Susanna Jääskeläinen

KYBERSODAN ANALYSOINTIA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

TIIVISTELMÄ

Jääskeläinen, Susanna
Kybersodan analysointia
Jyväskylä: Jyväskylän yliopisto, 2017, 31 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Moilanen, Panu

Tämä tutkielma on kirjallisuuskatsaus, johon lähteinä on käytetty pääasiassa tieteellisiä artikkeleita ja kirjoja. Tutkielman tarkoituksena on perehtyä kybersodan käsitteeseen ja sen käyttötapoihin sekä siihen, onko kybersotaa olemassa. Käsitteen moderniuden johdosta sen määritelmät eroavat tutkijasta ja lähteestä riippuen huomattavasti toisistaan, mutta tutkielmaan onnistuttiin löytämään suhteellisen kattava kuva kybersodasta.

Asiasanat: kybersota, kyberhyökkäys, kyberavaruus, sota, teknologia, tietoyhteiskunta

ABSTRACT

Jääskeläinen, Susanna
Analyzing Cyberwar
Jyväskylä: University of Jyväskylä, 2017, 31 p.
Information systems science, Bachelor's Thesis
Supervisor(s): Moilanen, Panu

This thesis is a literature review that is based mainly on scholarly articles and books. The purpose of this study is to familiarize with the concept of cyberwar and way of using the term, and consider the existence of cyberwar. In consequence of the modernity of the term its definitions differs significantly depending on the scholar and the repository. However, a relatively extensive concept of cyberwar was found based on the literature.

Keywords: cyberwar, cyberattack, cyberspace, war, technology, information society

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Johdantoluvussa pyritään kuvaamaan tutkielman aihe mahdollisimman tarkasti. Aiheen kiinnostavuus tutkimuksen kannalta perustellaan ja tutkielman rakenne käydään lyhyesti läpi. Käytetyt tutkimusmenetelmät, kuten myös tutkimuksen tavoite kuvataan. Noiden lisäksi johdannossa esitellään saavutetut tulokset ja niiden merkitys tutkimukselle.

On löydettävissä tieteellisiä lähteitä, joiden mukaan kybersota on kansallisvaltion toimia tunkeutua toisen valtion tietokoneisiin tai verkostoihin, tarkoituksenaan aiheuttaa vahinkoa tai häiriötä (esim. Clarke & Knake, 2011). Toisaalla kuvataan, että kybersodalla voidaan tarkoittaa pelkästään globaalissa verkossa tapahtuvaa häirintää ja vakoilua (Tiilikainen, 2015). Kybersodan sekä hyökkääjäettä kohdeosapuolena nähdään useimmiten valtiollinen toimija, mutta joissain määritelmissä myös yritykset voivat olla osapuolena kybersodassa. Sotivien osapuolten lisäksi myös tavalliset kansalaiset voivat kärsiä kybersodasta merkittävästi. Mielipiteet kybersodan toteutumismahdollisuudesta eroavat ehdottomasta kieltämisestä ehdottomaan myöntämiseen. Jotkut näkevät, että kybersotaa on jo käyty lähimenneisyydessä, kun taas toisten mielestä kybersotaa ei ole ollut eikä tule koskaan olemaankaan. Kaikki edellä mainittu osoittaa sen, ettei kybersotakäsitteen määritelmästä ole yhtenäistä, universaalia näkemystä.

Motiivi kybersota-käsitteen analysoinnille on löydettävissä sekä arkielämästä, että tieteen tekemisestä. Kybersodasta puhutaan lehtien otsikoissa ja ihmisten välisissä keskusteluissa, vaikka vain harvoilla on keskenään samankaltainen käsitys sanan merkityksestä. Kybersotaan liittyvää tieteellistä kirjallisuutta on julkaistu, mutta eri artikkeleiden tai teosten sisällöt voivat olla hyvinkin ristiriitaisia keskenään. Tutkimuksen kannalta on keskeistä tarkoituksenmukaisten käsitteiden käyttäminen, joten kybersota-käsite kaipaa ehdottomasti syvempää tarkastelua. Tässä tutkielmassa pyritään löytämään irrallisten argumenttien sijaan tukevia perusteita sille, mitä kybersota todellisuudessa tarkoittaa. Tämän paperin luettua lukija voi paremmin ymmärtää, mitä kyseisellä käsitteellä tarkoitetaan. Tavoitteena tutkielmassa on siis löytää vastaus seuraaviin tutkimuskysymyksiin:

- Mitä kybersota-käsite tarkoittaa?
- Mistä kybersota juontaa juurensa?

Tämä tutkielma on kirjallisuuskatsaus, joten siinä viitataan useisiin lähteisiin ja niitä vertaillaan toisiinsa. Tutkielmassa esitellään kattava katsaus kybersotaa käsittelevään tieteelliseen kirjallisuuteen. Lähteiden valintaprosessiin panostettiin, ja käytetyt lähteet pyrittiin rajaamaan kaikkein laadukkaimpiin ja relevantteihin. Seuraavaksi kerrotaan, millä perusteilla ja mistä lähteitä etsittiin, ja kuinka ne rajattiin nykyiseen muotoonsa.

Lähteiden valintaan vaikutti se, kuinka monesti lähteisiin oli viitattu. Sellaisia lähteitä ei otettu käytettäväksi tutkielmaan, mihin on niiden julkaisun jälkeisenä aikaan verrattuna viitattu suhteellisen vähän, tai ei ollenkaan. Osa tutkielmassa käytetyistä julkaisuista on luokiteltu korkeatasoisiksi julkaisufoorumissa, mutta näin ei ole kaikkien julkaisujen kohdalla. Sellaisiakin lähteitä, jotka eivät ainakaan toistaiseksi ole saaneet korkeaa luokitusta julkaisufoorumissa, on sisällytetty tutkielmaan. Tämä perustellaan siten, että kybersota-aiheen ja joidenkin julkaisukanavien uutuus vaikuttaa niiden löytymiseen julkaisufoorumissa.

Lähdemateriaalia etsittiin tietokannoista sekä suomen että englannin kielellä. Muun muassa seuraavia hakusanoja käytettiin: kybersota (engl. cyberwar), kybersodankäynti (engl. cyberwarfare), kyberavaruus (engl. cyberspace), sota (engl. war) ja sodankäynti (engl. warfare). Osasta valittujen, useita viittauksia saaneiden lähteiden lähdeluetteloista löydettiin edelleen uusia lähteitä käytettäväksi. Tämän lisäksi sopivaa lähdekirjallisuutta oli saatavilla Jyväskylän ammattikorkeakoulun kirjastossa.

Tämän tutkielman kirjoitusprosessi tapahtui muutamassa osassa. Aluksi hahmoteltiin paperille koko tutkielman sisältöä, ja osa noista hahmotelmista päätyi sellaisenaan tutkielman johdantolukuun. Kyseisiin hahmotelmiin luonnollisesti tuli kirjoittamisprosessin edetessä melko runsaasti muutoksia, joten johdantoluku valmistui vasta prosessin loppuvaiheessa. Tutkielman toinen luku kirjoitettiin ensimmäisenä, sillä itse *sodan* ja sen kehittymisen tarkastelu nähtiin välttämättömänä kybersodan ymmärtämiseksi. Sotaa käsittelevän kappaleen lähdemateriaalina käytettiin sekä uudempia tekstejä, että jopa yli kaksi sataa vuotta vanhaa teosta. Seuraavaksi kirjoitettiin kolmas, kybersotaa käsittelevä luku, joka oli luonnollinen jatkumo toisen luvun viimeisimmälle alaluvulle, jossa käsiteltiin konflikteja tietoyhteiskunnassa. Tämän jälkeen tehtiin yhteenveto tutkielman viimeiseen lukuun, minkä rinnalla myös johdantoa hiottiin niin, että myös ensimmäinen ja viimeinen luku ovat yhteneväisiä keskenään. Tutkielman ensimmäisen raakaversion jälkeen saadun palautteen perusteella sen jokaista lukua hiottiin, jotta lopullinen teksti saatiin aikaiseksi.

Tutkielman toinen luku käsittelee sotaa ja sodankäynnin evoluutiota. Sodankäynnin historiaa käydään lyhyesti läpi tuhansien vuosien takaa aina nykypäivään saakka, minkä jälkeen sodan määritelmä esitellään. Näiden jälkeen toisessa luvussa kuvataan sitä yhteiskunnallista muutosta, joka on vaikuttanut konfliktien luonteen muuttumiseen. Moderni yhteiskuntamuoto eli tietoyhteiskunta, kuten myös sen vaikutukset konflikteihin esitellään: informaatioteknologian vakiinnuttua kiinteäksi osaksi yhteiskuntaa myös kohteet ja tavat, joihin konflikti-

tilanteissakin usein pyritään vaikuttamaan, ovat muuttuneet. Kolmannessa luvussa esitellään lähdeaineistosta löytyneitä määritelmiä kybersodalle, sekä niiden yhtäläisyyksiä ja eroavaisuuksia. Havaintojen pohjalta laaditaan kybersodalle uusi, kattavampi määritelmä. Tämän jälkeen luvussa tarkastellaan lähdeaineistossa kuvattuja tapahtumia, joita on perusteltu kybersodaksi. Kyseisiä tapahtumia arvioidaan uuden kybersodalle annetun määritelmän pohjalta. Tämän myötä pohditaan, onko kybersotaa vielä ollut olemassa, ja että voiko sitä tapahtua tulevaisuudessa. Tutkielman viimeisessä luvussa vedetään yhteen löydetyt tulokset, ja esitetään arvioita siitä, mikä on vaikuttanut huomattaviinkin eroavaisuuksiin kybersodan määritelmissä. Havaintojen pohjalta tuodaan ilmi aiheeseen liittyvät puutteet nykyisessä lähdekirjallisuudessa. Viimeisessä luvussa esitellään myös tämän tutkielman rajoitteet sekä tutkielman kirjoittajan esittämät jatkotutkimusaiheet kybersotaan liittyen.

2 SODAN JA YHTEISKUNNAN KEHITTYMINEN

Tässä luvussa tarkastellaan konfliktitilanteiden sekä yhteiskunnan kehittymistä vuosituhansien aikana. Aiheen kannalta olennaiset käsitteet ja niiden määritelmät esitellään, jotta niiden käyttäminen ja merkitysten ymmärtäminen ovat yhtenäisiä läpi tutkielman. Lisäksi sodankäynnin evoluutiota esitellään aina nykypäivään asti. Tämän luvun tiedot vastaavat toiseen tutkimuskysymykseen, eli kybersota-käsitteen alkujuurien tunnistamiseen. Tämä johtuu ennen kaikkea kahdesta asiasta:

- Kybersota-käsite on kaksiosainen, *kyber* ja *sota,* joista jälkimmäistä tarkastellaan tässä luvussa.
- Yhteiskunnat ovat tulleet ajan myötä riippuvaiseksi informaatioteknologiasta, joka on väline kyberin ylläpitämiseksi.

