MAANPUOLUSTUSKORKEAKOULU

VERKKOSODANKÄYNNIN PELITEOREETTINEN MALLINTAMINEN

Kandidaatintutkielma

Kadettiylikersantti
Mikko Palmén

Merikadettikurssi 79
Johtamisjärjestelmäopintosuunta

Huhtikuu 2012

MAANPUOLUSTUSKORKEAKOULU

Kurssi Merikadettikurssi 79	Linja Johtamisjärjestelmäopintosuunta
Tekijä Kadettiylikersantti Mikko Palmén	
Tutkielman nimi **VERKKOSODANKÄYNNIN PELITEOREETTINEN MALLINTAMINEN**	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Kurssikirjasto (MPKK:n kirjasto)
Aika 25.4.2012	Tekstisivuja 30 Liitesivuja 0

TIIVISTELMÄ

Verkkosodankäynti on informaatiosodankäynnin laji, jota käydään tietokoneiden ja viestintäverkkojen avulla. Viestintäverkkoihin ja niiden sisältämään informaatioon pyritään vaikuttamaan, tai niiden avulla pyritään vaikuttamaan vastustajaan. Peliteoria on matematiikan osa-alue, jonka avulla kahden tai useamman tahon välisiä päätöksenteko-ongelmia voidaan mallintaa eksaktisti. Verkkosodankäynti soveltuu pitkälti mallinnettavaksi kahden pelaajan pelinä, joten tutkielmassa ei ole syytä tarkastella useamman pelaajan pelejä. Tutkielmassa esitellään verkkosodankäyntiä ja peliteoriaa yleisesti. Tämän lisäksi esitellään malleja, joissa peliteoriaa on käytetty verkkosodankäynnin analysointiin. Tutkielmassa osoitetaan, että peliteorian avulla on mahdollista analysoida verkkosodankäynnin osa-alueita tietoteknistä lähestymistapaa täydentäen. Täten peliteoria monipuolistaa käsitystä verkkosodankäynnistä.

AVAINSANAT

Informaatiosodankäynti, verkkosodankäynti, matemaattinen mallintaminen, peliteoria.

VERKKOSODANKÄYNNIN PELITEOREETTINEN MALLINTAMINEN

1. JOHDANTO

1.1. Aihealueen esittely

Peliteoria on matemaattinen teoria, jonka avulla usean toimijan välisiä päätöksentekotilanteita pyritään luokittelemaan ja tarkastelemaan täsmällisesti. Tarkastelun avulla on mahdollista saavuttaa tuloksia, jotka voivat konkreettisesti ohjata toimintaa mallinnetuissa tilanteissa. Verkkosodankäynti on tietokoneisiin ja viestintäverkkoihin kohdistuvaa tai niiden avulla toteutettavaa sodankäyntiä [1, s. 16]. Verkkosodankäynnin merkitys kasvaa jatkuvasti sodankäynnin ja yhteiskunnan tietoverkkoriippuvaisuuden lisääntyessä [10, s. 52–53]. Verkkosodankäynnin tutkimus keskittyy teknisten järjestelmien tutkimukseen, jossa harvoin käytetään matemaattisia menetelmiä [13, s.1]. Järjestelmien ominaisuuksien tarkastelu ohittaa kuitenkin tärkeän osan verkkosodankäynnin kokonaisuudesta: toimijoiden päätöksenteon.

Peliteoria on lähestymistapa, jonka avulla päätöksentekoa on mahdollista tarkastella sekä kvalitatiivisesti että kvantitatiivisesti [14, s.2]. Näin ollen peliteoria mahdollistaa verkkosodankäynnin tarkastelun uudesta näkökulmasta. Samalla peliteoria voi tarjota vastauksia siihen, miten tietynlaisissa verkkosodankäynnin tilanteissa kannattaa toimia, eli tukea päätöksentekoa.

Tässä tutkielmassa esitän kirjallisuuteen perustuen miten verkkosodankäynnin menetelmiä ja tilanteita on mahdollista muotoilla peliteoreettisiksi malleiksi. Kyseessä on siis peliteorian

tukema verkkosodankäynnin kvalitatiivinen tarkastelu. Osoitan, että peliteoria toimii analyysityökaluna useissa erilaisissa tilanteissa ja tukee suunnittelua ja päätöksentekoa verkkosodankäyntiin liittyen.

1.2. Rajaukset ja tutkimuskysymykset

Tässä tutkielmassa tarkastelen verkkosodankäyntiä yhtenä informaatiosodankäynnin lajina perustuen Libickin jakoon [21, s. x], jonka esitän luvussa 3.1.1. Esitän verkkosodankäynnistä yleiskatsauksen, jonka jälkeen keskityn niihin menetelmiin ja tilanteisiin, joita esittelemissäni peliteoreettisissa malleissa tutkitaan.

Esitän yleiskatsauksen peliteoriasta matemaattisena mallinnusmenetelmänä. Esitän verkkosodankäynnin tutkimuksen kannalta keskeisiä pelien ominaisuuksia ilman formaalia matemaattista merkintätapaa. Käytän täsmällisiä peliteoreettisia käsitteitä ja menetelmiä, mutta analyysini kannalta mallien ominaisuuksien yksityiskohtainen todistaminen ei ole tarpeellista: esittelen malleja, joissa peliteoriaa on käytetty verkkosodankäynnin tutkimiseen keskittymättä siihen, miten nämä mallit on muodostettu.

Keskeinen tutkimuskysymys on: ”Miten peliteorian avulla voi mallintaa verkkosodankäynnin ilmiöitä?” Alakysymys on ”Mitä peliteoreettiset mallit voivat kertoa verkkosodankäynnistä?”

2. JOHDATUS PELITEORIAAN

Peliteoria on matemaattinen teoria, jonka avulla on mahdollista käsitellä usean toimijan välisiä päätöksentekotilanteita [7, s. xi]. Toisin sanoen kyse on työkalusta, jonka avulla usein hankalasti hahmotettavia, ristiriitaisia tilanteita pyritään luokittelemaan ja tarkastelemaan täsmällisesti. Peliteoria soveltuu erityisen hyvin kilpailutilanteissa, kuten sodankäynnissä ja talouselämässä, tapahtuvan päätöksenteon analysoimiseen.

Peliteoria on normatiivinen yritys kertoa miten eri tilanteissa kannattaa toimia [33]. Kyseessä ei ole deskriptiivinen teoria, joka pyrkisi kuvaamaan päätöksentekijöiden toimintaa todellisuudessa [23, s.63]. Peliteoria ei kuitenkaan ole absoluuttisesti normatiivinen, eli pyri kuvaamaan miten on välttämätöntä toimia, vaan ehdollisesti normatiivinen, eli kertoo miten on toimittava, jos haluaa päästä tietynlaiseen lopputulokseen [23, s.63].

Peliteoria keskittyy erityyppisten yleispätevien, eli ei tiettyyn tilanteeseen sidottujen, mallien muodostamiseen ja näiden mallien ominaisuuksien tarkasteluun [7, s. xii]. Itse teorian kannalta ei ole kiinnostavaa vastaako jokin malli todellista tilannetta, mutta mikäli tilannetta vastaava malli löytyy, voi teoria kertoa tilanteesta merkittäviä asioita.

Yksi peliteorian keskeisistä kysymyksistä liittyy siihen, mihin toimijat eli pelaajat pyrkivät. Muun muassa Suppes [33] tarkastelee tätä kysymystä peliteoriasta osittain erillisenä hyötyteoriana. Pelaaja voi esimerkiksi pyrkiä maksimoimaan oman voittonsa, minimoimaan häviönsä tai maksimoimaan vastustajan häviön. Pelaajat voivat pyrkiä joko samaan tulokseen, eli esimerkiksi molemmat maksimoimaan oman voittonsa, tai keskenään eri tuloksiin. Pelaajat saattavat myös pyrkiä parhaaseen yhteiseen tulokseen. Ei ole järkevää etsiä yksittäistä parasta tapaa pelata mitä tahansa peliä, muun muassa koska pelaajien pyrkimykset voivat poiketa toisistaan, vaihdella ja muuttua. Näin ollen peliteoria ei anna yksiselitteistä suositusta mihin tahansa tilanteeseen. Sen sijaan peliteoria käsittelee pelaajien strategioita, eli tiivistyksiä siitä, miten pelaajat pyrkivät tavoitteisiinsa.

Käyttämäni matemaattinen käsitteistö löytyy useista alan oppikirjoista, kuten Gibbonsilta [7] sekä Lucelta ja Raiffalta [23]. Luce ja Raiffa esittelevät peliteoriaa aksioomista lähtien, mutta myös havainnollisesti. Gibbonsin käsittely on aiempaa vähemmän formaali ja keskittyy sovelluksiin taloustieteen alalla.

2.1. Miksi peliteoriaa?

Kuten Luce ja Raiffa huomauttavat [23, s. 2], nimestään huolimatta peliteorian käyttökelpoisuus ei rajoitu esimerkiksi korttipeleihin tai uhkapeleihin. Peliteoriaa on käytetty monien eri alojen ongelmien mallintamiseen. Ensimmäisessä merkittävässä peliteoriaa käsitelleessä teoksessa [38] esitettiin teorian käyttökelpoisuutta mallintamalla toimijoiden käyttäytymistä talouteen liittyvissä tilanteissa. Peliteoriaa on käytetty taloustieteessä siitä lähtien useasti [7]. Toisena, sotatieteille erityisen merkityksellisenä, sovellusesimerkkinä mainittakoon tässä kansainvälinen politiikka [5] [4] [2]. Verkkosodankäynnissä on tunnistettavissa monta ominaisuutta, jotka sopivat yhteen peliteoreettisten mallien kanssa. Lähtökohtana on se, että verkkosodankäyntiä on luonteva hahmottaa kahden toisiaan vastustavan toimijan välisenä päätöksentekotilanteena.

Peliteoria ei ole ainoa sotatieteissä käytetty matemaattinen teoria. Lehtinen [20] perustelee matemaattisten menetelmien käyttöä lyhyesti: matemaattinen mallinnus eli matemaattisten menetelmien käyttö voi tuottaa erittäin luotettavaa tietoa, olettaen että mallinnus perustuu luotettaviin faktoihin [20, s. 6]. Eräs tunnetuimmista sotatieteissä käytettävistä malleista on Lanchesterin teoria [20, s. 4], jossa yksinkertaistamalla lähtökohtia pystytään laskemaan joukkojen kulumisnopeutta taistelussa. Matemaattisia menetelmiä on mahdollista käyttää tukemaan tilanteenarviointia ja päätöksentekoa silloin, kun tarkasteltava asia on onnistuttu mallintamaan hyvin.

Lehtisen [20, s. 6] mukaan todellisuus on useimmiten niin monimutkaista, että yksinkertaistuksia on pakko tehdä, jotta tilanteen analysointi on mahdollista. Tämä ei rajoitu ainoastaan matemaattiseen mallinnukseen, vaan pätee myös muunlaisessa tarkastelussa. Sama pätee myös peliteoriaa käytettäessä: on tehtävä yksinkertaistuksia, jotta käsittely ei olisi matemaattisesti liiallisen monimutkaista. Kuitenkin saatavat tulokset voivat olla todellisuuden kannalta suuntaa antavia ja jopa antaa suosituksia käytännön toiminnalle [20, s. 6]. Peliteorian avulla on mahdollista arvioida tilanteita ja muodostaa käsitys siitä, mikä toimintavaihtoehto kannattaa valita, eli tukea suunnittelua ja päätöksentekoa.

Morrow [25, s. 164–165] osoittaa miten peliteoriaa on käytetty sotateorioiden analysoimiseen ja arvioimiseen. Hänen mukaansa peliteoria on erinomainen työkalu sotateorioiden arvioimiseen, koska sen avulla on mahdollista tutkia teorioiden sisäistä logiikkaa. Peliteoria osoittaa sotateorioiden rajoituksia ja ohjaa siten teorioiden jatkokehittelyä [25, s. 190–191].

Peliteorialla on myös rajoituksensa. Teorian avulla ei pyritä eikä pystytä kuvaamaan reaalimaailman ilmiöitä pikkutarkasti ja yksityiskohtaisesti. Peliteoreettinen malli on aina yksinkertaistava, mikä saattaa johtaa siihen, että mallinnettavan asian keskeisiä ominaisuuksia jää huomioimatta [2, s. 42–43]. Peliteoreettiset mallit eivät myöskään aina pysty antamaan vastauksia siitä, mitä eri tilanteissa kannattaa tehdä. Jo Gödel [8] osoitti, etteivät yksinkertaisetkaan teoriat ole matemaattiset täydellisiä, eli ettei teorian kaikkia tosia lauseita voi todistaa. Intuitiivisesti on selvää, että peliteoreettiset mallit eivät myöskään voi antaa matemaattisia vastauksia kaikkiin tilanteisiin [33]. Toisaalta tämä voidaan nähdä myös peliteorian ansiona: peliteoria osoittaa omalla tavallaan, ettei ole olemassa yksinkertaisia sääntöjä, joita soveltamalla voisi selvitä optimaalisesti kaikista tilanteista.

