VAASAN YLIOPISTO

Filosofinen tiedekunta

Viestinnän monialainen maisteriohjelma

Saara Jansson

Kansallisten kyberstrategioiden diskurssit

Digitaalisen median pro gradu -tutkielma

Vaasa 2017

SISÄLLYS

VAASAN YLIOPISTO
Filosofinen tiedekunta
Tekijä: Saara Jansson
Pro gradu -tutkielma: Kansallisten kyberstrategioiden diskurssit
Tutkinto: Filosofian maisteri
Koulutusohjelma: Viestinnän monialainen maisteriohjelma
Suuntautumisvaihtoehto: Digitaalinen media
Valmistumisvuosi: 2017
Työn ohjaaja: Tanja Sihvonen

TIIVISTELMÄ:

Tutkin pro gradu -tutkielmassani valtiollisen tason vaikutusmahdollisuuksia kybertoimintaympäristössä. Kyberturvallisuuden tehtävä on suojata kybertoimintaympäristössä olevaa informaatiota ja sen lähettämistä laitteelta, järjestelmältä tai ihmiseltä toiselle. Kybertoimintaympäristöllä tarkoitetaan tässä tutkimuksessa laitteista, järjestelmistä ja ihmisistä muodostuvaa verkkoa, jossa informaatio on digitaalisessa muodossa.

Viimeisen viiden vuoden aikana keskustelu kyberturvallisuudesta on yleistynyt, sillä ihmiset ja laitteet ovat yhä vahvemmin riippuvaisia tieto- ja viestintäverkkojen toiminnasta. Valtioilla on merkittävä rooli kyberkeskustelussa. Ne säätävät lait ja asetukset, joiden perusteella viestintä kybertoimintaympäristössä määritellään joko lailliseksi tai laittomaksi. Sen vuoksi valtioiden on saatava kaikki kybermaailman toimijat mukaan toimivan verkkoliikenteen rakentamiseksi. Tähän niillä on apunaan kyberstrategiat, joissa määritellään valtioiden mahdollisuudet ja uhat kybermaailmassa.

Tavoitteenani on selvittää, millaisia vakuuttamisen puhetapoja eli diskursseja valtioiden kyberstrategiat pitävät sisällään ja mitä niillä pyritään saavuttamaan. Tutkimusaineistoksi olen valinnut Australian, Iso-Britannian, Nigerian, Singaporen ja Yhdysvaltojen kyberstrategiat. Menetelmänä käytän diskurssianalyysia, johon lainaan työkaluja retoriikasta. Retoriset keinot osoittavat tekstistä vakuuttavat ilmaisut, joiden pohjalta diskurssit muodostuvat.

Analyysin tuloksena löysin kyberstrategioista viisi vakuuttamisen diskurssia. Diskurssit paikantuvat retorisiin keinoihin, joista käytetyimpiä ovat metafora, konsensus, puhujakategoria ja määrällistäminen. Kulttuuriset tekijät vaikuttavat osaltaan siihen, minkälaisia sisältöjä diskurssit käsittelevät. Diskurssien tavoitteena on tuottaa konkreettista muutosta yhtenäisen kansakunnan, kansainvälisen yhteistyön, talouskasvun ja valtiota hyödyttävän verkkokäyttäytymisen muodossa. Lisäksi diskurssien tehtävä on yksinkertaisesti osoittaa valtion valta kybertoimintaympäristössä.

AVAINSANAT: kyberturvallisuus, kyberstrategia, diskurssianalyysi, retoriset keinot

1 JOHDANTO

Lokakuussa 2016 Yhdysvalloissa huolestuttiin. Kirjautuminen suosittuihin internetpalveluihin, kuten Netflixiin, Twitteriin ja Spotifyhin, ei onnistunut. Pian selvisi, että kyse oli kyberhyökkäyksestä, jonka tarkoituksena oli estää internetpalvelujen toiminta ja aiheuttaa yrityksille rahallisia tappioita. (Ks. esim. BBC 2016; Menn, Finkle & Volz 2016.) Tavallinen verkon käyttäjä ei voinut tehdä ongelmalle mitään, koska hyökkäys kohdistui sellaisiin internetin perustoimintoihin, joita ymmärtävät vain alan ammattilaiset (Turunen 2016). Kyberhyökkäys oli mahdollinen samasta syystä kuin tämän kaltaiset tilanteet yleensäkin ovat: *kyberturvallisuuden* taso ei ollut riittävä.

Kyberturvallisuus on kybertoimintaympäristön turvaamista. Kybertoimintaympäristö koostuu useista toisiinsa yhdistyneistä verkoista eli internetistä, jossa dataa siirretään digitaalisessa muodossa käyttäjältä, näyttöpäätteeltä ja palvelimelta toiselle. Kybertoimintaympäristöön kuuluu olennaisesti ihminen, joka ainakin vielä toistaiseksi vastaa verkon ylläpidosta ja toiminnasta. Kyberturvallisuudella pyritään pitämään vahingolliset hyökkäykset kurissa niin, ettei verkossa oleva tieto joudu vääriin käsiin tai että verkkoon kytketyt laitteet suorittavat juuri ne tehtävät, jotka niille on määrätty.

Lokakuisen hyökkäyksen yhteydessä kyberturvallisuus petti. Internetsivut hidastuivat, koska jopa 10 miljoonaan yksittäiseen koneeseen tunkeuduttiin ja ne liitettiin osaksi hyökkäystä (York 2016). Koska käyttäjät eivät itse pystyneet reagoimaan hyökkäykseen, sen selvitys jäi valtionhallinnon tehtäväksi (Edwards, Beech & Walsh 2016). Valtiolla on valta ja vastuu selvittää, kuinka hyökkäykset korjataan ja parhaimmassa tapauksessa ennaltaehkäistään. Kyberiskuista eivät kärsi vain yritykset ja yksityishenkilöt, sillä myös monet yhteiskunnan perustoiminnot on digitalisoitu ja alttiita hyökkäyksille. Perustoimintoja vastaan hyökkää toiset valtiot tavoitteenaan murentaa kohdevaltion toiminta. Monissa valtioissa kyberhyökkäysten torjunta onkin annettu puolustusministeriön tehtäväksi, minkä seurauksena viimeisen viiden vuoden aikana kyberturvallisuus on nostettu prioriteetiksi valtioiden puolustusstrategioissa.

Tässä tutkimuksessa tarkastelen valtioiden kyberturvallisuutta niiden kyberturvallisuusstrategioiden kautta. Yli 80 valtiota on julkistanut ensimmäisen tai päivitetyn version maansa kyberturvallisuusstrategiasta 2010-luvulla (CCDCOE 2016). Kyberturvallisuusstrategia kartoittaa valtioon kohdistuvia uhkia ja toisaalta sen mahdollisuuksia ja on olennainen osa valtioiden uskottavuutta ja luotettavuutta (Limnéll, Majewski & Salminen 2014: 59, 158). Moni strategioista on julkaistu vuoden 2013 jälkeen, jolloin sattui yksi historian pahimmista tietovuodoista, kun Yhdysvaltojen entinen tiedustelutyöntekijä Edward Snowden paljasti maan tiedustelupalvelu NSA:n laajamittaisen kuuntelu- ja seurantaohjelman (Gellman, Blake & Miller 2013). Nuo tapahtumat eivät ole ainakaan vähentäneet valtioiden kasvavaa kiinnostusta kyberturvallisuuteen.

Kybertutkijoiden Jarno Limnéllin, Klaus Majewskin ja Mirva Salmisen (2014: 16–17, 20–21) mukaan kyberturvallisuudesta on tullut pysyvästi yksi valtioiden turvallisuuden alueista. Muutos on tapahtunut nopeasti, sillä pelkästään internetin valtavirtaistumisesta on vasta noin 15 vuotta. Jatkuvasti muuttuva kybermaailma ja sen turvaaminen vaikuttavat valtioiden välisiin suhteisiin ja siihen, mitä eri kybermaailman toimijat toiminnallaan tavoittelevat. Toisin sanoen kyberturvallisuudesta on tullut poliittinen väline. Sen vuoksi kyberturvallisuudesta puhutaan niin paljon. Valtiot ovat kiinnostuneita kybermaailman strategisista mahdollisuuksista, ja kyberturvallisuudesta on monissa maissa tullut yksi sodankäynnin ulottuvuuksista. Esimerkiksi Yhdysvallat ilmoitti vuonna 2013 suurimmaksi kansallista turvallisuutta uhkaavaksi tekijäksi kyberuhat terrorismin sijasta. Kyseessä on iso strateginen muutos, sillä Yhdysvallat on maailman johtavin sotilaallinen supervalta.

