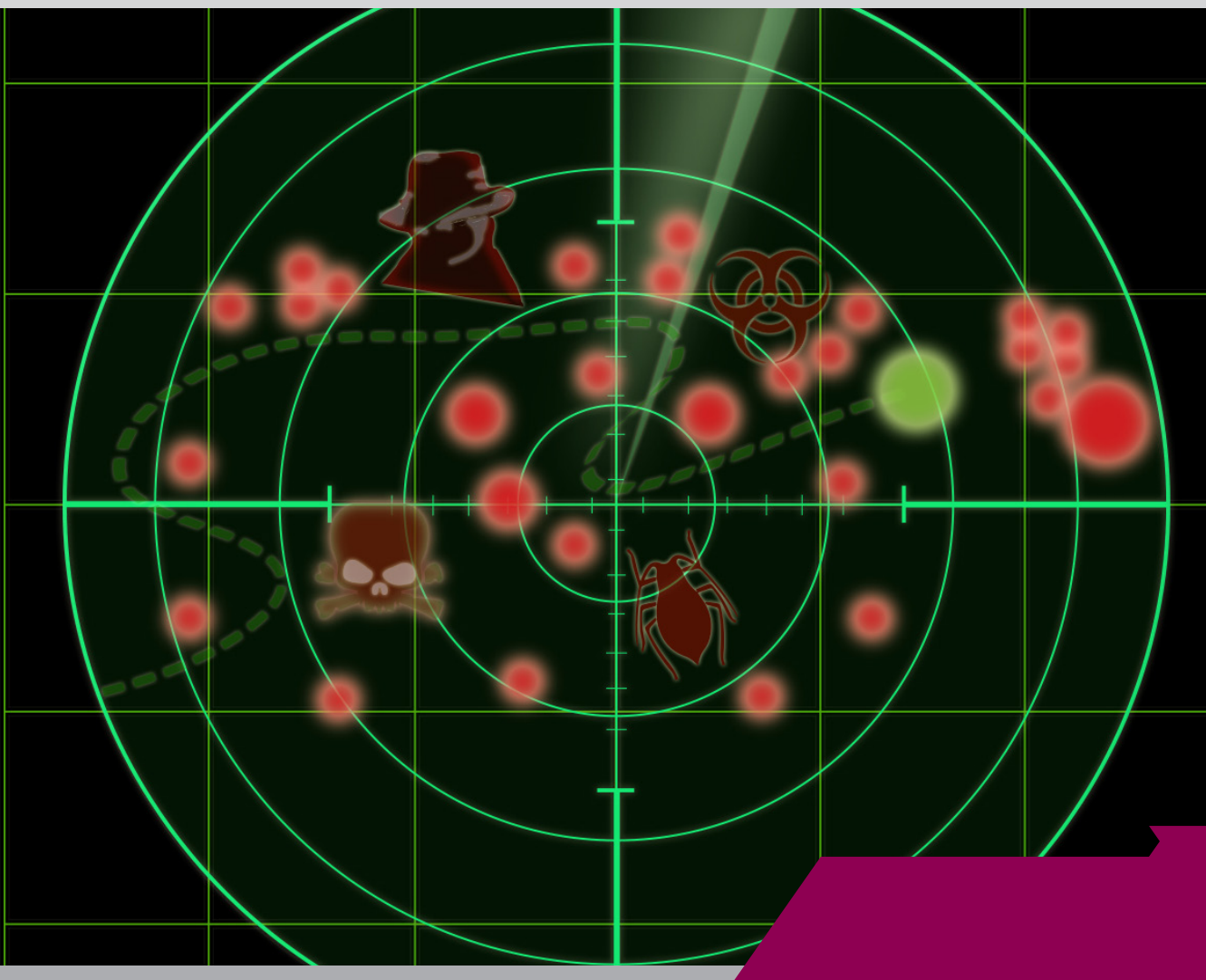
Maanpuolustuskorkeakoulu
Taktiikan laitos
Julkaisusarja 2, No. 1/2014

KYBERTAISTELU 2020

Toimittanut: Tuija Kuusisto

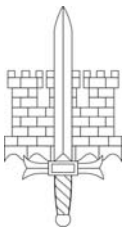


MAANPUOLUSTUSKORKEAKOULU
TAKTIIKAN LAITOS
JULKAISUSARJA 2: NO. 1/2014

NATIONAL DEFENCE UNIVERSITY
DEPARTMENT OF TACTICS AND OPERATIONAL ART
SERIES 2: NO 1/2014

KYBERTAISTELU 2020

TUIJA KUUSISTO (TOIM.)



MAANPUOLUSTUSKORKEAKOULU
Taktiikan laitos
HELSINKI 2014

Tuija Kuusisto (toim.): *Kybertaistelu 2020*
Maanpuolustuskorkeakoulu, Taktiikan laitos
Julkaisusarja 2: Asiatietoa, No. 1/2014

Uusimmat julkaisut pdf-muodossa: http://www.doria.fi

Kannen kuva: Eetu Rehmonen

ISBN 978-951-25-2618-5 (PDF)
ISSN 1238-2752

Maanpuolustuskorkeakoulu – National Defence University
Taktiikan laitos – Department of Tactics and Operational Art

Juvenes Print
Tampere 2014

Esipuhe

Idea on päivittää ja täydentää vuonna 2003 julkaistu *Verkkotaistelu 2020* -kirja pääosin samalla joukolla. Tärkeä osa artikkeleissa on reflektio asiassa, jonka merkitys on muuttunut enemmän kuin osasimme kuvitella. Kirjalla ei pyritä määrittelemään kokonaisuutta tai järjestelemään nykykäsityksiä, vaan jatkumona jo aiemmin tehdylle osallistua keskusteluun kybertaisteluista. Esimerkiksi informaatio-operaatiot sisältöinä – propaganda – ei kuulunut alkuperäiseen, eikä sitä ole liitetty tähänkään. Alkuperäisteoksen tulevaisuusoletukset ovat monin osin toteutuneet, eikä yhteiskunnan tai maanpuolustuksen informaatioistumiselle ole vielä tullut raja vastaan. Muutamassa artikkelissa on täsmennetty näitä oletuksia.

Luvut ovat kunkin kirjoittajan omia näkemyksiä. Kohteet ja skenaariot ovat esimerkkejä ja herätyksiä, koska varsinkin sotilaslukija on pragmaattinen. Niitä voinee yleistää, mutta niillä ei pyritä kattavuuteen. Vaikeaa tieteellistä tai kyberalan kieltä on vältetty tarkoituksella, eikä kirja edellytä ennakkotietoja asiasta. Näkökulma on puolustajan. Kirja on kirjoitettu maanpuolustuksen näkökannalta. Se ei pyri kokonaisvaltaisuuteen, eikä se ota kantaa muiden viranomaisten tai toimijoiden tehtäviin. Painopiste on operaatioissa ja taktiikassa, taisteluissa eli toiminnassa, ei motivaatioissa tai säädöksissä, jotka kuuluvat sodan ja siten valtion ja strategian piiriin. Maanpuolustusnäkökulma tarkoittaa, että asiaa katsotaan ikävimmän, valtion olemassaolon näkökannalta[1], ei arjen. Tarkastelu pysyy yhteiskunnan kokonaisturvallisuuden puitteissa, arkea ja kansalaisia ei käsitellä.

Kirja on osaltaan kannanotto Suomen tavoitteeseen olla johtava valtio kyberturvallisuudessa vuonna 2016. Uutena mukaan otettu yritysturvallisuus kuvaa, että tietoturvallisuuteen on panostettu Suomessa jo pitkään maailman kärkitasolla. Valtion turvallisuusstrategia ja menettelytavat sen toteuttamiseksi ovat Suomessa korkeaa luokkaa. Puolustushaaraosioissa kuvataan, että asiaan on panostettu ja panostetaan monin tavoin.

On syytä pohtia, onko kyberkyvykkyys laadun lisäksi määrä- vai suhdekysymys. Isolla maalla on paljon vastustajia ja suojattavia kohteita. Pienellä maalla on pieni määrä vastustajia ja suojattavia kohteita. Mitataanko kyky osallistujien määrällä vai sillä, kuinka moni osallistuu ja kuinka vahva näin muodostunut verkosto on?

Sotilasprofessori Mika Hyytiäinen

[1] Riskin siedon tasot voi hahmottaa seuraavasti. Jatkuvuudenhallinta turvaa yrityksissä taloudellisen olemassaolon, estää konkurssin. Turvallisuudella ehkäistään ja tarvittaessa hoidetaan ikävät asiat sekä kestetään myös henkilötappiot riittävä toiminnan taso palauttaen. Valmius on kyky tuottaa ennalta priorisoitu taso isotkin tappiot kestäen, jotta yhteiskunta toimii edes minimitasolla. Puolustus ääritilanteessa turvaa valtion eloonjäännin isoillakin tappiolla.

SISÄLLYS

Johdanto

Dosentti Tuija Kuusisto
Maanpuolustuskorkeakoulu
Taktiikan laitos

Puolustusvoimien lakisääteisten tehtävien toimintaympäristö on automatisoitumassa ja yhä kiinteämmin integroitumassa keskenään tosistaan riippuviin, jatkuvasti kehittyviin globaaleihin kyberympäristöihin. Tämä muutos ei koske vain käytettäviä teknologioita tai rajoitu ainoastaan Suomen valtion alueelle tai virtuaalisiin kyberympäristöihin, vaan kyseessä on globaalisti yhteiskunnan ja organisaatioiden digitalisoituminen. Tämä avaa uusia mahdollisuuksia puolustusvoimien tehtävien suunnittelulle ja toteuttamiselle sekä modernin teknologian hyödyntämiselle. Samalla tehtäviä ohjaaviin tietoihin kohdistuu yhä kompleksisempia uhkia, joita ei voida ainoastaan teknologisin keinoin ja menetelmin torjua. Kybertoimintaympäristö on tuntematon maasto. Tarvitaan enemmän kokonaisymmärrystä siitä, mitä kybertoimintaympäristö edellyttää toimijoilta, toiminnalta, toimintorakenteilta ja tietojenvaihdolta.

Suomen kyberturvallisuusstrategiassa visiona on elintärkeiden toimintojen suojaaminen kaikissa tilanteissa kyberuhkaa vastaan. Yhdeksi strategiseksi linjaukseksi on päätetty se, että puolustusvoimat luovat kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissä. Ministeriöille hyväksytyissä kyberturvallisuustehtävissä tätä on tarkennettu siten, että puolustushallinto vastaa Suomen sotilaallisesta puolustamisesta myös kybertoimintaympäristön kautta maan turvallisuuteen kohdistuvia, sotilaallisiin uhkiin rinnastettavia kyberuhkia vastaan.

Taistelukenttä 2020 -tutkimushanke ja siihen kuulunut majuri Mika Piiroisen toimittama Verkkotaistelu 2020 -taustatutkimus julkaistiin Maanpuolustuskorkeakoulun Taktiikan laitoksella vuonna 2003. Kuten edellä kuvattiin, niin vuoden 2003 jälkeen kybertoimintaympäristön vaikuttavuus puolustusvoimien lakisääteisiin tehtäviin ja siten myös taktiikkaan ja operaatiotaitoon on kasvanut. Verkkotaistelu 2020 -tutkimuksen ennakoinnit vuoteen 2020 ovat osittain onnistuneita mutta osittain kehitys on mennyt eri suuntaan. Tämän johdosta Taktiikan laitoksella käynnistettiin vuoden 2013 alusta sotilasprofessori Mika Hyytiäisen aloitteesta vuonna 2003 julkaistun *Verkkotaistelu 2020* -tutkimuksen ajantasaistaminen.

Tutkimus toteutettiin kutsumalla tutkimusryhmään ja tämän kirjan artikkelien kirjoittajiksi sekä *Verkkotaistelu 2020* -kirjan kirjoittajia että esille nousseista uusista näkökulmista kirjoittavia sotatieteiden ja teollisuuden asiantuntijoita. Tutkimuksen viitekehykseksi todettiin Suomen kokonaisturvallisuus, yhteiskunnan elintärkeiden toimintojen turvaaminen ja puolustusvoimien lakisääteiset tehtävät ja näiden integroituminen globaaliin kybertoimintaympäristöön. Tutkimuksen tuloksena tämä kirja on tarkoitettu sekä Maanpuolustuskorkeakoulun opiskelijoille että kaikille jotka ovat kiinnostuneita siitä, mitä haasteita kybertoimintaympäristö asettaa ja mitä mahdollisuuksia se tarjoaa puolustusvoimien lakisääteisille tehtäville, ennen kaikkea Suomen sotilaalliselle puolustamiselle.

Työseminaarit ja kirjan kirjoittaminen aloitettiin vuonna 2013 vertaamalla vuoden 2003 kirjaan tehtyjä ennakointeja taistelun kuvasta 2020 nykytilanteeseen: Minkä asioiden ennakoinneissa onnistuttiin ja mikä meni toisin kuin ajateltiin? Koska *Verkkotaistelu 2020* -kirjan painos on loppunut, niin vertailtavuuden säilyttämiseksi se päätettiin julkaista verkkojulkaisuna tämän tutkimuksen kanssa.

Tutkimuksessa ennakoitiin uudelleen kehitystä vuoteen 2020 mennessä ja arvioitiin syntyneitä tuloksia työseminaareissa. Tutkimuksen edetessä tutkimuksen nimi vaihtui verkkotaistelusta kybertaisteluksi. Käytyjen keskustelujen perusteella tutkimukseen otettiin mukaan lainsäädäntöön liittyvää pohdiskelua sekä puolustushaarojen ja elinkeinoelämän näkökulmia. Elinkeinoelämän näkökulma katsottiin tarpeelliseksi tässä tutkimuksessa, koska elinkeinoelämä toteuttaa keskeisesti yhteiskunnan turvallisuusstrategiaa.

Kyberasioihin liittyvät käsitteet ovat melko tuoreita ja siten edelleen muotoutumassa. Viime vuosina teknisen lähestymistavan rinnalle on noussut kybermaailman ilmiöiden laajempi käsittely organisaatioita ja niiden rakenteita ja toimintoja muuttavina asioina. Cyberspace on yleisesti käytetty kyberkokonaisuutta kuvaava termi. Se tarkoittaa laitteistojen, ohjelmistojen, tietojärjestelmien, ihmisten ja tietoverkoissa tapahtuvan sosiaalisen vuorovaikutuksen muodostamaa kokonaisuutta. Cyberspace käännetään suomeksi usein joko kybertoimintaympäristöksi, kybertilaksi tai kyberavaruudeksi. Tässä kirjassa samoin kuin Suomen kyberturvallisuusstrategiassa käytetään termiä kybertoimintaympäristö.

Suomen kyberturvallisuusstrategiassa todetaan, että ”Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle”. Kyberturvallisuus siten nähdään osana yhteiskunnan kokonaisturvallisuutta, jolloin kyberturvallisuus kuuluu yhteiskunnan elintärkeiden toimintojen turvaamiseen ja liittyy saumattomasti myös puolustusvoimien tehtäviin. ISO/EIC 27032:2012 termistössä tämä kokonaisvaltainen näkemys kyberturvallisuudesta liitetään termiin cybersafety kun taas cybersecurity on määritelty samaksi kuin tietoturvallisuus. Kokonaisvaltainen näkemys kyberturvallisuudesta tukee parhaiten tulevaisuuden ennakointia. Siten se muodostaa tämän kirjan lähtökohdan.

Verkkotaistelu on puolustusvoimissa 2000-luvun alkupuolella käyttöön otettu työnimi, josta on ryhdytty 2010-luvulle tultaessa käyttämään termiä kybertaistelu. Kokonaisturvallisuuden näkökulmalta katsottuna kybertaistelu on valtioiden suvereniteettiin, elintärkeisiin toimintoihin ja erityisesti kriittiseen infrastruktuuriin kohdistuvan haitallisen tai vihamielisen vaikuttamisen ennaltaehkäisyä ja torjumista kybertoimintaympäristössä. Kybertaisteluilla on mahdollista vaikuttaa sekä kybertoimintaympäristöön että fyysiseen ympäristöön. Kasvavaa huomiota on saamassa kineettinen kyber, jolla tarkoitetaan fyysisessä maailmassa ilmeneviä tapahtumia, jotka on saatu aikaan kybertoimintaympäristössä toteutetulla toiminnalla. Sodankäynnissä kybertaistelut muodostavat yhden osan käytettävissä olevia resurssi- ja keinovalikoimia suunniteltaessa ja toteutettaessa maalla, merellä, ilmassa, avaruudessa ja kybertoimintaympäristössä tapahtuvia sotilaallisia operaatioita.

Merkittävillä kybertaistelujen toimijoilla on mahdollisuus käyttää pitkälle kehittynyttä kyberpotentiaalia, joka perustuu kulttuuriperintöön, vaurauteen, koulutusjärjestelmään, tutkimukseen ja tuotekehitykseen, kansainväliseen liiketoimintaan, yhteiskunnallisiin rakenteisiin ja infrastruktuuriin. Kyberpotentiaali on globaalisti keskittynyttä ja sen käyttäminen perustuu yhteistoimintaan ja teknologisiin verkostoihin. Siten merkittävimpiä kybertaisteluissa vaikuttavia toimijoita ovat ne valtiot ja valtioiden kanssa yhteistyössä toimivat organisaatiot, joilla on pääsy kyberpotentiaaliin sekä kyberpuolustuskykyjä eli kyberosaamista ja kykyä käyttää sitä.

Kuten fyysisessä ympäristössä, niin myös kybertoimintaympäristössä toimitaan eri toiminnan tasoilla, jotka tyypillisesti jaetaan strategiseksi, operaatiotaidolliseksi, taktiseksi ja operoinnin toiminnan tasoiksi. Toiminnan taso vaikuttaa siihen mitä resursseja ja keinoja kybertoimintaympäristössä tai sen kautta käytetään ja miten. Esimerkiksi harhauttaminen kybertoimintaympäristössä tai sen kautta arvotetaan ja sitä toteutetaan eri tavoin toimittaessa valtioiden välisten strategisten suhteiden tasolla kuin tarkasteltaessa asiaa taisteluteknisenä kysymyksenä.

Tämä kirja on kirjoitettu Taktiikan laitoksella tarkoituksena tuottaa lähtökohtia pohdittaessa operaatiotaitoa ja taktiikkaa kybertoimintaympäristössä. Operaatiotaidollinen toiminta on askeleiden valintaa polulla kohti strategisia tavoitteita luoden sellaisia asetelmia ja resursseja joilla pystytään tekemään ratkaisuja.[1] Operaatiotaidolliseen toimintaan sisältyvät olennaisesti ennakoivat vastatoimenpiteet. Taktinen toiminta on ”resurssien ja keinojen optimaalista suunnittelua ja sovellettua käyttöä päämäärien saavuttamiseksi taisteluissa”.[2] Kybertoimintaympäristö tuntemattomana maastona tarjoaa mahdollisuuksia yllättävien asetelmien ja dynaamisten resurssien luomiselle sekä niiden optimaaliselle suunnittelulle ja sovelletulle käytölle.

Esimerkki onnistuneesta asetelman luomisesta taistelun voittamiseksi on omalle toiminnalle edullisten tietojen jatkuva syöttäminen sosiaalisen median ja tiedotusvälineiden kautta ja siten huomaamattoman kohteen valloittamisen mahdollistaminen ilman taistelua käyttäen tunnuksettomia joukkoja. Verkossa toteutettu mainoskampanja, joka houkuttelee uusia henkilöitä liittymään tuhansien kilometrien päässä toimiviin organisoituihin sotilaallista toimintaa harjoittaviin ryhmiin, on resurssien luomista edullisesti kybertoimintaympäristön kautta. Nämä esimerkit osoittavat, että operaatiotaitoa on jo toteutettu menestyksekkäästi kybertoimintaympäristössä.

Suomen kyberturvallisuusstrategian mukaan sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Tässä kirjassa kuvataan teoreettisia menetelmiä ja malleja sekä käsitteitä ja säädöksiä, joiden avulla voidaan tunnistaa kybertoimintaympäristön asettamia edellytyksiä kyberpuolustuskyvylle. Kirjassa pohditaan miten kybertoimintaympäristöä kohtaan hyökätään ja miten sitä puolustetaan eri toimijoiden muodostamien

[1] Kuusisto, T., Kuusisto, R. (2014). Prerequisites for Creating Resources and Compositions for Cyber Defence. Proc of 2014 SRI Security Congress, Perth, Australia.
[2] Huttunen, M. (2010). Monimutkainen taktiikka. Taktiikan laitoksen julkaisusarja 1, n:o 2/2010, Edita Prima Oy, Helsinki, 2010.

verkostojen yhteistyönä. Lisäksi kirjassa kuvataan maa- ja ilmapuolustuksen kybersuorituskyvyn kehittämisen perusteita. Kirja on laadittu yhteistyössä kirjoittajien kesken. Kukin kirjoittaja on kuitenkin artikkelissaan nostanut esille itse valitsemiaan näkemyksiä. Kirja ei edusta puolustusvoimien tai muiden organisaatioiden kantaa.

Kirja alkaa kolmella taustoittavalla luvulla, joista ensimmäisessä evl. (evp.) Sakari Ahvenainen tarkastelee verkkosodankäynnin historiaa ja verkkosodankäynnin käsitteen kehittymistä kolmesta eri näkökulmasta: systeemiteoria, kybernetiikka ja evoluutio. Ahvenainen osoittaa, että nämä uudet näkökulmat laajentavat verkkosodan historiaa ja tuovat siihen oleellista uutta ja ennen kaikkea systematiikkaa. Verkkosodan historia ulottuu ainakin 1980-luvulle Neuvostoliiton kaatamiseen tai sen kaatamisen edistämiseen ei-sotilaallisella strategisella informaatio-operaatiolla.

Seuraavassa luvussa dosentti, TkT Tuija Kuusisto käsittelee kybertoimintaympäristöä tietonäkökulmasta. Kuusisto toteaa, että yhteiskunnan ja taistelujen robotisoituminen ja automatisoituminen sekä massadatan jalostusmenetelmien kehittyminen ja laajeneva käyttö vaikuttavat yhteiskunnan elintärkeisiin toimintoihin sekä puolustusvoimien mahdollisuuksiin ja vaihtoehtoihin toimia. Kompleksisten systeemien teorioihin perustuvan sosiaalisen systeemin mallin avulla on mahdollista hahmottaa tätä muutosta ja siihen liittyviä ilmiöitä sekä niiden perusteella suunnata resursseja vaikuttavimpiin kohteisiin. Kybertoimintaympäristössä voidaan tietoon vaikuttamalla kohdistaa Suomen rajojen ulkopuolelta vaikutus Suomen alueella sijaitsevaan kohteeseen. Tältä vaikuttamiselta ei voida puolustautua pelkästään Suomen maantieteellisen alueen sisältä. Siten Suomessa tarvitaan vuonna 2020 kansallisia ja kansainvälisiä sopimuksia Suomen sotilaalliseksi puolustamiseksi ja kybertaisteluissa onnistumiseksi.

Viimeisessä taustoittavassa luvussa tietoturva-asiantuntija, diplomi-insinööri Tomi Hasu valottaa kyberlainsäädännön ja sen kehittymisen tulkintaa kansainvälisestä ja kansallisesta näkökulmasta sekä esittää kaksi kuvausta erilaisista lainsäädännöllisistä suhtautumisista kybertoimintaympäristöön. Ensimmäinen korostaa tietosuojan merkitystä ja kirjesalaisuuden koskemattomuutta. Toisessa pyritään takaamaan globaalin informaatioinfrastruktuurin toiminta vahvalla sääntelyllä ja lukuisilla kontrolleilla. Hasun näkemyksen mukaan 2010-luvulla yleisesti hyväksytty suhtautuminen kybersodankäynnin laillisuuteen on se, että kybertoimintaympäristö on fyysisen maailman jatke, johon sovelletaan olemassa olevia sopimuksia ja oikeuskäytäntöjä.

Kirjan neljännessä luvussa eversti (evp), dosentti Martti Lehto tarkastelee kybertaistelun toimintaympäristöä. Lehto käsittelee sodankäynnin muutosta, puolustusjärjestelmän kyberverkon rakennemallia sekä kyberajan johtamisteoriaa ja vaikuttamisteoriaa. Lehto toteaa, että tulevaisuuden kybersuorituskyvyn kehittämisessä korostuu systeeminen ajattelu. Kybermaalien valinnassa niitä tulee tarkastella systeemin osina, jolloin aikaan saadaan suoraa ja epäsuoraa vaikutusta. Maalien valinnassa on järkevää valita sellaisia, jotka nopeimmin, pitkävaikutteisimmin ja tehokkaimmin aikaansaavat systeemimuutoksen. Muutos saadaan tehokkaimmin toteutettua, kun toteutetaan kineettisiä ja ei-kineettisiä rinnakkaisoperaatioita kaikissa taistelutilan ulottuvuuksissa. Reaaliaikaisen tilannekuvan muodostaminen ja jaetun tilannetietoisuuden aikaansaaminen tulee

olla yhä nopeampaa. Johtamisprosessissa tarvitaan sisällöltään mahdollisimman tarkkaa ja oikein aikautettua informaatiota, jopa liikkeessä, jotta keskitetty johtaminen ja hajautettu toiminta voidaan toteuttaa sekä suojata oma toiminta kybertaistelutilassa.

Seuraavassa luvussa sotilasprofessori Mika Hyytiäinen pohtii sitä, miten kyberhyökkäys voitaisiin tehdä. Hyytiäinen visioi kolme erilaista ja nykykäsittelyssä marginaalissa olevaa valtiollista hyökkäystä, joita voitaisiin käyttää Suomen kokonaisturvallisuutta vastaan kybermaailmassa vuoden 2020 aikaikkunassa. Visioidut hyökkäysskenaariot ovat täsmähyökkäys suljettuun ympäristöön, kyberympäristön lamauttaminen kyberkeinovalikoimaa käyttämättä ja isku tietopääomaa vastaan. Yksi hyökkäyksistä on epäsymmetrinen kyberin suhteen. Lisäksi esitetään joukko havaintoja kyberperästä ja siellä käytävistä taisteluista keskittyen ”normaalista” sodankäynnistä poikkeaviin piirteisiin ja sitoen kybertaistelua osaksi laajempia operaatioita. Artikkeli täydentää Mikko Hyppösen vuosikymmen sitten visioimia taisteluskenaarioita..

Kirjan kuudennessa luvussa professori Jouko Vankka kuvaa analyyttisen hierarkiaprosessin sekä soveltaa sitä tietoverkkopuolustuksen 2020 haasteisiin. Kriteereiksi tietoverkkopuolustuksen haasteita arvioitaessa on valittu tiedon luottamuksellisuus, eheys ja saatavuus. Tietoverkkopuolustuksen haasteiden vaihtoehdoiksi on valittu pilvipalvelut, mobiililaitteet ja laitteistojen takaovet. Vankka toteaa, että suoritetun empiirisen tutkimuksen perusteella suurimmat haasteet ovat mobiililaitteissa.

Johtaja Kari Wirman tarkastelee verkkosodankäyntiä yritysten toiminnan kannalta. Kirjoituksessa kuvataan yritysten turvallisuusasioihin liittyvää ajattelua, jonka perusteella yritykset lähestyvät myös kyberturvallisuutta ja sen toteuttamiseen läheisesti liittyviä tietoturvallisuusasioita. Wirman painottaa, että vastuu kyberturvallisuudesta on jokaisella yrityksellä ja organisaatiolla itsellään. Kukaan ei voi tuottaa toisen kyberturvallisuutta. Eri toimijoiden välillä tarvitaan yhteistoimintaa, jotta keskinäisriippuvuuksien yhteiskunnassa toimijoiden muodostamien verkostojen kyberturvallisuus olisi riittävällä tasolla. Kyberturvallisuusverkoston keskeinen tavoite on tukea ja auttaa verkoston yksittäistä toimijaa selviytymään mahdollisimman hyvin kyberuhkista sekä kyberhäiriöistä. Artikkelissa kuvatut yritysten menettelyt ja eri organisaatioiden yhteistoimintamallit ovat se pohja, johon yhteiskunnan kyberpuolustus osaltaan tukeutuu meihin kohdistuvan verkkosodan aikana.

Kirjan kahdeksannessa luvussa evl. J-P Virtanen ja majuri Janne Jokinen kirjoittavat maavoimista kybertaistelukentällä. Virtanen ja Jokinen toteavat että päätähuimaavasta teknologiakehityksestä ponnistavana kybersodankäynti voidaan perustellusti luokitella uudeksi sodankäynnin ulottuvuudeksi, joka kaikkien vakavasti otettavien armeijoiden on omissa kehittämisohjelmissaan huomioitava. Vaikka kyberulottuvuutta ei olekaan viety maavoimien uudistetun taistelun keskiöön, ei se tarkoita sitä, etteikö kyberuhkaa olisi huomioitu. Maavoimien taistelu 2015:n tueksi kehitettävien johtamis- ja asejärjestelmien teknisten ja rakenteellisten ratkaisuiden ohella kyberpuolustuksellinen tarkastelu on perusteltua ulottaa myös verkkojen ja järjestelmien ulkopuolelle. Tällöin keskeiseen asemaan nousevat koulutus, ohjeistus, toimintatavat, johtaminen, yhteistoiminta ja asenteet.

Seuraavaksi eversti (evp), dosentti Martti Lehto kuvaa ilmapuolustuksen kybersuorituskyvyn kehittämistä. Lehto käsittelee sodankäynnin evoluutiota elektronisesta sodankäynnistä informaatiosodankäynnin, verkkokeskeisen sodankäynnin ja vaikutusperusteisten operaatioiden kautta kybersodankäyntiin. Lehto kuvaa ilma-aseen haavoittuvuutta sekä kyberajan ei-kineettisiä operaatioita. Lehto toteaa, että tarvitaan ei-kineettisten operaatioiden tehokasta integroimista keskenään, kineettisiin operaatioihin ja puolustusvoimien yhteisoperaatioihin. Tässä integrointikehityksessä korostuu ilmaoperaatio-keskuksen rooli sekä kineettisten että ei-kineettisten operaatioiden johtamispaikkana.

Viimeisenä lukuna on sotilasprofessori Jari Rantapelkosen kirjoittama näkemys kybertoimintaympäristön merkityksestä sodankäynnissä, taistelussa ja taktiikassa sekä kirjan artikkelien arvio.

Kirjoitettujen artikkelien perusteella voidaan todeta, että vuonna 2020 kybertaisteluilla vaikuttaisi olevan seuraavia piirteitä:

- Sodankäynnissä kybertaisteluita käydään yhdessä perinteisten maalla, merellä, ilmassa ja avaruudessa tapahtuvien sotilaallisten operaatioiden kanssa.
- Yhteisoperaatiot ja niiden suunnittelu ja johtaminen edellyttävät kattavaa tilanneymmärrystä myös koskien kybertoimintaympäristöä: jatkuvaa tilanteen tulkintaa kokonaisympäristössä sekä ennakointia paikallisesti ja ajallisesti välittömien tapahtumien ulkopuolelle.
- Yhteisoperaatioissa maaleiksi valikoituvat kybertoimintaympäristön kohteet, jos niihin vaikuttamalla on mahdollista nopeimmin, pitkävaikutteisimmin tai tehokkaimmin aikaansaada muutos kokonaissysteemissä.
- Kybermaaleihin hyökätään ja niitä puolustetaan. Hyökkäysten tarkoituksena on aikaansaada vaikutus kybertoimintaympäristössä tai kybertoimintaympäristön kautta fyysisessä ympäristössä.
- Elinkeinoelämä ja yksittäiset yritykset ovat kybertaistelujen kohteita ja välineitä vaikuttaa yhteiskuntaan.
- Suomessa sijaitsevaan kybertaistelutilaan voidaan vaikuttaa Suomen ulkopuolelta, eikä vaikuttamiselta voida puolustautua pelkästään Suomen maantieteellisen alueen sisältä, minkä johdosta tarvitaan kykyä toimia kybertoimintaympäristössä Suomen rajojen ulkopuolella.
- Kybertaisteluita käydään jokaisessa kolmessa kybertoimintaympäristön kerroksessa eli fyysisessä, loogisessa ja sosiaalisessa kerroksessa.
- Taistelutila automatisoituu ja robotisoituu edelleen. Taistelutilan teknologisen kompleksisuuden vuoksi taisteluissa tarvitaan verkostoyhteistyötä elinkeinoelämän kanssa.
- Kybertaistelujen johtamisprosessissa tarvitaan sisällöltään mahdollisimman tarkkaa ja oikein aikautettua tietoa, jopa liikkeessä, jotta keskitetty johtaminen ja hajautettu toiminta voidaan toteuttaa sekä suojata oma toiminta kybertaistelutilassa.

Brysselissä, Belgiassa 4.12.2014

Tuija Kuusisto

1.

Verkkosodan historia ja käsitteen kehittyminen – Kriittinen, systeeminen ja kyberneettinen katsaus vuoden 2003 artikkeliin

Evl (evp) Sakari Ahvenainen
Maapuolustuskorkeakoulu
sakari.ahvenainen@kolumbus.fi

Yleisesikuntaeverstiluutnantti (evp.) Sakari Ahvenainen on viestiupseeri, jolla on kokemusta myös elektronisesta sodankäynnistä. Hän on 1990-luvulta alkaen toiminut myös freelance-tutkijana. Tutkimusten aiheita ovat olleet mm. sodankäynti yleensä, informaatiosodankäynti erityisesti ja tekniikka osana sodankäyntiä. Informaatiosodankäynnin tutkijana hän on pitänyt useita kansainvälisiä esityksiä. Ahvenainen on jatko-opiskelija Tampereen Teknisessä Yliopistossa (pääaine) ja Maanpuolustuskorkeakoulussa (sivuaine). Hän on kirjoittanut kuusi artikkelia Suomen Sotatieteellisen Seuran vuosikirjaan Tiede ja Ase. Viimeisen noin kymmenen vuoden aikana Ahvenaisen tutkimukset ovat keskittyneet kysymykseen siitä, mitä tieto tai informaatio *pohjimmiltaan* on. Aihe on johtanut parin viime vuoden aikana kybernetiikan pariin. Viimeiset noin kymmenen vuotta Ahvenainen on toiminut osapäiväisenä valmiuspäällikkönä Huoltovarmuuskeskuksen joukkoviestintä- ja myöhemmin mediapoolissa. Lisätietoja Ahvenaisen kotisivuilta: *http://www.kolumbus.fi/sakari.ahvenainen/*

Tiivistelmä
Tämä artikkeli on arviointi ja päivitys vuodelle 2014 kirjoittajan artikkeliin ”Verkkosodan historia ja käsitteen kehittyminen”[1]. Artikkeli oli osa Maanpuolustuskorkeakoulun vuonna 2003 julkaistua kirjaa ”Verkkotaistelu 2020 – Taustatutkimus maavoimien Taistelunkuvat 2020 tutkimukseen”[2]. Tämän artikkelin tutkimuskysymys on: ”Mitä kirjoittaja voi nyt sanoa vuoden 2003 artikkelista kolmen uuden näkökulman – systeemiteorian, kybernetiikan ja evoluution – perusteella?” Osoittautuu, että tässä käyttöön otetut uudet näkökulmat laajentavat verkkosodan historiaa ja tuovat siihen oleellista uutta sisältöä ja ennen kaikkea systematiikkaa. Kirjoittamisen yhteydessä on syntynyt myös useampi suurempi havainto sodankäynnistä varsinaisen artikkelin ytimen ulkopuolelta. Merkittävä osa uusista havainnoista liittyy kyberiin. Tärkeimpien 12 johtopäätösten luettelo on esitetty luvun 7 alussa. Myös luvun 8 kuusi uutta ongelmaa voidaan nähdä tämän työn keskeisinä tuloksina.

[1] S. Ahvenainen, ”Verkkosodan historia ja käsitteen muodostuminen,” kirjassa M. Piiroinen, Toim., Verkkotaistelu 2020 – Taustatutkimus Maavoimien Taistelun kuvat 2020 tutkimukseen, Helsinki, Edita Prima Oy, 2003, s. 12 - 42.
[2] M. Piiroinen, Toim., Verkkotaistelu 2020 – Taustatutkimus maavoimien Taistelunkuvat 2020 tutkimukseen, Helsinki, Edita Prima Oy, 2003.

1.1 Johdanto

Tutkimusprosessina artikkelissa käytetään itävaltalais-brittiläisen tieteenfilosofin, professori Karl R. Popperin esittämää evolutiivista induktionäkemystä, joka tiivistyy prosessiksi: mielenkiintoinen ongelma, sen alustavat teoriat, virheiden karsinta ja uudet ongelmat[3]. Prosessin ydinsanoma on, että näin voidaan päästä lähemmäksi tieteellistä ”totuutta”, mutta sitä ei voida koskaan saavuttaa[4]. Prosessi on myös itseensä viittaava, rekursiivinen. Uudet ongelmat viittaavat vanhan ongelman käsittelyn jälkeen (uutena) ongelmana (alkuperäiseen, vanhaan) ongelmaan.

Tämän artikkelin ongelman alustavia teorioita ovat ensin systeemiteoria [5] [6], sitten kybernetiikka, informaation systeeminen[7] merkitys[8] [9] ja kolmantena evoluutio[10] [11]. Kutakin näistä arvioidaan sodankäynnin kannalta tavoitteena saada perusteita verkkosodan historian ja käsitteen uudelleenarvioinnille.

Popperin malli on, kuten kirjan nimestä selviää, evolutiivinen: *Objective Knowledge – An evolutionary Approach*. Kirjassaan Popper katsoo ratkaisseensa induktion ongelman: Yksittäisistä havainnoista saa tiedettä, todeksi prosessoitua ja varmennettua tietoa vain aiempiin yleisesti hyväksyttyihin teorioihin perustuen sekä käyttäen kriittisyyttä ja tervettä järkeä.[12]

Tämän artikkelin tutkimuskysymys, popperilaisittain mielenkiintoinen ongelma on: ”Mitä kirjoittaja voi nyt sanoa vuoden 2003 artikkelista systeemiteoriaan, kybernetiikkaan ja evoluutioon perustuen ja miksi?”

1.2 Alustava teoria I: Systeemiteoria

1.2.1 Systeemit, systeemin ympäristö ja systeemin tasot

Ensimmäinen alustava teoria ja analyyttinen väline vuoden 2003 artikkelin arviointiin on systeemiteoria. Siitä käsitellään vain seuraavat käsitteet ja nekin hyvin periaatteellisesti: Mitä ovat avoimet systeemit? Mikä on avoimen systeemin ja sen ympäristön suhde? Mitä ovat systeemitasot ja miten ne muodostuvat? Nämä ovat samalla artikkelin alatutkimuskysymyksiä ja tämän pääluvun tutkimuskysymyksiä.

---

[3] K. R. Popper, Objective Knowledge - An Evolutionary Approach, Clarendon Press Oxford, 1979 (Revised) s. 119 ja 242 - 4.
[4] Emt. s. 16 ja 71.
[5] L. von Bertalanffy, General Systems Theory – Foundations, Development, Applications, New York: George Braziller, 2003 (alunperin 1968).
[6] L. Skyttner, General systems theory – Problems, perspectives, World Scinetific, 2005.
[7] Systeemisessä mielessä epistemologia, oppi ihmisen tiedosta ja sen rajoista on toinen merkittävä näkemys tietoon. Kirjoittaja on aiemmin löytänyt yhdeksän suurempaa informaation tai tiedon periaatteellista luokkaa, joista kaksi ovat kybernettinen tieto ja epistemologia. (S. Ahvenainen, Informaatioteknologia ja ihmiskunta - Systeeminen ja evolutiivinen tarkastelu, kirjassa M. Laakkonen, S. Lamminpää, J. Malaprade (toim.), Informaatioteknologian filosofia, Lapin yliopistokustannus, Rovaniemi 2011, s. 118.
[8] N. Wiener, Cybernetics: or Control and Communication in the Animal and the Machine, 10. painos (2000) toim., Cambridge (USA): The MIT Press, 1948.
[9] V. F. Turchin, The Phenomenon of Science – a cybernetic approach to human evolution, Adobe Reader (pdf) toim., New York: Principia Cybernetica Project, 1977
[10] E. Paloheimo, Megaevoluutio, WSOY, 2002.
[11] J. M. Smith ja E. Szathmary, The Major Transitions in Evolution, Oxford University Press, 1995.
[12] Popper, 1979 (Revised) s. 22 ja 33 - 34.

Avoin[13] systeemi on erikoistuneista osista muodostuva kokonaisuus, jossa osat ovat yhteydessä toisiinsa ja tämä kokonaisuus yhteydessä ympäristöönsä. Se, millä tavalla osat voivat olla yhteydessä, määrittää hyvin fundamentaalisesti[14] avoimen systeemin luonnetta, muun muassa sen kokoa, käyttäytymistä ja sitä, mitkä ovat tärkeitä osakokonaisuuksia systeemissä[15].

Avoimen systeemin ja sen ympäristön suhde on jo edellä olleen systeemin määritelmän mukaan keskeinen käsite systeemiteoriassa. Avoin systeemi vaikuttaa ympäristöönsä ja ympäristö systeemiin. Suhde on siis rekursiivinen, itseensä viittaava. Toisen viittaus (vaikutus) toiseen palautuu takaisin alkuperäiseen viittaajaan (vaikuttajaan) muuttuneena toisen osapuolen kautta. Rekursiivisuus tarkoittaa epälineaarisuutta, esimerkkinä myöhemmin tässä artikkelissa esitetty Lancasterin neliölaki.

Biologiassa lajin ja sen ympäristön muodostaman systeemin perusvälineet lajin säilymiseen ovat kilpailu ja yhteistyö[16]. Avoin systeemi (laji) voi säilyä muuttuvassa ympäristössä kahdella tavalla, joko muuttamalla ympäristöään, kuten majava tai sopeutumalla siihen, kuten sairaalabakteerit, siis muuttamalla itseään[17].

Systeemitasot ovat evoluution kannalta oleellinen käsite. Systeemitaso tarkoittaa ensin, että olemassaolossa on systeemejä, jotka rakentuvat alisysteemeistä jotka rakentuvat alisysteemeistä ja niin edelleen. Toiseksi systeemitason idea tarkoittaa, että nykyisistä systeemeistä voi[18] rakentua uusi metasysteemi. Uudelle tasolle muodostuu emergenssin[19], laadullisen muutoksen, karkeistamisen kautta uusia ominaisuuksia, joita ei ole systeemin muodostaneissa osasysteemeissä.

1.2.2 Sodankäynnistä systeemiteorian valossa

Sodankäynnin pienin ja fundamentaalein systeeminen kokonaisuus on systeemi, jonka osat ovat oma puoli (A), vastustaja (B) ja näille yhteinen toimintaympäristö (Y)[20]. Näillä on kuusi[21] vaikutussuhdetta. Tähän kokonaisuuteen sisältyy ensin toisen osapuolen sisäinen toiminta (T_a tai T_b)[22], sitten reaktiona (A→B tai B→A) toisen osapuo-

---

[13] Avoimen systeemin lisäksi suljettu systeemi on systeemien toinen luokka. Suljetulla systeemillä ei ole yhteyksiä ympäristöön.

[14] Fyysikko Kari Enqvistiä tulkiten osien yhteydet kertovat miten heikko emergenssi synnyttää uudet tasot olemassaolon järjestelmiin (K. Enqvist, Monimutkaisuus – Elävän olemassaolomme perusta, WSOY, 2007 s. 317 – 328).

[15] B. Buzan ja R. Little, International Systems in World History – Remaking the Study of International Relations, Oxford: Oxford University Press, 2000 s. 91

[16] Skyttner, 2005 s. 383.

[17] Skyttner, 2005 s. 193.

[18] Mutta ei välttämättä rakennu. Tämä riippuu mm. systeemin ympäristöstä ja siinä tapahtuvista muutoksista, esimerkiksi uuden tietoteknologian synty voi olla mahdollisuus uudelle, suuremmalle organisaatiotasolle. Lisäksi voidaan tarvita jotain muita muutoksia, esimerkiksi väestönkasvua uudelle tasolle. Se taas voi edellyttää uudenlaista ruuan tuotantoa, esimerkiksi maanviljelyä. Myös kaikkien uuden systeemin osasysteemien on oltava olemassa. Vrt. muualla käytetty sanonta: ”Viimeinen pala loksahtaa kohdalleen”. Alkuräjähdyksen ensivaiheissa lämpötilan lasku ja avaruuden laajeneminen aiheuttivat useassa vaiheessa uusien systeemien syntymisen. Ensin säikeistä syntyivät alkeishiukkaset, niistä atomit (lähinnä vety), niistä tähdet ja niistä vetyä raskaammat alkuaineet (Paloheimo, 2002, s 71 - 81).

[19] Enqvist, 2007 s. 120, 124, 152, 279, 307, 313.

[20] S. Ahvenainen, ”Sotilas- ja siviiliteknologian eroista – evolutiivinen ja systeeminen tarkastelu,” kirjassa Tiede ja Ase 2007, 2007 s. 208 - 9.

[21] N * N-1 = 3 * 2 = 6: A → B, A → Y, B → A, B → Y, Y → A ja Y → B.

[22] Esimerkiksi siirtyminen, marssi.

len vastatoiminta (VT)[23] (hyökkäys) toisen osapuolen sisäiseen toimintaan ja vasta-vastatoiminta (VVT = V2T)[24] (puolustus) reaktiona (B→A tai A→B) vastatoimintaan ja niiden syvenevät kokonaisuudet reaktiona vastapuolen edelliseen toimintaan (V3T[25], V4T[26], …)[27]. Kyse on siis itseensä viittaavasta, epälineaarisesta toiminnasta.

Tämä ilmenee sodankäynnissä muun muassa Lancasterin neliölakina[28]. Se kertoo mullistavaa tietoa ylivoiman merkityksestä. Voittajan tappiot ovat kääntäen verrannolliset ylivoiman *neliöön*.[29]

Sodankäynnissä säilymisen peruskeinot ovat edellä esitetyn systeemiteorian sovellutusten mukaan (1) kilpailu (sota) (2) yhteistyö (liittoutuminen, naapuriyksikön auttaminen), (3) itsensä muuttaminen tai (4) ympäristönsä muuttaminen.

Myöhemmin luvussa 5.1 ”Sodankäynnistä evoluution valossa” esitetään amerikkalaisen professori Quincy Wrightin sodankäynnin historian megamalli, joka on evolutiivisyyden lisäksi systeeminen. Emergenssi – uudet ilmiöt ja lait – näkyy sodankäynnin tasoissa taistelutekniikkana, taktiikkana, operaatiotaitona ja strategiana[30].

Sodankäynti on sotilasstrategi Karl von Clausewitzin mukaan systeemistä. Jo yli 100 vuotta ennen systeemiteorian keksimistä hän totesi kirjansa ”Sodankäynnistä” 1. luvun aivan alussa seuraavasti:

> ”Tarkoituksenamme on tarkastella aiheemme yksittäisiä perustekijöitä, sitten sen yksittäisiä osia tai aineksia ja lopuksi kokonaisuutta ja siinä ilmeneviä sisäisiä yhteyksiä, siis edetä yksinkertaisesta moniaineksiseen kokonaisuuteen.”[31]

1.3 Alustava teoria II: Kybernetiikka

1.3.1 Kyberneettinen järjestelmä ja kyberneettinen tieto

Toinen alustava teoria ja analyyttinen väline vuoden 2003 artikkelin uudelleenarviointiin on systeemiteorian sovellutus, kybernetiikka. Siitä käsitellään vain seuraavat käsitteet ja nekin hyvin periaatteellisesti: Mikä on kyberneettinen systeemi ja mitä on kyberneettisen systeemin tieto? Nämä ovat samalla artikkelin alatutkimuskysymyksiä ja tämän pääluvun tutkimuskysymyksiä.

---

[23] Esimerkiksi siirtymisessä käytettävän sillan tuhoaminen.
[24] Esimerkiksi sillan ilmatorjunta tai/ja varasilta lähistöllä.
[25] Esimerkiksi sillan ilmatorjunnan lamauttaminen.
[26] Esimerkiksi sillan ilmatorjunnan lamauttamiseen käytettävän ohjuksen harhauttaminen.
[27] Ahvenainen, 2007 s. 214.
[28] M. Hyytiäinen, Report of Finnish Defence College, Tactical Department, Research Group 19.12.2001, 2001 s.16.
[29] Esimerkki 1: Voimasuhteet alussa 100 – 100. Molemmat kärsivät 100 yksikön tappiot, eli tuhoutuvat lopuksi yhtä aikaa. Esimerkki 2: Voimasuhteet 300 – 100. Heikompi tuhoutuu lopuksi kokonaan. Vahvempi on kärsinyt silloin 300/9 eli 33,3 yksikön tappiot.
[30] S. Ahvenainen, ”Sotilasfilosofi Quincy Wright ja sodankäynnin muutos - Informaatioajan evolutiivinen ja systeeminen näkemys sodankäyntiin,” Tiede ja Ase 2008, Suomen sotatieteellinen seura, 2008, s. 155 - 6.
[31] K. Clausewitz (von), Sodankäynnistä, Art House, 1998, s.15.

Kybernetiikkaa tarkoittaa oppia konemaisista ja inhimillisistä tietoa käsittelevistä itseohjautuvista automaattisista järjestelmistä[32] [33].

Kyberneettisessä systeemissä on neljänlaista tietoa[34]:

1. Järjestelmän *sensorin* syötetietoa (stimulaatiota) järjestelmään, dataa todellisuudesta: korva ja puhe, esimerkiksi kysymys.
2. Järjestelmään tallennettua ja syötetietoa käsittelevää ja sen merkityksen tunnistavaa tietoa *päätöksentekoelimessä*: aivot ja muisti. Kyseinen tieto on keskeisesti malleja todellisuudesta.
3. Tulostetietoa *vaikutuselimeen* (esimerkiksi vastaus, puheen tuottaminen), joka stimuloi järjestelmää: toisen ihmisen korvat, vaikutustietoa ja sitten vaikutusta todellisuuteen.
4. *Asetustietoa* systeemin tavoittelemasta tilasta, esim. eloonjäämis- ja lisääntymisvaisto, lämpötilan asetusarvo, tarve tyydyttävän vastauksen saamiseen jne.
5. *Palautetietoa* systeemin osien välillä systeemin säätämiseen: negatiivinen tai positiivinen palaute. Palautetieto on vaikutus- ja säätökanava systeemiin.

Näistä syötetieto (yllä 1) ja tulostetieto (3) ovat siirrettävää tietoa, jota ja vain jota viestintätekniikassa käytetty Claude E. Shannonin matemaattinen kommunikaatioteoria käsittelee[35]. Syötetieto on kyberneettisen järjestelmän sensoritietoa, dataa ulkopuolisesta todellisuudesta ja järjestelmästä itsestään ja tulostetieto kyberneettisen järjestelmän toimintatietoa ulkopuoliseen todellisuuteen ja järjestelmään itseensä vaikuttamiseen.

Jotta siirrettävällä tiedolla olisi merkitys, jotta se vaikuttaisi, tarvitaan tulkitsevaa tietoa (2). Tulkitseva tieto on päätöksentekoelimessä yksinkertaisemmillaan valinnan tekemistä joukosta[36] toimintavaihtoehtoja, sensorien välittämän tilanteen, todellisuudesta saadun datan muuttamista toiminnaksi[37] [38], mutta aina myös enemmän tai vähemmän todellisuutta kuvaavia malleja, virtuaalitodellisuutta ihmisen aivoissa tai tietokoneen muistissa. On siis olemassa kyberneettisen järjestelmän ulkopuolinen *fyysinen todellisuus* ja kyberneettisen järjestelmän sisäiset, ulkopuolista todellisuutta kuvaavat mallit, *virtuaalinen todellisuus*.

Informaatioetiikan professori Luciano Floridi toteaa kirjassaan ”The Philosophy of Information” vuodelta 2011, että hänen informaatiofilosofiansa yhtenä keskeisenä käsitteenä esitetty informaatiotoimija, kaksikoneinen keinotekoinen agentti toimii kahdella tasolla, kohdetasolla ja metatasolla. Kohdetaso on yhteydessä ympäristöönsä. Metatason toiminnan (elaboration) kohteena ovat agentin kohdetason sisäi-

[32] Wiener, 1948.
[33] Turchin, 1977.
[34] Skyttner, 2005 s. 81 - 84 ja 92
[35] C. E. Shannon ja W. Weaver, The Mathematical Theory of Communication, University of Illinois Press, 1949, 1998.
[36] Yksinkertaisin ”valinta”, kyberneettinen protosysteemi vaikuttamiseen on refleksi, aina sama vaste samaan syötetietoon, ärsykkeeseen (Turchin, 1977, s. 26). Muutama valinta voi olla esimerkiksi taistelu, pako tai paikalleen jähmettyminen.
[37] Turchin, 1977 s. 25 - 6.
[38] L. Floridi The Philosophy of Information, Oxford University Press, 2011 s. 164.

set tilat. Metataso liittää kohdetason kuhunkin tilaan symbolin ja tallentaa sen muistiin.[39]

Sensoritietoa tulkitseva tieto päätöksentekoelimessä, esimerkiksi aivoissa tai tietokoneessa, sisältää geneettisesti ja kulttuurisesti perityt ja kokemuksen kautta opitut tai ohjelmoidut todellisuuden mallit, joilla sensoritietoa, havaintoja, dataa todellisuudesta tulkitaan.[40]

Jotta systeemi saavuttaisi asetetun tavoitteensa, esimerkiksi tyydyttävän vastuksen saaminen, tarvitaan palaute, esimerkiksi saatiinko kysymykseen tyydyttävä vastaus.

Kyberneettisinä tietoa käsittelevinä järjestelminä voidaan nähdä solu (elämä), elämän evoluution eräs tulos, ihminen ja hänen laajennetut organisaationsa ja ihmisen teknisen evoluution eräs tulos, tietokone ja sen laajennukset eli tietokoneverkot. Näiden järjestelmien informaation perustasot ovat:

1. *Data*[41]: pienin tiedon yksikkö, jonka kohdesysteemi (solu, ihminen ja tietokone) pystyy tunnistamaan: viestin perusyksikkö (ATGS-pari[42], äänne, kirjain, bitti)[43].
2. *Informaatio*: N kertaa data, jolla on eritysmerkitys[44] systeemilleen: viesti [kodoni[45], sana lausuttuna, sana kirjoitettuna, konekielinen käsky (4–64 bittiä)].
3. *Tietämys*: Informaation muuttuminen informaation systeemissä toiminnaksi. Tässä vaiheessa informaatio (viesti) muuttuu merkitykseksi ja tulkinnaksi systeemissään: Yksi elämän käyttämistä 20 aminohaposta, lausutun sanan luoma mielikuva tai/ja käynnistämä toiminta, kirjoitetun sanan luoma mielikuva tai/ja käynnistämä toiminta ja konekielisen käskyn suorituksen seuraukset.
4. *Informaatiota ja tietämystä suuremmat tasot*, jotka muodostuvat (i) Y kertaa alemmista, metaviesti tai sen korkeammat luokat ja (ii) niiden eritysmerkityksestä, koodauksesta (metaviestin tulkinta, metamerkitys), systeemilleen. Ihmisellä nämä ylemmät tasot voivat olla esimerkiksi ymmärrys, viisaus ja valaistuminen. Ne taas voivat kulminoitua esimerkiksi osaamiseksi, arvoiksi ja elämänkatsomukseksi.

---

[39] Emt. s. 166 - 76.
[40] F. P. Osinga, Science, Strategy and War - The strategic theory of John Boyd, New York: Routledge, 2007 s. 231.
[41] Data on monikkomuoto latinan sanasta datum, ”annettu”. Se sopii tässä mielessä erityisen hyvin tiedon pienimmän yksikön nimeksi. Muut, korkeammat tietoluokat ovat ”luotuja”, dataan tai sen ylempiin luokkiin perustuvia.
[42] Adeniini, tymiini, guaniini tai sytosiini
[43] Data ja siis tieto on pohjimmiltaan ero, ”a difference that makes a difference” (G. Bateson, Steps to an Ecology of Mind, The University of Chicago Press, 2000 (1. painos 1972), s. 272, 381 ja 458), esim. tietokoneessa ero nollan ja ykkösen *välillä.*
[44] Erityismerkitys: Ei 64 satunnaista bittiä tai 5 kirjainta (”koira”) peräkkäin, vaan eritysmerkitys: Tietty spesifi konekielinen käsky tai tietty spesifi suomen kielen aito sana. Tämä on myös emergenssiä: Esim. ”koira” sanana, suomalaisilla aivoilla tulkittuna on enemmän kuin viisi kirjainta yhdessä. Tämä on myös kontekstia, tiedon systeemiriippuvuutta: Muille kuin suomenkielisille ja lukutaitoisille sana ”koira” on periaatteessa vain viisi kirjainta. Lukutaidottomalle ”koira” on ”tahra” paperilla.
[45] Kodoni: Kolme ATGS-paria a’ neljä mahdollisuutta, 4^3= 4 * 4 *4 = 64 mahdollisuutta, jotka koodaavat yhden elämän 20 aminohaposta.

Tämä malli tiedon tasoista on hyvin systeeminen. Siinä ylempi taso muodostuu alemman tason erikoistuneista osista ja uudelle tasolle muodostuu uusia ominaisuuksia. Esimerkiksi kirjaimista k, o, i, r ja a muodostuu suomenkieltä osaavassa ihmisessä mielikuva (tulkinta) tietyn eläinlajin idealisoidusta edustajasta. Jos ”Koira” on viestinnässä käytetty peitekoodi (viesti), se voi käynnistää vaikka kokonaisen sodan. Tämä on informaation kontekstiriippuvuutta: Tulkinta riippuu sitä, mistä systeemistä on kyse. Ihmisellä tulkinta voi olla eri yksilöillä? Mallissa on keskeisesti myös muodonmuutosta, koodausta eli viestimuodon muuttumista toimintamuodoksi tiedon käsittelyn joka vaiheessa.

1.3.2 Tietokoneesta kyberneettisenä toimijana

Nykyaikaan liittyvä mullistus on toisen kyberneettisen toimijan, tietokoneen syntyminen ihmisen rinnalle. Informaatioetiikan professori Luciano Floridi näkee tietokoneen merkityksen jopa vallankumouksellisena. Hänen mukaansa tietokone on neljäs vallankumous Kopernikuksen, Darwinin ja Freudin jälkeen. Kun Kopernikus romutti ihmisen paikan maailmankaikkeuden keskipisteenä, Darwin romutti ihmisen muusta elävästä luonnosta poikkeavana, jumalallisena oliona ja Freud oliona, jonka tietoisuus on selkeää ja täysin läpinäkyvää itsellemme, niin tietokone romuttaa ihmisen ainoana itsenäisenä ja loogisena informaatiotoimijana.[46] Tämä ajatus korostaa tässä artikkelissa esitettyä luokittelua kahdesta kybernettisestä toimijasta, ihmisestä ja tietokoneesta.

Jo aiemmin amerikkalainen fyysikko Heinz Pagels on esittänyt, että tietokone on seuraavan tieteen pitkän ajanjakson tärkein työväline, kuten mikroskooppi ja kaukoputki olivat aiemmin omiin tarkoituksiinsa, mikro- ja makromaailman salojen paljastamiseen. Tietokone avaa ihmiselle monimutkaisuuden maailman ihmisen ymmärtämään muotoon.[47]

1.3.3 Sodankäynnin tyypeistä kybernetiikan valossa

Tässä alaluvussa tarkastellaan vain kyberneettisen luokittelun perusteella luotavissa olevia sodankäynnin tyyppejä ensin siksi, että kyseinen asia oli melko paljon esillä artikkelin vuoden 2003 versiossa ja toiseksi, koska tätä kirjaa tehdessä päätettiin painottaa käsittelyä kyberiin. Kyberneettisen systeeminäkemyksen perusteella (kyber)sodankäynti voidaan jakaa edellisen luvun mukaan ensin kahtia toimintaympäristön mukaan, riippuen siitä missä toiminta tapahtuu: konkreettisessa fyysisessä, aineellisessa, atomeihin perustuvassa ympäristössä vai abstraktissa, virtuaalisessa, tietopohjaisessa, eroihin perustuvassa ympäristössä. Toiseksi kybersodankäynti jakautuu kahtia sen mukaan, kuka tai mikä on toimija: Ihminen tai tietokone[48].

Kolmanneksi kybersodankäynti jakautuu viiteen alaluokkaan sen mukaan mihin toiminta kohdistuu: Ensin (1) ihmisen tai (2) tietokoneen tietoon, siten niiden kyberfyysisiin[49] osiin (3) (4) ja lopuksi (5) kyberneettisen systeemien fyysiseen ympäristöön.

---

[46] L. Floridi, The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford University Press, 2014, loc. 1644–1765.

[47] H. R. Pagels, Dream of Reason – The Computer and the Rise of Sciences of Complexity, New York: Bantam Books, 1989.

[48] Kolmas kyberneettinen järjestelmäluokka on solu, mutta sitä ei käsitellä tässä artikkelissa.

[49] Kyberfyysiset osat tarkoittavat kyberneettisen järjestelmän kyberneettisten osien (sensori, päätöksentekoelin, toimielin, asetusarvo ja palautesilmukat) fyysisiä, todellisia ja atomaarisia rakenteita. Jaol-

Näin saadaan toimintaympäristön, toimijoiden ja kohteiden mukaan 2 * 2 * 5 = yhteensä 20 kybersodankäynnin perustyyppiä. Jakamalla tieto alalajeihin ja systeemi kyberfyysisiin pienempiin osiinsa saadaan 64 kybersodankäynnin tyyppiä. Aihetta on käsitelty laajemmin liitteessä 1.

Kybernetiikkaa ja kyberneettisiä järjestelmiä on hieman laajemmin esitelty sodankäynnin kannalta kirjoittajan artikkelissa ”What Can We Say About Cyberwar Based on Cybernetics?” MpKK:n kirjassa ”The Fog of Cyber Defence”[50] vuodelta 2013.

1.3.4 Sodankäynnistä tasoista kybernetiikan valossa

Tässä alaluvussa tarkastellaan lyhyesti ja alustavasti kybersodankäynnin tasoja ja niiden periaatteellista sisältöä sodankäynnin tavanomaisen luokittelun - taistelutekniikka, taktiikka, operaatiotaito ja strategia - perusteella. Tulkinnassa on käytetty kirjoittajan versiota aiheesta vuodelta 2007 ja 2008. Ne taas perustuvat Quincy Wrightin käsitykseen sodankäynnin historiallisista megavaiheista[51] ja niistä tehtyyn kirjoittajan artikkeliin vuodelta 2008. [52]

Ihmiskunnan pidemmässä evoluutiossa taistelutekniikka oli sodankäynnin vallitseva taso aina noin vuoteen 50.000 eaa. Quincy Wrightin sodankäynnin historian evolutiivisessa mallissa tämä on eläimellistä sodankäyntiä[53]. Sen organisaatiotaso oli suurperhe tai lauma. Se oli sodankäyntinä aseiden käyttötaitoa kaksintaistelun voittamiseen. Koska muita sodankäynnin tasoja ei ollut olemassa, kaksintaistelun voittamiseen sisältyi koko ”sodan” voittaminen ja se vastasi näin myöhempää strategiaa taitona sodan voittamiseen. Vastaavasti on nähtävissä, että kybertaistelutekniikka on kyberaseiden[54] käyttötaitoa kyberkaksintaistelun voittamiseen esim. välillä systeemioperaattori ja hyökkääjä.

Taktiikka oli sodankäynnin uusi taso noin vuodesta 50.000 eaa. Tämä oli primitiivistä sodankäyntiä. Se oli määrällisesti riittävien[55] kaksintaistelujen ja osin erikoistuneiden kaksintaistelijoiden käyttöä paikallisen taistelun voittamiseen. Koska aluksi muita korkeampia sodankäynnin tasoja ei ollut vielä olemassa, taistelun voittaminen merkitsi koko ”sodan” voittamista ja vastasi näin myöhempää strategiaa taitona sodan voittamiseen. Vastaavasti on nähtävissä, että kybertaktiikka syntyy, kun riittävän määrän erikoistuneita kybertaisteluvälineiden käyttäjiä muodostaa uuden kokonaisuuden paikallisen kybertaistelun voittamiseen esim. kahden kilpailevan organisaation välillä.

---

la korostetaan aineellisen todellisuuden jakautumista kyberneettisen järjestelmän aineellisiin osiin ja muuhun aineelliseen todellisuuteen.

[50] S. Ahvenainen, What Can We Say About Cyberwar Based on Cybernetics, kirjassa The Fog of Cyber Defense, Tampere, Juvenes Print Oy, 2013, s. 154 - 168.

[51] Wright 1942.

[52] Ahvenainen 2007, s. 210 ja 225 ja Ahvenainen 2008, s.155 - 6

[53] Q. Wright, A Study of War, The University of Chicago Press, 1942.

[54] Esim. (1) varsinaiset yleiset (esim. Word), (2) puolustukselliset ja (3) hyökkäykselliset tietokoneohjelmat, (1) varsinaiset yleiset, (2) puolustukselliset ja (3) hyökkäykselliset mikropiirit, käyttöjärjestelmät, social engineering jne.

[55] Tässä viitataan emergenssiin, siihen miten määrällinen muutos muuttuu jossain vaiheessa laadulliseksi. Esim. iso määrä kaksintaisteluja taisteluksi, taistelutekniikka taktiikaksi tai iso määrä vetyatomeja tähdeksi.

Taktiikka oli aluksi menneisyydessä heimon sodankäyntitapa. Valtio korvasi heimon suurimpana organisaationa ensimmäisen kerran noin 5000 vuotta sitten, mutta sodankäynti ei muuttunut[56], kuten aikaisempien vaiheiden perusteella olisi pitänyt tapahtua. Sodankäynti jatkui taktisena, paikallisena taisteluna. Sitä nimitetään mm. klassiseksi sotilaalliseksi strategiaksi (classical military strategy)[57]. Se on siis valtiotasoista sodankäyntiä periaatteessa taktiikan alla. Quincy Wrightin luokittelussa tämä oli historiallista sodankäyntiä.

Sodankäyntiin syntyi laajemmin ottaen seuraava taso vasta Napoleonin mukana ja eritysesti USA:n sisällissodassa 1860-luvulla. Uusi taso oli operaatiotaito (operational art). Se tarkoittaa useiden erikoistuneiden taisteluiden yhdistämistä yhdeksi laajan alueen (theater) operaatioiksi. Kyberoperaatio olisi tämän mukaan useiden kybertaisteluiden yhdistämistä laajemman alueen kattavaksi operaatioksi. Tällaisena voitaisiin pitää esim. USA:n 1980-luvun operaatiota Neuvostoliiton lyömiseksi tai USA:n ja Israelin väitettyä operaatiota Olympic Games Irakin ydinaseen valmistuksen hidastamiksi 2010-luvulla.

Mielenkiintoisen poikkeuksen, heikon signaalin operaatitaidon historiassa muodostaa mongolien sodankäynti 1200-luvulla. Se täyttää USA:n armeijan majuri Pittardin mukaan USA:n armeijan 1980-luvun vaatimukset operaatiotaidolle ja operaatioille. Kuvaavaa onkin, että mongolit suorittavat neljässä päivässä hevosilla Euroopan operaatiossaan vuonna 1241 kolmensadan kilometrin etenemisen useaa erillistä reittiä pitkin, juuri saman verran kuin amerikkalaiset Persianlahden 1. sodassa vuonna 1991 helikopterilla ja panssarivaunuilla.[58]

Quincy Wrightin luokittelussa historiallisen sodankäynnin jälkeen syntyi moderni sodankäynti, joka tarkoittaa kirjapainotaidon jälkeistä, tieteellis-teknologista sodankäyntiä 1500-luvulta alkaen.

Strategia perinteisesti tulkittuna (Clausewitz) on sodan yksittäisten taistelujen yhdistelyä ja käyttämistä sodan päämäärien tavoitteluun[59]. Kirjoittajan luokittelussa strategia on oppi sodan voittamiseksi usealla integroidulla operaatiolla. Sotilaallinen kyberstrategia olisi siis oppi kybersodan voittamiseksi usealla integroidulla kyberoperaatiolla. Tässä käsityksessä esim. ”War on Terror” - sodan voittamisessa Irakin operaatio oli yksi useammasta operaatiosta.

[56] Tässä artikkelissa esitetyn mallin mukainen hypoteesi selitykselle on, että uutta viestintäteknologiaa ei ollut käytössä.
[57] J. Pittard, Thirteenth Century Mongol Warfare - Classical Military Strategy or Operational Art, Fort Leavenwort: School od Advansed Military Studies - United States Army Command and General Staff College, 1994. s. 2.
[58] Emt. s. 26.
[59] Clausewitz, 1998 s. 101 ja 312.

1.4 Alustava teoria III: Evoluutio

1.4.1 Evoluutio ja aika

Kolmas alustava teoria ja analyyttinen väline vuoden 2003 artikkelin uudelleenarviointiin on evoluutio. Siitä käsitellään vain seuraavat käsitteet ja nekin hyvin periaatteellisesti: Mikä on evoluutio ja mikä on ajan merkitys evoluutiossa? Nämä ovat samalla artikkelin alatutkimuskysymyksiä ja tämän pääluvun tutkimuskysymyksiä.

Evoluutio on oppi olemassaolon muutoksesta (luonnonlakien perusteella) paitsi biologiaan[60] myös mm. kosmologiaan, kulttuuriin, moraaliin, uskontoon, kieleen, mediaan, teknologiaan, ihmiseen, oikeuteen ja geologiaan liittyvänä historiallisena jatkumona[61] [62]. Evoluutio on sovellutus systeemin ja sen ympäristön vaikutuksesta toisiinsa. Biologisen evoluution ympäristö maapallolla on auringon lämmittämä maapallo ja sen miljoonat eliölajit ja systeeminä kukin laji erikseen. Fysikaalisen evoluution (kosmologian) ympäristö oli alkuräjähdys ja siinä keskeisesti avaruuden laajeneminen ja lämpötilan lasku ja systeeminä aluksi atomia pienemmät osat, sitten atomit ja lopuksi atomeista koostuvat planeetat, tähdet, galaksit ja suuremmat galaksijoukot[63]. Evoluutiossa kaikki perustuu aiempaan, 13,7 miljardin vuoden historialliseen jatkumoon. Ihminenkin on evoluution tuote[64].

Kirjassaan ”Megaevoluutio” professori Eero Paloheimo käsittelee evoluutiota kokonaisvaltaisesti noin 13,7 miljardin vuoden ajalta alkuräjähdyksestä tähtien muodostumisen ja elämän synnyn kautta ihmiseen ja aivoihin sekä niistä edelleen teknologiaan ja avaruuden valloitukseen[65].

Evolutiivisten systeemien ominaisuuksia ovat muun muassa:

1. Olemassaolon systeemien koon kasvaminen.
2. Erikoistuminen.
3. Tiedon välityksen muuttuminen.
4. Kehittyminen aiemmista ja uusien tasojen mahdollisuus.

Seuraavassa näitä evoluution ominaisuuksia käsitellään tarkemmin: Olemassaolon systeemit rakentuvat tasoista, joista alemmat ovat erikoistuneita, suurempien ja monimutkaisempien tasojen rakenneosia[66]. Ihminen on noin 260 erikoistuneen solun ja niistä muodostuvien elimien ja elimistöjen muodostama kokonaisuus[67]. Ihmiseen vai-

---

[60] Biologinen evoluutio on myös esimerkki emergenssin mukaisesti uuden systeemitason mukana syntyvästä uudesta ilmiöstä, siitä miten (kompleksisesta) kemiasta tulee elämä ja myös esimerkki uuden tason uudesta teoriasta (biologia). Sama rakenne voidaan nähdä sodankäynnin evoluutiossa.
[61] Paloheimo, 2002.
[62] I. Hanski, I. Niininiluoto ja I. Hetemäki, Kaikki evoluuutiosta, Talinna: Gaudeamus.
[63] Fysikaalisen evoluution prosessi on siis systeemiteorian mukainen: Osat luovat uusia tasoja, joilla on uusia emergenttejä ominaisuuksia: atomin osat luovat *ympäristön muutoksessa* (lämpötilan lasku) atomin ja atomit luovat tähden. Tähden muodostuminen vetyatomeista on myös esimerkki siitä, että aina ei uuteen tasoon (tähti) tarvita erikoistuneita osia, siis jotain muuta vety-atomien lisäksi. Kuitenkin syntyy emergentti uuden tason ominaisuus, tähti ydinreaktioineen.
[64] Pagels, 1989 s. 48.
[65] Paloheimo, 2002.
[66] Paloheimo, 2002 s.19.
[67] S. Kauffman, At Home in the Universe – The Search of the Laws of Self-Organization and Complexity, Oxford University Press, 1995 s. 24.

kuttavat yksittäisen ihmisen tasorakenteen perusteella fysiikka, kemia ja biologia sekä ihmisen suuremmissa organisaatiosoissa niiden kautta myös psykologia ja sosiologia sekä valtioiden välinen politiikka ja globalisaatio. Uuden tason muodostuminen edellyttää yleensä erikoistumista[68].

Biologiassa uuden, suuremman systeemitason muodostuminen edellyttää tiedon välityksen muuttumista[69]. Yleisesti systeemin muodostuminen erikoistuneista osista edellyttää kommunikointimenetelmää systeemin osien välillä, jotta ne voivat toimia yhdessä[70]. Kommunikointimenetelmä on systeemin ylätasolle keskeinen edellytys osien kontrolliin.

Evolutiiviset systeemit kehittyvät aiemmista ja oleviin tasoihin sisältyy uusien tasojen mahdollisuus.[71] ”Kehittyvät aiemmista” sisältää ajatuksen, että mitään ei synny tyhjästä. Looginen jatkoajatus tästä on muun muassa se, että tietoisuus on aivojen emergentti ominaisuus, ei aineen ulkopuolelta tuleva erillinen ilmiö.

1.4.2 Sodankäynnistä evoluution valossa

Tässä luvussa käsitellään vain sodankäynnin historian kehitystä evoluution kautta tavoitteena saada pohjaa verkkosodan historian arvioinnille. Professori Quincy Wrightin johtaman Chicagon yliopiston laajan vuosien 1926–1942 tutkimusprojektin kaksiosainen ja 1552-sivuinen raportti ”A Study of War” sisältää sodankäynnin systeemisen ja evolutiivisen mallin[72] [73].

Wrightin tutkimusprojektin esittämän sodankäynnin historian mukaan sodankäynti ja ihmiskunnan evoluution megavaiheet voidaan jakaa historiallisesti neljään päävaiheeseen. Nämä päävaiheet ovat olleet eläimellinen vaihe ennen kieltä, primitiivinen vaihe kielen syntymisen jälkeen, historiallinen vaihe kirjoitustaidon syntymisen jälkeen ja moderni vaihe kirjapainotaidon syntymisen jälkeen. Näitä vastaavat organisaation koot ovat suurperhe (lauma), heimo, valtio ja kulttuuri.[74]

Wrightin mallissa teknologisista prosesseista nousevat kauppa ja teknologia näyttäisivät ennakoivan poliittista ja organisatorista kehitystä[75]. Kauppa on keskeinen tekijä myös professorien Buzanin ja Littlen teoksessa “International Systems in World History – Remaking the Study of International Relations”[76] sekä professori Robert K. Loganin teoksessa ”The Extended Mind: The Emergence of Language, the Human Mind and Culture”[77]. Nykyaikaa tarkastellessa kaupan ja teknologian muutos näyttävät selviltä: globaali vapaakauppa, erityisesti konttiliikenne[78] (valtamerillä) ja globaali

---

[68] Turchin, 1977 s. 56.
[69] Smith & Szathmary, 1995 s.12 - 3.
[70] Wiener, 1948 s. 156 ja 160 - 1.
[71] 1600-luvun kuuluisa filosofi Rene Descartes oli siis väärässä tässä valitun tulkinnan mukaan esittäessään mielen ja ruumiin erillisyyttä, dualismia.
[72] Wright 1942.
[73] Ahvenainen, 2008, s. 134 - 159.
[74] Wright, 1942 s. 29 - 33 ja 37.
[75] Q. Wright, A Study of War, Midway Reprint toim., The University of Chicago Press, 1983 s. 351 - 2
[76] Buzan & Little, 2000 s. 93 - 94, 154 - 156, 177, 234.
[77] R. K. Logan, The Extended Mind: The Emergence of Language, the Human Mind and Culture, University of Toronto Press, 2007 s. 58 - 60.
[78] M. Levinson, The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger, Princeton University Press. Kindle Edition.

tietoteknologia, bioteknologia jne. Odotettavissa on siis Wrightin perusteella poliittisia ja organisatorisia muutoksia, uusia rakenteita ja systeemiteorian mukaan uusia emergenttejä ilmiöitä uudelle globaalille tasolle.

Wright ei esitä em. asioita teoriana, eikä edes mallina, vaan kuvaa oman tutkimusprojektinsa lopputulosta, näkemystä sodankäynnin kehityksestä. Käytännössä kyse on ihmiskunnan evoluution systeemisestä teoriasta paria vuosikymmentä ennen varsinaisten yleisen systeemiteorian ilmaantumista.

Systeemiteorian kannalta mielenkiintoinen on Wrightin tulkinta sodankäynnin tasojen pääselitysmallien muuttumisesta sodankäynnin tasojen kasvaessa. Wright esittää ne seuraavasti: eläimellinen lauma (vaistot), primitiivinen heimo (sosiologia), historiallinen valtio (politiikka ja lait) sekä moderni kulttuuri (tiede ja teknologia) [79] [80]. Wright toteaa myös itse, että kyseiset muutokset näissä sodankäynnin vaiheissa olivat niin suuria, että kyse ei ollut evoluutiosta, vaan systeemitason muutoksista (emergence) sodankäynnissä[81].

Selvemmäksi asia olisi tullut, jos Wright olisi saanut sidottua kyseiset tasomuutokset taistelutekniikan, taktiikan, operaatiotaidon ja strategian kehitykseen. Asiaan vaikutti varmaan osaltaan Wrightin ”ympäristö”, eli hän oli lakitieteen professori.

Taistelutekniikkaan, taktiikkaan, operaatiotaitoon ja strategiaan liittyvä rakennelma viittaakin edellä esitettyyn vastaavaan ihmiskunnan evoluution tasoihin; vaeltava lauma (taistelutekniikka), heimo (taktiikka), valtio (klassinen sotilasstrategia[82]), kulttuuri (operaatiotaito ja strategia[83]) ja globaali ihmiskunta (strateginen kommunikaatio).[84] Aihe vaatii tarkempaa tutkimusta.

Tasomuutoksen välttämätön edellytys on Wrightin mallissa uusi kommunikaatiotekniikka: puhe, kirjoitustaito ja kirjapainotaito ja globaali tietokoneteknologia[85]. Kybernetiikankin mukaan informaatio sitoo systeemin osat yhteen, kokonaisuudeksi [86]. Edellä mainitussa sodankäynnin evoluutiossa on siis osaltaan kyse siitä, mitä kommunikaatiomenetelmiä on ollut olemassa aiempien sodankäynnin erikoistuneiden kokonaisuuksien yhdistämiseen uudeksi kokonaisuudeksi. Jatkokysymyksiä syntyy mm. siitä millä uusilla informaatiovälineellä taistelutekniikasta tuli taktiikkaa tai klassisesta sotilasstrategiasta operaatiotaitoa?

---

[79] Wright, 1942 s. vii.
[80] A. Roland, ”Technology and War,” 1997. [Online]. Available: http://www.unc.edu/depts/ diplomat/ AD_Issues/amdipl_4/roland.html. [Haettu 12 Kesäkuu 2010].
[81] Wright, 1942 s. 27.
[82] Tämä on merkittävin poikkeama. Valtion sodankäynti oli edelleen tuhansia vuosia klassista sotilasstrategiaa, yhden pisteen taistelua aina operaatiotaidon syntymiseen asti. Ainoa poikkeus lienee mongolien sodankäynti 1200-luvulla (Pittard, 1994).
[83] Strategia ymmärrettynä useamman erikoistuneen operaation muodostamana kokonaisuutena, systeeminä. Sodankäynnin voittamiseen liittyvä strategia sisältyy sodankäynnin aiemmissa tasoissa kyseiseen tason rakenteeseen.
[84] S. Ahvenainen, Kyber ja sodankäynnin 5. megavaihe, [Online]. Available: http://www.kolumbus.fi/ sakari.ahvenainen/Kyber_ja_5_Megavaihe_Julk_2013.pdf. [Haettu 1 Tammikuu 2014] 2013 s. 7 - 14
[85] Wright ei luonnollisestikaan käsittele vuoden 1942 teoksessaan globaalia tietokoneteknologiaa. Se on kirjoittajan käsittelemä ennustus Wrightin mallista (Ahvenainen, 2008, s. 134 - 159).
[86] Wiener, 1948 s. 156 ja 160 - 1.

Mielenkiintoinen on myös systeemitasojen tulkinta Wrightin mallin perusteella. Aiemmissa vaiheissa heimo, valtio ja kulttuuri ovat olleet uudet systeemiset kokonaisuudet. Jos siis viidennessä vaiheessa systeemikoko edelleen kasvaa globaaliksi, se merkitsee, että tämä taso on kokonaissysteemi, välttämätön kokonaisuus toiminnalle. Tämän jatkojohtopäätökset ovat taas mielenkiintoisia mm. huoltovarmuuden, sotilaallisen liittoutumisen ja yleensä globaalin työjaon kannalta. Yksinkertaistaen voidaan tähän ajatukseen perustuen sanoa, että jos ei ole globaalissa systeemissä integroitu osa (Venäjä, Pohjois-Korea), on häviäjä, menneen ajan ilmiö.

1.5 Virheiden karsinta

Tässä pääluvussa käsitellään lähinnä vuoden 2003 artikkelia tässä esitettyjen alustavien teorioiden – systeemiteoria, kybernetiikka ja evoluutio – kannalta ja siitä näkökulmasta, mitä virheitä tai puutteita vuoden 2003 versiossa oli edellä mainittujen näkökulmien perusteella. Seuraavassa pääluvussa ”Johtopäätöksiä” esitetään, miten vuoden 2003 johtopäätöksiä on korjattava tai täydennettävä edellä mainittujen uusien näkökulmien perusteella. Aluksi kuitenkin muutama sana käytetystä metodista.

1.5.1 Käytetystä metodista

Käytetty metodi tässä artikkelissa oli Popperin evolutiivinen induktio 1970-luvulta. Popperin idean on esittänyt jo vuonna 1919 maailmankuulu fyysikko Albert Einstein, eikä induktio ei ole hänen mielestä ainoa tieteen tekemisen tapa. Tässä mielessä tämän artikkelin pohjaksi valittu metodi on vain yksi muiden joukossa.

Einstein pitää induktiota ja deduktiota ja erityisesti intuitiota merkittävänä tieteen teorioiden luomis- ja löytämiskeinona:

> ”Olennaisen tajuaminen suuresta tosiasiajoukosta johtaa tutkijan yhden tai useamman peruslain laatimiseen. Tätä luovaa prosessia seuraa lähinnä käsityötä muistuttava vaihe, eli peruslakien seurausten päättely tai matemaattinen johtaminen sekä niiden vertaaminen kokemukseen.”[87]

Einsteinin vuonna 1919 hahmottama prosessi muistuttaa selvästi aiemmin esitettyä systeemin rakennetta ja emergenssiä: Ensin on suuri tosiasiajoukko ja sitten sen ”hahmo” tiivistyy yleiseksi ja yksinkertaiseksi laiksi. Prosessi on myös merkittävä esimerkki tiedon vähentämisen oleellisuudesta, jota tietotutkija Jan Kåhre pitää kehittämänsä matemaattisen informaatioteorian yhtenä merkittävänä kulmakivenä[88] ja fyysikko Kari Enqvist fysiikan kulmakivenä[89].

Vaikka muodollisesti tässä artikkelissa on kolme alustavaa teoriaa, ne ovat kaikki systeemiteoriaa tai sen sovellutuksia. Jos aihe vaatii tästä näkökulmasta jatkotutkimuksia, olisi hyvä löytää uusia teorioita asian tarkasteluun.

---

[87] A. Fölsing, Albert Einstein – Elämänkerta, Kolmas painos toim., Helsinki: Terra Cognita, 2005. s. 417.
[88] J. Kåhre, The Mathematical Theory of Information, Kluwer Academic Publisher, 2002 s. 71 ja 364 - 5.
[89] Enqvist, 2007. s. 209, 326 ja 340.

1.5.2 Systeemiteoria virheiden karsinnan lähteenä

Luvussa 3.1 esitettyjen systeemiteorian perusilmiöiden ja niiden luvussa 3.2. esitettyjen sodankäynnin sovellutusten perustella vuoden 2003 artikkelin rakenteesta ja johtopäätöksistä ei löytynyt merkittävämpiä korjaus- tai päivitystarpeita lähinnä siitä syystä, että vuoden 2003 artikkelissa aihetta ei käsitelty systeemiteorian kannalta eikä siinä ollut systeemiteoriaan muutenkaan liittyviä tarkasteluja.

1.5.3 Kybernetiikka virheiden karsinnan lähteenä

Luvussa 4.1 esitettyjen kybernetiikan perusilmiöiden ja niiden luvussa 4.2. esitettyjen sodankäynnin sovellutusten perusteella vuoden 2003 artikkelin rakenteesta ja johtopäätöksistä voidaan löytää seuraavat virheet tai täsmennystarpeet:

Kybernetiikan käyttö täsmensi ensin toimijanäkemystä. Vuoden 2003 vastaavassa artikkelissa esitettiin, että toimijat olisivat ihminen ja ohjelmisto. Kyberneettisesti tulkittuna ne ovat kuitenkin ihminen ja tietokone, kaksi fyysistä kyberneettistä systeemiä, toimijaa. Ihmisessäkin on ”ohjelma”. Ja toisaalta ihminen ja tietokone ovat molemmat järjestynyttä fyysistä ainetta, joka pystyy tunnistamaan ja käsittelemään tietoa, abstrakteja eroja.[90]

Toiseksi kybernetiikan käyttö täsmensi ja systematisoi tietoperusteisen sodankäynnin muotoja. Vuoden 2003 muodot olivat lähinnä alan asiantuntijoiden esittämiä luetteloita ja kirjoittajan alustavia ajatuksia, joihin ei liittynyt vielä kybernetiikan perusilmiöiden tuntemusta. Kahdeksan kyber – tai tietointensiivisen sodankäynnin lajia on laajentunut 20 perustyypiksi ja edelleen tarkemmalla jaolla 64 perustyypiksi. Uutta jaottelua on käsitelty tarkemmin alla johtopäätösluvussa.

1.5.4 Evoluutio virheiden karsinnan lähteenä

Luvussa 5.1 esitettyjen evoluution perusilmiöiden ja niiden luvussa 5.2. esitettyjen sodankäynnin sovellutusten perusteella vuoden 2003 artikkelin rakenteesta ja johtopäätöksistä voidaan löytää seuraavat virheet tai täsmennystarpeet:

Evoluution idean mukaisesti kaikella olevalla ja olleella on historia, eli mitään ei synny tyhjästä. Tämän seurauksena on mm. se, että systeemeillä on muutoksia, ensin menneisyys, esiasteita ja toiseksi myös aina tulevaisuus, ympäristön sallimissa puitteissa jopa metatasoja[91].

Evoluution idea laajentaa heti verkkosodan historiaa ja samalla käsitteen syntyä kauemmaksi historiaan, periaatteessa olemassaolon osalta alkuräjähdykseen asti 13,7 miljardin vuoden päähän. Sodankäynnin osalta verkkosodan historia on edellisen perusteella myös osa sodankäynnin yleistä historiaa ja ulottuu siis periaatteessa sodankäynnin syntyhetkeen. Informaatiosodankäynninkin osalta verkkosodan historia ulottuu hyvinkin toisen maailmansodan aikaiseen elektroniseen sodankäyntiin ja sa-

[90] Tässä olisi syvällisemmässä ja pidemmässä analyysissa ollut mahdollisuus ongelmiin, koska oli sotkettu kaksi eri tason ilmiötä, systeemi (ihminen) ja systeemin osa (päätöksentekoelimen prosessitieto, ohjelma). Eritasoisten ilmiöiden sekoittaminen toisiinsa on taas keskeinen virheiden ja paradoksien lähde. Kartta ei ole maasto eikä nimi nimen kohde eikä luku ole määrä (G. Bateson, Mind and Nature, Hampton Press, Inc, 2002 s. 27 - 8 ja 45 - 9).

[91] Entropian, eli hajeen mukaan aina voi tietysti tapahtua toisena vaihtoehtona systeemin ”huononeminen”, epäjärjestyksen kasvaminen.

lakirjoituksen murtamiseen[92]. Ja jos sinne, niin samalla salakirjoitukseen ja sen murtamiseen yleensä, siis jopa kahdentuhannen[93] vuoden päähän.

Verkkosodan esiaste ei ollut 1990-luvun informaatiosodankäynti, Persianlahden ensimmäinen sota vuonna 1991, koska se ei ollut ensimmäinen informaatiosodankäynnin doktriinia toteuttava sota[94]. Ensimmäinen informaatiosodankäynnin doktriinia toteuttava sota oli Kylmän Sodan voittaminen, Neuvostoliiton kaataminen tai ainakin kaatamisen avustaminen strategisella ja salaisella informaatiooperaatiolla[95]. Tämän hetken hypeen, kyberiin liittyen on merkittävää, että tietokoneteknologia ja ohjelmistot olivat keskeisessä roolissa kyseisessä 1980-luvun operaatiossa[96].

Kylmän sodan voittaminen on myös keskeinen esimerkki kiinalaisen sotilasstrategin Sunzin toteamuksesta, että sodankäynnin huippu ei ole sadan taistelun voittaminen sadasta taistelusta, vaan sodan voittaminen ilman taistelua[97].

Länsimainen sotilasstrategi Karl von Clausewitz toteaa edellisestä poiketen, että ”sodan … tarkoituksena on pakottaa vastustaja noudattamaan meidän tahtoamme” ja että keino siihen on fyysinen väkivalta. Käsitteellisesti sotilaallisen toiminnan tavoite on tehdä vastustaja puolustuskyvyttömäksi.[98]

Käsitteellisen tavoitteen saavuttaminen voi olla mahdollista muutenkin kuin väkivallalla, esimerkiksi tuhoamalla vastustajan sotavoiman ytimen muulla tavalla kuin asevoiminen suoralla tuhoamisella fyysistä väkivaltaa käyttämällä. Tämä voi tapahtua informaatioaikakaudella tuhoamalla vastustajan asevoimien ja yhteiskunnan informaatioteknologinen pohja kuten kylmässä sodassa tapahtui.

Toiseen suuntaan, tulevaisuuteen tarkasteltuna evoluution idea tarkoittaa uusia asioita, eli sitä, että vuoden 2003 jälkeen on voinut syntyä uusia asioita, uutta verkkosodan historiaa. Näin onkin tapahtunut, jopa kolmea[99] kautta, ensin vaikutusperusteiset operaatiot (EBO) ja toiseksi strateginen kommunikaatio tai kommunikaation synkronointi ja kolmantena operaation kehittäminen (Operational Design, OD).

Komentajakapteeri Janne Iivonen on diplomityössään ”Vaikutusperusteiset konseptit: EBO-, EBAO-, SOD- ja CA-käsiteanalyysi” tutkinut vaikutuskeskeisen sodankäynnin käsitettä ja myös sen mahdollista seuraajaa:

---

[92] Enigma: Saksan salakirjoituksen murtaminen. Purple: Japanin salakirjoituksen murtaminen. Suomessa Neuvostoliiton salakirjoituksen murtaminen.

[93] Roomalaisen Gaius Julius Caesarin keksimää salakirjoitusta pidetään yhtenä ensimmäisistä salakirjoituksesta (Caesar-menetelmä).

[94] A. D. Campen (Ed.), The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War, AFCEA International Press, 1992

[95] T. C. Reed, At the Abyss - An Insider’s History of the Cold War, New York: Ballantine Books, 2004.

[96] Emt. s. 268.

[97] Sunzi, Sodankäynnin taito, Tampere: Gaudeamus Helsinki University Press, 2005 (alunperin n. 500 e.a.a.) s. 73.

[98] Clausewitz, 1998 s. 15 - 6.

[99] Vuoden 2003 artikkelissa päiviteltiin sitä, miten paljon ”historiaa” oli saatu mahtumaan kymmeneen vuoteen. Kirjoittaja kuitenkin totesi keskeisenä johtopäätöksenä, että ”…verkkosodan käsite ja siihen liittyvä toiminta kehittyvät vielä merkittävästi eteenpäin seuraavina vuosikymmeninä” (Ahvenainen, 2003, s. 12 ja 89 - 90).

> ”Verkostokeskeinen sodankäynti ja erityisesti sen mahdollistama yhteinen tilannekuva toimivat vaikutusperusteisten konseptien mahdollistajana ja niiden ydinprosessien tukena erityisesti, kun asiaa tarkastellaan teknologiselta kannalta”[100].

Majuri Kaarel Mäesalu (Viron Puolustusvoimat) on tutkinut EBAO/EBO keskustelua Yhdysvaltojen asevoimissa:

> ”Effects-Based Operations (EBO) sekä siitä kehittynyt Effects-Based Approach to Operations ovat nykyajan operatiivisen sekä strategisen tason suunnittelun avainkäsitteitä Natossa ja useissa sen kumppanivaltioissa. Konsepti on levinnyt maailmalle alun perin Yhdysvaltojen asevoimista, mutta viimeaikaisten kokemusten perusteella Yhdysvallat on kuitenkin luopumassa konseptista.”[101]

> ”Yhteisoperaatioiden tasolla tullaan EBO:n sijaan kehittämään Operational Design konseptia, jossa otetaan esimerkkiä maavoimilta sekä merijalkaväeltä. Operational Design on filosofinen systemaattinen analyysimenetelmä, joka pyrkii koko operaation ajan tarkistamaan yhtymän keskittymistä oikeaan ongelmanratkaisuun. Operational Design mahdollistaa komentajakeskeisen lähestymistavan ongelmiin ja sopii monimutkaisia avoimia järjestelmiä vastaan. Operational Design mahdollistaa sotataidollisen ajattelun ja sopii paremmin ennustamattomien ja yllättävien tilanteiden ratkaisemiseen.”[102]

Ongelma ei ehkä ole niinkään ”monimutkaiset avoimet järjestelmät”, vaan se, että ne ovat dynaamisesti muuttuvia, itsensä viittaavia epälineaarisia järjestelmiä. Kun monimutkainen järjestelmä ongelmana on ratkaistu, se on muuttunut niin paljon, että tarvitaan uusi ratkaisu. Professori Markku Sotarauta kutsui näitä ongelmia väitöskirjassaan vuodelta 1996 ”ilkeiksi”, ja piti niitä aikakauden metaforina[103]. Operational Design on siis Sotaraudan jo 1990-luvun puolivälissä mainitsemaa jatkuvaa ongelmanratkaisua.

Strategisen kommunikaation asemaa yhdestä näkökulmasta kuvaa valtiotieteen tohtorin ja everstiluutnantti Torsti Sirenin toimittaman kirjan ”Strateginen kommunikaatio ja informaatio-operaatiot 2030” ensimmäisen luvun otsikko ”Informaatiosodankäynnistä kokonaisvaltaiseen strategiseen kommunikaatioon”[104]. Siren määrittelee edellä mainitussa kirjassa strategisen kommunikaation seuraavasti:

> ”Strategisella kommunikaatiolla tarkoitetaan sitä kokonaisvaltaista lähestymistapaa, jolla viranomaisyhteistyön, diplomatian, julkissuhteiden hoitamisen, informaatio-operaatioiden sekä kauppa- että sotilaspolitiikan keinoin edistetään

---

[100] J. Iivonen, Vaikutusperusteiset konseptit: EBO-, EBAO-, SOD- ja CA-käsiteanalyysi, Helsinki: Maanpuolustuskorkeakoulu, 2009 s. 2.
[101] K. Mäesalu, EBAO/EBO keskustelu Yhdysvaltojen asevoimissa, Helsinki: Maanpuolustuskorkeakoulu, 2010 s. ii.
[102] Emt. s. ii.
[103] M. Sotarauta, Kohti epäselvyyden hallintaa: Pehmeä strategia 2000-luvun alun suunnittelun lähtökohtana, Acta Futura Fennica No 6, Finnpublishers, Jyväskylä. 1996.
[104] T. Siren, Toim., Strateginen kommunikaatio ja informaatio-operaatiot 2030, Helsinki: Maanpuolustuskorkeakoulu - Johtamisen ja sotilaspedagokiikan laitos, 2011.

> Suomen kansallisia etuja osana läntistä arvomaailmaa sekä kotimaassa, että ulkomailla kaikissa valmiustiloissa. Strateginen kommunikaatio on luonteeltaan prosessi, jossa samaa perusviestiä (narrative) pyritään *proaktiivisesti* levittämään …"[105]

Sotatieteen tohtori Saara Jantunen toteaa väitöskirjansa "Strategic Communication: practice, ideology and dissonance" (2013) johtopäätöksenä, että:

> "Johtamisen näkökulmasta strateginen kommunikaatio on ennen kaikkea johtamismalli, jonka avulla organisaatio määrittelee itsensä, päämääränsä ja legitimiteettinsä. Strateginen kommunikaatio ei ole vain työkalu julkissuhteiden ja informaatio-operaatioiden toimeenpanossa, vaan sillä on tärkeä rooli organisaation[106] jäsenten hallinnassa ja kontrolloinnissa. Konseptin tämänhetkinen kehityssuunta viestii siitä, että sitä viedään kohti vielä raskaampia hallinnan keinoja."[107]

Jantunen siis liittää strategisen kommunikaation "ei vain" informaatiosodankäyntiin, vaan myös verkostojen hallintaan ja johtamiseen. Lisäksi hän viittaa hallintaan, joka on uusien viestijärjestelmien, tässä tapauksessa globaalin informaatioteknologian keskeinen tehtävä, kuten aiemmin on tässä artikkelissa esitetty. Tämä viittaa vahvasti vuonna 2013 alkaneeseen NSA-skandaaliin ja tietovuotaja Edward Snowdeniin.[108]

1.5.5 Muita havaintoja

Aiemmin todettiin, että uuden tason muodostuminen edellyttää erikoistumista[109]. Aiemmin todettiin myös, että alkuräjähdyksen jälkeen tähtien muodostuminen vetyatomeista[110] ei sisällä erikoistumista, mutta luo metasysteemin, tähden, kun vetyatomeja on tarpeeksi samassa tilassa. Tämä romuttaa ko. periaatteen ja muuttaa sen siis sellaiseksi, että metataso voi edellyttää osiensa erikoistumista, mutta ei välttämättä.