Ihmiskunnan pitkän historian aikana yhteiskuntarakenteet ja kulttuurit ovat muuttuneet huomattavasti. Teknologian kehitys rinnastetaan usein kulttuurievoluutioon, sillä uudet teknologiat ovat yksi näkyvimmistä uuden ajan merkeistä (Webster, 2014). Teknologialla pyritään tehostamaan tekemistä tai tekemään kokonaan jotain sellaista, mitä ilman sitä emme voisi tehdä. Jotta kulttuurievoluutio on voinut kehittyä nykyisen kaltaiseksi, teknologian ja kulttuurin kehittyminen ovat pitäneet yllä toinen toistaan. Mulderin, Ferrerin, ja Van Lenten (2011) mukaan teknologia on ollut suuressa roolissa kohtaamiemme ongelmien luomisessa, mutta se on merkittävä tekijä myös kyseisten ongelmien ratkaisemisessa. Heidän mukaansa teknologia on niin kietoutunut nykyiseen yhteiskuntaan, että ilman sitä yhteiskuntamme romahtaisi. Teknologia yhdessä muun yhteiskuntakehityksen osana on muokannut myös konflikteja etenkin viimeisen muutaman tuhannen vuoden aikana. Ymmärtääkseen tässäkin tutkielmassa käsiteltävää kybersotaa, täytyy tarkastella yleisesti myös sodankäynnin historiaa ja sen kehittymistä, sekä siirtymistä nykyiseen tietoyhteiskuntaan. Sota käydään aina sen aikaisessa kontekstissaan, joten siinä käytettävät aseet ovat ajankohtaisen teknologian mukaiset. (Mehan, 2009.)

2.1 Sodankäynnin historia

Kuten luvussa 2 kuvattiin, kybersota-käsite on kaksiosainen. Vastatakseen toiseen tutkimuskysymykseen kybersodan alkujuurista, täytyy ymmärtää myös sotaa ja sen historiaa. Tässä alaluvussa kuvataan lyhyesti sodankäynnin evoluutiota muutaman tuhannen vuoden ajalta. Konfliktit tai sodankäynti ovat olleet osa ihmiskunnan historiaa kautta aikojen. Ensimmäisissä ihmisten välillä käytävissä konflikteissa välineinä käytettiin nyrkkejä, keppejä ja kiviä, joten kehitys niistä modernimpien konfliktien luonteeseen on ollut huomattava.

Dennen (1995) kuvaa, että sota sai alkunsa jossain päin Mesopotamiaa noin viisi tuhatta vuotta sitten. Mehan (2009) kuvaa kirjassaan ensimmäistä sodankäynnillistä mullistusta, joka tapahtui noin 3500 eaa pronssikauden myötä. Tuolloin sotavälineet muuttuivat miekkoihin, kirveisiin, jousiin, ja sotavaunuihin teknologian kehittymisen myötä. Välineistön muuttumista tärkeämpää oli kuitenkin yhteiskunnallisten rakenteiden muutokset. Toisin kuin aikaisemmin, tuona aikana keskitettyjä valtiollisia instituutioita ja hallinnollisia järjestelmiä alkoi nousta toimintaan, mitkä onnistuivat suuntaamaan resursseja yhteisölähtökohtaisiin tavoitteisiin. Se helpotti vakaampien sotilaallisten rakenteiden kasvua, ja ne kehittyivätkin pian pysyväksi osaksi yhteisöä ja sotilaallista järjestelmää. Mehanin (2009) mukaan muutos oli seurausta suuremman yhteisön psykologisten suhteiden evoluutiosta liittyen julkiseen sosiaaliseen suhteeseen, minkä myötä heimot alkoivat muotoutua kohti laajempaa sosiaalista kokonaisuutta eli valtiota. Suuren yhteisön tai valtion halutessa selvitä muiden yhteisöjen saalistavasta toiminnasta, sodankäynnistä piti tulla niitä kuvaava tunnusmerkki. Useat sotilaalliset, poliittiset, taloudelliset, psykologiset ja sotilaalliset muutoksen noin kahden tuhannen vuoden aikana teki sodasta suhteellisen normaalin osan sosiaalista runkoa. Sodankäynnin luonne pysyi melko vakiona tuhansien vuosien ajan.

Moderni sodankäynti sai alkunsa Euroopassa käydyn satavuotisen sodan myötä, mikä käytiin vuosina 1337-1457. Tuolloin kuvaan tulivat myös ammattimaiset armeijat ja tuliaseet. 1900-luvulla käydyt maailmansodat olivat tuhoisimpia ihmiskunnan tähänastisista konflikteista, sillä teknologian edelleen kehityttyä käytössä oli aseita, tankkeja, pommeja, tykkejä, ja ohjuksia. Välineistön lisäksi aikaisempaan verrattuna maailmansodissa uutta oli myös se, että niissä toisiaan vastakkain olevat voimat olivat massiivisia ja toisiinsa nähden symmetrisen suuria. Ajattelutapa siitä, että sota oli osa tavanomaista elämää, pysyi pinnalla Neuvostoliiton hajoamiseen asti, mikä tapahtui vuonna 1991. Sen jälkeen epäsymmetriset konfliktit alkoivat yleistyä. Epäsymmetrisillä konflikteilla tarkoitetaan pienemmän voimakkuustason konflikteja, kuten esimerkiksi vastatoimia kapinallisuuksiin, kaupunkialueilla käytäviä taisteluita, ja rauhanturvaamisoperaatioita. Epäsymmetriset konfliktit ja niissä käytettävät taktiikat, välineet, ja osaaminen siis eroavat huomattavasti tavanomaisesta sotavoimien käytöstä. Nykyään kiinnitetyllä sotavyöhykkeellä toimivat massiiviset sotilasvoimat ovat hyvin epätodennäköisiä. (Mehan, 2009.)

Schmitt (2010) kuvaa artikkelissaan, kuinka historiallisessa sodassa sen aloittaminen oli riippuvainen sodanjulistuksesta. Sodanjulistus ei vaatinut sotatoimia, eivätkä sotatoimet itsessään merkinneet sotaa. Edellä kuvatun kaltainen

ymmärrys sodasta on nykypäivän lähestyessä korvattu monimutkaisella joukolla laillisia konsepteja. Toisen maailmansodan jälkeen kansainvälinen yhteisö laati Yhdistyneiden kansakuntien (YK) peruskirjan. Peruskirja sisältää sekä kiellon voimakeinojen käyttämisessä kansainvälisissä suhteissa, että menetelmät lainsäädännön täytäntöönpanolle. Toisen maailmansodan johdosta myös sodankäynnin aikaiset säännökset tarkastettiin uudelleen. Tuolloin kumottiin vaatimus siitä, että ottaakseen sodan lait käytäntöön, täytyy sota ensin julistaa alkaneeksi. Siitä lähtien kyseiset lakipykälät tulivat huomiotavaksi heti, kun aseellisia konflikteja tapahtui.

2.2 Sodan määritelmä

Edellisessä alaluvussa kuvattiin, kuinka sodankäynti on muuttunut vuosituhansien aikana, mutta varsinaista määritelmää sodalle ei vielä annettu. Tämä johtuu siitä, että sodan määritelmä on vakiintunut vasta viimeisen parin sadan vuoden aikana. Sodan määritelmä on tämän tutkielman kybersotaan liittyvien tulosten kanna hyvin oleellinen. Se johtuu siitä, että koska kybersota on käsitteenä kaksiosainen, sen analysoimiseksi siitä täytyy määritellä käsitteen molemmat osat. Ensimmäisenä määritellään sota, sillä siitä lähdettäessä liikkeelle tutkielmassa käsiteltävä aihe etenee luonnollisimmin.

Sotaa määritellessä kannattaa lähteä liikkeelle kenties maailman tunnetuimman sotateoreetikon Carl von Clausewitzin teoksesta vuodelta 1867. Clausewitz (1867) mukaan sodalla on kaksinainen luonne siinä suhteessa, että vihollinen voidaan joko haluta nujertaa, tai sitten tavoitteena on suorittaa vain joitain valloituksia valtakunnan rajoilla. Nujertamisen tarkoituksena on tuhota vastustajan poliittinen olemassaolo, tai saattaa se puolustuskyvyttömään tilaan rauhan hyväksymiseksi. Alueellisia valloituksia valtakunnan rajoilla tehdään joko sen takia, että ne halutaan ottaa haltuun pysyvästi, tai niitä halutaan käyttää vaihdon välineenä rauhaa solmittaessa. Kaksinaisen luonteen lisäksi huomioitavaa hänen mukaansa on myös se, että sota on ainoastaan politiikan jatkamista toisin keinoin.

Clausewitz (1867) määrittelee sodan olevan kokonaisuudessaan kolmielementtinen. Nuo kolme elementtiä ovat seuraavat:

- sota täytyy aina ymmärtää poliittisessa mielessä,
- sodalla on oltava sekä keinot, että päämäärä saattaa vastustaja puolustuskyvyttömäksi, ja
- sota on väkivaltainen.

Yllä mainittujen kolmen pysyvän elementin lisäksi Clausewitz (1867) kuvaa sotaa kameleonttina, joka lakkaamatta mukauttaa muotoaan olemassaolevien olosuhteiden mukaisesti. Hänen mukaansa puolustus on sodankäynnin vahvin muoto.

YK: mukaan sota on järjestäytyneiden yhteisöjen välinen aseellinen konflikti, jossa saa surmansa keskimäärin vähintään tuhat henkilöä vuodessa (ks. esim Singer & Small, 1994). Cioffi-Revilla (1996) kuvaa sotaa järjestäytyneiden,

aseellisten, ja keskenään vastakkaisten sosiaalisten ryhmien välisenä tappavana konfliktina. Hänen mukaansa sotaa esiintyy kulttuurista ja sijainnista riippumatta maailmanlaajuisesti, ja se on kiinteästi osana maailmanpolitiikkaa.

Yllä kuvatun perusteella voidaan todeta, että sota on väkivaltainen konflikti, joka esiintyy aina poliittisessa kontekstissa. Sodalla tulee olla alku ja loppu, ja siinä on osapuolena järjestäytyneet sosiaaliset yhteisöt, useimmiten valtiot. Sota on kameleontti, joka mukautuu sitä ympäröiviin olosuhteisiin. Näiden lisäksi sota on kokonaisuudessaan järjestelmällistä, niin hyökkäysten kuin puolustuksenkin osalta.

2.3 Yhteiskunnan muutos tietoyhteiskunnaksi

Kahdessa edellisessä alaluvussa avattiin sodan merkitystä ja historiaa. Mehankin (2009) toteaa, että sota käydään aina sen aikaisessa kontekstissaan. Sodan kontekstina voidaan selkeästi nähdä yhteiskunta tai –kunnat, joissa sotaa käydään. Yhteiskuntamuodoista viimeisin tähän asti on tietoyhteiskunta, joten se vallitsee parhaillaan länsimaissa. Ymmärtääkseen sotaa paremmin, tulee osata tarkastella myös itse yhteiskuntaa. Seuraavassa sisältöluvussa käsiteltävän kybersodan yksi lähtökohdista on täten myös tietoyhteiskunnan ymmärtäminen, johon tutustutaan tässä alaluvussa. Kuten yhteiskuntamuodon nimestäkin voin päätellä, *tiedosta* on tullut perusta moderneille talousjärjestelmille ja sekä sen merkittävyys, että kontrollointi kasvaa jatkuvasti niin liiketoiminnan kuin valtioiden osalta (Beniger, 2009).

Muiden muassa Webster (2014) on tutkinut tietoyhteiskuntaa ja siihen liittyviä näkökantoja. Hän on erottanut viisi eri määritelmää, joiden kannalta voidaan perustellusti tunnistaa tietoyhteiskunnan jo tapahtunutta ja jatkuvaa kehittymistä. Kyseisten eri määritelmien keskeisin tekijä on joko

- teknologinen,
- taloudellinen,
- ammatillinen,
- avaruudellinen, tai
- kulttuurinen.