Kybermaailma on tullut osaksi paitsi turvallisuuspolitiikkaa, myös muita yhteiskunnan alueita. Esimerkiksi Viro myöntää e-kansalaisuuksia, jonka kautta kansalainen saa digitaalisen identiteetin ja joka helpottaa yrityksen perustamista (e-Estonia 2017). Suomessa taas on mahdollista tunnistautua pankin verkkopankkitunnuksilla moniin yhteiskunnallisiin palveluihin, kuten vero-, sosiaalietu- ja potilastietokantoihin (Suomi.fi 2017). Kun iso osa valtion tarjoamista palveluista on digitalisoitu, voidaan sanoa, että valtiot ovat siirtyneet kyberaikakauteen. Verkossa oleva arkaluontoinen tieto houkuttelee toisia valtioita, rikollisia ja muita tiedusteluorganisaatioita etsimään keinoja päästä käsiksi siihen. Tämä on vaatinut valtioita kehittämään kyberturvallisuutta.

Kyberturvallisuusstrategioiden tutkiminen on tärkeää, sillä kyberhyökkäykset ovat monimuotoisia ja niitä tapahtuu usein. Pelkästään vuoden 2016 tammikuusta lokakuuhun välisenä aikana Viestintävirasto varoitti verkkosivuillaan 133:sta suomalaisia koskettavasta haavoittuvuudesta (Viestintävirasto 2016a). Valtioilla on merkittävä rooli kyberturvallisuuden ylläpitämisessä, sillä tieto- ja viestiliikenneverkot kuuluvat maiden infrastruktuuriin. Sen vuoksi kyberturvallisuuden tutkiminen valtioiden tuottamien dokumenttien kautta on mielestäni johdonmukaista: kybermaailman merkittävimpinä toimijoina niiden suunnittelemat strategiset toimenpiteet vaikuttavat jokaisen kansalaisen verkon käyttöön. Lisäksi valtiot määrittelevät lait, joiden puitteissa verkkoa käytetään. Kyberturvallisuusstrategiat vastaavat muuttuneen toimintaympäristön asettamiin haasteisiin.

1.1 Tavoite

Kyberturvallisuusstrategian julkaisseet valtiot perustelevat tarvetta strategialle niin aineettoman tiedon kuin kansalaisten fyysisen turvallisuuden näkökulmasta. Usein turvallisuutta ylläpidetään hallitsemalla eli olemalla tietoisia muiden kybermaailman toimijoiden liikkeistä. Tämä edellyttää tiedustelua. Ongelmalliseksi tiedustelu voi muuttua silloin, jos kerättyä dataa ei kyetä turvaamaan tai säilyttämään oikealla tavalla. (Limnéll ym. 2016: 60.) Valtio voi kansalaistensa turvallisuuteen nojaten kerätä tietoja laajastikin. Kyberturvallisuudesta tulee kyseenalaista tai ristiriitaista, jos sen varjolla pyritään rajoittamaan tai valvomaan kansalaisia liikaa.

Onko valtioiden tiedustelutoiminta sitten liian laajamittaista? Kyberturvallisuusstrategia on oikea väline vastaamaan tähän. Poliittinen teksti on aina tavoitteellista eli sillä on jokin päämäärä. Päämäärän saavuttaminen vaatii toimenpiteitä, ja se mitä tekstillä pyritään saavuttamaan, on lukijan vakuuttaminen. Tässä työssä tavoitteenani on selvittää, millaisia vakuuttamisen puhetapoja eli diskursseja valtiot kyberturvallisuusstrategioissaan käyttävät ja mitä niillä halutaan saavuttaa. Tutkimuskysymyksiäni ovat:

1) Millaisia vakuuttamisen diskursseja kyberturvallisuusstrategioissa esiintyy?
2) Miten ja mitä vakuuttamisen diskursseilla pyritään saavuttamaan?

Ensimmäinen tutkimuskysymys pitää sisällään sen, mitä vakuuttamisen keinoja strategioissa on käytetty ja millaisia diskursseja niiden taustalta löytyy. Tarkoituksena on paikantaa strategioista vakuuttamisen keinoja ja niiden pohjalta määritellä diskurssit. Tutkimuskysymyksistä toinen kattaa sen, mitä vakuuttamisen keinoilla on niiden käyttötilanteessa tehty ja millaisia tavoitteita valtioilla on kybermaailman suhteen. Toisin sanoen pohdin sitä, mihin valtiot diskursseillaan pyrkivät.

Diskurssien tutkiminen eli diskurssianalyysi on kielen ja viestinnän tutkimuksen työkalu, jonka avulla kielestä pyritään löytämään erilaisia merkitysrakenteita (Saaranen-Kauppinen & Puusniekka 2006). Diskurssianalyysin soveltaminen erilaisiin aineistoihin voi tuottaa monenlaisia vastauksia, mikä riippuu kysymyksenasettelusta ja teoreettisesta viitekehyksestä. Kyberturvallisuusstrategioita tarkasteltaessa diskurssianalyysi antaa vastauksia valtioiden välisistä suhteista ja kyberturvallisuuden asemasta niissä. Diskurssit eivät ole välttämättä suoraan luettavissa tekstistä, mutta oikeilla työkaluilla tutkijalle aukeavat huomaamattomatkin kielen vivahteet.

Diskurssianalyysi on tutkimukseni pääasiallinen tutkimusmetodi, mutta lainaan työkaluja analyysiin myös retoriikasta. Retoriikassa on kyse siitä, miten puhuja onnistuu vakuuttamaan yleisönsä ja argumentoimaan väitteensä. Niin kutsuttu uusi retoriikka, johon tästä eteenpäin retoriikasta puhuessani viittaan, tutkii keinoja, joilla väitteistä tehdään uskottavampia. Kun diskurssianalyysi ja retoriikka yhdistetään tutkimuksessa, analyysista saadaan moniulotteisempi. Retorisia keinoja tutkimalla voidaan sanoa enemmän siitä, miten diskurssit muodostuvat kielellisesti, sillä diskurssit itsessään katsotaan usein kulttuurin tuotteiksi. (Jokinen 1999/2006: 46–47.) Analyysissani retoriset keinot toimivat kahdella tapaa: 1) välineinä paikantaa diskurssit ja 2) esimerkkeinä diskurssien vakuuttavuudesta.

Tutkimuksessani tarkastelen valikoitujen valtioiden kyberturvallisuusstrategioita. Niitä ovat julkaisseet pääasiassa länsimaiset ja kehittyneet Aasian valtiot. Valtaosa kansallisista kyberturvallisuusstrategioista pitää sisällään jonkinlaisen yleiskuvauksen tai johdannon sekä toimenpidesuunnitelman. Johdantoa voi edeltää vastaavan ministerin tai strategian teettäneen työryhmän edustajan julkinen kirje, jossa pohditaan kansakunnan tilaa ja kyberturvallisuusstrategian oikeutusta.

Tutkimuksen kokonaisuuden kannalta on olennaista ymmärtää, miten kyberturvallisuusstrategiat asettuvat osaksi laajempaa kyberturvallisuuden ilmiötä. Kybermaailma ei ole vain teknologisen kehityksen huipentuma, vaan ”strateginen ja poliittinen asia, jossa ’ison kuvan ja suunnan määrittämisen’ ymmärrys on valitettavan heikkoa” (Limnéll ym. 2014: 14). Tämä tarkoittaa sitä, että vaikka kyberkeskustelut usein linkitetään teknologiaan, siihen liittyy paljon muutakin. Valtioilla, yrityksillä ja yksityishenkilöillä on kaikilla omat motiivinsa kybermaailmassa, eivätkä ne läheskään aina liity teknologiaan. Yksittäisiin asioihin keskittyminen ei Limnéllin ym. mukaan ole pitkällä aikavälillä kannattavaa, vaan he peräävät kyberasioiden pitkäjänteisempää suunnittelua etenkin valtioilta. Kyberturvallisuusstrategioissa keskitytään saavuttamaan kokonaisvaltaisempi ymmärrys kybermaailman sen hetkisestä tilasta.

1.2 Aineisto

Tutkimukseni aineisto koostuu kyberturvallisuusstrategioista niiden valtioiden osalta, jotka ovat sellaisen julkaisseet yleisesti saatavaksi. Strategiat on otettu tarkasteluun kokonaisuudessaan, mikä käsittää johdannot, visiot, perusperiaatteet, toimenpiteet sekä mahdolliset työryhmän tai vastaavan ministerin puheet. Aineisto on koottu kokonaisuudessaan syksyllä 2016 Naton kyberpuolustusyksikön verkkosivuilta, jonne on listattuna eri maiden kyberturvallisuusstrategiat (CCDCOE 2016). Diskurssianalyyttisessa tutkimuksessa aineisto on usein työläs suuren kokonsa vuoksi. Diskurssianalyytikot Arja Jokinen, Kirsi Juhila & Eero Suoninen (2016: 453–454) huomauttavat, että tällöin on mahdollista erottaa analysoitavaksi pieni joukko varsinaisesta laajemmasta aineistosta. Pienen joukon analysoiminen samankaltaisten tekstien osalta antaa todennäköisemmin uutta tietoa, kun tutkija pystyy analysoimaan aineistoaan yksityiskohtaisemmin. Aineiston rajauksessa on tärkeää, että sitä ohjaa jonkinlainen tutkimusintressi.