Vuoden 2003 artikkelin verkkosodan "historian" ajanjakson kattoi noin vuodet 1991–2003. Tässä päivityksessä kyseisen ajanjakson asioita ei ole arvioitu juurikaan uudelleen johtuen ensin rajallisista resursseista ja toiseksi siitä, että uusi näkökulma, alustavat teoriat, tuntui erityisen lupaavalta ja tarjosi työtä sekä myöhemmin riittävästi uusia lupaavia havaintoja. Kyseisen ajanjakson tarkempi analyysi jää siis jatkotutkimuksiin.

Mielenkiintoista on myös Wrightin toteamus, että sodankäynnin muutokset sodankäynnin megavaiheissa olivat niin suuria, että kyse ei ollut evoluutiosta, vaan systeemitason muutoksista (emergence) sodankäynnissä[111]. Tässä Wright ei siis ole

---

[105] S. Jantunen, Strategic Communication: practice, ideology and dissonance, Helsinki: National Defence University, 2013 s. 4.
[106] Englannin kielisessä tiivistelmässä organisaatio on käännetty "inter-organization", organisaatioiden väliseksi, verkoksi? (S. Jantunen, 2013 s. i).
[107] Jantunen, 2013 s. ii.
[108] The Guardian: Edward Snowden (http://www.theguardian.com/world/edward-snowden) (29.8.2014)
[109] Turchin, 1977 s. 56.
[110] Alkuräjähdyksessä muodostui vetyatomien myös lisäksi pienemmät määrät heliumia ja litiumia. Tällä ei ole kuitenkaan merkitystä tähden muodostumiseen ja ydinreaktioiden käynnistymiseen, pelkkä "erittäin" suuri määrä vetyatomeja riittää.
[111] Wright, 1942 s. 27.

oivaltanut (?), että systeemitason muutokset ovat oleellinen, ehkä jopa oleellisin osa (kaikenlaista) evoluutiota ja emergenssi on ko. muutosten moottori.

1.6 Johtopäätökset

Artikkelin vuoden 2003 version ja yllä esitettyjen vuoden 2014 täsmennysten osalta voidaan todeta tiivistetysti[112] seuraavaa:

1. Vuoden 2003 versiosta puuttui tieteen kannalta teoria (teoriat)[113]
2. Kybernetiikka uutena teoriana systematisoi aiheen käsittelyä
3. Verkkosodan historia ulottuu kauemmaksi kuin 2003 esitettiin
4. Verkkosota on kehittynyt jopa käsitteellisesti merkittävästi vuosien 2003–2014 välissä
5. Kylmä Sota oli lähihistoriassa oleva merkittävä esimerkki sodan voittamisesta ilman taistelua ja verkkosodan jatkon kannalta erityisen tärkeä asia
6. Kybersodankäynnin muotoja on uuden, systemaattisen jaottelun mukaan aiemman kahdeksan sijasta 20
7. Verkkosodan käsitteen ajallisen kehittymisen merkkipaalut ovat päivittyneet viidestä yhteentoista
8. Venäläiset ovat ehkä käyttäneet oman informaatiosodankäynnin teoriapohjana kybernetiikkaa
9. Kyberulottuvuus (cyberspace) on laajentunut kybernetiikalla tulkittuna tietokoneverkoista myös ihmisaivoihin ja niiden verkkoihin
10. Globaali taso uutena toiminnan tasona on suuri muutos
11. Sodankäynnin tyyppien lukumäärä on kasvanut 333 prosenttia tietokoneen tultua sodankäynnin ”täysivaltaiseksi” ja keskeiseksi toimijaksi
12. Tämän typpinen jatkotarkastelu on monessa mielessä tärkeä. Alla näitä kohtia on käsitelty tarkemmin.

Vuoden 2003 versiosta puuttui tieteen kannalta teoria (teoriat). Se perustui lähinnä ulkomaalaisiin informaatiosodankäynnin (vast.) asiantuntijoiden kirjoituksiin. Nyt teorioita on löytynyt neljä: (1) systeemiteoria ja sen sovellutuksena (2) kybernetiikka ja (3) evoluutio ja edelleen systeemiteorian ja evoluution sovellutuksena (4) Quincy Wright ja sodankäynnin systeeminen ja evolutiivinen historia.

Kybernetiikka uutena teoriana systematisoi aiheen käsittelyä. Kybernetiikka systematisoi kybersodankäynnin tai tietointensiivisen sodankäynnin käsittelyn ja laajentaa sodankäynnin tietoulottuvuuden käsittelyä kyberneettiseen, tietoa käsittelevän järjestelmään. Vuoden 2003 artikkelissa ”pyöritään asian ympärillä”, mutta (hyvä) teoria puuttuu. Oikeilla jäljillä kuitenkin oltiin.

---

[112] Tämän tyyppinen luettelo voi tuntua jostakusta ”ei-hyvältä”. Kirjoittajan omaksumassa ajattelussa tässä on kuitenkin kyse matemaattisen informaatioteorian (Kåhre, 2002) mukaisesta keskeisestä periaatteesta, informaation hukkaamisesta, tässä tapauksessa ainakin neljällä tasolla. Ensimmäisen tason muodostavat artikkelin viitatut lähteet, toisen tason artikkeli, kolmannen tason artikkelin johtopäätökset ja neljännen tason johtopäätösten luettelo, otsikot. Artikkelin prosessi on myös aina systeeminen siinä mielessä, että artikkelin tietona uudet johtopäätökset on helppo tulkita uuden systeemitason emergenteiksi ominaisuuksiksi. Viitatut lähteet sisältävät viittauksia niiden lähteisiin, joten parhaimmillaan ja periaatteessa tieteellinen artikkeli liittyy lopulta kaikkeen aiemmin kirjoitettuun.

[113] Artikkelin vuoden 2003 versiossa esitettiin, jopa laajasti, uusi vuoden 2000 vaihteen verkkoteoria, skaalavapaa verkko (Ahvenainen, 2003 s.34 - 8). Se ei kuitenkaan liittynyt artikkelin kannalta keskeiseen verkkosodan käsitteen *historian* tutkimukseen, vaan itse käsitteen perusteisiin.

Puuttuu kybernetiikka, joka on:

1. Oppi tietoa käsittelevistä konemaisista tai inhimillistä järjestelmistä tai
2. tiede erilaisten järjestelmien säätö- ja viestintätapahtumia tutkimiseen.

Kybernetiikka on kuitenkin vain yksi, joskin tämän kirjoituksen perusteella merkittävä teoria verkkosodan ja tietointensiivisen sodankäynnin yleiseenkin käsittelyyn. Oppi edellisestä on tärkeä mm. Karl R. Popperin esittämän idean ”Evolutiivinen induktio” kannalta. Sen mukaan tieteen tekemisen pohjalla alustavina teorioina on oltava parhaat ja testatuimmat teoriat. Vuoden 2003 artikkelissa käytettiin vielä Popperia tuntematta kolmea näkökulmaa, joista yksikään ei ollut varsinainen teoria. Mitä tämä tarkoittaa sodankäynnin tutkimiselle? Mitkä ovat sodankäynnin parhaat ja testatuimmat teoriat? Ne ovat toki vain ajattelun apuvälineitä, kuten jo Clausewitz totesi[114] ja tässäkin kirjoituksessa esiintyy EBO:n ja OD:n välisenä merkittävänä erona. Sodankäynti ei ole tiedettä (science), korkeintaan taitoa ja tiedettä (art and science). Onko evolutiivinen induktio niin voimakas malli, että sitä pitäisi opettaa yhtenä perusmallina mm. MpKK:ssa sodankäynnin tutkimiseen?

Verkkosodan historia ulottuu kauemmaksi kuin 2003 esitettiin. Historia ulottuu ainakin 1980-luvulle, Neuvostoliiton kaatamiseen tai sen kaatamisen edistämiseen ei-sotilaallisella strategisella informaatio-operaatiolla[115]. Evoluution ideaa soveltaen on selvää, että se ulottuu vielä kauemmaksi. Myös tämän artikkelin sisältävän vuoden 2003 kirjan majurien Jari Rantapelkonen ja Jukka-Pekka Virtanen kritiikkipuheenvuorossa esitettiin, että jopa suomalaisessa sotilaallisessa ajattelussa verkkosodan idean sovellutuksia löytyy viestitoiminnasta kauempaa menneisyydessä [116]. Tähän liittyen todettakoon, että sekä suomalainen että venäläinen verkkosodan historia ja käsitteen kehittyminen jäävät edelleen mahdollisten jatkotutkimusten varaan. Uudet verkkosodan historialliset vaiheet on esitetty alla vastaavassa kohdassa.

Verkkosota on kehittynyt jopa käsitteellisesti merkittävästi vuosien 2003–2014 välissä, ensin vaikutuskeskeisen sodankäynnin, toiseksi strategisen kommunikaation ja kolmanneksi ”Operational Design” termin kautta. Tämä kuvaa kirjoittajan vuoden 2003 artikkelin visiota tämän alan nopeasta kehityksestä myös tulevaisuudessa. Kehitys jatkunee samanlaisena ja edellyttää siis alan aktiivista ja hyvin resursoitua tutkimusta. Nopea kehitys on ilmiönä aikakauden yleinen trendi ja kaikkeen vaikuttava tekijä[117].

Strateginen kommunikaatio viittaa vahvasti Quincy Wrightin esittämiin sodankäynnin suuriin evolutiivisiin vaiheisiin, joissa viides vaihe on ennustus uuden tietokoneteknologian mahdollistamana globaalina vaikuttamisena, siis strategisena kommunikaationa[118]. Jos näin on, asialla on erityisen suuri merkitys sen takia, että kyse on suuresta sodankäynnin muutoksesta, uudesta ja ensi kertaa myös poikkeavasta tasosta.

[114] Clausewitz, 1998 s. 29 ja 273.
[115] Reed, 2004.
[116] Piiroinen, Toim., 2003 s. 96.
[117] Ahvenainen, 2008, s. 153.
[118] Emt. 134 -159.

Poikkeava se on ensin siinä mielessä, että globaalilla ihmiskunnalla ei ole maapallolla laajenemismahdollisuuksia suuremmaksi kokonaisuudeksi ja toiseksi siinä mielessä, että kun globaaleja ihmiskuntia on määritelmän mukaan maapallolla vain yksi, tällä tasolla ei ole sodankäynnin vaatimaan kahta, vastakkaiset intressit omaavaa toimijaa. Tällä tasolla ei siis ole sodankäyntiä (sic!).

Kylmä sota oli lähihistoriassa oleva merkittävä esimerkki sodan voittamisesta ilman taistelua ja verkkosodan jatkon kannalta erityisen tärkeä asia. Kylmän sodan voittamisen paljastuminen informaatiosodankäynnin ensimmäiseksi sovellutukseksi on merkittävä havainto. Vielä merkittävämpi havainnosta tulee sitä kautta, että kylmä sota voitettiin muilla keinoilla kuin asevoimilla, väkivallalla. Jos hyväksyy kylmän sodan ja tulkinnan sen voittamisesta muilla keinoin, hyväksyy samalla sen, että sodan voittaminen on mahdollista muutenkin kuin väkivallalla, asevoimilla. Tällöin ajattelu on kiinalaista, sunzimaista. Sodan tavoitteen, toisen osapuolen tekeminen puolustuskyvyttömäksi on siis mahdollista kybersodan välineillä? Tällä on merkittävä vaikutus muun muassa kyberturvallisuuteen ja verkkosodan uuteen kehitysvaiheeseen, strategiseen kommunikaatioon. Onko kylmän sodan voittaminen myös heikko signaali[119] uudesta globaalista sodankäynnin muodosta?

Kybersodankäynnin muotoja on uuden, systemaattisen jaottelun mukaan aiemman kahdeksan sijasta 20. Kyberneettisen järjestelmänäkemyksen perusteella kybersodankäynnin muodot voidaan jakaa systemaattisesti 20 luokkaan (2 * 2 * 5). Ensin kybersodankäynnin muodot voidaan jakaa toimintaympäristön perusteella kahteen luokkaan: fyysiseen todelliseen ja virtuaaliseen todellisuuteen. Edellinen muodostuu atomeista ja jälkimmäinen kyberneettisen systeemin sisällä olevasta todellisuuden malleista, virtuaalitodellisuudesta. Toiseksi kybersodankäynnin muodot voidaan jakaa kahteen luokkaan sen perustella, onko toimijana ihminen vai tietokone[120] (automaatio). Kolmanneksi kybersodankäynnin muodot voidaan jakaa kohteen perusteella viiteen luokkaan. Näistä kaksi kohdistuu ihmiseen ja kaksi tietokoneeseen, ensin niiden tietoon ja toiseksi niiden kyberfyysiseen rakenteeseen. Viides kohdeluokka liittyy muuhun fyysiseen ympäristöön, kuin ihmisen ja tietokoneen kyberfyysiseen rakenteeseen. Jaottelu on esitelty tarkemmin artikkelin liitteessä 1.

Muutama erityishavainto tästä luokittelusta:

1. Psykologinen sodankäynti on osa tätä mallia ja se jakautuu tässä luokittelussa kolmeen alaluokkaan: lyhytaikaiseen vaikutukseen, pitkäaikaiseen vaikutukseen ja erityisen pitkäaikaiseen vaikutukseen. Ensimmäinen perustuu viesteihin, toinen viestien tulkintaa ja kolmas ihmisen ”asetusarvoon”.
2. Psykotroninen sodankäynti, tietokoneen toiminta ihmisen tietoa vastaan saattaa kuulostaa erikoiselta[121], mutta on itse asiassa ainakin venäläisen informaatiosodankäynnin osa.[122]

[119] Heikko signaali tarkoittaa ensimmäisiä merkkejä uudesta nousevasta trendistä.
[120] Floridi 2014, loc. 1644–1765.
[121] Erikoisuudesta huolimatta se on joka tapauksessa looginen osa tässä käytettyä jaottelua. Looginen tarkoittaa tässä sitä, että kolmen luokan sisällä vaihtoehdot ovat sellaisia, että niihin sisältyy kaikki kyseisen luokan luokittelumahdollisuudet.
[122] Psykotroninen sodankäynti tarkoittaa vaikuttamista tietokoneen käyttäjiin erityyppisin menetelmin. Tällöin tietokoneesta tulee ase ihmistä, tietokoneen käyttäjää vastaan. Näillä aseilla voidaan aikaansaada hallusinaatioita, pahoinvointia, tahdottomuutta, jopa kuolema (J. Saarelainen, Näkemyksiä Ve-

3. Tietokoneen ollessa floridilainen[123] informaatiotoimija tai informaatioagentti, 10 kybersodankäynnin luokista liittyy toimijan perusteella ihmiseen ja 10 tietokoneisiin. Jälkimmäiset ovat vastaavan ihmissodankäynnin automaattisia muotoja.
4. Kybersodan jakautuessa fyysiseen ja virtuaaliseen todellisuuteen, sen muodoista 10 on todellisia ja 10 virtuaalisia. Virtuaalinen tarkoittaa tässä ”tietomallinnettua” todellisuutta, joka on esim. tietokonepelien ydin.

Verkkosodan käsitteen ajallisen kehittymisen merkkipaalut ovat päivittyneet viidestä yhteentoista seuraavasti (uusia asioita on käsitelty laajemmin yllä):

1. (Aiempi historia ja evoluutio)[124] *(uusi)*[125]
2. Mahdollisesti toisen maailmansodan elektronisen sodankäynnin ja etenkin salakirjoituksen murtamisen havainnot (uusi)
3. Kylmän sodan voittaminen ja Neuvostoliiton kaataminen. Ensimmäinen strateginen informaatio-operaatio 1980-luvulla, (uusi)
4. (*Operatiivisen*) Informaatiosodankäynnin osa-alueet: kybersota ja verkkosota (2003)[126]
5. Verkkokeskeinen sodankäynti (NCW) (2003)
6. Tietokoneverkkohyökkäys (CNA) ja sen organisaatio (2003)
7. USA:n puolustusministeriön NCW-raportti vuodelta 2001 (2003)
8. Uusi verkkoteoria, skaalavapaa verkko (2003)
9. Vaikutusperusteinen sodankäynti (EBO ja EBAO) (uusi)
10. Operational Design suunnittelukonsepti (uusi)
11. Strateginen kommunikaatio (uusi)

Venäläiset ovat ehkä käyttäneet oman informaatiosodankäynnin teoriapohjana kybernetiikka. Tähän viittaa se, että kyberneettisen systeemimallin soveltaminen luo kybersodan alalajin, jota venäläiset kutsuvat psykotroniseksi sodankäynniksi ja jota ei juurikaan esiinny julkisessa länsimaalaisessa keskustelussa.

Kyberulottuvuus (cyberspace) on laajentunut tietokoneverkoista myös aivoihin. Yleisesti kyberulottuvuutena pidetään tietokoneiden muodostamaa virtuaalista todellisuutta[127]. Kybernetiikan mukaan vastaava virtuaalinen todellisuus, todellisuuden tietopohjaiset mallit, löytyvät myös ihmisen aivoista. Molemmissa tapauksissa toiminta perustuu fyysisen, aineellisen todellisuuden abstrakteihin malleihin, joilla joko välitettävää sensoritietoa, dataa todellisuudesta tulkitaan todellisuuteen *vaikuttamiseksi* tai tietoa käsitellään vain ko. virtuaalitodellisuuden sisällä todellisuuden *ymmärtämiseksi.*

---

näjän informaatiosodankäynnistä, Maanpuolustuskorkeakoulu, Taktiikan laitos. Taktiikan tutkimuksia. julkaisusarja 1, No 1/1999 s. 50 - 63).
[123] Floridi 2014 ja Floridi 2011, s. 166 - 176.
[124] Tätä vaihetta ei ole käsitelty tässä artikkelissa. Käsittely jää jatkotutkimuksiin.
[125] (uusi) tarkoittaa tässä luettelossa vuoden 2003 versiosta puuttunutta vaihetta.
[126] (2003) tarkoittaa tässä luettelossa alkuperäisen vuoden 2003 artikkelin vaihetta.
[127] Ahvenainen, 2003 s. 22.

Globaali taso uutena toiminnan tasona on suuri muutos. Jos ihmiskunnan ylin systeemitaso on siirtymässä globaalille tasolle mm. työnjaon osalta aiemman kulttuurisen tason sijasta, muutos vaikuttaa kaikilla tasolla, kuten edellisetkin vastaavat muutokset. Kommunikaatiojärjestelmä, joka mahdollistaa uuden tason on globaali tietokoneteknologia, keskeisesti internet. Tässä mielessä kyber, ymmärrettynä hypenä globaalista tietokoneteknologiasta, on myös erityisen merkittävä ilmiö.

Sodankäynnin tyyppien lukumäärä on kasvanut 333 prosenttia tietokoneen tultua sodankäynnin keskeiseksi toimijaksi. Tämä perustuu esitettyyn kybersodankäynnin systemaattiseen luokitteluun, jossa sodankäynnin (kybernettiset) tyypit ovat kasvaneet ennen tietokonetta olevasta kuudesta tyypistä tietokoneiden jälkeisen ajan 20 tyyppiin.

Tämän tyyppinen jatkotarkastelu on monessa mielessä tärkeä. Ensin, perinteisesti ja käytännön kannalta se on tietysti päivitys tärkeään ja nopeasti muuttuvaan aiheeseen[128]. Toiseksi se on kyberneettinen, itseensä viittaava ja epälineaarinen järjestelmä ja tässä mielessä teoreettisesti ja tieteellisesti tärkeä[129]. Kolmanneksi se on tärkeää tieteellisen kritiikin kannalta. Tämä sopii myös siihen käsitykseen, että oppimisen perusmenetelmä on ”yritys ja erehdys”, esimerkiksi tieteessä hypoteesi tai biologisessa evoluutiossa variaatiot.

Jokaisen artikkelin osalta pystytään nyt sanomaan mitä kyseisen artikkelin aiheesta on opittu tai muuttunut noin kymmenessä vuodessa. Vähintään yhtä tärkeää olisi miettiä sitä, mitä itse prosessi on opettanut yleisemmin muun muassa sotatieteen tekemisestä, siis miettiä opitun metatasoa.

Tärkeistä aiheista tehtyjä tutkimuksia olisi päivitettävä säännöllisesti. Tämä näkyy perinteisessä tieteen tekemisessä muun muassa väitöskirjojen osalta katsauksena aiheen aiempaan tutkimushistoriaan. Tämä liittyy myös aiemmin esitettyyn professori Sotaraudan termiin ”ilkeät ongelmat”. Ne on pidettävä niiden dynaamisuuden ja kompleksisuuden takia koko ajan ratkaisun alla.

1.7 Uudet ongelmat

Artikkelin pohjana käytetty metodi edellyttää uusien ongelmien syntyä ja löytämistä. Tällaisiksi tunnistettiin seuraavat asiat:

1. Mitkä ovat sodankäynnin uudet emergentit ominaisuudet siirryttäessä taistelutekniikasta taktiikkaan, edelleen operaatiotaitoon ja sen kautta strategiaan? Ja vielä vaikeampi kysymys: Miten kyseinen ylätason uusi ominaisuus *yksityiskohtaisesti* muodostuu alatason osista fyysikko Kari Enqvistin heikon emergenssikäsityksen mukaisesti?[130]

---

[128] Seuraava kirja tästä aiheesta on siis syytä tehdä esimerkiksi vuonna 2024.

[129] Länsimainen sivistys ja etenkin tiede syntyi keskeisesti antiikin Kreikassa. Keskeinen tieto-opillinen muutos oli myyttien ja auktoriteettien tiedosta luopuminen ja epäilyn, järjen, väittelyn ja dialogin nostaminen tilalle. Periaatteessa edellinen artikkeli ja kirjoittajan uusi tieto käyvät dialogia em. periaatteella keskenään ja luovat uutta tietoa.

[130] Tämä on itse asiassa kaikkien monitasoisten organisaatioiden johtamisen perusongelma: Miten organisaation vaikutus välittyy tasolta toiselle? Miten prikaatin komentajan päätös vaikuttaa lopulta jokaisessa prikaatin ryhmässä ja miten se muutetaan tai muuttuu eri tasoilla?

2. Millä uusilla informaatiovälineellä taistelutekniikasta tuli taktiikkaa tai klassisesta sotilasstrategiasta operaatiotaitoa?[131]
3. Miten itseensä viittaava epälineaarinen prosessi, toiminta (T), vastatoiminta (VT), vastavastatoiminta V2T, V3T, V4T jne., näkyy yleisessä[132] sotilaallisessa ajattelussa?
4. Jos vaikutusperusteinen sodankäynti, Operational Design ja strateginen kommunikaatio ovat olleet vuoden 2003 jälkeistä kehitystä, mitä on tulossa vuoden 2014 jälkeen? Voidaanko siitä sanoa jotakin?
5. Verkkosodan historiasta on nyt kartoitettu tietyt vaiheet, eli on vastattu kysymykseen: Mitä? Mistä nämä vaiheet johtuvat, eli miten ne ovat muodostuneet edeltäjistään? Mikä on siis vastaus kysymykseen: Miksi?
6. Onko Popperin evolutiivinen induktio niin voimakas malli, että sitä pitäisi opettaa yhtenä perusmallina mm. MpKK:ssa sodankäynnin tutkimiseen? Käsitelläänkö sitä tällä tavalla missään?

Ei-uusina ongelmina jäävät jäljelle ensin aikajakson 1991–2003 tarkempi analyysi ja toiseksi se, että jos aiheen jatkotutkimus on tarpeen, olisi hyvä löytää systeemiteorian tai sen sovellusten lisäksi jokin muu poikkeava alustava teoria. Kolmanneksi suomalaisen ja venäläisen verkkosodan historia jää edelleen jatkotutkimusten varaan.

[131] Jälkimmäisen osalta voidaan mongolien osalta sanoa 1200-luvulta, että hevosten osalta ja amerikkalaisten osalta 1860-luvulta lennättimen osalta.
[132] Sotatieteessä se näkyy ainakin Lancasterin neliölaissa (Hyytiäinen, 2001 s. 16), joka kertoo mullistavaa tietoa ylivoiman merkityksestä. Voittajan tappiot ovat kääntäen verrannolliset ylivoiman neliöön.

Luku 1/ Liite: Kybersodankäynnin tyypit kybernetiikan perusteella

Kybersodankäynti voidaan jakaa kybernetiikan perusteella seuraavasti (2*2*5 =) 20 perustyyppiin:

1. **Toimintaympäristön** (TY) perustella kahteen[133] osaan, ensin (1) fyysiseen aineelliseen ympäristöön (TY-F), joka perustuu atomeihin ja (2) virtuaaliseen aineettomaan, tiedolliseen ympäristöön, joka perustuu tietopohjaisiin, eroihin perustuviin fyysisen todellisuuden malleihin (TY-V).
2. **Toimijan** (TO) perusteella kahteen[134] osaan sen mukaan, kuka tai mikä on toimija: (1) Ihminen (TO-I) tai (2) tietokone[135] (TO-T) ja lopuksi
3. **Kohteen** (K) perusteella viiteen osaan riippuen siitä, mihin toiminta kohdistuu: (1) ihmisen tietoon (K-I-Info), (2) tietokoneen tietoon (K-T-Info), (3) tietokoneen kyberfyysisisiin osiin (K-T-CF), (4) ihmisen kyberfyysisiin osiin (K-I-CF) tai (5) muuhun fyysiseen todellisuuteen, kuten maastoon ja rakennuksiin (K-MF).

Tieto (Info) sisältää tässä kolme aliluokkaa, ensin viestin, sitten viestin tulkinnan ja lopuksi asetusarvon.[136] Viesti edustaa lyhytaikaista vaikutusta, viestin tulkinta pitkäaikaista vaikutusta ja asetusarvo pitkäaikaisinta vaikutusta. Edelleen ihmisen ja tietokoneen kyberfyysinen atomaarinen rakenne voitaisiin jakaa kybernettisen järjestelmän perusosien perusteella sensorin, päätöksentekoelimen, toimielimen, asetusarvon ja palautekytkentöjen fyysisiin rakenteisiin, eli viiteen alaosaan. Tämä tarkempi jaottelu antaa 2 * 2 * (3 + 3 + 5 + 5) = 64 kybersodankäynnin tyyppiä. Alla on esitetty 20 perustyyppiä, vastaavat kybersodankäynnin alalajit tarkemmin.

Tässä alla esitetyssä ensimmäisessä osaluettelossa toimintaympäristö on fyysinen, atomaarinen todellisuus, jossa ihmisen tai tietokoneen toiminta kohdistuu fyysisiin kybertoimijoihin, ihmiseen ja tietokoneeseen tai niiden muuhun toimintaympäristöön:

1. TY-F / TO-I / K-I-Info:[137] Ihmisen tiedon (viestien, viestien tulkinnan ja asetusarvojen) manipulointi ihmisen toimesta. Tästä ovat esimerkkejä psykologinen sodankäynti ja harhauttaminen. Kaikissa näissä on tällä luokittelulla siis

[133] Myös informaatioetiikan professori Luciano Floridi jakaa ”maailman” hyvin saman tyyppisesti teoksessaan ”The Philosophy of Information”. Ensin on kyberneettisen toimijan kohdetaso, joka toimii ympäristön kanssa ja siten on kybernettisen toimijan metataso, jonka kohteena ovat kyberneettisen toimijan sisäiset tilat (Floridi 2011 s. 166 - 176).

[134] Edellä mainittu informaatioetiikan professori Luciano Floridi esittää tietokonetta suorastaan vallankumouksellisena uutena toimija ihmiskunnan historiassa (Floridi 2014).

[135] Kolmas kyberneettinen järjestelmäluokka on solu, mutta sitä ei käsitellä tässä artikkelissa.

[136] Tietoluokkia voisi laajentaa ihmisen ja tietokoneen osalta myös seuraavasti: (1) sensoridata sisään sensoriin, (2) sensorin sisäinen tieto, (3) tieto sensorista muunnoksen jälkeen päätöksentekoelimeen (vast.), (4) päätöksentekoelimen sisäinen tieto, (5) päätöksentekoelimen tieto ulos toimielimeen ja (6) toimielimen sisäinen tieto, (7) toimielimen tieto ulos sekä lopuksi (8) koko kybernettisen järjestelmän asetusarvo.

[137] Luettelon lyhenteet: TY-F = Toimintaympäristö, fyysinen. TY-V = Toimintaympäristö, virtuaalinen. TO-I = Toimija, ihminen. TO-T = Toimija, tietokone. K-I-Info = Kohde, ihminen, tieto. K-I-CF = Kohde, ihminen, kyberfyysiset osat. K-T-Info = Kohde, tietokone, tieto. K-T-CT = Kohde, tietokone, fyysinen. K-MF = Kohde, muu fyysinen todellisuus.

lyhytaikainen, pitkäaikainen ja erityisen pitkäaikainen vaikutus. Vrt. esim. aivopesu.

2. TY-F / TO-I / K-T-Info: Tietokoneen tiedon (viestien, viestien tulkinnan ja asetusarvojen) manipulointi ihmisen toimesta. Tästä ovat esimerkkejä hakkeri- tai crakkerisodankäynti. Kaikissa näissä on tällä luokittelulla siis lyhytaikainen, pitkäaikainen ja erityisen pitkäaikainen vaikutus. Vrt. tiedon tai ohjelmiston muuttaminen (vast.) tietokoneessa.
3. TY-F / TO-I / K-I-CF: Ihmisen kyberfyysisen rakenteen (osien) manipulointi ihmisen toimesta. Tästä ovat esimerkkejä tajuttomaksi lyöminen (vast.) ja sokaiseminen.
4. TY-F / TO-I / K-T-CF: Tietokoneen kyberfyysisen rakenteen (osien) manipulointi ihmisen toimesta. Tästä ovat esimerkkejä elektronisessa sodankäynnissä häirintä ja tuhoaminen, HPM, EMP, näppäimistönauhurien asentaminen ja mikropiirien (vast.) manipulointi
5. TY-F / TO-I / K-T-MF: Muun fyysisen ympäristön manipulointi ihmisen toimesta. Tästä ovat esimerkkejä siltojen ja rakennusten tuhoaminen tai ympäristön polttaminen.
6. TY-F / TO-T / K-I-Info: Ihmisen tiedon (viestien, viestien tulkinnan ja asetusarvojen) manipulointi tietokoneen[138] toimesta. Tästä on esimerkkinä psykotroninen[139] sodankäynti. Tässäkin luokassa on lyhytaikainen, pitkäaikainen ja erityisen pitkäaikainen vaikutus.
7. TY-F / TO-T / K-T-Info: Tietokoneen tiedon (viestien, viestien tulkinnan ja asetusarvojen) manipulointi tietokoneen toimesta. Tästä ovat esimerkkejä (automaattiset) vihamieliset koodit (virukset), vihamielisten koodien torjuntaohjelmat (virustorjuntaohjelmat) ja tunkeutumisen havaitsemisohjelmat (IDS).
8. TY-F / TO-T / K-I-CF: Ihmisen kyberfyysisen rakenteen (osien) manipulointi tietokoneen toimesta. Tästä ovat esimerkkejä (automaattiset) aseet, joiden kohteet ovat erityisesti esim. aivojen, silmien tai korvien fyysiset rakenteet, esim. lasersokaisu.
9. TY-F / TO-T / K-T-CF: Tietokoneen kyberfyysisen rakenteen (osien) manipulointi tietokoneen toimesta. Tästä ovat esimerkkejä (automaattiset) toisen tietokoneen komennot toiselle tietokoneelle, jossa komentojen suoritus tuhoaa[140] fyysisesti kohdetietokoneen osia.
10. TY-F / TO-T / K-I-MF: Muun fyysisen ympäristön manipulointi tietokoneen toimesta. Tästä ovat esimerkkejä kaikki (automaattiset) (täsmä)aseet ja muut vaikutussysteemit, joissa toiminta perustuu tietokoneen automaattiseen toimintaan ja joiden maalit kuuluvat tähän luokkaan, esim. sillat ja rakennukset.

Tässä alla esitetyssä toisessa osaluettelossa toimintaympäristö on simuloitu todellisuus, jossa toiminta kohdistuu vain kybertoimijoiden (ihminen ja tietokone) sisäiseen, virtuaaliseen maailmaan, Floridin informaatiotoimijan metatasoon[141]. Toiminnalla ei siis ole fyysisiä vaikutuksia. Kaikki tietokone(sota)pelit kuuluvat periaatteessa tähän

[138] Kun toimijana on tietokone, kaikkia kyseisiä kybersodankäynnin tyyppejä voidaan tulkita vastaavan ihmissodankäynnin automaattisina versiona.
[139] Psykotroninen sodankäynti tarkoittaa vaikuttamista tietokoneen käyttäjiin eri tyyppisin menetelmin. Tällöin tietokoneesta tulee ase ihmistä, tietokoneen käyttäjää vastaan. Näillä aseilla voidaan aikaansaada hallusinaatioita, pahoinvointia, tahdottomuutta, jopa kuolema (Saarelainen, 1999 s. 50 – 63).
[140] T. Shimomura ja J. Markoff, Takedown - The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw - by the Man Who Did It, New York: Hyperion, 1996 s. 59.
[141] Floridi 2011 s.168 - 76.

luokkaan, samoin muuten kuin tietokoneella toteutetut (sota)pelit. Periaatteellisesti on myös tärkeää, että puolet tällä tavalla määritellyistä kybersodankäynnin tyypeistä ovat simuloituja.

11. TY-V / TO-I / K-I-Info: Simuloitu ihmisen tiedon (viestien, viestien tulkinnan ja asetusarvojen) manipulointi ihmisen toimesta.
12. TY-V / TO-I / K-T-Info: Simuloitu tietokoneen tiedon (viestien, viestien tulkinnan ja asetusarvojen) manipulointi ihmisen toimesta
13. TY-V / TO-I / K-I-CF: Simuloitu ihmisen kyberfyysisen rakenteen (osien) manipulointi ihmisen toimesta.
14. TY-V / TO-I / K-T-CF: Simuloitu tietokoneen kyberfyysisen rakenteen (osien) manipulointi ihmisen toimesta.
15. TY-V / TO-I / K-I-MF: Simuloitu muun fyysisen ympäristön manipulointi ihmisen toimesta.
16. TY-V / TO-T / K-I-Info: Simuloitu Ihmisen tiedon (viestien, viestien tulkinnan ja asetusarvojen) manipulointi tietokoneen toimesta
17. TY-V / TO-T / K-T-Info: Simuloitu tietokoneen tiedon (viestien, viestien tulkinnan ja asetusarvojen) manipulointi tietokoneen toimesta
18. TY-V / TO-T / K-I-CF: Simuloitu ihmisen kyberfyysisen rakenteen (osien) manipulointi tietokoneen toimesta.
19. TY-V / TO-T / K-T-CF: Simuloitu tietokoneen kyberfyysisen rakenteen (osien) manipulointi tietokoneen toimesta.
20. TY-F / TO-T / K-I-MF: Simuloitu muun fyysisen ympäristön manipulointi tietokoneen toimesta.

On syytä huomata, että näistä 20:stä kybersodankäynnin muodosta oli olemassa ennen tietokoneita lähinnä tavanomainen sodankäynti, ensin ihmisen kyberfyysiseen tai muuhun fyysiseen rakenteeseen kohdistuneena (no 3 ja 5), sitten psykologinen sodankäynti (no 1) ihmisen tietoon kohdistuneena ja lopuksi ihmisen toiminta muuhun fyysiseen ympäristöön kohdistuneena (no 5). Näiden lisäksi edellisten simulointimuodot voidaan laskea mukaan ”sotapeleinä”, esim. sodanjohtajien päänsisäisinä pohdintoina, ajatteluna[142] (no 11, 13. 15).

Tällä tavalla kyberneettisesti tarkasteltuna sodankäynnin ”perustyypit” ovat lisääntyneet 333 prosenttia, kun tyyppien määrä on kasvanut kuudesta tyypistä 20 tyyppiin. Jos kaikki sodankäynnin tyypit (N) pitää koordinoida toisiinsa, kuten ideaalitapauksessa varmaan pitäisi, sodankäynnin monimutkaisuus on verrannollinen typpien lukumäärän N(N-1) tuloon. Kun tietokoneista on tullut sodankäynnin ”täysmääräisiä” toimijoita, sodankäynnin monimutkaisuus on kasvanut 1200 prosenttia, 30:sta (6 * 5) 360:aan (20 * 19).

[142] Kirjan vuoden 2003 version kritiikkipuheenvuorossa taktiikkaa ei pidetä niinkään ”oppina taisteluiden voittamisesta”, vaan ajatteluna (Piiroinen, Toim., 2003 s. 95). Onko kyse kuitenkin ajattelusta, joka tähtää taistelun voittamiseen? Keino – päämäärä?

2.

Tiedonhallinta päätöksenteossa kybertoimintaympäristössä

Dosentti Tuija Kuusisto
Maanpuolustuskorkeakoulu
Taktiikan laitos

Tekniikan tohtori Tuija Kuusiston osaamisalueita ovat tietopolitiikka, johtaminen ja tiedonhallinta päätöksenteossa sekä kyberturvallisuuden johtaminen ja projektijohtaminen. Hän on väitellyt geoinformatiikasta vuonna 1995. Hän on toiminut operaatiotaidon ja taktiikan, erityisesti tiedonhallinta päätöksenteossa dosenttina Maanpuolustuskorkeakoulussa vuodesta 2004 lähtien. Hän on toiminut johto- ja asiantuntijatehtävissä valtiovarain-, sisäasiain-, puolustus- ja maa-ja metsätalousministeriöiden hallinnonaloilla sekä Nokia-yhtymässä ja pk-yrityksissä. Lisäksi hän on toiminut tietojohtamisen professorina Tampereen teknillisessä yliopistossa, geoinformatiikan dosenttina Aalto-yliopistossa sekä vierailevana asiantuntijana Sitrassa ja asiantuntijana Euroopan komissiossa. Hän on julkaissut noin 70 tieteellistä artikkelia kansainvälisissä ja kansallisissa journaaleissa, konferenssijulkaisuissa ja kirjoissa sekä toimittanut kaksi kirjaa.

Tiivistelmä
Yhteiskunnan ja taistelujen robotisoituminen ja automatisoituminen sekä massadatan käsittelymenetelmien kehittyminen ja laajeneva käyttö vaikuttavat yhteiskunnan elintärkeisiin toimintoihin sekä puolustusvoimien mahdollisuuksiin ja vaihtoehtoihin toimia. Kompleksisten systeemien teorioihin perustuvan sosiaalisen systeemin mallin avulla on mahdollista hahmottaa tätä muutosta ja siihen liittyviä ilmiöitä sekä niiden perusteella suunnata resursseja vaikuttavimpiin kohteisiin. Tässä luvussa sosiaalisen systeemin mallia sovelletaan Suomessa vuonna 2013 toteutettujen kyberturvallisuusharjoitusten arviointitietojen sisältöjen analyysissä. Kybertaistelujen toimijoiden tiedonvaihtotarpeita käsitellään usean toimijan yhteistyötä vaatineiden kriisitilanteiden tiedonvaihtoa koskeneiden tutkimusten perusteella, joissa on todettu että tietojenvaihtotarpeet riippuvat toimijoiden rooleista, toiminnan vaiheesta ja yhteistyön kypsyystasosta. Kybertoimintaympäristössä voidaan tietotoon vaikuttamalla kohdistaa Suomen rajojen ulkopuolelta vaikutus Suomen alueella sijaitsevaan kohteeseen. Tältä vaikuttamiselta ei voida puolustautua pelkästään Suomen maantieteellisen alueen sisältä. Siten Suomessa tarvitaan vuonna 2020 kansallisia ja kansainvälisiä sopimuksia Suomen sotilaalliseksi puolustamiseksi ja kybertaisteluissa onnistumiseksi.

2.1 Arvio vuoden 2003 artikkelista ”Tiedon merkitys Suomen puolustamisessa”

Vuoden 2003 Verkkotaistelu 2020-kirjan artikkelissa ”Tiedon merkitys Suomen puolustamisessa”1 korostettiin tietoverkkojen toimivuuden ja tietojen turvaamisen olevan tulevaisuudessa yhä merkittävämpää yhteiskunnan kaikille toimijoille. Tietoverkkoihin vaikuttamalla todettiin voitavan hyökätä koko yhteiskuntaa vastaan. Nämä näkemykset vastaavat hyvin kuluneiden runsaan kymmenen vuoden aikana kertyneitä kokemuksia. Vuoden 2003 artikkeli kirjoitettiin keskellä 1900-luvun loppupuolella kasvavaa huomiota saanutta ajattelua, jossa modernien yhteiskuntien katsottiin olevan siirtymässä teollisesta yhteiskunnasta tietoyhteiskunniksi. Tietoon sekä tiedon laajamittaiseen käsittelyyn, jalostamiseen ja käyttöön liittyviin teknologioihin kohdistui suuria odotuksia sekä liiketoiminnassa että koko yhteiskunnassa niin uusien palvelujen ja tuotteiden kuin digitaalisten sisältöjen luomisen sekä organisaatioiden ja kansalaisten osaamisen kehittymisen mahdollistajana. Tietoyhteiskunta-ajattelu painottuen liiketaloudellisella näkökulmalla heijastuukin artikkelissa vahvasti. Tämä on luonnollista, sillä artikkeli kirjoitettiin Tampereen teknillisessä yliopistossa tuotantotalouden osastolla, jossa oli panostettu tietoyhteiskuntakehityksen vauhdittamiseen aloittamalla uusi tietojohtamisen koulutusohjelma vuonna 1999. Kirjoittajat edustivat tämän koulutusohjelman ensimmäistä opettaja- ja opiskelijasukupolvea.

Artikkelissa kuvataan kattavasti tietojohtamiseen liittyviä peruskäsitteitä ja -termejä. Tiedon luokittelu dataksi, informaatioksi ja tietämykseksi muodostaa myös kybertoimintaympäristön tiedonhallinnan lähtökohdan. Käytetyistä lähteistä Polanyin[2] kirja vuodelta 1966 oli vanhin. Polanyin kirjaan sisältyvät hiljaisen ja eksplisiittisen tiedon käsitteet ovat edelleen laajasti käytettyjä ja selittävät myös kybertoimintaympäristössä tarvittavaa tiedonhallintaa. Polanyin kirjasta on otettu uusintapainos vuonna 2009, mikä kertonee kirjan jatkuvasta suosiosta. Myös artikkelissa esiin nostettu tietoturvallisuuden hallintajärjestelmä BS7799-2:2002 oli kelpo valinta, sillä se päivitettiin ISO/EIC 27002:2005 tietoturvallisuusstandardiksi[3] ja on vakiinnuttanut paikkansa tietoturvallisuustoiminnassa.

Kiinnostus kriittistä infrastruktuuria kohtaan on huomattavasti kasvanut sekä hallinnossa että koko yhteiskunnassa artikkelin kirjoittamisen jälkeen. Artikkeli sisältää ajankohtaista ja oletettavasti myös vuoteen 2020 ulottuvaa kuvausta kriittisen infrastruktuurin toimivuuden merkityksestä yhteiskunnalle ja sen toimijoille. Artikkelissa myös tunnistettiin toimijoita eli kriittisiä kohteita, joille infrastruktuurin toimimattomuus aiheuttaisi haittaa. Myöhemmin kriittiset kohteet jäsennettiin Suomen ensimmäisessä Yhteiskunnan elintärkeiden toimintojen turvaamisen strategiassa vuonna 2003[4] elintärkeiksi toiminnoiksi. Artikkelissa esitetty matriisitarkastelu kriittisen infrastruktuurin ja toimijoiden välisestä suhteesta havainnollistaa hyvin toimijoiden riippuvuutta tietoverkoista sekä nykyhetkellä että vuonna 2020.

---

[1] Helokunnas, T., Laukkanen, T. & Viitanen, K. (2003). Tiedon merkitys Suomen puolustamisessa. Teoksessa Piiroinen, M. (ed.) *Verkkotaistelu 2020*, Taustatutkimus Maavoimien Taistelun kuvat 2020 tutkimukseen. Maapuolustuskorkeakoulu, Taktiikan laitos. Julkaisusarja 2, N:o 2/2003.

[2] Polanyi, M. (1966). The Tacit Dimension. Garden City, N.Y., Doubleday, 108s.

[3] ISO (2005). ISO/EIC 27002:2005 Information technology, Security techniques, Code of practice for information security management, ISO/IEC JTC 1/SC 27. 115s.

[4] Valtioneuvosto (2003). Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia. Valtioneuvoston periaatepäätös 27.11.2003.

Artikkelin varsinainen aihe on tiedon merkitys Suomen puolustamisessa. Artikkelissa on onnistuneesti viitattu OODA-luuppiin[5] perustuvaan malliin kun perustellaan sitä, että tiedolla on merkitystä toiminnassa, tässä tapauksessa siis Suomen puolustamisessa. Tässä kirjassa Martti Lehdon artikkelissa ”Kybertaistelun toimintaympäristön teoreettinen tarkastelu” käsitellään laajemmin yhä vuonna 2020 merkittävää OODA-luuppiin perustuvan ajattelun soveltamista taisteluissa ja strategiassa.

Vuoden 2003 artikkelissa ei käsitellä menetelmiä kuvata yhteiskunnan muutosta eikä kuvata tarkempia tavoitteellisessa toiminnassa tarvittavien tietojen luokittelujen malleja. Tämän johdosta artikkeli jää tiedon merkitystä pohtiessaan yleiselle yhteiskunnan tulevan kehittymisen ominaisuuksien kuvaamisen tasolle. Artikkelin pääteluvuissa pohditaan tietoon vaikuttamisen keinoja sekä valtiollisen toimijan mahdollisuuksia suojautua haitalliselta tietoon vaikuttamiselta kuten kriittisen infrastruktuurin lamauttamiselta. Tulevaisuuden ennakointina artikkelissa tunnistetaan valtiollisten toimijoiden kasvava riippuvuus globaalisti toisistaan sekä yrityksistä ja kolmannen sektorin toimijoista. Tämä ennakointi on enemmän todellisuutta nykypäivänä kuin kymmenen vuotta sitten. Esimerkiksi ulkoasiainvaliokunnan mietinnössä vuodelta 2013[6] koskien Valtioneuvoston selontekoa Suomen turvallisuus- ja puolustuspolitiikasta 2012 kehotetaan huomioimaan huoltovarmuudessa verkostoituneen yhteiskunnan keskinäisriippuvuuden tuomat haasteet. Huoltovarmuuskeskuksen Sopimuksiin perustuva varautuminen (SOPIVA)-hankkeessa[7] on ratkottu tätä haastetta tuottamalla ohjeita jatkuvuudenhallinnan suositusten liittämisestä sopimuksiin.

Artikkelissa myös todetaan valtioiden välisten rajojen hämärtyvän eri toimijaryhmien toiminnassa tulevaisuudessa, mikä onkin tapahtunut. Artikkelissa peräänkuulutetaan syvällisempää tietämystä sekä ihmisen toiminnasta että tietoverkoista. Tämä vaatimus on tällä hetkellä selkeästi esillä Euroopan unionin kyberturvallisuusstrategian[8] toteuttamisessa, jossa yhtenä alueena on kyberkapasiteettien kehittäminen. Kaikkien yhteiskunnan toimijoiden kyberosaamisen ja -ymmärryksen parantaminen on myös yksi Suomen kyberturvallisuusstrategian[9] strategisista linjauksista.

---

[5] Hammond, G.T. (2001). The Mind of War; John Boyd and American Security. Smithsonian Institution Press, Washington and London, 190 s.
Osinga, F. (2006). Science, Strategy and War: The Strategic Theory of John Boyd. Abingdon, UK, Routledge 313 s.

[6] Ulkoasiainvaliokunta (2013). Ulkoasiainvaliokunnan mietintö 1/2013, Valtioneuvoston selonteko Suomen turvallisuus- ja puolustuspolitiikka 2012.

[7] Huoltovarmuuskeskus (2014) Sopimuksiin perustuva varautuminen (SOPIVA) -hanke. http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/sopiva, vierailtu 7.3.2014

[8] Euroopan Unioni (2013). Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, vierailtu 7.3.2014.

[9] Valtioneuvosto (2013). Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. http://www.yhteiskunnanturvallisuus.fi, vierailtu 14.5.2013.

2.2 Kybertoimintaympäristön tiedonhallinnan lähtökohtia

2.2.1 Automatisoituva toimintaympäristö

Ihmiset, laitteet, prosessit, sovellukset ja robotit muodostavat parhaillaan toistensa kanssa vuorovaikutuksessa olevia entistä laajempia systeemejä. Tästä kehityksestä käytetään näkökulmasta riippuen nimityksiä teollinen internet, esineiden internet ja kaiken internet – Internet of everything. Se aiheuttaa merkittäviä muutoksia kaikkien organisaatioiden rakenteissa ja toiminnoissa. Myös puolustusvoimien lakisääteisiin tehtäviin yhä enenevässä määrin vaikuttavat ajasta, paikasta ja valtioiden välisistä rajoista riippumattomat digitaaliset sosiaaliset systeemit. Nämä automatisoituvat systeemit pystyvät suoriutumaan yhä itsenäisemmin eri tehtävistä ja niissä olevan datan määrä kasvaa. Kybertoimintaympäristö on kuitenkin tuntematon maasto. Tarvitaan enemmän kokonaisymmärrystä siitä, mitä kybertoimintaympäristö edellyttää toimijoilta, toiminnalta, toimintorakenteilta ja tietojenvaihdolta. Mistä asioista tarvitaan päätöksiä ja milloin, jotta puolustusvoimien lakisääteisiä tehtäviä voidaan toteuttaa myös kybertoimintaympäristössä ja sen kautta?

Eduskunnan tulevaisuusvaliokunnan tilaamassa ennakoinnissa ”Suomen sata uutta mahdollisuutta: Radikaalit teknologiset ratkaisut”[10] on käsitelty kansallisesti Suomelle lupaavia teknologiaratkaisuja, jotka ovat saatavilla vuoteen 2020 mennessä. Selvityksessä on analysoitu sataa tärkeintä uutta teknologiaa kaikkiaan kahdessakymmenessä eri arvonluontiverkossa. Yksi näistä arvonluontiverkostoista on maanpuolustus ja terrorismin torjunta, johon kuuluvien teknologiaratkaisujen ja siirtymäkauden ongelmien voidaan kaikkien katsoa sisältyvän kybertoimintaympäristön elementteihin. Raportissa käsitellyistä muista teknologiaratkaisuista kaiken kaikkiaan valtaosa liittyy yhteiskunnan digitalisoitumiseen ja siten kybertoimintaympäristöön. Tämä vahvistaa kybertoimintaympäristön merkityksen kasvua yhteiskunnan kokonaisturvallisuuden ja elintärkeiden toimintojen turvaamisen kannalta.

Ennakointiraportissa todetaan, että autonomiset ja kauko-ohjattavat nelikopterit, robottihyönteiset, suurtehokondensaattorit, laserkanuunat, dna-kirjoittimet, tarkka ilmakuvaus lennokeista, keinonenät, hahmontunnistus ja kemiallinen tunnistus ja verkkosodankäynti tekevät vanhoista maanpuolustuskeinoista riittämättömiä. Siirtymäkauden ongelmana nähdään se, että uusiin uhkiin vastaamisen tehokkaimmat keinot ovat vaikeasti toteutettavissa ilman kattavaa tiedustelutietoa maan rajojen ulkopuolelta ja ilman kykyä puuttua maan rajojen ulkopuolisiin tietojärjestelmiin. Uusien teknologioiden uhkina arvioidaan olevan uudet täsmäiskuihin kykenevät robotisoidut biologiset ja kemialliset joukkotuhoaseet, uusien tuhoaseiden ja vanhan puolustusvälineistön ilmeinen yhteensopimattomuus sekä tietoverkkoihin ja automaatioon perustuvan yhteiskunnan haavoittuvuuden kasvaminen.

Globaalien robottitilastojen[11] mukaan vuonna 2012 myytiin ammattimaiseen käyttöön tarkoitettuja palvelurobotteja noin 16 000 kappaletta. Niistä arviolta 40% oli palvelurobottien puolustussovelluksia, joiden suurimmat ryhmät muodostivat miehittämättö-

[10] Linturi, R., Kuusi, O. & Ahlqvist, T. (2013). Suomen sata uutta mahdollisuutta: Radikaalit teknologiset ratkaisut. Eduskunnan tulevaisuusvaliokunnan julkaisu 6/2013. 185s. http://web.eduskunta.fi/dman/Document.phx?documentId=ie27613151734377, vierailtu 16.1.2014.

[11] The International Federation of Robots (2014). World Robotics - Industrial Robots 2013, IFR statistical department, http://www.worldrobotics.org, vierailtu 12.3.2014.

mät lennokit ja kenttärobotit. Vuosina 2013–2016 arvioidaan myytävän 28 000 palvelurobottien puolustussovellusta.[11] Siten vuoteen 2020 mennessä voidaan edelleen arvioida palvelurobottien määrän kasvavan erilaisissa maanpuolustuksen tehtävissä. Yhden merkittävän teknologia-alueen muodostavat miehittämättömät ilma-, vesi- ja maa-ajoneuvot kuten lennokit ja robottiautot. Tämä ennakoitu robotisoituminen ja yleisemmin taistelujen välineiden automatisoituminen vaikuttavat puolustusvoimien mahdollisuuksiin ja vaihtoehtoihin toimia.

Suomen kyberturvallisuusstrategiassa[9] kyberturvallisuus nähdään osana yhteiskunnan kokonaisturvallisuutta, jolloin kyberturvallisuus on osa kaikkea yhteiskunnan toimintaa. Vastaavaa kokonaisturvallisuutta painottavaa näkemystä ovat edustaneet jo aikaisemmin esimerkiksi Virtanen[12] sekä Rintakoski ja Autti[13]. Vuoden 2009 Yhdysvaltain asevoimien tiedustelua koskevassa ohjeessa[14] painotetaan kokonaisvaltaista, koko yhteiskunnan kattavaa näkemystä. Huovinen et al.[15] perustelee toimintaympäristön kokonaisvaltaisen huomioon ottamisen tarvetta kyberasioiden sotilaallisessa tarkastelussa tähän ohjeeseen nojautuen. Myös ISOn[16] termeistä 'cybersafety' on lähellä Suomen kyberturvallisuusstrategian määritelmää kyberturvallisuudesta. Sen sijaan ISO määrittelee termin 'cybersecurity' suppeammin suoraan termin 'information security' määritelmän perustuen.

Kokonaisvaltainen näkemys kyberturvallisuudesta yhteiskunnan elintärkeiden toimintojen turvaamiseen ja puolustusvoimien tehtäviin saumattomasti liittyvinä asiana tukee parhaiten myös tulevaisuuden ennakointia. Siten tämä kokonaisvaltainen näkemys muodostaa myös tämän kirjan lähtökohdan.

2.2.2 Kybertoimintaympäristön piirteitä

Kybertermejä ovat kybertoimintaympäristö, kybertila ja kyberavaruus, joiden kaikkien voidaan katsoa olevan käännöksiä termistä cyberspace. Tässä kirjassa käytetään termiä kybertoimintaympäristö. Muita osin päällekkäisiäkin kybertermejä ovat kyberulottuvuus, englanniksi 'cyber domain' sekä harvinaisemmat kyberkulttuuri ('cyber culture') ja kybermaailma ('cyber world'). ITU[17] toteaa käyttävänsä termejä kybertoimintaympäristö, kyberympäristö ja kriittinen tietoinfrastruktuuri toistensa synonyymeinä. Maailma on laajempi käsite kuin ulottuvuus, ympäristö, tila tai avaruus ja sen johdosta laajin kyberasioita kuvaava termi. Kybermaailman määritelmä on johdettavissa termin kyber ja käsitteen maailma määritelmistä[18], jolloin kybermaailma on maa ja

[12] Virtanen, T. (2002). Four views on security. Helsinki University of Technology, Department of Computer Science and Engineering, Telecommunications Software and Multimedia Laboratory, Otamedia Oy, Espoo.
[13] Rintakoski, K. and Autti, M. (2008 eds.). Comprehensive Approach, Trends, Challenges and Possibilities for Cooperation in Crisis Prevention and Management. Seminar publication on 17th of June, 2008 Helsinki, Finland.
[14] USA (2009). Joint Intelligence Preparation of Operational Environment, Joint Publication 2-01.3, 16.6.2009, http://www.fas.org/irp/doddir/dod/jp2-01-3.pdf, vierailtu 15.1.2014
[15] Huovinen, P., Kärkkäinen, A., Lehto, M., Noronen, L., Pispa, K. & Viita, V. (2013). Kybersuorituskyvyt 2030. Yleisesikuntaupseerikurssi 56: Joukko vaihtoehtoja puolustusvoimien tulevaisuuteen 2030, Maanpuolustuskorkeakoulu.
[16] ISO (2012). ISO/EIC 27032:2012, Information technology-Security techniques -Guidelines for cybersecurity.
[17] ITU (2011). ITU National Cybersecurity Strategy Guide, viewed 5 November 2013, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf
[18] Merriam-Webster (2013). Merriam-Webster online dictionary, http://www.merriam-webster.com/, vierailtu 9.12.2013.

kaikki sen asukkaat, asiat ja esineet, jotka liittyvät tai koskevat tietokoneita tai tietoverkkoja. Tämä määritelmä on lähellä ITU-T:n[19] kuvaamaa kyberympäristön määritelmää sekä Hathawayn ja Klimburgin[20] näkemystä kybertoimintaympäristöstä. Hathaway ja Klimburg[20] viittaavat ITUn[17] ja ISOn[16] määritelmiin ja toteavat, että kybertoimintaympäristö on laitteistojen, ohjelmistojen, tietojärjestelmien, ihmisten ja tietoverkoissa tapahtuvan sosiaalisen vuorovaikutuksen muodostama kokonaisuus.

Suomen kyberturvallisuusstrategiassa[9] kybertoimintaympäristön kuvataan koostuvan informaation käsittelyyn tarkoitetusta, yhdestä tai useammasta tietojärjestelmästä. Ihmisten sisältyminen kybertoimintaympäristöön ei tässä määritelmässä ole yhtä selkeästi todettu kuin Hathawayn ja Limburgin[20] määritelmässä. Perinteisesti tietojärjestelmään kuitenkin katsotaan sisältyvän sekä ihmiset, ohjelmistot että laitteistot.

Suomen kyberturvallisuusstrategiassa[9] visiona on elintärkeiden toimintojen suojaaminen kaikissa tilanteissa kyberuhkaa vastaan. Yhdeksi strategiseksi linjaukseksi on päätetty se, että puolustusvoimat luovat kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissä. Ministeriöille hyväksytyissä kyberturvallisuustehtävissä[21] tätä on tarkennettu siten, että puolustushallinto vastaa Suomen sotilaallisesta puolustamisesta myös kybertoimintaympäristön kautta maan turvallisuuteen kohdistuvia, sotilaallisiin uhkiin rinnastettavia kyberuhkia vastaan.

Sotilaalliselta näkökannalta kybertoimintaympäristö määritellään usein yhdeksi toisiinsa liittyvästä viidestä ulottuvuudesta muiden ulottuvuuksien ollessa ilma, maa, meri ja avaruus. Kybertoimintaympäristö mallinnetaan koostuvaksi fyysisestä, loogisesta ja sosiaalisesta kerroksesta sekä paikkatieto, fyysinen verkko-, looginen verkko-, kyberpersoona ja persoonakomponenteista.[22] Fyysinen kerros muodostuu laitteistoista ja infrastruktuureista sekä näiden fyysisistä sijainneista. Looginen kerros sisältää loogiset yhteydet verkossa olevien laitteiden välillä. Sosiaaliseen kerrokseen kuuluvat sekä kyberpersoonat eli toimijat verkossa että ihmiset. Yhdellä henkilöllä voi olla useita kyberpersoonia ja vastaavasti yhteen kyberpersoonaan voi liittyä monta henkilöä.

Fyysisen kerroksen osia rakennetaan jatkuvasti lisää: Mannertenvälisiä tiedonsiirtoyhteyksiä on suunnitteilla ja rakenteilla laajasti, valtioiden sisäisiä tietoliikenneyhteyksiä parannetaan jatkuvasti ja rakenteilla on useita, laajoja palvelinkeskuksia eri puolilla maailmaa. Helposti kerättävissä ja varastoitavissa oleva aurinkoenergia mahdollistaa tulevaisuudessa erilaisten asioiden liittämisen ja käyttämisen verkossa. Näitä verkon loogisessa kerroksessa liitettäviä asioita voivat olla esimerkiksi mikä tahansa tavara tai tuote kuten puhelin, robotti sekä valvonta- ja asejärjestelmä. Sosiaalisessa

---

[19] ITU-T (2008). Overview of cybersecurity, Series X: Data Networks, Open System Communications and Security, Recommendation ITU-T X.1205, http://www.itu.int/rec/T-REC-X.1205-200804-I, vierailtu 5.11.2013.

[20] Hathaway, M. and Klimburg, A. (2012). 'Preliminary Considerations: On National Cyber Security'. In National Cyber Security Framework Manual (Klimburg, A. ed.), NATO CCD COE Publication, Tallinn, Estonia.

[21] Turvallisuuskomitea (2014). Ministeriöiden kyberturvallisuustehtävät. http://www.turvallisuuskomitea.fi, vierailtu 10.3.2014.

[22] US ARMY (2010). Cyberspace Operations Concept Capability Plan 2016-2028, US ARMY TRADOC Pamphlet 525-7-8, 22.2.2010, https://www.yumpu.com/en/document/view/8916697/cyberspace-operations-concept-capability-plan-2016-2028, vierailtu 15.1.2014.

kerroksessa tapahtuvan ihmisten välisen kanssakäymisen mahdollisuuksien ennakoidaan myös entisestään lisääntyvän.

Kybertoimintaympäristö on vuorovaikutteinen ja kompleksinen adaptiivinen systeemi[23], jonka yksityiskohtia ei kukaan toimijaryhmä täysin tiedä.[24] Tunne maasto ja sen tarjoamat vahvuudet ja heikkoudet, tässä tapauksessa kybertoimintaympäristö ja sen mahdollisuudet ja uhat, on edelleen käypä periaate. Kybertoimintaympäristön tuntemisen tunnusmerkeistä ja menetelmistä tarvitaan kuitenkin vielä lisää tietoa. Kybertoimintaympäristön uhkien torjunnassa tarvitaan hyväksi koettuja ja jatkuvasti kehittyviä tietoturvallisuuden menetelmiä ja ohjelmistoja. Tietoturvallisuus ei kuitenkaan voi ratkaista kaikkia kybertoimintaympäristön uhkia eikä hyödyntää sen mahdollisuuksia, koska tietoturvallisuus on vain yksi näkökulma monirakenteiseen ja monitoiminnalliseen kybertoimintaympäristöön.

Merkittävillä kybertaistelujen toimijoilla on mahdollisuus käyttää pitkälle kehittynyttä kyberpotentiaalia, joka perustuu kulttuuriperintöön, vaurauteen, koulutusjärjestelmään, tutkimukseen ja tuotekehitykseen, kansainväliseen liiketoimintaan, yhteiskunnallisiin rakenteisiin ja infrastruktuuriin. Valtioilla on parhaat edellytykset muodostaa tätä potentiaalia. Kyberpotentiaali on globaalisti keskittynyttä ja sen käyttäminen perustuu yhteistoimintaan ja teknologisiin verkostoihin. Globaalit yrityksetkin tarvitsevat kybertoimintaympäristössä toimiakseen isäntävaltion tai valtioita, joiden kyberpotentiaalia ne voivat käyttää. Siten merkittävimpiä kybertaistelujen toimijoita ovat ne valtiot ja valtioiden kanssa yhteistyössä toimivat organisaatiot, joilla on pääsy kyberpotentiaaliin sekä kyberpuolustuskykyjä eli kyberosaamista ja kykyä käyttää sitä.

Jonkin valtion kyberpotentiaalia hyödyntävät toimijat voivat toimia tämän valtion kannalta suotuisasti tai haitallisesti, jopa vihamielisesti. Vihamielisillä toimijoilla on taipumus siirtyä toimimaan ympäristöihin, joissa on vähiten valvontaa. Kybertoimintaympäristö jakaantuu lukuisiin erilaisiin ja eri tavoin pääsyrajoitteisiin ja erilaisin periaattein käyttäjien tunnistetietoja ylläpitäviin kokonaisuuksiin, joissa valtiolliset toimijat, yritykset ja muut organisaatiot sekä rikolliset toimivat. Kybertoimintaympäristöön kuluu myös ns. pimeä Tor-verkko, jossa käyttäjien identiteetti pyritään salaamaan ja jota käytetään myös rikollisiin tarkoituksiin. Kybertoimintaympäristön erilaisten käyttömahdollisuuksien johdosta Suomen valtiolla tulee olla kyky valvoa ja säädellä kyberpotentiaalin käyttöä Suomessa.

2.2.3 Kybertaistelu

Kokonaisturvallisuuden näkökulmalta katsottuna kybertaistelu on valtioiden suvereniteettiin, elintärkeisiin toimintoihin ja erityisesti kriittiseen infrastruktuuriin kohdistuvan haitallisen tai vihamielisen vaikuttamisen ennaltaehkäisyä ja torjumista kybertoimintaympäristössä. Kybertaisteluilla on mahdollista vaikuttaa sekä kybertoimintaympäristöön että fyysiseen ympäristöön. Kasvavaa huomiota on saamassa kineettinen kyber, jolla tarkoitetaan fyysisessä maailmassa ilmeneviä tapahtumia, jotka on saatu aikaan kybertoimintaympäristössä toteutetulla toiminnalla.

---

[23] Holland, J.H. (1996). Hidden Order: How Adaptation Builds Complexity. Cambridge, MA, Perseus Books.

[24] Kuusisto, T. & Kuusisto, R. (2014b). 'Cyber World as a Social System'. In Lehto, M. (ed.), Cyber Security Analytics. Springer, to be published.

Sodankäynnissä kybertaistelut muodostavat yhden osan käytettävissä olevia resurssi- ja keinovalikoimia sotilaallisia operaatioita suunniteltaessa ja toteutettaessa. Yhdysvaltojen asevoimien näkemyksen mukaan[22] operaation komentaja etsii toimintavapauden säilyttämistä kybertoimintaympäristössä samalla kun vastustajilta evätään mahdollisuudet tähän valittuna ajankohtana ja valitussa paikassa. Tavoitteena on sotilaallisten operaatioiden mahdollistaminen sekä kybertoimintaympäristössä että ilmassa, maalla, merellä ja avaruudessa.

Valtioiden väliset maantieteelliset rajat eivät määritä kybertoimintaympäristön tai kybertaistelujen maantieteellisiä ulottuvuuksia. Kybertaistelun kohteena olevia palveluita tuotetaan eri paikoissa kuin missä niitä käytetään. Kybertoimintaympäristössä tilanteen seuraamisen vaikeutena onkin tunnistaa se mitä milloinkin tapahtuu ja kenen toimesta ja mihin vaikutus kohdistuu? On haastavaa hahmottaa, missä eri toiminnoissa tarvittava kokonaisinfrastruktuuri sijaitsee ja mitkä ovat infrastruktuurien ja järjestelmien keskinäiset riippuvuussuhteet.

Toisaalta myös kybertoimintaympäristön edellyttämät toimenpiteet valtiollisilta turvallisuusviranomaisilta ovat paikoin ristiriitaisia ja vaativat selvennystä. Miten Suomi turvaa organisaatioiden ja kansalaistensa maksamisen peruspalveluiden toimivuuden yhtenäisellä euromaksualueella: Single Euro Payments Area (SEPA:ssa)? Mitä Suomen sotilaallinen puolustaminen tarkoittaa suhteessa Suomeen sijoittuneille kansainvälisille palvelinkeskuksille kuten yhdysvaltalaisen Googlen ja venäläisen Yandexin keskuksille? Puolustetaanko näiden keskusten maapinta-alaa, fyysistä infrastruktuuria, loogista tietoliikenneverkkoa, sosiaalista kyberpersoonien ja ihmisten muodostamaa kerrosta vai ei mitään edellä mainituista? Mitä resursseja ja keinoja puolustamisessa on käytettävissä? Kuka on mahdollinen vihamielinen toimija ja miten vihamielinen toiminta tunnistetaan ajoissa ennen kuin puolustettava asia on menetetty vihamielisen, aluksi ehkä tuntemattoman toimijan haltuun?

Kybertaistelujen jäsentämiseen liittyviä olennaisia käsitteitä ovat tilanne sekä tilannetietoisuus ja -ymmärrys. Suomi-sanakirjan[25] mukaan tilanne on määrähetkenä vallitseva asiaintila tai hitaasti kehittyvä tai muuttuva asema. Sotilaallisesta näkökulmasta tilanne on käsite, joka kuvaa erilaisilla ajallisilla määreillä rajattavissa olevia tapahtumia sellaisessa aika-avaruudessa, jossa vähintään kaksi keskenään vuorovaikuttavaa oliota toimii ja jossa vähintään yhden toimijan tulevaisuuteen tähtäävä toiminta on yhteisesti ymmärrettävästi ilmaistu.[26] Tämä määritelmä sopii hyvin kybertoimintaympäristön tilanteen määritelmäksi ja toimii myös tarkistuslistana tilannekuvausta laadittaessa. Kybertoimintaympäristön tilanne siis sisältää menneisyyden tapahtumien kuvauksen lisäksi ymmärrettävää ilmaisua vähintään yhden toimijan tulevaisuuteen tähtäävästä toiminnasta.

Multinational Experiment 7 (MNE7) oli 2010-luvun alkupuolella toteutettu kansainvälinen viranomaisyhteistyökokeiluhanke, joka paneutui globaalien toimintaympäristöjen – merien, ilmatilan, avaruuden ja maailmanlaajuisten tietoverkkojen – käyttöön.

[25] Suomi-sanakirja (2013). http://www.suomisanakirja.fi, vierailtu 16.12.2013.
[26] Kuusisto, R. & Kuusisto, T. (toim.) (2005a) Yhteinen tilanneymmärrys – Strategis-operatiivisten päätösten tukipalvelujen perusteet. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 4, nro 2/2005, Helsinki.

MNE7-hankkeessa tilannetietoisuus määriteltiin Endsleyn[27] määritelmän perusteella.[28] Tämän määritelmän mukaisesti tilannetietoisuus on ympäristön elementtien tulkitseva havainnointi ajassa ja tilassa sekä ymmärrys niiden merkityksestä ja kuvaus niiden asemasta lähitulevaisuudessa. Tilannetietoisuus on siten tilanteen tapahtumien tulkintaa, ymmärrystä ja ennakointia. Tilannetietoisuus on tarkemmin määritelty tilanteen tulkinnaksi ulkoa tulevan tapahtumadatan ja omien resurssien perusteella sekä kykynä tietää miten nyt pitää toimia.[26] Tämä määritelmä korostaa päämäärän mukaista tavoitteellista toimintaa tilannetietoisuutta muodostettaessa.

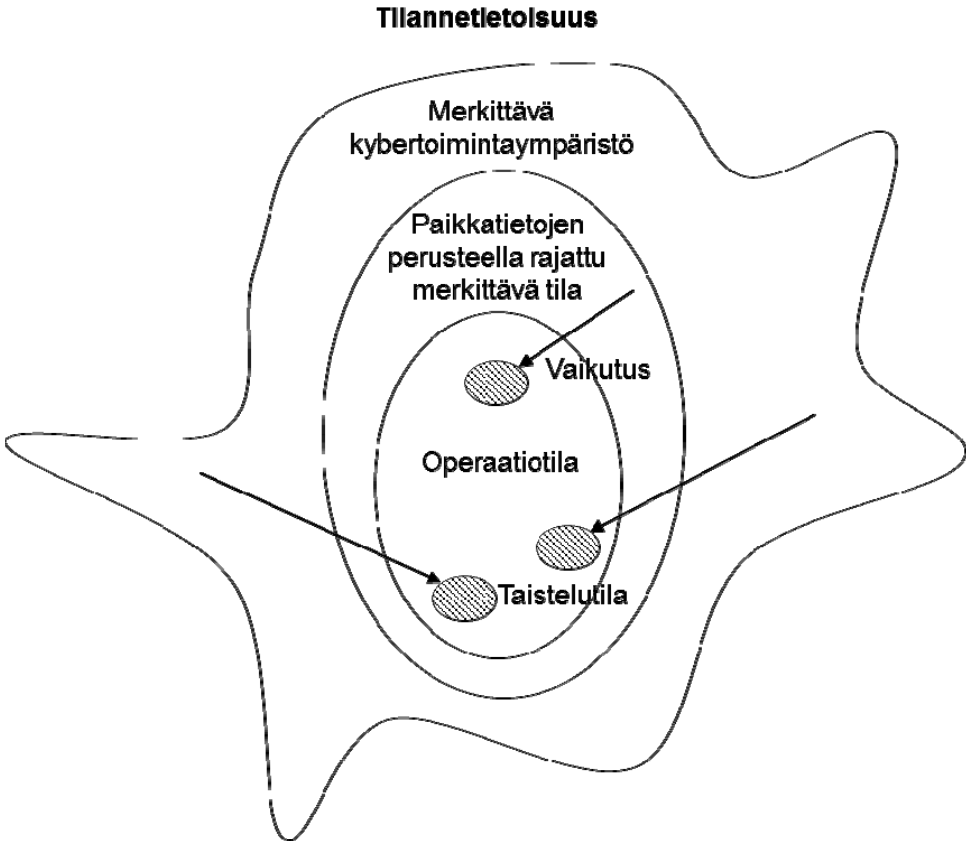
Tilanneymmärrys on tilannetietoisuutta laajempi käsite sisältäen tilanteen ja tilannetietoisuuden tulkinnan kokonaisympäristössä. Se perustuu itseen ja muuhun maailmaan tilanteessa vaikuttavien tekijöiden ja tilanteen kehittymisen tuntemiseen sekä kykyyn tietää miten tulevaisuudessa pitää toimia.[26] Kybertoimintaympäristössä kuten perinteisemmissäkin toimintaympäristöissä tulee siis pyrkiä sekä jatkuvaan tilanteen tulkintaan kokonaisympäristössä että ennakointiin paikallisesti ja ajallisesti välittömien tapahtumien ulkopuolelle.

Päätöksenteossa tarvittava tilannetietoisuuden ja -ymmärryksen sisältö on erilainen eri toiminnan tasoilla. Toiminnan tasoilla tarkoitetaan kansainvälisten organisaatioiden kuten YK, EU ja NATO tasoa, ylintä strategista valtiojohdon tasoa ja puolustusvoimien ylimmän johdon tasoa sekä operaatiotaidollista ja taktista sekä operoinnin ja taisteluteknistä tasoa. Ylimmillä strategisilla tasoilla tilannetietoisuus sisältää strategisen päätöksenteon ja toiminnan kannalta vaikuttavat tiedot, mukaan lukien kybertoimintaympäristöä koskevat tiedot. Sotilaallisten operaatioiden johdon tilannetietoisuus muodostuu operaation kannalta vaikuttavista kybertoimintaympäristön ja muiden toimintaympäristöjen tiedoista. Yksityiskohtainen kybertilannekuva on tällöin yksi lähde operaation johdon tilannetietoisuutta muodostettaessa. Operaation tieto- ja viestintäteknisestä toteutuksesta vastaavan kokoonpanon tasolla yksityiskohtainen, jatkuvasti ylläpidettävä kybertilannekuva muodostaa tilannetietoisuuden muodostamisen merkittävimmän osan.

Sotilaallisten operaatioiden näkökulmasta tilannetietoisuutta ja -ymmärrystä muodostettaessa huomioitava, yhteisoperaatioiden kannalta merkittävä kybertoimintaympäristö on usein laajempi kuin operaatiotila ja sen taistelutilat tai se paikkatietojen perusteella rajattu tila jolta operaatiotilaan voidaan fyysisesti vaikuttaa. Tätä on havainnollistettu kuvassa 1. Paikkatietojen perusteella rajatun merkittävän tilan laajuus samoin kuin merkittävän kybertilan laajuus riippuu uhkista joita operaatioita suunniteltaessa ja toteutettaessa otetaan huomioon. Esimerkiksi monen viranomaisen yhteistyössä toteutetuissa operaatioissa usein käytetään internetissä toimivia viestintävälineistä, joiden käyttöä voidaan haitata tai estää kaukanakin operaatiotilasta maantieteellisesti sijaitsevista paikoista. Sen sijaan kineettinen vaikutus usein on lähtöisin maantieteelliseltä lähialueelta, vaikka esimerkiksi miehittämättömiä lentäviä systeemejä voidaan ohjata kaukaakin niiden fyysisestä sijainnista katsottuna.

[27] Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems, Human Factors 37:1, http://uwf.edu/skass/documents/HF.37.1995-Endsley-Theory.pdf, vierailtu 15.1.2014
[28] MNE7 (2013) Campaing Lexicon 1.0, Multinational Experiment 7, 28.2.2013.

Kybertoimintaympäristössä voidaan tiedon avulla vaikuttaa yhdelle tai useammalle toiminnan tasolle. Koska eri toiminnan tasoilla päätöksenteossa tarvittava tilannetietoisuus poikkeaa sisällöllisesti toisistaan, niin siten myös eri toiminnan tasoilla tilannetietoisuuteen vaikutetaan erilaisella tiedolla. Esimerkiksi harhautus on käypä keino kybertaisteluissa. Harhautuksen toteuttaminen taisteluteknisellä toiminnan tasolla vaatii tyypillisesti lyhyellä aikavälillä toteutettua taistelutilan tapahtumia koskevaa disinformaation syöttämistä kybertoimintaympäristöön. Sen sijaan harhautus ylimmillä strategisilla tasoilla on usein pitkäjänteistä vaikuttamista strategisen kommunikaation keinoin.



Kuva 1. Tilannetietoisuutta muodostettaessa on huomioitava sekä operaatiotilassa ja operaatiotilaan vaikuttava kybertoimintaympäristö että paikkatietojen perusteella rajattu tila jolta operaatiotilaan voidaan kohdistaa fyysinen vaikutus.

Kybertoimintaympäristössä voidaan tietoon vaikuttamalla kohdistaa Suomen rajojen ulkopuolelta vaikutus Suomen alueella sijaitsevaan kohteeseen. Tältä vaikuttamiselta ei voida puolustautua pelkästään Suomen maantieteellisen alueen sisältä. Siten Suomessa tarvitaan vuonna 2020 kansallisia ja kansainvälisiä sopimuksia Suomen sotilaalliseksi puolustamiseksi ja kybertaisteluissa onnistumiseksi.

2.2.4 Tiedonhallinnasta

Yhteiskunnan digitalisoituminen sekä tieto- ja viestintäteknologian arkipäiväistyminen ovat muuttaneet tulkintoja ja luokitteluja sekä käsitteestä tieto että siihen liittyvistä käsitteistä ja termeistä. Tietoon liittyviä termejä käytetään usein päällekkäin ja niiden välinen ero on epäselvä. Tieto jaetaan tyypillisesti ainakin dataksi ja informaatioksi, mutta esimerkiksi avoin data ja avoin tieto ovat usein synonyymeinäkin käytettyjä termejä. Kybertoimintaympäristön tiedonhallinnan näkökulmasta on kuitenkin olennaista ymmärtää datan, informaation ja tietämyksen merkitykset. Data määritellään tavallisesti yleisesti tunnetuiksi faktoiksi, jotka voidaan tallentaa ja joilla on implisiittinen merkitys.[29] Suomi-sanakirjan[25] mukaan informaatio on tiedotus, tiedonanto ja neuvo. Tietämys on tiedot kokonaisuutena ja tietous.[25] Informaatiotutkimuksessa käytetään usein tiedon arvoketjua data, informaatio, tieto, tietämys ja viisaus, ks.[30]. Kuusisto[31] analysoi näitä termejä ja toteaa että viisaus on tietoisen olennon ominaisuus ja eroaa siten muista tiedon arvoketjun luokista. Tiedon perusluokat ovat siten data, informaatio ja tietämys.

Kybertoimintaympäristön tiedonhallintaan kuuluu datan, informaation ja tietämyksen kerääminen, tuottaminen, säilyttäminen, käsittely, jakaminen ja hävittäminen kybertoimintaympäristössä. Tiedonhallintaan liittyy tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaaminen ja tiedon salaamiseen, harhauttamiseen ja tuhoamiseen kohdistuvien toimintojen ennaltaehkäisy ja mahdollisista hyökkäyksistä toipuminen.

Viime vuosina tiedonhallinnan kehittämisen painopistealueita ovat olleet sisältöjen hallinta ja sosiaalinen media sekä kybertiedustelu, pilvipalvelut, liikkuvilla päätelaitteilla käytettävät palvelut sekä tieto- ja kyberturvallisuus. Sisältöjen hallintaan liittyvät avoin tieto ja massadata eli big data, jotka eduskunnan tulevaisuusvaliokunnan tilaamassa ennakoinnissa[10] on arvioitu kansallisesti Suomelle yhdeksi tärkeimmistä tulevaisuuden teknologisista ratkaisuista. Avoimella tiedolla tarkoitetaan tyypillisesti tietovarantoja, jotka ovat vapaasti käytettävissä ja kierrätettävissä avoimella lisenssillä. Avoimelle aineistolle määritellyt ehdot ovat saavutettavuus, uudelleenjakelu, uudelleenkäyttö, vapaa teknisistä rajoitteista, viittaaminen, integriteetti, ei henkilöiden tai ryhmien diskriminaatiota, ei diskriminaatiota käyttökohteiden suhteen, lisenssin jakelu, lisenssi ei saa olla kokoelmakohtainen ja lisenssi ei saa rajoittaa muiden aineistojen jakelua.[32] Usein avoimeksi tiedoksi kutsutaan tietovarantoja, joka eivät täytä kaikkia edellä kuvattuja ehtoja. Länsimaissa tiedon avoimuutta edistetään julkishallinnossa ja tieteessä. Suomessa avointa tietoa hallinnossa edistetään Avoimen tiedon ohjelmassa[33], joka liittyy laajempaan avoimen hallinnon käsitteeseen. Avoin hal-

[29] Elmasri, R. & Navathe, S. B. (2010) Fundamentals of Database Systems, 6th edition. Addison-Wesley.
[30] Haasio, A. & Savolainen, R. (2004). Tiedonhankintatutkimuksen perusteet, BTJ Kirjastopalvelu, Helsinki, 193 s.
[31] Kuusisto, R. (2004). Aspects on Availability, A Teleological adventure of information in the lifeworld. Edita Prima Oy, Helsinki, 124p.
[32] Open Knowledge Foundation (2014). The Open Knowledge Definition, http://opendefinition.org/od/suomi/ , vierailtu 17.1.2014.
[33] VM (2014) Avoimen tiedon ohjelma. http://www.vm.fi/vm/fi/05_hankkeet/02381_avoin_tieto/ndex.jsp, vierailtu 17.1.2014.

linto muodostuu avoimen datan, avointen prosessien ja avointen palvelujen kokonaisuudesta.[34]

Massadatalla eli big datalla ei ole vakiintunutta määritelmää. Gartner[35] määrittelee massadatan suureksi määräksi nopeasti muuttuvia erilaisia tietovarantoja, joiden käyttö ymmärryksen muodostamista ja päätöksentekoa varten tarvitsee kustannustehokkaita ja innovatiivisia tietojenkäsittelyn tapoja. Liiketoiminnassa massadatan sovellusalueiksi nähdään asiakkaista runsaasti tietoa keräävät yritykset kuten vähittäiskauppa ja teleoperaattorit. Avoimen datan ja massadatan laajamittainen käyttö on vasta alussa. Siten on oletettavissa että vuoteen 2020 mennessä niiden käyttö kasvaa huomattavasti.

Kybertiedustelu on kybermenetelmien käyttöä tiedustelussa sekä tiedustelua kybertoimintaympäristön fyysisessä, loogisessa ja sosiaalisessa kerroksessa. Kybertiedustelussa hyödynnetään myös avointa dataa ja massadataa ja sen tuottamia tietoja käytetään sekä operaatioissa kybertoimintaympäristössä että maalla, merellä, ilmassa ja avaruudessa tapahtuvissa operaatioissa.

Päätöksenteon näkökulmasta kybertoimintaympäristön tiedonhallinnan tavoitteena on tuottaa päätöksentekijälle tietoa siitä mistä asioista ja milloin on päätettävä sekä mitä edellytyksiä kybertoimintaympäristö asettaa ja mitkä ovat faktapohjaiset päätösvaihtoehdot. Tässä ei onnistuta keräämällä tai hävittämällä kaikki mahdollinen data. Tarvitaan edellisessä luvussa käsiteltyä kattavaa tilanneymmärrystä eli sekä jatkuvaa tilanteen tulkintaa kokonaisympäristössä että ennakointia paikallisesti ja ajallisesti välittömien tapahtumien ja tunnettujen keinojen ulkopuolelle.

Datan keruu, siirtäminen ja jakelu eivät riitä, vaan tarvitaan järjestelmissä ja ihmisissä olevaa kykyä muuntaa data informaatioksi ja tietämykseksi. Tulevaisuudessa datan analysoimiseen on tarjolla entistä kehittyneempiä menetelmiä. Tätä kehitystä avoin tieto ja massadata vauhdittavat. Erityisesti vuonna 2020 tarvitaan kybertoimintaympäristön sisältöanalyysejä: Parametrien ja indikaattorien tunnistamista ja niiden pohjalta tehtyjä kokonaistilanteen huomioivia arviointeja ja ennakointeja. Seuraavassa luvussa kuvataan joitakin systeemimallinnuksen lähestymistapoja datan abstrahointiin ja ilmiöiden tunnistamiseen.

Kybertoimintaympäristön kehittyminen mahdollistaa entistä vaivattomamman tietojen keräämisen ja jakamisen. Tämän johdosta kunkin toimijan keräämien tietojen luotettavuuteen, eheyteen ja saatavuuteen kohdistuu kasvavaa huomiota. Kybertaisteluissa ja kybertoimintaympäristön kautta tapahtuvassa vaikuttamisessa toimija voi saada merkittävästi etua kyetessään hankkimaan pääsyn jonkin toisen toimijan analysoimaan tai teknologisen palvelun keräämään tietoon. Erityisesti tietoturvapalvelujen tarjoajiin kohdistuu merkittäviä odotuksia ja haasteita tiedustelun ehkäisyä ja laajemmin kaikkia tietoturvallisuuden ominaisuuksia koskien. Tarvitaan myös viranomaisten suorittamaa valvontaa, joka turvaa mahdollisuuden yhteiskunnan elintärkeiden toimintojen turvaamiseen ja pääsyyn globaaliin kybertoimintaympäristöön.

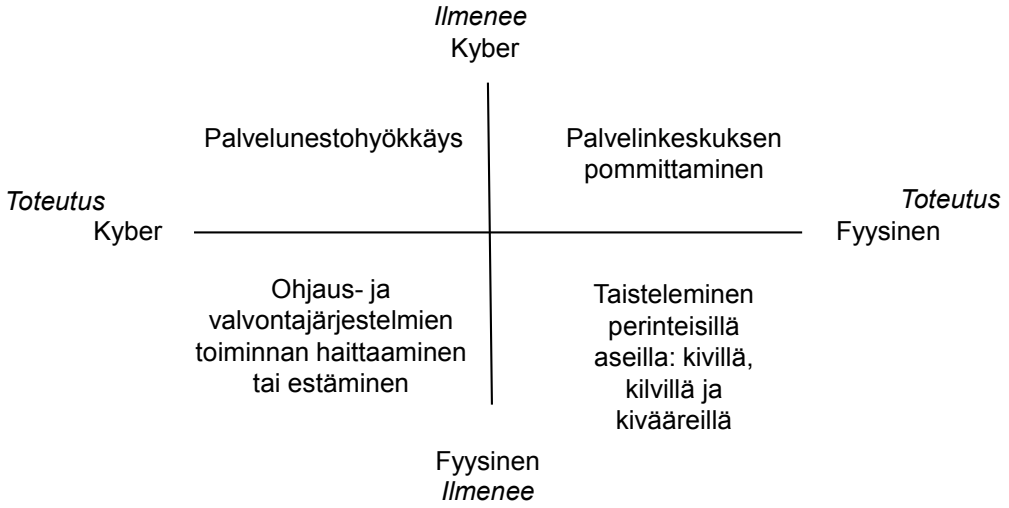
[34] European Commission (2013). A vision for public services, draft version dated 13/06/2013. http://ec.europa.eu/digital-agenda/en/news/vision-public-services, vierailtu 18.6.2014.
[35] Gartner (2014). Gartner IT Glossary. http://www.gartner.com/it-glossary/big-data/, vierailtu 17.1.2014.

Valvonnalla ehkäistään ja tunnistetaan kybertoimintaympäristön käyttäminen säädösten vastaiseen tai jopa rikolliseen toimintaan tai Suomen sotilaallista puolustamista uhkaavaan tarkoitukseen.

2.3 Kybertoimintaympäristön systeemimallinnuksesta

2.3.1 Fyysisen maailman ja kybertoimintaympäristön kehikko

Kybertoimintaympäristön tapahtumat voivat vaikuttaa sekä kybertoimintaympäristössä että sen ulkopuolisiin asioihin fyysisissä toimintaympäristöissä. Toisaalta kybertoimintaympäristön ulkopuolelta voidaan vaikuttaa kybertoimintaympäristöön. Kybertoimintaympäristön ja fyysisen maailman rajapinta voidaan mallintaa käyttämällä yksinkertaista fyysisen maailman ja kybertoimintaympäristön kehikkoa.[36] Tämä kuvassa 2 näkyvä kehikko koostuu neljästä kentästä: fyysinen-fyysinen, fyysinen-kyber, kyber-kyber ja kyber-fyysinen.



Kuva 2. Fyysisen maailman ja kybertoimintaympäristön kehikko; muokattu[36]

Kukin tapahtuma voidaan mallintaa toimeenpantavaksi ja realisoituvaksi yhdessä näistä kentistä. Kehikko on työkalu, jota voidaan käyttää esimerkiksi kun tahdotaan varmistaa että sekä kybernäkökulma että fyysisen maailman näkökulma on otettu huomioon vaatimusmäärittelyssä. Esimerkiksi taisteluissa, joissa käytetään ilman tieto- ja viestintäteknologiaa toimivaa aseistusta kuten kirveitä, miekkoja, kilpiä tai perinteisiä ampuma-aseita on tapahtumia, jotka sekä toimeenpannaan että realisoituvat fyysisessä maailmassa. Palvelinkeskuksen pommittaminen ja tuhoaminen tai tiedonsiirtoyhteyksien fyysinen katkaiseminen ovat esimerkkejä tapahtumista, jotka toimeenpannaan fyysisessä maailmassa mutta jotka realisoituvat kybertoimintaympäristössä. Palvelunestohyökkäys, joka kohdistuu vaikkapa tilannekuvajärjestelmää ylläpitäviin palvelimiin tai sähköpostiviestien tiedustelu ovat esimerkkejä tapahtumista, jotka sekä toimeenpannaan että realisoituvat kybertoimintaympäristössä. Ohjaus- ja valvontajärjestelmien kuten ilmavalvonnan järjestelmien toiminnan haittaaminen tai estäminen haittaohjelmilla on esimerkki tapahtumasta, joka toimeenpannaan kyber-

[36] Kuusisto, R. & Kuusisto, T. (2013a). 'Strategic Communication for Cyber-Security Leadership'. The Journal of Information Warfare, vol. 12, issue 3, pp. 41 - 48.

toimintaympäristössä, mutta joka realisoituu fyysisessä maailmassa jopa ohjattavien tai valvottavien kohteiden fyysisenä tuhoutumisena.

Viime aikoina kiinnostus kybertoimintaympäristöstä fyysiseen maailmaan vaikuttaviin tapahtumiin on kasvanut. Käytetään termiä kineettinen kyber, jolla tarkoitetaan fyysisessä maailmassa ilmeneviä tapahtumia, jotka on saatu aikaan kybertoimintaympäristössä toteutetulla toiminnalla. Kriittisimpiä ovat laajalle leviävät seurausvaikutukset, jotka voivat aiheutua yhdestäkin kybertoimintaympäristön vaurioituneesta järjestelmästä. Esimerkiksi vaurio energiantuotantojärjestelmässä saattaa välittömästi aiheuttaa vakavaa haittaa tai jopa pysäyttää useita yhteiskunnan kriittisiä toimintoja.

2.3.2 Sosiaalisen systeemin malli

Rauno Kuusiston väitöskirjassaan vuonna 2004[31] kuvaama sosiaalisen systeemin malli on johdettu Parsonsin[37] ja Habermasin[38] tieteellisestä työstä. Mallin jatkokehitystä on kuvattu artikkelissa Kuusisto & Kuusisto 2009[39]. Kuvassa 3 oleva malli[40,41] on kokonaisvaltainen yhteiskunnan tai organisaation dynaaminen kuvaus. Mallia on sovellettu tietoturvallisuustutkimuksessa[31] ja sitä on myös käytetty tilannetietoisuuden tutkimuksessa[26,40] sekä tietoturvallisuuskulttuurien tutkimuksessa[39,41]. Viimeksi mallia on sovellettu kybermaailman ominaisuuksien ja ilmiöiden hahmottamisessa[24] ja tunnistettujen kybermaailman ilmiöiden käyttämisessä strategisen kommunikoinnin suunnittelussa[36,42].

Mallin lähtökohtana on Aristoteleen ajoilta tunnettu käsitys siitä että kaikki systeemit koostuvat rakenteesta, toiminnoista ja tiedoista. Mallissa yhteiskunnan tai organisaation tiedot, rakenteet ja toiminnot on kukin jaettu neljään luokkaan. Mallissa alin kerros sisältää tietoa, keskikerros rakenteita ja ylin kerros toimintaa. Kuten kuvaan 3 on piirretty, niin sosiaalisen systeemin mallin perusajatus on se, että tieto rakenteessa aiheuttaa toimintaa ja rinnakkaiset rakenteet ovat vuorovaikutuksessa keskenään. [40]

Habermas[38] viittaa Parsonsiin[37] ja toteaa että toimijan toimintaa ohjaavat tiedot koostuvat neljästä perusluokasta: arvoista, nykyhetken faktoista, päämääristä ja normeista.[31] Samoin hän toteaa, että sosiaalisten systeemien rakenne koostuu kulttuurista, organisaatiosta, hallintorakenteesta ja yhteisöstä. Nykyhetken faktoja käyttävät ja arvoja muuttavat toiminnot ovat sopeutuminen, tavoitteen saavuttaminen, integroituminen sekä toimintatapojen ylläpitäminen ja säätäminen.[38,31] Kulttuuriset rakenteet ovat hitaammin muuttuvia kuin yhteisölliset, jotka ovat pysyvämpiä kuin hallintoraken-

---

[37] Parsons T. (1951). The Social System, Glencoe.

[38] Habermas, J. (1984). The Theory of Communicative Action, Volume 1: Reason and the Rationalization of Society. Beacon Press, Boston, USA.
Habermas, J. (1989). The Theory of Communicative Action, Volume 2: Lifeworld and System: A Critique of Functionalist Reason. Beacon Press, Boston, MA, USA.

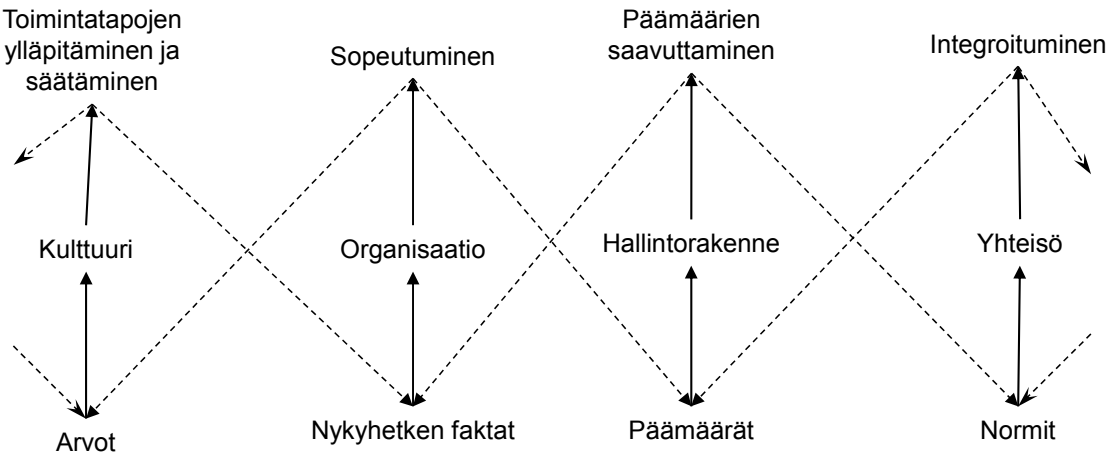
[39] Kuusisto, R., Kuusisto, T. (2009). “Information Security Culture as a Social System”. In Gupta, M. & Sharman, R. Social and Human Elements of Information Security. Information Science Reference, IGI Global, Hershey, New York, pp. 77 - 97.

[40] Kuusisto, R., Kuusisto, T. (2007). Tilannekuvasta. Tiede ja ase, Suomen Sotatieteellisen Seuran vuosijulkaisu N.o 65, 2007, s. 363 - 378.

