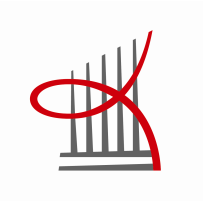


TIETOJENKÄSITTELYN KEHITTYMINEN SOTILASJOHTAMISJÄRJESTELMISSÄ

Tomas Ström

Opinnäytetyö
Huhtikuu 2011
Tietojenkäsittelyn koulutusohjelma
Tampereen ammattikorkeakoulu

TAMPEREEN AMMATTIKORKEAKOULU

Tampere University of Applied Sciences

TIIVISTELMÄ
Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

STRÖM, TOMAS: Tietojenkäsittelyn kehittyminen sotilasjohtamisjärjestelmissä

Opinnäytetyö 69 s.
Huhtikuu 2011

Sodankäynnissä on tapahtumassa suuria muutoksia tietojenkäsittelyn ja tietotekniikan kehityksen ansiosta. Opinnäytetyön tarkoituksena on tutkia uuden tekniikan vaikutusta sotilasjohtamisjärjestelmiin ja selvittää muutoskehitystä kuluvan kahden vuosikymmenen ajalta. Opinnäytetyössä keskitytään taktisen tiedonsiirron käsittelyyn. Opinnäytetyössä käytettävät menetelmät olivat kirjallisuusanalyysi, asiantuntijaluennoille osallistuminen, asiantuntijoiden haastatteleminen sekä muun julkisesti saatavilla olevan lähdemateriaalin tutkiminen ja johtopäätösten tekeminen. Opinnäytetyön kirjoittaja on palvellut ilmavoimissa johtokeskusupseerina ja työskentelee nykyään turvallisuusalalla ICT-asiantuntijana. Kirjoittaja yhdistää opinnäytetyössä kokemuksensa sotilasjohtamisjärjestelmistä tietojenkäsittelyn opiskeluunsa.

Sodankäynti ja sotilasjohtamisjärjestelmät tarvitsevat nykyistä nopeammin muodostettavia tietoverkkoja. Johtamisjärjestelmiä on kyettävä muodostamaan operaation tarpeen mukaisesti joustavin kokoonpanoin. Näihin tarpeisiin voidaan vastata yhtenäistämällä järjestelmiä yhteisesti sovittujen standardien mukaan, joita Nato pääasiassa määrittelee. Ohjelmistoradiotekniikka tulee voimakkaasti lisääntymään ja tuomaan ketterämpiä mahdollisuuksia kytkeä eri tietoverkkoja yhteen ad hoc -periaatteella. Uusia ohjelmistoja ja laitteistoja tullaan tuottamaan enenevissä määrin siviilimarkkinoiden tuotteiden avulla (COTS). Myös taistelukentän osapuolien tilannetietoisuus tulee merkittävästi kehittymään uusien järjestelmien ja niiden mahdollistamien tiedonjakamisen menetelmien myötä. Verkkojen rakenne tulee muuttumaan Mesh -mallin mukaiseksi nykyisistä keskitetymmistä ratkaisuista poiketen. Tietoverkkojen ja verkostosodankäynnin keinoin vastustajasta saatava tietoylivoima on avaintekijä tulevaisuuden sodankäynnissä.

Tietoverkkojen hyödyntämisen merkitys tulee kasvamaan sodankäynnissä entisestään. Suomella on hyvät edellytykset kehittää puolustustaan korkean teknologian osaajamaana. Järjestelmien rakenteeseen liittyvät päätökset vaikuttavat pitkälle tulevaisuuteen koko puolustuksessamme. Langattomaan tiedonsiirtoon siirtyminen, ohjelmistoradiotekniikan tuomat uudet mahdollisuudet ja Nato-standardien noudattaminen ovat keskeisessä asemassa tässä kehityksessä. Ohjelmistoradiotekniikan hyödyntäminen ja kansainvälisiin standardeihin sitoutuminen vievät Suomea myös lähemmäksi Nato-jäsenyyttä. Uudet tietoverkkosodankäynnin muodot luovat täysin uuden aselajin ja myös uuden ulottuvuuden, jota pitää kansallisen turvallisuuden kannalta valvoa ja puolustaa, niin kuin maamme alueellista koskemattomuuttakin puolustamme. Organisaatioita ja henkilökunnan koulutusta on kehitettävä siten, että uusissa johtamisjärjestelmissä kyetään hyödyntämään tiedonjakamista horisontaalisesti nykyistä enemmän. Lisäksi uudet järjestelmät ja tekniikat luovat tarpeen uudenlaiselle osaamiselle ja asiantuntijoille maanpuolustuksessamme.

Asiasanat: Johtamisjärjestelmät, tietojenkäsittely, ad hoc, tietoverkot, ohjelmistoradio

ABSTRACT
Tampere University of Applied Sciences
Degree Programme in Computer Science

STRÖM, TOMAS: The Development of Computing in C4IS Systems

Bachelor's thesis 69 pages
April 2011

The development of computing and information technology is causing remarkable changes to the warfare. The purpose of this thesis is to study the effect of this new technology on to the C4IS systems a period of two decades. Thesis is focused on area of tactical information transfer. The methods which were used to were book-analysis, specialist lectures, specialist interviews and study of other publicy available material. The writer of this thesis has served as C4IS officer at Finnish Air Force, now working as an ICT-specialist in security business. The writer compines his experience of C4IS systems with information science studies in this thesis.

Warfare and C4IS -systems need information networks which can be build-up faster than previously. C4IS -systems are need to build-up based on the operation needs. These needs can be responsed to integration of systems with common standards. These standards are developed mainly by Nato. Software defined radio technology will rapidly increase and bring more agile possibilities to connect different information networks together by the means of ad hoc principles. New software and hardware will be brought to military use from the civilian sector (COTS). The situation awarness on parties of the battlefield will evolve remarkably because of the new systems and the new possibilities for information sharing. The structure of the networks will change from traditional solution into a Mesh model. The situation awarness and situation picture will expand remarkably to all parties on the battlefield. Information superiority against opponent can be reached by combining networks and means of network based warfare. This will be a key factor on future warfare.

The significance of using information networks in warfare will increase. Finland has good prerequisites to develop its defence as it is a high-technology country. The decisions which are made for the system structure will have a long-term effect on our defence. Wireless information transfer, software defined radio systems and Nato standards are in the important role on this development. committing to international standards will take Finland closer to NATO membership. New ways of information network warfare will create totally new branch of service and also a dimension wich should be surveyed and defended like our countrys areal inviolability because of our national security. The training of organizations and personnels should be developed so, that new C4IS systems could be utilised in more horizontal information sharing. New systems and technologies also create a need for new kind of skills and specialists in our national defence.

Keywords: C4IS, computing, ad hoc, information networks, software defined radio

SISÄLTÖ

1 JOHDANTO

Sodankäynti on muuttunut sukupolvittain monimutkaisemmaksi. Erilaisten aseiden, viestintäyhteyksien ja muiden elementtien kehittymisen myötä. Ahvenainen (2008, 24) mainitseekin, että verkottunut toiminta ei ole jatkossa sodankäynnissä etu, vaan välttämättömyys. Johtamisjärjestelmät ja niihin liittyvä tietoliikenneinfrastruktuuri on myös erään maailman johtavan sotateoreetikon John Wardenin mukaan osa-alue, johon halutaan iskeä sodan alkuvaiheessa (Warden 2010). Näin ollen johtamisjärjestelmien ja tietoliikenneinfrastruktuurin tulee olla mahdollisimman kestävä ja korjautumiskykyinen.

Parin lähivuosikymmenen aikana puolustuksen ja sodankäynnin tietojärjestelmät tulevat muuttumaan suuresti. Kehitysaikaväli ja käyttöönottoaika näissä järjestelmissä tulee myös lyhentymään. Insta Defsec Oy:n teknologiajohtaja Antti Kerola kertoo, että 10 vuotta on tällä hetkellä lyhyt aika sotilastekniikan kehityksessä ja hankintavaihe sotilasjärjestelmissä kestää n. 2-5 vuotta (Kerola 2010).

Nykyinen sodankäynti on muuttunut symmetrisestä epäsymmetriseksi, missä rajat tapahtumille ovat epäselvät ja siviilejä on monesti tapahtumien keskellä. Tästä taistelukentän sirpaloitumisesta mainitsee myös Pasi Kesseli (2007). Kansainvälinen terrorismi on esimerkki epäsymmetrisestä uhasta, joka asettaa uudenlaisia haasteita puolustusjärjestelmiemme tietojenkäsittelylle. Tämän myötä myös johtamisen ja tiedonsiirron, sekä tiedonkäsittelyn on muututtava näissä järjestelmissä. Järjestelmien on oltava liikkuvampia, tehokkaampia ja yhteensopivampia useampien toimijoiden kesken kuin aikaisemmin. Pajuniemi ym. (2008, 227-245) määrittelevät kehittämisen tarpeeksi yhteensopivat tietopankit, tiedonsiirtoprotokollat, sanomarakenteet ja rajapintojen yhteensovittaminen eri järjestelmien kesken.

Sotilasoperaatiot ovat nyt ja tulevaisuudessa kansainvälisiä, monen eri kansallisen organisaation yhteenliittymiä, joiden toimenkuva vaihtelee humanitäärisistä tehtävistä aina varsinaisiin sotatoimiin. Tiedonsiirron näkökulmasta tarkasteltuna tarvitsemme enemmän kapasiteettia siirtää ja varastoida erilaista dataa sekä järjestelmän, jolla tätä tietoa voidaan jakaa kullekin organisaation osapuolelle tarpeen mukaan. Tiedonsiirtoverkostojen tulee kyetä muodostumaan erilaisten kokoonpanojen välille nopeasti ja helposti, niin

kansallisella kuin kansainvälisellä tasolla. Päämääränä on kaikkien toimijoiden tilannetietoisuuden lisääminen, jotta ne kykenisivät suoriutumaan niille osoitetuita tehtävistä mahdollisimman tehokkaasti.

Sotahistoriaamme tarkasteltaessa tieto ja sen välittäminen ovat olleet usein ratkaisevia lopputuloksen kannalta. Käskyjen välittäminen omille joukoille oikea-aikaisesti, tiedot vastustajan aikeista sekä järjestelmistä ovat osa sodankäynnin informaatioympäristöä, jolla on ratkaiseva merkitys. Nyt taistelevien joukkojen lukumäärää vähennettäessä jäljelle jääviä joukkoja kehitetään kyvykkäämmäksi. Tietoverkkojen kehitys sotilasjohtamisjärjestelmissä on yksi osa tätä kehitystyötä.

Tämä muutos on ollut käynnissä siitä lähtien kun ensimmäisiä "mekaanisia tietokoneita" käytettiin vastustajan salakirjoitusten aukaisemiseen tai tiedon salaamiseen. Mooren lain mukainen kehitys on johtanut tietotekniikan halpenemiseen ja lisääntyvään hyödyntämiseen. Tietojenkäsittely ja tietotekniikka ovat siirtyneet keskitetyistä suurista palvelimista ja strategisesta toiminnasta jokaisen työkaluksi aina taistelijan henkilökohtaiseen varustukseen saakka. Sama ilmiöhän on tapahtunut myös vuosien varrella siviilitekniikassa. Laskentateho, joka oli ennen yliopistojen käytettävissä, on tänä päivänä jokaisen matkapuhelimessa. Kehitys on keskittynyt nykyään ohjelmistoihin ja lisääntyvään tekoälyyn. Tämän vaikutuksia tarkastellaan tässä opinnäytetyössä tiedonsiirron kehityksen näkökulmasta.

Lisääntynyt kerättävän ja käsiteltävän tiedon määrä vaatii kehittyneempää tietoverkkoa, kuten aikaisemmin todettiin verkottunut toiminta on välttämätöntä nykyaikaisessa sodankäynnissä. Tietoverkot, informaatiosodankäynti ja muut tietotekniset järjestelmät ovat nousseet jopa omiksi asehaaroikseen maailmalla. Voidaan puhua postmodernista sodankäynnin kehityksestä, joka on synnyttänyt kilpavarustelua tälle tietoteknisen sodan alueelle sekä vaikuttanut uusien erilaisten tietosodankäynnin joukkojen perustamiseen.

Tulevaisuuden sotilasjohtamisjärjestelmien tietoverkkojen tulee kyetä vastaamaan tarpeisiin, joita uudet johtamistavat, -välineet ja informaation välittäminen asettavat. Tiedon siirtämisen, jakamisen, varastoinnin ja käsittelyn kapasiteetin on lisäännyttävä huomattavasti näissä järjestelmissä. Näin kyetään vastaamaan uusien vaatimusten mukaisiin haasteisiin. Keskeisintä tietoverkkojen toiminnallisuuteen liittyen on, että saavutetaan

käyttäjille parempi tilannetietoisuuden taso. Näin saavutetaan paremmat edellytykset tehtävien menestyksekkäälle ja tehokkaalle suorittamiselle. Pasi Kesseli (2007, 27) mainitsee verkostosodankäynnin pyrkivän pohjimmiltaan muuttamaan tietoylivoiman taisteluvoimaksi linkittämällä taistelukentältä saatava tieto tehokkaasti yhteiseksi tiedoksi.

Tämän opinnäytetyön tavoitteena on tarkastella tietojenkäsittelyn ja tiedonsiirtotekniikan muutoskehitystä tulevana 10-20 vuotena taktisissa sotilasjohtamisjärjestelmissä. Pääasiassa keskitytään langattomaan tiedonsiirtoon ja tietojenkäsittelyyn. Opinnäytetyön ulkopuolelle rajataan optiset kuidut ja kiinteät tietoliikenneverkot, näitä aiheita kuitenkin sivuutetaan silloin, kun ne liittyvät oleellisesti muuten asiayhteyteen.

Kirjallisten lähteiden tutkimisen lisäksi haastateltiin sähköpostilla alan asiantuntijoita käyttäen seuraavia kysymyksiä:

Mitkä ovat tämän vuosikymmenen tietojenkäsittelyn trendit sotilastekniikassa?

Miten informaatiotekniikka tulee muokkaamaan johtamisjärjestelmiä?

Mitä yhtäläisyyksiä on maa/meri- ja ilmavoimien johtamisjärjestelmissä?

Mitä uusia tekniikoita on tulossa johtamisjärjestelmiin?

Mihin nämä uudet tekniset mahdollisuudet ovat viemässä johtamisjärjestelmiä?

Olen palvelut ilmavoimissa johtokeskusupseerina 2000-luvulla ja yhdistän tässä työssä tietoni- sekä työkokemukseni johtamisjärjestelmistä ja taktisesta tiedonsiirrosta tietojenkäsittelyn opintoihini. Päivittääkseni tietoni viimeisimpään ajan tasalla olevaan, osallistuin opinnäytetyötä varten myös MPKK:n Sotatieteiden päivät 2010 -seminaariluentoihin. Seminaaritapahtuman teemana oli verkostoituminen.

Opinnäytetyön lopussa on sanasto, jossa on selvennetty tekstissä esiintyviä sotilastermejä.

2 SOTILASJOHTAMISJÄRJESTELMÄT

Sotilasjohtamisjärjestelmä käsittää johtamis-, valvonta-, viestintä-, tietotekniikka- ja tiedustelujärjestelmät. Tästä kokonaisuudesta käytetään lyhennettä C4IS (Command, Control, Communication, Computer, Intelligence, Surveillance). Riippuen kirjoittajasta tätä termiä käsitellään eri näkökulmista ja sen koetaan sisältävän erilaisia asioita. Useimmissa yhteyksissä tämänkaltaisen järjestelmän sisäistä prosessia kuvataan reaaliaikaisen tiedon tuottamisena operatiiviseen ja taktiseen tilanteeseen liittyen. Prosessin tuotos on tiedon esittäminen ja tulkinta sotilasoperaation suorittamiseksi (STAE 2020 osa 1. 2004, 275). Haasteet, joihin C4IS-järjestelmät pyrkivät vastaamaan ovat suuren informaatiomäärän käsittely ja hyödyntäminen järjestelmässä jopa reaaliajassa. Tätä tietojenkäsittelyn prosessia kuvataan mm. termillä OODA-loop (**o**bserve, **o**rient, **d**ecide, and **a**ct) eli vapaasti suomennettuna havainnointi, sopeutuminen, päätöksenteko ja toiminta. (Kuvio 1.)

KUVIO 1. OODA-loop päätöksentekoprosessina sotilasjohtamisjärjestelmässä (Lähde: Puolustusvoimat. Pääesikunta. Operatiivinen Osasto. Informaatio-operaatioiden Doktriini.)

Sotilasjohtamisjärjestelmiä kehitetään tietoverkkoja tehokkaammin hyödyntäviksi ympäri maailman. Teoksessa STAE 2020 osa 2 (2004, 124) mainitaan esimerkkeinä: Net-

work-Centric Warfare (USA), Network-Enabled Capability (UK) ja Net-Baserad Försvar (Ruotsi). Kyky valvoa ja hallita tietoa taistelutilassa muodostaa ulottuvuuden, joka on välttämätön vastustajan kukistamiseksi nykyaikaisessa sodankäynnissä. Joissakin yhteyksissä myös kerrotaan ns. "informaatiosodankäynnin joukoista", josta havaitaan, että tietotekniikkaa ja tietojenkäsittelyä ollaan kehittämässä omaksi aselajiksi/asehaaraksi.

STAE 2020 osa 1 (2004, 549) jakaa sotatekniikan tietojärjestelmät kahteen eri päätyyppiin:

1. spesifiset johtamisjärjestelmät
   - havainnointi- ja käskytysjärjestelmät

2. yleisen toiminnan tukemiseen liittyvät järjestelmät
   - järjestelmät yhteistyökumppanien kanssa kommunikointiin

Lisäksi Ahvenainen (2008, 18) jakaa sotilasjohtamisjärjestelmät kolmeen eri kategoriaan: taktiset järjestelmät, operatiiviset järjestelmät ja strategiset järjestelmät.

Järjestelmien tuottama informaatio toimii sotilasjohtamisjärjestelmissä perustana päätöksenteossa ja operaatioiden suunnittelussa vastustajaa vastaan. Tietojenkäsittely sisältää sotilasjohtamisjärjestelmissä prosessit, joissa näitä päätöksiä ja suunnitelmia tehdään sekä tuotetaan. (STAE 2020 osa 2. 2004, 57) Keskeinen tiedonlähde näihin päätöksentekojärjestelmiin on erilaiset tiedustelu- ja valvontajärjestelmät, näiden valvontajärjestelmien jako on mainittu STAE 2020 osa 2:ssa (2004, 57) seuraavasti:

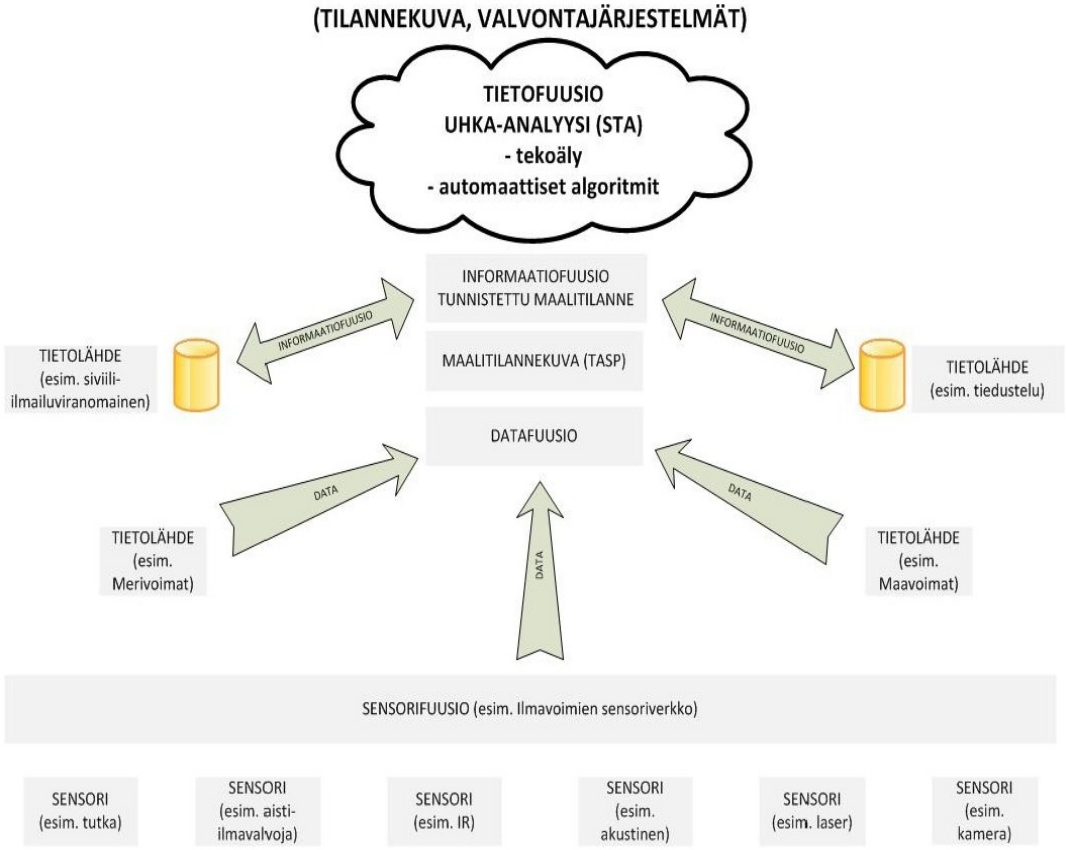
Reaaliaikainen tai lähes reaaliaikainen valvonta

- aluevalvonta
  - rajavalvonta
  - maavalvonta
  - merivalvonta
  - ilmavalvonta
  - vedenalainen valvonta
- toiminnan valvonta

- säteilyn valvonta
- lämpötilan valvonta
- seismisten tapahtumien valvonta
- tietoverkkojen valvonta
- henkilöiden toiminnan valvonta (esimerkiksi kulunvalvonta turvallisuustoimialalla)

- tiedustelujärjestelmillä kerättävät tiedot

Kaikki nämä järjestelmät luovat pohjadatan, jota analysoimalla luodaan kokonaistilannekuva (Kuvio 2.).



KUVIO 2. Tietojenkäsittely eri tasoilla ja tietojen kerääminen sekä yhdistäminen tilannekuvaksi päätöksentekijöille sotilasjohtamisjärjestelmässä.

3 TAKTISTEN SOTILASJOHTAMISJÄRJESTELMIEN NYKYTILA

3.1 Tietojenkäsittely ja tiedonsiirto

Suomen puolustuskykyä ja järjestelmiä on aikaisemmin kehitetty kansallisesta näkökulmasta. Parin viimeisen vuosikymmenen aikana lisääntynyt yhteistoiminta kansainvälisten toimijoiden kanssa edellyttää myös muutosta sotilasteknologiassamme. Tarvitaan kykyä sovittaa järjestelmiä kansainvälisten toimijoiden välillä ja toimia yhteistyössä muiden maiden vastaavien järjestelmien kanssa korostuu. Esimerkkeinä kansainvälisestä yhteistyöstä ja järjestelmien yhteensovittamisesta mainittakoon SCUBAS (Itämeren tilannekuvayhteistyö) ja ASDE (Naton ilmatilannekuvayhteistyö) (Tuominen, 2010). Tätä ei ole mahdollista toteuttaa, ellei käytetä näissä järjestelmissä kansainvälisesti tunnustettuja standardeja. Keskeisimmässä roolissa Suomen kannalta ovat Naton (North Atlantic Treaty Organization) julkaisemat standardit (STANAG). Yhteistyö materiaalihankinnoissa muiden valtioiden kannalta on oleellista, sillä on arvioitu, että puolustusmateriaalin hankintakustannukset kaksinkertaistuvat seitsemän vuoden välein.

