoavan hyvän mallin kyberturvallisuuden ja -puolustuksen kehittämiseksi. Aikaisempi kokemus Venäjän vihamielisistä kyberoperaatioista, kansainvälisten tietoturvayritysten ja liittolaisten asevoimien kyberjoukkojen tuki, siviiliyhteiskunnan ICT-osaajien mobilisointi ja kybersietoisuuden varmistaminen sekä jatkuva innovointi ovat auttaneet Ukrainaa selviytymään. Näiden oppien siirtäminen sellaisenaan muiden maiden käyttöön on kuitenkin ongelmallista. Ukrainan puolustuksen menestystekijät ovat varsin aika- ja paikkasidonnaisia. Jo pelkästään Ukrainan maantiede vaikuttaa siellä käytävän kybersodankäynnin luonteeseen.

Tulevaisuus

Erityisyydestään huolimatta Ukrainan sota on todennäköisesti murroskohta venäläisessä kybersodankäyntiin liittyvässä ajattelussa. Informaatiotuli-iskun konseptista tuskin luovutaan. GRU on sodan aikana kehittänyt kykyään toteuttaa kohdistettuja, tuhoavia kyberhyökkäyksiä osana ohjus- ja lennokkihyökkäyksiä. FSB:n vakoilu- ja vaikuttamisoperaatiot ovat kehittyneet. Operointi Ukrainan verkoissa on opettanut Venäjälle paljon sodan aikaisen kybertoimintaympäristön luonteesta. Hyökkäyssotaan on liittynyt Ukrainan kybertilan kaappaaminen ja hyväksikäyttö. ICT-infrastruktuurin haltuunottoon liittyviä tekniikoita on

varmasti kehitetty. Venäjä on myös harjoitellut kybertoiminnan käyttämistä peloteviestinnän välineenä yrittäessään vaikuttaa Lännen tukeen Ukrainalle. Tiedustelupalveluiden roolit tiedonhankinnassa, vaikuttamisessa ja sodankäynnissä ovat selkeytyneet.

Vahva usko teknologian suomaan asymmetriaan ja näkemys läntisten yhteiskuntien heikkoudesta saavat Venäjän asevoimat pitämään kiinni kyberaseista, varsinkin kun ne ovat niihin nyt tarttuneet. Hyökkäykselliset, tuhoavat kyberoperaatiot ovat osa venäläistä tulevaisuuden sotataitoa. Venäjä jatkaa kyberavusteisia informaatio-operaatioita vastustajiensa tahdon ja kilpailevien liittokuntien rapauttamiseksi. Kamppailu informaatiotilan hallinnasta on venäläisen ajattelun mukaan jatkuvaa. Uhkia voidaan ennaltaehkäistä kyberkeinoin myös rauhan aikana.

Suurvaltasuhteiden näyttäessä kehittyvän kohti entistä tiukempaa vastakkainasettelua on perusteltua olettaa, että Venäjän näkemysten ja toiminnan kehitystä ohjaa alueellisen tai jopa suursodan mahdollisuus tulevaisuudessa. Ukrainan sota on pakottanut Venäjän kehittämään suorituskykyjään jo sodan aikana. Kun taistelut päättyvät, näiden kykyjen kehittäminen sodan kokemusten perusteella varmasti jatkuu. Lähtökohtana tulee olemaan Ukrainan hyökkäyssodan virheiden ja epäonnistumisten välttäminen.

Teksti perustuu kirjoittajan aikaisempaan julkaisuun ”Suvereenit hiekkamadot - Venäjän kybertoiminta osana valtioiden välistä kamppailua 2000-luvulla.”

Panu Moilanen Kirjoittaja (KTT, LitM) on lehtori ja tutkinto-ohjelmavastaava Jyväskylän yliopiston Turvallisuus ja strateginen analyysi -maisteriohjelmassa.

TEKSTI JA KUVAT: PANU MOILANEN

Taistelua mielissä ja mielistä

Kognition merkitys korostuu sodankäynnissä

Vaikka sodan ja sodankäynnin ytimessä ovat nyt ja tulevaisuudessakin väkivalta ja fyysinen vaikuttaminen, on muiden sodankäynnin ja vaikuttamisen tapojen merkitys lisääntynyt teknologian kehittymisen myötä. Viestinnän ja viestintäteknologian kehitys ovat lisänneet toimintaa informaatioulottuvuudessa, ja kognitiosta on tullut yhä tärkeämpi vaikuttamisen kohde. Kognitio vaikuttamisen kohteena on alkanut korostua niin länsimaisessa kuin venäläisessäkin sodankäyntiajattelussa.

Suomalaisten mielissä sota käsitteenä linkittyy edelleen vahvasti historiallisiin kokemuksiimme Suomen vuosina 1939–1945 käymistä sodista. Kuluneiden kahdeksan vuosikymmenen aikana sodankäynti ja sodan kuva ovat kuitenkin muuttuneet merkittävästi. Suomalaista keskustelua pitkään hallinnut ”syvän rauhan aika” on ollut ohi jo pitkään, ja konflikteja ja taisteluja esiintyy myös muualla kuin reaalimaailmassa. Raja sodan ja rauhan välillä on hämärtynyt.

Ehkä keskeisin sodan kuvaa muuttanut tekijä on teknologian kehitys. Tätä muutosta voidaan jäljittää esimerkiksi ns. taistelutilan käsitteellä. Taistelutila on abstrakti tila, jossa tapahtuvat operaatiot ja muut tapahtumat vaikuttavat jonkin taistelun tai konfliktin etenemiseen. Taistelutilalla voidaan nähdä olevan erilaisia ulottuvuuksia, joista vanhimpia ovat maa-, meri- ja ilmaulottuvuus. Ne muodostavat tällä hetkellä mm. Puolustusvoimien puolustushaarajaon perustan.

Uudempia, teknologian kehittymisen myötä syntyneitä ulottuvuuksia on kaksi. Ensimmäisen maailmansodan aikaan syntynyt sähkömagneettisen spektrin ja avaruuden ulottuvuus muodostui, kun radio otettiin käyttöön viestintävälineenä. Informaatio- ja kyberulottuvuuden alku taas voidaan jäljittää toisen maailmansodan aikana käyttöön otettuihin erilaisiin tehokkaisiin laskennan apuvälineisiin.

Kuudentena taistelutilan ulottuvuutena voidaan nähdä kognition ulottuvuus. Se on ollut osa sotia ja taisteluita niin kauan kuin niitä on käyty, mutta sen merkitys vaikuttamisen kohteena on lisääntynyt ratkaisevasti viimeisten vuosikymmenten aikana ennen kaikkea tietoliikenteen ja mm. sosiaalisen median kehittymisen seurauksena.

Kognitiolla viitataan kaikkiin ihmisen tiedonkäsittelyn prosesseihin, esimerkiksi tiedon vastaanottamiseen, prosessointiin, muistamiseen ja ymmärtämiseen. Käytännössä se tarkoittaa päätöksentekoamme ja tarkoituksenmukaisten vasteiden tuottamista. Nämä vasteet ovat hyvin monenlaisia: ne voivat olla esimerkiksi emootioita, arvoja, asenteita ja mielipiteitä.

Yksilön kognitio ja vasteet ovat kaiken inhimillisen toiminnan perusta. Tietyllä tavalla kognition voidaan nähdä olevan samassa asemassa kuin johtamisjärjestelmien kuuluisassa Wardenin viiden kehän mallissa: kognition toimintaan vaikuttaen tai sen toiminta estäen voidaan vaikuttaa kaikkeen muuhun yksilön toimintaan.

Kognitiivista sodankäyntiä ja refleksiivistä kontrollia

Kognition merkityksen lisääntymisen myötä Nato on ottanut käyttöön uuden kognitiivisen sodankäynnin käsitteen. NATO määrittelee kognitiivisen sodankäynnin toimenpiteiksi, joita toteutetaan synkronoidusti muun voimankäytön kanssa asenteisiin tai käyttäytymiseen vaikuttamiseksi. Tavoitteena on toimijan oman aseman parantaminen. Nämä toimenpiteet voivat olla vaikuttamista, suojaamista tai häirintää, ja niiden kohteena voi olla yksilö tai ryhmä.

Kognitiivinen sodankäynti yhdistää psykologista ja neuraalista vaikuttamista. Tavoitteena on vaikuttaa vastustajan ajatteluun ja tunteisiin muuttaen havaittua ja koettua todellisuutta. Se on siis eräällä tavalla taistelua aivoista ja mielistä – kun psykologisella sodankäynnillä pyritään vaikuttamaan siihen, mitä ajattelemme, kognitiivisessa sodankäynnissä pyritään vaikuttamaan myös siihen, miten ajattelemme.

Vaikuttamisen kohteina ovat siis myös kognitiiviset prosessit, ei vain niiden lopputulos. Esimerkkejä tällaisesta vaikuttamisesta ovat mm. aisti- ja ha-

vaintojärjestelmien kuormittaminen, huomiokykyyn vaikuttaminen sitä suunnaten tai saturoiden, arviointivirheiden aiheuttaminen tai kognitiivisten harhojen katalysoiminen.

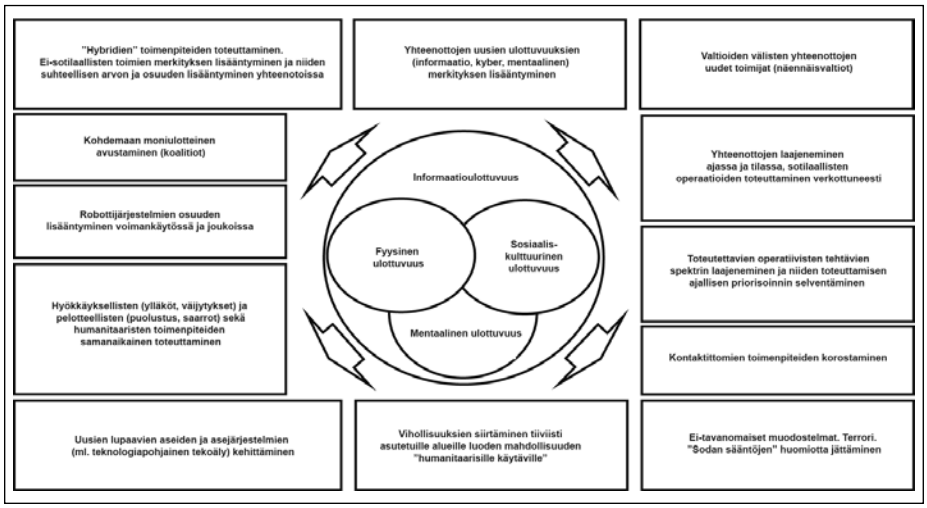
Venäläisessä sotatieteellisessä ajattelussa lähellä kognitiivisen sodankäynnin käsitettä on refleksiivisen kontrollin käsite. Se on perua jo Neuvostoliiton ajalta, ja sen keskeisin tavoite on vastustajan päätöksentekoon vaikuttaminen siten, että vastustaja saadaan tekemään omalta kannaltaan haitallisia, mutta vaikuttajan kannalta suotuisia päätöksiä tai siten, että vastustajan päätöksenteko heikentyy, hidastuu tai estyy kokonaan. Näistä voidaan puhua konstruktiivisena ja tuhoavana tapana.

Käytännössä refleksiiviseen kontrolliin kuuluvat päätöksenteon kuormittaminen luomalla mahdollisimman epäselvä tilanne, näköpiirissä olevien vaihtoehtojen rajaaminen sekä paineen luominen tehdä päätöksiä päätöksentekijän kannalta epäedulliseen aikaan ja puutteellisella informaatiolla. Tässä suhteessa refleksiivinen kontrolli voidaan nähdä myös sotilaallista harhauttamista sivuavana toimintatapana.

Informaatiosodankäynti – keskeinen osa venäläistä sodankäyntiä

Yhtenä merkittävänä refleksiivisen kontrollin muotona voidaan nähdä informaatiosodankäynti. Venäläisen informaatiosodankäynnin historia voidaan jäljittää ainakin 1920-luvulle, jolloin Neuvostoliiton salaiseen poliisiin Tšekaan perustettiin disinformaatio-osasto. Sen tehtävänä oli välittää ennen kaikkea länteen virheellistä tietoa Neuvostoliiton oloista ja vaikuttaa tätä kautta länsimaiden sisä- ja ulkopolitiikkaan.

Monien muutosten seurauksena Tšekasta kehittyi vuonna 1954 perustettu Valtion turvallisuuskomitea KGB. KGB:n informaatiovaikuttamisen pelikirjassa oli kolme perusmenetelmää. Ne olivat Neuvostoliitolle myötämielisten toimijoiden tukeminen, vaikuttaja-agenttien käyttö ja disinformaation levittäminen. Tavoitteena oli Neuvostoliiton etujen ajamisen lisäksi polarisoida ja heikentää kohteina olevia yhteiskuntia.



Kuva 1. Tulevaisuuden sotilaallinen konflikti Smolovyin mukaan.

Vladimir Putin on todennut, ettei Venäjä hävinnyt kylmää sotaa, koska kylmä sota ei koskaan päättynyt. Monien asiantuntijoiden mukaan Venäjä jatkaakin KGB:n pelikirjan menetelmien käyttöä omassa kylmässä sodassaan länttä vastaan.

Nykyistä Venäjän toimintaa informaatioympäristössä määrittelee vuoden 2016 informaatioturvallisuusdoktriini. Doktriinissa tavoitteeksi on asetettu Venäjän suojeleminen toiminnoilta ja tekijöiltä, jotka aiheuttavat vaaraa tai vahinkoa Venäjän eduille informaatiotilassa.

Informaatiosota ymmärretään Venäjällä länsimaita laajemmin, ja se nähdään oleellisena osana sodankäynnin kokonaisuutta. Sotaa käydään venäläisen ajattelun mukaan aina myös informaatiotilassa. Venäjällä ei puhuta lännen tavoin informaatiosodankäynnistä, vaan informaatiopsykologisen sodankäynnin operaatioista, joihin liittyy myös informaatioteknisiä operaatioita.

Informaatiopsykologisen sodankäynnin kohteina ovat vastustajan mieli, moraali ja päätöksentekokyky. Voidaan siis puhua vaikuttamisesta kognitioon, joka tuli tämän artikkelin alussa esille yhtenä taistelutilan ulottuvuutena. Informaatioteknisen sodankäynnin kohteina taas ovat erilaiset tekniset järjestelmät, ja tästä sodankäynnin tavasta lännessä puhutaan yleensä kybersodankäyntinä.

Venäläisen käsityksen mukaan informaatiosota on informaatiotilassa tapahtuvaa valtioiden välistä kamppailua. Sen tavoitteena on vahingon tuottaminen informaatioprosesseille ja kriittiselle infrastruktuurille, vaikuttaminen poliittisiin, taloudellisiin ja sosiaalisiin systeemeihin ja yhteiskunnan horjuttaminen psykologisella vaikuttamisella.

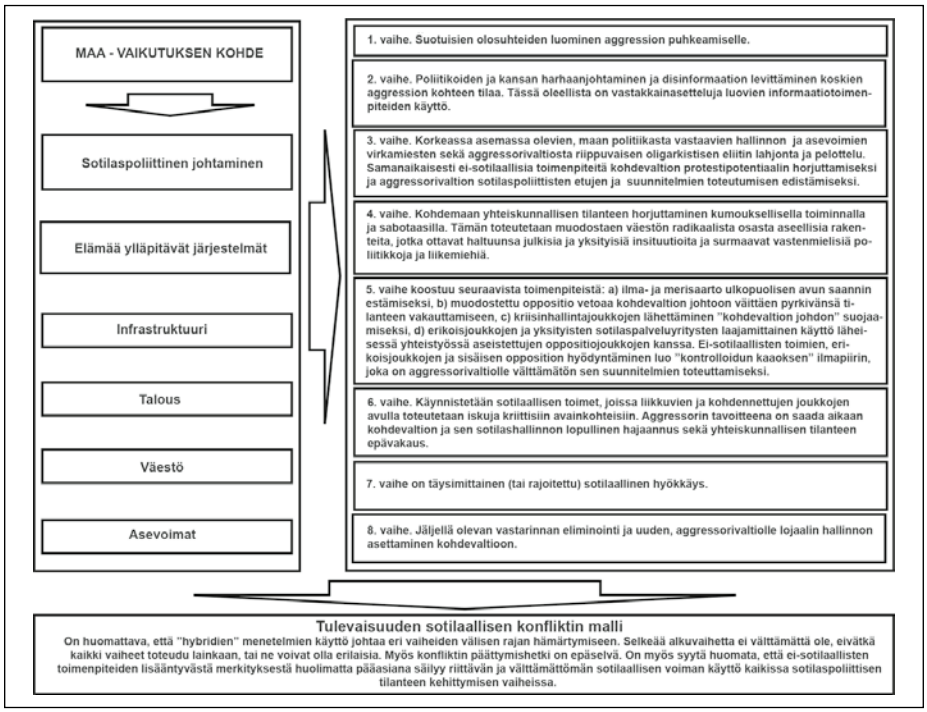
Venäjän ja venäläisen lähestymistavan informaatiosotaan on esitetty yhdistävän kognitiivisen ja teknisen vaikuttamisen osaksi sodankäyntiä paremmin kuin länsimaisen lähestymistavan. Venäläistä näkemystä informaatiosodasta ja modernista sodankäynnistä yleisesti voidaan jäljittää esimerkiksi venäläisten sotatieteellisten aikakauslehtien artikkeleiden avulla.

Venäjän uuden sukupolven sodankäynti

Venäläisessä tutkimuksessa informaatiosodankäynnin tutkimus sijoittuu usein ns. tulevaisuuden sotien tutkimukseen. Lännessä tulevaisuuden sodankäynti nähdään yhä teknisempänä ja yhä enemmän mm. erilaisia informaatioteknologian sovelluksia ja tekoälyä hyödyntävänä. Venäläinen ajattelu informaatiosodankäynnin merkityksen lisääntymisessä sopii tähän ennakoituun kehityskulkuun hyvin. Osa venäläistä sodankäynnin narratiivia on nimittäin jo Neuvostoliiton ajalta periytyvä katkeruus taloudellisesta ja teknologisesta alivoimaisuudesta. Tätä pyritään kompensoimaan mm. länteen verrattuna erilaisilla ja yllättävillä sodankäynnin muodoilla.

Venäläisessä sotatieteellisessä ajattelussa on jo noin kymmenen vuoden ajan puhuttu uuden sukupolven sodankäynnistä, venäjäksi ”война нового поколения”. Termi esiintyi ensimmäisen kerran vuonna 2013 kenraali Valeri Gerasimovin kirjoituksessa, jonka tunnetuin osa on konfliktimalli, jossa ei-sotilaallisten ja sotilaallisten vaikuttamiskeinojen suhteen esitettiin olevan 80/20. Tähän konfliktimalliin on usein viitattu myös Gerasimovin doktriinina, vaikkei kyseessä ole mikään varsinainen doktriini, vaan tiivistys useista nykyisiin sotilaallisiin konflikteihin liittyvistä tutkimuksista.

Venäjän sotatieteellistä ajattelua ja strategiaa tutkinut latvialainen tutkija Jānis Bērziņš on esittänyt yhteenvedon uuden sukupolven sodankäynnistä. Se voidaan määritellä epätyypilliseksi tai epäsymmetriseksi sodankäynniksi, jossa korostetaan muita kuin perinteisen sotilaallisen vaikuttamisen keinoja, ja jossa konfliktin katsotaan etenevän vaiheittain.



Kuva 2. Tulevaisuuden sodan vaihemalli Smolovyin mukaan.

Uuden sukupolven sodankäynnin keskeisin ajatus on se, että sota on jatkuvaa: Venäjä katsoo siis olevansa jatkuvasti sodassa, ja sillä on aina vihollinen tai vihollisia. Tällä hetkellä Venäjän keskeisin vihollinen on länsi ja länsimaiset sivilisaatiot arvoineen poliittisine järjestelmineen ja ideologioineen.

Esimerkiksi syksyllä 2022 Venäjän presidentinhallinto ohjeisti venäläismedioita kertomaan Ukrainassa käytävästä sodasta nimenomaan Venäjän kansan sotana NATOa vastaan, ja loppuvuodesta 2022 Venäjä totesi myös virallisissa lausunnoissaan käyvänsä Ukrainassakin sotaa nimenomaan länttä vastaan.

Venäjän uuden sukupolven sodankäynnissä tärkein taistelutila on ihmisen mieli: tavoitteena on saavuttaa ylivoima toisaalta aseellisesti, mutta ennen kaikkea lannistaen vihollisen siviiliväestö ja taistelevat joukot. Tämän vuoksi sodankäynnissä painottuvat informaatio- ja psykologinen sodankäynti.

Sotilaallisen voiman käyttö pyritään minimoimaan. Tavoitteena voittaa vihollisen siviili- ja sotilashenkilöstö omalle puolelle ja kääntää heidät omaa maataan ja hallintoaan vastaan. Venäjän ja venäläisen lähestymistavan informaatiosotaan on esitetty yhdistävän kognitiivisen ja teknisen vaikuttamisen osaksi sodankäyntiä paremmin kuin länsimaisen lähestymistavan.

Uusi malli kuvaa Venäjän käsitystä tulevaisuuden sodasta

Myös kenraalimajuri A. V. Smolovyi (А.В. Смоловый), joka johtaa Venäjän puolustusministeriön Yleisesikunta-akatemian sotilasstrategista tutkimuskeskusta, on vuonna 2022 Vestnik Akademi Voennyh Nauk (Вестник Академии военных наук) -lehdessä julkaistussa artikkelissaan pohtinut tulevaisuuden sotilaallisia konflikteja.

Artikkeli sisältää kaksi mallia: ensimmäinen malli kuvaa sitä, millaisia tulevaisuuden sotilaalliset konfliktit ovat ja millaisia vaikuttamisen tapoja niissä käytetään (”tulevaisuuden konfliktien muutosvoimat”, тенденции трансформации содержания военных конфликтов будущего), toinen malli taas on malli siitä, kuinka tulevaisuuden sotilaalliset konfliktit etenevät (этапы военного конфликта будущего). Smolovyi nimittää tulevaisuuden sotaa ”yhdistelmäsodaksi” (комбинационная война), jonka ”pääsääntö on sääntöjen puuttuminen, mikä tarkoittaa, että sellaisessa sodassa mikään ei ole kiellettyä”.