2.2. Pelien keskeisiä ominaisuuksia

Tässä luvussa esittelen peliteorian (*Game Theory*) pelien keskeisiä ominaisuuksia. Tarkastelu ei ole formaalia, koska se ei ole välttämätöntä teorian käyttökelpoisuuden hahmottamiseksi. Formaali käsittely löytyy muun muassa von Neumannilta ja Morgensterniltä [38] sekä Lucelta ja Raiffalta [23]. Esitän englanninkielistä termistöä suluissa, koska suomenkielinen termistö ei ole täysin vakiintunutta ja alan kirjallisuus on suurelta osin englanninkielistä.

Peli (*Game*) on kolmen elementin muodostama kokonaisuus. Pelissä on oltava määriteltynä pelaajat (*Players*), pelaajien strategiat (*Strategies*) ja pelaajien valitsemista strategioista riippuvat tulokset (*Payoffs*) [7, s. 2–3]. Näiden kolmen elementin kautta määriteltyä peliä kutsutaan normaalimuotoiseksi peliksi (*Normal Form Game*) [7, s. 3].

Pelaajat ovat toimijoita, jotka tekevät pelin aikana valintoja (*Choices*) [38, s. 49]. Pelaajia voi pelissä olla yksi tai useampia. Yhden pelaajan peli voidaan nähdä melko yksinkertaisena optimointiongelmana, joka ohittaa teorian kiinnostavimman alueen eli useiden toimijoiden välisen vuorovaikutuksen [38, s. 85–87]. Verkkosodankäynti soveltuu pitkälti mallinnettavaksi kahden pelaajan pelinä, joten tässä yhteydessä ei ole syytä tarkastella useamman pelaajan pelejä.

Pelaajan strategia on sääntö, joka määrittää miten pelaaja toimii missä tahansa tilanteessa [7, s. 117]. Tämä ei tarkoita sitä, että pelaaja tekisi saman valinnan joka tilanteessa, vaan että pelaajalla on ratkaisu jokaiseen valintatilanteeseen, joka hänen eteensä voi pelissä tulla. Strategia määrittää näin ollen täysin sen, miten pelaaja pelissä toimii. Strategian käyttäminen yksinkertaistaa pelin yhdeksi ainoaksi päätöksentekotilanteeksi: pelaajan on ainoastaan valittava

käyttämänsä strategia [23, s.51–55]. Tämä ei kuitenkaan tarkoita sitä, että itse peli muuttuisi yksinkertaisemmaksi, strategia voi koostua tuhansiin eri valintatilanteisiin määritetyistä valinnoista.

Pelin lopputilanteet (*Outcomes*) voivat näyttää hyvin vaihtelevilta [23, s. 57]. Pelissä voi olla esimerkiksi seuraavat mahdolliset lopputilanteet: pelaaja A saa pelaajalta B viisi euroa tai pelaaja B saa pelaajalta A viisi euroa. Toinen esimerkki on peli, jossa on seuraavat lopputilanteet: pelaaja A (hyökkääjä) kaataa pelaajan B (puolustaja) tietokoneen, pelaaja B estää pelaajan A hyökkäyksen ja pelaaja A joutuu vankilaan, tai pelaajan A hyökkäys epäonnistuu ilman että sitä havaitaan. Pelin lopputilanteessa ei siis tarvitse olla selkeää voittajaa tai häviäjää.

Jokaisella pelaajalla on pelin lopputilanteiden suhteen paremmuusjärjestys: pelaajan on mahdollista sanoa, mikä on hänen mielestään pelin paras lopputilanne [23, s. 48]. Tätä paremmuusjärjestystä kuvataan yleensä numeraalisesti: jokaiselle pelaajalle määritetään jokaista lopputilannetta vastaava arvo, yleensä numeroarvo, jota kutsutaan tulokseksi (*Payoff*) [23, s. 48]. Viime kappaleen esimerkeistä ensimmäisessä on luontevaa tämä määrittää siten, että pelaajan A voittaessa A:n tulos on 5 ja B:n -5, kun taas B:n voittaessa A:n tulos on -5 ja B:n 5. Yhtä hyvin tulokset voisi kuitenkin määrittää siten, että B:n voittaessa A:n tulos on -5 mutta B:n 1, koska B on A:ta rikkaampi. Vaihtoehtoiset tulokset on esitetty taulukossa 1. Pelin tulos ymmärretään siis siten, että se riippuu sekä pelin lopputilanteesta että pelaajan suhtautumisesta tähän tilanteeseen.

	Vaihtoehto 1	Vaihtoehto 2
A voittaa 5€ B:ltä	A: 5, B: -5	A: 5, B: -5
B voittaa 5€ A:lta	A: -5, B: 5	A: -5, B: 1

Taulukko 1. Lopputilanne on sama, mutta tulokset eri.

Vankien dilemma on tyypillinen ja usein käytetty esimerkki yksinkertaisesta pelistä [7, s. 2–3] [23, s. 94–96]. Poliisi pidättää kaksi samasta rikoksesta epäiltyä, mutta todisteet eivät riitä tuomitsemaan kumpaakaan, ellei toinen epäillyistä tunnusta. Epäillyt pidetään erossa toisistaan, joten he eivät tiedä toistensa ratkaisuja etukäteen. Mikäli kumpikaan epäillyistä ei tunnusta, tuomitaan molemmat toisesta vähäpätöisestä rikoksesta. Jos vain yksi tunnustaa, vapautetaan hänet heti ja toinen tuomitaan ankarasti. Jos molemmat tunnustavat, tuomitaan molemmat lievästi. Näiden lopputilanteiden perusteella määritetään pelaajille taulukossa 2 esitetyt tulokset. Taulukkoa käytetään usein havainnollistamaan pelaajien valitsemien strategioi-

den suhde pelin tuloksiin. Tässä tapauksessa näemme taulukosta esimerkiksi, että mikäli molemmat pelaajat tunnustavat, on pelin tulos pelaajalle A -4 ja mikäli molemmat vaikenevat, on pelin tulos pelaajalle B -1.

	A tunnustaa	A vaikenee
B tunnustaa	A: -4, B: -4	A: -6, B: 0
B vaikenee	A: 0, B: -6	A: -1, B: -1

Taulukko 2. Vankien dilemma.

Peliteoriassa pelaajan oletetaan yleensä toimivan siten, että hän pyrkii maksimoimaan oman tuloksensa. Näin toimivaa pelaajaa kutsutaan rationaaliseksi (*Rational*) [23, s. 49–51]. Koska pelin tulos jo sisältää pelaajan suhtautumisen tulokseen, on rationaalisuuden olettaminen hyvin perusteltua. Irrationaalinen pelaaja toimii omia preferenssejään vastaan. Irrationaalisten (*Irrational*) pelaajien pelejä ei ole tarvetta tarkastella enempää tässä yhteydessä, koska niitä käytetään luvun 3 verkkosodankäynnin tarkastelussa vain ohimennen.

Vankien dilemmassa molemmat pelaajat pyrkivät maksimoimaan oman tuloksensa. Jos A tunnustaa, kannattaa myös B:n tunnustaa, koska B saa silloin paremman tuloksen. Jos taas A ei tunnusta, kannattaa B:n jälleen tunnustaa. Sama päättely pätee A:n osalta. Näin ollen vaikeneminen ei kummankaan pelaajan kohdalla ole kannattava strategia. Vaikenemista kutsutaan tässä tilanteessa dominoiduksi strategiaksi (*Dominated Strategy*). Rationaalinen pelaaja ei missään tilanteessa valitse dominoituja strategioita [7, s. 5]. Kuitenkin intuitiivisesti vaikuttaa siltä, että molempien epäiltyjen kannattaisi vaieta, koska näin saavutettaisiin parempi tulos.

Peliteoreettinen rationaalisuus ei suoraan vastaa sitä, mitä yleiskielellä voimme kutsua järkeväksi toiminnaksi, kuten Vankien dilemma osoittaa. Esimerkiksi lottokupongin ostajan toiminta voi voittamisen todennäköisyyden huomioon ottaen vaikuttaa järjenvastaiselta, mutta mikäli hänen toimintansa mallinnetaan peliksi, on pelin tulosta määritettäessä otettava huomioon se, että pelaaja suhtautuu erittäin positiivisesti siihen jännitykseen, joka arvontaan liittyy. Näin ollen toiminta voi olla peliteoreettisessa mielessä rationaalista, vaikka voittamisen todennäköisyys olisi häviävän pieni.

Kun pelaajien oletetaan olevan rationaalisia, voi vaikuttaa siltä, että peliteoria yksinkertaistaa tilanteita niin paljon, ettei mallinnuksesta enää ole hyötyä: pelin lopputulos ratkeaa katsomalla

pelaajien mahdollisia tuloksia ja pelaaja voi päättää käyttämänsä strategian tutkimalla vastustajan tuloksia. On kuitenkin muistettava, että pelin tulos sisältää jo pelaajien suhtautumisen lopputilanteisiin. Vaikka pelaaja tietäisi pelin lopputilanteet, ei hän välttämättä tiedä vastustajan suhtautumista niihin, eli tunne pelin tuloksia [7, s. 143].

Täyden informaation (*Complete Information*) pelissä pelaajat tietävät kaikkien pelaajien tulokset [7, s. 143]. Tämä sisältää tiedon siitä, mihin tulokseen tiettyjen strategioiden valinnat johtavat. Vankien dilemma on täyden informaation peli: molemmille epäillyille kerrotaan minkälaisiin tuloksiin heidän valintansa johtavat, eli he tietävät kaiken sen, mitä kuva 2 kertoo. Huomionarvoista on se, että tämä sisältää toisen epäillyn suhtautumiseen lopputilanteisiin.

Vajaan informaation (*Incomplete Information*) pelissä tulokset eivät ole kaikkien tiedossa [23, s. 143]. Esimerkkinä tästä on salaisin tarjouksin pidettävä huutokauppa: jokainen pelaaja tietää, minkä arvoiseksi itse arvioi myytävän esineen, mutta ei tiedä muiden arviointeja. Toinen esimerkki on tilanne, jossa hakkeriryhmä uhkaa kaataa koko Internetin, ellei hallitus maksa sille miljoonaa euroa [Gib, s.55–56]. Koska hallitus tarvitsee Internetiä omaan toimintaansa, kannattaa sen maksaa lunnaat, jos se uskoo hakkeriryhmän olevan tosissaan. Toisaalta hallitus tietää myös hakkereiden tarvitsevan Internetiä omaan toimintaansa, joten hallitus ei voi olla varma siitä, toteuttaako ryhmä uhkauksensa.

Staattisessa (*Static*) pelissä kaikki pelaajat tekevät päätöksensä samaan aikaan, eli eivät tiedä muiden pelaajien valintoja [7, s. 1]. Vankien dilemma on staattinen peli: epäilyt joutuvat tekemään valintansa tietämättä mitä toinen pelaaja on valinnut. Dynaamisessa (*Dynamic*) pelissä puolestaan yksi pelaaja tekee valinnan ensin, minkä jälkeen toinen pelaaja tekee oman valintansa. Yksinkertainen esimerkki tästä on tilanne, jossa puolustaja A valitsee itselleen tietoturvaohjelmistoa ja hyökkääjä B valitsee hyökkäykseensä virusta. Ohjelmisto 1 torjuu viruksen X mutta ei virusta Y, kun taas ohjelmisto 2 torjuu viruksen Y mutta ei virusta X. Tulokset on esitetty taulukossa 3.

	A valitsee ohjelmiston 1	A valitsee ohjelmiston 2
B valitsee viruksen X	A: 1, B: -1	A: -3, B: 3
B valitsee viruksen Y	A: -2, B: 2	A: 0, B: -1

Taulukko 3. Ohjelmiston ja viruksen valinta.

Jos kuvan 3 peli on staattinen, voidaan intuitiivisesti todeta, että pelaajan B kannattaa valita virus X, koska silloin hänellä on mahdollisuus saada parempi tulos (3) kuin viruksella Y (enintään 2). Dynaamisessa pelissä puolestaan tilanne muuttuu: jos B tekee valintansa vasta A:n valinnan jälkeen, eli tietää etukäteen mitä ohjelmistoa A käyttää, pystyy B aina valitsemaan tilanteeseen sopivamman viruksen. Jos puolestaan B valitsee viruksensa ensin, on A:n taas helppo maksimoida oma tuloksensa. Pelaajien siirtojärjestyksellä on siis suuri merkitys pelaajien strategioiden kannalta. Koska siirtojärjestyksen muuttuminen tarkoittaa sitä, että pelin säännöt muuttuvat, on kyseessä peliteorian kannalta eri peli kuin alkuperäisessä tilanteessa.

