Heidi Puttonen

INFORMAATIO-OPERAATIOT JA NIIDEN KESKEISET VAIKUTUSMENETELMÄT

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

TIIVISTELMÄ

Puttonen, Heidi
Informaatio-operaatiot ja niiden vaikutusmenetelmät
Jyväskylä: Jyväskylän yliopisto, 2015, 34 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaajat: Seppänen, Ville ja Moilanen, Panu

Tutkielmassa määritellään, mitä informaatio-operaatioilla tarkoitetaan ja esitellään niiden keskeisiä vaikutusmenetelmiä. Lisäksi vaikutusmenetelmien aiheuttamaa informaatiovaikutusten kohdentumista tarkastellaan organisaation kokonaisarkkitehtuurin näkökulmasta. Informaatio-operaatiot ovat sotilaallista toimintaa, jonka kohteena on informaatio. Ne ovat osa nykyaikaista sodankäyntiä ja niiden avulla pyritään vaikuttamaan vastustajan toimintaan, tilannetietoisuuteen ja päätöksentekoon. Informaatio-operaatiot ovat monipuolinen menetelmäkokonaisuus ja tutkielmassa tarkastellaan tarkemmin viittä keskeistä vaikutusmenetelmää: elektroninen sodankäynti, tietoverkko-operaatiot, psykologiset operaatiot, operaatio turvallisuus ja sotilaallinen harhauttaminen. Kokonaisarkkitehtuurin näkökulmasta informaatio-operaatiot vaikuttavat monipuolisesti organisaation jokaisella tasolla.

Asiasanat: informaatio-operaatiot, informaatiosodankäynti, informaatioympäristö, kokonaisarkkitehtuuri

ABSTRACT

Puttonen, Heidi
Information operations and their methods
Jyväskylä: University of Jyväskylä, 2015, 34 p.
Information Systems, Bachelor's thesis
Supervisors: Seppänen, Ville and Moilanen, Panu

This Bachelor's thesis defines what information operations are and presents their essential methods. The allocation of effects caused by these methods is examined from the enterprise architecture point of view. Information operations are military activities which are focused on the information. They are part of modern warfare and they aim at influencing adversary's activities, situation awareness and decision-making. Information operations are a diverse set of methods and the thesis focuses in detail to five key methods: electronic warfare, computer network operations, psychological operations, operation security and military deception. From the perspective of enterprise architecture information operations affect to every level of an organization.

Keywords: Information operations, information warfare, information environment, enterprise architecture

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Informaation merkitys menestyksekkäässä sodankäynnissä ei ole uusi ilmiö. Sen avulla Napoleon pystyi toteuttamaan harhautuksensa Austerlitzin taistelussa ja kukistamaan venäläis-itävaltalaisenarmeijan vuonna 1805. Sen avulla liittoutuneet onnistuivat harhauttamaan saksalaisia Normandian maihinnousussa 1944 ja salaamaan tarkan maihinnousualueensa. Persianlahden sodassa 1991 taas informaatio tulvi televisioruuduista tavallisten ihmisten koteihin ja sitä hyödynnettiin yleisen mielipiteen muovaamisessa. (Järvinen, Mäntylä, Tainiola, Viinamäki & Wahlstein, 2011, 113 – 117). Oikea ja oikea-aikainen informaatio on osaltaan määrittänyt sotien lopputuloksia niin kauan kuin sotia on käyty.

Nykypäivän tietokoneiden ja internetin luomassa digitalisoituneessa yhteiskunnassa informaation merkitys on entistä korostuneempaa - informaatiota on joka puolella ja koko ajan enemmän. Jo 2000-luvun alussa uutta dataa tuotettiin maailmanlaajuisesti n. 10^{18}-10^{19} tavua vuodessa ja määrä on kasvanut koko ajan (Veijalainen ym., 2008, 540). Toisaalta taas datamäärä joka on tuotettu ihmiskunnan alkuajoista vuoteen 2003 asti, vastaa nyt määrä joka tuotetaan joka toinen päivä (Lehto, 2014a, 73). Tämä on johtanut uudenlaisen sodankuvan syntymiseen, jossa informaatioteknologian ja erilaisten järjestelmien muodostama kybermaailma on noussut yhdeksi sodankäynnin ulottuvuudeksi (Kuusisto, 2014, 38).

Informaatio-operaatiot ovat menetelmäkokonaisuus, jossa informaatio valjastetaan sodankäynnin tarpeisiin. Informaatio on niissä toisaalta operaatioiden kohde ja toisaalta vaikutusväline. Informaatio-operaatioilla luodaan informaatiovaikutus, jonka avulla pyritään vaikuttamaan vastustajan toimintaan itselle edullisella tavalla. Informaatio-operaatioissa korostuu niin kutsuttu pehmeä vaikuttaminen, mutta niitä voidaan käyttää myös perinteisempien sodankäynnin muotojen tukemisessa ja niiden vaikutusten tehostamisessa. Huolimatta informaatiovaikutusten pitkästä historiasta yhtenä sodankäynnin voiton avaimista, on varsinaisesta informaatiosodankäynnistä alettu puhua vasta 1980-luvulla. (Lehto, 2014b).

Teknologian nopea kehitys on antanut aivan uudenlaisia mahdollisuuksia informaation hyödyntämiseen kaikilla elämämme osa-alueilla, myös sodankäynnissä. Yhteiskuntiemme kriittinen infrastruktuuri nojaa pitkälti informaatioteknologian ratkaisuihin. Toisaalta monet meistä kantavat taskussaan laitetta, jossa on enemmän laskentatehoa kuin Nasalla kokonaisuudessaan vuonna 1969 (Kaku, 2011). On siis selvää, että kybermaailmassa tapahtuva informaatiovaikutus on sodankäynnille suuri mahdollisuus ja myös vakavasti otettava uhka. Nykyajan verkottuneen maailman epäsymmetrisiä taisteluita käydään yhä vähenevässä määrin juoksuhaudoissa. Informaatio-operaatioiden keinoin voidaan vaikutus ulottaa paljon laajemmalle ja paljon nopeammin kuin konekiväärillä on koskaan pystytty. (Huhtinen & Rantapelkonen, 2001).

2000-luvulla on alettu puhua kybersodankäynnistä, jossa informaatiokeskeisyyden rinnalle on nostettu myös kyberavaruuden rakenteet, esimerkiksi kriittinen infrastruktuuri ja sodankäynnin johtamisprosessit. Tämä sodankäynnin malli limittyy tiiviisti informaatiosodankäynnin maailmaan ja on joissain yhteyksissä jopa hieman korvannut informaatiosodankäynnin käsitettä. (Lehto, 2014b, 158 - 164). Ukrainan kriisi (2014) on kuitenkin hyvä osoitus siitä, että informaatio-operaatiot ovat edelleen tärkeä osa sodankäyntiä ja ne elävät kyberajattelun rinnalla. Kriisin yhteydessä suomalaisillekin nettipalstoille ja lukijakommentteihin ilmestyi kirjoituksia, joiden tarkoitus oli levittää huhuja ja luoda mielikuvaa Suomen kansan ja päättäjien mielipide-eroista (Korhonen, 2014). Sosiaalinen media ja sen merkityksen kasvu ovatkin tarjonneet uudenlaisia keinoja vaikuttaa valtioiden välisissä konflikteissa. Sosiaalisen median välityksellä toteutetuilla informaatio-operaatioilla voidaan vaikuttaa laajasti käsitykseen siitä kuka on oikeassa. Näin pystytään heikentämään vastustajan päätöksentekijöiden ja kansalaisten välistä suhdetta.

Nykypäivän taistelukenttä on laajentunut taistelutilaksi, jossa joukot ja sotilaat ovat tulleet riippuvaisiksi informaatiosta ja sähköisestä tiedonsiirrosta. Informaatiota on paljon ja sitä on yhä helpommin saatavilla. Tämä kaikki on nostanut Informaatiosodankäynnin ja informaatio-operaatiot nykyajan konflikteissa sodankäynnin keskiöön. (Lehto, 2014b, 161; Rantapelkonen, 2014).

Tutkielmassa selvitetään kirjallisuuden perusteella, mitä informaatio-operaatiot ovat ja eritellään niiden keskeisiä vaikutusmenetelmiä. Lisäksi selvitetään näiden menetelmien aikaansaaman informaatiovaikutuksen kohdentuminen organisaation kokonaisarkkitehtuurin näkökulmasta.

Tutkimuskysymyksiä ovat:

- Mitä ovat informaatio-operaatiot?
- Mitkä ovat informaatio-operaatioiden keskeiset vaikutusmenetelmät?
- Miten menetelmien vaikutus kohdistuu organisaation kokonaisarkkitehtuurin näkökulmasta?

Tutkielman toisessa luvussa esitellään informaatio-operaatioiden taustaa ja niiden suhdetta muuhun sodankäyntiin. Lisäksi käsitellään informaation

merkitystä sodankäynnissä, informaatioympäristön rakennetta ja informaatio-operaatioiden tavoitteita. Kolmannessa luvussa tutustutaan informaatio-operaatioiden vaikutusmenetelmiin. Tarkempaan käsittelyyn on valittu viisi keskeistä vaikutusmenetelmää. Lopuksi luvussa havainnollistetaan näiden viiden menetelmän vaikutusten kohdentumista organisaation kokonaisarkkitehtuuri näkökulman avulla. Neljännessä luvussa ovat tutkielman johtopäätökset ja jatkotutkimusaiheita.

2 INFORMAATIO-OPERAATIOT

Informaatio-operaation määritelmässä on jonkin verran vivahde-eroja riippuen määrittelevästä organisaatiosta. Tässä tutkielmassa käytetään Naton ja Yhdysvaltojen armeijan määritelmiä, jotka vastaavat pitkälti myös suomalaista näkemystä. Edellä mainittujen organisaatioiden mukaan informaatio-operaatiot ovat informaatioympäristöön liittyviä sotilaallisia toimenpiteitä, joilla pyritään vaikuttamaan vastustajan, potentiaalisen vastustajan tai muun kohdeyleisön tahtoon, tilannetietoisuuteen ja toimintakykyyn. Lisäksi informaatio-operaatioihin kuuluu oman toiminnan suojaaminen vastustajan vastaavalta toiminnalta. (NATO, 2009; U.S. Army War College, 2011).

Ajattelun keskiössä on informaatio, jolla tarkoitetaan missä muodossa ja järjestelmässä tahansa olevaa datakertymää (Lehto, 2014a, 74). Informaatiovaikutus toteutetaan esimerkiksi tätä datakertymää manipuloimalla. Sotilaallisena toimintana informaatio-operaatiot vaativat useiden puolustushaarojen yhteistyötä. Ne ovat kokoelma erilaisia menetelmiä, joiden avulla haluttu informaatiovaikutus pyritään saavuttamaan. Erilaisia menetelmiä ovat esimerkiksi elektroninen sodankäynti, psykologinen vaikuttaminen, harhauttaminen, tietoverkko-operaatiot sekä julkis- ja siviilisuhteiden hallinta. (NATO, 2009; U.S. Army War College, 2011; Kangasmaa, 2014).

Informaatio-operaatioissa korostetaan pehmeitä vaikutuskeinoja (Siren, Huhtinen & Toivettula, 2011). Pehmeillä vaikutuskeinoilla tarkoitetaan eikineettistä vaikuttamista. Kineettinen vaikuttaminen taas tarkoittaa suoraa aseellista vaikuttamista kohteeseen. (Puolustusvoimat, 2012). Pehmeiden menetelmien korostaminen ei välttämättä täysin poissulje kineettistä vaikuttamista. Erityisesti Yhdysvallat ja Venäjä näkevät aseellisen vaikuttamisen osaksi informaatio-operaatioita (U.S. Army War College, 2011; Rantapelkonen, 2014). Usein kuitenkin ajatellaan, että informaatio-operaatioilla keskitytään pääasiassa tukemaan aseellista vaikuttamista ja päinvastoin (Sirén ym., 2011).