Kuten aikaisempienkin ajanjaksojen murrosvaiheissa, myös tietoyhteiskunnan suhteen uudet teknologiat merkitsivät uuden yhteiskuntamuodon saapumista. Webster (2014) on tunnistanut kaksi eri vaihetta siinä teknologisessa kehityksessä, joka lopulta aiheutti järjestelmällisen yhteiskunnallisen muutoksen. Ensimmäinen vaihe oli 1970-luvun lopulla ja 1980-luvun alussa, kun tietojenkäsittelytieteilijät/-tutkijat ja kommentaattorit löysivät mikrosirujen mahdollisuudet. Toinen vaihe alkoi 1990-luvun puolessavälissä, jonka jälkeen useat kommentaattorit ovat uskoneet, että tieto- ja viestintäteknologioiden (ICT) yhteenliittyminen on aiheuttanut uudenlaiseen yhteiskuntaan siirtymisen. Teknologisia uudistuksia ovat olleet esimerkiksi sähköposti ja online-viestintä, sekä internetin pikainen

kasvu ja sen tuomat mahdollisuudet talouteen, koulutukseen ja tasa-arvoisempaan toimintaan. Edellisten lisäksi valtakunnallinen, kansainvälinen, ja globaali tiedonvaihtaminen esimerkiksi pankkien, yritysten, valtionhallintojen, ja yliopistojen välillä on muodostanut teknologista infrastruktuuria, joka mahdollistaa välittömän kommunikoinnin ajasta tai paikasta riippumatta (Connors, 1993).

Websterin (2014) tietoyhteiskuntaa tarkasteleva taloudellinen näkökulma käsittelee asiaa bruttokansantuotteen (BKT) kantilta. Mikäli valtion BKT: teen nousemisen on selitettävissä osittain informaatioon perustuvalla liiketoiminnalla, voidaan jossain vaiheessa todeta, että eletään tietoyhteiskunnassa. Ammatillinen lähestymistapa tietoyhteiskuntaan käsittää sen, että mikäli enemmistö ammateista löytyy tietotyöstä, tietoyhteiskunta on saavutettu. Teollisten työpaikkojen väheneminen ja palvelusektorin töiden lisääntyminen ilmenevät niin, että manuaalisen työt korvataan toimistotyöllä. Informaatio nähdään työn raakamateriaalina, mikä ilmentää tietoyhteiskunnan tuloa.

Avaruudellisella elementillä tietoyhteiskunnassa tarkoitetaan Websterin (2014) mukaan sitä, että tietoverkostot yhdistävät eri sijainteja, olivatpa ne sitten samassa rakennuksessa, kaupungissa, maakunnassa, maanosassa, tai missä päin maailmaa tahansa. Elämme siis verkottuneessa yhteiskunnassa, jossa voimme ICT:n avulla kurkottaa lähes mihin maailman kolkkaan tahansa, sekä työ- että yksityiselämässä. Teknologinen kehitys on mahdollistanut nyky-yhteiskunnassamme sen, ettei maailmassa eläminen ja toimiminen ole enää ollenkaan niin paikkasidonnaista kuin aikaisemmin.

Websterin (2014) viimeinen, kulttuurinen elementti tietoyhteiskunnasta on helpoiten havaittavissa, mutta vähiten mitattu. Jokainen on havainnut tiedon määrän valtavan kasvun sosiaalisessa ympäristössämme. Se on tapahtunut muun muassa television ja tietokoneiden yleistyttyä, sekä mainostuksen ja uutisoinnin lisääntymisen myötä. Mediakyllästeinen elämä, jossa eri symbolit ympäröivät meitä ja tietoa vaihtuu jatkuvasti, on meille jo itsestäänselvyys. Median täyteisen arjen lisäksi tieto on ehkä tiedostamattammekin lähempänä henkilökohtaista olemustamme kuin ennen. Nykyään esimerkiksi ulkonäkö on ihmisille merkittävämpää kuin aikaisemmille sukupolville, ja omaan ulkonäköön liittyviä asioita reflektoidaan tietoon muodista ja trendeistä.

Tietoyhteiskunnan käsittelyn pohjalta voidaan todeta, että informaation ja ICT:n merkitys ulottuu merkittävästi yhteiskuntien eri toiminta-alueille. Tämän myötä yhteiskunnat ja niiden toiminnot ovat tulleet laajalti myös riippuvaisiksi kyseisitä elementeistä. Tietoyhteiskunta sodankäynnin kontekstina on täten muuttanut huomattavasti myös sotia ja konflikteja.

2.4 Sota ja modernit konfliktit tietoyhteiskunnassa

Tietoyhteiskunnan mukanaan tuomien muutosten myötä länsimaisten yhteiskuntien toiminnat ovat nykyään laajalti riippuvaisia informaatioteknologioista ja verkostoista. Esimerkiksi kriittinen infrastruktuuri, maksuliikenne, ja hätätapauksista viestiminen ovat kehittyneet tietoyhteiskunnan muotoutuessa. Internetin liittäminen kaikkialle on luonut digitalisoidun maailman, joka on erittäin

heikko sekä tahattomille että tahallisille keskeytyksille. (Stiennon, 2010.) Aikaisemmin tutkielmassa esitelty YK:n peruskirja yhdessä muiden asiaan liittyvien kansainvälisten lakisääntöjen kanssa ohjaa vielä nykypäivänäkin sitä, kuinka ja milloin valtiot saavat käyttää voimakeinoja (Schmitt, 2010).

Tietoyhteiskunnan myötä myös sota ja konfliktit ovat modernisoituneet. Sana *kyber* on pudotettu abstraktimmasta merkityksestä myös turvallisuus- ja konfliktikontekstiin. Kyberiä käytetään useimmiten etuliitteenä muissa sanoissa, mutta sen voi nähdä käytettävän myös irrallaan oikeanlaisessa kontekstissa. Termillä viitataan virtuaaliseen, globaaliin, tietokoneiden ja internetin välityksellä ylläpidettävään maailmaan, jonka keskiössä on valtavat määrät dataa ja niistä johdettavaa informaatiota. Se muodostaa käyttäjilleen ympäristön erilaisiin aktiviteetteihin, kuten tiedonhakuun, kommunikointiin, opiskeluun, työntekoon, rikollisuuteen, valtion toimimiseen ja moniin muihin. Yhdysvaltojen tiedustelupalveluiden jokavuotisessa uhka-arvioraportissa vuonna 2016 kyberuhat listattiin maan vakavimmaksi uhaksi (Clapper, 2016), ja Suomessa kyber mainittiin ensimmäisen kerran yhteiskunnan turvallisuusstrategiassa vuonna 2010 (Suomen valtioneuvosto, 2010).

Gartzken (2013) mukaan Yhdysvallat ja muut valtiot ovat jo alkaneet tekemään kalliita muutoksia valmistautuakseen internetin välityksellä käytäviin sotatoimiin. Ainakin Yhdysvallat ja Kiina on todistetusti käyttäneet verkkosodankäyntiä ja kybervakoilua osana sotatoimia. Viro, Liettua, Intia, Pakistan ja Israel-Palestiinan molemmat puolet, sekä Pohjois- ja Etelä-Korea ovat osa kyberkonfliktien nousukautta. Kyberin avulla toteutetut konfliktit ovat edellä mainituissa onnistuneet ainakin propagandan ja ideoiden sodan osalta. Kyber ja internet nähdään toisaalta konflikteihin liittyvien toimenpiteiden suhteen demokratisoivana tekijänä (Stiennon, 2010.), kun taas toisaalla sen nähdään lähinnä suurentavan olemassa olevia kansainvälisiä eroavaisuuksia vallassa ja vaikuttamisessa (Gartzke, 2013).

Arquillan ja Ronfeldtin (1999) mukaan teknologian kehittymisen myötä kuvaan on tullut myös verkkosodankäynti (*engl. netwar*). Verkkosodankäynnillä tarkoitetaan uudenlaisia konflikteja sekä rikoksia yhteiskunnallisella tasolla, mitkä ovat ja tulevat olemaan keskeinen osa yhteiskuntaamme. Sekä uudet että vanhat teknologiat, kuten myös verkostot internetin ohella ovat osa verkkosodankäyntiä, ja sen toimenpiteet sekä vaikutukset realisoituvat itse verkostojen lisäksi myös niiden ulkopuolelle. Verkkosodankäynnin osapuolet eivät useimmiten ole valtiollisia, vaan voivat olla jopa täysin kansalaisuudettomia ja rajat ylittäviä, esimerkiksi terroristijärjestöjä. Vahvasti hierarkkisten rakenteiden, kuten joidenkin valtioiden, on hankalampi taistella verkostoja vastaan. Tietoyhteiskunnan myötä tulleiden uusien teknologioiden aikaiset omaksujat ovat paremmassa asemassa niistä saatavan hyödyn suhteen, kuin ne myöhemmin käyttöönottavat osapuolet.

Yksi selvästi erottuva kehityssuunta konfliktien suhteen on se, että niitä ja niiden ratkaisuja on alettu punnitsemaan talouden näkökulmasta yhä enemmän. Perinteinen sota on hyvin kallista verrattuna kyberin avulla toteutettaviin konflikteihin: on huomattavasti halvempaa kouluttaa kyberosaajia kuin rakentaa miljoonien arvoinen sotakoneisto. (Tiilikainen, 2015.)

Sota- ja konfliktikontekstissa kyberin lisäksi puhutaan nykyisin myös hybridistä ja hybridisodasta. Hybridillä perinteisesti ymmärretään joidenkin eri asioiden risteytymistä tai yhdistymistä, ja hybridisota yhdistääkin perinteistä sotaa moderneihin toimintoihin. Hybridisodankäynnilliset keinot ovat sekä sotilaallisia että ei-sotilaallisia (Hoffman, 2007). Renzin ja Smithin (2016) mukaan hybridisodankäynnillä kuvataan konseptia, joka näyttää tarjoavan hyödyntäjälleen uuden kaavan sodan voittamiseksi. Tiilikaisen (2015) mukaan hybridisodassa on kolme elementtiä:

- kineettinen,
- tiedustelullinen, ja
- informaatiosodankäynnillinen.

Kineettisellä elementillä tarkoitetaan perinteistä, fyysiseen väkivaltaan pohjautuvaa sotaa. Clausewitzinkin (1867) esittämä silmitön tappaminen tarvittaessa ei kuitenkaan Tiilikaisen (2015) mukaan onnistu enää nykymaailmassa. Hänen mukaansa sota voi nykyään alkaa niin, että näyttää aivan kuin sota käytäisiin rauhan tilassa. Nollatappioihin pyrkiminen ohjaa sotilaallisteknistä kehitystä miehittämättömien aseiden ja vastaavien suuntaan, ja perinteinen sotajoukko-vastaan-sotajoukko –asetelma on nykymaailmassa vanhanaikainen. Huolimatta sodankäynnin väkivaltaisen luonteen laimenemisesta sota on edelleen erittäin voimakasta.