Smolovyin – samoin kuin Gerasimovinkin – artikkeliin liittyen on todettava, että virallisesti ne kuvaavat sitä, kuinka Venäjällä nähdään länsimaiden Venäjän vastainen toiminta. Venäläiseen sotilaalliseen ajatteluun katsotaan kuitenkin kuuluvan ns. peilaamisen: vaikka virallisesti kuvataankin muiden havaittua tai ennakoitua toimintaa, niin itse asiassa ennemminkin kerrotaan siitä, mitä on itse tehty tai mitä aiotaan tehdä.

Smolovyi korostaa artikkelissaan informaatiosodankäynnin merkitystä: hänen mukaansa siitä on tulossa erottamaton osa kaikkia sotilaallisia operaatioita, ja keskeistä on, että informaatiosodankäynti aloitetaan jo ennen varsinaisten vihollisuuksien puhkeamista. Tällöin tavoitteena on saavuttaa täydellinen informaatioylivoima, jonka avulla vihollinen voidaan jopa lamauttaa. Tämän saavuttamiseksi vastustajan poliittiseen ja sotilasjohtoon sekä siviiliväestöön tulee kohdistaa massiivista psykologista vaikuttamista.

Myös oma väestö ja kolmansien maiden asukkaat altistetaan propagandalle, jonka avulla pyritään varmistamaan sodankäynnille mahdollisimman suotuisa ilmapiiri. Esimerkiksi Ukrainaan liittyvää mielipiteenmuokkausta alettiin Venäjällä tehdä jo 2000-luvun alussa.

Viime aikoina olemme useissa yhteyksissä havainneet myös Suomeen liittyvää propagandaa: näyttäisi ilmeiseltä, että venäläisten yleisesti melko positiivista kuvaa Suomesta ja suomalaisista pyritään muuttamaan negatiivisemmaksi. Yksi esimerkki tästä on mm. Petroskoissa kesällä 2024 pidetty näytösoikeudenkäynti, jossa Suomi todettiin syylliseksi kansanmurhaan Itä-Karjalassa sotien 1939–1945 aikana.

Informaatiosodankäynnin merkitys ja tärkeys käy selvästi ilmi myös tarkasteltaessa Smolovyin esittämää mallia (Kuva 1) tulevaisuuden sotilaallisista konflikteista ja niiden vaikuttamisen tavoista. Artikkelissa tunnistetut taistelutilan ulottuvuudet on esitetty mallin keskellä.

Kaikkein keskeisimpään rooliin mallissa nousee informaatioulottuvuus, joka vaikuttaa kaikkien muiden ulottuvuuksien taustalla. Sen rinnalla ulottuvuutena nostetaan esille kolme muuta ulottuvuutta: fyysinen ulottuvuus, sosiaalis-kulttuurinen ulottuvuus ja mentaalinen ulottuvuus.

Fyysinen ulottuvuus viittaa perinteiseen fyysisen tuhovoiman käyttöön. Jo pitkään venäläisessä sotilaallisessa ajattelussa on korostettu sitä, että fyysisen voiman käyttö tulee pyrkiä minimoimaan, ja tavoitteeksi tulee asettaa vihollisen sotilas- ja siviilihenkilöstön voittaminen omalle puolelle ja heidän kääntämisensä omaa maataan ja omaa hallintoaan vastaan.

Sosiaalis-kulttuurisessa ulottuvuudessa vaikuttamisen kohteena ovat vastustajan kulttuuri, arvot, perinteet, käsitteet, symbolit ja myytit – oikeastaan siis koko kansallinen narratiivi ja identiteetti. Tämä kansallinen narratiivi ja identiteetti pyritään kiistämään ja sitä pyritään haurastuttamaan kansallisen ja yhteiskunnallisen koheesion vähentämiseksi.

Mentaalisessa ulottuvuudessa vaikuttamisen kohteina ovat ihmisen mieli ja ajattelu, siis kognitio. Tämän ulottuvuuden hyödyntämisen kuvataan usein sijoittuvan nykyiseen ”totuudenjälkeiseen maailmaan”, jossa julkista mielipidettä sekä yksilöiden tunteita ja alitajuntaa pyritään aktiivisesti ja jatkuvasti manipuloimaan.

Mentaalisen sodankäynnin tavoitteeksi on esitetty kansan itsetietoisuuden tuhoaminen sekä kansan henkisen ja sivilisaationallisen perustan muuttaminen. On myös tärkeää huomata, että mentaalisen sodankäynnin aikajänne on pitkä: sitä mitataan venäläisen ajattelun mukaan vuosikymmenissä, jopa vuosisadoissa. Näyttäisi siltä, että venäläisessä sotatieteellisessä tutkimuksessa erityisesti mentaalinen sodankäynti on alkanut teemana painottua vuodesta 2021 alkaen.

Vaiheittain kohti sotaa

Smolovyi esittää artikkelissaan myös tulevaisuuden sodan vaihemallin (Kuva 2), joka kuvaa konfliktin etenemistä sen lietsomisesta vaiheeseen, jossa aggression kohde on täysin alistettu aggressorin valtaan, sen aiempi hallinto on likvidoitu ja tilalle on asetettu aggressorille lojaali hallinto. Mallissa on kahdeksan vaihetta, joiden esiintyminen kussakin konfliktissa Smolovyin mukaan vaihtelee. Vaiheet ovat

1. Aggression puhkeamisen lietsominen.

2. Harhaanjohtaminen ja polarisaation luominen informaatiosodan avulla.

3. Eliitin lahjonta ja pelottelu, protestipotentiaalin katalysoiminen ja edistäminen.

4. Yhteiskunnan horjuttaminen sabotaaseilla ja kumouksellisuutta hyödyntäen.

5. Saarrostus, opposition hyväksikäyttäminen, ”kriisinhallintajoukkojen” ja muun ”avun” lähettäminen, erikoisjoukkojen ja palkkasotilaiden käyttö yhdessä opposition tukemisen kanssa. Kaaoksen luominen.

6. Sotilaalliset toimenpiteet, joiden kohteina ovat kriittiset avainkohteet. Tavoitteena valtion ja sen hallinnon lopullinen hajaannus ja yhteiskunnallinen epävakaus.

7. Täysimittainen (tai rajoitettu) sotilaallinen hyökkäys.

8. Jäljellä olevan vastarinnan eliminointi, aiemman hallinnon likvidointi ja itselle lojaalin hallinnon asettaminen.

Suomen kannalta venäläisen sotatieteellisen ajattelun seuraaminen on kiinnostavaa ja tärkeää, sillä muuttuneessa turvallisuustilanteessa Venäjä ja sen toimet ovat Suomen kannalta yhä vakavammin otettava ja konkreettisempi turvallisuusuhka. Onkin jossain määrin huolestuttavaa tarkastella monia Suomessa viime vuosien aikana havaittuja ilmiöitä ja tapahtumia esimerkiksi Smolovyin artikkelissaan esittämien mallien näkökulmasta. Tässä suhteessa ei voida sulkea pois sitä mahdollisuutta, että Venäjän toimien taustalla olisi tulevan toiminnan ja aggression valmistelu.

Suomen ja suomalaisen yhteiskunnan puolustamiselle yhä laajempi vaikuttaminen nimenomaan kognitiivisessa ulottuvuudessa on haaste. Valtioneuvoston puolustusselonteossa vuodelta 2021 puhutaan informaatiopuolustuksesta, joka määritellään maanpuolustuksen toimintojen suojaamiseksi ulkoa ohjatun ja muun vahingoittamistarkoituksessa tehdyn viestinnän vaikutuksilta siten, että se on osa koko yhteiskunnan suojautumista informaatiovaikuttamiselta.

Koko yhteiskunnan suojautumista informaatiovaikuttamiselta ei kuitenkaan ainakaan julkisesti ole laajemmin keskusteltu, eikä tälle ole Suomessa määritelty vastuutasoa. Tällaiselle keskustelulle, vastuutaholle ja myös käytännön toimille on kuitenkin välitön tarve, sillä turvallisuustilanne ei tässäkään suhteessa ole ainakaan helpottumassa.

Kirjoittaja toimii Maanpuolustuskorkeakoulun Sotataidon laitoksen Simulaattori- ja sotapeliryhmässä Järjestelmäpäällikkönä

TEKSTI JA KUVAT: MATTI RUOTSALAINEN

Elektroninen sodankäynti Ukrainassa

Tämä artikkeli on jatkoa aiemmin Viestimies-lehden numerossa 2/2021 ilmestyneeseen artikkeliin. Aiemmassa artikkelissa käsiteltiin teoriatasolla Venäjän federaation elektronisen vaikuttamisen (ELVA), eli elektronisen häirinnän ja elektronisen tiedustelun kykyjä (ELTI). Keväästä 2022 alkaen olemme saaneet seurata lähes reaaliaikaisesti Venäjän asevoimien onnistumisia ja epäonnistumisia elektronisen sodankäynnin (ELSO) osalta. Tässä artikkelissa pohditaan – julkisiin lähteisiin nojautuen – ongelmia, toimintatapoja ja huomioitavia asioita, joita eri tasoilla toimivien johtamisjärjestelmä (JOJÄ) joukkojen tulisi pohtia ELSO:n osalta.

Venäläisen moottoroidun jalkaväkiprikaatin komentopaikka siellä jossakin keväällä 2022

”Mitä pirua se teidän rosvolaumanne touhuaa Majuri?” raivosi prikaatin komentaja eversti Grigori edessään asennossa seisovalle majurille komentovaunun takana. ”Ensin tukitte tiet ja minun patteristot eivät pääse ryhmittymään ajoissa. Sitten päätätte tukkia ensimmäisen portaan hyökkäyksen radioverkot juuri kun hyökkäys alkaa. Sitten ilmatorjunta ilmoittaa, että valvonta- tai tulenjohtotutkia ei voi käyttää, koska TE häiritsette niitä. Ilmoitatte viereisen prikaatin pataljoonan komentopaikan maalina omalle tykistöllemme ja lopuksi ette voi tehdä mitään noille lentäville ruohonleikkureille, joita pörrää pataljoonieni päällä, pommittaa niitä jauhelihaksi ja kuvaa kaiken livenä Youtubeen koko Lännen naurettavaksi!” karjuu Grigori ja osoittaa tälläkin hetkellä kaukaisuudessa lentävään Bayraktar -lennokkiin. ”Minun pitäisi ampua sinut ja köyttää ruumis vaununkannelle varoitukseksi lopuille foliohatuille!” komentaja päättää ryöpytyksen ja sysää majurin kauemmas, kuin estääkseen itseään toteuttamasta uhkaustaan.

Majuri Ivanov, prikaatin elektronisen sodankäynnin komppanian päällikkö, puree huultaan, jotta ei alkaisi karjua takaisin everstille. Kaikki mitä Grigori kuvaili, oli tapahtunut, mutta ei heidän komppaniansa toimesta. Armeijan ELSO-pataljoonan kuorma-autot olivat juuttuneet mutaan yrittäessään päästä tukemaan kärjen hyökkäystä ja tukkineet tien. Hänen komppaniansa käytti tela-ajoneuvoja, mutta sitä oli turha kertoa everstille. Myöskään sitä ei kannattanut kertoa, että Grigorin omat pataljoonat olivat käyttäneet vääriä itse päättämiään radiotaajuuksia ”koska niin oli tehty aina”, kun taas hänen komppaniansa oli erikseen käsketty lamauttaa samalla taajuuksilla toimivat ukrainalaisten radioverkot.

Tutkien taajuuksia häirittiin sotilaspiirin ELSO-helikoptereilla ja Ivanov vain välitti tiedon ylempää – syytön hän siihen oli. Viereisen prikaatin pataljoonan komentopaikan osoittaminen maaliksi oli prikaatin tiedustelupataljoonan ja prikaatin esikunnan syytä. Hän oli vain ilmoittanut tunnistamattomista hyppivätaajuusradioista prikaatien sauma-alueella. Ei hänellä ollut käytössään armeijan tilannekuvaa, viereisen prikaatin viestiperusteita tai edes tietoa, että heillä oli uudet digitaaliset radiot käytössään! Jonkun ylempää olisi pitänyt varmaan tarkistaa, että oliko alueella oma joukko ennen, kuin alkoi ammuttaa tykistöllä oman vastuualueen ulkopuolelle. Kaiken lisäksi komentaja oli itse käskenyt, että prikaatin sekä armeijan lennokkeja ei saanut häiritä missään tapauksessa – ei ollut Ivanovin syytä, että ukrainalaisten lennokit käyttivät samoja taajuuksia kuin heidän omansa. Eikö lennokeista eroon pääseminen kuulunut ilmatorjunnalle, jonka työnä oli ampua esineitä alas taivaalta? Ei niiden näkemiseen tutkaa tarvinnut – tuolla tuo yksikin lentää.

Juuri kun Ivanov aloitti puolustuspuheensa, hänet keskeytti korvia vihlova vihellys. Ensimmäiset ukrainalaiset kranaatit iskeytyivät komentovaunun läheisyyteen ja paineaalto paiskasi molemmat upseerit maahan. Ukrainalaisten elektroninen tiedustelu oli paikantanut heidät.

Taustat

Venäjän elektronisesta sodankäynnistä on annettu aikanaan kuva kaikkivoipaisena vastapuolen 1800-luvulle pakottavana luonnonvoimana. Keväästä 2022 alkaen on kuitenkin saatu muistutus siitä, että elektroninen sodankäynti on oman osapuolen toimintaa tukeva toimiala/aselaji, jonka tehokas käyttö vaatii joukolta hyvin onnistunutta yhteistoimintaa ja johtamista, tehokasta taajuushallintaa, sekä oikeanlaista ryhmitystä.

Artikkelin materiaali perustuu julkisiin lähteisiin ja lähteet on lueteltu artikkelin lopussa. Lukijan on hyvä palauttaa mieliin kirjoittajan aiempi artikkeli vuodelta 2021, ja palautella mieleen ainakin teoriatasolla Venäjän federaation ELVA- ja ELTI-joukkojen kokoonpanoa ja kalustoa.

Lähteitä lukiessa pitää muistaa lähdekriittisyys. Kumpikaan osapuoli Ukrainassa tuskin haluaa kertoa vapaasti, että

vastapuolen häirintä toimii järjestelmiään vastaan tai, että he itse häiritsevät omia joukkojaan. Varmuudella paikkansa pitävät havainnot ovat rajattuja. Kuitenkin taktiset reunaehdot ja fysiikan asettamat rajat onnistuneelle ELSO:lle ovat sinänsä mitattavissa sekä mallinnettavissa ja niitä yritän tässä artikkelissa nostaa esiin.

Ensimmäinen vaihe – Nopea hyökkäys teiden suunnassa

Sodan alkuvaiheessa Venäjä hyökkäsi useissa suunnissa mekanisoiduilla joukoilla teitä seuraten. Useista pataljoonan taisteluosastoista koostuvat armeijat, sotilaspiirien alaisuudessa, pyrkivät mahdollisimman nopeasti eteenpäin kapeissa ryhmityksissä. Venäjän ELVA vaikutti toimivan tehokkaasti ainakin Ukrainan ilmapuolustukseen. Valvonta- ja maalinosoitustutkien käyttö ilmeisesti estyi merkittävästi hyökkäyssuunnissa.

Venäjän ELVA ja omien ilmatorjuntajoukkojen uudelleen ryhmittyminen heti sodan alkaessa rajoitti Ukrainan ilmapuolustuksen kykyä toimia ensimmäisten päivien aikana. Muutamien päivien jälkeen ukrainalaisten ilmapuolustus

Kuva 1. Esimerkki prikaatin taajuushallinnasta VHF-alueella. Punaisella olevia taajuuksilla ELTI- ja ELVA-joukot saavat vapaasti toimia. Vihreällä oleville taajuuksille saa tiedustella ja vaikuttaa vain eri luvalla.

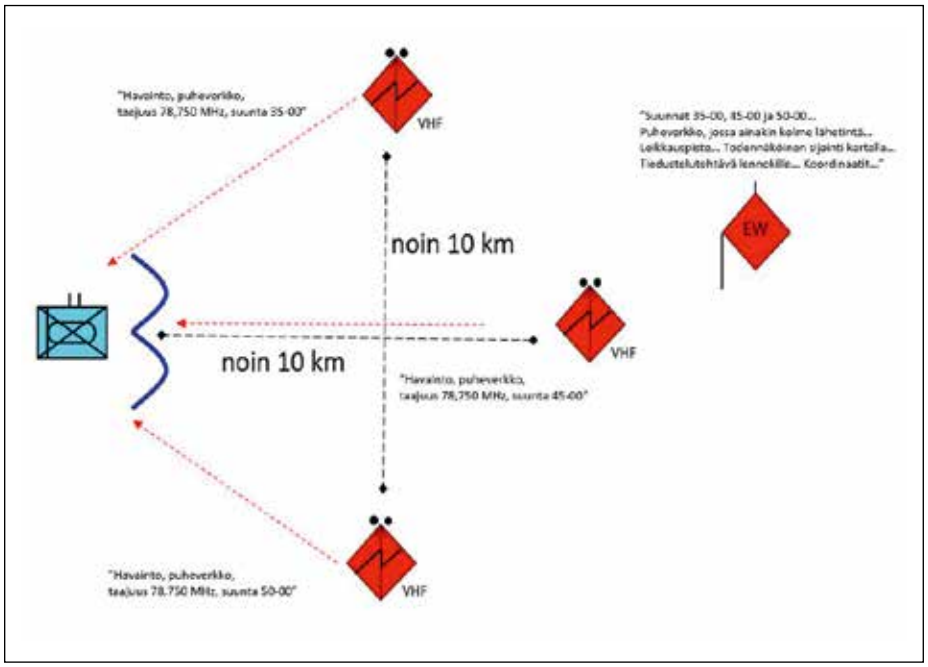
kuitenkin pakotti Venäjän kiinteäsiipiset koneet henkensä kaupalla puiden latvojen tasalle tai pysymään omassa ilmatilassaan. Vaikuttiko tähän häirinnän vähentyminen, pidemmät häirintämatkat hyökkäyskiilojen edetessä, vai ylipäätään ilmatorjuntajoukkojen edullisempi ryhmitys?

Häirintä kuitenkin todennäköisesti vaikutti myös venäläisten omiin järjestelmiin. Tästä kertoo se, että sodan alkuvaiheessa nähtiin useita videoita Bayraktar -lennokeista tuhoamassa venäläisiä ilmatorjuntajärjestelmiä. Joissain videoissa nähtiin Pantsir-S1 -ajoneuvoja tuhoutumassa tutkat ja tornit marssilukituksessa. Bayraktar -lennokkeja ehdittiin hetken ajan ylistää uutena ihmeaseena, mutta videot niiden osalta loppuivat kuitenkin lyhyeen. Tämä kielii Venäjän ilmatorjunnan saaneen itsensä takaisin tilanteen tasalle.

Toinen havainto taistelujen alkuvaiheessa oli salaamattomien ja osittain kaupallisilla taajuuksilla toimivien radioiden sekä ukrainan matkapuhelinverkossa toimivien matkapuhelimien laaja käyttö venäläisten toimesta. Syinä tähän on voinut olla omien radioverkkojen tahaton häirintä, omien johtamisjärjestelmien puute tai toimimattomuus, sekä mahdollisesti salattujen radioyhteyksien salausavaimien puuttuminen. Suunnitelmattomuudesta salaamattomien radioiden käytössä kielii selväkielinen viestittäminen radioverkoissa. Alkeellisen puheenpeitteistön tekeminen ei vaadi montaakaan minuuttia. Yhteyksien puuttuminen on siis tullut yllätyksenä, johtunut epäpätevyydestä tai molempia.

Nämä ongelmat kielivät kolmesta asiasta, joiden pitää onnistua, jotta ELVA- ja ELTI-joukot voivat toimia tehokkaasti. Ensimmäinen on onnistunut taajuushallinta. Kaikille taajuusalueille: HF, VHF, UHF, SHF jne. pitää varata taajuuskaistat omien joukkojen käyttöön, joita ei saa tiedustella tai häiritä. Jollakin johtamisen tasalla pitää taajuuksiin liittyen käydä keskustelu siitä paljonko taajuuksia tarvitaan omaan käyttöön ja millaiset alueet jäävät tiedustelulle sekä vaikuttamiselle. Etukäteen hankittu tiedustelutieto vihollisen käyttämistä taajuuksista kullakin taajuusalueella helpottaa työtä. Siksi rauhanajan koulutus toteutetaan pääsääntöisesti kaikissa maissa eri taajuuksilla kuin poikkeusolojen viestitoiminta. Näin vastapuoli ei voi etukäteen hankkia tarvittavaa tietoa käytetyistä taajuuksista, vaan tiedustelu pitää toteuttaa taisteluiden aikana.

Hankalaksi tilanne muodostuu jos kumpikin osapuoli toimii samalla kalustolla



Kuva 2. ELTI-asemien sekä johtoaseman edullinen ryhmitys radiolähetteen paikantamista varten.

ja samalla taajuusalueella, mikä todennäköisesti oli tilanne sodan alkuvaiheessa. Kummallakin osapuolella oli käytössään esimerkiksi Neuvostoliiton aikaisia ilmatorjuntajärjestelmiä (BUK ja S-300) ja esimerkiksi Suomessakin tuttuja vaunuradioita, kuten LV623. Mitä useammalla johtamistasolla ELSO-joukkoja on sitä tarkempaa suunnittelua ja käskytystä taajuushallinta vaatii.