Kriittiset tiedonsiirtoverkot, joihin myös sotilasjohtamisjärjestelmien tietoverkot kuuluvat, ovat siirtymässä ip-pohjaiseen rakenteeseen. Uusi tekniikka on tuonut mukanaan uudenlaiset tekniset uhat, jopa kokonaan uudenlaisen sodankäynnin muodon ja aselajin. F-Securen asiantuntija Mikko Hyppönen (2010) mainitsee uusina tietoverkkojen ilmiöinä verkkosabotaasin ja -vakoilun.

Suomen puolustusvoimien nykyiset viesti- ja tiedonsiirtojärjestelmät pohjautuvat pitkälti kansallisten tarpeiden pohjalta suunniteltuihin ratkaisuihin. Nyt järjestelmissä ollaan siirtymässä piirikytkentäisistä pakettikytkentäisiin, osaltaan tämä edesauttaa tulevia yhteensovittamisia uusien kansainväliseen toimitaan yhteensopivien järjestelmien kanssa. Hierarkista organisaatiomallia on aikaisemmin noudatettu myös viestijärjestelyissä ja langattoman tiedonsiirron ratkaisut ovat myös ns. keskitettyihin tukiasemiin tai ei reitittävään tekniikkaan perustuvia. Alemmalla tasolla, esimerkiksi ryhmä- ja joukkuetasolla on käytössä radiotekniikkaa, joka perustuu puheen- ja lyhyiden merkkijonojen siirtämiseen. Näitä ovat esimerkiksi kenttäradio LV217 ja SANLA-viestilaite. Erikoistarpeisiin esimerkiksi meri- ja ilmavoimilla on modernimpia tekniikoita, mutta ne ovat myös pit-

kälti kansallisten tarpeiden, standardien ja määritysten mukaisia, eivätkä siis välttämättä kansainvälisesti yhteensopivia. Yhtenä esimerkkinä mainittakoon ilmavoimien tietovuo-datalinkkijärjestelmä: sitä ollaan vaihtamassa kansainväliseen toimintaan sopivaan Nato standardien mukaiseen Link-16-järjestelmään.

3.2 Aselajit

3.2.1 Ilmavoimien taktinen tiedonsiirto ja tietoverkot

Ilmasodankäynnissä torjuntoja johdetaan johtokeskuksista, joissa tehtävät jaetaan taisteleville ilma-alus yksiköille. Johtokeskus kerää tilannekuvatietoa ja jakaa sitä alaspäin tarvitsijoille. Kokonaisuus koostuu BMC4I (Battle Management, Command, Control, Communications, Computers, Intelligence) taistelunhallintajärjestelmästä (STAE 2020 osa 2. 2004, 357). Tietoverkkojen osalta tässä järjestelmässä on mm. valvonta-, tiedustelu-, taistelunjohdon- ja tulenjohtojärjestelmien tietoverkot (STAE 2020 osa 2. 2004, 357). Juuri johtokeskusten keskeinen rooli ilmapuolustuksessa tulee saattamaan sen suurimpien tietoteknisten muutosten kohteeksi tulevaisuuden kehityksessä.

Hyvä ja modernikaan taistelukone ei pärjää nykyaikaisessa ilmasodankäynnissä yksin. Yhteinen ilmatilannekuva jaettuna datalinkillä jokaiselle hävittäjälle luo todellisen tilannetietoisuuden taistelulentäjälle. Ympäröivän tilanteen jakaminen yksiköiden ja toimijoiden kesken mahdollistaa myös yksittäisen toimijan havainnoinnin ja sensoreiden käytön tilanteeseen parhaiten sopivalla tavalla. Esimerkkinä tämänkaltaisesta tilanteesta ilmataistelussa on uhkamaalin korkeus, joka vaikuttaa siihen minkälaiset asetukset taistelulentäjä valitsee koneensa tutkaan sekä kuinka pari/parvi käyttää koneiden sensoreita keskenään parhaan tilannekuvan saamiseksi taistelutilanteeseen sidottuna.

Ilmavoimien taktisessa tiedonsiirtoympäristössä on tapahtumassa siirtyminen Nato-standardin mukaisen Link-16-järjestelmän käyttöön. Näin saavutetaan ilmavoimille kansainvälinen yhteensopivuus tiedonsiirtojärjestelmien osalta. Yhteensopiva järjestelmä mahdollistaa johtamisen eri verkkotason yhteisoperaatioissa (JOINT) (STAE 2020 osa 2. 2004, 297). Ad hoc -toimintaperiaatetta haetaan tulevaisuudessa kehittämällä tätä

järjestelmää ohjelmistoradiopohjaiseksi. Ad hocin soveltamisesta myös ilma-aluksissa mainitaan STAE 2020 osa 2:ssa (2004, 310).

Hyvää ilmatilannekuvaa ylläpidetään myös välillisin keinoin. Jatkuvalla seurannalla mittausympäristöstä ja mittausolosuhteista sekä olosuhteiden muutosten vaikutuksista kuvaan voidaan pitää yllä tietokantaa (Inkinen ym. 2008, 103-104). Tämänkaltaisen tietokannan antamaa "olosuhdekuvaa" voidaan taas käyttää arvioitaessa reaaliaikaisen kuvan tarkkuutta verrattuna aikaisempiin kokemuksiin.

3.2.2 Maavoimien taktinen tiedonsiirto ja tietoverkot

Yksittäisen sotilaan varustusta ollaan kehittämässä taistelijan henkilökohtaisella tietokoneella/järjestelmällä, jossa taistelija toimii itse yhtenä taistelukentän sensorina osana suurempaa yhtenäistä tietoverkkoa. Saarelainen (2010b) kertoo suomalaisen Elektrobit Oy:n valmistaneen puettavia päätelaitteita siviiliturva-alalle. Tietoa tässä yhteydessä voi olla paikka-, sijainti-, fyysinen kunto-, lämpötila-, syke-, verensokeri-, nestehukka-, lämpöhalvaus-, paleltumis-, ym. arvot.

Sen lisäksi että tietoa saadaan yksittäisestä sotilaasta, tietoa saadaan kerättyä koko toimivasta joukosta. Näin luoden perustaa isommalle toimintakykyarviolle johtamisjärjestelmässä. Tämäntyyppiset numeeriset arvot eivät tarvitse kovin suurta tietoliikennekaistaa langattomissa tiedonsiirtojärjestelmissä ja ovat siksi paremmin toteutettavissa olevia konsepteja verrattuna esimerkiksi puheen- tai videon reaaliaikaiseen siirtoon jokaiselta taistelijalta.

Kun yksittäisellä taistelijalla on hallussaan päätelaite, joka on reaaliaikaisessa kytköksessä taktiseen johtamisverkkoon, tarvitaan keinot tietoturvallisuuden toteutumiseen taisteluolosuhteissa, joissa päätelaite saattaa joutua vastustajan haltuun. Lemmetty ym. (2008, 182) mainitsevat keinoina käyttäjätunnistautumisen (esimerkiksi biotunniste). Yksinkertaisempiakin ja halvemmin toteutettavia tunnistautumismahdollisuuksia voidaan käyttää: esimerkiksi säännöllisin ajoin tehtävä avainkoodin antaminen päätelaitteelle ym. vastaavat menettelytavat. Tärkeää kuitenkin on, että taistelijan päätelaite voi-

daan kytkeä ja kenties jopa tuhota etäkäytöllä, kun havaitaan tai epäillään laitteen joutuneen vääriin käsiin.

Uusi johtamisjärjestelmä ja sen keräämän tiedon kasvu mahdollistavat vanhoihin järjestelmiin verrattuna huomattavasti suuremman tietomäärän välittämisen yksittäiselle taistelijalle. Tämän tietomäärän hyödyntäminen nopeissa taistelutilanteissa ja tilanteeseen sidottuna edellyttää myös panostamista käyttöliittymiin. Saarelainen kertoo (2007, 112) uusien laitteiden lisäävän taistelijan tilannetietoisuutta ja tämän olevan välttämätöntä, koska päätöksiä on tehtävä entistä lyhyemmässä ajassa.

STAE 2020 osa 1 (2004, 561) mainitsee käyttöliittymiksi visiirinäytöt, informaatiotekniikan integroinnin taisteluvälineistöön, kädet vapaana -toiminnot ja puheohjauksen. Kaikilla näillä pyritään minimoimaan tietotekniikan kuormittavuutta ympäristön havainnoinnissa yms. tehtävän suorittamiseen liittyvässä toiminnassa. Majuri Saarelainen (2007, 125) painottaa, että uusista välineistä huolimatta taistelijan tulee kiinnittää huomionsa tapahtumaympäristöönsä ja olla läsnä henkisesti taistelussa jatkuvan päätelaitteen seuraamisen sijaan.

Kehityssuuntana on siis nopeasti luettavissa oleva näyttö, johon voidaan valita eri näkymiä tilanteen mukaan, esimerkiksi selkäreppu tai rannetietokone, kun ajatellaan jalkaväen sotilasta. Ajoneuvoissa tarkoituksenmukaisemmin toiminee HUD (Heads Up Display) ja visiirinäytöt. Vaikka näitä järjestelmiä sovitetaan kunkin toimijan tarpeisiin, se ei silti tarkoita sitä, että haetaan entistä erikoistuneimpia henkilöitä omaan tehtäväänsä liittyen. Sodankäynnissä on usein edullisempaa, että henkilöt ovat tarvittaessa korvattavissa toisilla. Sama sääntö pätee myös järjestelmiin ja aseisiin.

3.2.3 Merivoimien taktinen tiedonsiirto ja tietoverkot

Merivoimat pyrkivät lisäämään toimintansa tehokkuutta verkkosodankäynnin keinoin. Tätä tehokkuutta tullaan hakemaan reaaliaikaisen satelliittivalvonnan, sensorifuusion, johtamis- ja tietojärjestelmien kehittämisen, tiedonsiirron hajaspektritekniikan sekä miehittämättömien alusten järjestelmillä. (STAE 2020 osa 1. 2004, 315.) Kaikki nämä osa-alueet tarvitsevat tehokkaan ja sulautuvan tavan kytkeä järjestelmät yhteiseen verkkoon,

hajaspektritekniikan ollessa tässä tiedonsiirrossa salauksen menetelmä tiedonsiirron salaamiseksi toimijoiden kesken.

Esimerkkinä merivoimaympäristöstä (STAE 2020 osa 1. 2004, 327) on sukellusveneiden tarve liittyä osaksi verkostosodankäyntiä. Edellytyksenä tähän vaaditaan jatkuvaa tietoliikenneyhteyttä, joka ei taas vedenalaisessa toimintaympäristössä ole täysin ongelmaton toteuttaa. Vedenalaisten yksiköiden tiedonsiirto on haasteellisempaa veden toimiessa radioaaltojen välittäjäaineena. Tiedonsiirtokyvyssä ei päästä samanlaisiin nopeuksiin kuin ilmateitse tapahtuvassa radiotekniikassa. Myös paikkatiedon osalta vedenalaisissa kulkuneuvoissa ei GPS-signaalia saada, vaan paikantamisen on perustuttava erilaiseen tekniikkaan. Kuitenkin näiden vedenalaisten elementtien paikkatieto pitäisi saada formaatiltaan yhteensopivaksi tulevaisuuden johtamisjärjestelmän kanssa. STAE 2020 osa 1 (2004, 297) mainitsee mahdollisuuden hyödyntää ad hoc multihopping -tekniikkaa miehittämättömien merivoimien alusten välillä.

3.2.4 Tiedustelujärjestelmät

Tiedustelujärjestelmät käsittävät erilaiset tekniset- ja ei-tekniset menetelmät tiedon keräämiseen, taltiointiin ja analysointiin liittyen. Näiden järjestelmien tietoverkkojen osalta on olemansa internet-pohjaisia järjestelmiä, joista yksi esimerkki on OSIS-järjestelmä (Open Source Information System). Järjestelmä on käytännössä VPN (Virtual Private Network) -verkko, johon on liitetty tietokantoja kaupallisista ja eri organisaatioiden kansallisista järjestelmistä. Yksi esimerkki tiedustelukäyttöön tarkoitetusta kaupallisesta tietoverkosta on Jane's Electronic Library, joka toimii lähteenä erilaisista asejärjestelmistä ja kulkuneuvoista. (STAE 2020 osa 2. 2004, 65.) Nimensä mukaisesti järjestelmä perustuu avoimiin tietokantoihin, vaikka toteutus onkin valvottu VPN-verkko.

Aika on kriittinen tekijä sodankäynnin päätöksenteossa. Näin ollen saatava tiedustelutieto tulee myös saada mahdollisimman nopeasti päättäjien ulottuville oikeassa muodossa. Nopeus on tärkeä tekijä tiedustelutiedon prosessoinnissa, analysoinnissa ja jakamisessa sotilasjohtamisverkoissa. Tästä voidaan edelleen johtaa vaatimus, että järjestelmän tulee olla reaaliaikainen tai ainakin lähes reaaliaikainen. Tiedustelutiedon hyödyntämiseksi

vaatimusten mukaisella tavalla jatkuva tietoliikenneyhteys tulee säilyttää tiedustelun lähteenä olevien elementtien ja päätöksentekijöiden välillä.

Elektronisella tiedustelulla voidaan havaita ja tunnistaa vastustajan järjestelmiä ja jopa yksittäisiä laiteyksilöitäkin erilaisten tunnistusmetodien avulla. Näitä metodeja ovat mm. elektronisen signaalin sormenjälkitunnistus ja tietoliikennevirran tunnistus. Tulevaisuudessa nämä elektronisen sodankäynnin menetelmät saattavat tulla myös taktiseen käyttöön (STAE 2020 osa 2. 2004, 140).

Uutena muotona tiedustelujärjestelmiin on tullut tietoverkoissa tapahtuva tiedustelu ns. "e-Sigint" (Halonen, V. 2008, 54). E-Sigint keskittyy siis käyttämään maailmanlaajuisia tietoverkkoja (Internet) tietojen keräämiseen ja se sisältää mitä ilmeisimmin erilaisia hakkeroinnin ja tiedon keräämisen keinoja.

STAE 2020 osa 2 (2004, 86) esittää keskeisimmäksi tiedustelu- ja valvontajärjestelmien kehitysalueeksi informaatiotekniikan. Erilaisten tietojen yhteen saattaminen eri sensorialueilta yhteiseksi kuvaksi luo uusia mahdollisuuksia analysoida toiminta-alueella tapahtuvia asioita. Taktisesta näkökulmasta saadaan siis tarkempi maalitilannekuva (Target Situation Picture, TASP).

Tietokantoja voidaan analysoida entistä paremmin tietolouhintamenetelmien ja ohjelmistojen kehittyessä eteenpäin. Tietoverkkosodankäynnissä tietolouhinnan avulla voidaan havaita poikkeava käyttäytyminen (esimerkiksi normaalista poikkeava verkkoliikenne) ja saada enemmän aikaa vastatoimien käynnistämiseen (Veijalainen ym. 2008, 540). Tietolouhinta ei rajoitu pelkästään tietoteknisten järjestelmien valvomiseen, vaan sillä voidaan käsitellä myös esimerkiksi valvottavan alueen ilmatilannekuvassa esiintyviä ilmiöitä, esimerkiksi tutkakuvaa tai sähkömagneettisen spektrin signaaleita.

4 TAKTISTEN SOTILASJOHTAMISJÄRJESTELMIEN TULEVAISUUS

4.1 Tietojenkäsittely ja tiedonsiirto

Yhdysvalloista pääosin peräisin oleva näkemys tulevaisuuden sotilasjohtamisjärjestelmistä perustuu eräänlaiseen "all ip" -ratkaisuun (STAE 2020 osa 1. 2004, 13). Ratkaisevaksi tekijäksi tämän tekniikan soveltuvuuteen tuleekin verkon vasteaika suhteessa tiedonsiirron kaistavaatimuksiin. Esimerkiksi paikkatiedon siirtämiseen useammalta taholta vaaditaan huomattavasti vähemmän kaistaa kuin reaaliaikaisen videokuvan siirtoon. Tähän taas vaikuttaa sotilasteknologiassa tiedon salattavuus, tiedusteltavuus ja häiriönsietokyky. Ip-verkkojen ja internetin käyttö sotilasjärjestelmissä ei ole täysin ongelmatonta. Keskeinen huoli on tietoturvasta ja muista internetin hyödyntämiseen liittyvistä riskeistä.

Yhtenäistä kaikille asehaaroille on maalitiedon välittäminen taktisissa järjestelmissä mahdollisimman tehokkaasti. Kehittämällä näitä järjestelmiä pyritään saavuttamaan parempi informaatiopohja ammunnanhallinnalle ja tulenkäytölle (STAE 2020 osa 1. 2004, 164).

Tavoite tulevaisuuden taistelukentällä on eri yksiköiden reaaliaikainen keskinäinen tiedonvälityskyky, sijainnista ja tehtävästä riippumatta. Jatkuva tiedonvaihtamiskyky horisontaalisesti ja vertikaalisesti organisaatiossa on edellytyksenä reaaliaikaisen tilannekuvan muodostamiseksi ja siihen perustuvalle johtamiselle. (STAE 2020 osa 1. 2004, 555.) Kehitystyössä onkin tänä päivänä voimakkaana pyrkimyksenä se, että mikä tahansa aselavetti voi käyttää minkä tahansa sensorin tuottamaa maalitietoa tulenkäyttönsä ja ammunnanhallintansa tarpeisiin (STAE 2020 osa 2. 2004, 221).

Ammunnanhallintajärjestelmien tietojenkäsittelykykyä pyritään kehittämään paikkatietoteknologian ja tiedon analysointikyvyn osalta (STAE 2020 osa 1. 2004, 165). Käytännössä tämä tarkoittaa sitä, että liikkuvista alustoista voidaan entistä paremmin käyttää tulta liikkeen aikana ja liikkuvaan kohteeseen. Kohteen liikettä ennustetaan ammuksen lentoradan aikana ja myös ammuksen lentorataa voidaan päivittää reaaliaikaisesti. Tämä osaltaan parantaa myös nopeasti muuttuvissa maalitilanteissa ja urbaanissa ympäristössä

toimittaessa tarkkuutta. Ammunnan keskeyttäminen/peruminen on paremmin mahdollista, näin vähentäen siviiliuhrien määrää.

Kehittyneemmillä johtamisjärjestelmillä ja niiden tiedonsiirrolla saavutetaan synergiaetua vastustajaan nähden. Tästä tavoitteesta mainitsee myös Sigholm Ruotsin puolustusvoimista. Sigholm (2010) puhuu "Time-Sensitive Targetting (TST)" eli vapaasti suomennettuna "aikakriittisestä maalintamisesta". Keskeinen ajatus tässä on mahdollisimman lyhyessä aikaikkunassa tapahtuva maalintaminen, ampumispäätös ja tulenkäyttö. TST ei ota kantaa, voisiko päätöksenteko olla myös automaattista. Edellytyksenä tälle on taistelukentän reaaliaikainen tiedonsiirto ja verkottunut toimintatapa. Sigholm (2010) mainitsee lisäksi "Mission Sensitive Targetting" -termin. MST tarkoittaa paikallista päätöksentekoa tehtävään liittyen, eli vastuuta on annettu enemmän alaspäin organisaatiossa. MST:llä pyritään vähentämään uusien järjestelmien tuottamaa informaatiotulvaa ja siitä aiheutuvista pullonkauloista pyramidimallisen organisaation hierarkiassa (Sigholm 2010).

Paikkatieto on myös kaikkia asehaaroja yhdistävä tekijä sotilasjohtamisjärjestelmissä. Vastustajaa tehokkaammalla tietojenkäsittelyllä paikkatiedon osalta pyritään saavuttamaan ns. "paikkatietoylivoima" (STAE 2020 osa 1. 2004, 528).

Autonomisissa järjestelmissä kuten ajoneuvoissa, ilma-aluksissa ja vesillä/veden alla liikkuvissa järjestelmissä yleinen tavoite on luoda järjestelmiä, jotka kykenevät tunkeutumaan vastustajan alueelle, suorittamaan valvotaan ja tiedustelua, osallistumaan taistelussa maalinosoitukseen sekä suoraan tulitoimintaan (STAE 2025 osa 1. 2008, 391-392). Nämä haasteet vaativat erittäin kehittynyttä tekoälyä ja suurta tiedon prosessointikykyä. Lähitulevaisuudessa onkin todennäköisempää, että tähän tavoitteeseen pyritään pääsemään sijoittamalla tiedon prosessointia sekä päätöksentekoa enemmän taktisen verkon yli keskitetympään ”tiedonkäsittelyklusteriin".

4.1.1 Tiedonsiirtokyky ja johtamisjärjestelmät

Päätöksentekoa ja vastuuta siirretään organisaatioissa alemmille tasoille, näin suoraviivaistetaan ja nopeutetaan kykyä hallita nopeasti muuttuvia tilanteita. STAE 2020 osa 1 (2004, 365) mainitsee myös tilannetiedon jakamisen kaikille osapuolille yhtenä vaatimuksena lisääntyneeseen tiedonsiirron tarpeeseen mm. miehittämättömissä järjestelmissä. Kaikki toimijat tuottavat tietoja ja saavat tietoa tässä verkossa. Siviilitekniikassa ja internet-teknologiassa on tämänkaltaisesta yhteistyöstä mainittu ns. "kollektiivinen äly", joka kuvaa omalla tavallaan myös samaa mitä em. kaltaisella verkottumisella haetaan sotilasinformaatiojärjestelmissä. Lisäksi reaaliaikaisten taistelujärjestelmien keskinäisellä koordinaatiolla haetaan parempaa synergiaa toiminnan johtamisen tehostumisena.