Kineettisen vaikuttamisen roolin suhteen kyse on näkökulmasta ja siitä, mihin rajanveto tehdään. Määritelläänkö esimerkiksi fyysiset iskut jotain tietojärjestelmää kohtaan informaatio-operaatioiden piiriin vai ei? Voivathan tällaisien iskujen informaatiovaikutukset olla hyvinkin laajoja: Kohdistettuina tie-

donsiirron solmukohtiin fyysisillä iskuilla voidaan aiheuttaa dramaattisia vaikutuksia vastustajan toimintaan. (Heikkala ym., 2011, 135). Oli näkökulma mikä hyvänsä, on syytä huomioida, että niin kineettisien kuin ei-kineettisien menetelmien käytöllä on aina informaatiovaikutus, joka on syytä ottaa huomioon informaatio-operaatioita suunniteltaessa (Jantunen, 2014).

Informaatio-operaatioiden synty alkoi 1970-luvulta, jolloin informaation ja johtamissodankäynnin merkitys kasvoi, sodankäynnin vaatiessa yhä monipuolisempia valmiuksia. Tällöin ajatuksena oli, että taistelukentän epävarmuus johtui puutteellisesta informaatiosta, jolloin informaation rooli korostui vallankäytön välineenä ja sen ymmärrettiin vaikuttavan koko konfliktin elinkaareen. (U. S. Army War College, 2011; Lehto, 2014b, 160). Varsinaisesta informaatiosodasta alettiin puhua 1980-luvulla (Lehto, 2014b).

Kylmä sota oli merkittävä ajanjakso, jossa informaatio-operaatiot näyttelivät ratkaisevaa osaa. Se oli ensimmäinen konflikti, jossa informaatiosodankäynnin doktriinia toteutettiin. Sotaa käytiin voimakaan psykologisen vaikuttamisen keinoin mannerten välisten ohjusten osumatarkkuuksilla ja ydinsodan uhalla. Kylmä sota on myös tärkeä osoitus informaatio-operaatioiden tehokkuudesta, sillä se on konflikti, joka ratkaistiin ilman aseellista taistelua. (Ahvenainen, 2014, 21–24; Rantapelkonen, 2014). Muita ensimmäisiä esimerkkejä nykymuotoisesta ja tietoisesta informaatio-operaatioiden käytöstä löytyy Persianlahden sodasta (1991) ja Kosovon sodasta (1998 – 1999). Persianlahden sotaa on usein nimitetty ensimmäiseksi informaatiosodaksi, vaikka se ajallisesti tapahtui Kylmän sodan jälkeen. (Huhtinen & Rantapelkonen, 2001).

Tultaessa 1990-luvulle informaation lisäksi alettiin korostaa sodankäynnin verkostomaista olemusta. Verkostokeskeisessä sodankäynnissä pyritään suorituskyvyn lisäämiseen yhdistämällä sensorien, päätöksentekijöiden ja aselavettien muodostama verkosto. Verkostoajattelun kehitys 2000-luvulla johti kybersodankäynnin syntymiseen. Kybersodankäynnissä sodankäynnin perinteisten ulottuvuuksien (maa, meri, ilma ja avaruus) lisäksi nähdään kyberulottuvuus, jossa toimijoiden tieto- ja informaatioperusteiset järjestelmät ja rakenteet sijaitsevat. Kybersodassa operaatiot tapahtuvat tässä kyberulottuudessa. (Kuusisto, 2014, 38; Lehto, 2014b, 162 – 165).

Vaikka sodankäynnin muutoksia ja tyylejä voidaan kategorioida eri nimitysten alle, eivät rajaukset kuitenkaan ole toisiaan poissulkevia ja eri sodankäynnin tyypit tarkastelevat samoja asioita usein vain erilaisista näkökulmista. Esimerkiksi informaatiosodankäynnissä keskiössä on informaatio, kun taas kybersodankäynnissä tarkastelunäkökulma on laajemmin koko kyberulottuvuudessa. Yksittäisen sodankäynnin menetelmän sijoittaminen yksiselitteisesti vain yhden yläkäsitteen alle on vaikeaa, ellei mahdotonta. Esimerkiksi elektroninen sodankäynti nähdään toisaalta osaksi menetelmäjoukkoa ja toisaalta se on yksi kybersodankäynnin osa-alueista. Toisissa yhteyksissä elektroninen sodankäynti on oma laajempi kokonaisuutensa. Monet sotilaalliset analyysit toteavatkin, että tulevaisuuden konfliktien sotilaallisten menetelmien yksiselitteinen tyypittely on vaikeaa. Viimeaikoina onkin alettu puhua hybridisodankäynnistä, joka yhdistää nykypäivän sodankäynnin monimuotoiset vaikutuskeinot - toteutuivat

ne sitten luodeilla tai biteillä, todellisella taistelukentällä tai ihmismielissä. (Hoffman, 2007, 35; Lehto, 2014b)

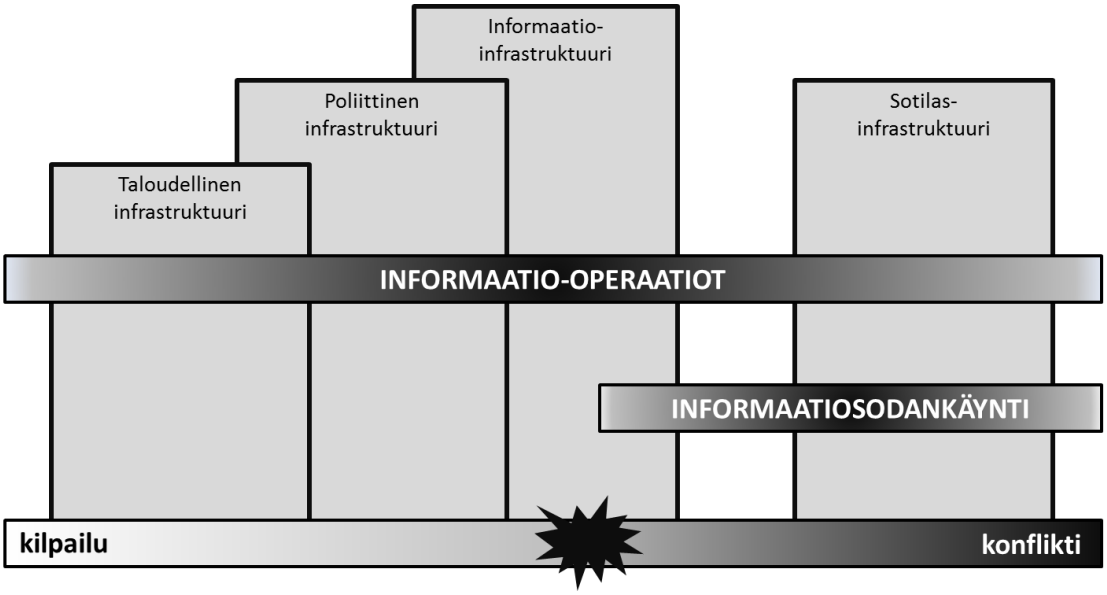
2.1 Informaatio-operaatiota vai informaatiosodankäyntiä?

Informaatio-operaatio termi esiintyi ensimmäisen kerran 1990-luvun puolessa välissä, kun siitä tuli korvaava termi sotilaalliselle informaatiosodankäynnille erityisesti Yhdysvaltojen ja Naton doktriineissa (Sirén, 2011, 204). Näiden termien suhde on edelleen erittäin läheinen. Monissa yhteyksissä puhutaankin pelkästään informaatiosodankäynnistä, eivätkä informaatio-operaatiot ole vielä juurtuneet puhekieleen. (Armistead, States, & Joint Forces, 2004).

Rajanveto termien välille on haastavaa, sillä lähteestä riippuen niitä käytetään vaihtelevin tavoin. ”Sota” voimakkaana ilmaisuna näyttää olevan keskeinen ongelma ja kysymys siitä voiko informaatio-operaatioita olla ilman informaatiosodankäyntiä, aiheuttaa ristiriitaisuuksia termien määritelmiin. Esimerkiksi Korhonen (2014), verkkovaikuttamiseen perehtynyt Helsingin Sanomien toimituspäällikkö, kirjoittaa Ukrainan kriisiin (2014) liittyen:

> ”Oliko Suomi sitten informaatiosodassa Ukrainan ja Krimin takia? Ei tietenkään. Kysymys pitääkin muotoilla toisin. Oliko Suomi informaatio-, kyber- tai psykologisten operaatioiden, harhautusten ja erilaisten disinformaatiokampanjoiden kohteena? Vastaus on kyllä, mutta ei pelkästään Ukrainan sodan takia. EU-jäsenmaana Suomi on unionin yhtenäisyyttä murentamaan pyrkivien vaikuttamisyritysten kohteena koko ajan, vaikka emme aina sitä edes huomaa.”

Samaa näkökulmaa edustaa esimerkiksi Armstead ym. (2004, 19), jotka näkevät kirjassaan informaatio-operaatiot informaatiosodankäyntiä laajempana kokonaisuutena. Heidän mukaansa informaatiosodankäynnissä on kyse jo olemassa olevasta aktiivisesta konfliktista, joka sisältää mahdollisesti myös muunlaista sotilaallista toimintaa. Informaatio-operaatio sen sijaan on strateginen kampanja, jonka elinkaari alkaa rauhasta ja jatkuu konfliktin kautta taas rauhaan (KUVIO 1). Näin ollen informaatiosodankäynti olisi yksi vaihe informaatio-operaatioiden elinkaaressa. Lisäksi heidän mukaansa informaatio-operaatiot eivät sisällä pelkästään sotilaallista toimintaa, vaan muutkin yhteiskunnalliset toimijat, esimerkiksi yritykset, osallistuvat niihin. Tämä ajatus totaalisesta sodasta, jossa vaikutukset kohdistuvat kaikkiin yhteiskunnan osiin, on myös usein liitetty kybersota-ajatteluun (Lehto, 2014b, 172).



KUVIO 1 Informaatio-operaation elinkaari (Armstead ym.,2004, 19)

Semanttisesti tarkasteltaessa ”sota” koostuu operaatiotaidon mukaisesti yksittäisistä operaatioista. Operaatioilla tarkoitetaan useiden erikoistuneiden taisteluiden yhdistämistä yhdeksi laaja-alaiseksi kokonaisuudeksi. Informaatio-operaatioiden kannalta se voisi tarkoittaa siis, että useat informaatiotaistelut yhdistyvät laajemmiksi informaatio-operaatioiksi, jotka muodostavat sitten informaatiosodan. (Ahvenainen, 2014, 15). Vaikka tällainen ajattelu ei välttämättä ole suoraan sovellettavissa informaatio-operaatioiden ja informaatiosodankäynnin väliseen suhteeseen, on tämä ajatusmalli luettavissa rivien välistä monissa lähteissä. Tällöin esiin nousee myös mielenkiintoinen kysymys siitä, koska informaatiosota alkaa ja koska sen voidaan katsoa loppuneen. Tähän kysymykseen vastaaminen vaatisi laajempaa pohdintaa sodankäynnin olemuksesta, eikä siihen siksi oteta kantaa tutkielmassa.