Jos prikaati-, armeija- ja sotilaspiiritasolla kaikilla on esimerkiksi HF-häirintäkyky, ja kaikki ovat maantieteellisesti samalla alueella, pitää kaikilla ELSO-joukoilla olla tiedossa kaikkien alueella olevien omien joukkojen käyttämät taajuudet. Muuten ylemmän tason ELVA-yksikkö voi vahingossa häiritä alemman tason joukkoja. Onnistuminen vaatii myös sen, että suunnitelma kyetään jalkauttamaan kaikille omille joukoille.

Kaikkien on haluttava ja osattava käyttää oikeita taajuuksia, kanavapaikkoja ja avaimia – ei vain ELSO-yksiköiden. Jos taajuushallinta ei onnistu, niin ELTI-resursseja menee hukkaan, kun tiedustellaan ja paikannetaan vahingossa omia joukkoja. Tällöin voi vain toivoa, että joukko tunnistetaan omiksi ennen vaikuttamista. Lisäksi ELVA-resursseja menee hukkaan, kun häiritään omia joukkoja ja todennäköisesti pahennetaan yleistä tilannetta omalla toiminnalla.

Toisena onnistumisen edellytyksenä on ELSO-joukkojen oman toiminnan tehokkaasti mahdollistava ryhmittyminen. Jotta ELTI:sta on hyötyä, pitää sen kyetä ryhmittymään ennen hyökkäyksen alkua. Tällöin ELTI kykenee tuottamaan tiedustelutietoa hyökkäyssuunnittelun tueksi, maalittamaan kohteita tulenkäyttöä varten ja osoittamaan taajuuksia sekä kohteita ELVA:lle.

Radiolähetteen paikantaminen maasijoitteisilla ELTI-asemilla riittävän tarkasti vaatii kolme asemaa. Jokaisen aseman saadessa tiedusteltavasta lähetteestä kompassisuunnan lähete voidaan paikantaa johtokeskuksessa näiden kolmen suunnan leikkauspisteeseen. Tarkin paikannus saadaan teoriassa, kun ELTI-asemat, yhdessä tiedusteltavan lähetteen kanssa, muodostavat ylhäältä tarkasteltuna tasasivuisen neliön.

Julkisissa lähteissä paikantamistarkkuudeksi maasijoitteisilla asemilla mainitaan 2–10 % tiedusteluetäisyydestä. Jotta siis voidaan paikantaa kohteita alle 1000 m paikantamistarkkuuteen vaati ELTI-ryhmitys leveydekseen ainakin kymmenen kilometriä. Jotta prikaati voi turvallisesti ryhmittää ELTI-asemia tälle leveydelle, pitää koko prikaatin ryhmityksen olla yli kymmenen kilometriä leveä.

Amerikkalaisen ATP 7-100.1 ohjesäännön mukaan Venäläisen prikaatin ryhmityksen leveys on tavoitetilanteessa alle kahdeksan kilometriä. Eli jotta ELTI-asemat edes teoriassa pääsevät edullisille paikoille, on niiden ryhmityttävä oman prikaatin vastuualueen ulkopuolelle tai prikaatin ryhmityttävä merkittävästi leveämmälle kuin ohjesääntö sanoo.

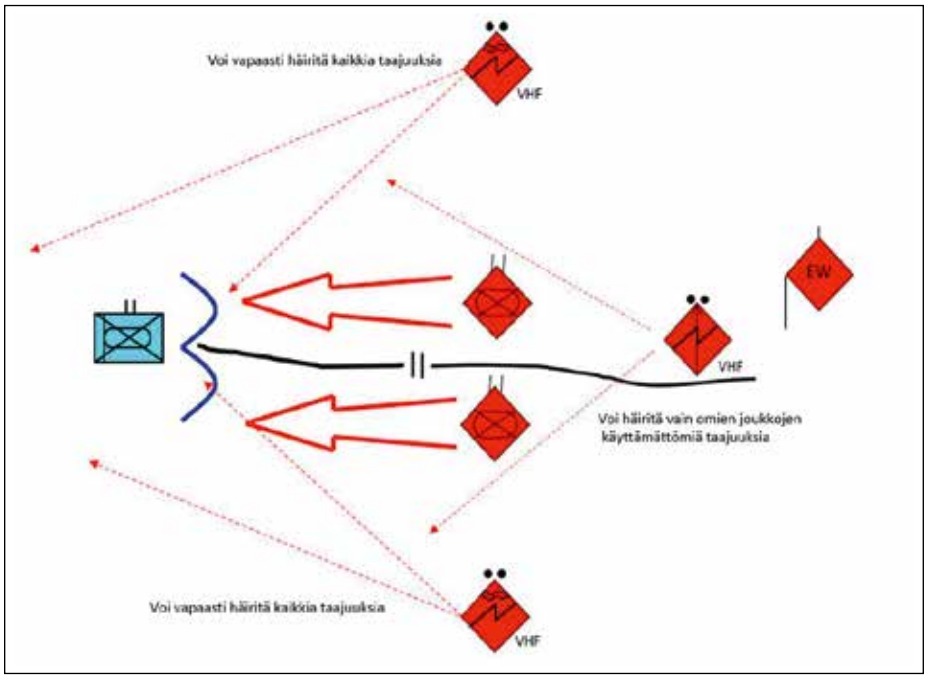
ELVA-joukot ovat parhaimmillaan ryhmittyessään mahdollisimman lähel-


EMPOWERING THE BEST
TO ALWAYS DO THEIR BEST
SAVOX
www.savox.com

le häirittäviä kohteita. Mitä lähempänä häirintäasema on sitä tehokkaammin ja pidemmälle vihollisen ryhmitykseen voidaan häirinnällä vaikuttaa. Julkisissa lähteissä mainitaan venäläisten VHF-häirintäasemien ryhmityksen olevan 2–3 km hyökkäyksen takana. Häirintä halutaan suorittaa omien joukkojen sivuilta, suuntaavilla antenneilla kohti vihollista. Tällöin vältetään omien verkkojen häirintä, vaikka vihollinen toimisi samoilla taajuuksilla omien joukkojen kanssa. Jos ELVA-asemat joutuvat häiritsemään vihollista omien joukkojen takaa pitää omien verkkojen lamauttaminen estää onnistuneella taajuushallinnalla, tai ajoittamalla se oikein hyökkäyksen kanssa.

Ryhmitykseen vaikuttaa myös kalusto ja sen asettamat vaatimukset ELTI- ja ELVA-joukoille. Asemapaikkavaatimukset ovat samanlaisia kuin viesti- ja tutka-asemilla. Asema pitää pystyä maadoittamaan, antennit tulee saada vapaaksi lähiesteistä (puiden latvojen yli) ja aseman välittömässä läheisyydessä ei saa olla sähkö- tai voimalinjoja. Taajuusalueesta riippuen ELSO-asemat vaativat myös optisen yhteyden (LOS line of sight) kohteeseen. Venäläisestä ELSO-kalustosta pääosa on kuvien perusteella varustettu käsikäyttöisillä, noin 10 m korkeilla mastoilla, joten puuston korkeus rajaa asemapaikan valintaa. ELSO myös kilpailee samoista ryhmitysalueista esimerkiksi ilmatorjunta- ja viestijoukkojen kanssa. Ryhmitysalueiden koordinointi vaatii siis myös oman suunnittelunsa ja käskemisensä.

Sodan alussa teiden suunnassa pitkissä marssirivistöissä etenevät venäläiset joukot eivät kyenneet helposti levittämään ryhmitystä peitteisessä maastossa. Huonoilla teillä olevissa marssirivistöissä ELSO-yksiköiden pitäisi olla aivan marssijonojen kärjessä ehtiäkseen ryhmittyä ajoissa tukemaan hyökkäystä yllättävissä tilanteissa. Nyt ELSO-asemat olivat jumissa marssirivistöissä, liian takana kyetäkseen toimimaan tehokkaasti ja omien joukkojen kannalta turvallisesti. Samoista ryhmityspaikoista kilpailivat myös ilmatorjunta- ja viestijoukot aiheuttaen omat ongelmansa. Tämä yhdistettynä huonoon taajuushallintaan ELSO:lla todennäköisesti aiheutettiin yhtä paljon ongelmia omille, kuin vihollisen joukoille. Venäjällä on usealla tasolla ELSO-yksiköitä pataljoonataisteluosastosta sotilaspiiriin, joten ongelmat todennäköisesti moninkertaistuivat, kun samalle tiestölle tungettiin useiden johtoportaiden ELSO-joukot huonoilla johtamisyhteyksillä.



Kuva 3. ELVA-asemien edullinen ryhmitys häirintää varten.

Toinen vaihe – ”Asemasota”

Venäjän siirtäessä joukkojen käytön painopisteen Itä-Ukrainaan, ja rintamalinjojen vakiintuessa Ukrainan vastahyökkäysten jälkeen 2023 vuoden alussa, ongelmat ELSO:n osalta vähenivät. Samalla havainnot Venäjän ELTI:n ja ELVA:n vaikutuksesta ukrainalaisiin kasvoivat. Paikallaan olevat ja selkeät rintamalinjat mahdollistivat ELSO-joukoille paremman ryhmityksen. Tiedusteluasemat saatiin levitettyä sopivasti oikeille etäisyyksille, omien joukkojen suojaamana ja häirintäasemat saatiin ryhmitettyä sivustoille.

Eri johtamistasoilla ELSO:n osalta ehdittiin sopia alue- ja taajuusvastuut, eli mikä joukko tiedustelee tai vaikuttaa milläkin alueilla ja mihinkin viholliseen. ELTI ehti tiedustella ajan kanssa vihollisen käyttämiä taajuuksia, alueita sekä varataajuuksia. Tieto myös ehdittiin jakaa tarvitsijoille ja ELVA suunnitella osaksi muuta tulenkäyttöä ennen hyökkäystä. Lisäksi omien järjestelmien käyttöä osattiin suunnitella ja tahdittaa esimerkiksi häirinnän kanssa. Ukrainalaiset huomasivat, että usein jonkin venäläisten asejärjestelmän käyttöä tai hyökkäystä edelsi tiettyjen taajuusalueiden häirinnän lakkaaminen. Esimerkiksi GNSS:n (global navigation satellite system) ja lennokkien ohjaussignaalien häirinnän päättyminen edelsi venäläisten omien lennokkien käyttöä.

Sodan kumpikin osapuoli on siirtänyt ELSO:n pelossa komentopaikkansa rakennuksiin, ja alkanut luottamaan johtamisessa lähinnä kaapeliyhteyksiin. Kaikki radiolähettimet joita komentopaikalla on pakko käyttää ovat kaukokäytettyinä mahdollisimman kaukana komentopaikasta. Jos paikannettuun lähettimeen ammutaan epäsuoralla tulella, niin komentopaikka henkilöstöineen säästyy ja vain hajonnut radiolähetin tarvittaessa korvataan. Kasvaneena ELSO-elementtinä rintamalla on ollut GNSS-alueen häirintä. Aiemmin venäläisillä prikaateilla oli yksi GNSS-alueelle tarkoitettu häirintäasema – R-330Zh. Ukrainan saatua GNSS-ohjattuja aseita lännestä, kuten HIMARS-raketteja ja Excalibur-ammuksia tykistölle, on GNSS-häirinnän tarve kasvanut merkittävästi. Yhdellä häirintäasemalla prikaati ei voi suojata koko ryhmitystään GNSS-hakeutuvilta ammuksilta tai lennokeilta. HIMARS-järjestelmien tullessa rintamalle ne kykenivätkin tuhomaan varsin vapaasti tiedustelun löytämiä kohteita. Ajan kuluessa kuitenkin häirintäjärjestelmien määrä kasvoi, ja tällä hetkellä GNSS-ohjattuja ampumatarvikkeita voidaan käyttää vain hyvin rajoitetusti. Lähes kaikki maalit, joihin arvokkaita ammuksia olisi järkevä käyttää, kuten huoltokeskukset, tykistön tuliasemat ja komentopaikat, ovat häirintäasemien suojaamia.

Merkittävin muutos ELSO:ssa on ollut erilaisilta lennokeilta suojautuminen.

Lennokkien käyttö on lisääntynyt valtavasti. Lennokkeja on käytössä 500 € eurosta ylöspäin maksavista kaupallisista lennokeista, joiden käyttöetäisyys on satoja metrejä, aina satojen kilometrien päähän toimiviin sotilaskoneisiin. Lennokkien torjunta on osoittautunut hankalaksi. Ammusaseilla osuminen pieneen kohteeseen on hankalaa, ja lennokki on usein joko liian pieni tai liian halpa ohjuksilla tuhottavaksi. Häirintä on osoittautunut ainoaksi ”halvaksi” ja riittävän tehokkaaksi aseeksi rajoittaa lennokkien toimintaa. Osa lennokeista kyetään lamauttamaan häiritsemällä niiden paikannusta GNSS-häirinnällä. Menettäessään paikannussignaalin osa kaupallisista lennokeista laskeutuu, jää leijumaan paikalleen tai palaa takaisin lähtöpaikalle. Toinen vaihtoehto on ”spoofing” eli väärän sijainnin lähettäminen ELVA-asemalla.

GNSS-häirinnän lisäksi lennokkeja voidaan torjua häiritsemällä niiden ohjaus- tai videosignaalia. Osa kaupallisista lennokeista voi käyttää ohjaussignaalina matkapuhelinverkkoa, ja osa suoraa radioyhteyttä ohjaimen ja lennokin välillä. Suoraa radio-ohjausta käyttävät lennokit, jotka kykenevät välittämään videokuvaa, toimivat yleensä 2–8GHz alueella. Näiden signaalien häirintään soveltuvaa kalustoa on tullut merkittävissä määrin rintamalle. Nyt nähdään juoksuhautojen reunalla häirintälähettimiä suojaamassa joukkueen tukikohtaa, ja jopa yksittäisissä panssarivaunuissa. Sotilaskäytössä olevat suuremmat ja kalliimmat operatiivisen tasan lennokit voivat käyttää satelliittiohjausta, mutta ELSO:n kyvystä vaikuttaa näihin ei ole havaintoja.

Mielenkiintoinen havainto on ollut Ukrainan Starlink -terminaalien käyttö. Järjestelmällä toteutetaan internet-yhteys satelliittien kautta, jota voidaan jakaa vaikka WLAN-tukiasemalla useille käyttäjille. Ukraina on käyttänyt näitä tiedustelupartioiden yhteytenä rintamalinjojen takana, tykistön tuliasemissa ja rintamavastuussa olevien komppanioiden suoja-asemissa tarjoamassa yhteyttä kotiin.

Venäjä ei ole kyennyt vielä tässäkään vaiheessa estämään näiden käyttöä edes välittömässä rintaman läheisyydessä.

Havainnot

Mitä johtamisjärjestelmäjoukot sitten voivat näistä asioista ottaa mahdollisesti opikseen ja pohdittavakseen?

Ensimmäinen nosto

ELSO on vaarallisimmillaan, kun vihollinen pääsee suorittamaan valmistellun hyökkäyksen. Jos vastustaja pääsee vapaasti omalla alueellaan vuorokauden tai kahden ajan ryhmittymään, tiedustelemaan ja seuraamaan vastatoimia, niin ELTI:n ja ELVA:n kyky vaikuttaa taistelunkulkuun kasvaa. Mikäli voimme painostamalla rajoittaa vihollisen vapaata ryhmittymistä ja pakottaa se reagoimaan ELSO:n toimintamahdollisuudet heikkenevät.

Toinen nosto

Taajuushallinnalla voidaan vaikeuttaa ELSO:n toimintaa. Jos omia taajuuksia voidaan suunnitella vihollisen käyttämien taajuuksien sekaan niin se kannattaa tehdä. Ylipäätään tieto millä kaikilla taajuuksilla omat ja alueella toimivien muiden joukkojen järjestelmät toimivat, ja miten ne käyttäytyvät eri moodeissa (taajuudet, hypintä, avaintenvaihto jne) on tärkeää. Taistelukenttä on perin kiusallinen paikka huomata järjestelmän toimivan eri tavalla kuin on harjoitellut.

Kolmas nosto

Komentopaikat pitää saada suojaan ja radiolähettimet saada niistä mahdollisimman kauas. Aikaikkuna ELTI:n havainnosta havainnon varmistavaan lennokkiin ja sitä seuraavaan tuli-iskuun on lyhentynyt merkittävästi. Kaukokäytetyt radiolähettimet, kaapeliyhteydet ja suojan hakeminen rakennuksista/linnoitteista on selviytymisen kannalta tärkeää kymmenienkin kilometrien päästä etulinjasta.

Neljäs nosto

GNSS-signaaliin toimintansa nojaavat järjestelmät eivät välttämättä toimi taistelualueella. Oli kyseessä sitten GNSS-paikannus ammuksissa ja asejärjestelmissä tai GNSS-kellosignaalin tarvitsevat laitteet. Vaihtoehtoisia toimintatapoja tai teknisiä ratkaisuja pitää olla ja ne pitää harjoitella.

Viides nosto

Lennokkien vapaan toiminnan kiistämiseen pitää valmistautua kaikilla tasoilla. Toistaiseksi (katsotaan mitä tekoäly tuo tullessaan) ohjausyhteyden häiritseminen on ”taloudellinen” ratkaisu. Joissakin maissa on hankittu tekoälyavusteisia optiikkoja käsiaseisiin kineettisenä torjuntaratkaisuna.

Kuudes nosto

Erilaiset kaupalliset välineet järkevillä tietoturvaratkaisuilla mahdollistavat paljon. Ukrainassa kumpikin osapuoli on ollut enemmän tai vähemmän riippuvainen Ukrainan matkapuhelinverkoista. Starlink on myös kaupallinen tuote, joka Yhdysvaltojen kustantamana tarjottiin Ukrainan käyttöön. Lisäksi Ukrainassa on käytössä valtava määrä erilaisia sovelluksia, jotka toimivat internetin päällä. Nämä mahdollistavat varsin taloudellisen ratkaisun, kun johtamislaitteita pitää hankkia nopeasti ja paljon. Vähintäänkin varmentavana yhteytenä niillä on paikkansa taistelukentällä.

Seitsemäs nosto

Joukon tunnistaminen puheradioverkkojen kautta pitää tehdä mahdollisimman vaikeaksi. Tiettyjen radioiden käyttämistä vain tietyllä joukkotyypillä tai johtoportaalla pitää välttää, ja peitteistöjä tulee käyttää kaikissa verkoissa. ELTI:n kyky luokitella havaittu kohde vaikeutuu ja tällöin kaupallisiakin radioita voidaan hyödyntää.

Lähteet:

EW LESSONS LEARNED Russian Hybrid Warfare in Ukraine. Major General Borys kremenetskyi Defence and Air Attache, Embassy of Ukraine to the UK. 20.3.2019. Слайд 1 (rusi.org)

“Russia’s Arms & Technologies: The XXI Century Encyclopedia, Volume 13: Control, Communication and Radio Electronic Warfare System.” 2006. Kustantaja Oruzhie i tekhnologii

ATP 7-100.1_Russian Tactics, ATP 7-100.1 Russian Tactics | TRADOC G2 Operational Environment Enterprise (army.mil)

“Russia’s Electronic Warfare Capabilities to 2025”. Roger N. McDermot. Republic of Estonia, ministry of defence. Syyskuu 2017. ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf

“Russia’s Electronic Warfare Capabilities to 2025” – YouTube. Center for Strategic & International studies

“Russian/Soviet/WarPac Ground Based ECM Systems” Air power Australia. Russian/Soviet/WarPac Ground Based ECM Systems (ausairpower.net)

“Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces”, Försvarsdepartementet/ Ministry of Defence, September 2018. FOIR4625.pdf

IEEE Spectrum “The Fall and rise of Russian Electronic Warfare”, https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

Join Air Power Competence Centre “Electronic Warfare in Ukraine”, https://www.japcc.org/articles/electronic-warfare-in-ukraine

RUSI ”Jamming JDAM: The Threat to US Munitions from Russian Electronic Warfare”, https://www.rusi.org/explore-our-research/publications/commentary/jamming-jdam-threat-us-munitions-russian-electronic-warfare

RUSI ”The latest in the battle of jamming with electronic beams”, https://www.rusi.org/news-and-comment/in-the-news/latest-battle-jamming-electronic-beams-special-report

The New York Times “`Jamming`: How Eletronic Warfare is Reshaping Ukraine`s Battlefields, https://www.nytimes.com/2024/03/12/world/europe/ukraine-drone-russia-jamming.html

The Defence Horizon Journal “The Underwhelming Performance of Russian Land Forces Electronic Warfare – Watt Happened”, https://www.thedefencehorizon.org/post/watt-happened

Voice of America “How Can Ukraine Counter Russia’s Electronic Warfare?”, https://youtu.be/aWy9QPovFm8?si=O2o931i8sOEXV2bO

Military History not Visualized “When Drones fall out of the Sky... Electronic Warfare 101”, https://youtu.be/8Y9O5U-4qJmc?si=ia4732jyLaWqi0UC

Military Aviation History “Electronic Warfare: The Invisible War Around Us “, https://youtu.be/sPL4vyApvAU?si=gH8JPqIfvCeUy8jh

Perun “More “Game Changers” (and Failures) in Ukraine - From Starlink & Electronic warfare to Hypersonics”, https://youtu.be/jaWVrphbHXI?si=0oCAUY-6VAl-y0JcI

Military History not Visualized “Lessons from Ukraine: Why Electronic Warfare matters”, https://youtu.be/iO-ARw-9GgWA?si=j43Dpjk1VKKJotzs

Center for a New American Security “The State of the War in Ukraine with Michael Kofman”, https://www.youtube.com/watch?v=K_ORTxeoQXg

Aarne Klemetti.

Janne-Matti Peltola.

TEKSTI:AARNE KLEMETTI JA JANNE-MATTI PELTOLA

Tekoälyn sääntely sotilaallisissa ympäristöissä

osa 2: sovelluksena sotilaallinen voimankäyttö

Johdanto

Miehittämättömiä ja tekoälyä hyödyntäviä asejärjestelmiä on kritisoitu siitä, että ihmisen poistuminen päätöksentekoketjusta siirtää vastuun koneelle. Tässä yhteydessä on käytetty termiä tappajarobotti. Toisaalta huoli on aiheellinen, koska sodan oikeussääntöjen noudattamisessa komentajan ja operaattorin vastuun tulee toteutua ja on yleinen edellytys sääntelyn noudattamiselle. Autonomisella järjestelmällä on kyky tehdä itsenäisiä päätöksiä ja suorittaa erilaisia toimintoja myös ennalta määrittelemättömissä tilanteissa. Autonomian määritelmä täyttyy, kun tekoäly kykenee yhdistelemään aiempia sääntöjä tai kokemuksiaan uuden tilanteen ratkaisemiseksi.