[41] Kuusisto, R. (2007). Tietoturvakulttuurin johtaminen. Julkaisussa: Ståhle, P. (toim.) Tieto ja osaaminen kilpailuetuna, Business Review 3/2007. 27s.

[42] Kuusisto, T. & Kuusisto, R. (2013b). ’Strategic Communication for Supporting Cyber-Security’. In Warren, M. (ed.) International Journal of Cyber Warfare and Terrorism, 3 (3): 72 - 79.

teet, jotka ovat pysyvämpiä kuin organisaatiot. Habermasin[38] ajattelussa organisaatioksi nimettynä rakenteena on talous. Organisaatioksi voidaan kuitenkin käsittää mikä tahansa resursseja käyttävä kokonaistoimijan alisysteemi. Esimerkiksi koko suomalaista yhteiskuntaa tarkasteltaessa hallintorakenne on Suomen hallintorakenne ja yksi organisaatio on valtioneuvosto ministeriöineen. Jos valittuna rakenteellisena tasona ovat puolustusvoimat, niin organisaatioina ovat puolustusvoimien organisaatiot.



Kuva 3. Sosiaalisen systeemin malli; muokattu[40,41]

Habermasin[38] näkemyksen mukaan sosiaalinen systeemi pyrkii asettumaan tilaan, jossa yhteisesti hyväksyttyihin normeihin mukautuva yhteisö asettaa yhteisesti hyväksyttävissä olevia tavoitteita hallintorakenteensa mukaisesti. Kuvassa 3 tämä näkyy tiedon virtaamisena kunkin sosiaalisen systeemin mallin sarakkeen tietoluokasta rakenteiden läpi suodattuneena ohjaamaan saman sarakkeen toimintaa.[40] Arvot siis ohjaavat kulttuurin kautta toimintatapojen ylläpitämistä ja säätämistä, nykyhetken faktat ohjaavat organisaation kautta sopeutumista, päämäärät ohjaavat hallintorakenteiden kautta päämäärien saavuttamista ja normit ohjaavat yhteisön kautta integroitumista. Kukin toiminta tuottaa tietoa myös vierekkäisille rakenteille eli sopeutuminen tuottaa tietoa arvoihin ja päämääriin, päämäärien saavuttaminen tuottaa tietoa nykyhetken faktoihin ja normeihin, integroituminen tuottaa tietoa päämääriin ja arvoihin sekä toimintatapojen ylläpitäminen ja säätäminen tuottaa tietoa normeihin ja nykyhetken faktoihin.

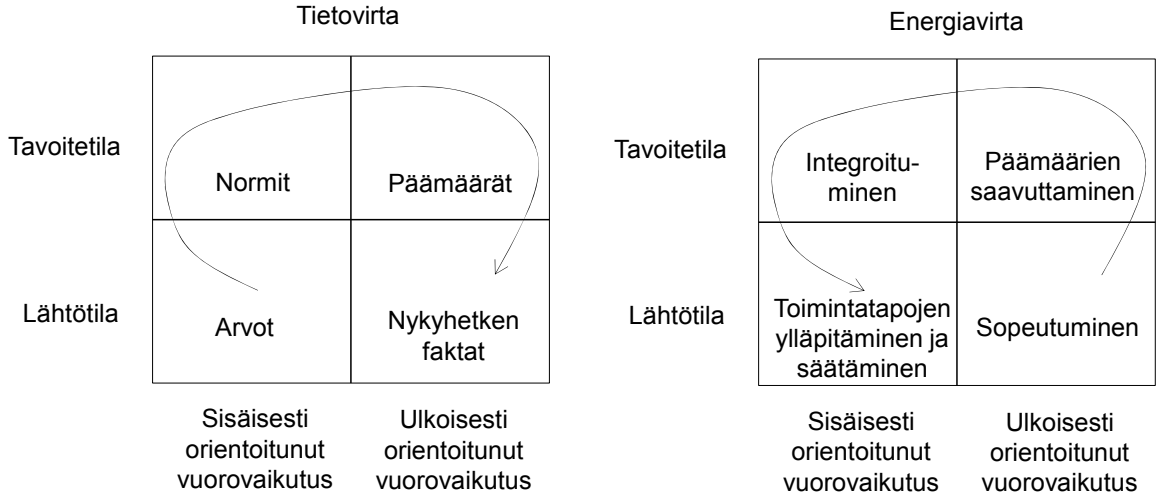
Tiedon virtaamista sosiaalisen systeemin mallissa on havainnollistettu kuvassa 4. Tieto virtaa[43,37] arvoista kulttuurin sekä toimintatapojen säätämisen ja ylläpitämisen kautta normeihin, josta edelleen yhteisön ja integroitumisen kautta päämääriin ja lopulta nykyhetken faktoihin. Tieto virtaa myös päinvastaiseen suuntaan eli sopeutumisesta päämäärien ja hallintorakenteiden kautta päämäärien saavuttamiseen ja edelleen normien, yhteisön ja integroitumisen kautta arvoihin, toimintatapojen ylläpitämiseen ja säätämiseen, nykyhetken faktoihin ja sopeutumiseen.

Habermas[38] toteaa, että jokaisella systeemillä on lähtötilanne ja tavoitetilanne sekä sisäistä ja ulkoista vuorovaikutusta. Kuten kuvasta 4 näkyy, niin sosiaalisen systeemin mallin kaksi vasemmanpuoleisinta saraketta kuvaavat lähtötilaa ja mallin kaksi oikeanpuoleisinta saraketta kuvaavat tavoitetilaa. Mallin vasemman- ja oikeanpuolei-

[43] Bergson, H. (1911). Creative Evolution, University Press of America.

sin sarake kuvaavat sisäisesti orientoitunutta vuorovaikutusta ja mallin kaksi keskimmäistä saraketta kuvaavat ulkoisesti orientoitunutta vuorovaikutusta.[31]

Sosiaalisen systeemin mallin luokkien sisältö on erilainen eri toimijoilla. Luokkien sisältö myös muuttuu ajan kuluessa kun ulkoinen ja sisäinen vuorovaikutus muuttavat toimijoita. Myös luokkien suhteelliset merkitykset eri toimijoille ovat erilaisia eri tilanteissa ja eri ajanhetkinä. Esimerkiksi valtion johdon asettamat uudet päämäärät aiheuttavat toimintaa yhteiskunnassa hallintorakenteiden kautta. Jos uusia päämääriä asetetaan paljon, niin päämäärien saavuttaminen toimintana korostuu edellyttäen, että normit ja nykyhetken faktat sisältäen resurssit tukevat tai muuttuvat tukemaan päämäärien saavuttamista.



Kuva 4. Tietovirrat sosiaalisessa systeemissä; perustuu[43,37,31]

2.3.3 Sosiaalisen systeemin mallin soveltaminen kybertoimintaympäristöön

Kybertoimintaympäristön toiminnot ja rakenteet muuttuvat jatkuvasti eikä ole olemassa ajanhetkeä jolloin kybertoimintaympäristön kaikki yksityiskohdat voitaisiin tietää. Nämä kybertoimintaympäristön piirteet ovat kompleksisten systeemien ominaisuuksia.[24] Kuten Kauffman[44] ja Ball[45] kuvaavat, niin kompleksisuus tarkoittaa sitä, että vuorovaikuttavien olioiden ja prosessien kokonaisuus ei ole täysin tai läpikotaisin tunnettu eikä tarkan tai jopa minkään kontrollin alainen. Kompleksisten adaptiivisten systeemien (CAS)[23] teorian tavoitteena on selittää yhden toimijan näkökulmasta monitoimijaisen, vuorovaikutteisen systeemin kaoottista luonnetta. Kybertoimintaympäristö on kompleksinen ja adaptiivinen systeemi.[24] Siten CAS-teorioita voidaan soveltaa ymmärryksen lisäämiseksi kybertoimintaympäristön ilmiöistä ja piirteistä.

Kompleksisille systeemeille on luonteenomaista, että ne tuottavat kehkeytyviä ilmiöitä. Kompleksista systeemeistä voidaan hankkia tietoa havainnoimalla näitä vasta muotoutumassa olevia ilmiöitä valittuun näkökulmaan sopivalta rakenteelliselta tasol-

[44] Kauffman S. (1995). At Home in the Universe: The Search for the Laws of Self-Organization and Complexity. Oxford University Press.
[45] Ball P (2004). Critical Mass: how one thing leads to another. London, UK, Sydney, Australia, Auckland, New Zeland: Arrow Books.

ta, ks. [44, 45, 46]. Kompleksisen systeemin sisältöanalyysi[47] siten että käytetään sosiaalisen systeemin mallia[31], on yksi mahdollinen lähestymistapa tunnistaa muotoutumassa olevia ilmiöitä.[24]

Sosiaalisen systeemin mallia sovellettiin Suomessa vuonna 2013 järjestettyjen kyberturvallisuusharjoitusten arviointitietojen sisältöjen analysointiin. Tässä tarkastelussa rakenteellisen tasona oli koko valtion johtaminen. Sosiaalisen systeemin malli sopii lähestymistavaksi tunnistaa kybertoimintaympäristössä kehittymässä olevia ilmiöitä, koska kybertoimintaympäristön tapahtumat ovat pelkistettävissä ihmisten väliseksi toiminnaksi ja sosiaalisen systeemin malli kuvaa ihmisyhteisöä. Kybertoimintaympäristö on levittäytynyt kaikille alueille, joten kybertoimintaympäristön ilmiöitä on perusteltua tarkastella valtion johtamisen tasolla.

Tämän artikkelin kirjoittaja poimi vuoden 2013 suomalaisten kyberturvallisuusharjoitusten arviointimateriaalista analysoitavaksi seuraavia dokumentteja: Yhden arviointiryhmän laatima kooste keskeisistä havainnoista, yhden arviointiryhmän johtajan muodostama esittely keskeisistä havainnoista sekä yksi yhteenveto kahden työryhmän suorittamasta arvioinnista ja jatkokehittämisajatuksista. Analysoitu dokumentaatio sisältää pääasiassa yhteiskunnan kokonaisturvallisuuden edistämistä koskevia havaintoja kybertoimintaympäristön näkökulmasta. Dokumentaation mallinnuksen tulos kuvassa 3 esitetyllä sosiaalisen systeemin mallilla Krippendorffin[47] kuvaaman sisältöanalyysitutkimustekniikan mukaisesti on kuvattu taulukossa 1.[42]

Kyberturvallisuusharjoituksista kerätyn aineiston sisältöanalyysin perusteella voidaan todeta, että hallinnossa on tarve organisoitua uudella tavalla ja luoda uuteen tilanteeseen soveltuva päätöksentekojärjestelmä. Tämä on yleinen tarve kaikissa tilanteissa, jossa toimintaympäristö muuttuu. On myös huomattava, että harjoituksissa yhtenä tavoitteena oli hallinnon ja yrityssektorin yhteistoiminnan kehittäminen kyberuhkatilanteissa. Siten oli odotettavissa, että kehittämistoimenpiteitä löytyy hallintorakenteesta ja organisoitumisesta. Toisaalta myös Kärkkäinen[48] toteaa, että yksi kyberturvallisuuden pääongelmista on vastuun jakautuminen kullekin hallinnonalalle hallinnonalan omien järjestelmien turvallisuuden osalta. Vastuu on jakautunut usean toimijan kesken eikä kenelläkään ole kokonaisvastuuta.

[46] Moffat, J. (2003). Complexity Theory and Network Centric Warfare, CCRP, USA.
[47] Krippendorff, K. (2013). Content analysis: an introduction to its methodology, 3rd edition. Sage, Newbury Park, CA, USA.
[48] Kärkkäinen (2013). The origins and the Future of Cyber Security in the Finnish Defence Forces. In Rantapelkonen, J. & Salminen, M. The Fog of Cyber Defence. National Defence University, Department of Leadership and Military Pedagogy, Series 2: Article Collection N:o 10.

Taulukko 1. Kehittämisalueet (%) Suomessa vuonna 2013 toteutetuissa kyberturvallisuusharjoituksissa.[42]

	Vuorovaikutus on sisäisesti orientoitunut	*Vuorovaikutus on ulkoisesti orientoitunut*		*Vuorovaikutus on sisäisesti orientoitunut*
toiminta	Toimintatapojen ylläpitäminen ja säätäminen	Sopeutuminen	Päämäärien saavuttaminen	Integroituminen
	0	10	9	4
rakenne	Kulttuuri	Organisaatio	Hallintorakenne	Yhteisö
	1	18	34	9
tieto	Arvot	Nykyhetken faktat	Päämäärät	Normit
	0	3	3	9
	Lähtötila		Tavoitetila	

Sisäisesti orientoituneen vuorovaikutuksen alueen toiminnoissa, rakenteissa tai tiedossa ei nähty merkittävää kehittämistarvetta. Erityisesti arvot ja kulttuuri sekä toimintamallien ylläpitäminen ja säätäminen vaikuttavat olevan alueita, joista ei nouse esille kehittämiskohteita. Normien alueella havaittiin jonkin verran kehittämistarpeita. Normien laadintatarpeet olivat olleet jo ennen harjoitusten toteuttamista esillä sekä julkisessa keskustelussa että valtionhallinnossa säädösvalmistelussa, mistä saattaa johtua se että lainsäädännön valmistelutarpeita ei näissä harjoituksissa niin voimakkaasti tuotu esille.

Sisältöanalyysissä haastavimmaksi osoittautui asioiden sijoittaminen rakenneluokkiin koskien erityisesti rajanvetoa organisaatio- ja hallintorakenne-luokkien välillä. Organisaatio-luokkaan mallinnuksessa luokiteltiin Suomen valtionhallinnon sekä yksityisen sektorin Suomessa vaikuttavien lähinnä tieto- ja viestintäteknologian alan yritysten organisoitumiseen ja eri toimijoiden väliseen yhteistyöhön liittyvät asiat. Hallintorakenne-luokkaan luokiteltiin hallinnolliseen valmisteluun ja päätöksentekoon liittyvät asiat painottuen ylimpiin hallintorakenteisiin liittyviin asioihin. Yhteisö-luokkaan luokiteltiin ihmisten väliseen vuorovaikutukseen liittyvät asiat huomioiden erityisesti kybermaailmassa toteutettu vuorovaikutus ihmisten välillä. Kulttuuri-luokkaan luokiteltiin kulttuurin pohjalta tapahtuvaan tulkintaan liittyvät asiat. Tämän tutkimuksen perusteella hallinto- ja organisaatiorakenteet kybertaisteluissa vaativat edelleen tutkimista.

Suomessa on viime vuosina toteutettu kriisijohtamisen kehittämistä. Varautumista varten on perustettu turvallisuuskomitea ja vuoden 2014 keväällä ministeriöille on hyväksytty kyberturvallisuustehtävät[21], mitkä ovatkin askeleita eteenpäin. Taulukossa 1 olevan analyysituloksen perusteella vuoteen 2020 mennessä arvioidaan tapahtuvan jonkin verran aikaisempaa enemmän vallitsevaan tilanteeseen sopeutumista ja merkittävästi enemmän asetettujen tavoitteiden saavuttamiseen tähtäävää toimintaa. Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelman[49] toteuttamisella voi onnistuessaan olla merkittävä vaikutus tavoitteiden saavuttamiseen tähtäävässä toi-

[49] Turvallisuuskomitea (2014). Kansallinen kyberturvallisuusstrategian toimeenpano-ohjelma. 11.3.2014. www.turvallisuuskomitea.fi, vierailtu 24.3.2014.

minnassa. Erityisesti tarvitaan yhteisesti hyväksyttyä tietopohjaa koskien kaikkia tietoluokkia: arvoja, nykyhetken faktoja, päämääriä ja normeja jotta saadaan luotua kestävä perusta kyberyhteisöön integroitumiseksi. Tällä on merkittävä vaikutus yhteiskunnan kokonaisturvallisuuteen ja elintärkeiden toimintojen turvaamiseen.

Toimintaprosessien kehittäminen on yksi tapa edistää hallinto- ja organisaatiorakenteiden selkiyttämistä. Puolustusvoimien näkökulmasta yksi merkittävä prosessi on Suomessakin käyttöön otettu Naton vuonna 2010 kuvaama yleinen operaatioiden suunnitteluprosessi[50]. Kybertaistelujen mahdollisuudet ja uhat voidaan ottaa kokonaisvaltaisesti huomioon kun tätä suunnitteluprosessia käytettäessä myös kybertoimintaympäristöön liittyviä tietoja käsitellään prosessin kaikissa vaiheissa. Seuraavassa luvussa tarkastellaan tarkemmin suunnittelu- ja päätöksentekoprosesseissa tarvittavien tietojen luokittelua ja tietotarpeita.

2.4 Kybertoimintaympäristön toimijoiden tietoprofiileista

Kybertoimintaympäristössä toimittaessa tarvitaan tyypillisesti jatkuvaa tilannetietoisuuden ylläpitämistä ja yhteistyötä sekä eri viranomaisten että julkisen hallinnon ja yksityisen sektorin toimijoiden välillä. Tavoitteellisesti toimivan organisaation sisäisiä tietovirtoja on Suomessa tutkittu 2000-luvulla ja tutkimusten tuloksena on ollut yleinen tietovirtamalli.[31,51] Mallia on tämän jälkeen sovellettu useissa kriisitilanteiden ja verkostopuolustuksen monen toimijan ympäristön tietotarpeiden tutkimuksessa.[26,52] Mallia on edelleen jalostettu toimijoiden välisen yhteistyön ja tiedonvaihdon näkökulmasta ja sovellettu kansainvälisissä, moniviranomaisyhteistyötä tutkineissa Multinational Experiment 5 ja 7 (MNE5)[53,54] ja (MNE7)[55] kokeiluhankkeissa sekä Barents Rescue 2007[54] harjoituksessa. Näihin tutkimuksiin perustuvia tiedonvaihdon malleja on hiljattain sovellettu myös tiedonintressien profiilien muodostamisessa hätäkeskus-

---

[50] NATO (2010a). Allied Command Operations Comprehensive Operations Planning Directive, COPD Interim V1.0, 17.12.2010, Supreme Headquarters Allied Power Europe, Belgium, http://publicintelligence.net/nato-copd/, vierailtu 16.1.2014.

[51] Kuusisto, R. (2006). Flowing of Information in Decision Systems, In proc. of 39th Hawaiian Conference on Information Systems Sciences, (HICSS-39), USA January 2006

[52] Kuusisto, T. & Kuusisto, R. (2005b). The Management of Geographic Information Flows in Crisis Situations. Proc. of the 11th Americas Conference on Information Systems, Omaha, NE, USA, 2005, pp. 1659–1667.

Kuusisto, T., Kuusisto, R. (2006). System Modeling Approach to Network-Enabled Defense. Proceedings of 2006 Command and Control Research and Technology Symposium (CCRTS), San Diego, USA, June 20 - 22, 2006.

Kuusisto, T., Kuusisto, R., Nissen, M. (2007). Information Flow Aspects of Inter-organizational Crisis Management. In: Journal of Information Warfare. Vol. 6, issue 2, 2007, pp. 39 - 51

[53] Kuusisto, R. (2008a). “SHIFT” Theoretically-Practically Motivated Framework, Information exchange viewpoint on developing collaboration support systems. Maanpuolustuskorkeakoulu, Taktiikan ja operaatiotaidon laitos, Sarja 3, No 1/2008, 74p.

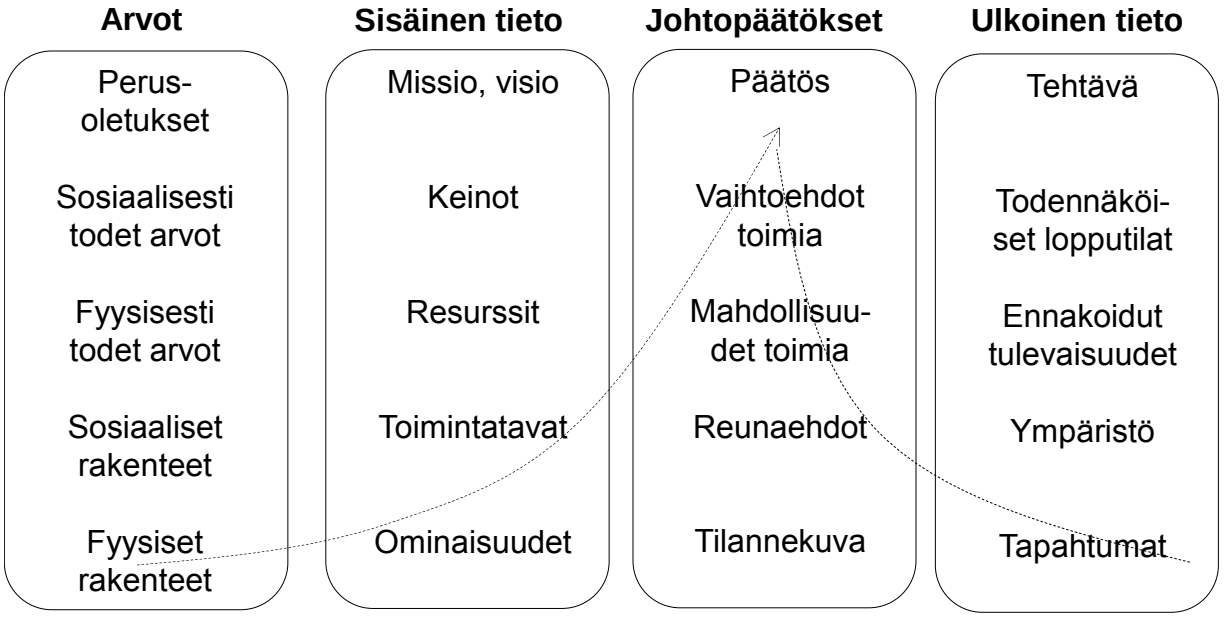
Kuusisto, R. (2008b). Analyzing the Command and Control Maturity Levels of Collaborating Organizations. In: Proceedings of 13th International Command and Control Research and Technology Symposium (13th ICCRTS), Bellevue, WA, USA, 17 -19 June 2008.

[54] Kuusisto, R. (2010). User Approach to Knowledge Discovery in Networked Environment. In: Syväjärvi, A. & Stenvall, J. (eds.) Data Mining in Public and Private Sectors. Information Science Reference, IGI Global, Hershey, New York, pp. 358 - 374.

[55] Kuusisto, R. (2012). Information Sharing Framework for Agile Command and Control in Complex Inter-domain Collaboration Environment. In Proc of 17th International Command and Control Research and Technology Symposium, USA.

ten toimijoiden tilannetietoisuutta varten.[56] Tutkimusten tuloksena syntynyt ihmisten tiedonvaihdon malli näkyy kuvassa 5. Mallin tietoluokkien kuvaukset ovat taulukossa 2.

Ihmisten tiedonvaihdon malli on suunnittelussa ja päätöksenteossa tarvittavan tiedon systemaattinen kuvaus. Se perustuu filosofian, viestinnän, sosiologian, kognitiotieteen, organisaatiokulttuurien, tietämyksen hallinnan ja päätöksentekojärjestelmien teorioihin. Perusoletuksena on se, että tietojen hyödyntämisen näkökulmasta organisaatiot ovat yksittäisistä ihmisistä koostuvia sosiaalisia systeemejä. Ihmiset tekevät valintoja saatavilla olevien tietojen perusteella. Kun organisaatioita tutkitaan tietonäkökulmista, niin siten sekä sosiaalisten systeemien että ihmisten tiedonprosessoinnin näkökulmat on otettava huomioon.



Kuva 5. Ihmisten tiedonvaihdon malli; perustuu[53]

Kuvan 5 malli sisältää suunnittelun ja päätöksenteon lähtötietoluokat, tiedon jalostamisen askeleet sekä tulostietoluokat. Mallissa tiedon pääluokat ovat tietonäkökulmasta arvot, sisäinen tieto, johtopäätökset ja ulkoinen tieto. Tietoluokat sisältävät dataa, informaatiota ja tietämystä sekä hiljaista ja eksplisiittistä tietoa. Arvot-pääluokkaan kuuluvien tietoluokkien tiedot muuttuvat kaikkein hitaimmin, seuraavaksi hitaimmin muuttuvat sisäisen tiedon pääluokkaan kuuluvien tietoluokkien tiedot sekä reunaehdot, ympäristö ja ennakoidut tulevaisuudet. Muut ulkoinen tieto- ja johtopäätökset -pääluokkiin kuuluivat tiedot päivittyvät tyypillisesti tiheämmin.

Päätöksentekoprosessin näkökulmasta tiedon pääluokat ovat taulukossa 2 kuvatusti tilanne, rajoitukset, resurssit, keinot ja päätös. Mallin alimmalla tasolla eli tilanne-pääluokan tasolla, joka koostuu fyysisten rakenteiden, ominaisuuksien, tilannekuvan ja tapahtumien tietoluokista on tiedon määrä suurin. Tieto jalostuu siirryttäessä kohti mallin ylempiä kerroksia.

[56] Norri-Sederholm, T., Kuusisto, R., Kurola, J., Saranto, K. & Paakkonen, H. (2014) A Paramedic Field Supervisor's Situational Awareness in Prehospital Emergency Care. In: Journal of Prehospital and Disaster Medicine, Vol. 29, No. 2, pp. 1 - 9.

Taulukko 2. Tietoluokkien kuvaukset päätöksentekoprosessin näkökulmasta.[26,53,56]

Päätös	Perusoletukset	Piiloisia oletuksia, jotka ohjaavat toimijan käyttäytymistä. Kulttuurin perustavaa laatua olevia ominaisuuksia.
	Missio ja visio	Subjektiivisia ja ilmaistuja sisäisiä näkemyksiä toimijan lopputilasta.
	Päätös	Harkinnan, arvioinnin ja eri vaihtoehtojen välillä tapahtuneen valinnan jälkeen tehty ratkaisu.
	Tehtävä	Suoritettavaksi annettu tai otettu, jonkin itselleen asettama tai jollekin kuuluva työ, tekeminen tai velvollisuus.
Keinot	Sosiaalisesti todet arvot	Ajattelun ja toimintojen toteuttamisen perustaksi jossakin ryhmässä yhteisesti hyväksytyt oletukset.
	Keinot	Toimenpide tai menetelmä, jota sovelletaan tavoitteen saavuttamiseksi tai tarkoituksen täyttämiseksi.
	Vaihtoehdot toimia	Realistisesti toteutettavissa olevat toimintavaihtoehdot.
	Todennäköiset lopputilat	Asetelmat, joihin toimintojen päättyessä voidaan jokseenkin varmasti olettaa päädyttävän.
Resurssit	Fyysisesti todet arvot	Päteviksi hyväksyttyjä oletuksia rakenteista kuten organisaatio, työnjako ja osaamiset.
	Resurssit	Saatavilla olevia aineellisia resursseja kuten ihmiset, taloudelliset resurssit, materiaali, laitteet ja toimistotila.
	Mahdollisuudet toimia	Toimijan valittavissa olevia, jotakin uutta tarjoavia mahdollisia polkuja tavoitteeseen kuten strategiavaihtoehdot.
	Ennakoidut tulevaisuudet	Asioita, tapahtumia tai kehittymistä jota voidaan ajatella tai odottaa tapahtuvaksi.
Rajoitukset	Sosiaaliset rakenteet	Sosiaalisen systeemin rakenne, vuorovaikutuksen periaatteet, solmujen ja niiden keskinäisten sijaintien kuvaukset ja havaittavissa oleva käyttäytyminen.
	Toimintatavat	Kuvaavat kuinka toimija voi eri tilanteissa käyttäytyä ja miten toiminta ilmenee, esimerkiksi prosessikuvaukset ja -ohjeet.
	Reunaehdot	Tekijöitä, jotka on otettava huomioon ennen kuin suunnittelu resurssien ja keinojen käytöstä ennakoiduissa tulevaisuuksissa voidaan aloittaa.
	Ympäristö	Kuvaa sitä aluetta tai tilaa, jonka katsotaan olevan vaikuttava tässä tilassa olevan toimijan kannalta. Esimerkiksi median toiminta sekä kansalliset ja globaalit trendit.
Tilanne	Fyysiset rakenteet	Toimintojen lopputuloksia kuten ryhmän tekniset tulokset, kirjoitettu ja puhuttu kieli ja taide.
	Ominaisuudet	Kohteiden ominaisuudet kuten organisaatioiden tai laitteiden omaisuudet, esimerkiksi infrastruktuurikuvaukset.
	Tilannekuva	Kuvaus joka mahdollistaa tilanteen hahmottamisen. Esimerkiksi raportti, dokumentti ja analysoidut johtopäätökset kuten laaturaportit, tilastot, piirrokset ja kartat.
	Tapahtumat	Erilaisilla ajallisilla määreillä rajattavissa olevia tapahtumia kuten ihmisen syntymä, kokous tai palvelunestohyökkäys .

Moniviranomaisyhteistyötä tutkineen MNE5 -kokeiluhankkeen tiedonvaihdon tutkimuksessa todettiin, että toimijoiden tiedonintressi riippuu toimijan roolista organisaatiossa, toiminnan vaiheesta ja toimijoiden yhteistyösuhteen kypsyystasosta.[53,55] Tutkimuksissa tunnistetut toimijoiden roolit: päätöksentekijä, suunnittelija, analyytikko ja tilanteen seuraaja löytyvät tyypillisesti turvallisuusalan tilannekeskusorganisaatioista.

Tunnistetut toiminnan vaiheet ovat yhteistyösuhteen muodostaminen, suunnittelun valmistelu, suunnittelu ja toteutus. Nämä toiminnan vaiheet valikoituivat tutkimuksessa käytetyksi vaihejaoksi, koska niistä jokaisessa on erilainen tietojenvaihdon tarve.

Kun tutkimuksessa käytettyä toiminnan vaihejakoa verrataan yleisen toiminnan vaihejakoon OODA-looppiin[5], niin havaitaan että vaihejako on sisällytettävissä OODA-loopin vaiheisiin. OODA-loopin havainnointi-vaihetta vaihejaossa ei varsinaisesti ole, perehtyminen on jaettu useaan eri vaiheeseen eli yhteistyösuhteen muodostamisen, suunnittelun valmistelun ja suunnittelun vaiheisiin sekä päätös ja toiminta on yhdistetty toteuttaminen-vaiheeseen. Toimijoiden eri rooleissa ja toiminnan eri vaiheessa kiinnostavat tietoluokat on kuvattu taulukossa 3.

Taulukossa 3 vasemmalta lukien toisessa sarakkeessa on merkitty se toimijan rooli, joka on kiinnostunut ko. tietoluokan tiedoista: P tarkoittaa päätöksentekijää, S on suunnittelija, A on analyytikko ja T tilanteen seuraaja. Kolmannesta sarakkeesta kuudenteen sarakkeeseen on merkitty tiedonintressi kussakin toiminnan vaiheessa riveittäin kunkin tietoluokan osalta. XX tarkoittaa merkittävää intressiä ja X tarkoittaa intressiä tietoluokkaan. Taulukon 3 kuvaus ei ole täydellinen selitys eri roolien ja eri toiminnan vaiheiden tiedonvaihdon profiileista vaan pikemminkin tiedonintressien yleinen hahmo.

Tutkimuksissa[53,55] käytettiin toimijoiden yhteistyösuhteen kypsyystasoina Albertsin ja Hayesin[57] viisitasoista mallia, jossa johtamisen ja yhteistyösuhteen tasot on jaettu seuraavasti: Konfliktoitunut, ei-konfliktoitunut, koordinoitu, kollaboratiivinen ja ketterä[58]. Konfliktoituneessa yhteistyösuhteessa ei jaeta mitään tietoa ja ketterässä yhteistyösuhteessa kaikkien tietoluokkien sisällöstä keskustellaan avoimesti yhdessä. Taulukossa 4 on esitetty ei-konfliktoituneessa, koordinoidussa ja kollaboratiivisessa yhteistyösuhteessa jaettavat ja keskustelun kohteena olevat tietoluokat. Tietoluokat, joiden sisältö jaetaan, on tummennettu ja tietoluokat, joiden sisällöistä keskustellaan yhdessä, on ympyröity katkoviivalla.

Taulukoissa 3 ja 4 kuvatut tietoprofiilit perustuvat viranomaistoimijoiden sekä yksityissektorin ja kolmannen sektorin toimijoiden yhteistyöstä kansainvälisissä kriisinhallintaharjoituksissa saatuihin kokemuksiin. Myös kybertoimintaympäristössä toimittaessa tarvitaan useimmiten monen erilaisen toimijan kansallista ja kansainvälistä yhteistyötä. Siten tietoprofiilien voidaan olettaa muodostavan perustan myös kybertoimintaympäristössä tarvittavalle tiedonvaihdolle. Tämä tarkoittaa, että vuonna 2020 kybertoimintaympäristössä toimiminen edellyttää, että kunkin yhteistyökumppanin kanssa jaetaan jatkuvasti toimijoiden roolien, toiminnan vaiheiden ja yhteistyösuhteen kypsyystasojen perusteella poimittuja tietoja. Tämän oletuksen verifiointi ja validointi on jatkotutkimuksen aihe.

[57] Alberts, D.S., Hayes, R.E. (2007). Planning: Complex Endeavors. CCRP, USA.
[58] NATO (2010b). NATO NEC C2 Maturity Model. CCRP, USA.

Taulukko 3. Toimijan roolista ja toiminnan vaiheesta riippuvat tietoprofiilit.[53,54]

Tietoluokka	**P Päätöksentekijä S Suunnittelija A Analysoija T Tilanteen seuraaja**	Yhteistyö-suhteen muodos-taminen	Suunnittelun valmistelu	Suunnittelu	Toteutta-minen
Perusoletukset	P	XX			
Missio ja visio	P	XX			
Päätös	P,T		XX		XX
Tehtävä	P	X			X
Sosiaalisesti todet arvot	P	X			
Keinot	P,S	XX	XX	XX	X
Vaihtoehdot toimia	P,S			XX	
Todennäköiset lopputilat	P,S			X	
Fyysisesti todet arvot	S	X			
Resurssit	S,A	XX	XX	XX	XX
Mahdollisuudet toimia	S,A		X	XX	
Ennakoidut tulevaisuudet	S,A		X	X	
Sosiaaliset rakenteet	A				
Toimintatavat	A	XX	X		XX
Reunaehdot	A		XX	XX	
Ympäristö	A			X	X
Fyysiset rakenteet	A				
Ominaisuudet	A,T	XX			XX
Tilannekuva	A,T		X		X
Tapahtumat	A,T		XX		XX

Kybertoimintaympäristössä toimittaessa viranomaisten, yksityissektorin toimijoiden ja kolmannen sektorin toimijoiden on tarpeen jakaa yhteistyökumppaneidensa kanssa taulukossa 3 kuvattuja tietoja toiminnan eri vaiheissa. Kun verrataan taulukossa 3 kuvattuja tietotarpeita ja taulukossa 4 kuvattuja yhteistyösuhteen eri kypsyystasoilla vaihdettavia tietoluokkia toisiinsa, niin havaitaan, että vasta kollaboratiivisella ja ketterällä yhteistyösuhteen tasoilla on mahdollista jakaa ja avoimesti keskustella kaikista eri toiminnan vaiheissa tarvittavista tiedoista. Kullakin kybertoimintaympäristön toimijalla tulee siten olla poliittisten, taloudellisten ja teknologisten kriteerein valittuja yhteistyökumppaneita kollaboratiivisilla ja ketterillä yhteistyösuhteiden tasoilla. Siten Suomessa tarvitaan vuonna 2020 kansallisia ja kansainvälisiä sopimuksia syvien yhteistyösuhteiden muodostamista ja yhteistyötä sekä niissä tarvittavaa tietojenvaihtoa varten.

Taulukko 4. Tiedonvaihto yhteistyösuhteen kypsyystasoittain.[55]

4. Kollaboratiivinen Tilannetta seurataan sekä suunnitelmat, tietoanalyysit ja päätökset tehdään yhdessä	**Arvot**	**Sisäinen tieto**	**Johtopää-tökset**	**Ulkoinen tieto**
	Perusoletukset	Missio ja visio	Päätös	Tehtävä
	Sosiaalisesti todet arvot	Keinot	Vaihtoehdot toimia	Todennäköiset lopputilat
	Fyysisesti todet arvot	Resurssit	Mahdollisuudet toimia	Ennakoidut tulevaisuudet
	Sosiaaliset rakenteet	Toimintatavat	Reunaehdot	Ympäristö
	Fyysiset rakenteet	Ominaisuudet	Tilannekuva	Tapahtumat
3. Koordinoitu Tilannetta seurataan ja suunnitelmat tehdään yhdessä	**Arvot**	**Sisäinen tieto**	**Johtopää-tökset**	**Ulkoinen tieto**
	Perusoletukset	Missio ja visio	Päätös	Tehtävä
	Sosiaalisesti todet arvot	Keinot	Vaihtoehdot toimia	Todennäköiset lopputilat
	Fyysisesti todet arvot	Resurssit	Mahdollisuudet toimia	Ennakoidut tulevaisuudet
	Sosiaaliset rakenteet	Toimintatavat	Reunaehdot	Ympäristö
	Fyysiset rakenteet	Ominaisuudet	Tilannekuva	Tapahtumat
2. Ei-konfliktoitunut Tilannetta seurataan yhdessä	**Arvot**	**Sisäinen tieto**	**Johtopää-tökset**	**Ulkoinen tieto**
	Perusoletukset	Missio ja visio	Päätös	Tehtävä
	Sosiaalisesti todet arvot	Keinot	Vaihtoehdot toimia	Todennäköiset lopputilat
	Fyysisesti todet arvot	Resurssit	Mahdollisuudet toimia	Ennakoidut tulevaisuudet
	Sosiaaliset rakenteet	Toimintatavat	Reunaehdot	Ympäristö
	Fyysiset rakenteet	Ominaisuudet	Tilannekuva	Tapahtumat

Yhteistyösuhteiden kehittäminen kybertoimintaympäristössä toimimista varten tapahtuu tietojen jakamisen näkökulmasta siten, että vaiheittain laajennetaan ja syvennetään toimijoiden rooleittain ja toiminnan vaiheittain yhteistyökumppaneille jaettavien ja keskusteltavien tietojen joukkoa. Yhdistämällä taulukon 3 ja 4 tuloksia havaitaan, että yhteistyösuhteen kehittämisen vaiheessa toimittaessa ei-konfliktoituneella yhteistyösuhteen tasolla jaetaan tietoja tyypillisesti ainoastaan toimintatavoista sekä organisaatioiden ja laitteiden ominaisuuksista. Siirryttäessä koordinoidulle yhteistyösuh-

teen tasolle jaettavien tietojen joukko laajenee yhteistyösuhdetta kehitettäessä resursseihin, keinoihin, fyysisesti tosiin arvoihin ja sosiaalisesti tosiin arvoihin.

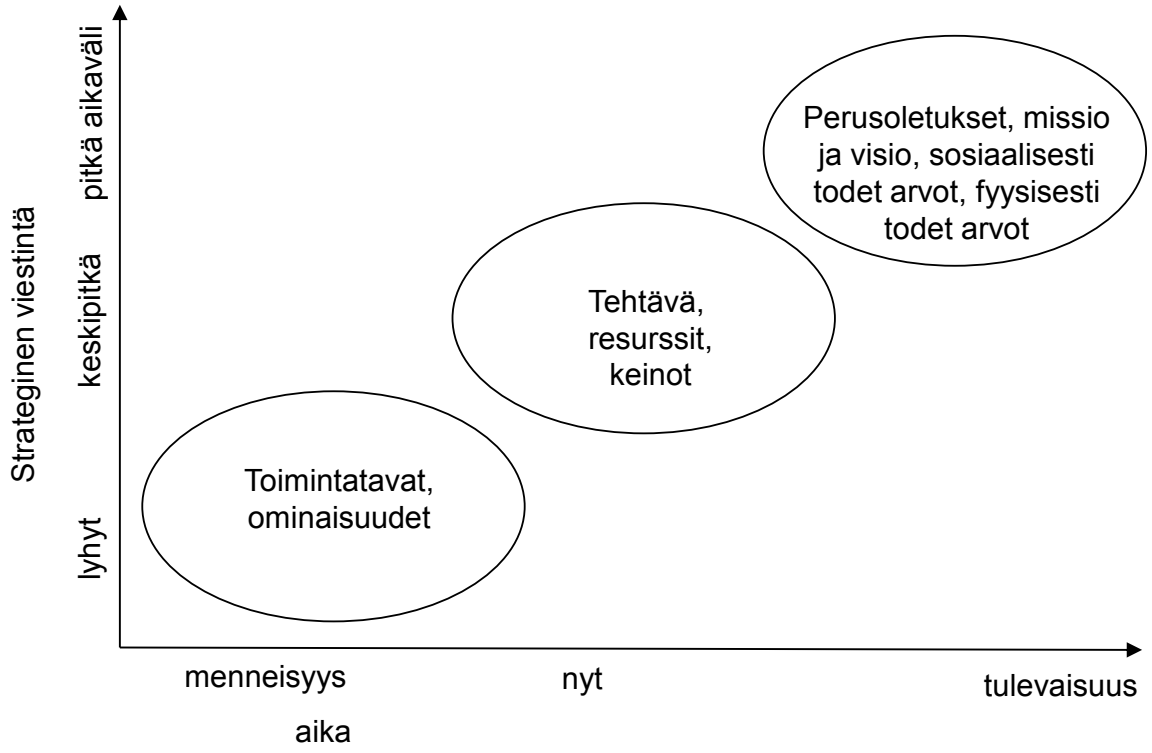
Kollaboratiivisella ja ketterällä yhteistyösuhteen tasoilla yhteistyötahojen päätöksentekijöiden, suunnittelijoiden, analyytikoiden ja tilanteen seuraajien rooleissa toimivien henkilöiden kanssa jaetaan jatkuvasti kunkin roolin mukaisia yhteistyösuhteen lujittamisessa tarvittavia tietoja tilanteesta, rajoituksista, resursseista, keinoista ja päätöksistä. Ensisijaisesti viestittävät tietoluokat yhteistyösuhteen lujittamiseksi ovat perusoletukset, missio ja visio, keinot, resurssit, toimintatavat sekä organisaatioiden ja laitteiden ominaisuudet. Myös tietojen jakamista tehtävästä, sosiaalisesti tosista arvoista ja fyysisesti tosista arvoista tarvitaan yhteistyösuhdetta lujitettaessa.

Strateginen viestintä on organisaation päämäärätietoista viestintää tehtävän täyttämiseksi.[59] Se voidaan jakaa lähinnä menneisyystietoja koskevaan lyhytkestoiseen viestintään, nykyisyystietoja koskevaan keskipitkän aikavälin viestintään ja tulevaisuustietoja koskevaan pitkäkestoiseen viestintään.[42] Menneisyystietoja ovat esimerkiksi erilaiset raportit, nykyisyystietoja tavoitteita ja normeja koskevat tiedot sekä tulevaisuustietoja arvoja, arvostuksia ja ennakoituja tulevaisuuksia koskevat tiedot. Kuvan 6 mukaisesti sekä lyhyen, keskipitkän että pitkän aikavälin strategista viestintää tarvitaan, jos tahdotaan vaikuttaa kybertoimintaympäristönkeskeisten yhteistyökumppaneiden käsityksiin yhteistyösuhteen muodostamisessa ja lujittamisessa tarvittavista tiedoista.

Mitä hitaammin tiedot päivittyvät, sitä kauemmin käsityksen muuttaminen niistä yleensä kestää. Kuten kuvasta 6 näkyy, niin kollaboratiivisella ja ketterällä yhteistyötasoilla yhteistyösuhteiden muodostaminen ja lujittaminen kybertoimintaympäristössä toimimista varten tarkoittaa lyhytkestoisen strategisen viestinnän osalta viestintää toimintatapoja sekä organisaatioiden ja laitteiden ominaisuuksia koskevista tiedoista.

Keskipitkän strategisen viestinnän sisältöä ovat tehtävä, resurssit ja keinot. Pitkäkestoisen strategisen viestinnän keskeisen sisällön muodostavat perusoletuksia, mission ja vision, sosiaalisesti tosia arvoja sekä fyysisesti tosia arvoja koskevat tiedot. Suunnittelun valmistelua ja suunnittelua varten tarvitaan pitkäkestoista strategista viestintää myös yhteistyökumppaneiden yhteisten kokonaisvaltaisten ennakoitujen tulevaisuuksien muodostamista varten.

[59] Hallahan, K., Holtzhausen, D., van Ruler, B., Verčič, D. & Sriramesh, K. (2007). Defining strategic communication. In: International Journal of Strategic Communication, vol. 1, no. 1, pp 3 - 35.



Kuva 6. Strateginen viestintä keskeisten yhteistyösuhteiden muodostamisessa ja lujittamisessa kybertaisteluja varten; muokattu[60,42]

2.5 Yhteenveto

Lähitulevaisuudessa Suomi on liittymässä mukaan tällä hetkellä suunnitteilla ja rakenteilla oleviin mannertenvälisiin tiedonsiirtoyhteyksiin ja eri puolilla maailmaa rakenteilla olevien laajojen palvelinkeskusten verkostoon. Suomessa toimii runsaasti edistyneitä tieto- ja viestintäteknologisten palvelujen tarjoajia ja Suomessa organisaatiot myös käyttävät laajalti näitä palveluja. Sekä palvelujen tarjonnan että käytön arvioidaan edelleen kasvavan vuoteen 2020 mennessä. Yhden maanpuolustukselle merkittävän kasvavan teknologia-alueen muodostavat miehittämättömät ilma-, vesi- ja maa-ajoneuvot eli esimerkiksi lennokit ja robottiautot. Myös palvelurobottien käytön arvioidaan kasvavan maanpuolustuksessa. Lisäksi massadatan ja avoimen datan jalostamiseen liittyvien teknologioiden ja menetelmien ennakoidaan entisestään parantuvan ja niiden käytön lisääntyvän vuoteen 2020 mennessä.

Yhteiskunnan ja taistelujen robotisoituminen sekä laajemminkin taisteluvälineiden automatisoituminen ja massadatan jalostusmenetelmien kehittyminen ja kasvava käyttö vaikuttavat yhteiskunnan elintärkeisiin toimintoihin sekä puolustusvoimien mahdollisuuksiin ja vaihtoehtoihin toimia strategisella, operatiivisella, taktisella ja operoinnin tasoilla. Kybertoimintaympäristö on tuntematon maasto. Päätöksentekijät tarvitsevat tietoa siitä mistä asioista ja milloin on päätettävä sekä mitä edellytyksiä kybertoimintaympäristö asettaa ja mitkä ovat faktapohjaiset päätösvaihtoehdot, jotta puolustusvoimien lakisääteisiä tehtäviä voidaan toteuttaa myös kybertoimintaympä-

[60] Helokunnas, T. & Kuusisto, R. (2003). Strengthening Leading Situations via Time-divergent Communication Conducted in Ba. Journal of eBusiness Review. Volume III.

ristössä ja sen kautta. Tarvitaan kattavaa tilanneymmärrystä eli sekä jatkuvaa tilanteen tulkintaa kokonaisympäristössä että ennakointia paikallisesti ja ajallisesti välittömien tapahtumien ja tunnettujen keinojen ulkopuolelle kaikilla toiminnan tasoilla. Erityisesti vuonna 2020 tarvitaan kunkin toiminnan tason tietotarpeita täyttäviä kybertoimintaympäristön sisältöanalyysejä: Parametrien ja indikaattorien tunnistamista ja niiden pohjalta tehtyjä kokonaistilanteen huomioivia arviointeja ja ennakointeja sekä tilanteen mukaista toimintaa.

Kybertoimintaympäristössä voidaan tiedon avulla vaikuttaa yhdelle tai useammalle toiminnan tasolle. Eri toiminnan tasoilla päätöksenteossa tarvittava tilannetietoisuus poikkeaa sisällöllisesti toisistaan, ja siten myös eri toiminnan tasoilla tilannetietoisuuteen vaikutetaan erilaisella tiedolla. Esimerkiksi harhautus on käypä keino kybertaisteluissa. Harhautuksen toteuttaminen taisteluteknisellä toiminnan tasolla vaatii tyypillisesti lyhyellä aikavälillä toteutettua taistelutilan tapahtumia koskevaa disinformaation syöttämistä kybertoimintaympäristöön. Sen sijaan harhautus ylimmillä strategisilla tasoilla on usein pitkäjänteistä vaikuttamista strategisen kommunikaation keinoin.

Kybertoimintaympäristössä voidaan tietotoon vaikuttamalla kohdistaa Suomen rajojen ulkopuolelta vaikutus Suomen alueella sijaitseviin kohteisiin. Tältä vaikuttamiselta ei voida puolustautua pelkästään Suomen valtion maantieteelliseltä alueelta käsin. Siten Suomessa tarvitaan vuonna 2020 kansallisia ja kansainvälisiä sopimuksia Suomen sotilaalliseksi puolustamiseksi ja kybertaisteluissa onnistumiseksi.

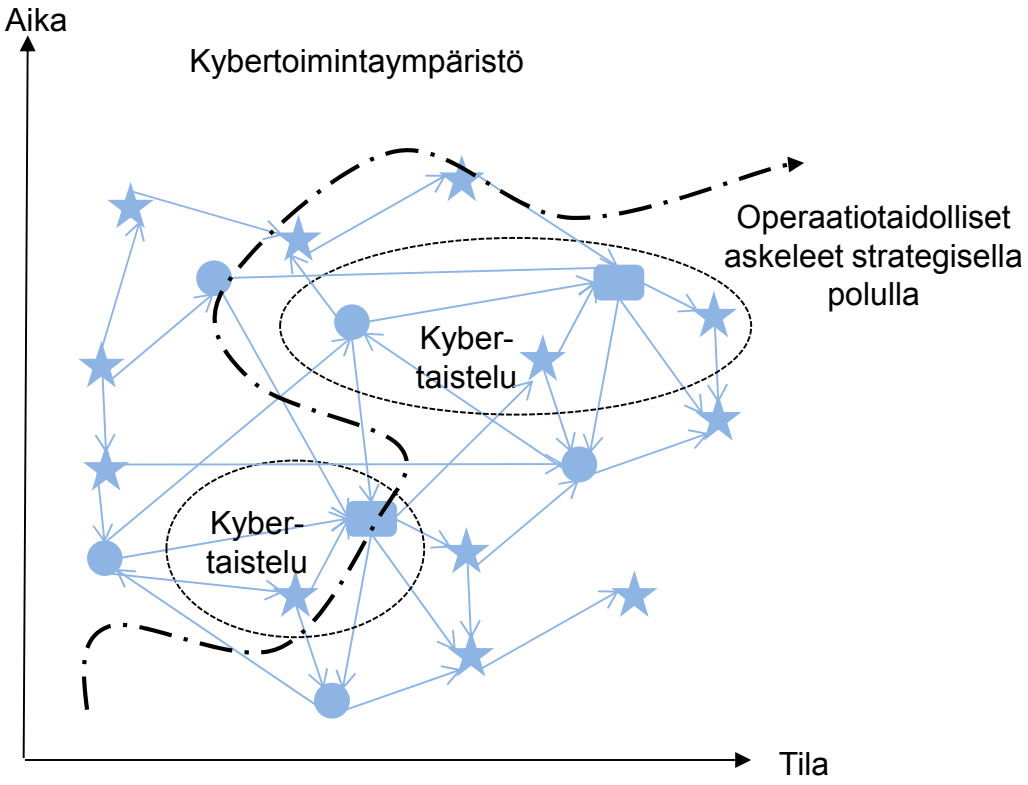
Operaatiotaidollinen toiminta on askeleiden valintaa polulla kohti strategisia tavoitteita luoden sellaisia asetelmia ja resursseja joilla pystytään tekemään ratkaisuja.[61] Operaatiotaidollista toimintaa kybertoimintaympäristössä on havainnollistettu kuvassa 7. Kybertoimintaympäristö tarjoaa mahdollisuuksia luoda yllättäviä asetelmia ja dynaamisia resursseja taistelujen voittamiseksi. Onnistuneella operaatiotaidollisella valinnalla kybertaistelu voidaan kokonaan välttää. Esimerkiksi kybertoimintaympäristössä vaeltelevilla muistitikuilla levitettyjen haittaohjelmien hyödyntäminen tuotantolaitosten tuotantovälineiden rikkomisessa oli yllättävä asetelman luominen. Tällä asetelmalla saavutettiin voitto ilman taistelua.

Operaatiotaito perustuu ajatteluun, jolloin on mahdollista ajattelemalla ennakoida myös vastustajien mahdolliset toimet. Tällöin vihamielisiin toimiin voidaan varautua ja ne voidaan mahdollisesti myös torjua. Tämä vaatii kokonaisymmärrykseen perustuvan tilanneymmärryksen muodostamista. Systeemimallinnuksella on mahdollista saavuttaa tarvittavaa kokonaisymmärrystä ja kokonaisymmärrykseen perustuen on mahdollista kohdentaa sisältöanalyysit siten että riittävän tasoinen tilanneymmärrys saadaan muodostettua.

Systeemimallinnukseen ja sisältöanalyysiin perustuvan sosiaalisen systeemin mallin avulla kompleksisista systeemeistä kuten kybertoimintaympäristöstä saatavissa olevien tietojen sisältöä voidaan analysoida ja tunnistaa kehittymässä olevia ilmiöitä. Tunnistettuja ilmiöitä voidaan käyttää päätöksenteossa ohjaamaan resurssien suuntaamista vaikuttavimpiin kohteisiin. Tässä luvussa sosiaalisen systeemin mallia sovellettiin Suomessa vuonna 2013 toteutettujen kyberturvallisuusharjoitusten arviointi-

[61] Kuusisto, T., Kuusisto, R. (2014a). Prerequisites for Creating Resources and Compositions for Cyber Defence. Proc of 2014 SRI Security Congress, Perth, Australia.

aineistojen sisältöanalyysiin. Tämän perusteella voidaan todeta, että hallinnossa on tarve organisoitua uudella tavalla ja luoda uuteen tilanteeseen soveltuva päätöksentekojärjestelmä. Tämä on yleinen tarve kaikissa tilanteissa, jossa toimintaympäristö muuttuu. Vuoteen 2020 mennessä tarvitaan yhteisesti hyväksyttyä tietopohjaa koskien arvoja, nykyhetken faktoja, päämääriä ja normeja, jotta saadaan luotua kestävä perusta globaaliin kyberyhteisöön integroitumiseksi.



Kuva 7. Operaatiotaito on askeleiden valintaa polulla kohti strategisia tavoitteita luoden sellaisia asetelmia ja resursseja joilla pystytään tekemään ratkaisuja[61]

Kansainvälisten kriisihallinnan kokeiluhankkeiden tiedonvaihtotutkimusten tulosten perusteella päätöksentekijöillä, suunnittelijoilla, analysoijilla ja tilanteen seuraajilla on erilaiset, toiminnan vaiheista ja yhteistyön kypsyystasosta riippuvat tietotarpeet. Vasta kollaboratiivisella ja ketterällä yhteistyösuhteen tasoilla on mahdollista jakaa ja avoimesti keskustella kaikista eri toiminnan vaiheissa tarvittavista tiedoista. Yhteistyösopimuksen solmineiden yhteistyökumppaneiden kanssa on siten vuonna 2020 jatkuvasti jaettava toimijoiden roolien, toiminnan vaiheiden ja yhteistyösuhteen kypsyystasojen perusteella poimittuja tietoja. Pitkäkestoisella strategisella viestinnällä vahvistetaan yhteistyötä ja tuetaan kumppaneita jaettujen tietojen ymmärtämisessä ja käyttämisessä.

Kybertoimintaympäristön kehittyminen mahdollistaa entistä vaivattomamman tietojen keräämisen ja jakamisen. Tämän johdosta kunkin toimijan keräämien tietojen luotettavuuteen, eheyteen ja saatavuuteen kohdistuu kasvavaa huomiota. Kybertaisteluissa ja kybertoimintaympäristön kautta tapahtuvassa vaikuttamisessa toimija voi saada merkittävästi etua kyetessään hankkimaan pääsyn jonkin toisen toimijan analysoimaan tai teknologisen palvelun keräämään tietoon. Tarvitaan myös viranomaisten

suorittamaa valvontaa, joka turvaa mahdollisuuden yhteiskunnan elintärkeiden toimintojen turvaamiseen ja pääsyyn globaaliin kybertoimintaympäristöön. Valvonnalla ehkäistään ja tunnistetaan kybertoimintaympäristön käyttäminen säädösten vastaiseen tai jopa rikolliseen toimintaan tai Suomen sotilaallista puolustamista uhkaavaan tarkoitukseen.

Kiitokset

Esitän lämpimät kiitokset kommenteista ja palautteesta koko kirjaa ja tätä artikkelia koskien kirjaa työstäneelle työryhmälle, eli sotilasprofessori Mika Hyytiäiselle, evl (evp) Sakari Ahvenaiselle, diplomi-insinööri Tomi Hasulle, dosentti, eversti (evp) Martti Lehdolle, professori Jari Rantapelkoselle, professori Jouko Vankalle, evl J-P Virtaselle ja johtaja Kari Wirmanille. Erityisesti tahdon kiittää arvokkaista kommenteista ev (evp) Aapo Cederbergiä sekä evl Vesa Valtosta sekä jatkuvasta ajattelun kehittämisestä professori Rauno Kuusistoa.

3.

Kybersodankäyntiä koskevan lainsäädännön tarkastelua

Tietoturva-asiantuntija Tomi Hasu
Kyberturvallisuuskeskus
Viestintävirasto

Tiivistelmä
Tässä luvussa käsitellään aluksi Yhdysvaltojen, Naton ja muiden länsimaiden sekä Venäjän ja Kiinan näkökulmia kybersodankäynnin lainsäädäntöön sekä kybersodankäyntiin liittyvää lainsäädäntöä Suomessa. Tämän jälkeen esitetään kaksi kuvausta erilaisista lainsäädännöllisistä suhtautumisista kybertoiminta-ympäristöön. Ensimmäinen korostaa tietosuojan merkitystä ja kirjesalaisuuden koskemattomuutta. Toisessa pyritään takaamaan globaalin informaatioinfrastruktuurin toiminta vahvalla sääntelyllä ja lukuisilla kontrolleilla.

3.1 Johdanto

Tietomurtojen ja kyberhyökkäysten noustessa otsikoihin 2000-luvulla alkoi myös keskustelu kyberhyökkäysten ja niihin reagoimisen laillisista perusteista. Kuten muidenkin uusien ilmiöiden yhteydessä, alussa kybertoimintaympäristön tapahtumat tuntuivat kovin vaikeilta rinnastaa mihinkään aikaisempaan. Näin saattoi helposti syntyä käsitys, että kybertapahtumat olivat jotain erillistä, yleisen lainsäädännön ja oikeuskäsityksen ulkopuolella olevaa. Kuultiin jopa mielipiteitä, joiden mukaan olemassa oleva lainsäädäntö ei pätisi kybertoimintaympäristössä ja olisi tarpeen kehittää uusi oikeuskäsitys. Varsin pian kuitenkin nousi ajatus siitä, että vaikka kyseessä on uusi teknologia ja entisestä poikkeavat menetelmät, ehkä pohjimmiltaan kyseessä olisikin vuosituhansia vanhasta toiminnasta. Näin ollen tähän uudelta vaikuttavaan toimintamuotoon voitaisiin soveltaa yleisesti käytössä olevia oikeuskäytäntöjä.

Sotilaallisen toiminnan perusperiaatteet on kirjattu YK:n peruskirjaan[1] ja niitä on tarkennettu yleisesti hyväksytyissä niin sanotuissa Geneven sopimuksissa[2], joista käytetään myös nimityksiä *“International Humanitarian Law”* tai *“Law of Armed Conflict”*. Näissä sopimuksissa käsitellään niin voimankäytön sääntöjä (*“jus in bello”*) kuin kansakunnan oikeutta voimankäyttöön (*“jus ad bellum”*). Nyrkkisääntönä voidaan pitää sitä, että jokaisella kansakunnalla on oikeus itsepuolustukseen, voimankäytöllä ei saa aiheuttaa tarpeetonta humanitaarista kärsimystä ja voimankäytön tulee olla suhteutettu uhkaan.

Toistaiseksi kybertoimintaympäristö on kehittynyt spontaanisti ja markkinavetoisesti ilman yleismaailmallisia lainsäädännöllisiä linjauksia. Toiminnan siirtyessä seuraavalle kypsyystasolle tarve yhteisten pelisääntöjen sopimiseen korostuu kybertoimintaympäristön eriarvoistumisen estämiseksi.

---

[1] https://www.unric.org/fi/perustietoa-yksta/13
[2] http://www.icrc.org/eng/resources/documents/publication/p0173.htm

3.2 Erilaisia lainsäädännöllisiä suhtautumisia

3.2.1 Yhdysvallat, NATO ja muut länsimaat

Vuonna 2007 Viron Pronssisoturikiistan[3] yhteydessä tapahtuneiden kyberhyökkäysten johdosta NATO perusti vuonna 2008 Tallinnaan kybertoimintaympäristön tutkimiseen keskittyvän tutkimuskeskuksen, NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)[4]. Keskuksen päätehtävä oli pohtia, kuinka hyvin olemassa oleva lainsäädäntö ja yleiset sopimukset kykenevät käsittelemään kybertoimintaympäristön tapahtumia. Pitkällisen keskustelun ja useiden väliraporttien jälkeen CCDCOE julkaisi vuonna 2013 johtopäätöksensä julkaisussa "*Tallinn Manual on the International Law as Applicable to Cyber Warfare*"[5]. Monet länsivaltiot perustavatkin oman lainsäädännöllisen tarkastelunsa edellä mainitun Tallinnan käsikirjan johtopäätöksiin ja suosituksiin. Käsikirjassa linjataan 95 sääntöä, jotka tulisi ottaa huomioon kyberoperaatioiden suunnittelussa ja toimeenpanossa.

Länsimaissa on yleisesti vallalla käsitys, että olemassa olevat lait ja kansainväliset sopimukset pätevät kybertoimintaympäristöön sellaisenaan. Lakien ja periaatteiden tapauskohtaisessa soveltaminen ja tulkinta on haastavaa, mutta tämä johtuu pääsääntöisesti kulttuurieroista perinteisten lainoppineiden ja teknisesti orientoituneiden kybertoimintaympäristön toimijoiden välillä.

3.2.2 Venäjä ja Kiina

Jotkut valtiot, erityisesti Venäjän ja Kiinan johdolla, kannattavat varsin erilaista lähestymistapaa. Heidän näkemyksensä mukaan nykyinen kybertoimintaympäristö ei ole millään tavalla säädelty tai hallittu, mikä vaarantaa kaikkien toimijoiden turvallisuuden ja viimekädessä koko toimintaympäristön tulevaisuuden. Tämä ryhmittymä kannattaa uudenlaisen sääntelymekanismin perustamista ja toimintaympäristön tiukempaa kontrollointia[6]. Perusteluina käytetään parantuvaa turvallisuutta ja toimintavarmuutta. Kantaa pyritään viemään eteenpäin kansainvälisen telekommunikaatiounionin ITU:n[7] kautta. Länsimaat Yhdysvaltain johdolla suhtautuvat esitykseen hyvin nuivasti.

3.3 Lainsäädäntö Suomessa

Eräs vuonna 2013 julkaistun kansallisen kyberturvallisuusstrategian[8] linjauksista oli lainsäädännön muutostarpeiden kartoitus. Kartoitustyössä tultiin siihen tulokseen, että kyberpuolustuksen osalta suojautumiseen ja vaikuttamiseen liittyen olemassa oleva lainsäädäntö mahdollistaa riittävät ja tarkoituksenmukaiset toimivaltuudet. Tiedusteluun liittyen lainsäädäntö koettiin vajavaiseksi.

---

[3] http://www.theguardian.com/world/2007/may/17/topstories3.russia

[4] https://www.ccdcoe.org/

[5] https://www.ccdcoe.org/249.html

[6] http://www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity/

[7] http://www.itu.int/en/Pages/default.aspx

[8] http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit/doc_download/50-suomen-kyberturvallisuusstrategia-ja-taustamuistio

Oman kybertoimintaympäristön suojaamisen osalta laki sähköisen viestinnän tietosuojasta[9] ja tietoyhteiskunnan lakikaari mahdollistavat varsin laajat toimet uhkien havaitsemiseksi, torjumiseksi ja hyökkäyksistä toipumiseksi. Vaikuttamisen osalta päädyttiin muiden länsimaiden tavoin toteamaan, että yleisesti hyväksytyt sodankäynnin säännöt pätevät myös kybertoimintaympäristössä. Mikäli havaitut hyökkäykset tulkitaan kyberterrorismiksi, niihin kohdistuvat samat oikeuskäytännöt kuin tavanomaiseen terrorismiin.

Ongelmalliseksi koettiin myös kansallisen kybertoimintaympäristön valvonnan käsite. Tarve maa-, meri- ja ilmavalvonnan kaltaiseen, Suomen valtion alueellista koskemattomuutta valvovaan mekanismiin kybertoimintaympäristössä on tunnistettu[10], mutta keskustelu sen käytännön toteuttamisesta ja lainsäädännöllisistä perusteista on vielä kesken. Asian käsittelyä vaikeuttaa suuret erot fyysisen maailman ja kybertoimintaympäristön välillä. Aluevedet ja kansallinen ilmatila on selvästi määritelty, mutta modernin globalisaation aikana vastaavanlaisen kansallisen kybertoimintaympäristön rajaaminen voi olla jopa mahdotonta.

3.4 Kaksi mahdollista maailmankuvaa

3.4.1 Korostunut tietosuoja

2010-luvun urkintapaljastusten[11] ansiosta erilaisten salausratkaisujen suosio ja saatavuus on noussut räjähdysmäisesti. Valtaosa tietoliikenteestä on vahvasti salattua ja useimmissa tiedon tallennuspalveluissa on mahdollisuus suojata tieto salausteknisin menetelmin. Tämä on romuttanut monien, erityisesti tunnisteisiin perustuvien, tunkeutumisenestojärjestelmien toimintaperiaatteen. Tunnisteisiin perustuvat automaattiset tietoturvamekanismit pyrkivät havaitsemaan viestin sisällöstä ennalta määriteltyjä merkkijonoja. Kun viestintä ovat pääosin salattua, viestin sisältöä on huomattavasti hankalampi tarkastella.

Palveluntarjoajilla tai teleoperaattoreilla ei ole velvoitetta toimia yhteistyössä viranomaisten kanssa. Vaikka yhteisöjä ja yrityksiä pyritään kannustamaan yhteistyöhön, monien palvelujen markkinointi perustuu tietosuojan korostamiseen ja toiminnan ehdottomaan anonymiteettiin. Lainsäädännössä tietosuojan merkitys on yleisesti korostunut. Haitallisen toiminnan menetelmillä on merkittävä rooli syyteharkinnassa. Mikäli esimerkiksi petoksessa käytetään sähköisen identiteettivarkauden avulla anastettuja vääriä henkilötietoja, tapausta ei käsitellä talousrikoksena vaan identiteettivarkautena. Tämä on johtanut osassa väärinkäytöstapauksissa lievempiin tuomioihin.

Viranomaisilla on velvollisuus tiedottaa asianomaisia välittömästi heihin kohdistuvista valvontatoimista, kuten tietoliikenteen seurannasta. Parantunut yksilön tietosuoja koskee poikkeuksetta kaikkia, myös rikollisia ja vieraan valtion toimeksiannosta toimivia.

---

[9] http://www.finlex.fi/fi/laki/ajantasa/2004/20040516?search%5Btype%5D=pika&search%5Bpika%5D=laki%20s%C3%A4hk%C3%B6isen%20viestinn%C3%A4n

[10] http://www.defmin.fi/files/2669/Kyberlainsaadantotyoryhman_asettamispaatos.pdf

[11] http://www.theguardian.com/world/the-nsa-files

Tällaisessa toimintaympäristössä väärinkäytösten tutkinta ja erityisesti ennaltaehkäisy on haastavaa. Vaikka kaikilla tahoilla on edelleen oikeus valvoa omien tietojärjestelmien toimintaa, viranomaisten ennaltaehkäisevä tiedonhankinta on vaikeutunut huomattavasti. Usein tiedonhankintaa onkin tarkoituksenmukaista tehdä muualla kuin kybertoimintaympäristössä. Ennaltaehkäisevään toimintaan kohdistuvien rajoitteiden takia haitallisen toiminnan torjunnan painopiste onkin siirtynyt vahinkojen rajoittamiseen. Koska kyberhyökkäyksiä ei kyetä tehokkaasti estämään, niiden haitallisia vaikutuksia pyritään minimoimaan tai rajaamaan. Toiminnan jatkuvuuden takaaminen on korostunut ensisijaiseksi vastatoimeksi väärinkäytösten varalle. Varautumistoimien puutteellinen suunnittelu tai toteutus on pakottanut useita organisaatioita keskeyttämään tai jopa lopettamaan toimintansa.

3.4.2 Vahva kontrolli

Kaikilla kybertoimintaympäristössä toimivilla palvelujen tarjoajilla ja käyttäjillä on velvollisuus huolehtia niin palvelujen kuin toimiensa turvallisuudesta. Velvollisuuden toteuttamista valvotaan aktiivisesti ja se sisältää myös ilmoitusvelvollisuuden kaikista yleistä tai yksityistä tietoturvaa tai turvallisuutta uhkaavista tapahtumista. Ilmoitusvelvollisuus koskee kaikkia toimijoita, myös yksittäisiä loppukäyttäjiä. Erityisesti tietoliikenneoperaattorit ja palveluntarjoajat ovat velvollisia seuraamaan kybertoimintaympäristöä väärinkäytösten varalta ja ilmoittamaan havainnoistaan viranomaisille.

Yleisesti saatavilla olevien päätelaitteiden ominaisuuksia on rajoitettu ja niiden toimintaa seurataan. Laajemmilla ominaisuuksilla varustettujen laitteiden, kuten henkilökohtaisten tietokoneiden, käyttäjien tulee suorittaa tutkinto kybertoimintaympäristön toimintasäännöistä ja hyväksyä toiminnan edellyttämät velvollisuudet. Organisaatioiden tietojärjestelmiin tehdään määräajoin tietoturvatarkastuksia valtuutettujen tahojen toimesta. Mahdollisissa tietomurroissa ja muissa kyberhyökkäyksissä hyödynnettävien niin sanottujen hakkerityökalujen valmistaminen, myynti, hallussapito ja käyttö on luvanvaraista. Luvan perusteena voi olla esimerkiksi tietoturvatarkastusten tekeminen tai väärinkäytösten selvittäminen. Tyypillisiä luvanhaltijoita ovat viranomaiset, tietoturvayhtiöt ja erilaiset tutkimuslaitokset. Luvanvaraista toimintaa valvotaan tiukasti.

Syyteharkinnassa rikokset tulkitaan toiminnan tarkoituksen eikä välineiden mukaan. Tietomurto rinnastetaan fyysiseen murtautumiseen tai kotirauhan rikkomiseen, mikäli murtokohteen suojautumismekanismit tulkitaan puutteellisiksi.

Yksilön ja organisaatioiden toiminnalle kybertoimintaympäristössä on asetettu useita rajoitteita ja velvoitteita. Viranomaisella on kattavat valtuudet päästä käsiksi jopa luottamuksellisen viestinnän sisältöön, mikäli lainsäädännössä määritellyt edellytykset täyttyvät. Väärinkäytösten tekemistä kybertoimintaympäristössä on pyritty vaikeuttamaan ja niiden havaitsemista parantamaan.

3.5 Yhteenveto

2010-luvulla yleisesti hyväksytty suhtautuminen kybersodankäynnin laillisuuteen on se, että kybertoimintaympäristö on fyysisen maailman jatke, johon sovelletaan olemassa olevia sopimuksia ja oikeuskäytäntöjä. Eri ympäristöt ovat vertailtavissa jopa siinä määrin, että vakavaan kyberhyökkäykseen on täysin hyväksyttävää vastata kineettisin toimin, mukaan lukien perinteinen asevoima.

2020-luvulle saavuttaessa keskustelu kybertoimintaympäristöön suhtautumisesta käydään yksilön tietosuojan korostamisen ja kokonaisuutta suojaavien kontrollien välillä. Tietosuojan puolestapuhujat painottavat yksilön oikeutta luottamukselliseen viestintään ja yksilöimättömään toimintaan. Suojausmekanismien kannattajat haluavat luoda kybertoimintaympäristöön vastaavanlaisen lainsäädännön kuin on käytössä liikenteessä tai ampuma-aseiden hallussapidossa. Kukaan ei kuitenkaan kiistä kansakuntien oikeutta käyttää kybertoimintaympäristöä valtiollisen voimankäytön välineenä.

4.

Kybertaistelun toimintaympäristön teoreettinen tarkastelu

Dosentti Martti Lehto
Jyväskylän yliopisto
Tietotekniikan laitos

Kyberturvallisuuden dosentti, sotatieteiden tohtori, eversti evp. Martti Lehto on palvellut ilmavoimissa eri tehtävissä ja Pääesikunnassa vuosian 1978–2007. Jäätyään eläkkeelle Ilmavoimien esikunnan apulaisesikuntapäällikön tehtävästä, hän suoritti jatko-opinnot MPKK:n Johtamisen laitoksella vuosina 2007–2012. Vuodesta 2009 hän on työskennellyt kyberturvallisuuden maisteri- ja jatkokoulutusohjelmien koordinaattorina sekä kyberturvallisuuden ja kyberpuolustuksen tutkijana ja opettajana Jyväskylän yliopiston Tietotekniikan laitoksella. Hän on osallistunut asiantuntijana mm. Suomen kyberturvallisuusstrategian ja sen toimeenpanosuunnitelman sekä kansallisen kyberturvallisuuden strategisen tutkimusagendan laadintaan. Hän toimii asiantuntijana Euroopan verkko- ja tietoturvaviraston (ENISA) kyberturvallisuuden tutkimusta ja koulutusta käsittelevässä työryhmässä. Hänellä on yli 50 julkaisua, tutkimusraporttia ja artikkelia kansainvälisissä ja kansallisissa journaaleissa, konferenssijulkaisuissa ja kirjoissa, joka käsittelevät puolustusvoimien johtamisjärjestelmää, kyberturvallisuutta ja -puolustusta, informaatiosodankäyntiä sekä puolustus- ja turvallisuuspolitiikkaa.

Tiivistelmä
Asevoimien uudet suorituskyvyt luovat uusia mahdollisuuksia sekä kineettiseen että ei-kineettiseen voimankäyttöön kyberavaruudessa. Kyberajan suorituskyvyt mahdollistavat toiminnan uudessa epälineaarisessa ja rajoiltaan epämääräisessä hybridimäisessä taistelutilassa. Tässä tilassa tulee voida integroida saumattomasti päätöksentekijät, toimijat sekä ilmassa, pinnassa, pinnan alla, avaruudessa ja kyberavaruudessa toimivat miehitetyt ja miehittämättömät alustat.

Kybermaailma voidaan mallintaa viisikerroksiseksi rakenteeksi, jonka osia ovat fyysinen, syntaktinen, semanttinen, palvelut ja kognitiivinen. Kybermaailman uhat, haavoittuvuudet ja riskit voidaan kuvata ja mallintaa näissä kussakin kerroksessa. Näihin kerroksiin on kehitetty dedikoituja hyökkäysoperaatiomalleja ja kyberaseita.

Kyberajan boydilaisen teorian mukaan sotilaallisten operaatioiden tavoitteena on "murtaa vastustajan johtamisen henki ja tahto luomalla yllättäviä ja vaarallisia toiminnallisia tai strategisia tilanteita". Saavuttaakseen halutun loppuasetelman täytyy toimia nopeammalla tempolla tai rytmillä kuin vastustaja. Kybersodankäynnissä ei ole rintamalinjoja vaan sodankäynti tapahtuu kaikkialla kybertilassa. Kyberhyökkäykset ja hyökkäysvektoreiden muutokset ovat hyvin nopeita. Sodankäynnissä on siirrytty päivä- ja tuntiluokasta minuutteihin ja sekunteihin.

Kybersodankäynti korostaa oman tilannetietoisuuden merkitystä ja kykyä estää vastustajaa luomasta omaa tilannetietoisuuttaan. Kybersodankäynnissä korostuu periaate, jossa ihannetapauksessa vihollinen ei koskaan havaitse omaa toimintaamme ja se yllätetään täysin.

Kybersodankäynnissä vaikuttaminen tulee kohdistaa vastustajan elintärkeisiin kohteisiin. Sotanäyttämöllä toteutettavat operaatiot täytyy suunnitella, koordinoida ja toteuttaa päämääränä vastustajan lyöminen ratkaisevilla iskuilla. Vastustajan johtamisprosessiin ja -järjestelmään voidaan iskeä kolmessa eri kyberulottuvuudessa: tiedon ulottuvuudessa, päätöksenteon ulottuvuudessa ja tietoliikenneyhteyksien ulottuvuudessa. Näkemys vihollisesta systeeminä ja vihollisen johtamisjärjestelmästä tuon systeemin tärkeimpänä toimintajärjestelmänä, kohdistaa kaiken kineettisen ja ei-kineettisenvaikutuksen strategiseen lamauttamiseen ja systeemiseen vaikuttamiseen.

Kyberhyökkäysten kohteena eivät ole vain asevoimat vaan yhteiskunnan elintärkeät toiminnat. Näin kansallisesta kyberpuolustuksesta muodostuu kiinteä osa kokonaismaanpuolustusta.

2020-luvun kehitykselle on leimallista perinteisen ja epätavanomaisen sodankäynnin rajan hämärtyminen. Sodankäyntiin sekoittuu uusia elementtejä erityisesti kybertoimintaympäristössä, tavoitteena pysyttäytyä sodan kynnyksen alapuolella. Tarkoituksellisen epävakauden ylläpito ei-kineettisten operaatioiden avulla erityisesti suurvalta voi perustella läsnäoloa ja vaikuttamista tietyllä alueella.

Kybertoimintaympäristöstä on muodostunut uusi toimintatila, jossa käytetään hyväksi erilaisia sotilaallisia ja ei-sotilaallisia painostuskeinoja sekä ei-kineettisiä operaatioita sodan jatkamiseksi asetettujen strategisten tavoitteiden saavuttamiseksi.

4.1 Johdanto

Maailma, jossa elämme, on muuttunut toiminnallisesti ja rakenteellisesti sadassa vuodessa varsin paljon. Asevoimien rooli ja tehtävät ovat kuitenkin muuttuneet varsin vähän, jos asiaa tarkastellaan riittävän abstraktilla tasolla. Sodan luonteessa, tavoitteissa ja teoriassa on tapahtunut vähän muutoksia viimeisen 100 vuoden aikana. Muutos on siis olemisen ja toiminnan tavassa – siinä, miten asioita tehdään, millaisissa rakenteissa toimitaan ja millaisilla välineillä asioita tehdään.

Teknologian kehityksessä ilmenee inkrementaalisia ja revolutionaarisia vaiheita sekä voimakkaita teknologioiden välisiä kilpailutilanteita, jossa disruptiiviset innovaatiot syrjäyttävät perinteisiä teknologioita. Kehitys esiintyy yksittäisinä suorituskykyä parantavina prosesseina ja kompleksisten systeemien rakenteiden eri tasoilla. Tuloksena on suuria muutostiloja teknologioiden ja niiden kehitysasteiden välillä. Kaikilla tasoilla ilmaantuu uusia teknologioita ja vanhoja katoaa ja teknologia etenee jatkuvasti kohti osin tuntemattomia alueita, luoden uusia ratkaisuja, systeemien tilaisuuslokeroita ja uusia tarpeita päättymättömässä kehitysprosessissa.

Uudet teknologiat luovat systeemien uusia tilaisuuslokeroita uuden teknologian täytettäväksi. Kehitysprosessin aikana emme pysty ennustamaan luotettavasti, minkälaisia kombinaatioita syntyy tai millaisia tilaisuuslokeroita luodaan, koska potentiaalis-

ten kombinaatioiden lukumäärän kasvaessa eksponentiaalisesti, kasvavat myös systeemin epävarmuustekijät. 3000 vuotta sitten oli mahdollista ennakoida teknologia 100 vuoden päähän, nyt jo muutaman kymmenen vuoden ennusteen tekeminen on vaikeaa.[1] Tämä kiihtynyt muutosnopeus ja lisääntynyt epävarmuus lisäävät tarvetta luoda tehokkaita teknologian seuranta- ja analyysimenetelmiä, jotta päätöksentekotilanteessa olisi riittävä tilannetietoisuus ja mahdollisimman luotettavia tulevaisuusarvioita.

Paul Edwards määrittelee nopeasti tietokoneistuvan asevoiman suljetun maailman (closed world) rakenteeksi, jonka taistelutilassa liikutaan asetelmaan, jossa jokainen ajatus, sana ja toiminta on kohdistettu ratkaisutaisteluun. Tässä diskurssissa tietokoneet esiintyvät voimakkaina välineinä ja metaforat lupaavat totaalista valvontaa, tehokasta kontrollia ja teknologisia ratkaisuja lukuisiin kompleksisiin ongelmiin. Edwards kytkee suljetun maailman diskurssin kybernetiikan ja informaatioteknologian kehitykseen. Tietokoneet luovat ja kasvattavat tätä maailmankuvaa kahdella tavalla. Ensiksi ne mahdollistavat suuren mittakaavan reaaliaikaisen tiedustelu-, valvonta- ja johtamisjärjestelmän rakenteet. Toiseksi ne helpottavat kansainvälisen politiikan metaforien ymmärtämistä erilaisina systeemeinä, jotka on alistettu teknologian johtoon. Samalla uudet rakenteet mahdollistavat uusien kybermaailman uhkien ilmentymisen.[2]

Tämä vuosituhat jatkaa sitä teknologista kehitystä, joka on alkanut 200 vuotta sitten. Olemme astumassa aikakauteen, jossa nanoteknologia ja erittäin nopea tietokoneprosessointi (kvanttitietokoneet) yhdistetään massiivisiin tietovoimaloihin ja niiden muodostamiin virtuaalisiin verkostoihin. Teknologia kehittyminen on ollut eksponentiaalista, joten tulevat vuosikymmenet tuottavat yhä kiihtyvällä tahdilla uusia innovaatioita. Kaikki tämä antaa olettaa, että seuraavien 30 vuoden kehitys on tuloksellisempaa kuin kuluneiden 30 vuoden kehitys.[3]

1970 luvun alussa Apollo-raketin kuualuksen tietokonekapasiteetti oli noin 40 kilobitin luokkaa – vähemmän kuin tämän päivän funktiolaskimissa. Tänä päivänä puhutaan yleisesti giga- ja terabittien kapasiteeteista. Uusimmissa älypuhelimissa ja tableteissa on perinteisen kannettavan tietokoneen suorituskyky. Nykyinen kehitysvauhti on neljä kertaa nopeampaa kuin kuluneina 30 vuotena, joten seuraavan 30 vuoden kehityksen arviointi on hyvin haasteellista. 1800-luvun lopulla tiedemiesten ajatuksissa olivat mallit ilmaa raskaammista lentokoneista, elokuvasta, massatuotantoautoista ja radiosta. Jos tuolloin olisi kysytty mikä voimakkaammin tulisi vaikuttamaan sodankäyntiin seuraavan 30 vuoden aikana, tuskin kukaan olisi osannut sanoa, että saksalaisen Nicolaus Otton työ polttomoottorin kehittämisessä uudistaisi maasodankäynnin 1914 tai Wrightin veljesten työ vuonna 1903 johtaisi strategisen ilma-aseen kehitykseen 20-vuosituhannella.[4]

---

[1] Arthur W. Brian, Teknologian luonne, Terra Cognita, Helsinki 2010, s. 166 - 173.
[2] Edwards Paul, The Closed World, Computers and Politics of Discourse in Cold War America, MIT Press, Cambridge, 1996, s. 12 -15.
[3] Weisbrook Ronald E., Captain, USN, Adapt or Die, The US Military's Responsibility to Protect America by Leading the Transformations in Science and Technology, Strategic Studies Quarterly, Vol I, Winter 2007, number 2, s. 19.
[4] Ibid

Asevoimien uudet suorituskyvyt luovat uusia mahdollisuuksia sekä kineettiseen että ei-kineettiseen voimankäyttöön kyberavaruudessa. Kyberajan suorituskyvyt mahdollistavat toiminnan uudessa epälineaarisessa ja rajoiltaan epämääräisessä hybridimäisessä taistelutilassa. Tässä tilassa tulee voida integroida saumattomasti ilmassa, pinnassa, pinnan alla, avaruudessa ja kyberavaruudessa toimivia miehitettyjä ja miehittämättömiä alustoja. Uusien järjestelmien avulla voidaan yhä tehokkaammin havaita, seurata ja identifioida maaleja sekä johtaa joukkoja ja ohjata asejärjestelmiä halutun vaikutuksen saavuttamiseksi. Tässä toimintaprosessissa nousee keskeiseksi elementiksi aika. Reaaliaikaisen tilannekuvan muodostaminen ja jaetun tilannetietoisuuden aikaansaaminen tulee olla yhä nopeampaa. Johtamisprosessissa tarvitaan sisällöltään mahdollisimman tarkkaa ja oikein aikautettua informaatiota, jopa liikkeessä, jotta keskitetty johtaminen ja hajautettu toiminta voidaan toteuttaa sekä suojata oma toiminta kybertaistelutilassa.

4.2 Teoreettinen tarkastelu

4.2.1 Sodankäynnin muutostrendi

4.2.1.1 Verkottumisen muutos

Internet on luonut verkostojen maailman. Minuutin aikana internetissä jaetaan 216 000 valokuvaa Instagram-palvelussa, Amazonissa tehdään kauppaa 83 000 dollarin arvosta, YouTubeen ladataan 72 tuntia videoita ja Google-hakuja tehdään 2 miljoonaa, 70 uutta domainia rekisteröidään ja 570 uutta web-sivua luodaan, Facebookissa tapahtuu 1,8 miljoonaa ”tykkäystä”, 204 miljoonaa emailia ja 278 000 twiittiä lähetetään.

Sotilaallisten operaatioiden toimintalogiikkana on liittää tiedon kokoojat, päätöksentekijät ja vaikuttajat toisiinsa joustavalla ja yksinkertaisella tavalla. Tietoverkko- ja tietojärjestelmäfuusion avulla luodaan informaatioinfrastruktuuri, jossa tietoa jaetaan verkon osien välillä, lähetetään ja vastaanotetaan tietoa. Informaatioinfrastruktuuri sisältää fyysisiä ja virtuaalisia rakenteita, tietokantoja ja menetelmiä tiedonjakamista varten. Verkon rakenne on kehittymässä ohjelmistoperustaiseksi, jossa laitteet ja ohjelmisto erotetaan toisistaan. Ohjelmistoperustainen verkko (Software Defined Networking, SDN) tarjoaa keinon lisätä verkon käytettävyyttä ja joustavuutta. SDN-verkko jakaantuu kolmeen abstraktiotasoon, joita ovat infrastruktuuri-, verkonhallinta- ja palvelukerros. SDN-verkon virtualisointi mahdollistaa redundanssin kasvattamisen, mikä lisää sen kyberhyökkäysten sietokykyä ja siten taistelunkestävyyttä.

Verkkokeskeisyys mahdollistaa käyttäjien liikkumisen, hajautumisen maantieteellisesti sekä virtuaalisten organisaatioiden toiminnan. Verkkokeskeisen toimintamalli aiheuttaa muutoksia ja asettaa vaatimuksia johtamisjärjestelmälle. Esikunta/johtokeskus perinteisinä johtamispaikkoina muuttuvat ja siirrytään keskitetystä hajautetumpaan johtamispaikkakonseptiin. Samalla johtamisen tietojärjestelmät muuttuvat työasemaan integroiduista järjestelmistä käyttäjäprofiileihin perustuviin järjestelmiin, jossa data on sijoittunut verkon osaksi ”pilviin”. Tiedon luotettava reaaliaikainen välitys ja käyttö koko operaatioalueella ovat välttämätön ehto muutokselle ja yhtenäinen tilannekuva analyyseineen on tarjottava taistelija-, hävittäjä- ja alustasolle saakka ja tyhjän alueen tiedot on hallittava oman toiminnan mahdollistamiseksi. Valvonta, tulenkäytönjohtaminen ja tilannekuva liittyvät saumattomasti toisiinsa. Perus-

teet resurssien käytölle pitää syntyä vastustajaa nopeammassa päätösprosessissa tilannekuvaa ja vastustajan toimintatapoja ja rakennetta analysoimalla, jotta voimankäyttö olisi tehokasta. Samalla, kun tärkeimpien (operatiivisten) joukkojen johtaminen on oltava mahdollista liikkeestä, tarvitaan kiinteä laajakaistainen verkko maanpuolustuksen kokonaisjohtamista ja yhteisoperaatioiden johtamista varten.

Tässä uudessa verkostomaailmassa verkostokeskeinen sodankäynti ja kaikki siihen liittyvät sodankäynnin muutokset liittyvät kehitykseen, jossa painopiste on siirtynyt alustoista verkostoihin, jossa kaikki toimijat muodostavat adaptiivisen ekosysteemin ja jossa huomio kohdistuu strategisiin valintoihin ja päätöksen optimointiin.[5] Verkkokeskeinen sodankäynti on operatiivinen konsepti, joka kuvaa informaatioon ja tietoverkkoihin perustuvaa joukkojen organisoitumista ja taistelutapaa. Tavoitteena on lisätä suorituskykyä liittämällä yhteen sensorit, päätöksentekijät ja aselavetit verkostoksi, joka parantaa tilannetietoisuutta, nopeuttaa päätöksentekoa, lisää toimeenpanonopeutta ja taistelunkestävyyttä.

4.2.1.2 Aikakäsitteen muutos

“ . . . A good plan violently executed now is better than a perfect plan next week.”
– Kenraali George S. Patton, Jr.

Eräs taistelukentän vaikeimmin hallittavista tekijöistä on aika. Suuri määrä nopeita operaatioita edellyttää johtajilta entistä tehokkaampaa kykyä kommunikoida suoraan operaatioissa olevien joukkojen kanssa. Moderni taistelukenttä vaatii kykyä nopeasti muuttaa toiminnan painopistettä, jotta voidaan säilyttää aloite omissa käsissä. Tämä edellyttää, että nykyiset johtamisrakenteet, järjestelmät ja toimintatavat on sopeutettu muuttuneen taistelukentän olosuhteisiin.[6]

Tulevaisuuden taistelukenttä on muuttuvampaa, hajautetumpaa, tarkempaa ja toiminnaltaan nopeampaa. Taulukossa 1 kuvataan muutosta, joka sodankäynnissä on tapahtunut kuluneiden parin vuosisadan aikana Boydin OODA-Loopin näkökulmasta.[7]

Aikakäsitteen muutoksesta esimerkkinä on tulitukioperaatio Afganistanin sodassa 2001. Marraskuun lopussa Kunduzin taistelun aikana eräs Pohjoisen Liiton komentaja pyysi amerikkalaisilta pikaista ilmaiskua alle kahden kilometrin päässä olevalla harjanteella kokoontuvaa talebanien joukkoa ja tankkeja vastaan. Komentaja vaati iskua vuorokauden sisällä. Yhdysvaltain erikoisjoukkojen sotilas välitti pyynnön välittömästi radiolla Prince Sultanin tukikohdan operaatiokeskukseen (CAOC), joka määräsi B-52-pommittajan pudottamaan 16 rypälepommia kohteeseen. B-52:n miehistö ei koskaan nähnyt yhdeksän kilometrin korkeudesta maalia, jota erikoisjoukot valaisivat lasersäteellä. Talebaneja ei isketty vuorokauden päästä pyynnöstä, vaan 19 minuutin kuluttua.

---

[5] Cebrowski Arthur K. and Garstka John J., Network-Centric Warfare: Its Origin and Future, Naval Institute Proceedings, Annapolis Maryland, January 1998.
[6] Miller, C.B., USAF TACS Battle Management: Preparing for High Tempo Future Operations, United States Air Force, 1997, s. 6.
[7] Ibid, s. 5.

Useat tekijät tekivät edellä mainitun 19 minuutin ajan mahdolliseksi: maali oli selvä ja näkyvissä, tulenjohtaja oli riittävän lähellä tunnistamaan maalin ja harjanne oli alueella, jonne tulenjohtajalla oli lupa myöntää pommituksia esimerkiksi panssarivaunukohteita vastaan. Erilaisten teknisten, toiminnallisten ja poliittisten syiden vuoksi pommitusluvan saaminen kestää usein kauemmin kuin 19 minuuttia. Kosovon sodassa kolme vuotta sitten 12 maan edustajat äänestivät siitä, mitä pommitetaan. Kiinteiden maalien pommitusten hyväksyminen kesti keskimäärin kaksi viikkoa. Yhdysvallat päätti välttää Afganistanin operaatiossaan Kosovon ilmasodassa käytetyn koalitiomallin tuomia päätöksentekovaikeuksia. Käytännössä operaation hyökkäysvaiheessa vain brittijoukot osallistuivat amerikkalaisten rinnalla varsinaisiin sotatoimiin, jolloin maalittamisen aikaviiveet voitiin supistaa minimiin.

Taulukko 1. Sodankäynnin muutos OODA-Loopin näkökulmasta.

OODA Loop	**1700-luku**	**I MS**	**II MS**	**Persianlahti 1991**	**Tuleva sota**
Havainnointi	Kaukoputki	Lennätin	Radio	Lähes reaaliaika	Reaaliaika
Orientaatio	Viikkoja	Päiviä	Tunteja	Minuutteja	Jatkuva
Päätös	Kuukausia	Viikkoja	Päiviä	Tunteja	Välitön
Toiminta	Vuoden ajan mukaan	Kuukausi	Viikko	Päivä	Tunti tai vähemmän

Seuraava kuvaus Irakin sodasta vuonna 2003 havainnollistaa myös aikakäsitteen muutosta. 21. maaliskuuta 1.Panssaridivisioonan esikunta (Iso-Britannia) antoi viisi erilliskäskyä Basran valtaamisoperaatiota varten, joissa H-hetkeksi oli määrätty 6.4 02.15. Huhtikuun 6. päivänä klo 08.15 annettiin vielä divisioonan erilliskäsky, vaikka toiminta oli käytännössä ohi Basran kaupungin romahtaessa aamupäivällä 6.4. 7.Panssariprikaatin operaatiokäsky oli päivätty samalle päivälle kello 06.00, jossa oli maininta että ”muutamat käskyssä määritellyt asiat ovat ehkä jo tapahtuneet”. Toimintaa johdettiin erillisten myöhässä olevien erilliskäskyjen varassa. [8]

Huhtikuun 21. päivänä valmistui 1.panssaridivisioonan lopullinen 4.vaiheen operaatiokäsky: normaalipaksuisena mutta aivan liian myöhään Basran operaation näkökulmasta. 1.Merijalkaväkidivisioona kommentoi tapahtunutta seuraavasti: ”Suunnittelusykli oli kaukana varsinaisen toiminnan perässä, jota edessä olevat komentajat johtivat. Oma divisioonan esikunta tuotti pitkiä erillis- ja operaatiokäskyjä, jotka saavuttivat liian myöhään rintamakomentajat, jotka olivat jo edenneet seuraavaan vaiheeseen.” [9]

Korean sodan aikana pommituskohteet valittiin yleensä joka toinen viikko. Yleensä uuden maalin havainnosta meni pommituskohteen antamiseen, käskyttämiseen ja toimeenpanoon aikaa noin yhdestä kahteen viikkoon. Vietnamin sodan alkuvaiheessa maalit määrättiin kerran viikossa Valkoisen talon tiistailounaalla. Vietnamissa ei päästy havainnosta toimintavaiheeseen juuri alle kahden viikon ja huonolla säällä aika oli paljon pitempi. Persialahdella 1991 toimintakäsky (Air Tasking Order, ATO), jossa olivat lentokierrokset ja niiden tavoitteet, julkaistiin kerran päivässä. ATO:n tekeminen vaati päiviä, vaikka viime hetken muutoksia oli mahdollista tehdä. Vuonna

[8] Storr Jim, Network Enabled Capabilities 2007: Exploring Situational Awareness and Decision Superiority in NEC Environment, 25th to 26th September 2007 Geneva.
[9] Ibid.

2003 Irakissa voitiin ATO:a päivittää vieläkin nopeammin ja tietyissä tilanteissa koko OODA-Loop toteutui minuuttiluokassa. OODA-Loop:in kehityksestä nousee esiin mielenkiintoinen kysymys, mikä on sen teoreettinen minimi ja kuinka nopeaksi se voidaan käytännössä virittää?[10]

Kun edellä kuvattuun sodankäynnin kehitykseen lisätään aika-käsitteen supistuminen, olemme päässeet verkkokeskeisen sodan käynnin ytimeen. Päätöksentekijöillä aina poliitikoista joukon komentajaan ja yksittäiseen taistelijaan on entistä vähemmän reagointiaikaa. Päivä- ja tuntiluokan aikakäsitteestä olemme siirtymässä minuutti-sekunti-luokkaan koneiden avulla. Voidaksemme olla proaktiivisia tulee sotilaalliset valvonta-, päätöksenteko ja toimintasyklit olla todella huippuunsa viritettyjä ja verkottuneita.