Tässä tutkielmassa informaatio-operaatiot käsitetään kokonaisuutena, joka sisältää varsinaisen aktiivisen konfliktin aikaisen informaatiovaikuttamisen (informaatiosodankäynti) sekä sitä edeltävät ja sen jälkeiset, tähän konfliktiin liittyvät ja informaatioon kohdistuvat toimet. Keskeiseksi nähdään jokin sotilaallinen tavoite, mutta yhteiskunnan muut toimijat voivat olla välillisesti osallisena operaatioissa. Kysymys varsinaisen sodan olemassaolosta nähdään tässä yhteydessä merkityksettömäksi, sillä tutkielman päämielenkiinto on informaatiovaikutuksissa ja informaatio-operaatioiden menetelmissä.

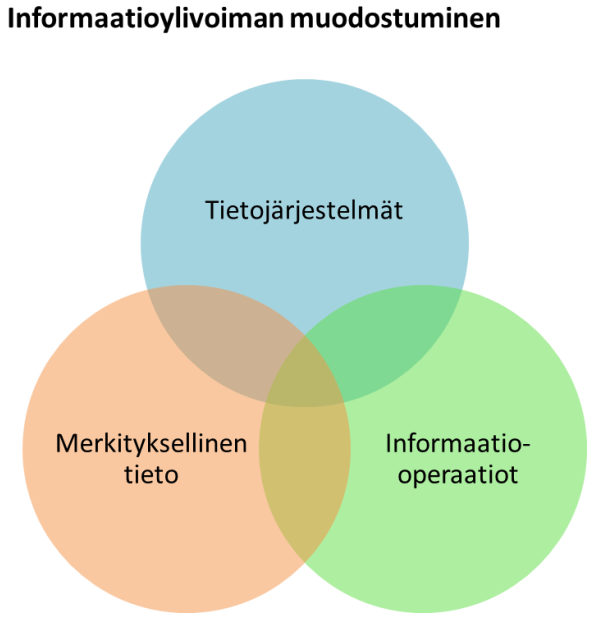
2.2 Informaation merkitys

Käytettiin ilmiöstä mitä termiä tahansa, ovat informaatio-operaatiot samalla uusi, että ikivanha ilmiö. Oikea ja oikea-aikainen informaatio on määrittänyt sotien lopputuloksia ja sillä on ollut merkittävä vaikutus päätöksentekoon. Sen

avulla on myös voitu muokata yleistä käsitystä siitä, kuka on oikeassa ja kuka väärässä. Paras strategi on aina ollut se, joka pystyy voittamaan sodan ja saavuttamaan päämääränsä mahdollisimman pienin sotilaallisen voimankäytön keinoin. Tämä on informaation vaikutuksen ydin koko sodankäynnissä. (Kalliomaa, 2014).

Informaatio itsessään ei ole ase. Se on prosessi ja tapa ymmärtää asioiden suhteita. Sodankäynnissä sen voidaan ajatella olevan työkalu, joka parantaa mahdollisuuksia toimia operatiivisessa ympäristössä. (Armistead ym., 2004). Informaatio muodostuu datasta, tiedon pienimmistä yksiköistä, sekä ohjeistuksesta (systeemistä), jolla data analysoidaan ja tulkitaan. Tämän seurauksena data saa merkityksen ja muodostuu informaatiota. (Wilson, 2006; Ahvenainen, 2014, 12). Informaation hyödyntäminen informaatio-operaatioissa informaatiovaikutuksen saavuttamiseksi noudattelee kuitenkin samaa kaavaa kuin asevaikuttaminen: nopeus, tarkkuus, ulottuvuus, teho ja ennakoimattomuus kasvattavat asevaikutusta ja tuhoa (Kangasmaa, 2014).

Informaatio on myös vallan väline: Kun osapuolella on hallussaan oikeaa ja oikea-aikaista tietoa, kun vastaavasti vastustajan tiedot ovat puutteellisia, vääriä tai/ja vääräaikaisia, on osapuoli saavuttanut niin kutsutun informaatioylivoiman (KUVIO 2). Kuvio havainnollistaa sitä, kuinka informaatioylivoima koostuu merkittävästä tiedosta, informaatio-operaatioista (joiden avulla se on hankittu tai ylläpidetty) sekä tietojärjestelmistä, jossa tätä tietoa prosessoidaan ja säilytetään. Informaatioylivoima johtaa päätöksentekoylivoimaan ja siten ylivoimaan koko toiminnan kirjossa. Vastaavasti informaatioalivoima johtaa epäilyksiin sekä huonoihin ja viivästyneisiin päätöksiin. (Allen, 2007).



KUVIO 2 Informaatioylivoiman muodostuminen (Armstead ym., 2004, 16)

2.3 Informaatioympäristö

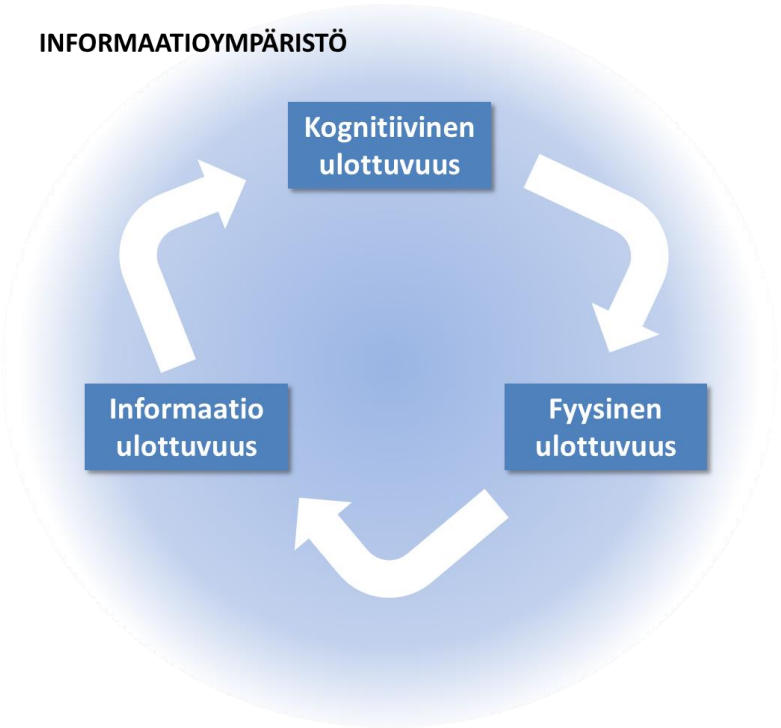
Taustalla informaatio-operaatioiden synnyssä on ollut koko sodankäynnin kuvan murros teollisen aikakauden muuttuessa informaation aikakaudeksi (Huhtinen & Rantapelkonen, 2001). Teknologian nopea kehitys, internetin vaikutus sekä globalisaatio ovat johtaneet siihen, että valtiot eivät enää ole itsenäisiä toimijoita, vaan nykypäivän verkottunut maailma koostuu monista toisiinsa liittyneistä toimijoista, jotka kommunikoivat keskenään. (Allen, 2007).

Informaatioteknologian merkityksen kasvu yhteiskunnan toimivuuden kannalta on johtanut tilanteeseen, jossa vastustajan voi saada polvilleen vaikuttamalla yhteiskunnan kriittisiin ja elintärkeisiin järjestelmiin. Enää ei tarvitse valloittaa maa-alueita jalkaväen ja panssarivaunujen voimin. Nyt pieni, vähän taloudellisia resursseja vaativa ja osaava hakkeritiimi pystyy saamaan aikaan paljon tuhoa. (Rantapelkonen, 2014). Tämä voi tasoittaa sodan valta-asemia, kun pienelläkin toimijalla on mahdollisuus tasavertaisuuteen suurempia toimijoita vastaan. Kangasmaa (2014) sanoo artikkelissaan: ”Informaatioaseet ovatkin tehokkaita nimenomaan altavastaajan arsenaalissa”.

Armeijat omaavat erilaisia toiminnalleen kriittisiä järjestelmiä, joihin voidaan kohdistaa informaatio-operaatioita. Esimerkiksi nykyaikaiset hävittäjät, risteilyohjukset ja ilmatorjuntajärjestelmät ovat riippuvaisia monimutkaisesta reaaliaikaisesta tiedon käsittelystä ja moderneilla armeijoilla on erilaisia digitaalisia hallinto-, komento- ja viestijärjestelmiä. (Veijalainen ym., 2008, 529). Armeijoiden tukeutuessa entistä enemmän informaatioteknologian tarjoamiin ratkaisuihin on syntynyt paljon uusia mahdollisuuksia, mutta myös uhkia, joihin informaatio-operaation keinoin pyritään vastaamaan (NATO, 2009). Tämä suhtautumisen muutos informaatioteknologian kehitykseen näkyy hyvin Korhosen (2014) artikkelissa hänen kertoessa erään everstin lausuneen noin kymmenen vuotta sitten: ”T-72 lähtee käyntiin vaikka kuusen alta, riippumatta siitä, onko internet pystyssä tai ei”. Nyt, kymmenen vuotta myöhemmin, sähköistyneen yhteiskunnan mahdollisuudet, haavoittuvuudet sekä asenteet ovat aivan eri luokkaa (Korhonen, 2014).

Nykyisen informaatio aikakauden tyypillinen piirre on informaation määrän suuri kasvu ja informaation kommunikoinnin nopeus (Joint Publication 3-13, 2012). Esimerkiksi minuutin aikana internetissä tehdään 2 miljoonaa Google hakua, lähetetään 204 miljoonaa sähköpostia ja 216 000 valokuvaa jaetaan Instagram-palvelussa. Myös käyttäjien liikkuminen, maantieteellinen hajautuminen ja virtuaalisten organisaatioiden toiminta on mahdollistunut. (Lehto, 2014a, 71). Lisäksi tietoverkkojen teho, monimuotoisuus ja kattavuus ovat lisääntyneet merkittävästi viimeisen kahdenkymmenen vuoden aikana. Informaatio on myös yhä useamman saatavilla ja internet on vähentänyt sensuuria. (Allen, 2007; Kangasmaa, 2014). Myös media on erottamaton osa sodankäyntiä ja suuressa asemassa vaikuttamassa yleiseen mielipiteeseen, kaikkien nykyaikaisten konfliktien ollessa eri medioiden kirkkaassa valokeilassa. (NATO, 2009).

Tämä kehitys on luonut aivan uudenlaisen informaatioympäristön, joka yhdistää informaation, toimijat ja tietojärjestelmät, jotka mahdollistavat informaation hyödyntämisen (Joint Publication 3-13, 2012; NATO, 2012). Yhdysvaltojen armeijan julkaisu Joint Publication 3-13 (2012) jakaa tämän informaatioympäristön kolmeen ulottuvuuteen, jotka ovat kognitiivinen, informaatio- ja fyysinen ulottuvuus (KUVIO 3). Näiden ulottuvuuksien välillä kulkee informaatiovirtoja, jotka on kuvioon kuvattu valkoisina nuolina. Kuvion informaatio ulottuvuus kuvaa sitä missä ja miten informaatiota kerätään, prosessoidaan, säilötään, levitetään ja suojellaan. Toiminta tässä ulottuvuudessa vaikuttaa informaation kulkuun.



KUVIO 3 Informaatioympäristö (Joint Publication 3-13, 2012).

Informaatioympäristön fyysinen ulottuvuus pitää sisällään komento- ja ohjausjärjestelmät, avainpäätöksentekijät ja niitä tukevan infrastruktuurin, joka mahdollistaa yksilöiden ja organisaatioiden vaikutusten toteutumisen. Se koostuu fyysisistä alustoista ja niitä yhdistävistä kommunikaatiokanavista. Fyysinen ulottuvuus pitää sisällään esimerkiksi ihmiset, tietojärjestelmät, sanomalehdet ja älylaitteet. Fyysinen ulottuvuus ei rajoitu pelkästään sotilaallisiin tai edes kansakuntiin perustuviin järjestelmiin ja prosesseihin. Se on osista koostuva verkosto, joka ylittää kansalliset, maantieteelliset ja taloudelliset rajat. (Joint Publication 3-13, 2012).