Tämä on kolmiosaisen artikkelisarjan toinen osa. Ensimmäisessä osassa taustoitettiin sääntelyn perusteita ja soveltamista tekoälyn käyttöön sodankäynnin yhteydessä. Tässä artikkelissa etsitään yksinkertaisen skenaarion avulla vastausta kysymykseen: “miten käytännössä pitää toimia, kun tekoälyä sovelletaan sotilaalliseen voimankäyttöön?” Asiaa tarkastellaan käsittelemällä tilanteeseen soveltuvaa sääntelyä ja pohditaan miten tekoäly noudattaa sodan oikeussääntöjä. Lopuksi esitellään malli, jossa operaattorin ja komentajan vastuu saadaan toteutumaan kun tekoäly vastaa toiminnasta.

Tekoälyn mukaantulon myötä kynnys sotilaallisen voiman käyttämiseen saattaa laskea, koska omien henkilöstötappioiden mahdollisuus on pienempi erityisesti kun ratkaisuun liittyy autonomiaa. Toisaalta kaukovaikutteisia ja miehittämättömiä asejärjestelmiä voi käyttää myös ilman tekoälyä ja ihmisuhreista ollaan huolestuneita vain maissa, joissa ne pitää perustella äänestäjille. Tekoälyyn liittyvien sovellusten käyttökelpoisuus ja kypsyys perinteisessä sodankäynnissä on vielä saavuttamatta. Sen sijaan kyber- ja kognitiivisissa toimintaympäristöissä hybridisota on jo käynnissä, mutta se ei ole tämän artikkelisarjan aiheena.

Skenaarion kuvaus

Skenaariossa dronen tavoitteena on, että se osaa hakeutua itse tekoälyä hyödyntäen pistemaaliin ja toimia ilman operaattorin tukea. Tehtävä tulee kyetä täyttämään etulinjan ylittämisen jälkeen ilman yhteyttä vasta-asemaan noudattamalla itsenäisesti sodan oikeussääntöjä. Esimerkissä tarkastellaan tekoälyä hyödyntävän dronen päätöksentekoprosessia tilanteessa, jossa sillä ei ole yhteyttä operaattoriin. Tilanne voi syntyä, jos vastatoimintaan liittyy häirintää tai kun dronea käytetään vaanivana asejärjestelmänä.

Sodan oikeussäännöt ja aseellisen voimankäytön sääntely

Sodasta käytetään kansainvälisessä oikeudessa nimitystä aseellinen selkkaus, jossa on noudatettava humanitaarisen oikeuden sääntöjä, joiden perusperiaatteet sitovat kaikkia osapuolia. Humanitaarinen oikeus on osa kansainvälistä oikeutta ja sen tavoitteena on rajoittaa sotien ja kansainvälisten selkkausten vaikutuksia siviiliväestöön sekä niihin taistelijoihin, jotka eivät ota enää osaa aktiivisiin sotatoimiin sekä rajoittaa käytettäviä sodankäyntikeinoja ja -menetelmiä. Humanitaarisen oikeuden oikeuslähteinä ovat – kuten muussakin kansainvälisessä oikeudessa – kansainväliset sopimukset ja tapaoikeus.

Kansainvälisen humanitaarisen oikeuden keskeisiä ja kaikkia aseellisten selkkausten osapuolia velvoittavia periaatteita ovat erotteluperiaate, suhteellisuusperiaate, varotoimiperiaate ja kielto käyttää aseita tai sodankäyntimenetelmiä, jotka aiheuttavat liiallisia vammoja tai tarpeetonta kärsimystä. Autonomisesti toimivan asejärjestelmän on siis kyettävä sensoriensa ja tekoälyn avulla tekemään tarvittavat johtopäätökset ainakin erotteluperiaatteen ja suhteellisuusperiaatteen osalta, kun taas kaksi jälkimmäistä kohtaa tulee arvioitavaksi ennen kuin päädytään käyttämään autonomista asejärjestelmää. Tehtävä ei ole helppo ja sitä vaikeuttavat entisestään tilanteet, joissa taistelijat pyrkivät suojautumaan tulenkäytöltä kiellettyjen kohteiden sisään tai läheisyyteen.

Erotteluperiaatteen mukaan aseellisen hyökkäyksen saa kohdistaa vain sotilaskohteisiin ja taistelijoihin, ei siviileihin tai siviilikohteisiin. Tähän liittyy umpimähkäisen voimankäytön kielto, jonka mukaan ei saa käyttää sellaisia aseita tai sodankäyntimenetelmiä, joiden vaikutuksia ei kyetä riittävästi rajaamaan vain sallittuihin kohteisiin. Tekoälyn tulee kyetä erottamaan sallitut kohteet ja lisäksi kyettävä arvioimaan oheisvahinkoja ennen vaikuttamispäätöksen tekoa suhteellisuusperiaatteen mukaisesti. Sen mukaan hyökkäykseen ei saa ryhtyä, jos siitä odotettavissa olevat vahingot siviileille tai siviilikohteille olisivat liiallisia hyökkäyksellä välittömästi saavutettavaan sotilaalliseen hyötyyn nähden.

Geneven yleissopimusten (SopS 7–8/1955) lisäpöytäkirjassa (SopS 81–82/1980) ja niiden muutokset (SopS 5/1987) velvoitetaan sopimusosapuolet selvittämään ennen uuden aseen tai asejärjestelmän käyttöönottoa onko niiden käyttö joissakin tai kaikissa olosuhteissa kansainvälisen oikeuden mukaan kielletty. Selvittämisvelvollisuus ei koske ainoastaan käyttöönottoa vaan myös aseiden ja sodankäyntimenetelmien tutkimusta, kehittämistä ja hankintaa. Tekoälyn pitäminen kokonaan kiellettynä olisi erittäin ongelmallista, koska kyseessä on

murroksellinen teknologia, jota kehitetään joka tapauksessa siviilitarkoituksiin. Näin ollen ennemmin tai myöhemmin tulee tilanne, jolloin tekoälyä sovelletaan sotilaallisiin tarkoituksiin ainakin niin sanotuissa kaksoiskäyttötuotteissa.

Martensin lauseke on kansainvälisen humanitaarisen oikeuden periaate, jonka mukaan sodankäynnissä on noudatettava inhimillisyyden periaatteita, vaikka missään kansainvälisen oikeuden säännöksessä ei määriteltäisi sodankäynnin sääntöjä. Martensin lausekkeen mukaan yleiseen humaanisuuteen ja julkisen omatunnon periaatteisiin vedoten tulee suojata aseellisen yhteydenoton osallisiksi joutuneita yksilöitä, niin taistelijoita kuin siviilihenkilöitä, konfliktitilanteissa, joissa ei ole sovellettavissa valtiota velvoittavaa sopimusta. Martensin lauseketta on käytetty yhtenä argumenttina autonomisten asejärjestelmien kieltämisen puolesta.

Haagin IV sopimuksen liitteenä olevassa maasotaohjesäännössä määritetään edellytykset sotilaallisten konfliktien osapuolten asevoimille. Sotilaallisten tunnusten ja aseiden kantamisen lisäksi keskeisenä vaatimuksena on se, että joukon johtajana toimii alaisistaan vastuussa oleva sotilasesimies. Hänellä on tähän asemaan liittyviä vastuita, joista käytetään nimitystä komentajan vastuu. Sillä tarkoitetaan sotilaskomentajan vastuuta noudattaa kansainvälisiä humanitaarisia oikeussääntöjä (engl. International Humanitarian Law, IHL) ja varmistaa, että myös hänen alaisuudessaan toimivat sotilaat noudattavat niitä. Komentajan vastuu sisältää velvollisuuden kouluttaa sotilaitaan IHL:stä ja sen soveltamisesta konfliktitilanteissa, mukaan lukien sotavankien kohtelu, siviilien suojeleminen ja kulttuuriperinnön kunnioittaminen. Komentajan on myös otettava käyttöön asianmukaiset toimenpiteet IHL:n rikkomusten estämiseksi sekä tutkimiseksi ja hän voi olla vastuussa näiden rikkomusten seurauksista.

Operaattorin tai sotilaan vastuu tarkotaa sotilaan henkilökohtaista vastuuta noudattaa sodan oikeussääntöjä. Periaatteellisella tasolla jokainen sotilas on vastuussa omasta käyttäytymisestään, eikä rikkomuksia voi aina perustella sotilaskäskyn noudattamisella. Sotilaalla on myös velvollisuus raportoida IHL:n rikkomuksista, joita hän on todistanut tai jotka hän on itse tehnyt, ja olla valmis vastaamaan niistä. Operaattorin ja komentajan vastuut ovat keskeinen osa kansainvälistä humanitaarista oikeutta, koska ne edistävät ihmisoikeuksien ja humanitaarisen oikeuden kunnioittamista konfliktitilanteissa.

Kuva 1. Tekoälyn avulla luotu kuva artikkelin skenaariosta. Kuva Janne-Matti Peltola.

Suomen lainsäädännössä komentajan ja operaattorin vastuusta säädetään Rikoslaissa (39/1889, RL). Rikoslain sotarikoksia ja rikoksia ihmisyyttä vastaan käsittelevän 11 luvun säännökset muutettiin 2008 vastaamaan kansainvälisen rikostuomioistuimen Rooman perussääntöä. Lakiin lisättiin säännökset esimiehen vastuusta ja erikseen ilmoitusvelvollisuuden laiminlyönnistä sekä säännökset esimiehen käskystä rikosoikeudellisesta vastuusta vapauttavana seikkana. Näillä säännöksillä tavoiteltiin esimiesten ja alaisten vastuun jakautumista aikaisempaa paremmin Rooman perussääntöä vastaavaksi.

Rikoslain 11 luvun 12 § käsittelee esimiehen vastuuta. Pykälän ensimmäisessä momentissa esimiehen vastuu sidotaan alaisten tekoihin valvontavastuun kautta niin, että valvontavastuun laiminlyönti aiheuttaa esimiehelle samat seuraukset kuin tekijälle. Esimiehen laiminlyöntiin suhteessa sodan oikeussääntöihin voisi tulla sovellettaviksi myös yleisten osallisuutta koskevien säännösten lisäksi esimerkiksi eräät rikoslain 40 luvun säännökset virkarikoksista tai 45 luvun säännökset palvelusrikoksista.

Rikoslaissa (39/1889) esimiehen käskyn noudattamisesta säädetään 45 luvun 26 b §:ssä (515/2003). Sen mukaan teosta, jonka sotilas on tehnyt esimiehensä käskystä, tuomitaan käskynalainen rangaistukseen vain, jos hän on käsittänyt tai hänen olisi pitänyt käsittää, että hän käskyn täyttämällä toimisi lakia taikka virka- tai palvelusvelvollisuutta vastaan. Jos teko on tapahtunut olosuhteissa, joissa käskynalaiselta ei ole voitu kohtuudella edellyttää käskyn täyttämättä jättämistä, tekijä on kuitenkin rangaistusvastuusta vapaa. Sotarikoksiin johtavan esimiehen käskyn toteuttamisesta on säädetty myös RL 11:14. Sen mukaan tekijä on rangaistuksesta vapaa, jos hänellä on ollut oikeudellinen velvoite noudattaa käskyä, hän ei tiennyt käskyn lainvastaisuudesta tai käsky ei ollut selvästi lainvastainen.

Puolustusvoimista annetun lain (551/2007) 4 §:n mukaisesti puolustusvoimien käyttämien sotilaallisten voimakeinojen tulee olla sopusoinnussa Suomea sitovien kansainvälisten velvoitteiden kanssa.

Tekoälyn kansainvälisestä sääntelystä asejärjestelmissä

Yhdistyneiden kansakuntien neuvotteluja autonomisista asejärjestelmistä käydään tavanomaisia aseita koskevan yleissopimuksen (Convention on Certain Conventional Weapons, CCW) alla. CCW on aseriisuntasopimus, joka pitää sisällään tavanomaiset aseet (muut kuin ydinaseet), joiden voidaan katsoa aiheuttavan tarpeettoman vakavia vammoja tai olevan vaikutuksiltaan umpimähkäisiä, kuten havaitsemattomat sirpaleet, miinat ja ansat, polttoaseet, sokeuttavat laserit sekä räjähtämättömät jäänteet.

Euroopan parlamentin päätöslauselmassa vuodelta 2018 todetaan, että koneet ja robotit eivät pysty ihmisen tavoin tekemään päätöksiä, joihin sisältyy erotteluun, suhteellisuuteen ja varotoimiin liittyviä eli sodan oikeussääntöjen mukaisia oikeusperiaatteita, joita sovelletaan täysipainoisesti kaikkiin asejärjestelmiin ja niiden käyttäjiin ja että kansainvälisen oikeuden noudattaminen on perusedelly-

Patria

Kun kaiken on pakko toimia.

Patria tarjoaa huippuluokan suorituskykyä

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

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

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

tys, joka valtioiden on täytettävä. Asiakirjassa korostetaan, että on äärimmäisen tärkeää estää kehittämästä ja valmistamasta sellaisia tappavia autonomisia asejärjestelmiä, joissa kriittiset toiminnot, kuten kohteen valinta ja siihen iskeminen, eivät ole ihmisen valvonnassa. Toisaalta päätöslauselmassa muistutetaan, että tappavina autonomisina asejärjestelminä ei pidetä aseita ja asejärjestelmiä, jotka on suunniteltu erityisesti omien alustojen, asevoimien ja väestön puolustamiseen erittäin dynaamisilta uhilta, kuten ohjuksilta tai muilta hyökkäyksiltä. Samalla kuitenkin korostetaan, että vastatoimien kohdistuessa alukseen, jossa on ihmisiä, tulisi ihmisen päättää voimankäytöstä.

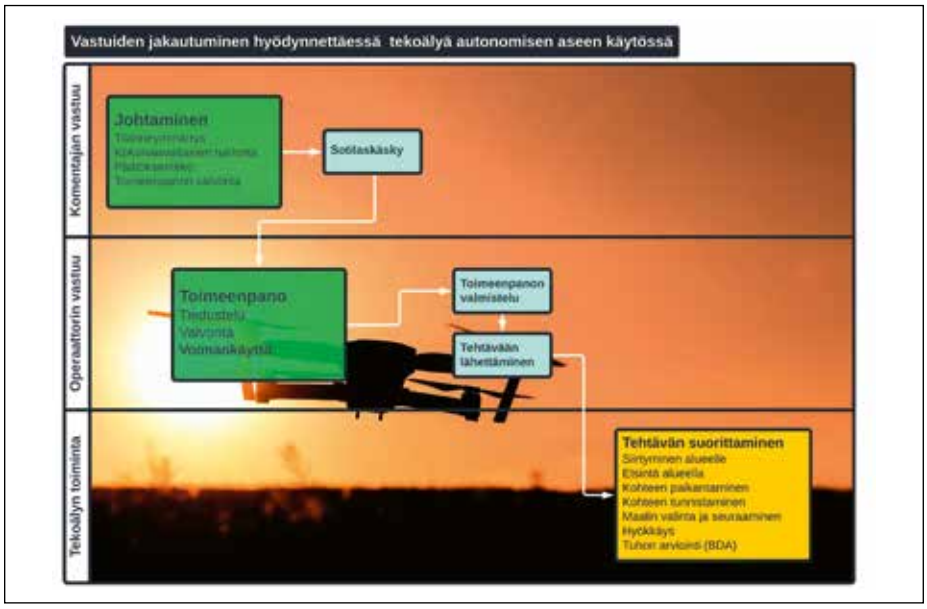
Euroopan parlamentin päätöslauselmalla ei ole yleisesti eikä tässäkään tapauksessa välitöntä oikeudellista merkitystä, toisin sanoen se ei luo uusia lakeja tai oikeudellisia velvoitteita. Päätöslauselmat ovat kuitenkin tärkeitä poliittisia asiakirjoja, joilla on merkitystä EU:n toiminnassa ja lainsäädännön kehittämisessä, koska ne ilmaisevat parlamentin kantaa tiettyihin asioihin ja ne voivat vaikuttaa EU:n päätöksentekoprosessiin.

Yhdysvaltojen kanta autonomisten aseiden kieltämiseen on ollut pidättyväinen. Valtionhallinnon asiantuntijaryhmä suositteli loppuraportissaan, että Yhdysvaltojen ei tule tukea autonomisten aseiden täyskieltoa johtuen määrittely- ja valvontaongelmien lisäksi siitä, että sen pahimmat kilpailijat eli Kiina ja Venäjä ovat osoittaneet epäluotettavuutensa sitoutumisessa kansainvälisiin sopimuksiin.

Automaattisen päätöksenteon sääntely

Suomessa julkisen hallinnon automaattinen päätöksenteko tehtiin mahdolliseksi lakimuutoksella maaliskuussa 2023. Asiassa ei säädetty erillislakia vaan muutos toteutettiin muuttamalla hallintolakia, julkisen hallinnon tiedonhallinnasta annettua lakia, digitaalisten palvelujen tarjoamisesta annettua lakia, henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia ja maakaarta.

Hallintopäätösten automatisointi vertautuu teoreettisesti myös valtion väkivaltamonopolin käyttämiseen, josta käytetään hallintotoimintana termiä merkittävä tai tosiasiallinen julkisen vallan käyttäminen. Täysin suoraa yhtäläisyyttä sotilaallisen voiman käyttämiseen ei voida tehdä, mutta prosessia voidaan pitää teoreettisesti samankaltaisena ja sen



Kuva 2. Vastuiden jakautuminen hyödynnettäessä tekoälyä autonomisen aseen käytössä. Kuvasta ilmenee teoreettinen tarkastelu siitä, miten vaikuttamispäätös voidaan tehdä ja jakaa pienempiin osakokonaisuuksiin kansainvälisen oikeuden edellyttämien vastuiden mukaisesti. Kuva Janne-Matti Peltola/Aarne Klemetti.

sisältämiä ilmiöitä voidaan verrata oikeudellisesti. Yhtenä keskeisenä asiana on laillisuusperiaate ja lailla säätämisen vaatimus. Näiden periaatteiden mukaisesti ja automaattiseen päätöksentekoon soveltaen julkisen vallan käytön tulee perustua lakiin ja sen tulkintaan perustuviin käsittelysääntöihin ja sen lisäksi automatisoidun toimintaprosessin käyttö hallintolaissa, tiedonhallintalaissa ja muissa erityislaeissa säädettyihin edellytyksiin. Toisin sanoen oikeusvaltioperiaatteen mukaan automatisoidulla julkisen vallan käyttämisellä on oltava peruste laissa ja hallinnon lainalaisuusperiaatteen mukaan automaattisen päätöksenteon on noudatettava tarkoin lakia.

Perustuslakivaliokunta on pitänyt selvänä, ettei päätöksenteon siirtäminen automaattiseen käsittelyyn saa johtaa siihen, että virkavastuuta koskevat perustuslain säännökset menettävät merkityksensä. Valiokunnan mukaan automatisoidun hallintomenettelyn ja päätöksenteon sääntelyn tulee täyttää hallinnon lainalaisuuden, julkisuusperiaatteen ja hyvän hallinnon perusteisiin kuuluvien hallinnon oikeusperiaatteiden asettamat vaatimukset sekä turvata oikeusturvan ja virkamiesten virkavastuun asianmukainen toteutuminen.

Automatisoitu päätöksenteko on perustuslakivaliokunnan mukaan mahdollista asiassa, johon ei sisälly seikkoja, jotka viranomaisen etukäteisen harkinnan mukaan edellyttäisivät tapauskohtaista harkintaa, tai johon sisältyvät tapauskohtaista harkintaa edellyttävät seikat virkamies tai muu asian käsittelijä on arvioinut. Lisäksi valiokunta on todennut erikseen, että automatisoitu päätöksenteko ei sovellu sellaiseen hallinnolliseen päätöksentekoon, joka edellyttää päätöksentekijän käyttävän laajaa harkintavaltaa. Näin ollen autonomisen päätöksenteon tuominen viranomaistoimintaan ei ole perustuslain mukaista ainakaan hallintopäätösten osalta, mikäli tekoälylle annetaan tehtäviä, jotka liittyvät viranomaisen harkintavallan käyttämiseen. Voidaan kuitenkin pitää oikeudellisesti mahdollisena, että autonomiaa hyödynnetään päätöksenteon muissa vaiheissa.

Tekoälyn vastuu päätöksestä

Vastuu toimintaan liittyvistä seurauksista voi olla luonteeltaan moraalista tai oikeudellista. Tässä tarkastelussa keskiössä oleva oikeudellinen vastuu jakautuu edelleen rikosoikeudelliseen ja vahingonkorvausoikeudelliseen vastuuseen. Vastuun kantamisen seurauksena voi olla tuomitseminen rangaistukseen tai velvollisuus korvata aiheutunut vahinko.

Kehittyneen tekoälyn käyttöön liittyy vastuukuilun käsite, joka syntyy tilanteessa, jossa kukaan ei kontrolloi koneen toimintaa riittävästi voidakseen ottaa siitä vastuuta, sen paremmin juridisessa kuin moraalisessakaan mielessä. Se siis tarkoittaa sitä ristiriitaa, joka syntyy vastuun kohdistuessa ihmiseen, jolla ei ole ollut tosiasiallista mahdollisuutta estää tapahtumaa tai tuottamuksen aste ei rinnastu tahallisuuteen tai edes lievään tuot-

tamukseen, jos virheellisen päätöksen tekee tekoäly eikä sen käynnistäjä voinut sitä etukäteen tietää toimiessaan hyvässä uskossa (bona fide).