Edellisessä dynaamisen pelin esimerkissä oletettiin, että pelaaja B tiesi A:n tekemän valinnan ennen omaa valintaansa. Peliä, jossa vuorossa olevalla pelaajalle on tieto kaikkien pelaajien kaikista aikaisemmin tekemistä siirroista, kutsutaan täydellisen informaation (*Perfect Information*) peliksi [7, s. 55]. Jos puolestaan pelin aikana tulee vastaan tilanne, jossa pelaaja valintavuorossa ollessaan ei tiedä kaikkia edeltäviä siirtoja, on kyseessä epätäydellisen informaation (*Imperfect Information*) peli [7, s. 55, 72]. Mikäli äskeisen esimerkin pelissä vallitsisi epätäydellinen informaatio, vastaisi se siis käytännössä staattista peliä, koska pelaajaan B ei mitenkään vaikuttaisi se, että hän tekee valintansa pelaajan A jälkeen. Dynaaminen peli voi rakentua staattisen pelin toistamisesta: pelaajat tekevät valintansa ja saavat tuloksensa, minkä jälkeen peli toistetaan. Pelaajat voivat näin ollen seurata sitä, miten vastustaja tekee valintojaan [7, s. 82–83] [23, s. 97].

Nollasummapeli (*Zero-Sum Game*) on peli, jossa pelaajien tulosten summa on nolla, eli jossa pelaaja A voittaa aina yhtä paljon kuin B häviää ja toisin päin [23, s. 63–64]. Tarkastellaan kahden pelaajan nollasummapeliä, jossa pelaaja A on rationaalinen. Tässä tapauksessa pelaajan B irrationaalisuus ei haittaa pelaajaa A mitenkään: jos vastustaja pelaa irrationaalisesti, eli valitsee muun kuin oman tuloksensa maksimoivan strategian, aiheuttaa hän itselleen alkuperäistä huonomman tilanteen. Tämä tarkoittaa nollasummaominaisuuden nojalla sitä, että pelaajan A tilanne paranee [38, s. 128]. Pelaajan A kannattaa tässä pelata samoin kuin rationaalista vastustajaa vastaan. Pelaajan irrationaalisuus ei siis välttämättä tarkoita sitä, ettei peliteorialla olisi mitään sanottavaa tilanteesta.

Vankien dilemman yhteydessä tarkasteltiin tilannetta, jossa molempien pelaajien kannatti valita tunnustaminen. Strategiapari on sellainen, ettei kummankaan pelaajan kannata vaihtaa strategiaansa, mikäli vastustajan tiedetään valitsevan tämä strategia. Tällaista strategiaparia

kutsutaan Nashin tasapainoksi (*Nash Equilibrium*) [7, s. 8]. Nashin tasapaino on merkittävästi yleisempi tulos kuin dominoitu strategia, eli tasapainoja löytyy myös monista peleistä, joissa dominoituja strategioita ei ole [7, s. 2]. Tästä syystä Nashin tasapainoa voi käyttää analyysin välineenä monenlaisissa tilanteissa.

Tarkastellaan tunnettua 1950-luvulta peräisin olevaa esimerkkiä, jota kutsutaan Sukupuolien taisteluksi [23, s. 90–91] [7, s. 11–12]. Kyseessä on staattinen kahden pelaajan täyden informaation peli. Pariskunta on valitsemassa iltamenoa. Pelaaja A, perinteisesti nainen, haluaa mennä oopperaan. Pelaaja B, perinteisesti mies, haluaa puolestaan nyrkkeilyotteluun. Kuitenkin molemmille on tärkeämpää mennä jonnekin yhdessä kuin kukin taholleen. Tulokset on esitetty taulukossa 4.

	A menee oopperaan	A menee otteluun
B menee oopperaan	A: 2, B: 1	A: -1, B: -1
B menee otteluun	A: -1, B: -1	A: 1, B: 2

Taulukko 4. Sukupuolten taistelu.

Sukupuolten taistelussa ei ole dominoituja strategioita. Nashin tasapainoja sen sijaan ovat molemmat tilanteet, joissa kummatkin pelaajat tekevät saman valinnan. Jos A menee oopperaan, ei B:n kannata vaihtaa strategiaansa otteluun menoksi. Vastaava pätee sekä A:n osalta, että otteluun menon osalta. Pelissä on kaksi erillistä Nashin tasapainoa. Tässä tapauksessa ei siis saada selkeää suositusta siitä, miten peliä kannattaa pelata, elleivät pelaajat voi keskustella keskenään ennen päätöksentekoa.

Toistaiseksi tarkastelluissa esimerkeissä pelaajat ovat tehneet päätöksensä keskustelematta toistensa kanssa. Tällaisia pelejä kutsutaan ei-yhteistyöpeleiksi (*Non-Cooperative Game*) [23, s. 114]. Yhteistyöpelissä (*Cooperative Game*) pelaajilla on mahdollisuus keskustella ennen pelin alkua ja tehdä sitovia sopimuksia käytettävistä strategioista [23, s. 114–120]. Tämä ei tarkoita sitä, että pelaajat esimerkiksi laskisivat korkeimman yhteisen tuloksensa ja jakaisivat sen sitten tasan keskenään. Tulos ei välttämättä ole mitään konkreettista, jota olisi mahdollista jakaa. Yhteistyöpeli ei myöskään edellytä sitä, että pelaajat jossain mielessä suhtautuisivat toisiinsa ei-yhteistyöpeliä positiivisemmin.

Tarkastellaan jälleen Sukupuolten taistelua, nyt yhteistyöpelinä. Pelaaja A ilmoittaa aikovansa mennä oopperaan siitä riippumatta, mitä pelaaja B tekee. Jos pelaaja B uskoo A:n väitteeseen,

kannattaa hänen nyt valita ooppera [23, s. 91]. Pelaajalla B ei kuitenkaan välttämättä ole mitään syytä uskoa tähän väitteeseen. Tarkastellaan seuraavaksi samaa esimerkkiä toistettuna dynaamisena pelinä, eli pelinä, jossa sama valinta tehdään useaan kertaan. Pelaaja A ilmoittaa jälleen aikovansa valita oopperan riippumatta pelaajan B valinnasta. Pelaaja B voi nyt arvioida pelaajan A uskottavuutta myöhemmissä toistoissa sen perusteella, mitä pelaaja A valitsee. Uskottavuus on tärkeä ominaisuus dynaamisia pelejä käsiteltäessä [7, s. 55].

Pelaajan epävarmuutta vastustajansa toiminnasta esitetään peliteoriassa usein yhdistetyn strategian (*Mixed Strategy*) avulla [23, s. 70–71] [7, s. 30–31]. Yhdistetty strategia liittää pelaajan eri strategioihin todennäköisyydet sille, että kyseinen strategia valitaan. Yhdistetyn strategian avulla voidaan tutkia tilanteita, joissa pelaajan ei aina kannata valita samaa strategiaa, koska vastustaja pystyisi ajan myötä reagoimaan tähän pelityyliin. Sen sijaan eri strategioiden todennäköisyyksiä voi käyttää ohjaamaan sitä, kuinka usein valittua strategiaa tulisi vaihtaa.

Tähän mennessä esitellyn peliteorian yhteydessä ei vielä ole tuotu esiin konkreettisia verkkosodankäyntiin liittyviä sovelluksia. Pelien ominaisuuksia on käsitelty siinä laajuudessa, että seuraavan luvun verkkosodankäynnin tarkastelun yhteydessä on mahdollista esittää useita erilaisia peliteoreettisia mallinnuksia verkkosodankäynnin tilanteista ja menetelmistä.

3. VERKKOSODANKÄYNTI

Tässä luvussa esittelen verkkosodankäynnin piirteitä ja osoitan, miten verkkosodankäyntiä on mahdollista mallintaa peliteorian avulla. Ensimmäisessä alaluvussa esittelen informaatiosodankäyntiä ja sen jakoa alalajeihin, jotta verkkosodankäynti on mahdollista liittää laajempaan kokonaisuuteen. Toisessa alaluvussa esittelen viestintäverkkoihin liittyviä termejä, jotka ovat verkkosodankäynnin kannalta keskeisiä. Kolmannessa alaluvussa tarkastelen verkkosodankäynnin eri menetelmiä ja esittelen peliteoreettisia malleja, joita on käytetty verkkosodankäynnin mallintamiseen.

3.1. Informaatiosodankäynti

Candolinin [6, s. 9] mukaan informaation käyttö sodankäynnissä ei ole uusi keksintö: kautta aikain on muun muassa vastustajasta kerätty tiedustelutietoa ja vastustajan päätöksentekoon pyritty vaikuttamaan informaation avulla. Candolin toteaa nykyteknologian kuitenkin muuttavan informaation roolia sodankäynnissä: informaatio ei rajoitu pelkäksi tiedustelutiedoksi, vaan informaatiota voidaan entistä enemmän käyttää hyökkäyksen välineenä ja informaatioon on mahdollista kohdistaa entistä merkittävämpiä hyökkäyksiä. Maailmanlaajuisen uutisvirran ja lähes viiveettömän yhteydenpidon ansiosta kansainvälisen yhteisön ja yleisen kansalaismielipiteen vaikutukset konflikteihin ovat lisääntyneet merkittävästi. Myös käsitykset sodasta ovat muokkaantuneet teknologisen kehityksen myötä informaatiota korostaviksi [29, s. 24–29].

Viestintäteknologia on nyky-yhteiskunnalle kriittinen komponentti [9, s. 9] ja edellytys sille, että informaatiota pystytään käsittelemään ja välittämään laajamittaisen informaatiosodankäynnin vaatimassa laajuudessa. Erityisesti viestintäteknologia on välttämätön edellytys verkkosodankäynnille. Informaatiosota ei kuitenkaan tarkoita sotaa, jossa pyritään ainoastaan tuhoamaan vastustajan informaatioteknologiaa. Tarkoitus on vaikuttaa vastustajan käsityksiin, päätöksentekoon ja mielipiteisiin, ei teknisiin järjestelmiin [9, s. 10–11].

Sekä Candolin [6, s. 9–12] että Jormakka ja Mölsä [18, s. 12] [13, s. 28] korostavat informaatiosodankäynnissä päätöksentekoon vaikuttamisen merkitystä. Heidän mukaansa yksi informaatiosodankäynnin keskeisistä tavoitteista on oman päätöksentekosyklin nopeuttaminen ja vastustajan päätöksentekosyklin hidastaminen. Candolin ja Jormakka kuvaavat päätöksentekosykliä Boydin [3, s. 4] OODA-silmukan avulla. OODA-silmukka on malli, joka esittää päätöksenteon nelivaiheisena prosessina. Ensimmäisessä vaiheessa (*Observation*) ympäristöstä ja

tilanteesta kerätään dataa. Toisessa vaiheessa (*Orientation*) kerätty data liitetään osaksi aiempaa tietoa ja kontekstia. Kolmannessa vaiheessa (*Decision*) tiedon perusteella muodostetaan vaihtoehtoisia toimintamalleja ja tehdään päätös yhden käyttämisestä. Neljännessä vaiheessa (*Action*) päätös pannaan toimeen, minkä jälkeen silmukka alkaa alusta.

Hutchinsonin ja Warrenin [11, s. 1] määritelmässä edellä esitetty tiivistyy seuraavaan muotoon: informaatio on informaatiosodankäynnissä sekä pääasiallinen ase että kohde ja tavoitteena on informaatioylivoiman saavuttaminen. Heiskanen [9, s. 28] muotoilee informaatiosodankäynnin tavoitteen seuraavasti: pyritään vaikuttamaan ihmiseen verkoston osana siten, että koko verkoston toimintakyky lamautuu. Informaatiosodankäynnillä pyritään Candolinin [6, s. 9–12], Jormakan ja Mölsän [18, s. 12] [13, s. 28] mukaan edistämään omaa päätöksentekosykliä ja hidastamaan vihollisen vastaavaa sykliä siten, että oma päätöksentekotahti on vihollista nopeampaa. Tämä on yksi tapa ymmärtää Hutchinsonin ja Warrenin [11, s. 1] käyttämää termiä informaatioylivoima: suojataan oma päätöksentekokyky ja lamautetaan vastustajan toimintakyky syöttämällä väärää informaatiota ja estämällä oikean informaation käyttö.

3.1.1. Informaatiosodankäynnin alalajit

Libicki [21, s. x] jakaa informaatiosodankäynnin seitsemään lajiin, joita Ahvenainen [2, s. 16], Candolin [6, s. 12–13] ja Heiskanen [9, s. 14–15] kuvailevat tarkemmin. Candolinin mukaan Libickin jako alkaa olla vanhentunut, mutta kuvaa silti hyvin informaatiosodankäynnin keskeisiä piirteitä. Kuten Ahvenainen tekee [2, s. 32], voidaan informaatiosodankäynti jakaa myös muilla tavoin, eikä Libickin lajeja tule käsittää täysin erillisiksi kokonaisuuksiksi.