Valtavan määrän vuoksi – 81 julkaistua tai suunniteltua strategiaa – rajasin aineistosta viisi kyberturvallisuusstrategiaa analysoitavaksi tähän tutkimukseen. Rajaus toteutettiin deduktiivisesti eli aineistosta on rajattu pois strategioita siltä osin, kun ne eivät sopineet tutkimusasetelmaan. Tavoitteenani oli paikantaa strategiat, jotka ovat tämän tutkimuksen

puitteissa mahdollista analysoida ja jotka vastaavat tutkimuksen tavoitteisiin. Aluksi aineistoon sisällytettiin pelkästään sellaiset strategiat, joiden alkuperäiskieli on englanti ja joista on tehty virallinen englanninkielinen käännös. Tässä vaiheessa mukana oli vielä Suomen kyberturvallisuusstrategia. Lisäksi strategiat olivat valtioiden virallisia kyberturvallisuusstrategioita, eivätkä esimerkiksi osa yleistä puolustusstrategiaa tai toiselle kielelle käännettyjä yhteenvetoja. Tämän jälkeen strategioita oli jäljellä 47.

Tutustuttuani strategioihin tarkemmin havaitsin, että toisista välittyy selkeämmin tavoite vakuuttaa kuin toisista. Tämä näkyy siten, että osassa strategioista on käytetty paljon retorisia keinoja (ks. luku 3.3), kuten me-retoriikkaa tai metaforia, kun taas toiset kyberturvallisuusstrategiat toteavat asiat yksinkertaisesti ja asiapitoisesti. Havaintoni ei tarkoita, etteikö kaikissa strategioissa olisi käytetty retorisia keinoja – toisissa niitä on vain vähän tai ne eivät näy itse tekstissä. Esimerkiksi se, mitä tekstistä on jätetty pois, on retorinen keino, mutta se ei ole konkreettisesti näkyvissä. Koska tutkin vakuuttamisen diskursseja ja keino niiden paikantamiseen on retoristen keinojen erittely, rajasin aineistosta pois sellaiset strategiat, joissa retorisia keinoja ei ole juuri käytetty tai ne eivät näy itse kielestä. Näkyvä retoristen keinojen käyttö osoittaa, että puhujalla on enemmän syitä pyrkiä vakuuttamaan, jolloin vakuuttaminen on tietoista toimintaa. Pyrkiessäni paikantamaan diskursseja tämä oli tutkimukseni kannalta erityisen kiinnostava seikka.

Edellisen rajauksen jälkeen strategioita oli vielä 17 jäljellä. Näistä rajasin pois sellaiset, joissa ei ollut asiasta vastaavan ministerin tai strategian laativan työryhmän jäsenen kirjoittamaa alustuspuhetta. Kasvojen antaminen tekstille on erityinen keino vakuuttaa lukija, koska henkilössä kiteytyy koko tekstin eetos eli luonne, joka on kenties tärkein vakuuttamisen syy (ks. esim. Aristoteles 2012: 11). Tämän vuoksi alustuspuheelliset strategiat ovat olennaisia tutkimusintressieni kannalta. Jäljelle jääneet 13 maata kattavat lähes kaikki maapallon maanosat, joten saadakseni aineistooni moniäänisyyttä eri puolilta maailmaa, valitsin jokaisesta maanosasta yhden strategian. Jokainen strategia on maanosassaan julkaisuajankohdaltaan tuorein. Uusimmat strategiat antavat ajankohtaisen kuvan kyseisten maiden käsityksistä kybermaailman ja kyberturvallisuuden osalta. Analyysivaiheeseen alkuperäisestä aineistokorpuksesta rajautui lopulta Australian, Iso-Britannian,

Nigerian, Singaporen ja Yhdysvaltojen strategiat. Lopullinen aineisto on koottu taulukkoon 1.

Taulukko 1. Analysoitavat kyberturvallisuusstrategiat

Maa	**Maanosa**	**Julkaisuvuosi**
Australia	Oseania	2016
Iso-Britannia	Eurooppa	2016
Nigeria	Afrikka	2015
Singapore	Aasia	2016
Yhdysvallat	Amerikka[1]	2003/2015[2]

Pyrin rajaamaan aineiston niin, että mukaan sijoittuisi mahdollisimman monenlaisia valtioita. Lukuprosessi on aina subjektiivinen tapahtuma, ja diskurssianalyysin kautta tekstistä nousee esiin seikkoja, joihin maallikkolukija ei välttämättä kiinnittäisi huomiota, eikä rajaukseni tällöin olisi hänelle perusteltu. Diskurssianalyysissa tutkija on kuitenkin itse valinnut tutkimusasetelmansa ja käsitteet, joiden pohjalta tutkimus etenee (Jokinen ym. 2016: 453) ja aineisto rajautuu. Jäljelle jäävien maiden kyberturvallisuusstrategiat voidaan laajentaa käsittämään muita samankaltaisia strategioita, eli lähes neljäsosaa olemassa olevista strategioista. Rajauksen jälkeen on jo tässä vaiheessa mahdollista todeta, että koska jokainen analysoitavista valtioista on alueellaan vaikutusvaltainen ja suurimman osan kohdalla valtamedia kirjoittaa kyberasioista usein, näiden strategioiden taustalla on tarve saavuttaa jokin päämäärä. Koska kyseisillä valtioilla on lisäksi kokemusta kyberhyökkäyksistä – sekä itse toteutetuista että niitä vastaan puolustautumisesta – niillä on myös laajempi käsitys kybermaailmasta kuin valtioilla, joilta ei vielä tämän kaltaista kokemusta löydy.

[1] Aineistossa Pohjois-ja Etelä-Amerikka on yhdistetty, sillä Etelä-Amerikan kyberturvallisuusstrategioista yksikään ei täyttänyt rajauksen ehtoja viimeisten rajausperusteiden osalta.
[2] Yhdysvaltojen kyberturvallisuusstrategia koostuu useammasta eri julkaisusta. Tässä työssä tarkasteltavana on ensimmäinen vuonna 2003 julkaistu kyberturvallisuusstrategia, jota on myöhemmin täydennetty vuonna 2015 julkaistulla puolustusministeriön strategialla.

1.3 Menetelmä

Analyysimenetelmänä hyödynnän diskurssianalyysia, johon yhdistän työkaluja retoriikasta. Diskurssianalyysi on kvalitatiivinen eli laadullinen menetelmä, jonka pyrkimyksenä on ymmärtää kulttuuria ja selittää merkityksellistä toimintaa (Alasuutari 2011: 24). Diskurssianalyysilla pyritään löytämään kielestä erilaisia puhetapoja eli diskursseja. Samasta asiasta voidaan puhua lukemattomin eri diskurssein ja olennaista onkin, missä kontekstissa puhe tapahtuu. (Saaranen-Kauppinen & Puusniekka 2006.) Arja Jokinen, Kirsi Juhila & Eero Suoninen (1993/2000: 9, 17) kirjoittavat, että diskurssianalyysissa kieli rakentaa ja muokkaa todellisuutta sen sijaan, että vain kuvaisi sitä. Diskurssianalyysi on keino ymmärtää kielen rakentamia todellisuuksia ja eritellä niitä toisistaan. Retoriikka sen sijaan tutkii tekstin vakuuttavuutta ja argumentointikeinoja (Jokinen 1999/2006: 46).[3]

Diskurssianalyysi on jakautunut moniin eri perinteisiin, joissa kussakin painotetaan kieltä eri tavoin. Eri suuntauksia ja perinteitä käyttämällä voidaan saada monipuolisia tuloksia samoista teksteistä, sillä tutkimuskohdetta lähestytään useista näkökulmista. Omat tutkimussuuntauksensa ovat muun muassa Ranskassa, Saksassa ja Iso-Britanniassa. Ranskassa diskurssin katsotaan muodostuvan kulttuurisissa käytänteissä, kun taas saksalaisessa traditiossa korostetaan todellisuudesta nousevia diskursseja. Iso-Britannian koulukuntaa kiinnostaa keskusteluun pohjautuvat diskurssit. Maantieteellisten alueiden lisäksi diskurssianalyysia jaotellaan muun muassa tieteenfilosofisesti, lähtöoletuksista ja tavoitteista käsin tai tutkijan position mukaisesti. Positioitumisessa on kyse siitä, millä tavalla tutkija tekstiä lähestyy. Se voi olla puhtaasti tekstuaalista, tulkinnallista tai kriittistä. (Pynnönen 2013: 24–25, 39–40.) Kun tekstianalyysista siirrytään kriittiseen lähestymistapaan, kontekstin merkitys korostuu. Tällöin tutkija analysoi tekstin lisäksi sen syntykontekstia ja pystyy siten sanomaan enemmän tutkittavasta aiheesta kuin mihin tekstianalyysi yksinään riittäisi.

[3] Tässä tutkimuksessa diskurssianalyysiin on yhdistetty retoriikkaa vain retoristen keinojen osalta. Koska retoriikka toimii menetelmässäni välineenä diskurssianalyysin toteuttamiseksi, en tässä kohdin perehdy tarkemmin retoriikan perinteeseen. Retoriikan roolia tutkimuksessa käsittelen luvussa 3.2 ja retoriset keinot esittelen luvussa 3.3. Enemmän uudesta retoriikasta metodina voi lukea esimerkiksi Perelmanilta (1996).