Toisena koneoppimiseen perustuvan päätösautomaation ongelmana voidaan pitää päätöksenteon läpinäkymättömyyttä, jota kuvataan termillä Black box. Sillä tarkoitetaan tilannetta, joka syntyy, kun päätöksentekosovellus muodostaa itsenäisesti käyttämänsä päättelysäännöt eikä käyttäjä tiedä tarkalleen tai ollenkaan, millä tavalla tekoäly päätyy tiettyyn ratkaisuun sille annetun aineiston perusteella, vaan päätöksenteon logiikka kätkeytyy mustaan laatikkoon. Päätöksenteon läpinäkymättömyyden vuoksi saattaa joissain tilanteissa olla mahdotonta selvittää, mistä virheellinen päätös tai epäonnistuminen johtui ja mihin tahoon vastuu tulisi kohdistaa. Black box -ongelma liittyy erityisesti koneoppivaan automaatioon, koska sääntöpohjaisessa automaatiossa säännöt on lähtökohtaisesti määritelty täsmällisesti ja päätöksentekopolku on jäljitettävissä.

Keskeinen ongelma on erityisesti se, että oikeusjärjestykseen kuuluvat vastuun kantamisen muodot eivät sovellu ei-inhimillisiin toimijoihin. Rikosoikeudelliset rangaistukset ovat tehottomia, koska tekoälylle ei voi määrätä vapausrangaistusta ja vahingonkorvausvastuu puolestaan edellyttää, että tekoälyllä voi olla ja on omaisuutta, josta se voisi korvaukset maksaa.

Johtopäätökset

Aikaisemmin esitetyn perusteella keskeinen rooli sodan oikeussääntöjen noudattamisessa on komentajalla ja operaattorilla. Prosessi voidaan jakaa johtamiseen, toimeenpanoon ja tehtävän suorittamiseen. Johtamisessa korostuu komentajan vastuu. Toimeenpano on operaattorin vastuulla.

Komentajan vastuulla on johtaminen, joka perustuu tilanneymmärrykseen. Kokonaisvaltaisen harkinnan jälkeen komentaja tekee päätöksen ja antaa sotilaskäskyn, jonka perusteella operaattori aloittaa toimeenpanovaiheen, jonka valvontavastuu säilyy komentajalla. Tehtävä voi sisältää muun muassa tiedustelua, valvontaa ja voimankäyttöä. Tehtävään lähettämistä edeltävä toimeenpanon valmistelu pitää sisällään ohjelmoinnin, tarvittavat parametrit ja laitteiston lataamisen tai tankkaamisen sekä lopuksi tehtävään lähettämisen. Tämä vaihe voi sisältää suunnitelman hyväksyttämisen käskyn antaneella komentajalla.

Tekoälyn vastuulle jää tehtävän suorittaminen. Se voidaan jakaa alueelle siirtymiseen ja siellä tapahtuvaan kohteen etsintään, paikantamiseen ja tunnistamiseen. Tämän jälkeen tekoäly valitsee maalin, seuraa sitä ja toteuttaa hyökkäyksen. Lopuksi se suorittaa vielä vaikutusten arvioinnin. Erityisesti kohteen tunnistamiseen liittyy suuria vaatimuksia tekoälyn kehittämissä ja kyvykkyyksissä. On selvää, että väärän kohteen tuhoaminen tai suurien oheisvahinkojen aiheuttaminen asettaa tekoälyn käyttämisen arvostelulle alttiiksi myös myöhemmissä operaatiossa ja lisäksi se asettaa operaattorin ja komentajan yllä mainittujen vastuukuilun ja black box -ongelmien eteen.

Vastuukuilua ja Black box -dilemmoita voidaan pitää suomalaisessa oikeusjärjestyksessä kuitenkin teoreettisena vastuukysymyksen kannalta, koska vastuun siirtäminen käyttäjältä tai valmistajalta tekoälylle ei ole toteutettavissa nykyisessä oikeusjärjestelmässä. Suomalaisen oikeusjärjestyksen mukaan oikeussubjektina voi olla luonnollinen henkilö eli ihminen tai oikeushenkilö, jolla tarkoitetaan muun muassa yhdistyksiä ja yhtiöitä. Vain oikeussubjekteilla eli tässä tapauksessa komentajalla ja operaattorilla voi olla oikeuksia ja velvollisuuksia.

Pelkistetysti voidaan siis todeta, että vastuu päätöksistä ei ole (eikä voi olla tulevaisuudessakaan) tekoälyllä vaan, kuten perustuslakivaliokunta on tuoreissa automaattista päätöksentekoa koskevissa lausunnoissaan todennut ”automaattiseen päätöksentekomenettelyyn on voitava liittää viime kädessä myös virkamiehiin kohdistuva vastuu virkatoimista”. Näin ollen sodan oikeussääntöjä noudattavan tekoälyn vastuulle tulee suunnitella tehtäviä, jotka eivät sisällä päätöksenteko vaan niiden toimeenpanoa.

Kuvassa 2 esitetty jaottelu mahdollistaa komentajan vastuun päätöksen tekijänä ja toimeenpanon valvojana sekä operaattorin (sotilaan) vastuun käskyn toimeenpanemisessa. Näin ollen tekoälylle jää tehtäviä, joita se voi suorittaa tulevaisuudessa todennäköisesti paremmin ja tarkemmin kuin ihminen. Ratkaisussa toteutuu ainakin periaatteellisella tasolla ”meaningful human control” ja sillä taataan riittävä ihmisen rooli vaikuttamisratkaisun tekemisessä, valvomisessa ja toteuttamisessa.

Lähdeluettelo

KALLIONIEMI, Ismo: Tekoälyoikeus – varallisuusoikeuden ja riskienhallinnan kysymyksiä, ALMA 2022.

MÄÄTTÄ, Tapio (Toim): Oikeudellisen ajattelun perusteita. UEF 2018

KOIVISTO, Ida: Thinking inside the box: The promise and boundaries of transparency in automated decision-making. Academy of European Law Working Papers 2020/01, s. 1–22.

OIKEUSMINISTERIÖ: Arviomuistio hallinnon automaattiseen päätöksentekoon liittyvistä yleislainsäädännön sääntelytarpeista. Oikeusministeriön julkaisuja2020.

ROSEN, Gunnar – PARKKARI, Juhani: Sodan lait käsikirja: Edita 2004.

PeVL 81/2022 vp, Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi.

HE 145/2022 vp, Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi.

PeVL 7/2019 vp, Hallituksen esitys eduskunnalle laiksi henkilötietojen käsittelystä maahanmuuttohallinnossa ja eräiksi siihen liittyviksi laeiksi

Kirjoittajat

DI Aarne Klemetti toimii Metropolia ammattikorkeakoulun ICT ja tuotantotalous osaamisalueella tutkijaopettajana. Hänen tehtäviinsä kuuluvat tietojenkäsittely-, AI/ML/DS-, (A)IoT- ja mediatekniikka-alojen opetus sekä monitieteinen TKI-toiminta. Aarnella on yli 40 vuoden kokemus medatekniikkaan, sovelluskehitykseen ja ohjelmistotuotantoon liittyvästä tutkimuksesta, kehityksestä ja soveltamisesta niin tutkimuslaitoksissa, yrityksissä, yrittäjänä kuin opettajana. Tekoäly, koneoppiminen ja datan kanssa työskentely laajasti sovellettuina ovat olleet mukana käytännön työskentelyssä koko hänen uransa ajan.

Majuri Janne-Matti Peltola on sotatekniikan ja -talouden jatko-opinnoissa tekoälystä kiinnostunut hallintotieteen yliopppilas ja palvelee tällä hetkellä Naton esikuntatehtävässä Belgiassa.

TEKSTI: HANNA LIITOLA

Haastattelussa MPK:n johtamisjärjestelmäkoulutuspäällikkö

Majuri (evp) Jouni Purhonen toimii Maanpuolustuskoulutuksen (MPK) yhtenä koulutuspäällikkönä vastuualueenaan johtamisjärjestelmät. Hän on aloittanut tehtävässään 15.2.2024. Millaisten mutkien kautta Jouni on päätynyt nykyiseen pestiinsä ja mitä kaikkea johtamisjärjestelmäkoulutusta MPK:n tarjontaan sisältyy? Muun muassa näihin ja moniin muihin kysymyksiin saadaan vastaus VM-lehden henkilökuvassa.

Mistä olet kotoisin?

Olen kotoisin Espoon Matinkylästä. Toinen kotipaikkani on Lappeenranta, jossa vietin osan nuoruuttani. Sukujuureni ovat kuitenkin Savossa Mikkelissä, jossa ovatkin lapsuuteni kesälomamaisemat. Nykyään asun Vantaalla puolisoni kanssa.

Millainen on opiskelutaustasi sekä uran kehitys ja tehtävät Puolustusvoimissa?

Olen valmistunut sotatieteiden kandidaatiksi kadettikurssilta 88 vuonna 2004. Ensimmäinen palveluspaikkani oli Viestirykmentti, jossa toimin joukkueen johtajan tehtävässä neljä vuotta ennen maisteriopintoja, jotka suoritin 92. kadettikurssin mukana ja valmistuin sotatieteiden maisteriksi 2009. Tämän jälkeen siirryin Reserviupseerikoulun Viestikomppaniaan, jossa työskentelin vuoteen 2015 saakka. Olin tänä aikana vuoden opintovapaalla (2012–2013), jolloin opiskelin liiketalouden johtamista Saint Mary´s Universityssä Kanadan Halifaxissa. Kauppatieteiden maisteritutkinnon suoritin töiden ohessa Lappeenrannan teknillisessä yliopistossa, josta valmistuin vuonna 2015. Toimin Maasotakoululla johtamisen opettajana vuosina 2015–2017 ja seuraavat kaksi vuotta opiskelin yleisesikuntaupseerikurssilla 59, josta valmistuin vuonna 2019. YE-kurssin jälkeen palvelin pari vuotta Kainuun prikaatin operatiivisella osastolla sektorin johtajan tehtävässä sekä vuoden verran Maavoimien esikunnan operatiivisella osastolla JOJÄ-suunnittelu-upseerina. Reserviin siirryin vuonna 2022.

Miten viihdyit Puolustusvoimissa?

Puolustusvoimissa viihdyin todella hyvin. Selkeä toimintakulttuuri, selkeät tavoitteet ja yhtenäinen työyhteisö olivat työn parhaita puolia. Haasteiksi taas koin suuret työmäärät, työn ja perhe-elämän yhteensovittamisen ja epävarmuuden tulevasta työtehtävästä ja työpaikkakunnasta.

Millainen työpaikka Puolustusvoimat on ollut verrattuna muihin työnantajiin?

Olen työskennellyt Puolustusvoimien jälkeen puolitoista vuotta teollisuuslogistiikan parissa ja nyt puoli vuotta MPK:ssa. Teollisuudessa koin työkulttuurin hyvin samanlaiseksi kuin Puolustusvoimissa. Linjaorganisaatio toimii hyvin teollisuuden johtamisessa, jossa tähdätään tuottavuuteen resurssitietoisesti. MPK:n ja Puolustusvoimien kulttuurissa on hyvin paljon samaa. Tämä johtuu varmastikin siitä, että MPK:ssa työskentelee paljon EVP-henkilöstöä. Toki MPK on organisaationa hierarkialtaan kevyempi kuin Puolustusvoimat.

Mitkä tehtävät ovat erityisesti jääneet mieleesi työuran varrelta Puolustusvoimissa?

Sanoisin, että mielekkäintä aikaa Puolustusvoimissa oli työskennellä RUK:ssa ja kouluttaa upseerioppilaita. Koulutus oli kovaa ja vaativaa, mutta asiallista. Työn mielekkyyttä lisäsi myös se, että upseerioppilaat olivat hyvin motivoituneita. Toinen huippuhomma oli Kainuun prikaatissa operatiivisen suunnittelun tehtävissä, jossa koin tekeväni erittäin tärkeää ja vaikuttavaa työtä puolustussuunnittelun parissa.

Miten päädyit töihin MPK:lle?

Teollisuuden parissa tekemäni projekti saatiin osaltani valmiiksi ja oli aika etsiä uusia haasteita. Huomasin MPK:n rekrytoivan kahta koulutuspäällikköä, joista tulin valituksi johtamisjärjestelmäkoulutuspäällikön tehtävään. Maanpuolustuskoulutuksen parissa työskentely on minulle kuitenkin hyvin luontevaa ja mielekästä PV-taustani vuoksi.

Mitkä ovat vahvuutesi MPK:n tehtävässäsi?

Vahva JOJÄ-tausta maavoimien kenttäviestijärjestelmien parissa ja yleisesikuntaupseerikurssin käyminen ovat varmasti tärkeimmät vahvuuteni. Nämä molemmat antavat erittäin vahvan pohjan ohjata reservin johtamisjärjestelmäkoulutusta.

Millainen koulutustarjonta MPK:lla on, kun puhutaan johtamisjärjestelmistä ja kyberistä?

MPK:lla JOJÄ-koulutusohjelma on jaettu seuraaviin kokonaisuuksiin: Taistelijan

perusviestitiedot ja -taidot, esikunta- ja viestikomppaniaan sijoitettujen koulutus, paikallispataljoonan komppanioiden johtamisjärjestelmä- ja viestikoulutus, arjen välineet sekä sissiradistikoulutus. Näiden lisäksi meillä on erikseen elektronisen suojautumisen koulutusta, HF- ja radioamatöörikoulutusta sekä JOJÄ-kouluttajakoulutusta.

Kyberin osalta meillä on kattava kurssitarjonta aina perustasolta vaativiin erikoiskursseihin. Kyberkoulutusta teemme yhteistyössä mm. Jyväskylän yliopiston, Metropolia AMK:n ja eri yritysten kanssa.

Millaisia haasteita työssäsi kohtaat? Mistä pidät työssäsi erityisesti?

Työtä on paljon. Reserviläisten ja muiden kansalaisten halu osallistua kursseille on kahden viime vuoden aikana kasvanut rajusti Euroopan turvallisuustilanteen muutoksen vuoksi. Lisäksi kansalaisten ja organisaatioiden kiinnostus muutenkin toimintaamme kohtaan on lisääntynyt ja yhteydenottoja esimerkiksi median osalta on huomattavasti enemmän kuin aiemmin. Tämä luo organisaatiollemme painetta selvitä koulutuksen järjestelyistä ja hallinnollisesta puolesta. Nämä ovat toki kaikki positiivisia haasteita.

Erityisesti työssäni pidän vapaaehtoisten pyyteettömyydestä ja halusta jakaa osaamistaan kurssilaisille. Samalla olen erittäin tyytyväinen kouluttajiemme osaamisen tasoon ja asenteeseen. He järjestävät vapaaehtoisina erittäin laadukasta koulutusta, jota kelpaa seurata ja mainostaa kiinnostuneille.

Mitä asioita painotat omassa ja organisaatiosi toiminnassa?

Olen todennut useaan kertaan, että MPK:n johtamisjärjestelmäkoulutuksen piirissä keskustellaan asioista asiantuntevasti ja asiallisesti. Tekninen aselaji korostaa teknistä osaamista ja silloin korostuu yksityiskohtainenkin osaaminen. Samalla itse koulutuksen tulee perustua tuttuihin hyvän johtamisen kulmakiviin; innostukseen, luottamuksen rakentamiseen, oppimisen korostamiseen ja kaikkien arvostamiseen.

Millaisena näet Puolustusvoimien johtamisjärjestelmätoimialan muutosten vaikutukset MPK:n toimintaan lyhyellä ja pitkällä aikajänteellä?

Johtamisjärjestelmäkoulutuksessa tärkeää on laite- ja järjestelmäosaaminen. Olemme riippuvaisia Puolustusvoimien kalustosta koulutuksemme suhteen. Samalla kyse on osaamisen siirtämisestä; Puolustusvoimien uudistaessa kalustoaan tulee osaaminen kyetä siirtämään myös MPK:n kouluttajien piiriin. Tämä vaatii tiivistä yhteistyötä meidän JOJÄ-kouluttajiemme ja ammattisotilaiden välillä. Lyhyellä aikavälillä koen, että yhteistyömme joukko-osastojen henkilöstön ja kouluttajiemme kesken on hyvällä tasolla.

Pidemmällä aikavälillä koulutustamme ohjaavat Pääesikunta ja Maavoimien esikunta ja niiden koulutus- ja johtamisjärjestelmäosastot. Osastojen kautta saamme ohjauksen siitä, mitä koulutukseltamme odotetaan ja mitä erityisiä asioita tulisi tänään ja tulevaisuudessa huomioida. Tämä ohjaus toimii hyvin. Seuraava tärkeä steppi on tekoälyn hallitseminen ja hyödyntäminen.

Miten Nato-jäsenyys on vaikuttanut MPK:n toimintaan? Näkyykö se esimerkiksi koulutussisällöissä jollain tavalla?

Konkreettisin esimerkki NATO-jäsenyyden vaikutuksista MPK:n koulutukseen on järjestämämme Naton perusteet -verkkokurssi. Tämän kurssin tavoitteena on, että kurssilainen ymmärtää Naton ydintehtävät ja Nato-jäsenyyden keskeiset vaikutukset Suomelle. Siinä missä Nato-jäsenyydellä on merkittäviä vaikutuksia paitsi Suomen turvallisuus- ja puolustuspolitiikkaan, on sillä vaikutusta myös jokapäiväiseen kansalaiskeskusteluun, jossa olemme koko ajan mukana. NATO-jäsenyys on ollut vahvasti esillä mm. johtamisen teemaseminaarissamme.

Kyberkoulutukseen NATO-jäsenyys ja sitä ennen NATO-yhteistyö on tuonut uutta kulmaa. MPK on ansioitunut mm. NATO-johtoisissa Locked Shields -harjoituksissa ja yhteistyö Yhdysvaltojen 91st Cyber Brigaden kanssa on käynnissä. Näiltä foorumeilta kyberkouluttajamme tuovat tietenkin uusia oppeja Suomeen. Samalla viemme omaa kyberosaamistamme ulkomaille.

Miten irrottaudut työasioista vapaa-ajalla?

Viimeisen vuoden aikana olen palannut rakkaan nuoruuden harrastukseni, eli miniatyyrisotapelaamisen pariin. Tällä hetkellä askartelupöydällä ovat 101st Airborne Divisionin muutama kivääriryhmä, joilla on tarkoitus pelata Bolt Action nimistä miniatyyripeliä syksyllä pelikerhollamme.

MPK:n koulutustarjontaan pääset tutustumaan tarkemmin osoitteessa: https://mpk.fi

TEKSTI:JYRKI PENTTINEN, ENGINEERING CONSULTANT, ALPHACORE INC., USA

Matkaviestintäverkkoihin kytketyt droonit

TkT, tietokirjailija Jyrki Penttinen on toiminut telealalla vuodesta 1994 Suomessa, Espanjassa, Meksikossa ja Yhdysvalloissa. Penttinen työskentelee nykyään konsulttina Pohjois-Amerikassa pääaiheenaan 5G ja luennoi televiestintäteknologioista. Penttisen julkaisuihin voi perehtyä blogissaan www.5g-simplified.com.

Matkaviestinnän standardointi on luonut pohjan droonien vaatimien toiminnallisuuksien integrointiin matkaviestintäverkkoihin, erityisesti 4G- ja 5G-järjestelmiin, hyödyntäen monia siviili- ja maanpuolustussovelluksia. Droonimarkkinat kehittyvät edelleen, ja uusia toimijoita tulee mukaan ekosysteemiin niin palveluiden tarjoajien kuin käyttäjien rooleissa.

Taustaa

Miehittämättömien ilma-alusten (unmanned aerial vehicle, UAV), kuten siviilikäytössä suosittujen droonien, komento- ja ohjauslinkki (command and control, C2) perustuu usein lyhyen kantaman Wi-Fi -yhteyteen. Wi-Fi:n kautta käytettäessä C2:n radiolinkki rajoittaa droonin käytännöllisen toimintasäteen visuaaliseen näköyhteyteen. Esimerkkejä muista erikoiskäyttöön soveltuvista menetelmistä ovat suljetut RF-järjestelmät ja satelliittilinkit. Näillä menetelmillä on kuitenkin tekniset rajoitteensa esimerkiksi kapasiteetin, suojauksen ja luotettavuuden suhteen.

Matkaviestintäverkkoihin kytketyt droonit ovat lupaava tekninen kehitysalue, sillä droonien reaaliaikaista ohjausta ja siten toiminta-aluetta voidaan niiden avulla laajentaa merkittävästi. Perustuen matkaviestintäjärjestelmien yleisiin periaatteisiin, droonien käyttö näköyhteyden takana (beyond visual line of sight, BVLOS) mahdollistuu koko radioverkon peittoalueella, ja ohjauksen lisäksi verkot soveltuvat myös droonien hyötykuorman (data payload) vaatimiin tietoliikenneyhteyksiin, kuten korkean resoluution videon siirtoon. Droonit voivat tukeutua yksittäisen matkaviestintäverkon koko peittoalueeseen, mutta yhtä lailla ne voivat käyttää kansallisten ja kansainvälisten verkkojen vierailua.

Nykyisistä matkaviestintäverkkojen sukupolvista 4G ja 5G soveltuvat teknisten ominaisuuksiensa puolesta luontevasti drooniliikennöintiin. 4G:n datanopeus on riittävä droonien C2- ja datalinkin tarpeisiin, ja 5G:n päivitetty suorituskyky ja uudistettu toiminnallinen arkkitehtuurimalli mahdollistavat vielä loogisemman alustan niillä alueilla, missä 5G:n radioverkon peittoalue on tarjolla. 5G perustuu verkkotoimintojen virtualisointiin, mikä mahdollistaa datayhteyksien personoinnin eri käyttäjäryhmille verkkopaloittelun kautta. Siten 5G-verkko-operaattori voi ottaa käyttöön muiden verkkopalojen ohella erityisesti drooneille sopivan verkkopalan (network slice, NS).