Kognitiivinen ulottuvuus kuvaa ihmismieltä, joka välittää, vastaanottaa ja toimii informaation perusteella. Se viittaa yksilön tai joukon informaation prosessointiin, havaintoihin, harkintaan ja päätöksentekoon. Näihin seikkoihin

vaikuttaa hyvin moni asia kuten kulttuuri, normit, kokemukset ja koulutus. Näiden vaikuttimien ymmärtäminen on kriittistä määriteltäessä niitä keinoja, joilla pyritään vaikuttamaan päätöksen tekoon. Kognitiivinen ulottuvuus on siksi informaatioulottuvuuksista kaikkein tärkein. (Joint Publication 3-13, 2012).

2.4 Informaatio-operaatioiden tavoitteet

Konfliktien lopputulos perustuu toimiin, toimet perustuvat päätöksiin, päätökset perustuvat tilannekuvaan ja tilannekuva muodostuu informaatiosta (Allen, 2007). Ne, joilla on paras kyky kerätä, ymmärtää, kontrolloida ja käyttää olemassa olevaa oikeaa informaatiota, saavuttavat merkittävän edun päätöksen tekoon (informaatioylivoima). Yhdysvallat ovat määritelleetkin juuri informaatioylivoiman saavuttamisen yhdeksi informaatio-operaatioiden päätavoitteista. (U.S. Army War College, 2011, 55). Informaatio-operaatioille voidaan eritellä muitakin tavoitteita, mutta keskeisin on vastustajan käyttäytymiseen vaikuttaminen nimenomaan vastustajan päätöksentekoon vaikuttamalla. Päätöksenteko koostuu oikeasta tilannekuvasta sekä toimintakyvystä ja halusta toimia. Mikäli joku näistä puuttuu, vastustajan kyky toimia sille edullisella tavalla häiriintyy. Informaatio-operaatioilla vaikutetaan näihin kolmeen tekijään. Samaan aikaan tavoitteena on myös suojella omaa kykyä tehdä oikeita päätöksiä. (NATO, 2009; U.S. Army War College, 2011).

Informaatioympäristön lävitse kulkevien informaatiovirtojen manipulointi on yksi informaatio-operaatioiden mekanismi, jolla voidaan vaikuttaa tilannekuvan syntymiseen. (NATO, 2009). Oikea tilannekuva nähdään yhdeksi tärkeimmistä tekijöistä menestyksekkääseen sodankäyntiin ja tehokkaaseen johtamiseen (Kott, 2008). Esimerkiksi persianlahden sodassa liittouma pystyi teknologisen ylivoimansa turvin hyödyntämään tiedustelun, valvonnan ja johtamisen järjestelmiään vastustajaansa tehokkaammin. Kaikki oleellinen informaatio taistelutilasta oli heidän saatavillaan ja samalla pystyttiin estämään vastustajaa saamasta vastaavia tietoja liittouman omasta toiminnasta. Tämä johti salamannopeisiin, kirurgisen tarkkoihin iskuihin heti, kun vihollinen oli havaittu. (Rantapelkonen, 2014).

Tilannekuva muodostuu aina lopulta ihmisten mielessä ja siihen vaikuttavat muun muassa seuraavat tekijät (Kärkkäinen, 2013):

- Tietoisuus nykyisestä tilanteesta
- Tietoisuus toiminnon seurauksista
- Tietoisuus tilanteen kehittymisestä
- Tietoisuus vastustajan käyttäytymisestä
- Tietoisuus miten nykytilanteeseen on päädytty ja miksi
- Tietoisuus kerätyn tilannetiedon (informaation tai datan) luotettavuudesta
- Arvio tilanteen mahdollisesta kehittymisestä.

Oman tilannekuvan ylläpidossa on monia haasteita, joihin informaatio-operaatioilla vastataan. Esimerkiksi informaation määrän ollessa suuri, haasteiksi nousee sen tehokas käsittely ja käytettävyys. Väärinymmärrykset ovat sitä todennäköisempiä, mitä enemmän informaatiota on. Jaettu informaatio ei välttämättä takaa jaettua ymmärrystä. (Kott, 2008).

Vastustajan tahtoon vaikuttaminen tarkoittaa sitä, että vaikutetaan kohdeyleisön haluun toimia tietyllä tavalla. Tällöin informaatio-operaatioilla vaikutetaan suoraan toimijan ymmärrykseen ja niihin kykyihin ja keinoihin, joilla ymmärrys muodostetaan. Vaikutus kohdistuu siis erityisesti informaatioympäristön kognitiiviselle tasolle. Tahtoon vaikutetaan esimerkiksi oman puolen yhteishenkeä kohottamalla ja vastustajaa painostamalla. (NATO, 2009).

Informaatio-operaatioilla vastustajan tahto pyritään lamauttamaan ja kyseenalaistetaan oikeutus sodankäynnille (Rantapelkonen, 2014). Tämä voidaan saavuttaa esimerkiksi vaikuttamalla kansakunnan yleiseen mielipiteeseen. Kuten Rantapelkonen (2014) sanoo artikkelissaan: ”Kotirintama on informaatiosodan tärkein rintama ja ilman sen tukea, on sotilaiden vaikea taistella.” Tällä tavoin voidaan myös heikentää valtaapitävien ja kannattajien suhdetta, mikä vaikuttaa kohteiden haluun toimia tai jatkaa vahingollista toimintaa (NATO, 2009). Informaatio-operaatioita ei tarvitse kohdistaa suoraan vastustajan päätöksen tekijöihin, vaan heihin vaikuttaminen voi tapahtua käänteisesti äänestäjien ja virkamiehien kautta (Kangasmaa, 2014). Esimerkiksi Ukrainan kriisissä (2014) näkyy selkeästi piirteitä informaatio-operaatioista, joissa Ukrainan valtiollinen eheys on pyritty rikkomaan, sekä hajottamaan EU:n talouspakoterintama (Rantapelkonen, 2014).

Nykypäivän sodissa mielikuvilla on suuri merkitys tahdon muodostumisessa. Media on tiiviisti mukana konflikteissa luomassa käsitystä sodan tilanteesta. Erityisesti internetin ja sosiaalisen median välityksellä mielikuvia luodaan yhä enemmän kuivin ja äänin. (Huhtinen & Rantapelkonen, 2001). Informaatio-operaatioilla vaikutetaan näiden mielikuvien syntymiseen ja niitä muokataan itselle edullisiksi. Nykyään sodankäynnissä ei ole usein oleellista, miten asiat ovat, vaan miltä ne näyttävät. Mielipiteitä ohjailemalla voidaan edesauttaa tai vaikeuttaa osapuolten toimintaa. (Rantapelkonen, 2014). Jo Napoleonin tiedetään sanoneen, että moraali ja mielipiteet muodostavat puolet sodankäynnin todellisuudesta (Huhtinen & Rantapelkonen, 2001). Korhonen (2014) kiteyttää artikkelissaan seuraavasti: ”Elämme yhä enemmän elämys- ja mielipidetaloudessa, jossa ihmiset säntäilevät ja tekevät isojakin taloudellisia ja poliittisia valintoja pelkän yleisen mielipiteen ja mutu-tiedon varassa.”

Toimintakykykyyn kohdistuvissa informaatio-operaatioissa kohteena on esimerkiksi vastustajan johtamis- ja kommunikointi järjestelmät sekä propagandakoneisto, jotka mahdollistavat vastustajan päätöksentekijän tahdon toteutumisen. Informaatio-operaatioiden avulla pyritään häiritsemään, estämään ja tuhoamaan niitä toimintoja, joiden avulla vastustaja pystyy lisäämään ymmärrystään olemassa olevasta tilanteesta ja jotka tukevat, määräävät, lisäävät ja ylläpitävät heidän tahtoa toimia. Toimintakykyyn vaikutetaan myös kohdistamalla iskuja vastustajan keskeisiä voimavaroja vastaan ja pyrkimällä erotta-

maan eri voimaryhmittymät toisistaan. Tämä voi tarkoittaa esimerkiksi vastustajan liittolaissuhteiden sabotointia. (NATO, 2009).

Koska informaatio-operaatioilla vaikutetaan konfliktien koko elinkaareen, niitä käytetään myös rauhan ylläpidossa ja varsinaisen aseellisen yhteenoton synnyn ehkäisyssä. Sirén (2011, 5) kertoo artikkelissaan:

> ”Sotataidollisesti ajatellen voitto sodassa tarkoittaa mahdollisesti lähitulevaisuudessa vastustajan, potentiaalisen vastustajan tai muiden nimettyjen kohdejoukkojen suvaitsemattomien identiteettirakenteiden muuttamista niin, että kineettiset sodat voidaan välttää jo ennakolta häviämättä rauhaa”.

Informaatio-operaatioiden keinoja käytetään siis myös siten, että varsinaista konfliktia ei pääse syntymään.

3 INFORMAATIO-OPERAATIOIDEN VAIKUTUSMENETELMÄT

Informaatioteknologian kehitys on antanut paljon uusia työkaluja erilaisten sotilaallisten tavoitteiden saavuttamiseksi. Informaatio-operaatioissa näitä työkaluja hyödynnetään informaatiovaikutuksen aikaansaamiseksi. Informaatio-operaatiot ovat erilaisia menetelmiä kokoava toimintakokonaisuus – ei niinkään yksittäinen toimintamalli. (NATO, 2009). Mitä menetelmiä tähän kokoelmaan luetaan, vaihtelee paljon lähdeaineiston ja määrittelevien organisaatioiden kesken. Alla olevassa taulukossa (TAULUKKO 1) on esitelty Suomen, Yhdysvaltojen ja Naton informaatio-operaatioihin lukemia menetelmiä. (NATO, 2009; Heikala ym., 2011, 130; Joint Publication 3-13, 2012).

TAULUKKO 1: Informaatio-operaatioissa hyödynnettäviä menetelmiä eri sotilasorganisaatioissa

Suomi	**Yhdysvallat**	**Nato**
Psykologiset operaatiot / sodankäynti	Julkissuhteiden hoito, Psykologiset operaatiot	Julkissuhteiden hoito, Psykologiset operaatiot
Elektroninen sodankäynti	Elektroninen sodankäynti	Elektroninen sodankäynti
Operaatioturvallisuus	Operaatioturvallisuus	Operaatioturvallisuus
Operatiivinen /sotilaallinen harhauttaminen	Sotilaallinen harhauttaminen	Sotilaallinen harhauttaminen
Tietojärjestelmäsodankäynti	Kyberoperaatiot	Tietoverkko-operaatiot
Kansallinen informaatiosodankäynti		
	Viranomaisyhteistyö	Viranomaisyhteistyö
	Tiedustelu / Vakoilu	
	Avainhenkilöiden sitouttaminen	Avainhenkilöiden sitouttaminen
	Informaation varmistus	Tietoturva
	Strateginen kommunikaatio	PPP (Presence, Posture and Profile)
	Avaruusoperaatiot	

On syytä huomioida, että monia näistä menetelmistä voidaan käyttää myös paljon laajemmin kuin pelkästään informaatio-operaatioiden tarkoituksiin. Eri menetelmien välillä on myös paljon rinnakkaisuutta. Oli käyttötarkoitus mikä tahansa, eri menetelmistä aiheutuvat tahattomat informaatiovaikutukset tulee huomioida yleisessä toiminnan suunnittelussa. (NATO, 2009).