Tiilikainen (2015) näkee tiedusteluelementti-käsitteen yksiselitteisenä, eli mahdollisen tehokkaana tiedusteluna läpi koko sotaan ja sen osapuoliin liittyvällä kohdealueella. Informaatiosodankäynnillinen elementti sisältää sekä informaatiosodankäynnin, että kybersodankäynnin, joista jälkimmäistä käsitellään tutkielman kolmannessa luvussa. Tämä kolmas elementti on hybridisodankäynnin uusin ja tuntemattomin alue.

Moderneja konflikteja on kuvattu edellä mainittujen lisäksi muun muassa ”uusiksi sodiksi”, neljännen sukupolven sodankäynniksi ja asymmetriseksi sodankäynniksi. Niitä on käytetty käsitteellistämään nykyaikaisen sodankäynnin muutoksia yhdenmukaisesti niiden ideoiden kanssa, joiden mukaan modernit sodat eroavat huomattavasti vanhemmanmallisista konflikteista. Hybridisotaa erillisenä sodankäynnin muotona on kritisoitu muun muassa siinä mielessä, että kaikki sodat voidaan nähdä tietyllä asteella ”hybridiksi”. (Renz & Smith, 2016.)

Vastaus toiseen tutkimuskysymykseen eli siihen, mistä kybersota juontaa juurensa, on löydettävistä kokonaisuudessaan luvusta 2. Konfliktien ja sodan historiaa ja kehittymistä avattiin ja huomattiin, että ne ovat kiinteä osa yhteiskuntien ja politiikan toimintaa. Tämän lisäksi sotien mukautumista vallitseviin olosuhteisiin esiteltiin, jotta sodan niin sanotusti kameleontti luonne voidaan ymmärtää. Tutkielman seuraavassa luvussa edetään kybersodan käsittelemiseen, jolloin saadaan vastaus myös ensimmäiseen tutkimuskysymykseen.

3 KYBERSOTA

Kolmas luku tuo sodankäynnin käsittelemisen lähemmäs 2000-lukua ja sen ensimmäisille vuosikymmenille, jolloin tietoyhteiskunta on vakiintunut ihmiskuntaamme. Kybersota nähdään niin ajankohtaisena, että modernien valtioiden tulisi alkaa valmistautua siltä suojautumiseen. Sillä on sekä suoria että epäsuoria vahingollisia vaikutuksia fyysiseen infrastruktuuriin. (Colarik & Janczewski, 2015). Tässä luvussa tarkastellaan kybersodan määritelmiä sekä niiden eroavaisuuksia ja yhtäläisyyksiä. Kybersotaa puoltavia ja kieltäviä näkökantoja kuvataan paikoin lähes rinnakkain, jotta niille annettuja perusteluja on helpompi arvioida. Löydetyt esimerkit kybersodasta esitellään, ja kaikki edellä mainittu käsitellään niin, että aiheesta on mahdollista saada kattava kokonaiskuva. Tässä luvussa vastataan siis ensimmäiseen tutkimuskysymykseen, eli selvitetään, mitä kybersota-käsite tarkoittaa.

Kybersodan tarkastelemista aloittaessa yksi tavallisimmista kysymyksistä on se, että mikä kybersodankäynnin toimintaympäristö eli *kyberavaruus* on (Robinson, Jones & Janicke, 2015). Kyberavaruus on luonut uusia tapoja sekä kansainvälisen jännittyneisyyden pahentamiselle, että konfliktien välttämiselle (Choucri & Goldsmith, 2012) Kuehl (2009) on tullut tutkimuksensa pohjalta siihen tulokseen, ettei kyberavaruus ole ainoastaan tietokoneita ja digitaalisessa muodossa olevaa informaatiota. Hänen mukaansa kyberavaruuteen kuuluu neljä eri osaa, jotka tulee kaikki ottaa huomioon käsitettä määritellessä. Kyberavaruuden neljä osaa ovat seuraavat:

- operationaalinen tila, jossa ihmiset ja organisaatiot käyttävät teknologioita toimiakseen ja vaikuttaakseen, joko pelkästään kyberavaruudessa tai myös muilla vaikutusalueilla
- luontainen tila, joka on muodostettu sähkömagneettisien energian avulla ja johon pääsee sisään sähköisen teknologian avulla
- informaatioon perustuva alue, jossa luodaan, varastoidaan, muutetaan, vaihdetaan ja hyödynnetään informaatiota sähköisellä tavalla
- yhteiskäyttöverkko, jossa käytetään itsenäisesti ja yhteisesti käytettäviä verkostoja sähköisten informaatio-kommunikaatioteknologioiden avulla.

Kuehl (2009) on määritellyt kyberavaruuden olevan "informaatioympäristössä oleva globaali alue, jonka erottava ja uniikki ominaisuus on elektroniikan ja elektromagneettisen spektrin puitteissa tehty toiminta, jolla luodaan, varastoidaan, muunnellaan, vaihdetaan, ja hyödynnetään informaatiota itsenäisesti ja yhteisesti käytettävien verkostojen kautta, jotka käyttävät informaatio-kommunikaatioteknologioita." Internet-perustaiset kehitysaskeleet ja kyberavaruus antavat lähes kenelle tahansa mahdollisuuden levittää viestejä, joilla on mahdollisuus aiheuttaa häiriötä verkostoille ja kaupankäynnille, ilman verrattain suurta pelkoa kiinnijäämisestä. Kyberavaruudessa on hankala jäljittää, kuka on minkäkin nimenomaisen toiminnan takana, ja toiminnalla voi olla vaikutuksia ympäri maailman. (Choucri & Goldsmith, 2012.)

Ymmärrettäessä mitä kyberavaruus tarkoittaa, voidaan todeta, että jo kybersodan toimintaympäristö tekee siitä moniulotteisemman verrattuna perinteiseen sotaan. Kyberavaruus poistaa sodankäynnistä esimerkiksi maantieteelliset sekä fyysiseen voimaan liittyvät rajoitteet, ja mahdollistaa paljon nopeampisykliset sotatoimet. Se lähes mitätöi materiaan perustuvat vahvuudet, ja tekee sodasta vähemmän ihmisiä ja ympäristöä vahingoittavan tapahtuman.

3.1 Kybersodan määritelmät

Kybersodan toimintaympäristön tunnettua on helpompi käsittää kybersodan eri määritelmien ominaisuuksia. Kybersotaa määrittelemään on olemassa useita kuvauksia, joista on löydettäviä sekä yhteneviä että eriäviä piirteitä. Kaikki kyberhyökkäykset eivät ole kybersotaa vaan ne voidaan nähdä esimerkiksi pelkästään rikoksina. Tarkemmin organisoituja kyberoperaatioita kuvataan kybersodaksi ja –konflikteiksi useissa lähteissä. Kyberkonflikteja ei kuitenkaan ole vielä vakiinnutettu kansainväliseen lakiin (Gartzke, 2013), ja kansanvallat ovat väistelleet yrityksiä muotoilla kansainvälistä sopimusta, joka kattaisi kyberkonfliktit (Dunlap, 2011). Tämän voidaan todeta olevan yksi merkittävimmistä syistä sille, että kybersodan eri määritelmät voivat erota toisistaan huomattavasti.

Lähtiessä tarkastelemaan kybersotaa, sitä kannattaa lähestyä historian kannalta. Lewis (2002) muotoilee asian niin, että kybersodan tarkastelu tulee aloittaa sodan historiallisesta kontekstista, jossa infrastruktuuri on iskujen kohde. Hänen mukaansa yli yhdeksänkymmenen viimevuoden ajan eri strategioissa on painotettu hyökkäyksiä kriittiseen siviili-infrastruktuuriin. Tämän tutkielman toisessa luvussa todettiin, että tietoyhteiskunnan myötä ihmiset ovat tulleet laajalti riippuvaisiksi informaatioteknologiasta ja verkostoista. Kyberavaruutta käsiteltäessä huomattiin myös se, että tuo informaatioympäristö saadaan toteutettua muun muassa sähkön avulla. Noiden havaintojen pohjalta voidaan sanoa, että erilaisiin sähkö- ja tietoverkostoihin iskeminen toteuttaa Lewisin (2002) kuvaamaa sodalle tunnusomaista piirrettä iskeä siviili-infrastruktuuriin.

Stiennon (2010) lähtee kybersodan käsittelyssä liikkeelle siitä, että verkostojen ja teknologian hyödyntäminen hyökkäyksissä on sodankäynnin historian evoluutiota. Hänen mukaansa kybersota koostuu neljästä pilarista, jotka ovat tie-

dustelu, teknologia, logistiikka, ja johtaminen. Tiedustelu tarkoittaa informaatioylivoimaa, jonka avulla toimija voi joko käyttää tietojärjestelmiä ja -kyvykkyyksiä hankkiakseen operationaalisia etuja konflikteissa, tai kontrolloida tilannetta ennen sotaa. Samanaikaisesti omia hyötyjä maksimoidessaan toimija estää vastaavat kyvykkyydet vastustajaltaan. Teknologia nähdään sodan metodeita ja tuloksia muuttavana tekijänä, kun esimerkiksi hyökkäyksiä voidaan automatisoida. Kohteen teknologiasta pyritään löytämään haavoittuvuuksia, joita voidaan hyödyntää omassa toiminnassa. Logistiikalla tarkoitetaan sitä, että toimija pitää huolen verkostoista, joita pitkin hyökkäyksiä tehdään, samanaikaisesti suojaten omia vastaavanlaisia verkostojaan. Johtamisella tarkoitetaan oman toiminnan johtamisen lisäksi vastapuolen siihen kommunikointiverkostoon hyökkäämistä, mitä käytetään komentoihin ja johtamiseen. (Stiennon, 2010.)

Arquillan ja Ronfeldtin (1993) mukaan kybersota on merkki sodan luonteen muuttumisesta. He kuvaavat, että kybersota on syvällisemmällä tasolla *sotaa tiedosta*. Heidän lisäksi muiden muassa Nye (2011) näkee kybersodan ”verettömänä sotana”. Arquillan ja Ronfeldtin (1993) mukaan kybersodassa sotivien osapuolten tavoitteena on selvittää kuka tietää ja mitä, milloin, missä, ja miksi. Tämän lisäksi halutaan tietää, kuinka suojattu yhteiskunnan tai armeijan tieto itsestään tai vastustajistaan on. Heidän mukaansa kaikki kybersodan osapuolet ovat organisoituja sotilasvoimia. Tieto- ja kommunikointijärjestelmiä, joihin vastapuoli toiminnassaan nojaa, yritetään häiritä tai jopa tuhota. Vastustajasta pyritään tietämään kaikki, samalla kun sitä estetään tietämästä itsestä juuri mitään. (Arquilla & Ronfeldt, 1993.) Näiden lähteiden perusteella voidaan todeta, että perinteinen käsitys siitä, että sodassa tulee poikkeuksetta ainakin potentiaalisesti kuolla paljon ihmisiä, ei ole enää ajantasainen. Clausewitzinkin (1867) korostama sodan väkivaltaisuus ei täten välttämättä päde moderneissa konflikteissa.