Haasteena tutkijalla on löytää juuri omaan tutkimukseensa sopivat työkalut niin, etteivät erilaiset teoriaperinteet ole ristiriidassa keskenään. Itse lähestyn diskurssianalyysia brittiläisestä perinteestä käsin hyödyntämällä muun muassa Norman Fairclough'n ja Michael Billigin diskurssiteorioita. Tutkijapositioni on läpi tutkimuksen kriittinen ja näin ollen korostan kontekstin merkitystä tekstianalyysin yhteydessä. Kirsi Juhilan (1999/2006: 207–208) mukaan kriittisesti tekstiä lähestyvä tutkija asemoi itsensä *asianajajaksi*. Tällöin tutkijalla on jokin motiivi tai päämäärä murtaa diskursseja ja tekstuaalisia valtarakenteita. Lisäksi asianajaja nojautuu usein Michel Foucault'n valtateoriaan. Vaikka omassa lähestymistavassani on paljon samaa kuin asianajajan positiossa, en tarkastele tekstiä vain yhdestä asemasta käsin, vaan toisinaan tutkijapositioni on ollut *analyytikko.* Analyytikkona tutkija häivyttää oman osallisuutensa minimaaliseksi (Juhila 1999/2006: 203), kuten olen itsekin pyrkinyt tekemään tekstuaalisen analyysin osalta. On kuitenkin hyvä muistaa, että huolimatta siitä, millaisista lähtökohdista tutkimusta aletaan tehdä, tekstistä muodostetut diskurssit ovat aina tulkintoja (Saaranen-Kauppinen & Puusniekka 2006).

Kriittisessä diskurssianalyysissa tutkitaan, miten valtasuhteet syntyvät ja kuinka vallanpitäjät tavoittelevat, saavuttavat ja ylläpitävät valta-asemaansa sekä sitä, kuinka sen mahdollista väärinkäyttöä vastustetaan (Pynnönen 2013: 28). Tutkimukseni aineisto koostuu poliittisista strategiateksteistä. Strategiat eivät ole ilmestyneet tyhjästä, vaan niiden taustalla on joukko asiantuntijoita, joiden ideoita uskova poliitikko julkaisee strategian nimissään kansalaisille. Poliittiset johtajat ovat käytännössä aina jonkinlaisessa päätösvalta-asemassa kansalaisiin nähden. Kansalaiset halutaan vakuuttaa päätösten oikeellisuudesta, mutta se ei tarkoita, että päätös olisi aina oikein tai paras mahdollinen vaihtoehto. Vakuuttaminen on kuitenkin poliittisen kielen teko. Kun kriittisen diskurssianalyysin puitteissa tutkitaan vakuuttamista ja taivuttelua, puhutaan retorisesta kritiikistä. Retorinen kritiikki antaa vastauksia siihen, kuinka yksittäisissä teksteissä taivutellaan valta-asetelman heikompia osapuolia (Pynnönen 2013: 30).

Kriittisen diskurssianalyysin soveltaminen strategiateksteihin tarjoaa epäilemättä hyödyllistä tietoa valtahierarkioista. Eero Vaara, Virpi Sorsa & Pekka Pälli (2010: 688, 694,

696) toteavat, että diskurssianalyysin kautta paljastuu strategioiden valta- ja dominointisuhteet. Strategiateksteissä käytetty retoriikka on usein niin taitavasti kirjoitettu tekstiin sisään, ettei lukija välttämättä tunnista sitä, mistä taas seuraa väärät mielikuvat ja tilanteiden yksinkertaistaminen. Valta on siis usein piilotettuna strategiateksteissä. Mitä ohjaavampi tai määräävämpi strategiateksti on luonteeltaan, sitä todennäköisemmin strategian toteamukset tulkitaan suorina käskyinä, eli vastaanottaja alkaa muokata käytöstään halutunlaiseksi. Tämän pohjalta kriittinen diskurssianalyysi vastaa tutkimukseni tavoitteisiin: millaisin keinoin vallanpitäjät pyrkivät kyberturvallisuusstrategioissa valtansa oikeuttamaan ja mitä he yrittävät niillä saavuttaa.

1.4 Tutkimuksen konteksti ja rakenne

Kyberavaruus ja kyberturvallisuus on uusia asioita niin valtioille kuin sen kansalaisillekin. Kyberin tutkiminen on tärkeää, sillä siihen liittyy usein digitaalinen uhka, mikä sävyttää pitkälti myös siitä käytyä keskustelua, eikä suotta, sillä globaalisti kyberiskut ovat jo melko tavallisia. Historian suurin tietomurto kohdistui Yahoota vastaan vuosina 2013 ja 2014, mutta hyökkäys huomattiin vasta vuonna 2016. Iskussa varastettiin miljardin käyttäjätilin tiedot. (Thielman 2016.) Vuonna 2014 hyökkääjät iskivät Sony PlayStation Networkiin ja varastivat pelaajien luottokorttitietoja (BBC 2014). Loppuvuodesta 2016 pidetyt Yhdysvaltojen presidentinvaalit aiheuttivat useita kohuja: ennen vaaleja vuodettiin demokraattiehdokas Hillary Clintonin sähköposteja ja vaalien jälkeen Yhdysvaltojen tiedustelupalvelu ilmoitti, että Venäjä on saattanut vaikuttaa vaalien lopputulokseen Donald Trumpin hyväksi (ks. esim. Kähkönen 2016; Liimatainen 2016). Alkuvuodesta 2017 Suomessa arvosteltiin autoverolakiuudistusta, jonka seurauksena autoihin kaavailtiin asennettavaksi ”musta laatikko”, joka kerää ajokilometrit talteen. Useasti testatun laitteen todettiin olevan hyökkääjille helposti läpäistävä ja näin ollen uhka kansalaisten yksityisyydensuojalle. (Mansikka 2017.)

Kyberturvallisuutta siis todella tarvitaan, ja siksi tarvitaan myös tutkimusta siitä. Kyberturvallisuusstrategioita ovat tutkineet Eric Luiijf, Kim Besseling, Maartje Spoelstra ja Patrick de Graaf (2011; myös Luiijf, Besseling ja de Graaf 2013) vertaamalla valtioiden

heikkouksia ja mahdollisuuksia kybermaailmassa erilaisista aineistoista käsin. Jarno Limnéll on kirjoittanut kybersodasta ja Suomen strategiasta useita artikkeleita vuosina 2014–2016. Kyoung-Sik Min, Seung-Woanin Chai ja Mijeong Han (2015) tutkivat artikkelissaan yksityisen ja julkisen sektorin kumppanuutta kybermaailmassa. Myös ei-valtiollisilta organisaatioilta, kuten ENISA (2014) ja OECD (2012), on julkaistu raportit strategioiden pääpiirteistä. Monissa julkaisuissa aineistona on 10–20 raporttia, joten oma tutkimukseni, joka keskittyy vain viiteen strategiaan, pääsee huomattavasti syvemmälle tutkittavaan aineistoon. Diskurssianalyyttista tutkimusta kyberturvallisuusstrategioista on aikaisemmin tehnyt Aleksi Saloharju (2015) pro gradu -tutkielmassaan, jonka näkökulma on kyberturvallisuuskäsityksissä ja alueellisissa eroissa. Tällä tutkimuksella kyberkeskusteluun tuodaan uusia sävyjä pohtiessani, minkälaisilla vakuuttamisen diskursseilla valtiot perustelevat valintojaan ja tavoittavat lukijansa.

Tutkimuksen tavoitteen, aineiston ja menetelmän esittelyn jälkeen tutkimus etenee niin, että luvussa 2 tarkastelen kybermaailmaa ja kyberturvallisuutta uutena teknologisena ympäristönä. Määriteltyäni käsitteet pohdin, mitä kyberturvallisuudella todella turvataan ja millaisia muita turvallisuuden lajeja digitaaliseen maailmaan yleensä liitetään. Kybermaailma on tuonut mukanaan myös ongelmia, joista yleisimpiä tarkastelen turvallisuuslajien jälkeen. Valtioiden vastine ongelmille on kyberturvallisuusstrategiat, mutta tärkeää on lisäksi ymmärtää, mikä valtion rooli kybermaailmassa on. Tämän perusteella voidaan todeta, millaisia strategioita valtiot ovat saaneet aikaiseksi.

Luvussa 3 avaan laajemmin kriittistä diskurssianalyysia ja vakuuttamisen keinoja sekä näiden keskinäistä suhdetta. Luvussa 4 esittelen laajemmin aineiston valtioiden tilannetta kybermaailmassa ja analysoin kyberturvallisuusstrategioita soveltamalla diskurssianalyysia. Luvun lopuksi esitän vastaukset tutkimuskysymyksiini. Luvussa 5 kokoan tutkimustulokset yhteen, pohdin tutkimukseni onnistumista ja esitän mahdollisia jatkotutkimuskysymyksiä.