Libickin mukaan johtamissodankäynti on informaatiosodankäynnin sotilaallinen osa-alue [21, s. 9]. Se kattaa asevoimien avulla toteutettavat sotatoimet, kuten psykologiset operaatiot, fyysisen tuhoamisen ja elektronisen sodankäynnin [2, s. 16]. Tiedusteluperusteinen sodankäynti tarkoittaa sensoreiden ja sensoritietoa käsittelevien tietokoneiden yhdistämistä yhdeksi järjestelmäksi, jonka avulla voidaan tiedustelutietoa käyttää tehokkaasti valvontaan ja asevaikutukseen [2, s. 16]. Libicki toteaa lisäksi, että tiedusteluperusteisessa sodankäynnissä on mahdollista ohittaa johtamistasoja ja käyttää sensoridataa suoraan asejärjestelmillä vaikuttamiseen [21, s. 19].

Elektroninen sodankäynti käsittää kaikkien elektromagneettista säteilyä käyttävien laitteiden tiedustelun, niihin vaikuttamisen ja vaikuttamiselta suojautumisen [2, s. 16]. Libicki erottelee varsinaisen elektronisen sodankäynnin, jolla pyritään estämään elektromagneettisen spektrin

hyödyntäminen, ja salaussodankäynnin, jossa pyritään murtamaan vastustajan käyttämät salausmenetelmät [21, s. 27]. Psykologiset operaatiot pyrkivät vaikuttamaan muun muassa ihmisten mielipiteisiin, arvoihin, päätöksentekoon ja käyttäytymiseen [9, s. 14]. Näillä voidaan pyrkiä esimerkiksi oman kansan tai joukkojen taistelutahdon parantamiseen ja vastaavasti vastustajan heikentämiseen [21, s. 35].

Hakkerisodankäynti on tietokoneisiin ja viestintäverkkoihin kohdistuvaa tai niiden avulla toteutettavaa sodankäyntiä [21, s. 49–50]. Viestintäverkkoihin tai niiden sisältämään informaatioon pyritään vaikuttamaan, tai niiden kautta pyritään vaikuttamaan viholliseen. Taloudellisessa informaatiosodankäynnissä informaatiota käytetään taloudelliseen vaikuttamiseen esimerkiksi estämällä pääsy kansainvälisiin pankkijärjestelmiin [21, s. 64] tai talousvakoilulla [9, s. 15]. Kybersodankäynti on täysin viestintäverkoissa käytävää sotaa [9, s. 15]. Sitä voivat käydä tietokoneohjelmat itsenäisesti riippumatta ulkoisista käyttäjistä, eikä sen täydy vaikuttaa suoraan ulkomaailmaan [2, s. 17].

Informaatiosodankäynnin sotatoimet voivat liittyä useaan Libickin lajiin [19, s. 264]. Esimerkiksi tietokoneiden fyysinen tuhoaminen liittyy sekä johtamissodankäyntiin että verkkosodankäyntiin, ja väärän sensoritiedon syöttäminen viestintäverkkoon voi liittyä psykologisiin operaatioihin, vastustajan tiedusteluperusteiseen sodankäyntiin ja verkkosodankäyntiin.

Käytän tässä tutkimuksessa Puolustushallinnon asiasanaston [27] mukaista termiä verkkosodankäynti vastaamaan Libickin [21, s. 49] hakkerisodankäyntiä. Ahvenainen [2, s. 32] käyttää samasta asiasta termiä tietokoneverkkosodankäynti. Ahvenaisen termit verkkosodankäynti ja verkkosota puolestaan tarkoittavat eri asiaa kuin tässä tutkimuksessa. Lukin [24, s. 9] käyttää termejä tietoverkkosodankäynti sekä virus- ja ohjelmistosodankäynti kuvaamaan samaa asiaa. Heiskanen käyttää verkkosodankäyntiä lähes samoin kuin sitä käytetään tässä tutkimuksessa [9, s. 13], mutta ei rinnasta sitä suoraan Libickin hakkerisodankäyntiin [9, s. 21]. Ristiin menevät ja päällekkäiset termit kertovat siitä, ettei kansainvälisesti hyväksyttyä standardia terminologiasta ole onnistuttu muodostamaan.

3.1.2. Esimerkki peliteoreettisesta mallista

Jormakka ja Mölsä [18, s. 15–18] mallintavat informaatiosodankäyntiä peliteorian avulla. He muotoilevat terroristipelin, joka on kahden rationaalisen pelaajan staattinen täyden informaation peli. Pelaaja A, terroristi, on kaapannut panttivankeja ja uhkaa räjäyttää vangit ja itsensä ilmaan. Pelaaja B, hallitus, vaatii terroristin antautumista. Molemmat pelaajat voivat joko

suostua vaatimuksiin tai olla suostumatta. Jos molemmat suostuvat, hallitus antaa periksi terroristin vaatimuksille ja kärsii arvovaltatappion, mutta panttivangit pelastuvat ja terroristi joutuu antauduttuaan vankilaan. Jos kumpikaan ei suostu, räjäyttää terroristi itsensä ja panttivangit. Jos hallitus suostuu mutta terroristi ei, pääsee terroristi vapaana karkuun mutta panttivangit selviävät. Jos terroristi suostuu mutta hallitus ei, joutuu terroristi vankilaan saavuttamatta tavoitteitaan. Pelin tulokset on esitetty taulukossa 5.

	Hallitus A suostuu	Hallitus A ei suostu
Terroristi B suostuu	A: -1, B: -1	A: 0, B: -5
Terroristi B ei suostu	A: -5, B: 1	A: -10, B: -10

Taulukko 5. Terroristipeli.

Jormakka ja Mölsä [18, s. 16–18] osoittavat, että mikäli peliä toistetaan ja hallitus ei missään vaiheessa suostu vaatimuksiin, on terroristin ajan myötä ruvettava suostumaan vaatimuksiin minimoidakseen omat tappionsa, mikäli terroristi pelaa rationaalisesti. Tässä tilanteessa hallitus voi siis päästä dominoivaan asemaan, jossa rationaalinen terroristi aina häviää. Dominoiva asema ei kuitenkaan todellisuudessa ole pysyvä: alistumisen hinta terroristille kasvaa ja muuttaa vähitellen eri lopputilanteiden tulosta siten, että kieltäytyminen voi muuttua paremmaksi strategiaksi [18, s. 18]. Näin ollen dominoivan strategian käyttö ei tarkoita sitä, että kriisien syttyminen voitaisiin ehkäistä.

Terroristipelin jatkoksi Jormakka ja Mölsä [18, s. 21–23] muotoilevat kapinallispelin, jossa liian voimakkaan dominoivan strategian käyttö johtaa kapinan syttymiseen. Tässä tilanteessa osoitetaan, että dominoivan pelaajan kannalta on edullisempaa pelata yksittäiset valintatilanteet ajoittain epärationaalisesti. Tällöin dominoidun osapuolen hinta ei kasva kestämättömäksi, eikä kapinaa syty.

3.2. Viestintäverkkojen terminologiaa

Verkkosodankäynti on tietokoneisiin ja viestintäverkkoihin kohdistuvaa tai niiden avulla toteutettavaa sodankäyntiä. Viestintäverkkoihin tai niiden sisältämään informaatioon pyritään vaikuttamaan, tai niiden kautta pyritään vaikuttamaan viholliseen [2, s. 16]. Viestintäverkko on järjestelmä, joka koostuu laitteista ja niitä yhdistävistä viestinsiirtotavoista eli siirtoteistä [36, s. 28]. Viestintäverkkoja ovat esimerkiksi Internet, GSM-matkapuhelinjärjestelmä ja

Suomen viranomaisradioverkko VIRVE. Ennen verkkosodankäynnin käsittelyä esittelen verkkosodankäynnin kannalta keskeistä viestintäverkkoihin liittyvää terminologiaa.

Viestintäverkko koostuu solmuista ja siirtoteistä [36, s. 28]. Solmu on viestintäverkossa kiinni oleva tietoliikennelaite [36, s. 27]. Solmut voivat olla esimerkiksi palvelintietokoneita, kotitietokoneita, älypuhelimia, radiolaitteita tai sensoreita. Siirtotie on menetelmä, jolla dataa siirretään laitteesta toiseen [36, s. 27]. Siirtotiet perustuvat joko johtimien tai optisten kuitujen käyttöön, tai sähkömagneettisen aallon vapaaseen etenemiseen.

Protokolla määrittää ne toiminnot, joiden mukaan laitteet siirtävät tietoa välillään ja sisältää yhteyden avaamisen, tiedonsiirron ja yhteyden purkamisen [36, s. 26]. Toisin sanoen se on sääntö, jonka mukaan kaksi osapuolta keskustelee keskenään [34, s. 27]. Protokolla määrittää sanomien rakenteen, käsittelyn ja niihin vastaamisen [36, s. 26]. Protokollat määrittävät sen, miten viestintä teknisesti toteutetaan viestintäverkoissa.

Transmission Control Protocol / Internet Protocol -malli eli TCP/IP-malli on viestintäverkkomalli, joka kuvaa Internetin ja muiden IP-protokollaan perustuvien viestintäverkkojen toimintaa. Internet Protocol eli IP-protokolla on erittäin yleinen pakettikytkentäinen protokolla, jonka käyttöön perustuu muun muassa Internet [34, s. 432] [36, s. 24]. IP-protokollaa käytetään laajalti myös sotilasverkoissa [6, s. 18]. Paketti on tietoyksikkö, joka sisältää vastaanottajan osoitetiedon, varsinaisen sisällön sekä mahdollisia muita tietoja, kuten esimerkiksi lähettäjän osoitteen ja virheentarkistustiedon [34, s. 15] [36, s.25]. Pakettikytkentäisessä tiedonsiirtoverkossa suuremmat tietokokonaisuudet jaetaan määrämuotoisten pakettien sisään ja nämä paketit välitetään erillisinä osoitetietojen mukaan vastaanottajalle [36, s. 25].

Protokollataso [34, s.26–28] kuvaa useissa viestintäverkkomalleissa eri protokollien välistä hierarkiaa. Alemman tason protokolla luo tietyn palvelun ylemmän tason protokollalle. Esimerkiksi TCP/IP-mallissa IP-protokolla luo ylemmille protokollatasoille reitityspalvelun, joten ylempien protokollien ei tarvitse huolehtia pakettien reitityksestä. Saman tason protokollat keskustelevat keskenään eri laitteissa: esimerkiksi TCP/IP-mallissa verkkokerroksella käytetään IP-protokollaa ja kuljetuskerroksella TCP- tai UDP-protokollaa. IP-malli ei ota kantaa peruskerroksen eikä sovelluskerroksen protokolliin [34, s. 41–44]. Monia verkkosodankäynnin menetelmiä on mahdollista kohdistaa useille eri protokollatasoille [16, s.66] [17, s. 7.].

Reititysprotokolla on menetelmä, jonka mukaan viestintäverkon paketit ohjataan lähettäjältä vastaanottajalle [34, s. 20, 31]. Esimerkkejä Internetin reititysprotokollista ovat RIP ja OSPF [34, s. 454–455]. TCP/IP-mallin mukaan tietokoneet voivat muodostaa TCP-protokolla-yhteyden. Tämä tarkoittaa sitä, että TCP-protokollan mukainen data pakataan IP-paketin sisään. IP-paketti sisältää myös vastaanottajan osoitteen ja se ohjataan vastaanottajalle OSPF-reititysprotokollan määrittämällä tavalla. Vastaanottajan koneessa IP-paketti avataan ja TCP-yhteys muodostetaan lähettämällä TCP-protokollan mukainen vastaus jälleen IP-pakettiin pakattuna.

Palvelin on ohjelmisto tai laite, joka tarjoaa viestintäverkossa palvelun muille laitteille [34, s. 4]. Muut laitteet eli asiakkaat ottavat yhteyttä palvelimeen saadakseen palvelun käyttöönsä. Esimerkkejä ovat nimipalvelin, joka ohjaa reititystä, avainpalvelin, joka ohjaa salausta, ja tiedostopalvelin, jolle tallennettaan dataa.

Salaus jaetaan symmetriseen ja asymmetriseen salaukseen [32, s. 17]. Symmetrinen salaus [32, s. 24–25] tarkoittaa sitä, että lähettäjällä ja vastaanottajalla on käytössä sama avain. Tämä avain on siis kyettävä luotettavasti siirtämään vastaanottajalle. Asymmetrisessä salauksessa [32, s. 260] eli julkisen avaimen infrastruktuurissa jokaisella käyttäjällä on kaksi avainta: yksityinen ja julkinen avain. Yksityinen avain on ainoastaan käyttäjän itsensä tiedossa, julkinen avain puolestaan kaikkien tiedossa. Lähettäjä salaa viestinsä vastaanottajan julkisella avaimella ja omalla yksityisellä avaimellaan. Tällöin vastaanottaja tietää viestin tulleen lähettäjältä, koska lähettäjän julkinen avain avaa ensimmäisen salauksen. Toisen salauksen vastaanottaja pystyy avaamaan ainoastaan omalla yksityisellä avaimellaan, joten kukaan muu ei pääse viestiä lukemaan.