Clarken ja Knaken (2011) mukaan kybersota on kansallisvaltion toimia tunkeutua toisen valtion tietokoneisiin tai verkostoihin, tarkoituksenaan aiheuttaa vahinkoa tai häiriötä. Heidän mukaan kybersodassa lähetetään käytännössä binäärilukuja, eli ”ykkösiä ja nollia” vastapuolen verkostoon, jotta tietty tavoite voidaan saavuttaa. Heidän mukaansa Yhdysvalloissa, Venäjällä, Kiinassa, ja monissa muissakin valtioissa informaatioteknologiaa ja internetiä pyritään käyttämään aseena kybertaistelukentällä. Kyberin avulla aseistautumisen lisäksi koko kybersotailmiötä varjellaan valtionhallinnon tasolle asti hyvin tarkasti. Tiilikaisenkin (2015) mukaan uudenlaisessa sodankäynnissä käytetään eri keinojen kombinaatioita niin, että ne voidaan kiistää. Kun sodankäynnin historiaa käsittelevässä luvussa kävi ilmi, että tavasta käydä sotaa muotoutui valtioita kuvaava tunnusmerkki, kybersodassa puolestaan sodankäynnin aseet ja keinot pyritään pitämään salassa. Esimerkiksi eri valtiot puhuvat melko avoimesti, minkä kokoisia niiden sotakoneistot ovat, mutta kyberoperaatioita potentiaalisesti toteuttavista teknologioista ja osaajista pysytään vaiti. Tästä voidaan täten Arquillan ja Ronfeldtin (1993) tavoin huomata, että kybersota muuttaa sodan luonnetta.

Aikaisempien kybersotaa käsittelevien lähteiden kohdalla huomattiin, että kybersodan osapuolet ovat valtiollisia ja militäärisiä. Tiilikainen (2015) nostaa kybersodan poliittisen aspektin esille, mikä on sodalle välttämätöntä myös tutkielman toisessa luvussa esitellyn sodan määritelmän mukaan. Tiilikaisen (2015)

mukaan kybersodassa murtaudutaan poliittisista syistä vastustajan tietojärjestelmiin tekemään sabotaasia, sekä vakoilemaan. Hän kuvaa, että kybersota nähdään osana informaatiosotaa, ja että sen vaikutukset voivat aiheuttaa suurta tappiota kohteensa sekä elinympäristölle, että siviiliväestölle.

Clarke ja Knake (2011) kuvaavat, että kybersotaa voidaan käyttää esimerkiksi kahdella eri tavalla. Yksi tapa käyttää sitä on tehdä perinteiset, kineettiset hyökkäykset helpommiksi lamauttamalla vastustajan puolustus. Toinen keino käyttää kybersotaa on propagandan lähettäminen vastustajan lannistamiseksi, esimerkiksi sähköpostien ja muiden internetin kautta toimitettavien medioiden avulla. Tarkastellessa kuvauksen jälkimmäistä tapaa huomataan, että se kuvastaa myös informaatiosodankäynniksi kutsuttuja toimia. Täten informaatiosodankäynnin voidaan nähdä olevan osa kybersotaa joissain tilanteissa.

Kirjallisuudesta on löydettävissä hyvin yksinkertaisiakin määritelmiä kybersodalle. Kybersodan on kuvattu olevat vihamielisiä toimia kyberavaruudessa, millä on vaikutuksia, jotka lisäävät tai vastaavat laajamittaista kineettistä väkivaltaa (Nye, 2011). Nyen (2011) selkeä kuvaus kybersodasta ilmentää sitä, että kybersodalla todennäköisesti on myös vahingollisia vaikutuksia fyysiseen maailmaan. Gartzke (2013) puolestaan kuvaa, että kybersodalla on kaksi peruselementtiä, jotka tekevät siitä erilaisen muihin konflikteihin verrattuna. Kyseiset elementit ovat seuraavat: suurin osa kybersodalla tehdyistä vahingoista on mitä todennäköisemmin väliaikaista, ja suoran hyökkäämisen sijaan voi käyttää hyväksi myös itse *mahdollisuutta* tehdä vahinkoa, esimerkiksi pelottelemalla. Gartzken (2013) kuvaama ensimmäinen elementti voi ilmentää muun muassa sitä, että kybersodan tapahtumien syklit ovat todennäköisesti huomattavasti muiden konfliktien vastaavia nopeampia. Jälkimmäinen elementti puolestaan kuvaa Clarken ja Knaken (2011) kirjoitusten tapaan mahdollista informaatiosodankäyntiä.

Tiilikaisen (2015) mukaan kybersota on ale-versio perinteiselle sodalle, sillä kyberosaajien kouluttaminen on huomattavasti halvempaa, kun sotakoneiston rakentaminen. Kybersodassa käytettäviä kyberaseita voidaan hankkia nykyään todella halvalla, ja esimerkiksi sähkömagneettisen pommin rakentaminen, minkä tavoitteena on käristää jokin tietokone, maksaa vain 400 Yhdysvaltojen dollaria (Knapp & Boulton, 2006). Lynn (2010) nostaa kybersodan taloudellisesta lähestymiskannasta esille sen, että kybersodan uniikkius ilmenee siinä, etteivät sen osapuolet ole rajallisia rahallisten tai fyysisten rajoitteiden toimesta. Erilaisia haitalliseen tarkoitukseen olevia kybertoimenpiteitä on myytävänä esimerkiksi itänaapurissamme, ja hinnat alkavat muutamasta kymmenestä eurosta. Sellaisen häirinnän toteuttamiseksi, mikä joissakin lähteissä määritellään myös kybersodaksi, riittäisi helpostikin nelinumeroinen summa. Muiden muassa Kiinassa on tunnetustikin erittäin taitavaa kansaa myös kyberin osalta, ja siellä osaavien henkilöiden kouluttaminen on huomattavasti edullisempaa kuin esimerkiksi Suomessa. Täten voidaan sanoa, että niin sanottujen kybersotilaidenkin kouluttaminen ja jalkauttaminen toimintakentälle on huomattavasti edullisempaa, kuin esimerkiksi pitkät sotilaskoulutukset ja aseiden teollinen valmistaminen.

Lindsayn (2013) mukaan huolimatta siitä, millainen kybersota tuleekaan olemaan, sitä käydessä johtavinta toimintaa tulee olemaan puolustautuminen. Samaa mieltä on myös Lynn (2010), kenen mukaan paras asia, mitä kyberavaruudessa voi sotakontekstissakin tehdä, on kyberpuolustus. Sekä Lindsayn (2013)

että Lynnin (2010) kuvaukset ovat yhteneväisiä sodan määritelmän kanssa sotilaallisen puolustautumisen merkityksestä.

Kybersodan käsittelemiseen liittyviä ongelmakohtiakin on tunnistettu, ja ne esitellään seuraavaksi. Kyber voi antaa hyökkääjälle mahdollisuuden anonyymiyteen, mutta se voi myös poistaa kohteelta keinot antautua (Gartzke, 2013). Tämän lisäksi Clark ja Landau (2011) korostavat sodankäyntiin liittyvää kriittistä ominaisuutta, joka voi olla kyberissä hankala selvittää. Kyseinen ominaisuus on se, että kostotoimenpiteet vaativat varmaa tietoutta siitä, kuka hyökkääjä on. Anonyymiyteen edelleen liittyen, se että ”jäädään kiinni” tai ”saadaan kiinni” viittaa sanallisestikin enemmän rikokseen kuin sotaan (Gartzke, 2013). Sotajoukon anonyymiys on perinteisessä sodassa käytännössä mahdotonta, mikä on varmasti painavin syy sille, että edellä viitatut kirjoittajat näkevät anonyymiydessä ja modernissa sodankäynnissä huomattavia ristiriitoja.

Edellisten lisäksi organisoitujen rikosten ja terroristijärjestöjen esiintyminen kyberissä hankaloittaa kybersodan tutkimista, sillä noissa ”sodissa” vastapuolet eivät välttämättä ole valtioita, vaan esimerkiksi vastakkaisia etnisiä tai uskonnollisia ryhmiä (Stiennon, 2010). Edellä kuvattujen lisäksi Robinson, Jones ja Janicke (2015) nostavat esille sen, ettei termejä *kybersota* ja *kybersodankäynti* ole erilaistettu tarpeeksi hyvin, mikä voi aiheuttaa sekaannuksia.

Sotaan liittyvä lainsäädäntö asettaa omat haasteensa kybersodan määrittelemiselle. Schmitt (2010) kuvaa, että kybersodassa käytettäviä kyberhyökkäyksiä voitaisiin kenties katsoa kuten aseellisia hyökkäyksiä, mutta siinä on huomattavissa seuraavan kaltainen ongelmakohta. Aseellisen konfliktin lainmukaiseen kuvaukseen sisältyy: ”merkittävästi tuhoavia hyökkäyksiä, jotka tapahtuvat jonkin ajan kuluessa ja jotka on toteutettu hyvin organisoidun ryhmän toimesta”. Kyseisen kaltaista tilannetta ei ole vielä pätevästi demonstroitu kyberavaruudessa. (Schmitt, 2010.) Kybersodalle ei myöskään ole määritelty vastaavanlaista mitta-asteikkoa kuin perinteiselle sodalle (Tiilikainen, 2015). Toisin sanoen ei ole olemassa tunnusmerkistöä, joihin eri kyberkonflikteja voisi verrata saadakseen varmuuden siitä, onko kyseinen kyberkonflikti –sotaa, vai ei.

Yllä kuvattujen ongelmakohtien lisäksi kyberin välityksellä toteutettavat operaatiot ovat strategisessa mielessä osittain rajoitettuja. Gartzke (2013) kuvaa, että on aivan eri asia katkaista kohteen infrastruktuuri, kommunikaatio, sekä sotilaalliset ohjaukset ja suunnittelu, kuin pitää ne katkaistuina pidemmän aikaa. Tämän pohjalta voidaan todeta, että sotilaallisesta näkökulmasta tarkasteltuna ongelmakohdaksi muodostuu kybersodalla aikaansaatavat vaikutukset: jotta kybersota voisi olla tehokas, sen aikana toteutettavien operaatioiden tulee aiheuttaa pidempiaikaista harmia.

Lähdeaineistoa läpi käytäessä huomattiin, että kaikki tutkijat eivät määrittele kybersotaa kattavasti. Sen sijaan osassa julkaisuja on saatettu ainoastaan esitellä kybersodan tärkeimpiä ominaisuuksia. Seuraavalle sivulle on laadittu taulukko 1, johon on koottu tässä alaluvussa kuvattujen määritelmien ja kuvausten pohjalta tehdyt johtopäätökset. Johtopäätösten muotoutumiseen vaikutti myös tutkielman toisessa luvussa tehdyt havainnot sodan ja yhteiskunnan kehityksestä. Taulukon tavoitteena on helpottaa laadittujen johtopäätösten hahmottamista.