STAE 2020 osa 1 (2004, 365) kuvaa tulevaisuuden tiedonsiirtoverkon arkkitehtuuria dynaamiseksi verkoksi, jossa on itseorganisoituvia solmuja (ad hoc -periaate) ja datalinkin toiminnan jatkuvaa tarkkailua. Puolustusvoimat on hiljattain tehnyt sopimuksen erään Pirkanmaalaisen ohjelmistotalon (Kilosoft Oy) kanssa taktisen tietoverkon valvontaohjelmistosta. Yritys tekee myös siviilisektorilla verkonvalvontaohjelmistoa. Sotilasversio tuotteesta on nimeltään TitanNMS. Tämä on yksi esimerkki ohjelmistosta, joka vastaa niihin tarpeisiin, joita Halonen (2008, 52-53) mainitsee valvonta- ja hallintatarpeiksi tietoverkoissa. Vastaavankaltaisia ohjelmia on myös saatavilla OpenSource-ratkaisuna (Nagios). Juuri em. kaltaiset ohjelmistot ovat hyvä esimerkki siitä, kuinka visuaalisesti esitettynä ja viimeistellyllä käyttöliittymällä voidaan hallita muuten hankalasti ymmärrettävää informaatioympäristöä. Kuten Hyytiäinen, Lindberg & Mattila (2008, 61) kertovat, tavoitteena tiedon visuaalinen esittäminen sellaisessa muodossa, että se tukee nopeaa ja optimaalista päätöksentekoa. TitanNMS:n ja Nagiosin kaltaiset sovellukset ovat työkaluja, jotka visuaalisesti vastaavat niihin tarpeisiin, joita Lemmetty ym. (2008, 134-135) tarkoittavat: moninkertaistuva ip-osoitemäärä sekä käyttäjämäärä vaativat uudenlaisia työkaluja hallinnointiin ja verkon tilanteen seurantaan. Tiedonsiitokyvyn valvonta on em. tavoilla on erityisen tärkeässä asemassa siksi, että voidaan luottaa järjestelmän päätöksentekomahdollisuuksiin ja siihen, että prosessit toimivat niin kuin on tarkoitus. Tämä on siis osa aikaisemmin mainittua järjestelmän olosuhteiden valvontaa.

4.1.2 Muutoskehitys sotilasjohtamisjärjestelmien tietojenkäsittelyssä

Aikaisempina vuosikymmeninä johtamistavat, työmenetelmät ja prosessit luotiin käytettävissä olevien järjestelmien sekä tekniikan ehdoilla. Nyt johtamistavat ja prosessit asettavat ehdot järjestelmille sekä tekniikalle (STAE 2020 osa 2. 2004, 117). Tulevaisuudessa tiedustelu- ja valvontajärjestelmät suorittavat enemmän toimintoja automaattisesti ja tuovat tiedon päättäjille valmiimpana kuin tällä hetkellä (STAE 2020 osa 2. 2004, 88). Tarvitaan siis vähemmän tiedon käsittelijöitä ja nopeutetaan tiedon eteenpäin viemistä. Tästä kuitenkin aiheutuu se, että koulutusta ja ymmärrystä järjestelmän teknisiin ominaisuuksiin pitää lisätä johtamisorganisaation ylemmällä tasolla. Tiedusteluverkko toimii infrastruktuurina järjestelmään, jonka tehtävä on etsiä, seurata, kerätä, käsitellä ja analysoida tietoa (STAE 2020 osa 2. 2004, 88).

Ohjelmistoista on tullut yksi sodankäynnin taso (STAE 2020 osa 2. 2004, 157). Ohjelmistoja käytetään tässä yhteydessä useaan eri tarkoitukseen: oman toiminnan ja johtamisen tehostamiseen, tilannekuvan ylläpitoon ja laajentamiseen, tiedon tallentamiseen ja analysointiin eri aikajaksoilla. Muutoskehitystä on myös se, että ohjelmistovalmistajien on yhä tarkemmin sovittava keskenään rajapinnoista, joilla ohjelmat keskustelevat keskenään ja alan yleisiä standardeja (NATO STANAG) on myös noudatettava tiukemmin. (STAE 2020 osa 2. 2004, 157.) Suomalainen puolustuskonserni Patria mainostaa tuotteissaan integraatiota ”Integrated Intelligence” -konseptilla, joka sisältää tiedustelun, valvonnan ja johtamisjärjestelmien yhteensovittamisen.

4.1.3 Tiedonsiirron ja tietojenkäsittelyn kehittämisen tavoitteet

Tietojenkäsittelyn kehittämisellä pyritään luomaan tehokkaampi infrastruktuuri sekä ohjelmistoympäristö sotilasjohtamisjärjestelmien informaatioavaruuteen tehostamaan resurssien käyttöä sotilasoperaatioissa. Tämä tehokkuus osaltaan tekee kokonaisjärjestelmästä taistelussa kestävämmän. Näin nopeampi päätöksentekosykli (OODA-loop) tuottaa järjestelmässä paremman tilannetietoisuuden sekä järjestelmien itsesynkronoinnin. (STAE 2020 osa 2. 2004, 116). STAE 2020 myös mainitsee tässä yhteydessä mahdollisuuden kasvattaa alaisten määrää kutakin johtajaa kohden. Tämä kuitenkin lienee mah-

dollista vain tietyissä osakokonaisuuksissa, sillä kasvava informaation määrä vaatii lisää ihmisiä toisenlaisiin tehtäviin kuin aikaisemmin.

Tietoa pitää analysoida, käsitellä ja järjestellä myös tavoin, joita vielä seuraavan 10-20 vuoden aikana ei tekoälyllä ja ohjelmistoilla kyetä täysin toteuttamaan. Kokonaisuudessaan järjestelmiä pyritään integroimaan yhdeksi suureksi johtamisjärjestelmäksi. Pajuniemi ym. (2008, 217-218) mainitsevat tämän integraation kohdistuvan ensin taktisen tason järjestelmiin ja tämän jälkeen ylemmän (strategisen) tason järjestelmiin. Tässä yhteydessä on kuitenkin syytä muistaa, että johtamisessa ja päätöksentekoprosessissa toimiva verkosto on yhtä nopea kuin sen hitain lenkki. Näin ollen johtamisverkkoa on katsottava kokonaisuutena, eikä vain tiettyjen osa-alueiden kehittämisen kautta.

4.1.4 Radiotekniikka ja tietoverkot

Radioverkkojen käytössä sotilastarkoituksiin on aina kaksi puolta. Radioiden käyttö omassa toiminnassa tehostaa johtamista, mutta myös samalla altistaa toiminnan vastustajan radiotiedustelulle (STAE 2020 osa 2. 2004, 55). Näin ollen radioviestinnän käytössä pyritään mahdollisimman vaikeasti häirittäviin ja tiedusteltaviin tiedonsiirtomenetelmiin.

Ohjelmistoradiotekniikka ja sitä käyttävät edulliset päätelaitteet saattavat tulla ns. "joka sotilaan viestivälineeksi". Hyytiäinen (2010b) ennustaa jopa ohjelmistoradioiden korvaavan muut langattomat tietoliikennejärjestelmät.

Jos ajattelemme yksittäisen sotilaan, ryhmän ja joukkueen kokoista toimijaa sotilasorganisaatiossa, niin keskinäiseen viestintään voidaan muodostaa UWB (Ultra-wideband) -tekniikalla lähiverkko melko nopeallakin tiedonsiirtoyhteydellä (STAE 2020 osa 1. 2004, 18). Saarelainen (2010a) myös mainitsee UWB-tekniikan olevan tulevaisuuden järjestelmien tiedonsiirtotekniikka. Näin ollen voisi esimerkiksi joukkueen sisällä välittyä videokuvaa ja ääntä taistelijoiden kesken. Ongelmallisempaa onkin siirtää tätä dataa hierarkiassa ylöspäin esimerkiksi komppanian päällikölle, jos halutaan kaiken datan siirtyvän samanaikaisesti keskitetysti komppanian johtamispaikalle. Kaistan riittävyys

tuleekin olemaan ongelmallinen jo kymmenien videovirtojen ja äänivirtojen välittämiseksi niin tämän päivän kuin lähitulevaisuuden tekniikalla. Todennäköisempää onkin, että ääni ja videodataa välitetään tällä välillä "On-Demand" -tyyppisesti. Yhteys avataan vain silloin kun on tarvetta ja vain niiden osapuolien välille, joilla sitä erityisesti vaaditaan. Verkon resursseja voidaan käyttää siis säästeliäästi, laajakaistaistatiedonsiirtoa tarvitsevat palvelut toimisivat multicast-periaatteella hierarkiassa alhaalta ylöspäin.

Tietoverkkojen hyödynnettävyyttä kasvatetaan tarkemmalla palveluiden profiloinnilla. Paikkatieto yhdistettynä laajennettuun virtuaalitodellisuuteen (Augmented Reality) mahdollistaa kentällä toimivan yksittäisen taistelijan tilannetietoisuuden kasvattamisen. Tätä tarjottavaa tietoa on esimerkiksi taistelukentän valvontasensoreiden tuottama tilannetieto. STAE 2020 esittää näkemyksen siitä, että tulevaisuuden käyttöliittymät ovat enemmän "ei visuaalisella" puolella yksittäiselle taistelijalle, keskittyen mm. puhesynteesiin ja tunnistukseen. Näin vältytään käyttäjille liiallisen visuaalisen informaation tuottamasta kuormituksesta, mikä saattaisi häiritä itse tehtävän suoritukseen keskittymistä. (STAE 2020 osa 1. 2004, 241-242, 561.) Tämä sama seikka on huomattu siviiliteknologiassa mm. autonavigaattoreissa ja erilaisissa ohjausjärjestelmissä, joissa on puheentunnistus. Tällä perusteella voidaan todeta, että puheensiirron merkitys ja näin ollen QoS (Quality of Service) toiminnot ip-pohjaisessa verkossa ovat jatkossa tärkeitä. Tulevaisuuden johtamisverkossa tarvitaan siis riittävästi kaistanleveyttä puheensiirtoa varten langattomassa ympäristössä.

Yleensä sotilasjohtamisjärjestelmien tietojenkäsittelyä pyritään hajauttamaan, osittain siksi, että taistelunkestävyys näin paranisi. Tämä hajauttaminen lisää tarvetta paikalliseen laskentaan ja tiedon varastointiin näissä verkoissa (STAE 2020 osa 1. 2004, 540). Hajauttamiseen liittyy myös tietosuojariskejä, joita esimerkiksi hiljattain julkisuudessa olleet WikiLeaks-vuodot ovat myös todistaneet. STAE 2020 osa 1 (2004, 563) mainitseekin riskinä laitteiden anastamisen, jonka seurauksena tietoverkosta saadaan anastettua salaista tietoa. Juuri näin kävi WikiLeaks-tapauksessa, jossa Yhdysvaltojen salaisia diplomaattiviestejä ajautui julkisuuteen SIPRNet (Secret Internet Protocol Router Network) verkosta. Tietovuoto tässä tapauksessa kuitenkin tapahtui sisäpuolelta. Ehkä tiedusteluverkon suunnittelussa ko. tapauksessa oli mahdollistettu yksittäisen tiedustelu-henkilön pääsy liian suureen määrään tietoa kerralla.

4.1.5 Tiedonsiirron langattomat tekniset ratkaisut tulevaisuudessa

STAE 2020 ennustaa sotilasradiotekniikan kehityksessä kansainvälisiä, yhteisiä standardeja noudattavia ohjelmistoradioratkaisuja tulevan laajasti käyttöön. Erilaisten radioverkkojen yhteiskäyttö on mahdollista ohjelmistoradioilla. Tämä tekniikka mahdollistaa erilaisten toimijoiden esimerkiksi maa-, meri- ja ilmavoimien nopean verkottamisen keskenään. Standardeja (NATO STANAG) noudattamalla kyetään yhdistämään tietoverkot myös kansainvälisissä operaatioissa. (STAE 2020 osa 1. 2004, 14.) Edellytyksenä on ainakin tietyssä määrin avoimen arkkitehtuurin luominen tähän tekniikkaan. Näin eri valmistajat kykenevät tuottamaan keskenään yhteensopivia ratkaisuja (STAE 2020 osa 1. 2004, 67). Lähinnä kyse lieneekin tietoteknisten rajapintojen määrittelystä, yhteisten tiedonsiirron formaattien sekä käytettävien salausmenettelyjen sopimisesta. Tohtori Jarmo Mölsä (2010) kertoo ohjelmistoradioiden ja avoimien standardien olevan tulevaisuuden tiedonsiirtojärjestelmä sotilassovelluksena. Kansainvälisiä lähtökohtia ohjelmistoradiohankkeelle ovat Mölsän mukaan: Air Force R&D (Air Force tactical data link), ARMY R&D (SDR architectures), NAVY R&D (SDR waveformat) ja NAVY MOR. Suomessa kansallinen ohjelmistoradio kehityshanke sisältää OHRA demonstaattorin, hajaspektriaaltomuodon merivoimille (HAME) ja kotimaisen paikannusaaltomuodon (KOMPA). Laitteisto tulee COTS (Commercial Off The Shelf) -pohjaisena noudattaen SCA-laitteistoarkkitehtuuria standardin mukaisesti. SCA määrittely on vapaasti saatavissa, mutta tietoturvarajapinnat ovat vain Yhdysvaltojen kansalliseen käyttöön. Puuttuvia tietoturvarajapintamäärittelyjä tehdään osana eurooppalaista puolustusmateriaaliyhteistyötä (EDA). (Mölsä, 2010.)

Merkille pantavaa on myös, että ohjelmistoradio mahdollistaa verkottumisen myös muihin viranomais- ja kaupallisiin verkkoihin (STAE 2020 osa 1. 2004, 36). Suomessa käytössä tässä yhteydessä voisi olla viranomaisverkko VIRVE sekä laajakaistaiset mobiili-internetyhteydet (3G/4G). VIRVE-verkko perustuu EADS konsernin TETRA tuoteperheeseen, tässä tuoteperheessä on mm. TDR880i dataradio, joka käyttää tiedonsiirtoon siviili matkapuhelinverkkoa. Merkillepantavaa on myös se seikka, että luotaessa viranomaisyhteistyöorganisaatioita ad hoc -periaatteella nopeasti ja dynaamisesti on toimijoiden roolit oltava tarkoin määritelty päällekkäisyyksien ja epäselvyyksien välttämiseksi operaatiossa (Valtonen 2007, 47). Valtonen (2010) pitää myös VIRVE-järjestelmää hyvänä esimerkkinä uuden tekniikan tuomista mahdollisuuksista edistää viranomaistaho-

jen yhteistyötä. Hän huomauttaa kuitenkin, että koordinointia on liian vähän ja kommunikaatiota tiedon kerääjien sekä etsijöiden välillä täytyy kehittää (Valtonen 2010).

"Uuden sukupolven adaptiiviset sotilasaaltomuodot HF-, MIL-VHF- ja MIL-UHF taajuusalueilla pystyvät siirtämään dataa nopeudella yli 1Mbit/s" (STAE 2020 osa 1. 2004, 38). Tämä nopeusluokka riittää niukasti äänensiirtoon, mutta videokuvan reaaliaikainen siirtäminen useammasta kohteesta yhtäaikaisesti lienee mahdotonta tai ainakin kovin huonolaatuista.

STAE 2020 osa 1 (2004, 365) mainitsee myös optiset linkit mahdollisuutena siirtää dataa suuremmalla kaistalla, jopa 1,1Tbs siirtonopeuksilla. Optiset linkit eivät kuitenkaan ole täydellinen ratkaisu, sillä optinen yhteys vaatii toimiakseen aina näkö- tai kuituyhteyden vastaanottajalle. Optinen tiedonsiirto siis sopii huonosti jatkuvasti muuttuvaan ja liikkuvaan käyttäjäympäristöön. Lisäksi sääolosuhteet vaikuttavat optiseen tiedonsiirtokykyyn eikä näin ollen vastaa vaatimuksia kaiken sään toimintakyvylle, joka pääsääntöisesti sotilasjärjestelmissä on.

Tarkasteltaessa tavoitteita yhdistää nopeasti ja tilanteenmukaisesti eri asehaaroja- ja viranomaisverkostoja ohjelmistoradiotekniikan avulla keskenään, voidaan todeta tarve verkon luonteen toimivuudesta ad hoc -periaatteella, tai ainakin samankaltaista toiminnallisuutta haetaan langattomasta tiedonsiirrosta tulevaisuudessa. Tietoturvan suhteen STAE 2020 mukaan salausmenetelmä tulee olemaan taajuushyppelevä hajaspektritekniikka radiolähetteissä (STAE 2020 osa 1, 2004, 39). Ilvesmäki ym. (2008, 59-60) mainitsevat ohjelmistoradioiden tulevaisuudessa kykenevän adaptiiviseen aaltomuotojen käyttöön. Näin saadaan hyvällä signaalikohinasuhteella suuri datasiirtonopeus ja taas häirinnän alaisena kyetään varmistamaan tiedonsiirto alhaisemmalla datanopeudella. Tulevaisuuden taistelukentällä käydään siis tiedonsiirron nopeuskamppailua sähkömagneettiseen spektriin ja sen hyödyntämiseen vaikuttamalla.

4.1.6 Tietoverkkojen kehitysnäkymät tulevilla vuosikymmenillä

Maalla, merellä, ja ilmassa toimivien taistelukentän yksiköiden tiedonkäsittelyn kyky kasvaa ja samalla erilaisten järjestelmien kehittyminen johtaa pidemmälle automatisoituihin toimintoihin ja päätöksentekoon. Tältä osalta tiedonsiirron tarve vähenee, mutta nykyistä enemmän kaistanleveyttä tullaan tarvitsemaan johtuen tavoitteesta jakaa kaikkien toimijoiden tilannekuva eteenpäin johtamisjärjestelmälle. STAE 2020 ennustaa radiotekniikan tiedonsiirtokyvyn nopeusrajaksi 10 Gb/s pidemmällä aikavälillä. (STAE 2020 osa 1. 2004, 377.) Palveluiden virtualisointi ei liene taktisissa järjestelmissä kovin järkevä ratkaisu. Sen sijaan hajautettu laskenta sekä tiedonsiirto erilaisine peer-to-peer ratkaisuineen tuottanee tietoverkkoihin enemmän taistelunkestävyyttä. Peer-to-peer tekniikan soveltamisesta hajautettuun laskentatehoon tulevissa järjestelmissä mainitsee myös Saarelainen (2010a).

Lisääntyvä tiedon määrä, suurta kapasiteettia vaativat relaatiotietokannat ja tarve käyttää kehittynyttä tekoälyä yksittäisessä työasemapäätteessä ovat kallis vaihtoehto. Kustannustehokkaampaa onkin luoda kevyitä päätteitä, joissa on selainratkaisu keskitettyyn palvelimeen (STAE 2020 osa 2. 2004, 104). Ns. "tyhmä pääte" taistelukentällä on myös tietoturvallisempi kokonaisuuden kannalta. Vastaavasti heikkoutena tämänkaltaisen päätteen osalta on sen jatkuva riippuvuus tietoliikenteestä. Laitteiden fyysistä sijaintia rajoittaa ainoastaan tietoliikenneyhteyksien asettamat rajoitteet.

Tiedon esittämisen kehittäminen käyttöliittymätasolla on lähitulevaisuuden keskeinen asia johtamisjärjestelmissä. Tähän viittaa STAE 2020 osa 2 (2004, 117), jossa mainitaan symbolit graafisena esitysmuotona, sisältäen useamman tiedon kokonaisuuden fuusioituna yksinkertaiseen näkymään. Samassa yhteydessä mainitaan animaation käyttömahdollisuuksia menneen ja tulevan esittämiseen. Eli toisin sanoen tulevaisuuden taktinen johtamisjärjestelmä sisältää käyttöliittymän, jossa tietoa esitetään nopeasti omaksuttavin graafisin symbolein. Taistelun etenemistä voidaan takautuvasti kelata historiatietona tietokannan kautta, lisäksi tekoäly kykenee ennustamaan mahdollista tapahtumien kehittymistä eteenpäin tulevaisuudessa. Siviilimaailmasta vastaavaa voisi hakea esimerkiksi kaikille tutun sääennustuksen tapaisesta järjestelmästä.

Erilaiset itsenäisesti toimivat laitteet kuten miehittämättömät lennokit, ajoneuvot ym. vastaavat lisääntyvät taistelukentällä. Näin myös lisääntyy tarve siirtää dataa miehittämättömien yksiköiden ja johtamisjärjestelmän välillä. Mitä itsenäisemmäksi laite halutaan, sen enemmän se tarvitsee tekoälyä ja vastaavasti kappalehinta laitteelle kasvaa. Tehokkaan tiedonsiirtoverkon ja tekoälyn siirtämisellä verkkoon ns. pilvipalveluksi voidaan laskea hintaa miehittämättömien laitteiden ja erilaisten sensorien osalta. STAE 2020:ssä kerrotaan, että miehittämättömissä laitteissa voisi olla automatiikka, joka mahdollistaisi tietoliikenneyhteyden ollessa poikki myös itsenäisen toiminnan (STAE 2020 osa 1. 2004, 240). Esimerkiksi joissakin nykyisissä miehittämättömissä ilma-aluksissa on toiminto, joka tietoliikenteen katkeamistilanteessa ohjaa koneen takaisin tukikohtaan.

4.1.7 Vaatimukset tietojenkäsittelylle tulevaisuuden sotilastietoverkoissa

STAE 2020 mainitsee reaaliaikaisuuden ja datan yhtenäisen esitystavan olevan vaatimuksia tulevaisuuden tietoverkolle sotilasjohtamisjärjestelmissä (STAE 2020 osa 2. 2004, 109,124,189,211). Nato julkaisee standardeja, joiden mukaan voidaan yhtenäistää sotilasorganisaatioiden tietojärjestelmiä kansainvälisesti. STAE 2020 mainitsee tässä yhtenäisen arkkitehtuurin, tietomallit ja yhtenevät tietoliikenneratkaisut standardien mukaan kehitettäviksi kohteiksi (STAE 2020 osa 2. 2004, 96, 99, 296). Arkkitehtuuri tarkoittaneen tässä yhteydessä mm. ip-arkkitehtuuriin siirtymistä suurimmassa osassa verkkoratkaisuja, tietomalleilla voidaan tarkoittaa mm. yhteneviä esitystapoja esimerkiksi paikkatiedolle (esimerkiksi ilmailussa WGS84 -koordinaatisto) tai sitten tarkemmin esimerkiksi SQL-tietokantaan tallennettavan tiedon malli ja muoto.

Naton julkaisussa (ADatP-34(C)) mainitaan J3IEDM-standardi, joka määrittelee tietomallit niin maa-, meri- kuin ilmavoimien käyttöön tulevissa järjestelmissä. Tietoliikenneratkaisuissa haetaan mm. ohjelmistoradiotekniikalla helposti yhteen sovitettavia järjestelmiä eri kansallisuuksien kesken huomioiden myös kansainvälisten operaatioiden vaihtelevat tarpeet kaistan käytölle (Mölsä 2010). Jotta järjestelmien sovittaminen ja yhteisten tietovarantojen käyttö niiden kesken saataisiin mahdolliseksi, on suunnittelussa haettava Nato-standardeihin soveltuvaa relaatiotietokantarakennetta. Tieto tähän kantaan tallennettaan jollakin yleisesti hyväksytyllä standardilla. Tämä voisi olla esimerkiksi XML-kieli, jota olisi hyvä sovittaa COTS-tuotteiden kanssa (STAE 2020 osa 2. 2004,

100). Naton tekninen arkkitehtuuri määrittää myös rakenteet, palvelut ja tuotevalinnat, joita Nato-yhteensopivissa johtamisjärjestelmissä tulee käyttää (STAE 2020 osa 2. 2004, 100). XML-kielen mainitsevat myös Veijalainen ym. (2008, 545-546) sopivaksi tekstien ja dokumenttien jakeluun. Sopivuus liittyy siihen, että XML on alustariippumaton ja siten hyvin skaalautuva eri laitteistoille. Myös Nato ADatP-34(C) sisältää XML-kielen käytön tulevissa järjestelmissä.