2 UUSI TOIMINTAYMPÄRISTÖ

Tämän luvun tavoitteena on selvittää tarkemmin, mitä tarkoittavat käsitteet kybertoimintaympäristö ja kyberturvallisuus. Koska kyberturvallisuutta ei olisi ilman digitaalisen verkon eli internetin turvattomuutta, tarkastelen myös lyhyesti internetin historiaa ja kyberturvallisuuden kehittymistä sekä sitä seuranneita uhkia. Pohdin myös lyhyesti valtion roolia kybermaailmassa, sillä valtiot ovat vastanneet ongelmiin julkaisemalla kyberturvallisuusstrategioita, ja on olennaista ymmärtää, mikä strategiateksti on ja miten se soveltuu kybermaailmaan.

2.1 Kyber käsitteenä

Kyber-etuliitteen historia yltää 1940-luvulle saakka ja sitä seuranneiden vuosikymmenien aikana sen merkitys on muuttunut useaan otteeseen. Ensimmäisenä käsitettä käytti Norbert Wiener teoksessaan *Cybernetics: Or Control and Communication in the Animal and the Machine* (1948). Wiener yhdisti tutkimuksessaan viestintää teknologian ohjaukseen ja havaitsi, että ihmisellä on merkittävä rooli koneiden hallinnassa. Hän nimesi uuden tieteenhaaran kybernetiikaksi, joka tulee kreikan kielen sanasta *kybernētēs* (perämies). (Mindell 2003: 4.) *Kybernētēs*in kantasana taas on *kybereo*, joka tarkoittaa ohjaamista, opastusta tai hallintaa (Limnéll ym. 2014: 29). Alkujaan kyber-etuliitteellä viitattiin siis ihmisen ja koneiden väliseen viestintään, jossa ihminen toimi ohjaajana.

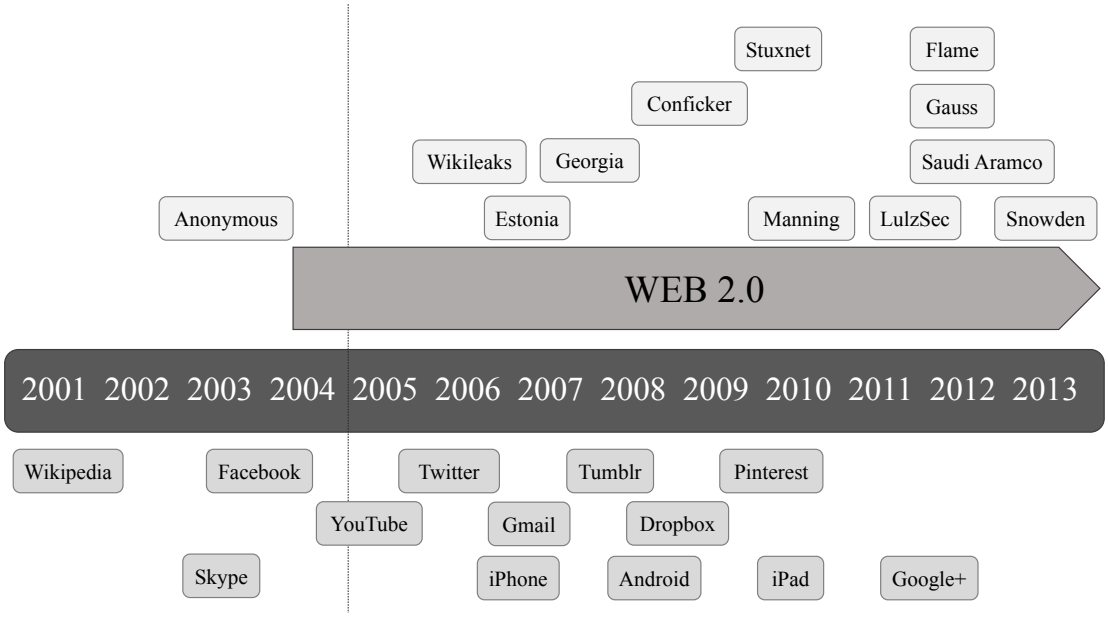
Kybernetiikka on aina liitetty jollakin tasolla tietotekniikkaan. 1980-luvulla tietokoneiden kehittyessä kybernetiikka alettiin nähdä edistystieteenä. Valtavirran tietoisuuteen kyber tuli vuonna 1984, kun William Gibson yhdisti tieteisromaanissaan *Neurovelho* (engl. *Neuromancer*) sanat kyber ja avaruus toisiinsa (engl. *cyberspace*). Limnéllin ym. (2014: 30) mukaan 1990-luku oli kyberneettisen ajatusmaailman kulta-aikaa internetin mahdollistaessa ihmisen ja koneen ”saumattoman yhteistyön”.

Vaikka kyberin tausta juontuu kybernetiikasta, ei se enää tarkoita ihmisen tulemista osaksi koneita ja niiden kontrollointia. Käsitteen uudelleenmäärittely on kesken, ja toisinaan tutkijat jopa kieltäytyvät määrittelemästä sitä (ks. esim. Hamilton 1998: 179; Limnéll 2014: 3–4). Limnéllin ym. (2014: 30–31) mukaan käsitteelle on ollut tarve määritettäessä uudenlaista toimintaympäristöä, jossa ihmisellä on erilaisia toiminnan mahdollisuuksia, ja toisaalta uhkia, joita fyysisessä maailmassa ei ole. Yksinkertaisuudessaan kybertoimintaympäristöllä viitataan digitaaliseen maailmaan.

Yhdysvaltalaiset kybertutkijat Peter W. Singer ja Allan Friedman (2014: 13) määrittelevät kybertoimintaympäristön koostuvan ”verkossa olevien tietokoneiden valtakunnasta, -- jossa tietoa varastoidaan, jaetaan ja kommunikoidaan online-tilassa” – mukaan lukien verkon ja koneiden käyttäjät. Singerin & Friedmanin määrittely on varsin yhtenäinen Limnéllin ym. kanssa, sillä molempien mielestä ihminen ja sen toiminta kuuluvat olennaisesti kybertoimintaympäristöön.

Erona Limnélliin ym. Singer & Friedman pohtivat laajemmin kybertoimintaympäristön fyysisiä ulottuvuuksia. Heidän mukaansa kybertoimintaympäristö ei ole maantieteellisesti tai millään muullakaan määritelmällä rajaton. Valtiot hallinnoivat toimintaympäristöä maiden rajojen sisäpuolella, ei-valtiolliset organisaatiot taas jotakin muuta globaalin verkon osa-aluetta. Lisäksi kybertoimintaympäristöä määrittää jatkuva muutos. Jos alussa se näyttäytyikin pelkästään tiedonsiirron välineenä, 2010-luvulla kaikki valtioiden kriittisimmät infrastruktuurit toimivat kybermaailmassa aina sähkö- ja vesilaitoksia sekä liikenteenohjausta myöten. (Singer & Friedman 2014: 14–15.)

Kybermaailmalle on ominaista suhteellisen lyhyt ikä. Internet levisi laajan yleisön käyttöön 1990-luvun lopulla, mutta varsinaisen liiketoiminnan katsotaan alkavan vuodesta 2005. Tällöin puhutaan Web 2.0:sta. Sosiaalinen media ja älypuhelimet, jotka ovat erottamaton osa kansalaisten arkea vuonna 2017, esiteltiin vain hieman yli kymmen vuotta sitten. Kuuluisimmat kyberhyökkäykset ja haittaohjelmatkin sijoittuvat viimeisen vuosikymmenen sisään. Kybermaailman merkittävät virstanpylväät on koottu kuvioon 1. Vasta viimeiset viisi vuotta ovat näyttäneet mihin suuntaan kybermaailma on kehittymässä. (Limnéll ym. 2014: 16–17.)



Kuvio 1. Kybermaailman kehitysaskelia ja -tapahtumia (Limnéll ym. 2014: 17)

Siksi on myös haastavaa sanoa, kuinka paljon erilaiset kyberhyökkäykset ovat lisääntyneet edellisistä vuosista, sillä vertailtavia vuosia ei juuri ole. Viestintäviraston mukaan vuosina 2013–2014 Suomessa jylläsi ”haittaohjelmaepidemioita”, mutta vuonna 2015 niitä löydettiin huomattavasti vähemmän, ja määrät ovat edelleen pienoisessa laskussa (Viestintävirasto 2016b). Ei kuitenkaan voida olettaa, että Web 2.0:n ongelmat katoaisivat. Kuviosta 1 ilmenee, että kaupallistumisen myötä kybermaailma on tuonut ihmisille yhä enemmän uusia palveluita ja tuotteita, kuten Facebookin, YouTuben ja iPhonen. Samanaikaisesti haitat ovat lisääntyneet tietovuotojen (Snowden, Manning) ja kyberhyökkäysten osalta (Conficker, Stuxnet, Gauss). Myös valtioiden välille on syntynyt uudenlaisia jännitteitä (Georgia, Viro), kun hyökkääjä on käyttänyt poliittisesti arkaluontoisia tilanteita edukseen kyberkohtaamisissa.