Kybersota: johtopäätökset	
Lainsäädäntö	- Yksi suurimmista syistä eri määritelmien ja kuvausten eroavaisuuksille on se, että kybersotaa koskevaa, kansainvälisesti hyväksyttyä lainsäädäntöä ei ole vielä olemassa. - Perinteiseen sotaan liittyvää lainsäädäntöä on nykyisellään suhteellisen hankala soveltaa kyberkonflikteihin.
Väkivalta ja kohde	- Käsitys siitä, että sodassa tulee poikkeuksetta ainakin potentiaalisesti kuolla paljon ihmisiä, ei päde kybersotaan. - Kybersodalla voi olla haitallisia vaikutuksia fyysiseen maailmaan, mutta suurten ihmisjoukkojen kuoleminen tai ympäristön merkittävä tuhoutuminen ei ole todennäköistä. - Kybersodassa kohteena ovat vastapuolen erilaiset verkostot ja järjestelmät, joihin iskemällä voidaan joko suorasti tai epäsuorasti vaikuttaa haluttuihin valtiollisiin elimiin.
Avoimuus	- Toisin kuin perinteisistä sotakoneistoista, kybersotilaista ja –operaatioissa käytettävistä teknologioista on vain vähän, jos ollenkaan tietoa kenelläkään muulla, kuin kyseisillä toimijoilla ja yksiköillä.
Taloudellisuus	- Kybersodankäynti sekä –osaajien kouluttaminen ja hankkiminen on huomattavasti halvempaa, kuin perinteinen maanpuolustukseen tai muuhun sotatilanteeseen valmistautuminen.
Toimijat ja motiivit	- Kybersodassa tulee osapuolina olla aina valtiolliset, sotilaalliset toimijat. - Kyberrikollisuus ja –terrorismi tulee erottaa kybersodasta. - Kybersodassa, kuten perinteisissäkin sodissa, lähtökohdat ovat aina poliittisia.

Taulukko 1 Kybersota: johtopäätökset

3.1.1 Määritelmien eroavaisuuksia

Edellisessä alaluvussa kuvattiin eri määritelmiä ja kuvauksia, joita kybersodalle on laadittu. Toisiinsa liittyviä kuvauksia käsiteltiin rinnakkain, ja erilaiset ominaisuudet, jotka eivät poissulje toisiaan, esiteltiin. Kybersodan eri määritelmissä on kuitenkin huomattavissa myös eroavaisuuksia. Eroavaisuudet liittyvät kybersodan luonteeseen, mahdolliseen toteutumiseen, osallistuviin osapuoliin, sekä

sillä tehtävin vaikutuksiin. Käsitteen paremman ymmärtämisen kannalta on tärkeää tarkastella kyseisiä eroja, jotta kattavamman käsitteen luominen on mahdollista.

Eri koulukunnilla on kybersodasta näkemyseroja. Raja kulkee jossain idän ja lännen, välisellä alueella. Idäksi nähdään lähinnä Kiina ja Venäjä, ja länttä kuvaavat Yhdysvallat ja sen voiman suojaan hakeutuvat maat. Lännessä korostetaan itse teknologian merkitystä ja sitä, että kyberoperaatiot ovat vain yksi osatekijä sodankäynnin perinteisemmässä kokonaisuudessa. Idässä puolestaan informaatiosota on keskeisimmässä osassa, ja kyberteknologia on vain sen alusta ja kuljetin. Tavoitteena on vaikuttaa mahdollisimman moniin kognitiivisiin toimintoihin. Edellä kuvattujen asioiden johdosta onkin mahdollista, että mikäli kybersota tapahtuu, sen voittaja ei välttämättä ole teknologisesti etevämpi osapuoli. Sen sijaan voittamiseen voi riittää vieraan ja etenkin oman informaation tehokas manipuloiminen ja kontrollointi. (Tiilikainen, 2015.)

Kybersodan toteutumisesta ja mahdollisuudestakin on erimielisyyksiä. Joidenkin lähteiden mukaan kybersotaa on jo tapahtunut vuoteen 2017 mennessä (mm. Stiennon, 2010; Clarke & Knake, 2011). Toisaalta muun muassa Arquillan ja Ronfeldtin (1993), Stonen (2013), Tiilikaisen (2015), ja Lynnin (2010) mukaan kybersotaa ei ole vielä tapahtunut, mutta että se on hyvin paljon mahdollista tulevaisuudessa. Esimerkiksi Lynn (2010) on ilmaissut asian niin, että kybersodan koko voi olla ennenkuulumaton, ja että se on tapahtumana huomattava ja ehdottomasti lähestyvä uhka.

Kybersodan todellisuutta puoltavien näkökantojen lisäksi myös päinvastaisia näkemyksiä on esitettu. Kieltäviä mielipiteitä edustavat esimerkiksi Gatzke (2013) ja Rid (2012), keiden mukaan kybersotaa ei ole vielä tapahtunut eikä todennäköisesti tule tapahtumaan tulevaisuudessakaan. Kybersodan kieltämisen lisäksi on esitetty myös näkemyksiä siitä, että kybersota voi ilmetä osana muunlaisia sotia, kuten informaatiosotaa (Tiilikainen, 2015). ja vastavuoroisesti jotkut näkevät, että informaatiosodankäynti on osa kybersotaa (Clarke & Knake, 2011).

Eroavaisuuksia nähdään myös siinä, minkälaiset toimijat voivat olla osana kybersotaa. Esimerkiksi Clarken ja Knaken (2011) määritelmässä molempina osapuolina ovat kansallisvaltiot. Arquilla ja Ronfeldt (1993) tarkentavat, että kyseessä ovat aina organisoidut sotilasvoimat. Toisaalta, muun muassa Stiennon (2010) kuvaa, että vastapuolet voivat olla myös esimerkiksi yrityksiä.

Kybersodan voimakkuuteen liittyvät näkemykset eroavat myös huomattavasti. Yhtäällä ollaan sitä mieltä, että kybersota voi olla pelkkää häirintää ja vakoilua globaalissa verkossa (Tiilikainen, 2015). Toisaalla se voidaan nähdä kansallisvaltion hyökkäyksinä vastustajan verkostoihin, tarkoituksenaan aiheuttaa vahinkoa (Clarke & Knake, 2011).

Seuraavalle sivulle on laadittu taulukko 2, johon on koottu kaikki löydetyt, yllä kuvatut eroavaisuudet kybersodan määritelmissä. Eroavaisuudet on esitetty taulukossa samassa järjestyksessä, kuin tässä alaluvussa. Vasemmassa sarakkeessa ilmoitetaan, mitä ominaisuutta eroavaisuudet koskevat. Oikeassa sarakkeessa kuvataan, kuinka määritelmät eroavat toisistaan.

Ominaisuus, jossa eroavaisuuksia	Eroavaisuudet
Keskeisin väline	- Teknologia. Teknologian merkitystä korostetaan lännessä. Lännellä tarkoitetaan karkeasti jaoteltuna Yhdysvaltoja ja sen suojaan hakeutuvia maita. (Tiilikainen, 2015.) - Informaatio. Informaation merkitystä ja kognitiivisiin toimintoihin vaikuttamista korostetaan idässä. Idällä tarkoitetaan karkeasti jaoteltuna Venäjää ja Kiinaa. (Tiilikainen, 2015.)
Todellisuus/olemassaolo	- Kybersota on totta, ja sellainen/sellaisia on jo nähty (mm. Stiennon, 2010). - Kybersota on mahdollinen tulevaisuudessa, mutta sitä ei ole vielä nähty (mm. Lynn, 2010). - Kybersota ei ole mahdollinen, sitä ei ole koskaan ollut, eikä tule koskaan olemaankaan.
Ilmeneminen	- Osana muita sotia, kuten informaatiosotaa (Tiilikainen, 2015). - Muut sodat, kuten informaatiosota, ovat osa kybersotaa (Clarke & Knake, 2011).
Vastakkaiset osapuolet	- Kansallisvaltioita (Clarke & Knake, 2011), organisoituja sotilasvoimia (Arquilla & Ronfeldt, 1993). - Mahdollisesti myös yrityksiä (Stiennon, 2010).
Voimakkuus	- Pelkkää häirintää internetliikenteessä (Tiilikainen, 2015). - Tarkoitus aiheuttaa vahinkoa vastapuolelle (Clarke & Knake, 2011).

Taulukko 2 Kybersodan määritelmien eroavaisuuksia

3.1.2 Uusi määritelmä

Kahdessa edellisessä alaluvussa esiteltiin eri määritelmiä, joita kybersodalle on laadittu, sekä kyseisten määritelmien eroavaisuuksia. Huomattavien eroavaisuuksien vuoksi ei ole mahdollista yksiselitteisesti todeta, onko kybersotien mahdollisuus todellinen. Huomattiin myös se, että kaikki tutkijat eivät ole kunnolla

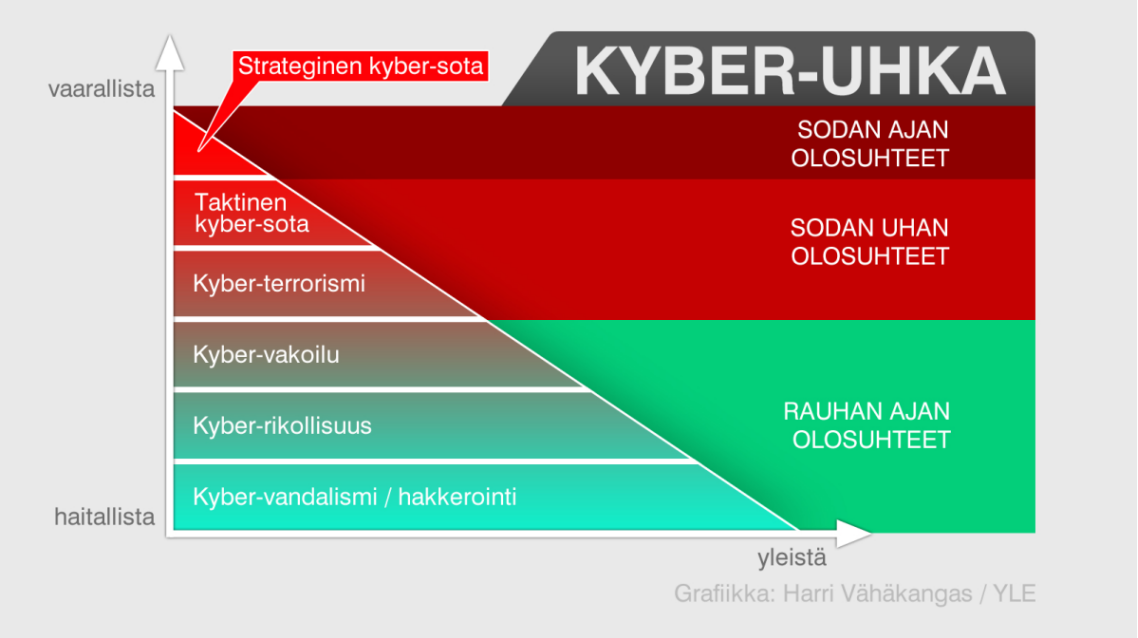
määritelleet kybersotaa, vaan ovat nostaneet siitä esille vain valitsemiaan ominaisuuksia. Lähteäkseen käsittelemään niitä tapahtumia, joita on kuvattu kybersodiksi, täytyy kybersota ensin määritellä kattavasti. Määritelmän myötä tapahtumia voidaan arvioida monipuolisesti, niistä osataan etsiä oikeita elementtejä, ja täten ne voidaan mahdollisesti todeta kybersodaksi. Toisaalta on mahdollista, että mikäli tarvittavat ominaisuudet eivät täyty, voidaan esittää vastaväitteitä sille, että kybersotaa olisi tapahtunut.