Tässä luvussa tutustutaan tarkemmin informaatio-operaatioiden vaikutusmenetelmiin ja tarkastellaan miten näiden menetelmien vaikutus kohdistuu organisaation kokonaisarkkitehtuurin kannalta. Tutkielman laajuuden vuoksi kaikkia kirjallisuudessa tai edellä olevassa taulukossa esiintyviä menetelmiä ei käydä läpi. Tarkempaan tarkasteluun on valittu viisi useassa lähteessä keskeiseksi esiteltyä vaikutusmenetelmää: *Elektroninen sodankäynti*, *Operaatioturvallisuus*, *Psykologiset operaatiot, Sotilaallinen harhauttaminen ja tietoverkko-operaatiot*. (Wilson, 2006; Kelley, 2010, 18; Sirén, 2011, 18).

3.1 Elektroninen sodankäynti

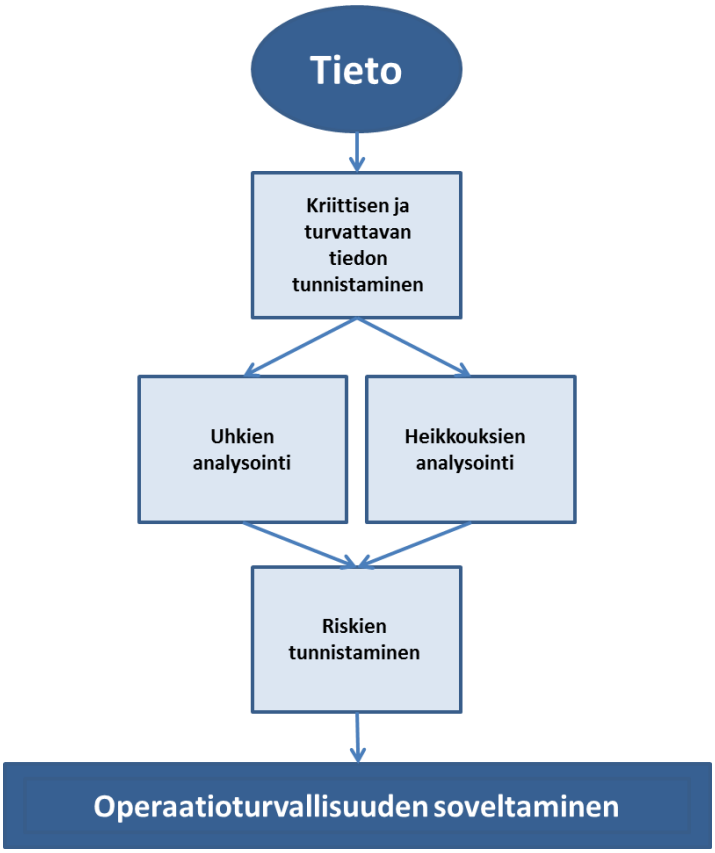
Jokainen laite ja teknologia, jota käytetään nykypäivän informaatioyhteiskunnassa, toimii jollain sähkömagneettisella taajuudella – oli kyseessä sitten tietokone, langaton verkkoyhteys tai digitaalinen tutka. Elektronisen sodankäynnin tarkoituksena on tämän sähkömagneettisen spektrin hallinta ja kontrolli oman sodankäynnin edistämiseksi ja vastustajan sodankäyntikyvyn heikentämiseksi. Sähkömagneettisten taajuuksien hallinnan avulla erilaiset oman toiminnan kannalta kriittisten elektronisten laitteiden kuten tutkien, kommunikaatioyhteyksien ja sensorien toimivuus varmistetaan. Elektroninen sodankäynti jaetaan kolmeen osaan: elektroninen tuki, elektroninen vaikuttaminen ja elektroninen suojautuminen. (Hakala ym., 2003, 181; Wilson, 2006).

Elektronisen sodankäynnin avulla voidaan tukea muiden informaatiovaikutusten toteutumista ja se on olennainen osa datan keräämisessä. (NATO, 2009). Elektronisen sodankäynnin avulla voidaan manipuloida informaatiovirtoja siten, että esimerkiksi johtamisen ja tulenkäyttöjärjestelmien luotettavuus alenee ja informaatiorakenteiden käytettävyys pienenee (Lehto 2014b, 160). Elektronisessa sodankäynnissä on paljon samankaltaisuuksia tietoverkko-operaatioiden kanssa, sillä langattoman tiedonsiirron tekniikat ovat osa elektronisen sodankäynnin keskeistä välineistöä (Hakala ym., 2011, 190).

Elektronisen sodankäynnin järjestelmät ovat kehittyneet vaihtelevasti Kylmän Sodan päättymisen jälkeen. Kehitys on kuitenkin kiihtynyt voimakkaasti 2000-luvun aikana erityisesti Irakin ja Afganistanin konfliktien jälkeen. Näissä kriiseissä länsimailla oli vastassaan vihollinen, joka pystyi hyödyntämään halpaa kaupallista elektroniikkaa ja sähkömagneettisia taajuuksia iskuissaan. Lännessä tähän ei ollut varauduttu, minkä johdosta elektronisen sodankäynnin kykyjä on alettu korostaa uudella tavalla. Tämä on hyvä esimerkki tilanteesta, jossa myös heikompi, vähemmän resursseja omaava osapuoli pystyi saavuttamaan tuloksia informaatio-operaatioiden keinoin. (Hakala ym., 2011).

3.2 Operaatioturvallisuus

Operaatioturvallisuus on prosessi, jossa keskitytään toiminnalle kriittisen tiedon turvaamiseen. Keskeisiä toimintoja ovat kriittisen informaation tunnistaminen, siihen kohdistuvien uhkien arvioiminen, haavoittuvuuksien analysoiminen, informaatioriskien arvioiminen ja sopivien toimintamallien valinta ja toteutus (KUVIO 4). Tämä tarkoittaa sitä, että pyritään estämään vastustajaa saamasta haltuunsa tietoja esimerkiksi joukkojen sijoittelusta, toimintakyvystä ja toimintasuunnitelmista. (NATO, 2009; Heikala ym., 2011). Informaatiooperaatioiden alaisuudessa operaatioturvallisuudella on merkittävä rooli vastustajan ja omien joukkojen oikean tilannekuvan syntymisessä ja ylläpidossa (Joint Publication 3-13, 2013).



KUVIO 4 Operaatioturvallisuuden prosessikuvaus (Heikala ym., 2011, 138).

Strategisella tasolla operaatioturvallisuus on koko puolustusjärjestelmän toimivuuteen liittyvien tietojen turvaamista. Taktisella tasolla vastaavasti sillä tarkoitetaan muun muassa yksittäiseen sotilaaseen kohdistuvan kriittisen tiedon turvaamista. Tämä tarkoittaa esimerkiksi sitä, ettei yksittäinen suomalainen rauhanturvaaja saa jakaa toimialueella kuvattuja videoita internetissä. (Heikala ym., 2011, 131).

Sosiaalinen media onkin uusi ilmiö, joka on tuonut paljon uudenlaisia haasteita toimintaan operaatioturvallisuuden näkökulmasta eikä niihin ole vielä osattu suhtautua järkiperäisesti. (Heikala ym., 2011, 131). Puolustusvoimat on toteuttanut erilaisia ohjeistuksia sosiaalisessa mediassa toimimiseen, joista käy ilmi esimerkiksi mitä yksittäinen varusmies saa sotaharjoituksista kertoa internetissä ja mitä ei. Operaatioturvallisuuden kannalta varjeltavaa tietoa on edellä mainitussa tilanteessa esimerkiksi henkilön sijainti ja sotilaallinen tehtävä. (Puolustusvoimat, 2015).

Operaatioturvallisuuden kokonaisuus voidaan jakaa logistisiin, operatiivisiin, teknisiin ja hallinnollisiin toimenpiteisiin. Logistisiin ja operatiivisiin toimenpiteisiin kuuluu taktiikan tai toimintatapojen muuttamista epäsäännöllisesti tai muuttamalla joukkojen toimintaa niin, ettei toiminta paljasta niiden aikomuksia tai toimintakykyä. Teknisiä toimenpiteitä ovat mm. salattujen yhteyksien käyttäminen ja valelaitteiden käyttö. Hallinnollisiin keinoihin taas voidaan lukea esimerkiksi asiakirjaturvallisuus tai niin kutsuttu tyhjän työpisteen periaate (Työpisteelle ei saa jättää arkaluontoista materiaalia näkyville). (Heikala ym., 2011, 139).

Tietoturva on keskeinen osa operaatioturvallisuutta ja se on perinteisesti tähdännyt informaation luotettavuuden, eheyden ja käytettävyyden turvaamiseen (Veijalainen ym., 2008, 550). Usein se kuitenkin mielletään pelkästään tietojärjestelmiin ja tiedonsiirtojärjestelmiin liittyväksi kokonaisuudeksi. Operaatioturvallisuus kattaa tämän tyyppisen tietoturva-ajattelun lisäksi myös muuhun toimintaan liittyvän tietoturvan. Esimerkiksi joukkojen toiminta saattaa paljastaa omasta operaatiosta sen laajuuden ja tavoitteet. Operaatioturvallisuuden kannalta on tärkeää myös muistaa, että monimuotoisten tietojärjestelmien keskiössä toimii ihminen, joka tulee aina oleman informaation käsittelyn ”heikoin lenkki” ja ihmisen synnyttämät informaatiouhat ja –riskit voivat olla tahattomia tai tahallisia. (Heikala ym., 2011, 134–140).

3.3 Psykologiset operaatiot

Psykologisten operaatioiden tärkein tavoite on vaikuttaa halutun kohteen tai kohderyhmän identiteettirakenteisiin, asenteisiin ja käyttäytymiseen itselle edullisella tavalla. Psykologiset operaatiot ovat selkeä esimerkki ei-tappavia menetelmiä käyttävästä vaikuttamisesta ja se nähdään läntisissä asevoimissa kineettistä vaikuttamista tukevana ja kokonaisvoimaa lisäävänä tekijänä. (NATO, 2009; Sirén, 2011, 199–209).

Psykologiset operaatiot liittyvät voimakkaasti propagandaan. Kautta historian kineettisen sodankäynnin vaikuttavuutta on lisätty sanoin, äänin ja kuvin. Propaganda-sanaa on käytetty 1600-luvulta asti ja alun perin se tarkoitti mainostamista tai sanoman levittämistä. Nykyään termi on vahvasti politisoitunut eikä sitä käytetä kuvaamaan omaa toimintaa. Nykypäivän sodankäynnissä propagandalla tarkoitetaan valehtelemista, petkuttamista ja manipulaatiota. (Sirén, 2011, 201–206).

Toisen maailmansodan aikana propagandaa alettiin nimittää psykologiseksi sodankäynniksi, jolloin keskeistä oli oman toiminnan kaunistelu ja vastustajan ”mustamaalaus”. Vietnamin sodan aikana termiksi vakiintui psykologiset operaatiot. Psykologiset operaatiot eivät varsinaisesti tuo mitään uutta aikaisempien sotien propaganda-ajatteluun, mutta informaatioaika on tarjonnut uusia menetelmiä sen levitykseen. Perinteisten keinojen kuten sanomalehtien ja television rinnalle on noussut älylaitteet ja internetin mahdollistamia uusia kanavia kuten sosiaalinen media. (Sirén, 2011, 201–206).