Arvioiden mukaan perustavalaatuinen muutos sodankäynnissä tapahtuu komentajien roolissa sodankäynnissä. Ensimmäinen muutos teknologian vaikutuksessa johtamiseen on ollut se, kuinka komentajat kykenevät johtamaan joukkojaan tietoverkon yli. Toinen muutos tapahtuu operaatioiden johtamisprosesseissa, kun saadaan aikaan toimintatapamalli operaatiojohdon roolista taisteluiden johtamisessa. Viimeisin muutos on ymmärtää, mikä osa johtamisesta kuuluu ihmiselle ja mikä voidaan jättää koneiden varaan. Kun tutkitaan tulevaisuuden koneiden sotaa, yleensä fokusoidutaan koneiden suorituskykyyn, toimintalogiikkaan ja siihen, kuinka suuri rooli koneille voidaan antaa taistelukentällä. Mutta asia on paljon monimutkaisempi, koska lisääntynyt johtamisulottuvuus ja näkyvyys taistelutilanteisiin tuovat uusia haasteita ja riskejä johtamiseen (mikrojohtaminen). Sodan nopeus ja kompleksisuus jatkavat kasvamistaan, mikä lisää tarvetta johtamisen rinnakkaisten OODA-prosessien kehittämistä.[11]

Yksi esimerkki aikatekijän muutoksesta on Slammer-verkkomato, joka lamautti osan internetin verkkoliikenteestä vuonna 2003. Hyökkäys alkoi aamulla tammikuun 25. päivänä ja se saavutti 10–15 minuutissa pääosin ne kohteet, joihin hyökkäys oli kohdistettu. Lamauttamalla viisi internetin nimipalvelua ohjaavasta 13 keskuspalvelimesta aiheutettiin internetin suorituskyvyssä 30 prosentin suorituskyvyn menetys. Tätä aikakäsitteen muutosta voi verrata tilanteeseen vuonna 1632, jolloin Ruotsin kuningas Kustaa II Adolf kaatui Lützenin taistelussa ja tieto hänen kuolemastaan saapui Tukholmaan kolmen viikon kuluttua.

4.2.1.3 Informaation ja datan lisääntyminen

Datan määrä on kasvanut eksponentiaalisesti. Googlen toimitusjohtaja on todennut, että ihmiskunnan alkuajoista vuoteen 2003 mennessä informaatiota on luotu 5 exatavua ja nyt sama määrä luodaan joka toinen päivä. Me tuotamme 2,5 kvintiljoonaa (2.5×1018) tavua joka päivä. Esimerkiksi CERN-laboratorion Large Hadron Colliderin 150 miljoonaa sensoria tuottivat 22 petatavua dataa vuonna 2012.

Datan määrä ja asema myös sotilaallisessa toimintaympäristössä on radikaalisti muuttumassa. Datan määrä kasvaa eksponentiaalisesti ja jalostettu ja analysoitu data on yhä keskeisempi suorituskykyä lisäävä tekijä. Datan perusteella luodun tilannekuvan esittämisen muodot ja keinot monipuolistuvat. Datan kasvu on luonut käsitteen

[10] Vincent Gary A., In the Loop: Superiority in Command and Control, Vol. 6, No. 2,Airpower Journal - Summer 1992, s. 22.
[11] Singer P. W., Tactical Generals, Leaders, Technology and the Perils of Battlefield Micromanagement, Ai & Space Journal, Summer 2009, Volume XXIII, No. 2, s. 83 - 86.

”Big data” ja sen määrän kasvu lisää tarvetta analyysimenetelmien kehittämiselle. Big data-analyysiä voi lähestyä yleisesti käytettyjen neljän V:n määrittelyjen perusteella:

- volume: datan määrä (sekä havaintojen että muuttujien),
- variety: datan moninaisuus ja heterogeenisuus,
- velocity: nopeus jolla dataa syntyy ja
- veracity: datan laatu.

Big datan hyödyntäminen on vasta alkutekijöissään, mutta tarjoaa suuria mahdollisuuksia niin suorituskyvyn parantamiseen ja tehostamiseen sekä uusiin toimintatapoihin.

Sotilaallisissa informaatio-operaatioissa informaatio on ajattelun keskiössä. Informaatio nähdään neljäntenä operatiivisena tekijänä, joka sitoo yhteen operatiivisina perustekijöinä pidetyt joukot, tilan ja ajan. Informaatiosodankäynnissä informaatio käsitetään missä tahansa muodossa tai järjestelmässä olevana datakertymänä, joka on hyödynnettävissä eri tekijöiden väliseen kommunikointiin ja vaikuttamiseen. Lisäksi informaatiosodankäynti sisältää käsitteet informaatiojärjestelmät, informaatioympäristö, informaatiotoiminnot ja informaatioylivoima.[12]

Erilaiset verkostot ovat levittäytyneet lähes kaikille elämän alueille. Yhteiskunnan kaikki elintärkeät toiminnat ovat enemmän tai vähemmän verkottuneita. Verkottuneisuus tarkoittaa ajasta ja paikasta riippumatonta toimintaa ja toimintojen hallintaa. Informaation ohella verkkorakenteista on tullut tärkeitä. Toinen merkittävä muutos on siinä, että informaatiosodankäynti katsotaan kuuluvaksi kriisien ja sodan aikaa, mutta kyberuhat ovat osa jokapäiväistä ihmisten ja instituutioiden arkea.

4.2.1.4 Autonomouksen lisääntyminen

Jokainen uusi ICT-teknologiasukupolvi tuottaa taistelukentällä olevan sotilaan ja hänẗ johtavien komentajien välille yhä kasvavaa etäisyyttä. Komentajien ei enää tarvitse olla etulinjassa miestensä kanssa, vaan voivat operoida komentopaikoilla, jotka siirtyvät yhä taemmas uuden teknologian salliessa. Nyt tuo saman ICT-teknologian trendi työntää kohti keskitettyä johtamista ja riskiä mikrojohtamisesta. Tämän mahdollistaa taistelutilaan levittäytyneet erilaiset miehittämättömät valvonta- ja seurantajärjestelmät sekä globaali kommunikaatiojärjestelmä. Yhdysvaltain käyttämät robottijärjestelmät ovat tulleet laajamittaisesti käyttöön tavalla, jota useimmat ihmiset eivät ole edes huomanneet. Yhdysvaltain asevoimien hyökätessä Irakiin 2003 heillä oli vain kourallinen miehittämättömiä järjestelmiä käytössään; vain yksi UAS-järjestelmä (Unmanned Aerial System) tuki koko V Armeijakuntaa. Vuoden 2008 lopussa käytössä oli yhteensä 5331 UAS-laitetta; noin 700 lennokkia tuki tuota samaa V Armeijakuntaa. Yhteensä maa- ja ilmavoimia tuettiin lähes 600 000 UAS-lentotunnilla vuodessa.

Verkottuneiden järjestelmien ja miehittämättömien systeemien kombinaatio vaikuttaa nykypäivän komentajiin aivan uudella tavalla. Se linkittää heidät lähemmäksi taistelukenttää yhä pitemmän etäisyyden päästä ja irrottaa heidät taistelutilasta. Samalla on tapahtunut irrottautuminen ajasta. Komentajat voivat antaa käskyjä reaaliajassa aivan alimman tason joukoille saakka tai järjestelmille taistelukentällä ja heillä on sa-

[12] Sotatekninen arvio ja ennuste 2025, osa 2, Puolustusvoimien Teknillinen Tutkimuslaitos, julkaisuja 15, Helsinki 2008, s. 111–117.

manaikaisesti reaaliaikainen näkyvyys sinne. Aikaisemminkin komentajat ovat olleet etäällä taistelukentältä, mutta he eivät ole voineet nähdä sitä, mitä taistelija näkee aseen tähtäimen läpi, eivätkä he ole voineet vaikuttaa suoraan toimintaan taistelutilassa. Uudet järjestelmät kuten Predator-lennokki tai maasijoitteiset sensorijärjestelmät antavat operaattorille mahdollisuuden nähdä reaaliaikaisen pintatilanteen ja samanaikaisesti tehdä päätöksiä siitä, ammutaanko vai ei.

Tämä on synnyttänyt kehityspolun, jossa jokainen sotilas ja järjestelmä on mahdollista linkittää suureen informaatioverkkoon, mikä mahdollistaa hajautetut operaatiot ja antaa suuremman aloitteellisuuden alemman tason yksiköille ja siten vähentää sodan sumussa muodostuvaa kitkaa. Miehittämättömät järjestelmät ovat muuttaneet ja muuttavat radikaalisti toimintaa taistelukentällä, mutta samalla ovat lisänneet riskiä komentajien mikrojohtamiseen.

Teknologia on auttanut ylintä johtoa olemaan pois taistelukentän pintatilanteesta, mutta nyt he ovat yhä enemmän vaikuttamassa reaaliaikaiseen toimintaan taistelutilassa. Muuttaako tämä kehitys sotilasjohtajuutta tulevaisuudessa? Neljän tähden kenraali, joka kertoo ylpeänä ja oma-aloitteisesti, kuinka hän vietti kaksi tuntia katsomalla Pedatorin kuvaa, kertoo hänen tarkoituksestaan osoittaa henkilökohtaista johtajuutta vastuullaan olevissa operaatioissa. Jokainen komentaja, joka voi nähdä mitä tapahtuu taistelukentällä, haluaa tehdä sen mahdollisimman täydellisellä tavalla. Kuka muu tuntee parhaiten komentajan tahdon, kuin komentaja itse? Monenlaisia taisteluita on hävitty, kun alijohtajat ovat tulkinneet väärin tai toimenpanneet väärin komentajan käskyt. Operaatiosta vastaava komentaja voi nopeasti tehdä muutoksia toimintaan taistelun keskellä, mieluummin kuin seurata vanhaa operaatiosuunnitelmaa, joka ei enää ole relevantti taistelukentän tapahtumien muuttumisen vuoksi.[13]

Raja oikea-aikaisen johtamisen ja mikrojohtamisen välillä on hiuksenhieno ja hämärtyy nopeasti toimittaessa miehittämättömien asejärjestelmien kanssa. Eräs pataljoonan komentaja Irakissa kertoi, kuinka hänellä oli 12 tähden arvosta kenraaleja (yksi neljän tähden, kaksi kolmen tähden ja yksi kahden tähden kenraali) kertomassa hänelle, mihin paikkaan hänen tuli joukkonsa taistelun aikana sijoittaa. Eräs erikoisjoukkojen kapteeni kertoi, kuinka prikaatikenraali neljä organisaatiotasoa ylempää, otti häneen radioyhteyden heidän jahdatessaan yhtä irakilaiskapinallista, joka oli päässyt karkuun hyökkäyksen aikana. Katsoen Predatorin kuvaa komentokeskuksessa Bagdadissa, kenraali antoi ohjeita kapteenille, ei vain kuinka hänen tuli järjestää joukkonsa, vaan kuinka hänen yksittäiset sotilaansa tuli sijoittaa. Afganistanissa eräälle taisteluajoneuvon kuljettajalle antoi upseeri satojen kilometrien päästä ohjeita, mitä tietä hänen tuli edetä hyökkäyksessä.[14]

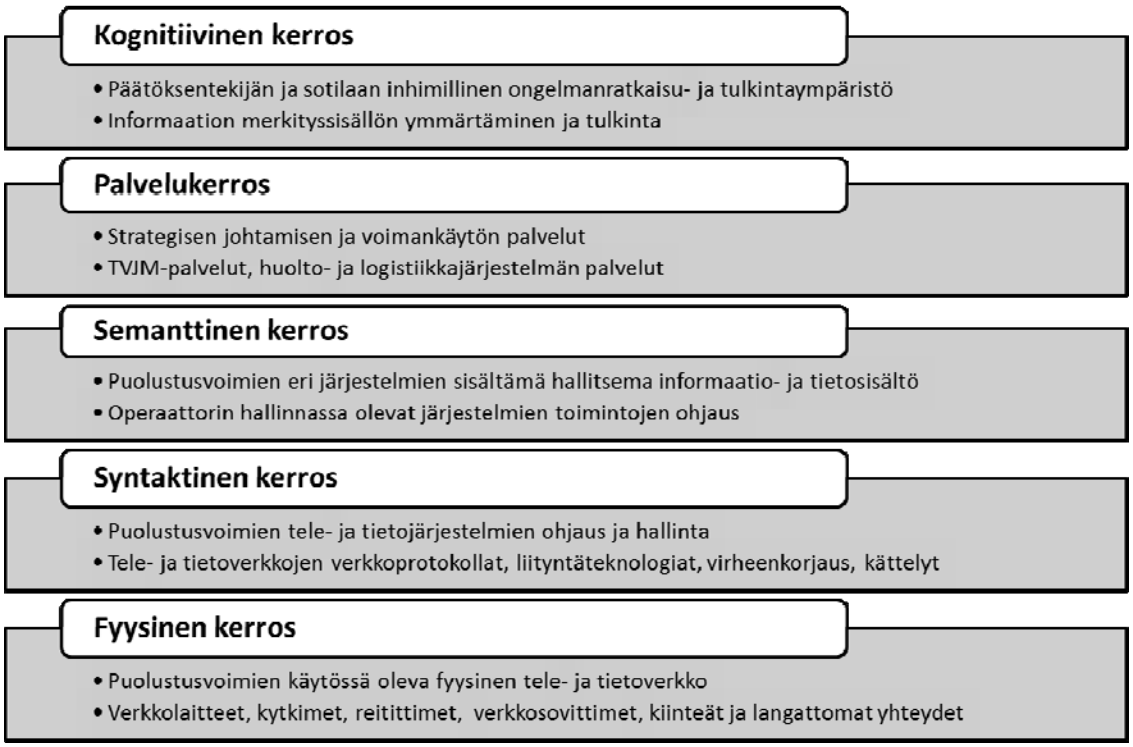
4.2.2 Puolustusjärjestelmän kyberverkon rakennemalli

Puolustusvoimien kybertoimintaympäristön infrastruktuuri koostuu puolustusvoimien ja puolustushaarojen erilaisista verkostoista sekä yhteiskunnan muista verkoista ja internet-ympäristöstä. Puolustusvoimien kyberinfrastruktuuri fuusioi kaikki tietoliikenneverkot, tietokannat ja informaatiolähteet maan kattavaksi virtuaalisysteemiksi.

---

[13] Singer P. W., Tactical Generals, Leaders, Technology and the Perils of Battlefield Micromanagement, Air & Space Journal, Summer 2009, Volume XXIII, No. 2, s. 78 - 80.
[14] Ibid.

Martin C. Libicki[15] on luonut kybermaailmaan rakenteen, jonka idea perustuu OSI-malliin (Open Systems Interconnection Reference Model). OSI-malli kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa. Kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs. Soveltaen Libickin kybermaailman mallia on mallinnettu viisikerroksinen hierarkkinen verkostomalli, jossa kerroksina ovat fyysinen, syntaktinen, semanttinen, palvelut ja kognitiivinen (kuva 1).



Kuva 1. Kybertoimintaympäristön hierarkkinen tasomalli

Fyysiseen kerrokseen kuuluvat tiedonsiirtoverkon fyysiset osat, kuten verkkolaitteet, kytkimet, reitittimet sekä kiinteät että langattomat yhteydet. Syntaktinen kerros muodostuu erilaisista järjestelmien ohjaus- ja hallintaohjelmista, liityntäteknologioista sekä toiminnoista, joilla verkkoon kytketyt laitteet ovat vuorovaikutuksessa keskenään, kuten verkkoprotokollat, virheenkorjaus, kättely jne. Semanttiseen kerrokseen kuuluu käyttäjien ja operaattoreiden järjestelmissä oleva informaatio ja tietosisällöt sekä erilaiset, käyttäjän hallinnassa olevien toimintojen ohjaus. Palvelukerros sisältää puolustusvoimien tiedustelu-, valvonta- ja johtamisjärjestelmien, taistelu- sekä huolto- ja logistiikkajärjestelmien erilaiset palvelukokonaisuudet. Kognitiivinen kerros kuvaa päätöksentekijän, operaattorin ja yksittäisen sotilaan informaation ongelmanratkaisu- ja tulkintaympäristöä, maailmaa, jossa informaatiota tulkitaan ja muodostetaan henkilökohtainen tilannetietoisuus.[15]

[15] Libicki Martin C., Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New York 2007, s. 236 - 240.

4.2.3 Kyberajan johtamisteoria

Yhdysvaltalaisen eversti John Boydin (1927–1997) teorian mukaan sotilaallisten operaatioiden tavoitteena on "murtaa vastustajan johtamisen henki ja tahto luomalla yllättäviä ja vaarallisia toiminnallisia tai strategisia tilanteita".[16] Saavuttaakseen halutun loppuasetelman täytyy toimia nopeammalla tempolla tai rytmillä kuin vastustaja. Toisin sanoen Boydin sodankäynnin päämääränä on tehdä vastustajasta toimintakyvytön estämällä häntä käyttämästä riittävästi aikaa päätöksentekoon ja toimintaan sodan jo muutenkin epävarmoissa olosuhteissa. Sotatoimien tulee fokusoitua viholliselle (1) epävakaan ja uhkaavan toimintaympäristön luomiseen ja ylläpitämiseen, ja (2) häiritä tai lamaannuttaa hänen kykynsä sopeutua tällaiseen ympäristöön.

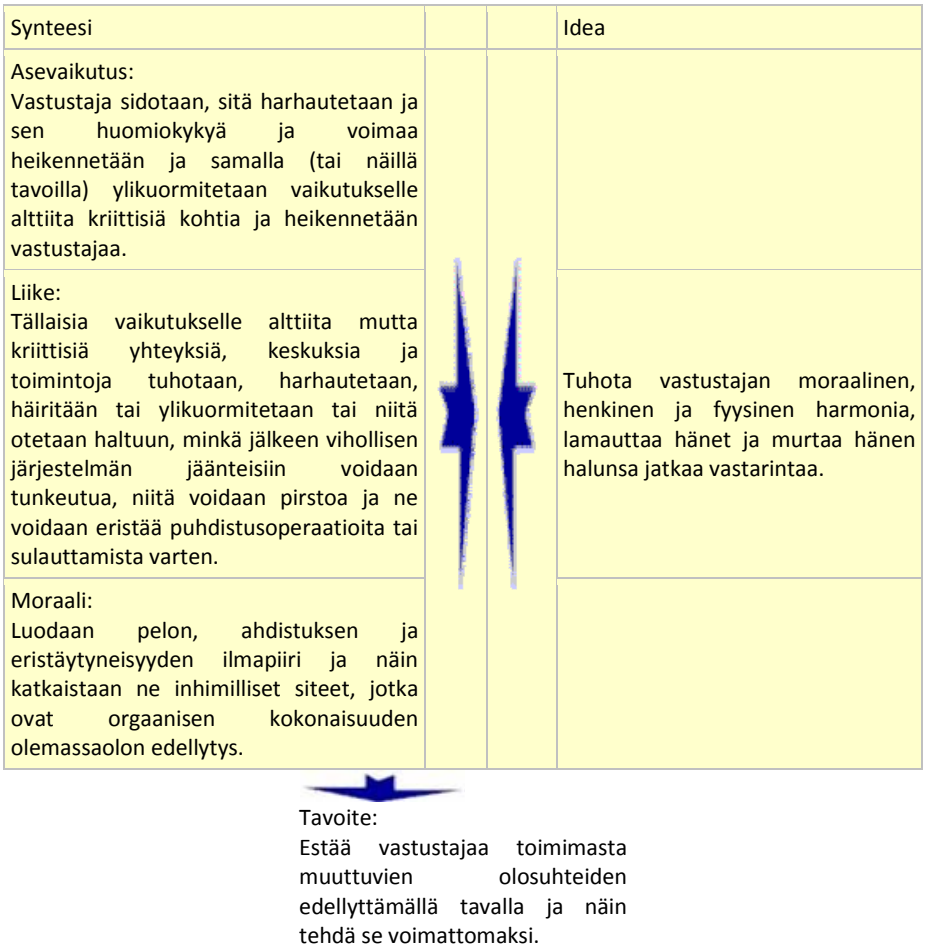
Boyd toteaa, että jokaisen operaatiomallin tavoitteena on estää vastustajan toiminnan vapaus, samalla kun parannetaan omaa toimintavapauttamme ja kykyä toimia ennen vastustajaa.[17] Boydin analyysissä ja synteesissä strateginen peli koostuu vuorovaikutuksesta ja eristämisestä; strategia on peli missä meidän on kyettävä vähentämään vastustajan kykyä kommunikoida ja olla vuorovaikutuksessa ympäristönsä kanssa samalla kuin ylläpidetään tai parannetaan omaa kykyämme tehdä samoin. Hän keskittyy ajattelussaan kolmeen tasoon: fyysiseen, henkiseen ja moraaliseen. Fyysinen taso edustaa materia-, energia- ja informaatiomaailmaa, jossa me itse kukin olemme osa, maailma, jossa elämme. Henkinen taso edustaa tunteellista/älyllistä toimintaa, me kehitämme sopeutuaksemme tai selviytyäksemme tuossa fyysisessä maailmassa. Moraali edustaa kulttuurisia menettelyohjeita tai käytösnormeja, jotka sekä rajoittavat että ylläpitävät ja fokusoivat meidän emotionaalisia/älyllisiä reaktioitamme. Näitä tasoja hän käsittelee eristäytymisen ja vuorovaikutuksen näkökulmasta. Suljettu ja eristäytynyt järjestelmä romahtaa ja sopeutuva, strategisesti ketterä sekä muuntautumiskykyinen järjestelmä selviytyy.[18]

Boydin teorian mukaan operatiivisen tason taisteluoperaatioprosessissa suunnitellaan ja toimenpannaan alkuperäiset ja edelleen jalostetut operaatiosuunnitelmat. Tätä vastustajan prosessia tulee voida häiritä nopeasti ja toistuvasti monitasoisilla toimenpiteillä. Nämä monitasoiset toimenpiteet, joita on kompressoitu ajan suhteen, aikaansaavat nopeasti tosia ja epätosia yhteensopimattomuuksia tai anomalioita, jotka uhkaavat vastustajan toimintakykyä. Vihollisen täytyy eliminoida nämä epätodet yhteensopimattomuudet, jotta hänen reaktionsa pysyisivät relevantteina.[19]

Sodassa tulee toimia vastustajan OODA-silmukoiden sisällä tai tunkeutua hänen mieleensä sekä ajan ja tilan hahmotuskykyynsä tavoitteena luoda uhkaavien tai eiuhkaavien tapahtumien ja toimien kasaumia sekä aiheuttaa toistuvasti ristiriitaisuuksia vastustajan havaitsemien tai kuvittelemien tapahtumien ja toimien ja sellaisten tapahtumien ja toimien, joihin hänen täytyy selviytyäkseen reagoida, välillä. Tällä tavalla vastustaja kiedotaan epämääräiseen, uhkaavaan ja ennalta arvaamattomaan maailman, jossa vallitsee epävarmuus, epäily, epäluottamus, sekaannus, epäjärjestys, pelko, paniikki ja kaaos. Boydin teoriassa tuli tuhota vastustajan moraalinen-

[16] Lind William S., Military Doctrine, Force Structure, and the Defense Decision-Making Process, Air University Review 30, No. 4, May–June 1979, s. 22.
[17] Boyd John R., Patterns of Conflict, December 1986, s. 128.
[18] Boyd John R., The Strategic Game of ? And ?, June 1987, s. 33 - 37.
[19] Fadok David S., John Boyd and John Warden, Air Power's Quest for Strategic Paralysis, Thesis in Air University, Montgomery Alabama 1995, s. 15.

mentaalinen-fysikaalinen harmonia, tuottaa lamautusvaikutus ja romahduttaa hänen tahtonsa vastarintaan (kts. kuva 2).[20]



Kuva 2. Boydilainen malli vastustajan toimintakyvyn tuhoamisesta

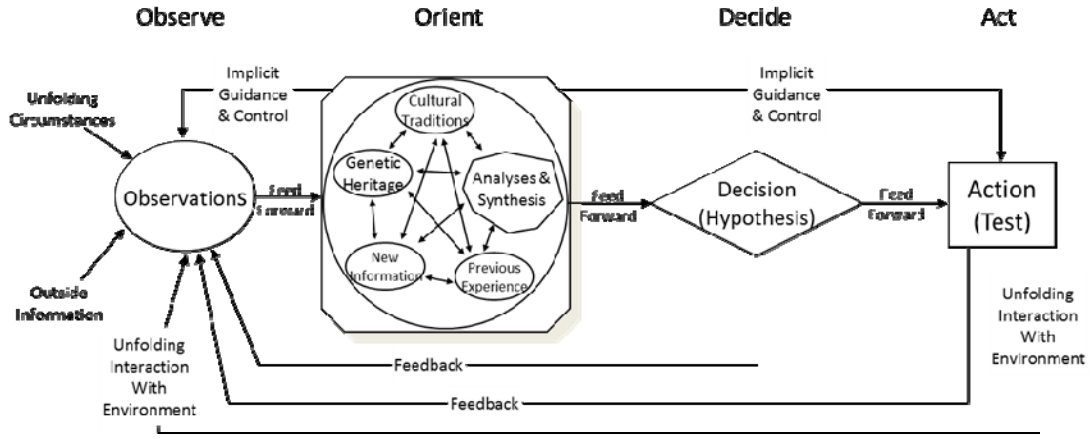
Boydin analyysin mukaan kompleksisten systeemien, kuten asevoimien lamauttaminen ja tuhoaminen onnistui parhaiten vaikuttamalla systeemin tärkeimpien osien vuorovaikutukseen. Vastustajan elintärkeiden osien kommunikaation ja vuorovaikutuksen tuhoaminen estäisi sen koordinoidun toiminnan. Clausewitziläiseen perinteeseen kuuluu vaikuttaminen vihollisen painopisteeseen.[21] Boydin mielestä tehokkainta oli vaikuttaa painopisteiden välisiin yhteyksiin ja toimintoihin kuin itse painopisteeseen.[22]

Boydin mukaan menestyäksemme taistelussa meidän tulee toimia ja reagoida nopeammin kuin vastustaja. Tämän mallin hän esitti OODA-Loopissaan (Observe-Orient-Decide-Act). Hänen mukaansa ”jos emme luo kaikkia edellä esitettyjä asioita sisältä-

[20] Boyd John R., Patterns of Conflict, December 1986, s. 136.
[21] Clausewitz von, Carl, Sodankäynnistä, Art House, 2002, s. 16-17, 30, 34 - 37.
[22] Kagan Frederick W., Finding the Target, the Transformation of American Military Policy, Encounter Books, New York 2006, s. 108 - 110.
Hammond Grant T.; The Mind of War, John Boyd and American Security, Smithsonian Books, Washington, 2001, s. 129.

viä OODA-Loop:ja ja jos emme pysty tunkeutumaan muiden OODA-Loop:ien (tai muiden ympäristöjen) sisään, huomaamme olevamme kykenemättömiä ymmärtämään ja muokkaamaan todellisuutta, joka on jatkuvassa kehityksen tilassa, alati muuttuva, epävarma, ja ennalta arvaamaton, emmekä pysty sopeutumaan tällaiseen todellisuuteen, eikä se pysty muokkaamaan ajatteluamme."[23]

Boyd yhdistää suurstrategian epistemologiaan, ja esittää päätöksenteon mallin kyberneettisenä kaksoissilmukkana (kts. kuva 3). Sinänsä yksinkertainen malli on kuitenkin moniosainen ja kokonaisvaltainen, sisältäen syvällisen prosessin, joka on enemmän kuin idea nopeasta OODA-Loop:ista.[24]



Kuva 3. The OODA "Loop"[25]

OODA-Loopin idea on, että henkilö havainnoi tapahtumaa tai tilannetta, evaluoi havaintoa geneettisestä, kulttuurisesta, psykologisesta ja muiden mentaalisten taipumusten näkökulmasta, päättää tarkoituksenmukaisista vastatoimenpiteistä ja sitten panee päätöksen toimintaan. Tätä prosessia toistetaan jatkuvasti. Kompleksisilla organisaatioilla, kuten asevoimilla, on moninkertaisia OODA-Loopeja toiminnassa samanaikaisesti. Alemman tason loopit toimivat yleensä nopeammin kuin ylemmän tason, mutta ne ovat harmonisoitu yhteen kompleksisella tavalla. Boydin mielestä on olennaista ylläpitää suurinta mahdollista joustavuuden ja aloitteellisuuden tasoa, jotta toimenpiteet voidaan pitää säännönmukaisesti nopeina ja ennakoimattomina. [26]

Boydin synteesin mukaan asevoima, joka kykenee adaptoitumaan ja reagoimaan nopeimmin jatkuvasti muuttuvissa taistelukentän ympäristöissä, on voittaja. Toisin sanoen sota on pelkästään suurella nopeudella tapahtuva luonnonvalintainen pro-

[23] Boyd John R., The Essence of Winning and Losing, June 1995, s. 2.
[24] Osinga Frans P.B., Science, Strategy and War, The Strategic Theory of John Boyd, Routledge, London and New York, 2007, s. 230.
[25] Boyd John R., The Essence of Winning and Losing, June 1995, s. 4.
[26] Kagan Frederick W., Finding the Target, the Transformation of American Military Policy, Encounter Books, New York 2006, s. 104 - 105.
Hammond Grant T.; The Mind of War, John Boyd and American Security, Smithsonian Books, Washington, 2001, s. 129.

sessi. Paikallaan pysyvä armeija (fyysisesti tai virtuaalisesti), joka on sitoutunut yksittäiseen muuttumattomaan teknologiaan, voitetaan ja tuhotaan nopeasti.[27]

OODA-silmukan tai päätöksentekosyklin ehdoton edellytys on ketteryys taktisella, operatiivisella ja strategisella tasolla. Meidän ei pidä vain ajatella vastustajaa nopeammin, meidän täytyy myös liikkua häntä nopeammin fyysisessä ja virtuaalisessa taistelutilassa. Jotta nopeasta tekniikan kehityksestä hyödyttäisiin parhaiten, tarvitaan sekä henkistä että fyysistä ketteryyttä niin operaatiokeskuksissa kuin taistelutilassakin.[28]

OODA-Loop:in periaatteen mukaisesti johtajien tulee tehdä päätöksiä nopeasti mutta joustavuutta täytyy ylläpitää sopeutumalla jatkuvasti muuttuvaan ympäristöön. Johtajien täytyy myös harjaantua tilanteisiin, jossa heidän tulee toimia komentajan tahtotilan perusteella. Jatkuvaa havainnointia ja tilannetietoisuuden ylläpitoa tullee myös kouluttaa, jotta OODA-Loop saadaan toimimaan optimaalisesti.[29]

Vihollisen OODA-Loop:in analyysissä kysymys on siitä, mitä vihollinen tulee havaitsemaan, tai mitä hän havaitsee nyt? Ihannetapauksessa vihollinen ei koskaan havaitse omaa toimintaamme ja se yllätetään täysin. Sun Zu:n näkemys harhautuksesta on havaittavissa Boydin ajattelussa. Yllätystä voi toteuttaa hyökkäämällä yöllä päivän sijasta. Se voidaan saada aikaan hyökkäämällä taistelualueen takaosasta, sivustasta tai vähiten odotetusta suunnasta. Oikein toteutetut harhautukset ja demonstraatiot ovat perusasioita, kun halutaan kiistää vastustajan kyky tarkkaan havainnointiin. Komentajan ei pitäisi luoda tunnistettavissa olevaa toimintatapaa, jonka vihollinen voi tunnistaa ja käyttää hyväkseen.[30]

Tämä myös koskee myös vihollisen taistelukentän tiedustelukykyä. Ilman jatkuvaa tiedustelua vihollisella on vaikeuksia laatia toimivia taistelusuunnitelmia. Vihollisen tiedustelukyvyn estäminen tai vaikeuttaminen mahdollistaa komentajan pääsemisen vihollisen OODA-Loop:in sisälle, ja tämä lisää komentajan suunnitelman tehokkuutta. Jos komentaja estää viholliselta kyvyn havaita tarkkaan tilannetta, vihollisen OODA-Loop:lla ei ole toimintaedellytyksiä. Tämän jälkeen vihollisen tilanteen hahmottaminen, päätöksenteko ja toiminta ovat aina virheellisiä.[31]

4.2.4 Kyberajan vaikuttamisteoria

Yhdysvaltalaisen everstin John Wardenin (1943–) teorian mukaan sodan kineettiset operaatiot käydään kolmiulotteisessa tilassa: maalla, merellä ja ilmassa. Ilma-aseella voidaan iskeä vastustajaan satoja tai tuhansiakin kilometrejä maa- ja merivoimien edellä. Hänelle ilmavoima on monella tavoin hyökkäyksen ensimmäinen aalto riippumatta siitä, toimiiko se maatukikohdista vai lentotukialuksilta. Se on erittäin liikku-

---

[27] Mason Steven, John Boyd and strategic Naval air power, United States Naval Institute Proceedings, Vol. 129, No. 7, Annapolis, Jul 2003, s. 77.
[28] Shanahan John N.T., Shock-Based Operations, New Wine in an Old Jar, Air & Space Power Journal - Chronicles Online Journal, 15 October 2001, s. 3.
[29] Bazin Aaron A., Boyd's O-O-D-A loop and the infantry company commander, Infantry, Vol. 94, No.1, January/February 2005, s. 18.
Curtenaz Sylvain, Effects-Based… what, Military Power Revue, eine Beilage zur Allgemainen Schweizerischen Militärzeitschrift, ASMZ, August 2008, s. 23.
[30] Bazin Aaron A., Boyd's O-O-D-A loop and the infantry company commander, Infantry, Vol. 94, No.1, January/February 2005, s. 18 - 19.
[31] Ibid, s. 19.

vaa ja helposti keskitettävää. Ilmavoimalla voidaan hallita taistelutilan kolmatta ulottuvuutta ja voittaa aikaa maavoimien siirtämiseen ja ryhmittämiseen toisessa ulottuvuudessa käytävää taistelua varten.[32]

Vaikuttaminen tulee kohdistaa vastustajan elintärkeisiin kohteisiin (= painopiste), jotka muodostavat hierarkkisen rakenteen. ”Sodankäynnin jokaisella tasolla on yksi tai useampia painopisteitä. Jos painopisteitä on useita, voimaa täytyy suunnata niistä jokaista vastaan tavoitteen saavuttamiseksi. Kaikissa tilanteissa sotanäyttämöllä suoritettavat operaatiot täytyy suunnitella, koordinoida ja toteuttaa siltä pohjalta, että niiden päämäärä on vastustajan lyöminen ratkaisevilla iskuilla. Painopisteitä, joilla todella on merkittävä vaikutus systeemin toimintaan, on suhteellisen vähän. Vaikuttaminen painopisteisiin on hyvin kustannustehokas tapa toimia. Rinnakkaisoperaatioilla voidaan aikaan saada suhteellisen lyhyessä ajassa hyvin suuria muutoksia vastustajan elintärkeissä järjestelmissä ja toiminnoissa.[33]

Warden kuvaa vastustajaa ja yhtä järjestelmällistä maalien valintatapaa Five Ring-mallilla (kts. kuva 4). Sisin kehä on hänen mukaansa tärkein, sillä siellä on johto - ”ainoa vastustajan toimija, joka voi tehdä myönnytyksiä”. Kaiken toiminnan ”tulisi kohdistua vastustajan johdon mieleen tai vastustajan järjestelmään kokonaisuutena”. Jos johtoon ei voida iskeä suoraan, johtajiin on kohdistettava epäsuoraa painetta niin paljon, että he toteavat myönnytykset välttämättömiksi, huomaavat toimintamahdollisuuksiensa kadonneen tai havaitsevat valtionsa olevan fyysisesti kykenemätön jatkamaan vihollisuuksia.[34]

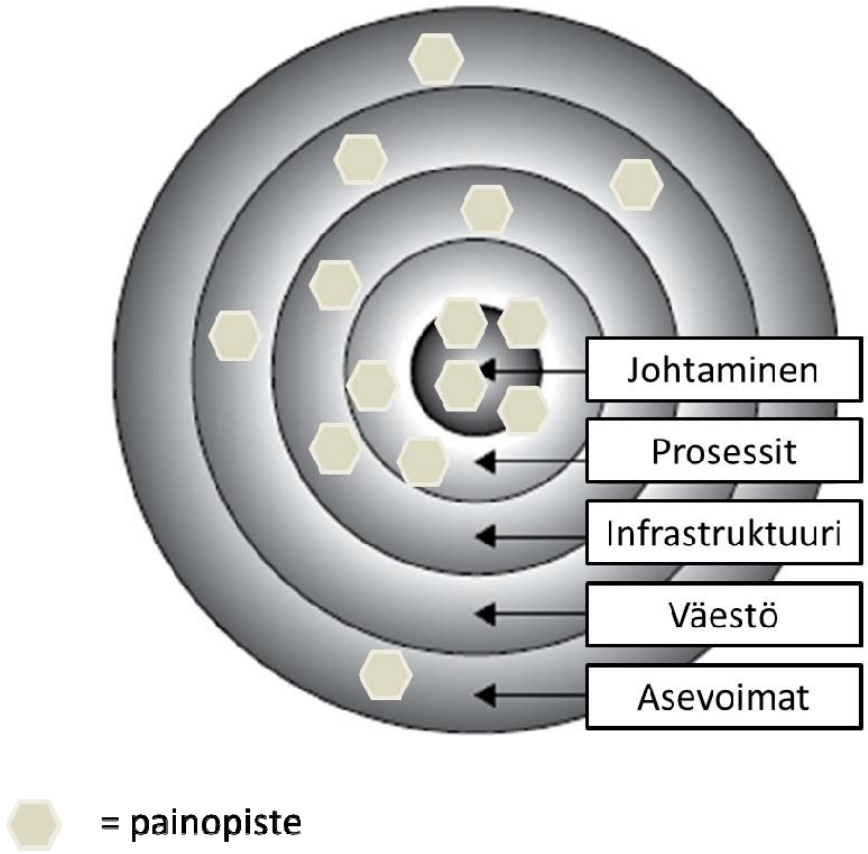
Tärkeysjärjestyksessä seuraava kehä edustaa yhteiskunnan elintärkeitä toimintoja/prosesseja, sillä niiden tuhoaminen tekee elämisen vaikeaksi, eikä valtio kykene huolehtimaan kansalaistensa elintärkeistä toiminnoista, joten se joutuu tekemään merkittäviä myönnytyksiä.[35]

Seuraava kehä on kriittinen infrastruktuuri. Tuossa kehässä on logistiikkaverkko, joka kuljettaa siviili- ja sotilaskäyttöön tarkoitettuja tavaroita ja palveluja valtion koko alueella. Siihen kuuluvat rautatiet, lentoyhtiöt, valtatiet, sillat, lentokentät, satamat ja muut vastaavat laitteistot ja järjestelmät samoin kuin pääosa teollisuudesta, josta suurin osa jää yhteiskunnan elintärkeiden toimintojen kehän ulkopuolelle. Hyökkäys infrastruktuuria vastaan tarkoittaa, että ”valtiojärjestelmän energiataso romahtaa nopeasti ja järjestelmän kyky vastustaa vastustajan vaatimuksia heikkenee”.[36]

---

[32] Warden John A., Planning to Win, Air University Review, Vol. XXXIV, No. 3, March–April 1983, s. 97.
[33] Warden John A., The Air Campaign: Planning for Combat, toExcel reprint, 1998, s. 7.
Warden John A., Strategic Thinking and Planning, Venturist Publishing, Montgomery Alabama, 2000, s. 36.
[34] Warden John A., The Enemy as a System, Airpower Journal, Spring 1995, s. 49 - 51
West Scott D., Warden and the Air Corps Tactical School -Déjà Vu?, thesis presented to the Faculty of The School Of Advanced Air and Space Studies, Air University Press, Maxwell AFB, Alabama, October 1999, s.11.
[35] Warden John A., The Enemy as a System, Airpower Journal, Spring 1995, s. 49 - 51.
West Scott D., Warden and the Air Corps Tactical School -Déjà Vu?, thesis presented to the Faculty of The School Of Advanced Air and Space Studies, Air University Press, Maxwell AFB, Alabama, October 1999, s.11.
[36] Ibid.

Seuraavaa, väestöä kuvaavaa kehää, vastaan on ”vaikea hyökätä suoraan, vaikka moraalisia näkökohtia ei otettaisikaan huomioon”. Warden ei kannata suoria tai epäsuoria hyökkäyksiä vihollisvaltion väestön moraalin murentamiseksi, sillä hänestä suorat iskut siviilejä vastaan ovat ”moraalisesti tuomittavia” ja yritykset moraalin heikentämiseksi epäsuorilla iskuilla ovat aina olleet tehottomia.[37]



Kuva 4. Wardenin Five Rings -malli[38]

Viimeisessä kehässä ovat vihollisvaltion asevoimat. Vaikka asevoimia yleensä pidetään clausewitziläisestä näkökulmasta sodankäynnin toimijoista tärkeimpinä, ne ovat tosiasiassa keino tavoitteiden saavuttamiseksi; toisin sanoen, niiden ainoa tehtävä on suojata omien sisempien kehien toimijoita tai uhata vastustajan sisempiä kehiä. Valtio saadaan varmasti taipumaan myönnytyksiin heikentämällä se asevoimia, ja jos ne tuhotaan kokonaan, valtio saattaa olla pakotettu tekemään viimeisimmänkin myönnytyksen yksinkertaisesti siitä syystä, että johto tietää sisempien kehiensä joutuneen puolustuskyvyttömiksi ja todennäköisesti tuhon omiksi. Nykytekniikka on tuonut saataville uusia ja poliittisilta vaikutuksiltaan tehokkaita vaihtoehtoja, joiden myötä kenttäarmeijoista on tullut keino päämäärien saavuttamiseksi sen sijaan, että ne olisivat itsetarkoituksellisia päämääriä.[39]

[37] Ibid.
[38] Warden John A., Martti Lehdon haastattelu Montgomery, Alabama, 23.2.2011.
[39] Ibid.

Lopuksi Warden korostaa, että hänen viiden kehän mallinsa kuvaa nykyaikaisen vihollisvaltion toimijoita, ja että hyökkäämällä jokaista kehää vastaan vastustajan asevoima voidaan eristää johdosta ja tehdä merkityksettömäksi. Tavoitteeseen päästään parhaiten edellä kuvatulla tavalla sen sijaan, että iskut kohdistettaisiin vain uloimpaan, vastustajan asevoimaa kuvaavaan kehään.[40]

Kehillä sijaitsevia painopisteitä/kohteita on yleensä toiminnan kannalta liikaa. Irakin 1991 ilmaoperaation suunnitteluvaiheessa Checkmate-ryhmä määritteli yli 200 000 tärkeää maalia Irakissa. Maalin valinnassa maalien määrä ole itsetarkoitus, niitä tulee tarkastella systeemin osina. Tämä tarkoittaa, että vaikuttaminen johonkin maaliin vaikuttaa suoraan tai epäsuoraan toiseen. Irakissa vaikutettiin maan energiajärjestelmään tavalla, joka esti sen strategisen tason toiminnan ja lamautti myös asevoimien suorituskykyä. Maalien valinnassa on järkevää valita sellaisia, jotka nopeimmin, pitkävaikutteisimmin, taloudellisimmin ja tehokkaimmin aikaansaavat systeemimuutoksen.[41]

Wardenin mukaan vastustajan johtamisprosessiin ja -järjestelmään voidaan iskeä kolmessa eri kyberulottuvuudessa: tiedon ulottuvuudessa, päätöksenteon ulottuvuudessa ja tietoliikenneyhteyksien ulottuvuudessa. Jos johtoa kyetään häiritsemään riittävästi missä tahansa näistä ulottuvuuksista, vastustajan operaatioiden tehokkuus alkaa heikentyä dramaattisesti. Johto on todellinen painopiste ja sitä vastaan kannattaa iskeä kaikissa olosuhteissa, joissa hyökkäys on mahdollista. Jokaista ulottuvuutta vastaan voidaan hyökätä suorasti tai epäsuorasti, ja paras toimintamalli riippuu kulloisestakin tilanteesta. Päätöksenteon ulottuvuus on selvästi avainasemassa, sillä ilman sitä kaksi muuta ulottuvuutta menettävät merkityksensä.[42]

Wardenin mukaan emme voi ajatella strategisesti, jos ajattelumme lähtökohtana ovat yksittäiset lentokoneet, lentosuoritukset tai asejärjestelmät — tai jopa vastustajan koko sotilaallinen voima. Meidän täytyy keskittää huomiomme ensin vastustajaamme kokonaisuutena. Strategisessa ajattelussa tulee huomio kohdistaa systeemivaikutuksiin eikä yksittäisiin maaleihin. Tuhotut lentokoneet, panssarivaunut, laivat, sotilaalliset rakenteet tai aiheutetut tappiot elävälle voimalle eivät välttämättä ilmennä systeemivaikutusta. Warden mainitsee esimerkkinä hyökkäykset Irakin sähköverkostoa vastaan. Ilmahyökkäyksellä tuhottiin vain 10 % sähköverkosta, joka taktisen arvion mukaan oli kehno suoritus. Käytännössä näiden iskujen perusteella Irak pimeni täysin, jolloin strategisen vaikutusanalyysin mukaan suoritus oli erinomainen, ts. systeemivaikutus on yksittäisiä taktisia vaikutuksia järkevämpi analyysimuoto.[43]

---

[40] Ibid.

[41] Warden John A., Strategic Thinking and Planning, Venturist Publishing, Montgomery Alabama, 2000, s. 31.
Warden John A., luento Maanpuolustuskorkeakoulussa Helsingissä 25.5.2010.

[42] Warden John A., The Air Campaign: Planning for Combat, toExcel reprint, 1998, s. 44 - 47.

[43] Warden John A., The Enemy as a System, Airpower Journal, Spring 1995, s. 42.
Warden John A., Strategic Thinking and Planning, Venturist Publishing, Montgomery Alabama, 2000, s. 36.
Warden John A., luento Sotatieteen päivillä Maanpuolustuskorkeakoulussa Helsingissä 25.5.2010.

4.2.4.1 Five Rings operaatiokonsepti

Persianlahden sodan ilmaoperaatioita vuonna 1991 voidaan pitää kyberajan ilmasodan avauksena. Elokuun 2. päivänä Irak hyökkäsi Kuwaitiin ja valloitti maan nopeasti. Presidentti Saddam Hussein liitti Kuwaitin Irakin 19. maakunnaksi. YK:n talouspakotteet ja vaatimukset eivät tehonneet, joten Yhdysvaltain johtama liittokunta suunnitteli kaksiosaisen operaation Desert Shield ja Desert Storm. Desert Shield alkoi 7.8.1990 jatkuen siihen saakka, kunnes 17.1.1991 alkoi monikansallinen operaatio Desert Storm tavoitteenaan saada Irak vetäytymään Kuwaitista. Desert Storm alkoi ilmaoperaatiolla, jota seurasi 24.2 alkanut maaoperaatio. 100 tuntia kestänyt maaoperaatio päätti sodan 28.2.1991.

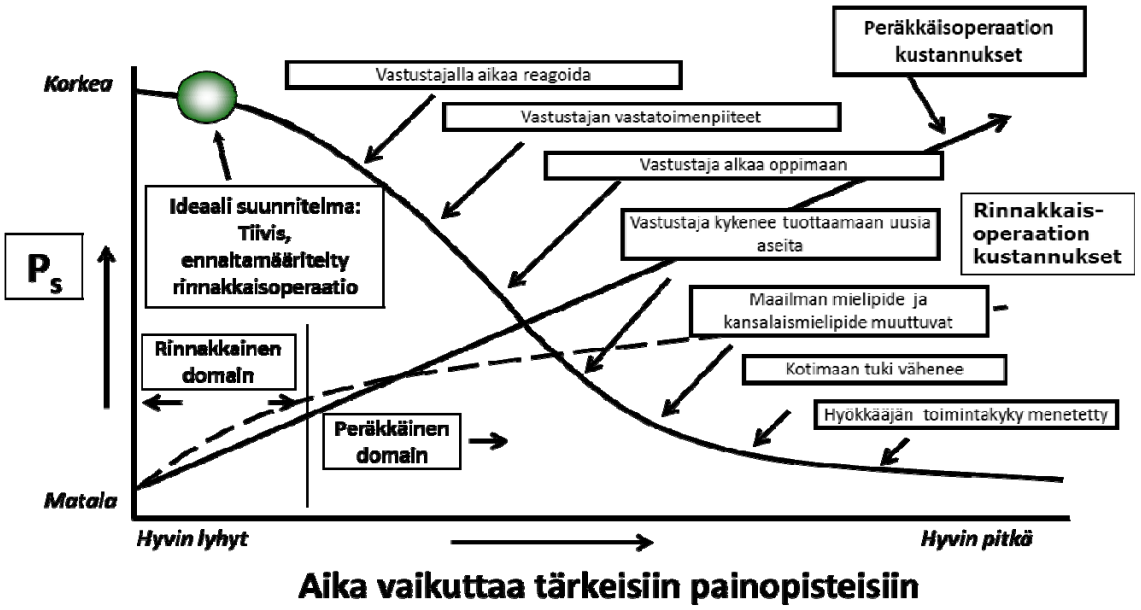
Sodan kestettyä 24 tuntia pommitusten kohteeksi olivat joutuneet sotilaallisten kohteiden lisäksi Irakin alueella olevat sillat, tehtaat, telakat ja satamat. Tuon vuorokauden aikana lennettiin yli 1300 hyökkäyksellistä lentosuoritusta. Sodan ensimmäisen vuorokauden tärkein saavutus ei kuitenkaan ollut lentosuoritusten määrä, vaan tapa, jolla ne oli suunniteltu haluttujen vaikutusten aikaansaamiseksi. Ilmasodan ensimmäisen 24 tunnin ajalle laaditussa hyökkäyssuunnitelmassa iskujen kohteeksi oli määritetty 152 erillistä maalia ja lisäksi Irakin maavoimien joukkoja ja ilmatorjuntaohjusasemia.

Ensimmäisen vuorokauden hyökkäyssuunnitelmassa oli enemmän maaleja, kuin mitä koko Yhdysvaltain 8th Ilma-armeijalla oli ollut vuosina 1942 ja 1943 (noin 50 maalia), ja noiden 24 tunnin aikana ilmasta käsin oli isketty useampaan erilliseen kohteeseen kuin koskaan ilmasodankäynnin historiassa. Iskunopeus oli yli tuhat kertaa suurempi kuin ilmaoperaatioissa Saksaa vastaan vuonna 1943. Tuolloin Saksa kykeni toipumaan pommituksista ja saattoi jatkaa sotatoimia yli kaksi vuotta. Irakissa iskut aiheuttivat 24 tunnissa shokkivaikutuksen, josta maa ei pystynyt toipumaan lainkaan.[44]

Rinnakkaissodankäynnissä isketään yhtä aikaa valtion johtoon ja yhteiskunnan elintärkeisiin toimintoihin kuten öljynjalostamoihin, voimalaitoksiin, liikenneverkkoon, johdon ja väestön välisiin tiedotuskanaviin ja vastustajan asevoimaan. Näin voidaan vaikuttaa vastustajan toimintakykyyn selvästi nopeammin ja tehokkaammin kuin perinteisissä peräkkäisoperaatioissa.[45] Kuvassa 5 on esitetty rinnakkais- ja peräkkäisoperaatioiden vaikuttavuus Wardenin näkemyksen mukaan.

[44] Deptula David A., Effects Based Operations: Change in the Nature of Warfare, Aerospace Education Foundation, Defence and Airpower Series, Virginia 2001, s. 1 - 2.
Warden John A., luento Sotatieteen päivillä Maanpuolustuskorkeakoulussa Helsingissä 25.5.2010
Warden John A., Strategic Thinking and Planning, Venturist Publishing, Montgomery Alabama, 2000, s. 43 - 44.

[45] Deptula David A., Effects Based Operations: Change in the Nature of Warfare, Aerospace Education Foundation, Defence and Airpower Series, Virginia 2001, s. 3 - 4.
Warden John A., luento Sotatieteen päivillä Maanpuolustuskorkeakoulussa Helsingissä 25.5.2010.



Kuva 5. Rinnakkaisoperaatiot vs. peräkkäisoperaatiot Wardenin mallin mukaan[46]

4.2.4.2 Vaikutusperustainen operaatiokonsepti

Vaikutusperustainen operaatiokonsepti (Effects Based Operation, EBO) sai alkunsa John Wardenin luomasta operaatio Desert Stormin maalittamisstrategiasta. Tuolloin sekä Wardenin Checkmate-suunnitteluryhmä Pentagonissa että everstiluutnantti David Deptulan Black Hole -suunnitteluryhmä Riadissa keskittyivät pelkän maalien tuhoamisen sijasta analysoimaan maalien vaikutuksia, jotka tukisivat ilmaoperaation tavoitteita.

EBO-konseptin perustana on Wardenin Five Rings -malli. Sodan jälkeen David Deptula jatkoi maalittamisen analysointia ja hahmotteli EBO-käsitettä Five Ringsin pohjalta. Wardenin mukaan Five Rings -prosessissa toinen kehitysaskel tai -vaihe on haluttujen vaikutuksien määrittäminen painopistettä varten. Ensimmäinen askel on painopisteiden tunnistaminen. Deptula päätti keskittyä syvällisemmin vaikutusanalyyseihin. Yhdysvaltain Tactical Air Commandin (TAC) sisällä oli paljon Five Rings -mallin vastustajia, minkä vuoksi Five Rings nimenä herätti epäluuloja ilmavoimissa, joten uusi konsepti nimettiin EBO:ksi. Deptula keskittyi painottamaan toiminnan vaikutuksia ja pystyi täten edistämään konseptin kehittämistä.[47]

EBO-käsite laajentaa taktista ajattelua ja tuo siihen mukaan sodan operatiiviset ja strategiset tasot. Mikäli pitää vihollisvaltiota "järjestelmien järjestelmänä", siitä seuraa, että häiriö yhtä järjestelmää vastaan vaikuttaa järjestelmän muihin osiin kuten tuhotut tietoliikenneyhteydet integroidussa TVJ-järjestelmässä.[48]

[46] Warden John A., luento Sotatieteen päivillä Maanpuolustuskorkeakoulussa Helsingissä 25.5.2010.
[47] Warden John A., Martti Lehto haastattelu, Montgomery Alabama, 25.11.2009.
[48] Foster H. A., Organizing for Effect: Assessing the Institutional Machinery Needed to Effectively Conduct Effects-based Operations, Master of Military Studies, United States Marine Corps, Command and Staff College, Marine Corps University, Quantico, Virginia, 2002.

Rinnakkaissodankäynti on yksi sotilaallisen voiman käyttötapa. Se on sarja vastustajan painopisteitä vastaan tehtäviä samanaikaisia hyökkäyksiä tavoitteena vastustajan strateginen lamauttaminen. Vastustaja on lamautettu strategisesti, kun se ei enää kykene tehokkaaseen vastarintaan. Samanaikaisten hyökkäysten tunnusomainen piirre on niiden nopeus. Rinnakkaissodankäynnin perimmäinen tavoite ei ole yksinomaan strateginen lamauttaminen, vaan lamauttamisen on myös tapahduttava nopeasti. Rinnakkaissodankäynti on nopeatempoista ja usein sitä kutsutaankin hypersodaksi. Sillä voidaan vähentää (kummankin osapuolen) tappioita, pienentää voimavarojen tarvetta, säilyttää omien näkökantojen uskottavuus (jos aika on merkittävä tekijä) ja estää vastustajaa toipumasta tai ryhtymästä vastatoimiin.[49]

Rinnakkaissodankäynti edustaa ”vallankumousta sotilaallisessa ajattelussa”, ja vaikutusperustaiset operaatiot ovat tämän sodankäynnin muodon yksi tärkeimmistä tekijöistä. Vaikutusperustainen lähestyminen ei ole vain tapa hyödyntää uutta tekniikkaa, vaan se edellyttää jo perustasolla uusien ajatusmallien omaksumista sotatoimien suunnittelussa. Vaikutusperustaisilla operaatioilla saavutetaan useita hyötyjä. Ensiksikin ne ovat toteuttamiskelpoinen vaihtoehto kulutus- ja tuhoamissodalle keinona pakottaa vastustaja käyttäytymään halutulla tavalla; toiseksi, niissä hyödynnetään olemassa olevia asejärjestelmiä samalla kun uusi tekniikka tekee tuloaan; ja kolmanneksi, sotilasorganisaatioiden täytyy muuttua voidakseen suorittaa vaikutusperustaisia operaatioita parhaan mahdollisen hyödyn tuottavalla tavalla. Vaikutusperustaisten operaatioiden onnistumisen ehdoton edellytys on järjestelmäperustainen tiedustelutiedon analysointi. Ellei tiedetä riittävän tarkasti, mitä vastustaja tarvitsee pystyäkseen johtamaan sotatoimia ja vaikuttamaan haluamallaan tavalla, rinnakkaissodankäynti ei voi olla tehokasta. Avaruuteen sijoitetuilla järjestelmillä, ICT-teknologioilla ja nopealla tiedonsiirrolla voidaan pienentää varsinaiselle taistelualueelle sijoitettujen joukkojen ja asejärjestelmien määrää ja siten pienentää systeemin haavoittuvuutta. Tarvittavat muutokset voivat tuoda mukanaan aikaisempaa laajemman tukeutumisen sotatoimialueen ulkopuolisiin johtamis- ja tiedusteluorganisaatioihin, hajautettuja strategisen tiedustelun rakenteita ja alustasta riippumattomia järjestelmiä, jotka kykenevät tuottamaan tietoa suoraan käyttäjille.[50]

4.3 Johtopäätöksiä kybertaistelun kehityksestä

Sotilaalliset operaatiot edellyttävät tarkkaa analysointia, joiden kohteina ovat vastustajan painopisteet, solmukohdat ja elintärkeät haavoittuvat kohteet. Vain tällaista kokonaisvaltaista lähestymistapaa käyttämällä sotilaskomentajat pystyvät ymmärtämään kaikilla tasoilla, miten strategiset tavoitteet ovat saavutettavissa kineettisillä ja ei-kineettisillä operaatioilla. Operaatiot onnistuvat, jos vastustajan elintärkeisiin solmukohtiin hyökätään kaikin mahdollisin fyysisin ja informaatioteknologian keinoin. Tällä tavalla voidaan tuhota vastustajan kyky mukautua tilanteen muutoksiin ja saadaan hänet uskomaan, että häneen kohdistuu iskuja aina fyysisestä kerroksesta kognitiiviseen kerrokseen saakka. Silloin mikään ei näytä olevan turvassa. Aina kun

[49] Pardo Jr. John R., Parallel Warfare, Its Nature and Application, in Karl P. Magyar, ed., Challenge and Response, Air University Press, Maxwell AFB, Alabama, 1994, s. 313 - 314.
Warden John A., Strategic Thinking and Planning, Venturist Publishing, Montgomery Alabama, 2000, s. 42.

[50] Deptula David A., Effects Based Operations: Change in the Nature of Warfare, Aerospace Education Foundation, Defence and Airpower Series, Virginia 2001, s. 17 - 20.

vastustaja kokoaa itsensä toimintaympäristön muutoksen edellyttämällä tavalla, vaihdetaan painopistettä ja isketään muihin vastustajalle yhtä tärkeisiin kohteisiin, jolloin vastustajan tilannetietoisuus heikentyy ja pirstoutuu, ennen kuin hän tietää, mistä isku tuli. Kineettiset ja ei-kineettiset operaatiot perustuvat informaatioteknologian laaja-alaiseen hyödyntämiseen.[51]

Kyberoperaatioissa korostuu vaatimus toiminnan nopeudesta ja laajuudesta. Puolustajan järjestelmät ovat alttiita kyberhyökkäyksille asevoimien koko taistelutilan laajuudessa. Kybersodankäynnissä ei ole rintamalinjoja vaan sodankäynti tapahtuu kaikkialla kybertilassa. Kyberhyökkäykset ja hyökkäysvektoreiden muutokset ovat hyvin nopeita. Sodankäynnissä on siirrytty päivä- ja tuntiluokasta minuutteihin ja sekunteihin.

Kyberhyökkäysten kohteena eivät ole vain asevoimat vaan yhteiskunnan elintärkeät toiminnat. Yhteiskunnan elintärkeät toiminnot on pystyttävä turvaamaan kaikissa tilanteissa. Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja siksi kybertoimintaympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella.[52] Näin kansallisesta kyberpuolustuksesta muodostuu kiinteä osa kokonaismaanpuolustusta.

Kybersodankäynnissä korostuu Boydin ajattelu, jossa meidän tulee toimia ja reagoida nopeammin kuin vastustaja kehittämänsä OODA-Loopin (Observe- Orient-Decide-Act) mukaisesti. OODA-Loop soveltuu erinomaisesti kybersodankäynnin mallintamiseen ja kyberoperaatioiden johtamiseen. Kybertilannetta tulee havainnoida ja evaluoida useista eri näkökulmista päättää tarkoituksenmukaisista vastatoimenpiteistä ja toteuttaa näitä toimenpiteitä vastustajaa nopeammassa syklissä. Asevoima, joka kykenee adaptoitumaan ja reagoimaan nopeimmin jatkuvasti muuttuvissa kybertaistelukentän ympäristöissä, on voittaja.

Boydilaiseen ajatteluun liittyy myös tarve ketteryyteen taktisella, operatiivisella ja strategisella tasolla. Vastustajaa nopeamman päätöksenteon lisäksi tarvitaan häntä nopeampaa liikettä ts. kykyä operoida vastustajaa nopeammin kybertoimintaympäristössä. Aikatekijöiden ollessa minuutti- ja sekuntiluokkaa tarvitaan lisääntyvää tehokkuutta ja autonomusta päätöksenteko ja toimintaprosesseissa.

Boyd korostaa oman tilannetietoisuuden merkitystä ja kykyä estää vastustajaa luomasta tilannetietoisuuttaan. Kybersodankäynnissä korostuu periaate, jossa ihannetapauksessa vihollinen ei koskaan havaitse omaa toimintaamme ja se yllätetään täysin. Lisäksi tarvitaan tehokasta harhautusta. Oikein toteutetut harhautukset ja demonstraatiot ovat perusasioita, kun halutaan kiistää vastustajan kyky tarkkaan havainnointiin. Tehokas kybertiedustelu mahdollistaa pääsemisen vihollisen OODA-Loop:in sisälle, mikä lisää operaatioiden tehokkuutta ja vaikuttavuutta.

[51] Shanahan John N.T., Shock-Based Operations, New Wine in an Old Jar, Air & Space Power Journal - Chronicles Online Journal, 15 October 2001, s. 6 - 7.
[52] Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013.

Wardenin teorian mukaisesti kybervaikuttaminen tulee kohdistaa vastustajan elintärkeisiin kohteisiin. Kybervaikuttamista voidaan kohdistaa Five Ring-mallin mukaisesti kaikille eri tasoille, joista johtaminen muodostaa tärkeimmän kohteen. Kaiken toiminnan ”tulisi kohdistua vastustajan johdon mieleen tai vastustajan järjestelmään kokonaisuutena”. Toteuttamalla kyberhyökkäyksiä jokaista kehää vastaan vastustajan asevoima voidaan eristää johdosta ja tehdä merkityksettömäksi.

Tulevaisuuden kybersuorituskyvyn kehittämisessä korostuu systeeminen ajattelu. Kybermaalien valinnassa niitä tulee tarkastella systeemin osina, jolloin aikaan saadaan suoraa ja epäsuoraa vaikutusta. Maalien valinnassa on järkevää valita sellaisia, jotka nopeimmin, pitkävaikutteisimmin ja tehokkaimmin aikaansaavat systeemimuutoksen. Muutos saadaan tehokkaimmin toteutettua, kun toteutetaan kineettisiä ja ei-kineettisiä rinnakkaisoperaatioita kaikissa taistelutilan ulottuvuuksissa. Jokaista ulottuvuutta vastaan voidaan hyökätä suorasti tai epäsuorasti, ja paras toimintamalli riippuu kulloisestakin tilanteesta. Strategisessa ajattelussa tulee huomio kohdistaa systeemivaikutuksiin eikä yksittäisiin maaleihin.

Wardenin mukaan: ”Jos haluamme ajatella strategisesti, meidän täytyy käsitellä vastustajaa alajärjestelmistä koostuvana järjestelmänä. Kun miellämme vastustajan järjestelmäksi, meillä on paremmat mahdollisuudet pakottaa tai houkutella hänet tilanteeseen, jossa omista tavoitteistamme tulee hänen tavoitteitaan, ja voimme tehdä tämän mahdollisimman vähällä vaivalla ja onnistumisen mahdollisuutemme ovat parhaimmat.”[53] Edelleen Warden toteaa, että ”sodan strateginen päämäärä on pakottaa vihollisvaltio tai vihollisjärjestelmä toimimaan halutulla tavalla. Äärimmäisessä tapauksessa tavoitteen saavuttamiseksi saattaa olla tarpeen tuhota vihollisvaltio tai sen järjestelmä. Kohteenamme on kuitenkin koko järjestelmä, eivät vastustajan sotilaalliset voimavarat.” [54]

Näkemys vihollisesta systeeminä ja vihollisen johtamisjärjestelmästä tuon systeemin tärkeimpänä toimintajärjestelmänä, kohdistaa kaiken kineettisen ja ei-kineettisenvaikutuksen strategiseen lamauttamiseen ja systeemiseen vaikutukseen.

2000-luvun asymmetrinen sodankäynti on luonut uuden asetelman, jossa raja perinteisen ja epätavanomaisen sodankäynnin välille on hämärtynyt. Tälle uudelle usein jäätyneisiin konflikteihin liittyvälle konseptille on annettu nimeksi hybridisodankäynti. Käsite on hankala, koska hybridisodankäynnissä toimitaan sodan ala- ja ulkopuolella. Sodankäynti sodan ulkopuolella on vaikeasti määriteltävissä, koska kansainvälinen oikeus ei määrittele tämän tyyppistä tilannetta. Toiminta perinteisin sodankäyntikäsittein sodan ja osittain fyysisen maailman ulkopuolella virtuaalisessa kybermaailmassa on haasteellista.

Hybridisodankäynnin määrittelyn ja aseman haasteista huolimatta yhä laajemmin on esimerkkejä, jossa kineettistä sodankäyntiä on jatkettu matalan intensiteetin kineettisten ja ei-kineettisten operaatioiden avulla. Venäjän sotatoimet Ukrainassa vuonna 2014 ovat esimerkki sodankäynnistä, jossa erikoisjoukkojen rajoitetun voimankäytön, poliittisen, sotilaallisen ja taloudellisen painostuksen, strategisen kommunikaation

[53] Warden John A., The Enemy as a System, Airpower Journal, Spring 1995, s. 42.
[54] Ibid, s. 47

sekä erilaisten ei-kineettisten operaatioiden avulla on luotu epävakaa Itä-Ukraina alue, jota Venäjä hallitsee.

Afganistanissa ja Irakissa aktiivisten sotatoimien päättyminen ei päättänyt sotaa. Tilanne on jatkunut epävakaana, jossa edellä kuvatut kineettiset ja ei-kineettiset operaatiot ovat arkipäivää. Perinteisin sodankäynnin keinoin ei ole saavutettu rauhaa vaan siirrytty sodankäynnin toiselle tasolle, jossa siis hybridi-periaatteella yhdistetään pehmeitä ja kovia sotilaallisia operaatioita. Hybridisodankäynnin ilmentymistä ovat edistäneet hyökkäyksellisten kybersuorituskykyjen kehittyminen ja miehittämättömyyden lisääntyminen. Tätä kehityssuuntaa on edistänyt ajatus yhä tarkemmista täsmäoperaatioista, joissa voidaan optimoida vaikutus kohteessa, minimoida omat tappiot sekä vaikutukset siviileihin ja siviilikohteisiin.

Kybertaistelutila ja miehittämättömyys ovat alentaneet sodankäynnin kynnystä muuttaneen perinteistä sota-rauha-asetelmaa. Tähän asetelmaan liitettiin kylmän sodan aikana käsite harmaasta vaiheesta, jolla ymmärrettiin aikaa ennen varsinaista sotaa. Hybridisodankäynti on tuonut tilan, joka voi edeltää perinteistä sotaa, ilmetä sodan aktiivisen vaiheen jälkeen tai ilman perinteistä sodankäyntiä. Uusi sodankäynnin paradigma on syrjäyttämässä perinteisen mallin sodan julistamisesta rauhan sopimukseen luomalla tilan, jossa sotaa ei julisteta eikä rauhaa solmita, vaan hybridisodankäynnin kohde joutuu elämään hyvinkin pitkään konfliktin ja epävakauden keskellä, jossa yhä enenevässä määrin kybertoimintaympäristö on toiminnan kohteena.

2020-luvun kehitykselle on leimallista perinteisen ja epätavanomaisen sodankäynnin rajan hämärtyminen. Sodankäyntiin sekoittuu uusia elementtejä erityisesti kybertoimintaympäristössä tavoitteena pysyttäytyä sodan kynnyksen alapuolella. Tarkoituksellisen epävakauden ylläpito ei-kineettisten operaatioiden avulla erityisesti suurvalta voi perustella läsnäoloa ja vaikuttamista tietyllä alueella. Toimintaa perustellaan rauhanturvaamisella, tasapainon säilyttämisellä, omien etujen ja kansalaisten suojaamisella tai liittolaisten tukemisella, kaikella näennäisesti hyväksyttävällä toiminnalla. Kybertoimintaympäristö on luonut uuden tilan vaikuttaa toisen valtion alueella käyttäen hyväksi erilaisia sotilaallisia ja ei-sotilaallisia painostuskeinoja poliittisten ja sotilaallisten tavoitteiden saavuttamiseksi.

5.

Miten tekisin kyberhyökkäyksen?

Mika Hyytiäinen
Sotilasprofessori, suomalainen sotataito
Maanpuolustuskorkeakoulu

Tiivistelmä
Artikkelissa visioidaan kolme erilaista ja nykykäsittelyssä marginaalissa olevaa valtiollista hyökkäystä, joita voitaisiin käyttää Suomen kokonaisturvallisuutta vastaan kybermaailmassa vuoden 2020 aikaikkunassa. Yksi hyökkäyksistä on epäsymmetrinen kyberin suhteen. Lisäksi esitetään joukko havaintoja kyberperästä ja siellä käytävistä taisteluista keskittyen ”normaalista” sodankäynnistä poikkeaviin piirteisiin ja sitoen kybertaistelua osaksi laajempia operaatioita.

Artikkeli täydentää Mikko Hyppösen vuosikymmen sitten visioimia taisteluskenaarioita. Painotus on nyt valtioiden toimissa. Lukeminen ei edellytä teknistä tai syvällisempää kyber-tietämystä.

Artikkelin lopussa on joukko kirjoitustyön aikana syntyneitä ajatuksia ja johtopäätökset. Kaikki pohdinta on kirjoittajan omaa eikä edusta puolustusvoimien tai Maanpuolustuskorkeakoulun virallista kantaa.

5.1 Tausta ja tarkoitus

Artikkeli on jatkumoa Mikko Hyppösen vuonna 2003 kirjoittamaan tekstiin, jota kannattaa lukea rinnalla. Aloitan Mikon itsensä tekemällä analyysilla. Vastasin vuonna 2003 koko tutkimushankkeesta, jonka osa alkuperäinen kirja oli: asetin raamit ja osallistuin skenariointiin, joten vahdinvaihto on helppo. Olen itse lähestynyt kyberiä aiheena kun paikkatietotekniikkaopintojeni jälkeen siirryin pääesikuntaan johtamisjärjestelmäosastoon ja sitten tutkimuslaitokseen, jossa tätäkin asiaa tutkittiin.

Edellisen kirjan kokoaja, tuolloinen viestitaktiikan opettaja Mika Piiroinen kirjoitti diskussiossa näin: *”Pelottavaa on se, että asiat, jotka me kuvittelemme tapahtuvan tulevaisuudessa, kyetäänkin toteuttamaan jo tänään. Mitä sitten kyetään toteuttamaan tulevaisuudessa?”*. Yritän vastata osaltani tähän haasteeseen. Koska tehtävänä on innovoida, eikä taktiikan näkökulmasta kirjoitettua kybermateriaalia juuri ole, teksti nojaa ennen muuta päättelyyn. En siis ole tietoisesti referoinut kenenkään muun skenaarioita, vaikkakin viime vuodet ovat tartuttaneet mieleen ja muistiinpanoihin paljon muilta. Stuxnet-analyysi on toki ollut osaltaan pohjana.

Mikon ennakoimat hyökkäysskenaariot ovat jo ehtineet pienimuotoisempina tapahtua, joten päivitys on tarpeen. Käytän samaa kolmen erilaisen skenaarion rakennetta, mutta painotan niitä eri tavalla. Kymmenessä vuodessa verkkohyökkäys on muuttunut eksoottisesta ilmiöstä ensin arkipäiväksi, sitten laajaksi valtioidenkin painostusvälineeksi ja jo nyt täsmäytetyksi aseeksi. On kuitenkin hyvä muistaa, että sotimisesta harvoin poistuu mitään, joten edellisen kirjan skenaariot ovat sinällään edelleen voi-

massa muistuttaen, että sotimiseen käytetään aina erilaisia keinoja, myös kyberiä, toisiinsa lomittaen.

Maalina on Suomi Oy, eivät yksittäiset kansalaiset tai yritykset. Hakkereiden ja tavallisten tai epätavallistenkin rikollisten toimet olen jättänyt ne paremmin osaaville ja suuntaan siihen, minkä Mikko toteaa edellisen version suurimmaksi puutteeksi, valtiollisiin toimijoihin. Käsittely tapahtuu kokonaisturvallisuuden viitekehyksessä, mutten ota kantaa viranomaisten välisiin työnjakoihin. Katson kuitenkin, että jos vaikkapa sähkönjakelun tai sillan katkaiseminen on ”luvallista” ohjuksella, se on sitä myös kyberasein ja matalammalla käyttökynnyksellä. En pohdi lakia tai valtuuskysymyksiä, mutta toimin sodan oikeussääntöjen puitteissa.

Haluan ravistella nyt vallalla olevaa ajattelua, jossa kyber = internet, kyber = koodi, kyber = kivaa ja vapaata tai kyber = kaikki. Kybertaistelu on raakaa ja päämäärätietoista, yksi taistelutanner muiden joukossa. Kaikki aseeksi sopiva teknologia on tähänkin asti sellaiseksi muutettu, eikä kyber ole poikkeus. Monia aseita on myös käytetty rikoksiin. Kyberissä ehkä pelottavinta on aseiden hankinnan ja valmistamisen helppous yhdistettynä siihen, kuinka vähän asiaa valvotaan, kuinka pieniä ovat rangaistukset ja kuinka isoja voivat olla vaikutukset. Jos tähän ei saada muutosta, verkkotaisteluita tullaan käymään pidäkkeettömästi ja matalin kynnyksin.

Otan itselleni vastuuvapautuksen. Jos siviili visioi taktiikkaa, sen voi tehdä julkisesti. Kun sotilas tekee samaa, syntyy kysymys: näinkö puolustusvoimat todella tekee ja ajattelee. Vastaus on EI. Annoin Mikon tapaan ajatukseni lentää ja valitsin kärjistettyjä esimerkkejä, joilla olen itse yrittänyt omia ammattirutiinejani rikkoa. Ajatukset ovat omiani. Jos ne löytyvät muualtakin, olkoon se esimerkkinä niiden yleisyydestä, ei akateemisesta tai muusta varkaudesta.

Suurin pontimeni on sama kuin hyvän scifikirjailijan: dystopiaa ei kirjoiteta toivomukseksi vaan varoitukseksi, ettei kuvattu tapahtuisi.

5.2 Vuoden 2003 artikkelin itseanalyysi

Mikko Hyppönen arvioi ennakointiaan kesällä 2013 seuraavasti:

Vuonna 2002, kun kirjoitin ennustuksia vuoden 2020 verkkotaisteluista, annoin ajatuksen todella lentää. Mielestäni onnistuin ennustuksissani hyvin - ja huonosti.

Lienee nyt jo selvää, että vuonna 2020 markkinoilta ei tule löytymään ennustamiani 3D-muistipiirejä, joilla voisi tallentaa Hollywood-elokuvien koko historian. Tällaiselle ei ole tarvetta internetin videopalveluiden läpilyönnin ansiosta.

Sen sijaan onnistuin ennustamaan Anonymous-liikkeen nousun aika tarkalleen oikein. Kuten ennustin, verkossa todella nykyään toimii autonomisesti toimivia aktivistiryhmiä, jotka käyttävät verkkohyökkäyksiä protestoinnin välineenä. Tärkeimpänä työvälineenä heillä ovat palvelunestohyökkäykset ja tietomurrot ja kohteena mm. pankkimaailma. Vuonna 2002 ei vielä ollut olemassa juuri minkäänlaista vuotokulttuuria ("leaking"), joten senkin ennustamista voi pitää hyvin onnistuneena. Viittasin myös haktivistiliikeen "karismaattiseen johtajaan", ja tekisi mieli todeta että ennustin Julian Assangen tai kenties Edward Snowdenin nousun.

Suurin virheeni tulevaisuuden verkkotaisteluiden ennustamisessa kuitenkin oli se, etten ennustanut valtiollisten toimijoiden nousemista. Vuonna 2002 olisi tuntunut täydeltä utopialta ajatella, että sivistyneet valtiot oikeasti kehittäisivät valtiollisia haittaohjelmia ja oikeasti hyökkäisivät niillä muita valtiota vastaan – jopa ydinjärjestelmiä vastaan. Näin kuitenkin kävi.

Tänä päivänä valtiot käyttävät haittaohjelmia monella eri tavalla. Poliisit käyttävät takaportteja ja troijalaisia osana rikostutkintaa. Tiedusteluorganisaatiot tekevät vakoilua esim. APT-hyökkäyksillä, ja tiedämme, että monien maiden armeijat valmistautuvat oikeaan verkkosotaan rakentamalla hyökkäyskykyä. Nyt, vuonna 2013, verkkosotaa emme ole vielä nähneet. Lähinnä sitä lienee tapaus Stuxnet, mutta sekin pitänee laskea vasta verkkosabotaasiksi eikä varsinaiseksi sodankäynniksi. Lienee kuitenkin selvää että seuraava sota, joka soditaan teknisesti kehittyneiden valtioiden välillä, tulee varmasti sisältämään verkkosodan tai kybersodan elementtejä.

Olen nyt Mikkoon nähden siinä suhteessa edullisessa tilanteessa, että 2020 on varsinkin sotilaallisesti jo kulman takana, aseita rakennetaan ja kyber otetaan vakavasti. Kun lisäksi suuntaan skenaariot kovempiin kohteisiin, niihin osin pätee sama kuin aseisiin yleisemminkin: teknologia ei ole aivan viimeisintä uutta, kun ei ole maalikaan: valtiomaalit ovat kerrostumia eri ikäisistä tekniikoista. 2020 parhaassa iskukunnossaan olevat Hornet-hävittäjämme ovat esimerkiksi paljolti 1970-luvun tekniikkaa, joka on lähes immuunia 2020-luvun uusimmille internetasekeksinnöille.

Muutama havainto[1] Stuxnetistä perustaksi. Hyökkäyksen ammattitaito, koodin vaatiman analyysin monimutkaisuus ja hyökkäyksen tavoite osoittavat, että kyse oli tämän artikkelin kuvaamasta hyökkääjästä. Hyökkäys kohdennettiin suljettuun teollisuusautomaatioympäristöön välineellä, jota virussuojausohjelmistot eivät voineet tuntea. Maali oli monimutkainen, samoin kaksi hyökkäysvektoria, ja tavoite oli jopa salata koko hyökkäys. Jos vastaava hyökkäys olisi kohdennettu helpompiin, internetiin avoimiin yhteiskunnalle kriittisiin järjestelmiin, sitä ei olisi haluttu salata ja vahingot olisi maksimoitu, tuho olisi ollut merkittävää. Samalla kun hyökkääjien kyvyt kasvavat, hyökkäyksille kriittisiä järjestelmiä kytketään yhä enemmän verkkoon liiketaloudellisista, tehokkuus- ja mukavuussyistä. Toisaalta osa maista on jo nyt ilmoittanut, että vakavaan kyberhyökkäykseen vastataan kaikilla sotilaallisilla keinoilla. Kybersotiminen on siis jo käynnissä, samoin kyberkilpavarustelu.

5.3 Taustaoletukset vuoden 2020 tilanteesta

Ihmisellä on taipumus ylikorostaa lähiajan muutosvauhtia ja aliarvioida pidempää aikaa, joten ihan tarkkana määreenä en vuotta 2020 pidä.

Käytän seuraavia perusolettamia Suomen tilanteesta:

- Suomi on kehittynyt kyberriippuvainen tietoyhteiskunta, jonka toimintoja vastaan on hyökätty aktiivisesti jo kahden vuosikymmenen ajan. Vaikka haavoittuvuuksia on, resilienssi normaaliajan tapahtumille on kehittynyt korkeaksi. Suomessa on paljon maaleja, mutta Suomi on vaikea maali.

[1] Kuvaus on tiivistetty tutkimusraportista Ralph Langner: How to kill a Centrifuge, November 2013, www.langner.com]

- Uhka tämän artikkelin näkökulmasta on valtiollinen vahva toimija tai mahdollisesti erittäin vahva ja pitkäjänteiseen itsenäiseen kehittämistyöhön kykenevä verkottunut yhteisö.
- Suomi on edelleen sotilasliittojen ja niiden suoman tuen ulkopuolella.

Teknologisesti käytän seuraavia olettamia[2]:

- Tietoverkot, järjestelmät, läsnä-äly ja piirit ovat teollista perua pääosaltaan muualta kuin Suomesta. Niitä operoivat moninaiset yritykset. Kaikki toiminnat ovat kilpailun ja tarjonnan takia monin osin päällekkäisiä.
- Esineiden internet on käytössä, liittymien määrä on satakertaistunut nykyisestä. Yhä useampi laite on ”aina verkossa”.
- Yksikään teknologia ei omaa enemmistöä sen paremmin käyttöjärjestelmissä kuin verkoissa. Poikkeuksia tähän löytyy hyvin kapeilta sektoreilta.
- Riippuvuus tietoverkoista ja tietoa tuottavista sekä käsittelevistä laitteista on sellainen, ettei niille löydy manuaalista korvaajaa kuin siirtymällä takaisin 1960-luvulle. Tämä koskee myös viranomaisia, joiltakin osin myös puolustusvoimia.
- Laajennettujen turvallisuusviranomaisten TUVE-ympäristö eristettynä ratkaisuna on käytössä suojaten ”irtikytkennällä” internetistä yhteiskunnan turvallisuuden tärkeimpiä toimintoja. Myös valtionhallinnon muu verkko on osin erotettu. Internetin haavoittuvuus on osin johtanut klusteroitumiseen muuallakin, mutta internetin koko rakenne ei ole hajautunut.

5.4 Ensimmäinen skenaario: Täsmähyökkäys suljettuun ympäristöön (TY-F / TO-T / K-F4, TY-F / TO-I / K-T-C-VT)[3]

Isku Iranin ydinmateriaalin jalostusta vastaan[4] tapahtui suljettua valtiolle keskeistä korkean turvallisuuden kohdetta vastaan. Merkittävää oli, että kohteena oli teollisuusautomaatio ja sen ohjausjärjestelmä, SCADA, jonka rooli ja verkottuminen esineiden internetin myötä myös suljetuissa ympäristöissä kasvavat koko ajan.

Vastaavia ympäristöjä on yhteiskunnalle kriittisessä infrastruktuurissa jo nyt laajasti alkaen sähkönjakelusta ja energiantuotannosta päättyen elintarvikejalostukseen ja sairaala-automaatioon laboratorioineen[5]. Kohteena voi olla mikä tahansa tällainen

[2] Alkuperäisessä teoksessa Mikko Hyppönen on esittänyt suurehkon määrän yhteiskunnan oletettuja konkreettisia ominaisuuksia, joista pääosa on edelleen relevanttia. Itse listasin sellaisia asioita, jotka vaikuttavat enemmän taktisella tasolla yleisemmin.

[3] Ks. luku 2 teoreettiset määritelmät.

[4] STUXNET hyökkäys on ehkäpä eniten popularisoitu tapaus tällä hetkellä. Tarkoitus tässä tekstissä ei ole viitata vain siihen, koska vastaavia tapahtuu ennen tarkasteluvuotta varmasti useita maalien, tunkeutumiskeinojen ja vaikutusten vaihdellessa – epäilemättä merkittävä osa ellei pääosa näistä jää julkisen tiedon ulkopuolelle. Hyökkäys on kuitenkin siinä mielessä merkittävä, että se ainakin julkisuudessa aloitti uuden aikakauden kybersodankäynnissä sekä myös siksi, että hyökkäys oli vaihtoehto fyysiselle vaikuttamiselle sisältäen myös kustannusvertailua.

[5] Tällaisen mikropiireillä ohjatun ja erilliseksi luullun välineistön määrä on jo nyt jokaisella kriittisen infrastruktuurin alalla hyvin merkittävä, eikä asiaa sen uutuuden vuoksi ainakaan asiakas hallitse. Kokonaisuus muodostuu suuresta joukosta eri-ikäisiä ja varsin suljettuja niin asiakkaalle kuin muille toimittajille näyttäytyviä ”mustia laatikoita”, joita kuitenkin kasvavissa määrin verkotetaan yhteen ja ylläpidetään etäyhteyksin suljetuiksi luulluissa verkkorakenteissa. Energia jakeluineen, logistiikka ja teolli-

ympäristö riippuen siitä, mikä hyökkääjän kokonaistavoite on. Kosovon ja Irakin sodissa länsi täsmäiski energianjakeluun ja tieverkostoon, joten kyberissäkään kynnystä tuskin on. Myös sotilasorganisaatiot käyttävät ytimissään aivan tavallisia ohjelmistoja toiminnanohjauksesta välikerroksiin ja tietokantoihin, jolloin niihin suunnatut hyökkäykset saattavat helposti karata myös siviililaitoksiin.

Tyypillistä on, että kyberase tuodaan tällaiseen ympäristöön ihmistä hyväksi käyttäen. Teko voi olla ajattelematon, vahinko tai tahallinen. Kuten alkuperäisen teoksen puolustusluvussa todetaan, tällaiselta ei voi suojautua koskaan täysin.

Uusi tapa on tuoda ase käyttäen kokonaisuuden omia piirteitä hyväksi. Tällaisesta nykyesimerkki on RFID kun fyysinen tavara varustetaan radiotaajuisesti luettavalla sirulla. Siru laajimmillaan paitsi tietää lähettäjänsä, määränpäänsä ja käsittelijänsä, myös seuraa itse kulkuaan. Mitä tehokkaammaksi logistiikka kehitetään, sitä enemmän älyä on rakennettava myös sen kuljettamiin tavaroihin. Tällainen etäluettava siru voidaan esimerkiksi laittaa paketin sisään ja aktivoida aikautettuna tai aktivoijan ohi mennessään, tai se voidaan viedä sisään fyysisesti tunkeutumalla ja vaihtamalla joku laillinen siru. Ihmistenkin tunnistaminen ja käyttövaltuushallinta on haaste, ja esineiden internetissä tämä haaste moninkertaistuu.

On siis syytä olettaa, että haluttuun suljettuunkin ympäristöön päästään sisään.

Merkittävin hyökkääjän resursseja kuluttava tekijä on, että suljettu ympäristö ja sen tekniikat pitää tuntea erittäin hyvin. Koska Suomi on pieni, ostamme lähes kaiken muualta ja lähes kaikki loputkin voi ostaa täältä ennalta, joten tekniikassa salaisuuksia on vähän. Yksi tapa on yrittää salata käytetyt tekniikat, mutta se on Suomessa muutamia erikseen päätettyjä poikkeuksia lukuun ottamatta laitonta julkisissa hankinnoissa. Vaikka tiettyjen materiaalien, kuten aseiden, viennissä on rajoituksensa, on sinisilmäistä luottaa siihen, ettei vastustajamme niitä saisi yksittäisinä hankituksi. Samoja välineitä käyttävät muutkin, ehkä vastustajamme isommat vastustajat, joten paras suojamme saattaakin olla haluttomuus paljastaa löydetyt heikkoudet Suomen kaltaisen vähäarvoisen maalin takia.

Alkuperäisessä skenaariossa kohteena oli yritys. Yleisimmin tällaisia hyökkäyksiä on meillä väläytelty energianjakelua, teleoperointia tai logistiikanhallintaa vastaan. Kohdennan tämän skenaarion vähemmän tunnettuun Suomen suljetun sotilasympäristön teollisuusautomaatioon käyttäen yhtä esimerkkiä hyväksi.

Sotilaslaitteissa on kasvava määrä teollisuusautomaatiota. Uusin panssarintorjuntaaseemme on tästä hyvä esimerkki[6]. Sen edeltäjä oli täysin tyhmä rekyylitön raketti, jolloin kaikki osumiseen liittyvä päättely etäisyydestä ja maalin liikenopeudesta lähtien, ja nämä kompensoiva tähtäyspisteen valinta, oli käyttäjän vastuulla. Raketti vaikutti osuttuaan ehkä kohtaan, johon ampuja halusi, tai johonkin muuhun todennäköisesti vaikeammin läpäistävään kohtaan. Uudessa aseessa käyttäjä vain seuraa maa-

---

suustuotanto ovat jo olleet fyysisen sodankäynnin kohteena useammassa sodassa, joten niiden voidaan olettaa olevan sitä myös vähemmän väkivaltaisessa kybersodankäynnissä.

[6] Uskallan käyttää tätä, koska käytän vain aseeseen liittyviä jo julkaistuja ominaisuuksia esimerkkinä. Vastaavia laitteita modernilla asevoimilla on kymmeniä erilaisia alkaen yksittäisistä ohjelmoitavista kranaateista.

lia, kunnes laite on päätellyt oikean lentoradan. Lisäksi raketti lentää maalin yli, tunnistaa sen ja räjähtää oikealla hetkellä maalin heikon kohdan yllä.

Uusi ase ei toki ole kiinni esineiden internetissä edes suojatussa ja suljetussa verkossa, enkä oleta näin laajasti olevan vielä 2020 aikaikkunassa uudempienkaan järjestelmien osalta. Ase kuitenkin kiinnitetään aika ajoin järjestelmään, joka paitsi tarkistaa huollollisen kunnon myös päivittää aseen älyä. Tämä järjestelmä taas kytketään ainakin jollakin tavalla valmistajan lähdejärjestelmään, josta päivitys saadaan. Sekä valmistajan järjestelmä että huoltojärjestelmä ovat jo nyt tyypillisesti tavallisia työasemia, joissa asetekniikka on lähinnä erikseen koodattu sovellus.

Näin avautuu ainakin kolme hyökkäysväylää. Itse aseen ”älyn” voi yrittää rikkoa vaikkapa HPM-pulssilla tai joissakin tapauksissa kytkeytymällä siihen mock up-tyyppisella laitteella. Oikea taajuus ja teho voidaan valita sekä tunkeutumiskokeilu tehdä, mikäli saadaan haltuun vastaava ase. Toisena huoltolaite voidaan saastuttaa asentamalla siihen koodia tai jopa väärentämällä vain parametreja, yksinkertaisimmillaan ostamalla joku huoltohenkilö tämä tekemään. Kolmanneksi voi olla mahdollista ostaa valmistajan rikolliselta työntekijältä koodi, jota käytetään. Vaikka temppu ei ole helppo, se ei ole mahdoton, ja integroituvassa välineistössä se on myös varsin kustannustehokas.

Esimerkkitapauksessa pienin harmi syntyy siitä, ettei osa aseista toimi kun niiden äly on rikottu. Merkittävä harmi syntyy siitä, että osa aseista käyttäytyy väärin ja räjähtää esimerkiksi aina maalin takana paljastaen käyttäjän. Suurin harmi syntyy siitä, jos ase muuttuu myös vaaralliseksi käyttäjälle. Viimeinen on ehkä mahdotonta siksi, että aseissa edelleen tällainen estetään enemmänkin mekaanisesti kuin ohjelmistollisesti. Lyhyen aikaa voi myös riittää, että hyökkääjä kykenee uskottavasti osoittamaan tekonsa vaikutukset käyttäjille ja aikaansaamaan näin epävarmuutta ja epäluottamusta omaan sotavarustukseen.

Mikäli hyökkäys johtaa siihen, että kyseinen asejärjestelmä on epäluotettavuutensa takia kokonaan poissa käytöstä, haitta on todella merkittävä. Panssarintorjunta on kokonaisuus, jossa jokainen pala nojaa toiseensa. Jos joku pala puuttuu, kokonaisuuteen jää paha aukko ja vahinko on paljon suurempi kuin esimerkiksi tärkeänkin materiaalivaraston täydellinen fyysinen tuhoaminen. Juuri tietynlaisen materiaalin tuhoaminen nopeasti monista kymmenistä fyysisistä varastoista täysin olisi kineettisellä vaikuttamisella mahdotonta. Kyber siis kykenee oikein kohdennettuna yllättävään järjestelmävaikutukseen, se on täsmäytettävissä. Pahimmillaan vaikutus ulottuu koko taktiikkaan.

Hyökkäys eskaloituu myös muihin asetta käyttäviin maihin epävarmuutena. Se vaikuttaa paljon myös kyseisen aseen valmistajaan. Koska oma kykymme poistaa ongelma perustuu lähinnä oikean päivityksen ajamiseen kaikkiin aseyksilöihin, syntyy vähintään aikavoitto. Lisäksi herää epäilys siitä, mitä muuta on manipuloitu, ja hyökkääjä voi varsin uskottavasti uhata näin muitakin suorituskykyjä.

Sotilasympäristö on 2020 edellä kuvatuissa rakenteissa edelleen varsin hajautettu. On myös huomattava, että tällöinkin on edelleen käytössä jopa 1970-luvulla tehtyjä ohjelmistoja, joten tuijottaminen vain uusimpaan ei anna kuin pienen kuvan asiasta.

Heterogeenisuus suojaa kokonaisuutta, mutta toisaalta se tekee puolustuksesta haastavaa ja jopa uskottavalla propagandalla voi saada tuloksia aikaan.

Kuvatunlainen hyökkäys voi olla osa painostusta tai sotilaallista ensi-iskua. Se voi olla myös osa pitkittynyttä kriisiä, jossa vastustaja osoittaa kohteeksi valitun toimijan kyvyttömyyden suojata oma ”älynsä” ja vaaran aiheuttamisen omalle henkilöstölleen. Materiaaliin kohdennettuna hyökkäys saa enemmän aitojen tekojen luonteen kuin ihmisiin propagandana suunnattuna, jolloin tulos on monin osin vakuuttavampi ja vaikeampi kiistää.

5.5 Toinen skenaario: kyberympäristön lamauttaminen kyberkeinovalikoimaa käyttämättä

(TY-F / TO-I / K-F4 + TY-F / TO-I / K-I-C-VT, TY-F / TO-T / K-(T+I)-S)

Alkuperäisessä skenaariossa fyysinen vaikuttaminen on merkittävä osa toimia, joilla verkkohyökkäystä tuetaan tai joita toteutetaan verkkohyökkäyksen rinnalla. Koska kyber-alan ihmiset yllättävän usein unohtavat, että vuorovaikutus toimii myös fyysisestä maailmasta kybermaailmaan, tämä skenaario on pelkistetty käyttämään vain fyysistä ja henkistä hyökkäysväylää.

Pilvipalvelu viittaa siihen, että tieto sijaitsisi jossakin ei-fyysisessä ympäristössä. Mobiilikäyttö taas saa aikaan illuusion siitä, että tieto kulkisi jotenkin aineettomasti. Molemmat ovat vääriä käsityksiä. Tieto on fyysisissä muisteissa ja ”kybersäteilyn” estäminen on sotilaallisin elektronisen sodankäynnin keinoin varsin helppoa.

Maamme kriittiset tietovarastot sijaitsevat fyysisesti Suomessa. Tietovarastot ovat eritasoisesti fyysisesti suojattu sekä tiedot kohtuullisin määrin monennettu ja suojattu varmuuskopioin. Harva tietovarasto on kuitenkaan suojattu kovalta sotilaalliselta iskulta. On myös ymmärrettävä, että tietovarastojen laitekanta ja ohjelmistot ovat spesifejä, eikä niiden korvaaminen suurissa määrin nopeasti ole mahdollista. Näin iskun ei tarvitse kohdistua täsmälleen tiettyyn tietoon, vaan isku voidaan kohdistaa tiettyyn ympäristöön ja aiheuttaa kapasiteetille vakava häiriötila.

Oletan, että 2020 tällaisia suojattuja tietovarastotiloja on jotakuinkin saman verran kuin nykyisin, ja että niiden sijainteja on tiedusteltu 5-20 vuoden ajan, osin kauemminkin. Hyökkäys voi kohdentua itse laitteisiin, välittömiin tietoliikenneyhteyksiin, kulkuväyliin tai energianjakeluun. Valitsemalla kohde oikein voidaan vaikuttaa koko fyysiseen tietovarastoon eli usein useampaan toimijaan, ja jossakin määrin samalla varmuuskopioihin ja jopa monennettuihin palveluihin. Väline voi olla fyysisen tuhoamisen lisäksi myös elektroniikkaan kohdistettu HPM-pommi[7].

[7] HPM eli korkean energian mikroaaltoase, on ollut peikkona ainakin kaksi vuosikymmentä. Nyt välineet ovat arkipäiväistymässä muun muassa tienvarsipommien laukaisun estämisessä, ja kertakäyttösähkövirtalähteiden kehitys on pitkällä. Jo alkuperäisessä raportissa esitetty kohtuullisen pienikokoinen ja varsinkin perinteisiin tietokoneisiin verrattuna riittävän tehokas väline on kohtuullisin kustannuksin tehtävissä. Laitteen jäljet elektroniikassa muistuttavat vakavia käyttöhäiriöitä ja elektroniikkaoikosulkuja, eikä niitä ole helppoa todentaa. Lainsäädännöllisesti laite rinnastuu tahalliseen häirintään. Voi olla mahdollista, että tällaisen kohtuutehoisen laitteen voi valmistaa itse COTS-osista 2020-luvulla.

Kaikki tietoliikenne kulkee valokaapeleissa runkoverkon osalta. Kaapeliverkko on sijainniltaan tiedusteltavissa, kaivinkoneyrittäjämme kertovat tämän tästä fyysisen vaikuttamisen tehokkuudesta. Osa haavoittuvista paikoista löytyy uutisista päättelemällä. Valokaapeliverkko on yleensä sellainen, että kohtuullisella määrällä tavallista louhintaräjähdysainetta maahan upottaen se on tuhottavissa korjaajan kannalta hyvin hankalalla tavalla. Räjähteiden maahan upottaminen on mahdollista tehdä nopeastikin käyttäen linnoittamistekniikoita, tai se voidaan tehdä jo ennalta.