3.3. Verkkosodankäynnin menetelmiä

Verkkosodankäynnissä käsitettään sitä, miten viestintäverkkoihin, eli solmuihin ja siirtoteihin, voi vaikuttaa ja miten vaikutukselta voi suojautua sekä miten viestintäverkkoja voi käyttää hyväksi viholliseen vaikuttamista varten [6, s. 13] [2, s. 16–17] [19, s. 255]. Tässä alaluvussa esittelen verkkosodankäynnin keskeisiä menetelmiä ja matemaattisia malleja, joilla verkkosodankäyntiä on mallinnettu. Kaikki mallit eivät suoraan perustu peliteoriaan, mutta niihinkin voi liittää peliteoreettisen tarkastelun, kun huomioon otetaan hyökkääjän ja puolustajan päätöksenteko.

Verkkosodankäynnin mallintamisessa käytetyillä peleillä on usein seuraavia ominaisuuksia. Tilanteet voidaan nähdä kahden pelaajan, hyökkääjän ja puolustajan, välisinä peleinä. Pelit ovat ei-yhteistyöpelejä, koska hyökkääjä ja puolustaja harvoin ovat tietoisia toistensa toiminnasta. Mitä realistisemmin tilanteita pyritään mallintamaan, sitä useammin vallitsevat sekä vajaa että epätäydellinen informaatio. Tällöin matemaattinen mallinnus vaikeutuu, koska näistä malleista on vaikea muotoilla tuloksia ilman huomattavaa matemaattista kalustoa. Seuraavien alalukujen esimerkeissä käsitellään tarkemmin sitä, miksi verkkosodankäynnin peleillä on juuri edellä esitettyjä ominaisuuksia.

3.3.1. Verkkohyökkäys

Jormakan [13, s. 28] mukaan verkkohyökkäyksen merkitys informaatiosodankäynnissä on seuraava: verkkohyökkäyksellä vastustajalle aiheutetaan informaation puutetta. Informaation puutteen vuoksi OODA-silmukan mukainen päätöksenteko hidastuu ja vastustaja tekee vääriä päätöksiä, jotka voivat johtaa tappioihin ja taistelun häviöön [13, s. 28]. Vastustajan viestintäverkon liikenteen häiritseminen palvelunestohyökkäyksellä tai reitityksen häirinnällä hidastavat vastustajan OODA-silmukkaa. Syöttämällä väärää tietoa vastustajan tietojärjestelmiin on mahdollista saada vastustaja tekemään virheitä päätöksenteon eri vaiheissa: OODA-silmukan ensimmäisessä vaiheessa vastustaja voi huomioida virheellistä tietoa, toisessa vaiheessa vastustaja voi verrata oikeita havaintoja syötettyyn väärään taustatietoon. Vastustajan verkkoon tunkeutumalla hyökkääjä voi seurata vastustajan tilannekuvaa ja viestiliikennettä ja kyetä siten vastustajaa yllättävämpään ja nopeampaan toimintaan. Täten verkkosodankäynti tukee informaatioylivoiman saavuttamista [6, s. 54–58]. Yllä mainitut verkkohyökkäyksen toteuttamismenetelmät esitellään tässä alaluvussa.

Candolin [6, s. 60–68] esittää verkkosodankäynnin menetelmiä, joilla hyökätään viestintäverkkoja vastaan ja vaikutetaan siten vastustajan päätöksentekoon. Verkkoon soluttautumisella Candolin [6, s. 60–61] tarkoittaa sitä, että hyökkääjän vihamielinen solmu osallistuu verkon tiedonsiirtoon verkolle haitallisin tavoin. Hyökkääjällä on solmun kautta verkossa useita toimintamahdollisuuksia, joista yksi merkittävimmistä on palvelunestohyökkäys. Palvelunestohyökkäys on verkkosodankäynnin menetelmä, jossa hyökkääjä tuhlaa kohdeviestintäverkon resursseja [34, s. 778]. Palvelunestohyökkäyksen voi kohdistaa verkoissa eri resursseja kohtaan: tiedonsiirtokapasiteettia voi tuhlata lähettämällä mitä tahansa dataa, mutta esimerkiksi palvelinta voi estää vastaanottamasta uusia yhteyksiä TCP-protokollalla käyttämällä pienempää määrää rikkonaisia paketteja [34, s. 778].

Hajautetuksi palvelunestohyökkäykseksi kutsutaan useasta solmusta käynnistettyä palvelunestohyökkäystä. Hajautetun hyökkäyksen potentiaalinen suorituskyky on merkittävästi suurempi kuin yksittäisen solmun hyökkäyksen, koska solmuja voi olla käytössä suuria määriä [34, s. 778–779]. Langattomat siirtotiet ovat erityisen herkkiä palvelunestohyökkäyksille, koska niiden tiedonsiirtokapasiteetti on rajallinen [6, s. 61]. Hyppösen mukaan [12, s. 58] hajautettua palvelunestohyökkäystä voidaan käyttää myös niin, että esimerkiksi suomalaisilta koneilta hyökätään laajasti muuta maailmaa vastaan, minkä seurauksena Suomen viestintäyhteydet muuhun maailmaan katkaistaan. Tästä menetelmästä käytetään nimeä käänteinen palvelunestohyökkäys (*Inverted Denial of Service Attack*). Kuten muiltakin palvelunestohyökkäyksiltä, on myös tältä vaikea suojautua.

Verkkoon soluttautunut hyökkääjä voi myös häiritä liikennettä myöhästyttämällä tai pudottamalla paketteja, eli jättämällä paketteja kokonaan reitittämättä, tai seurata viestintäverkon liikennettä ja siten selvittää esimerkiksi verkolle elintärkeiden solmujen paikkoja ja verkon rakennetta [6 s. 61] [19, s. 264]. Lisäksi hyökkääjä voi häiritä viestintäverkon protokollien käyttöä: lähettämällä väärennettyjä reititysprotokollan mukaisia ohjauspaketteja voi solmu esimerkiksi häiritä verkon reititystä [19, s. 264].

Tyypillistä edellä mainituille hyökkäysmenetelmille on se, ettei puolustaja tarkkaan tiedä, mitä resursseja hyökkääjällä on käytössään. Puolustusmenetelmiä valitaan sen mukaan, mitä hyökkääjän toimista voidaan arvata. Vastaavasti hyökkääjä ei aina tiedä, mitä suojautumismenetelmiä puolustaja hyödyntää. Mikäli kumpikaan osapuoli ei ole etukäteen tietoinen toisen toimista, ei vastustajan päätös vaikuta pelaajan päätöksentekoon. Tilannetta voidaan siis mallintaa staattisena pelinä, koska päätökset käytännössä tehdään samanaikaisesti. Osapuolet tietävät harvoin tarkalleen toistensa aikeet, eivätkä siksi tiedä toistensa suhtautumista mahdollisiin lopputilanteisiin, joten malleissa on usein syytä käyttää vajaata informaatiota. Verkkohyökkäyksen edetessä toimijat voivat reagoida havaittuihin hyökkäyksiin ja puolustusmenetelmiin. Tämä aspektin huomioimiseksi voidaan tilanne mallintaa dynaamiseksi peliksi. Yleensä pelaaja ei pysty todentamaan mitä keinoja vastapuoli on käyttänyt, jolloin pelissä vallitsee epätäydellinen informaatio. Verkkosodankäynnin tilanteita on siis mahdollista mallintaa erilaisiksi peleiksi riippuen siitä, mitä ominaisuuksia halutaan painottaa.

Jormakka ja Mölsä [18, s. 19–20] muotoilevat vandaalipelin, usean pelaajan staattisen täyden informaation pelin, jossa hyökkääjä pyrkii estämään viestintäverkon käytön palvelunestohyökkäyksellä, ja muut käyttäjät pyrkivät käyttämään verkon palveluita. Hyökkääjän tulos

perustuu muille käyttäjille aiheutettuun haittaan. Mallin avulla perusteellaan, ettei hyökkääjän kannata kaataa verkkoa kokonaan, koska silloin käyttäjät yksinkertaisesti siirtyvät käyttämään vaihtoehtoista menetelmää. Hyökkääjän kannalta tulos on paras, jos verkkoa häiritään vain ajoittain, koska oikeutetuille käyttäjille aiheutuu näin enemmän harmia. Mallia muokkaamalla on mahdollista laskea arvioita sille, kuinka tiiviisti hyökkääjän kannattaa verkkoa häiritä [18, s. 20].

Viestintäverkkoon soluttautunut hyökkääjä voi lähettää väärää informaatiota verkkoon esimerkiksi esiintymällä sensorina, jolloin vastustajan tilannekuva vääristyy [6, s. 61]. Tarkastellaan mallia, jossa käsitellään langatonta sensoriverkkoa [28]. Langattomalla sensoriverkolla on seuraavia ominaisuuksia: verkko voi sijaita vihamielisellä alueella ja siten altistua hyökkäyksille, tiedonsiirtonopeus on rajallinen, solmuilla on niukasti muistikapasiteettia ja sähkönkulutus rajoittaa toiminta-aikaa. Suojautumismekanismin käyttäminen tarkoittaa sitä, että sensorin varsinainen toiminta kärsii muistin ja sähkön kulutuksen takia. Mallissa vallitsee vajaa ja epätäydellinen informaatio: sensoriverkko ei kykene ylläpitämään tietoisuutta koko verkon tilasta eikä tiedä, mitä toimenpiteitä hyökkääjä on tehnyt. Mallissa osoitetaan, että mikäli sensorit kykenevät rajoitetusti seuraamaan verkon tilaa ja sen perusteella päättämään suojautumismekanismin käytöstä, kykenee koko verkko suojautumaan hyökkäyksiä vastaan rajoittamatta varsinaista toimintaansa liikaa [28]. Malli tukee langattomien sensoriverkkojen suojausmenetelmien suunnittelua.

Infrastruktuurin tuhoamisessa [6, s. 62–64] keskitytään verkon keskeisien solmujen tuhoamiseen, koska koko verkon tuhoaminen vaatii lähtökohtaisesti turhan paljon resursseja. Tuhoamalla keskeisiä solmuja on mahdollista esimerkiksi eristää verkon osia toisistaan, kuten langaton verkko langallisesta runkoverkosta, tai estää tietyn palvelun, kuten nimi- tai avainpalvelimen, käyttö. Viestintäverkkojen ulkopuolisten menetelmien, kuten solmujen fyysisen tuhoamisen, käyttö lisää hyökkääjän toimintamahdollisuuksien määrää. Samalla puolustaja joutuu ottamaan kantaa useampiin suojautumismenetelmiin, ja molempien osapuolten epävarmuus tilanteesta kokonaisuutena kasvaa. Mallinnuksen kannalta tämä tarkoittaa sitä, että eri siirtojen ja strategioiden määrä kasvaa ja mallit monipuolistuvat: mitä enemmän eri aspekteja tarkasteluun tuodaan mukaan, sitä monimutkaisemmiksi mallit muodostuvat ja sitä vaikeampi niistä on saada konkreettista tietoa. Toisaalta peliteoria tukee juuri tällaisissa tilanteissa tilanteen arviointia yksinkertaistettujen mallien avulla.

Solmun kaappaus [6, s. 64–67] tarkoittaa sitä, että hyökkääjä saa täysin käyttöönsä viestintäverkkoon kuuluvan solmun. Hyökkääjä pystyy siten tekemään solmun kautta kaikkea mihin oikeakin käyttäjä pystyy ilman, että verkon muut solmut tunnistavat hyökkääjän. Solmun kaappauksen voi toteuttaa muun muassa selvittämällä vaadittavat salasanat tai käyttämällä haittaohjelmistoja. Seppälä [31, s. 188] toteaa, että hyökkääjän on mahdollista selvittää tai ohittaa salasanasuojaukset, mikäli hänellä on pääsy solmulle. Myös liikennettä seuraamalla on mahdollista selvittää salasanoja [31, s.188].

Jormakka [14, s. 4] mallintaa tilannetta, jossa hyökkääjä pyrkii murtamaan salasanan. Hyökkääjä ei tiedä käytössä olevan salasanan tyyppiä, mutta tietää vaihtoehtoja olevan kaksi: heikompi ja vahvempi salasana. Hyökkääjällä on ennestään näkemys näiden salasanojen murtamisen todennäköisyyksistä. Mallissa muotoillaan menetelmä, jolla hyökkääjä voi arvioida kuinka monen yrityksen jälkeen voi olettaa kyseessä olevan vahvan salasanan, jolloin hyökkäystä ei kannata jatkaa [14, s. 4]. Mallia voi siis sopivin reunaehdoin käyttää hyökkäyksen suunnittelussa.