Droonien käyttöympäristö kattaa ilma-alueen kansallisten regulaattoreiden sallimilla alueilla luvalliseen maksimikorkeuteen saakka, ja siten droonit voivat liikkua myös tyypillisten tukiasema-antennien yläpuolella. Matkaviestinnän radioverkkosuunnittelun periaate on kuitenkin ollut mitoittaa riittävä radiolinkin laatu ja kapasiteetti katutason käyttäjille sekä rakennusten sisätiloihin samalla, kun antennien suuntaamista muualle on vältetty häiriöiden minimoimiseksi. Droonien lisääntynyt käyttö erityisesti tukiasema-antennien yläpuolella on siten ristiriidassa tämän periaatteen kanssa. Asiaa tutkitaan parhaillaan, ja monet tulokset indikoivat nykyisten matkaviestintäverkkojen sopivan usein tyypillisiin droonien käyttökohteisiin sellaisenaan tai pienillä muutoksilla.

Voidaan kuitenkin olettaa, että peittoalueen optimointiin saattaa olla tarvetta niillä alueilla, joissa on odotettavissa erityisen tiheää drooniliikennöintiä. Esimerkkejä tutkimuksista ovat Maanmittauslaitoksen useat testialueet [1] sekä Verizonin, T-Mobilen ja Ericssonin julkaisemat UAV-testitulokset kaupallisessa verkossa. [2] Jälkimmäinen toteaa esimerkiksi operatiivisten verkkojen millimetriaaltojen sopivan UAV-sovelluksiin, mutta matalampien taajuuksien suorituskyvyssä on vaihtelevia eroja korkealla lentävillä drooneilla. Samoin, kyseinen lähde toteaa, että erityisesti droonin vastaanottosuunnan videolähetteen datanopeus saattaa vaatia verkon optimointia.

Droonit ovat osa isompaa kokonaisuutta, jota voidaan hallita miehittämättömien ilma-alusten hallintajärjestelmän (uncrewed aerial system, UAS) kautta. Peittoalueen riittävyyden ohella UAV- ja UAS-ekosysteemi on ilmaissut myös muita kehitystarpeita. Esimerkiksi Euroopan UAS Test Centres Alliance on Euroopan Unionin jäsenmaiden puolustusvoimien ja siviilikeskusten UAS-testiorganisaatioiden yhteenliittymä, jonka

tehtävänä on edistää ekosysteemin kansainvälistä opastusta ja standardointia ja viranomaissääntelyä sekä seurata alan trendejä. Eurocontrolin helmikuussa 2024 julkaiseman kyselyn perusteella kyseisten organisaatioiden huolenaiheina todettiin olevan mm. integrointihaasteet (droonit ja muut ilma-alukset), tekninen luotettavuus, luottamuksellisuus, ympäristölliset näkökohdat, ja tietoturvallisuus. [3]

Muiden toimijoiden ohessa esimerkiksi GSMA on edistänyt UAV/UAS-ekosysteemin tietoisuutta ja tutkinut haasteita, joihin standardointi ja alan yritykset voivat kehittää ratkaisuja. Esimerkkinä GSMA:n tutkimuksista on GSMA:n Pohjois-Amerikan operaattoreiden ja UAV/UAS-ekosysteemin edustajien raportti ”Cellular-enabled aerial vehicles: exploration of the landscape of the North American ecosystem”. Kyseinen työryhmä totesi, että yksi merkittävistä nykyisistä kehityskohteista on droonien verkkopohjainen etätunnistus. 3GPP:n Release 18 -spesifiointityö on ottanut tämän huomioon määrittämällä toiminnon droonien yleislähetykseen suoralla PC5-linkillä, joka vastaa ajoneuvojen ja infrastruktuurin välistä matkaviestintäpohjaista C-V2X -liikennöintiä (cellular vehicle to everything). [4]

Matkaviestintäkytkettyjen droonien kehitys

Matkaviestintäverkkoja käyttävien droonien kehitys alkoi 4G-teknologian kautta. Se mahdollistaa luotettavan pohjan droonioperaatioille BVLOS-ympäristössä. Tämä on tärkeä seikka sovelluksille, jotka vaativat pitkiä droonilentoja. Esimerkkejä ovat sähkönjakeluinfrastruktuurin ja maatalousalueiden ilmakuvaukset sekä jakelupalvelut. 4G on mahdollistanut riittävän kaistanleveyden videolähetyksiin, telemetrian datansiirtoon sekä C2-linkeille, laajentaen droonien käytettävyyttä monesta näkökulmasta.

Siirtymä 4G:stä 5G-verkkoihin on edelleen edistänyt droonien käytettävyyttä. 5G tukee merkittävästi nopeampia datayhteyksiä, pienempiä tiedonsiirron viiveitä ja korkeampaa verkkokapasiteettia 4G:hen verrattuna, minkä johdosta 5G on erityisen soveltuva monimuotoiseen ja kriittiseen droonioperointiin. Lisäksi 5G:n mahdollisuus tarjota korkean luotettavuuden yhteyksiä (URLLC, ultra-reliable low latency communications) sopii hyvin kriittisille sovelluksille, kuten kriisi- ja onnettomuusalueiden valvontaan ja ensiaputarvikkeiden toimituksiin, joissa pikainen viestintä ja päätöksenteko ovat tärkeitä.

Lisäksi, 5G:n tuki massiiviseen laitteiden väliseen liikennöintiin (massive machine type communications, mMTC) mahdollistaa useiden droonien helpomman yhteishallittavuuden, mikä auttaa drooniparvien koordinoinnissa ja ohjauksessa. Se on erityisen hyödyllistä laajan alueen ympäristön monitoroinnissa, onnettomuus- ja katastrofitilanteiden hallinnassa sekä ilmakuljetuksissa (urban air mobility, UAM), missä useiden droonien on toimittava koordinoidusti ja turvallisesti.

5G:n integrointi reunalaskentaan (edge computing) hyödyntää puolestaan matkaviestinverkkoihin kytkettyjen droonien käytettävyyttä. Droonien siirtäessä prosessoitavaa dataa reunalaskennan palvelimille, droonit voivat suorittaa verkon tukemana monimutkaisia tehtäviä, kuten reaaliaikaista videokuvan analyysiä ja koneoppimista (machine learning) siten, että itse drooniin asennetut laitteet voivat säästää prosessoinnin vaatimissa komponenteissa ja tehonkulutuksessa. Voidaan olettaa, että tämä synergia droonien ja verkkojen välillä edesauttaa myös itsenäisesti toimivien ja älykkäiden droonien kehitystä.

4G- ja 5G-matkaviestinverkkoihin kytketyt droonit edustavat merkittävää teknistä teemaa, johon standardointiorganisaatiot ja teollisuus ovat jo nyt panostaneet vahvasti. Verkkojen kehittyessä, ne mahdollistavat uusia sovelluksia, pidempiä droonilentoja, paremman suorituskyvyn, sekä kehittyneen keinoälykkyyden tason, mikä puolestaan avaa uusia mahdollisuuksia sektoreilla, joilla drooneja ei ole aiemmin käytetty.

Standardointi

Release 15

3GPP Release 15:n mukaiset UAV-liikennöinnin parannukset keskittyivät 4G:n verkkoarkkitehtuuriin. 3GPP:n radioverkkoryhmän (radio access network, RAN) tutkimuskohde alusti teknisen spesifikaation TS 36.331 (LTE-radioresurssien ohjauksen protokollakerros) ja TS 23.401 (yleisen pakettiradioverkkopalvelun parannukset E-UTRAN:lle).

Release 15:n UAV-liikennöinnin parannukset liittyvät lähinnä ilmaliikennevälineiden valtuutukseen. 3GPP TS 23.401 esittelee UAV-päätelaitteen (user equipment, UE) indikaation, jonka avulla järjestelmäarkkitehtuuri tunnistaa, mitkä 3GPP UE:t ovat UAV-tilaajatyyppisiä. Tämä mahdollistaa sen, että 4G-kytkentäverkko aktivoi oikein UAV-tilaajien ominaisuudet.

3GPP TS 36.331-spesifikaatiossa esitellyt LTE-UAV-UE -ominaisuudet minimoivat päätelaitteiden aiheuttamat häiriöt LTE-tukiaseman (evolved NodeB, eNB) kanssa.

Release 16

Release 16 toi mukanaan useita uusia verkkotoimintoja, joista UAV:n osalta esimerkkinä on 3GPP TS 22.125 (UAS:n 3GPP-tuki), joka tarjoaa ensimmäisen vaiheen vaatimukset UAV-tuelle.

Release 17

Release 17 sisältää useita 5G-verkkojen UAV-vaatimusten parannuksia, jotka on koottu 3GPP TS 22.125 -spesifikaatioon (UAS-tuki). Muita tähän liittyviä raportteja tai spesifikaatioita ovat TR 23.754 (tutkimus UAS-järjestelmien yhteyden, tunnistamisen ja seurannan tukemisesta), TS 23.256 (UAS-järjestelmien yhteyden, tunnistamisen ja seurannan tuki) ja TS 23.255 (sovelluskerroksen tuki UAS- järjestelmille; toiminnallinen arkkitehtuuri ja tietovirrat).

3GPP on määrittänyt UAV/UAS-ekosysteemiin myös UAS-palveluntarjoajan roolin (UAS service supplier, USS). Kuva 1 esittää verkkoarkkitehtuurin periaatteen kuten se on esitetty spesifikaatiossa 3GPP TS 23.256. Kuvan elementeistä, uusi UAS-verkkotoiminto (UAS NF) tukee UAV:n tunnistusta, verkkopääsynvalvontaa ja seurantaa sekä etätunnistusta (remote identification).

Release 18 ja myöhemmät vaiheet

3GPP jatkaa julkaisujen spesifiointia. Kuten on jo perinteeksi muodostunut,

uusi sukupolvi on tuotu kaupallisille markkinoille kymmenen vuoden välein. 6G seuraa tätä trendiä, sillä ITU on jo aloittanut uusien IMT-2030 -vaatimusten pohdinnan tavoitteenaan valmistella 6G:n kaupallinen vaihe vuoteen 2030 mennessä. Vaikka 6G:n konkreettinen spesifiointi on vielä alkuvaiheissaan, löytyy 6G:n yleisen tason tietoa esimerkiksi ITU:n referensseistä [5].

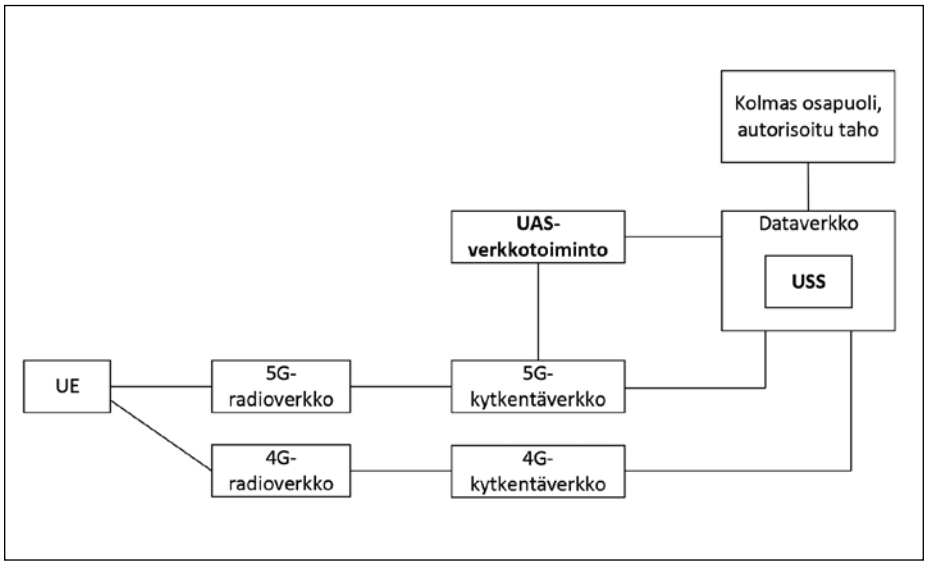
Droonimarkkinat

Droonien markkinat ovat kasvaneet merkittävästi viimeisen vuosikymmenen aikana teknologian kehittyessä. Sääntelymuutokset ja droonien yhä laajempi käyttöönotto eri toimialoilla ovat myös edesauttaneet markkinoiden laajentumista. Vuoteen 2024 mennessä maailmanlaajuisten drone-markkinoiden arvoksi arvioidaan yli 30 miljardia dollaria, ja ennusteet osoittavat kasvun jatkuvan voimakkaana. Tätä laajenemista edistävät droonien monipuoliset sovellukset teollisuudenaloilla, kuten maataloudessa, rakentamisessa, logistiikassa, viihteessä ja yleisessä turvallisuudessa.

Maataloussektorilla drooneista on tullut täydentäviä työkaluja tarkkuusviljelyssä. Monispektrikameroilla ja sensoreilla varustetut maatalousdroonit voivat seurata viljelykasvien tilaa, optimoida kastelua ja havaita tuholaisten aiheuttamat vahingot. Droonien avittama tietoon perustuva lähestymistapa viljelyyn on parantanut satojen talteenottoa ja resurssien hallintaa.

Myös rakennusteollisuus hyötyy drooneista. Drooneja voidaan käyttää työmaan kartoitukseen, projektiseurantaan ja infrastruktuurin tarkastukseen, ja niillä voidaan tallentaa korkean resoluution ilmakuvia ja 3D-malleja rakennustyömailta. Droonit tarjoavat projektivastaaville reaaliaikaisen näkyvyyden työmaan tilanteesta, mikä parantaa tehokkuutta ja turvallisuutta, koska droonien mahdollistaman tilannekuvan kautta työntekijöiden tarvetta liikkua vaarallisilla alueilla voidaan välttää.

Logistiikkasektorilla droonien hyötyjä tutkitaan nk. viimeisen kilometrin toimituspalveluissa. Useat jakeluyritykset investoivat droonitoimitusjärjestelmiin parantaakseen logistiikkaoperaatioidensa nopeutta ja tehokkuutta. Drooneilla on mahdollista ohittaa liikenneruuhkat ja toimittaa paketit suoraan kuluttajien ovelle, mikä lyhentää toimitusaikoja ja -kustannuksia. Vaikka sääntelyhaasteita on edelleen, droonitoimituspalvelujen onnistunut käyttö pilottiluonteisissa projekteissa antaa jo viitteitä tulevasta.



Kuva 1. 3GPP-pohjainen USS-ekosysteemi.

Viihdeteollisuus on käyttänyt drooneja esimerkiksi elokuvauksessa ja ulkoilmatapahtumien taltioinnissa. Korkearesoluutiokameroilla varustetut droonit ovat kehittäneet ilmakuvausta tarjoten entistä dynaamisempia näkökulmia ja katsojakokemuksia.

Yleinen turvallisuus ja hätätilanteisiin reagointi ovat esimerkkejä kriittisestä droonien markkinasta. Poliisilaitokset, palokunnat ja muut katastrofien torjuntatiimit käyttävät drooneja yhä enemmän valvontaan, etsintä- ja pelastustehtäviin sekä tilannekuvan luomiseen. Lämpökameroilla ja edistyneillä sensoreilla varustetut droonit voivat auttaa tilannekatsauksissa, paikantaa kadonneita henkilöitä ja tarjota reaaliaikaista tietoa parantaen operaatioiden tehokkuutta.

Nykyiset droonimarkkinat kasvavat nopeasti, ja drooneista on tulossa välttämättömiä työkaluja useilla teollisuudenaloilla.

Lähitulevaisuuden näkymät

Voidaan olettaa, että matkapuhelinverkkoon liitettyjen droonien merkittävyys kasvaa edelleen samalla, kun 5G-verkot kehittyvät ja yleistyvät. Erityisesti 5G:n stand alone (SA) -arkkitehtuurimallin yleistyminen mahdollistaa kehittyneimmät ominaisuudet ja tehokkaimman suorituskyvyn. Useat nousevat trendit muokkaavat todennäköisesti drooniteknologian tulevaisuutta ja laajentavat niiden roolia entisestään eri teollisuudenaloilla ja yhteiskunnallisissa sovelluksissa.

Yksi odotetuista kehitysalueista on autonomisten droonien laajamittainen käyttöönotto. Nykyiset droonit vaativat vielä pääasiassa ihmisen valvontaa, mutta tekoälyn (artificial intelligence, AI) ja koneoppimisen (machine learning, ML) kehitys yhdistettynä 5G:n tarjoamiin alhaisiin viivearvoihin ja korkean luotettavuuden viestintään mahdollistavat autonomiset droonit, jotka kykenevät navigoimaan monimutkaisissa ympäristöissä, tekemään reaaliaikaisia päätöksiä ja suorittamaan tehtäviä minimaalisella ihmisen ohjauksella. Siviilisovelluksista autonomiset droonit ovat erityisen hyödyllisiä esimerkiksi pakettien toimituksessa reittilentojen dynaamisine muutoksineen.

Drooniparvien konsepti on toinen mielenkiintoinen lähitulevaisuuden kehityskohde. Parviteknologia tarkoittaa useiden droonien koordinoitua toimintaa yhteisen tavoitteen saavuttamiseksi. 5G:n mMTC -ominaisuuksien tukemana on mahdollista hallita suuria drooniparvia saman-

aikaisesti, mikä on hyödyksi esimerkiksi maataloudessa, jossa useat droonit voivat yhdessä valvoa suuria peltoalueita, tai katastrofiaputyössä, jossa parvet voivat nopeasti kattaa laajoja alueita vahinkojen arvioimiseksi ja selviytyjien löytämiseksi. Drooniparvia voidaan myös käyttää puolustus- ja turvallisuussovelluksissa, joissa ne voivat suorittaa koordinoitua valvontaa.

Kaupunkien ilmaliikenne (urban air mobility, UAM) on todellisuutta lähitulevaisuudessa, ja matkapuhelinverkkoon liitetyillä drooneilla on siinä keskeinen rooli. UAM-infrastruktuurin, kuten vertiporttien ja ilmaliikenteen hallintajärjestelmien kehitys riippuu vahvasti 5G-verkkojen tarjoamasta yhteydestä. UAM-aikakaudella drooneja käytetään lyhyen matkan matkustajakuljetuksiin, ilmataksipalveluihin ja tavarankuljetuksiin kaupunkiympäristöissä, mikä mahdollistaa liikennekeskuksien harventamisen, nopeammat matkustusajat ja uudet kaupunkilogistiikan ratkaisut. Menestyäkseen UAM-ekosysteemi vaatii kuitenkin droonien integroimista nykyisiin ilmaliikenteen valvontajärjestelmiin, mikä varmistaa turvallisuuden ja tehokkuuden ruuhkaisessa kaupunkien ilmatilassa.

Matkapuhelinverkkoon liitetyistä drooneista voidaan olettaa tulevan hyödyllisiä työkaluja viranomaisille ja hätäpalveluille. Tulevaisuuden droonit voitaisiin ottaa käyttöön ensiapuyksiköinä hätätilanteissa tarjoamaan reaaliaikaisia tietoja komentokeskuksille ennen henkilökunnan saapumista paikalle. Drooneja voitaisiin käyttää myös yleiseen valvontaan ja liikenteen hallintaan. 5G:n kautta droonit toimivat saumattomasti kaupunkiympäristöissä korkean liikennekeskittymän alueilla. Kyky kerätä ja lähettää korkearesoluutioista dataa reaaliajassa mahdollistaa entistä paremman näkyvyyden ympäristön muutoksiin ja tehokkaamman reagoinnin ekologisiin uhkiin. Lisäksi drooneja voitaisiin käyttää tarkkuusmetsityksessä, jossa ne voivat auttaa istuttamaan puita hakkuualueille tarkasti ja tehokkaasti.

Droonien integrointi muihin lupaaviin teknologioihin, kuten lohkoketjuun (blockchain) ja esineiden internetiin (IoT), voi lisätä edelleen droonien hyötyjä. Esimerkkinä, lohkoketjua voitaisiin käyttää tietojen siirron turvaamiseen droonien ja maanpäällisten asemien välillä, mikä varmistaa kerätyn tiedon eheyden ja aitouden. IoT-integraatio mahdollistaisi puolestaan droonien vuorovaikutuksen muiden älylaitteiden, kuten sensoreiden ja autonomisten ajoneuvojen kanssa, luoden entistä enemmän yhteydessä olevan ja älykkään ekosysteemin.

Yhteenvetona voidaan todeta, että matkapuhelinverkkoon liitettyjen droonien lähitulevaisuus on lupaava. Kun 5G-verkot jatkavat laajenemistaan maailmanlaajuisesti, monet suunnitellut ja täysin uudet käyttökohteet konkretisoituvat monilla eri teollisuudenaloilla, mikä puolestaan edistää entistä tehokkaamman tietoyhteiskunnan kehitystä.

Matkaviestintäpohjaiset UAV/UAS maanpuolustuksessa

UAV/UAS on jo todellisuutta maanpuolustuksen sovelluksissa, ja on tulossa entistä kiinteämmin liitetyksi muihin sotilasjärjestelmiin. UAV/UAS mahdollistaa kehittyneen valvonnan, tunnistuksen, logistiikan, ja edesauttaa taisteluvalmiuden ylläpidossa.

Maanpuolustuksen droonien tehokkuus riippuu vahvasti niiden tietoliikenneyhteyksien toimivuudesta ja laadusta, millä on suora merkitys droonien toimintasäteeseen, datansiirtokyvykkyyteen sekä operatiiviseen luotettavuuteen.

C2:n ja datalinkin suhteen maanpuolustuksen UAV/UAS:n kytkettävyys voidaan jakaa lyhyen kantaman tekniikoihin kuten Wi-Fi, maanpäällisiin solukkoverkkoihin kuten 4G ja 5G (niin julkiset verkot kuin privaattiverkot), sekä laajan alueen satelliittiverkkoihin.

Wi-Fi-yhteydellä varustetut droonit

Wi-Fi-yhteydellä varustettujen droonien ensisijainen etu on niiden helppo käyttöönotto ja alhaiset käyttökustannukset. Sotilasosastot voivat nopeasti ottaa niitä käyttöön ilman tarvetta laajan infrastruktuuri tukeen, mikä tekee niistä ihanteellisia ad hoc -operaatioihin rajatuilla alueilla.