Vaikka kyber on muuttuva ja moniulotteinen, Suomen puolustusvoimien kyberjaoston päällikkö Catharina Candolin (2012) puolustaa blogissaan kyberiä käsitteenä. Hänen mukaansa kyberistä keskusteltaessa yleinen mielipide on, että sitä ei pitäisi käyttää, mutta

toisaalta kukaan ei ole tarjonnut parempaakaan tilalle. Kyberille tarjotut vastineet, kuten tietoverkko, tietoturvallisuus tai tietoverkkoturvallisuus, eivät kata kokonaisuudessaan kaikkea, mihin kyberillä viitataan. Tässäkään tutkimuksessa ei tehdä käsiteanalyysia kyberistä eikä tarkoituksena ole keksiä uutta käsitettä kyberin tilalle, joten käytän johdonmukaisinta ilmaisua. Niinpä kyberistä puhuessani tarkoitan sillä *ihmisen aikaansaamaa toimintaympäristöä, johon linkittyvät koneet, ihmiset ja kaikki niiden toiminnan mahdollistavat instituutiot.* Kybermaailma tai kybertoimintaympäristö on digitaalinen tila, jossa varastoidaan ja jaetaan tietoa. Kybermaailmasta puhutaan erityisesti sotilaallisissa ja puolustuspoliittisissa yhteyksissä. Sen suojaamiseen käytetään kyberturvallisuutta.

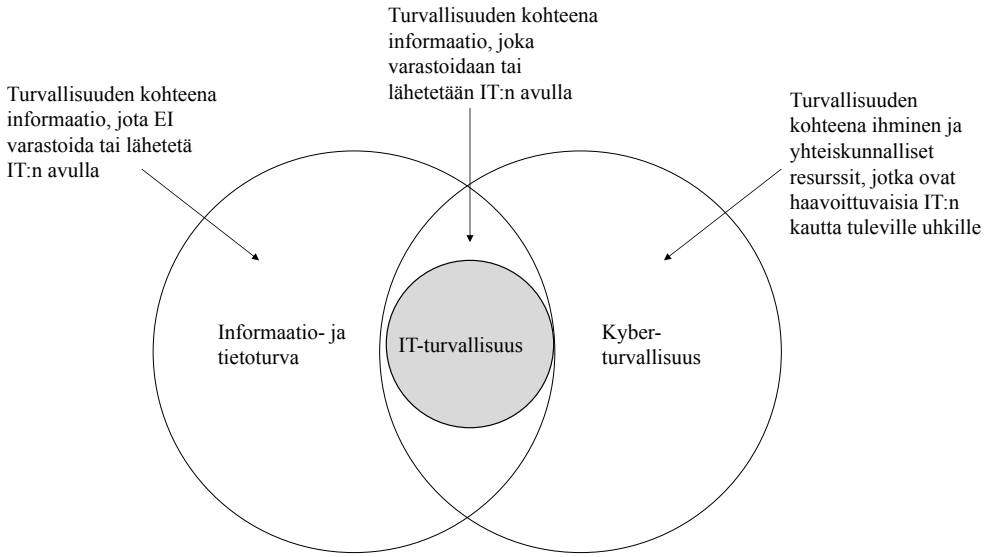
2.2 Turvallisuuden eri muodot

Kyberturvallisuudessa on kyse siitä, että jotakin pitää turvata. Jos ei olisi olemassa kyberhyökkäyksiä tai -sotaa, ei koko kyberturvallisuutta edes tarvittaisi. Turvallisuus on yksi yhteiskunnan perustarpeista. Kybermaailma on uusin turvallisuuden alue, jossa kaiken toiminnan tulisi jo alkujaan perustua tuotteen tai palvelun turvalliseen käyttöön. Se ei kuitenkaan vielä riitä, vaan käyttäjien täytyy lisäksi olla tietoisia kyberturvallisuudesta. Yksi kybermaailman suurimmista ongelmista onkin sen tuntemattomuus, eivätkä ihmiset tai yritykset osaa toimia verkossa ylläpitämällä turvallisuutta. (Limnéll ym. 2014: 13–14.) Tietoturva-asiantuntijoiden Kyoung-Sik Minin, Seung-Woanin Chain ja Mijeong Hanin (2015: 13) mukaan kyberturvallisuudelle ei ole yhtenäistä globaalia määritelmää, vaan jokainen maa, joka julkaisee kyberturvallisuusstrategian, tai tutkija, joka kirjoittaa aiheesta, määrittelee käsitteen uudelleen. Yhdenmukaiselle määritelmälle olisi kuitenkin tarvetta. Piia Holmgrenin pro gradu -tutkielmassa kyberturvallisuutta kuvaillaan seuraavasti:

> **Kyberturvallisuus** on digitalisoituneen maailman turvallisuutta, jossa sen [käyttäjillä] on [luottamus] turvallisuuteen. Kyberturvallisuus sijoittuu tieto- ja viestintäverkkoihin ja sen uhkina ovat muun muassa kyberuhkat, joihin kuuluvat kyberhyökkäykset, kybersodat ja kyberterrorismi. (Holmgren 2016: 29.)

Määritelmä ei kuitenkaan ole vielä kokonaisvaltainen, vaan siitä on jätetty pois muun muassa se, *mitä* kyberturvallisuudella lopulta turvataan. Tietotekniikan tutkijoiden Rossouw von Solmsin ja Johan van Niekerkin (2013: 97) mukaan suojauksen kohteen määrittäminen on tärkeää, sillä kyberturvallisuutta käytetään yleisesti informaatio- tai tietoturvan synonyymina.

Informaatiolla, tiedolla ja kyberillä on kuitenkin omat merkityksensä. Informaatio voi olla fysikaalista materian järjestystä tai kielen käyttöön perustuvaa ilmaisua. Esimerkiksi atomin järjestyminen osiensa kokonaisuudeksi on fysikaalista informaatiota samalla tavoin kuin sanojen järjestyminen kirjaimista suomen kieleksi. Tiedoksi informaatio muuttuu, kun se saa semanttisen merkityksen, eli kun ihminen tulkitsee kieltä itsellensä ymmärrettävään muotoon. Tieto ei silti ole lopullista tai ehdotonta, vaan sitä korjataan ja siihen lisätään informaatiota. Tieto on siis informaation alakäsite, joskin sitä yleisesti käytetään arkikielessä huomattavasti laveammassa merkityksessä. (Niiniluoto 1989: 48, 58–61.) Jos puhutaan tällaisen tiedon tai informaation turvaamisesta, informaatio- ja tietoturva on silloin oikea käsite.



Kuvio 2. Turvallisuuslajien kolmijako (von Solms & van Niekerk 2013: 97) [kääntänyt S.J.]

Von Solms & van Niekerk (2013: 97, 99) erittelevät informaatio-ja tietoturvan ja kyberturvallisuuden lisäksi kolmannen turvallisuuden muodon: informaatio- ja tietoturvateknologiaturvallisuuden eli IT-turvallisuuden. Käytän tässä tutkimuksessa suomenkielistä lyhennettä IT siitä teknologisesta kentästä, josta englanniksi puhutaan ICT:nä (*information and communication technology*). IT on lyhenne sanasta informaatioteknologia. Eri turvallisuuslajien kolmijako on esitetty kuviossa 2. Sen mukaan informaatio- ja tietoturvassa suojauksen kohteena on informaatio. Kyseinen turvallisuuden muoto kattaa digitaalisten sisältöjen lisäksi myös fyysisessä muodossa olevan informaation. Sen sijaan IT-turvallisuudella suojataan teknologian välityksellä tallennettavaa ja lähetettävää tietoa. Kyberturvallisuus eroaa näistä kahdesta siinä, että sen suojaamisen kohteena on kuka tai mikä tahansa, johon voidaan päästä käsiksi kybermaailman kautta. Turvallisuuden muodot eroavat toisistaan siis turvallisuuden kohteen perusteella. Informaatio- ja tietoturvallisuuden sekä kyberturvallisuuden kohteet voivat olla samoja, minkä lisäksi kaiken keskiössä on IT-turvallisuus, joka mahdollistaa muut turvallisuusmuodot.

Taulukko 2. Turvallisuusalueiden uhat, haavoittuvuudet ja turvallisuuden kohteet (von Solms & van Niekerk 2013: 99, 101) [kääntänyt S.J.]

	Uhat	Haavoittuvuudet	Turvallisuuden kohde
IT-turva	Useita	Useita	IT
Informaatio- ja tietoturva	Useita	IT, etc.	Informaatio
Kyberturvallisuus	Useita	IT, informaatio, etc.	Ihminen ja hänen resurssinsa

Toinen erottava tekijä on haavoittuvuus. IT-turvallisuus on altis niin viruksille, haitta- ja vakoiluohjelmille kuin fyysisen maailman ongelmillekin (mm. sähkökatkokset, pöly). Informaatio- ja tietoturvan yhtenä heikkoutena taas on IT-turvallisuus: jos teknologia pettää, informaatioon ei päästä käsiksi. Kyberturvallisuus on haavoittuvainen näille molemmille: kybermaailma voi vaarantua sekä tietoteknisistä syistä että informaation leviämisestä. Näin ollen kyberturvallisuus ikään kuin kattaa kaksi muuta turvallisuuden muotoa

haavoittuvuuden perusteella. Jos palataan vielä kybertoimintaympäristön määritelmään, joka koostuu koneista, ihmisistä ja instituutioista, kyberturvallisuus suojelee myös niiden toimintaa eikä pelkästään sisältöä. Nämä ilmenevät taulukosta 2. Yhteenvetona voidaan todeta, että kyberturvallisuudella turvataan ihmisten toimintaa ja resursseja digitaalisessa maailmassa. Koska kyberturvallisuuden haavoittuvuuksia ovat IT- sekä informaatio- ja tietoturvallisuus, myös niiden turvaaminen on oleellista kybertoimintaympäristön ylläpitämiseksi.