Hyökkääjällä on solmun kaappauksen jälkeen käytössään kaikki samat menetelmät kuin soluttauduttaessa verkkoon ja lisäksi muita toimintamahdollisuuksia [6, s. 64–67]. Hyökkääjä voi kaapata muita solmuja syöttämällä niille virheellistä tietoa. Tämä voi vähitellen johtaa koko viestintäverkon kaappaamiseen. Hyökkääjä voi kerätä tietoa verkossa käytettävistä salausmenetelmistä ja esimerkiksi selvittää käytössä olevat radioiden ja sensoreiden taajuushypytykset, jotta niihin voidaan kohdistaa häirintää [19, s. 264]. Lisäksi solmun kautta voi muuttaa viestintäverkon toimintaa vaikuttamalla verkon asetuksiin. Tämä voi tarkoittaa esimerkiksi reititysprotokollan häiritsemistä.

Kaapatun solmun avulla hyökkääjä voi käyttää kaikkia solmun käytössä olevia palveluita [6, s. 65–67]. Tämä voi tarkoittaa esimerkiksi väärän tiedon syöttämistä tietokantoihin tai vastustajan tilannekuvan seuraamista. Koska solmu näyttää puolustajan kannalta harmittomalta, on hyökkääjällä etulyöntiasema ja mahdollisuus kerätä tietoa puolustuksesta. Tilannetta voidaan näin ollen mallintaa vajaan informaation peliksi.

Theodorakopoulos ja Baras [35] tarkastelevat mallissaan viestintäverkkoa, jossa solmut toimivat yhteistyössä mahdollistaakseen verkon toimivuuden. Esimerkki tällaisesta verkosta on langaton Ad Hoc -verkko, jossa reititystä ei määritetä ennalta, vaan kaikki solmut osallistuvat reititykseen, joka määräytyy tilanteen mukaan [36, s. 22]. Ad Hoc -verkkojen käyttöä sotilas-

sovellutuksiin tutkitaan ja kehitetään paljon [26, s. 35–36]. Mallissa [35] käsitellään erityisesti hyökkääjien toimintamahdollisuuksia tällaisessa verkossa. Malli esittelee hyökkääjille yhteistoimintamenetelmiä, joiden avulla verkolle aiheutetaan mahdollisimman suurta vahinkoa. Toisaalta mallin avulla löydetään myös oikeutetuille käyttäjille strategioita, joiden avulla on mahdollista rajoittaa hyökkääjien aiheuttamaa haittaa. Näin ollen malli voi tukea sekä Ad Hoc -verkon suunnittelua, että hyökkäystä verkkoa vastaan.

Liikenteen valvontaa [6, s. 67–68] on mahdollista suorittaa myös ilman viestintäverkkoon soluttautunutta tai kaapattua solmua etenkin jos kyseessä on langatonta siirtotietä käyttävä verkko. Verkon rakennetta ja tärkeimpiä solmuja on mahdollista tunnistaa liikenteen määrää ja tyyppiä tarkkailemalla.

Jormakan ja Mölsän [18, s. 18–19] pahantekijäpelissä hyökkääjä A pyrkii toteuttamaan etähyökkäyksen puolustajan solmua vastaan. Puolustaja B seuraa verkkoliikennettä ja saattaa tunnistaa hyökkääjän liikkeet verkossa. Hyökkääjällä on mahdollisuus yrittää harhauttaa puolustajaa aiheuttamalla suuri määrä vaaratonta liikennettä, joka häiritsee puolustajan valvontaa. Jormakan ja Mölsän mukaan harhautustoiminnan voi katsoa kohdistuvan puolustajan OODA-silmukkaan: häiritsevän liikenteen aiheuttamat väärät hälytykset lisäävät havaitun datan määrää ja vaativat lisää työstämistä, jolloin varsinainen hyökkäys voi jäädä puolustajalta huomaamatta. Puolustajalla vaihtoehtoina on joko kaiken häiritsevän liikenteen analysointi, tai suurpiirteisempi analysointi joka antaa paremman yleiskuvan tilanteesta. Tulokset on esitelty taulukossa 6.

	Hyökkääjä A ei harhauta	Hyökkääjä A harhauttaa
Puolustaja B tarkastaa kaiken	A: -10, B: 20	A: 4, B: -5
Puolustaja B ei tarkasta kaikkea	A: 30, B: -20	A: 3, B: -2

Taulukko 6. Pahantekijäpeli.

Jos hyökkääjä harhauttaa, on puolustaja tietoinen siitä, että jotakin on tapahtumassa ja pystyy rajoittamaan vahinkoa. Jos hyökkääjä ei harhauta ja puolustaja tarkastaa kaiken, jää hyökkääjä kiinni. Jos hyökkääjä ei harhauta eikä puolustaja tarkasta kaikkea, ei hyökkäystä huomata lainkaan. Tässä tilanteessa Jormakka ja Mölsä [18, s. 19] osoittavat, että hyökkääjän kannattaa 40%:ssa tilanteista harhauttaa ja 60%:ssa käyttää vain yhtä hyökkäystä. Vastaavasti puolustajan kannattaa tarkastaa kaikki liikenne 40%:ssa tilanteista ja 60%:ssa olla tarkastamatta. Yhdistetty strategia, eli käytännössä strategioiden vaihtelu, tilanteessa, jossa vastustajan toimin-

nasta ei ole varmaa tietoa tuottaa siis paremman tuloksen, kuin yksittäisen strategian valitseminen.

Seppälä [31, s. 188] ja Tanenbaum [34, s. 806–808] käsittelevät hyökkäystä nimipalvelinta vastaan. IP-protokolla on yksi Internetin keskeisimmistä tiedonsiirtoprotokollista. Nimipalvelimen tehtävä on muuntaa verkkotunnukset, esimerkiksi www.mil.fi, IP-osoitteiksi, joiden avulla paketit reititetään. Hyökkääjä voi Seppälän esimerkin mukaan [31, s. 188] korvata koko nimipalvelimen omalla laitteellaan ja täten johtaa IP-verkon käyttäjät haluamiinsa osoitteisiin. Tanenbaumin menetelmällä [34, s. 807–808] hyökkääjä voi syöttää käyttäjälle vääriä osoitteita myös ilman, että varsinaisen nimipalvelimen toimintaan vaikutetaan. Tämä menetelmä ei siis vaadi solmun kaappaamista.

Sallhammar, Helvik ja Knapskog mallintavat nimipalvelimen toimintavarmuutta kombinatoriikan avulla [30]. Mallissa tarkastellaan palvelimen virheherkkyyttä ja haavoittuvuutta erilaisille hyökkäyksille. Tuloksena esitetään aika-arvioita sille, miten kauan nimipalvelimen voi olettaa toimivan halutulla tavalla. Malli antaa perusteita palvelinjärjestelmän suunnittelulle ja suojaustoimenpiteille. Mallia on myös mahdollista kehittää peliteorian avulla: hyökkääjän ja palvelimen ylläpitäjän päätöksentekoa mallissa esitettyihin palvelimen ominaisuuksiin liittyen voi mallintaa pelinä, jolloin kombinatoriikka tukee pelin tulosten muodostamista.

Lukin [24, s. 47–52] esittelee venäläisten hakkerien käyttämiä verkkohyökkäysmenetelmiä. Yleistä on hyötyohjelmistojen ja käyttöjärjestelmien heikkouksia hyödyntävien haittaohjelmistojen käyttö. Haittaohjelmia suunnitellaan sellaisiksi, että niitä on vaikea havaita tietoturvaohjelmistoilla, koska niiden aiheuttama verkkoliikenne muistuttaa luvallista liikennettä. Haittaohjelmat tehoavat varsinkin solmuihin, joiden tietoturvaohjelmistoja ei päivitetä säännöllisesti. Lukinin mukaan omaa toimintaa suojataan käyttämällä hyökkäyksiin esimerkiksi vertaisverkkojen kautta kaapattuja solmuja. Laajat bot-verkot, eli hyökkääjän etäkäyttämät usean koneen verkot, mahdollistavat monenlaiset hyökkäykset siten, ettei varsinaista hyökkääjää voida helposti tunnistaa.

Lin, Chen, Chen ja Chien tarkastelevat mallissaan [22] tilannetta, jossa hyökkääjällä on käytössään useita eri menetelmiä ja mahdollisina kohteinaan puolustajan verkon eri solmuja. Puolustajan vaihtoehtoina ovat eri solmujen valvonta, jolloin hyökkäyksen tehoa voidaan pienentää. Hyökkääjä ja puolustaja mallinnetaan kahdeksi pelaajaksi. Molemmat toimijat voivat tehdä kaksi valintaa peräkkäin toisistaan riippumatta, joten kyseessä on dynaaminen peli, jos-

sa pelataan peräkkäin kaksi staattista vaihetta. Pelaajat pyrkivät salaamaan toimintansa toisiltaan, joten kyseessä on ei-yhteistyöpeli. Pelaajat eivät ole tietoisia toistensa toimenpiteistä, joten pelissä vallitsee epätäydellinen informaatio. Mallissa pelaajien oletetaan tietävän toistensa prioriteetit, joten täysi informaatio vallitsee. Lisäksi prioriteettien oletetaan olevan vastakkaisia, eli hyökkääjän voiton olevan vastustajan häviö, joten peli on nollasummapeli. Näiden valintojen todetaan olevan yksinkertaistuksia [22, s. 80].

Perustuen pelaajien prioriteetteihin löydetään mallissa laskemalla strategia, jolla hyökkääjä pystyy takaamaan itselleen tietyn minimituloksen [22, s. 78]. Vastaavasti osoitetaan puolustajalle strategia, jolla voidaan estää pahin mahdollinen tulos. Pelaajien epävarmuutta toisiensa toimista mallinnetaan siten, että kannattavien strategioiden vallinnoille voidaan suositella todennäköisyyksiä. Malli voi siis ohjeistaa molempien pelaajien toimintaa, mikäli oletukset hyväksytään.

3.3.2. Verkkopuolustus

Jormakka [16, s. 64–72] esittelee useita käytössä olevia tietoturvamekanismeja, joita käytetään verkkohyökkäyksiä vastaan puolustautumiseen. Käyttäjän tunnistaminen perustuu pääasiassa salasanan käyttöön [16, s. 64–65]. Salasanoja käytettäessä merkittävin heikkous on käyttäjä, joka voi paljastaa salasanansa hyökkääjälle tai valita heikon salasanan. Salasanan, esimerkiksi PIN-koodin, yhdistäminen älykorttiin tai muuhun lisätunnisteeseen lisää menetelmän turvallisuutta. Hyökkääjän yritystä päästä murtautumaan järjestelmään voidaan kuvata pelinä, jossa puolustajan lisätunnisteen käyttö vaikuttaa merkittävästi hyökkääjän tuloksiin: järjestelmään pääsy edellyttää huomattavia lisätoimenpiteitä.

Pääsyoikeuksilla rajoitetaan käyttäjien toimintoja tietokoneessa [16, s. 65]. Kaikki käyttäjät eivät pääse käsiksi sellaisiin toimintoihin, jotka voivat vaarantaa tietoturvaa. Käytännössä rajoituksia on silti mahdollista ohittaa hyödyntämällä ohjelmistovikoja tai pääkäyttäjältä hankittua salasanaa. Virustarkistuksessa etsitään haittaohjelmakoodin tunnistettavia palasia [16, s. 65–66]. Hyökkääjä voi helposti testata, löytääkö virustarkistus haittaohjelman, ja sen jälkeen tarvittaessa muokata ohjelmaa. Näin ollen virustarkistusohjelmisto on päivitettävä riittävän usein, jotta tietokannat pysyvät ajan tasalla.

Tarkastellaan mallia, jossa uusi haittaohjelma pyrkii saastuttamaan verkon [15, s. 8–10]. Haittaohjelman, tässä tapauksessa viruksen, leviäminen muistuttaa sairausepidemian leviämistä ja sitä voi mallintaa vastaavalla tavalla, varsinkin jos verkon solmujen määrä on suuri. Malli

antaa käsityksen siitä, miten nopeasti vastatoimiin virusta vastaan on ryhdyttävä, jotta leviäminen saadaan estettyä. Lisäksi mallin avulla voidaan tarkastella sitä, miten virustarkistusohjelman päivittäminen vaikuttaa viruksen leviämiseen. Päivittämistä ei yleensä ole mahdollista tehdä kaikkiin solmuihin kerralla, joten päivityksen olemassaolo ei riitä pysäyttämään leviämistä. Yksityiskohtana mainittakoon itsestään leviävän ohjelman käyttö virustarkistusohjelman päivittämiseen: viruksen tavalla toimivaa ohjelmaa voi käyttää myös virukselta suojautumiseen. Tällaisella ohjelmalla on lisäksi se etu, että se pääsee oikeutetusti solmuihin suorittamaan päivityksiä ja leviää siten virusta nopeammin [15, s. 9–10]. Tätä mallia on mahdollistaa hyödyntää viestintäverkon haavoittuvuutta ja virustorjuntamenetelmiä arvioitaessa. Peliteorian avulla tilannetta voidaan mallintaa esimerkiksi siten, että tarkastellaan puolustajan vaihtoehtoja ja päätöksentekoa hyökkääjän viruksen ominaisuuksista riippuen.