Informaatio-operaatioiden alaisuudessa psykologisten operaatioiden vaikutus kohdistuu erityisesti informaatioympäristön kognitiiviseen ulottuvuuteen. Psykologisten operaatioiden onnistuminen vaatii tarkkaa kohdeyleisön analysointia ja ymmärtämistä. Ollakseen tehokas, halutun sanoman täytyy sopia kohdeyleisön kulttuuriympäristöön. Lisäksi keskeistä on oikeiden välityskanavien valinta. (Joint Publication 3-13.2, 2010). Psykologisia operaatioita ei välttämättä kohdisteta suoraan päätöksentekijöihin, vaan niiden kohteena ovat usein tavalliset ihmiset. Esimerkiksi sosiaalisessa mediassa käynnistynyt yleisöreaktio voi vaikuttaa valtaa pitävien toimintaan. Avoin ja demokraattinen yhteiskunta onkin erittäin otollinen kohde psykologisissa operaatioissa käytettävälle dis-informaatiolle. (Korhonen, 2014).

3.4 Sotilaallinen harhauttaminen

Sotilaallinen harhauttaminen keskittyy toimiin, joilla tarkoituksenmukaisesti johdetaan harhaan vastustajan sotilaallisten organisaatioiden päätöksentekijöitä (U.S. Army War College, 2011). Harhauttamisessa operaation kohteena ovat keskitetysti ne päätöksen tekijät, joilla on valta harhautuksen kohteena oleviin päätöksiin. Tavoitteena on saada päätöksentekijä toimimaan tai luopumaan toiminnasta siten, että se edesauttaa omien joukkojen tavoitteiden toteutumista. (Järvinen ym., 2011, 112).

Onnistuakseen harhautus vaatii keskittymistä turvallisuuteen. Aktiivisten salauspyrkimysten yhteydessä on pystyttävä salaamaan sekä oikeat, että harhautustoimet. Myös ajoitus on keskeisessä roolissa. Harhautusoperaatiot voivat viedä paljon aikaa esimerkiksi vastustajan poliittisen- tai tiedustelujärjestelmän reaktioiden vuoksi. Harhautusoperaatiot on usein integroitu muihin korkeamman tason operaatioihin. (NATO, 2009; Järvinen ym., 2011, 112–113).

Operaatiomielessä harhauttamisella voidaan saavuttaa suoria ja epäsuoria vaikutuksia. Suora vaikutus on esimerkiksi itselle edullinen yllätysmomentti ja epäsuora turvallisuuden lisääntyminen. Yllätyksen saavuttaminen onkin nähty tärkeimmäksi yleisistä taktisista periaatteista, joka voidaan saavuttaa harhauttamalla. (NATO, 2009; Järvinen ym., 2011, 112–113).

Georgian lyhyt sota vuonna 2008 on yksi viimeisimmistä esimerkeistä sotilaallisesta harhauttamisesta. Siinä harhauttamisen keinoin Venäjä haki oikeutusta operaatiolle kansainväliseltä yhteisöltä ja toisaalta sai Georgian aloitta-

maan näkyvät taistelutoimet, jolloin syy sotilaalliselle interventiolle syntyi. (Järvinen ym., 2011, 113).

3.5 Tietoverkko-operaatiot

Tietoverkko-operaatiot ovat menetelmäkokonaisuus, joka on vahvasti esillä myös kybersodankäyntiajattelussa. Informaatio-operaatioiden yhteydessä näkökulma on erityisesti niiden informaatiovaikutuksessa. Ratkaisevaa tietoverkko-operaatioiden hyödyntämismahdollisuuksissa on vastustajan riippuvuus informaatioteknologian käytöstä. (NATO, 2009). Tietoverkko-operaatioissa vastustajan käyttämiin tietoverkkoihin ja niiden sisältämään tietoon vaikutetaan niitä vastaan hyökkäämällä tai niitä häiritsemällä. Vastustajan tietoverkkoja hyödynnetään myös tiedusteluun. Samaan operaatiokokonaisuuteen kuuluu myös omien tietoverkkojen ja niiden sisältämän tiedon puolustus. Puolustuksen tärkein lähtökohta on informaatio turvallisuus ja sitä toteutetaan käytännössä esimerkiksi palomuureilla. (Wilson, 2006).

Tietoverkot muodostavat tietojärjestelmien kanssa informaatioinfrastruktuurin, jossa informaatiovirta kulkee eri verkon osien välillä. (Lehto, 2014a, 70). Tietoverkot ovat siksi keskeinen ja monipuolinen vaikuttamisen kanava, sillä niiden avulla voidaan vaikutus kohdistaa myös muuhun kuin sotilaallisiin kohteisiin. (Kuusisto, 2014, 34). Sotilaallisten tietoverkko-operaatioiden menetelmät ovat hyvin samankaltaisia tavallisten tietoverkkorikosten kanssa. Ero on tavoitteissa. Siinä, missä yksityiset tietoverkkorikolliset tavoittelevat usein taloudellista hyötyä, on tietoverkko-operaatioiden tavoitteita esimerkiksi kohdejärjestelmän haltuunotto tai sen toiminnan selvittäminen, muuttaminen tai estäminen jonkin sotilaallisen tavoitteen saavuttamiseksi. Tietoverkko-operaatioiden vaikutus voi kestää sekunnin murto-osista useisiin vuosiin, mutta yksittäinen menetelmä on usein kertakäyttöinen. (Illi, Karppinen, Palokangas & Seppälä, 2011).

Tietoverkko-operaatioita vastaan puolustauduttaessa keskeistä on informaation turvallisuus. On tärkeää turvata omissa tietoverkoissa liikkuvan informaation luottamuksellisuus, eheys ja saatavuus. Luottamuksella tarkoitetaan sitä, että tietoa pääsevät käsittelemään vain ne, joilla on siihen oikeus. Eheys taas tarkoittaa, ettei tieto muutu tiedonkäsittelyprosessin aikana ja saatavuus korostaa sitä, että tieto on aina saatavilla, kun siihen oikeutetut henkilöt sitä tarvitsevat. (Vankka, 2014). Puolustus voi olla passiivista, jolloin tarkoitetaan esimerkiksi palomuurien käyttöä tai luvattoman käytön valvontaa. Aktiivinen puolustus taas voi tarkoittaa vastaiskun tekemistä tai harhauttamista. (Kärkkäinen, 2013, 5-6). Tietoverkko-operaatioissa hyödynnetään usein järjestelmissä olevia haavoittuvuuksia, ja näiden tunnistaminen onkin avain asemassa toisaalta hyökkäävissä tietoverkko-operaatioissa, mutta myös omien tietoverkkojen ja järjestelmien puolustuksessa (Illi ym., 2011).

Hyökkäävillä tietoverkko-operaatioilla pyritään vaikuttamaan edellä mainittuihin informaation ominaisuuksiin. Tietoverkkohyökkäyksissä tavoite voi olla vaikuttaa pelkästään tietojärjestelmiin ja niiden sisältämään dataan. Toinen vaihtoehto on tietoverkkoja hyödyntäen kohdistaa vaikutus johonkin tietojärjestelmästä riippuvaiseen prosessiin tai toimintoon esimerkiksi haittaohjelman avulla. (Wirman, 2014, 124).

3.6 Informaatio-operaatioiden vaikutus kokonaisarkkitehtuurin näkökulmasta

Tutkielman lopuksi havainnollistetaan informaatio-operaatioiden vaikutusmenetelmiä kokonaisarkkitehtuurin näkökulmasta. Kokonaisarkkitehtuurin avulla havainnollistetaan informaatiovaikutuksen kohdentumista koko organisaatioon ja helpotetaan eri osatekijöiden vuorovaikutussuhteiden hahmottamista.

Kokonaisarkkitehtuuri (*Enterprise architecture*) kuvaa organisaation kokonaisrakennetta. Se on keino havainnollistaa organisaation tietoa sen prosesseista, informaatiosta ja organisaatiorakenteesta sekä näiden välisistä vuorovaikutussuhteista. (Giachetti, 2010). Kokonaisarkkitehtuurin avulla määritellään organisaation keskeiset komponentit. Näitä ovat esimerkiksi IT-infrastruktuuri, käytänteet ja teknologiat. (Schmidt ym., 2014). Kokonaisarkkitehtuuri auttaa organisaatiota tunnistamaan kehitysalueensa niin rakenteessaan kuin toimintatavoissaan (Graves, 2009, 10).

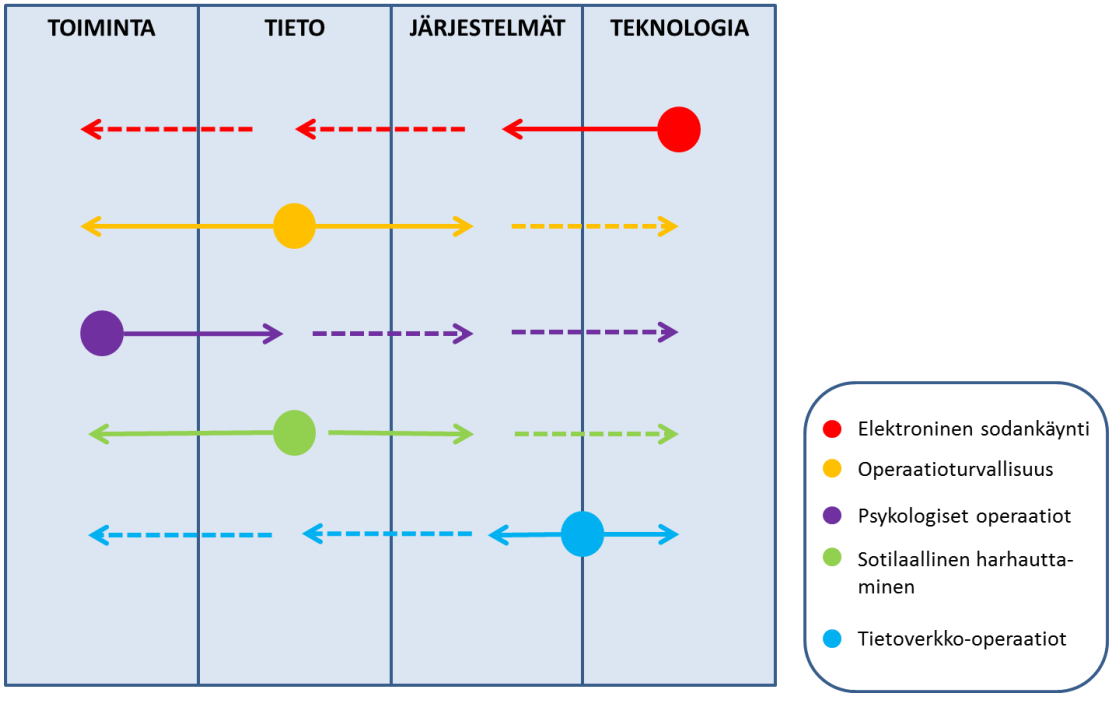
Kokonaisarkkitehtuurin kuvaamisessa hyödynnetään kehyksiä (*frameworks*), joiden avulla havainnollistetaan eri konteksteja (Graves, 2009, 32). Kehyksiä on monia ja niiden lähestymistapa vaihtelee paljon hyvin abstrakteista ohjeista hyvinkin yksityiskohtaisiin metodologioihin. Kehyksiä voidaan käyttää hyvin monenlaisissa ympäristöissä. Jotkut palvelevat puhtaasti yritysmaailman tarpeita, kun taas toisia voidaan hyödyntää myös muunlaisissa organisaatioissa. Esimerkiksi DoDAF (*Department of Defence Architecture Framework*) on Yhdysvaltojen armeijan käyttämä kokonaisarkkitehtuurikehys. (Urbaczewski & Mrdalj, 2006). Kehyksien avulla kokonaisarkkitehtuuri jaotellaan pienempiin kokonaisuuksiin, useimmiten neljään osa-alueeseen: liiketoiminta, tieto, sovellus ja teknologia (Pulkkinen, 2006). Monissa kokonaisarkkitehtuureissa jaottelu on paljon yksityiskohtaisempi, mutta usein yleistettävissä takaisin näihin neljään osa-alueeseen.