Kahtena keskeisenä vaatimuksena STAE 2020 osa 2 (2004, 109) mainitsee omien joukkojen tunnistamisen (blue force tracker) ja omien joukkojen tulenkäytön verkottamisen (sensor-to-shooter). Yhdessä nämä vähentävät omia tappioita, ehkäisevät omien joukkojen joutumista oman tulen alle (friendly fire) ja tehostavat kokonaisjärjestelmän tulenkäyttöä vastustajaa vastaan.

4.1.8 Link-16

Sotilastekniikassa Yhdysvallat ja Nato ovat keskeisessä asemassa, kun määritellään tulevaisuuden johtamisjärjestelmien tiedon muotoja ja siirtotapaa. Esimerkkinä tästä standardointityöstä Hyytiäinen, Lindberg & Mattila (2008, 64) mainitsevat mm. Shared Tactical Group Picture (STGP) -ohjelman. Se määrittelee yhtenäisen kehyksen ja siirtoprotokollan tiedonsiirrolle. Samassa yhteydessä lähde mainitsee myös avoimen OMG (Object Management Group) SOPES-ohjelman. Nato organisaationa hyväksyy siis myös avoimen kehityksen järjestelmissään. Kaiken sotilastekniikassa ei tarvitse olla suljettua ja yhden tietyn tuottajan valmistamaa tuotetta.

Teknisenä standardiesimerkkinä mainittakoon Link-16 standardi. Tämän standardin mukainen järjestelmä päivitetään suomalaisiin Hornet-hävittäjiin kansallisella tasolla kehitetyn datalinkin tilalle. Link-16-järjestelmän kehitys on aloitettu 1975. Yhtenä viimeisimmistä tapahtumista on MIDS-päätelaitteiden käyttöönotto. Yhdysvallat käyttävät järjestelmästä nimitystä JTIDS (Joint Tactical Information Distribution System, JTIDS). Järjestelmä käyttää hyppivätaajuista radiotekniikkaa häirinnän estämiseksi. (Pajuniemi ym. 2008, 226.) Jotkut ovat arvostelleet Link-16-järjestelmän olevan ominaisuuksiltaan vaatimattomampi kuin kotimaista tuotantoa oleva järjestelmä, joka alun perin asennettiin tietovuojärjestelmäksi Hornet-hävittäjäkoneisiimme. Tässä suhteessa kuitenkin kan-

sainvälistä yhteensopivuutta ja Nato-standardien noudattamista päättäjät ovat pitäneet tärkeämpänä kuin teknistä kehittyneisyyttä. Link-16-standardi edellyttää yhteensopivuuden toteuttamista kaikilla OSI-mallin tasoilla: fyysisessä ilmarajapinnassa, tiedonsiirtoprotokollassa, sanomarakenteessa ja esitystavassa (Pajuniemi ym. 2008, 227).

Link-16-järjestelmä ei kuitenkaan sisällä adaptiivisia aaltomuotoja ollessaan sen verran vanha standardi, että ohjelmistoradiotekniikka ja sen tuomat uudet mahdollisuudet eivät vielä olleet ajankohtaisia Link-16-järjestelmää kehitettäessä. Pajuniemi ym. (2008, 228-229) mainitsevatkin, että Link-16 saattaa vanhentua hyvin nopeasti. Suomen kannalta tämä on erityisen hankalaa 2010-luvulla koska järjestelmiämme päivitetään kansallisista Link-16 yhteensopivaksi Nato-yhteensopivuuden saavuttamiseksi, mutta alalla ollaan kuitenkin menossa uusiin adaptiivista aaltomuotoa käyttävään ohjelmistoradioratkaisuun.

4.1.9 JTRS (Joint Tactical Radio Systems)

Sotilasradiotekniikka on siirtymässä ohjelmistoradiopohjaiseksi. Ohjelmistoradion toimintaperiaate on, että radion käyttämät taajuudet ja modulaatiot voidaan muuttaa ohjelmallisesti (Pajuniemi ym. 2008, 227-228). Näin ollen esimerkiksi kansainvälisissä organisaatioissa voidaan sovittaa taajuusalueet ja viestintäverkot yhteen pelkästään ohjelmistoja muokkaamalla.

Ohjelmistoradiojärjestelmiä varten Natolla on olemassa JTRS (Joint Tactical Radio Systems) standardi (Pajuniemi ym. 2008, 228). JTRS on Yhdysvaltojen ohjelmistoradiohanke, jonka aaltomuotojen kehittäminen perustuu SCA (Softare Communication Architecture)-ohjelmistoarkkitehtuuriin. Nämä aaltomuodot ovat ladattavissa kaikkiin SCA-yhteensopiviin laitteisiin (Pajuniemi ym. 2008, 228). JTRS standardi pyrkii tuomaan Link-16-järjestelmää kehittyneemmän tiedonsiirron mm. WNW (Wideband Networking Waveform) aaltomuodon avulla taktisiin tietoverkkoihin. JTRS standardin mukaisessa siirtoverkossa tiedonsiirtokapasiteetiksi on arvioitu 2-5Mbit/s (Pajuniemi ym. 2008, 228). Tämä riittää yhden kanavan videosiirtoon melko hyvällä tarkkuudella.

JTRS järjestelmässä haetaan myös kykyä muodostaa dynaaminen, skaalautuva ad hoc -verkko (Pajuniemi ym. 2008, 225-228). Ohjelmistoradiot tulevat ensimmäisinä tukiasemiin ja ajoneuvoihin, joissa kyetään tarjoamaan laitteistolle riittävä virransyöttö eikä laitteiden koko ole niin merkittävä tekijä (Ilvesmäki ym. 2008, 29). Näin ollen voidaan myös päätellä, että tulevaisuuden johtamisjärjestelmien päätteet sijaitsevat ensin kulkuneuvoissa ja muissa raskaammissa yksiköissä ennen kuin ne siirtyvät yksittäisen taistelijan päätelaite varustukseen. Ohjelmistoradion etuna on myös erinomaiset LPI/LPD- ja AJ-ominaisuudet (häirinnän sieto-, väistö- ja tunnistusominaisuudet) (Mölsä 2010).

4.1.10 Ad hoc -verkot

Tietoverkot tulevat olemaan kaikkialla läsnä ja aina kytkettävissä. Tätä läsnäoloa voidaan saavuttaa mm. taistelijan puettavilla laitteilla. Tämä ei kuitenkaan välttämättä tarkoita sitä, että jokaisella taistelijalla olisi oma henkilökohtainen tietokone näyttöpäätteineen. Todennäköisemmin jo pelkästään taloudellisista syistä näitä päätelaitteita tuodaan ensin joukkueenjohtajatasolle ja sitten mahdollisesti ryhmänjohtajatasolle. Verkon rakenne tulee kuitenkin toimimaan siten, että jokainen päätelaite toimii myös itsenäisenä tukiasemana verkolle P2P (peer-to-peer) -periaatteella.

Tietoliikenneratkaisuna mitä todennäköisimmin tullaan näkemään ohjelmistoradioratkaisu, joka toimii ad hoc -periaatteen mukaan tuottaen palvelua niihin tarpeisiin, jotka juuri kyseistä kokoonpanoa ja yksikköä tietystä tilanteessa parhaiten palvelee. Palveluprofiilit tulevat olemaan personoitavissa laitteiston käyttäjille, sekä tarpeen mukaan muokattavissa. Mahdollisesti tulemme näkemään jonkinlaista "laajennetun todellisuuden" (Augmented Reality) tyyppisiä toteutuksia paikkatiedon lisäksi tulevaisuuden taistelijan päätelaitteissa. (STAE 2020 osa 1. 2004, 16-25)

Sotilasjohtamisjärjestelmien tietoverkoissa ollaan keskittämässä tietojen säilytystä palveluhotelleissa. Tietoa jaetaan näistä keskuksista tarvitsijoille. Palvelinhotellijärjestelyillä mahdollistetaan taistelunkestävä, varmennettu verkosto. Lisäksi tämä rakenne tulee muokkaamaan toimivien organisaatioiden kokoonpanoa: toimipisteiden ja toimijoiden ei tarvitse sijaita fyysisesti samassa paikassa. Tämä parantaa myöskin taistelunkes-

tävyyttä. (STAE 2020 osa 1. 2004, 28.) Hyytiäinen (2010b) kertoo organisaatio muutoksen vähentävän päätöksentekoketjun väliportaita ja verkon kautta tapahtuvan johtamisen lisääntyvän.

Ad hoc -verkot soveltunevat myös muuhun kuin henkilöjohtamiseen. Erilaisten järjestelmien väliseen tietojenvaihtoon ja sensorien kytkemiseen keskenään toimivaksi verkoksi voidaan soveltaa ad hoc -tiedonsiirtotapaa. Käytännön esimerkkinä voisi olla esimerkiksi tukikohdan vartiointiin liittyvät tilapäiset sensorit, jotka hälyttäisivät havaitessaan liikettä valvonta-alueellaan. Tämänkaltaisia antureitahan käytetään nykyään mm. rajavalvonnan yhteydessä.

Ad hoc -verkon hyödyntämismahdollisuudet

Ad hoc -verkkoa voidaan käyttää maavoimien toimintaympäristössä erilaisten sensorien verkottamiseen. Sensorit ja verkon tarvitsema tekniikka voidaan integroida sotilaiden varustuksiin. Pidemmällä etäisyydellä voisi esimerkiksi joukon ohjelmistopohjainen kenttäradio toimia välittimenä taktiseen verkkoon. (STAE 2020 osa 1. 2004, 28-31.) Jos ajattelemme esimerkiksi joukkueen kokoista (n. 30 miestä) osastoa, jolla jokaisella yksilöllä olisi mukanaan sensorit, jotka keräisivät taistelijan fyysisestä kunnosta, paikkatiedosta, aseistuksen tilasta, ääniympäristöstä (puheyhteys) ja mitattavia arvoja esimerkiksi sääolosuhteista. Näin luodaan 30 liikkuvan sensorin verkosto. Tämä kykenee tuottamaan aivan uudenlaisen tilannekuvan verrattuna pelkkään kenttäradio/puheyhteysmenetelmään.

Uudessa ad hoc -mallissa saavutetaan kollektiivista tietoutta, ns. "joukkoälyä". Tilanne muuttuu vielä paremmaksi, mikäli kaistanleveys riittäisi jopa videoyhteyden siirtämiseen jokaiselta taistelijalta. Esimerkiksi niin, että jokaisen taistelijan aseessa olisi maalikamera. Sen lisäksi, että toiminnasta saadaan reaaliaikainen kuva, saadaan myös taltioitua tapahtumia myöhemmän analyysin, tilannearvion ja tiedustelun tarpeisiin. Maalikamerakuva voi sisältää tässä tapauksessa myös muuta kuin perinteistä videokuvaa, esimerkiksi valonvahvistin- tai lämpökamerakuvaa.

Tulevaisuudessa esimerkiksi panssarivaunun kohdatessa kohde, jonka luokituksesta maaliksi tai siviiliksi ei voi olla varma (esimerkiksi urbaanissa ympäristössä), voi kaksisuuntaisella taktisella ad hoc -tietoverkolla ottaa etäyhteyden panssariajoneuvon sensoreihin. Toinen operaattori taistelujärjestelmässä lisää omaan tilannekuvaansa esimerkiksi miehittämättömän lennokin tuottaman kuvan ja näin saa päätöksenteon tueksi paremman kuvan, kuin mitä panssariajoneuvon miehistö kykenee omilla sensoreilla saamaan. Mikäli maalikuva on vieläkin epäselvä, voidaan kohteen lähettämiä herätteitä analysoida tietokannasta löytyviin malleihin ja kenties niiden avulla päätellä, onko esimerkiksi kohteesta saatu sähkömagneettisen spektrin heräte vihollisen vai jonkin muun. Tässä lyhyt esimerkki miten uusia johtamisjärjestelmiä soveltaessa toiminta voisi muuttua ja samalla tilannetietoisuus paranisi taistelukentän toimijoilla.

Mälkki (2009 25) esittää kriittisempää arviota ad hoc -periaatteen hyödyntämismahdollisuuksista. Mälkki kyseenalaistaa laaja-alaisen ja massiivisen organisaation kyvyn toimia ad hoc -tyyppisesti, tarvitaan yhteisesti etukäteen harjoiteltuja ja ymmärrettyjä perusperiaatteita. Toisaalta ad hoc -menetelmän hyödyntäminen ei tarkoita sen jatkuvaa käyttöä, vaan tilanteen niin vaatiessa hyödyntämistä.

Ad hoc -verkon soveltuvuus sotilaskäyttöön

Ad hoc -rakenne ja ratkaisumalli vaikuttaisi olevan erittäin soveltuva sotilaskäyttöön. Myös STAE 2020 osa 2 (2004, 312) ennustaa ad hoc -verkkojen yleistyvän laajasti. Naton pitkän aikavälin kehityskonsepti on mobiili ad hoc -verkko (MANET) (Nato. 1998-2998. NISP. Online).

Rajoitteensa kuitenkin tekniikalla on, käytännössä lyhyemmät etäisyydet mahdollistavat suuremman tiedonsiirtokapasiteetin ja pidemmät yhteydet ad hoc -verkossa taas pienemmän (Ilvesmäki ym. 2008, 27). Puhe- ja videokuvansiirtotarve usein onkin taistelukentällä juuri lähietäisyyksillä, kun taas johto-/komentoportaaseen riittänee tekstimuotoinen data. Myös verkon solmujen määrä vaikuttaa tiedonsiirtokapasiteettiin. Mitä enemmän solmuja, sen vähemmän tarvitaan todennäköisesti hyppyjä paketin viemiseksi perille vastaanottajalle. Eli toisin sanoen mitä suurempi ja tiheämpi joukko on kyseessä fyysisesti, sen paremmin ad hoc -verkko antaa edellytykset tiedonsiirrolle joukon sisäisessä rakenteessa. Verkkotekniikan ja tiedonsiirtotavan täytyy kuitenkin tässä ratkaisus-

sa olla joustava ja muuttua dynaamisesti tilanteen mukaan, hieman samaan tapaan kuin esimerkiksi mobiililaajakaista laitteet kuluttajapuolella nykyään vaihtavat 3G-, EDGE-, UMTS-, GPRS-tekniikoiden välillä kuuluvuuden mukaan.

Lyhyillä etäisyyksillä langattomissa tiedonsiirtomenetelmissä on saavutettu nykyään mm. langattomalla USB-standardilla 480Mbit/s nopeuksia silloin, kun etäisyys on alle kolme metriä (Ilvesmäki ym. 2008, 35). On vaikea kuitenkin nähdä sotilassovellusalueita, joissa alle kolmen metrin etäisyyttä voitaisiin tehokkaasti hyödyntää. Ehkä esimerkiksi yksittäisten taistelijoiden välinen video- ja puheyhteyssiirto voisi olla sellainen sovellusalue, mutta sekin hyvin rajoitetusti. Saarelainen (2007, 177) kertoo puheen ja videon siirtoon esikuntatasolle saakka kykenevää järjestelmää testatun Yhdysvalloissa "Land Warrior" -nimisessä hankkeessa. Emme todennäköisesti tule näkemään "Land Warriorin" kaltaista ratkaisua, joka sotilaalla Suomen puolustusvoimissa kustannuskysymysten takia. Saarelainen toteaakin näiden järjestelmien käyttäjiksi vain ammattisotilaat, eivät varusmiehet tai reserviläiset (Saarelainen 2007, 119).

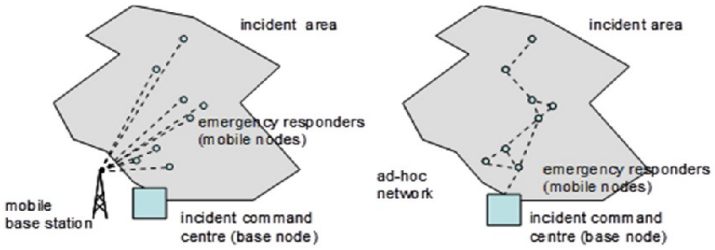
Ilvesmäki ym. (2008, 60) mainitsevat taajuushyppely hajaspektritekniikan olevan soveltuva ad hoc -radioverkkoihin. Tämä edellyttänee kuitenkin sitä, että kaikki järjestelmässä olevat laitteet on synkronoitu toisiinsa nähden, jotta taajuushyppelyn seuraaminen onnistuisi (sen lisäksi, että salausmenetelmä avaimineen on määritelty). Tämä taas johtaa siihen, että ylläpidollisesti esimerkiksi komppanian kokoisella osastolla, jossa kaikilla toimijoilla on päätelaite perustuen em. ad hoc -verkkoon täytyy synkronoida laitteensa keskenään taajuushyppelyn järjestelmävaatimusten mukaisesti.

Yhdysvaltojen määrittelemä JTRS-ohjelmistoradiostandardi ja WNW-aaltomuoto tulee olemaan merkittävin ad hoc -kyvyn luoja tulevaisuudessa sotilasjohtamisjärjestelmien langattomassa tiedonsiirrossa. Se ei kuitenkaan ole ainoa mahdollisuus, sillä myös Ranska on kehittämässä omaa vastaavaa eurooppalaiseksi aaltomuodoksi (Pajuniemi ym. 2008, 226-230). Merkittävintä kuitenkin on kotimaisen järjestelmän kehityksen kannalta juuri ohjelmistoradiotekniikkaan siirtyminen, sillä aaltomuotoa voidaan ko. tekniikalla aina tarpeen mukaan vaihtaa. Erillisiä datalinkkejä ei enää kehitetä järjestelmäkohtaisesti (STAE 2020 osa 2. 2004, 312), vaan kaikkien uusien pakettiradiojärjestelmien ja niissä käytettävien tiedonmuotojen tulee olla uuteen kokonaisuuteen yhteensopivia. Tässä määrittelytyössä toimivat Naton julkaisemat standardit.

Ad hoc -verkkojen edut ja heikkoudet sotilastietoverkoissa

Lähi vuosikymmeninä sotilasjohtamisjärjestelmien tietoverkkoja viedään ad hoc -ratkaisumalleihin. Ad hoc -verkko ei tarvitse rakennettua infrastruktuuria, se konfiguroituu itsenäisesti ja erityisesti verkon solmut pystyvät välittämään toisten solmujen liikennettä. Tämä viimeksi mainittu ominaisuus parantaa huomattavasti verkon taistelunkestävyyttä, häiriönsietokykyä sekä soveltuu nopeasti muodostettaviin organisaatioihin. Ad hoc -verkot ovat huomattava parannus verrattuna keskitettyihin verkkoratkaisuihin sodankäynnin kannalta. (STAE 2020 osa 2. 2004, 311-312, 407.) Pajuniemi ym. (2008, 221) mainitsevat verkkoon kytkeytyvät järjestelmäsolmut, joiden rooli mukautuu käytettävän ohjelmiston mukaisesti. Tämä seikka myös viittaa ad hoc -toteutukseen ja hyödyntämiseen tulevissa sotilasjohtamisjärjestelmissä.

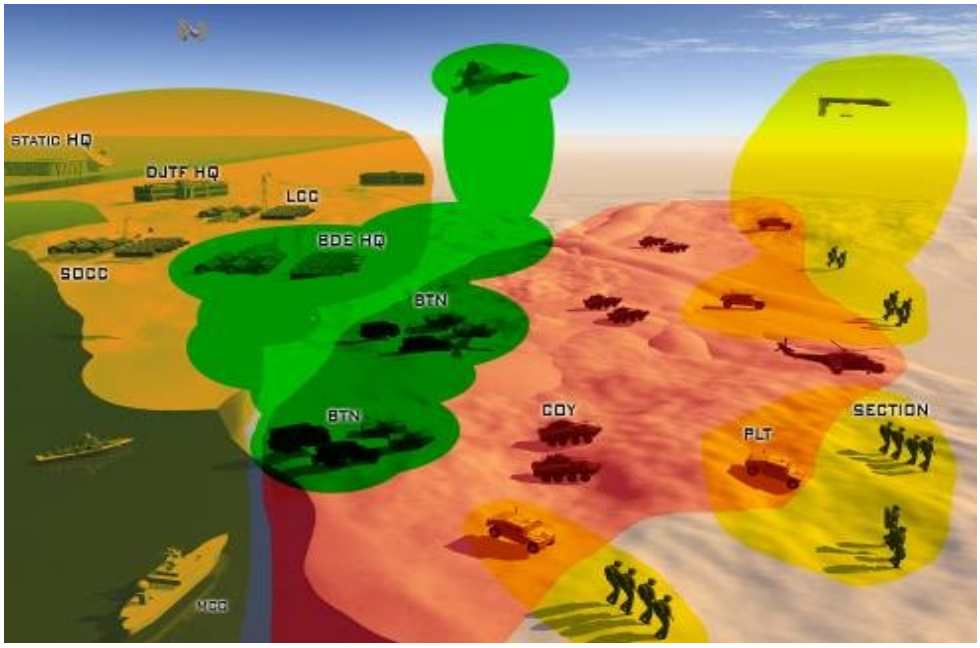
Ad hoc -verkon haittapuolena on pienempi kaistanleveys verrattuna keskitettyihin verkkoratkaisumalleihin. Tämä johtuu ad hoc -verkon rakenteesta, jossa yksi solmu (node) joutuu välittämään toisen solmun tietoa eteenpäin (Kuvio 3). (STAE 2020 osa 1. 2004, 28-31.) Edut ko. tekniikan käyttämiselle ovat kuitenkin huomattavat paremman häirinnänsietokyvyn ja huonomman tiedusteltavuuden myötä. Ad hoc -verkko nykyisten taktisten radioverkkojen mahdollistamalla kaistanleveydellä voisikin soveltua parhaimmillaan paikkatiedon ja muun pientä kaistanleveyttä vaativan numeerisen/tekstitiedon siirtämiseen, ehkä jopa puheen välitykseen rajoitetuissa määrin. Kansainväliseen toimintaan tarvitaan luonnollisesti yhteiset standardit ja mallit tiedonsiirtoon sekä käsittelyyn myös ad hoc -verkoissa.



KUVIO 3. Keskitetty vs. ad hoc -verkko (mukaillen Nato. MP-IST-086-02)

JTRS (Joint Tactical Radio System) -standardi tarjoaa ad hoc -ominaisuudet ohjelmistoradiotekniikalla. WNW (Wideband Networking Waveform) -modulointi tässä radiotekniikassa tarjoaa 2-5Mbit/s tiedonsiirtonopeuden. Erityisen tärkeäksi tulee tämän tekniikan tarjoamat uudet ominaisuudet: verkottunut yhteistoiminta eri puolustushaarojen vä-

lillä, saumaton videon, puheen ja datan siirto, adaptoituminen tiedonsiirtotarpeen mukaan ja verkkomuutosten mukaan, skaalautuva ad hoc -verkko (Kuvio 4). (STAE 2025 osa 2. 2008, 229.)