Hyvin mietittynä on mahdollista fyysisesti yhteyksiltään eristää ja välittömiltä tietovarastoilta tuhota yhteen paikkaan keskitetty tietointensiivinen kohde kuten lennonjohto, rautatieohjauskeskus tai energianohjauskeskus. Mikäli tällaisille ei ole aitoja hajautettuja väistöpaikkoja, vaikutus voi olla varsin pitkäkestoinen. Vaikka kyberissä etäisyydet eivät merkitse, liika fyysinen keskittäminen saattaa nopeasti johtaa fyysiseen haavoittuvuuteen, jota vain tietojen varmistaminen kauaksikin ei suojaa. Paras tapa on pitää myös tilat ja käyttäjät riittävän hajautettuna, ja käyttää kyberin mahdollisuuksia keskittää hajautettu fyysinen toiminta hyväksi.

Ehkäpä haavoittuvin osa kyberympäristöä ovat sen tärkeimmät ylläpitäjät. Esimerkiksi kokoamalla ja analysoimalla seminaarien osallistujalistoja saa jo kohtuullisen hyvän maaliluettelon, joka sisältää paitsi julkiesiintyjät myös keskeiset kuulijat. Oletan, että 2020 kyseinen joukko on vain vähän suurempi kuin nykyisin.

Kun kohderyhmä maalitetaan hyvin ja isketään viisaasti suhteessa tavoitteisiin, voidaan hyökkäys kohdentaa vain johonkin kriittiseen infrastruktuuriin se jopa romahduttaen osaamiseltaan, tai vaikkapa OSI-mallin tai tietyn sovelluskokonaisuuden kautta poikittain laajasti koko tietoinfrastruktuuriin. Esimerkiksi SAP-toiminnan ohjausjärjestelmää käyttävät niin puolustusvoimat kuin koko valtionhallinto, useampi keskeinen kaupunki ja tärkein teollisuutemme. Jos äkkiä tällaisen kokonaisuuden keskeisimmät asiantuntijat puuttuvat, ja järjestelmää vastaan hyökätään myös muutoin, vaikutus voi olla hyvinkin pitkäkestoinen. Kun kaameimmat hyökkäyksen tulokset julkaistaan kiihkoislamistien tyyppisenä propagandana ja riittävän usealle asiantuntijalle todistetaan heidän olevan fyysisesti vaarassa, vaikutus voi pienessä maassa olla hyvinkin merkittävä. Kaikkea ei voi suojata, joten resilienssi on rakennettava muilla keinoin.

Taktinen järjestelmävaikutus saadaan aikaan, kun osataan iskeä hallinnonalojen välisiin rakenteisiin, jolloin sektoroitunut puolustus haastetaan tehokkaasti. Rakenne, jossa yksi on sopinut fyysiset asiat, toinen palvelut, kolmas on käyttäjä ja neljäs toisiokäyttäjä, antaa mahdollisuuden aiheuttaa merkittävä hallinnollinen sekaannus kriittisessä vaiheessa hyökkäystä. Paras vaikutus syntyy, mikäli eri hallinnonalat saadaan riitelemään keskenään vastuista ja toimenpiteistä harvoissa asiantuntijayrityksissä, mikäli priorisointeja ei ole yhdessä kyetty tekemään ja jokaisen alan vaatiessa itselleen luvattua palvelutasoa jopa viranomaisvelvoittein. Jos palvelun varsinaisista tuottajista ei ole kokonaiskuvaa, yksi isku saattaa kohdentua ennakoimattomalla tavalla useampaan hallinnonalaan.

Mitä monimutkaisempi ja sektoroituneempi hallinto on, sitä haavoittuvampi se on niin fyysisille kuin verkon kyberiskuille. Toisaalta vääränlainen keskittäminen, jossa palvelun omistajan käsitys palvelusta ja sen tuotantotavasta irtautuvat toisistaan, altistaa myös hallintorajapintoihin kohdennettaville iskuille.

Tietotekniseen kyberympäristöön kohdentuu jatkuvasti hyökkäyksiä ja yksittäisiä aloja on jo ollut ”pois pelistä” pitkiäkin aikoja laite-, yhteys- ja sovellusvirheiden takia. Koska kokonaisvaikutusta ei ole syntynyt, on syytä olettaa, että nykyisen kokonaisuuden keskeinen suojamekanismi on sen hajautuneisuus. Reikiä on helpompi löytää, mutta toisaalta ne eivät johda kovin laajalle. Nykyjärjestelmä ei siis ole riittävän kompleksi siinä merkityksessä, että siihen olisi syntynyt emergenttejä haavoittuvuuksia. Toisaalta fyysisiä vaikutuksia kyberympäristöämme kohtaan ei ole kertaakaan massoitettu, joten tämä asia on tavallaan testaamatta.

Kun katsoo sekä julkishallinnon että keskeisten palveluntuottajien suunnitelmia, vuonna 2020 kyberympäristömme on nykyistä paljon keskitetympi. Jos suojausta kehitetään hyvin, tilanne paranee, vaikkakin integraation kasvaessa myös vahinkojen suuruus kasvaa. Emergenttien haavoittuvuuksien syntymisen todennäköisyys on kasvussa. Haastavinta saattaa kuitenkin olla muutostilanne, jossa hajautuneet asiakkaat eivät enää päivitä nykypalvelujaan uutta odotellessa: jossakin kohdassa kehitystä olemme nykytilan ja tavoitetilan erityisen haavoittuvassa yhdistelmässä. Näihin hetkiin kohdentuu myös paljon inhimillistä osaamispuutetta, koska oppimisprosessi vanhojen rakenteiden ylläpitäjillä on vielä kesken.

Kuvatuilla välineillä voi myös tehdä hyökkäyksen, jossa hyökkääjä jää ainakin rikosoikeudellisessa mielessä paljastumatta. Laitetiloissa tapahtuu tulipaloja, kaivinkoneet katkovat kaapeleita ja räjähdyksiä sattuu. Kohtuutehoisia HPM-lähteitä pystyy jo nyt ostamaan, ja 2020 sellaisen kyennee myös valmistamaan COTS-osista. HPM etuna on, että sen vaikutus näyttää paljon laitevialta. Väkivaltaa saa ostaa yhä tuotteistetummin, varsinkin sillä uhkaamista, ilman välitöntä paljastumisriskiä. Merkittävä osa hyökkäyksestä voidaan tehdä työtä ostamalla, laillisesti. Kyberverkkohyökkäyksen erityisenä haasteena nähdään kyky hyökkääjän salaamiseen, mutta tietyssä mitassa tämä koskee myös fyysistä vaikuttamista kybermaailmaan.

Kun fyysiseen iskuun liittää viivästettynä perinteisen kyberhyökkäyksen, teho on suurin. Puolustaja on joutunut siirtymään varamenetelmiin ja paljastanut verkossa muutoksiaan. Korvaavat järjestelyt omaavat heikomman suojan ja käyttöoikeuksia joudutaan nopeasti parsimaan aiheuttaen verkkovalvojille pitkään häiriöitä, joiden kohinaan hyökkääjä kykenee soluttautumaan. Fyysisellä iskulla voidaan avata väylä bittioperaatioille riisuen suojauksia ja aiheuttaen hämmennystä.

Haluan kiistää sen itsestäänselvyyden, että sota aina alkaisi kyberin bittioperaatiolla laajentuen vasta myöhemmin, ellei tavoitteisiin jo päästy, fyysisempiin vaikutuksiin. Varsinkin, jos kyber tuijottaa vain bittejään, se muuttaa itsensä yhä haavoittuvammaksi fyysiselle vaikuttamiselle.

5.6 Kolmas skenaario: Isku tietopääomaa vastaan

(TY-F / TO-I / K-I-C-VT, TY-F / TO-T / K-T-C-V, TY-F / TO-T / K-T-C-VT)

Alkuperäisessä skenaariossa hyökkäys kohdennettiin kiivaassa kilpailutilanteessa Suomi Oy:n arvokkaimpaan yritykseen, Kapulaan, ja hyökkääjä oli toinen monikansallinen jättiläinen. Skenaario sopi myös maan painostamiseen uhkaamalla sen arvokkainta yritysresurssia ja kiistämällä maan kyky suojata vakavilta hyökkäyksiltä.

Vastaava tilanne voitaisiin saada aikaan käyttämällä edellisten skenaarioiden välineitä, joten en kertaa niitä. Sen sijaan kohdennan tässä hyökkäyksen tietovarantojen oikeellisuutta, laajassa mitassa tulkiten siis eheyttä vastaan, pyrkien tekemään tästä 2020-ajan keskeisestä omaisuudesta arvotonta. Lisään myös hyökkäyksen toteutusaikaa. Erityisesti pyrin horjuttamaan luottamusta julkista valtaa kohtaan osoittamalla, että se on paitsi puolustuskyvytön, myös uhka kansalaisilleen. Luottamus on kyberin voimanlähde, se on siis tärkein maali.

Hyökkäyksen tavoitteena on mahdollisimman laaja epävarmuuden aiheuttaminen. Tässä skenaariossa hyökkäys kohdennetaan julkishallintoon, joka toimii yhä enemmän yritysmäisesti. Suoritustapana on laaja todistettu eheyshyökkäys.

Hallinnossa on joukko ydinrekistereitä, joihin muu hallinto perustuu. Tällaisia ovat muun muassa väestörekisteri henkilötunnuksineen, jota ilman emme olisi kybermaailmassakaan olemassa, verorekisteri joka on sama yrityksille, maanomistusrekisteri ja vaikkapa 2020-luvun valtion keskitetty käyttäjähallintorekisteri, jota ilman virkamiehistö ei pääse töihinsä. Ydinrekisterit suojataan jo nyt monin eri keinoin.

Laskin väitöskirjassani, että neliportaisessa analyysissa riittää, kun 6% lähtöaineiston datasta on väärää[8]. Lähtötilanteessa väärää on luontojaan aina jonkin verran, koska tiedonkeruu ei koskaan ole virheetöntä. Tehokas tapa salata ydinrekisteri kokonaisuutena on siis väärentää siitä haluttu osa, ja toimittaa väärennyksen oikaisukoodi vastaanottajille muiden saadessa vapaasti katsella väärennettyä varantoa jopa uskoen sitä oikeaksi. Tätä siis voidaan käyttää myös salaamiskeinona.
Jo pitkään on esitetty skenaarioita, joissa tunkeutuja muuttaa dataa pidemmän ajan kuluessa vähä vähältä, jolloin myös kaikki varmennukset ja varmuuskopiot saastuvat. Varsin pitkään tällainen toiminta pysyy perusvirheiden kohinan suuruisena, varsinkin mikäli koko aineistoa ei ajoittain käydä erikseen läpi massana. Koska ydinrekisteri on muiden vertailukohtana, integroidussa ympäristössä virheet siirtyvät tehokkaasti koko tietoinfrastruktuuriin.

Ensimmäisen skenaarion hyökkäys on pahimmillaan juuri eheyshyökkäys. Jos esimerkiksi sotilas ei luota aseeseensa, potilas laboratoriotuloksiinsa, johtaja myyntiraporttiin tai maanmittaaja lähtötietoihinsa, vaikutus kohdentuu varsin laajalle.

Eheyshyökkäyksessä ei ole tarpeen saada aikaan tietojärjestelmien romahtamista. Riittää todistus siitä, että riittävä määrä tietoa on väärennettyä, jolloin käyttäjät kiistävät loput aiheuttaen vakavan viiveen ydinvarannon käytölle. Kun tietotekniikkaan perustuva prosessi saadaan virhetilanteessa manuaaliseksi, se jo nyt vie monin kerroin aikaa. Useasti manuaalisesta prosessista on joko kokonaan luovuttu tai ainakaan sitä ei ole harjoiteltu. Vaikka vaikutustapa on hiipivä, myös eheyshyökkäyksen voi ajoittaa haluamalleen hetkelle.

[8] En esitä tässä tarkkaa laskukaavaa, mutta jo laskulla 0,94 potenssiin N varsin pian saa aikaiseksi luvun, jonka suuruista riskiä päätöksenteko ei enää kestä. Mitä monimutkaisemmaksi hallinto tulee, sitä pidempiä ovat ketjut ja sitä herkempi hallinto on datavirheille.

Eheyshyökkäystä voidaan tehostaa varastamalla tietoa ja julkaisemalla sitä, osin myös väärennettynä. Harvalla kansalaisella tai yrityksellä on viranomaisrekistereissä oikeasti salattavaa tietoa, mutta jos epäilee rekisteritiedon olevan väärää, tilanne muuttuu aivan eri tavalla uhkaavaksi.

Erityisen tehokas hyökkäys on, mikäli se johtaa kiistoihin hallinnonalojen välillä, alojen ja keskitetyn palvelutuotannon välillä tai eri hallintotasojen välillä. Tällainen vaikutus syö nopeasti keskinäistä luottamusta ja lamauttaa johtamisen, jolloin kansalaisten ja yritysten tärkein odotus eli turvallisuus, petetään. Mikäli kaikki on lisäksi säädelty tarkasti, tilanne voi olla normaalisäätelyllä korjaamaton ja johtaa nopeastikin poikkeusvaltuuksien käyttötarpeeseen ja kriisiytymisen vahvistamiseen. Tämä voi juuri olla hyökkääjän tavoite, joka oikeuttaa muiden vahvempien hyökkäysvälineiden käytön.

Yrityksillä alkaa jo nyt olla käsitys aineettoman pääomansa arvosta. Jopa brändille osataan laskea hinta. Julkishallinnolla ei tietääkseni ole mitään vastaavaa, ja esimerkiksi jo myytävä peruskoulu edelleen kirjoitetaan pienellä ilman ™-merkintää. Tietovarantojen priorisointi on aloitettu osana kyberstrategian jalkauttamista, mutta haavoittuvuuksia loogisellakin tasolla lienee vielä vuonna 2020.

Jos eheyshyökkäys suunnataan käyttäen vaikkapa etnistä vähemmistöä erityisenä kohteena osoittamaan julkishallinnon syrjintää, ja sitä tehostetaan vahvalla informaatio-operaatiolla, vaikutus voi olla pitkäkestoinen.

5.7 Yhdistetyistä operaatioista ja hyökkäysrakenteista

Nykyajattelussa kybertaistelu nähdään laajemman väkivaltaisen vaikuttamisen valmisteluna tai ensimmäisenä asteena.[9] Joskus jopa nähdään, että koko taistelu voitaisiin käydä kyberympäristössä, varsinkin kun siihen luetaan mukaan sähköinen informaatioympäristö ja siellä käytävä propagandataistelu.

Itse näen sotilaana, että kyber on sekä ympäristönä että välineinä täydennys sodankäynnin kokonaisuuteen siitä mitään aiempaa poistamatta. Kyberiä käytetään, kun se sopii operaation rakenteeseen ja on muita sotilaallisesti edullisempi, tai muita resursseja käytetään muualle. Jälkimmäisestä johtuen kyberaseita myös käytetään, kun ne on kerran rakennettu.

Sodan fyysinen intensiivivaihe toteutetaan suljetussa ympäristössä, johon kyber perinteisesti vaikuttaa fyysisen laitteiden tuhoamisen ja elektronisen tiedonsiirtoon vaikuttamisen kautta. Mikäli bittien maailman vaikuttamista ei ole valmisteltu ja tätä laukaista, on epävarmaa, ehditäänkö koko operaatiota tehdä intensiivivaiheen aikana. Tällaisesta esimerkkinä on ensimmäisen skenaarion hyökkäys, jonka kärki voidaan suunnata puolustajaa vastaan myös operaation aikana, mikäli ollaan varmoja siitä, että vaikutus käyttäjiin on suurempi kuin hyökkäämällä hieman ennalta.
Kyberhyökkäyksen salattavuus on sotilaallisesti pääosin myytti. On eri asia ”tietää” hyökkääjä kuin pystyä se lainsäädännön mukaisesti aukottomasti todistamaan. Myös vastahyökkäykseen voidaan käyttää samoja salaamisen välineitä ja isku voidaan suunnata hyökkääjän haavoittuvuuksiin, ei sen hyökkäysrakenteisiin. Jos vaikutukset ylittävät kansallisen normaaliajan kestokyvyn, käyttöön otetaan uudenlaisia välineitä.

[9] Ks. esimerkiksi puolustusvoimien vaikuttamisen doktriini (TLL IV).

Kybermaailmassa on jo nyt ”palkkasotilaita”, joita saa ostettua hyökkäyksiinsä, mutta kun katsoo valtioiden jo nyt kohdentamia panoksia kyberjoukkoihinsa, palkkasotilaiden vaikuttavuus vähenee.

Skenaariossa kaksi pyrin jo osoittamaan, että kybermaailmaa vastaan saattaa olla tehokasta aloittaa hyökkäys epäsymmetrisesti fyysisen maailman kautta. Koska tämä on tehokasta ja varsin varmaa, fyysinen vaikuttaminen voi hyvin olla kyberpainotteisenkin sodan ensimmäinen vaihe.

Kyber on informaatiosodankäynnin ja propagandan keskeinen alusta. Tällä hetkellä vaikutus nähdään ensi sijassa sortotoimissa heikomman mahdollisuutena saada äänensä kuuluviin. Suomi on maana vuonna 2020 edelleen niin vahva kybertilan toimija, ettei edellä esitetty ole relevantti näkökulma hyökkääjän vahvuudesta huolimatta: suomalaista verkkoviestintää ei voi kokonaisuutena lamauttaa. Myös hyökkääjä kykenee avoimessa yhteiskunnassa esittämään jatkossakin haluamansa argumentit montaa eri kanavaa pitkin myös Suomessa ja suomalaisille. Tämä ulottuvuus on käytössä sodan kaikissa vaiheissa, siis kaikissa taisteluissa.

5.8 Joitakin havaintoja

Yhteiskunnan internetiin liitetyt verkottuneet toiminnat ovat luontainen kyberiskujen kohde. Koska sotilaat iskevät näihin taisteluissa myös fyysisesti, niihin epäilemättä isketään myös kyberissä. Vaikka iskujen estäminen fyysisessä maailmassa on viranomaisten ja äärimmillään sotilaiden tehtävä, perusturvallisuudesta ja toipumisesta vastaa iskujen kohde itse. Oletan, että 2020 mennessä sama jako on käytössä myös kyberperän taisteluissa. Kybertaistelu 2020 on siis mitä suurimmissa määrin yhteiskunnan kaikkien tasojen voimavarojen käyttöä. Jo nykykriisit osoittavat, että yhteiskunnan laajemmat voimavarat aina rikollisia myöten voidaan myös valjastaa hyökkääjän käyttöön.

Kyberhyökkäysten erityinen ominaisuus on, että sen lähde voidaan ainakin pitäviltä todisteilta salata ”normaalia” hyökkäystä paremmin. Tämä tarkoittaa myös sitä, että kyberissä ”Mainilan laukaukset” voidaan ampua paljon luovemmin kuin vuonna 1939 tehtiin. Hyökkäyksiä tapahtuu jatkuvasti, ja niihin liittyvät todisteet on lähes yhtä helppoa väärentää kuin kätkeä itse hyökkäys.

Kyberin erityinen ominaisuus on, että se tällä hetkellä tulkitaan yhteiseksi vapaaksi tilaksi. Ennakoin, että jo nyt käynnissä oleva kehitys kybermaailman rajojen määrittämiseksi jatkuu kiihtyen, jolloin 2020 tilanne on jo nykyisestä poikkeava. Käytän kansallisvaltion määrittämästä kyberalueestaan nimitystä kyberperä vertauksena maaperään aluevesineen ja ilmatiloineen, jotka valtio katsoo omakseen, joita se valvoo ja joihin kohdistuvilta hyökkäyksiltä maa puolustautuu.

Suomen fyysisellä maaperällä on kasvava määrä muiden maiden lakien mukaan kyberissä toimivia yrityksiä ja tilanne on lainsäädännön osalta nyt epäselvä. Toisaalta suomalaisessa kyberperässä eli yrityksissä, jotka toimivat Suomen lakien mukaan, tuotetaan palveluita muiden valtioiden toimijoille ja näiden vastustajille. Ruotsi katsoo jo oikeudekseen seurata kaikkea sen kyberperän rajat ylittävää liikennettä. Kiina rajoittaa voimakkaasti sekä ulkoliikennettä että maan sisäisiä kyberpalveluita.

Ilmatilan korkeus ja merialueen kansallinen koko määrittyivät aikoinaan sillä, mikä oli kunkin valtion todellinen kyky valvoa ja vaikuttaa alueella. Lakirakenteet ja sopimukset tulivat myöhemmin. Vastaava kehitys on jo nyt käynnissä kyberissä ja kukin valtio valvoo jo omalla tavallaan ja kyvyillään omaa kyberperäänsä.

Tavoitteeni ei tässä tekstissä kuitenkaan ole perustella, miksi juuri kuvaamallani tavalla kävisi vaan pohtia, mihin kyberperän käyttö ja suojaaminen voisi taistelujen kannalta johtaa.

On jo nyt mahdollista, että Suomen kyberperällä sotaa käy kaksi tai useampia tahoja ilman, että Suomi on sinällään tämän sodan osapuoli. Herää siis kysymys, mitä suomalaiset kyberjoukot tällöin tekevät, ketä ne mahdollisesti suojaavat ja miten suojaudumme taistelujen tuholta? Koska kyberin kaupallinen teknologia on kaikkialla hyvin samanlaista, suurena vaarana on, että tällainen sodankäynti kohdentuu tietovoimaloissamme harhalaukauksina myös meihin.

Vastaavasti me saatamme joutua puolustautumaan jonkun muun valtion omaksi kyberperäkseen tulkitsemalla alueella. Voi jopa olla, että taisteluja käydään laajastikin muualla. Fyysisessä maailmassa koukkausmahdollisuuksia hyökkääjälle on rajallinen määrä, mutta kybermaailmassa niitä on erittäin paljon. Staattinen puolustus linnoituksineen ei siis ole vaihtoehto, on osattava puolustautua liikesodankäynnin keinoin. Niinpä hyökkäyksestä seuraus ei välttämättä olekaan puolustustaistelu, vaan kohtaamishyökkäyksen tyyppinen tilanne.

Jo tällä hetkellä jotkut yritystoimijat, kuten suuret pornonlevittäjät, ilmeisesti käyttävät automaattisia verkkohyökkäyksiä osana puolustustaan. Ammattimaista hyökkääjää tämä tuskin pelottaa, mutta satunnaiselle avoimesta hyökkäysarsenaalista ammentavalle tämä on pelote. Vastaavat automaattihyökkäykset voivat hyvin olla valtavirtaa 2020 tienoilla, jotta kaapatut koneet saadaan nopeasti hiljennettyä. Jo tällä hetkellä esimerkiksi fyysisten sotilaslentokoneiden puolustustoimista osa on automatisoitu ja on syytä olettaa, että näin menetellään myös verkoissa.

Automatisointi avaa mielenkiintoisia mahdollisuuksia hyökkääjälle. Käyttämällä sopivaa palvelinta apuna puolustaja saatetaan saada taistelemaan jopa itsensä kanssa tai ystävällismielisen, neutraalin tai vielä osallistumattoman tahon kanssa. Toisaalta koneiden valtaaminen voi aiheuttaa vastatoimia jo ennen kuin oma hyökkäys on edes aloitettu. Onkin nähtävissä, että hyökkäys voi aiheuttaa laajan ”parvimaisen” vastahyökkäyksen, jota sotilasliittojen ”kyberreserveillä” saatetaan vielä tukea monesta kanavasta. Mikäli hyökkäysten määrä kasvaa nykyistä vauhtia, osa tällaisesta saatetaan hyvinkin automatisoida.

Mielenkiintoinen kysymys on, kuinka vakava hyökkäys Suomen kyberperällä voidaan tehdä ja ketä vastaan, jotta se tulkitaan hyökkäykseksi valtiovaltaa vastaan tai hyökkäyksen kohteen puolustautumista tuetaan ulkopuolisin toimin. Uskon, että nykyinen käsitys yhteiskunnan kriittisestä infrastruktuurista tulee vuoteen 2020 mennessä kattamaan myös kyberympäristön nykyistä paljon laajemmin.

Mikäli hyökkää reaalimaailmassa sotilaskohteeseen, sotilailla on kaikissa maissa oikeus väkivallan käyttöön ilman poliisia. Pidän erikoisena, jos vastaava oikeus ei pätisi myös 2020-ajan kybermaailmassa.

Muistutan sotilaille, että työnjaosta riippumatta kyberhyökkäykseen voidaan käyttää kaikkia keinoja hakkereista ja rikollisista alkaen, vaikkei näin ole menetelty fyysisessä maailmassa enää aikoihin. Tästä syystä viranomaisten saumaton yhteistoiminta on elintärkeää kyberpuolustusta käytettäessä.

5.9 Johtopäätökset

Ahvenainen esittää luvussa 2 vertailukohdat systeemiteoriaan ja siinä taisteluyhtälöihin. Palvelunestohyökkäys vertautuu epäsymmetriseen parveilutaisteluun, jota Lanchester kuvaa taisteluyhtälöissään neliölain (maaleihin tähdätään) ja lineaarilain (ammutaan maalialuetta) yhdistelmänä. Tällöin myös puolustajan ylivoimatilanteessa hyökkääjän alkuvaiheen etu on merkittävä[10]. Yleisimmissä palvelunestohyökkäyksissä tällainen taistelutapa näkyy puhtaimmillaan. Fyysistä iskua ei ole laajamittaisena ja täsmäytettynä käytetty kyberympäristöä vastaan, vaikkakin isoissa operaatioissa on isketty palvelukeskuksia ja tiedonsiirtoyhteyksiä vastaan. Toisaalta palvelinkeskuksia on fyysisesti suojattu vuosikymmeniä. Kun kyberpuolustusta kehitetään, ei ole syytä unohtaa sen fyysistä haavoittuvuutta eikä varsinkaan mahdollistaa tilanteita, joissa kaksoistornien tapaan myös varmistukset tuhoutuvat fyysisessä iskussa. On hyvä myös muistaa teknisten avainhenkilöiden ylläpitävä ja vaurioita korjaava rooli kybertoiminnoissa.

Eheyshyökkäys on esimerkki pitkäaikaisesta vaikuttamisesta, johon käytetään paljon panoksia, mutta jonka tulokset käytetään tarvittaessa nopeasti ja jopa liioitellusti. Tietoa voidaan varastaa tai pääsy siihen estää, mutta pelottavinta on tiedon tekeminen arvottomaksi.

Resilienssi on keskeinen puolustajan väline. Vaikka hyökkääjä tietää pääsevänsä läpi ja iskevänsä kohteisiin, puolustajan kykyä sietää, kestää ja toipua hyökkäyksistä on hyvin vaikea ennakoida. Tässä tullaan sodankäynnin perinteiseen ajatteluun, jossa taistelut kietoutuvat toisiinsa ja ”sodan usvaan”.

Vastahyökkäys on tekijä, joka hyökkääjän on aina otettava huomioon.

[10] Ks. Hyytiäinen 2002, jossa asiaa on tarkasteltu yhtälöiden ja fyysisen maaston näkökulmasta. Kyber muodostaa myös tavallaan taistelumaaston.

6.

Tietoverkkopuolustuksen haasteiden 2020 arviointi analyyttisellä hierarkiaprosessilla

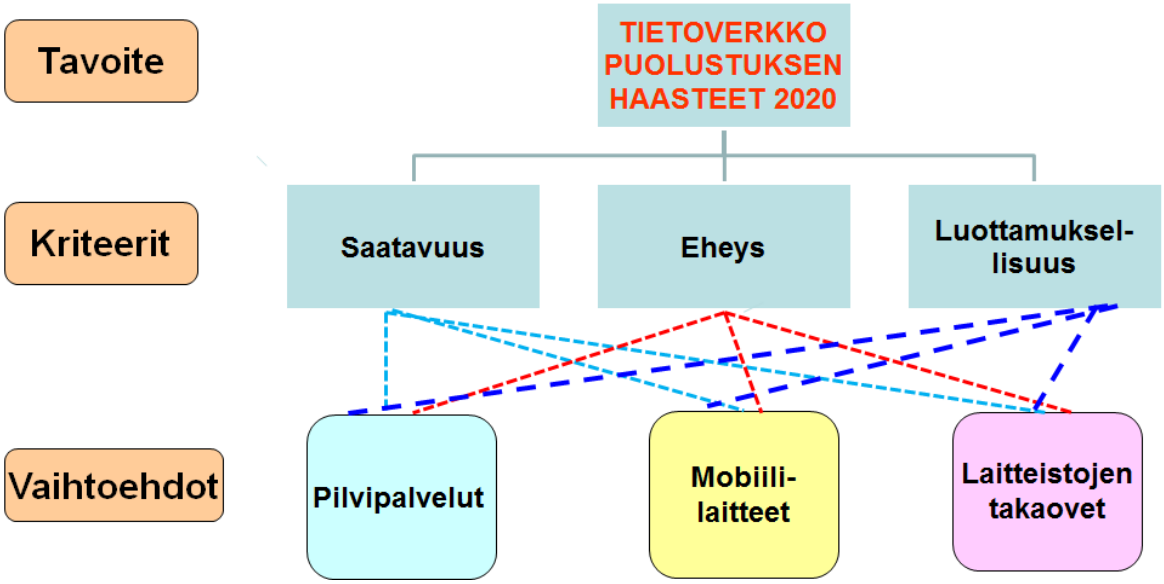
Jouko Vankka
Maanpuolustuskorkeakoulu
Sotatekniikan laitos

Professori Jouko Vankan osaamisalueita ovat tietoverkko-operaatiot, ohjelmistoradiot, kriittisen infrastruktuurin tilannekuva ja käyttöliittymäsuunnittelu. Hän on väitellyt signaalinkäsittelystä vuonna 2000 Teknillisestä Korkeakoulusta. Hän on ollut tutkijana Puolustusvoimissa ja Teknillisessä Korkeakoulussa. Hän on toiminut sotatekniikan, erityisesti radiotietoliikennetekniikka dosenttina Maanpuolustuskorkeakoulussa vuodesta 2007 lähtien. Hän on julkaissut noin 90 tieteellistä julkaisua, kolme patenttia ja kolme kirjaa (Direct Digital Synthesizers: Theory, Design and Applications (Kluwer Academic Publishers, 2001), Digital Synthesizers and Transmitters for Software Radio (Springer-Verlag New York, 2005) ja Maavoimien Taktisen Verkon Tekniikat ja Standardit, 2009).

Tiivistelmä
Analyyttinen hierarkiaprosessi (AHP) on monikriteerimenetelmään perustuva päätöksentekomenetelmä. Monikriteerianalyysillä useita ristiriitaisia näkemyksiä voidaan ottaa huomioon ongelman ratkaisussa. Suurehkojen moniulotteisten ongelmien ratkaisussa täytyy ottaa huomioon monia kriteerejä, jotka saattavat olla luonteeltaan hyvinkin erilaisia. Kriteereitä voivat olla puhtaasti tekniset kysymykset esimerkiksi saatavuus, eheys, luottamuksellisuus, kustannukset sekä vaikkapa psykologiset tekijät.[1]

AHP:ssä tutkittava ongelma jaetaan osatekijöihin hierarkiarakenteella (ks. kuva 1). Lähtökohtana on yksinkertaistaa monimutkainen ongelma parivertailutasolle, jossa ihminen kykenee helposti hahmottamaan kahden samankaltaisen vaihtoehdon välille eron tietyn kriteerin kautta. Monitasoinen ongelma pilkotaan siis käsittelykelpoisiksi osiksi, jolloin arvioitsija pystyy kerrallaan keskittymään pienempään asiakokonaisuuteen ja saa oletettavasti luotettavamman tuloksen. AHP:ssä suositellaan, että kullakin hierarkian tasolla keskenään vertailtavaksi asetettaisiin enintään noin 7 vaihtoehtoa/kriteeriä. Suositukselle esitetään psykologisia perusteita: ihmisen on vaikea hahmottaa tilannetta, jossa mukana on kovin monta vaihtoehtoa/kriteeriä.[2]

[1] *Analytic hierarchy process*. [viitattu 25.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/Analytic_hierarchy_process.
[2] Lehtinen, M. *Operaatioanalyysia sotilaille*. Maanpuolustuskorkeakoulu, Tekniikan laitos, Helsinki 2003, 69 s.



Kuva 1. Hierarkiapuu

6.1. Analyyttinen hierarkiaprosessi (AHP)

AHP-menetelmässä käytetään hierarkkista mallia, joka käsittää kriteerit sekä vaihtoehdot (ks. kuva 1), joilla tavoitteeseen päästään tai se voidaan ratkaista. Menetelmä on kehitetty seuraaville periaatteille:[3]

- hierarkian rakentaminen: tavoitteeseen pääsemiseen vaikuttavat kriteerit/vaihtoehdot
- parivertailut: määritetään kriteerien ja vaihtoehtojen painokertoimet
- parivertailujen johdonmukaisuuden arviointi (ks. luku 6.1.3).

Hierarkian yläpään muodostaa tutkittava tavoite eli ongelma. Hierarkian alimmalla tasolla on valinnan kohteena olevat vaihtoehdot (ks. kuva 1). Tavoitteen ja vaihtoehtojen väliin sijoitetaan kriteerit alakriteereineen. Jos vertaillaan kriteerejä (ks. kuvan 2 vasen yläosa), kysytään: "Kumpi kriteereistä on parempi ao. tavoitteen suhteen ja kuinka paljon parempi se on?". Jos vertaillaan vaihtoehtoja (ks. kuvan 2 alaosa), kysytään: "Kumpi vaihtoehdoista on parempi ao. kriteerin suhteen ja kuinka paljon parempi se on?". Parivertailussa päätetään ensin, onko A_i vai A_j toivottavampi tai parempi tai tärkeämpi kriteerin K_i kannalta (ks. kuvan 2 alaosa), ja jos esim. A_i päätetään paremmaksi, paremmuuden määrää arvioidaan viisiportaisesti: "yhtä hyvä" - "hiukan enemmän" - "selvästi enemmän" - "erittäin selvästi enemmän" - "äärimmäisen selvästi enemmän" (ks. taulukko 1). Vaihtoehdot konvertoidaan numeroarvoiksi 1, 3, 5, 7, 9, jolloin tilaa jää vielä "siltä väliltä" –arvioille (2, 4, 6, 8). Jos tätä lukua merkitään a_{ij}:lla, on tultu tulokseen, jonka mukaan A_i on a_{ij} kertaa niin suotava tai tärkeä kuin A_j vertailtavana olevan kriteerin/vaihtoehdon suhteen.[2]

[3] Salminen, E. & Lehtinen, M. *Analyyttinen hierarkiaprosessi- Expert Choice – ohjelman käyttö*. Maanpuolustuskorkeakoulu. Tekniikan laitos. Helsinki 2000, 10 s.

Taulukko 1. Parivertailussa käytettävä asteikko[2,3]

Lukuarvo	Määritelmä	Kuvaus
1	Yhtä hyvä	Kahden elementin välille ei voida tehdä eroa
3	Hiukan enemmän	Elementtiä voidaan pitää jonkin verran toista parempana
5	Selvästi enemmän	Elementti on selkeällä tavalla vertailukohdetta parempi
7	Erittäin selvästi enemmän	Elementti on selkeällä tavalla voimakkaasti vertailukohdetta parempi
9	Äärimmäisen selvästi enemmän	Elementti on voimakkaimmalla mahdollisella tavalla vertailukohdetta parempi

Kun parivertailut on tehty, voidaan kaikille AHP-mallin kriteereille laskea omat painokertoimensa, jotka mahdollistavat mallin käyttämisen vaihtoehtojen vertailemiseen ja saatujen arvojen hyödyntämiseen lopullisessa päätöksenteossa. Parivertailut eivät yleensä johda täysin johdonmukaisiin lukuihin: siitä, että A_i on arvioitsijan mielestä kaksi kertaa niin suotava kuin A_j ja A_j kaksi kertaa niin suotava kuin A_k, ei välttämättä seuraa, että A_i olisi arvioitu neljä kertaa niin suotavaksi kuin A_k. Tämän epätasapainon poistamiseksi muodostetaan luvuista matriisi

$$A = \begin{bmatrix} 1 & a_{12} & \dots & a_{1k} \\ a_{21} & 1 & \dots & a_{2k} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & 1 \end{bmatrix},$$

josta pyritään matemaattisesti määrittämään "paras" vaihtoehtojen preferenssisuhde.[2]

Alakolmiomatriisin elementit ovat yläkolmiomatriisin käänteislukuja, jolloin vertailu on siinä mielessä symmetristä, että A_j on tällöin $1/a_{ij} = a_{ji}$ kertaa niin suotava tai tärkeä kuin A_i. Yllä olevan k x k-tyyppisen matriisin A ja k x 1-tyyppisen vektorin

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_k \end{bmatrix}$$

kertolasku tuottaa *k* x 1-tyyppisen vektorin

$$AX = \begin{bmatrix} x_1 + x_2 a_{12} + \ldots + x_k a_{1k} \\ x_1 a_{21} + x_2 + \cdots + x_k a_{2k} \\ \ldots \\ x_1 a_{k1} + x_2 a_{k2} + \cdots + x_k \end{bmatrix}.$$

Jos sattuu käymään niin, että *AX* on suorastaan lukuvakio *λ* kertaa *X,* niin *X* on *A*:n ominaisvektori ja *λ* vastaavasti *A*:n ominaisarvo, *k* x *k*-tyyppisellä matriisilla on enintään *k* eri ominaisarvoa.[2]

Jos parivertailujen tuottamat arviot olisivat täysin johdonmukaisia, matriisin *A* vaakarivit saataisiin ensimmäisestä jakamalla tämän alkiot vuoron perään luvuilla a_{1j}. Tällaisella matriisilla on vain yksi ominaisarvo, joka on *k,* ja sen ominaisvektoreita ovat matriisin pystyvektorit. Vaihtoehdon A_i painokerroin olisi ominaisvektorin elementti x_i jaettuna ominaisvektorin elementtien summalla.[2]

Tarkastellaan sitten realistisempaa tilannetta, jossa matriisi *A* perustuu likimain johdonmukaisiin arvioihin. Silloin *A*:n suurin ominaisarvo on vähän suurempi kuin *k* ja *A*:lla saattaa olla useampia ominaisarvoja. AHP:ssä approksimoidaan parivertailujen kokonaisuutta *A*:n suurimpaan ominaisarvoon (λ_{max}) liittyvällä ominaisvektorilla. Suurimpaan ominaisarvoon liittyvän ominaisvektorinkäyttö preferenssilukujen yhdistämisessä on sopimuskysymys, mitä ei voi perustella puhtaasti matemaattisesti. Matriisin ominaisarvojen ja ominaisvektorien laskenta on matemaattinen tehtävä, josta ei yleensä suoriudu "manuaalisesti".[2]

6.1.1 Kokonaispainokertoimet

Parivertailujen ja matriisin ominaisvektorien määrityksen jälkeen lasketaan eri vaihtoehtojen kokonaispainokertoimet (ks. kuva 2). Jos vaihtoehdon A_j painokerroin kriteerin K_i suhteen on s_{ij} ja vaihtoehdon K_i tärkeys ylemmän tavoitteen suhteen on w_n, niin vaihtoehtojen A_j kokonaispainokertoimet tavoitteen suhteen saadaan kaavasta (ks. kuva 2)

$$\textit{Kokonaispainokerroin}\, A_j = \sum_{n=0}^{t} w_n\, s_{n,j}.$$

Lopputuloksena saadaan vaihtoehtojen kokonaispainokertoimet tavoitteen kannalta.[2] Artikkelissa käytetään painokertoimien laskentaan Expert Choice tietokoneohjelmaa, jossa ylläoleva laskentatapa on distributive mode.[4]

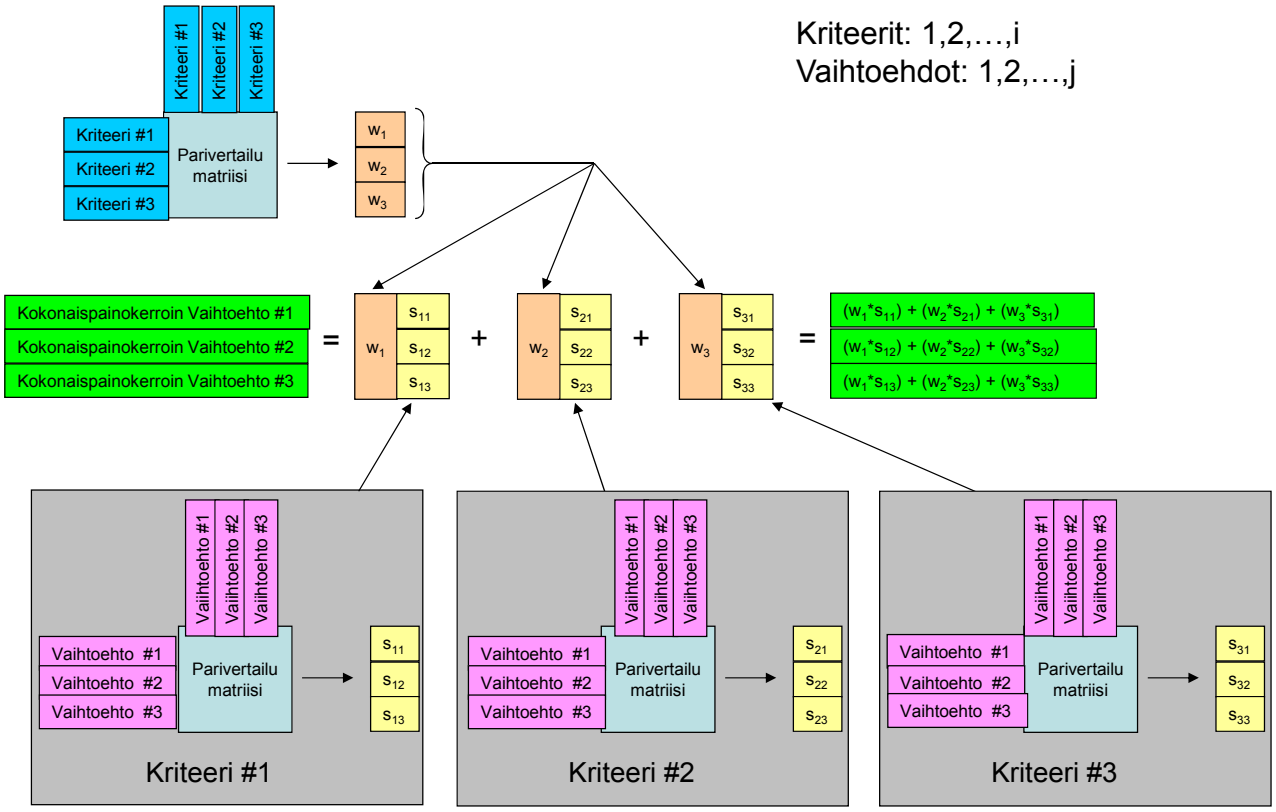
Kaikkien vaihtoehtojen tulee olla tarkastelussa yhtä aikaa mukana. Jos alkuperäiseen vaihtoehtovalikoimaan lisätään vaihtoehto, saattaa uusi laskenta vaihtaa myös alkuperäisten vaihtoehtojen keskinäistä järjestystä vaikka alkuperäisten parivertailujen tulokset pysyisivät ennallaan. Syy tähän ilmiöön on kunkin vertailun tuottamien painokertoimien pieneneminen, kun kokonaispainokertoimien summaa 1 jaetaan useammalle ottajalle. Eräs tapa välttää tätä ongelmaa on jakaa pisteet niin, että jokaisessa alimman tason vertailussa (ks. kuvan 2 alareuna) paras vaihtoehto saa piste-

[4] Ishizaka, A. & Labib, A. *Analytic Hierarchy Process and Expert Choice: Benefits and Limitations*. ORInsight, 22(4), 2009, s. 201 - 220.

määrän 1 ja muiden pistemääräksi tulee s_{ij}/max(s_{ij}), missä s_{ij}:t ovat alkuperäiset painokertoimet. Tätä laskentatapaa (ideal mode Expert Choice tietokoneohjelmassa[5]) suositellaan käytettäväksi erityisesti silloin, kun ensisijaisesti tarkoitus on etsiä parasta vaihtoehtoa, ei niinkään kaikkien vaihtoehtojen paremmuusjärjestystä.[2]

6.1.2 Useita arvioitsijoita

Jos parivertailuja tekee usea asiantuntija, ja he eivät voi neuvottelemalla sovittaa yhteen näkemyksiään, on parivertailujen pisteet yhdistettävä järkevästi. Aritmeettinen keskiarvo ei ole hyvä tapa. Jos kahdesta arvioijasta toinen tuottaa luvun a_{ij}= 5 ja a_{ij} = 1/5, ei keskiarvo 2,6 tunnu järkevältä yhteismielipiteeltä. AHP suosittaa käyttämään mielipiteiden yhdistämisessä geometrista keskiarvoa. Edellä olevan esimerkin tilanteessa geometrinen keskiarvo on $(5 \times 1/5)^{1/2} = 1$.[3]



Kuva 2. Painokertoimien laskeminen parivertailumatriisin avulla

[5] *Tutorial for Analytic hierarchy process*. [viitattu 25.5.2014]. Saatavissa: http://www2.ing.puc.cl/ics2805/lecturas/ahp.pdf

6.1.3 Parivertailujen johdonmukaisuus

Parivertailujen johdonmukaisuutta arvioidaan laskemalla johdonmukaisuusindeksi (*CI*, consistency index)

$$CI = \frac{\lambda_{max} - k}{k - 1},$$

jossa λ_{max} on k x k-tyyppisen matriisin suurin ominaisarvo. Johdonmukaisuussuhde (*CR*, consistency ratio)

$$CR = \frac{CI}{RI}$$

saadaan jakamalla johdonmukaisuusindeksi teoreettisesti lasketulla sellaisen vertailumatriisin satunnaisindeksillä, joka perustuu aivan satunnaisesti tehtyihin valintoihin.[2] Nämä satunnaisindeksit (*RI*, random index) ovat seuraavanlaisia:

k	3	4	5	6	7	8	9	10	11	12	13	14
RI	0,52	0,89	1,11	1,25	1,35	1,40	1,45	1,49	1,51	1,54	1,56	1,57

Katsotaan, että johdonmukaisuussuhde (*CR*) tulisi olla alle 0,1. Muussa tapauksessa parivertailut ovat niin epäjohdonmukaisia, että niitä on syytä vielä harkita.[4]

AHP-hierarkian johdonmukaisuussuhde (*CRH,* consistency ratio of the hierarchy) lasketaan jakamalla hierarkian johdonmukaisuusindeksi (*CIH,* consistency index of the hierarchy) hierarkian satunnaisindeksillä (*RIH,* random index of the hierarchy) [6]

$$CRH = \frac{CIH}{RIH} = \frac{\sum_i w_i CI_i}{\sum_i w_i RI_i}.$$

AHP-hierarkian johdonmukaisuusindeksi (*CIH*) lasketaan kertomalla jokaisen parivertailumatriisin johdonmukaisuusindeksi (*CI*) tavoitteen tai hierarkiapuussa välittömästi yläpuolella olevan kriteerin painoarvolla, ja kertolaskujen tulokset lasketaan yhteen. Esim. kuvassa 2 kriteerien parivertailumatriisin johdonmukaisuusindeksi kerrotaan ykkösellä (tavoitteen painoarvo), ja jokaisen kriteerin painokertoimella w_i kerrotaan vastaavan parivertailumatriisin johdonmukaisuusindeksi CI_i. Vastaavasti AHP-hierarkian satunnaisindeksi (*RIH*) lasketaan kertomalla jokaisen parivertailumatriisin satunnaisindeksi (*RI*) tavoitteen tai hierarkiapuussa välittömästi yläpuolella olevan kriteerin painoarvolla, ja kertolaskujen tulokset lasketaan yhteen.

[6] Saaty, T. *Decision Making with Dependence and Feedback The Analytic Network Process*. RWS Publications, Pittsburgh, 1996, 287 s.

6.1.4 AHP-menetelmän luotettavuus

Menetelmän luotettavuutta tarkastellaan seuraavien epävarmuustekijöiden kautta:

- **Keskinäinen riippuvuus:** Kriteerien keskinäinen riippuvuus toisistaan voi aiheuttaa tilanteen, jossa AHP-menetelmän hierarkkista mallia on hankala rakentaa.[3]
- **Parivertailujen johdonmukaisuus:** Asiantuntijan johdonmukaisuutta tarkastellaan hierarkian johdonmukaisuussuhteella (*CRH*), jonka raja-arvo satunnaisuudelle on 0,1 (ks. luku 6.1.3).[3]
- **Rank reversal:** Jos alkuperäiseen vaihtoehtovalikoimaan lisätään vaihtoehto, saattaa uusi laskenta vaihtaa myös alkuperäisten vaihtoehtojen keskinäistä järjestystä vaikka alkuperäisten parivertailujen tulokset pysyisivät ennallaan (ks. luku 6.1.1). [7]
- **Tärkeysjärjestys:** Ihmisellä on taipumus käyttää vain tiettyjä numeroita tai vastauksia, jotka voivat sisältää kaikesta huolimatta lähinnä ordinaalista informaatiota (tärkeysjärjestys) eivätkä vastaa taulukon 1 asteikkoa.[7]
- **Preferenssivastaavuus:** AHP:n lukuarvoja (ks. taulukko 1) vastaavat numeeriset arviot riippuvat asiayhteydestä. Valmiiksi rakennetut asteikot eivät välttämättä vastaa vastaajan todellisia preferenssejä (mieltymyksiä).[7]
- **Range effect:** Asiantuntijat eivät huomioi riittävästi kriteerien ja vaihtoehtojen vaihteluvälien edellyttämiä muutoksia vertailuissa. Esimerkiksi saatavuuden paino saattaa olla sama riippumatta siitä onko saatavuushäiriön vaihteluväli hetkellistä katkosta useita päiviä kestävään katkoon. Vika voi olla AHP-kyselyssä, jotka ei tuo vaihteluväliä tarpeeksi selkeästi esiin.[7]

6.2 Tietoverkkopuolustuksen haasteet 2020

Tietoverkkopuolustusta kuvaava malli (ks. kuva 1) muodostuu kolmesta pääkriteeristä:

- luottamuksellisuus,
- eheys
- ja saatavuus,

sekä vaihtoehdoista:

- pilvipalvelut,
- laitteistojen takaovet
- ja mobiililaitteet,

ja tavoitteesta (ongelmasta)

- tietoverkkopuolustuksen haasteet 2020.

[7] *Analyyttinen hierarkiaprosessi (AHP)*. Aaltoyliopiston verkkojulkaisu. 5. luento: 10.10.2006. [viitattu 25.5.2014]. Saatavissa: http://www.sal.tkk.fi/vanhat_sivut/Opinnot/Mat-2.3134/luennot2006.html

6.2.1 AHP-mallin kriteerit

Tietoturvan analysointimalleista CIA on yksinkertaisin ja yleisimmin käytetty.[8] CIA on lyhenne termeistä confidentiality (luottamuksellisuus), integrity (eheys) ja availability (saatavuus). Tietoverkkopuolustuksen haasteista 2020 kuvaava malli muodostuu kolmesta kriteeristä, jotka ovat luottamuksellisuus, eheys ja saatavuus (ks. kuva 1). Parivertailujen tuloksista (ks. kuva 2 oikea yläreuna) lasketaan eri kriteereille painokertoimet, jotka ilmaisevat niiden painoarvoa tietoverkkopuolustuksen haasteissa 2020. Tietoverkkopuolustuksen haasteiden 2020 kriteerien tarkastelu rajautuu CIA malliin:

Luottamuksellisuus (engl. confidentiality): tietoa pääsevät käsittelemään ainoastaan ne, joilla on oikeus käsitellä tietoa.

Eheys (engl. integrity): tiedon käsittelymekanismit takaavat tiedon virheettömän käsittelyn. Tieto ei siis voi huomaamatta muuttua käsittelyprosessin aikana. Kriteeri ei takaa tiedon oikeellisuutta, jos tieto on lähtökohtaisesti väärin.

Saatavuus (engl. availability): tieto ja sen käsittelymekanismit ovat aina oikeutettujen käyttäjien saatavilla.

6.2.2 AHP-mallin vaihtoehdot

Analyyttisen hierarkiaprosessin mallin eri vaihtoehtoja kerättiin kirjallisista lähteistä [9, 10, 11, 12, 13.] Sotatekniikan laitoksen asiantuntijaryhmä (kolme henkilöä) valitsi Delfoi-menetelmän[14] haastattelukierrosten jälkeen seuraavat kuvan 1 vaihtoehdot (pilvipalvelut, laitteistojen takaovet ja mobiililaitteet). Parivertailujen tuloksista laskettiin jokaiselle vaihtoehdolle painokertoimet kriteerin suhteen, ja tämä toistetaan jokaiselle kriteerille (ks. kuva 2 alareuna). Seuraavaksi selvitetään AHP-mallin eri vaihtoehtojen perusteita.

6.2.2.1 Pilvipalvelut

Pilvipalvelut on yleisnimitys palveluille, joita voi käyttää Internetin avulla riippumatta palvelun sijainnista.[15] Pilvipalvelut jaetaan julkiseen, yksityiseen tai niiden hybridiin, joilla on eri turvallisuusriskit.[16] Ulkoisten palveluiden lisäksi myös pilvipalvelumallin

---

[8] *Information security*. [viitattu 25.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/Information_security

[9] DeGusta, M. *Are Smart Phones Spreading Faster than Any Technology in Human History?*. MIT Technology Review. 2012 Toukokuu 9. [viitattu 25.5.2014]. Saatavissa: http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/

[10] Evans, D. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*. Cisco. 2011 Huhtikuu. [viitattu 25.5.2014]. Saatavissa: www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[11] Burt, D. *Cyberspace 2025: Today's Decisions, Tomorrow's Terrain*. Microsoft. 2014 Kesäkuu. [viitattu 25.5.2014]. Saatavissa: http://www.microsoft.com/security/cybersecurity/cyberspace2025/

[12] Clark, J. *Cloud computing: 10 ways it will change by 2020*. 2012 Heinäkuu 31. [viitattu 25.5.2014]. Saatavissa: http://www.zdnet.com/cloud-computing-10-ways-it-will-change-by-2020-7000001808/

[13] Andress, J. & Winterfeld S. *Cyber Warfare: techniques, tactics and tools for security practioners*. 2. painos. Elsevier: USA, 2013, 324 s.

[14] *Delfoi-metodi*. [viitattu 15.8.2014]. Saatavissa: http://fi.wikipedia.org/wiki/Delfoi-metodi

[15] Salo, I. *Pilvipalveluiden edut ja riskit yritysnäkökulmasta*. Maaliskuu 2010, Systeemityö. [viitattu 25.5.2014]. Saatavissa: http://www.eufris.fi/kuvat/Systeemityo3_2010_ImmoSalo.pdf

[16] Zaerens, K. *Enabling the Benefits of Cloud Computing in a Military Context*. 2011 IEEE Asia-Pacific Services Computing Conference (APSCC'11). Korea (South). Joulukuu 2011, s. 166 - 173.

mukaisesta organisaation omasta arkkitehtuurista käytetään nimitystä yksityinen pilvipalvelu.[15] Palveluita käyttöönottavalle organisaatiolle pilvipalvelut lupaavat kustannussäästöjä ja parempaa kustannusrakennetta kiinteiden kustannusten vaihtuessa muuttuviksi, lähes rajatonta skaalautuvuutta tietotekniikkaresursseihin, paikkariippumattomuutta, ajantasaisuutta ja muita houkuttelevia etuja.[15] Pilvipalveluiden käyttö on haaste sotilasorganisaatiolle, koska palveluiden saatavuudessa täytyy luottaa monesti ylikansalliseen organisaatioon. Sotilasorganisaatiolle on tärkeää tietää tietojen säilytyksen ja käsittelyn fyysinen paikka, ja millä organisaatioilla ja viranomaisilla on pääsy tietoihin.

Palveluntarjoajista suurimmilla kuten Amazonilla, Googlella ja Microsoftilla on palvelinkeskuksia usealla mantereella, milloin ongelmia voi aiheuttaa kansainvälisessä pilvipalvelussa maakohtaiseen tietosuojaan ja sen lainsäädäntöön liittyvät ristiriidat (esim. USA:n ja EU:n yksityisyyden lait ovat erilaisia).[17] Palvelinkeskukset mahdollistavat keskitetyn tietoturvan, mutta palveluita hyödyntävien käyttäjäkohtaisten aineistojen tai sovellusten tietoturva täytyy huolehtia tilaajan toimesta. Palvelinkeskukset ovat kohteita palvelunestohyökkäyksille ja tietomurroille. Suuret palveluntarjoajat pystyvät mitoittamaan palvelimet ja tiedonsiirtokapasiteetin kestämään laajoja hajautettuja palvelunestohyökkäyksiä. Palvelunestohyökkäyksiä suurempi haaste on tietojärjestelmien haavoittuvuudet ja niiden avoimuus sekä saavutettavuus tietoverkossa.[18] Tietoturva on kustannus palveluntarjoajalle, siksi tilaajan edut eivät aina ole yhtenevät toimittajan etujen kanssa. Epäonnistumisista ja tietovuodoista esimerkkinä ovat Microsoftin omistaman Dangerin Sidekick-skandaali vuodelta 2008,[19] jossa Sidekick-puhelimien pilveen tallentamat tiedot hetkeksi kadotettiin täysin, sekä Operaatio Aurora tietomurto vuodelta 2009 kohteena esim. Google.[20]

Pilvipalveluiden saatavuuteen liittyviä riskejä ovat pilvipalvelun ongelmat, palveluntarjoajan konkurssi ja palvelunestohyökkäykset. Palveluntarjoajat tarjoavat saatavuuden takaavia palvelutasosopimuksia (SLA), joista tyypillinen on 99,9 %:n palvelutason lupaava SLA.[14] Kolmansien osapuolien tai pilviorganisaation työntekijät voivat muuttaa tiedostoja ja järjestelmiä, mikä voi aiheuttaa ongelmia tietokantojen eheyteen. Pilvipalveluiden luottamuksellisuuden uhkia ovat salakuuntelu, kolmansien osapuolien tai pilviorganisaation työntekijöiden pääsyoikeudet tietoihin, huijaukset, tietoryöstöt. Pilvipalveluarkkitehtuuri, jossa pilviympäristön sisältö on salattu ja tietoliikenne valvottua ja todennettua, suojaa osittain tiedustelulta ja tiedon vääristämiseltä sekä virheellisen tiedon syöttämiseltä (huom. National Security Agency:n (NSA) kyvykkyys[21]). Tietosisällön salaus saattaa hidastaa ulkopuolisen toimijan sisällön selvitystä riittävästi, jotta esimerkiksi tiedon ajantasaisuus ja oikeellisuus saadaan varmistettua operatiivisella tasolla.

---

[17] *Pilvilaskenta*. [viitattu 25.5.2014]. Saatavissa: http://fi.wikipedia.org/wiki/Pilvilaskenta

[18] Zaerens, K. FM, jatko-opiskelija, Maanpuolustuskorkeakoulu. Helsinki. Haastattelu, pilvipalvelut, 25.5.2014. Haastattelumuistiinpanot tutkijalla.

[19] *2009 Sidekick data loss*. [viitattu 25.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/2009_Sidekick_data_loss

[20] *Operation Aurora*. [viitattu 25.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/Operation_Aurora

[21] Appelbaum, J., *ym*. *NSA's Secret Toolbox: Unit Offers Spy Gadgets for Every Need*. 2013 Joulukuu 30, Spiegel International. [viitattu 25.5.2014]. Saatavissa: http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html

6.2.2.2 Mobiililaitteet

Kaupalliset mobiililaitteet ovat tällä hetkellä kehityksen moottori.[9] Sotilastietoliikennetekniikka on jäänyt jälkeen siviilitekniikan kehityksessä, koska siviiliteknologian tuotekehityspanokset ovat suuremmat ja kilpailu kovempaa siviilimarkkinoilla.[22] Vertaamalla uusimman älypuhelimen[23] ja sotilasradion[24] ominaisuuksia huomaa eron, vaikkakin sotilasradio toimii vaativissa ympäristöolosuhteissa esim. akunkesto pakkasella. Todennäköisesti tämä kehitys jatkuu tulevaisuudessa, koska siviilipuolen markkinat ja kehitysresurssit ovat suuremmat.[22]

Tässä luvussa käsitellään mobiililaitteita (esim. älypuhelimet, tabletit ja kannettavat tietokoneet) sovellusalustan näkökulmasta. DARPA Transformative Apps projektissa Yhdysvaltojen armeija kehittää ohjelmistosovellusten (engl. apps) sovelluskauppaa, josta sotilaat voivat ladata taistelukentän vaatimukset täyttäviä ohjelmistosovellutuksia älypuhelimiin ja tabletteihin.[25] Sovellutukset palvelevat erilaisia tarpeita taktisella taistelukentällä esim. raportointia, operaatioiden suunnittelua, tiedustelua, valvontaa, reaaliaikaista yhteistyötä, paikkatietoa, visualisointia, analyysia, kielen kääntämistä, koulutusta ja kuljetusten seurantaa. Android-käyttöjärjestelmä on sovellusten alustana, ja käyttöliittymäsuunnittelussa painotetaan yksinkertaisuutta ja helppokäyttöisyyttä. Jotkut sovellukset toimivat ilman verkkoyhteyttä, toiset taas tarvitsevat verkkoyhteyden, jonka täytyy kestää yhteyskatkoja. Ohjelman tavoitteena on turva-arkkitehtuuri taktiselle tasalle, joka on yhteensopiva kaupallisten mobiililaitteiden kanssa. Nykyisin monilla sotilailla ja reserviläisillä on älypuhelin, siksi konseptilla on valtava potentiaali.

Huolta ovat herättäneet muun muassa laitteiden katoaminen ja varastaminen, laitteiden ja tietojen hävittäminen käytön jälkeen, tietovuodot, armeijan tietojen luvaton käyttö sekä haittaohjelmien leviäminen mobiililaitteista armeijan verkkoon. Tuhannet yritykset kohtaavat samoja haasteita, kun työntekijät tekevät työtehtäviä omilla mobiililaitteilla. Tästä käytetään termiä engl. BYOD (bring your own device). Työntekijät käyttävät mobiililaitteita työssään joka tapauksessa, siksi tämä kannattaa huomioida yrityksen tietoturvakäytännöissä. Mobiililaitteista puuttuvat usein salasanasuojaus, tietoturvaohjelma sekä käyttöjärjestelmä- ja ohjelmistopäivitykset (alttiita hyväksikäytölle). Monesti mobiililaitteissa on luottamuksellisia tietoja, ja ne yhdistetään suojattuihin verkkoihin ilman valvontaa.[13] Mobiililaitteiden käyttäjien tunnistamiseen viranomaisverkoissa voidaan käyttää biometristä tunnistamista, mutta ongelmaksi muodostuu biometristen tunnisteiden vaihtaminen niiden joutuessa vääriin käsiin, mikä on mahdotonta (esim. sormenjäljen vaihtaminen).

Mobiililaite on yhteydenpitoväline sosiaaliseen mediaan (esim. Facebook), jossa henkilöt jakavat digitaalisia henkilötietoja, operaatioiden paikkatietoja ja valokuvia. Mobiilaitteissa on langaton yhteys, joka voi paljastaa sotajoukon sijainnin elektroni-

---

[22] Tegnelia J. (ym.). *The Strategic Direction For Army Science and Technology*. Department of the Army Army Science Board Directorate. Washington. 2013. [viitattu 25.5.2014]. Saatavissa: http://www.fas.org/irp/doddir/army/asb-strat.pdf

[23] *Galaxy S5*. [viitattu 25.5.2014]. Saatavissa: http://www.samsung.com/fi/consumer/mobile/mobilephones/smartphones/SM-G900FZWANEE

[24] *RF-7800V Handheld VHF Radio*. [viitattu 25.5.2014]. Saatavissa: http://rf.harris.com/capabilities/tactical-radios-networking/rf-7800v/

[25] *Transformative apps*. [viitattu 25.5.2014]. Saatavissa: http://www.darpa.mil/Our_Work/I2O/Programs/Transformative_Apps.aspx

sen tiedustelun avulla (esim. älypuhelin lähettää jatkuvasti tietoja tukiasemalle). Tulevaisuudessa mobiililaitteet ovat kasvava haaste turvallisuusvastaaville. Riskiä voidaan vähentää koulutuksella, laitteiden rekisteröinnillä, palomuureilla, haittaohjelmien estoilla, kunnollisilla salasanoilla tai muilla luotettavilla todentamismenetelmillä ja tiedostojen automaattisella hävittämisellä murtautumisyritysten jälkeen. Matkapuhelimet yleistyvät tulevaisuudessa taistelukentillä sotilaiden varustuksessa, mikä tekee niistä keskeisiä tekijöitä tulevaisuuden verkkotaistelussa.[26]

6.2.2.3 Laitteistojen takaovet

Takaovi on ohjelma, joka antaa hyökkääjän ohittaa järjestelmän normaalit turvallisuustarkastukset ja laskee tunkeutujan sisään järjestelmään tämän itsensä määrittämillä käyttöoikeuksilla.[27] Spiegel-lehden mukaan National Security Agency:n (NSA) vakoilusovelluksia on ollut mukana Samsungin, Western Digitalin, Seagaten ja Maxtorin laitteissa, Juniper Networksin palomuureissa sekä Ciscon, Dellin ja Huawein (!) verkkojärjestelmissä.[20] Takaovia voidaan nykyään kehittää viruskehittimillä, ja takaoven kehittäjä voi aina tarkistaa löytääkö virustarkistus sen. Siksi on suoraviivaista kirjoittaa uusi takaovi, jota virustarkistus ei tunnista. Virukseen voi myös liitää erilaisia näppäriä menetelmiä ohjelmakoodin muuttamiseksi, virustarkistusohjelman sormenjälkitietokannan tuhoamiseksi, ym. Käytännössä virustarkistus siis toimii siten, että tarkistusohjelma tunnistaa tunnetut virukset (oletus: virustarkistusohjelman päivitykset ovat kunnossa). Puolustusmenetelmässä on siis aukko; uudet hyvin tehdyt virukset pääsevät läpi. Virustorjuntaohjelmien tunnistuskykyä viruksia vastaan voi parantaa lisäämällä niihin heuristisia menetelmiä (esim. käyttäytymisen seurantaa ja arveluttavien komentojen etsimistä). Ei voida kuitenkaan olettaa, että ero normaalissa tai haittaohjelman toiminnassa olisi kovin suuri. Laaja tulkinta johtaa useampien haittaohjelmien havaitsemisen, mutta myös useampiin vääriin hälytyksiin. Vastaavasti tiukka tulkinta johtaa pienempään määrään virhehälytyksiä, mutta samalla myös useampia uusi haittaohjelma jää huomaamatta. Jos hyökkäys on kohdennettu niin tarkasti, että käytössä oleva virustorjuntaohjelmisto ja sen versio on hyökkääjän tiedossa, virustorjuntaohjelman tunnistuskyky haittaohjelmaa vastaan voidaan testata etukäteen.

Perinteisesti asevoimilla on ollut käytössä ns. Goverment Off the Shelf (GOTS) ohjelmistoja, mutta nykyisin suuntaus on Commercial Off the Shelf (COTS) ja/tai Open Source ohjelmistojen käyttö kustannuksien säästämiseksi. On hyvin vähän laitteistoja tai ohjelmistoja, jotka eivät sisällä ulkomaisia ohjelmistokirjastoja ja komponentteja.[13] Monimutkaisten laitteistojen todentaminen ja testaaminen on erittäin vaikeaa. Jokainen toiminto on tarkistettava, että laite toimii luvatulla tavalla ja siinä ei ole piilotettuja ominaisuuksia, jotka voivat aiheuttaa haittaa koko asejärjestelmälle tai sisältää piilotetun takaoven ja tuntemattomia haavoittuvuuksia. Takaovi voi olla piilotettuna mikropiireihin, joita on monissa ase- ja johtamisjärjestelmissä (viestiasemat, aselavetit jne.). Vihollinen voi aktivoida loogisen pommin, joka poistaa pelistä monet edistyneet ase- ja johtamisjärjestelmät.

---

[26] *IBM: Mobile Phone, Cloud Security Issues Can Impact IT*. [viitattu 25.5.2014]. Saatavissa: http://www.cio.com/article/678717/IBM_Mobile_Phone_Cloud_Security_Issues_Can_Impact_IT?page=1&taxonomyId=3089

[27] *Takaovi*. [viitattu 25.5.2014]. Saatavissa: http://fi.wikipedia.org/wiki/Takaovi

6.3 AHP-Kysely

AHP-mallin (ks. kuva 1) kriteerien ja vaihtoehtojen painokertoimet määritettiin parivertailuilla, joiden suorittajiksi valittiin Maanpuolustuskorkeakoulun sotatekniikan laitoksen asiantuntijoita. Kysely toteutettiin kyselylomakkeella, johon Sotatekniikan laitoksen kolme asiantuntijaa. Tarkennettu ohjeistus annettiin järjestettyjen kyselyjen yhteydessä. Kolmen asiantuntijan parivertailujen pisteet on yhdistettävä järkevästi, mihin analyyttinen hierarkiaprosessi suosittaa käyttämään geometristä keskiarvoa (ks. luku 6.1.2).

6.3.1 AHP-kyselyn tulokset

Expert Choice-tietokoneohjelman laskemat kriteerien ja vaihtoehtojen painokertoimet on esitetty kuvassa 3. Kolmen asiantuntijan vastausten perusteella kriteerien painoarvot muodostuivat seuraavasti:

- luottamuksellisuus 0,413 (41,3 %)
- eheys 0,26 (26 %)
- ja saatavuus 0,327 (32,7 %).

ja vaihtoehtojen painoarvot:

- pilvipalvelut 0,356 (35,6 %)
- laitteistojen takaovet 0,439 (43,9 %)
- ja mobiililaitteet 0,205 (20,5 %).

Luottamuksellisuus on tärkein CIA-mallin kriteeri 2020 (ks. kuva 3). Luottamuksellisuus on paljon esillä lehdistössä esim. Snowdenin tapaus.[21] Saatavuuden ovat nostaneet toiseksi tärkeämmäksi haasteeksi palvelunestohyökkäykset, joita on tapahtunut esim. Virossa[28] ja Georgiassa[29]. Palvelunestohyökkäyksiä on helppo toteuttaa ja niitä vastaan on vaikea täysin suojautua, siksi saatavuus on tulevaisuudessa toiseksi tärkein haaste. Eheyden painoarvo oli 26 %, koska eheyteen liittyviä hyökkäyksiä on ollut julkisuudessa vain vähän. Siksi niitä ei ehkä nähty tulevaisuuden uhkana.

Kriteerikohtaisesti tarkasteltuna asiantuntijat arvioivat mobiililaitteiden olevan suurin haaste kaikissa kriteereissä, pois lukien saatavuus, jossa pilvipalvelut olivat samoissa lukemissa (ks. kuva 4). Mobiiliympäristössä puuttuu usein keskitetty hallinta, ja käyttäjät hallitsevat laitteitaan pääkäyttäjän oikeuksin. Siksi suurin uhka eheydelle ja luottamuksellisuudelle ovat mobiililaitteet. Pilvipalvelut teoriassa mahdollistavat keskitetyn ja ammattitaitoisen tietoturvan, mutta käytännössä näin ei aina ole.[30] Pilvipalvelujen luottamuksellisuuteen liittyy ongelmia esim. sisäpiirin uhka (insider threat) ja valtioiden tiedustelu.[31] Laitteiston takaovista on vähän tietoa, siksi sen painoarvo oli pienin kaikissa kriteereissä. Laitteiston takaovet ovat uhka isoille organisaatioille, jotka ovat kohdistettujen hyökkäysten (advanced persistent threat, APT) kohteita.

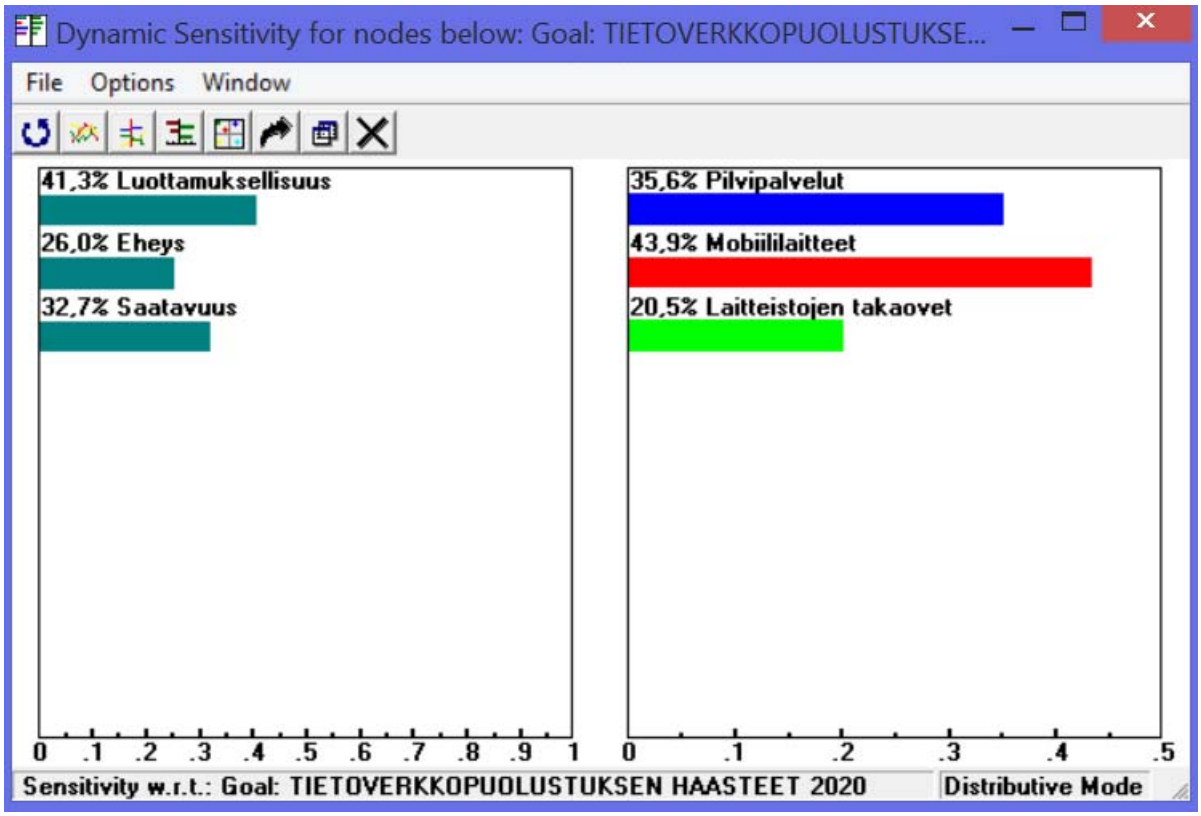
---

[28] *2007 cyberattacks on Estonia*. [viitattu 25.5.2014]. Saatavissa: http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

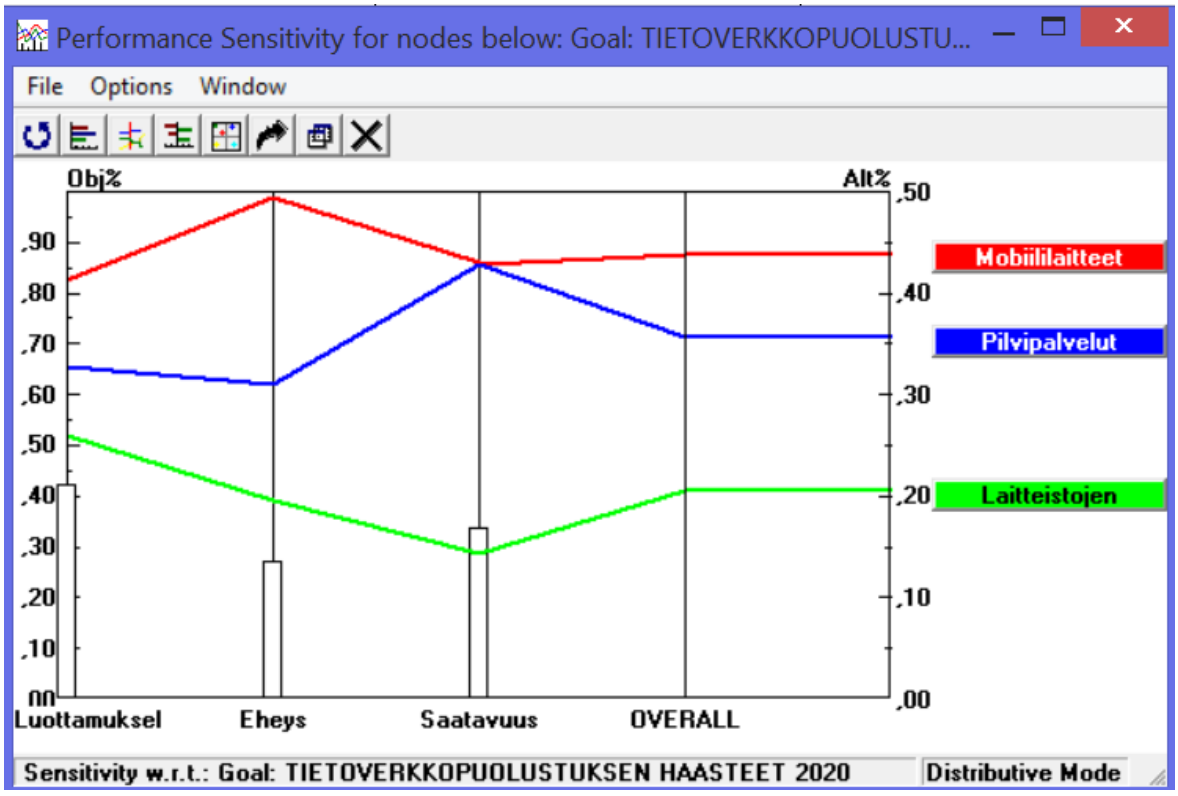
[29] *Cyberattacks during the Russo-Georgian war*. [viitattu 25.5.2014]. Saatavissa: http://en.wikipedia.org/ wiki/Cyberattacks_during_the_2008_South_Ossetia_war.

[30] Warr, P. *Evernote hacked, forces millions of users to reset their passwords*. 2013 Maaliskuu 13, Wired. [viitattu 25.5.2014]. Saatavissa: http://www.wired.co.uk/news/archive/2013-03/04/evernote-hacked

[31] Zetter, K. *Report: NSA Is Intercepting Traffic From Yahoo, Google Data Centers*. 2013 Lokakuu 30, Wired. [viitattu 25.5.2014]. Saatavissa: http://www.wired.com/2013/10/nsa-hacked-yahoo-google-cables/



Kuva 3. Kriteerien ja vaihtoehtojen painokertoimet



Kuva 4. Kriteerikohtainen tarkastelu

6.3.2 AHP-menetelmän luotettavuus

Preferenssivastaavuutta (ks. luku 6.1.4) tarkasteltaessa on muistettava, että tutkimuksessa vastaajina oli suppea ryhmä saman toimialan asiantuntijoita. Asiantuntijajoukon toimialatuntemus on merkittävää, valittavina olevien vaihtoehtojen erikoisasiantuntijuus ei ollut välttämättä syvällistä. Asiayhteyksien voidaan olettaa olevan näin suppealla CIA-mallin kriteeristöllä suhteellisen yhteneväiset, joten vastaajien todelliset preferenssit on mahdollista saada esiin. Preferenssivastaavuutta karsittiin kokeilemalla kyselylomakkeen käyttöä kyselyn ulkopuolisella asiantuntijalla ja korjaamalla kysymysasettelua epäselvissä kohdissa. Lisäksi asiantuntijoille annettiin vielä opastus kyselylomakkeen täyttöön henkilökohtaisesti, millä vähennettiin tärkeysjärjestysongelmaa ja range effect:iä (ks. luku 6.1.4).

Asiantuntijoiden ja heidän keskinäistä johdonmukaisuutta tarkastellaan hierarkian johdonmukaisuussuhteella (*CRH*), jonka arvoksi Expert choice -tietokoneohjelma palautti 0,06. Koska raja-arvo satunnaisuudelle on 0,1 (ks. luku 6.1.3), vertailun lopputulos on johdonmukainen. Tulevaisuuden ennustaminen on vaikeaa tietoverkkopuolustuksen haasteissa, siksi asiantuntijoiden painotuksissa oli eroja (johdonmukaisuussuhde ei ollut selvästi alle 0,1). Erot syntyivät jokaisen näkemysten, kokemusten ja intuitioiden vaikuttaessa vastausten painoarvoihin. AHP-kysely oli asiantuntijahaastattelu tietoverkkopuolustuksen haasteista 2020 sotilaallisessa kontekstissa (kapea erityisala), siksi otoskoko jäi suppeaksi (Sotatekniikan laitoksen kolme asiantuntijaa). Asiantuntijoiden määrän kasvattaminen ei välttämättä paranna merkittävästi ennustuksen osuvuutta tulevaisuudesta tällä nopeasti kehittyvällä alalla. Esim. asiantuntijoiden väärä paradigma aiheuttaa sen, että otoskokoon kasvattaminen ei paranna tuloksia, koska AHP-kyselyssä lasketaan geometrinen keskiarvo asiantuntijoiden parivertailujen vastauksista (ks. luku 6.1.2).

6.4 Johtopäätökset

Artikkelissa on esimerkillä osoitettu AHP-päätöksentekomenetelmän käyttökelpoisuus tietoverkkopuolustuksen haasteiden analyysissä. Luottamuksellisuus on tällä hetkellä CIA-mallin tärkein kriteeri ja hyvin todennäköisesti myös vuonna 2020. Palvelunestohyökkäyksiä on helppo toteuttaa ja niitä vastaan on vaikea täysin suojautua, siksi saatavuus on tulevaisuudessa toiseksi tärkein haaste.

AHP-kyselyssä suurimmat haasteet liittyivät mobiililaitteisiin. Palomuurit, haittaohjelmien estot, kunnolliset salasanat ja tiedostojen automaattinen hävittäminen murtautumisyritysten jälkeen parantavat mobiililaitteiden tietoturvaa. Organisaatioiden kannattaa myös salata mobiililaitteiden tiedot niin, että ainakin organisaation tärkeimmät tiedot pysyvät salaisina. Suurin heikkous on ihminen, ja organisaatioiden politiikan vastainen toiminta (tahallisesti tai tahattomasti).

Organisaatiot ottavat käyttöönsä koko ajan uusia pilvipalveluja ja -sovelluksia. Pilvipalvelujen tarjoajilla on teoriassa paremmat resurssit huolehtia tietoturvasta kuin yksittäisillä yrityksillä, koska he voivat jakaa kalliin ratkaisun kustannukset usealle tilaajalle. Ammattilaisten tekemät pilven turvapalvelut suojaavat organisaationverkostoja tehokkaammin kuin asiakkaiden omat toteutukset. Pilvipalveluiden käyttö on haaste organisaatiolle, koska palveluiden saatavuudessa täytyy luottaa monesti ylikansalliseen organisaatioon. Ongelmaa voidaan ratkaista yksityisellä pilvipalvelulla, mutta silloin menetetään ainakin osa kustannushyödyistä ja teoreettisesta rajattomasta kapasiteetista.

7.

Verkkotaistelu yritysten näkökulmasta

Johtaja Kari Wirman
FiCom, Huoltovarmuusorganisaation ICT-pooli
kari.wirman@ficom.fi, kari.wirman@kolumbus.fi

Tiivistelmä
Tämän artikkelin tarkoituksena on tarkastella verkkosodankäyntiä yritysten toiminnan kannalta. Kirjoituksessa on kuvattu yritysten turvallisuusasioihin liittyvää ajattelua, jonka perusteella yritykset lähestyvät myös kyberturvallisuutta ja sen toteuttamiseen läheisesti liittyviä tietoturvallisuusasioita.

7.1 Johdanto

Yksityinen sektori tuottaa monet nyky-yhteiskunnan toiminnan kannalta tärkeistä palveluista. Lisäksi kriittinen infrastruktuuri on lähes kokonaan yksityisessä omistuksessa. Tästä johtuen elinkeinoelämän ja osittain myös kolmannen sektorin (vapaaehtoissektori kuten esimerkiksi yhdistykset ja säätiöt) merkitys on kasvanut aikaisempaan verrattuna.

Tätä taustaa vasten on perusteltua olettaa, että Suomeen mahdollisesti kohdistuvien vihamielisten toimien kohteena tulee olemaan myös yksityisen sektorin toimijoita. Yritykset tulevat olemaan hyökkääjän kohteita, mikäli yrityksiin vaikuttamalla hyökkääjä kokee saavuttavansa omia tavoitteitaan. Mahdollisessa sodankäynnissä elinkeinoelämän toimijoihin kohdistuvat kybertoimet liittyvät todennäköisesti verkkotaistelun kybertaistelutekniikkaan ja -taktiikkaan.

Kirjoituksen ”piilotettu” pääviesti on seuraava: yritykset pyrkivät tilanteeseen, jossa riskienhallinnan keinoin määritelty ja saavutettu yrityksen toimintaan ja toimintoihin liittyvät jäännösriskit olisivat toiminnan kannalta tarkoituksenmukaisella tasolla – eivät liian suuria mutteivat myöskään liian pieniä.[1]

Jäännösriskin arviointia helpottaa se, että monet yritykset ovat normaalioloissakin ”taistelutilanteessa” niihin kohdistuvien tietoturvaloukkausten takia: tietoverkkojen kautta tapahtuvat ”koputtelut” ja erilaiset tunkeutumisyritykset ja hyökkäykset ovat varsin yleisiä – ”business as usual”. Vaikka näitä tietoturvaloukkauksia ja niiden yrityksiä ei pidä rinnastaa sodankäyntiin, ne kuitenkin palvelevat osaltaan puolustuskyvyn kehittämistä. Varsinaisista kybersotatoimista tämän päivät hyökkäykset poikkeavat todennäköisesti vain kahdella tavalla: (1) tekijä on ensisijaisesti joku muu kuin valtiollinen toimija ja (2) hyökkäysten intensiteetti on alhaisempi. Muilta osin tietojärjestelmiin kohdistuvat toimet vastaavat varsinaisia kyberhyökkäyksiä (hyökkääjän ammattitaito, menetelmät, jne.). Puolustuksen kannalta sillä ei liene merkitystä, poikkeavatko hyökkääjän lopullinen tavoite ja motivaatio nykytoimijoiden vastaavista.

[1] Haluan tässä yhteydessä korostaa, että jäännösriskiä ei suinkaan aina määritellä taloudellisin perustein, vaikka ne lienevätkin varsin vallitsevia.

Artikkelissa on ensin tarkasteltu yleisesti yritysten uhkamaailmaa mitenkään erityisesti korostamatta kyberuhkia, sillä niiden kohtelu yritysten riskienhallinnassa ei oleellisesti poikkea muiden merkittävien riskilähteiden käsittelystä – tärkeät asiat saavat aina ansaitsemansa painoarvon. Kyberhyökkäyksiä on kuvattu varsin lyhyesti niihin sen syvällisemmin tässä yhteydessä paneutumatta.

Artikkelin ehkäpä tärkein sisältö liittyy lukuun 7.3, jossa kuvataan käytännön kyberturvallisuustyötä. Vastuu kyberturvallisuudesta on jokaisella yrityksellä ja organisaatiolla itsellään, ja vain organisaatiolla itsellään: kukaan ei voi tuottaa toisen kyberturvallisuutta. Eri toimijoiden välillä tarvitaan yhteistoimintaa, jotta keskinäisriippuvuuksien yhteiskunnassa toimijoiden muodostamien verkostojen kyberturvallisuus olisi riittävällä tasolla. Kyberturvallisuusverkoston keskeinen tavoite on tukea ja auttaa verkoston yksittäistä toimijaa selviytymään mahdollisimman hyvin kyberuhkista sekä kyberhäiriöistä.

Tässä artikkelissa kuvatut yritysten menettelyt ja eri organisaatioiden yhteistoimintamallit ovat se pohja, johon yhteiskunnan kyberpuolustus osaltaan tukeutuu meihin kohdistuvan verkkosodan aikana.

7.2 Yrityksiin kohdistuvista uhkista ja riskeistä

Suomen kyberturvallisuusstrategian perustelumuistiossa todetaan seuraavasti: ”Nykyisin valtaosa kriittisestä infrastruktuurista ja sen palveluista on yksityisen sektorin omistamaa ja tuottamaa. Yritysten edellytyksiä huolehtia liiketoimintansa jatkuvuudesta kyberuhkatilanteissa parannetaan ja siten lisätään luottamusta niiden tuottamien hyödykkeiden saatavuuden jatkuvuuteen.”

Yrityksiin kohdistuu oikeushenkilöinä samoja uhkia kuin luonnollisiin henkilöihin ja muihinkin toimijoihin kuten viranomaisiin.

Kuvassa 1 yritykset on sijoitettu vuoden 2006 yhteiskunnan elintärkeiden toimintojen suojaamisen strategiassa kuvattuun suomalaisittain nähtyyn uhkakenttään. Kaikki kuvassa esitetyt uhat – niin kansalliset kuin kansainväliset – heijastuvat myös Suomessa toimiviin yrityksiin. Ne ilmenevät yritysten riskien hallinnassa muun muassa liike-, tuote-, sopimus- ja vastuu- sekä tietoriskeinä. Kaikki riskit edellyttävät niiden arviointia ja hallintaa, jotta riskit pysyvät toiminnan kannalta hyväksyttävällä tasolla.

Kuva 1. Yritykset ja yritystoiminnan riskit vuoden 2006 YETT-periaatepäätöksen uhkakentässä

Jokainen yritys harjoittaa muodossa tai toisessa riskien hallintaa. Riskienhallinnan prosessi ja sen systemaattisuus vaihtelevat toiminnan luonteesta ja laajuudesta riippuen, mutta jokainen yritys pyrkii hallitsemaan riskejään käytettävissään olevin tarkoituksenmukaisin keinoin.

7.2.1 Riskien hallinnasta

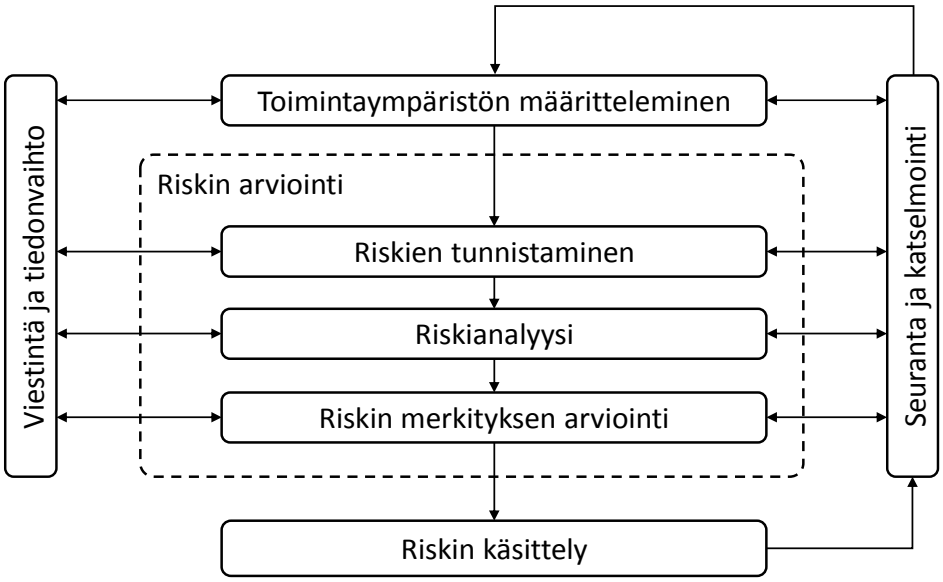
Riskienhallinta on seurauksiltaan merkittävien kielteisten tapahtumien (riskien) järjestelmällistä määrittelyä ja niihin varautumista. Merkittäviä riskejä ovat ne, joista tietoisuus vaikuttaa tai vaikuttaisi organisaation johdon päätöksentekoon. Riskienhallinta on prosessi, joka nivoutuu toimintoihin, joiden riskejä käsitellään.[2,3]

Usein väitetään, että kaikki mahdolliset uhkat voivat kohdistua mihin tahansa yritykseen samalla tavalla. Tällä perusteella kaikkien yritysten riskien pitäisi olla samanlaisia. Näin ei tietenkään käytännössä ole.

Uhkan ja riskin suhde on jokaisella yrityksellä erilainen, sillä yritysten toimintaympäristö luo perustan kyseisen yrityksen riskeille. Vaikka yritykset toimisivat jopa samalla toimialalla, niiden riskit eivät ole samanlaiset johtuen yritysten erilaisista toimintamalleista ja tavoista organisoitua niin sisäisesti kuin suhteessa niiden ympäristöön.[4]

---

[2] http://fi.wikipedia.org/wiki/Riskienhallinta, viitattu 3.7.2014.
[3] Riski voidaan nähdä myös mahdollisuutena eikä pelkästään kielteisenä ilmiönä kuten edellä kappaleen alussa annetaan ymmärtää.
[4] Katso Ahvenaisen systeemien käyttäytymistä koskeva luku.



Kuva 2. Riskienhallinnan prosessi (SFS-ISO 31000:2011)

Tietoihin liittyvät riskit kuuluvat luonnollisesti systemaattisen hallintamenettelyn piiriin. Näitä riskejä on totuttu lähestymään tietoturvaan liittyvinä riskeinä (Information Security => Cyber Security -riskeinä). Tätä perinteistä lähestymistapaa pyritään täydentämään[5] yhä enemmän sillä, mikä merkitys tai vaikutus tiedoilla, tietovarannoilla sekä niiden käsittelyyn tarkoitetuilla teknisillä tietojärjestelmillä on yrityksen toimintoihin. Tietoihin ja tietojärjestelmiin liittyvien riskien hallinnassa tulee korostumaan yhä enenevässä määrin tietojärjestelmille sekä niiden toiminnalle ja toimintavarmuudelle asetettujen vaatimusten määrittely ja vaatimusten toteutuminen käytännössä.

7.2.2 Tietoihin liittyvistä uhkista ja riskeistä

Tietoturvauhkien taustalla olevien tekijöiden tarkoitusperät voidaan jaotella monella eri tavalla.

Uhkakuvatarkasteluun vaikuttaa olennaisesti se, miltä toiminnan tasolta tarkastelu tehdään. Jos tarkastelu tehdään koko organisaation toiminnan kannalta, tulokset ja johtopäätökset poikkeavat täysin niistä, joihin päädytään tarkasteltaessa yksittäisen toimintaprosessin tai tietojärjestelmän uhkia. Jotta tarkastelu tekemisessä olisi jotain järkeä, keskeistä on valita ja määritellä tarkasteltava asiakokonaisuus tarkoituksenmukaisella tavalla.

Organisaation toiminnassaan käsittelemä tieto[6] (Ahvenainen on käsitellyt tarkemmin luvussa 1, mitä tieto on.) tulee ottaa lähtökohdaksi useimmissa kybertoimintaympäristöön liittyvissä uhkatarkasteluissa. Uhkien tarkastelu tiedon näkökulmasta auttaa organisaatiota määrittelemään tietojen suojaamisen kannalta tarkoituksenmukaiset menettelyt: mikäli tieto on tunnistettu, sitä mahdollisesti uhkaavat tekijät on mahdol-

[5] Esimerkiksi Suomen kyberturvallisuusstrategia pyrkii tähän.
[6] Tieto tarkoittaa tässä yhteydessä tieto kyberneettisen järjestelmän merkityksessä, jolloin tieto on järjestelmän kannalta merkityksellinen ero. Ero voi esimerkiksi olla anturilta saatu lämpötilatieto, säätölaitteen ohjaussignaali, asiakkaan henkilötunnus, ohjelmakäsky jne.

lista tunnistaa. Tämän jälkeen valitaan suojautumiskeinot[7] käyttäen hyväksi riskienhallinnan[8] yleisiä periaatteita ja käytänteitä.

7.2.3 Tietojärjestelmän turvallisuutta vai tietojärjestelmän avulla tuetun tai toteutetun toiminnan turvallisuutta

Tietojärjestelmiin liittyvien uhkien tarkastelun kannalta on tärkeää erottaa kaksi erilaista lähestymistapaa: tarkastellaanko uhkia (1) tietojen ja niitä käsittelevien tietojärjestelmien kannalta[9] tai tarkastellaanko uhkia (2) niiden toimintojen tai toimintaprosessien kannalta[10], joita tehostetaan tai jotka ovat tietotekniikan mahdollistamia uusia toimintamalleja.

Ensimmäinen vaihtoehto kuvaa lähinnä sitä toimintamaailmaa, jota on perinteisesti totuttu kutsumaan tietojärjestelmien tietoturvallisuudeksi ja siitä huolehtimiseksi (Information security, Cybersecurity). Jälkimmäinen taas liittyy ensisijaisesti erilaisten prosessien ja toimintojen varmistamiseen (Cybersafety). Ero on erityisesti tarkastelukulmassa ja -tavassa eikä niitä pysty täysin erottamaan toisistaan.

Tarkastelukulmat eroavat kuitenkin toisistaan merkittävästi. Toimintaprosessin[11] kannalta tehty tarkastelu pakottaa pohtimaan erilaisten tietojen merkitystä kyseisessä systeemissä. Tämä tarkastelutapa korostaa varsinaisen toimintaprosessin omistajan roolia.

Järjestelmien tietoturvallisuuteen liittyvä tarkastelu puolestaan painottaa järjestelmien toiminnan turvallisuudesta vastuussa olevien toimijoiden panosta.

Järjestelmän omistajat asettavat vaatimukset toiminnan turvallisuudelle (Cybersecurity) ja toteuttajien vastuulla on huolehtia siitä, että kyseiset vaatimukset toteutuvat käytännössä (Information Security, Cyber Security).

Kyberuhka tarkoittaa Suomen kyberturvallisuusstrategian mukaan mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon.[12] Strategian sisältö painottuu kyberturvallisuuden ”Cybersafety”-näkökulmaan. Tämä onkin luonnollista, sillä tietoturvallisuus on ollut agendalla jo pitkään.