Wi-Fi-yhteydellä varustettujen droonien rajoitukset ovat kuitenkin merkittäviä sotilaskäytössä. Wi-Fi -kantama on suhteellisen lyhyt ja se on altis häiriöille. Rajoitettu kantama voi olla merkittävä haitta lyhyen matkan operaatioihin, ja elektronisen sodankäynnin häirintämenetelmät voivat haavoittaa C2-linkkiä ja tietoliikenneyhteyttä verrattain helposti. Lisäksi tiedonsiirtonopeus ei välttämättä riitä korkearesoluutioiseen videoon tai reaaliaikaiseen data-analytiikkaan, mikä rajoittaa niiden käyttöä tiedustelu- ja valvontatehtävissä, jotka vaativat nopeaa tiedonkäsittelyä ja päätöksentekoa.

LTE-yhteydellä varustetut droonit

LTE-yhteydellä varustetut droonit tarjoavat merkittävän parannuksen kantaman ja luotettavuuden suhteen Wi-Fi -järjestelmiin verrattuna. LTE-kytketyt droonit hyödyntävät laajalle levinnyttä 4G -verkkojen kattavuutta, mikä mahdollistaa niiden toiminnan kaukana ohjauspisteestä. LTE-yhteydellä varustetut droonit soveltuvat hyvin sotilaskäyttöön, kuten laajennettuihin tiedustelu- ja valvontatehtäviin, taistelukentän logistiikkaan ja UAV-parvien koordinointiin.

LTE-yhteydellä varustettujen droonien keskeinen etu on niiden kyky ylläpitää vakaa yhteys laajoilla toiminta-alueilla, mahdollistaen reaaliaikaisen videostriimauksen, telemetrian ja ohjauksen jopa syrjäisissä tai puolikaupunkimaisissa ympäristöissä. Tämä kyvykkyys tekee niistä erityisen hyödyllisiä taistelukentän tilannetietoisuudessa ja komento- ja valvontaoperaatioissa, mikäli vain LTE-peittoalue on käytettävissä. LTE-yhteys tukee myös useiden droonien samanaikaista toimintaa, mikä mahdollistaa monimutkaiset tehtävät, jotka vaativat koordinoituja ponnisteluja, kuten parvitaktiikat taistelutilanteissa.

LTE-verkot ovat kuitenkin edelleen alttiita häirinnälle. Korkean uhkatason ympäristöissä, joissa elektroniset vastatoimet ovat yleisiä, LTE-yhteydellä varustetut droonit saattavat olla alttiita viestinnän häiriöille, mikä voi vaarantaa tehtävän onnistumisen. Lisäksi riippuvuus siviili-infrastruktuurista voi aiheuttaa turvallisuusriskejä, koska nämä verkot voivat olla kyberhyökkäysten kohteena.

5G-yhteydellä varustetut droonit

5G-yhteydellä varustetut droonit edustavat UAV- ja UAM-teknologian huippua sotilasympäristössä. Erittäin alhainen viive, korkea kaistanleveys ja parannettu luotettavuus mahdollistavat erittäin reagoivien datasovellusten käyttöönoton. 5G-yhteydellä varustetut droonit ovat ihanteellisia reaaliaikaiseen tiedustelutoimintaan, autonomisiin operaatioihin ja monimutkaisiin taistelutehtäviin.

Yksi merkittävimmistä 5G-yhteydellä varustettujen droonien eduista on niiden kyky tukea autonomisia ja puoliautonomisia operaatioita minimaalisella ihmisen puuttumisella ohjaukseen. 5G:n alhaisella viiveellä droonit voivat reagoida komentoihin lähes välittömästi, mikä tekee niistä tehokkaita dynaamisissa taistelutilanteissa. Lisäksi 5G-verkkojen korkea kaistanleveys mahdollistaa suurten datamäärien, kuten korkearesoluutioisen videon ja sensoridatan, siirtämisen, mikä mahdollistaa edistyneen analytiikan ja tekoälypohjaisen päätöksenteon lennossa.

5G:n kyky tukea massiivista koneiden välistä viestintää mahdollistaa myös suurten UAV-parvien käytön, jotka voivat suorittaa koordinoituja hyökkäyksiä, valvontaa tai elektronisen sodankäynnin tehtäviä. Suurin haaste 5G-yhteydellä varustetuilla drooneilla on kuitenkin riippuvuus kehittyvästä infrastruktuurista, joka ei välttämättä ole saatavilla kaikilla sotilasoperaatioiden alueilla, erityisesti syrjäisissä tai vihamielisissä ympäristöissä.

Satelliittiyhteydellä varustetut droonit

Satelliittiyhteydellä varustetut droonit tarjoavat maailmanlaajuisen kattavuuden, mikä tekee niistä korvaamattomia sotilasoperaatioissa syrjäisillä, vaikeapääsyisillä tai kiistellyillä alueilla, joissa maanpäälliset verkot eivät ole saatavilla tai luotettavia. Nämä droonit ovat erityisen hyödyllisiä pitkän matkan tiedustelussa, merivalvonnassa ja strategisissa tehtävissä, jotka vaativat jatkuvaa valvontaa laajoilla maantieteellisillä alueilla.

Satelliittiyhteyden ensisijainen etu on sen kestävyys ja luotettavuus monenlaisissa ympäristöissä. Toisin kuin maanpäälliset verkot, satelliittilinkit ovat vähemmän alttiita häirinnälle ja voivat ylläpitää viestintää haastavimmissakin olosuhteissa, mukaan lukien suurilla korkeuksilla tai valtamerien yli tapahtuvissa operaatioissa. Satelliittiyhteydellä varustetut droonit voivat myös tarjota reaaliaikaista dataa ja kuvamateriaalia komentokeskuksiin, jotka sijaitsevat tuhansien kilometrien päässä, varmistaen, että strategiset päätökset perustuvat ajantasaiseen tiedusteluun.

Satelliittiyhteyden suurin haittapuoli on viestinnän mahdollinen viive, mikä voi vaikuttaa reaaliaikaisiin operaatioihin. Satelliittiteknologian edistysaskeleet kuitenkin vähentävät näitä viiveitä vähitellen, mikä tekee satelliittiyhteyksistä yhä käyttökelpoisempia kiireellisissä sotilastehtävissä. Lisäksi satelliittiyhteyksien korkeat kustannukset ja infrastruktuurivaatimukset voivat rajoittaa niiden käyttöä erityisesti laajamittaisissa operaatioissa.

Johtopäätökset

Jokaisella yhteysvaihtoehdolla — esimerkkeinä Wi-Fi, LTE, 5G ja satelliitti, sekä niiden kombinaatioilla — on omat etunsa ja haasteensa UAV- ja UAM-järjestelmien sotilaskäytössä. Wi-Fi-yhteydellä varustetut droonit soveltuvat lyhyen kantaman ja taktisiin operaatioihin, kun taas LTE-yhteydellä varustetut droonit tarjoavat laajemman kantaman ja luotettavuuden monimutkaisempiin tehtäviin. 5G-yhteydellä varustetut droonit tarjoavat mahdollisuuden erittäin autonomisiin ja reagoiviin operaatioihin, vaikka ne ovatkin riippuvaisia kehittyvästä infrastruktuurista. Lopuksi satelliittiyhteydellä varustetut droonit tarjoavat maailmanlaajuisen kattavuuden ja kestävyyden syrjäisissä ja kiistellyissä ympäristöissä, mikä tekee niistä korvaamattomia strategisissa sotilaskäytöissä. Yhteysvaihtoehdon valinta riippuu tehtävien vaatimuksista, toimintaympäristöstä ja käytettävissä olevasta infrastruktuurista, ja jokaisella vaihtoehdolla on kasvava rooli modernissa sotilasarsenaalissa.

Lähteet

Maanmittauslaitos, ”Six drone testing areas established in Finland – research and development made easier,” 3 2023. https://www.maanmittauslaitos.fi/en/topical_issues/six-drone-testing-areas-established-finland-research-and-development-made-easier.

GSMA, ”UAV Commercial Network Field Test,” 11 2023. https://www.gsma.com/get-involved/gsma-foundry/wp-content/uploads/2023/12/UAV-Commerical-Network-Field-Test.pdf.

EUROCONTROL, ”“European UAS Test Centres Alliance” overview - Survey Results,” 2 2024. https://www.eurocontrol.int/sites/default/files/2024-06/eurocontrol-european-uas-test-centres-alliance-survey-results.pdf.

GSMA, ”Cellular-enabled Aerial Vehicles,” 10 2023. https://www.gsma.com/solutions-and-impact/industries/smart-mobility/wp-content/uploads/2024/01/GSMA-North-America-Drones-White-Paper_Final-Nov_30_2023.pdf.

ITU, ”Focus Group on Technologies for Network 2030,” ITU SG13 FG NET-2030. https://www.itu.int/en/ITU-T/focusgroups/net2030/Pages/default.aspx.

TEKSTI: MARTTI AHO

Jatkosodan päättymisestä 80 vuotta

Jatkosodan ajan Jalkaväkirykmentti 4 perustettiin sodanuhka-aikana kesäkuussa 1941 Kotkan–Haminan–Virolahden alueella. Sen pääperustajana ja samalla runkona oli välirauhan ajan vakinainen joukko-osasto, 4.Prikaati, joka rykmentin tultua perustetuksi lakkasi olemasta. JR 4:stä tuli siis ns varusmiesrykmentti (Punamustarykmentin historia I).

Tiistaina kesäkuun 10. päivänä 1941 klo 11.26 saatiin 4.Pr:n esikuntaan II AKE:sta Lahdesta kapt T Kopran antama puhelinsanoma: ”Toimeenpankaa esikäsky-yhdistelmän kohdat 172, 173, 174 ja 178 (4.Pr). Pääkonttorin yleishankinnat alkavat 11.6.1941”. Tulkittuna tämä merkitsi 4.Pr:n osalta seuraavaa: 4.Prikaati on saatettava sa-määrävahvuuteen. Sitä varten kutsutaan ylimääräiseen palvelukseen siihen kuuluva henkilöstö. Hevoset, ajoneuvot ja moottoriajoneuvot on otettava ja suunnitellut hankinnat suoritettava. Ensimmäinen yh-päivä 11.6.1941 (Punamustarykmentin historia I).

”Tiistaina 10.6.1941 klo 13.00 huudettiin kasarmilla hälyytys (kasarmi oli nykyinen RUK:n päärakennus). Kasarmissa majaili mm 4.Prikaatin Viestikomppania. Iltapäivä käytettiin pakkausten ja muitten varusteitten matkakuntoon laittoon. Klo 18.00 suoritettiin ryhmäjako. Minut määrättiin 8.D:n JR 4:n viestijoukkueen II radioryhmään. Ryhmän johtajana toimi reservin korpraali Wanamo. Yö vietettiin kasarmilla.”

Näin alkoi isäni, Vilho Aho, päiväkirja Jatkosodan ajalta, jota hän piti aina kotiuttamiseensa 16.11.1944 asti. Isäni oli astunut vapaaehtoisena varusmiespalvelukseen 2.4.1941 4.Prikaatin Viestikomppaniaan Haminassa. Varusmiespalvelus päättyi 2.4.1943, mutta palvelus jatkui sitten reserviläisenä JR 4:ssä. Isäni osallistui jo Talvisotaan III luokan nostomiehenä Turun Lohkolla Örön linnakkeella vaakakantamittaajana 24.11.1939–29.5.1940.

Kuva 1: Vilho Aho, Korteslampi 1944. Kuva otettu Vilho Ahon kameralla.

Isäni ei juurikaan puhunut sotien aikaisista tapahtumista, joten on ollut todella mieleenpainuvaa lukea hänen kirjoittamaansa päiväkirjaa, josta selviää tarkasti paikkakunnittain hänen sotataipaleensa. Hän otti myös paljon valokuvia koko sodan ajalta. Olen kirjoittanut Jatkosodan alkamisesta Viestimies 3/2021- lehdessä ja tämä on jatkoa sille artikkelille.

Seuraavassa on otteita isäni pitämästä päiväkirjasta heinäkuusta 1944 kotiutumiseen asti.

”7.7. Perjantaina. Tuli taas lähtöön valmistautumismääräys samaan aikaan kuin viime yönäkin. Pian sitä sitten lähdettiinkin ja marssimme noin kolme kilometriä tietä taaksepäin Käsnäselälle päin. Tässä paikassa emme olleet kuin hetken sillä seitsemän aikaan olimme jo uudessa majapaikassamme erään sivutien varrella. (Noin km Uuksujoen eräästä haarasta Uomaan kylän suuntaan). Tämän viimeisen matkan varrella meitä ahdistivat ryssän lentokoneet jonkin verran ja ampuivat ne tykilläkin tien varsille. Niillä oli nimittäin mahdollisuus tähystää Käsnäselän kylästä erästä kohtaa maantiestä, jota kuljimme. Tässä paikassa en ehtinyt nukkua kuin pari tuntia kun taas tuli lähtömääräys. Tällä kertaa tavoitteemme olikin pitkällä sillä marssimme noin 8 km Uomaan kylän ohi ja poikkesimme eräälle Loimolan suuntaan johtavalle sivutielle. Tätä tietä marssimme 12km ja majoituimme Ahvenjärven rannalle (jonkun matkaa Syskyjärveltä itään). Tämän matkan marssiminen multa kesti melko kauan, sillä olin perillä illalla 9 aikoihin ja liikkeelle lähdimme yhdentoista maissa päivällä. Kaikkiaan tuli tämän vuorokauden kuluessa marssittua noin 35 km.”

”8.7. Lauantai. Masinamme alkoi vähän kenkkuilla ja sapuskan jälkeen 12 tienoissa lähdimme koko ryhmä rykmenttiin viemään sitä korjattavaksi. Rykmentti oli Äänislinna–Sortavala tien varrella noin 5 km Sortavalaan päin siitä tiestä jonka varrella me olimme. Malm ei kuitenkaan saanut sitä täällä korjattua, sillä hänen vehkeensä olivat toisessa paikassa. Osa rykmentin esikunnasta oli nimittäin muuttanut toiseen paikkaan, Syskyjärveltä pari kilometriä Leppäsyrjään johtavan tien varteen. Seilamo antoi meille määräyksen ajaa sinne etukäteen ja vartoa siellä. Malm nimittäin tulee sinne loppuporukan mukana. Ajelimme tänne pikkuhiljaa Lemetin kautta ja illalla yhdeksän aikoihin olimme perillä. Ryssät ammuskelivat tänne leirialueelle pitkin päivää tykeillään.”

”9.7. Sunnuntai. Aamuyöstä tuli loppukin porukka tänne ja Seilamo määräsi tämänki porukan herätettäväksi sen takia että toisetkin kuulemma olleet aika liemessä (kumma määräys).”

”2.9. Lauantai. Päivällä ei mitään erikoista. Illalla pääministeri Heckzell piti radiopuheen ja ilmoitti että Neuvostoliiton kanssa on otettu yhteys rauhan aikaan-

saamiseksi. Saksalaiset joukot kuulemma täytyy poistaa Suomesta kahden viikon kuluessa ennen 15.9.1944.”

”4.9. Maanantai. RAUHA VAI ASELEPO? Aamuyön päivystelin ja neljän aikaan aamulla Oitsi soitti keskuksesta että vihollisuudet lopetetaan klo 07.00 tänään. Puoli viiden jälkeen tuli rykmentistä samansisältöinen puhelinsanoma. Kuuden aikaan uutisissa ilmoitettiin että 08.00 lopetetaan vihollisuudet Suomen ja Neuvostoliiton välillä. Nyt täytyy vaan yön päivystyksen jälkeen painua nukkumaan ja odottaa koska tämän sotapäiväkirjan perään saa pistää pisteen. Aselepo se sitten oli vaikka naapurit kyllä ammuskelivat tykillä ja jv-aseilla pitkin päivää. Iltapäivällä oli pitempi tauko mutta nyt illalla ne taas ampuivat muutaman kerran tykillä. Ne kuulemma eivät olleet aselevosta tietoisia kuin iltapäivällä. Omat joukot eivät ole klo 07.00 jälkeen ampuneet laukaustakaan. Illalla puoli kahdentoista aikaan ryssä alkoi pudotella tykillä tästä yli tuonne järvelle ja teki sitä koko yön.”

”5.9. Tiistai. Vasta tänään aamulla kahdeksan aikaan naapuri lopetti ammuskelemisensa. Eilen oli kuulemma Tenho käynyt välimaastossa esittämässä vastassa olevan pataljoonan komentajalle vastalauseen sopimuksen rikkomisen johdosta. Se komentaja oli kuulemma pyytänyt kovasti anteeksi ja sanonut ettei heillä ollut ollenkaan tietoa aselevosta. Toisen pataljoonan lohkolla oli myös käynyt paljon sakkia naapurin leirialueilla ja saanut rauhassa tulla poiskin. Kuusi ukkoa tästä meidänkin lohkoltamme oli mennyt tonttuilemaan sinne, mutta ne eivät päässeetkään pois enään. Vaulo oli kanssa kuollut mentyään hv-miinaan vanjan kanssa neuvotellessaan tai oikeastaan rykmentin komentaja neuvotteli. Tämän päivän on kyllä ollut oudon hiljaista. Korsutyö kanssa lopetettiin niin ettei enään keritty asumaan korsuun. Pian se kyllä olis valmiskin ollut.”

”19.9. Tiistai. Kävin päivällä saunassa ja samalla uimassa. (viimeisen kerran tällä paikalla) Saunasta tullessani kuulin että Suomen ja Venäjän välillä oli allekirjoitettu välirauhan sopimus. Illalla pääministeri pitää puheen ja selostaa tätä sopimusta. Tästä taitaa tulla lähtö tosissaan, sillä Jämsä ilmoitti että aamulla 04.30 on oltava marssivalmiina. Yksi pyörä meiltä meni kuulemma taas pois ja paristolaatikko saadaan pistää kuormaan. Ankarat olivat rauhanehdot. Nyt täytyy alkaa laittaa kamppeitaan kuntoon huomista lähtöä varten.”

”19.10. Torstai. Syntymäpäiväni. Täytin 22 vuotta.”

Kuva 2: Tapsiryhmä matkalla linjanvetoon. SA-kuva.

Kuva 3: ”Unkarilainen” toiminnassa. Kivikoski, Malm, Jääskeläinen, Ala-Kujala. SA-kuva.

”16.11.1944 Torstai. KOTIUTTAMINEN RAUMALTA! Raumalta Pyhärantaa saakka pääsimme normaalilla linja-autovuorolla ja siitä eteenpäin Uuteenkaupunkiin kovalla puhumisella ja sopivalla lisämaksulla. Uudestakaupungista minun oli pakko kävellä kotiin (18 km), sillä yksikään auto ei pysähtynyt ottamaan peukalokyytiläistä. Kotona olin johonkin aikaan illalla.”

JR 4, ”Kolmen Kannaksen Koukkaajat” taisteli Karjalan, Maaselän ja Aunuksen kannaksilla ja sen sotapolkua voi tarkastella osoitteessa www.sotapolku.fi. Sotapolkuun olisi hyvä saada kaikkien veteraanien henkilötiedot. Tätä kirjoitettaessa palvelussa on yli 129 000 henkilön tiedot.

Kuva 4: Viihdytyskietue. Korteslampi 1944. Kuva otettu Vilho Ahon kameralla.

Kuva 5: Marssilla. SA-kuva.

TEKSTI: TERO PALOKANGAS, KUVAT: JUHA PELTOMÄKI.
TERO PALOKANGAS TOIMII VIESTIKILTOJEN LIITTO RY:N PUHEENJOHTAJANA.

Viestimiespäivät Kanta-Hämeessä

Perinteiset Viestimiespäivät järjestettiin 24.–25.8. Etelä-Hämeen Viestikillan toimesta Riihimäen–Räyskälän–Hämeenlinnan alueella. Kolmisenkymmentä osallistujaa pääsi nauttimaan erinomaisesti toteutetun viikonlopun aikana muun muassa aurinkoisesta kesäsäästä, ajankohtaisista tietoiskuista, leikkimielisistä kisailuista, hyvästä ruosta, maittavista löylyistä ja mikä tärkeintä, toistensa seurasta.

KUVA 1: Viestimiespäivien osallistujat kuuntelemassa MPK:n koulutuspäällikkö (JOJÄ) Jouni Purhosen ajankohtaiskatsausta. Etenkin HF-koulutusohjelmaan liittyneet kysymykset kiinnostivat.

KUVA 2: Etelä-Hämeen Viestikillan puheenjohtaja Pekka Wallenstjerna ohjaamassa kalustoesittelyihin osallistujia oikealle rastille.

”Älä anna yhteyden katketa”

Väliotsikon perusohjetta on käytetty Viestimiespäivien kantavana teemana. Ensimmäiset Viestimiespäivät järjestettiin Riihimäen varuskunnassa kesäkuussa 1964 – vain reipas vuosi Viestikillan perustamisen jälkeen. Tarkkaa lukua osallistujamäärästä ei ole, mutta palveluksessa olevat varusmiehet ja kertausharjoituksiin kutsutut reserviläiset mukaan lukien kesäpäivillä oli lähes tuhat maanpuolustajaa. Ohjelmassa oli vapaamuotoisen yhdessäolon lisäksi muun muassa jumalanpalvelus ja viestikalustonäytös. Lukuisten lehtitoimittajien lisäksi myös Suomen televisio oli lähettänyt paikalle kuvausryhmän, mikä lisäsi merkittävästi päivien saamaa julkisuutta.

Eri puolilla maata sijainneet Viestikillan paikallisosastot ehdottivat jo vuonna 1968 yhteisten Viestimiespäivien järjestämistä. Tähän vaikutti myös se, että osallistuminen päiville, sen aikaiset liikenneyhteydet huomioiden, tuotti esimerkiksi Lapissa asuville erityisiä haasteita. Ajatus toteutuikin vaiheittain ja käytäntö alkoi vakiintua Viestikillan siirryttyä liitto- ja alueorganisaatioon vuonna 1989. Viestimiespäiviä alettiin järjestää kiertävällä vastuulla aluekiltojen toimenpitein. Käytäntö on jatkunut näihin päiviin saakka ja kesäpäivät onkin järjestetty vuosien saatossa mitä moninaisimmissa paikoissa.