KUVIO 4. Eri puolustushaarojen verkottuminen keskenään ad hoc -periaatteella (mukaillen Nato. MP-IST-083-15)

4.1.11 Lyhyesti ohjelmistokehityksen vaikutuksista johtamisjärjestelmiin

Puolustusalamme johtamisjärjestelmien ohjelmistoja on kehitetty perinteisesti "vesiputous"-tekniikalla (STAE 2020 osa 2. 2004, 105). Sotilaskäytössä olevat tietokoneohjelmat ovat aikaisemmin tehty usein tilaustyönä ja vain tiettyä tehtävää varten.

Sovelluskehityksessä niin siviili- kuin oletettavasti sotilasympäristössä ollaan ottamassa käyttöön yhä enenevissä määrin modulaarisia olio-ohjelmistoja. Käytännössä tämä tarkoittaa sitä, että jokaista tehtävää varten ei tarvitse suunnitella koko ohjelmaa uudelleen, vaan useista moduuleista kootaan sopiva ohjelmisto kutakin tarvetta varten. Tämä menettely tuo säästöjä ohjelmistokehityksessä. Myös Saarelainen (2007, 114) mainitsee menestyksen edellytykseksi taistelukentällä modulaariset järjestelmät. Edellytyksenä on kuitenkin se, että vähintään rajapinnat ovat tilaajan tiedossa. Näin ohjelmat voidaan saada keskustelemaan keskenään.

SOA (Service Oriented Architecture), missä ohjelmistojen eri toiminnot on suunniteltu toimimaan itsenäisinä palveluina avoimien rajapintojen kautta on tapa, jolla näitä ohjelmistoja tullaan tulevaisuudessa arkkitehtuurin osalta suunnittelemaan. Myös Insta Defsecin teknologiajohtaja Antti Kerola (2010) vahvistaa tämän kuitenkin mainiten, että ohjelmistopaketit yleensä myydään isoina kokonaisuuksina, näin saadaan selkeämmin määriteltyä vastuurajoitukset ja takuuasiat ohjelmistoissa. Myös puolustusvoimien eli asiakkaan edustaja Mika Hyytiäinen (2010b) Puolustusvoimien johtamisjärjestelmäosastosta korostaa SOA:n tuomaa muutosta järjestelmiin. Etuna modulaarisissa ohjelmistoissa on mahdollisuus suorittaa päivityksiä pienemmissä osissa (STAE 2020 osa 2. 2004, 99-100).

Ohjelmistojen luominen pienemmistä osista siis tuottaa kustannussäästöjä ohjelman koko elinkaarta tarkasteltaessa. Samaa perusrunkoa voidaan käyttää pidemmän aikaa ja vain tarvittavia palasia päivittää tilanteen niin vaatiessa. Suomi kehittää iTVJ (integroidun tiedustelun, valvonnan ja johtamisen järjestelmä) -kokonaisuuttaan modulaarisista ohjelmisto-osista (STAE 2020 osa 2. 2004, 102). Ketterän ohjelmistokehityksen (AGILE metodi) keinot mahdollisesti tulevaisuudessa syrjäyttävät vesiputous-tekniikan käyttöä, toisaalta sotilassovellukset tarvitsevat täsmällisemmän testauksen ja virheettömämmän ohjelmakoodin, joten tämä seikka puolustaisi edelleen vesiputousta. Yksi Naton tuottamia yleisohjeita ohjelmistokehitykselle ja hankinnalle on ARMP-9-dokumentti, siinä on lueteltu osa-alueet, mitkä pitää huomioida ohjelmistojen kehittämisessä ja hankinnassa Naton yhteensopiviin järjestelmiin.

4.2 Aselajit

4.2.1 Ilmavoimat

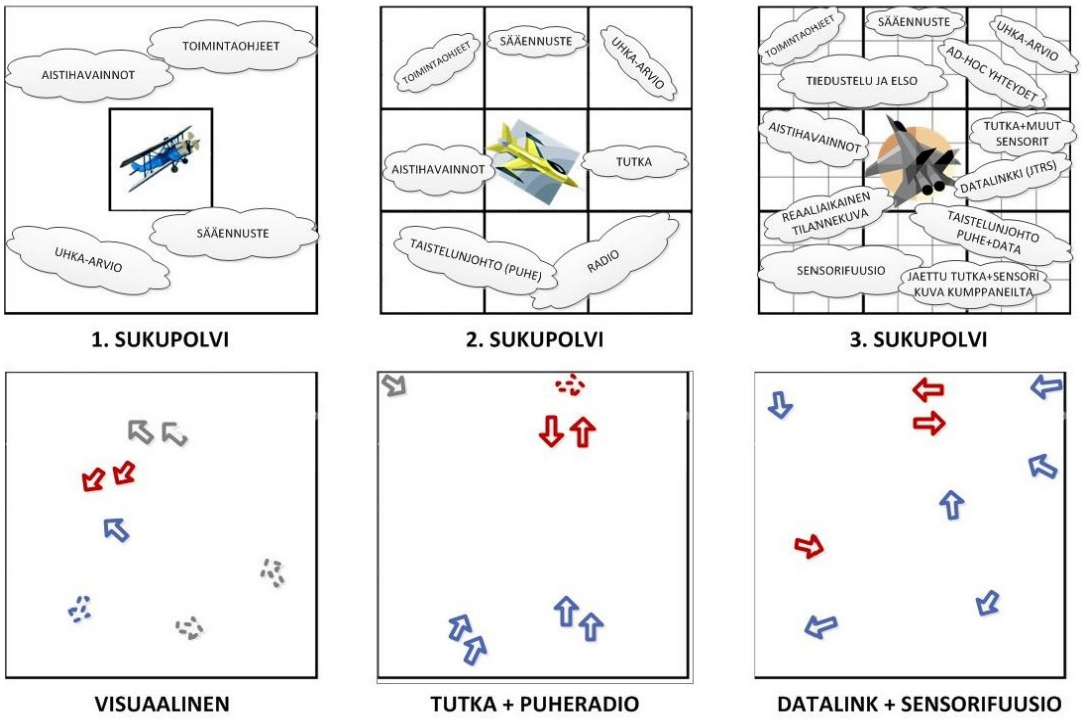
Taistelunjohtotoiminta tulee perustumaan lisääntyvässä määrin taktisen informaation käsittelyyn digitaalisesti johtokeskusten ja ilma-alusten välillä (STAE 2020 osa 2. 2004, 211). Tämä tarkoittaa käytännössä puheella tapahtuvan taistelunjohtamisen merkityksen vähenemistä. Taistelunjohtaja työskentelytavat ja viestintä hävittäjälentäjien kanssa tulee siirtymään puheradiosta entistä enemmän datalinkin kanssa kommunikointiin ja

elektroniseen tiedon esittämistapaan. Siirtyminen pelkkään datalinkkijohtamiseen mahdollistaisi todennäköisesti yhden taistelunjohtajan koneiden käsittelykapasiteetin kasvattamisen useampaan. Käyttöliittymän ja järjestelmän automaation merkitystä ei voi tässä yhteydessä liikaa korostaa. Pajuniemi ym. (2008, 226-228) mainitsevatkin datalinkin kehityksen siirtyvän kansainväliseksi ja kansallista datalinkkijärjestelmästä luovutaan taktisten radioverkkojen yhteensopivuusvaatimusten vuoksi Nato -standardien kanssa.

Tarkasteltaessa taistelulentäjän tilannetietoisuuden kehittymistä taktisen tiedonsiirron kehityksen näkökulmasta havaitaan, että tiedonsiirron kehittyminen vaikuttaa samalla tilannetietoisuuden paranemiseen. Kesseli (2007, 24) mainitsee sodankäynnin vallankumouksen alkaneen informaatioteknologian ja älykkäiden aseiden tulemisen myötä. Myös yhteistoiminta on muuttunut yksilötason suorituksista ryhmätasolle ja viimeisessä sukupolvessa saavutetaan tilannetietoisuus koko taistelukentän sensoreiden tarjoamasta informaatioympäristöstä (Kuvio 5).

Tietojenkäsittelyn kolme sukupolvea taistelulentäjän näkökulmasta:

1. sukupolven versio
   - omien aistien varassa toimiminen, kertaluontoinen ohje esimieheltä sanallisesti/kirjallisesti
2. sukupolven versio
   - omat aistit, radio, tutka ja ir (infra red) -kamera => tilannekuva laajeni ja syveni, puhe ja radio tärkeitä viestintätapoja
3. sukupolven versio "parveilu"
   - verkottunut järjestelmä: omat aistit, radio, oma tutka ja ir, koko valtakunnan ilmatilannekuva, muiden koneiden tutkakuvat, ELSO:n (elektronisen sodankäynnin) toimittama tulkittu kuva muista sensoreista, tieto kulkee salattuna datalinkin kautta radioteitse



KUVIO 5. Tietojenkäsittelyn ja tilannekuvan kehittyminen kolmessa eri sukupolvessa, taistelulentäjän näkökulmasta.

Ns. parveilussa useat tahot iskevät useilta suunnilta samanaikaisesti. Tämän jälkeen joukot hajautuvat iskeäkseen jälleen uudelleen (Hyytiäinen, Lindberg, Mattila & Nenonen 2008, 84-85). Uudet tietoverkot mahdollistavat tämän, sillä toimintojen ja joukkojen täydellinen synkronointi onnistu vain reaaliaikaisella tilannekuvalla ja jatkuvalla tiedonsiirtoyhteydellä taistelukentän toimijoiden kesken. Ei tarvita massiivisia taisteluyksiköitä, vaan yksittäiset toimijat yhdistetään tietoverkolla dynaamiseksi organisaatioksi (Ylitalo 2008, 117-119).

Parveilu edellyttää taistelussa mukana olevilta johtajilta erilaista päätöksentekotapaa ja ymmärrystä oman roolin sekä suuremman kokonaisuuden välillä (Hyytiäinen, Lindberg, Mattila & Nenonen 2008, 85). Tämä tarve perustuu juuri siihen, että tässä 3. sukupolven tietojenkäsittelyn sotilasjohtamisjärjestelmissä päätöksenteko ei enää joka tilanteessa perustu hierarkiseen organisaatioon kuten esimerkiksi linjaorganisaatiossa. Siirtymisvaiheessa vanhasta tähän uuteen malliin tulee todennäköisesti esiintymään muutosvastarintaa ja eturistiriitoja, jotka kuitenkin tulevat ennen pitkään ratkaistua, kun järjestelmän käyttäjät huomaavat edut, jota tämä dynaamisempi johtamisjärjestelmä kykenee antamaan. Myös Kesseli (2007, 25-30) mainitsee, että sotataidollinen puoli ei ole

vielä sopeutunut sotatekniikan tarjoamiin mahdollisuuksiin. Kesseli jatkaa, että epäsymmetriset konfliktit vaativat kykyä vaihdella hajauttamisen ja voimien keskittämisen välillä. Tästä voimme tehdä johtopäätöksen, että tietojärjestelmä, joka kykenee tuottamaan johtamisjärjestelmän parveilumetodia käyttävälle taistelevalle joukolle, kykenee myös vastaamaan epäsymmetrisellä periaatteella toimiviin uhkiin.

Datalinkin kautta voi myös siirtää puhetta ja lähitaistelutilanteessa lentäjän huomio keskittyykin ilma-aluksen ulkopuolisten tapahtumien seurantaan, näin jää vähemmän aikaa maalitilannekuvan seurantaan näyttölaitteelta. Toisaalta tietoa voidaan myös esittää kypäränäytölle suoraan lentäjälle. Puhe on siis tietyissä tilanteissa parempi kuin teksti tai visuaalinen informaatio hävittäjän ohjaamoon datalinkillä lähetettynä. Sama sääntö pätee myös muihin aselajeihin.

Kehitys näyttäisi jatkuvan siten, että itse taistelukoneen fyysinen suorituskyky (nopeus ja liikehtimiskyky) eivät ole enää niin tärkeitä ilmataistelun kannalta vaan häivetekniikka, ilmatilannekuvaa parantavat järjestelmät sekä ilmataisteluohjusten ominaisuudet tulevat olemaan merkityksellisiä menestymisen kannalta. (STAE 2020 osa 1. 2004, 314.) Toisin sanoen, mitä paremmat häiveominaisuudet, sen paremmin torjutaan paljastumista vastapuolen sensoreille ja taas mitä parempi oma sensoriverkko ja tilannekuvan välityskyky on, sen paremmin kyetään paljastamaan vastustajan sijainti ja näin käyttämään omaa asevaikutusta vastustajaan. Yhä kehittyvät häiveominaisuudet ilma-aluksissa tuovat tarpeen lisätä erilaisia sensoreita tähän valvontajärjestelmään perinteisten tutkien ja aistivalvonnan lisäksi. Kehittyneinkään häivetekniikka ei pärjää järjestelmälle, joka kattaa kaikki käytettävissä olevat sensorit ja valvontajärjestelmät. Häivetekniikan- ja valvontatekniikan kilpailu onkin havaintojen tarkkuus ja tämän tarkkuuden tuoma tarkempi resoluutio tilannekuvaan.

Ilma-aluksissa ja miehittämättömissä sotilasilma-aluksissa autonomisuus on kenties vietty kaikkein pisimmälle tähän mennessä verrattuna muihin asehaaroihin. Todennäköisesti itsenäinen toiminta näillä alustoilla tulee lisääntymään tekoälyn (ohjelmiston) kehityksen myötä, näin vähentäen aluksen kontrollin ja tiedonsiirron tarvetta.

STAE 2020 osa 1 (2004, 370) mainitsee autonomisen ilma-alusten itsenäisemmän toiminnan edellyttävän integroitumisen lennonjohdon järjestelmien kanssa. Tämä tarve tu-

lee esiin, jos siviilialusten sallitaan toimia samassa ilmatilassa autonomisten ilma-alusten kanssa. Suomessa on kuluneen 10 vuoden aikana otettu käyttöön eurooppalainen FATMI (Finnish Air Traffic Management Integration) -lennonjohtojärjestelmäliityntä, joka käyttää erityistä ilmaliikenteelle tarkoitettua tietoliikenneverkkoa ja on yhteydessä Eurocontrol-keskukseen Brysseliin. Eurocontrollin verkostosta säädetään koko Euroopan ilmatilankäyttöä siviili-ilmailun sääntöjen ja määräysten mukaisesti. Viitaten em. miehittämättömän ilma-aluksen toiminnan integroimiseen siviili ilma-alusten kanssa, täytyy rajapinnat ja tietoliikenne myös sovittaa tähän järjestelmään (ainakin Euroopassa). Toisaalta asia voidaan kiertää myös niin, että konetta operoivat sotilaat etäkäytöllä ja he huolehtivat tarvittavista toimenpiteistä siviili-ilmailun osalta. Tässä tapauksessa ei kuitenkaan toteudu skenaario miehittämättömien ilma-alusten täysin autonomisesta toiminnasta.

Lentokoneiden välillä voidaan käyttää automaattista TCAS-törmäyksenestojärjestelmää, mutta tämäkin järjestelmä on tarkoitettu varojärjestelmäksi jo tapahtuneita virheitä varten. Tämä ei sinänsä sovellu ainoaksi keinoksi sovittamaan autonomisia sotilaskoneita ja tavallisia ilma-aluksia samaan ilmatilaan. Tavallisten ilma-alusten keskinäinen kommunikaatio tapahtuu usein puheyhteydellä ilmailuradiolla ja se taas ei sovi miehittämättömälle ilma-alukselle kommunikaatiorajapinnaksi siviili-ilmailun kanssa.

4.2.2 Maavoimat

Käytännön esimerkkinä yksittäisen maavoimien taistelijan toiminnan kehittämisessä rajoitetussa voimankäytön tilanteessa, ns. "harmaan vaiheen" aikana, voisi tulevaisuudessa olla reaaliaikainen tulenkäytön ja voimankäytön hallinta. Maavoimien taktisten viestijärjestelmien kehitys kasvattaa digitaalisten kenttäradioiden myötä tiedonsiirron nopeutta (STAE 2020 osa 2. 2004, 218). Tämänkaltainen järjestelmä vähentäisi mahdollisia siviiliuhreja ja oman tulen aiheuttamia tappioita. Järjestelmässä täytyisi kuitenkin olla jonkinlainen "ohitusmoodi", sillä taistelija itse tekee lopullisen tulenavauspäätöksen.

STAE 2020 osa 1 (2004, 130) kuvaa järjestelmää, jossa videokamera, kypärän visiirinäyttö, tähtäinkuva ja aseen piippulinja on kontrolloitu niin, että ase laukeaa vasta kun

em. elementit kohtaavat. Toinen seikka missä, kyettäisiin suojelemaan omia joukkoja, olisi suora ennakkovaroitus uhasta johtamisjärjestelmällä esimerkiksi taistelijan varustukseen integroidulla värinähälyttimellä. Kovassakin metelissä tämänkaltainen hälytin voisi toimia esimerkiksi ilmavaarasta tai suojeluvaroituksesta kertovana indikaattorina, näin komentoketju nopeutuu perinteiseen radioviestintään ja huutoyhteyteen perustavasta menetelmästä. Tämä hälytin voisi olla kytkettynä mobiiliin taistelijan PDA-laitteeseen, johon voisi tulla tarkentava tieto uhasta tai maalin sijainnista.

Yksittäisellä sotilaalla voisi olla esimerkiksi mahdollisuus katsoa ilmatilannekuvaa ja tarkistaa mahdolliset uhkatekijät henkilökohtaiselta tietokoneeltaan (Kuva 1.). Näin jaettu tilannekuva lisäisi jopa yksittäisen taistelijan tilannetietoisuutta, samalla parantaen kollektiivisesti koko joukon suorituskykyä taistelukentällä. Saarelainen (2010b) kertoo divisioona, pataljoona, joukkue ja yksittäinen taistelija tasolla kaiken viestinnän keskittyvän yhteiseen järjestelmään, jossa kaikille jaetaan sama tilannetietoisuus. Ajateltavissa olevia tietoja voisi olla erilaisten ABC-aseiden käytöstä välitettävät varoitukset, tai vihollisen toiminnasta saatuja tiedustelutietoja. Luonteeltaan tämänkaltainen tieto voidaan toteuttaa hierarkisesti broadcast-tyyppisesti ylhäältä alaspäin, mutta varsinainen hyöty saavutetaankin uusilla tietoverkoilla, kun tiedonsiirrosta tehdään kaksisuuntaista.

Kuva 1. Prototyyppejä taistelijan henkilökohtaisesta tietokoneesta, kotimaista tuotantoa. (TTY, Reserviläisten koulutustilaisuus. Tampere. n.d. Valokuva T. Ström).

Tykistöaselajissa ollaan myös viemässä järjestelmiä itsenäiseen ammunnanhallintaan. Järjestelmässä on tietoliikenneyhteys komentopaikalle ja tulenjohtajiin. Kansainväliset tehtävät edellyttävät myös tässä yhteensopivuutta. (STAE 2020 osa 1. 2004, 144.) Yksi

tällainen yhteensovittamiseen liittyvä seikka on puolustusvoimissa viime vuosina tehty uudistus, jossa kansallisen karttakoordinaatiston käytöstä siirryttiin kansainväliseen koordinaatistoon. STAE 2020 osa 1 (2004, 144) mukaan ammunnanhallinnassa haetaan verkottunutta järjestelmää, joka toimii lähes automaattisesti verkon maalitiedon perusteella. Riskinä tämänkaltaisessa verkossa on mahdolliset häiriötilanteet ja riippuvuus tietoliikenneyhteyksistä.

Panssarivaunujen tulevaisuuden vaatimuksiin kuuluu kyky toimia välitysasemana taistelukentän tiedonsiirtoverkossa, kyky toimia perusasemana taistelukentän johtamisjärjestelmässä (STAE 2020 osa 2. 2004, 256). Ajoneuvoihin mukaan lukien panssarivaunut siis tulee tulevaisuudessa lisää tietotekniikkaa ja radiojärjestelmä, joka kykenee keskustelemaan taistelukentän muiden toimijoiden johtamisjärjestelmien kanssa reaaliaikaisen tilannekuvan ja maalitiedon välittämiseksi.

Ajoneuvoissa taktiseen tietoverkkoon liittyminen tulee tapahtumaan ajoneuvon oman taistelunhallintajärjestelmän kautta, järjestelmät tulevat käyttämään reaaliaikaista tiedonsiirtoa (STAE 2020 osa 1. 2004, 276). Soveltuva tiedonsiirtojärjestelmä täytyy luonnollisesti olla langatonta tiedonsiirtoa käyttävä linkki. Nykyisillä tekniikalla mahdollista on esimerkiksi ajoneuvon huoltoon liittyvien tietojen välittäminen, mutta esimerkiksi ajoneuvon etäohjaus vaatinee videokuvansiirron ja huomattavasti suuremman kaistanleveyden tiedonsiirtoon (>1mb/s). Saarelainen (2010b) jakaa langattoman tietoverkon siirtojärjestelmät 3,5,10,100 mailin järjestelmiin sisältäen WLAN/LAN/PTT-radio ja satelliittiviestintäjärjestelmät. Saarelainen (2010b) mainitsee myös suomalaisyrityksen nimeltä "Nethawk", joka kehittää langattoman tiedonsiirron tekniikkaa.

STAE 2020 osa 1 (2004, 380) mukaan ajoneuvoissa tiedonsiirtoa tulee vaatimaan muita asehaaroja monimutkaisempi kulkuympäristö, joka tarvitsee enemmän tietoa ulkopuolelta. Tekoäly on kykenemätön käsittelemään kaikkea eteen tulevia haasteita. Tämä kehitys on kuitenkin edennyt huomattavasti Yhdysvaltojen asevoimien tutkimusorganisaatio DARPA:n ansiosta. DARPA:n järjestämissä kilpailuissa "autonomisen ajoneuvon" luomiseksi ovat ajoneuvot suoriutuneet oman tekoälyn, tehokkaiden lasersensorien ja riittävän maastodatan sekä GPS:n avulla hyvinkin pitkistä ja monimutkaisista maastoreiteistä. Myös kaupungeissa ja liikenteessä on tätä tekniikkaa jo sovellettu niin sotilaskuin siviilikokeissakin. Onkin odotettavissa, että 20 vuoden kuluessa on jo miehittämät-

tömiä maastoajoneuvoja käytössä ainakin sotilaskäytössä. Ajoneuvojen lienee mahdollista tulevaisuudessa toimia myös keskenään ja tässä yhteydessä nousee jälleen tarve nopeasti muodostettaville tietoliikenneyhteyksille näiden ajoneuvojen keskinäiseen tiedonsiirtoon. Tässäkin yhteydessä ad hoc -yhteydenmuodostustapa lienee oikea ratkaisu.

Maavoimissa on taistelukentän taktisen tiedonsiirron alimman tason ajateltu käsittävän ryhmätason radion, joka olisi toteutettu ohjelmistoradiotekniikalla (Lemmetty ym. 2008, 182).