---

[7] Control: countermeasure; means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature (ISO-IEC 27032:2012).

[8] Tähän voisi lisätä muutaman viittauksen joko standardeihin tai käytettävissä oleviin muihin työkaluihin (esim. pk-rh –sivustoon).

[9] Cybersecurity: Cyberspace security, preservation of confidentiality, integrity and availability of information in the Cyberspace, ISO-IEC 27032:2012.

[10] Cybersafety: condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable, ISO-IEC 27032:2012.

[11] Toimintaprosessin (useimmiten avoin systeemin, ks. Ahvenaisen luku).

[12] Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013.

7.2.4 Hyökkäysten motiiveista

Tietoihin ja tietojärjestelmiin pyritään vaikuttamaan monista eri syistä ja monien eri vaikuttimien takia.

Kyberhyökkäysten[13] tekijöiden vaikuttimet voidaan luokitella esimerkiksi seuraaviin ryhmiin:

- haitan aiheuttaminen
- haktivismi
- vakoilu (taloudellinen tai valtiollinen)
- taloudellisen edun hankkiminen

Useiden hyökkäysten tarkoituksena on pyrkiä aiheuttamaan haittaa teon kohteena olevalle taholle ilman varsinaista suurempaa ideologista tavoitetta. Keskeisenä vaikuttimena tekijällä on usein jännityksen tavoittelu tai pyrkimys ansaita arvostusta kollegoiden keskuudessa esimerkiksi osoittamalla kykenevänsä johonkin aikaisemmin tekemättömään (”proof of concept”).

Haktivismilla tarkoitetaan tietoverkossa tapahtuvaa toimintaa, jolla halutaan saada aikaan huomiota tai muutosta johonkin tiettyyn asiaan[14]. Haktivismia on esimerkiksi www-palveluun murtautuminen ja sen sotkeminen.

Vakoilun avulla tavoitellaan etua kilpailijan tai vastapuolen toimintaa selvittämällä. Yritysvakoilulla pyritään hankkimaan oikeudettomasti tietoa toiselle kuuluvasta yritys-salaisuudesta ja käyttämään sitä tavalla tai toisella omaksi hyväksi.

Valtioihin kohdistuva vakoilu on yleensä vieraan valtion lukuun tehtävää toimintaa, jonka tavoitteena on hyödyttää vierasta valtiota tai vahingoittaa vakoiltua valtiota hankkimalla tietoa kohteena olevan maan tärkeästä edusta tai toiminnasta.

Erityisesti järjestäytyneen rikollisuuden tavoitteena on taloudellisen edun tavoittelu erilaisiin tietojärjestelmiin ja niiden käsittelemään dataan[15] oikeudettomasti vaikuttamalla.

---

[13] Hyökkäyksellä tarkoitetaan tässä yritystä tuhota, paljastaa, muuttaa, estää, varastaa tai saavuttaa oikeudettomasti pääsy tai käyttää muutoin oikeudettomasti joko tietojärjestelmää tai sen käsittelemää dataa. (*attack*: attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset, ISO-IEC 27000:2014).

[14] http://fi.wikipedia.org/wiki/Haktivismi, viitattu 3.7.2014.

[15] *Datalla* tarkoitetaan sellaisessa muodossa olevien tosiseikkojen, tietojen tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon. Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU ”Tietoverkkorikosdirektiivi”.

7.3 Kyberhyökkäyksistä

7.3.1 Tietoverkkohyökkäyksen anatomia

Tietojärjestelmään kohdistuva hyökkäys noudattaa varsin pitkälti perinteiseen taisteluun valmistautumista. Kohdistettua hyökkäystä ei käytännössä koskaan tehdä sattumanvaraisin menetelmin, vaan toteutus on suurella todennäköisyydellä huolellisesti valmisteltu ja toteutus on tarkkaan harkittu jo edeltä käsin.

Tietojärjestelmään kohdistuvan hyökkäyksen päävaiheet ovat:
1. tiedustelu
2. tunkeutuminen
3. haittaohjelmien lataaminen ja asentaminen
4. tietoihin kohdistuvat toimet
5. jälkien hävittäminen

Tiedusteluvaiheessa (1) kohteesta kerätään eri menetelmin tietoja, joiden perusteella hyökkäyksen onnistumisen todennäköisyyttä parannetaan. Esimerkiksi internetin eri julkisista tietolähteistä on todennäköisesti saatavilla suuri määrä kohteeseen liittyviä tietoja. Ensisijaisesti tiedusteluvaiheessa pyritään selvittämään kohteen suojaustavat (preventive controls, detective controls).

Tunkeutumisvaiheen (2) tavoitteena on saada omaa ohjelmakoodia kohteen tietojärjestelmiin. Hyökkääjän toimintatavasta riippuen koodi saattaa jäädä passiiviseksi tai se saattaa aktivoitua. Aktivoiduttuaan ohjelmakoodi yleensä hakee varsinaista haittaohjelmakoodia ja asentaa sen kohdejärjestelmään (3).

Tämän jälkeen alkaa varsinainen tietoihin kohdistuva toiminta (4), joka saattaa liittyä kyseisten tietojen luottamuksellisuuteen, eheyteen tai käytettävyyteen. Hyökkäyksen tavoitteita ja vaikuttamisen eri tapoja on tarkasteltu tämän kirjan luvussa 1. Hyökkäyksiä tarkasteltaessa on tarpeen tehdä ero siinä, onko teon tavoitteena vaikuttaa pelkästään tietojärjestelmään ja sen dataan (pyritään esimerkiksi saamaan tieto salassa pidettävästä suunnitelmasta) vai onko varsinaisena kohteena tietojärjestelmän toiminnasta riippuva toiminto tai prosessi ja tietojärjestelmää käytetään niihin vaikuttamiseen (esimerkiksi Stuxnet, jolla pyrittiin vaikuttamaan kohdevaltion oletettuun kykyyn rikastaa uraania).

Viimeinen vaihe on yleensä hyökkäyksestä jääneiden jälkien siivoaminen (5), jotta hyökkäyksen ja sen tekijän selvittäminen olisi mahdollisimman vaikeaa ja hankalaa. Nämä toimet kohdistuvat yleensä erilaisiin järjestelmien lokitiedostoihin, jotka joko tuhotaan tai joiden sisältöä muutetaan. Jos hyökkäyksen paljastumisesta ei ole hyökkääjälle haittaa, äärimmäinen keino jälkien peittämiseen on koko kohdejärjestelmän ja sen kaikkien tietojen tuhoaminen palautuskelvottomaan muotoon.

7.3.2 Hyökkäykseen käytettävistä työkaluista

Kyberhyökkäyksen tekemiseen on lähes lukematon määrä erilaisia keinoja ja työkaluja, mikä oleellisesi vaikeuttaa puolustajan tehtävää. Tässä kirjoituksessa ei ole tarkoitus paneutua syvällisemmin erilaisiin hyökkäystekniikoihin.

Hoque et al. ovat kirjoittaneet erittäin kattavan verkkohyökkäyksiin sekä niiden toteuttamiseen ja hyökkäystyökaluihin liittyvän artikkelin nimeltä Taxonomy, tools and systems[16].

Kirjoittajat esittelevät artikkelissa hyökkäyksen eri vaiheissa käytettäviä työkaluja. Tekstin tärkein anti muille kuin tietotekniikan ammattilaisille lienee se, että lukija saa käsityksen siitä huimasta valmiiden keinojen valikoimasta, joka hyökkääjällä on käytettävissään.

Tämän kirjoituksen liitteeseen on poimittu lyhyet kuvaukset kolmesta eri hyökkäysmenetelmien luokittelujärjestelmästä. Taksonomioiden perusteella lukijan on mahdollista muodostaa kuva kyberympäristöön kohdistuvista uhkista ja hyökkäysmahdollisuuksista.

Kyberhyökkäysten luokitteluun ei ole yleisesti käyttöön hyväksyttyä luokittelua. Vuosien saatossa on esitetty useita eri luokitteluperiaatteita ja -menettelyjä, mutta mistään niistä ei ole muodostunut yleistä, tosiasiallista käytäntöä. Asiassa on myös syytä ottaa huomioon se, että aikaisemmin ei edes ole käytetty termiä *kyberhyökkäys*, vaan tietojärjestelmiin kohdistuneita hyökkäyksiä on kutsuttu – ja kutsutaan – nimellä *tietoturvaloukkaus*.

7.3.3 Tietojärjestelmien turvallisuuteen ja kyberturvallisuuteen liittyvästä materiaalista

Netti on täynnä erilaisia tietojärjestelmien turvallisuuteen liittyviä kirjoituksia[17]. Samaten erilaisia kirjoja asiasta löytyy runsain mitoin. Järjestelmien turvallisuuteen liittyvän tiedon puutteella tai tiedon hankalalla saatavuudella ei ainakaan mahdollisia turvallisuuspuutteita voi selittää. Ongelma onkin ehkä juuri päinvastainen: tietoa on ”liikaa” ja sen johdosta oleellisen erottaminen epäoleellisesta saattaa osoittautua hankalaksi.

7.4 Kyberturvallisuustyö käytännössä

Suomen kyberturvallisuusstrategian vision mukaan Suomi pystyy suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.

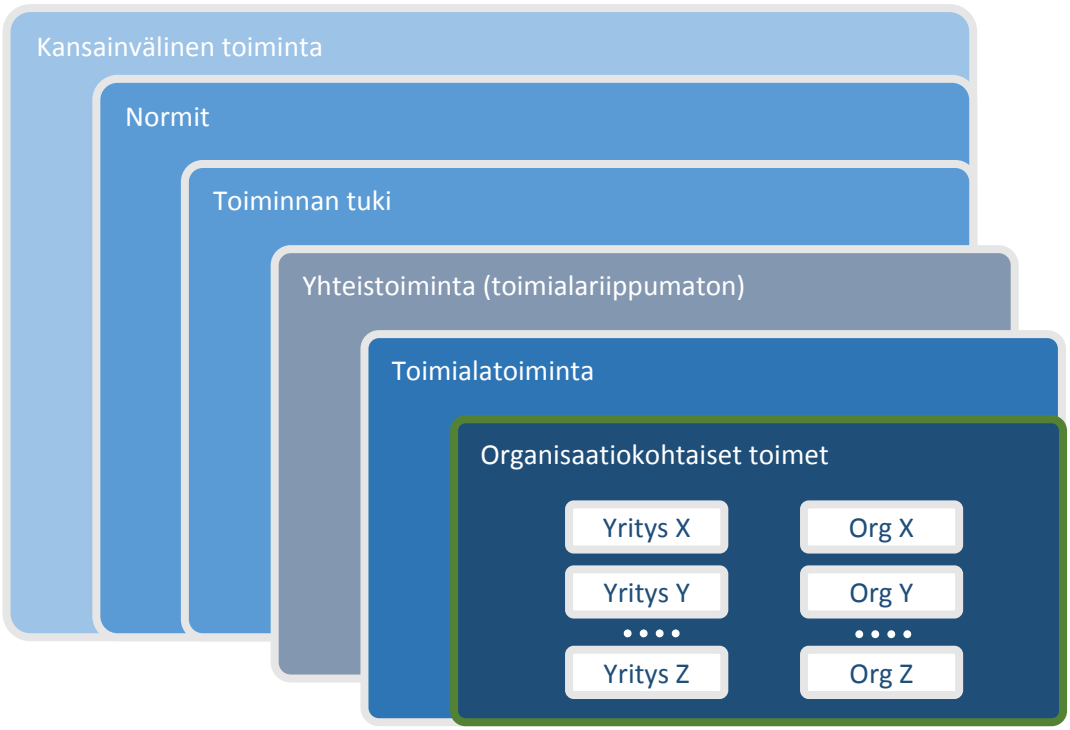
Visiossa esitetyn tavoitteen saavuttaminen edellyttää panostuksia usealla eri tasolla. Perusta onnistumiselle luodaan kussakin yksittäisessä organisaatiossa, jonka toimintaa tuetaan useilla eri tavoilla. Verkottunut toiminta ja erikoistumisen johdosta syntyneet verkottuneet toimintamallit myös edellyttävät yhteistoiminnan osapuolilta sitoutumista yhteisiin menettelyihin. Normisto toimii tässä keskeisenä välineenä. Lisäksi

---

[16] Hoque, Monowar H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, J.K. Kalita, Network attacks: Taxonomy, tools and systems, Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2013.08.001.
Tätä kirjoitettaessa viitatun artikkelin tarkistamaton käsikirjoitus on saatavilla verkko-osoitteesta https://acg6415.wikispaces.com/file/view/Journal+of+Network+and+Computer+Applications+2013+Hoque.pd. Viitattu 4.7.2014.

[17] Hyvä ja lyhyt yhteenveto tietojärjestelmien turvallisuuteen vaikuttavista tekijöistä löytyy esimerkiksi verkko-osoitteesta http://www.academia.edu/5203365/The_Current_Status_of_Network_Security_and_Forensics_ -Literature_Review_2013_-_Semester_One_PAPER_IT8417-Network_Security_and_Forensics_Post_Graduate_Diploma_Faculty_of_Business_and_Information_Technology_Lecturer. Kirjoitus sisältää myös kattavan koosteen lähdeteoksia. Viitattu 4.7.2014

toimijoiden on otettava myös huomioon kansalliset rajat ylittävät toimintaprosessit ja niihin liittyvät informaatiovirrat.



Kuva 3. Kyberuhkaa vastaan suojaudutaan usealla eri tasolla ja tavalla

7.4.1 "Kohdepuolustusta" eli yksittäisten organisaatioiden suojautumista

Jokaisen toimijan tulee huolehtia oman toimintansa turvallisuudesta. Käytännössä tämä tarkoittaa sitä, että yksittäisen organisaation on suunniteltava ja rakennettava omista lähtökohdistaan ja omaan riskihallintaansa perustuva turvallisuusratkaisu.

Lähtökohta on jälleen kerran riskienhallinta ja kyberturvallisuudesta puhuttaessa erityisesti yrityksen tai organisaation tietoihin kohdistuvien riskien hallinta.

Suomen kyberturvallisuusstrategia korostaa kybertoimintaympäristön turvallisuuden merkitystä (elintärkeiden) toimintojen suojaamisessa. Suojaamisen ensimmäinen askel on organisaation toiminnan kannalta kriittisen kyberympäristön tunnistaminen: mitkä tiedot ja tietojen järjestelmät ovat keskeisiä organisaation toiminnan kannalta? Tunnistaminen luo edellytykset kriittisten järjestelmien toimintavarmuuteen liittyvien vaatimusten määrittelylle ja asettamiselle. Vaatimusten ensisijainen tavoite on pyrkiä suojaamaan organisaation toiminta kybertoimintaympäristön mahdollisten häiriöiden vaikutuksilta.

Asetetut vaatimukset toteutetaan käytännössä tietoturvallisuuden hallintajärjestelmän mukaisin menettelyin. Hyviä malleja ja parhaita käytänteitä (best practices) turvallisuuden kehittämiseen ja ylläpitämiseen on lukuisia. ISO-IEC 27000 -sarjan tietoturvastandardeihin perustuvat hallintajärjestelmät ovat yleisesti käytössä.[18]

Sarjan standardien ohjeet ja suositukset liittyvät ensisijaisesti kunkin organisaation omien tietoturvamenettelyjen ja -rakenteiden ylläpitämiseen sekä kehittämiseen. Standardisarjaan kuuluu myös osia, jotka keskittyvät organisaation ja sen sidosryhmien väliseen tietojen ja tietojärjestelmien turvallisuuteen.

7.4.2 ”Aluepuolustusta” eli toimialan yhteistyötä

Useilla toimialoilla on tarkoituksenmukaista harjoittaa yhteistoimintaa erilaisissa kyberturvallisuuteen liittyvissä kysymyksissä.

Yhteistyö liittyy käytännössä toimialalla useampaan toimijaan kohdistuvien uhkien tunnistamiseen, tarkoituksenmukaisten suojautumiskontrollien valintaan ja kehittämiseen, hyökkäysten torjumiseen sekä hyökkäyksistä palautumiseen. Yhteistoiminta tähtää siihen, että toimialaverkoston kokonaisosaaminen tukisi mahdollisimman hyvin yksittäisen toimijan toimintaedellytyksiä yhteistä uhkaa vastaan.

Yhteistoimintarakenteista huolimatta vastuu käytännön suojautumisessa on aina viime kädessä yksittäisellä toimijalla.

7.4.3 ”Valtakunnan puolustusta” eli toimialarajat ylittävää yhteistyötä

Yhteiskunnan toimintojen keskinäiset riippuvuudet edellyttävät toimialarajat ylittävää yhteistoimintaa kybertoimintaympäristöön kohdistuvien hyökkäyksiin (eli useimmiten käytännössä tietoturvaloukkauksiin tai tietomurtoihin[19]) suojautumisessa ja niiden torjumisessa.

Viestintäviraston osana toimiva kyberturvallisuuskeskus toimii yhteistoimintaverkoston ytimenä. Keskus kerää verkostostaan tietoja erilaisista kybertoimintaympäristöön kohdistuvista uhkista, häiriöistä ja tietoturvaloukkauksista, analysoi saamiaan tietoja sekä jakaa tietoja verkostoonsa verkoston toimijoissa (organisaatioissa) hyödynnettäväksi päätöksenteon tukena.

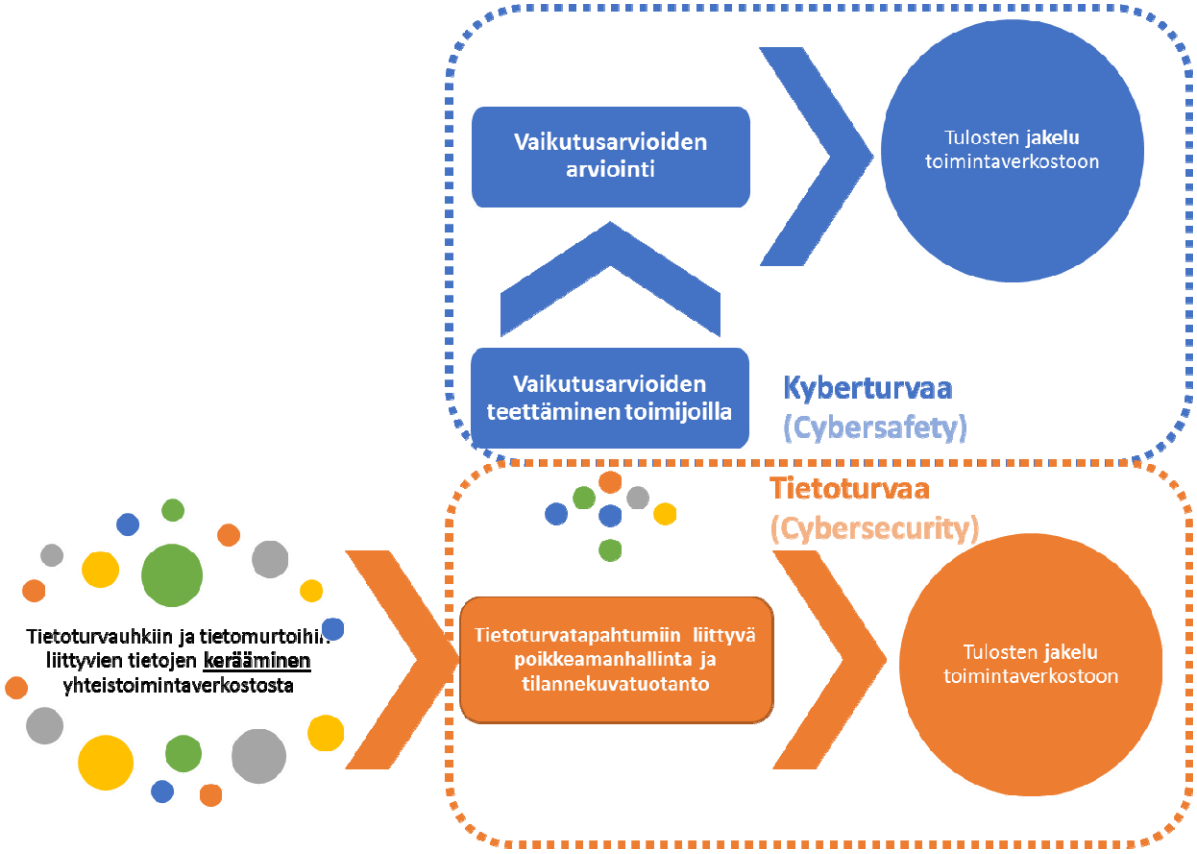
Kyberturvallisuuskeskuksen toiminta jakaantuu tässä tarkasteluyhteydessä kahteen: (1) tietoturvallisuustoiminnan tukemiseen sekä (2) kyberturvallisuuden edistämiseen tietoturvauhkien vaikutusarviointien avulla.

---

[18] Standardisarjasta ja sarjan standardien käytöstä on lisätietoa esimerkiksi verkko-osoitteissa https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en sekä http://www.27000.org/. Viitattu 15.8.2014.

[19] Tietomurto tarkoittaa tässä yhteydessä sellaista tekoa, jonka avulla joku tunkeutuu oikeudettomasti käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka murtamalla muuten turvajärjestelyn tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan. Tietomurto tarkoittaa myös sellaista tekoa, jossa tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla tai muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon tietojärjestelmässä olevasta tiedosta tai datasta. (Tietomurron kuvaus johdettu Euroopan parlamentin ja neuvoston direktiivistä 2013/40/EU eli ”Tietoverkkorikosdirektiivistä”).

Tietoturvallisuuden parantamiseksi kyberturvallisuuskeskus kerää yhteistoimintaverkostonsa jäseniltä tietoja tietoturvauhkista sekä mahdollisista tietomurroista. Keskus jalostaa tiedoista tietoturvallisuuteen liittyviä ohjeita ja yhteenvetoja verkostonsa jäsenten käyttöön ja verkostossa hyödynnettäväksi.



Kuva 4. Kyberturvallisuuskeskus tukee tietoturvallisuuden ja kyberturvallisuuden ylläpitoa sekä kehittämistä

Kyberturvallisuuden parantamiseksi keskus lähettää keräämiään tietoja yhteistyötahoilleen, jotta nämä laatisivat havaintoihin liittyviä vaikutusarvioita oman toimintansa tai toimialansa kannalta. Palautteena saamiensa arvioiden pohjalta kyberturvallisuuskeskus laatii arvioitavan ilmiön tai tapahtuman vaikutuksista koosteen – vaikutusarvioiden arvio, analyysien analyysin – jonka keskus toimittaa edelleen yhteistyötahojensa käyttöön. Kuva 4 pyrkii havainnollistamaan toimintamallien liittymistä toisiinsa.

7.4.4 Yhteistoiminnan tuki

Yhteistoimintaverkostot saattavat tarvita tukitoimintoja, joiden tarkoituksena on palvella kaikkia yhteistoimintaverkostoja niiden toimialoista riippumatta.

Tällaisia tukitoiminnoiksi kuvattavia toimijoita ovat esimerkiksi akateeminen maailma, erilaisia tietoturvapalveluja tarjoavat organisaatiot ja klusterit, jonkin teeman tai jonkin

tarkoituksen toteuttamiseksi perustetut organisaatiot kuten huoltovarmuusorganisaatio.

Tunnusomaista näille toimijoille on se, että niiden tarkoituksena on tukea omalla erikoisosaamisellaan ja palveluillaan muita toimijoita selviämään omista haasteistaan.

7.4.5 Normisto

Erilaiset normit muodostavat pohjan niin yksittäisen organisaation turvallisuustoimien toteuttamiselle kuin yhteistoiminnan harjoittamiselle. Normien merkitys korostuu sitä enemmän, mitä useampien toimijoiden tulisi noudattaa samoja periaatteita osana informaatioekosysteemiä, informaatioprosesseja tai toimintaverkostoa.

Normipakin raskain työkalu on lainsäädäntö ja sen nojalla annetut alemman asteiset säädökset. Pakissa on myös muita välineitä, joista mainittakoon erilaiset standardit (esimerkiksi tietoturvastandardit sekä korttimaksamiseen liittyvä PCI-standardi), viralliset ja epäviralliset käytännesäännöt (esimerkiksi best practices, huoltovarmuusorganisaation kyberturvallisuussuositukset ja muut julkaisut), yleisesti hyväksytyt toimintatavat (esimerkiksi netiketti), jne.

7.4.6 Kansainvälinen toiminta

Suomalainen yhteiskunta on nykyisin pitkälti integroitunut erilaisiin kansallisiin toimintaprosesseihin. Nämä prosessit tukeutuvat kybertoimintaympäristöön. Voitaneen väittää, että itse asiassa suuri osa kyseisistä ylikansallisista prosesseista on olemassa kybertoimintaympäristön luomien mahdollisuuksien johdosta.

Kansainvälinen toimintaverkosto, sen turvallisuus sekä verkoston jäsenten kesken harjoitettava yhteistoiminta on välttämätön kyseisen informaatioekosysteemin eri informaatioprosessien toimintavarmuudelle ja -kyvylle. Erilaiset uhka- ja häiriötilanteet asettavat verkoston ja sen jäsentenyhteistoimintakyvylle lukuisia vaatimuksia.

Edellä kuvatun perusteella voitaneen väittää, että ”puhdas impivaaralaisuus” on tullut tiensä päähän: Suomen tulee pysyä mukana kansainvälisissä järjestelmissä ja prosesseissa viimeiseen saakka eikä lähtökohtaisesti pyrkiä rakentamaan pelkästään Suomea palvelevia korvaavia järjestelyjä. Lentoliikenne käy hyvästä esimerkistä: sujuvan lentoliikenteen mahdollistamiseksi Suomen tulee pysyä osana kansainvälistä lennonohjausjärjestelmää. Vastaavalla tavalla maksuliikenne ei suju häiriöittä, mikäli yhteydet[20] kansainväliseen maksujenvälitysjärjestelmään eivät toimi.

7.5 Johtopäätöksiä ja kysymyksiä

Yritykset tulevat olemaan mahdollisessa verkkotaistelussa hyökkäysten kohteina. Mihin yrityksiin hyökätään, riippuu siitä, mikä on hyökkääjän tavoite: jos halutaan vaikuttaa esimerkiksi kansalaisten henkiseen toimintakykyyn, kohteena ovat sellaiset yritykset ja organisaatiot, joiden toiminnan häiriöt vaikuttavat eniten ihmisten sietokykyyn – talvella sähkön ja lämmön jakelu. Jos taas halutaan vaikeuttaa fyysisten vikojen korjausta, voidaan pyrkiä häiritsemään korjaajien pääsyä vikapaikalle esimerkiksi ruuhkauttamalla liikenne kaoottiseen tilaan sekoittamalla liikennevalojen ohjaus. Hyökkääjän käytettävissä oleva keinovalikoima on teoriassa lähes rajaton.

[20] Yhteydet tarkoittavat tässä laajempaa kokonaisuutta kuin pelkästään tietoliikenneyhteyksiä.

Hyökkäyksen kohteeksi joutumisen todennäköisyyttä kasvattaa toimijan yhteiskunnallinen merkitys: infrastruktuurit[21] ja niitä ylläpitävät toimialat tulevat olemaan ensisijaisia kohteita, sillä niiden kautta voidaan vaikuttaa laajasti koko yhteiskuntaan.

Yhteiskunta on systeemi, joka muodostuu osajärjestelmistä. **Voidaanko yksittäiseen osajärjestelmään (esimerkiksi yritykseen tai toimialaan) vaikuttamalla hajottaa ylätason systeemi (yhteiskunnan toiminta)?** Kysymys liittyy oleellisesti tässä artikkelissa tarkasteluihin kysymyksiin, sillä erilaisten yrityksille ja niiden toiminnalle verkkohyökkäysten keinoin aiheutettujen häiriöiden suorat ja epäsuorat kaskadiset vaikutukset saattavat olla vähintäänkin yllätyksellisiä. Tulokulma edellyttäisi lisätutkimista.

Tietoverkkojen kautta toimintoihin kohdistuvia uhkia ei voida millään menetelmillä täysin poistaa. 'Käytetään-tietotekniikkaa-hyväksi-kaikista-uhkista-huolimatta' -ajatuksen hyväksyminen ja siihen nojautuvan ICT-järjestelmien käyttöä koskevan lähestymistavan valinta takaa ICT:n käytön evolutiivisen kehittymisen edellytykset. Yksi ajattelumallin käytön seuraus on monimuotoisuuden lisäämisen kautta toimintojen kompleksisuuden lisääntyminen, jolloin hyökkääjän on entistä vaikeampaa vaikuttaa laajoihin kokonaisuuksiin. Hyvä esimerkki ajattelumallin tuloksesta on Internet: sen väitetään toimivan juuri siksi, että se on koko ajan rikki.

Verkkohyökkäyksiltä suojautumista ei voida rakentaa pelkän hyökkäysten torjunnan varaan. **Puolustuksen on perustuttava luonteeltaan erilaisiin kontrolleihin**[22]: pelote (deterrant controls), ennaltaehkäisy (preventive controls), havaitseminen (detective controls), reagointi ja toipuminen (reactive and recovery measures and tools) sekä korjaavat toimet (corrective measures).

Tietoverkkohyökkäysten havaitsemiseen liittyvien menettelyjen kehittäminen edellyttää merkittäviä lisäpanostuksia: uusia hyökkäysmenetelmiä (haavoittuvuuksien hyväksikäyttötapoja) keksitään jatkuvasti, jolloin niiden avulla toteutettujen tietoturvaloukkausten havaitsemisen merkitys korostuu – ainoastaan tunnetut hyökkäystavat on mahdollista estää kattavasti ja tunnetut haavoittuvuudet voidaan korjata.

Jokainen luvussa 7.4 kuvattu taso edellyttää omaa suojautumisen strategiaa, joissa alemmat tasot tukevat ja toteuttavat käytännössä ylemmän tason strategiaa. **Tärkein toimija on kuitenkin aina yksittäinen yritys tai organisaatio sen hallitessa omaa kyberturvallisuuttaan,** sillä koko verkoston toimintakyky riippuu aina tavalla tai toisella verkoston yksittäisten solmujen kyvykkyyksistä. Yksittäisen toimijan kyvyt ovat verkoston kannalta tärkeitä etenkin kahdesta syystä: ensinnäkin kaikki vihamieliset toimet kohdistuvat aina johonkin yksittäiseen kohteeseen, joita toki voi olla

[21] Valtioneuvoston päätös huoltovarmuuden tavoitteista (VNp 857/2013) määrittelee kriittisiksi infrastruktuureiksi seuraavat: energian tuotanto-, siirto- ja jakelujärjestelmät, tieto- ja viestintäjärjestelmät, -verkot ja -palvelut, finanssialan palvelut, liikenne ja logistiikka, vesihuolto, infrastruktuurin rakentaminen ja kunnossapito sekä jätehuolto.

[22] Kontrolli, engl. control (ISO/IEC 27000:2014(en)): measure that is modifying risk
Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.
Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

samaan aikaan useita), jolloin kyseisen kohteen havaitsemis- ja torjuntakyvystä riippuu paljon. Toiseksi hyökkääjä saattaa pyrkiä vaikuttamaan mieluummin verkoston huonommin suojattuun solmuun kuin hyvin suojattuun ytimeen ja saada onnistuneen sivustahyökkäyksen avulla aikaan toivomansa vaikutuksen koko systeemissä. Tätä voi havainnollistaa kysymyksellä: ”Miksi tunkeutua hyvin suojattuun ’ytimeen’, jos saman vaikutuksen saa aikaiseksi tunkeutumalla muutamaan huonosti suojattuun ’sensoriin’?”

Kokonaisuus ratkaisee. Kaikilla sodankäynnin tasoilla (strategia, operaatiotaito, taktiikka) riittävän kyvykäs voittaa, yhdellä tasolla kyvykkyys ei välttämättä takaa onnistumista. Suomen kyberturvallisuusstrategiassa esitetyn vision ja tavoitteiden saavuttamisen kannalta on tärkeää panostaa yhteistyöhön ja yhteiseen toimintamalliin perustuvaan kyberturvallisuuden ja kyberuhkien torjunnan edistämiseen. Aito yhteistoiminta luo edellytykset verkoston emergenssille.

Jokaisen toimijan on suojattava omat tietojärjestelmänsä kyberuhkia vastaan tarkoituksenmukaisella tavalla. Toteutus määräytyy edellä kohdassa 7.2.1 kuvatun hyväksyttävän jäännösriskin arvioinnin perusteella.

Jäännösriskin määrittelyyn liittyy merkittävä kysymys: **onko yksittäisen organisaation kannalta hyväksyttävä riski koko yhteiskunnan kannalta tarkasteltuna riittävän pieni?** Voiko siis syntyä tilanne, jossa organisaation toiminnan kannalta tarkoituksenmukainen ratkaisu olisi yhteiskunnan toimivuuden kannalta riittämätön? Vastaus kysymykseen ei ole yksinkertainen: jäännösriskin mitoittaminen aina nollaksi eli riskin poistaminen – kaiken tulee toimia aina ja kaikissa tilanteissa – on utopistinen ja kansantalouden kannalta kestämätön ratkaisu. Toisaalta kriittisten järjestelmien pettäminen saattaa romahduttaa muita järjestelmiä ennalta arvaamattomalla tavalla. Asia vaatisi lisäselvityksiä ja tutkimusta.

Luku 7/ Liite: Hyökkäysten luokittelusta

Kyberhyökkäysten luokitteluun ei ole yleisesti käyttöön hyväksyttyä luokittelua. Vuosien saatossa on esitetty useita eri luokitteluperiaatteita ja -menettelyjä, mutta mistään niistä ei ole muodostunut yleistä, tosiasiallista käytäntöä. Asiassa on myös syytä ottaa huomioon se, että aikaisemmin ei edes ole käytetty termiä *kyberhyökkäys*, vaan tietojärjestelmiin kohdistuneita hyökkäyksiä on kutsuttu nimellä *tietoturvaloukkaus*. Käytännössä on myös tarpeen tehdä ero siinä, onko teon tavoitteena vaikuttaa pelkästään tietojärjestelmään ja sen dataan vai onko varsinaisena kohteena tietojärjestelmän toiminnasta riippuva toiminto tai prosessi ja tietojärjestelmää käytetään niihin vaikuttamiseen.

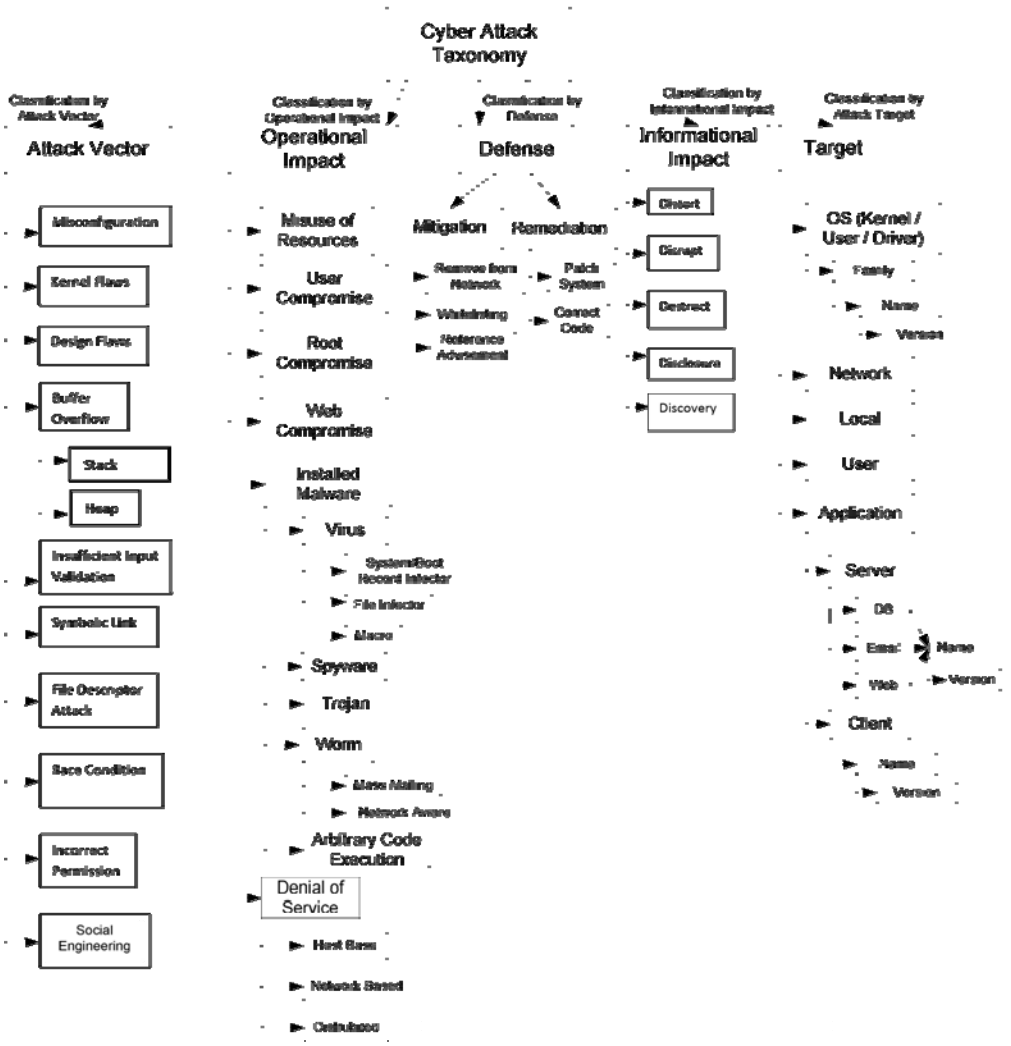
Hyökkäysmenetelmien luokittelusta on poimittu tähän mukaan lyhyet kuvaukset kolmesta eri luokittelujärjestelmästä. Taksonomioiden avulla on helpompi muodostaa yleiskuva erilaisista kyberympäristöön kohdistuvista uhkista sekä vaikutuskeinoista ja -mahdollisuuksista.

AVOIDIT: A Cyber Attack Taxonomy

Simmons et al.[23] ovat kehittäneet hyökkäysten luokittelujärjestelmän, joka perustuu viiteen hyökkäystä kuvaavaan tekijään. Ne ovat hyökkäyksen toteutustapa (**A**ttack **V**ector), hyökkäyksen vaikutus toimintaan (**O**perational **I**mpact), puolustautumistapa (**D**efense), hyökkäyksen vaikutus tietoon (**I**nformational Impact) ja hyökkäyksen kohde (**T**arget). Tekijöiden mukaan puolustautumistapa-luokittelutekijä on tarkoitettu helpottamaan tietojärjestelmien pääkäyttäjiä suojaamaan järjestelmänsä kyseistä hyökkäystä vastaan tai pienentämään hyökkäyksen aiheuttamaa haittaa.

Tekijöiden mukaan heidän kehittämänsä luokittelun avulla on mahdollista luokitella aikaisempia luokittelumenetelmiä helpommin eri hyökkäystapojen yhdistelmiä käyttävät hyökkäykset. Luokittelun avulla hyökkäys on myös mahdollista palastella, jotta hyökkäys ja sen toteutustapa olisi helpompi ymmärtää ja siten helpottaa suojautumisen suunnittelua ja toteutusta.

[23] Chris Simmons, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Qishi Wu, AVOIDIT: A Cyber Attack Taxonomy, University of Memphis, Department of Computer Science, http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf, viitattu 3.7.2014.



Kuva 5. AVOIDIT: A Cyber Attack Taxonomy

Luokittelu antaa hyvän ja havainnollisen kuvan hyökkääjän käytössä olevista lukuisista keinoista, joista hän voi valita tavoitteensa saavuttamisen kannalta parhaat.

ENISA
Euroopan unionin tietoturvavirasto ENISA esittelee omilla verkkosivuillaan eri CERT-ryhmien kehittämiä ja käyttämiä luokittelujärjestelmiä[24].

Virasto esittelee sivuillaan neljä eri luokittelutapaa. Ne poikkeavat toisistaan merkittävästi eikä virasto edes varsinaisesti suosittele mitään niistä yhteiseen ja yleiseen käyttöön.

Virasto perustelee verkkosivustollaan yleisellä tasolla jonkin luokittelujärjestelmän käyttöön oton tarpeellisuutta. Tärkeimpänä syynä virasto pitää muun muassa sitä, että ilman yhteistä (kansallista) luokittelujärjestelmää luotettavan tilastotiedon kerääminen ei käytännössä ole mahdollista.

[24] http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies, viitattu 3.7.2014.

A *taxonomy of network and computer attacks - Hansman & Hunt*
Luokittelujärjestelmistä kiinnostuneiden kannattaa tutustua artikkeliin[25], jossa Simon Hansman ja Ray Hunt esittelevät kehittämäänsä luokittelutapaa.

Artikkelissa esitetään myös varsin kattava katsaus aikaisempiin luokittelumenetelmiin.

Edellä kuvattu AVOIDIT-menetelmä perustuu osaltaan tähän Hansman et al. esittämään luokitteluun.

[25] http://ants.iis.sinica.edu.tw/3BkMJ9lTeWXTSrrvNoKNFDxRm3zFwRR/17/ attacks%20taxonomy.pdf, viitattu 3.7.2014.

8.

Maavoimat kybertaistelukentällä – Näkökulmia viidenteen sodankäynnin ulottuvuuteen

Everstiluutnantti Jukka-Pekka Virtanen ja majuri Janne Jokinen
Johtamisjärjestelmäosasto
Maavoimien esikunta

Everstiluutnantti Jukka-Pekka Virtanen työskentelee palvelupäällikkönä Maavoimien esikunnan johtamisjärjestelmäosastolla vastaten maavoimien käytössä olevista johtamisjärjestelmäpalveluista ja niiden kehittämisestä. Hän on palvellut aikaisemmin muun muassa Maavoimien esikunnan suunnitteluosastolla, viestipataljoonan komentajana, Liikenne- ja viestintäministeriön yhteysupseerina, Viesti- ja sähköteknisen koulun apulaisjohtajana, viestitaktiikan opettajana Maanpuolustuskorkeakoulussa, osastoesiupseerina Maavoimaesikunnan viestiosastolla sekä joukkueenjohtajana ja varapäällikkönä Reserviupseerikoulun Viestikomppaniassa. Viestiaselajin ja johtamisjärjestelmäalan tehtävien ohessa Virtanen on ollut kehittämässä informaatio- ja johtamissodankäynnin kokonaisuutta, joka käynnissä olevassa muutoksessa on painottunut yhä vahvemmin kyberpuolustuksen eri osa-alueisiin. Hän on kirjoittanut useita johtamisjärjestelmäalaa, viestiaselajia ja tietoverkkosodankäyntiä käsittelevää artikkelia erilaisiin maanpuolustuksen ja turvallisuusalan julkaisuihin.

Majuri Janne Jokinen työskentelee tietoturvallisuus- ja tietohallintosektorin johtajana Maavoimien esikunnan johtamisjärjestelmäosastolla. Hän vastaa maavoimien tietoturvallisuudesta, tietohallinnosta ja kyberpuolustuksen suorituskykyjen kehittämisestä. Aikaisemmin hän on palvellut Karjalan prikaatissa viestipataljoonan pataljoonaupseerina ja toimistoupseerina sekä pitkäaikaisesti perusyksikön varapäällikön ja päällikön tehtävissä. Jokisen aikaisempi kokemus esikunta- ja viestijoukkojen johtamisesta ja niiden käytössä olevista johtamisjärjestelmistä tuo käytännön läheisen näkökulman kyberpuolustuksen suorituskykyjen kehitystyöhön.

Tiivistelmä
Arvioidaan, että kybersodankäynti tulee olemaan suurempi vallankumous kuin mitä ruuti ja ilma-aseet olivat aiemmissa sodissa. Päätähuimaavasta teknologiakehityksestä ponnistavana se voidaankin perustellusti luokitella uudeksi sodankäynnin ulottuvuudeksi, joka kaikkien vakavasti otettavien armeijoiden on omissa kehittämisohjelmissaan huomioitava. Vahva viesti uhkan olemassa olosta ja vaikutusmahdollisuuksista niin vastapuolen päätöksentekoon kuin varsinaisiin sotatoimiinkin välittyy tarkastelemalla esimerkiksi Georgian tai Ukrainan tapahtumia. Vaikka kyberulottuvuutta ei olekaan viety maavoimien uudistetun taistelun keskiöön, ei se tarkoita sitä, etteikö kyberuhkaa olisi huomioitu. Maavoimien taistelu 2015:n tueksi kehitettävien johtamis- ja asejärjestelmien teknisten ja rakenteellisten ratkaisuiden ohella kyberpuolustuksellinen tarkastelu on perusteltua ulottaa myös verkkojen ja järjestelmien ulkopuolelle. Tällöin keskeiseen asemaan nousevat koulutus, ohjeistus, toimintatavat, johtaminen, yhteistoiminta ja asenteet.

8.1 Taistelu verkoissa – maapuolustuksen uusi elementti?

Puolustusvoimat on entistäkin vahvemmin sidoksissa yhteiskunnan suorituskykyihin. Tietotekninen kehitys on tehostanut toimintaa ja mahdollistanut asioita, jotka entisaikoina kuuluivat lähinnä tieteiselokuviin – mielikuvituksen ollessa rajana. Tänä päivänä on toisin. Järjestelmät linkittyvät toisiinsa ja kokonaismaapuolustuksen viitekehyksessä raja yhteiskunnan eri toimijoiden ja puolustusvoimien välillä hämärtyy. Syventyvä järjestelmäintegraatio hyödyntää yhteisiä tekniikoita ja palveluita, joiden käyttöä todellisuudessa vain pääsyoikeudet rajoittavat – jos nekään. Samalla tietotekninen riippuvuus on lisännyt yhteiskunnan haavoittuvuutta, jonka kriittisyyttä lisäävä kehityskulku linkittää kansallisen puolustuksen lisääntyvässä määrin laajempiin kansainvälisiin turvallisuusrakenteisiin. Verkkojen kautta suunnattuja uhkia onkin yhä vaikeampi torjua pelkästään perinteisiä organisaatio- tai valtiorajoja noudatellen.

Tehokkuusajattelusta ja ydintehtäviin keskittymisestä seuranneet ulkoistamiset ja kumppanuudet ovat lisänneet keskinäisriippuvuutta ja samalla myös kyberturvallisuuden merkitystä. Mikäli tieto ei liiku, ei myöskään tavara tai ihmiset liiku, eikä esimerkiksi tykistö ammu tai muonatäydennys tavoita etulinjassa taistelevaa komppaniaa. Kyberturvallisuuteen on suhtauduttava vakavasti ja meidän on kehitettävä kykyämme toimia uudessa ulottuvuudessa. Meidän kriittisiin toimintoihimme kohdistuvan tiedustelun lisäksi kyberuhkia ovat tietomadot, virukset ja haittaohjelmat sekä varsin tutuiksi käyneet palvelunestohyökkäykset, joiden aiheuttamat hidasteet tuotantoprosesseissa ja logistiikkaketjuissa voivat olla merkittäviä. Sotatoimissa tietoverkkosodankäyntiin kytkeytyy vahvasti myös fyysinen vaikuttaminen – siis järjestelmien ja niiden avainosaajien tuhoaminen asein ja pommein. Helpohkon saatavuutensa johdosta on tuhovoimaisia kyberaseita armeijoiden ja muiden ”virallisten” tahojen lisäksi myös erilaisten epävirallisten ryhmien hallussa, mistä johtuen verkkoja hyödyntävän ”haktivismin” ja rikollisuuden uhka on yhä merkittävämpi. Toisaalta kyberympäristö muuttaa myös mahdollisuuksiamme kerätä esimerkiksi ennakkovaroituksessa tarvittavia tietoa, koska aikaisemmin perinteisillä menetelmillä kerätyt tiedot ovat siirtyneet tietoverkkoihin.

Puolustusvoimauudistuksen vanavedessä maavoimat uudistavat taistelutapaansa, jossa lähtökohdat ovat varsin perinteisissä uhkamalleissa. Koko maata puolustetaan – edelleenkin. Toki uusia elementtejä on mukana, joihin muun muassa kybersodankäynnin suorituskyvyt luetaan. Vähemmistä joukoista on saatava aina ja aina vain enemmän tehoa, jota uudistetulla joukkorakenteella sekä kehittyvillä johtamis-, tiedustelu- ja asejärjestelmillä pyritään optimoidusti tukemaan. Sotakokemukset ja erityisesti suomalaisen sotilaan vahvuudet viedään keskiöön. Uudistetussa taistelussa pyritään aktiivisuuteen ja joustavuuteen, jossa hyödynnetään koko taistelutilan syvyyttä. Materiaalihankinnoilla korvataan elinkaarensa päässä olevien järjestelmien suorituskykyjä, mutta massan ollessa suuri jää sodan ajan joukoilla mittava määrä myös vanhaa kalustoa käyttöön.

Maavoimallisten toimintatapojen uudistaminen edellyttää johtamisjärjestelmän ohella myös johtamisen ja toimintatapojen kehittämistä. Komentajien on kyettävä johtamaan taistelussa hajallaan olevia joukkojaan taktisen johtamisjärjestelmän tiedoilla ja palveluilla, joihin alajohtoportaan ja aselajien taistelujohtojärjestelmien on kyettävä joustavasti ja taistelunkestävästi liittymään. Näin komentaja voi ottaa johtamisprosesseihinsa alaistensa lisäksi myös tukevat ja tuettavat sekä kaikki muut taistelutilassa toimivat osapuolet. Taistelukonseptin toimeenpanossa johtamisjärjestelmät ovat

merkittävässä asemassa ja voidaan perustellusti todeta, ettei uudistetun taistelutavan toimeenpano onnistu ilman johtamisjärjestelmämuutosta. Uudistetun taistelutavan ohjaamana kehitetään voimallisesti Maapuolustuksen johtamisjärjestelmä M18:aa (MAPUJOJÄ M18) alhaalta ylöspäin ryhmä- ja joukkuetasalta alkaen painopisteen ollessa maavoimien perusyhtymissä eli taisteluosastoissa.

Johtamisjärjestelmien tärkeys nostaa kybersodansodankäynnin elementit aivan uuteen asetelmaan. Kiihtyvän teknologiakehityksen ja lyhenevien elinkaarien rinnalla haasteen tai miksipä ei jopa mahdollisuuden juuri verkkosodankäynnin näkökulmasta tuovatkin uusimuotoisten taisteluosastojen rinnalle jäävät vanhemmalla kalustolla varustetut joukot, joita maavoimien sodan ajan vahvuudessa säilyy varsin mittava määrä. Toinen, ehkä vieläkin mielenkiintoisempi näkökulma syntyy Pääesikuntajohtoisista yhteisen vaikuttamisen resursseista, jotka näyttelevät merkittävää roolia erityisesti sotatoimien ratkaisuvaiheissa. Tämä korostaa myös puolustushaarojen välistä yhteistoimintaa, joka sekin perustuu lähes täysin verkkoihin sekä järjestelmien ja laitteiden yhteentoimivuuteen. Myös kehitystyön kohteena oleva paikallispataljoonakonsepti tuo kehittämiseen uudenlaista haastetta.

Viestijärjestelmien näkökulmasta on tietoverkkosodankäynnin toimintaympäristössä tapahtunut muutakin kuin pelkkää teknistä kehitystä. Vielä viime sodissa vallitsi vahva viestiyhteyskeskeinen ajattelumalli. Sotien jälkeisinä vuosikymmeninä siirryimme materiaalitilanteen kehittyessä verkkoajatteluun, jolloin tosiasiallisesti elementit verkko-operaatioihin alkoivat pikku hiljaa syntyä. Viestitoiminnan rinnalla kehittyi myös elektroninen sodankäynti, joka alkuaan keskittyi radioyhteyksien kuunteluun ja tulkintaan laajentuen aikojen saatossa myös vaikuttamisen osa-alueille. Elektronista sodankäynti voidaankin hyvällä syyllä pitää verkkosodankäynnin esiasteena. Teknisen kehityksen edetessä verkkoajattelu muuttui yhtymän viestijärjestelmähankintojen siivittämänä järjestelmäajatteluksi. Verkkoja ja järjestelmiä oli ryhdyttävä valvomaan, joka tietotaidon ja tekniikan kehittyessä avasi mahdollisuuden myös verkkojen avulla tapahtuvaan vastustajan johtamisjärjestelmien tiedusteluun ja häirintään. Kehitystyön kohteena oleva Maapuolustuksen johtamisjärjestelmä M18 jatkaa valittua kehityskulkua tarjoten uusia mahdollisuuksia niin puolustajalle kuin hyökkääjällekin.

Verkkoulottuvuus on siis läsnä kaikessa toiminnassa, lävistäen erilaiset rajapinnat ja ulottuen käytännössä etulinjan taistelijasta korkeimpiin esikuntiin ja niissä toimiviin sodan johtajiin. Tietoliikenteen, järjestelmien ja ohjelmistojen lisäksi tietoverkkosodankäynnin kohteena ovat niin ylläpitäjät kuin käyttäjätkin. Järjestelmiin tunkeutuminen ja haittaohjelman asentaminen on mahdollista yhtälailla normaali- kuin poikkeusoloissa. Haittaohjelman tai viruksen syöttäminen järjestelmiin voi tapahtua tahallisesti, mutta myös inhimillisen virheen tai selkeän laiminlyönnin seurauksena. ”Saastuneet” järjestelmät eivät toimikaan halutulla tavalla – tykistö ei ammu tai ampuu pahimmassa tapauksessa haittaohjelman saastuttamalla maalitiedolla omia joukkoja!

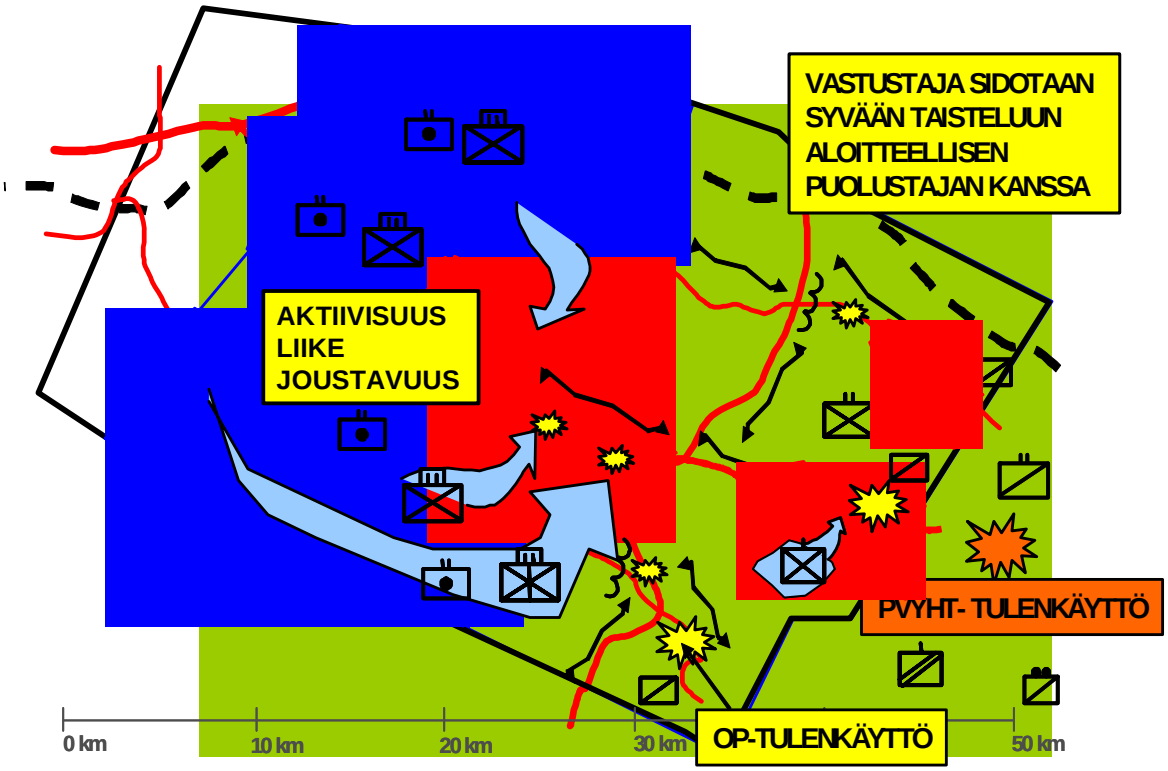
Pohdintoihin nouseekin kysymys: Mitä on suomalainen tietoverkkosodankäynti tai kyberpuolustus? Kopioimmeko edelleenkin suurvaltojen toimintamalleja sellaisenaan, jotka aktiivisimmat pyrkivät lähes väkipakolla jalkauttamaan meikäläisiin toimintamalleihin. Toki tässä on paljon hyvääkin – ”pyörää ei kannata keksiä uudelleen” ja ”rusinat kannattaa kerätä pullasta”, mutta tunnistamme myös uhkan, jossa juuri kansallisista lähtökohdista ja ennen muuta resursseista tehty kriittinen tarkastelu jää liian vähälle. Muutoksessa keskeisintä onkin ymmärtää, mihin muutos perustuu ja mitkä

ovat muutoksen edellytykset. Jos kansainvälinen malli täyttää kansallisen ympäristön vaatimukset, ei periaatteessa ole syytä hylkiä myöskään suurvaltojen uusia konsepteja. Kansallisesti onnistumisen edellytyksenä on huolellisesti rakennettu vastuunjako ministeriön, Pääesikunnan ja puolustushaarojen välillä.

8.2 Maavoimien taistelu 2015 - uusia vaatimuksia johtamisjärjestelmälle

Uudistetun maapuolustuksen tavoitteena on tuottaa vastustajalle sellaiset tappiot, että sen hyökkäysvoima tyrehtyy. Tulevaisuuden taistelukentällä joukkojen vastuualueet kasvavat ja taisteluja käydään syvemmällä alueella - koko taistelutilassa. Maavoimien on toteutettava sille käsketty tehtävä vähemmillä, mutta suorituskykyisemmillä ja eri taistelulajeja monipuolisesti hyödyntävillä joukoilla. Tavoitteidensa tueksi maavoimat uudistavat taistelutapaansa. Maavoimien taistelu 2015 on hyökkäyksestä, puolustuksesta ja viivytyksestä muodostuva kokonaisuus, jolla kulutetaan, lyödään tai tuhotaan vihollinen. Uudistettu taistelutapa yhdistää monia käytössä olevia taktisia periaatteita korostaen kaavamaisuuden ja jäykän puolustustaktiikan sijasta aktiivisuutta, aloitteellisuutta, liikettä ja joustavuutta.

Maavoimien taistelu 2015 uudistaa organisaatioiden, materiaalin ja johtamisen ohella erityisesti alueellisten joukkojen käyttö- ja toimintaperiaatteita. Se perustuu alueellisten joukkojen vaikuttamiskykyyn, johon yhdistyvät operatiivinen tulenkäyttö hyökkääjän syvyyteen sekä operatiivisten joukkojen käyttö tilanteen vakauttamiseksi ja aloitteen tempaamiseksi. Taistelua tuetaan raja- ja paikallisjoukoilla. Uudistettu taistelutapa korostaa taistelutilan valmistelujen merkitystä, joita joukot tekevät muokatakseen taistelutilaa omalle toiminnalle edulliseksi ennen taistelua, taistelun aikana ja vielä taistelun jälkeenkin. Linnoittamisen ja suluttamisen lisäksi siihen sisältyy muun muassa materiaalin hajauttaminen, tiestön käyttö, johtaminen sekä salaaminen ja harhauttaminen. Vaikutuskeskeisyys korostuu, joka on maavoimien joukkojen ja asejärjestelmien koordinoitua käyttöä puolustusvoimien yhteisten suorituskykyjen sekä muiden puolustushaarojen tukemana.



Kuva 1. Maavoimien taistelu 2015 perustuu syvään vaikuttamiseen ja suorituskykyjen optimoituun käyttöön.

Maaoperaatioissa käytettäviä yleisiä taktisia periaatteita ovat aktiivinen ja päättäväinen toiminta, yllätykseen pyrkiminen, olosuhteiden ja maaston hyväksikäyttö, voimien vaikutuksen keskittäminen, voimien taloudellinen käyttö ja vaikutusperusteinen operointi. Maaoperaatioiden suunnittelua ja toimeenpanoa ohjataan toteutusperiaatteilla, joita ovat vaikutuskeskeisyyden lisäksi aktiivisuus ja tavoitteellisuus, monipuolisuus, ennakointi, synkronointi ja ketteryys. Maavoimien suorituskykyjen käytettävyyttä säädellään valmiuden säätelyjärjestelmällä tilanteenmukaisesti. Valmiuden kohottaminen käynnistetään normaaliolojen voimavaroilla ja valtuuksilla, joita vahvennetaan tilanteen edellyttämällä tavalla käyttöön saatavien valmiuslainsäädännön toimivaltuuksien perusteella.

Maapuolustuksen joukot jaetaan käyttöperiaatteensa mukaan operatiivisiin, alueellisiin ja paikallisjoukkoihin. Operatiivisia joukkoja käytetään sotilaallisen voimankäytön ennaltaehkäisyyn, yllättävien tilanteiden hallintaan ja ratkaisutaisteluissa painopisteen muodostamiseen sekä hyökkääjän lyömiseen ensisijaisesti osana yhteisoperaatiota. Alueellisilla joukoilla luodaan maapuolustuksen valtakunnallinen kattavuus. Niillä suojataan puolustusvalmisteluja ja luodaan edellytykset operatiivisten joukkojen toiminnalle. Alueellisilla joukoilla sidotaan hyökkääjä taisteluun, kulutetaan sen taisteluvoimaa, suojataan tärkeitä kohteita ja estetään hyökkääjän pääsy strategisesti tärkeille alueille. Paikallisjoukkojen tehtävinä ovat joukkojen perustaminen, kohteiden ja henkilöiden suojaaminen, valvonta ja vartiointi, joukkojen perustaminen ja täydennyskoulutus sekä virka-apu muille viranomaisille. Paikallispuolustuskonseptissa vapaaehtoinen maanpuolustuskenttä kytketään entistäkin vahvemmin sotilaallisten suo-

rituskykyjen kehittämiseen. Joukot jaetaan valmiusvaatimusten mukaan valmiusjoukkoihin, pääjoukkoihin ja erikseen perustettaviin joukkoihin.

Alueelliset joukot organisoidaan pääosiltaan taisteluosastoiksi, joiden organisaatio ja erityisesti sotavarustus räätälöidään tehtävien edellyttämällä tavalla. Puolustavan taisteluosaston taistelukyky muodostuu eri aselajien tukemasta komppanioiden taistelusta ja näin saatavasta yhteisvaikutuksesta. Taistelu perustuu jalkaväen käsiaseiden, panssarintorjunta-aseiden, sulutteiden ja epäsuoran tulen käyttöön, joka kulminoituu entistäkin enemmän yksittäisen taistelijan tilannetietoisuuteen. Hajautettuun taisteluun tarkoitettu jääkäripataljoona taistelee laajalla ja syvällä alueelle partio-, joukkue- ja komppaniakokonaisuuksina tehden ylläköitä ja iskuosastoiskuja. Hyökkäykseen tarkoitetun taisteluosaston suorituskyky muodostuu panssaroitujen ajoneuvojen liikkuvuudesta ja jalkaväen lähitaistelukyvystä, jota tuetaan muilla aselajeilla. Operatiiviset joukot ovat edelleen maavoimien suorituskykyisimpiä joukkoja ja niillä luodaan taisteluiden painopiste. Operatiivisiin joukkoihin kuuluu muun muassa jääkäriprikaateja, mekanisoituja ja moottoroituja taisteluosastoja, helikopteripataljoona ja erillisyksiköitä.

Maavoimien taistelu 2015 muuttaa myös tiedustelun tehtäväkenttää ja asettaa uusia vaatimuksia toimintaympäristö- ja tilannetietoisuudelle. Tieto on voiman moninkertaistaja. Oma toiminta on pystyttävä muuttamaan reagoivasta aloitteelliseksi. Omat joukot ja tuli on kyettävä suuntaamaan tehokkaasti taisteluun ja taisteluita on voitava käydä informaatioylivoiman mahdollistavan tilannekuvan avulla. Operaation aikana on pystyttävä selvittämään riittävän aikaisin, minkä vaihtoehdon hyökkääjä valitsee. Myös vaikutus kohteessa on kyettävä arvioimaan - lamautuiko vai tuhoutuiko. Tiedustelu, valvonta ja maalittamistuki (TVM) muodostavat kokonaisuuden, jolla yhdistetään tiedustelujärjestelmän suorituskyvyt kokonaisuudeksi. Johtamisjärjestelmä mahdollistaa tiedustelutietojen esittämisen erilaisissa päätelaiteissa. Maavoimien tiedustelu toimii kiinteänä osana verkottunutta sotilastiedustelun kokonaisjärjestelmää, joka mahdollistaa eri tiedustelualojen kuten partio-, signaali-, elektronisen-, lento-, kuvaus-, henkilö-, geo- ja vastatiedustelun hyväksikäytön. Uusina järjestelminä käyttöön otetaan muun muassa minilennokkeja ja maasensoreita.

Uudistetussa taistelutavassa on kyettävä paikantamaan vastustajan kriittisiä joukkoja ja järjestelmiä ja tuotettava käytössä olevilla suorituskyvyillä riittävät kertautuvat tappiot. Kineettisten suorituskykyjen rinnalla on käytettävä ennakkoluulottomasti ja rohkeasti ei-kineettisiä suorituskykyjä, kuten elektronista ja psykologista vaikuttamista sekä harhauttamista. Tiedustelusensoreiden on kyettävä paitsi havaitsemaan haluttuja kohteita, paikantamaan niiden kriittisiä osia maaleiksi tulenkäytön edellyttämällä tarkkuudella ja lähettämään tulikomento. Tulta käytetään laaja-alaisesti myös oman ryhmityksen sisään, mikä korostaa tosiaikaisen ja eheän tilannekuvan merkitystä. Vaikutusperustainen toimintatapa edellyttää kykyä arvioida vaikutusta maalissa. Monimuotoiset tilanteet asettavat suuria vaatimuksia myös ampumatoiminnan johtamiselle sekä toiminnan mahdollistavalle johtamisjärjestelmälle. Tulitehtävät on kyettävä tarvittaessa jakamaan aseittain, johon kytkeytyy erikoisampumatarvikkeiden käyttö. Tavoitetilassa vaikuttamisen keinovalikoiman tulisi perustua tietojärjestelmäavusteiseen systemaattiseen laskentaan ja siitä johdettuun suositukseen. Raskasaseyksiköiden on tuliasematoiminnassa haettava suojaa hajaryhmityksestä ja liikkeestä, eri tavoin hankittua ballistista suojaa unohtamatta.

Ilmatorjunnan valvonta- ja johtamisjärjestelmän merkitys tilannetietoisuudessa ja johtamistoiminnassa on ilmatorjuntayksiköiden tehokkaan käytön kannalta keskeistä. Tavoitteena on integroida ilmatorjunnan tulenkäytön johtaminen kiinteäksi osaksi ilmapuolustuksen tulenkäytön johtamista. Kalustohankintojen lisäksi olemassa olevia järjestelmiä on modernisoitu, joiden ansiosta maavoimien joukkojen ilmatorjunta on siirtymässä erityisesti johtamisjärjestelmän, tulenantokyvyn ja pimeätoimintakyvyn osalta uuteen aikakauteen. Maavoimien taistelu 2015 muuttaa ilmatorjunta-aselajin taktisia käyttöperiaatteita. Yksiköiden rajallinen määrä pakottaa monikäyttöisyyteen sekä organisaatiosidonnaisuuden sijasta tehtävän ja toiminnallisuuden perusteella muodostettuihin joustaviin taistelujaotuksiin. Yksittäisten kohteiden tai kohderyhmien suojaamisen sijasta korostetaan kumulatiivisten tappioiden tuottamista ilma-aseelle. Ohjuksia ammutaan pääsääntöisesti vain erittäin edullisista maalitilanteista. Kiväärilmatorjunnan sijasta helikoptereita ammutaan vaunuaseilla ja singoilla sekä muilla perinteisillä panssarintorjunta-aseilla. Taistelutapa huomioi paremmin ilmasuojelulliset näkökohdat, mutta edelleen on perusteltua korostaa sään ja liikkeen hyödyntämistä, huoltokuljetusten suuntaamista suojaisille reiteille, hajaryhmitystä, peitteisen ja linnoittamiskelpoisen maaston käyttöä sekä maastouttamista.

Suomen puolustusdoktriinin lähtökohtana on oman maan puolustaminen ja siten taistelut valmistaudutaan käymään valtakuntamme maa-, meri- ja ilmatilassa. Asetelma tarjoaa meille merkittävän edun hyökkääjään nähden – voimme valmistella taistelutilaa tahtomme mukaisesti jo normaalioloista alkaen. Hyödyntämällä tämän edun täysimääräisesti vaikutamme merkittävästi taisteluihin ja voimasuhteiden kehittymiseen niiden eri vaiheissa. Uudistettuun taistelutapaan sisältyvä omien joukkojen aktiivinen käyttö koko taistelualueen syvyydessä edellyttää toimintojen valmistelua, joukkojen suojaamista ja vastustajan liikkeen ohjaamista taistelusuunnitelmaa tukevalla tavalla. Taistelutilan valmisteluun voidaan lukea ainakin tiedustelun, tulenkäytön ja johtamisen toimintaedellytysten rakentaminen sekä joukkojen perustamisen ja niiden käytön edellytyksien tukeminen. Pioneeritoiminnallisesti tarkasteltuna tehtävät voidaan jakaa taistelutilan valmisteluun, taistelutilan muuttamiseen taistelujen aikana ja suorituskyvyn ylläpitoon. Linnoitteita on rakennettava selvästi entisaikoja enemmän ja niiden on oltava yksinkertaisia. Maanrakennus- ja elementtiteollisuus sidotaan etupainoiseen toimintaan normaalioloissa tehtävin sopimuksin. Yritysten toiminta testataan harjoituksissa ja samalla harjoitellaan linnoittamisen johtamisjärjestelmää.

Vaikutusperusteinen suluttaminen suunnitellaan suluttamisvyöhykkeinä, jotka liitetään komentajan taisteluajatuksessa kiinteästi joukkojen ryhmitykseen tai liikkeeseen sekä muiden vaikuttamisen elementtien keskitettyyn käyttöön. Suluttamisvyöhykkeet ovat ohjaavia, hidastavia tai pysäyttäviä ja niiden avulla yksittäisten sulutteiden suunnittelu laajenee vaikutusperusteiseksi taktiseksi ajatteluksi. Tähän käyttöön ollaan hankkimassa kehittyneitä ohjelmoitavia, monikäyttöisiä miinoja. Vyöhykkeiden rakenteen suunnittelussa huomioidaan epäsuoran tulen, panssarintorjunnan ja joukkojen suorittamien iskujen koordinoitu toimeenpano. Samanaikaisesti oma toiminta tulee salata sekä säilyttää joukot ja järjestelmät taistelukykyisinä. Maastouttamisella ja hajauttamisella vaikeutetaan joukon paikantamista ja tunnistamista sekä asevaikutuksen kohdistamista. Paljastumisen lisäksi maastouttamisella voidaan kätkeä joukon tai toiminnan luonne, kun sähkömagneettisen tiedustelun tuottama tieto niistä saadaan mahdollisimman samankaltaiseksi.

Menestyminen taistelukentällä edellyttää myös toimivaa logistiikkajärjestelmää, jossa korostuvat ampumatarvikkeiden, polttoaineiden ja veden täydennysjärjestelmä sekä suorituskykyinen lääkintähuolto. Huollon on pystyttävä tukemaan laajalla alueella liikkuvia ja teknisellä materiaalilla varustettuja taistelujoukkoja. Kenttähuollolta vaaditaan liikkuvuutta, korkeaa teknistä osaamista, hyvää tilannekuvaa ja toimivia johtamisjärjestelmiä. Tuen kohdistuminen oikea-aikaisesti ja oikeaan paikkaan korostuu. Hallitakseen tilaus-toimitusketjuja on kyettävä liittymään sekä tuettavien johtamisyhteyksiin että niihin verkkoihin, joissa ylemmät huollon laitokset ja naapurit toimivat. Huollon luoman tukeutumisverkoston rakenteen ja volyymin säätämiseksi on huollon johtajien tiedettävä asiakkaiden liikkeet ja huoltotilanteen kehittyminen. Materiaalin tietojärjestelmän kautta tilannut asiakas pystyy seuraamaan tekemänsä tilauksen käsittelyä ja toimituksen etenemistä omalta päätelaitteeltaan. Tekniikan kehittyessä käyttäjien oma kyky ja muu kenttähuolto rajoittuu vain vika-analyysiin ja komponenttien vaihtoon sekä pieniin korjauksiin. Teollinen korjaus tulee saada yhä lähemmäs tuettavia joukkoja esimerkiksi kunnossapitopartioin. Haasteita hallitaan varaamalla vaihtolaitteistoja, tehostamalla varaosalogistiikkaa, seuraamalla sotavarusteiden käytettävyyttä ja rakentamalla liikkuvia kunnossapitoyksiköitä ja -partioita, johon myös strategisen kumppanin, Millog Oy:n suorituskykyjen kehittäminen kiinteästi kytkeytyy.

Maajoukkojen toimintatapojen uudistaminen edellyttää johtamisjärjestelmän ja johtamistapojen uudistamista. Merkittävää on, että muutos siirtää viestitoiminnan painopisteen perinteiseltä prikaatitasolta taisteluosastoihin ja hajautettuihin jääkäripataljooniin, joihin rakennetaan yhtenäinen digitaaliseen tekniikkaan perustuva taistelujärjestelmä. Uusia taisteluosastoja johdetaan taktisen johtamisjärjestelmän palveluilla, joihin kaikki perusyksiköiden ja aselajien taistelujohtojärjestelmät liittyvät. Taisteluosaston komentaja voi halutessaan liittää johtamisprosesseihinsa alaisten lisäksi myös tukevat, tuettavat sekä muut taistelutilassa toimivat osapuolet. Taisteluosaston johtajille tuotetaan reaaliaikaista tilannekuvaa, jonka tukemana he kykenevät hahmottamaan omien joukkojen toimintavaiheen ja vastustajan tilanteen. Taisteluosasto kykenee analysoimaan taistelutilassaan toimivan vastustajan tavoitteita, voimia ja heikkouksia. Suunnitteluprosessin tavoite on rajoittaa vastustajan ja laajentaa omia operaatiomahdollisuuksia sekä mahdollistaa operatiivinen yllätys, jossa komentajan ja asiantuntijoiden kesken toteutettu sotapelaaminen näyttelee merkittävää roolia. Johtamisjärjestelmän tuella komentaja kykenee säilyttämään ymmärryksensä yleisja perustilanteesta, eikä hän jää ”komentokorsunsa” vangiksi. Komentaja pystyy jalkautumaan johdettaviensa luokse menettämättä otetta taktiseen johtamiseen tai yhteyttä esikuntansa suunnitteluprosessiin.

Johtamisjärjestelmä tukee joukkojen yhteenkuuluvuutta kyberulottuvuudessa, ennakkovaroituksen saamista sekä johtajien päätöksentekoa ja tahdonilmausten saamista tukeviin organisaatioihin. Se liittää johtajat, erilliset ase- ja sensorijärjestelmät, ajoneuvot, joukot ja niiden tuen taistelujärjestelmäksi. Johtamisjärjestelmän tuottaman tilannekuvan tieto vastustajasta, omasta toiminnasta ja olosuhteista on erityisen tärkeää joukkojen toimiessa hajaantuneena. Tilannekuva on jaettavissa ajallisesti ja alueellisesti kaikkiin maavoimien tieto- ja taistelujohtojärjestelmän päätelaiteisiin aina jääkäriryhmän johtajasta huoltopartioon asti. Taistelujohtojärjestelmän avulla joukkojen tehtävätaktinen toiminta tehostuu ja oma toiminta kyetään tahdittamaan muiden toimintaan. Taistelujohtojärjestelmässä tulenjohtokykyiset partiot ja ryhmät näkevät toisensa useimmiten vain ”kybertilassa” - taktisena merkkinä tilannekuvassa. Tilannekuvan perusteella ne kykenevät tunnistamaan vastustajan heikot kohdat ja vaikut-

tamaan niihin taisteluosaston ja sen taistelua tukevien järjestelmien yhteisvaikutuksella. Järjestelmien kokonaisvaltaiseen kehittämiseen kytkeytyy ohjelmoitavan elektroniikan ylläpito- ja varastointijärjestelyt. Järjestelmien laitteet säilytetään verkkovarastoissa, jolloin niitä voidaan päivittää tarvittaessa.

Taisteluosaston suorituskykyjen tehokas käyttö ja menestyminen yhä monimutkaistuvassa taistelutilassa edellyttävät vahvaa tukea verkostolta. Tiedonvälityksen painopiste siirtyy puheesta tiedonkäsittelyyn, jossa korostuvat yksittäisten komentopaikkojen sijasta verkostojen sekä joukkueiden ja näiden johtajien tukeminen. Viestitoiminnan johtaminen laajenee viestiasemien ja komentopaikkojen johtamisesta taistelujohtojärjestelmän palveluiden ja tietojen johtamiseen. Tärkeimpiä tuettavia prosesseja ovat tilannekuva sekä tulenkäytön ja tuen johtaminen. Viestijärjestelmältä vaaditaan tappioiden sietokykyä. Järjestelmän on kyettävä käyttämään automaattisesti erilaisia yhteysmuotoja. Taistelutilan valmistelu ja kaapeliverkon muokkaaminen sekä rakentaminen taistelusuunnitelmaa tukevalla tavalla korostuvat. Johtamisjärjestelmän toimintaa ohjataan viestitaktiikalla, jossa tärkeimpinä mittareina ovat johtamisjärjestelmäpalveluiden käytettävyys ja luotettavuus. Johtamisjärjestelmän on kyettävä taistelutekniikan ja taktiikan tavoin oppimaan uutta eteen tulevista ennakoimattomista tilanteista. Viestitaktiikalla onkin vastattava kysymykseen: Milloin on paras hetki opettaa järjestelmille uusia asioita ja milloin järjestelmän tulisi olla muuttumaton.

Käytännön tasolla tietoverkkosodankäynti tai kyberpuolustus kytkeytyy operaatioturvallisuuden kokonaisuuteen. Kysymys on tiedon kokonaisvaltaisesta eheydestä, käytettävyydestä ja luottamuksellisuudesta – ei siis pelkästään siirrettävästä tiedosta. On varmistuttava järjestelmissä olevien ohjelmistojen eheydestä, käytettävyydestä ja luottamuksellisuudesta, samalla kun huolehditaan ihmisten eheydestä, käytettävyydestä ja luottamuksellisuudesta. Perusteiksi meidän on arvioitava, mistä tiedoista olemme itse toiminnan kannalta riippuvaisia. Vastaava pohdinta on tehtävä viholliselle elintärkeästä tiedosta. Liittämällä näihin tiedon ajallinen tarve, eli se milloin tieto pitää olla käytössä, voidaan jo varsin mallikkaasti rakentaa toiminta-ajatusta verkkorakenteista, tiedonsiirtotarpeista sekä salaus- ja taltiointiratkaisuista. Rinnalla voimme pohtia sitä, vastaako johtamisen konsepti ja toimintamallit tilanteisiin, joissa yhteydet ovat poikki ja sähköiset järjestelmät lamautuneita.

Pitämällä tehtävätaktiikan periaatteet keskiössä, voimme perustellusti arvioida, milloin ylemmän johtoportaan komentopaikan puuttuminen verkoista alkaa oikeasti vaikuttaa alemman johtoportaan toimintaan ja milloin viimeistään tarvitaan ”peliliikkeitä”? Hyvä on myös pohtia sitä, pitääkö kaiken tiedon olla järjestelmissä vai voisiko osa siitä olla edelleenkin taltioituna pelkästään ihmisten aivoihin, joista viime vuosina on tullut enintään varmuuskopiointiin soveltuvia tietovoimaloita. Ja tulisiko tärkeimmät asiat hoitaa jollain muilla tavoin kuin järjestelmiä hyödyntäen – esimerkiksi henkilökohtaisina tapaamisina? Paraskaan järjestelmä kun ei korvaa alaisten tuntemusta ja suullisen käskyn tehokkuutta. Kyberaikakausi korostaakin juuri perinteisten johtamistapojen hyödyntämisen elintärkeyttä.

Tärkeää on tehdä pohdintaa myös siitä, miten verkkotaisteluja johdetaan. Onko meille syntymässä ristiriitatilanne nykyisen johtamiskulttuurin ja verkkosodankäynnin johtamisen asettamien vaatimuksien välille? Vain ihmistä voi johtaa, josta lähtökohdasta arvioiden minkään ei pitäisi perusteiltaan muuttua. Kokemukset verkkotaistelujen johtamisesta ja suunnitelmien toimivuudesta ovat vasta karttumassa, mutta kehitys kul-

kee vääjäämättä eteenpäin. Tässä, kuten monessa muussakin tekniikan ja tilannekuvan kehittymiseen kytkeytyvässä asiakokonaisuudessa saattaa vaarana olla mikromanagerointi, jolloin kokonaisuus ja verkkosodankäynnin kytkeytyminen siihen saattavat hämärtyä. Pidettäköön tietoverkkosodankäynti edelleenkin tukevassa roolissa, koska sillä ei tulla nyt, eikä myöskään näkyvässä olevassa tulevaisuudessa ratkaisemaan ainuttakaan sotaa.

Toki johtamisprosessin kehittämiselle on aina tarvetta. Tietoverkkosodankäynti on linkitettävä osaksi prosesseja, joissa taisteluista vastaavien komentajien on kyettävä asettamaan yksilöityjä vaatimuksia muun muassa operaatioiden turvallisuudelle. Olemmekin varsin mielenkiintoisessa tilanteessa. Samanaikaisesti, kun maavoimat näyttäytyvät uudessa doktriinissa sotatoimien taktisena tasona muiden puolustushaarojen tapaan, olemme ottaneet käyttöön FINGOP-suunnitteluprosessin. Työkalun, joka pakottaa meidät keräämään perusteita taktisen tason lisäksi niin operatiiviselta kuin jopa poliittis-strategiselta tasolta. Prosessi pakottaa perusteellisuuteen. Sen perusteella syntyy täydellinen systeemikuvaus, joka mahdollistaa tarvittaessa myös oman järjestelmämme romahduttamisen. Kaikesta huolimatta tai juuri mainituista syistä uusi prosessi tarjoaa erinomaisen työkalun myös verkkosodankäynnin suunnitteluun.

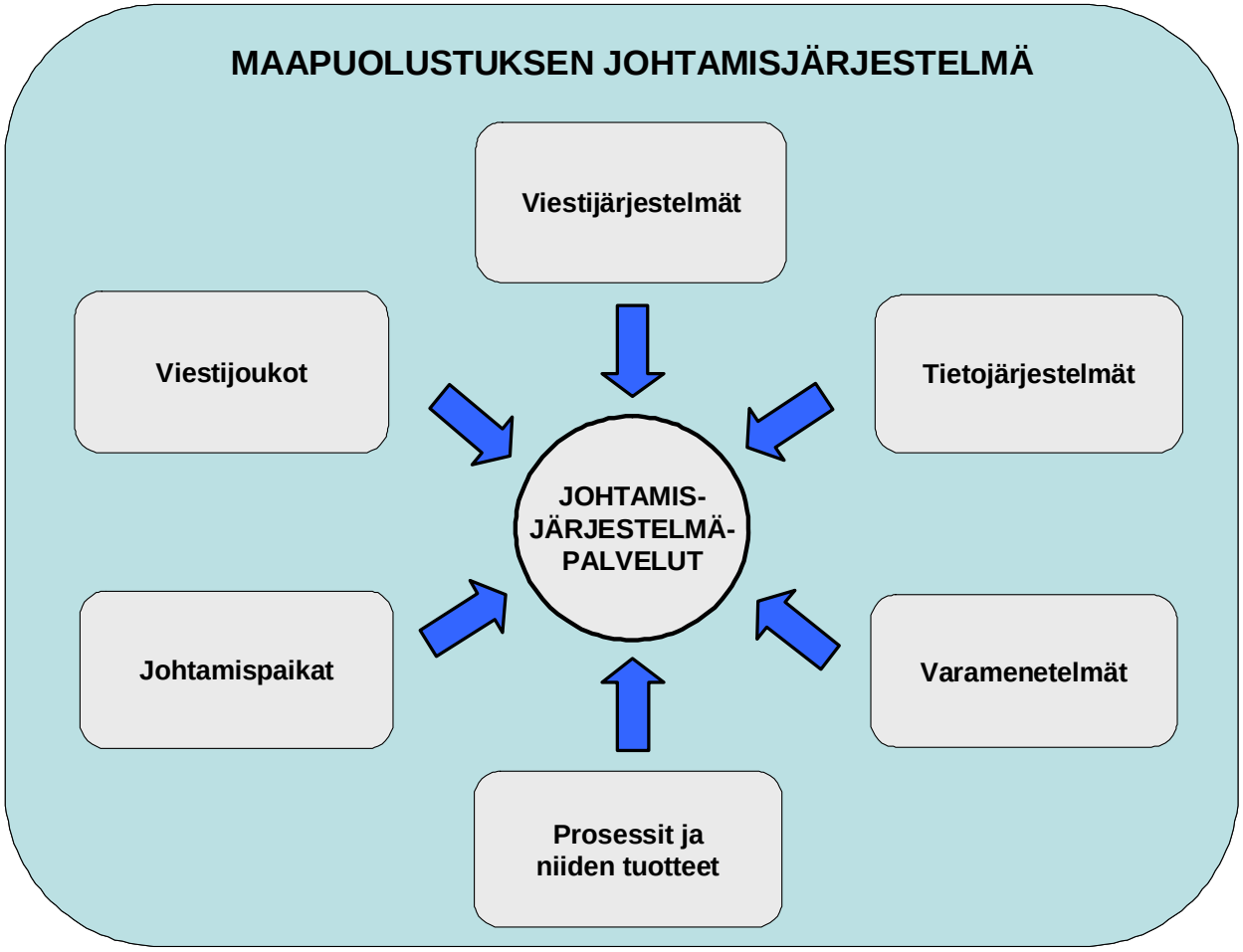
8.3 Johtamisjärjestelmä M18 – tekninen ja taktinen haaste

Puolustusvoimissa johtamisjärjestelmän suorituskyky muodostuu joukkojen ja järjestelmien johtamisen mahdollistavasta johtamisen tuesta ja johtamisen infrastruktuurista. Suorituskyky näyttäytyy tarvitsijoille johtamista tukevina johtamisjärjestelmäpalveluina, niiden tuottamisessa käytettävinä tietojenkäsittely- ja tiedonsiirtojärjestelminä sekä palveluiden tuottamisesta vastaavina johtamisjärjestelmäalan joukkoina. Johtamisjärjestelmän suorituskyvyllä yhdessä tiedustelun, valvonnan ja maalittamisen tuen (TVM) kanssa mahdollistetaan kyberpuolustus – joka sekin korostaa verkkojen ja erityisesti niiden suojaamisen merkitystä.

Puolustusvoimallisesti johtamisjärjestelmäpalvelut jaetaan tieto- ja järjestelmäpalveluihin. Tietopalvelut tukevat johtamisessa tarvittavaa organisointia, tilanneymmärryksen muodostamista, suunnittelua, päätöksentekoa, toimeenpanoa ja arviointia. Tietopalvelujen käyttö edellyttää järjestelmäpalveluja. Järjestelmäpalvelut tukevat tietopalveluihin liittyvää tietojen käsittelyä, välitystä, tallennusta, hallintaa ja hakua sekä aika- ja paikkatietojen hallintaa. Tietopalvelut antavat perusteet johtamisjärjestelmän verkostorakenteen eli johtamisen infrastruktuurin suunnittelulle, rakentamiselle ja ylläpidolle sekä käytölle. Johtamisjärjestelmäpalveluita ohjataan ja kehitetään kahdessa palvelulinjassa. Puolustusvoimien päätehtävissä tarvittavat operaatioiden johtamisen ja vaikuttamisen operatiiviset johtamisjärjestelmäpalvelut tuotetaan puolustusvoimien palvelulinjaa käyttäen. Operaatioiden tukemisen ja yhteiskuntaan tukeutumisen mahdollistavat hallinnolliset johtamisjärjestelmäpalvelut hankintaan pääosin kumppaneilta Valtionhallinnon palvelulinjaa käyttäen.

Maapuolustuksen näkökulmasta johtamisjärjestelmällä ymmärretään viestijoukkojen, viesti- ja tietojärjestelmien, johtamispaikkojen, prosessien ja niiden tuotteiden sekä varamenetelmien muodostamaa kokonaisuutta. Johtamisjärjestelmä mahdollistaa operatiivisen suunnittelun, operaatioiden toimeenpanon sekä tilannekuvan muodostamisen, jakamisen ja ylläpitämisen. Järjestelmä hyödyntää maavoimien viestijoukko-

jen ja Puolustusvoimien johtamisjärjestelmäkeskuksen sekä sitä tukevien organisaatioiden palveluita ja resursseja. Maapuolustuksen johtamisjärjestelmä mahdollistaa valmiuden kohottamisen, perustettavien johtoportaiden ja hajautetusti toimivien joukkojen johtamisen, taistelutilan valvonnan, tiedustelun, tilannekuvan kokoamisen sekä tulen keskitetyn johtamisen ja vaikutuksen koordinoinnin. Se mahdollistaa myös yhteistoiminnan meri- ja ilmavoimien, Rajavartiolaitoksen sekä muiden viranomaisten ja yhteistyökumppaneiden kanssa.



Kuva 2. Maapuolustuksen johtamisjärjestelmä sisältää sekä toiminnallisia että teknisiä osakokonaisuuksia.

Johtamisjärjestelmän suunnittelu, rakentaminen ja ylläpito noudattavat rinnakkaisen suunnittelun, toimeenpanon ja tilannekuvan prosesseja siten, että kukin joukko vastaa ensisijaisesti omasta johtamisjärjestelmästään. Perusratkaisussa ylempi johtoporras vastaa alemman johtoportaan liittämisestä omaan järjestelmäänsä. Prosesseissa huomioidaan palveltavien joukkojen toiminta, joka korostaa taistelutilan valmistelujen, hajauttamisen, liikkeen, linnoittamisen, ryhmitysmuutosten, harhauttamisen ja vastustajan maalitiedustelun kyllästämisen merkitystä. Järjestelmä tukee joukkoja puhe-, sanoma- ja tietojärjestelmäpalveluilla siten, että ne kykenevät toteuttamaan tehtävänsä kaikissa taistelun vaiheissa. Maapuolustuksen johtamisjärjestelmä on samanaikaisesti sekä palvelukykyinen että taistelunkestävä. Järjestelmän ylläpito perustuu porrastetusti toteutettuun tekniseen valvontaan ja hallintaan. Kokonaisvalvonnasta

vastaa Maavoimien operatiivinen järjestelmäkeskus, joka toimii myös valtakunnallisena tukiorganisaationa häiriöiden korjaamisessa.

Maapuolustuksen viestijärjestelmä muodostuu maapuolustuksen liityntäverkosta (MAAVNET) ja siihen liitetyistä alueellisten johtoportaiden, yhtymien, taisteluosastojen, pataljoonien ja rajavartiostojen sekä aselaji- ja toimialajoukkojen viestijärjestelmistä, jotka jakaantuvat edelleen erilaisiin verkkoihin. Yhteydet voidaan toteuttaa langattomina tai langallisina. Maapuolustuksen viestijärjestelmä on yhtenäinen internetin tavoin toimiva digitaalinen tiedonsiirtoalusta, joka varmistaa keskeisten taktisten palveluiden toimivuuden ja alustan yhteensopivuuden kohdearkkitehtuurin sekä muiden puolustushaarojen kanssa. Se on kiinteä osa puolustusvoimien verkostorakennetta, joka mahdollistaa puolustusvoimien kaikkien suorituskykyjen integroidun käyttämisen ja puolustusjärjestelmän osajärjestelmien yhteistoimintakyvyn. Viestijärjestelmästä muodostetaan yhteydet turvallisuusviranomaisten yhteiseen tietoliikenneverkkoon (TUVE) ja sen palveluihin sekä tarvittaessa eri operaattoreiden tietoliikenneverkkoihin.

Kuva 3. Maapuolustuksen viestijärjestelmä muodostaa tietoverkkosodankäynnin teknisen alustan.

Yhtymien viestijärjestelmät ovat liikkuvia ja suurimman tiedonsiirtokapasiteetin omaavia. Taisteluosastojen viestijärjestelmät ovat myös liikkuvia, mutta tiedonsiirtokapasiteetiltaan yleensä pienempiä. Viestijärjestelmissä käytetään A-, C- ja E-tyypin viestiasemia. Viestiasema (A) on sekä yhtymien että taisteluosastojen viestijärjestelmien rungon viestiasema, jolla muodostetaan runkoverkko ja liitetään alajohtoportaita siihen. Liityntäverkon viestiasemalla (C) laajennetaan taisteluosaston viestijärjestel-

män runkoa liityntäverkoksi, liitetään alajohtoportaita viestijärjestelmään ja liitytään ylemmän johtoportaan viestijärjestelmään. Viestiasema (E) on komppanian asema, jolla liitytään taisteluosaston runko- tai liityntäverkkoon. Kaikkia asemia käytetään johtamispaikkojen, alajohtoportaiden ja aselajijoukkojen liittämiseen.

Maavoimien tietojärjestelmä (MATI) on yhtenäinen ohjelmisto-, sovellus-, verkko- ja päätelaiteperhe, jonka palveluilla tuetaan maaoperaatioiden johtamista ja yhteisten suorituskykyjen käyttöä kaikilla johtamistasoilla sekä yhteistoimintaa muiden puolustushaarojen ja yhteistyötahojen kanssa. Tietojärjestelmällä suunnitellaan toimintaa, toimeenpannaan suunnitelmia ja tehtäviä, muodostetaan johtamista tukevaa tilannekuvaa sekä johdetaan taisteluita. Tietojärjestelmän kehittämisen painopiste on maavoimien taisteluosastoissa (perusyhtymä). Perusyksiköissä tietojärjestelmäpalvelut tuotetaan ryhmä- ja partiotasolle maavoimien tietojärjestelmäperheeseen kuuluvalla taistelunjohtojärjestelmällä (TSTJJ). Ylemmillä johtamistasoilla palvelut integroidaan osaksi puolustusvoimien yhteistä Leijona-ympäristöä.

Tietojärjestelmäpalveluiden lisäksi johtamista tuetaan muun muassa puhe- ja sanomapalvelulla, jotka ulottuvat liikkuville partioille, sensoreille ja aselaveteille. Maapuolustuksen johtamisjärjestelmäpalveluiden rinnalla käytetään puolustusvoimien yhteisiä hallinnollisia ja operatiivisia tietojärjestelmäpalveluita, viranomaisten kenttäjohtamisjärjestelmäpalveluita sekä meri- ja ilmavoimien tietojärjestelmäpalveluita. Varamenetelmillä varmennetaan johtamista tilanteissa, joissa sähköiset palvelut eivät ole käytössä. Näihin kuuluvat muun muassa lähetti- ja kuriiripalvelut, henkilökohtainen tapaaminen sekä karttojen ylläpito.

8.4 Verkkotaistelu – maavoimien näkökulma

Kansallisen kyberturvallisuusstrategian mukaisesti puolustusvoimiin luodaan kokonaisvaltainen kyberpuolustuskyky lakisääteisten tehtävien hoitamiseksi. Tämä edellyttää tarvittavia toimivaltuuksia, sujuvaa tiedonvaihtoa ja yhtenäisiä toimintamalleja eri toimijoiden välillä, sekä ennen kaikkea henkilöstön osaamisen kehittämistä. Maavoimien rooli osana kyberpuolustuksen kokonaisuutta korostaa omien johtamisjärjestelmien ja -ympäristöjen suojaamista. Tehtävä edellyttää maavoimilta kykyä muodostaa kyberpuolustuksen tilannekuva käytössä olevista lähteistä, valvoa oman kohdearkkitehtuurin järjestelmiä, havaita ja torjua niihin kohdistuvat vihamieliset toimenpiteet sekä kykyä toipua hyökkäysten vaikutuksista.

Kyberympäristö on sähköisessä muodossa olevan informaation käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö, jolle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon tiedonsiirtoyhteyksien avulla. Kyberpuolustus on kyberturvallisuuden maanpuolustuksellinen osa-alue. Kyberpuolustuksen suorituskyky muodostuu tiedustelu- ja valvontakyvyistä sekä vaikuttamisen ja suojautumisen kyvyistä. Kyberpuolustuksen kokonaisuuden suunnittelusta vastaa Pääesikunnan johtamisjärjestelmäosasto. Kyberpuolustusoperaatiot toteutetaan osana muita puolustusvoimien operaatioita. Lisäksi johtamisen suorituskyvyllä, yhdessä tiedustelun, valvonnan ja maalittamisen tuen suorituskyvyn kanssa, mahdollistetaan tiedustelu ja valvonta, suojautuminen sekä vaikuttaminen kybertoimintaympäristössä (kyberpuolustus).