Tässä tutkielmassa sotilasorganisaation kokonaisarkkitehtuuria käsitellään yksinkertaistetun kehyksen avulla, jossa arkkitehtuuri koostuu toiminnasta, informaatiosta, järjestelmistä ja teknologioista (KUVIO 5). Tutkielmassa käytettävässä mallissa on hyödynnetty pohjana DoDAF:ia ja TOGAF:ia (*The Open Group Architecture Framework*) kokonaisarkkitehtuurimalleja (The Open Group, 2011; Department of Defense, 2015).

TOIMINTA	TIETO	JÄRJESTELMÄT	TEKNOLOGIA
• Operaatiot • Tavoitteet • Ihmiset	• Data • Informaatio	• Tietojärjestelmät • Järjestelmien tuottamat palvelut	• IT infrastruktuuri • Laitteet • Fyysiset tietokannat • Tietoverkot • Aseet

KUVIO 5 Sotilasorganisaation kokonaisarkkitehtuuri

Vaikka informaatio-operaatioiden kohteena on itse informaatio, eri menetelmien voidaan katsoa vaikuttavan kokonaisarkkitehtuurin näkökulmasta eri tavoin. Alla olevassa kuvassa on viiden aikaisemmin esitellyn menetelmän vaikutus kuvattu sotilasorganisaation kokonaisarkkitehtuuriin (KUVIO 6). On syytä huomioida, että yksittäinen menetelmä sisältää monipuolisia vaikutuskeinoja, joten kuvio havainnollistaa informaatiovaikutusten syntymistä hyvin yleisellä tasolla. Kuvio havainnollistaa myös, kuinka kaikkien menetelmien aikaansaama informaatiovaikutus heijastuu kaikilla kokonaisarkkitehtuurin tasoilla.



KUVIO 6 Vaikutusmenetelmät kokonaisarkkitehtuurissa

Elektroninen sodankäynti sijoittuu kaikkein selkeimmin kokonaisarkkitehtuurin teknologia-osa-alueeseen, koska siinä informaatiovaikutus toteutetaan sähkömagneettisen spektrin hyödyntämiseen tarkoitettujen teknologioiden avulla.

Fyysisten laitteiden ja komponenttien, kuten erilaisten sensorien tai tutkien, merkitys on voimakas elektroniseen sodankäyntiin perustuvassa vaikuttamisessa. (Hakala ym., 2011, 182–183). Erilaiset järjestelmät taas perustuvat näihin fyysisiin komponentteihin, joten vaikutus järjestelmätasolle on ilmeinen.

Tietoverkojen avulla taas yhdistetään fyysinen teknologia ja järjestelmät. Tietoverkko-operaatioiden vaikutus heijastuu siksi molemmille kokonaisarkkitehtuurin tasolle. (Kuusisto, 2014, 34). Tietoverkko-operaatioille on hyvin tyypillistä, että heijastusvaikutukset ovat merkityksellisemmät kuin suorat vaikutukset. Tämä johtaa siihen, että niiden kokonaisvaikutuksia on vaikea tarkasti arvioida etukäteen. (Illi ym., 2011, 162).

Tietotasolla vaikutetaan operaatioturvallisuuden ja sotilaallisen harhauttamisen keinoin. Molemmissa keskeistä on informaation oikeellisuus informaatioturvallisuus sekä se, kenen hallussa informaatio on. Operaatioturvallisuudessa tunnistetaan itselle kriittinen tieto ja pyritään suojaamaan sitä. Tämä johtaa vaikutukseen niin toiminta- kuin järjestelmätasolla, kun esimerkiksi henkilöstö lähettää salattuja sähköposteja tai kun kriittinen järjestelmä vaatii sisään kirjautumista.

Harhauttamisessa taas pyritään vaikuttamaan vastustajan päätöksentekoon harhaanjohtavan tiedon avulla. Tällöin virheellinen tieto johtaa muutoksiin vastustajan toiminnassa tai voi esimerkiksi heijastua järjestelmätasolla virheellisenä datana, joka vääristää vastustajan tilannekuvaa muodostavaa informaatiota. Psykologisten operaatioiden vaikutus on hyvin samankaltainen sotilaallisen harhauttamisen kanssa, mutta kuviossa on haluttu korostaa sen ihmiskeskeisyyttä. Psykologisten operaatioiden keinoin pyritään ennen kaikkea vaikuttamaan kohdeyleisön mielipiteeseen ja identiteettirakenteisiin. (Sirén, 2008 s. 199). Tällöin sen keskeisin vaikutus tapahtuu ensisijaisesti ihmisten mielissä.

4 JOHTOPÄÄKSET

Informaatio-operaatioiden yksiselitteinen määritteleminen ja tarkka rajaaminen on vaikeaa. Lähteestä ja määrittelevästä organisaatiosta riippuen painotuseroja on esimerkiksi informaatio-operaatioihin laskettavissa menetelmissä ja kineettisen vaikuttamisen roolissa. Tämä on luonnollista, koska sotilasorganisaatiot määrittelevät informaatio-operaatiot vastaamaan oman toimintansa tarpeita. Määritelmän muodostamista hankaloittaa myös se, että saatavilla oleva lähdemateriaali pohjaa pitkälti Yhdysvaltalaiseen tulkintaan asiasta - johon toki suomalainenkin näkemys pitkälti perustuu.

Tärkein informaatio-operaatioiden määritelmiä yhdistävä tekijä on näkökulma, jonka keskiössä on informaatio. Tämä on myös tärkein ero, kun tarkastellaan informaatio-operaatioiden suhdetta esimerkiksi kybersodankäyntiin. Informaatio-operaatioissa informaatio on sekä operaatioiden kohde, että vaikutusväline. Informaatiovaikutuksella tavoitellaan haluttuja muutoksia vastustajan toiminnassa ja vaikutetaan sekä omaan, että vastustajan tilannekuvaan. Informaatio-operaatiot kokoavat erilaisia menetelmiä, joilla nämä informaatiovaikutukset pyritään saavuttamaan. Näitä menetelmiä yhdistää se, että niissä korostuu ei-kineettinen vaikuttaminen.

Informaatioteknologian kehitys, tiedon määrän kasvu ja globalisaatio ovat aiheuttaneet sodankäynnin kuvan muutoksen, jossa perinteisten sodankäynnin ulottuvuuksien rinnalle (maa, meri, ilma ja avaruus) on noussut kyberulottuvuus. Tämä on nostanut informaationäkökulman rinnalle kyberajattelun, jossa informaatiota ja järjestelmiä tarkastellaan osana laajempaa kokonaisuutta. Joissain yhteyksissä kybersodankäynti on jopa osittain korvannut informaatiosodankäynnin.

Informaatio itsessään on kuitenkin olemassa ilman järjestelmiä ja informaatioteknologiaa. Napoleonilla ei ollut käytössään tietokoneita tai tietojärjestelmiä, joiden avulla hän sijoitteli joukkonsa Austerlitzin taistelussa. Silti nimenomaan oikeasta informaatiosta muodostettu tilannekuva vaikutti merkittävästi hänen menestykseensä. Tämä on keskeistä informaatio-operaatioissa ja tärkeää huomioida erityisesti kun keskustellaan siitä, onko informaatiokeskeinen ajattelu väistynyt kyberajattelun tieltä. Vaikka informaatioteknologian ke-

hitys on linkittänyt informaatio-operaatiot kybermaailmaan, on muistettava että informaatio-operaatiot ovat mahdollisia myös ilman sähköistä teknologiaa.

Kun medioissa puhutaan informaatio-operaatioista tai informaatiosodankäynnistä syntyy helposti kuva siitä, että olemme jatkuvasti jonkinlaisten informaatioon kohdistuvien operaatioiden kohteena. Tällainen totaalisen sodan ajatus on ollut erityisesti läsnä kyberajattelussa (Illi ym., 2011, 172). Informaatio-operaatiot kuitenkin nähdään liittyvän tiettyyn konfliktiin ja niiden taustalla on jokin sotilaallinen tavoite. Informaatio-operaatiot ovat prosessi, joka alkaa rauhasta ja jatkuu konfliktin kautta jälleen rauhaan. Erityisesti nykypäivän konflikteissa kuitenkin korostuu niiden epäsymmetrisyys ja ajallinen limittyneisyys, jolloin tarkan alku- ja loppuajankohdan määrittäminen on hankalaa – jopa mahdotonta. Tämä johtaa siihen, että myös informaatio-operaatioiden kohdalla on vaikea määritellä milloin ne alkavat ja milloin loppuvat, joten illuusio jatkuvasta informaatiosodasta voi syntyä.

Informaatio-operaatioiden keskeisimpiä tavoitteita on vastustajan tahtoon, tilannetietoisuuteen ja toimintakykyyn vaikuttaminen. Näiden kautta voidaan aiheuttaa toivottuja muutoksia vastustajan päätöksentekoon. Erityisesti oikean tilannekuvan ylläpito on nähty erittäin tärkeänä tekijänä menestyksekkäässä sodankäynnissä. Informaatio-operaatioiden vaikutukset tapahtuvat informaatioympäristössä, joka yhdistää fyysisen-, kognitiivisen- ja informaatioulottuvuuden. Informaatio-operaatioita voidaan käyttää myös siten, että vältytään varsinaiselta aseelliselta yhteenotolta. Tästä merkittävin esimerkki on Kylmä sota, jossa informaatio-operaatioiden käyttö oli ratkaisemassa asemassa: Sotilaallisessa mielessä välillä hyvinkin räjähdysaltis konflikti saatiin ratkaistua ilman kineettisen sodan syttymistä.

Informaatioympäristön lisäksi tutkielmassa tarkasteltiin informaatio-operaatioiden vaikutuksien syntymistä organisaation kokonaisarkkitehtuurin näkökulmasta. Tutkielmassa esiteltiin tarkemmin viisi keskeistä informaatio-operaatioiden vaikutusmenetelmää: elektroninen sodankäynti, operaatioturvallisuus, tietoverkko-operaatiot, psykologiset operaatiot ja sotilaallinen harhauttaminen. Näiden viiden menetelmän synnyttämät informaatiovaikutuksien kohdentuminen organisaation kokonaisarkkitehtuuriin kuvattiin kuviossa 6.

Kokonaisarkkitehtuuritarkastelusta voi havaita informaatio-operaatioiden vaikutuksien jakautuvan monipuolisesti jokaiselle kokonaisarkkitehtuurin osa-alueelle. Vaikutus ei myöskään rajoitu vain yhteen osa-alueeseen vaan toiminnasta syntyy aina heijastusvaikutusta myös muille arkkitehtuurin tasoille. Mitä laajemmin asiaa halutaan tarkastella, sitä pidemmälle heijastusvaikutukset voivat ulottua. On tärkeää myös muistaa, että kaikki heijastusvaikutukset eivät aina ole tarkoituksellisia ja tämä tulee ottaa huomioon informaatio-operaatioita suunniteltaessa.

Viisi tarkempaan esittelyyn valittua informaatio-operaatioiden menetelmää kuvaavat hyvin miten monipuolisesti informaatiovirtoihin voidaan vaikuttaa. Informaatio-operaatioiden keinoihin kuuluu toisaalta hyvin teknisiä menetelmiä, kuten tutkalaitteiden häirintä elektronisessa sodankäynnissä ja toisaalta hyvin voimakkaasti ihmismieliin suunnattua vaikuttamista, kuten erilaiset dis-

informaatiokampanjat sosiaalisessa mediassa. Tämä näkyy selvästi myös kokonaisarkkitehtuuritarkastelussa.