STAE 2020 osa 2 (2004, 265) ennustaa ryhmä- ja taistelijatasolla muodostuvan tulevaisuudessa ohjelmistoradiopohjainen soluverkko joka mahdollistaisi joustavat kokoonpanomuutokset. Tämä tultaisiin todennäköisesti toteuttamaan ad hoc ja multi hop -periaatteiden mukaisesti. Käyttäjät ja verkot erotetaan toisistaan tunnistusmenetelmällä. Tämä voisi olla esimerkiksi digitaalinen allekirjoitus salausjärjestelmän yhteydessä. Hyvin samantapainen menetelmä on jo käytössä olemassa olevassa kenttäradio LV331 -järjestelmässä, jossa salausavain syötetään tietyn käyttäjäryhmän mukaan päätelaitteeseen. Yksittäinen taistelijakin siis kykenee tulevaisuuden johtamisjärjestelmässä saamaan tilannekuvaa kaikilta taistelukentän sensoreilta ja tietoa tuottavilta lähteiltä. Se halutaanko sen toteutuvan käytännössä riippuu paljolti siitä, onko resursseja varustaa jokainen sotilas omalla päätelaitteella. Myös informaation jakamisen prioriteetit ja tasot on ratkaistava ensin. Saarelainen (2007, 128) mainitsee, että yksittäisellä taistelijalla on oltava myös kyky tukeutua hierarkiassa ylempien järjestelmien tietoverkkoihin ja palveluihin.

Yksittäisten sotilaiden ollessa kyseessä täytyisi kuitenkin verkon topologian olla luotu siten, että kaikki käyttäjät ja käyttäjäryhmät voidaan verkon hallinnan kautta erotella toisistaan. Tämä edesauttaa verkonvalvontaa, ylläpitoa ja viestintää ylemmältä hierarkia tasolta alemmalle (esimerkiksi komppanian päällikön käsky tietylle joukkueelle ja ryhmälle). STAE 2020 osa 2 (2004, 265) mainitsee tähän liittyen ryhmätasolla olevan ohjelmistoradion, joka välittää liikennettä taistelukentän verkkoon. Tästä voitaisiin päätellä, että tulevaisuuden johtamisjärjestelmässä pienin lähetys/vastaanotto segmentti verkon topologiassa on siis ryhmätaso.

Yksittäisen taistelijan välineistöön lisääntyvä tietotekniikka tulee muodostamaan henkilökohtaisen verkon (Personal Area Network, PAN) (Hyytiäinen, Lindberg, Mattila & Nenonen 2008, 66). Kytkemällä nämä verkot keskenään saadaan jo ryhmä- ja joukkuekohtaisia yhteenliittymiä.

4.2.3 Merivoimat

Miehittämättömät alukset lisääntyvät myös merivoimaympäristössä tulevaisuudessa. Tämä tuo mukanaan uusia tarpeita ja haasteita tiedonsiirtoon sekä viestintään. Mitä pidempiä aikoja miehittämättömän aluksen täytyy toimia dynaamisesti ilman tietoliikenneyhteyttä johtamisjärjestelmään, sitä enemmän tekoälyn täytyy vastata autonomisen aluksen toiminnasta sekä navigoinnista. Tästä voidaan päätellä, että mitä enemmän panostetaan toimivaan tietoliikenneyhteyteen joka tilanteessa, saadaan vastaavasti autonomisen aluksen, kulkuneuvon, lentolaitteen yksikköhintaa alemmaksi, kun tekoälyyn tarvittavaa infrastruktuuria ei tarvita per yksikkö niin paljon. Toisaalta STAE 2020 osa 1 (2004, 392) mainitsee sensorien oman älykkyyden kasvattamisen tarpeen tietoliikenteen määrän tarpeen vähentämiseksi. Tämä taas aiheuttaa sen, että yksikön hinta nousee kun halutaan älykkäämpiä, tietoa jo paikanpäällä käsitteleviä sensoreita. Kenties jonkinlainen "kultainen keskitie" on tässä yhteydessä paikallaan.

Käytännön esimerkkinä STAE 2020 osa 1 (2004, 394) näistä haasteista tekoälyn ja sensorien suhteen mainitsee mm. sääolosuhteiden aiheuttamat vaikeudet tunnistamiselle sekä navigoinnin onnistumisen erilaisten virtaus- ja tuuliolosuhteiden vaikutuksen alaisena. Vedenalaisissa järjestelmissä keskeinen ongelma on jatkuvan tiedonsiirtoyhteyden ylläpitäminen. Näin ollen tiedonsiirrontarvetta pyritään vähentämään järjestelmien omaa älykkyyttä ja autonomisen toiminnan edellytyksiä kasvattamalla (Laine, Kaurila, Appelqvist & Kylä-Lassila 2008, 402-403). Tämä taas tarkoittaa vedenalaisten yksiköiden kustannusten kasvua verrattuna muissa ympäristössä toimiviin. Tekoäly ja tiedon prosessointi alemmalla tasolla johtaa siis kustannusten nousuun niin sensoreissa kuin yksiköissäkin.

4.3 Huolto- ja tukitoiminnot

Taistelutehtäviin liittyvän tiedonsiirron lisäksi sotilasoperaatioiden suorittamisen kannalta elintärkeää on erilaisen logistiikkaan ja huoltoon liittyvän tiedon välittäminen. Esimerkiksi ajoneuvojen toimintakyvyn ylläpitoon liittyvä tiedonsiirto on myös siviilimaailmassa siirtymässä valmistajan tietokantaan tukeutuviin huoltojärjestelmiin. Tämä pätee myös moniin muihin ajoneuvoihin ja järjestelmiin jatkossa.

Perinteisiä huolto- ja korjaamokäsikirjoja ei kannata enää tuottaa painettuina versioina. Keskeistä tässä on seikka, jossa asiantuntemus siirtyy suoraan valmistajan tehtaalta tietoliikenneyhteyden kautta kentälle, kaikki väliportaat jäävät välistä pois. (STAE 2020 osa 1. 2004, 209.) Tätä näkemystä vasten peilataan esimerkiksi hävittäjäkalustomme ylläpitojärjestelmää, joka nykyisin vielä pitkälti pohjautunee paperisiin manuaaleihin, joiden sivuja päivittämällä tietyn syklin mukaisesti ylläpidetään ajan tasalla olevaa huoltokäsikirjastoa. Tämä käsikirjasto muuttuu sähköiseksi etäkirjastoksi, joka päivittyy valmistajan tehtaan tietokannasta. Kaikki keskeiset päivitykset ja kriittiset asiat tulevat nopeasti, lähes reaaliajassa toimijoiden käyttöön kaikissa niissä maissa, joissa kyseinen hävittäjäkalusto on käytössä. Tämä tulee vaatimaan kuitenkin tiedonsiirtoprosessin suunnittelemista siten, että kansalliset olosuhteet ja määräykset otetaan huomioon uudenmuotoisesta tiedonsiirrossa.

Kokonaan tiedon ylläpidollisista tehtävistä ei päästä, mutta ne tehostuvat ja suoraviivaistuvat huomattavasti. Logistiikassa taas reaaliaikaisella tiedonsiirrolla ja paikkatietojärjestelmillä kyetään saavuttamaan materiaalin toimituksen reaaliaikeinen tilannekuva (Lemmetty ym. 2008, 141-142). Käytännössä logistiikka tehostuu tulevaisuudessa huomattavasti tavaran toimittajien kyetessä jatkuvasti seuraamaan materiaalin kulkua kohteeseensa. Myös reittejä voidaan optimoida kustannusten ja ajan säästämiseksi. Vaurio-tietojen kirjaamiseen ja tallentamiseen on odotettavissa yhteisen tietoverkon käytön lisääntyminen. Tämä seikka korostunee sodan ajan toiminnassa, jossa välttämättä ei ole aina varaosia saatavilla määrällisesti ja ajallisesti riittävästi, silloin voidaan esimerkiksi kahdesta eri tavalla vaurioituneesta hävittäjästä koota yksi toimintakykyinen.

5 SUOMEN PUOLUSTUSVOIMAT JA KANSAINVÄLINEN KEHITYS

5.1 Tietojenkäsittelyn kehittymisen vaikutus seuraavan 10-20 vuoden aikana

Kansainvälistyminen ja eri aselajien välinen tietojärjestelmien integraatio edellyttää yhtenäisiä tietoliikennerajapintoja (STAE 2020 osa 1. 2004, 165). Tämä määrittelytyö tulee olemaan pitkäkestoinen ja runsaasti resursseja kuluttava tehtävä, sillä Puolustusvoimien käytössä on lukuisia järjestelmiä ja eri laitevalmistajien tuotteita.

Todennäköisesti kustannustehokkain tapa on luoda laitekohtaiset tietoliikenne adapterit/viestimuuntimet ja siirtää ip-tekniikalla tietoa verkossa eteenpäin. Ip-tekniikalla mahdollistetaan myös verkon taktinen hajauttaminen ja taistelunkestävyys. Ip-tekniikka luotiin aikoinaan juuri ydinsodan uhkaa varten varmistetuksi tietoliikenneverkoksi. Sama sääntö pätee myös pienemmässä mittakaavassa. Käytettävän tekniikan avoimuus rajapintojen osalta on oleellista, näin eri valmistajien tekniikat voidaan saada keskustelemaan keskenään. Tiedonsiirto tulee kuitenkin asettamaan rajoitteensa, mitä voidaan siirtää ja missä ympäristössä. Tähän vaikuttavat käytettävän siirtokerroksen kapasiteetti ja tiedon suojausvaatimusten asettamat rajat (STAE 2020 osa 1. 2004, 165).

Langatonta hajaspektriä tiedon salauksessa hyödyntävä tekniikka soveltuu numeerisen tilannetiedon viemiseen eteenpäin ip-pohjaisena, mutta reaaliaikaisen videokuvan siirtoon joudutaan hakemaan kenties lähempänä COTS-tekniikoita olevia toteutuksia useassakin ympäristössä. Kaistanleveyden, tietoliikenteen salauksen ja tiedusteltavuuden väliltä täytyy siis löytää kompromissi.

Tietojenkäsittelyn kapasiteetti tulee siis kasvamaan. Aineistoa kyetään esittämään tarvitsijoille entistä visuaalisemmin ja nopeammin sisäistettävässä muodossa (STAE 2020 osa 1. 2004, 538). Tämä onkin edellytyksenä, sillä kasvava informaation määrä edellyttää aikaisempaa pidemmälle vietyä esitystapaa pelkän tekstipohjaisen tai numeerisen tiedon sijasta. Käytännössä tämä tarkoittaa esimerkiksi sitä, että esimerkiksi ilmavoimien taistelunjohtaja näkee tulevissa johtamistyökaluissaan enemmän visuaalisia elementtejä numeeristen arvojen sijaan. Esimerkiksi korkeustieto maalilla voidaan esittää värikoodeilla tai symboleilla numeerisen arvon sijaan. Hävittäjälentäjälle tarvittava informaatio (matalalla, keskikorkeudella, korkealla) käsittely taistelunjohtajalla tapahtuu

huomattavasti nopeammin graafisen esitysmuodon avulla kuin siten, että ensin lukee numeroarvon ja sen jälkeen tekee päätöksen mille korkeusalueelle maali tuon numeroarvon mukaan kuuluu. Juuri tämänkaltaisilla pienillä parannuksilla käytettävyyteen ja ymmärrettävyyteen, saavutetaan aikaetuja taktisissa tilanteissa, joissa sekunnit ratkaisevat.

Tietokannat ja tietokantatekniikan kehittyminen tulevat olemaan keskeisessä asemassa tulevaisuuden sotilasjohtamisjärjestelmissä. Erityisesti multimediatiedon taltioimiseen erikoistuneet tietokannat tulevat olemaan tarpeellinen. Näin lisääntynyttä sensori ja visuaalista dataa voidaan käsitellä sekä taltioida taistelukentältä. (STAE 2020 osa 1. 2004, 533); NATO AdatP-34(C).) Se mikä tässä tulee uudistumaan vanhaan tekniikkaan verrattuna on tiedon hakeminen kannasta käyttäjän tarpeen mukaisesti. Nykyiset järjestelmät perustuvat pitkälti tietyn esitysmuodon esittämiseen kaikille tarvitsijoille ja lähitulevaisuuden tuotos lienee juuri tämän yhtenäisen esitystavan yhdistäminen eri asehaarojen kesken.

Seuraava kehitysvaihe tulee olemaan yhteiset tietokannat, joista saadaan tarvitsijoiden tarpeiden mukaista dataa esitykseen. Loppukäyttäjätaho määrittelee itse parametrin, jonka mukaan hän saa dataa tilannekuvaansa kulloiseenkin tilanteeseen liittyen tarkoituksenmukaisimmalla tavalla. Tämänkaltaisella tekniikalla saavutetaan myös se etu, että vältytään välittämästä sellaista informaatiota organisaatiossa alaspäin, jota loppukäyttäjä ei tilanteeseensa sidottuna tarvitse. Näin ehkäistään loppukäyttäjän ylikuormittamista turhalla informaatiolla. Myös Warden (2010) toteaa, että tärkeämpää on saada tekijälle tieto siitä mitä pitää tehdä kuin, että kaikki saavat tietää mitä tapahtuu. Vain suunnitelman kannalta olennainen tieto tarvitaan sitä työstettäessä (Warden 2010).

Kun tarkastellaan johtamisjärjestelmien jakautumista eri osa-alueisiin ja niiden mukaisia valvontajärjestelmiä, voidaan havaita tarve suurille tietokannoille ja raakadatan käsittelykapasiteetille. Haasteena järjestelmillä on olennaisen tiedon löytäminen, analysointi, toimittaminen oikeassa muodossa, oikealle taholle ja oikea-aikaisesti (STAE 2020 osa 2. 2004, 57). Suurenevan tietomassan käsittelyyn ja johtamisprosessien tehostamiseen on luotu monia erilaisia työkaluja sekä kehitysprojekteja. STAE 2020 osa 2 (2004, 62) luettelee muutamia esimerkkejä:

- Puoliautomaattinen kuvaprosessointi (Semi-automated Imagery Processing, SAIP)
- Taistelukentän tilannetietoisuus ja tiedon jakaminen (Battlefield Awareness and Data Dissemination, BADD)
- Jaettu yhteinen maajärjestelmä (Distributed Common Ground System, DCGS)
- Automaattinen syvien operaatioiden koordinaatiojärjestelmä (Automated Deep Operations Coordination System, ADOCS)
- Yhteistoiminnan mahdollistava tietoympäristö (Collaborative Information Environment, CIE)
- Operatiivinen verkottunut arviointi (Operational Net Assessment, ONA)
- JakoPiste portaalipalvelin (SharePoint Portal Server, SPPS)
- Tietotyötila (Information Work Space, IWS)
- Yhteinen operatiivinen tilannekuva (Common Operational Picture, COP)

Käytännössä kansainvälistä kehitystyötä ja standardeja luo Nato, ainakin kun asiaa tarkastellaan Suomen ja sen kansainvälisen sotilasyhteistyön kannalta. Nato Network Enabled Capability (NNEC) tutkimusohjelman tavoitteena on verkottaa Naton ja sen jäsenmaiden strategisen, operatiivisen ja taktisen tason tiedustelu- ja valvontajärjestelmät keskenään (STAE 2020 osa 2. 2004. 62; NATO AdatP-34(C)).

5.2 Tiedonkäsittelyn vaatimukset taistelukentällä ja tulevaisuus

Sotilasoperaatioissa päätöksenteon perustana olevan tiedon tulee välittyä päättäville tahoille mahdollisimman nopeasti ja reaaliaikaisesti. Tähän tavoitteeseen ei monikansallisissa operaatioissa päästä, ellei käytössä ole yhtenäinen arkkitehtuuri, yhteensopivat tietomallit ja yhtenevät tietoliikenneratkaisut. Tästä syystä Suomi ja muut länsimaat pyrkivät standardisoimaan järjestelmiään paremman yhteensopivuuden aikaansaamiseksi (STAE 2020 osa 1. 2004, 170, 315). Nämä standardit ovat käytännössä Naton määrittelemiä ja julkaisemia. Suomi kehittää ja testaa näitä asioita mm. kansainvälisissä rauhanturvaoperaatioissa ja yhteispohjoismaisessa NBG-taisteluosastossa.

Yhteensopivat tietomallit merkitsevät käytännössä erilaisten tietojen esittämistä järjestelmien välillä samassa formaatissa, esimerkiksi GPS-paikkatiedon tulee olla samalla ta-

valla esitettynä mahdollisten virheiden välttämiseksi. Pieni virhe etäisyydessä voi merkitä taistelukentällä omien tai siviilien joutumista vaaralle alttiiksi. WGS84 -koordinaatisto on hyvä esimerkki ilmailussa yleisesti käytetystä standardista paikkatiedon osalta. Toisaalta standardeja voidaan käsitellä myös lähemmin teknisenä määrittelynä esimerkiksi SQL-tietokantojen ja niistä input/output-tietojen välittämisenä toisen tahon vastaaviin järjestelmiin. Mitä yhteneväisemmät kannat ovat, sitä vähemmän tarvitaan erilaisia ohjelmistoratkaisuja muuttamaan tietoa formaatista toiseen näiden tietokantojen välillä. Tästä syntyy kustannussäästöjä, virheiden määrä pienentyy ja vikasietoisuus kasvaa järjestelmissä. Kun järjestelmät ovat kytketty yhteiseen tietoverkkoon, päätöksenteko ja toimeenpano tehostuvat parantuneen informaatiohallinnan kautta (Pajuniemi ym. 2008, 217-218).

IPSec VPN -yhteyksien käyttämisellä voidaan parantaa verkkoyhteyksien turvallisuutta julkisessa internetissä (STAE 2020 osa 1. 2004, 16). Sotilasjohtamisympäristössä on keskeinen tarve mobiiliin tiedonsiirtoon ja nopea yhteyksien muodostamistarve erilaisissa kokoonpanoissa (niin kotimaisesti kuin kansainvälisestikin). Tämä osoittaa langattomien verkkojen tarpeen korostuvan. Tähän muodostamiseen tarvitaan mm. sotilasradioverkkoja, jotka kykenevät toteuttamaan em. "all ip" -tietoliikenneympäristöä.

Tavoitetilanne tulevaisuuden sotilasjohtamisjärjestelmien tietoliikennejärjestelyissä on, että järjestelmät kättelevät joustavammin ja mukautuvat tiedonsiirrossaan tarvittavan johtamisjärjestelmän kokonaisuuden mukaan. (STAE 2020 osa 1. 2004, 16) Puolustusvoimien johtamisjärjestelmäkeskus ylläpitää ja kehittää olemassa olevia ja lähitulevaisuudessa käyttöön otettavia tietojärjestelmiä kansallisesti (Määttä 2010).

6 POHDINTA JA JOHTOPÄÄTÖKSET

6.1 Kansainvälinen kehitys ja muutokset sotilasjohtamisjärjestelmissä

Sotilasjohtamisjärjestelmät tulevat muuttumaan tietotekniikan, tietojenkäsittelyn ja tiedonsiirron kehityksen mukana. Yleisenä trendinä näyttäisi olevan keskitetyt tietokannat ja hajautettu tietoliikenne. Keskitettyjä tietokantoja hyödyntämällä voidaan tukeutua samaan potentiaaliin useampaa eri sovellusta varten.

Yhä lisääntyvä langaton tiedonsiirto sotilasjoukoissa tuo myös haasteen taajuuksien ruuhkautumisesta (Hyytiäinen, Lindberg, Mattila & Nenonen 2008, 67). Näin ollen suunnittelu ja koordinaatio langattoman tiedonsiirron taajuuksien hallinnasta korostuu. Tähän luontevinta olisikin oma työkalunsa, jossa eri osapuolien käyttämien järjestelmien taajuuksien hallinta voidaan toteuttaa keskitetysti, taktiseen tilanteeseen sopivimmalla tavalla. Toistaiseksi ei vielä ole käytössä sotilaskäytön kriteerit täyttävää tekniikkaa, joka tarjoaisi riittävän laajan tiedonsiirtokaistan langattomasti koko taistelukentällä siten, että saavutetaan reaaliaikainen tilannekuva kaikille osapuolille jokaisesta sensorista. Muutosta kuitenkin tiedonsiirtokykyyn on luvassa tulevien erittäin laajaa kaistanleveyttä (Ultra Wideband, UWB) käyttävien tiedonsiirtomenetelmien myötä. Tähän tiedonsiirron kykyyn vaikuttaa se, miten tulevia langattomia yhteystapoja (ohjelmistoradio) halutaan käytettävän otettaessa huomioon siirtokapasiteetin, häirinnänsietokyvyn ja havaittavuuden asettamat vaatimukset.

Naton standardit tulevat olemaan jatkossakin merkittävin yksittäinen johtamisjärjestelmien tietojenkäsittelyä ohjaava elementti. Standardit tulevat jatkossakin määrittelemään entistä tarkemmin ja syvemmälle arkkitehtuuriin kuuluvia asioita. Keskeisimpinä motivaattoreina Nato-mailla ja -kumppaneilla tulee olemaan tässä yhteensopivuus muiden maiden järjestelmien kanssa. Yhtenäinen tietoturvallisuus pyritään saavuttamaan kaikkien osapuolten kesken, vain siten voidaan saavuttaa riittävä luottamuksen taso kansainvälisiin operaatioihin osallistujien kesken.

Ohjelmistokehityksen osuudesta sotilasjohtamisjärjestelmissä mielenkiintoinen suuntaus on avoimien ohjelmistojen sekä ohjelmisto-osien käyttäminen. Avoimen koodin etu on sen läpinäkyvyys loppukäyttäjälle. Sama läpinäkyvyys kuitenkin mahdollistaa informaatiosodankäynnin "ohjelmistopommien" teon, joita vasta tositilanteessa näihin avoimen ohjelmakoodien ratkaisuihin käytettäisiin. Näissä uusissa aseissa algoritmit, haittakoodit ja erilaiset parametrit ovat "uusia ammuksia". Ei tosin ole sanottu etteikö suljetun koodin ohjelmistoja vastaan voisi hyökätä samalla tavalla. Stuxnet-haittaohjelman tapaus osoittaa sen, että kaupallinen, avoimien rajapintojen järjestelmä voi joutua ohjelmistohyökkäyksen kohteeksi. Eroa tuskin varsinaisesti tämän suhteen on kaupallisten ja vapaiden ohjelmistojen kesken, kysymys on enemmänkin kuinka usein ja paljon ohjelmistoja testataan sekä miten löydetyt haavoittuvuudet paikataan.

Sotilaskäyttöön tarkoitettujen ohjelmistojen koodin maastavientiä on usein rajoitettu kansallisesti. Usein toiseen maahan myytävä asejärjestelmä ei sisällä niin täydellistä ohjelmistoa kuin mitä ko. järjestelmä kansallisessa käytössä sisältää. STAE 2020 osa 2 (2004, 185) mainitsee mm. Hornet-hävittäjän tämänkaltaisena järjestelmänä, joka ei todennäköisesti ole ohjelmistoltaan yhtä suorituskykyinen Suomeen tuotuna versiona kuin mitä Yhdysvaltojen oman järjestelmän ohjelmisto on. Samaa näkemystä tukee myös Michelsen (2010) mainitsemalla, että sotatekniikka muuttuu uhkaksi itselle, jos sitä myy ulospäin.

Verkkokeskeisen sodankäynnin asettamat vaatimukset laitealustoille edellyttävät verkkovalmiutta (Network Ready Platforms). Uudet järjestelmät tulee siis suunnitella siten, että niitä voidaan hyödyntää taistelukentän taktisessa tietoverkossa (Pajuniemi ym. 2008, 217).