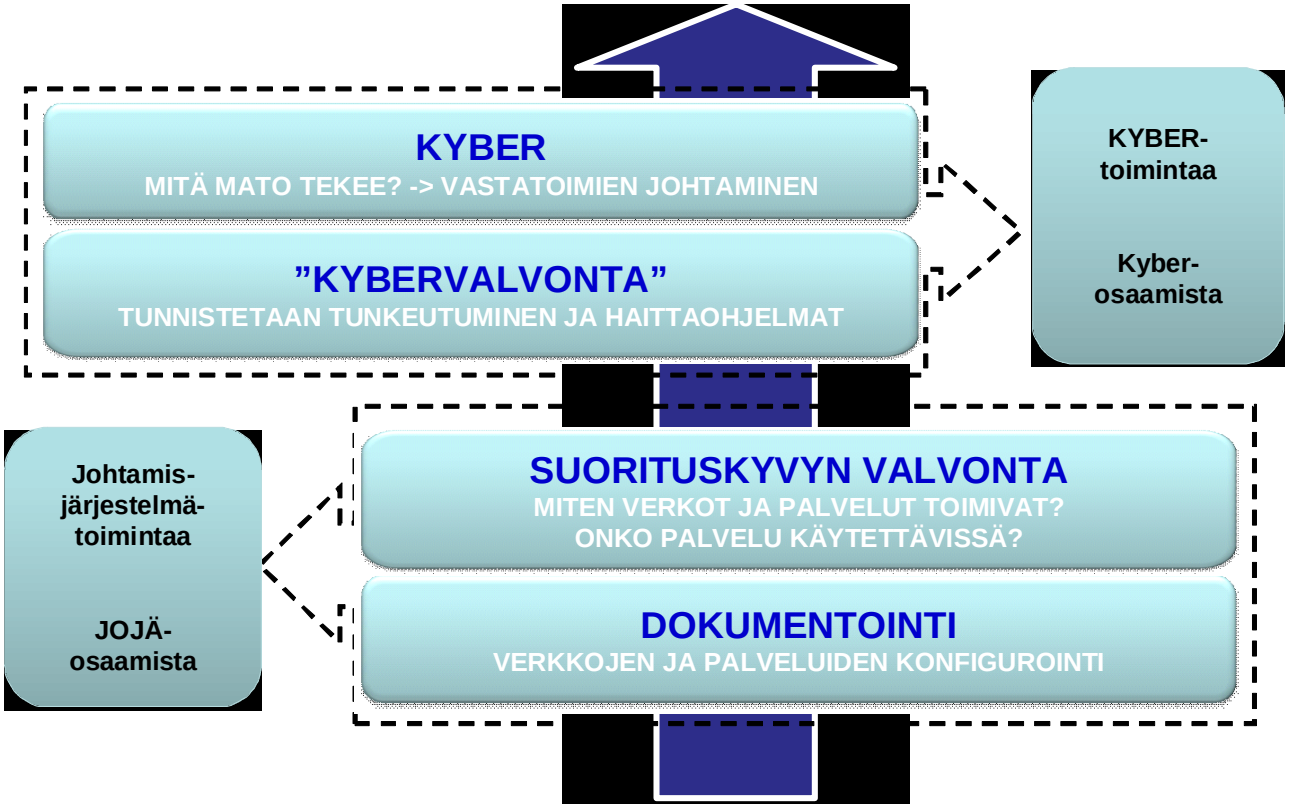
Ennaltaehkäisevässä toiminnassa korostuu tuotannossa olevien ja kehitettävien johtamisjärjestelmäkokonaisuuksien tai niiden osien tietoturvallisuuden perustekijöistä huolehtiminen. Teknisellä tietoturvallisuudella voidaan suojaamistoimenpiteitä toteuttaa tiettyyn rajaan asti kustannustehokkaalla tavalla, mutta täysin suljettuja ja turvallisia tietoliikenneverkkoja tai tietojärjestelmiä ei nykypäivänä kyettäne rakentamaan. Oleellista onkin ymmärtää omat haavoittuvuudet ja peilata niitä vasten uhkia, joita vastaan suojautumistoimenpiteitä tulee suunnitella, valmistella ja tarvittaessa toimeenpanna. Kokonaisuudessa merkittävää roolia näyttelee edelleenkin ihmisten osaaminen – toki teknisten apuvälineiden tuottamien suorituskykyjen rinnalla.

Yleisesti tarkasteltuna kyberturvallisuusympäristössä uhkat muodostuvat ei valtiollisten ja valtiollisten toimijoiden toteuttamista operaatioista. Ei-valtiollisten toimijoiden muodostaman uhkan voidaan arvioida vaikuttavan maavoimien toimintaan lähinnä hallinnollisten järjestelmien kautta, joten niiden vaikutukset operatiiviseen toimintaa lienevät vähäiset. Valtiollisten toimijoiden kyky vaikuttaa operatiivisiin järjestelmiin muodostaakin huomattavasti vakavamman uhkan niin normaali- kuin poikkeusoloissa. Tästä johtuen maavoimilla tulee olla kyky arvioida sitä vastaan kohdistuvia uhkia, havainnoida poikkeamat omissa järjestelmissään ja käynnistää tarvittavat toimenpiteet hyökkäyksen estämiseksi tai rajoittamiseksi ja palauttaa toimintakyky onnistuneesti. Keskeistä kyberhyökkäysten torjunnassa on kyky pitää käytössä olevat järjestelmät ajan tasaisina, joka edellyttää säännöllisin väliajoin tehtäviä järjestelmäpäivityksiä. Perusvaatimuksena on, että tuotantoympäristöön asennetaan vain testattuja ja vakioidussa prosessissa hyväksyttyjä päivityksiä. Suurempien päivitysten ohella tuotantoympäristön ajantasaisuus varmistetaan säännöllisillä tietoturvapäivityksillä, joiden tarpeellisuutta ylläpitohenkilöstö arvioi päivittäisessä toiminnassaan.

Omien haavoittuvuuksien tunnistaminen ja niihin kohdistuvien hyökkäysten vaikuttavuuden arviointi on oleellinen osa suojautumistoimenpiteiden tehokkuutta. Perusvaatimuksena on verkkojen aukoton ja yli rajapintojen ulottuva automatisoitu tekninen valvonta. Tilanteenarviointiprosessin avulla kyetään hallitsemaan riskejä sekä luomaan järjestelmien valvonnan ja hallinnan painopiste vallitsevan tilanteen edellyttämällä tavalla. Näin resurssit kyetään kohdentamaan hyökkäysten havaitsemiseen, torjuntaan ja aiheutuvien tappioiden minimoimiseen sekä nopeaan toipumiseen. Toimenpiteiden onnistuminen edellyttää johtamisjärjestelmien ylläpidosta vastaavan henkilöstön vankkaa ammattitaitoa sekä tiivistä vuoropuhelua tekniikan ammattilaisten ja operatiivisten päätöksen tekijöiden välillä.

Maapuolustuksen suorituskykyjen teknistyminen ja yhä vahvempi IP-pohjaisuus (internet protocol) myös taktisen tason johtamisjärjestelmissä vaikuttaa voimakkaasti juuri kyberpuolustuksen näkökulmasta annettavaan koulutukseen yksittäisestä sotilaasta ylimpään johtoon. Teknisten johtamisjärjestelmien ja päätelaitteiden tuomiin haasteisiin ei kyetä vastaamaan vain teknisillä apuvälineillä. Yleisesti voidaankin arvioida kyberpuolustuksen suorituskykyjen muodostuvan suurilta osin inhimillisistä tekijöistä. Kysymys on ennen muuta sekä loppukäyttäjien että järjestelmien ylläpitotehtävissä työskentelevien ihmisten osaamisesta ja asenteista. Tarvittavan osaamisen kehittämisessä keskeistä onkin eri toimijoiden välinen tiivis ja tavoitteellinen yhteistyö.

Puolustusvoimien verkkosodankäyntioperaatioita johtaa Puolustusvoimien johtamisjärjestelmäkeskus, jonka kokonaisuuden osana maavoimat toimii. Johtamisjärjestelmäkeskus ylläpitää puolustusvoimien CERT-toimintaa (Computer Emergency Response Team, PVCERT). PVCERT toimii tiiviissä yhteistyössä sekä valtionhallinnon että kansainvälisten toimijoiden kanssa. Maavoimissa verkkosodankäyntiä johtaa Maavoimien esikunnan johtamisjärjestelmäosasto ja toteuttajana on Maavoimien operatiivinen järjestelmäkeskus. Alajohtoportaat osallistuvat oman johtamisjärjestelmänsä suojaamiseen. Johtamisjärjestelmämateriaalin ja ohjelmistojen hallinta varmistetaan ohjelmoitavan elektroniikan ylläpidolla ja samalla edesautetaan myös tärkeimpien järjestelmien toimintakykyä ja tietoturvallisuutta joukkoja perustettaessa. Näin mahdollistetaan myös perustettavien joukkojen ja järjestelmien joustava sekä tietoturvallinen liittäminen johtamisjärjestelmään valmiutta kohotettaessa.



Kuva 4. Vaikka verkot ovat kyberulottuvuuden keskeisintä toimintakenttää, on vastuunjako johtamisjärjestelmä- ja kybertoiminnan välillä oltava selvä.

Maapuolustuksen johtamisjärjestelmä suojataan vastustajan tietoverkkosodankäynniltä, jonka lähtökohtana on, että operaatioiden suunnittelussa ja johtamisessa huomioidaan vastustajalla olevat suorituskyvyt. Operaatioiden suunnittelu ja toimeenpano on varmennettava siten, että toimintaa kyetään jatkamaan myös tietojärjestelmien lamautumisen jälkeen. Toiminnan tueksi joukot laativat tietoturvaohjeita, joihin kirjatut käytännöt koulutetaan koko henkilöstölle ja niiden noudattamista myös valvotaan.

Maavoimien kohdearkkitehtuuriin kohdistuvien riskien hallinta toteutetaan kahdessa vaiheessa. Ensimmäisessä vaiheessa varaudutaan perustamisjärjestelmään kohdistuvaan kyberuhkaan pitämällä sovellukset ja laitteet ajantasaisena verkkovarastoinnin, ohjelmistojen ja konfiguraation palautuskyvyn sekä ottomateriaalitäydennysten avulla. Tietoturvallisuuden kannalta jakelu- ja konfiguraatiohallinta on avainasemassa. Toisessa vaiheessa maapuolustuksen tietosisältöjen eheys- ja luottamuksellisuusriski muodostuu taistelun aikana, mikäli vastustajan tai muiden operaatiotilassa vaikuttavien haltuun joutuu tietoja laitteiden ja solmujen menetyksestä johtuen. Riskiä hallitaan säilyttämällä tärkeä tieto puolustusvoimien keskitetyissä palveluissa, joista otetaan taistelujärjestelmien käyttöön tehtävän edellyttämä ote. Tietoturvan järjestelyihin vaikuttaa myös tiedon elinkaari, joka lyhenee siirryttäessä organisaatiotasossa alemmas. Taisteluosastossa tiedon elinkaari on erittäin lyhyt ja mahdollisuuksien mukaan syntyvä tieto välitetään kiinteisiin tietovarastoihin säilytettäväksi.

Perusta maavoimissa palvelevien asevelvollisten ja palkatun henkilöstön osaamiselle muodostuu Pääesikunnan ohjauksen mukaisesti tietoturvallisuuden perus-, ylläpito- ja täydentävästä koulutuskokonaisuudesta. Koko henkilöstölle koulutetaan tietoturvallisuuden perusteet, jossa tavoitteena on varmistaa henkilöstön osaaminen tietojen suojaamisessa, palveluympäristöjen suojaamisessa väärinkäytöksiltä ja salassa pidettävän tiedon käsittelyssä sekä ennalta ehkäistä tahattomia virheitä ja vahinkoja. Tietoturvallisuuden perusta rakennetaan osaavaan, motivoituneeseen ja hyvällä asenteella toimivaan henkilöstöön. Koulutuksen perusteella joukkoihin sijoitettu henkilöstö osaa käyttää tehtävässä tarvittavia päätelaitteita turvallisesti. Henkilökunnan osaamista varmistetaan vuosittain järjestettävällä ylläpitävällä koulutuksella ja reserviläisten kertausharjoituksiin liitetyllä koulutuksella. Koulutuksessa hyödynnetään monimuotoisia opetuspaketteja. Tähän kuluu muun muassa internetissä toimiva koulutusjärjestelmä, joka sisältää koulutus- ja testiosuudet. Täydentävään koulutukseen voidaan liittää tietojärjestelmien ja -sovellusten eriytyviä osuuksia sekä tietoturvallisuuden osa-alueisiin painottuvia koulutuksia. Näiden koulutuspakettien avulla reserviläiset voivat aiempaa paremmin valmistautua tuleviin harjoituksiin.

Henkilöstön osaamisen pitkäjänteisessä kehittämisessä on sotilasopetuslaitoksilla merkittävä rooli. Kyberpuolustuksen opetusta kehitetään kiinteäksi osaksi sotilasopetuslaitoksissa annettavaa perus- ja jatkokoulutusta. Tämä mahdollista koulutuksen sisällön kehittämisen palvelemaan kokonaisuutta, yhtenäistää annettavan koulutuksen sekä vapauttaa joukoissa koulutukseen sidottuja resursseja ylläpitävään ja täydentävään koulutukseen. Uudelleen organisoidun Maasotakoulun koulutustarjonnassa säilytetään johtamisjärjestelmäalalla työskentelevälle henkilöstölle suunnatut opintokokonaisuudet. Niiden avulla voidaan rakentaa hyvä perusta johtamisjärjestelmien ylläpitotehtäviin harjaantuvalle henkilöstölle. Osaamista syvennetään käytännön harjaantumisella omissa joukko-osastoissa.

Säännöllinen harjoittelu on edellytys osaamisen ylläpidolle, johon vaikutetaan suunnittelemalla ja sitouttamalla henkilöstö harjaantumaan sodan ajan sijoituksensa mukaiseen tehtävään. Kokonaiskehittämisen kannalta on keskeistä tuoda kyberpuolustuksen osa-alueiden harjoittelu osaksi normaalia maavoimien harjoitustoimintaa. Tähän voidaan tehokkaasti hyödyntää rakennettuja kyberpuolustuksen harjoitusympäristöjä sekä toteuttamalla harjoitteita säännöllisesti myös tuotantokäytössä olevissa johtamisjärjestelmäympäristöissä. Keskeinen osa suorituskykyjen kehittämisessä on

myös eri toimijoiden välisellä tiiviillä yhteistyöllä sekä kyberturvallisuuden verkostojen hyödyntämisellä.

Maavoimat kehittää omalta osaltaan kyberpuolustuksessa tarvittavaa yhteistoimintaa puolustusvoimien sisäisten, muiden viranomaistahojen sekä yksityisen sektorin toimijoiden kanssa. Verkostojen luominen ja niiden täysipainoinen hyödyntäminen edesauttaa kaikkien toimijoiden tilannetietoisuuden ja osaamisen kehittymistä kaikilla osa-alueilla. Yhteistoiminnan tavoitteena on samalla välttää päällekkäisten toimintojen rakentumista ja vapauttaa kunkin toimijan resursseja sille tärkeimpiin toimintoihin. Pienen maan resurssit on kaikissa tilanteissa osattava ja kyettävä kohdentamaan oikein.

Maavoimien henkilöstö osallistuu aktiivisesti kyberpuolustuksen suorituskykyjen kehittämiseen. Kyberpuolustuksen kehittämisessä alan osaajia sitoutetaan rakentamaan yhteiskäyttöisiä ja yhteensopivia työkaluja. Yksin ei kukaan tässä ympäristössä kykene turvaamaan johtamisjärjestelmiensä käytettävyyttä kaikissa tilanteissa. Kyberpuolustus onkin oiva esimerkki siitä, kuinka vain rakentavalla yhteistyöllä voi jokainen toimija saavuttaa omat tavoitteensa.

Maavoimissa yhteistyö näkyy konkreettisesti henkilöstön osallistumisena kansainvälisiin ja kansallisiin harjoituksiin, seminaareihin, tutkimushankkeisiin sekä eri kursseille ja opetustilaisuuksiin. Kansainvälisissä harjoituksissa voidaan kehittää henkilöstön yksilöllistä osaamista sekä erityisesti organisaatioiden välistää yhteistoimintaa ja yhteensopivuutta kansainvälisessä toimintaympäristössä. Harjoituksiin osallistuminen mahdollistaa myös kyvykkyyksien vertailun eri maiden osallistujien välillä. Tilaisuuksissa on keskeistä tunnistaa parhaita käytäntöjä, joita voidaan tehokkaasti käyttää myös kansallisessa kyberpuolustuksessa.

Osallistuminen kansallisiin kyberpuolustus- tai kyberturvallisuusharjoituksiin mahdollistaa maavoimien verkostoitumisen ja yhteistoiminnan kehittämisen muiden puolustusvoimien toimijoiden sekä puolustusvoimia keskeisesti tukevien tahojen välillä. Keskiössä tulee olla kansallisesti yhteensopivat prosessit ja toimintatavat. Selkeät yhteistoimintasuhteet ja vastuujako eri toimijoiden välillä on edellytys sujuvalle kanssakäymiselle ja tiedon vaihdolle. Myös kansallisesti tarkasteltuna parhaiden käytäntöjen vertailu sekä niiden hyödyntäminen oman organisaation toiminnan kehittämisessä tulee olla tavoitteena.

Yhteistoimintaa harjoitetaan sekä aluehallinto- että paikallistasolla. Paikallistason yhteistoiminnan merkitystä ei pidä missään tilanteessa väheksyä. Sen onnistuminen voi parhaimmillaan luoda sellaisen voimavaran, jonka merkitys varsinkin poikkeusolojen toiminnassa muodostuu jopa ratkaisevaksi tekijäksi. Paikallistason yhteistoiminnassa on vielä tällä hetkellä varsin paljon toisistaan poikkeavia käytäntöjä. Toimivien osien tunnistaminen ja niiden koostaminen yhtenäiseksi toimintamalliksi siirtää yhteistoiminnan seuraavalle tasolle.

Organisaatioiden välisen yhteistoiminnan merkitystä vähäisemmälle huomiolle ei tule myöskään jättää organisaation sisäisten toimijoiden yhteistyötä ja kommunikaatiota. Ymmärrettävä vuoropuhelu operaation johdon ja kyberasiantuntijoiden välillä on edellytys toiminnalle asetettujen tavoitteiden saavuttamiselle. Nykytilanteessa mainitut

toimijat eivät ymmärrä riittävän usein ja syvällisesti toisilleen lähettämiä signaaleja. Tästä esimerkkinä ovat MNE7-kokeiluharjoituksesta raportoidut havainnot.

Kokeiluharjoitus keskittyi tilannetiedon välittämisen haasteeseen tietoverkkoja ja -järjestelmiä ylläpitävien toimijoiden ja kokonaisuudesta vastaavien päätöksentekijöiden välillä. Keskeiset havainnot kiteytettiin kahteen kokonaisuuteen: Päätöksentekijälle ymmärrys kyberasiantuntijan toiminnasta on osin puutteellinen. Kyberympäristön tilannetieto on vaikeasti yhdistettävissä muuhun tilannetietoon ja se on vaikea ymmärtää osaksi kokonaistilannekuvaa. Luontaisesti sitä on helpompi käsitellä muusta toiminnasta erillisenä osana, joka kuitenkin on väärä lähestymistapa. Kehittyminen vaatii säännöllisiä kokeilutapahtumia tai -harjoituksia, jotta ymmärrys eri tasoille syntyisi ja syvenisi. Päätöksen teossa korostuu lopulta aina ihmisen osaaminen ja ymmärrys. Päätöksen tekijän kiinnostus ja aito vuorovaikutus ovat perusedellytyksiä tilannetietoisuuden syntymiselle.

Kyberasiantuntijoille tärkeää on kyky ymmärtää ja ennakoida vahingollisen toiminnan mahdolliset vaikutukset omaan kriittiseen tekemiseen. Asiantuntijoiden on kuitenkin vaikea kuvitella niitä tarpeita, joita päätöksen tekijällä voisi olla. Tähän problematiikkaan ei liene ratkaisuna teknisten apuvälineiden lisääminen, vaan pikemminkin johdon tietotarpeiden parempi ymmärtäminen. Tämä edellyttää kyberasiantuntijalta laajempaa ymmärrystä kokonaistoiminnasta ja omasta roolistaan siinä. Asiantuntijalta edellytetään siis monimutkaistuvassa ympäristössä entistä laaja-alaisempaa koulutusta ja ymmärrystä sekä pidempää kokemusta paremman kommunikaation synnyttämiseksi johdolle.

Sotilasorganisaation toiminnassa ei pidä väheksyä toimivan vuorovaikutuksen merkitystä. Jokaisen toimijan on astuttava pois omalta mukavuusalueeltaan laajemman ymmärryksen luomiseksi ja tavoitella näin molemmin puolin parempaa tilannetietoisuutta. Toki tarkastelussa on huomioitava organisaatiotaso, jossa lähtökohtaisesti voidaan olettaa alemman organisaatiotason toimijoiden olevan kiinteämmässä vuorovaikutuksessa päivittäisessä toiminnassa kuin ylemmän tason toimijat, jolloin ymmärrys voi olla luontaisesti parempi. Tarvitsemme kokemusperäistä tietoa kyberasiantuntijoiden ja yleisjohdon välisistä tiedonvaihtotarpeista, jonka perusteella on mahdollista kehittää ohjeistusta erilaisissa tilanteissa käytettävistä menetelmistä. Yleisjohtajia tulisi sijoittaa ”yhteysupseereiksi” kyberkeskuksiin ja päinvastoin. Lisäksi yleisjohtajien koulutukseen tulisi sisältyä jakso, jossa toimitaan osana ”kyberorganisaatiota” omaa organisaatiota vastaan.

Tarkasteltaessa maavoimien poikkeusolojen joukkojen varustelua tai tehtäviin sijoitetun henkilöstön osaamista on huomioitava asevelvollisuuteen perustuva järjestelmämme. Palkatun henkilöstön määrä suhteessa reserviläisiin on erittäin pieni. Tämä edellyttää taktisilta johtamisjärjestelmiltä yksinkertaisuutta ja helppoa hallittavuutta monimutkaisuuden ja erityisosaamisen sijasta. Tämä näkökulma onkin otettava johtamisjärjestelmien kehittämisessä erityisen tarkasti huomioon. Peruskäyttäjätasolle kehitettävät ja tarjottavat ratkaisut tulee rakentaa mahdollisimman yksinkertaisiksi.

Teknistyvät johtamisjärjestelmät edellyttävät joka tapauksessa sitä operoivalta ja ylläpitävältä organisaatiolta osaamista, joka on kyettävä kouluttamaan joukolle varusmiespalveluksen aikana ja ylläpitämään käytettävien kertausharjoitus-vuorokausien ja sitä tukevan vapaaehtoisen maanpuolustuskentän toimenpitein. Tässä suhteessa

asevelvollisuusarmeijan hyvänä puolena voidaan nähdä erittäin vahva ICT-alan osaaminen. Tunnistamalla jo varusmiespalveluksen aikana oikeat osaajat oikeisiin tehtäviin voidaan edesauttaa osaamisen syntymistä esikunta- ja viestiyksiköiden organisaatioihin. Osaamisen ylläpitäminen edellyttää vähintään avainhenkilöstön säännöllistä kertausharjoittamista, jotta hankittu ammattitaito kyetään säilyttämään ja mahdolliset siviilissä hankitut taidot jalkauttamaan sodan ajan joukkojen toimintaan.

Perusta poikkeusolojen toiminnalle on rakennettava jo normaaliolojen aikana. Johtamisjärjestelmät on rakennettava tietoturvallisuudelle asetettavat perusvaatimukset huomioiden. Kytkemällä tekninen tarkastustoiminta, mukaan lukien säännölliset haavoittuvuustestaukset, luontevaksi osaksi suorituskyvyn elinkaarihallintaa, luodaan perusta johtamisjärjestelmän ajan tasalle pitämiseksi. Järjestelmä-kokonaisuuksien valvontaan ja hallintaan luotavat tekniset apuvälineet ovat vain osa siihen liittyvää suorituskykyä. Jo aiemmin useasti mainittu henkilöstön osaaminen lienee vielä huomattavasti tärkeämpi osa. Tietoturvallisuuden perusta syntyy osaavasta ja vastuunsa tuntevasta henkilöstöstä. Tätä koulutuksen osa-alueen sisältöä tuleekin tarkastella jatkuvasti kriittisesti ja päivittää sitä tilanteen edellyttävällä tavalla.

Sotilaskulttuurissa organisaatiot ovat tottuneet toimimaan tiukastikin kontrolloitujen toimintatapojen mukaisesti - ja näin varmasti myös tulevaisuudessa. Tämä edellyttää kaikilla toiminnan tasoilla vakioituja prosesseja ja toimintamalleja sekä niiden mukaista säännöllistä harjoittelua. Tilanteenmukainen toiminta edellyttää aina selkärankaan iskostuneen rutiininomaisen toimintatavan, jonka jälkeen soveltaminen mahdollistuu tilanteen vaatimalla tavalla.

8.5 "Huomispäivän sotiakaan ei ratkaista verkoissa"

Tekniikan alati kiihtyvä kehitys ja sillä hallittavan tietomassan moninkertaistuminen nostaa tietoverkkojen merkityksen aivan uudelle tasolle ja on omalta osaltaan pakottanut puolustusvoimat rakentamaan kybersodankäynnin suorituskykyjä. Tämä ei kuitenkaan ole nykypäivänä pelkästään sotaväen haaste, vaan sen tärkeyteen on herätty laajasti koko tietoyhteiskunnassa. Ihmisten teknologiaosaaminen on syventynyt ja tietotekniikan hyödyntäminen kuuluu lähes jokaisen kansalaisen perustoimintoihin. Tietotekniikka on arkipäiväistynyt merkittävällä tavalla, joka kehityspolkuna voidaan tunnistaa myös puolustusvoimissa. Kaupallisen teknologian käytön yleistyessä kehitys jalkauttaa taistelunjohtojärjestelmät perusyksiköihin ja päätelaitteet lähes jokaiselle taistelijalle. Toki matkaviestimet ja erityisesti älypuhelimet ovat tehneet tämän siviilimaailmassa jo aika päiviä sitten.

Tietoverkkosodankäynti näyttäytyykin monilla tavoin myös tietoyhteiskuntakehityksessä. Hyvä niin, sillä kyberpuolustuksen suorituskykyjä ei ole mahdollista, eikä edes järkevää rakentaa pelkästään puolustusvoimalähtöisesti. Verkottuneen yhteiskunnan kehittämisen tueksi on valtioneuvoston johdolla rakennettu kansallinen kyberturvallisuusstrategia, jolla hallinnonaloilla suoritettavia toimenpiteitä koordinoidaan. Merkittäviä toimenpiteitä onkin käynnistetty jo varsin mittava määrä. Pääesikuntaan on perustettu aiheeseen vihkiytynyt sektori. Olemme niin ikään siirtymässä erillisistä, varsin omaehtoisesti ja vaihtelevalla menestyksellä toteutuneista tietoliikenneratkaisuista yhteiseen kaikkia tarvitsijoita palvelevaan turvallisuusverkkoratkaisuun. Kybersuorituskyvyt ovat niin ikään prioriteetissa kansainvälisiä yhteistyömuotoja ja painotuksia tarkasteltaessa. Taustalla on hyvä muistaa, että olemme edelleenkin

sidoksissa varsin voimallisesti kansalliseen infrastruktuuriin ja voimavaroihin. Esimerkiksi tele- ja tietotekniikka-alan yritysten merkitystä poikkeusoloissa ja niihin varautumisessa ei ole millään muotoa syytä aliarvioida tai laiminlyödä – energia-alan yrityksistä puhumattakaan.

Kyberpuolustuksen lähtökohdat, tavoitteet ja päämäärät yhtyvät muuhun sodankäyntiin. Tarvetta oman aselajin, toimialan tai peräti puolustushaaran rakentamiselle ei ole, vaikkakin kyberulottuvuudesta muodostuva kokonaisuus on niin merkittävä, että se tulee huomioida yhä vahvemmin operatiivisessa päätöksen teossa. Ristiriitaiset tarpeet ja tavoitteet on ratkaistava kokonaisuuden kannalta parhaalla tavalla, ei osajärjestelmiä optimoimalla. Kyberistä ei tule sellaista sodankäynnin ulottuvuutta, joka ratkaisisi sodat yksin. Näin siitäkin huolimatta, että jo informaatiosodankäynnissä keskeinen kysymys oli, voitaisiinko sillä toteuttaa sotataidon huipentuma - sodan voittaminen ilman taistelua. ”Vanhanaikaisten” sotien käyminen ei olekaan millään muotoa todiste siitä, ettei sodan voittamista ilman taistelua tapahtuisi. Krimin liittäminen Venäjään on hyvä esimerkki tästä.

Tietoverkkosodankäynnillä tuetaan muita operaatioita, joka pelkistettynä tarkoittaa oman toiminnan mahdollistamista sekä suojaamista vihollisen vaikutuksilta ja samanaikaista vihollisen toiminnan vaikeuttamista. Maapuolustuksessa siihen kytkeytyy paljon muutakin kuin pelkästään verkossa tapahtuva toiminta. Se on osa operaatioturvallisuutta, jossa verkkojen ja verkostojen ohella pitää suojautua myös fyysiseltä vaikuttamiselta. Käytettävissä olevat välineet määräytyvät hankittavien järjestelmien ja niiden suorituskykyjen, mutta myös käytettävissä olevien toimivaltuuksien mukaan. Tähän kytkeytyy vahva poliittinen ulottuvuus, jossa tietoverkkosodankäynti haastaa myös valmiuslainsäädännön kehittäjät. Verkkoulottuvuus tulee huomioida etupainoisesti valmiuden säätelyn eri vaiheissa, jottemme kriisin syvetessä jää ”tuleen makaamaan” ja joudu valmistautumattomana ”kybertulikasteen” yllättämäksi.

Johtamisjärjestelmä ja siihen kuuluvat viesti- ja tietojärjestelmät ovat keskeinen osa tämän päivän taistelukenttää - tulevaisuudesta puhumattakaan. Johtamisjärjestelmän tekninen tuntemus ja kyberulottuvuuden ymmärtäminen osana kokonaisuutta onkin kyberosaamisen kehittämisen perusta. On ymmärrettävä, mitä ollaan suojaamassa. Merkittävin ero kyberin ja ”perinteisten” sodan ulottuvuuksien välillä on se, että kyberissä taistelukentäksi muodostuvat verkot ja niissä toimivat järjestelmät sekä tietovarannot. Verkkotaistelukenttä ei siis tunne maantieteellisiä rajoja, vaan näyttäytyy globaalina, jonka käsitteellistämistä vihollisen epämääräisyys vaikeuttaa merkittävästi.

Toimijoiden määrä kyberulottuvuudessa kasvaa jatkuvasti. Monet valtiot panostavat vahvasti kybersuorituskykyihin ja kehittävät omia kyberorganisaatioitaan, yhteistoimintaa ja johtamista, mutta toistaiseksi vahva koordinaatio eri toimijoiden väliltä puuttuu. Keskeisimmät kybervaikuttamisen kohteet ovat poliittinen päätöksentekojärjestelmä sekä energia- ja taloussektori, joilla luonnollisesti on välillinen vaikutus myös puolustusvoimien toimintaan. Haasteellisuutta asian hallitsemiseen tuo se, että kybertoimintaan kytkeytyy niin nyt kuin tulevaisuudessakin merkittävällä tavalla verkkorikollisten ja haktivistien toiminta, joiden toiminnassa lainsäädäntö ja politiikka eivät ole millään muotoa rajoittavia tekijöitä.

Vastaavalla tavalla, kun meillä on oikeus puolustaa maa-, meri- ja ilmatilaamme vihollisen hyökkäyksiltä, tulee meillä olla oikeus puolustaa tietoyhteiskunnan verkkoja ja järjestelmiä eli kyberulottuvuutta – tarvittaessa myös sotilaallisin keinoin. Samalla myös sodankäynnin raja hämärtyy, joka tekee asiasta vieläkin haasteellisemman ja edellyttää politiikoilta rohkeita päätöksiä jo syvässä rauhan tilassa – tässä on hyvä seurata millaisia päätöksiä lähialueella olevat valtiot tekevät. Tietoverkkosodankäynnin luonteesta ja toimintatavoista johtuen on siihen valmistauduttava kaikilla tasoilla niin siviili- kuin sotilasyhteisöissä, jossa pätee varsin mainiosti sanonta ”yhtä vahva, kuin heikoin lenkki”, sillä on turha uskotella, että verkkoulottuvuus jäisi vastustajalta käyttämättä.

Maavoimat uudistavat taistelutapaansa kokonaisvaltaisesti. Lähes kaikki elementit ovat muutoksessa, jossa tavoitteena on uuden konseptin optimaalinen tukeminen. Maavoimien taistelu 2015 korostaa taistelutilan valmistelujen merkitystä, johon myös verkkotaisteluvalmistelut on kytkettävä. Konseptiin sisällytetyt ajatukset aktiivisesta, yllätykseen pyrkivästä ja syvästä tappiota kumuloivasta taistelusta, johon kytkeytyvät vahvasti menestyksen hyväksikäyttö sekä oveluuden ja harhauttamisen elementit istuvat varsin mallikkaasti myös tietoverkkopuolustuksen kehittämiseen. ”Kyberesimerkiksi” taistelutilan muokkaamisesta voidaan nostaa Edward Snowden, joka onnistui hyvinkin ansiokkaasti muokkaamaan internettiä itselleen edulliseksi. Kyberpuolustuskonsepti pitää rakentaa yhdessä, mutta sisään on ehdottomasti kirjattava kyky saarekkeisesta, täysin muista erillään tapahtuvasta toiminnasta. Passiivisella, syviin poteroihin perustuvalla linjapuolustuksella ei huomispäivän taistelussa ole mahdollisuuksia menestyä. Puolustuksen on oltava syvä, koko yhteiskunnan käsittävä ja siihen on sisällytettävä vaikuttamisen elementtejä – hyökkäys kun on edelleenkin paras puolustus!

Päätähuimaavasta teknisestä kehityksestä huolimatta kansallinen puolustus rakentuu tulevaisuudessakin reserviläisten ja heidän osaamisensa varaa. Kaadereiden vähäisyys ja sodan kitka korostavat tietoverkkosodankäyntikykyjen kehittämisessä valittujen teknisten ja toiminnallisten ratkaisumallien yksinkertaisuutta. Teknisinä keinoina voidaan käyttää muun muassa jakelunhallintaa, palveluluetteloita, verkkovarastointia osana ohjelmoitavan elektroniikan ylläpitoa, pääsyoikeuksien rajaamista sekä tietoliikenteen ja palveluiden valvontaa, jonka tulisi olla mahdollisimman pitkälle automatisoitua. Toiminnallisesta näkökulmasta menestyminen verkkotaistelukentällä edellyttää ajantasaista tietoturvaohjeistusta, sen mukaisesti rakennettuja ja ylläpidettyjä järjestelmiä sekä ennen muuta henkilöstön jatkuvaa kouluttamista, jossa myös asenteellinen näkökulma saa riittävän huomion.

Uudistettu taistelutapa yhdessä uusien viesti- ja tietojärjestelmien kanssa siirtää meidät yhä syvemmälle järjestelmäajattelun polulla – uhkine ja mahdollisuuksineen. Viimeistään internet-protokollan yleistyminen on poistanut loputkin tekniset esteet verkkosodankäynnin läpimurrolta. Järjestelmät älyllistyvät ja taistelutila tyhjenee, jonka seurauksena yksittäisten henkilöiden osaamisen merkitys nousee entistäkin tärkeämpään asemaan. Edellä mainittu ei sulje millään muotoa pois sitä, etteikö johtajien tulisi osata edelleenkin käyttää joukkoja ja välineitä tilanteen vaatimalla ja mahdollisimman innovatiivisella tavalla. Ja mikä hienointa käynnissä oleva kehitystyö synnyttää käyttöömme elementtejä, joilla on uskoaksemme lähes rajattomat mahdollisuudet rakentaa juuri sitä peräänkuulutettua suomalaista kyberpuolustusta.

Lähdemateriaali

Maavoimien esikunta, Suunnitteluosasto: Kenttäohjesääntö 3.1 Maaoperaatiot (L) STIV, Maaliskuu 2013.
Maavoimien esikunta, Johtamisjärjestelmäosasto: Johtamisen, hallinnon ja johtamisjärjestelmän muutoksen perusta maapuolustuksessa 2010-2015.
Pääesikunta, Johtamisjärjestelmäosasto: Kenttäohjesääntö 6 Johtamisjärjestelmä (L) STIV, Heinäkuu 2014.
Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma, Turvallisuuskomitea 11.3.2014
Pääesikunta, Johtamisjärjestelmäosasto: Kyberpuolustushankkeen hankesuunnitelma (L) STIV, huhtikuu 2014.
MNE7 Cyber situational awareness -kokeilutapahtuman raportti, PVJJK:n ak AI8375, 20.4.2012
PVHSM turvallisuus 402 - PEOPOS tietoturvakoulutus puolustusvoimissa
Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013.
Candolin Catharina, Kärkkäinen Anssi: Kyberpuolustuksesta uusi puolustushaara, Viestimies 2/2014.
Hartikainen Esko: Vaikuttaminen maavoimien uudistetussa taistelutavassa, Sotilasaikakauslehti 11/2012.
Hirvonen Jussi-Petri: Kenttähuolto uudistuu vastaamaan taistelutavan muutokseen, Sotilasaikakauslehti 4/2013.
Huovinen Petri, Kärkkäinen Anssi, Lehto Mikko, Noronen Lauri, Pispa Kimmo, Viita Ville: Sotilaallisen kybersuorituskyvyt – Toimintaympäristön tarkastelua, osa 1, Sotilasaikakauslehti 12/2013.
Huovinen Petri, Kärkkäinen Anssi, Lehto Mikko, Noronen Lauri, Pispa Kimmo, Viita Ville: Sotilaallisen kybersuorituskyvyt – Näkökulma suorituskyvyn kehittämiseen, Sotilasaikakauslehti 2/2014.
Kauppinen Harri: Taistelutilan muokkaaminen maavoimien uudistetussa taistelutavassa, Sotilasaikakauslehti 1/2013.
Kiravuo Timo, Särelä Mikko, Manner Jukka: Kybersodan taistelukentät, Sotilasaikakauslehti 3/2013.
Kuparinen Petri: Tiedustelu maavoimien uudistetussa taistelutavassa, Sotilasaikakauslehti 11/2012.
Kvist Jouni: Maavoimien uudistettu taistelutapa – näkemyksiä ruohonjuuritasolta, Sotilasaikakauslehti 3/2013.
Lankila Rauno: Maavoimien uudistettu taistelutapa ilmatorjunnan kannalta tarkasteltuna, Sotilasaikakauslehti 2/2013.
Lehto Martti: Kybermaailman määrittelyä, Sotilasaikakauslehti, 12/2013.
Limnéll Jarno: Kybermaailma osana sodankäyntiä, Viestimies 1/2014.
Mattila Juha: Uudistetun maataistelun johtaminen ja viestitoiminta, Sotilasaikakauslehti, 12/2012.
Parkatti Pekka: Maavoimien taistelu uudistuu, Sotilasaikakauslehti 9/2012.
Tuukkanen Topi: Puolustusvoimien rooli tietoverkkosodankäynnissä? Rannikon puolustaja 1/2014.
Valkeajärvi Jukka: Uudistetun taistelutavan joukot, varustaminen ja joukkotuotanto, Sotilasaikakauslehti 10/2012.
Virtanen Jukka-Pekka: Maavoimien verkkotaistelukyky - osa voiton kaavaa, Sotilasaikakauslehti, 12/2013.

9.

Kybertaistelu ilmavoimaympäristössä

Dosentti Martti Lehto
Jyväskylän yliopisto
Tietotekniikan laitos

Kyberturvallisuuden dosentti, sotatieteiden tohtori, eversti evp. Martti Lehto on palvellut ilmavoimissa eri tehtävissä ja Pääesikunnassa vuosina 1978–2007. Jäätyään eläkkeelle Ilmavoimien esikunnan apulaisesikuntapäällikön tehtävästä, hän suoritti jatko-opinnot MPKK:n Johtamisen laitoksella vuosina 2007–2012. Vuodesta 2009 hän on työskennellyt kyberturvallisuuden maisteri- ja jatkokoulutusohjelmien koordinaattorina sekä kyberturvallisuuden ja kyberpuolustuksen tutkijana ja opettajana Jyväskylän yliopiston tietotekniikan laitoksella. Hän on osallistunut asiantuntijana mm. Suomen kyberturvallisuusstrategian ja sen toimeenpanosuunnitelman sekä kansallisen kyberturvallisuuden strategisen tutkimusagendan laadintaan. Hän toimii asiantuntijana Euroopan verkko- ja tietoturvaviraston (ENISA) kyberturvallisuuden tutkimusta ja koulutusta käsittelevässä työryhmässä. Hänellä on yli 50 julkaisua, tutkimusraporttia ja artikkelia kansainvälisissä ja kansallisissa journaaleissa, konferenssijulkaisuissa ja kirjoissa, joka käsittelevät puolustusvoimien johtamisjärjestelmää, kyberturvallisuutta ja -puolustusta, informaatiosodankäyntiä sekä puolustus- ja turvallisuuspolitiikkaa.

Tiivistelmä
Elektronisen sodankäynnin, informaatiosodankäynnin ja kybersodankäynnin operaatiot muodostavat kyberajan ei-kineettisten verkostoperustaisten operaatioiden kokonaisuuden. Ilmasodankäynnissä nämä operaatiot muodostavat verkottuneen kokonaisuuden, jossa eri operaatiomuotojen avulla pyritään saavuttamaan Ilmasodankäynnille asetetut tavoitteet. Kybersodankäynti ei ole syrjäyttänyt aikaisempia ei-kineettisiä sodankäynnin muotoja vaan laajentunut kybermaailman uusille bittien muodostamille toiminta-alueille.

Kyberturvallisuusteknologian kehitys ei ole irrallinen ilmiö vaan se on vahvasti linkittynyt yhteiskuntarakenteisiin ja sen eri turvallisuustoimijoiden tarpeisiin ja odotuksiin. Uusista teknologisista ratkaisuista otetaan käyttöön ne mitkä parhaiten tuottavat lisäarvoa, tehokkuutta, vaikuttavuutta jne.

Teknologian kehitys on jatkuvaa, syklistä, epälineaarista ja perustuu aikaisemmille innovaatioille. Mitään ei luoda tyhjästä vaan jokaisella teknologialla on historiansa. Teknologialla on suhde omaan aikaansa, ilmiö valjastetaan teknologian käyttöön, kun teknologian kypsyysaste on oikea.

Kyberteknologian kehittämisen rinnalla on huolehdittava kybersodankäynnin kognitiivisen dimension kehittämisestä. Yksilö (päätöksen tekijä – yksittäinen sotilas) laitteiden ja järjestelmien käyttäjänä on viimekädessä luomassa kybersuorituskykyisyyttä.

Kyberteknologia nopea kehitys ja systeemien monimutkaistuminen edellyttävät kognitiivisen osan kehittämistä rinnan teknologian kanssa. Kehittämisen keskiöön nousee kaikkien toimijoiden kyberosaamisen kehittäminen uusien suorituskykyvaatimusten edellyttämälle tasolle.

Kybersodankäynnin suorituskykyjen kehittämisellä luodaan ilmasodankäynnin evoluution transformaatiohyppyjä, jotka vievät sodankäynnin luonnetta ja olemusta uusille tasoille ja tuottavat uuden strategisen tilan, jossa ilmasota voitetaan tai hävitään.

9.1 Johdanto

Maailma, jossa elämme, on muuttunut toiminnallisesti ja rakenteellisesti sadassa vuodessa varsin paljon. Asevoimien rooli ja tehtävät ovat kuitenkin muuttuneet varsin vähän, jos asiaa tarkastellaan riittävän abstraktilla tasolla. Ilmasodan luonteessa, tavoitteissa ja teoriassa on tapahtunut varsin vähän muutoksia lentokoneen historian aikana. Muutos on siis olemisen ja toiminnan tavassa – siinä, miten asioita tehdään, millaisissa rakenteissa toimitaan ja millaisilla välineillä asioita tehdään.

Ilmakomponentin uudet suorituskyvyt antavat mahdollisuuden sekä aseellisen voiman käyttöön että ei-kineettisen voiman käyttöön kyberavaruudessa. Lisäksi nämä suorituskyvyt antavat mahdollisuuden toimia uudessa epälineaarisessa ja rajoiltaan epämääräisessä taistelutilassa. Tässä tilassa tulee voida integroida saumattomasti ilmassa, pinnassa, pinnan alla, avaruudessa ja kyberavaruudessa toimivia miehitettyjä ja miehittämättömiä alustoja, joiden avulla voidaan havaita, seurata ja identifioida maalit sekä johtaa asejärjestelmiä halutun vaikutuksen saavuttamiseksi. Verkottuneiden ei-kineettisten operaatioiden johtamisessa keskeiseksi elementiksi nousee aika. Johtamisprosessissa tarvitaan sisällöltään mahdollisimman tarkkaa ja oikein aikautettua informaatiota, jopa liikkeessä, jotta keskitetty johtaminen ja hajautettu toiminta voidaan toteuttaa sekä suojata oma toiminta kybertaistelutilassa.

9.2 Ilmapuolustuksen kybersuorituskyvyn kehittäminen

9.2.1 Kybersodankäynnin määrittely

Kybersodankäyntikäsitteelle ei ole yleisesti hyväksyttyä määritelmää ja sitä käytetään hyvinkin laajasti kuvaamaan tapahtumia ja toimia. Kybersodankäyntikäsite tuli voimakkaasti esiin vuosina 2008–2010 ja se osin syrjäytti aikaisemmin käytetyn informaatiosodankäynti-käsitteen, joka oli formuloitu 1990-luvun puolivälissä. Toisille kybersodankäynti on sotaa virtuaalimaailmassa, toisille se on vastakohta kineettiselle sodankäynnille. OECD:n vuoden 2011 raportin mukaan kybersodankäyntiin liittyy samat elementit kuin ns. tavalliseen sotaankin: kosto ja pelote. Tutkijat yhtyvät käsitykseen siitä, että kybersodankäynnin määrittelyn tulisi perustua sodan tavoitteisiin ja motiiveihin eikä niinkään kyberoperaatioiden muotoihin. Heidän mielestään sota on aina muodoltaan laaja-alainen käsittäen kaikki sodankäynnin muodot, jolloin kybersota on yksi sodankäynnin muoto, jota käytetään perinteisen kineettisen vaikuttamisen rinnalla.[1]

[1] OECD/IFP Project on Future Global Shocks, report: Reducing Systemic Cybersecurity Risk, 14.1.2001, s. 13.

Vuonna 2008 Yhdysvaltain ilmavoimat määritteli kyberavaruuden seuraavasti: *"Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."* [2]

Samana vuonna Yhdysvaltain apulaispuolustusministeri Gordon England määritteli kyberavaruuden seuraavasti: *"Cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*[3]

Kybersodankäyntiin pätevät sodankäynnin yleiset periaatteet. Kyberoperaatioita ei toteuteta satunnaisesti, vaan niitä edeltää tilannekuvan muodostaminen tiedustelun ja valvonnan avulla sekä tarkka maalien analysointi ja valinta.[4]

Kybersodankäynnissä käytetään hyväksi globaaleja tietoverkkoja. Keväältä 2007 Viroon kohdistui verkkohyökkäysten sarja, jonka kohteina olivat kolmen viikon ajan mm. valtiojohto, poliisi, pankkilaitos, media ja yritysmaailma. Päätoimintamuotoina olivat palvelunestohyökkäykset, joiden kohteina olivat mm. web-serverit, e-mail-serverit, DNS-serverit ja reitittimet. Virolaisten mukaan tätä hyökkäystä ei voida pitää varsinaisena kybersodankäyntinä vaan kyberkonfliktina.[5] Muodoiltaan siinä oli elementtejä, jotka antavat viitteitä valtiollisesta kybersodankäynnistä, mutta Viron oman määrittelyn mukaisesti kysymys oli sotaa alemmasta kyberkonfliktista, koska Viro ja Venäjä eivät olleet sotatilassa keskenään.

Venäjän ja Georgian välinen sota, toiselta nimeltään Etelä-Ossetian sota oli elokuun 2008 ensimmäisellä viikolla Georgian sotavoimien ja Etelä-Ossetian armeijan sekä Venäjän federaation joukkojen välillä käyty sota. Useat georgialaiset ja eteläossetialaiset verkkosivut joutuivat jo 8. elokuuta palvelunestohyökkäysten kohteiksi. Georgialaisia sivustoja vastaan hyökkäys alkoi 9. elokuuta vastaisena yönä. Hyökkäykset kohdistuivat Georgian valtion ja presidentin sivustoille sekä Georgia-online-sivustolle. Georgian viranomaiset päättivät 11. elokuuta taistella ”disinformaatiota” vastaan ja keskeyttivät kaikkien venäläisten televisiokanavien lähetykset maassa. Georgian johtava internetyhteyden tarjoaja Caucasus Online esti pääsyn kaikille .ru-päätteisille verkkosivuille. Venäjän uutistoimiston RIA Novostin sivuille hyökättiin ja ne kaatuivat muutamaksi tunniksi 10. elokuuta. Venäläisen englanninkielisen tv-kanavan RussiaTodayn sivuilla hyökättiin ja ne kaatuivat 12. elokuuta noin vuorokauden ajaksi. Georgian keskuspankin ja puolustusministeriön sivuille murtauduttiin, joissa kuvamateriaalia muutettiin.

---

[2] Program Action Directive (PAD) 07-08, *Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER)*, Office of the Secretary of the Air Force, Washington, D.C January 24, 2008.

[3] Gordon England, "The Definition of Cyberspace," memorandum, Washington, D.C., May 12, 2008, in Air Force Cyber Command (Provisional) Decision Support, RAND Corporation, 2010.

[4] Filiol Eric, Operational Aspects of Cyberwarfare or Cyber-Terrorist Attacks: What is truly Devastating Attack Could do, Proceedings of the 8th European Conference on Information Warfare and Security, University of Minho and the Military Academy Lisbon, Portugal 6-7 July 2009, s. 71 - 79.

[5] Rain Ottis, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Proceedings of the 7th European Conference on Information Warfare and Security University of Plymouth, UK, 30 June – 1 July 2008, s. 163 - 167.

9.2.2 Sodankäynnin evoluutio

Antoine Bosquet jakaa sodankäynnin evoluution neljään periodiin. 1600–1700-lukujen manööveri-intensiivinen toimintatapa perustui mekanistiseen (clockwork) sodankäyntiin. Tämä aikakausi huipentui Frederik Suuren kehittämään Preussin armeijaan, joka oli aikansa tehokkain. Hän pyrki ratkaisemaan komentajan ikuisia haasteita: taistelukentän epävarmuus ja komentajan tahdon täytäntöönpanon rajoitukset. Juuri kun näytti siltä, että Frederik Suuri olisi löytänyt ratkaisun asevoiman käytölle, sodankäyntiin tuli uusia dynaamisia vaatimuksia.[6] 1800-luvun alussa alkoi termodynamiikan kehittyminen, joka näkyi joukkojen operatiivisen ja jopa strategisen liikkuvuuden parantumisena. Aikaisemmin joukkojen liikkuvuus oli perustunut ”ihmisvoimaan” ja ”hevosvoimaan”, nyt niitä voitiin korvata aluksi höyryvoimalla sitten polttomoottorin voimalla. Sodankäynnistä tuli energiaintensiivinen, joka näkyi sekä aseissa että joukkojen liikkuvuudessa. II maailmasota oli tämän vaiheen huipentuma, jossa materiaalisista resursseista tuli sodan voiton avain.[7]

9.2.2.1 Elektroninen sodankäynti

Toisen maailmansodan jälkeen elektromagneettisesta ulottuvuudesta tuli uusi sodankäynnin elementti. Vietnamin sodasta aina Irakin ensimmäiseen sotaan 1991 saakka johtamisen ja päätöksenteon tarvitseman informaation riittämättömyyttä taistelukentällä pyrittiin ratkaisemaan tietotekniikan avulla. Taistelukentän epävarmuuden uskottiin johtuvan informaation puutteesta. Uusi kybernetiikan aika pyrki ratkaisemaan ongelmia tietokoneiden laskentakyvyn avulla ja luomalla uusia kommunikaatioteknologioita. Teknologiaa lähestyttiin erilaisten systeemianalyyttisten mallien avulla, jolloin laitteet ja koneet muodostivat monimutkaisia systeemeitä. Peter Checkland määrittelee systeemin ominaisuuksiksi, että se koostuu erityisestä, määriteltävissä olevasta yhtenäisestä kokonaisuudesta, jonka osat ovat hierarkkisessa suhteessa toisiinsa. Nämä osat voivat kukin muodostaa oman systeeminsä. Siitä huolimatta systeemi on sellaisenaan jotain enemmän kuin osiensa – alasysteemiensä – summa. Tämä johtuu siitä, että sen luonteeseen kuuluu osien lisäksi myös prosesseja niiden välillä, vuorovaikutusta, informaation ja energian siirtoa.[8] Kylmän sodan aikana informaatioteknologiaa kehitettiin ratkaisuksi taistelukentän kaaoksen ja epävarmuuksien ratkaisemiseen. Tietoteknisten järjestelmien miniatyyrisoinnin, diffuusion ja uusien kommunikaatiovälineiden seurauksena on ollut informaatioparadigman kehittyminen. Kaaos- ja kompleksisuusteorioiden kehittyminen on lisännyt ymmärtämystä verkostojen ja hajautetun johtamisen mahdollisuuksista.[9]

Elektronisen sodankäynnin (Electronic warfare, EW) keinoin hyökkääjä pyrkii vaikuttamaan informaation kulkuun siten, että johtamisen ja tulenkäyttöjärjestelmien luotettavuus alenee ja informaatiorakenteiden käytettävyys pienenee. Elektroninen sodankäynti on keskeinen tekijä tavoiteltaessa ilmanherruutta ja informaatioylivoimaa. EW:n tehokkuus perustuu sen suhteeseen ilma- ja informaatio- ja kyberoperaatioihin, joita tuetaan laajalla skaalalla erilaisia kyvykkyyksiä.

---

[6] Bosquet Antoine, The Scientific Way of Warfare, Columbia University Press, New York, 2009, s. 62.
[7] Bosquet Antoine, The Scientific Way of Warfare, Columbia University Press, New York, 2009, s. 90 - 91.
[8] Checkland P. (1981), Systems Thinking, Systems Practice, John Wiley & Sons Ltd., reprinted version 1990, s. 4 - 11.
[9] Bosquet Antoine, The Scientific Way of Warfare, Columbia University Press, New York, 2009, s. 161.

9.2.2.2 Informaatiosodankäynti

Tieto on aina ollut tärkeää taistelukentällä. Taistelukenttä on laajentunut taistelutilaksi, jossa joukot ja sotilaat ovat tulleet riippuvaiseksi informaatiosta, sähköisestä tiedonsiirrosta ja energian jakelusta. Martin C. Libicki määritteli vuonna 1995 informaatiosodankäynnin (Information Warfare, IW) osa-alueiksi:[10]

- Johtamissodankäynti (command-and-control warfare, C2W)
- Tiedusteluperusteinen sodankäynti (intelligence-based warfare, IBW)
- Elektroninen sodankäynti (electronic warfare, EW)
- Psykologinen sodankäynti (psychological operations, PSYOPS)
- Hakkerisodankäynti (hackerwar)
- Taloudellinen informaatiosodankäynti (information economic warfare, IEW)
- Kybersota (cyberwar)

Hänen määrittelyssään informaatiosodankäynnistä tuli yläkäsite, joka sisältää sekä elektronisen sodankäynnin että kybersodankäynnin osa-alueet. Yhdysvaltain ilmavoimissa informaatio-operaatiot jaetaan seuraavasti: [11]

- vaikutusoperaatiot (Influence Operations)
- psykologiset operaatiot (psychological operations, PSYOPS)
- sotilaallinen harhautus (military deception, MILDEC)
- operaatioturvallisuus (operations security, OPSEC)
- vastatiedusteluoperaatiot (counterintelligence (CI) operations)
- vastapropagandaoperaatiot (counterpropaganda operations)
- viestintä (public affairs (PA) operations)
- Verkko-operaatiot (Network Warfare Operations)
- verkkohyökkäys (network attack, NetA)
- verkkopuolustus (network defense, NetD)
- verkko-operaatiotuki (network warfare support, NS)
- elektronisen sodankäynnin operaatiot (Electronic Warfare Operations)
- elektroninen hyökkäys (electronic attack)
- elektroninen suojautuminen (electronic protection)
- elektronisen sodankäynnin tuki (electronic warfare support)

Suomalaisen näkemyksen mukaan ”informaatiosodankäynti on yhteiskunnalliseen ja sotilaalliseen päätöksentekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista ja tältä suojautumista käyttämällä hyväksi informaatioympäristöä. Informaatiosodankäyntiä voidaan käydä yhteiskunnallisin, poliittisin, psykologisin, sosiaalisin, taloudellisin ja sotilaallisin keinoin kaikilla sodankäynnin tasoilla. Informaatiosodankäynti koskee koko yhteiskuntaa ja on siten luonteeltaan pääosin turvallisuuspoliittista sekä toiminnallisesti valtakunnallista strategista tasoa koskettavaa toimintaa. Informaatiosodankäynnissä päämääränä on kansallisten tavoitteiden mukaisesti hankkia ja ylläpitää informaatioylivoima.”[12]

[10] Libicki Martin C., What Is Information Warfare? Strategic Forum Number 28 May 1995.
[11] Air Force Doctrine Document 3-13, Information Operations, 11 January 2005.
[12] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004.

Suomalaisessa doktriinissa sotilaalliset informaatio-operaatiot (SIO) ovat puolustusvoimien suunnittelemia toimia, joilla suojataan elintärkeä informaatioympäristö. Sotilaallisilla informaatio-operaatioilla vaikutetaan valikoitujen kohteiden informaatioon, informaatiorakenteisiin ja informaatiotoimintoihin sekä toimijoiden käyttäytymiseen samalla kun vastaavalta vihamieliseltä toiminnalta suojaudutaan.[13]

Informaatio voidaan määritellä resurssiksi, jolla on kaksi ulottuvuutta. Se muodostuu eri keinoin kerätystä datasta sekä systeemistä, jonka avulla dataa on tulkittu ja analysoitu, siten tuottaen datalle merkitystä. Teknologian avulla voidaan lisätä informaation arvoa. Tietokantojen, tietoverkkojen ja data-analyysin avulla asevoimat voivat luoda korkeamman tason jaettua tilannetietoisuutta, paremmin synkronoitua johtamista ja tiedustelua sekä muuttaa informaatioylivoima ylivoimaksi myös fyysisessä taistelutilassa.

9.2.2.3 Verkkokeskeinen sodankäynti

Yhdysvaltalaisessa diskurssissa tuli 1990-luvun lopulla käyttöön käsite verkkokeskeinen sodankäynti (Network Centric Warfare, NCW), jossa informaation rinnalle nostettiin verkosto. NCW-konsepti tuli julkisuuteen vuonna 1998 US Naval Instituten julkaisussa "*Network-Centric Warfare: Its Origin and Future*", jonka olivat laatineet varaamiraali Arthur K. Cebrowski ja John Gartska. Heidän mukaansa "melkein 200 vuoden ajan välineet ja sodankäynnin taktiikka ovat kehittyneet sotilaallisten teknologioiden kanssa. Nyt perustavanlaatuiset muutokset vaikuttavat sodan luonteeseen".[14]

Yhdysvaltalainen termi verkostokeskeinen sodankäynti ja brittiläinen vastine verkostoavusteinen puolustus (Network Enabled Defence, NED) viittaavat samaan käsitteeseen. Kyseessä on verkottuneesti toimivan yhteiskunnan kaikkien voimavarojen hyödyntäminen sotilaallisiin tarkoituksiin. Eron ajattelussa tekee suhtautuminen verkoston asemaan – onko verkosto määräävässä asemassa vai verkostomaisena alustana eri järjestelmille.[15]

Verkkokeskeinen sodankäynti ja kaikki siihen liittyvät sodankäynnin alalla tapahtuneet vallankumoukselliset muutokset syntyvät ja saavat voimansa Yhdysvalloissa tapahtuvista perustavaa laatua olevista yhteiskunnallisista muutoksista. Näille muutoksille on ollut ominaista ennen muuta yhtäaikainen kehitys talouselämän, tietotekniikan, liike-elämän toimintatapojen ja organisaatioiden aloilla ja niitä yhdistää kolme teemaa:[16]

- painopiste on siirtynyt alustoista verkostoihin.
- on siirrytty tarkastelemasta toimijoita itsenäisinä tekijöinä tarkastelemaan niitä osana jatkuvasti mukautuvaa ekosysteemiä ja
- on ymmärretty, kuinka tärkeitä strategiset valinnat ovat tällaisiin ekosysteemeihin mukautumiselle tai jopa niissä selviytymiselle.

---

[13] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004.

[14] Cebrowski Arthur K. and Garstka John J., Network-Centric Warfare: Its Origin and Future, Naval Institute Proceedings, Annapolis Maryland, January 1998.
Senenko Christopher M., Network Centric Warfare And The Principles Of War, Master of Science Degree, Joint Forces Staff College, Joint Advanced Warfighting School, 5 April 2007, s. 1 - 6.

[15] Ilvonen Janne, Vaikutusperusteiset konseptit: EBO-, EBAO-, SOD- ja CA-käsiteanalyysi, diplomityö, MPKK, 2009.

[16] Cebrowski Arthur K. and Garstka John J., Network-Centric Warfare: Its Origin and Future, Naval Institute Proceedings, Annapolis Maryland, January 1998.

Konsepti julkaistiin myöhemmin kirjassa *Network Centric Warfare*, jonka kirjoittajia olivat John Gartskan lisäksi David S. Alberts ja Frederick P. Stein. Heidän määrittelynsä mukaan verkostokeskeinen sodankäynti on informaatioylivoiman mahdollistava toimintakonsepti, joka luo kasvavaa taisteluvoimaa verkottamalla sensorit, päätöksentekijät ja aselavetit, jotta saavutetaan jaettu tilannetietoisuus, kasvava päätöksenteon nopeus, suurempi toiminnan nopeus, suurempi voimankäytön fyysinen vaikuttavuus, suurempi omien joukkojen eloonjäämistodennäköisyys ja suurempi toiminnan itsesynkronointi.[17]

Verkostokeskeinen sodankäynti käsitteenä kuvaa laajasti ottaen verkostoituneiden strategioiden, uusien taktiikoiden, tekniikoiden, menetelmien ja organisaatioiden yhdistelmää, jolla voidaan saavuttaa ratkaiseva etu – ylivoimatekijä – sotilaallisissa operaatioissa.[18]

Verkostokeskeisyys sodankäynnissä on tarkoittanut siirtymistä tietokoneiden laskentaintensiivisestä mallista verkostointensiiviseen malliin. Tässä mallissa Antoine Bosquet yhdistää kompleksisuuden ja kaoottisuuden muodostaen monimutkaisen kaaosmallin (chaoplexity). Tämän mallin kehityssuuntia ovat olleet verkkokeskeinen sodankäynti ja sen monet muunnelmat, kuten verkostopuolustus. Verkostopuolustuksen teoreettiseen viitekehykseen liittyvät mm. itseorganisoituminen, itsesynkronisoituminen ja parveilu.[19]

9.2.2.4 Vaikutusperusteiset operaatiot

Vaikutusta korostava operaatiomalli (Effects Based Operation, EBO) sai alkunsa operaatio Desert Stormin maalittamisstrategiasta. Tuolloin suunnittelijat keskittyivät pelkän maalien tuhoamisen sijasta analysoimaan maalien vaikutuksia, jotka tukisivat ilmaoperaation tavoitteita.

EBO-käsite laajentaa taktista ajattelua ja tuo siihen mukaan sodan operatiiviset ja strategiset tasot. Mikäli pitää vihollisvaltiota "järjestelmien järjestelmänä", siitä seuraa, että häiriö yhtä järjestelmää vastaan vaikuttaa järjestelmän muihin osiin, kuten rikkoutuneet tietoliikennelinkit integroidussa ilmapuolustusjärjestelmässä. EBO:n tavoitteena on:[20]

- tunnistaa vihollisen kriittiset haavoittuvuudet ja kytkökset, jotka pitävät sen järjestelmät koossa;
- määrittää vaikutukset, jotka ovat välttämättömät vihollisen koheesion rikkomiseksi tai vihollisen pakottamiseksi alistumaan tahtoomme tai muuttamaan hänen käyttäytymistänsä;
- ottaa käyttöön kaikki tarvittavat valtion diplomaattiset, sotilaalliset, taloudelliset ja tiedolliset resurssit, jota vaaditaan tuottamaan halutut vaikutukset; ja
- arvioida operaation kehittymistä ja tehdä tarvittavia muutoksia.

---

[17] Alberts David S., Garstka John J., and Stein Frederick P., Network Centric Warfare: Developing and Leveraging Information Superiority, 2d revised ed., Washington, D.C.: CCRP, 2000, s. 2.
[18] Garstka John J., Network-Centric Warfare Offers Warfighting Advantage, Signal, May 2003, s. 58.
[19] Bosquet Antoine, The Scientific Way of Warfare, Columbia University Press, New York, 2009, s. 233 - 234.
[20] Foster H. A., Organizing for Effect: Assessing the Institutional Machinery Needed to Effectively Conduct Effects-based Operations, Master of Military Studies, United States Marine Corps, Command and Staff College, Marine Corps University, Quantico, Virginia 2002, s. 3 - 4.

Tutkijoilla ei ole yhtenevää käsitystä siitä, ovatko vaikutusperusteiset konseptit kiinteästi liitoksissa verkostosodankäyntiin. Yleisesti niitä pidetään toisiaan täydentävinä. Verkostokeskeinen sodankäynti luo mahdollisuuksia ja toimii alustana vaikutuksiin perustuvien operaatioiden toimeenpanolle. Lisäksi verkostokeskeisyys ja erityisesti sen mahdollistama yhteinen tilannekuva toimivat vaikutusperusteisten konseptien mahdollistajana ja niiden ydinprosessien tukena.[21]

EBO analyyttisena käsitemallina ei ollut riittävä toimeenpantavaksi osana sotilaallista päätöksenteko- ja johtamisjärjestelmää. Tästä syystä Yhdysvalloissa siitä muokattiin EBAO (Effect Based Approach to Operations). EBAO:ssa vaikutusperusteinen ajattelu on keskittynyt ja sovellettu sotanäyttämön strategiselle ja operatiiviselle tasolle sekä mukautunut osaksi silloisia suunnittelu-, toimeenpano- ja arviointiprosesseja. EBAO:sta tuli käsitteellisemmän systeemiperustaisen EBO-mallin, sovellus hyödynnettäväksi sotanäyttämön strategisella ja operatiivisella tasalla.[22]

9.2.2.5 Kybersodankäynti

Kybersodankäynti on 2000-luvun malli, johon on koottu yli 100 vuoden elektronisen toimintaympäristön evoluutio.

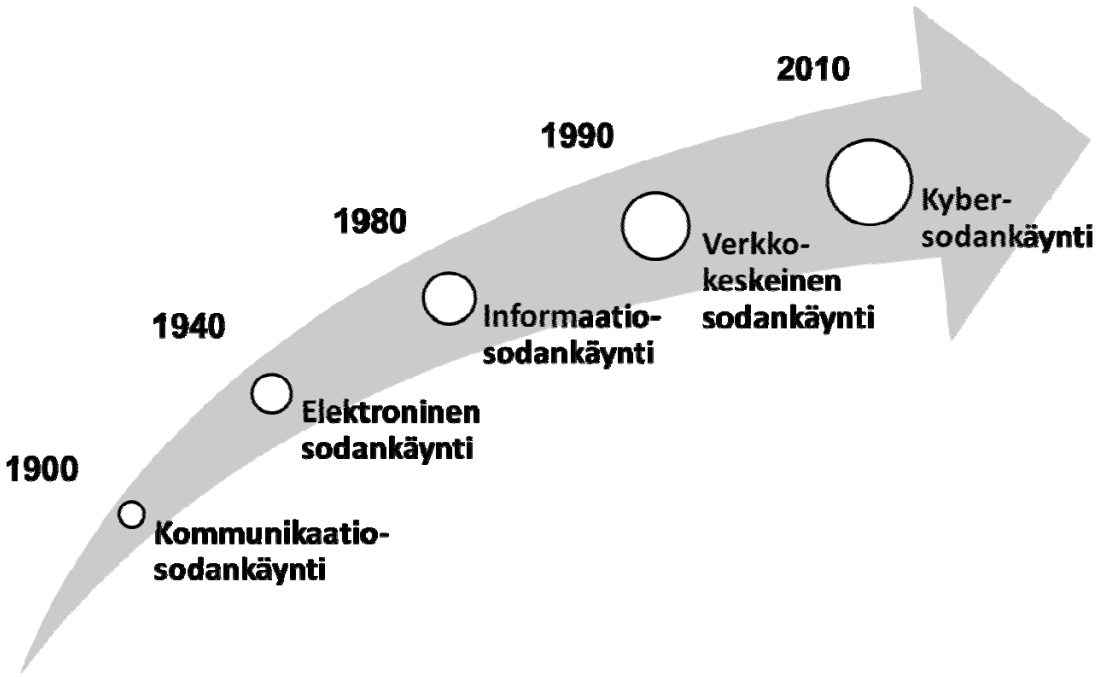
Kyberajattelun myötä on haluttu tuoda informaatioympäristön keskiössä olevan informaation rinnalle kyberavaruuden rakenteet eli kriittinen infrastruktuuri ja sodankäynnin johtamis- ja toimeenpanoprosessit. Lisäksi kyberajattelussa on esitetty uudelleen ajatus totaalisesta sodasta, jossa vaikuttamisen kohteena ei ole vain sotilaallinen toimintaympäristö vaan koko yhteiskunta ja sen rakenteet. Erilaiset verkostot ovat levittäytyneet lähes kaikille elämän alueille. Yhteiskunnan kaikki elintärkeät toiminnat ovat enemmän tai vähemmän verkottuneita. Verkottuneisuus tarkoittaa ajasta ja paikasta riippumatonta toimintaa ja toimintojen hallintaa. Informaation ohella verkkorakenteista on tullut tärkeitä. Toinen merkittävä muutos on siinä, että informaatiosodankäynti katsotaan kuuluvaksi kriisien ja sodan aikaa, mutta kyberuhat ovat osa jokapäiväistä ihmisten ja organisaatioiden arkea.

Asevoimat ovat vastaavalla tavalla kehittyneet informaatiosta, verkostoista, sähköenergiasta riippuvaisiksi, siis koko elektronisesta maailmasta, jossa tietotekniikan erilaiset sovellukset ovat kiinteä osa asevoimien laitteita ja järjestelmiä. Kyberavaruus fuusioi kaikki tietoliikenneverkot, tietokannat ja informaatiolähteet globaaliksi virtuaalisysteemiksi.

Ilmanherruuden hankkiminen ja säilyttäminen on kompleksinen tavoite. Perinteisen ilmatilan hallinnan lisäksi hallittavaksi tiloiksi ovat tulleet avaruus ja kyberavaruus. Myös suomalaisessa kontekstissa näillä elementeillä on yhä suurempi merkitys. Avaruudellisten kykyjen käyttö tulee tulevaisuudessa olemaan yhä merkityksellisempää erityisesti kun käytetään ilma-aseen ilmasta maahan kykyä tai kun toimitaan kansainvälisissä kriisinhallintaoperaatioissa. Ilmapuolustuksen toimintakyky tulee perustumaan näiden kolmen tilan hallintaan. Samalla luodaan kyky käyttää hyväksi yhteisoperaatioiden synergiaetuja. Taistelutilan hallinta edellyttää joustavaa kykyä toimia eri tilojen välillä ja suhteellisen edun saavuttamista ja sen ylläpitoa. Tämä eri taistelu-

[21] Ilvonen Janne, Vaikutusperusteiset konseptit: EBO-, EBAO-, SOD- ja CA-käsiteanalyysi, diplomityö, MPKK, 2009.
[22] Ilvonen Janne, Vaikutusperusteiset konseptit: EBO-, EBAO-, SOD- ja CA-käsiteanalyysi, diplomityö, MPKK, 2009.

tilojenhallinnan suorituskyky mahdollistaa vaikutusperusteisen toimintatavan, jossa maalin valinta tapahtuu ilmasodankäynnin kannalta tärkeimpiin kohteisiin.



Kuva 1. Evoluutio kommunikaatiosodankäynnistä kybersodankäyntiin

Ilmakomponentin eri taistelutilojen hallinta antaa mahdollisuuden sekä aseellisen voiman käyttöön että ei-kineettisen voiman käyttöön kyberavaruudessa. Tämä suorituskyky antaa mahdollisuuden toimia uudessa epälineaarisessa ja rajoiltaan epämääräisessä taistelutilassa. Tässä tilassa tulee voida integroida saumattomasti ilmassa, pinnassa, pinnan alla, avaruudessa ja kyberavaruudessa toimivia miehitettyjä ja miehittämättömiä alustoja, joiden avulla voidaan havaita, seurata ja identifioida maalit sekä johtaa asejärjestelmiä halutun vaikutuksen saavuttamiseksi. Tässä prosessissa nousee keskeiseksi elementiksi aika. Johtamisprosessissa tarvitaan sisällöltään mahdollisimman tarkkaa ja oikein aikautettua informaatiota, jopa liikkeessä, jotta keskitetty johtaminen ja hajautettu toiminta voidaan toteuttaa. Tämä vaatii johtamisen ja doktriineiden kehittämistä, joista on tullut yhä kriittisempiä.

9.2.3 Uhka- ja haavoittuvuusmalli

Uhka, haavoittuvuus ja riski muodostavat toisiinsa liittyvän kokonaisuuden. Lähtökohtana on jokin arvoa sisältävä fyysinen esine, tieto, osaaminen tai muu immateriaalinen oikeus, joka halutaan suojata ja turvata. Uhka on jokin haitallinen ja mahdollinen kybermaailman tapahtuma, jonka ilmentymistä kuvataan todennäköisyydellä. Haavoittuvuus on systeemin eri osissa oleva heikkous, joka lisää tapahtuman todennäköisyyttä tai kasvattaa sen aiheuttamia vahinkoja. Haavoittuvuus voidaan jakaa ihmisten toiminnassa, prosesseissa tai teknologiassa ilmentyviin haavoittuvuuksiin.

Riski on vahingon odotusarvo. Se saadaan kertomalla todennäköisyys vahingon suuruudella. Riskiä voidaan tarkastella sekä taloudellisen arvon että maineen menettämisen kannalta. Riskiä voidaan hallita sitä poistamalla, pienentämällä tai hyväksymällä. Riskiä voidaan pienentää ohjeistuksin ja sääntelytoimenpitein, kehittämällä puolustusvoimien prosesseja ja sisästä yhteisöllisyyttä sekä kehittämällä teknologisia ratkaisuja.

Richard Hundley ja Robert Anderson jakavat kybermaailman haavoittuvuudet seuraavasti:[23]

- **Toimintoperustaisia**
  - toimintajärjestelmät
  - prosessit
- **Käyttäjäperustaisia**
  - autentikointi
  - salasanat
- **SW-perustaisia**
  - takaovi
  - ohjelmistovirheet
  - asennusvirheet
- **HW-perustaisia**
  - suunnitteluvirheet
  - komponenttivirheet
- **Verkkoperustaisia**
  - TCP/IP

9.2.3.1 Ilma-aseen haavoittuvuudesta

Asejärjestelmät ovat yhä riippuvaisempia ohjelmistosta, tietokonelaitteistosta ja verkottuneesta toiminnasta taistelukentällä ja siksi asejärjestelmät ovat myös kyberhyökkäysten kohteita. Lentokone on hyvä esimerkki kybersodankäynnin siirtymisestä asejärjestelmiin. Aikaisemmin hävittäjän suorituskyky ja toiminta perustuivat kokonaan fyysisiin laitteisiin ja konstruktioihin. Nykyisin vähintään 75 prosenttia hävittäjän suorituskyvystä perustuu ohjelmistoihin ja tietotekniikkaan. Ilman tietotekniikan sovelluksia koneet eivät olisi hallittavissa tai eivät saavuttaisi haluttuja suorituskykyjä. Koneiden ohjelmistoriippuvuus kasvaa ja tietokoneille annetaan suurempi vastuu erityisesti äärriolosuhteissa. Esimerkiksi F-22 käyttää tiukassa kaartotaistelussa tietokonetta työntövoiman ja liikehtimisen hallintaan ja suorituskyvyn optimointiin. Nykyaikaista hävittäjää ohjataan ja sen moottoreita hallintaan elektronisesti ja sen asejärjestelmät ovat tietokoneohjattuja. Koneen fyysisestä ja mekaanisesta hallinnasta on siirrytty tietokoneiden ohjelmistoavusteiseen hallintaan.[24]

[23] Hundley Richard 0. and Anderson Robert H., Emerging Challenge: Security - and Safety in Cyberspace, IEEE, Winter 1995/1996.
[24] Alford Lionel D., Cyber Warfare: The Threat to Weapon Systems, WSTIAC Quarterly, Vol.9, Nr.4, 2009.

Nykyisin ohjelmisto määrittelee nykyaikaisen asejärjestelmän vahvuuden tai tehokkuuden ja tarjoaa perustan monien erilaisten laitteiden ja systeemien yhteistoiminalle verkottuneessa toimintaympäristössä. Ohjelmistollisuus ja verkottuneisuus tarjoavat aivan uudenlaisia ratkaisuja ilmasodankäynnin operaatioihin, mutta samalla lisääntyvät haavoittuvuudet, jotka tarjoavat kasvavia hyökkäysmahdollisuuksia.[25]

F-22 on esimerkki tietokoneohjelmistojen kontrolloimasta lentokoneesta, joka sisältää ja on yhteydessä integroituihin tietojärjestelmiin. F-22 ei ole suljettu systeemi; ulkoiset tietojärjestelmät päivittävät ja integroivat F-22:n osaksi ilmaoperaatiota lennon aikana. Näiden ulkoisten yhteyksien vuoksi eivät ainoastaan tietojärjestelmät ole hyökkäysten kohteena vaan kaikki koneen tietojärjestelmät ja niiden ohjaamat fyysiset systeemit. Taulukossa 1 on esitetty eri aikakausien lentokoneiden riippuvuus ohjelmistoista ja tietojärjestelmistä.[26]

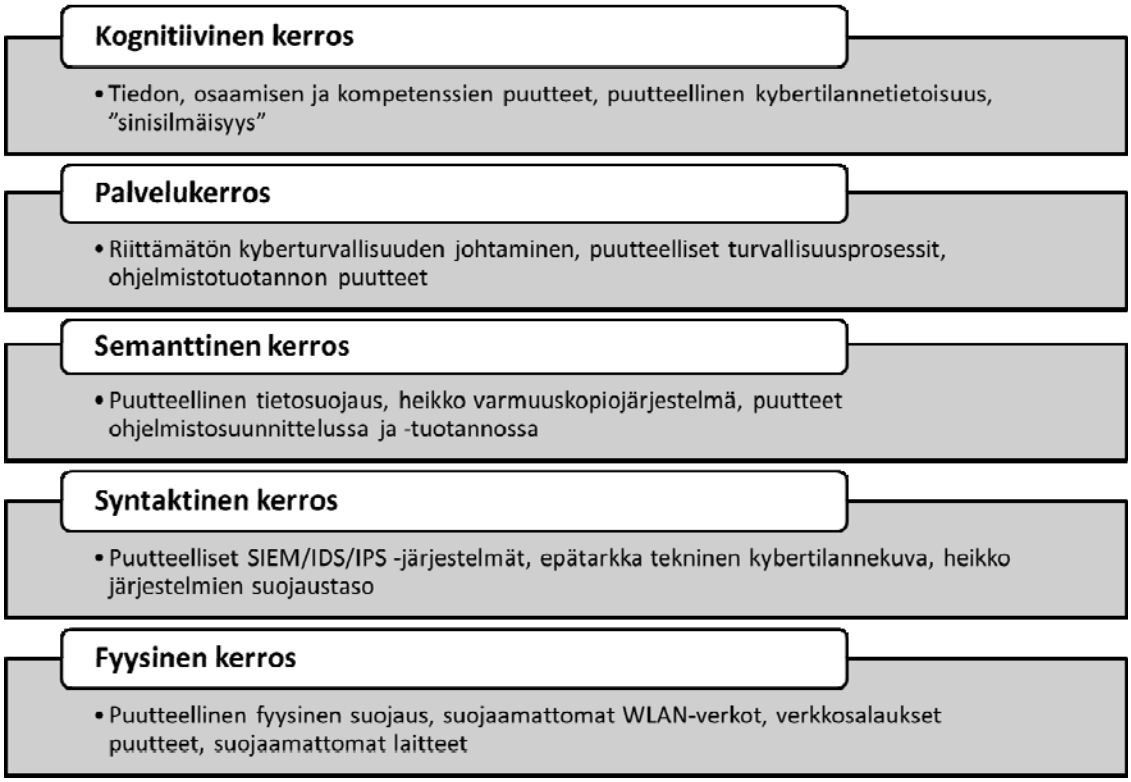
Taulukko 1. Sotilaslentokoneen riippuvuus ohjelmistoista ja tietojärjestelmistä

Hävittäjä	**Vuosi**	**Ohjelmistojen osuus toiminnoista (%)**
F-4	1960	8
A-7	1964	10
F-111	1970	20
F-15	1975	35
F-16	1982	45
B-2	1990	65
F-22	2000	80

Nykyinen ilmasodankäynti on täysin riippuvainen C4ISR-järjestelmästä. Ilmaoperaatioiden johtaminen, koordinointi ja kommunikaatio edellyttävät toimivaan johtamisjärjestelmää. Johtamisjärjestelmä on haavoittuvin osa ja siksi sen tulee olla asevoimien kyberpuolustuksen tärkein kohde. Tämän päivän ilmapuolustuksen johtamisjärjestelmä on monimutkainen kokonaisuus radioista, tutkista, suurtietokoneista, PC-laitteisiin ja sulautettuihin järjestelmiin. Se käyttää asevoimien tietoverkkojen lisäksi internettiä, siviiliverkkoja, langattomia ratkaisuja, siviili- ja sotilasviestintäjärjestelmiä, navigaatiojärjestelmiä sekä laajan taajuusalueen radioverkkoja. Johtamisjärjestelmän verkottuneisuus luo haavoittuvuuden. Tunkeutuminen on mahdollista missä tahansa järjestelmän osassa ja hyökkäys voi vaikuttaa tutkavalvontaan, tietoliikenteeseen tai ilmatorjuntaohjusjärjestelmään. Se voi lamauttaa tulenkäytön johtamisjärjestelmän, paikannusjärjestelmän tai liikkuvat viestijärjestelmät. Systeemin kompleksisuus tekee mahdottomaksi kokonaan eliminoida haavoittuvuudet sekä havaita ja jäljittää tunkeutumiset systeemin sisälle. Verkottuminen lisää ilmapuolustusjärjestelmän suorituskykyä, mutta samalla lisää kyberturvallisuutta vaarantavia haavoittuvuuksia.[27]

[25] Alford Lionel D., Cyber Warfare: The Threat to Weapon Systems, WSTIAC Quarterly, Vol.9, Nr.4, 2009.
[26] Alford Lionel D., Cyber Warfare: The Threat to Weapon Systems, WSTIAC Quarterly, Vol.9, Nr.4, 2009.
[27] Alford Lionel D., Cyber Warfare: The Threat to Weapon Systems, WSTIAC Quarterly, Vol.9, Nr.4, 2009.

Kuvassa 2 on esitetty luvussa 5 kuvatun tasomallin mukaan jaoteltuna eri kerroksiin liittyviä haavoittuvuuksia ilmapuolustusjärjestelmän näkökulmasta.



Kuva 2. Haavoittuvuudet kybermaailman eri tasoilla

9.2.4 Kyberajan ei-kineettiset operaatiot

Elektronisen sodankäynnin, informaatiosodankäynnin ja kybersodankäynnin operaatiot muodostavat kyberajan ei-kineettisten verkostoperustaisten operaatioiden kokonaisuuden. Ilmasodankäynnissä nämä operaatiot muodostavat verkottuneen kokonaisuuden, jossa eri operaatiomuotojen avulla pyritään saavuttamaan Ilmasodankäynnille asetettuja tavoitteita. Kybersodankäynti ei ole syrjäyttänyt aikaisempia ei-kineettisiä sodankäynnin muotoja vaan laajentunut kybermaailman uusille bittien muodostamille toiminta-alueille.

Kyberoperaatio voidaan määritellä kyberperusteisiksi hyökkäyksiksi niin sotilas- kuin siviili-infrastruktuuria vastaan. James Mulvenon määrittelee kyberkonfliktin ”*laajamittaiseksi poliittisesti fokusoiduksi konfliktiksi, jossa käytetään hyökkäyksellisiä ja puolustuksellisia suorituskykyjä digitaalisten järjestelmien, verkkojen ja infrastruktuurien häiritsemiseksi*”.[28]

9.2.4.1 Sotilaalliset informaatio-operaatiot

Informaatiosodankäynnin operaatioiden avulla pyritään hankkimaan informaatioylivoima eli tilanne, jossa on kyetty luomaan itselleen edullisen asetelman informaatio-

[28] Mulvenon James, Toward a Cyberconflict Studies Research Agenda, the IEEE Computer Society, 2005, s. 52 - 55.

ympäristössä. Tällöin informaatioylivoiman omaavalla on luotettavampaa, tarkempaa ja oikea-aikaisempaa tietoa. Informaatioylivoiman haltijalla on käytettävissä hyvät tiedon saamis- ja hyödyntämismahdollisuudet, ajankohtainen ja tarkka tilannekuva sekä operatiivinen toimintavapaus operaatioalueella.[29]

Kyberajan informaatio-operaatiot kohdistuvat tietoon/informaatioon. Sotilaalliset informaatio-operaatiot vahvistavat ja tukevat ilmavoimien operaatiokykyä sekä ilmapuolustuksen johtamisjärjestelmän toimintaa tiedon ja informaation näkökulmasta. Informaatio-operaatioita ovat operaatioturvallisuus, harhauttaminen, psykologiset operaatiot ja viestintä. Operaatiot sovitetaan yhteen muiden ei-kineettisten operaatioiden ja kineettisten ilmaoperaatioiden kanssa. Lisäksi näillä operaatioilla on kiinteä yhteys puolustusvoimien yhteisoperaatioihin.

Operaatioturvallisuudessa keskitytään kriittisen tiedon tunnistamiseen, informaatiouhkien arvioimiseen, haavoittuvuuksien analysoimiseen, riskien arvioimiseen ja sopivien operaatioturvallisuustoimien valintaan ja toteuttamiseen.[30]

Psykologiset operaatiot tukevat sekä kansallista että puolustusvoimien strategista kommunikaatiota. Operaatioiden avulla vahvistetaan kansallisia sodankäynnin päämääriä, puolustusvoimien toimintakykyä aina komentajatasolta yksittäisiin taistelijoihin saakka. Tavoitteena on erityisesti suojata omat kriittiset informaatiotoiminnot.

Tiedottaminen on organisatorisesti erillinen, mutta toiminnallisesti läheinen osa psykologisia operaatioita. Viestintä ja siihen keskeisenä osan kuuluva tiedottaminen suunnitellaan tukemaan sotilaallisia informaatio-operaatioita, vaarantamatta viestintäorganisaation uskottavuutta.[31]

9.2.4.2 Elektronisen sodankäynnin operaatiot

Elektronisen sodankäynnin operaatiot jaetaan elektroniseen vaikuttamiseen, elektroniseen suojautumiseen ja elektroniseen tukeen. Elektroninen vaikuttaminen tarkoittaa häirintää ja harhauttamista, elektroninen tuki tarkoittaa tiedustelua ja valvontaa. Elektroninen suojautuminen on elektronisten järjestelmien käyttäjien suojautumistoimenpiteitä vastustajan elektronisen sodankäynnin operaatioita vastaan. Kaikilla näillä on yhteys informaatio- ja kyberoperaatioihin sekä ilmasodankäynnin kokonaisuuteen.[32]

Elektroninen vaikuttaminen käsittää kaikki ne toimenpiteet, joilla sähkömagneettisen spektrin välityksellä pyritään estämään, hidastamaan tai vähentämään vihollisen sähkömagneettista säteilyä hyödyntävien tai elektroniikasta riippuvien järjestelmien käyttöä taikka suuntaamaan käyttö oman toiminnan kannalta edulliselle alueelle. Elektroninen vaikuttaminen jakautuu elektroniseen häirintään, elektroniseen harhauttamiseen ja elektroniseen lamauttamiseen.[33]

---

[29] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004
[30] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004
[31] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004
[32] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004
[33] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004

Elektronisen suojautumisen toimenpitein varmistetaan omien järjestelmien tehokas käyttö huolimatta vihollisen elektronisesta vaikuttamisesta ja tuesta. Elektroninen suojautuminen jakautuu aktiiviseen ja passiiviseen suojautumiseen.[34]

Elektroninen tuki tuottaa elektronisten lähetteiden ilmaisun ja paikantamisen perusteella tilannekuvaa ja sitä täydentäviä tietoja. Se on reaaliaikaista tiedustelua ja valvontaa, joka kohdistuu sähkömagneettista säteilyä käyttäviin järjestelmiin. Elektroninen tuki jakautuu elektroniseen tiedusteluun ja valvontaan, elektroniseen maalinosoitukseen ja elektroniseen uhkavaroitukseen. [35]

9.2.4.3 Kyberoperaatiot

Kyberoperaatiot muodostavat kokonaisuuden, jolla horjutetaan vastustajan kybertoimintaympäristön tieto- ja informaatioperusteisia järjestelmiä ja rakenteita sekä eri toimijoiden tilannetietoisuuden muodostumista samalla, kun suojataan omia sekä defensiivisin että offensiivisin keinoin. Kybersodankäynnissä kyberoperaatiot eivät ole kokonaan itsenäisiä, muusta sodankäynnistä erillään olevia operaatioita, vaan kiinteä osa kokonaisoperaatioita.

Kyberoperaatiot voidaan jakaa hyökkäyksellisiin toimiin (kybervaikuttaminen), puolustuksellisiin toimiin (kybersuojautuminen) ja tiedusteluun (kybertiedustelu) kybertoimintaympäristön eri rakenteissa.[36]

Kyberpuolustuksen suorituskyvyt merkitsevät uusia määrittelyitä ja tarkennuksia voimankäytön säännöksiin erityisesti kybertiedustelun ja -vaikuttamisen osalta. Kybervaikuttamisen kehittämisen tavoitteena tulee olla, että siihen soveltuisivat samat periaatteet kuin perinteiseen voimankäyttöön.

Kybervaikuttamisen suorituskyvyllä vaikutetaan vastustajan toimintaan kohdistamalla toimenpiteitä sen järjestelmiin ja verkkoihin niiden haavoittuvuuksia hyödyntäen. Vaikuttamisen tavoitteena on vastustajan tietojärjestelmien, tietoverkon ja sen laitteiden toiminnan häiritseminen, tietoverkon tai sen sisältämän tiedon käytön rajoittaminen, käytettävyyden heikentäminen tai tuhoaminen sekä ylivoiman saavuttaminen kybertilassa.

Kybersuojautumisen suorituskyvyllä estetään, rajataan ja lievennetään hyökkääjän eri järjestelmiin ja verkkoihin toteuttamien tietoverkko-operaatioiden vaikutuksia. Kybersuojaaminen käsittää sellaisia tietoverkoissa tapahtuvia toimia kuten suojautuminen, valvonta, analysointi, havainnointi ja vastatoimenpiteiden toteuttaminen verkkohyökkäyksiä, tunkeutumisia ja muita luvattomia toimia sekä häiriöitä vastaan, joilla pyritään tekemään tietojärjestelmät ja -verkot toimintakyvyttömiksi. Suojautumisen tavoitteena on kyky suojata oma tieto sekä johtamis- ja tietojärjestelmät säilyttäen riittävä operaatioiden johtamiskyky.

---

[34] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004
[35] Sotilaalliset informaatio-operaatiot doktriini, Pääesikunta 2004.
[36] Joint Doctrine for Information Operation (Joint Pub 3-13), Department of Defence, 9 October 1998.

Kybertiedustelun suorituskyvyllä tuotetaan tietoa kybertoimintaympäristön toimijoiden järjestelmien ja verkkojen kokoonpanoista ja haavoittuvuuksista sekä arviota toimijoiden kyvyistä toteuttaa tietoverkko-operaatioita. Kybertiedustelun tavoitteena on luoda suojautumisen ja vaikuttamisen edellyttämä tilannetietoisuus, uhkavaroitus ja maalinosoitus.

Vastustaja toteuttaa erilaisia kyberhyökkäyksiä kybermaailman eri rakenteisiin. Luvussa 5 esitetyn kybermaailman rakennemalliin liitettynä fyysiseen kerroksen voidaan kohdistaa sekä kineettistä että ei-kineettistä vaikutusta. Kineettisellä asevaikutuksella voidaan tuhota fyysisiä verkkoja, ilmapuolustuksen eri järjestelmiä ja niiden osia sekä tietovarastoja (data warehouse). Persianlahden sodissa kineettisillä hyökkäyksillä tavoiteltiin myös vaikutusta kybertoimintaympäristössä. Fyysisen maailman uhkia ovat myös laitejärjestelmien komponenteissa olevat haittaohjelmat ja takaportit.

Hyökkäyksellä syntaktista kerrosta vastaan tavoitellaan järjestelmän tai sen osien saamista hallintaan. Hyökkäyksillä voidaan lamauttaa verkkojen toimintaa ja avata mahdollisuuksia hyökkäyksille muita kerroksia vastaan.

Kyberhyökkäyksen kohteena semanttista kerrosta vastaan on informaatio. Kybervakoilu voidaan määritellä toimiksi, joilla hankitaan salaisia tietoja (sensitiivinen, yksityisoikeudellinen tai turvaluokiteltu) yksityisiltä ihmisiltä, kilpailijoilta, ryhmiltä, hallituksilta ja vastustajilta poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi käyttäen laittomia menetelmiä internetissä, verkoissa, ohjelmistoissa tai tietokoneissa.[37]

Hyökkäyksellä palvelukerrosta vastaan pyritään lamauttamaan verkkopalveluiden toiminta. Palvelunestohyökkäys (Denial of Service, DoS) tarkoittaa verkkohyökkäystä, jossa pyritään estämään verkkosivuston tarkoitettu käyttö.

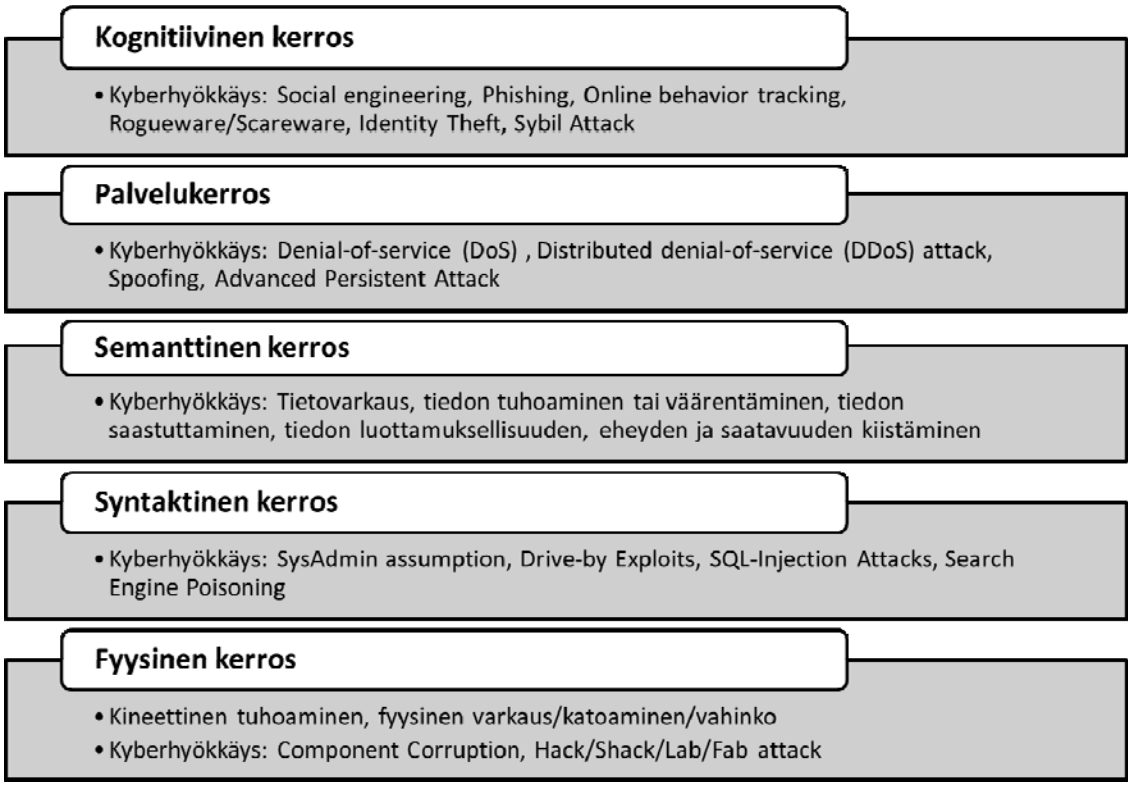
Hyökkäys kognitiivista kerrosta vastaan on hyökkäys päätöksentekijöitä, komentajia ja kaikkia järjestelmien käyttäjiä vastaan. Hyökkäyksillä pyritään estämään oikeanlaisen tietoisuuden syntyminen ja boydilaisen ajattelun mukaisesti romahduttaa taistelijan moraalinen-mentaalinen-fysikaalinen harmonia, tuottaa lamautusvaikutus ja romahduttaa hänen tahtonsa vastarintaan.

Kuvassa 3 on esitetty erilaisia hyökkäysmalleja ja -vektoreita kybermaailman eri kerroksia vastaan.

Informaatiosodankäynnin, elektronisen sodankäynnin ja kybersodankäynnin operaatiot muodostavat toisiaan täydentävän monikerroksisen ei-kineettisen operaatiokokonaisuuden, joka edellyttää eri osa-alueiden saumatonta yhteistoimintaa. Näiden sodankäyntimuotojen tarkkarajainen määrittely on vaikeaa, kun kullakin niistä on oma kehitysprosessinsa mukainen historia. Tarkkoja määrittelyjä tärkeämpää on tarkastella toteuttavia operaatiota ilmasodankäynnin kokonaistavoitteiden näkökulmasta ja luoda kyky eri operaatioiden tehokkaalle suunnittelulle ja toimeenpanolle verkostoituneessa kybertoimintaympäristössä.