2.3 Internet: verkkojen verkko

Kybertoimintaympäristöön ja kyberturvallisuuteen liittyy olennaisesti internet. Internetiä käytetään usein synonyymina kybertoimintaympäristölle, sillä internet on ikään kuin konkreettinen ilmaisu sille, miten saadaan yhteys kybertoimintaympäristöön. Modernissa internetissä on kyse tiedonsiirrosta useiden erillisten verkkojen välillä. Vaikka internetiä ajatellaan usein yhtenäisenä koko maailman kattavana kokonaisuutena, todellisuudessa se pitää sisällään alueellisia pienempiä verkkoja, jotka keskustelevat keskenään yhteisellä teknisellä kielellä, joka lähes yksinomaan mahdollistaa internetin toiminnan. (Singer & Friedman 2014: 18.) Tässä tutkimuksessa internet nähdään ensisijaisesti välineenä, jonka avulla tieto liikkuu kybertoimintaympäristössä.

Perinteisesti internetin historia ajoitetaan alkamaan ARPANETistä. Vuonna 1969 käyttöönotettu ARPANET oli Yhdysvaltojen puolustusministeriö Pentagonin ja tiedeyliopistojen yhteinen hanke tehokkaamman tiedonsiirron toteuttamiseksi instituutioiden välillä (Singer & Friedman 2014: 17). Mediahistorioitsija James Curranin (2012: 36–38) mukaan Pentagon halusi rakentaa teknologian, joka kestäisi Neuvostoliiton mahdollisen hyökkäyksen ja jonka avulla puolustusvoimien kalusto – autot, laivat, lentokoneet – pystyisivät kommunikoimaan keskenään. Tiedeyhteisölle taas oli tärkeää, että pääsy verkkoon ei olisi keskitetty vain tiettyyn lokaatioon. Yhteinen tavoite sai kumppanit työskentelemään rauhanomaisesti keskenään, kunnes Vietnamin sodan myötä kysymykset verkon turvallisuudesta pakottivat internetin jakamisen puolustusvoimien ja tiedeyhteisön kesken. Molempia verkkoja kehitettiin autonomisesti sotilasverkon jäädessä salaiseksi.

Tiedeyhteisön verkko avautui laajemmalle yleisölle. Varhaisen internetin käyttäjät olivat samalla sen luojia ja kehittäjiä, ja heitä kiehtoi uudessa teknologiassa ensisijaisesti se, että he pääsivät itse muokkaamaan sitä. Tällaisten muokattavien eli *generatiivisten*[4] teknologioiden ideana on, että käyttäjällä on vapaus innovoida, pelata ja ”harrastella” niillä. Internetin kehittäjistä muodostui yhteisö, joka halusi oma-aloitteisesti parantaa generatiivista verkkoa. Erimielisyydet ratkaistiin keskustelemalla. Internet kasvoi useita vuosia kehittäjäyhteisön hallinnan alla. (Zittrain 2008: 2, 27–28.) 1980-luvulla internetin suosio oli niin suuri, ettei yhteisö enää pystynyt hallinnoimaan verkkoa yksin. Internetin perustoiminnot yksityistettiin 1990-luvun alussa, minkä seurauksena uudet tahot pääsivät kehittämään ja innovoimaan internetiä. Tämä teki internetistä demokraattisemman, kun tavallinen kansalainen pääsi osalliseksi uudesta teknologiasta. (Singer & Friedman 2014: 18–20.) Kehityskulku koski kuitenkin vain Eurooppaa ja Pohjois-Amerikkaa: lännessä nautittiin vapaasta internetistä ja pidettiin sitä demokratian jatkeena, kun taas idässä verkkoon pääsyä rajoitettiin ja sisältöä sensuroitiin[5] (Curran 2012: 49–50).

Yksityistämisen myötä internetillä ei ollut yhtä ainoaa hallinnoijaa, vaan sen perusarkkitehtuuri oli jaettu usean eri toimijan kesken (Zittrain 2008: 27). Koska toimijoiden joukossa oli niin julkisia kuin yksityisiäkin organisaatioita, konsensuksen muodostamisesta internetin kehittämiseksi tuli käytännössä mahdotonta. Kuka tahansa pystyi lisäämään verkkoon omia sovelluksia tai ohjelmiaan, mikä osaltaan laukaisi sen, että joukkoon päätyi paljon myös huonoa koodia. Internet avautui viruksille, vakoilu- ja haittaohjelmille. Nykyisin niiden määrä on lukematon.

[4] Generatiivisen teknologian vastakohta on *steriili* (engl. *sterile*) teknologia. Tuolloin käyttäjällä ei ole vapaa muokkaamaan sitä, vaan teknologian valmistanut yritys pitää tiukasti itsellään sekä kehitys- että innovaatiotyön. (Zittrain 2008: 2.)

[5] Valtiot ovat perustelleet internetin rajoittamista muun muassa nationalismilla, uskonnolla tai taloudella. Koska valtio ylläpitää internetinfrastruktuuria, se voi sulkea koko verkon ”vetämällä töpselin seinästä”, kuten Kiinassa on käynyt. Lisäksi valtio voi rangaistusten uhalla luoda pelon ilmapiirin, minkä seurauksena kansalaiset rajoittavat itse omaa verkon käyttöään. Joissakin maissa rajoitettu internet toimii valtion omana propagandavälineenä. (Curran 2012: 49–50.)

2.4 Uudenlaiset uhat

Saksalainen elokuvaohjaaja Werner Herzog julkaisi kesällä 2016 dokumenttielokuvan *Lo and Behold, Reveries of a Connected World*, joka kuvaa melko dystooppisesti digitaalisen maailman tulevaisuutta. Elokuvassa haastateltu tutkija kommentoi, että ”ihmiskunta on jo nyt niin riippuvainen digitaalisesta teknologiasta että tarpeeksi voimakas aurinkotuuli johtaisi pörssien kaatumiseen, energiantuotannon katkeamiseen ja lukemattomien ihmisten kuolemaan.” (Tamminen 2016.)

Kybermaailman uhat ovat yhä enenevässä määrin osa tavallisen internetkäyttäjän arkea. Ongelmat näkyvät usein sosiaalisessa kanssakäymisessä. Yksilö ajautuu helposti sanaharkkaan sosiaalisessa mediassa, minkä seurauksena hänen tilinsä voivat joutua alttiiksi asiattomille kommenteille. Nuorten ja lasten ongelmana on kiusaamisen siirtyminen verkkoon, kuten WhatsApp-pikaviestisovellukseen, jossa valheelliset tai muutoin henkilökohtaiset asiat lähtevät leviämään lukijoiden keskuudessa. Tällöin puhutaan kyberhäirinnästä (engl. *cyber harassment*) (Salter & Bryden 2009: 99) tai kyberkiusaamisesta (engl. *cyber bullying*) (von Solms & van Niekerk 2013: 99). Pienelläkin kiusalla voi olla vakavia seurauksia niin häirinnän kohteelle kuin sen aiheuttajallekin, mutta olennaista on erottaa, onko kyseessä kohdistettu hyökkäys vai hyökkäys ”hyökkäyksen itsensä vuoksi” (Singer & Friedman 2014: 38). Jotkut kyberhyökkäykset tapahtuvat vain siksi, että niiden toteuttaja kykenee siihen ja että hän saisi huomiota teoillaan. Toiset taas ovat strategisesti kohdistettuja esimerkiksi yksilöä, yritystä, valtiota tai jotakin tiettyä toimintaa vastaan.

Yksilöä suurempien organisaatioiden tai valtioiden kohdalla kyberuhatkin kasvavat. Perinteisten virusten, haittaohjelmien ja identiteettivarkauksien lisäksi kybertoimintaympäristö on jatkuvasti alttiina muun muassa luonnonkatastrofeille ja kyberrikollisten hyökkäyksille. Valtioiden harjoittama kybervakoilu on yleistä ja useat maat suunnittelevat vastaiskuja niitä vastaan kohdistettuihin kyberhyökkäyksiin. Kybersotakin on mahdollinen. Uusi kasvava uhka on *esineiden internet* (engl. *Internet of Things,* IoT), joka tarkoittaa kodinkoneiden, laitteiden ja kulkuvälineiden yhdistämistä verkkoon (von Solms & van

Niekerk 2013: 100). Esineiden internetin kasvaessa kyberhyökkäys voi tapahtua esimerkiksi niin, että auton ajotietokoneeseen tunkeudutaan sen ollessa käytössä ja kuljettaja menettää ajoneuvonsa hallinnan.