Pajuniemi ym. (2008, 228) mainitsevat tulevaisuuden taktisen tiedon siirtämisen vaatimuksena olevan reaaliaikaisen tiedonsiirron. Myös Saarelainen (2007, 121) mainitsee tämän vaatimuksen olevan keskeinen ja haastava. Tämä tuo myös ohjelmistoille vaateen käsitellä ja esittää tietoa reaaliajassa. Järjestelmiä ja ohjelmistoja suunniteltaessa tulee myös ottaa huomioon yhteensopivuus kansainvälisten standardien mukaan kaikilla OSI-tasoilla (fyysinen rajapinta, tiedonsiirtoprotokolla, sanomarakenne, esitystapa ja C4IS -sovellusohjelmistot) (Pajunen ym. 2008, 228; Nato AdatP-34(C) 2009).

Tiedon saanti taistelukentälle säilyy kuitenkin haastavana edelleen tulevaisuudessa, sotilasoperaatioissa yleensä tiedon tarve on suurin silloin kun ollaan lähimpänä vihollisvaikutusta ja liikutaan nopeasti. Vihollisvaikutus, etäisyydet ja liikkeen nopeus asettavat vaatimuksia luotettavalle tiedonsiirrolle langattomasti. Tähän haasteeseen voidaan vastata mm. tehokkaalla salauksella, hajaspektritekniikalla ja ohjelmistoradioverkoilla. Ohjelmistoradiotekniikan erityinen etu on sen alaspäin yhteensopivuus vanhojen järjestelmien kanssa. Tämä helpottaa tekniikan käyttöönottoa portaittain.

Kautta aikojen sodankäynnissä on kehitetty uusia järjestelmiä ja innovaatioita ylivoiman saavuttamiseksi vastustajasta. Aina kuitenkin on uudelle keksinnölle keksitty vastatoimi. Niin tulee varmasti myös käymään verkostosodankäynnin osalta, toisaalta kun katsomme meneillään olevia konflikteja mm. Lähi-idässä ja Afganistanissa niin voidaan asettaa kyseenalaiseksi, onko ylivoimaa saavutettu lainkaan uusimmalla ja hienoimmalla tietojenkäsittelyn menetelmillä? Kun vastustaja ei hyödynnä sähkömagneettista spektriä omassa toiminnassaan ja piiloutuu siviilien sekaan tehden vastarintaa epäsymmetrisesti mm. itsemurhapommittajia hyväksi käyttäen tulemme tilanteeseen, jossa paraskaan johtamisjärjestelmä tai taktinen tiedonsiirto ei kykene voittamaan taistelua näillä pelisäännöillä.

Mitä enemmän järjestelmiin lisätään tekoälyä, sen enemmän tarvitaan muuttujia näiden järjestelmien päätöksentekoalgoritmien tueksi ja se tekee taas näistä järjestelmistä entistä kalliimpia ja monimutkaisempia. Puheyhteys on edelleen tehokkain tapa johtaa, tämä yhteys saadaan useampien tahojen välille ja esimerkiksi "broadcast"-tyyppisenä isommalle joukolle kerralla. Puheviestintä vie myös vähiten taistelijanhuomiota tehtävän suorituksen aikana.

COTS (Commercial Off The Shelf) -ratkaisujen lisääntyvä käyttö uusissa järjestelmissä avaa markkinoita myös yrityksille, jotka eivät välttämättä ole erikoistuneet juuri puolustusalaan. Näiden järjestelmien päälle on rakennettava tietoturvallinen verkkoratkaisu sekä keinot, joilla vastatoimien sietokykyä ja tietoturvaa testataan jatkuvasti harjoituksissa.

Kuten John A Warden (2010) kehäteoriassaan toteaa, tietoliikenne ja johtamisjärjestelmät ovat ensi-iskun kohteita sodankäynnissä. Suomen kansallisen puolustuksen kannalta infrastruktuurin pitäisikin olla suunniteltu siten, että sitä on vaikea tuhota, käytännössä tietoliikennerakenteen tulisi siis olla topologialtaan mahdollisimman moninkertainen rakenteeltaan Mesh-periaatteen mukaisesti.

Miehittämättömien järjestelmien keskeisin rooli lähitulevaisuudessa tulee säilymään tiedustelu- ja valvontatehtävissä (Laine, Kaurila, Appelqvist & Kylä-Lassila 2008, 407). Itsenäiseen taistelutoimintaan kykenevien järjestelmien kehittäminen on erittäin kallista. Yksiköiden kustannukset ovat huomattavat verrattuna perinteisiin ihmisen ohjaamiin vastaaviin. Näin ollen huomataan, että tekniikan ja ohjelmistokehityksen pitää vielä edetä vuosia, ennen kuin tullaan saavuttamaan kustannuksissa sellainen raja, jossa miehittämättömät vielä tulevat saavuttamaan miehitetyn. Laskentatapa, jolla kustannuksia arvioidaan järjestelmissä vaikuttaa myös lopputulokseen tässä yhteydessä. Esimerkiksi miehittämättömän ilma-aluksen kustannusta miehitettyyn verrattaessa on myös otettava huomioon lentäjän koulutus, henkilöstön tarve ja ylläpito, sekä ilma-aluksen tarvitsemat järjestelmät pilotille ja näiden asettamat rajoitukset koneelle teknisesti sekä toimintakyvyllisesti.

On myös poliittisesti helpompaa laittaa "robotti asialle" vaarallisessa ja riskialttiissa tehtävässä verrattuna ihmishenkeen. Lähitulvaisuuden järjestelmät tulevat vaatimaan jatkuvaa tiedonsiirtoyhteyttä, jotta reaaliaikaiseen jatkuvaan tilannekuvaan taistelukentällä päästäisiin, niin miehittämättömissä kuin miehitetyissä yksiköissä.

Perinteisesti siviilimaailmassa tietoturva-asioita käsitellään tiedon luottamuksellisuuden, eheyden ja käytettävyyden turvaamisen kannalta. Sotilasverkkoympäristössä asioita ajatellaan myös hyökkäyksen kannalta: vaikuttaminen, häiritseminen, korruptoiminen ja tietojärjestelmien kaappaus (Veijalainen ym. 2008, 550-551). Siviilimaailmassa hyökkäävät ohjelmistot ja toimenpiteet lasketaan rikolliseksi ja hakkereiden puuhaksi, mutta sotilasympäristössä yhdeksi aseeksi/aselajiksi.

Kuitenkin pitää muistaa se seikka, jonka John A Warden (2010) hyvin osuvasti on todennut, että pelkällä informaatioteknologialla ei sotia voiteta, vaan jonkun on tehtävä myös ns. "likainen työ".

6.2 Suomen Puolustusvoimat kehityksessä mukana

Tulevana kahtena vuosikymmenenä odotettavissa on suuria muutoksia toimintakulttuuriin ja johtamistapoihin tietoteknisten järjestelmien tuomien uusien mahdollisuuksien vuoksi. Kesseli (2007, 28) korostaa samaa todetessaan, että verkostokeskeisen konseptin käyttöönotto vaatii myös sotilaallisen kulttuurin muutoksen.

Tietotekniikan roolin voimistuva asema näissä järjestelmissä tekee siitä myös haavoittuvaisemman tietoverkkosodankäynnin tuomille uhkille. Hyytäinen (2010a) mainitsee Suomen it-riippuvaisena maana olevan erittäin haavoittuvainen EBO (Effect Based Operations) lähestymistavalle. On kuitenkin yleisesti todettava, että emme voi jäädä kehityksestä, pysähtyä tietotekniikassa johonkin tiettyyn vaiheeseen uusiaksemme sen taas 10-20 vuoden kuluttua. Meidän on pysyttävä jatkuvassa tietojenkäsittelyn kehityksessä mukana. Tietoylivoima (information superiority) on samanlainen elementti sodankäynnissä kuin esimerkiksi ilmaherruus tai aseellinen ylivoima vastustajaa vastaan tämän päivän sodankäynnissä.

Tekninen kehitys vie sotilasjohtamisjärjestelmiä ja niiden taktisia tiedonsiirtomenetelmiä piirikytkentäisistä verkoista pakettikytkentäisiin. Käytännössä tämä mahdollistaa helpomman integraation eri järjestelmien saattamiseksi keskustelemaan keskenään. Ip-pohjainen tiedonsiirto on yhteensopiva ratkaisu niin sotilas- kuin siviilijärjestelmien (COTS) kesken. Kuitenkin tulee muistaa, että pakettikytkentäinen tiedonsiirto on luonteeltaan hyvin erilaista kuin vanhojen järjestelmien tiedonsiirto. Erilaiset kuormitushuiput, tietoliikennehäiriöt ja kaistavaatimukset tuovat tiedonsiirtoon toisenlaisia ilmiöitä kuin aikaisemmin on totuttu kohtaamaan.

TCP/IP-protokollan käyttäminen kuljetus- ja verkkokerroksena lienee helpointa, etenkin kun halutaan yhdistää COTS-tuotteita tulevaisuudessa sotilaskäyttöön lisääntyvissä määrin. Tämä protokolla ei itsessään kykene vastaamaan sellaisesta tietoturvasta, jota sotilasjärjestelmät edellyttävät. TCP/IP-paketit toimivat sinänsä luotettavana tapana siirtää tietoa muuttuvissakin verkkorakenteissa, mutta salaus ja tietoturvan taso tullaan saavuttamaan siirtokerroksen (data link layer) ja fyysisen kerroksen (physical layer) tietoturvaratkaisujen avulla sotilasjohtamisjärjestelmissä, esimerkkinä hajaspektritekniikka pakettiradioverkoissa. IPv4 standardi TCP/IP-tekniikassa alkaa vanhentumaan ja sen ti-

lalle on tulossa hyvin nopealla aikataululla Ipv6, jonka on yleisesti mainittu olevan myös parempi mobiilissa tiedonsiirrossa. IPv4:n osoiteavaruus on pian ehtymässä, näin ollen Ipv6 on seuraava standardi tulevaisuuden internetjärjestelmissä. Ongelmana tulee kuitenkin muutosvaiheessa olemaan, että vanhat Ipv4-järjestelmät eivät ole ylöspäin yhteensopivia Ipv6-ratkaisuiden kanssa. Tarvitaan siis ohjelmisto- ja laitepäivityksiä vanhoissa järjestelmissä takaamaan Ipv6-yhteensopivuus.

Myös ohjelmisto- ja palvelupuolella löytyy uusia COTS-tuotealueita, jotka ovat herättäneet kiinnostusta sotilasjohtamisjärjestelmien kehittäjissä, näistä mm. Professori Anders Törnen (2010) mainitsemat web-pohjaiset palvelut, kuten Ruotsin Wikipedia muunnos sotilaskäyttöön "KUPAL FOI" ja Yhdysvaltojen tiedusteluyhteisön "Intellipedia". Ehkä samanlaisia sovelluksia on käytettävissä myös Suomella tulevaisuudessa.

Tiedonsiirron siirtyessä internet-verkkoon sotilasjohtamisjärjestelmissä tullaan kohtaamaan myös internetin rakenteen muodostamia tietoturvauhkia. Internetin rakennehan perustuu läpinäkyvyyteen ja tiedon neutraliteettiin (Ilvesmäki ym. 2008, 15-16). Tämä ei ole täysin sopivaa sotilasnäkökulmasta. Nykyiset tietoverkkojärjestelmät perustuvat monilta osin suljettuihin verkkoihin tai sitten pidetään rinnalla julkiseen verkkoon kytkettyä tietoverkkoa ja operatiivista suljettua verkkoa (niin ohjelmallisesti kuin fyysisestikin). Suljetun verkon heikkoutena on vain sen kytkeytymättömyys dynaamisesti muiden toimijoiden kanssa esimerkiksi kansainvälisesti.

Tietoverkot, ohjelmistot ja muu ICT tulevat myös muokkaamaan asehaaroja siten, että syntyy informaatioaselaji. Koska sotilaskäytössä olevia tietoverkkoja ollaan integroimassa yhdeksi kokonaisuudeksi, on myös tällä perusteella oletettavaa, että tämä aselaji tulee olemaan yhteinen eikä erillisiä maa-, meri- ja ilmavoimien informaatiojoukkoja tarvita.

Pajuniemi ym. (2008, 217-219) mainitsevat ongelmakohtia sensorifuusion ja uusien johtamisjärjestelmien kehityksessä. Nämä ongelmat ovat lisääntynyt informaation tulva, epävarman tiedon suodattaminen ja haavoittuvuus väärälle tiedolle. Juuri em. syistä johtuen tulevaisuuden järjestelmät tarvitsevat sekä teknisesti että koulutuksellisesti päteviä osaajia, jotka suodattavat sekä käsittelevät tietoa ennen kuin sitä viedään järjestelmässä

korkeammalle hierarkiatasolle. Tarvitsemme siis informaatioajan tai informaatioaselajin sotilaita.

Tekoälyllä eli ohjelmistojen toimintoja sekä päätöksenteon algoritmeja kehittämällä toki voidaan vaikuttaa tähän tarpeeseen, mutta 10-20 vuoden kehityksen aikana ei kuitenkaan ihmistä kyetä korvaamaan tietojenkäsittelijänä. Järjestelmiä voidaan kyllä kehittää tuottamaan tieto helpommin sisäistettävässä muodossa, mutta tiedon suodattamiseen tarvitaan yhä ihminen. Etenkin tämä tulee esiin tilanteissa, joissa vastapuoli tarkoituksella yritettää harhauttaa tai estää järjestelmän toimintaa. Ihminen kykenee havaitsemaan tämänkaltaisen toiminnan paremmin kuin yksikään tekoälyohjelma vielä lähitulevaisuudessa.

Uudet johtamisjärjestelmät luovat paremmat edellytykset tiedonkäytölle johtamisessa ja päätöksenteossa. Tiedonkäsittelyssä jo siviilimaailmastakin tutut tavat suorittaa "tietolouhintaa" tehokkaiden hakumoottorien avulla mahdollistaa myös sotilasmaailmassa tehokkaamman tavan analysoida tiedustelutietoa yhä lisääntyvästä tiedon määrästä. Lisääntyvät sensorit ja kehittyneempi sensoritekniikka tuottaa tietoa, joka taltioidaan massiivisiin tietokantoihin. Tieto taltioidaan kansainvälisten standardien mukaisesti näihin tietokantoihin ja se myös lajitellaan tietoturvan mukaisesti siten, että vain sallitut käyttäjätasot voivat käyttää heille osoitettua tietolähdettä. Luottamuksellinen tieto tulee siis edelleenkin erottaa selkeästi ei-luottamuksellisesta.

Verkottuminen ja verkkokeskeinen johtamisjärjestelmien suunnittelu tulee mahdollistamaan entistä ketterämmät organisaatiot, joita muodostetaan tilanteen vaatimusten mukaisesti. Nykyiset kankeat linjaorganisaatiot saavat osittain väistyä uusien johtamisjärjestelmien tullessa käyttöön. Päätöksentekijät, asiantuntijat ja toimijat muodostuvat nopeammin, ketterämmin ja tapahtumasidonnaisesti operaatioon liittyen. Uudenmuotoisella organisaatiolla toteutetaan kuitenkin edelleen komentajan taisteluajatusta, vastuunjako organisaatiossa jakautuu vain tulevaisuudessa eri tavoin. Organisaatiot muuttuvat matalammiksi ja samalla johtaminen sekä viestintä liikkuu enemmän horisontaalisesti toimijoiden kesken.

Verkot tulevat olemaan järjestelmien ja käyttäjien kesken nopeasti muodostettavia ad hoc -verkkoja, joiden tiedonsiirto tapahtuu multi hop -verkon periaatteella, kunkin sil-

mukan toimiessa verkon tukiasemana. Ipv6:en siirtyminen edesauttaa ad hoc -rakenteen toteuttamista ja hyödyntämistä sen paremman mobiiliuden ja helpomman dynaamisen konfiguroitavuuden ansiosta. Nämä järjestelmät pystyvät tuottamaan käyttäjälleen informaatiota sen mukaan, miten kaistanleveyttä ja yhteyden vakautta on tilanteeseen sitoen mahdollista tarjota. Ad hoc ja joustava langaton tekniikka, kuten ohjelmistoradiot, ovat vähemmän vihollisen toiminnan vaikutukselle alttiita, kuin kiinteästi rakennetut langalliset ja langattomat verkot.

Tulevaisuudessa tietosodankäynnissä tullaan varmasti vaikuttamaan vastustajan kykyyn saada tilannekuvaa näissä verkoissa, uusi tekniikka luo siis vastustajalle myös uusia vaikuttamisen mahdollisuuksia. Toimijat ja tukiorganisaatiot eivät tulevaisuuden organisaatioissa toimi lähellä toisiaan, vaan verkottumisen avulla luovat virtuaaliorganisaatioita, joilla vastataan operaation tavoitteisiin parhaimmalla mahdollisella tavalla. Myös kansallinen puolustuksemme ja sisäinen turvallisuus edellyttää entistä tiiviimpää viranomaisten välistä yhteistyötä ja näin ollen näiden kumppanien tietoverkkojen sujuvaa keskustelua keskenään.

Myös itse johtamisjärjestelmän ja tietoverkkojen tilasta on käyttäjien saatava tietoisuus, jotta ei "sokaistuttaisi" todellisen tilanteen ja tietoverkon luoman tilannekuvan välillä. Erilaiset verkonvalvontajärjestelmät ovat mm. tähän valvontaan sopivaa tekniikkaa. Tilannekuvan kannalta ei myöskään riitä pelkkä sensorifuusio ja reaaliaikaisuus, kuva pitää myös jatkojalostaa ns. "tunnistetuksi kuvaksi". Tämän tunnistetun kuvan luomiseksi tarvitaan vielä 10-20 vuoden aikana varmastikin ihmistä operaattoriksi.

Teknisessä sodankäynnissä vastustaja on aina oppinut virheistään ja kehittänyt joko vastajärjestelmän tai toimintatavan, jolla tämä tekniikka on sitten menettänyt taisteluarvoaan. Tämä seikka asettakin kyseenalaiseksi sen, kannattaako kuitenkaan uhrata valtavia resursseja sellaisen järjestelmän luomiseksi, jonka toimivuudesta emme voikaan olla varmoja tosipaikan tullen? Tulisiko puolustustamme saattaa eteenpäin niiden esimerkkien mukaan, jotka näemme maailmalla luoneen menestystä uusimmissa konflikteissa ja onko tämä menestys informaatioylivoiman vai sissisodankäynnin menestystä? Verkostokeskeinen sodankäyntimalli on hyvin teknologiapainotteinen ja se onkin saanut osakseen kritiikkiä mm. sotataidon merkityksen vähättelystä lopputuloksen kannalta.

Uudet järjestelmät, lisääntyvä tietojenkäsittelyn tekniikka ja kokonaan uusi informaatioaselaji tuo myös uudenlaisia henkilöstötarpeita puolustusvoimille. Järjestelmien ylläpito, käyttö ja operointi tulee vaatimaan teknillisesti koulutettuja upseereita organisaation tueksi. Näin taataan kaikissa olosuhteissa riittävä osaaminen ja tulkintakyky uusien johtamisjärjestelmien tuottamassa informaatiokentässä. Myös uusi tekniikka luo tarpeen tietoverkkosodankäynnin joukoille, jotka kykenevät vastaamaan taistelukentän uudella alueella tapahtuviin toimiin joko puolustuksellisin tai hyökkäyksellisin metodein. Tässä yhteydessä on hyvä myös todeta, että järjestelmien toiminta tiedon esittämiseksi tulee saattaa sille tasolle, että henkilöstön määrää ei tarvitse organisaatiossa lisätä, vaan olemassa oleva henkilöstö selviytyy paremmin nykyisistä tehtävistään.

Langattoman tiedonsiirron merkitys näyttäisi kasvavan entisestään, toisaalta tämä seikka saattaa meidät sähkömagneettisen spektrin alueella tehtävien sotatoimien osalta entistä haavoittuvaisemmaksi. Jos esimerkiksi langattoman tiedonsiirron salaus onnistuttaisiin murtamaan, olisi sen seuraukset kohtalokkaat koko johtamisjärjestelmälle. Optiset ja kaapeloidut tiedonsiirtoväylät tulevat siis näin ollen olemaan edelleen tärkeä varmistuskeino. Tämä on kuitenkin sidoksissa siihen, olemmeko luomassa järjestelmää ammattiarmeijaa vai suurempaa reserviä varten. Pienempikokoinen liikkuva ammattiarmeija on erikoistunut lyhytkestoiseen ja nopeaan sotaan, tarpeenaan mobiili ja tehokas langaton johtamisverkko. Suurempikokoinen reserviarmeija, joka on suunniteltu alueelliseen puolustamiseen ja kulutustaisteluun tarvitsee toisenlaista, varmennettua ja kiinteämpää tietoliikenneverkkoa. Tästä näemme yhteyden puolustuspoliittisten päätösten ja puolustustekniikan kehitystyön välillä, vaikuttaen 10-20 vuotta eteenpäin puolustusteknisiin ratkaisuihimme.

Langattoman tiedonsiirron tekniikka tulee jatkossakin kehittymään nopeudeltaan ja kapasiteetiltaan siten, että reaaliaikainen kaikenkattava tilannekuva saadaan kaikille taistelukentän toimijoille. Siviilitekniikassa esimerkiksi VSF-OFDM (Variable Spreading Factor OFDM) on jo kenttätesteissä mahdollistanut 100Mbit/s 120km/h nopeudella liikkuvalle kohteelle ja 2.5Gbit/s 20km/h liikkuvalle kohteelle (Ilvesmäki ym. 2008, 28). Nämä liikkumisnopeudet ja tiedonsiirtokyvyt riittävät hyvin toteuttamaan uudenlaisia johtamisjärjestelmiä erilaisine ääni, video ja laajennettutodellisuus -sovelluksineen.

Siviilitekniikka on vain modifioitava sotilasjärjestelmien asettamien lisävaateiden mukaisesti (mm. salaus-, häirinnänsieto-, luotettavuus-, tiedusteltavuus). STAE 2025 osa 1 (2008, 385) mainitsee ilma-alusten hyödyntämisen tukiasemina taistelukentän taktisessa tiedonsiirrossa. Ilmasta käsin tapahtuva tiedonsiirron releointi voisi parantaa sellaisen taajuusalueen hyödyntämistä, jota muuten pitkien etäisyyksien tai suoran näköyhteyden vaateen (esimerkiksi mikroaallot) takia ei voi hyödyntää. Teknisenä kaupallisena ratkaisuna voisi olla miehittämättömän lentokoneen toimiminen datalinkkinä mobiili-WiMAX verkolle (Laine, Kaurila, Appelqvist & Kylä-Lassila 2008, 387). Jarmo Mölsä (2010) mainitsee TETRA WIMAX -verkkojen tiedonsiirtokyvyn olevan tällä hetkellä useista megabiteistä kymmeniin megabitteihin siviili- ja turvallisuuspuolella. Nykyiset WIMAX-järjestelmät eivät kuitenkaan tarjoa riittävän hyviä yhteyksiä liikkeessä oleville alustoille (Mölsä. 2010). Em. kaltaisia WIMAX-ratkaisuja valmistaa mm. Alvarion niin puhe- kuin datasiirtoon (BreezeACCESS ja BreezeNET), maahantuojana Daimler Finland Oy.