Kuten aiemmin tutkielmassa mainittiin, kaikki kyberhyökkäykset tai –operaatiot eivät ole kybersotaa tai edes kybersodankäyntiä, joka voi olla osa esimerkiksi hybridisotaa. Yle:n vuonna 2012 kirjoittamassa uutisessa on kuvattu hyvin eri kyberuhkia ja niiden sijoittumista rauhan ja sodan aikojen olosuhteisiin, sekä niiden esiintymisen yleisyyttä. Nämä yhteydet on havainnollistettu kuvioon 1, joka on tutkielman seuraavalla sivulla. Kuvion sisältö on laadittu Caveltyn (2007) määritelmien pohjalta. Koko kyberuhkien skaala on jaettu kuuteen eri luokkaan, ja ne ovat vaarallisuuden kuvaan järjestettynä seuraavat: kybervandalismi/hakkerointi, kyberrikollisuus, kybervakoilu, kyberterrorismi, taktinen kybersota, ja strateginen kybersota. Yhteiskunnan olosuhteet on jaettu kolmeen luokkaan: rauhan ajan olosuhteet, sodan uhan olosuhteet, ja sodan ajan olosuhteet.

Kybervandalismilla/hakkeroinnilla voidaan tarkoittaa esimerkiksi sitä, että murtaudutaan toisen yksityiskäyttäjän tietokoneeseen katsomaan, mitä sieltä löytyy. Kyberrikollisuus on rikosten tekemistä kyberin avulla, ja se voi tarkoittaa esimerkiksi pelihahmon varastamista, mistä nähtiin Suomessakin esimerkki vuonna 2009. Kybervakoilulla tarkoitetaan kohteen tietojärjestelmään murtautumista, aikeena vakoilla ja tarkastella esimerkiksi sitä, minkälaista dataa siellä liikkuu ja minkälaisella aikasyklillä. Mehan (2009) kuvaa, että Yhdysvaltiain kotimaan turvallisuusministeriössä käytetään kyberterrorismille seuraavaa määritelmää: kyberterrorismi on rikollinen, tietokoneiden välityksellä tehty toimi, joka saa aikaan väkivaltaa, kuolemaa ja/tai tuhoa, ja luo pelkoa, jonka tarkoituksena on painostaa valtionjohtoa muuttamaan menettelytapojaan. Taktisella kybersodalla tarkoitetaan kyberin suunnitelmallista käyttämistä sodankäynnin välineenä, tavoitteena voittaa sota. Strategisessa kybersodassa vastakkaiset osapuolet ovat sotilaallisia/valtiollisia toimijoita. Välineinä on kyberaseet, ja niitä käytetään tarvittavalla tavalla, jotta sota voidaan voittaa.

Kolme ensimmäistä kyberuhkaa sijoittuvat rauhan ajan olosuhteisiin. Kyberterrorismia ja taktista kybersotaa esiintyy sodan uhan olosuhteissa, ja strategisen kybersodan tapahtuessa yhteiskunnan olosuhteet ovat sodan aikaiset. Eri

kyberuhkien yleisyys on sitä pienempää, mitä vakavampi kyseinen kyberuhka on.



Kuvio 1 Kyberuhat (kuva: Harri Vähäkangas/YLE, 2012)

Lähdeaineistosta nousseiden huomioiden perusteella voidaan sanoa, että kuvio 1:ssä esiintyviä kyberuhkia toteuttavat osapuolet voivat olla uhasta riippumatta valtiollisia. Strategisen kybersodan elementit täyttääkseen toimijan on kuitenkin välttämättömästi oltava sotilaallinen. Kybersodan kattava määritelmä kannattaa muotoilla seuraavasti:

Kybersota on kansallisvaltion sotilaallisen elimen strategisia kyberhyökkäyksiä toisen kansallisvaltion tietojärjestelmiin ja verkostoihin. Kybersodan molemmat osapuolet täytyy olla tiedossa kuten fyysisen maailman sodassakin, jotta sotaa koskevien lakien soveltaminen on mahdollista.

Kyberhyökkäysten tavoitteena on aiheuttaa harmillista vaikutusta kohdejärjestelmiin ja –verkostoihin. Hyökkäysten vaikutukset ulottuvat myös siviilien hyödyntämään ICT-infrastruktuuriin. Tämän lisäksi hyökkäyksillä hankitaan tarvittavaa tietoa omien sotatoimintansa edistämiseksi ja paremman tilannekuvan saamiseksi. Samoin kuin hyökkäysten, myös kyberpuolustuksen tulee olla järjestelmällistä ja tavoitteellista.

Pystyäkseen puhumaan kybersodasta, sen motiivit sekä lopputulos täytyy olla poliittisesti vaikuttavia ainakin yhden sodan osapuolen kannalta. Sillä täytyy olla myös alku, toteutus, ja loppu, ja sodan loppuessa täytyy olla mahdollista kiistatta todeta sen vaikutukset kaikkiin osapuoliin. Kybersodassa käytettävät hyökkäykset sekä puolustus toteutetaan kyberavaruudessa, mutta tapahtumilla voi olla suuriakin vaikutuksia fyysiseen maailmaan, ihmisiin, ja organisaatioihin.

Määritelmä muotoutui ylläolevaan muotoonsa tutkielman työprosessin edetessä. Löydetyistä kybersodan määritelmistä ja kuvauksista tehtiin johtopäätöksiä, joihin vaikutti myös tutkielman toisessa luvussa tehdyt havainnot sodan ja yhteiskunnan kehittymisestä. Johtopäätösten pohjalta kybersodasta pyrittiin löytämään sellaiset ominaisuudet, jotka ovat joko yhteneväisiä sodan määritelmän kanssa, tai ilmentävät tietoyhteiskunnan myötä tapahtunutta sodan evoluutiota. Valitut ominaisuudet rajattiin niin, ettei ne ole keskenään ristiriitaisia.

3.2 Tapahtuneet kybersodat

Useissa lähteissä esitellään jo tapahtuneita konflikteja, joita on kybersodiksikin kuvattu. Kyseisiä konflikteja ovat Viron patsaskiistan yhteydessä tapahtunut verkkohyökkäys sekä Israelin hyökkäykset Syyriaan vuonna 2007, Yhdysvaltojen ja Iranin kiistojen aikana tapahtunut Stuxnet, ja Georgian sota vuonna 2008.

Clarke ja Knake (2011) esittävät, että Viron tapahtumat vuodelta 2007 ilmentävät sitä, miltä itsenäinen kybersota voisi näyttää. Tuolloin Tallinnassa olevaa pronssipatsasta, jolla oli myös Venäjälle suuri merkitys, haluttiin siirtää fyysisesti paikasta toiseen. Kiistan jatkuttua ja kehityttyä tilanne äityi keväällä 2007 mellakaksi, jolloin konfliktit siirtyivät myös kyberavaruuteen. Yhtenä maailman verkostoituneina maina Viro on täydellinen kohde kyberhyökkäyksille, ja sinne iskikin siihen mennessä maailman suurin hajautettu palvelunestohyökkäys (DDoS). Hyökkäyksellä saatiin laitettua alas julkisten verkkosivujen lisäksi muun muassa servereitä, jotka pitivät yllä puhelinliikennettä, luottokortin varmennusjärjestelmää sekä Internet hakemistoa. Yli miljoona tietokonetta saatiin kiinnitettyä toteuttamaan hyökkäystä, jonka vaikutusten täydelliseen korjaamiseen meni viikkoja. DDoS-hyökkäyksen takana oli mitä todennäköisimmin Venäjä, mutta vastuuta ei ole saatu todistettua (Choucri & Goldsmith, 2012).

Muutamaa kuukautta Viron hyökkäysten jälkeen myös Syyrian kyberavaruudessa kuohui. Clarke ja Knake (2011) kuvaavat, kuinka Israel toteutti ilmaiskun Syyrian ydintutkimuslaitokseen 6. syyskuuta 2007. Mikä teki tapauksesta osan kybersotaa, on se, että israelilaiset olivat manipuloineet Syyrian ilmavoimien tutkajärjestelmää ennen hyökkäyksiä. Käytännössä syyrialaiset eivät voineet valmistautua hyökkäykseen millään tavalla, sillä tutkajärjestelmä näytti katsojilleen vain sen, mitä israelilaiset halusivat. He olivatkin tehneet näkymästä itselleen mieleisen, ja ruutu näytti käytännössä täysin normaalia, lähes koneetonta keskiöistä taivasta.

Stuxnet-tapaus on globaalisti tunnettu kyberhyökkäys, jonka hyökkääjästä ei ole edelleenkään täyttä varmuutta, mutta minkä kohteena oli Iran. Stuxnet oli mato, joka iski Iranilaiseen ydinlaitokseen, ja tartutti yli 60 000 tietokonetta. Yli puolet tartunnoista kohdistui Iraniin. Muita maita, joihin mato vaikutti, olivat muiden muassa Intia, Kiina, Etelä-Korea, Yhdysvallat, Australia, Suomi ja Saksa. Alun perin Stuxnet saatiin ujutettua Iranin ydinlaitoksen koneisiin USB-tikun avulla, ja se havaittiin ensimmäisen kerran vuonna 2010. Sekä Yhdysvaltoja, että Israelia on syytetty viruksen luomisesta ja liikkeelle laittamisesta (ks. esim. Choucri & Goldsmith, 2012; Farwell & Rohozinski, 2011).

Stiennonin (2010) mukaan Georgian sota oli historiamme ensimmäinen kybersota. Georgian ja Venäjän välinen sota vuonna 2008 ei alkanut tyhjästä, vaan mailla oli ollut hieman arvaamattomat välit jo yli sata vuotta. Ennen sodan alkamista Venäjä oli pitkään harjoittanut provokaatiota Georgiaa kohtaan. Provokaatiota oli toteutettu esimerkiksi niin, että valtionhallinnon verkkosivuille tehtyjen hyökkäysten avulla sivuille lisättiin kuvia, jotka vertasivat Georgian presidenttiä Adolf Hitleriin. Elokuun 7. päivänä vuonna 2008 Georgia hyökkäsi Etelä-Ossetiaan, ja seuraavana päivänä Venäjä vastasi hyökkäyksiin. Samanaikaisesti, kun Venäjän armeija aloitti toimintansa, myös heidän kybersotilaansa lisäsivät panoksiaan. Georgiaan kohdistettiin laajempi DDoS-hyökkäys, jonka tavoitteena oli estää georgialaisten tietämys sodasta. Hyökkäys tavoitti maan hallinnon verkkosivut sekä mediatalot, minkä lisäksi CNN:n ja BBC:n verkkosivuille pääsy Georgiasta käsin estettiin. Vapaaehtoiset pystyivät liittymään mukaan hyökkäykseen anti-georgialaisilta verkkosivuilta lataaman ohjelman avulla (Clarke & Knake, 2011.)

Hollisin (2015) mukaan Georgiaan kohdistuneet verkkohyökkäykset olivat alkaneet muutamaa viikkoa ennen varsinaista sodankäyntiä. Toisin kuin esimerkiksi Viron tapauksessa, Georgiassa kyberhyökkäyksiä täydensi fyysinen taistelu. Venäjä teki kyberhyökkäyksillään tiedustelua Georgian verkostoissa, mitä käytti todennäköisesti hyväksi omissa strategisen, operationaalisen, ja taktisen tason sotilaallisissa toiminnoissa. Tutkielman toisen luvun sodankäynnin evoluutiota käsittelevässä alaluvussa kuvattiin suuren yhteisön psykologista muutosta liittyen sosiaaliseen suhteeseen, mistä todennäköisesti myös isänmaallisuuskin on saanut alkunsa. Isänmaallisuus hyökkäyksen yhtenä motivoivana tekijänä on Hollisin (2015) mukaan toimiva ajuri myös kyberympäristössä, mikäli osallistujat saadaan ensin motivoitua kunnolla konseptiin. Georgialaiset yrittivät suojautua hyökkäyksiltä, mutta venäläiset vastasivat jokaiseen liikkeeseen (Clarke & Knake, 2011).