[37] Liaropoulos Andrew, War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory, Proceedings of the 9th European Conference on Information Warfare and Security, the Department of Applied Informatics University of Macedonia Thessaloniki Greece 1-2 July 2010, 177 - 182.

Ilmasodankäynnissä ei-kineettisistä operaatioista korostuvat elektronisen sodankäynnin operaatiot. Ilmavoimilla on pitkä perinne toimia elektromagneettisessa toimintaympäristössä. Ilmasodankäynnin johtamiselle ja ilmaoperaatioiden toteuttamiselle elektromagneettisen toimintaympäristön hallinta on välttämätöntä. Ilmapuolustuksen informaatio-operaatioissa korostuu operaatioturvallisuus. Kybersodankäynnissä kybervaikuttamisen tulee olla keskitetysti johdettua yhteisoperaatiotoimintaa. Kybermaailman laajuus ja kompleksisuus eivät mahdollista tehokkaita puolustushaarakohtaisia kybervaikutusoperaatioita. Ilmapuolustuksen osalta painopiste on kybersuojaamisen toteuttamisessa ja osallistumisessa kybertilannekuvan muodostamiseen. Kybertilannekuvan muodostaminen tulee olla keskitetty koko puolustusvoimia koskeva toiminta, jossa käytetään hyväksi puolustushaarojen erityisosaamista. Kuvassa 4 on esitetty malli verkkokeskeisten ei-kineettisen operaatioiden kokonaisuudesta.

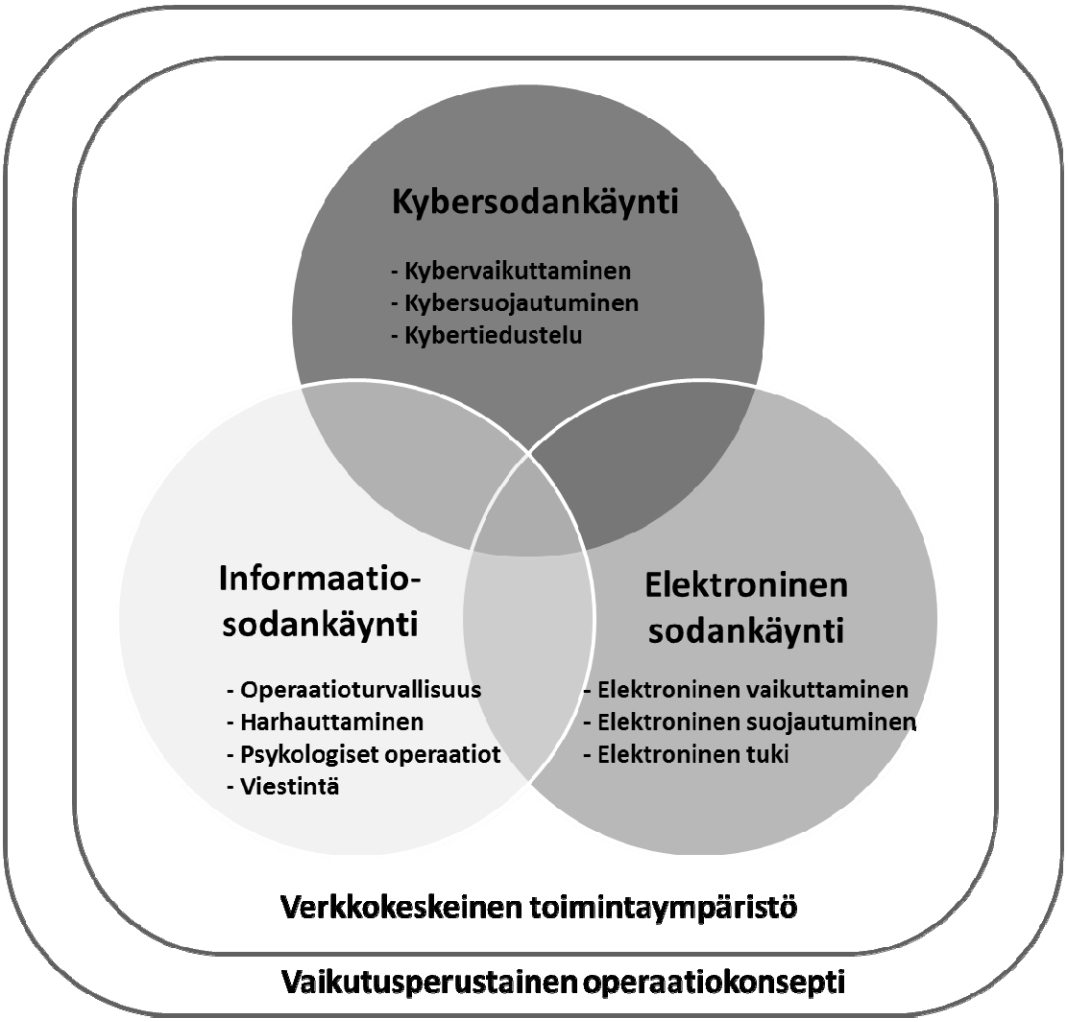


Kuva 3. Kyberhyökkäysmuotoja eri kybermaailman kerroksia vastaan

Verkkokeskeisyys ja vaikutusperustaisuus voidaan kytkeä osaksi ei-kineettisiä operaatioita. Verkostokeskeisyys toimii sotilaallisen toimintaympäristön alustana, jossa ei-kineettisiä operaatioita yhdessä kineettisten operaatioiden kanssa toteutetaan vaikutusperustaisen operaatiokonseptin avulla. Yhteinen tilannekuva ja jaettu tilannetietoisuus toimivat koko operaatioajattelun keskiössä.

Vaikutusperustainen operaatiokonsepti kytkee toisiinsa strategisen ja operatiivisen tason tavoitteet ja halutut tulokset sekä tavoitteisiin pääsemiseksi tarvittavat kineettiset ja ei-kineettiset toimenpiteet. Yhdysvaltain puolustushaarojen yhteisen johtoportaan tutkimus- ja kehittämisosaston yhdessä luonnosasiakirjassa määritellään vaiku-

tusperustaiset operaatiot ”prosessiksi, jonka päämäärä on vaikuttaa vastustajaan taktisella, operatiivisella ja strategisella tasolla käyttäen kaikkia sotilaallisia ja muita kansallisia kykyjä synergiaa toteuttaen ja kertautuvalla ja voimaa asteittain kasvattavalla tavalla niin, että saadaan haluttu strateginen tulos”.[38]



Kuva 4. Verkkokeskeinen ei-kineettisten operaatioiden kokonaisuus

Kyberajan taistelukenttä ja -tila tulee nähdä kokonaisuutena ilman ajallisia tai tilaan liittyviä rajoitteita. Komentajien tulee ymmärtää kaikki keskeiset taistelutilan järjestelmät ja niiden osat sekä vuorovaikutussuhteet, riippumatta niiden ajallisesta, fyysisestä tai virtuaalisesta paikasta.[39]

[38] Herndon Robert B., Robinson John A., Creighton James L., Torres Raphael, Bello Louis J., Effects-Based Operations in Afghanistan - The CJTF-180 Method of Orchestrating Effects to Achieve Objectives, Field Artillery, January-February 2004, s. 26

[39] Ilvonen Janne, Vaikutusperusteiset konseptit: EBO-, EBAO-, SOD- ja CA-käsiteanalyysi, diplomityö, MPKK, 2009.

Vuorovaikutteisuus on taistelukentän ja -tilan perusominaisuus. Omien ja vastustajan toimien vuorovaikutus tulee nähdä kaksisuuntaisena ja dynaamiseen vuorovaikutukseen perustuvana. Operaatioiden vaikuttavuutta tulee tarkastella kokonaistoiminnan näkökulmasta. Oleellista on ymmärtää systeemien ja niiden osien suhteiden ja vuorovaikutuksen merkityksellisyys, sillä vuorovaikutusten esiintyminen paljastaa tärkeimmät taistelutilan systeemit. Tällaiset systeemit ovat usein tärkeitä halutun vaikutuksen kohteita.40 Samalla kun taistelukentän tilan eri osien keskinäisriippuvuus antaa yhä parempia mahdollisuuksia tehokkaaseen puolustukseen, luo se uusia haavoittuvuuksia hyökkääjän näkökulmasta.

9.2.5 Kybersuorituskykyisyyden teknologinen kehittäminen

Kyberturvallisuusteknologian kehitys ei ole irrallinen ilmiö vaan se on vahvasti linkittynyt yhteiskuntarakenteisiin ja sen eri turvallisuustoimijoiden tarpeisiin ja odotuksiin. Uusista teknologisista ratkaisuista otetaan käyttöön ne mitkä parhaiten tuottavat lisäarvoa, tehokkuutta, vaikuttavuutta jne.

Teknologian kehitys on jatkuvaa, syklistä, epälineaarista ja perustuu aikaisemmille innovaatioille. Mitään ei luoda tyhjästä vaan jokaisella teknologialla on historiansa. Teknologialla on suhde omaan aikaansa, ilmiö valjastetaan teknologian käyttöön, kun teknologian kypsyysaste on oikea. Teknologian kypsymistä on vaikea ennustaa, sillä kehityksessä on monia teknologiaan, talouteen ja osaamiseen liittyviä tekijöitä, jotka ratkaisevat sen, milloin mikin läpimurto tapahtuu.

Kyberteknologian kehitys muodostaa kollektiivin, jossa mukana ovat kaikki aikaisemmat ja nykyiset tekniset tietomallit, käsitemallit, algoritmit, arkkitehtuurit, komponentit, laitteet, moduulit, systeemit, teknologiat, prosessit, toimintatapamallit ja instituutiot, jotka ovat tai ovat olleet käytössä. Kyberteknologian kehitys perustuu alkioille, jotka toimivat premisseinä seuraaville teknologisille innovaatioille. Tällä perusteella mm. W. Brian Arthur väittää, että teknologia kehittyy olemassa olevien teknologioiden kombinaatiosta. Teknologian kollektiivin uudet premissit siis syntyvät ja nousevat esiin jo olemassa olevista teknologioista autopoieettisen teorian mukaisesti.[41] Tietokoneen kehittyminen edellytti pitkää elektroniikka-alan eri alan alkioiden ja komponenttien evoluutiota ja niiden tulemista esiin sekä fysikaalisten ja elektromagneettisten ilmiöiden ymmärtämistä, ennen kuin tietokone teknologisena kombinaationa oli valmis syntymään. Kombinaatio toimii yhtenä teknologian evoluutiota eteenpäin vievänä voimana ja toisena voimana on tilaisuuslokeroita luova kysyntä/tarve. Teknologian tilaisuuslokerot syntyvät teknologian ja tarpeen välisessä jatkuvassa vuorovaikutusprosessissa, joka saa sekä ulkoisia että sisäisiä syötteitä.

Kybersuorituskyvyn muutosta analysoitaessa voidaan tekninen, toiminnallinen ja teknologinen muutos erottaa toisistaan. Teknisenä muutoksena voidaan ymmärtää fyysiset laitteet, kuten esimerkiksi tietokoneen uudet kehitysversiot tai ohjelmistojen uudet versiot. Toiminnallisena muutoksena voidaan pitää uusien toiminnallisuuksien joukkoa, ts. uusia toimintatapamalleja ja prosesseja, joita otetaan käyttöön. Tietokone laitteena edustaa teknistä muutosta ja tietokoneen avulla toteutettu kybertilannekuvan muodostaminen tai kyberoperaation toteuttaminen edustavat toiminnallista

[40] Ilvonen Janne, Vaikutusperusteiset konseptit: EBO-, EBAO-, SOD- ja CA-käsiteanalyysi, diplomityö, MPKK, 2009.
[41] Arthur W. Brian, Teknologian luonne, Terra Cognita, Helsinki 2010, s. 155.

toimintatavan muutosta. Teknologinen muutos edustaa uusien parametrien joukkoa, ts. uutta kontekstia, jossa tekniset ja toiminnalliset muutokset tuovat esiin uuden toimintaympäristön. Tietokone laitteena loi uusia toiminnallisuuksia ja toimintatapamalleja ja teknologisena muutoksena se loi ilmasodankäyntiin uuden tilaisuuslokeron, uuden kontekstin.[42]

Kybersodankäynnin uusilla laite- ja palveluinnovaatiolla luodaan ilmasodankäynnin evoluution transformaatiohyppyjä, jotka vievät sodankäynnin luonnetta ja olemusta uusille tasoille ja tuottavat uuden strategisen tilan, jossa ilmasota voitetaan tai hävitään.

Suomen kansallinen kyberturvallisuusstrategia taustamuistioineen määrittää puolustusvoimien kybervastuut ja -tehtävät yleisellä tasolla. Strategian mukaan puolustusvoimien tulee luoda kokonaisvaltainen kyberpuolustuskyky lakisääteisissä tehtävissään. Sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Puolustusvoimien tulee suojata omat järjestelmänsä ja verkkonsa sekä luoda ja ylläpitää kykyä tiedusteluun ja vaikuttamiseen. Tiedustelun suorituskyvyillä on tuotettava tietoa kybertoimintaympäristön toimijoiden järjestelmien ja verkkojen kokoonpanoista ja haavoittuvuuksista. Lisäksi on kyettävä tuottamaan tietoa toimijoiden kyvyistä toteuttaa kyberoperaatioita.[43]

Kyberuhkien syntyminen on kyettävä havaitsemaan ajoissa ja kybermaailman ilmiöitä ja tapahtumia on kyettävä seuraamaan reaaliajassa. Tämä edellyttää sotilaallisen kybertilannekuvan muodostamista puolustushallinnon verkoissa ennakkovaroituksen ja valmistautumisajan saamiseksi sekä vaikuttamisen toteuttamiseksi. Tilannetietoisuuden muodostaminen edellyttää kykyä valvoa ja tehdä havaintoja kybermaailmasta. Puolustusvoimien kybertilannekuvaympäristö toimii kiinteässä yhteistyössä kansallisen kyberturvallisuuskeskuksen kanssa.

Puolustusvoimat rakentaa kyberpuolustuksen suorituskykyä, johon luodaan tiedustelun, vaikuttamisen ja suojautumisen edellyttämät tekniset ja toiminnalliset ratkaisut. Kybersuorituskyvyn rakentaminen perustuu sotilaallisen kyberuhkan perusteella laadittuihin suorituskykyvaatimuksiin ja käytettävissä oleviin resursseihin.

Pääesikunta johtaa kyberpuolustuksen suorituskykyjen kehittämistä ja käyttöä Puolustusvoimissa. Pääesikunnan alaiset laitokset kehittävät, rakentavat ja ylläpitävät kybersuorituskykyjä sekä vastaavat käytännön toimenpiteistä. Puolustushaarat vastaavat omien kohdejärjestelmiensä suojaamisesta ja valvonnasta sekä tuottavat kybervaikuttamisen suorituskykyä omalla osaamisellaan.

Kyberteknologian kehittämisen ytimessä on eri kombinaatioiden fysikaalinen ja mentaalinen yhdistäminen toiminnalliseksi kokonaisuudeksi. Tätä prosessia pitää yllä teknologian autopoieettisen luonteen lisäksi ulkoiset vaikutteet. Ilmasodankäynnin uudet operaatiokonseptit luovat uusia kysyntätarpeita, systeemin kysyntälokeroita, joiden vaatimusten täyttämiseksi teknologia kehittyy. Sotilasorganisaation toiminnasta syntyvät institutionaaliset tarpeet luovat myös uusia kysyntälokeroita. Kysyntätar-

[42] Beyerchen Alan, From radio to Radar, in Murray Williamson and Millett Allan R. (edit.), Military Innovation in the Interwar Period, Cambridge University Press, Cambridge 1996, s. 268.
[43] Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013.

peiden ja teknologisten mahdollisuuksien välillä on yleensä ristiriita, joka pyrkii tasapainotilaan. Epätasapainoa luo teknologian sisäinen kehittyminen, kun uudet innovaatiot edellyttävät muutoksia systeemin muissa rakenteissa. Teorian ja instituutioiden evoluutio kohtaa usein teknologian rajoituksia ja siten syntyy näiden välille ristiriitatilanteita. Näitä ratkaistaan uusilla teknologisilla innovaatioilla, jotka voivat luoda uusia epätasapainotilanteita. [44]

Tämä kehitysprosessi ei ole yhtenäinen ja tasainen. Teknologian kehityksessä lisätään ja poistetaan teknologioita, luodaan tilaisuuslokeroita uusille teknologioille ja paljastetaan uusia ilmiötä. Evoluutiossa ilmenee inkrementaalisia ja revolutionaarisia vaiheita sekä voimakkaita teknologioiden välisiä kilpailutilanteita, jossa disruptiiviset innovaatiot syrjäyttävät perinteisiä teknologioita. Kehitys esiintyy yksittäisissä teknologioissa suorituskykyä parantavina prosesseina sekä suurissa ja laajoissa kompleksisissa systeemeissä, jossa yhä uudet alkiot muokkaavat kokonaisuutta yhä monimutkaisemmaksi. Tuloksena on turbulenssia teknologioiden ja kehityksen eri tasoilla. Kaikilla tasoilla ilmaantuu uusia teknologioita ja vanhoja katoaa ja teknologia etenee jatkuvasti kohti osin tuntemattomia alueita, luoden uusia ratkaisuja, systeemin lokeroita, uusia tarpeita päättymättömässä kehitysprosessissa. Kehityksessä on orgaanisen evoluution piirteitä, koska uudet teknologia kerrokset muodostuvat entisten päälle, joiden ajallinen kehittyminen voidaan identifioida. Teknologia on omaksunut sukupolvi-käsitteen, joka kuvaa tietokoneen tai ohjelmiston uusimman tuotteen suhdetta aikaisempiin malleihin. [45]

Puolustusvoimien kybertoimintaympäristön verkottuneisuus aina voimankäytöstä huolto- ja logistiikkajärjestelmiin saakka edellyttävät keskitettyä tilannekuvan luomista ja kybervaikuttamista. Ilmapuolustuksen ei-kineettiset operaatiot keskittyvät elektronisen sodankäynnin operaatioihin, osallistumiseen yhteisinformaatio-operaatioihin ja kybertiedusteluun sekä omien järjestelmien suojaamiseen kyberhyökkäyksiä vastaan.

Kybersodankäynnissä ilmapuolustuksen toiminta kohdistuu defensiivisiin toimintoihin. Ilmavoimissa tulee kehittää kybertilannetietoisuutta yhdessä muiden toimijoiden kanssa ja luoda uhka- ja riskianalyysin ilmapuolustuksen kriittisestä infrastruktuurista ja informaatioinfrastruktuurista. Lisäksi tarvitaan edellä kuvattujen ei-kineettisten operaatioiden tehokasta integroimista keskenään, kineettisiin operaatioihin ja puolustusvoimien yhteisoperaatioihin. Tässä integrointikehityksessä korostuu ilmaoperaatiokeskuksen rooli sekä kineettisten että ei-kineettisten operaatioiden johtamispaikkana.

Kyberteknologian kehittämisen rinnalla on huolehdittava kybersodankäynnin kognitiivisen dimension kehittämisestä. Yksilö (päätöksen tekijä – yksittäinen sotilas) laitteiden ja järjestelmien käyttäjänä on viimekädessä luomassa kybersuorituskykyisyyttä. Kyberteknologia nopea kehitys ja systeemien monimutkaistuminen edellyttävät kognitiivisen osan kehittämistä rinnan teknologian kanssa. Kehittämisen keskiöön nousee kaikkien toimijoiden kyberosaamisen kehittäminen uusien suorituskykyvaatimusten edellyttämälle tasolle.

---

[44] Arthur W. Brian, Teknologian luonne, Terra Cognita, Helsinki 2010, s. 188 - 189.
[45] Arthur W. Brian, Teknologian luonne, Terra Cognita, Helsinki 2010, s. 189 - 190

9.2.6 Kybermaailma 2020

Kybermaailman sotilaallisessa ulottuvuudessa korostuvat 2020-luvulla tilannetietoisuus, kyberpelote, kyberfyysiset systeemit ja kognitiotason vaikuttaminen.

Sotilaallista kybertilannetietoisuutta rakennetaan lähes kaikissa maissa. 2010-luvulla useissa maissa on perustettu kyberturvallisuuskeskuksia vastaamaan kansallisesta kybertilannekuvasta ja koordinoimaan kyberturvallisuustoimenpiteitä. Seuraava askel on ollut asevoimien kyberpuolustuskeskusten rakentaminen, joiden tehtävänä on kansallisen kybertilannekuvan muodostaminen ja kyberoperaatioiden johtaminen.

Kybersodankäynnin asema puolustushaarana, aselajina tai operaatiokonseptina vaihtelee maittain, mutta tavoitteena on kybertilannetietoisuuden kehittäminen päätöksenteon ja kyberoperaatioiden johtamisen perustaksi.

Kyberpelotetta tulevat ainakin kaikki suurvallat rakentamaan. Kiina on julkisesti ilmoittanut rakentavansa kyberpelotteen ydinpelotteen rinnalle. Kyberpelotteen kehittämistä kiihdyttää sen edullisuus. Siinä missä modernin häivehävittäjän hinta on yli 100 miljoonaa euroa, niin hyökkäysohjelmien koodaaminen maksaa korkeimmillaan kymmeniä miljoonia euroja. Koulutettuja osaajia ei tarvita kyberaseiden suunnitteluun, kehittämiseen ja käyttöön tuhansia vaan kymmenillä huippuosaajilla voidaan tuottaa maailmanluokan kybersuorituskykyjä. Tässä uudessa tilanteessa maailmanpolitiikan voimasuhteet saattavat muuttua, jos useat maat todella investoivat kyberpelotteeseen.

Kyberfyysisen maailman asioiden ja laitteiden verkottuminen eli Internet of Things (IoT) on nopeasti kasvava ala, jossa syntyy miljardiluokan liiketoimintaa. Internet of Things -markkinan suurin kasvu syntyy analytiikasta, sovelluksista ja palveluista. IoT:n sanotaan edustava kolmatta teollista vallankumousta, jossa tuotanto ja liiketoiminta siirtyvät digitaalisiin toimintaprosesseihin, kanaviin, sisältöihin ja transaktioihin. IoT tulee olemaan kyberfyysinen ekosysteemi, jossa miljardit esineet ja laitteet kommunikoivat keskenään.

Sotilaalliset järjestelmät eivät jää IoT:n ulkopuolelle. Siitä muodostuu sotilaallisten asioiden ja laitteiden internet eli Internet of Military Things. Laite- ja järjestelmätasolla tapahtuu konvergenssi sotilaallisten ja siviilipohjaisten ratkaisujen välillä. Laitteiden ja järjestelmien älykkyys rakentuu mikro- ja nanoelektroniikan perustalle niin sotilaskuin siviilisovelluksissakin. Tämä kehitys on aiheuttanut kyberuhkien laajentumista ohjelmisto- ja verkkotasolta (software) laite- ja järjestelmätasolle (hardware). Pahimpien arvioiden mukaan 40 %:ssa Yhdysvaltain asevoimien järjestelmiä on korruptoituneita laitteita ja osia.

Samalla, kun yhä enemmän huomiota on kiinnitetty haittaohjelmien havaitsemiseen ja torjuntaa, niin hyökkäykset ovat siirtyneet verkkojen ohella laitteisiin. Tällaisia hyökkäysvektoreita on erilaisia, kuten haittaohjelman asentaminen laitteen installointivaiheessa, toimintalogiikkaa muuttavan osan asentaminen laitteeseen sen varastointivaiheessa, hyökkäyksen kohdistaminen laitteen kehittämisprosessiin jo laboratoriovaiheessa tai haittaohjelman asentaminen mikropiireihin jo niiden valmistusvaiheessa. 2020-luvulla korostuu kyberfyysinen toimintaympäristö, jossa kyberoperaatiot kohdistuvat sekä virtuaaliseen maailmaan että fyysiseen laiteympäristöön. Tämä korostaa valvonnan, hallinnan ja tilannetietoisuuden rakentamista aina laitteiden ja

ohjelmistojen suunnittelu- ja laboratoriovaiheesta niiden tuotantovaiheeseen, implementaatio- ja käyttöönottovaiheeseen ja itse systeemien käyttöön.

2020-luvun kybermaailman suurimmat taistelut käydään ihmisten mielissä. Strategisessa kommunikaatiossa ei-kineettisten operaatioiden avulla tavoitellaan sodan voittamista käyttäen mahdollisimman vähän kineettistä voimaa. Strategisesta kommunikaatiosta on tullut valtioille toimintatapa, jolla se pyrkii luomaan kansallista turvallisuutta ja kansakunnan yhtenäisyyttä sekä vahvistamaan tarvittavia uhkakuvia kansalaisten ja sotilaiden mielissä. Strategisen kommunikaation paradigmassa koko maailma on kybertaistelutila, jossa informaatiota on vaikea hallita. Sosiaalisen median eri muodot ulottuvat taistelukentälle ja se haastaa valtiollisen kontrollin.

Strategisen kommunikaation paradigma ei hylkää kineettisten suorituskykyjen suunnittelua, kehittämistä, rakentamista ja käyttöä, mutta niiden ensisijaisuus asetetaan kyseenalaiseksi. Siinä missä kineettisten suorituskykyjen käyttö on näkyvää, niin strateginen kommunikaatio on näkymättömämpää ja se halutaankin verhota esimerkiksi patriotismin ja kansallisten etujen suojaamisen taakse. Ei-kineettisten operaatioiden suorituskykyjen kehittämiskohteina ovat erityisesti psykologiset operaatiot, harhauttaminen ja operaatioturvallisuus.

Kansallisen puolustuksen näkökulmasta puolustusvoimien tulee säilyttää oma toimintavapautensa ja vaikuttaa vastustajaan kaikilla ei-kineettisillä operaatioilla kybertaistelutilassa kaikissa olosuhteissa. Puolustusvoimien tulee kyetä kiistämään vastustajan toimintavapaus koko kybertaistelutilassa. Tämä edellyttää puolustusvoimien kyberpuolustuskeskusta, jolla on riittävä kyky kybertilannekuvan luomiseen ja yhteisten kyberoperaatioiden johtamiseen. Puolustusvoimat tarvitsee kyvykkyyksiä tilannetietoisuuden luomiseen, vastustajan kyberhaavoittuvuuksien tiedusteluun, maalittamiseen ja vaikuttamiseen tavoitteena kohteiden haltuunotto, lamauttaminen tai tuhoaminen. Puolustushaaroilla tulee olla kyky hallita omaa kybertoimintaympäristöään.

10.

Kybertaisteluiden kritiikki - kohti menetettyä vai menestynyttä taktiikkaa?

Sotilasprofessori Jari Rantapelkonen
Taktiikan laitos
Maanpuolustuskorkeakoulu

Jari Rantapelkonen on tulevaisuuden sotataidon sotilasprofessori Maanpuolustuskorkeakoulussa. Rantapelkonen on väitellyt sotatieteiden tohtoriksi sodan johtamisesta vuonna 2006. Everstiluutnantti Rantapelkonen on kiinnostunut teknologian vaikutuksista operaatiotaitoon ja taktiikkaan sekä informaatiosodan filosofiasta ja käytännöistä.

10.1 Kyberin hämärä ja valo

Kyberin hämärä on vertauskuva sille, kuinka kyber koetaan asevoimissa. Kyberistä puhutaan jo sujuvasti, vaikka käsitteen määrittelytyö on koettu vaikeaksi. Kyber koetaan sotilaskulttuurissa vielä pääosiltaan kaukaiseksi ja epämääräiseksi alueeksi. Tätä vaikeasti tartuttavaa möykkyä pidetään kuitenkin tulevaisuuden sodankäynnille tärkeänä kehitettävänä suorituskykyalueena.

Kyberin hämärään etsitään valoa tutkimuksen keinoin ja harjoittelemalla kybertaisteluita. Kyberin hämärän valaistumista ei edistä se, että kyberistä puhutaan taisteluihin jotenkin erillisenä kuuluvana tekijänä, bittien ujelluksena tietoverkoissa. Valaistuminen koetaan vasta kun kybertaisteluilla on konkreettista vaikutusta sotilasjoukkojen toimintaan: tiedusteluun, johtamiseen, tulenkäyttöön ja/tai logistiikkaan.

Aina silloin tällöin vielä kuulee väitettävän, että kyber on tulevaisuutta. Väite siitä, että kyber ei olisi asevoimien toiminnassa tämän päivän arkea, on yksi suurimmista sotataidollisista väärinymmärryksistä. Kyber näkyy, tuntuu ja on läsnä konflikteissa vahvasti jo tänään[1]. Näin ei ole vain pelkästään huipputeknologisten maiden asevoimissa, kuten Yhdysvalloissa tai Ruotsissa. Kyber on sekä toimintaympäristö että väline toimijoille niin Afganistanissa kuin erilaisissa kumouksellisissa aseellisissa ryhmittymissä Syyriasta Somaliaan. Tästä käy esimerkkinä Anonymous-järjestö, joka julisti kybersodan Isisille syyskuussa 2014[2].

Tietoverkkoja on käytetty jo vuosia tiedusteluun, sekä tietojen keräämiseen että niiden analysoimiseen. Tietoverkkoja on käytetty jo vuosia tietojen välittämiseen ja viestintään. Maavoimien tulenkäyttöä ei ole ilman tietoverkkoja, ilmavoimien hävittäjät eivät lennä ilman ohjelmistoja eivätkä merivoimien alukset liiku saaristossa ilman tietoteknisiä navigoimisjärjestelmiä. Tämä riippuvuus vain kasvaa. Kyber hiipii ja on jo hiipinyt hämärästä tekijäksi, jota ilman fyysistä väkivaltaa on vaikea käyttää ja sotia

[1] Arquilla (2012). Cyberwar Is Already Upon Us. Foreign Policy, Mar/Apr 2012, issue 192, s.-1 - 4.
[2] Kashyap, Praveen (2014). Anonymous Hackers to launch Cyber War against ISIS. Anonymous Anonymous Headlines News, Sept 24, 2014.

käydä. Kyber ei ole enää tulevaisuutta eikä kyber ole pelkästään hakkereiden touhua. Kyberiin suhtaudutaan vakavasti asevoimissa[3]. Toisaalta on ymmärrettävä, että kyber ei ole pelkästään asevoimien vastuulle sälytetty asia, pikemminkin päinvastoin. Suuri väärinymmärryksen hämärä valaistuu vasta, kun kyberin ymmärretään merkitsevän kaikille: politiikalle, taloudelle, asevoimille, viihteelle – kaikille ihmisille jotain tärkeää – jo tänään.
Kyberiin liittyvien epämääräisyyksien selkeyttäminen ei ole helppoa. Kyberin rajojen määrittäminen on lähes mahdotonta monien keskinäisriippuvuuksien takia. Toisista sodista saamme, kiitos kyberin, päivittäin informaatiota suoraan koteihimme (Ukraina), kun taas toisista emme kuule juuri mitään (Kongo). Ilman kyberverkkoja sodat tuskin olisivat nykyisenkaltaisia informaatiointensiivisiä mediaspektaakkeleita.

Kyber mahdollistaa aikamme informaatiosodat, joissa sekoittuvat fakta ja fiktio sekä tieto ja tunne. Kyber ei suinkaan ole tehnyt tilannekuvista ymmärrettävämpiä vaan hämärämpiä. Mediasta ja sosiaalisesta mediasta on tullut osa kyberiä, joka vielä vuosia sitten oli hakkereiden ja tekniikan erikoisosaajien temmellyskenttää. Kyber on paradoksaalisesti osaltaan vaikuttanut siihen, että uutisoinnin peruspilarit, viestinnän uskottavuus ja luotettavuus, ovat koetuksella, vaikka tarkoituksena on parantaa tilannekuvaa ja ymmärrystä siitä, mitä ympärillämme tapahtuu. Tämän päivän kyber piiloutuu informaatiovirtoihin tavalla, jota asevoimat eivät voi jättää huomiotta omassa toiminnassaan.

Kyber laajentaa taistelutilaa. Kun tarkastellaan taistelukenttiä Ukrainassa, Syyriassa tai Irakissa, kyber on eittämättä osa sodankäyntiä. Kyberin erityispiirteenä voidaan pitää sitä, että kyber ei tunnusta valtioiden rajoja samaan tapaan kuin fyysiset valtioiden rajat kontrolloivat liikennettä. Kyber saa taistelut ulottumaan taisteluita käyvien maiden fyysisten rajojen ulkopuolelle. Taistelut verkossa eivät rajoitu sotaakäyviin maihin, vaan ne ulottuvat fyysisen alueen ulkopuolelle, myös verkkojen ulkopuolelle, sotaa käymättömien ihmisen tajuntaan, jolloin kyberympäristössä kaikista tulee osallisia. Kyber kyseenalaistaa perinteisen sodankäynnin käsitteen.[4]

Kyber tekee aseen määrittelystä ongelmallisen[5]. Kyberiä on kuitenkin käytetty taktisena ”aseena” jo vuosia ennen nykyhetkeä, esimerkiksi Egyptissä (2012), Libyassa (2011), Iranissa (2010), Georgiassa (2008) ja Virossa (2007) ja Lähi-idässä (2006). Kyberin valo on näyttäytynyt hakkereiden harmittomasta matosodasta Stuxnet-haittaohjelman aiheuttamiin fyysisiin vaikutuksiin. Samalla kyberin käsitteistö kyseenalaistaa sotilaan ja koko sodan määritelmän siitä, kuka käy sotaa ja mitä sota on. Kyber ei ole käytännössä pelkästään jäänyt aseen määrittelyn tasolle, tekniseksi taituruudeksi tai kikkailuksi verkoissa, vaan kyberistä on muodostunut toimintaympäristö, jossa tiedustellaan, maalitetaan, mobilisoidaan ihmisiä sotaan ja vaikutetaan mielipiteisiin.[6]

[3] Ks. myös Rantapelkonen, Jari & Salminen, Mirva (2013). The Fog of Cyber Defence.
[4] Huhtinen, Aki ja Rantapelkonen, Jari (2008). Messy Wars. Finn Lectura, Helsinki.
[5] Ulkoasiainvaliokunta (2014). Asevalvontaa kehitettävä vastaamaan uuden aseteknologian ja kyberturvallisuuden haasteita. Eduskunnan ulkoasiainvaliokunnan mietintö koskien aseteknologian kehitystä ja sen vaikutusta aseriisuntaan ja asevalvontaan (K 13/2013 vp). Ulkoasianvaliokunnan mietintö 5/2014 vp, 9. huhtikuuta 2014.
[6] Ks. esim. Hollis, David (2010). Cyberwar Case Study: Georgia 2008. Small Wars Journal.

Informaatio- ja viestintäteknologia on kyberisoinut yhteiskuntia. Teknologian muovaama evoluutio on samalla laajentanut sodankäynnin ulottuvuuksia mittoihin, joita ei ollut *Verkkotaistelut 2020* -kirjan julkistamisen aikoihin, hieman yli kymmenen vuotta sitten, yhtä helppoa kuvitella kuin tänä päivänä. Valtioista on tullut keskeisiä toimijoita kyberavaruudessa niin tiedustelun kuin vaikuttamisenkin suhteen. Ohjelmistoista on tullut aseisiin verrattavia vaikuttamisen välineitä. Koneista on tullut sotilaita tehokkaampia, ainakin informaation välittämisen rintamilla. Samalla kyberistä on tehty yhä kokonaisvaltaisempaa asiakokonaisuutta, jonka merkitysten ymmärtäminen ja hallinta on tullut haasteelliseksi.

Tulevaisuus ei välttämättä näytä pelkästään positiiviselta, sillä kyberhyökkäyksien arvioidaan seuraavan vuosikymmenen aikana lisääntyvän. Osana Digital Life in 2025 -projektia, asiantuntijat arvioivat, että vuoteen 2025 mennessä kyberhyökkäyksillä aiheutetaan laajaa vahinkoa ja haittaa kansalliselle turvallisuudelle ja kyvylle puolustaa maata ja ihmisiä. Laaja vahinko on määritetty merkittäväksi ihmishenkien menetyksiksi, omaisuuden tuhoksi ja varkauksiksi arvoltaan kymmeniä miljardeja dollareita. Näin tulevaisuus vaatii toimenpiteitä, joihin valtion ja yhteiskunnallisten toimijoiden, kuten asevoimien ja organisaatioiden, tulee ryhtyä varautuakseen kyberuhkiin.[7]

10.2 Kybertaktiikan lupauksen lunastaminen

Vuonna 2003 julkaistun *Verkkotaistelu 2020* -kirjan kritiikkipuheenvuorossa peräänkuulutettiin tekniikan ensisijaisuuden sijaan kybertaktiikan kehittämistä[8]. Kybertaistelut eivät ole nousseet taktiikan huomion keskiöön kuten jalkaväki, tykistö, viesti tai huolto – huolimatta kyberpuheiden hypestä[9].

Kybertaistelut eivät ole taktisen ajattelun ytimessä. Yksi syy on kyberin kompleksisuus ja samalla muutoksen nopeus, joka ei ole jättänyt tilaa taktiikalle. Kybersuorituskyvyn kehittäjillä on ollut tarpeeksi tekemistä toimivan kybertoimintaympäristön kehittämiseksi. Toinen syy voi olla kyberin teknologinen luonne, jossa ei ole tilaa taktiikalle. Kolmas syy, joka juontaa juurensa kahdesta edellä mainitusta, on asevoimien kulttuuri. Kybertaisteluiden suunnittelua ja toimeenpanoa ei ole asevoimissa koettu – huolimatta retoriikasta – samalla tavalla operatiiviseksi asiaksi, kuten 2000-luvun alussa kuviteltiin. Kyberistä ei ole tullut asevoimissa samalla tavalla koettua välinettä kuin muista, perinteisemmistä, aseista ja sotilasjoukoista. Tämä taas voi johtua asevoimien kulttuurista, jossa korostuu fyysisyys ja konkreettisuus, se, että vaikutus halutaan nähdä saman tien.

Vuonna 2003 kirjoitetusta kritiikkipuheenvuorosta voi lainata tähän yhteyteen edelleen osuvan ajatuksen: ”Sotilaiden on vaikea ollut tarttua tähän monimutkaiseen ja moniselitteiseen verkkotaisteluilmiöön. Se näkyy tässä kirjassa kirjoittajien valinnas-

---

[7] The Guardian (2014). The Guardian (2014). Internet experts see ‘major cyber attacks’ increasing over next decade. The Guardian, Oct 29, 2014. Online http://www.theguardian.com/technology/2014/oct/29/major-cyber-attacks-internet-experts

[8] Rantapelkonen, Jari & Virtanen, Jukka-Pekka (2003). Kritiikkipuheenvuoro – verkkotaistelut ”tekniikasta taktiikkaan” -tiellä? Kirjassa Piiroinen, Mika (toim.) (2003). Verkkotaistelu 2020. Taustatutkimus Maavoimien taistelun kuvat 2020 tutkimukseen, Taktiikan laitos, Julkaisusarja 2, N:o 2/2003, s.93-111.

[9] Rantapelkonen Jari (2014). Kyberpuheen osumat ja heittolaukaukset. Maanpuolustuskorkeakoulu, 7.2.2014. Saatavilla Googlesta hakemalla otsikon mukaista tekstiä.

sa. Toisaalta kirjoittajien valinta osoittaa viisasta harkintaa, sillä mukaan on saatu Puolustusvoimien ulkopuolisia asiantuntijoita.[10]”

Kyber ei ole onnistunut lunastamaan tai raivaamaan paikkaa ainakaan sotilaallisesta ytimestä, kuten komentajien operatiivisista perusajatuksista tai operaatiopäälliköiden piirtämistä hyökkäys- ja puolustusliikkeistä. Se panee kysymään, onko kyberin aseman tuleminen operatiiviseen ytimeen vielä tulevaisuudessa vai onko se löytänyt paikkansa erikoisasiantuntijoiden taistelutekniikkana, hieman samaan tapaan kuin johtamisjärjestelmien ”pyörittäminen” yhtymissä asemoituu.

Kyber on mitä todennäköisimmin tekemässä suurempaa läpimurtoa Suomeen ja sen puolustusvoimiin. Yksi indikaatio on Suomen kyberturvallisuusstrategian ja sen toimeenpano-ohjelman julkaiseminen. Puolustusvoimissa on harjoiteltu kybertaisteluita, pienessä mittakaavassa ja valikoidulla joukolla, jo vuosikymmenen ajan. Suomalaiset kyberasiantuntijat yrityksistä ja turvallisuustoimijoista ovat harjoittaneet kyberyhteistyötä useiden maiden kanssa niin tiedonvaihdon kuin oppimisen ja harjoittelun alueilla useiden maiden välillä.

Kyberin tulemisen pitkään uumoilu osoittaa, että sodankäynnissä harvoin tapahtuu vallankumouksia, ainakaan kovin nopeasti. Sodankäynnin muutokset ovat usein hyvin evolutiivisia, joihin kuuluu toki sykäyksellisyys. Vaikka teknologian puolella tapahtuisi harppauksia, muutokset tapahtuvat hitaasti, mikä taas johtuu kulttuurisista tekijöistä. Kyber on selkeästi muuttanut suomalaisten tapoja (pankissa-asiointi, lehtien ja kirjojen lukeminen, suunnistaminen teknisten välineiden avulla, uutisten lukeminen verkosta tai vaikkapa ystävien tapaaminen verkossa ja sosiaalisessa mediassa). Muutos on ravisuttanut myös perinteistä asevoimakulttuuria, joskin muutos olisi teknologian puolelta tarkasteltuna voinut olla nopeampaa ja dramaattisempaa.

Puolustusvoimat on haasteiden tienhaarassa, jossa se joutuu tekemään arvovalintoja tulevaisuuden suhteen. Sodan ajan vahvuutta on supistettu sadoilla tuhansilla ihmisillä. Luku on hurja. Puolustusvoimille osoitetut määrärahat eivät kasva, ja samoilla määrärahoilla ei ole samanlaista ostovoimaa kuin aiemmin, sillä teknologia kallistuu nopeammin kuin ostovoima. Puolustusvoimille osoitetuilla taloudellisilla varoilla saa aiempaa vähemmän. Kompensaatiota haetaan uudesta teknologiasta ja uusista toimintatavoista.

Puolustusvoimat haluaa kehittää tulevaisuuden sotilaallisia kykyjään myös verkossa, kybertoimintaympäristössä. Kybertaistelut ovat osa sodankäyntiä, mutta verkossa voidaan taistella myös itsenäisesti ilman niiden liittymistä toimintaan maalla, merellä ja ilmassa. Tämä tosin voi olla hyvin hankalaa. Vaikka verkkotaistelut eivät enää ole uusi asia, on uutta se, että sodan ajan joukot ovat yhä enemmän riippuvaisempia kyberistä, tiedustelun, valvonnan ja johtamisen sekä tulenkäytön järjestelmistä, jotka perustuvat kriittisiltä toiminnoiltaan informaatio- ja viestintäteknologiaan.

Muutamissa läntisissä asevoimissa on kyberiä varten perustettu oma puolustushaara tai ainakin merkittävä johtoporras koordinoimaan verkoissa tapahtuvaa puolustusta ja

[10] Rantapelkonen, Jari & Virtanen, Jukka-Pekka (2003). Kritiikkipuheenvuoro – Verkkotaistelut ”Tekniikasta taktiikkaan” – tiellä? Teoksessa Piiroinen, Mika, toim. (2003). Verkkotaistelu 2020. Taktiikan laitoksen julkaisusarja 2, N:o 2/2003, Maanpuolustuskorkeakoulu, Helsinki, s.96.

hyökkäystä. Esimerkiksi Yhdysvalloissa perustettiin vuonna 2009 kyberiä varten oma johtoporras suunnittelemaan ja toimeenpanemaan niin puolustuksellisia kuin hyökkäyksellisiä kyberoperaatioita maailman tietoverkoissa. Kyberjohtoportaan tavoitteena on taata Yhdysvalloille ja sen liittolaisille toimintavapaus kyberavaruudessa samalla kun se estetään niiden vastustajailta.

Myös Venäjä on ollut aktiivinen kyberrintamilla. Kyberhyökkäykset Virossa vuonna 2007 ja Georgiassa vuonna 2008 ovat paljon käytettyjä esimerkkejä siitä, kuinka kyberiä on viime vuosina käytetty. Viroon on perustettu ”Nato Cooperative Cyber Defence Center of Excellence”, joka sai kansainvälisen tunnustuksen vuonna 2008 siitä, että kyseessä on sotilaallinen kyberiin keskittyvä organisaatio. Keskuksen tehtävänä on tukea kyberpuolustuksen kehittämistä. Norjassa perustettiin vuonna 2012 asevoimiin uusi puolustushaara nimeltä ”Cyberforsvaret”. Kyberistä on selkeästi tullut asevoimien osa ja osa niiden sotilaallista toimintaa.

Tärkeä kysymys, jota puntaroidaan, on pitäisikö erillistä kyberrintamaa johtaa vai onko kyber keskeinen osa kaikkea toimintaa. Tämä vaikuttaa myös mahdollisuuksiin kehittää verkkotaisteluissa vaadittavaa kybertaktiikkaa. Ilman kybertaktiikkaa taisteluilta puuttuu ajatus. ja ilman ajatusta ei ole päämäärätietoista toimintaa.

10.3 Operaatiotaidon kehittämisestä

Pelkkä kyberstrategia ei anna riittävästi perusteita kybertaktiikan kehittämiselle. Kybertaistelutekniikan kehittäminen sen sijaan antaa perusteita kybertaktiikan kehittämiselle. Sotataidossa operaatiotaito on avain menestyksekkääseen taktiikkaan, sillä operaatiotaidon unohtaminen johtaa vain loputtomiin taisteluihin ilman liityntää laajempiin sodankäynnin kokonaisuuksiin.

Operaatiotaidollisesti kyberissä riittää haasteita aina kyberin käsitteestä ja käsitteellistämisestä verkkotaistelukentän laajuuteen. Kun verkkotaisteluiden käsitteen epämääräisyyttä kritisoitiin yli kymmenen vuotta sitten, sama pätee nykyisin kyberin tai paljon kiistellyn kybersodankäynnin käsitteisiin. Kyberoperaatioiden rajojen määrittäminen ja niiden hallinta johtanee laadukkaampaan taktiikkaan.

Verkkotaisteluiden laajenemisen kannalta haasteet tuntuvat kuitenkin lisääntyvän. Internet monimutkaistuu samalla kun se on yhä isompi osa tulevaisuuden kybertaistelukenttää, myös asevoimien toimintaa. Australian asevoimien mukaan kybersodankäynti, harhauttaminen ja disinformaatio internetissä ovat keskeinen osa tulevaisuuden sodankäyntiä ja asevoimien sotilaallisia operaatioita. Trendi on jo laajemmaltikin eri maissa havaittavissa, joskaan Australian asevoimissa ei ole selkeitä ohjeita siitä, kuinka näillä taktisilla keinoilla vaikutetaan vastustajaan[11]. Kyber ei ole enää itsenäinen saareke, jolla ei olisi selviä yhteyksiä ja liittymäpintoja sotataidon muille alueille.

Läntisissä asevoimissa kuljetaan operaatiotaidollisesti ja taktisesti eriskummalliseen suuntaan. Harhauttamista rajataan ulos operaatiotaidon välinepakista. Esimerkiksi puolustusvoimain komentaja on todennut, että ”Suomi ei perusta disinformaatiojouk-

[11] Dorling, Philip (2014). ADF to embrace cyber warfare in future military operations. The Sydney Morning Herald, May 5, 2014. See: http://www.smh.com.au/federal-politics/political-news/adf-to-embrace-cyber-warfare-in-future-military-operations-20140505-zr4ws.html#ixzz3CM3Br4FN.

koja”. Tämä on Akilleen kantapää taistelukentällä, jossa vastassa on joukko, jolla kyseiset keinot ovat käytössä. Toisaalta voisi helposti kuvitella, että tekninen harhauttaminen olisi hyväksytympää kuin sisällöllinen harhauttaminen, esimerkiksi mediassa. Tämä puoltaa ajatusta, jossa kybertaktiikka ja sen kehittämisen suunta jäisi tekniikan tasolle, ja se olisi siten hallitumpi kokonaisuus. Tällaisille ajatuksille, jossa jokin sodankäynnin keskeinen periaate jätettäisiin kybertaktiikan kirjosta pois, tulisi varata aikaa ja paikkoja keskustella läpikotaisin mistä oikein on kysymys. Harhauttaminen kun on ollut kautta sotataidon historian keskeinen osa sodankäyntiä. Paradoksaalista on se, että informaatioaika on vain lisännyt harhauttamisen mahdollisuuksia ja käytäntöjä. Media on köyhän miehen tiedustelumaasto ja rikkaan miehen propagandaalusta. Kyberympäristö luo molemmille oivia mahdollisuuksia. Kuinka hyväksyttäviä ne ovat, on kysymys, jota tulee jatkossa avata, sillä sitä kysymystä ei tässä kirjassa tarkastella.

Suomen puolustuksen strategia on perustunut puolustamisen ajatukselle. Suomen kyberstrategian linjausten mukaan Puolustusvoimille tulisi kuitenkin kehittää kokonaisvaltainen kyberpuolustuskyky. Se tarkoittaa kykyä tiedustella kyberympäristössä ja analysoida informaatiotulvaa sekä toimeenpanna puolustuksellisia ja hyökkäyksellisiä kyberoperaatioita. Tiedustelulain valmistelu Suomessa on viime aikoina herättänyt keskustelua. Aika näyttää, millaisia ratkaisuja sen suhteen tehdään, mutta vaikutukset voivat pahimmillaan olla ”kokonaisvaltaisen puolustuskyvyn” kannalta dramaattisia. Kyberoperaatioiden mahdollisuuksia saatetaan Suomessa rajata itse ja oma-aloitteisesti. Seurauksena voi olla puutteellinen verkkotiedustelukyky, mikä tarkoittaa sitä, että puolustaja on enemmän tai vähemmän sokea ennen kuin yhtään laukaustakaan on ammuttu. Seurauksena on puutteellinen hyökkäyskyky. Puolustaja ei voi tietää, mihin se hyökkää, jos se ei tunne kybertoimintaympäristöä, kyberin ”taistelumaastoa”, riittävän hyvin.

Toisaalta voidaan ajatella ja samalla välttää kyseinen kritiikki siten, että itse laki ei estäisikään suorituskykyjen kehittämistä eikä kybertaisteluiden harjoittelua, vaan se estäisi pelkästään tiedustelu- ja hyökkäyskyvyn rauhanaikaista käyttöä. Näin ollen vuonna 2003 kritiikkipuheenvuorossa tehty ehdotus liittää verkkotaisteluiden käsitteet valmiuslainsäädäntöön pitää edelleen ajankohtaisuudessaan paikkaansa.

10.4 Verkkotaisteluiden ja kyberaseiden luonteesta

Verkkotaisteluista on käsitteellisesti ja taisteluteknisesti kirjoitettu paljon. Sen sijaan Puolustusvoimien näkökulmasta aiheesta ei julkisesti juuri ole kirjoitettu. Merkittävin lienee 2013 Maanpuolustuskorkeakoulun sarjassa julkaistu *The Fog of Cyber Defence*.

Maailmalla on kuitenkin menty kymmenessä vuodessa lujaa, niin kybertaistelukyvyn kehittämiseksi kuin sen käyttämisen suhteen. Verkkotaistelukyvyn kannalta tarkasteltuna Suomessa kamppaillaan edelleen kybertoimintaympäristön perusteiden ja suorituskyvyn kehittämisajatusten parissa. Toisaalta Suomessa on kehitetty huippuosaamista erityisesti tietoturvallisuuden ja siihen liittyvän toiminnan alueilla.

Verkkotaisteluiden kannalta tarkasteltuna keskeinen kehitys on näkynyt ”kyberaseiden” saralla. Niiden rinnastaminen perinteisiin aseisiin on ongelmallista, mutta ”kyberaseiden” käyttö tuntuu vain lisääntyvän. ”Tähän on useita syitä, joista yksi on kybe-

raseiden edullisuus verrattuna perinteisiin aseisiin. Ongelmaksi tässä kehityksessä nähdään muun muassa se, että kyberaseet tarjoavat käytännössä mahdollisuuden anonymiteettiin. Kyberase, esimerkiksi haittaohjelmisto, poikkeaa luonteeltaan rynnäkkökivääristä, ohjuksista, panssarivaunuista ja muista tavanomaisista aseista. Vertaus aseeseen on ongelmallinen. Lisäksi kyberaseiden kaksoiskäyttö sekä siviilitarkoituksiin että sotilaallisiin tarkoituksiin lisää valvonnan haasteita. Samalla kyberaseiden havaittavuus lisää haasteita.[12]

Ehkä yksi vaikeimpia haasteita aseriisunnalle on yleisesti ohjelmistojen elinaika." Tämä kertoo hyvin verkkotaisteluiden luonteesta, siitä, kuinka "Kyberiin vaikuttavat trendit haastavat perinteisen turvallisuusajattelun varaan rakennetut ajatusmallit, valtarakenteet, johtamismallit ja jäykähköt toimintatavat." Tässä maailmassa "ratkaisuksi on haettu joustavampia ajatusmalleja ja toimintatapoja sekä verkostoitumista sillä kyberympäristöä ei voi yksiselitteisesti rinnastaa muihin toimintaympäristöihin."[13]

10.5 "Tartuntoja" kirjan artikkeleista

Tarkastelen seuraavaksi mitä kirjan artikkelit saavat ajattelemaan verkkotaisteluista. Kirja *Kybertaistelu 2020* tarjoaa kybertaisteluun useita eri näkökulmia. Lähtökohta on perusteltu, sillä ei ole olemassa yhdenlaista kybertaistelua. Kyber näyttäytyy hyvin erilaiselle riippuen mistä sitä tarkastellaan, esimerkiksi kyberhistorian, teoreettisesti, tiedonhallinnan, lainsäädännön, hyökkäyksen, puolustuksen, yrityksen, maavoimien tai ilmavoimien näkökulmasta. Oleellista onkin kysyä mikä näistä näkökulmista määrittää kybertoimintaympäristöä ja mikä niistä luo toiminnalle rajat. Tämä kirja kertoo tarpeesta, jossa yhdellä näkökulmalla ei ole mahdollisuuksia menestyä verkottuneessa maailmassa vaan tarvitaan useita, rinnakkaisia, yhtäaikaisia näkökulmia, jotka vaikuttavat puolustusvoimien kybertaistelukyvyn kehittämiseen.

"Verkkotaisteluiden historia" on erittäin tarpeellinen artikkeli kuvaamaan kyberin historiaa ja kytkemään kyber osaksi laajempaa kehitystä. Ahvenaisen artikkelin ansiosta lukijalla on mahdollista paremmin ymmärtää nykyistä keskustelua verkkotaisteluista. Ahvenaisen näkökulma panee miettimään miten kävisi kybertaktiikan jos kyber pohjaisi teoreettisen ajattelun kybernetiikkaan. Kävisikö kybertaktiikalle kuten kritiikissäni yhtenä vaihtoehtona esitän, että kyber jäisi pelkästään joko systeemiksi tai taistelutekniikaksi ilman taktiikkaa.

Samalla Ahvenainen kuitenkin muistuttaa, että sodankäynti on myös taitoa, joka liittyy ihmisiin – pelkän kyberneettisen järjestelmän ja sen "säätelyn" sijaan. Jatkopohdintoja varten olisi mielenkiintoista kuulla millaisia taitoja verkkotaisteluissa tarvitaan. Onko kysymys yksilön kybertaidoista, organisaation taidoista toimia kybertoimintaympäristössä vai onko kysymys kybertaisteluiden perusajatuksista, taisteluiden suunnittelusta ja taidokkaasta toimenpanosta? Tämä saattaa johtaa vastaukseen kuinka kyber tulisi ymmärtää.

---

[12] Rantapelkonen, Jari (2014). Kansallinen turvallisuus kohtaa kybertrendit – haasteista tänään ja huomenna. Futura 2/2014, s.49 - 57.

[13] Rantapelkonen, Jari (2014). Kansallinen turvallisuus kohtaa kybertrendit – haasteista tänään ja huomenna. Futura 2/2014, s.49 - 57.

Vallalla olevan käsityksen mukaan kyber on asevoimille uusi toimintaympäristö, jossa tulisi kyetä taistella. Ahvenaisen mukaan tämä käsitys kyberistä on kuitenkin liian pelkistetty ymmärrys. Ahvenainen antaa ymmärtää, että kysymys on väärinymmärryksestä sillä kyber on myös ihmisen päässä[14]. Juuri tämä päätelmä puoltaa ajatusta kybertaktiikan kehittämiseksi. Taktiikan tulee kertoa selkeistä tavoitteista ja päämääristä. Taktiikassa tulee toimeenpanna tilanteeseen sopivia periaatteita. Ilman ihmistä ei ole ajattelua ja ilman ajattelua ei ole taktiikkaa. Ehkä tämä on verkkotaisteluiden historian sanoma, josta myös systeeminäkökulma kertoo.

"Tiedonhallinta päätöksenteossa kybertoimintaympäristössä" -artikkeli ”ilotulittaa” erilaisia malleja, jotka osoittavat kuinka monimutkaisessa toimintaympäristössä kybertaistelut tapahtuvat. Samalla artikkeli on erinomainen kattaus kybertoimintaympäristön teoreettisesta hahmottamisesta.

Huolimatta toimintaympäristön monimutkaisuudesta, Tuija Kuusisto kertoo selkeästi kuinka tiedonkeruu on entistä helpompaa. Tämä johtuu kybertoimintaympäristön robotisoitumisesta ja automatisoitumisesta. Ne luovat uusia mahdollisuuksia käyttää hyväksi erilaista massadataa kybervaikuttamisen alueella niin konflikteissa kuin rauhan aikana sekä niin yritystoimijoiden kuin kansallisten turvallisuustoimijoidenkin.

Puolustusvoimille oleellista on pohtia millaisilla organisaatiorakenteilla ja toimintaprosesseilla päästäisiin kybertoimintaympäristössä parhaisiin tuloksiin erityisesti johtamisen ja päätöksenteon alueilla. Yhdeksi teoreettiseksi ratkaisuksi on esitetty rihmastoteoriaa, jossa rinnakkainen tekeminen on nousemassa ratkaisuksi aikamme informaatiosotien sekametelisoppiin[15]. Kuusisto kiinnittää menetelmien tasolla huomiota muun muassa sisällönanalyysimenetelmien hyödyntämisen tärkeyteen. Bisnesmaailmassa niiden käyttö on arkipäivää. Liiketoimintamallit ovat yksi mahdollisuus tutkia kuinka pärjätä digitaalisessa maailmassa. Toisaalta esimerkiksi Amazon on osoittanut, että on parempi toimeenpanna liiketoimintamalli hyvin kuin ottaa tyhjästä otettu uusi malli. Amazonin esimerkki rohkaisee pohtimaan menestystekijöitä, mutta samalla asiakaslähtöisyyttä. Organisaatiorakenteiden ja toimintaprosessien tulisi Amazonin mallin mukaan lähteä ajatuksesta, jossa kaikki tehdään asiakkaan ehdoilla.

Mitä tämä sitten voisi tarkoittaa verkkotaisteluille ja kybertaktiikalle? Laadukas taktiikka perustuu tiedolle. Tiedonkeruun ja analyysin laajentaminen kybertoimintaympäristöön on tapahtunut mutta siihen liittyvien organisaatiorakenteiden ja prosessien kehittäminen on kesken. Tässä Kuusiston esiin nostamat mallit ja työkalut voisivat tuoda lisäarvoa. Samalla keskeiseksi kybertoimintaympäristön kysymykseksi on noussut sosiaalisen mediaympäristön analysoiminen. Tämä taas nostaa kysymyksen mikä on sosiaalisen median merkitys puolustusvoimille (sensori, toimintaympäristö, vaikuttamisen väline jne.) ja mitä se merkitsee kybertaisteluiden taktiikalle.

"Kybersodankäyntiä koskevan lainsäädännön tarkastelua" on hyvä osoitus kuinka uusi ilmiö voi sisältää vanhoja jo aiemmin koettuja asioita ja toimintoja. Keskustelu kyberoperaatioiden laillisista perusteista on tärkeä osa puolustuskyvyn kehittämistä.

[14] Ahvenainen, Sakari (2014). Kun hype riisutaan kyberistä saadaan kybernetiikka. Viestimies 3/2014, s.15 - 18.
[15] Huhtinen, Aki ja Rantapelkonen, Jari (2014). Rihmastoajattelu strategisena kommunikaationa. Teoksessa Rantapelkonen, Jari, toim. (2014). Helsinki, Maanpuolustuskorkeakoulu, s.126 - 134.

Tomi Hasu kiinnittää huomiota siihen, kuinka kybertoimintaympäristö on fyysisen maailman jatke. Suurvallat ovat ottaneet strategioihinsa oikeuden vastata kyberhyökkäyksiin kineettisin toimin. Tämä herättää pohtimaan kuinka puolustusvoimissa, yhteistyössä muiden toimijoiden kanssa, tulisi verkoissa operoida rauhan, kriisin ja konfliktin aikoina ja kuinka operoida strategisella, operatiivisella ja taktisella tasolla.

Lainsäädännön merkitys on keskeinen määrittämään sitä mikä kybertoimintaympäristössä on sallittua ja mikä ei. Lainsäädäntö luo rajat kybertoiminnalle. Hasu toteaa selvästi, että jo nykyisellään yleisesti pätevät sodankäynnin säännöt pätevät myös kybertoimintaympäristössä. Tässä mielessä suomalainen doktriini alueellisesta puolustuksesta näyttää esimerkillään kuinka maalla, merellä ja ilmassa voidaan harjoittaa tiedustelua sekä puolustaa ja hyökätä. Miksipä ei sitten ”touhuttaisi” jo täysillä kybertoimintaympäristössä sillä, kuten Hasu osuvasti kirjoittaa, kybertapahtumat eivät ole erillisiä, yleisen oikeuskäsityksen ulkopuolella olevaa toimintaa.

"Kybertaistelun teoreettinen tarkastelu" -artikkelissa pohditaan sodankäynnin trendejä ja niiden merkityksiä. Martti Lehto kirjoittaa kuinka kybersodankäynnistä puuttuvat rintamalinjat. Taistelemisen aika on kaventunut sekuntiluokkaan. Jos tämä pitää paikkaansa, voidaan hyvin todeta, että kysymys on vallankumouksellisesta sotataidollisesta muutoksesta. Kun kybertaisteluita voidaan käydä kaikkialla ja kun jokapäiväiset ”kyberhyökkäykset” saavat aikaan jatkuvan hälytystilan, voidaan todeta kuinka kybertaisteluista on tullut normaali olotila. Järjestelmille normaalista olotilasta on samalla pysyvä poikkeustila: Pysyvästä turvattomuudesta ei ole paluuta turvalliseen elämään, jossa elettäisiin ilman huolia. Aika pessimistinen näkymä.

Sotataidollisesti lähin esimerkki löytyy Israelista. Lähi-idässä on käyty sotaa, välillä enemmän ja välillä vähemmän intensiivisesti viimeiset vuosikymmenet aina valtion synnystä lähtien. Teoreettisesti ajateltuna keskittyminen sotimiseen vailla päämäärää on hyvän yhteiskunnallisen elämän kannalta tarkasteltuna epäsuotuisa ajatus, ainakin poliittisesti, onhan sota politiikan jatkamista toisin keinoin. Sodalla pyritään ratkaisemaan poliittisia ongelmia. Millaisia ongelmia kybersotimisella pyritään ratkaisemaan?

Kybersodankäynnin teoreettinen perusta ei ole irrallaan muusta sosiaalisesta todellisuudesta. Kybersodankäynti on liitoksissa myös maalla, merellä ja ilmassa, mutta myös ihmisen kognitiivisessa tietoisuudessa käytäviin kamppailuihin. Tässä mielessä Lehdon artikkeli antaa roimasti pohdittavaa sotatieteelliselle keskustelulle, mikä kybersodankäynnissä on uutta ja mikä vanhaa ja mikä niiden väliltä.

Toisaalta artikkelissa tarkastellaan kybersodankäyntiä nimenomaan jo tunnettujen sodankäyntimallien ja teorioiden kautta. Clausewitzilaisittain ajateltuna sodankäynnissä olevat piirteet muuttuvat teknologian muuttumisen myötä. Suuri kysymys on muuttuuko sodankäynnin luonne, kun sota ymmärretään väkivaltaisena toimena ja jossa ihmiset saatetaan hengenvaaraan, jopa kuolemaan. Jos kybertaistelut muuttavat tämän oletuksen, on kysymys uudenlaisesta toiminnasta. Näin kybertaktiikka saattaa tarvita uudenlaisia teorioita ja perusteita selittämään rintamalinjojen puutetta ja ikuisesti jatkuvia kybertaistelujen käytäntöjä. Artikkelissa kybertaistelut kuitenkin sijoitetaan jo olemassa oleviin teoreettisiin sotataidon kehityksiin. Tämä saattaa kertoa siitä, että joko kybertaisteluissa ei lopulta olekaan mitään uutta tai sitten emme ole vielä kyenneet vanhoilla teorioilla uudenlaista sodankäyntiä hahmottamaan.

"Miten tekisin kyberhyökkäyksen?", on Mika Hyytiäisen kirjoittama artikkeli, jossa kuvitellaan yksi tapa kuinka vieras valtio hyökkäisi Suomeen. Hyytiäisen mukaan eksoottisten verkkohyökkäysten arki ja aika on ohitse. Valtiot eivät käytä verkkohyökkäyksiä pelkästään painostamiseen. Ohjelmistojen kehittyminen on johtanut tilanteeseen, jossa kyberiä voidaan käyttää ”täsmäaseena”.

Täsmäasevertaus hieman yllättää, mutta on mielenkiintoinen. Kyberiä on pidetty – huolimatta Stuxnetin esimerkistä – yleisesti aseena, jonka vaikutusta ei voida ajoittaa eikä kohdistaa samalla tavalla kuin perinteisillä aseilla. Voidaan kysyä, onko kybertäsmäaseille edes tarvetta, jos vieras valtio päättää hyökätä suomalaista kriittistä infrastruktuuria, joka on jo rauhan aikana haavoittuvainen erilaisille häiriötekijöille, vastaan. Toisaalta laajemmin kybertoimintaympäristöä tarkasteltuna voidaan kysyä löytyykö kyberverkoista ja infrastruktuureista yhtä sellaista kohdetta ja maalia, joka lamauttaisi koko Suomen tietoliikenteen. Tätä pohdintaa on joka tapauksessa syytä jatkaa sillä se luo pohjaa kybertaktiikalle sekä operaatiotaidolle.

Toinen tekijä, joka tulee vaikuttamaan kybertaktiikkaan, on autonomisoituminen. Osa kyberhyökkäyksissä käytettävistä ”aseista” on jo itsenäisesti toimivia. Ja mikäli näitä ”aseita” on helppo valmistaa, kuten annetaan ymmärtää, niin olisiko pelottavin kansallista turvattomuutta aiheuttava skenaario sittenkin se, että kuka tahansa voi ulkoistaa kyberhyökkäykset ohjelmistoille ja koneille ilman tiivistä hyökkäyksiin osallisuutta. Mitä tämä merkitsee tulevaisuuden kyberhyökkäyksille?

Tämä ajatuspolku palauttaa Hyytiäisen kuvaaman valtiollisen toimijan tekemät hyökkäykset lähtöruutuun. Valtio ei tämän logiikan mukaan enää omista sotaa eikä kyberhyökkäyksiä. Kyberin kehitys on johtanut tilanteeseen, jossa valtion monopoli sodankävijänä on murrettu. Päätelmä on itse asiassa sama, johon jo yli kymmenen vuotta sitten *Verkkotaistelut 2020* -julkaisussa päädyttiin. Tämä panee kysymään onko ajattelu kyberistä kehittynyt vai onko se kulkemassa kehää tai palaamassa juurilleen hakkereiden asearsenaaliksi. Se kuka on kyberhyökkäysten takana todennäköisimmin ja mikä on se taho joka saa vakavinta tuhoa aikaan ovat kaksi eri kysymystä.

Todennäköisin kyberhyökkääjä saattaa olla ei-valtiollinen toimija. Valtiollisen toimijan taas voidaan ajatella saavan eniten Suomessa tuhoa aikaan. Toisaalta terroristi- tai aktivistijärjestöt saattavat saada aikaan yhtä pahaa jälkeä kuin valtiolliset toimijat. Tällöin Hyytiäisen kuvaama visio matalan tason kriisistä, jatkuvasta kybersodankäynnistä, saisi jo rauhan aikana yhtä vahvoja seurauksia aikaan kuin sota-aikana. Olipa toimija kuka tahansa, niin kyber hämärtää tässäkin perinteisen ajattelun, koska kybertoimintaympäristössä käydään tämän logiikan mukaan jatkuvaa sotaa. Sotilaallisesti tarkasteltuna tällainen skenaario lamauttaa etenkin uudet aseet ja sotilaalliset järjestelmät, sillä niissä on entistä enemmän mikropiirejä ja bittejä eivätkä suljetutkaan sotilaalliset tietojärjestelmät ole suojassa ulkopuolisilta vaikutuksilta monista keskinäisriippuvuuksista johtuen. Näin hyökkäys Suomi Oy:ta kohtaan ei jätä puolustusvoimien tiedustelun, valvonnan, johtamisen ja tulenkäytön järjestelmiä ja palveluita rauhaan. Sotilaallisesti kriittisiä järjestelmiä voidaan vahingoittaa pelkällä informaatiosodankäynnillä ja propagandalla, jolle kybertoimintaympäristö antaa uusia mahdollisuuksia.

Miten tällaista skenaariotta vastaan voidaan Suomelle ja sen puolustusvoimille rakentaa resilienssiä? Hyytiäisen kuvaamissa skenaarioista selviämiseksi resilienssi on ennen kaikkea asennetta eikä tekniikkaa. Kybertaktiikan kehittämiselle tämä antaa selvän suunnan: kybertaistelutekniikan ensisijaisuus tulee kyseenalaistaa, mutta ei unohtaa.

"Tietoverkkopuolustuksen haasteiden 2020 arvioiminen" -artikkelissa kuvataan kybertoimintaympäristössä vaikuttavia teknisiä haasteita. Jouko Vankan artikkeli yllättää siinä, että se ei yllätä. Tulevaisuuden puolustuksessa keskeisiä kriteereitä, joita artikkelissa käytetään arvioinnin tukena, ovat saatavuus, eheys ja luottamuksellisuus. Yllättävää kyllä, psykologiset tekijät on nostettu tekniikan artikkelissa kriteeriksi, joskin sitä valitettavasti ei kuitenkaan arvioida. Kybertaktiikan kannalta olisi tärkeää pohtia, mikä vaikutus henkiseen kriisinsietokykyyn vaikuttavilla tekijöillä on kybertaisteluille.

Vankan tavoitteena on testata voidaanko analyyttistä hierarkiaprosessia (AHP) käyttää päätöksentekomenetelmänä kybertoimintaympäristön kaltaisessa ympäristössä moniulotteisten ongelmien ratkaisemiseen tilanteissa, joissa on useita ristiriitaisia näkemyksiä. Artikkelissa arvioitiin pilvipalveluita, laitteistojen takaovia ja mobiililaitteita tulevaisuuden tietoverkkopuolustuksen haasteina. Artikkelissa päädytään arvioon, jonka mukaan luottamuksellisuus on tärkein kriteeri, ja saatavuus toiseksi tärkein. Luottamuksellisuus on ollut paljon esillä ns. Snowden tapauksen johdosta. Saatavuus on noussut tärkeäksi tekijäksi niin Viron kuin Georgian sodan yhteyksissä.

Artikkelissa ei ole tarkasteltu asiaa puolustusvoimien kannalta. Tosin kriteerit saattaisivat olla paljolti samansuuntaisia. Yksi peruste on se, että puolustusvoimien omien järjestelmien eristäminen internetistä tulee olemaan tulevaisuudessa haaste. Ulkopuoliset voivat päästä helpommin salassa pidettäviin tietoihin käsiksi. Kybertäsmäase-retoriikassa luottamuksellisuuden ongelma saattaakin olla huomattavasti suurempi sillä järjestelmät ja ohjelmistot päivittyvät lähes päivittäin – usein operatiivisen toimijan kannalta ulkopuolisten tahojen tekemien päivitysten vuoksi. Toisaalta kybertäsmäaseen käytön helppous on ongelmallista hyökkääjän kannalta. Puolustajana kannalta jatkuvat päivitykset saattavatkin olla hyvästä, vaikka käyttäjät saattavat ajatella toisin.

Eheyttä sen sijaan ei nähty tulevaisuuden uhkana. Tämä hieman yllättää, sillä aikamme sodat ovat osoittaneet, että käytettävissä olevien tietojen luotettavuus, ajantasaisuus ja oikeellisuus voidaan haastaa, ainakin julkisuudessa.

Suurimmaksi haasteeksi tulevaisuudessa nousi mobiililaitteet. Artikkelin lopussa jään hieman ihmettelemään päätelmää, jonka mukaan suurin heikkous on ihminen. Eikö tietoverkkopuolustuksessakin kehitys vie kohti yhä kyberisoituneempaa tulevaisuutta, jossa koneet ja ohjelmistot hoitavat yhä enemmän ihmisten ja sotilaiden puolesta kriittisiä prosesseja ja tiedonvirtaa. Eivätkö koneet ja ohjelmistot ole tällöin suurin ongelma. Onko kybersodankäynnin virallisella agenda asia, jonka mukaan ihminen pitäisi poistaa tietoverkkopuolustuksen kriittisistä solmuista. Mitä tämä tarkoittaa kybertaktiikan taitamiselle? Tätäkin tulisi tutkia lisää.

"Verkkotaistelu yritysten näkökulmasta" -artikkelissa valotetaan kybertaisteluiden kuvaa sotilaallista näkökulmaa laajemmin. Kari Wirman osoittaa kuinka kyberistä on tullut yrityksille uhkakuva, jota puntaroidaan riskin näkökulmasta. Yritykset ovat joutuneet mukaan verkkotaisteluiden maailmaan, jossa ei enää tarvita sotilaallisia uhkakuvia osoittamaan kuinka vakavasta uhasta on kysymys. Verkkouhista muodostuu yrityksille taloudellisia uhkia, joista taas voi muodostua uhkia kansalliselle turvallisuudelle.

Yksi mielenkiintoisimmista ajatuksista, joka Wirmanin artikkelista nousee pintaan, on riskinäkökulma. Taisteluiden näkeminen riskienhallinnan näkökulmasta haastaa sotataidollista ja taktiikan ajattelua. Riskinäkökulma on suhteellisen tuore näkökulman taisteluiden luonteen arviointiin. Kybertaisteluita ei käydä välttämättä taistelutahdosta, ideologisista, uskonnollisista tai fyysisiin resursseihin liittyvistä syistä vaan riskienhallinnan näkökulmasta. Yritystoiminnan digitalisoitumisessa ei ole kysymys pelkästään kaupankäynnistä ja brändistä vaan organisaation käyttäytymismallista ja sen muutoksesta.

Juuri tämä sama tuore näkökulma riskienhallinnasta antaa samalla mahdollisuuden kybertaistelukritiikille. Kyberistä tulee yritykselle riskitekijä, koska kyberin suomia ja luomia mahdollisia haavoittuvuuksia ei tunneta. Kyber on vienyt sodan verkkoon, verkko on tuonut sodan yrityksiin ja yritykset kybersotiin. Yritykselle on jäänyt jäljelle vain riskienhallinta, sillä hyökkääjällä on enemmän valtaa yrityksen puolustajiin nähden. Lähtökohta on tappiollinen, mutta ilmeisesti realistinen. Kybertoimintaympäristön merkitys näkyy yrityksissä asenteissa kohdata kyberhyökkäys.

Kybertaisteluiden kritiikki riskeistä panee pohtimaan, ratkeaisiko kirjoituksessa esiin nostettu kybertaisteluiden riskienhallinnan ongelma ajattelun tasolla eikä kyberteknologian tasolla. Tulevaisuus on ennustamaton ja odottamaton eikä niinkään lineaarisesti skenaarioitu, jolloin kaikkeen ei voi varautua ja tappioita syntyy. Onko niin, että yrityksissä hyväksytään lähtökohtaisesti tietty määrä tappioita? Riskinäkökulman mukaan toiminnassa otetaan riskejä koska aloite on hyökkääjällä eikä kyberhyökkäyksiä voi täysin hallita.

Riskienhallinnan näkökulmasta täydellistä kybertaktiikkaa ei ole eikä tule. Näin ollen myös riskienhallinnan näkökulma johtaa ajatteluun resilienssin kehittämisestä. Tämä taas voi johtaa kehittämään yritysten kykyä kokeilla ja verkottua. Kokeilukulttuurin kehittäminen on yrityksissä tärkeää varsinkin kun elämme ”Internet of things” -aikaa, jonka on sanottu olevan yhtä suuri disruptio kuin itse Internet Tämän vuoksi kybertaistelut tulisi nähdä laajemmassa kontekstissa kuin pelkästään riskienhallinnan kautta.[16]

"Maavoimat kybertaistelukentällä" -artikkeli osoittaa selkeästi kuinka riippuvaisia maavoimat on informaatioteknologiasta. Maavoimat keskittää arvokasta, jopa sen toiminnalle erittäin kriittistä tietoa pilveen. Pilvipalveluiden käytettävyydestä ei voi sodan aikana olla varma, koska pilvipalvelut eivät ole käyttäjänsä kontrollissa. Näin maavoimat on yhteiskunnan heijastuma palveluiden keskittämisessä.

[16] Coker, Christopher (2009). War in an Age of Risk. Cambridge: Polity Press.

Toisaalta maavoimat uudistaa taistelutapaansa hajauttamalla joukkoja. Akilleen kantapääksi voi muodostua taktisen johtamisjärjestelmän kyky palvella tilanteissa, joissa joko vihollisen asevaikutus tai kybervaikutus mukaan lukien elektroninen sodankäynti kohdistuu palveluiden kannalta maapuolustuksen kriittisiin kohteisiin.

Kirjoittajat huomauttavat, että johtamisjärjestelmien tärkeys nostaa kybersodankäynnin elementit uuteen asetelmaan. Tästä ”uudesta asetelmasta” ja palveluajattelun vaikutuksista viestitaktiikkaan olisi mielellään lukenut lisää, erityisesti siitä mitä se käytännössä merkitsee maavoimien taktiikalla. Toisaalta kirjoittajat toteavat – hieman ristiriitaisesti – monien tietoteknisten riippuvuuksien ja niiden lisääntymisen kuvaamisen jälkeen, että ”pidettäköön tietoverkkosodankäynti edelleenkin tukevassa roolissa, koska sillä ei tulla nyt, eikä myöskään näkyvässä olevassa tulevaisuudessa ratkaisemaan ainuttakaan sotaa”. Tosin esimerkiksi Ukrainan sodassa Krim vallattiin 2014 pelkällä informaatiolla ampumatta käytännössä laukaistakaan.

Maavoimissa kybersodankäynti konkretisoituu operaatioturvallisuudeksi. Teknisten järjestelmien tietoturvallisuus nousee tärkeään asemaan. Vaikka kirjoittajat eivät arvota maavoimissa olevien kriittisten tietojen eheyttä, käytettävyyttä ja luottamuksellisuutta, niin voisi kuvitella, että tiedon käytettävyys nousisi tärkeimpään asemaan maavoimien taisteluosastojen liikettä ja tulenkäyttöä. Tällä arvottamiselle saattaa olla vaikutuksia myös kybertaktiikan kehittämiselle.

Artikkeli kertoo yhdestä maapuolustuksen suorituskykyä koskevasta vakavasta oireesta. Kybertaistelukenttä nähdään maavoimissa vain puolustuksen kautta. Joko maavoimilla ei ole edes ajatusta nähdä kybertaistelukenttää vakavasti otettavana uhkana, maavoimilla ei ole tarkoitus käydä kyberhyökkäyksiin tai sitten kyberhyökkäyskyvyn käyttäminen on maavoimissa leimattu salaisten leimojen taakse. Kirjoittajat antavat yhden loogisen selityksen: maavoimissa kyber näyttäytyy omien järjestelmien suojaamisena ja tukitoimintana. Kyberillä ei ole maavoimissa muuta merkitystä. Artikkeli antaa kuvan, jonka mukaan Maavoimien johtamisjärjestelmä on sama kuin maavoimien kyberpuolustus.

Toisaalta Jukka-Pekka Virtanen ja Janne Jokinen kirjoittavat kuinka taktisen johtamisjärjestelmän palvelut nousevat osana maavoimien tiedustelua, liikettä ja tulenkäyttöä avainasemaan. Tällöin olisi hedelmällistä lukea pohdintaa palveluiden vaikutuksista taktiikkaan esimerkiksi siitä kuinka paljon palveluiden käytettävyyden puuttuminen on itse aiheutettua ja miten viholliselta estetään kyky vaikuttaa palveluihin. Entä ovatko maapuolustuksessa korostetut taktiset periaatteet päteviä myös maavoimien kybertaistelukentällä?

Tämä kertoo toisesta vakavasta oireesta, siitä, että kybertaistelukentällä ei ole maavoimissa taktiikkaa. Näyttää sille, että kybertaktiikka on vasta kehitteillä ja se näyttäytyy tänä päivänä johtamisjärjestelmätekniikkana, johtamisjärjestelmien suojaamisena ja johtamisjärjestelmien tuottamina palveluina. Johdannossa kirjoitetaankin kuinka kyberpuolustuksen tarkastelu tulisi ulottaa kyberin; verkkojen ja järjestelmien ulkopuolelle koulutukseen, ohjeistukseen, toimintatapojen kehittämiseen, johtamiseen ja yhteistoimintaan. Näiden aukaiseminen on tarpeen maavoimien kybertaistelukentän avaamiseksi. Sellainen saattaisi avartaa kokonaisvaltaisempaa kuvaa kybertaisteluista.

"Kybertaistelu ilmavoimaympäristössä" -artikkeli kertoo kybertaisteluiden evoluutionäärisestä luonteesta. Sodankäynnin käytännöt ovat muovanneet sotataidon teorioita. Martti Lehdon artikkelista huokuu näkemys kuinka maailmalla tapahtuva sotataidollinen kehitys vaikuttaa vahvasti myös Suomen ilmavoimien tapaan taistella.

Toisaalta artikkeli osoittaa kuinka kyber koetaan erilliseksi, hieman kaukaiseksi asiaksi. Lehto kuitenkin kirjoittaa kuinka ”kybersodankäynnissä kyberoperaatiot eivät ole kokonaan itsenäisiä, muusta sodankäynnistä erillään olevia operaatioita, vaan kiinteä osa kokonaisoperaatioita.” Myös ilmavoimissa kyberiin liittyvät määritelmät ja suorituskyvyn kehittäminen sekä kybertaisteluiden mallit ovat vasta alkutekijöissään. Sen sijaan ilmavoimissa elektronisella sodankäynnillä on pitkät perinteet. Voidaankin kysyä onko elektromagneettisen spektrin hallinta myös tulevaisuudessa ensisijainen toimintaympäristö kyberiin nähden sillä ilmapuolustuksessa kyber koetaan lähinnä puolustuksellisena kybersuojaamisena.

Toisaalta Lehto näkee kuinka kyberteknologialla, uusilla laitteilla ja palveluinnovaatioilla voidaan luoda ilmasodankäynnin tulevaisuutta jopa ”transformaatiohypyin”. Aika näyttää voidaanko kyberillä tai kyberohjelmilla ja kyberroboteilla tuottaa uudenlaista strategista tilaa, jossa ilmasota voitetaan tai hävitään, kuten Lehto pohtii. Tämä panee kysymään onko sotilaskulttuurissa valmiutta hypätä teknologiapolven yli. Eivaltiollisilla toimijoilla on tällaista valmiutta, mutta onko valtiollisilla toimijoilla. Tämä panee kysymään onko ilmavoimat evolutiivisen kehityksen vanki. Tällöin teknologiassa ei voi hypätä tulevan teknologian yli esimerkiksi odottamalla 10 vuotta tai ei voida myöskään mennä taaksepäin sukupolvella, koska on elettävä evoluution mukana.

Ilmavoimien kybertaistelu artikkelissa esitellään erittäin mielenkiintoinen taulukko, jossa kerrotaan kuinka paljon hävittäjän suorituskyvystä on kyberin varassa ja kuinka paljon se on lisääntynyt. Lehto havahduttaa lukijansa kuinka ”nykyisin vähintään 75 prosenttia hävittäjän suorituskyvystä perustuu ohjelmistoihin ja tietotekniikkaan”. Mitä kehittyneempi hävittäjä sitä enemmän hävittäjän riippuvuus kasvaa ohjelmistoista ja tietojärjestelmistä. Tämän mukaan ilmavoimien taisteluiden menestys perustuu entistä enemmän kyberteknologiaan, jossa haavoittuvuuksien hyväksikäyttäminen on vakavasti otettava uhka. Tämä saattaa selittää sen, miksi ilmavoimissa kyber koetaan ennen kaikkea puolustuksellisena asiana, kybersuojaamisena.

Toisaalta jos ilmavoimien kybertaisteluissa jo lähtökohtaisesti ”jumiudutaan” vain puolustamiseen, niin voidaan kysyä sotataidon historian perusteella, mitkä ovat onnistumisen mahdollisuudet menestyä – varsinkin kun hävittäjien toiminta ei perustu suljettuun systeemiin sillä ilmaoperaatioiden aikana voidaan tietojärjestelmiä päivittää.

Ehkä suurin kyberympäristöön liittyvä operaatiotaidollinen puute ei olekaan se kuinka riippuvaisia ilmavoimissa ollaan kyberistä tai kuinka puolustuksellisia ilmavoimat ovat vaan se kuinka ei-kineettisissä operaatioissa hallitaan aikaa. Ajanhallinta koskettaa ennen kaikkea kysymystä kognitiivisen dimension ymmärtämisestä. Se määrittää kuinka ilmavoimien kybertaistelukyvystä voitaisiin kehittää kokonaisvaltainen taistelukyky. Näin ilmavoimien kybertaistelulle annettaisiin mahdollisuus kehittyä teknologian tasolta aivan uudelle tasolle; kybertaktiikan tasolle.

10.6 Päätelmiä ongelmista ja niiden ratkaisuista

Kirja verkkotaisteluista on tervetullut nostamaan keskustelua kybertaisteluiden kehittämisestä sekä niiden roolista Puolustusvoimien sodan ajan toiminnassa. Kirjan johdannon päätelmissä todetaan selvästi, kuinka kybertoimintaympäristö on yhä merkittävämpi osa muuttuvaa sodankäyntiä, ja sodankäynnin perusteista halutaan käydä perusteellista keskustelua.

Kirjan artikkeleista, kun niitä vertaa vuonna 2003 julkaistuun *Verkkotaistelu 2020* -kirjaan, voidaan päätellä, että kyber on kehittynyt teknologisesti uudelle tasolle. Voidaan myös väittää, että kyberin teoreettinen perusta lepää teknologian varassa. Teknologia ei sotahistorian perspektiivistä ole kuitenkaan ratkaissut sotia, harvoin myöskään taisteluita.

Vuoden 2003 julkaisussa peräänkuulutettiin verkkotaisteluiden taktiikan kehittämistä. Tämä kuulutus on osoittanut yltiöoptimistiseksi harhaksi. Kybertaisteluille ei ole onnistuttu kehittämään kymmenessä vuodessa taktiikkaa puhumattakaan operaatiotaitoa. ”Kybertaistelut” ovat hyvin tekninen, osin myös taistelutekninen asia. Tämä on sikäli erikoista, että tämän kirjan kirjoittajat toteavat lähes yksissä tuumin, kuinka riippuvaisia aikamme asevoimat ovat teknologiasta. Tällaisiin teknoriippuvuuden tuottamiin haavoittuvuuksien ongelmiin ei kuitenkaan löydetä ratkaisua. Teknologisen ongelman ratkaiseminen lisäämällä kyberteknologiaa näyttää väistämättömälle suunnalle. Toisaalta ratkaisu kyberongelmiin voisi löytyä toimintatapojen muuttamisesta uudenlaisten digitaalisen ajan liiketalousmallien esimerkkien mukaisesti. Sotilaskielellä se tarkoittaa taktiikan kehittämistä, kybertaktiikan. Kybertaisteluiden taktiikkaan ei ole saatu vielä kokonaisvaltaista otetta, ei kunnolla edes ajatuksen tasolla.

Kehittyneestä taktiikasta, esimerkiksi kybertaktiikasta voidaan puhua vasta silloin, kun kybertaisteluiden käymiseksi on selvillä yleiset kybertaisteluiden periaatteet, kyberjoukoilla on hyväksytyt käyttöperiaatteet ja kybertaisteluiden käymiseksi on kirjoitettu ohjesääntö. Taktiikan kehittäminen edellyttää, että kybertaisteluiden käymisestä keskustellaan ja kirjoitetaan sotatieteellisessä yhteisössä, johon tämäkin kirja pyrkii.

Mikäli kyber ei ole luonnollinen osa taistelusuunnitelmia eikä sitä systemaattisesti kouluteta sodan ajan johtajille ja joukoille, ei voi puhua kybertaktiikasta. Kun kyber leimautuu yleiseksi filosofiseksi keskusteluksi ilman käytäntöjä, jäävät kybertaistelut teknohakkereiden bittipuuhasteluksi, yksittäisiksi haittaohjelmiksi, mediaseksikkääksi aiheeksi tai puolihalvaantuneiden (puolustus ilman hyökkäyskykyä) ja sokeiden (tiedustelu ilman kaukonäkökykyä) rampojen suojautumispuuhasteluksi. Sellainen ei edistä todellisen taktiikan kehittämistä.

Todellinen kybertaktiikka pohtii, mistä taistellaan, milloin taistellaan, miten taistellaan sekä mistä taistelut aloitetaan ja missä ratkaisutaisteluita käydään. Kybertaktiikan kehittäminen vaatii taktisten ajatusten ja taktisten periaatteiden kehittämistä, taistelusuunnitelmia sekä taktisten periaatteiden soveltamisen taitoa. Kyberiltä puuttuu taktiikan opetus. Opetuksessa voitaisiin käyttää tunnettuja taisteluita mallia Tolvajärven taistelut tai Normandian maihinnousuoperaatio. Stuxnet ei täytä näitä vaatimuksia.

Kybertaistelutaktiikan kehittämisen ongelma voidaan ratkaista kahdella tavalla:

1. Luodaan kybertaistelutaktiikan perusteet.
2. Todetaan kyber taistelutekniseksi tai toimintaa tukevaksi tekijäksi, eikä haihatella taktiikan kehittämisen perään.

Kybertaktiikkaa voidaan kehittää hankkimalla omia kokemuksia sekä oppimalla muiden kokemuksista, kuten taisteluteknisellä tasolla on jo harjoiteltukin. Näistä voidaan jalkauttaa kybertaktiikkaa. Kybertaistelutaktiikan luominen edellyttää taktisten periaatteiden tutkimusta opetuksen tueksi. Hieman on Suomessakin jo pohdittu, säilyvätkö taktiset periaatteet, kuten aktiivisuus, harhauttaminen[17] tai menestyksen hyväksikäyttö kybertaisteluita ohjaavina tekijöinä[18]. Synnyttääkö kyber uusia taktisia periaatteita, tai painotetaanko kybertaktiikassa sotahistoriassa tuttuja periaatteita jollain tavalla? Samalla on pohdittava, millaisia kyberiin liittyviä taktisia käyttöperiaatteita ja keinoja on mahdollista informaatioympäristössä sekä maalla, merellä ja ilmassa käyttää.

Toinen ratkaisu kybertaktiikan kehittymättömyyteen on lopettaa haikailu pääsystä taktiikan kineettiseen ytimeen. Todetaan, että kyber tukee kaikkea toimintaa maalla, merellä ja ilmassa. Kyber on korkeintaan taistelutekninen asia, josta ei kehitetäkään kybertaktiikkaa sen teknisestä luonteen takia. Kyber voisi ytimetisoitua näin menneeseen, tietoturvallisuuteen.

Vaihtoehto yksi tuntuisi kuitenkin houkuttelevimmalta. Se voitaisiin analogisesti rinnastaa maavoimien aselajien taktiikoihin, sillä esimerkiksi tykistöllä on tykistötaktiikka, viestillä viestitaktiikka ja huollolla huoltotaktiikka. Suunnitelmallinen ja menestyksellinen toiminta kyberympäristössä ei onnistu pelkästään juoksemalla kilpaa teknologian kanssa, sillä puolustaja on aina reagoivassa moodissa hyökkääjään nähden. Suunnitelmallinen toiminta kyberympäristössä vaatii kybertaktiikan kehittämistä.

Kyber näyttäytyy kuitenkin lähitulevaisuudessakin taistelutekniikalle. Teknologian nopea kehitys sekä sotataidon kineettisyyden kulttuuri tukevat tätä päätelmää. Se mikä voi muuttaa ajatusta kybertaistelutaktiikan kehittämiseksi, on kulttuurimuutos, jossa informaatiolla on merkitystä taisteluille. Esineiden internet on osiltaan jo läsnä, ja se on suuri asiakokonaisuus, joka muuttaa sodankäyntiä ja sotataitoa 2020-luvulla. Esineiden internetin merkitys johtamiselle, tulenkäytölle ja logistiikalle on kysymys, jota ei saa unohtaa ja jota kannattaa tutkia myös kyberin näkökulmasta. Tällainen fyysisen ja virtuaalisen ympäristön yhteen kietoutuminen pakottaa pohtimaan kybertaisteluiden mahdollisuuksia ja merkityksiä Puolustusvoimien sodan ajan toiminnalle.

[17] Miettinen, Eero & Pakarinen, Markku (2001). Harhauttaminen tietoverkoissa. Viestimies 2/2001.
[18] Palm, Veiko; Salin, Kari; Kuusisto, Rauno & Huttunen, Mika (2005). The Principles of War in the Information Age. Teoksessa Kuusisto, Rauno & Rantapelkonen, Jari (2005). Struggling to Understand Information war. Department of Leadership and Management Studies & Department of Tactics and Operations Art. National Defence University, Helsinki, s. 181 - 199.

Todellista operaatiotaitoa on kyky yhdistää toiminta eri ympäristöissä maalla, merellä, ilmassa ja kybertoimintaympäristössä tai kuten Tuija Kuusisto kirjoittaa johdannossa kybertaktiikka, joka näyttäytyy kybertaisteluina ”kolmessa kybertoimintaympäristön kerroksessa eli fyysisessä, loogisessa ja sosiaalisessa kerroksessa”. Tämä edellyttää sellaisen tulevaisuuden kybertaktiikan kehittämistä, jossa ihmisiä on entistä vähemmän ja automatisoituja koneita ja ohjelmistoja enemmän. Se panee kysymään, voidaanko kybertaisteluita nähdä tai voidaanko kybersodankäynnistä saada ennakkovaroitus.[19]

Teknologinen kehitys joka tapauksessa tulee olemaan yksi keskeinen kybertaisteluiden määrittäjä. Kyberoperaatioiden rajaamisesta ja samalla luonteen muutoksesta kertoo hyvin John Arquilla, joka lanseerasi kybersota (cyberwar) termin vuonna 1993. Hän kuvaa kybersodankäynnin kehityksen seuraavaa askelta: lennokit ovat jo lentäneet merivoimien testeissä tietokoneidensa turvin. Tämä tarkoittaa sitä, että koneet päättävät itsenäisesti, milloin ne ampuvat ja milloin eivät[20]. Arquillan mukaan tästä on useita etuja: suurempi kyky kestää G-voimia, ja taisteluissa ei tarvitse huomioida esimerkiksi sellaisia vaaroja, joissa jouduttaisiin arvioimaan omien tappioiden vaikutuksia tai kohtaamaan tilanteita, joissa ihminen väsyy ja tekee virheitä.[21]

Samalla tulevaisuuden teknologia ja sen käyttäjät tulevat määrittämään, mikä on kyberin asema ja paikka osana sotataitoa, operaatiotaitoa ja taktiikkaa. Ihmisten osaaminen on kybertaisteluissa, ainakin vielä lähitulevaisuudessa, tärkein kyky[22]. Lienee selvää, että pelkällä taistelutekniikalla ei kybertaisteluiden melskeessä pitkälle pötkitä – eikä myöskään pelkällä strategialla. Kyberin hämärä kertoo tämän kirjan valossa siitä, että on ratkaistava perusongelma, mihin kyber asemoituu osana sotilaallista toimintaa, ytimeen operatiiviseksi kyvyksi, reunalle tukitoiminnoksi vai sodankäynnin alustaksi teknologiseksi asiaksi. Ainakin kahdessa ensimmäisessä vaihtoehdossa on tilausta kehittää suomalaista kybertaktiikkaa ja jälkimmäisessä kyber tulee ottaa taktiikassa huomioon.

[19] Rantapelkonen, Jari (2014). Kansallinen turvallisuus kohtaa kybertrendit – haasteista tänään ja huomenna. Futura 2/2014, s. 49 - 57.
[20] Arquilla (2012). Cyberwar Is Already Upon Us. Foreign Policy, Mar/Apr 2012, issue 192, s.1 - 4.
[21] Cooper, Elise (2012). The Future and Fears of Cyber-Warfare. American Thinker, March 31, 2012. See http://www.americanthinker.com/2012/03/the_future_and_fears_of_cyber-warfare.html.
[22] Moshkovitz, Uzi (2014). Yesterday IDF Thwarted Cyber Attack; Today IDF General Speaks About Future of Cyber Warfare. Ks. http://www.idfblog.com/blog/2014/04/08/future-cyber-warfare-speech-head-idf-telecommunications-branch/

Maanpuolustuskorkeakoulu
Taktiikan laitos
PL 7, 00861 HELSINKI
Suomi ▸ Finland

Puh. +358 0299 800
www.mpkk.fi

ISBN 978-951-25-2618-5 (PDF)
ISSN 1238-2752