Suomessa on tällä hetkellä kaksi eri näkemystä siitä mihin puolustustamme kehitetään. Toinen näistä on alueellisen puolustuksen ja varusmiespalveluksen kautta koulutettavan reservin käyttö säilyttäen sotilaallinen liittoutumattomuus. Toinen näkemys on Suomen siirtyminen sotilasliitto Naton täysjäseneksi. Näyttäisi siltä, että johtamisjärjestelmiämme ja tietoliikenneyhteyksiä näihin järjestelmiin liittyen on kehitetty jälkimmäisen vaihtoehdon mukaan.

Kotimaisen puolustusteollisuuden mahdollisuudet tuottaa Nato-järjestelmiä ovat kuitenkin osittain rajoitetut, kunnes Suomi on täysimääräinen Naton jäsen. Langattoman tiedonsiirtton kehityksessä hyödynnetään avointa arkkitehtuuria mutta esimerkiksi salaukseen liittyvät tekniset määrittelyt ovat suljettuja Naton ulkopuolisilta tahoilta. Kehitystyön tiedonsiirtotekniikassa ja ohjelmistoissa on hyvä olla läpinäkyvää sekä avoimien standardien mukaista. Tämä ei kuitenkaan tarkoita sitä, että kaiken pitäisi olla "koko maailmalle" julkista. Ohjelmistoradiotekniikan osalta tämä ei välttämättä ole niin suuri este, sillä kyseessähän on vain "ohjelmistojen päivitys" tarpeen ja tilanteen mukaan.

Kaupallisen tekniikan kehityssykli on tällä hetkellä huomattavasti nopeampaa, kuin mitä sotilastekniikassa yleisesti. Kansainvälinen yhteistyö onkin näin ollen tärkeää, jotta saavutetaan pitkäjänteistä yhteensopivuutta kaikkien osapuolten kesken.

Sotilasjohtamisjärjestelmät ovat tulevaisuudessa joko suoraan tai epäsuorasti kytköksissä kansainväliseen internet-verkkoon. Tietoturvan osalta tämä muodostaa riskin niin tietovuodoista ulospäin omasta verkosta, kuin oman verkon altistuminen ulkopuolisille tietoturvauhkille. Tiedon tehokkaat salausmenetelmät (esimerkiksi AES, IpSec ym.) ja virtuaaliset yksityisverkot (VPN) ovat COTS-ratkaisuja, joita voidaan myös sotilaskäytössä hyödyntää.

Tieto tulee myös luokitella omien käyttäjien kesken ja sallia pääsy vain roolien sekä tarpeen mukaan. Tähän tiedonluokitteluun STAE 2020 osa 2 (2004, 108) mainitsee mm. kehystiedon asettamisen tiedolle, josta löytyy käyttäjä-, tuottaja- ja julkaisija-elementit. Käytännössä tämä tullaan asettamaan itse tietokannan määrittelyillä ja rajapintaohjelmistoilla, jotka sallivat/estävät pääsyn tietokantaan. Tietoturvaratkaisut sotilasjohtamisjärjestelmissä ovat korostetun tärkeitä myös rauhan aikana, sillä verkkoon murtautumalla ja mahdollisesti ohjelmistoihin käsiksi pääsemällä kyetään saamaan kuvaus järjestelmän toiminnasta, suorituskyvystä sekä harhauttamis- ja häirintämahdollisuuksista (Ahvenainen 2008, 12-13).

Esimerkiksi netistä jokaisen helposti ladattavissa oleva ohjelma LOIC on tarkoitettu palvelunestohyökkäystä varten. Tätä ohjelmaa onkin käytetty monien "nettiaktivistien" toimesta liittyen WikiLeaks-vuotoihin ja ko. organisaatiota vastustaneiden tahojen nettipalvelujen häirintään. Kyseessä on siis amatööripohjalta tehty ohjelma, jota joukko halukkaita käyttää häiritsemään tietoliikennettä. Tulevaisuudessa onkin nähtävissä, että tietoterkkosodankäynti tulee myös toimimaan sotilasorganisaatioissa ammattimaisesti tehdyillä, tehokkailla tiedustelu- ja häirintäohjelmistoilla.

STAE 2020 osa 1:ssä (2004, 550) ennustettiin varsin osuvasti menetelmä, joka vastasi hyvin hiljattain julkisuuteen tullutta Stuxnet -haittaohjelmatapausta. Mediassa on spekuloitu viime aikoina Stuxnet-madon olleen Israelin tietoverkkosodankäynnin operaatio Iranin ydinvoimaloiden uraanirikastinlaitteita (sentrifugeja) vastaan. Niin kuin STAE 2020 ennusti, Stuxnettia ei alkuvaiheessa havaittu ja se ehti levitä hyvin laajalle maail-

malla. Stuxnet-mato käytti ns. "nollapäivä aukkoja" Windows-käyttöjärjestelmissä. Tämä tarkoittaa siis tietoturva-aukkoa järjestelmässä, johon ei ole ollut olemassa korjausta lainkaan ennen kuin se havaitaan. Tavoitteena oli siis juuri tunkeutua kriittisiin järjestelmiin huomaamatta.

Stuxnet-haittaohjelma toimi ainoastaan tietynlaisen teollisuuden logiikkaohjaimen kanssa ja tietyin arvoin. Julkisuudessa onkin esitetty väitteitä, että tämä haittaohjelma oli suunniteltu muuttamaan Iranin ydinkoelaitoksen sentrifugien kierrosnopeuksia huomaamattomasti siten, että uraanin rikastamisprosessi asekelpoiseksi olisi saanut hidastunut. Se tulkitaanko tämänkaltainen operaatio sodankäynniksi vai joksikin muuksi, on vielä epäselvä, koska ennakkotapauksia ei ole enempää.

Yhteiskuntamme muuttuessa entistä riippuvaisemmaksi tietoverkoista herääkin kysymys, onko tietoliikenneverkot samankaltainen ympäristö, jota tulisi puolustaa rauhanaikanakin samoin kuin ilmatilaa, aluevesi- ja maarajaa? Tarvitsemmeko "internetrajavalvonnan" kansallisesti?

Sotilastekniikassa yhtenäisten standardien noudattaminen ja tietojärjestelmien samankaltaistamisen puolesta puhuu se seikka, että tuolloin kokonaisuutta on helpompi ymmärtää. Asiantuntijuutta löytyy myös helpommin silloin, kun järjestelmät ovat samankaltaiset Nato-maissa. Toisaalta tätä seikkaa vastaan on se tosiasia, että kaikkien samoja ohjelmistoja ja laitteita käyttävien maiden järjestelmät ovat myös samoista kohtaa haavoittuvia, esimerkiksi ns. "nollapäiväaukkojen" kohdalla. Myös John A Warden (2010) korostaa, että ICT-infran tulee kestää ja toipua vihollisen yrityksistä lamaannuttaa se, näin tietoverkkohyökkäysten sietokyvyn tullee olla keskeinen suunnittelukriteeri sotilasjohtamisjärjestelmissä.

LÄHTEET

Ahvenainen, S. 2008. Tekniika sodankäynnin osana. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 2 Puolustusjärjestelmien kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 9-46.

Halonen, V. 2008. Tiedustelu- ja valvontajärjestelmät. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 2 Puolustusjärjestelmien kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 47-58.

Hyppönen, M. Studia Generalia luentosarjat. 2010. Helsingin Avoin Yliopisto. Tietoturva ja tietosota luento. Viitattu 7.11.2010. http://www.helsinki.fi/videot/

Hyytiäinen, M. Insinöörieverstiluutnantti. Puolustusvoimat. 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Hyytiäinen, M. Insinöörieverstiluutnantti. Puolustusvoimat. Sähköpostihaastattelu 29.6.2010. Haastattelija Ström, T.

Hyytiäinen, M., Lindberg, J. & Mattila, J. V. 2008. Johtamisjärjestelmät. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 2 Puolustusjärjestelmien kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 59-86.

Ilvesmäki, M., Jäntti, R., Latvakoski, J., Luoma, M., Peuhkuri, M., Rantanen, H. & Määttä R. 2008. Tiedonsiirtoteknologiat. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 1 Teknologian kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 12-69.

Inkinen, E., Kantsila, A., Korhonen, R., Luoma, P., Marttinen, J., Närhi, I., Poikonen, A., Raerinne, P., Serkola, A. & Terho, L. 2008. Sensoriteknologiat. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 1 Teknologian kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 70-108.

Jantunen S. 2010. Lingvistinen uhka-analyysi kyberdiskurssista. Maanpuolustuskorkeakoulu Johtamisen ja sotilaspedagogiikan laitos. Julkaisusarja 1: Tutkimuksia Nro 4/2010. MPKK

Kerola, A. Teknologiajohtaja. Haastattelu 31.8.2010. Haastattelija Ström, T. Ei litteroitu. Insta Oy, Pirkkala

Kesseli, P. Vaikutuskeskeistä parveilua verkostossa. Teoksessa Salminen, P., Tammikivi, J., Jäppinen, I., Halonen, K., Toiskallio, J., Sivonen, P., Turtola, M. & Jaskari, T. (toim.) Tiede ja ase nro: 65. 2007. Suomen Sotatieteellinen seura, Helsinki: Waasa Graphics, 24-44.

Kihlman, H., Heikkilä, I., Hurme, T., Hintikka, M., Iivonen, V., Kekkonen, E., Kovero, A., Lankinen, M., Lehtinen, J., Leväsmaa, P., Pynnönen, A., Rantanen, J., Rajala, L., Toivonen, A. & Tuominen, A. 2008. Konventionaalinen aseteknologia. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 1 Teknologian kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 142-180.

Kosola, J. & Jokinen, J. 2008. Elektronisen sodankäynnin kehitys 2010-luvulla. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 2 Puolustusjärjestelmien kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 87-108.

Kylkirauta lehti nro 2/2010, 20-23. Pohjoismainen puolustusyhteistyö NORDEFCO. Evl Manu Tuominen, Pääesikunnan suunnitteluosasto. Kadettikunta

Laine, A., Kaurila, T., Appelqvist, P. & Kylä-Lassila, J. 2008. Miehittämättömät järjestelmät. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 1 Teknologian kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 366-407.

Lemmetty, I., Forselius, T., Sihvonen, A., Holma, P., Juusela, J., Klemola, O., Haapasalo, M., Honkela, M., Laaksonen, A., Tauru, M. & Valta, A. 2008. Ilmapuolustusjärjestelmä. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 2 Puolustusjärjestelmien kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 132-195.

Michelsen, Karl-Erik. LUT. 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Mälkki, J. Vaikutusperusteisen operatiivisen ajattelun (EBAO) sotataidolliset lähtökohdat. Teoksessa Turunen, I. (päätoim.) Tiede ja ase nro: 67. 2009. Suomen Sotatieteellinen seura, Helsinki: Multiprint Oy, 7-31.

Määttä, R. PVTT. Sähköpostihaastattelu 22.2.2010. Haastattelija Ström, T.

Mölsä, J. Tohtori. 2010 Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

NATO. 1998-2008. NATO Interoperability Standards and Profiles. [online] [viitattu 23.1.2011]. http://nhqc3s.nato.int/architecture/_docs/NISPv3/volume4/ch02.htm

NATO. 2009. CCC NATO Open Systems Working Group. Allied Data Publication 34. (ADatP-34(C)) Volume 4. NATO Interoperability Standards and Profiles Date: 9 February 2009

NATO. MP-IST-083-15

NATO. MP-IST-086-02
Pajuniemi, R., Paukkeri, I., Kangas, M., Suhonen, J., Laitinen, T., Renko, K., Passoja,

K., Männistö, E., Nousiainen, J., Tilvis, H., Välikangas, A., Majamaa, T., Sorsakivi M. & Kiviluoma, J. 2008. Ilmapuolustusjärjestelmä. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 2 Puolustusjärjestelmien kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 208-266.

Palojärvi, P. OTM. 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Puolustusvoimat. Pääesikunta. Operatiivinen Osasto. Informaatio-operaatioiden Doktriini.

Quincy Wright. "A Study of War". University of Chicago Press. 1942, 1965, 1983.

Saarelainen, T. Majuri. Puolustusvoimat. Sähköpostihaastattelu 28.6.2010. Haastattelija Ström, T.

Saarelainen, T. Majuri. Puolustusvoimat. 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Saarelainen, T. Majuri. ”Tulevaisuuden jalkaväkitaistelijan kehitystyö Suomessa – katse oman maan puolustamisessa ja tulevaisuuden kriisinhallintaoperaatiossa”. Teoksessa Salminen, P., Tammikivi, J., Jäppinen, I., Halonen, K., Toiskallio, J., Sivonen, P., Turtola, M. & Jaskari, T. (toim.) Tiede ja ase nro: 65. 2007. Suomen Sotatieteellinen seura, Helsinki: Waasa Graphics, 111-130.

Sigholm, Johan. Majuri. Swedish Defence Forces. 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Takamaa, Kari & Palojärvi, Pia. 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Törne, Anders. Professori. Totalförsvarets forkningstitut (FOI). 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Valtonen, Vesa. Majuri. 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Valtonen, V. Näkökulmia viranomaisyhteistyöstä. Teoksessa Salminen, P., Tammikivi, J., Jäppinen, I., Halonen, K., Toiskallio, J., Sivonen, P., Turtola, M. & Jaskari, T. (toim.) Tiede ja ase nro: 65. 2007. Suomen Sotatieteellinen seura, Helsinki: Waasa Graphics, 45-54.

Veijalainen, J., Hoinkaranta, A., Hämäläinen, N., Kaijanaho, A., Kiviharju, M., Kurhinen, J., Kärkkäinen, K., Mazhelis, O., Pekkola, S. & Penttilä, J. 2008. Tietojenkäsittelyn kehittyminen ja tietoturvallisuus. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 1 Teknologian kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 529-564.

Warden, John A. Colonel (ret). 2010. Luento. Sotatieteiden päivät 25.-26.5.2010. MPKK. Santahamina

Ylitalo, T. 2008. Informaatiosodankäynnin järjestelmät. Teoksessa Kari, M., Hakala, A., Pääkkönen, E. & Pitkänen, M. (toim.) Sotatekninen arvio ja ennuste 2025, STAE 2025, osa 2 Puolustusjärjestelmien kehitys. Puolustusvoimien Teknillinen Tukimuslaitos, Helsinki: Edita Prima Oy, 109-131.

SANASTO

Ad hoc -verkko

Ad hoc -menetelmää kutsutaan myös yhteistyöreititykseksi (collaborative routing). IEEE802.11 standardissa on myös määritelty ad hoc -moodi. (Ilvesmäki ym. 2008, 26.) Sotilasnäkökulmasta tämän järjestelmän etuna on se, ettei erillistä tukiasemaa tarvita, vaan kaikki verkon toimijat muodostavat verkon rungon yhdessä. Taistelunkestävyys ja häiriönsietokyky ovat parempia kuin perinteisillä langattoman verkon tukiasemalähetin/vastaanotin ratkaisuilla.

Ammunnanhallinta

Ammunnanhallinnalla käsitetään ampuvan joukon tai yhtymän tulenkäyttö, tätä tulenkäyttöä pyritään optimoimaan ammunnanhallinnan järjestelmillä. Ammunnanhallinta on kytköksissä viestijärjestelmineen johtamisjärjestelmiin ja on keskeinen osa joukkojen taktista hyödyntämistä taistelukentällä. (Kihlman ym. 2008, 176.)

Blue force tracking

Blue force tracker on Nato-termistöä ja tarkoittaa järjestelmää, joka mahdollistaa omien joukkojen tilanteen sekä paikkatiedon reaaliaikaisen ja automaattisen seurannan (Hyytiäinen, Lindberg, Mattila & Nenonen 2008, 63).

Datalinkki

Datalinkki nimitystä käytetään sotilastekniikassa kun tarkoitetaan tiedonsiirtolaitetta jolla sähköinen informaatio viedään eteenpäin sotilasjohtamisjärjestelmissä. Datalinkki siirtää mm. kaikkien sensorien tietoa, maalitilannekuvaa ja maaliin ohjausinformaatiota (Pajuniemi ym. 2008, 227).

Häivetekniikka

Erilaiset tekniset keinot ja menetelmät joilla pyritään vähentämään kohteen havaituksi tulemista.

Mesh-periaate

Mesh-periaatteen mukaisella verkkoliikenteellä joka verkon solmukohta vastaanottaa ja välittää tietoa keskenään. Jokainen solmu toimii välittäjänä sen lisäksi että lähettää omaa dataa. Jokaisen solmun täytyy siis tehdä yhteistyötä verkossa reitityksen aikaansaamiseksi.

Multi hop -verkko

Multi hop -verkko käyttää verkon omia soluja tiedon välittämiseen (STAE 2020 osa 1. 2004, 43). Tämänkaltainen rakenne sopii hyvin liikkuviin yksiköihin, joiden määrä vaihtelee.

Ohjelmistoradio

Ohjelmistoradio on tekniikka jossa radion käyttämät taajuudet ja modulaatiot ohjataan ohjelmistopohjaisesti. Ohjelmistoradio kykenee siis mukautumaan olosuhteiden ja laitevaatimusten mukaisesti eri arvoille tilanteen ja tarpeen mukaan.

OODA-loop

OODA-loop on keskeinen käsite sodankäynnin johtamisjärjestelmissä. OODA-termi tulee sanoista "Observe, Orient, Decide, Act", eli kyseessä siis sotilasjohtamisen toistuva prosessi (tiedon keräys – prosessointi – analysointi – tiedon jakaminen) (Halonen 2008, 55). Uudet tietoverkot ja tietojenkäsittelymenetelmät sotilasjohtamisjärjestelmissä pyrkivät siis parantamaan laadullisesti, nopeuttamaan ja tehostamaan tätä prosessia.

OODA-loop pyrkii päätöksentekoprosessissa vastustajaa nopeampaan sykliin (Mälkki 2009, 20).

Paikkatieto

Paikkatieto on sotilasjohtamisjärjestelmissä keskeinen elementti. Paikkatieto voi sisältää sijaintitiedon lisäksi myös ominaisuustietoja, näin myös yleensä on. Erilaiset nopeus-, toiminto-, kartta-, olosuhde- ja henkilötiedot voivat sisältyä paikkatietoon. Jotta sotilasjohtamisjärjestelmät voitaisiin sovittaa keskenään yhteensopivaksi, edellyttää se yhteisen paikkatiedonesitysformaatin luomista jokaiselle johtamisjärjestelmän tasolle. (STAE 2020 osa 1. 2004, 538.)

Sensori

Sensorilla tässä työssä käsitetään kaikki ne laitteet ja järjestelmät, joka tuottavat tietoa ympäristöstään tilannekuvan muodostamista varten sotilastietoverkkoon. Sensori voi myös olla ihminen joka välittää tiedon esimerkiksi tiettyä päätelaitetta käyttäen eteenpäin tässä tietoverkossa.

Sensori- ja datafuusio

Sensorifuusiolla tarkoitetaan useamman eri sensorin tiedon yhdistämistä yhdeksi ilmaisimeksi, siviilitekniikassa esimerkiksi rikosilmoittimissa on saatavilla liiketunnistimia jotka toimivat sekä ir-alueella ja mikroaaltoalueella. Sotilastekniikassa vastaavanlaisia sensorifuusion menetelmiä käytetään luomaan parempia ja älykkäämpiä sensoreita. Uudet sensorit siis kykenevät antamaan tietoa monimutkaisia taustoja vasten (STAE 2020 osa 1. 2004, 83).

Datafuusiolla käsitetään tiettyyn alueeseen liittyvien havaintojen koostaminen yhdeksi kuvaksi. Tässä yhteydessä käytetään eri tietolähteitä joista tilannekuvajärjestelmällä kootaan yksi ehyt tilannekuva. Datafuusio parantaa erilaisten valvontajärjestelmien

herkkyyttä, tarkkuutta, luotettavuutta, kattavuutta ja häiriönsietoa (Inkinen ym. 2008, 103). Esimerkki sotilassovelluksesta tänä päivänä datafuusiosta on ilmavoimien MST (Multi Sensor Tracking) -järjestelmä, jossa useamman eri sensorityypin tuottamaa dataa yhdistetään yhdeksi tilannekuvaksi. Edeltäjä tällä järjestelmällä oli ns. MRT (Multi Radar Tracking) jossa yhdensensorityypin (tutka) datat yhdistettiin useammasta saman lajin sensorista yhdeksi tilannekuvaksi.

Tietoylivoima (Information Supermacy)

Tietoylivoimalla tarkoittaa tilannetta, jossa omien joukkojen tiedonsiirto ja tiedonkäsittelykyky on ylivertainen vastustajaan nähden. Tämä voidaan saavuttaa perinteisten ja modernien sodankäynnin menetelmien avulla. Tietoylivoiman syntyy tiedon hallinnasta, prosessoinnista, visualisoinnista ja jakamisesta (STAE 2020 osa 2. 2004, 93).

Tilannekuva

Tilannekuva ja sen muodostuminen koostuu tietoverkon- ja tietojärjestelmien antamien kuvien, tekstien ja kaavioiden esityksestä, näin antaen päätöksentekijälle ymmärrystä tilanteesta (STAE 2020 osa 2. 2004, 63). Jokainen asehaara käsittää oman tilannekuvan johtamisjärjestelmässä, nämä ovat ilma-, meri- ja maalitilannekuvat. Rauhanaikana näitä tilannekuvia täydennetään mm. siviili-ilmailun tilannekuvan (FATMI -lennonjohtojärjestelmän ja AFTN -ilmailuverkon lentosuunnitelmatietojen) sekä merenkulun liikenteen tunnistusjärjestelmien kautta (AIS). Yhdistämällä nämä tilannekuvat luodaan yhteinen operatiivinen tilannekuva (Common Operational Picture, COP) strategisen päätöksenteon tueksi (STAE 2020 osa 2. 2004, 86). Näistä tiedoista operaatioiden suunnittelijat muodostavat myös reaaliaikaisen uhka-arvion (”Situation Threat Assessment”, STA). Taktisen tason tilannekuvan tietomallin rakenne on saatavilla Nato standardina (NATO STANAG 5525).

Verkkokeskeinen sodankäynti, NCW (Network Centric Warfare)

Verkkokeskeisellä sodankäynnillä tarkoitetaan tilannekuvan ja tilannetietoisuuden jakamista joukoille taistelukentällä yhteistä tietoverkkoa käyttämällä. Tavoitteena on kohottaa suorituskykyä paremmalla tietämyksellä ja toiminnan synkronoinnilla. Edellytyksenä verkkokeskeiselle sodankäynnille on, että verkostoituminen ulottuu mahdollisimman laajalle ja syvälle johdettavissa joukoissa sekä järjestelmissä. Eli verkkokeskeinen johtamisjärjestelmä rakentuu sensorien, päätöksentekijöiden ja asejärjestelmien yhteisestä tietoverkosta. (Pajuniemi ym. 2008, 217-218.)