Tässä tutkielmassa kokonaisarkkitehtuurikehyksenä käytetään hyvin yksinkertaistettua mallia. Toisaalta tutkielmassa on osoitettu, että kokonaisarkkitehtuuritarkastelu on toimiva tapa havainnollistaa eri vaikutusmenetelmien kohdentumista organisaatioon. Tutkimusta voisi jatkaa yksityiskohtaisempien kokonaisarkkitehtuurikehyksien avulla ja tarkasteluun olisi syytä ottaa mukaan myös muita informaatio-operaatioiden vaikutusmenetelmiä kuin esitellyt viisi. Tulevaisuuden konfliktien käydessä entistä monimutkaisemmiksi voi yksityiskohtaisesta informaatiovaikutuksien kartoituksesta olla hyötyä. Sen avulla voidaan hahmottaa eri menetelmien käytön heijastusvaikutuksia ja kehittää sitä kautta omaa informaatio-operaatiotoimintaa – erityisesti puolustusta.

Millaista sodankäynti on 20 vuoden päästä? Sitä kukaan tuskin pystyy varmasti sanomaan. Mikäli teknologian kehitys jatkaa samaa vauhtia, on selvää, että kybermaailma ja sen tuomat haasteet sekä mahdollisuudet näyttelevät siinä tärkeää osaa. Kyberajattelussa ei kuitenkaan sovi unohtaa informaatiovaikutuksia ja – virtoja eri informaatioulottuvuuksien välillä. Informaatio on kaikkien päätösten, järjestelmien ja tilanteiden taustalla vaikuttava voima ja sen valjastaminen oman toiminnan tarpeisiin tulee jatkossakin ratkaisemaan konfliktien lopputuloksia. Informaatio-operaatiot monipuolisena sodankäynnin kokonaisuutena tuskin koskaan häviävät täysin sodankäynnistä.

LÄHTEET

Ahvenainen, S. (2014). Verkkosodan historia ja käsitteen kehittyminen - Kriittinen, systeeminen ja kyberneettinen katsaus vuoden 2003 artikkeliin. Teoksessa T. Kuusisto (toim.), *Kybertaistelu 2020* (s. 7-32). Helsinki: Maanpuolustuskorkeakoulu Taktiikan laitos.

Allen, P. (2007). *Information operations planning*. Norwood, MA: Artech House.

Armistead, L., States, U., & Joint Forces, S. C. (2004). Information operations: Warfare and the hard reality of soft power. (1. Painos). Washington, D.C.: Brassey's.

Departmen of Defence. (2015) The DoDAF Architecture Framework Version 2.02, Change 1. Haettu 16.3.2015 osoitteesta http://dodcio.defense.gov/TodayinCIO/DoDArchitectureFramework.aspx

Giachetti, R. E. (2010). Design of enterprise systems: Theory, architecture, and methods CRC Press.

Graves, T. (2009). *Enterprise architecture: A pocket guide*. Ely, Cambridgeshire, UK: IT Governance Pub.

Hakala, V., Harras, J., Kankare, V., Lehtoranta, T., Passinen, P. & Sipilä, P. (2011). Teoksessa T. Sirén (toim.), *Strateginen kommunikaatio ja Informaatio-operaatiot 2030* (s. 181–198). Helsinki: Maanpuolustuskorkeakoulu Johtamisen ja sotilaspedagogiikan laitos.

Heikkala, T., Källi, J. Majuri, P., Puuperä, S., Rissanen, T., Terämä, S., Toivanen, J. & Vaara, I. (2011). Operaatioturvallisuus 2030. Teoksessa T. Sirén (toim.), *Strateginen kommunikaatio ja Informaatio-operaatiot 2030* (s. 127–146). Helsinki: Maanpuolustuskorkeakoulu Johtamisen ja sotilaspedagogiikan laitos.

Hoffman, F. (2007). Conflict in the 21st century: The rise of the hybrid wars. Arlington: Potomac Institute for Policy Studies. Haettu 11.1.2015 osoitteesta http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Huhtinen, A., & Rantapelkonen, J. (2001). *Imagewars: Beyond the mask of information warfare*. Espoo: Marshal of Finland Mannerheim's War Studies Fund.

Illi, M., Karppinen, M., Palokangas, T. & Seppälä, P. Tietoverkko-operaatiot 2030. Teoksessa T. Sirén (toim.), *Strateginen kommunikaatio ja Informaatio-operaatiot 2030* (s. 161-180).

Jantunen, S. (2014), Itä, Länsi ja informaatiosodankäynti. *Kylkirauta,* 265(4), 25–27.

Joint Publication 3-13. (2012). Joint Publication 3-13: Information Operations. Haettu: 18.11.2014 osoitteesta http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Joint Publication 3-13.2. (2010). Joint Publication 3-13.2: Psychological Operations. Haettu 28.1.2015 osoitteesta http://fas.org/irp/doddir/dod/jp3-13-2.pdf

Järvinen, O., Mäntylä, V., Tainiola, M., Viinamäki, J. & Wahlstein, M. (2011). Stateginen ja operatiivinen harhauttaminen osana strategista kommunikaatiota – mennyttä ja tulevaisuuden pohdintaa. Teoksessa T. Sirén (toim.), *Strateginen kommunikaatio ja Informaatio-operaatiot 2030* (s. 111–121). Helsinki: Maanpuolustuskorkeakoulu Johtamisen ja sotilaspedagogiikan laitos.

Kaku, M. (2011). *Physics of the future: How science will shape human destiny and our daily lives by the year 2100*. New York: Anchor books

Kalliomaa, M. (2014). Informaatiosodan rintamalinjat. *Kylkirauta,* 265(4), 1.

Kangasmaa, T. (2014), Informaatio-operaatiot – isku keittiön kautta. *Kylkirauta*, 265(4), 29–31.

Kelley, O. (2010). Cyberspace domain: A warfighting substantiated operational environment imperative. Teoksessa A. Elsworth (toim.), *Electronic warfare* (s. 13 – 36). New York: Nova Science Publishers.

Korhonen, P. (2014), Sotaa sydämistä, mielestä ja sumutuksesta. *Kylkirauta,* 265(4), 21–23.

Kott, A. (2008). *Battle of cognition: The future information-rich warfare and the mind of the commander*. Westport, Conn: Praeger Security International.

Kuusisto, T. (2014). Tiedonhallinta päätöksenteossa kybertoimintaympäristössä. Teoksessa T. Kuusisto (toim.), *Kybertaistelu 2020* (s. 33-62). Helsinki: Maanpuolustuskorkeakoulu Taktiikan laitos.

Kärkkäinen, A. (2013). Computer network defence in military cognitive networks. Teoksessa J. Vankka (toim.), *Cyber warfare*. Helsinki: Maanpuolustuskorkeakoulu sotatekniikan laitos.

Lehto, M. (2014a). Kybertaistelun toimintaympäristön teoreettinen tarkastelu. Teoksessa T. Kuusisto (toim.), *Kybertaistelu 2020* (s. 67–86). Helsinki: Maanpuolustuskorkeakoulu Taktiikan laitos.

Lehto, M. (2014b). Kybertaistelu ilmavoimaympäristössä. Teoksessa T. Kuusisto (toim.), *Kybertaistelu 2020* (s. 157–177). Helsinki: Maanpuolustuskorkeakoulu Taktiikan laitos.

Lehto, M (2015).

NATO. (2009). *Allied joint doctrine for information operations*. Haettu 18.11.2014 osoitteesta https://info.publicintelligence.net/NATO-IO.pdf.

NATO. (2012). *NATO military policy on information operations.* Haettu 18.11.2014 osoitteesta https://info.publicintelligence.net/NATO-IO-Policy.pdf

Pulkkinen, M. (2006). Systemic management of architectural decisions in enterprise architecture planning. four dimensions and three abstraction levels. *System Sciences, 2006. HICSS '06. Proceedings of the 39th Annual Hawaii International Conference On, 8* 179a-179a.

Puolustusvoimat. (2012, 30. elokuuta). Erikoisjoukot toiminnassa. Haettu 12.1.2015 osoitteesta http://www.puolustusvoimat.fi/wcm/Erikoissivustot/NLBG2011/Suomeksi/tietoa+erikoisjoukoista/Erikoisjoukot+toiminnassa/

Puolustusvoimat. (2015). Sosiaalisessa mediassa toiminnan ohje varusmiehille ja reserviläisille. Haettu 13.1.2015 osoitteesta http://www.puolustusvoimat.fi/wcm/c8664380499bfe4b8790bf759929fd62/Varusmiehen+ja+reservil%C3%A4isen+some-ohje+esimerkkeineen.pdf?MOD=AJPERES

Rantapelkonen, J. (2014). Historiasta tulevaisuuteen - informaatiosodankäynnin paluu. *Kylkirauta*, 265(4), 15–18.

Schmidt, R., Wissotzki, M., Jugel, D., Mohring, M., Sandkuhl, K., & Zimmermann, A. (2014). Towards a framework for enterprise architecture analytics. *Enterprise Distributed Object Computing Conference Workshops and Demonstrations (EDOCW), 2014 IEEE 18th International,* 266-275.

Sirén, T. (2011). Psykologiset operaatiot osana informaatio-operaatioita 2030. Teoksessa T. Sirén (toim.), *Strateginen kommunikaatio ja Informaatio-operaatiot 2030* (s. 199–218). Helsinki: Maanpuolustuskorkeakoulu Johtamisen ja sotilaspedagogiikan laitos.

Sirén, T., Huhtinen, A. & Toivettula, M. (2011). Informaatiosodankäynnistä kokonaisvaltaiseen strategiseen kommunikaatioon. Teoksessa T. Sirén (toim.), *Strateginen kommunikaatio ja Informaatio-operaatiot 2030* (s. 3-22). Helsinki: Maanpuolustuskorkeakoulu Johtamisen ja sotilaspedagogiikan laitos.

The Open Group. (2011) TOGAF Version 9.1. Haettu 16.3.2015 osoitteesta http://pubs.opengroup.org/architecture/togaf9-doc/arch/

U.S. Army War College. (2011) *Information Operations Primer.* Pennsylvania: United States army war college and Carlisle barracks. Haettu 18.11.2014 osoitteesta http://www.au.af.mil/au/awc/awcgate/army-usawc/info_ops_primer.pdf

Urbaczewski, L. & Mrdalj, S. (2006). A comparison of enterprise architecture frameworks. *Issues in Information Systems*, 6(2), 18-23.

Vankka, J. (2014). Tietoverkkopuolustuksen haasteiden 2020 arviointi analyyttisellä hierarkiaprosessilla. Teoksessa T. Kuusisto (toim.), *Kybertaistelu 2020* (s. 104–117). Helsinki: Maanpuolustuskorkeakoulu Taktiikan laitos.

Veijalainen, J., Honkaranta, A., Hämäläinen, N., Kaijanaho, A., Kiviharju, M., Kurhinen, J., Kärkkäinen, K., Mazhelis, O., Pekkola, S. & Penttilä, J. (2008). Tietojenkäsittelyn kehittyminen ja tietoturvallisuus. Teoksessa M. Kari, A. Hakala, E. Pääkkönen & M. Pitkänen (toim.), *Sotatekninen arvio ja ennuste 2025 STAE 2025, osa1 Teknologian kehitys* (s. 529–563). Ylöjärvi: Puolustusvoimien Teknillinen Tutkimuslaitos.

Wilson, C. (2006). Information operations and cyberwar: Capabilities and related policy issues. Haettu 20.1.2015 osoitteesta http://fas.org/irp/crs/RL31787.pdf

Wirman, K. (2014). Verkkotaistelu yritysten näkökulmasta. Teoksessa T. Kuusisto (toim.), *Kybertaistelu 2020* (s.118–124). Helsinki: Maanpuolustuskorkeakoulu Taktiikan laitos.