Tarkastellessamme yllä kuvattuja tapahtumia edellisessä alaluvussa esitellyn, uuden määritelmän kannalta, havainnot ovat selkeitä. Voidaan todeta, ettei yksikään edellä kuvatuista tapahtumista täytä kybersodan kaikkia ominaisuuksia. Tästä saadaan johtopäätökseksi se, että kybersotaa ei ole vielä tapahtunut. Ainoastaan Georgian sodasta on puhuttu laajemminkin sotana myös kyberoperaatioiden lisäksi. Muut esimerkeistä edustavat melko yksittäisiä hyökkäyksiä tai hyökkäyssarjoja, jotka eivät täytä sodan tai kybersodan määritelmiä.

Vaikka tutkielman keskeisin johtopäätös on se, ettei kybersotaa ole tapahtunut, perusteita kybersodan kieltämiselle ei ole. Toisin sanoen, kybersodan toteutuminen tulevaisuudessa on täysin mahdollista. Mahdollista kuitenkin on myös se, ettei kybersotaa tule tapahtumaan tulevaisuudessakaan.

4 YHTEENVETO

Tähän tutkielmaan etsittiin kirjallisuuskatsauksen avulla selvitys siitä, kuinka sota on kehittynyt historiansa aikana, ja muuttunut tietoyhteiskunnan myötä. Lähdemateriaali pyrittiin rajaamaan luotettavimpiin, ja niistä löytyneet tulokset jaettiin yhteensä neljään lukuun. Ensimmäinen luku on johdanto, jota seuraa kaksi sisältölukua, ja viimeisenä on yhteenveto.

Ensimmäisessä sisältöluvussa määriteltiin tutkielmalle olennaisia käsitteitä, jotka ovat sota, tietoyhteiskunta, kyber, ja hybridisota. Luvussa kuvattiin sodankäynnin evoluutiota, yhteiskunnan kehittymistä tietoyhteiskunnaksi, sekä sotaa ja moderneja konflikteja tietoyhteiskunnassa. Ensimmäinen luku vastasi toiseen tutkimuskysymykseen kybersota-käsitteen alkuperästä. Ensimmäinen luku rakennettiin niin, että toinen luku oli sille luonnollinen jatkumo.

Toinen sisältöluku oli omistettu kokonaan kybersodan käsittelemiselle. Luvun alussa määriteltiin, mitä kybersodan toimintaympäristö, eli kyberavaruus, tarkoittaa. Sen jälkeen esiteltiin lähdeaineistosta löytyneitä määritelmiä kybersodalle. Määritelmien esittelemisen jälkeen niistä havaitut eroavaisuudet nostettiin esille, jonka jälkeen laadittiin kontribuutiona uusi määritelmä kybersodalle. Uutta määritelmää seurasi luku, jossa kuvattiin tapahtumia, joita on lähdeaineistossakin väitetty kybersodiksi. Toisen sisältöluvun lopussa, kybersota-käsitteen uuden määritelmän nojalla kumottiin esitykset siitä, että kybersotaa olisi tähän päivään mennessä jo tapahtunut. Luvussa saatiin täten myös vastaus ensimmäiseen tutkimuskysymykseen, eli siihen, mitä kybersota-käsite tarkoittaa.

Lähdeaineistosta löytyneiden yksittäisten teosten erilaisiin näkökantoihin kybersotaan liittyen vaikuttanee vahvasti se, kuinka hyvin kirjoittaja on perehtynyt sodan määritelmään, tai ainakin kuinka merkittävänä kirjoittaja sitä pitää. Sota-käsitettä voidaan Ridinkin (2012) mukaan käyttää tuomaan ainoastaan vertauskuvallista arvoa eri konteksteissa. Tätä on esiintynyt myös esimerkiksi siinä, kun Yhdysvallat julistivat sodan terrorismia ja huumeita vastaan, ja kun Venäjän nähdään harjoittavan informaatiosotaa nykyään lähes taukoamatta. Kybersodan käsite tullee saamaan laajamittaisesti hyväksytyn, kattavamman määritelmän vasta sitten, kun kansallisvaltiot sopivat yhdessä käsitteen merkityksestä ja sitä koskevasta lainsäädännöstä.

Tälle tutkielmalle on nähtävissä kolme rajoitetta. Ensimmäinen niistä on se, että tutkielma on suppea kirjallisuuskatsaus. Voi siis olla mahdollista, ettei kaikkea relevanttia lähdemateriaalia ole välttämättä löydetty. Tutkielmaan ei ole

myöskään esimerkiksi haastateltu asiantuntijoita, joilta voisi saada kirjallisuudesta löytymättömiä näkökantoja aiheeseen.

Toisena rajoitteena voidaan nähdä se, että koska kybersodalle ei ole vielä laadittu laajamittaisesti hyväksyttyjä merkityksiä tai lainsäädäntöä, osa tutkimuskirjallisuudestakin perustuu kyseisen tutkijan omiin preferensseihin ja mielipiteisiin. Lähteistä on huomattavissa yhteinen kanta siitä, että sota ja kybersota ovat eri asia. Siitä huolimatta, että sota on kohdannut huomattavan evoluution myös siinä käytettävän teknologian osalta, kyberavaruuden tuomien mahdollisuuksien ei nähdä olevan ainoastaan sodan evoluutiota. Sen sijaan kybersota nähdään eri asiana kuin sota. Näkemykset kybersodan luonteesta sekä siitä, kuinka lähellä tai kaukana toisistaan sota ja kybersota voivat esiintyä, näyttävät kuitenkin olevan ainakin osittain mielipide-eroja.

Kolmas rajoite on se, että tutkielma on sen kirjoittajalle ensimmäinen akateeminen tutkimus, mikä voi vaikuttaa argumentointiin, lähdekritiikkiin, sekä havaintojen tekemiseen. Lisäksi kirjoittajalla on puutteellinen tuntemus liittyen sotaan ja sen lainsäädäntöihin, sekä valtioiden toteuttamiin kyberoperaatioihin.

Kybersodan aihealue kaipaa ehdottomasti jatkotutkimuksia tulevaisuudessa. Tämä on perusteltavissa sillä, ettei kybersodalle ole vielä olemassa kansainvälisesti hyväksyttyä määritelmää. Määritelmän puuttumisen myötä myöskään kybersotaan liittyviä kansainvälisiä sopimuksia tai liittoumia ei ole luonnollisesti voitu laatia, toisin kuten esimerkiksi perinteisen sodan suhteen. Tutkielman kirjoittajan esittämät jatkotutkimusaiheet ovat seuraavat:

- Tutkimus niistä taustatekijöistä, jotka aiheuttavat suuret näkemyserot kybersodan todellisuuteen ja luonteeseen liittyen.
- Tutkimus kybersodan ja kybersodankäynnin eroavaisuuksista.
- Tutkimus hybridisodasta ja siitä, voiko kybersota ja/tai –sodankäyntiä esiintyä siitä irrallisena.
- Tutkimus sodan evoluutioon liittyen. Esimerkiksi Clausewitz (1867) ja Mehan (2009) kuvaavat sitä, kuinka sota muotoutuu ajankohtaisten olosuhteiden mukaisesti. Tuleekin tarkastella sitä, voidaanko kybersota tai -sodankäynti nähdä pelkästään sodan evoluutiona. Toisin sanoen: voiko olla mahdollista, että on edelleenkin olemassa ainoastaan sotaa, joka voi evoluutionsa takia sisältää myös tutkielmassa kuvattuja kyberoperaatioita.

LÄHTEET

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141-165.

Arquilla, J., & Ronfeldt, D. (1999). The Advent of Netwar: Analytic Back-ground. *Studies in Conflict and Terrorism*, Vol. 22, No. 3, pp. 193–206.

Beniger, J. (2009). The control revolution: Technological and economic origins of the information society. *Harvard university press.*

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, *68*(2), 70-77.

Cioffi-Revilla, C. (1996). Origins and evolution of war and politics. *International Studies Quarterly*, *40*(1), 1-22.

Clapper, J. R. (2016). Worldwide threat assessment of the US intelligence community. *OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE WASHINGTON DC.*

Clark, D. D., & Landau, S. (2011). Untangling attribution. *Harv. Nat'l Sec. J.*, *2*, 323.

Clarke, R. A., & Knake, R. K. (2011). Cyber war. *HarperCollins.*

von Clausewitz, C. (1867). Hinterlassene werke über krieg und kriegführung: Vom kriege (Vol. 1). Suomentanut Eskelinen, H. *Helsinki: Art House 2009*

Colarik, A., & Janczewski, L. (2015). Establishing cyber warfare doctrine. In *Current and Emerging Trends in Cyber Operations* (pp. 37-50). Palgrave Macmillan UK.

Dennen, J. M. G. V. D. (1995). The origin of war: the evolution of a male-coalitional reproductive strategy. s.n.

Dunlap Jr, C. J. (2011). Perspectives for cyber strategists on law for cyberwar. *Strategic Studies Quarterly*, *5*, 81.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Su vival*, *53*(1), 23-40.

Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security*, *38*(2), 41-73.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars (p. 51). Arlington, *VA: Potomac Institute for Policy Studies.*

Hollis, D. (2015). Cyberwar case study: Georgia 2008.

Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: expansion into commercial environments. *Information Systems Manage ment*, *23*(2), 76.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, 24-42.

Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Washington, DC: *Center for Strategic & International Studies.*

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365-404.

Lynn, W. J. (2010). Defending a new domain: the Pentagon's cyberstrategy. *Foreign Affairs*, *89*(5), 97-108.

Mehan, J. E. (2009). Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger. *IT Governance Ltd*.

Mulder, K., Ferrer, D., & Van Lente, H. (2011). *What is Sustainable Technology?: Perceptions, Paradoxes and Possibilities*. Greenleaf Publishing.

Mäkelä, J. (24.3.2012). Verkkojen mukana kaatuu koko yhteiskunta. Yle Uutiset.

Nye Jr, J. S. (2011). Nuclear lessons for cyber security. *AIR UNIV PRESS MAXWELL AFB AL.*

Renz, B., & Smith, H. (2016). Russia and Hybrid warfare-going beyond the label.

Rid, T. (2012). Cyber war will not take place. *Journal of strategic studies*, *35*(1), 5-32.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security*, *49*, 70-94.

Schmitt, M. N. (2010). Cyber operations in international law: The use of force, collective security, self-defense, and armed conflicts. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (Vol. 151, pp. 163-64).

Singer, J. D., & Small, M. (1994). Correlates of war project: International and civil war data, 1816-1992 (ICPSR 9905). *Ann Arbor, MI: Inter-University Consortium for Political and Social Research.*

Stiennon, R. (2010). Surviving cyberwar. *Government Institutes.*

Stone, J. (2013). Cyber war will take place! *Journal of Strategic Studies*, *36*(1), 101-108.

Suomen valtioneuvosto. (2010). Yhteiskunnan turvallisuusstrategia. *Puolustus-ministeriö, Helsinki.*

Tiilikainen, H. (2015). Hybridisota – Rintamaraportti. *Helsinki: Auditorium Kustannus*

Webster, F. (2014). *Theories of the information society*. Routledge.