Palomuuri on laitteistolla tai ohjelmistolla toteutettu järjestelmä, joka suojaa solmua tai viestintäverkon osaa hyökkäyksiltä estämällä ei-toivottujen pakettien välityksen [34, s. 776–779] [36, s. 26]. Välitystä valvotaan arvioimalla tietyillä kriteereillä jonkin protokollatason liikennettä ja pudottamalla ne paketit, jotka eivät vastaa näitä kriteerejä. Palomuuriratkaisut toteutetaan yleensä ohjelmistolla ja ne toimivat TCP/IP-mallin verkko-, kuljetus- tai sovelluskerroksella [16, s. 66–67]. Jormakka esittää myös palomuurin heikkouden: hyökkääjä voi muodostaa salatun yhteyden esimerkiksi sovelluskerroksen protokollan avulla siten, että verkkokerroksen palomuuri ei havaitse liikenteessä olevan mitään tavallisuudesta poikkeavaa.

Hyökkääjän havaitsemisen järjestelmät (*Intruder Detection System*, IDS) ovat ohjelmistoja, joilla pyritään havaitsemaan ja mahdollisesti myös estämään solmuun kohdistuvia hyökkäyksiä [16, s. 69–70]. Solmuun kohdistuva IDS voi esimerkiksi valvoa niitä komentoja, joita koneella suoritetaan, ja estää haitallisten komentojen suorittamisen. Verkkoon kohdistuva IDS voi lukea kaiken datan, joka kulkee yksittäisen solmun läpi, ja pyrkiä sen perusteella tunnistamaan haitallista toimintaa. IDS-järjestelmät aiheuttavat myös vääriä hälytyksiä, jotka kuormittavat verkkoa ja mahdollisesti käyttäjiä turhaan.

IDS-järjestelmän toimintaa voi tarkastella Jormakan peliteoreettisella mallilla [15, s. 2–4]. Pyritään selvittämään miten tiukaksi järjestelmän asetukset kannattaa laittaa, jotta hyökkääjiä havaitaan, mutta oikeutetut käyttäjät eivät aiheuta vääriä hälytyksiä. Väärät hälytykset aiheuttavat negatiivisen tuloksen järjestelmälle, koska niiden käsittely vaatii resursseja ja käyttäjien työ häiriintyy. Kuitenkin hyökkäyksen päästäminen läpi aiheuttaa aina suuremman haitan kuin väärä hälytys. Järjestelmällä on lisäksi maksimikapasiteetti, jonka täytyttyä liikennettä ei

voida analysoida. Jormakka osoittaa miten asetuksia voidaan optimoida [15, s. 3–4]. Huomionarvoista on se, että hyökkääjä pystyy tässä tilanteessa käyttämään tietoa mallista hyväksi: puolustajaa voi harhauttaa siten, että hyökkääjä erehtyy asettamaan hälytysrajan liian tiukaksi, jolloin vääriä hälytyksiä tulee paljon, tai liian löysäksi, jolloin oikeat hyökkäykset voivat jäädä havaitsematta. Optimaalisten ratkaisujen ja harhautusmenetelmien tunteminen voi tukea molempia pelaajia päätöksenteossa.

Hunajapurkki on huonosti suojattu kone, jonka ainoa tarkoitus on havaita siihen tunkeutuvat ohjelmistot. Hunajapurkilla pyritään havaitsemaan uusia haittaohjelmia ennen kuin ne pääsevät aiheuttamaan haittaa [16, s. 72]. Merkittävä hyöty hunajapurkin käytössä on se, että näin on mahdollista havaita uusia hyökkäysmenetelmiä [14, s. 5]. Virustarkistusohjelmistot vaativat etukäteen tietoa etsittävästä ohjelmakoodista ja palomuuri estää ennalta ohjelmoidun liikenteen. Koska hunajapurkissa ei ole muuta tuntematonta liikennettä, on kaikki tavallisuudesta poikkeava helppo tunnistaa epäilyttäväksi.

Jormakka [14, s. 5] tarkastelee tilannetta, jossa hunajapurkilla pyritään havaitsemaan hyökkääjän läsnäolo verkossa, eikä siis vain tunnistamaan uusia haittaohjelmia. Rationaalinen hyökkääjä kohdistaa hyökkäyksensä verkon heikoimpaan kohtaan, ellei se vaikuta ansalta. Jos hunajapurkin suojaus asetetaan hieman heikommaksi kuin muun verkon, eikä hyökkääjällä ole tapaa tunnistaa sitä ansaksi, hyökkää rationaalinen toimija hunajapurkkiin. Tässä tapauksessa rationaalinen pelaaja siis toimii ennakoitavasti. Toisaalta hyökkääjällä ei ole varmaa tapaa määrittää eri solmujen suojaustasoja, joten hunajapurkkiin osuminen ei ole varmaa. Lisäksi hyökkääjän houkuttelemisesta hunajapurkkiin ei olisi juuri hyötyä [14, s. 5].

Jormakka [16, s. 73–75] nostaa esiin uhkia, joita vastaan puolustusmekanismit tarjoavat ainoastaan puutteellisia ratkaisuja: palvelunestohyökkäykset ja kehitettävät uudet haittaohjelmistot. Palvelunestohyökkäys on aina periaatteessa mahdollista toteuttaa siten, että kohteen resurssit ylitetään, kunhan hyökkäyksessä käytetään riittävästi omia resursseja. Erityisesti IP-protokolla on haavoittuvainen palvelunestohyökkäyksille, koska protokolla antaa yksittäisen käyttäjän aiheuttaa suuria määriä liikennettä verkkoon.

Jormakan [16, s. 73–74] mukaan uuden ohjelmistokoodin määrän kasvaessa kasvaa myös ohjelmistovirheiden määrä ja sen myötä niiden hyväksikäyttö. Haittaohjelmia voidaan siis myös vastaisuudessa räätälöidä toimimaan yksittäisien heikkouksien avulla. Uusia haittaohjelmia pyritään havaitsemaan ohjelmiston käyttäytymisen seuraamisella, käytettyjen tiedon-

siirtoprotokollien analyysillä ja hunajapurkeilla. Jormakan mukaan nämä vastatoimet eivät kuitenkaan ole riittäviä.

Candolin [6, s. 70–103] esittää ratkaisuja verkkohyökkäyksiltä puolustautumiseen. Pakettitason autentikoinnissa (*Packet Level Authentication*, PLA) IP-paketin sisään lisätään tietoa, jonka avulla jokainen solmu pystyy varmistumaan paketin lähettäjästä riippumatta siitä, onko solmu aiemmin ollut lähettäjään yhteydessä. PLA tunnistaa saman paketin kopiot ja pystyy siten estämään paketteja kopioimalla toteutetun palvelunestohyökkäyksen leviämisen verkossa [6, s. 124]. Kontekstitietoisessa hallinta-arkkitehtuurissa (*Context Aware Management Architecture*, CAM) kaikki käytössä olevat protokollatasot keskustelevat CAM-protokollatason kanssa. Tällöin CAM-protokollan avulla on mahdollista toteuttaa automaattisia muutoksia verkon toimintaan, kun verkossa havaitaan häiriöitä: esimerkiksi palvelimen tuhoutuessa voidaan sen tehtäviä automaattisesti jakaa muille solmuille [6, s. 125]. Viestintäverkot pystyvät korjautumaan itsestään CAM- ja PLA-menetelmien avulla [6, s. 125]. Verkon toimintaa haittaaviin muutoksiin on mahdollista reagoida automaattisesti ja luotettavasti. Peliteorian avulla voidaan mallintaa myös tilannetta, jossa pelaajat ovat ohjelmistoja eivätkä käyttäjiä: PLA- ja CAM-ominaisuuksilla varustetun verkon itsensä korjaaminen perustuu protokollien päätöksentekoon. Mallinnuksella voidaan analysoida miten protokollan asetuksia tulee säätää, jotta verkon toimintavarmuus optimoidaan, ja miten verkko selviytyy erilaisista hyökkäystilanteista.

3.3.3. Viestintäverkon tietoturvallisuudesta

Viestintävirasto [37] jakaa tietoturvallisuuden kolmeen osa-alueeseen. Luottamuksellisuus (*Confidentiality*) tarkoittaa sitä, että ainoastaan oikeutetut tahot voivat käyttää tietoa. Eheys (*Integrity*) tarkoittaa tiedon muuttumattomana säilymisen takaamista: tietoa ei voi poistaa eikä muuttaa ilman lupaa ja tieto on suojattu esimerkiksi järjestelmien rikkoutumiselta. Käytettävyys (*Availability*) tarkoittaa oikeutettujen käyttäjien esteetöntä pääsyä tietoon: suojausjärjestelmien ei tule tehdä tiedon käsittelystä niin vaikeaa, että tiedon hyödyntäminen kärsii.

Tarkastellaan tiedon luottamuksellisuutta, eli kysymystä siitä, miten tietoa voi säilöä niin, etteivät muut tahot pääse siihen käsiksi. Tiedon luottamuksellisuutta voidaan parantaa salauksella, joka voidaan toteuttaa usealla eri protokollatasolla ja monen protokollan avulla. Symmetrisen salauksen ongelma on avainten jakaminen. Asymmetrisen salauksen ongelma on sertifikaattien luotettavuus: sertifikaatin avulla varmennetaan julkisten avainten oikeellisuus, mutta sertifioijan luotettavuutta voi puolestaan olla vaikea varmentaa.

Usein oletetaan luottamuksellisuuden lisäämisen merkitsevän käytettävyyden laskemista. Toinen yleinen mielikuva on, että verkossa kiinni oleva tietokone ei ole turvallinen paikka tiedon säilyttämiselle. Jormakka [14, s. 5–6] käsittelee tilannetta, jossa oikeutetun käyttäjän tunnistamiseen on käytössä menetelmä, jota ei voi teknisesti murtaa. Tämä tarkoittaa sitä, ettei hyökkääjä voi ohittaa tunnistusta, mutta voi kuitenkin murtautua yksittäisiin solmuihin. Tallennetaan nyt tieto siten, että se jaetaan pieniin salattuihin yksiköihin, jotka jaetaan verkossa siten, että jokainen yksikkö tallennetaan usealle koneelle, mutta yhdeltä koneelta ei löydy kuin yksi yksikkö.

Jormakan mukaan [14, s. 6] käyttäjän kannalta käytettävyys ei laske merkittävästi, koska tiedon hakeminen usealta koneelta ei ole paljoa hitaampaa kuin yhdeltä koneelta. Hyökkääjällä ei ole tapaa selvittää, mille koneille tieto on tallennettu. Jos hyökkääjä haluaa päästä käsiksi tietoon, on hänen murtauduttava useaan koneeseen ja kerättävä kaikki erilliset yksiköt, koska salauksen purkaminen edellyttää kaikkien yksikköjen yhdistämistä. Kun verkon solmujen määrää kasvatetaan, laskevat tiedon löytämisen ja salaamisen purkamisen todennäköisyydet niin merkittävästi, että rationaalinen hyökkääjä toteaa verkkoon hyökkäämisen olevan kannattamaton menetelmä.

Tiedon luottamuksellisuus on käytännössä mahdollista taata verkkoon liitetyissä koneissa, kuten Jormakka toteaa [14, s. 6]. Mallissa oletetaan tunnistusmenetelmän murtamattomuus. Tätä ei vielä ole käytännössä toteutettu, mutta se ei myöskään ole kaukana nykytilanteesta. Malli ei käsittele muita hyökkäysmenetelmiä: hyökkääjä voi edelleen esimerkiksi vahingoittaa verkkoa tai käyttää solmuja omiin tarkoituksiinsa. Hyökkääjän on myös mahdollista vaikuttaa oikeutettuun käyttäjään esimerkiksi huijaamalla käyttöönsä käyttöoikeudet tai suoraan ostamalla tietoa. Malli kuitenkin kyseenalaistaa yleisen käsityksen siitä, ettei tieto voisi olla turvassa verkossa olevalla koneella [13, s. 38].

Epätäydelliseen luottamukseen perustuvan luottamusmallin avulla on mahdollista vähentää kaapattujen solmujen aiheuttamaa haittaa [6, s. 125]. Luottamus määrittää tässä sen, miten solmu suhtautuu toisiin solmuihin. Täydellisen luottamuksen mallissa solmu voi joko täysin luottaa toiseen solmuun, jolloin kaikki tältä solmulta tuleva tieto hyväksytään, tai olla luottamatta, jolloin kaikki tieto hylätään. Epätäydellisen luottamuksen mallissa luottamukselle annetaan arvoja, joiden avulla solmu laskee sen, miten eri tilanteisiin tulee reagoida. Tällöin rajoitetaan merkittävästi kaapattujen solmujen ja verkkoon soluttautuneiden solmujen toimintamahdollisuuksia.