Viestimiespäivien toteutus ja ohjelmallinen sisältö on muuttunut jossain määrin alkuajoista. Yhdessäolo ja kiltalaisten tapaaminen ovat säilyneet keskeisessä asemassa osana vuotuista tapahtumaa, kuten myös erilaiset osallistujien väliset kilpailut. Sotaveteraanien osallistuminen tapahtumaan on luonnollisista syistä vähentynyt 2000-luvulle tultaessa, eikä varusmiehiäkään ole joitain poikkeuksia lukuun ottamatta tapahtumaan osallistunut. Myös Puolustusvoimien rooli järjestelyjen mahdollistajana on ollut vähenemään päin, koska tapahtumia järjestävien kiltojen toimialueilla ei useinkaan enää ole Puolustusvoimien joukkoja, viestijoukoista puhumattakaan.

Iloisia kohtaamisia, yhdessäoloa ja leikkimielistä kisailua

Vuoden 2024 kesäpäivät aloitettiin Riihimäen varuskuntaravintola Liedessä, jossa nautittiin maittava lounas. Tämän jälkeen liiton puheenjohtaja everstiluutnantti Tero Palokangas avasi tapahtuman. Hän toi samalla Johtamisjärjestelmäpäällikkö Jarmo Vähätiiton terveiset tapahtumaan, sekä valotti johtamisjärjestelmäalan ajankohtaisia Nato-jäsenyyteen liittyviä asiakokonaisuuksia. Tämän jälkeen MPK:n koulutuspäällikkö (Johtamisjärjestelmät) Jouni Purhonen esitelmöi MPK:n ajankohtaisista asiakokonaisuuksista, painottuen viesti- ja HF-koulutusohjelmiin. Mielenkiintoinen esitelmä kirvoittikin useampia kysymyksiä, etenkin HF-koulutusohjelmasta sekä yhteistyöstä Suomen radioamatööriliiton kanssa.

Riihimäeltä siirryttiin Räyskälän ilmailuopistolle, jossa toteutettiin majoittuminen ”päämajoitusmestari” Pekka Wal-

lenstjernan tahdittamana. Tämän jälkeen osallistujille esiteltiin rastikoulutusperiaatteella niin vapaaehtoista pelastuspalvelua, kyläradiotoimintaa, MPK:n HF-radiokalustoa sekä Etelä-Hämeen Viestikillan kehittämää innovatiivista johtamispaikkakonseptia. Useampaankin vastaavaan esittelyyn osallistuneena sanoisin aiheiden olleen erittäin mielenkiintoisia, esittelytavan olleen kohderyhmälle hyvin suunnattu sekä esittelijöiden olleen omaan aiheeseensa vihkiytyneitä ja esittelyyn hyvin valmistautuneita. Esittelyjen jälkeen vuorossa oli maittava päivällinen Räyskälän lentokeskuksen ravintola Huhkajalammessa.

Ruoan jälkeen siirryttiin ”tositoimiin” eli perinteiseen herrashenkilökilpailuun. Tällä kertaa kilpailulajeina toteutui perinteinen tikan heitto sekä ehkä ei niin perinteinen älylaitteilla toteutettu ”pubivisa”. Pubivisan toinen toistaan haastavammat kysymykset rajallisine vastausaikoineen saivat osallistujat tosissaan rapsuttelemaan aivonystyröitään. Tikanheiton osalta tyyli oli perinteisen vapaa ja aika monenlaista suoritusta niin tuloksen kuin tyylinkin osalta nähtiin. Liiton hovikuvaaja everstiluutnantti Juha Peltomäki osoitti melkoista ”TK-kuvaajan” rohkeutta hakeutumalla optimaalisten kuvauskulmien perässä heittojen vaara-alueelle. Illan kruunasi lämpimät löylyt Ilmailuopiston saunoilla sekä syventävät jatkokeskustelut iltapalan kera opiston yleisissä tiloissa.

Sunnuntaina inhimillisen aamuherätysajankohdan ja maittavan aamupalan voimaannuttamat osallistujat lastautuivat linja-autoon, jolla matkattiin Hämeenlinnaan ja Vankilamuseoon. Asiantuntevan opaskierroksen aikana tutustuttiin vuonna 1871 valmistuneeseen entiseen Hämeenlinnan lääninvankilaan. Vankeinhoito lääninvankilassa päättyi vuonna 1993. Lääninvankila muutettiin Hämeenlinnan kaupungin ylläpitämäksi museoksi 1997. Vankilassa tuomiotaan ovat kärsineet monet historian tunnetut rikollishahmot, kuten murhamies Matti Haapoja ja puukkojunkkarit Isoo-Antti ja Rannanjärvi. Linnan naisvangeista tunnetuimpia olivat runoilija Elvi Sinervo ja unisaarnaaja Maria Åkerblom. Hämeenlinnan kuritushuoneeksikin kutsun Vankilan esikuvana olivat sen toiminnan alussa amerikkalaisvankilat, joissa sellit ryhmiteltiin keskikäytävän molemmin puolin. Aiemmin vangit olivat asuneet yhteismakuusaleissa. Tänä päivänä vankeinhoidon ja vankielämän historia ja kertomukset elävät muun muassa seinäkirjoituksissa, esineissä ja ajan kolhimissa selleissä.

Museokierroksen jälkeen matkattiin linja-autolla Riihimäelle ja paikalliselle

KUVA3: Kalustoesittelyssä saatiin ajankohtaiskatsaus muun muassa vapaaehtoisen pelastuspalvelun toiminnasta sekä kyläradiotoiminnasta.

KUVA4: Herrashenkilökilpailun perinteisempänä lajina oli ”supisuomalainen” tikanheitto. Liiton sihteeri Kalle Gripenwaldt tyylittelee, muut kannustavat ja liiton TK-kuvaaja pyrkii pysymään poissa tulilinjalta.

ABC-asemalle, jossa nautittiin monipuolinen lounas. Tämän jälkeen jaettiin herrashenkilökilpailun palkinnot kolmelle parhaalle. Tasaväkisen kisan voitti liiton koulutuspäällikkö Juha Peltomäki, liiton puheenjohtajan Tero Palokankaan tullessa toiseksi, ja Juha Lehtisen Kymen Viestikillasta kolmanneksi. Lopuksi liiton puheenjohtaja kiitti osallistujia sekä Etelä-Hämeen Viestikiltaa erinomaisesti järjestetyistä Viestikiltapäivistä. Samalla muistutettiin syksyn keskeisistä tapahtumista, joista seuraavaksi toteutetaan 20.9.2024 A.R. Saarmaan seminaari.

Ei anneta yhteyden katketa

Tapahtuman päättyessä oli osallistujien keskuudessa aistittavissa tyytyväisyys juuri nähdystä ja koetusta – osallistumismaksulle tuli varmasti moninkertaroin katetta. Tapahtumaa pyrittiin jo tänä vuonna markkinoimaan viesti- ja johtamisjärjestelmäalan vapaaehtoiskentän yhteisinä kesäpäivinä. Totuuden nimissä kauhean paljon ei Viestikiltojen ulkopuolisia tahoja ollut edustettuna. Tässäpä oiva kehityskohde jatkovuosille. Pienellä vaivalla ja lisäpanostuksella Viestimiespäivistä on saatavissa koko toimialan iloisen kesäinen vapaehtoistapahtuma. Haastankin Viestikiltojen lisäksi muutkin alan vapaaehtoistahot, samoin kuin myös aktiivipalveluksessa olevat, mukaan ensi vuoden tapahtuman yhteiseen ideointiin ja toteutukseen. Viestikillat kantavat mielellään jatkossakin pääjärjestämisvastuun, mutta järjestelyihin ja ennen kaikkea osallistumaan otetaan muutkin tahot ilomielin mukaan. Palataan asiaan ensi vuoden tapahtumasuunnittelun käynnistyessä: ei anneta yhteyden tämänkään osalta katketa!

Telealan uutisia

Droonipalveluverkoista

Droonimarkkinat kehittyvät vahvasti, ja ratkaisuja ilmestyy erillislaitteita ja niiden sovelluksia täydentäen myös palvelurintamalla. Esimerkkinä tästä Nokia ja Swisscom Broadcast suunnittelevat laajaa droonipalveluverkkoa (Drones-as-a-Service). Ratkaisuun kuuluu 300 drooniyksikköä parantamaan julkisen turvallisuussektorin operatiivista tehokkuutta sekä teollisia käyttökohteita Sveitsissä. Yhteistyö sisältää myös droonioperaatioiden automaation näköyhteyden takana (beyond visual line of sight, BVLOS) sekä 3GPP-pohjaisen teknologian käyttöönoton. Kyseiset drooniyksiköt on suunniteltu valmiiksi käyttöönotettavaksi (Drone-in-a-Box) vastaamaan mm. hätäpalvelujen tarpeisiin ja kenttäinfrastruktuurin tutkintaan varmistaen samalla pelastushenkilökunnan turvallisuuden. [1]

5G-verkkojen kaupallinen kehitys

Euroopan Unioni on julkaissut uusimpia 5G-tilastoja 5G Observatory -dokumentissaan. Vaikka kyseinen dokumentti seuraa pääasiassa EU-maiden kehitystä, se vertailee myös hiukan globaalia 5G:n käyttöönottoa. Julkaisu on mielenkiintoinen siksi, että se perustuu pääasiassa kansallisten hallitusten toimittamaan dataan.

Julkaistun tiedon perusteella kansainvälisesti aktiivisin 5G-käyttöönottojen maa suhteutettuna asukaslukumäärään on tällä hetkellä Etelä-Korea, joka on selkeä maajohtaja lukemalla 593 tukiasemaa tuhatta asukasta kohti (307 000 5G-tukiasemaa). Tilastoissa seuraavina ovat Kiina lukemalla 245 5G-tukiasemalla tuhatta asukasta kohden (3 500 000) ja EU lukemilla 103 per tuhat asukasta (363 000 tukiasemaa).

5G-taajuusalueista 3.6 GHz on ollut tähän asti suosituin variantti globaalisti. Millimetrialueelta 28 GHz:n taajuus on laajassa käytössä Etelä-Koreassa, Japanissa ja Yhdysvalloissa. Euroopan Unionissa tilanne on monimutkaisempi, sillä kukin jäsenmaa käyttää itsenäisesti omia taajuusalueitaan. Siitä huolimatta lähes kaikki EU-maat käyttävät 3.6 GHz:n taajuutta siinä, kun vain 12 maata käyttää 26 GHz:n taajuutta. Lähde [2] koostaa nykyisen taajuusjaon.

Valmistautumisesta 6G-aikakauteen

ITU:n IMT (International Mobile Telecommunications) -järjestelmät esittävät suorituskykyvaatimukset 3G-, 4G- ja 5G-verkoille. Tällä hetkellä relevantteja käyttöskenaarioita ovat mobiililaajakaista (eMBB), massiivinen esineiden Internet (mMTC) sekä luotettava ja nopea tietoliikenneyhteys (URLLC). ITU on myös tutkinut seuraavan sukupolven oletettavia trendejä ja vaatimuksia, ja on koostanut monia uusia käyttökohteita, jotka toimivat esimerkkeinä uusien potentiaalisten palveluiden vaatimusten konkretisoimiseksi spesifiointityötä tekeville organisaatioille kuten 3GPP:lle. [3]

Näistä ITU:n järkeilemistä palveluista yksi on holografinen viestintä, joka on tietoliikenteelle äärimmäisen vaativa sen prosessoinnin sekä nopean ja viiveettömän, monesta lähteestä yhdistetyn datan vuoksi mahdollistamaan mukaansatempaavia ja interaktiivisia käyttäjäkokemuksia. Niiden toteuttamiseksi, riittävän tehokkaan datansiirron lisäksi myös laadukas näyttömenetelmä on avainasemassa. Onkin siksi mielenkiintoista seurata holografisten kolmiulotteisten laitteiden kehitystä. Nykyinen haaste on kuitenkin kuvien nykytekniikan rajoitteista johtuva vaatimaton laatu.

Eräs käytännön menetelmistä on esittää holografeja perustuen optisiin linsseihin silmälasikehyksiin integroituna. Muiden toimijoiden ohessa Princetonin yliopistossa tutkitaan tekniikkaan vaadittavaa optista elementtiä. [4] Fyysisesti se muistuttaa mittatilaustyönä valmistettua huurretun lasin palaa, jonka pintaan kaiverrettu kuvio on avainasemassa. Tässä tutkimuksessa tekoälyn ja optisten tekniikoiden yhdistelmänä suunniteltu kaiverrettu pinta hajottaa spatiaalisen valomodulaattorin luoman valon tarkasti siirtäen osan kuvan elementtejä taajuuskaistoihin, joita ihmisen silmä ei helposti havaitse. Tämä parantaa holografisen kuvan laatua ja laajentaa näkökenttää. Silti toimivan holografisen näytön luomisessa – oli kyseessä puettava silmälasimallinen tai ilmaan heijastava laite – on edelleen monia haasteita, mutta tutkimus osoittaa yhden konkreettisista etenemissuunnista.

Vakiopalstan kirjoittaja, TkT, tietokirjailija Jyrki Penttinen toimii telealan konsulttitehtävissä Yhdysvalloissa. Voit lähettää Jyrkille kysymyksiä tietoliikennetekniikasta LinkedIn:n kautta www.linkedin.com/in/jypen.

Lähteet

Nokia, ”Nokia and Swisscom Broadcast to deploy largest Drones-as-a-Service network,” 8 2024. https://www.nokia.com/about-us/news/releases/2024/08/08/nokia-and-swisscom-broadcast-to-deploy-largest-drones-as-a-service-network/.

European Commission, ”Digital Decade 2024: 5G Observatory Report,” 7 2024. https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-5g-observatory-report.

ITU, ”Report ITU-R M.2516-0: Future technology trends of terrestrial International Mobile Telecommunications systems towards 2030 and beyond,” 11 2022.

J. Schwarz, ”Holographic displays offer a glimpse into an immersive future,” Princeton University, 4 2024. https://engineering.princeton.edu/news/2024/04/22/holographic-displays-offer-glimpse-immersive-future.

EVERSTILUUTNANTTI R PENTTINEN

Sotakorkeakoulu 50 vuotta

Marraskuun 3. päivänä tänä vuonna on kulunut 50 vuotta Sotakorkeakoulun – maamme ylimmän sotilasopetuslaitoksen ensimmäisen kurssin alkamisesta.

Esitys Sotakorkeakoulun perustamisesta tehtiin jo vuoden 1918 elokuussa silloiselle sota-asiantoimituskunnalle, ja seuraavana vuonna Valtioneuvosto myönsi määrärahan Helsinkiin perustettavalle korkeakoululle. Perustamisvalmistelut, joihin kuului mm lain säätäminen upseerien opetuslaitoksista, veivät aikaa runsaat kuusi vuotta ja vasta 3.11.1924 ensimmäisen kurssin 34 oppilasupseeria pääsivät aloittamaan opiskelunsa.

Sotakorkeakoulun ensimmäisenä johtajana toimi kenraalimajuri V P Nenonen, joka avajaispuheessaan lausui korkeakoulun toiminnan yhä edelleen voimassa olevan perusajatuksen: ”Meidän on luotava sodankäyntimenetelmämme, doktriinimme. Meidän on kasvatettava itsenäisesti ja loogisesti ajattelevia upseereita.”

Sotakorkeakoulu vakinaistettiin hallituksen esityksen mukaisesti v 1930. Talvisodan alkuun mennessä oli noin 350 upseeria saanut korkeakoulun diplomin. Sotien aikana v 1939–1945 koulun toiminta oli keskeytyneenä. Sotien jälkeisinä vuosina Sotakorkeakoulussa on koulutettu noin 800 yleisesikuntaupseeria.

Sotakorkeakoulu tänään

Nykyisellä Sotakorkeakoululla on perustanaan koko itsenäisyytemme aikaiset kokemukset ja perinteet. Laki ja asetus sotilasopetuslaitoksista ovat muotoutuneet useita kertoja uudelleen. Tämän hetken säännökset ovat vuodelta 1966 ja niiden mukaan ”Sotakorkeakoulun tehtävänä on antaa sotatieteellistä ja sotateknillistä opetusta sekä suorittaa vastaavaa tutkimustyötä”. Koulun johtosäännön vahvistaa Puolustusvoimain komentaja ja sen opetussuunnitelmat sekä työjärjestyksen korkeakoulun esimiehenä koulutuspäällikkö.

Koulun johtoon kuuluu kenraalimajurin arvoisen korkeakoulun johtajan lisäksi yleisesikuntaupseerikoulutuksen, sotateknillisen koulutuksen ja maanpuolustuskurssien johtajat, jotka ovat kaikki everstejä tai kommodoreja.

Korkeakoulun johtajana toimii tällä hetkellä kenraalimajuri Pentti Multanen sekä em muissa tehtävissä eversti Juhani Ruutu, kommodori Kauko Konttinen ja kommodori Jan Klenberg.

Opettajaneuvosto on itsenäistä, kollegiaalista päätösvaltaa käyttävä elin, johon kuuluvat korkeakoulun johto ja vakinaiset opettajat. Opettajaneuvosto arvostelee oppilasupseerien tiedot ja taidot sekä päättää heidän siirtämisestään vuosikurssilta toiselle. Se esittää mahdolliset opintojen keskeyttämiset, hyväksyy diplomitöiden aiheet ja antaa oppilaille lopulliset arvostelut. Opettajaneuvosto päättää myös stipendirahastojen varojen käytöstä.

Sotakorkeakoulun kurssit jakaantuvat säännönmukaisesti kaksivuotiseen maasotalinjaan (2–3 opetusluokkaa), merisotalinjaan ja ilmasotalinjaan sekä kolmevuotiseen sotateknilliseen linjaan.

Viimeksi mainittu käsittää opintosuuntia, joita ovat ase- ja ampumateknillinen (ATO), ohjusteknillinen (OTO), pioneeriteknillinen (PTO), viesti- ja sähköteknillinen (VTO), merisotateknillinen (MTO) ja ilmasotateknillinen (ITO)opintosuunta.

Nykyisin kurssit alkavat joka toinen vuosi ja niille otetaan oppilaiksi 80–100 korkeakoulun pääsytutkinnon läpäissyttä upseeria.

Viestialan opetus Sotakorkeakoulussa

Viestialan opetus tapahtuu Sotakorkeakoulussa kolmessa eri tasossa. Näitä ovat yleisen opintosuunnan opetusohjelmaan sisältyvä viestitaktiikan ja viestitekniikan tuntimäärältään varsin vaatimaton opetus- viestiteknillinen opintosuunta ja jossain määrin myös muut tekniliset opintosuunnat sekä ylemmän päällystön viestiteknillinen kurssi.

Yleisellä opintosuunnalla on varsinaisia viestiopin tunteja kahden vuoden aikana maasotalinjalla noin 80 h sekä meri- ja ilmasotalinjoilla noin 60 h. Viestitekniikan osuus em tunneista on noin 20 % loppujen ollessa viestitoiminnan järjestelyä käsitteleviä yleisluentoja (20 %) ja taktiikan harjoituksiin liittyviä toiminnallisia harjoitustöitä (60 %). Opetusta täydentävät merkittävällä tavalla kaikkiin johtamis- ja esikuntaharjoituksiin sekä sotapeleihin sisältyvä, todellisen viestitoiminnan harjoittelu. Näitä harjoituksia on kaikkiaan 7–9 viikkoa.

Viestitaktiikan opetuksen yleisenä päämääränä on muuhun taktiikan opetukseen liittyen perehdyttää oppilaat ensimmäisenä opintovuotena oman puolustushaaransa perusyhtymän viestitoimintaan ja toisena opintovuotena armeijakunnan (vast) ja sotilaslääninviestitoimintaan sekä strategiseen harjoitukseen liittyen antaa yleiskuva myös valtakunnallisesta viestitoiminnasta.

Edellä määritetty viestitoimintaan perehtyminen sisältää tiedot viestijoukkojen organisaatioista, materiaalista ja suorituskyvystä, viestiverkkojen järjestelyperiaatteet yleensä ja erikseen eri sotatoimissa, suurvaltojen viestiorganisaatiot ja niiden vaikutuksen omaan viestitoimintaan (mm kuunteluvaara ja häirintä), viestiliikenteen ja salaamisen järjestelyn sekä viesti- ja sähköteknillisen huollon järjestelyn.

Johtamis- ja esikuntaharjoitukset

Opetusohjelmaan sisältyvät useat johtamis- ja esikuntaharjoitukset ovat yleisten puitteittensa lisäksi useimmiten myös viestitoiminnallisesti varsin laajoja. Tässä suhteessa on merkittävin joka kesä toistuva esikunta- ja viestiharjoitus, josta on muodostunut samalla viestijoukkomme huomattavin ja vaativin sotaharjoitus. Laajimmillaan siihen ovat osallistuneet kaikki Etelä-Suomen viestijoukot aselajista riippumatta.

Esikunta ja viestiharjoitus on täysin todenmukainen johtamisharjoitus, jossa toimii lukuisia oppilasupseerien miehittämiä yhtymäjohtoportaita, ja jonka tilanteenmukaisista viestiyhteyksistä viestijoukot vastaavat.

Lopuksi

Viestiupseerienkin koulutusjärjestelmässä Sotakorkeakoulu muodostaa ylimmän asteen antamalla yleisen yleisesikuntaupseerin pätevyyden lisäksi kelpoisuuden sotilaslääninviestipäälliköksi sekä ylläpitämällä erikoiskurssien avulla heidän maanpuolustukselliset ja viestiteknilliset tietonsa ajan tasalla.

Artikkelin kirjoittaja: Pasi Puhakka

Yhteydet maastoon Nestorin tuotteilla

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

nestor cables

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

Mittarikuja 5,
90620 Oulu
PL 276, 90101 Oulu