4. JOHTOPÄÄTÖKSET

Verkkosodankäynnillä aiheutetaan vastustajalle informaation puutetta. Informaation puute hidastaa päätöksentekoa ja johtaa vääriin päätöksiin. Vähäinenkin määrä vääriä päätöksiä voi johtaa tappioihin ja taistelun häviöön. Verkkosodankäynti tukee täten informaatiosodankäynnin tavoitetta: informaatioylivoiman saavuttamista.

Verkkosodankäynnin tutkimus on perinteisesti teknisten järjestelmien ominaisuuksien tutkimusta. Tällainen tutkimus ei huomioi toimijoiden päätöksentekoa. Peliteoria soveltuu erityisen hyvin juuri kilpailutilanteissa, kuten sodankäynnissä, tapahtuvan usean toimijan välisen päätöksenteon analysoimiseen.

Peliteoria antaa mahdollisuuksia analysoida verkkosodankäynnin lainalaisuuksia ja etenkin niitä ongelmia, joihin teknologian tutkimus ei tarjoa vastauksia. Mikäli peliteoreettisen mallin muodostus onnistuu hyvin, voi peliteoria antaa jopa käytännöllisiä suosituksia sille, miten konkreettiseen verkkosodankäynnin uhkaan kannattaa varautua.

Peliteorian vahvuus on tilanteiden matemaattisen täsmällisessä tarkastelussa, mutta jo heuristinen peliteoriaan tukeutuva analyysi, jota tässä tutkielmassa on tehty, tukee tarkasteltavien tilanteiden kokonaisvaltaista jäsentämistä. Näin ollen myös ei-formaali peliteoreettinen lähestymistapa tukee toiminnan suunnittelua.

Tässä tutkimuksessa esitetyt mallit tarjoavat useita mahdollisia jatkotutkimuskohteita. Mallien formaali tarkastelu tuottaa tarkempaa tietoa tilanteiden erityispiirteistä. Jos formaalin tarkastelun kautta mallista löytyy uusia lainalaisuuksia, saattaa ymmärrys mallinnetusta tilanteesta muuttua merkittävästi.

On tärkeä muistaa, että peliteoreettinen malli on aina yksinkertaistava, eikä siis vastaa täysin todellisuutta. Lisäksi mitä tarkemmin tilannetta halutaan mallintaa, sitä enemmän matemaattista välineistöä vaaditaan tulosten saamiseksi. Monimutkaisista peleistä ei aina ole mahdollista vetää johtopäätöksiä, joista olisi jotakin hyötyä. Suurta tarkkuutta ja mahdollisimman monien parametrien huomiointia vaativassa tilanteessa peliteoria ei ole paras työkalu.

Vaikka peliteoreettinen mallinnus ei antaisi selkeätä vastausta siihen, miten mallinnetussa tilanteessa kannattaa toimia, on usein mahdollista määrittää ala- ja ylärajoja saavutettaville

lopputuloksille. Nämä rajat voivat tukea riskianalyysiä ja päätöksentekoa mallinnetussa tilanteessa.

Viestintäverkkojen ja verkkosodankäynnin merkitys sodankäynnissä korostunee tulevaisuudessa yhä enemmän, joten omien järjestelmien haavoittuvuutta verkkosodankäynnille on syytä tutkia oman toiminnan turvaamiseksi. Peliteoria antaa yhden metodin tähän tutkimukseen. Olen tässä tutkielmassa osoittanut, että peliteoria toimii analyysityökaluna useissa erilaisissa tilanteissa ja tukee suunnittelua ja päätöksentekoa verkkosodankäyntiin liittyen.

LÄHTEET

[1] Ahvenainen, Sakari. Verkkosodan historia ja käsitteen kehittyminen. Teoksessa Piiroinen, Mika (toim.). Verkkotaistelu 2020. Sivut 12–42. MPKK, Taktiikan laitos. Helsinki 2003. ISBN 951-25-1423-0.

[2] Allan, Pierre & Dupont, Cédric. International Relations Theory and Game Theory: Baroque Modeling Choices and Empirical Robustness. International Political Science Review 1999, Vol. 20, No. 1. Sivut 23–47. http://ips.sagepub.com/content/20/1/23.full.pdf+html [viitattu 23.4.2012].

[3] Boyd, J. The Essence of Winning and Losing. Näyttöesitys. 1996. Ei virallisesti julkaistu. http://www.danford.net/boyd/essence.htm [viitattu 23.4.2012].

[4] Brams, Steven J. Negotiation Games. Routledge, Chapman and Hall, Inc. USA 1990. ISBN 0-415-90337-8.

[5] Brams, Steven J. Superpower Games. Yale University. USA 1985. ISBN 0-300-03323-0.

[6] Candolin, Catharina. Securing Military Decision Making in a Network-Centric Environment. Väitöskirja, Teknillinen korkeakoulu, Tietotekniikan osasto. Helsinki 2005. ISBN 951-22-7980-0.

[7] Gibbons, Robert. A Primer in Game Theory. Hartnolls Ltd, Bodmin 1992. ISBN 0-7450-1159-4.

[8] Gödel, Kurt. On Formally Undecidable Propositions of Principia Mathematica and Related Systems. Teoksessa Hawking, Stephen (toim.). God Created the Integers. Sivut 1097–1118. Penguin Books 2006. ISBN 0-141-01878-X.

[9] Heiskanen, Mikko. Informaatiosodankäynti johtamissodankäynnin yläkäsitteenä. Teoksessa Saarelainen, Jorma (toim.). Johtamissodankäynti. Sivut 4–31. MPKK, Taktiikan laitos. Helsinki 2000. ISBN 951-25-1187-8.

[10] Helokunnas, Tuija & Laukkanen, Terhi & Viitanen, Kalle. Tiedon merkitys Suomen puolustamisessa. Teoksessa Piiroinen, Mika (toim.). Verkkotaistelu 2020. Sivut 43–54. MPKK, Taktiikan laitos. Helsinki 2003. ISBN 951-25-1423-0.

[11] Hutchinson, W. & Warren, M. Principles of Information Warfare.
Journal of Information Warfare Volume 1, Issue 1. 2001. Sivut 1–6.
ISSN 1445-3347.
http://www.jinfowar.com/wp-content/uploads/2011/11/JIW1_1.pdf
[viitattu 23.4.2012].

[12] Hyppönen, Mikko. Miten tekisin verkkohyökkäyksen.
Teoksessa Piiroinen, Mika (toim.). Verkkotaistelu 2020. Sivut 55–59.
MPKK, Taktiikan laitos. Helsinki 2003.
ISBN 951-25-1423-0.

[13] Jormakka, Jorma. Combinatorial Decision Theory with applications in Hacker Warfare Modelling.
MPKK, Tekniikan laitos. Helsinki 2003.
ISBN 951-25-1427-3.

[14] Jormakka, Jorma. Hacker Warfare as a Game (preprint).
Teoksessa Jormakka, Jorma. Combinatorial Decision Theory with applications in Hacker Warfare Modelling (Preprints).
MPKK, Tekniikan laitos. Helsinki 2003.
ISBN 951-25-1428-1.

[15] Jormakka, Jorma. Mathematical Methods for Hacker Warfare (preprint).
Teoksessa Jormakka, Jorma. Combinatorial Decision Theory with applications in Hacker Warfare Modelling (Preprints).
MPKK, Tekniikan laitos. Helsinki 2003.
ISBN 951-25-1428-1.

[16] Jormakka, Jorma. Miten verkkotaistelussa puolustaudutaan.
Teoksessa Piiroinen, Mika (toim.). Verkkotaistelu 2020. Sivut 60–87.
MPKK, Taktiikan laitos. Helsinki 2003.
ISBN 951-25-1423-0.

[17] Jormakka, Jorma. Network Centric Warfare from a Technical Perspective.
Teoksessa Jormakka, Jorma & Candolin, Catharina (toim.). Technical Aspects of Network Centric Warfare. Sivut 1–8.
MPKK, Tekniikan laitos. Helsinki 2004.
ISBN 951-25-1499-0.

[18] Jormakka, Jorma & Mölsä, J. Modelling Information Warfare as a Game.
Teoksessa Journal of Information Warfare. Volume 4, Issue 2. 2005.
Sivut 12–25.
http://lib.tkk.fi/Diss/2006/isbn9512282151/article7.pdf [viitattu 23.4.2012].

[19] Keskiväli, Kari. Verkkosodankäynti.
Teoksessa Saarelainen, Jorma. Johtamissodankäynti. Sivut 255–296.
MPKK, Taktiikan laitos. Helsinki 2000.
ISBN 951-25-1187-8.

[20] Lehtinen, Matti. Matemaattinen analyysi sotatekniikan tutkimusmenetelmänä. Teoksessa Lappalainen, Esa & Jormakka, Jorma (toim.). Tekniset tutkimusmenetelmät Maanpuolustuskorkeakoulussa.
MPKK, Tekniikan laitos. Helsinki 2004.
ISBN 951-25-1540-7.

[21] Libicki, Martin. What is Information Warfare?
Center for Advanced Concepts and Technology Institute for National Strategic Studies, National Defense University. USA 1995.

[22] Lin, Jin-Cherng & Chen, Jan-Min & Chen, Chou-Chuan & Chien, Yu-Shu. A Game Theoretic Approach to Decision and Analysis in Strategies of Attack and Defense.
2009 Third IEEE International Conference on Secure Software Integration and Reliability Improvement. Sivut 75–81. IEEE 2009.

[23] Luce, R. Duncan & Raiffa, Howard. Games and Decisions – introduction and critical survey.
John Wiley & Sons, Inc. USA 1957.
ISBN 978-0486659435.

[24] Lukin, Kimberly. Venäläisten käyttämät tietoverkkosodankäynnin menetelmät. Pro gradu -tutkielma. Turun yliopisto 2007.

[25] Morrow, James D. The Ongoing Game-Theoretic Revolution.
Teoksessa Midlarsky, Manus I. (toim). Handbook of War Studies II. Sivut 164–192. University of Michigan. USA 2000.
ISBN 0-472-06724-9.

[26] Nordman, Mika. Issues on using QoS in tactical ad hoc networks.
Teoksessa Jormakka, Jorma & Oksa, Sakari (toim.). Technical Solutions for Network Enabled Defence. Sivut 35–48.
MPKK, Tekniikan laitos. Helsinki 2006.
ISBN 951-25-1723-X.

[27] PHA: Puolustushallinnon asiasanasto.
http://www.puhaas.net/index.php [viitattu 23.4.2012].

[28] Qiu, Yihui & Chen, Zhide & Xu, Li. Active Defense Model of Wireless Sensor Networks Based on Evolutionary Game Theory.
Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on. IEEE 2010.

[29] Raitasalo, Jyri & Sipilä, Joonas. Sodan määrittelystä.
MPKK, Strategian laitos. Helsinki 2004.
ISBN 951-25-1489-3.

[30] Sallhammar, Karin & Helvik, Bjarne E. & Knapskog, Svein J. Towards a Stochastic Model for Integrated Security and Dependability Evaluation.
Proceedings of the First International Conference on Availability, Reliability and Security. IEEE 2006.

[31] Seppälä, Jari. Security Questions of Network Centric Warfare.
Sivut 181–190 teoksessa Jormakka, Jorma & Candolin, Catharina (toim.).
Technical Aspects of Network Centric Warfare.
MPKK, Tekniikan laitos. Helsinki 2004.
ISBN 951-25-1499-0.

[32] Stallings, William. Cryptography and Network Security – Principles and Practices.
Pearson Education Inc. USA 2003.
ISBN 0-13-091429-0.

[33] Suppes, Patrick. The Philosophical Relevance of Decision Theory.
Teoksessa Suppes, Patrick. Studies in the Methodology and Foundations of Science. Selected Papers from 1951 to 1969.
D. Reidel. Dordrecht 1969.
ISBN 978-9048183203.

[34] Tanenbaum, Andrew S. Computer Networks.
Pearson Education, Inc. New Jersey 2003.
ISBN 0-13-038488-7.

[35] Theodorakopoulos, George & Baras, John S. Game Theoretic Modeling of Malicious Users in Collaborative Networks.
IEEE Journal on Selected Areas in Communications, Vol. 26, No. 7, September 2008. IEEE 2008.

[36] Vankka, Jouko. Maavoimien taktisen verkon tekniikat ja standardit.
Viestikoulu/Viestirykmentti. Helsinki 2009.
ISBN 978-951-25-2025-1.

[37] Viestintävirasto. Tietoturva ja -suoja.
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html [viitattu 23.4.2012].

[38] von Neumann, Jon & Morgenstern, Oskar. Theory of Games and Economic Behaviour. Princeton University Press. Princeton 1944.
ISBN 691-04183-0.