Ulkoisten uhkien lisäksi kybertoimintaympäristön vaarana on ihminen. Ihmisen ymmärrys turvallisesta käytöksestä kybertoimintaympäristössä on auttamatta liian vähäistä, mistä seuraa väärien liitteiden klikkaaminen tai heikon salasanan luominen. (Singer & Friedman 2014: 249.) Kybertoimintaympäristöön kohdistuvat uhat ovatkin moninaisia ja uusia syntyy joka päivä. Rikollisuus, vakoilu ja sota muodostavat kyberuhkien tavallisimman kolmijaon (McGraw 2013: 110). Käsittelen seuraavaksi tarkemmin nuo kolme uhkaa, sillä ne ovat toistuvasti esillä niin tutkimuskirjallisuudessa kuin valtioiden kyberturvallisuusstrategioissakin.

2.4.1 Rikollisuus

Kyberrikollisuus on kybertoimintaympäristön uhkista yleisimpiä. Kuten valtaosa kybermaailman termeistä, myös kyberrikollisuus on ongelmallinen. Kyberrikokset ovat teknologisesti niin kehittyneitä, ettei lainsäädäntö pysy niiden perässä. On helppo sanoa, että kyberrikollisuuteen liittyy tietotekniikka. Toisaalta lähes jokainen rikollinen käyttää tietotekniikkaa jossakin vaiheessa tekoaan, mutta tämä ei automaattisesti tee rikoksesta kyberrikosta. Limnéll ym. (2014: 119–120) määrittävät kyberrikoksen olevan ”tapahtuma, jossa tietokoneet ja/tai –verkot ovat rikollisen toiminnan välineitä, kohteita tai rikoksen tekemisen paikka”. Kybermaailman asiantuntija Mark Johnsonin (2013) mukaan kyberrikoksessa käytetyn tietokoneen tulee lisäksi olla yhteydessä internetiin tai muuhun vastaavaan verkkoon.

Valtaosassa kyberrikoksista taustalla on taloudellinen motiivi. Kyberrikollisuuden globaaleja kustannuksia on lähes mahdotonta mitata, sillä seuraukset ovat usein aineettomia. Arvioiden mukaan summa liikkuu jossakin 300 miljardin ja triljoonan dollarin välillä. (Limnéll ym. 2014: 126–127.) Kyberrikollisuus ei ole suuren luokan bisnes vain rahallisesti, vaan myös skaalautuvuutensa vuoksi. Kyberrikoksia tehtailee joukko alan yrityksiä,

jotka myyvät verkossa valmiita viruksia tai palvelinestohyökkäyksiä, jollaisen kuka tahansa voi hankkia. Toimintaa rahoittavat paitsi yksityishenkilöt, myös tietyt valtiot, jotka kokevat kyberrikokset keinona puolustautua muiden valtioiden kyberhyökkäyksiä vastaan. (Singer & Friedman 2013: 90.) Ei ole siis mikään ihme, että kyberrikollisuutta on haastavaa saada kuriin, kun lakia valvova valtiovalta on siinä epäsuorasti mukana.

Taulukko 3. Yleisimmät kyberrikollisuuden metodit (Johnson 2013)

Metodi	**Kuvaus**
Hakkerointi (*Hacking*)	Murtautuminen tietokonejärjestelmiin ja tietoverkkoihin manuaalisesti hakkerin omia kykyjä hyödyntämällä.
Tunkeutuminen (*Code Injection*)	Koodin syöttäminen tietokoneohjelmaan niin, että sen alkuperäistä toimintoa häiritään.
Cross-site Scripting (XXS)	Verkkosivuston linkittäminen haittaohjelman sisältävän verkon yhteyteen, jolloin alkuperäinen sivusto saastuu.
Mies välissä -hyökkäys (*Man-in-the-middle*)	Tapahtuma, jossa hyökkääjä asettuu kahden osapuolen väliin tarkoituksenaan häiritä niiden välistä kommunikaatiota.
Vakoiluohjelma (*Spyware*)	Ohjelma, jolla kerätään henkilökohtaista tietoa, kuten sisäänkirjautumistietoja, tietokoneen käyttäjästä.
Troijalaiset, madot, virukset (*Trojans, worms, viruses*)	Haittaohjelmia, jotka välittävät tietoa tai häiritsevät ohjelman käyttöä tai jopa vahingoittavat tietoverkkojärjestelmää.
Palvelunestohyökkäys (*DoS attacks*)	Hyökkäyksen tarkoituksena on kaataa valikoidut palvelimet tai verkot ylikuormittamalla sivusto palvelinpyynnöillä.
Bottiverkko (*Botnet*)	Tuhansista tai jopa miljoonista tietokoneista koostuva verkko, joka valjastetaan rikollisen toiminnan käyttöön.

Kyberrikokset luokitellaan useaan eri kategoriaan: 1) tietoa ja tietojärjestelmiä vastaan tehdyt hyökkäykset, 2) tietokoneita hyödyntävät rikokset, 3) sisällöltään rikolliset toimet (esimerkiksi lapsipornografia, rasismi tai vihapuhe) ja 4) kopiosuojaa tai tuotemerkkiä loukkaavat rikokset (Limnéll ym. 2014: 125). Sen lisäksi, että kyberrikokset luokitellaan

rikoksen tavoitteen mukaan, on olemassa myös joukko konkreettisia keinoja, joilla tuo päämäärä saavutetaan. Metodeja on enemmänkin kuin taulukkoon 3 on koottu, eikä mikään metodi ilman muuta toimi vain sellaisenaan. Esimerkiksi bottiverkkoja käytetään usein palvelunestohyökkäyksen toteuttamiseksi, sillä valtava tietokoneverkko voidaan yhdellä komennolla saada lähettämään palvelinpyyntöä jollekin sivustolle. Rikollisille tämä on vaivattomampaa kuin pyytää yksittäisiä ihmisiä siirtymään sivustolle samanaikaisesti palvelun kaatamiseksi.

Tilastoja kyberhyökkäysten yleisyydestä on vaikea löytää – ainakaan tilastoja, jotka olisivat ajanmukaisia. Syynä tälle on, ettei kyberhyökkäyksistä välttämättä ilmoiteta, koska turvallisuuden pettämistä pidetään häpeällisenä, tai iskun kohde ei edes tiedä tapahtuneesta. On kuitenkin hyvä tunnistaa yleisimmät kyberrikollisuuden keinot, koska vain siten rikollisuutta voidaan jotenkin ehkäistä. Internetkäyttäjien pitää olla tietoisia, millaisiin sähköpostiliitteisiin tai pop–up-ikkunoihin he voivat luottaa. Tietoisuutta lisäämällä myös rikosten määrä voidaan saada laskuun.

2.4.2 Vakoilu

Tiedon kerääminen jotakin erityistä päämäärää varten ei ole uusi ilmiö. Tiedustelemalla hankittua tietoa on käytetty vallan välineenä läpi ihmiskunnan historian. Esimerkiksi sotatoimissa on välttämätöntä tuntea vastapuolen taktiikat ja joukkojen fyysinen sijoittuminen. Kun tiedustelua aletaan harjoittaa laittomin keinoin, siitä tulee vakoilua. Kyberaikakausi on mullistanut vakoilun mahdollisuudet. Ennen tieto oli fyysisessä muodossa ja vakoilijan oli fyysisesti mentävä sinne, missä tieto sijaitsi. Nykyään digitalisoituun tietoon voidaan päästä käsiksi toiselta puolelta maailmaa tietovarastojen ollessa yhteydessä verkkoon. (Limnéll ym. 2014: 129.)

Tieto- ja viestiliikenteen tutkija Herbert S. Lin (2010: 63) määrittelee kybervakoilun olevan “toimintoja ja operaatioita – mahdollisesti pitkälle aikavälille sijoitettuna –, joiden avulla hankitaan luottamukselliseksi tarkoitettua tietoa ja joiden on tarkoitus säilyä tai levitä vastapuolen tietokoneissa ja tietoverkoissa”. Linin mukaan kybervakoilu on *ei-tu-*

hoava kyberuhka, kun taas kyberhyökkäysten tarkoitusperät ovat *tuhoavia*. Vakoilun tarkoituksena on hankkia tietoa, mutta kyberisku tavoittelee jonkin tietojärjestelmän, ohjelman tai muun kybertuhoamista. Lisäksi vakoilulle olennaista on se, että sillä on yleensä jokin taloudellinen, poliittinen tai sotilaallinen päämäärä. Sen vuoksi todennäköisimmät kybervakoilun toimijat ja kohteet ovat yrityksiä ja valtioita (Limnéll ym. 2014: 129–130).

Kiinan ja Yhdysvaltojen toisiinsa kohdistuvia kybervakoilusyytöksiä ei voida ohittaa puhuttaessa kybervakoilusta. Moni tutkija mainitsee nämä maat maailman suurimmiksi kybervakoilun harjoittajiksi (ks. esim. Limnéll ym. 2014: 130; Pelican 2012; Singer & Friedman 2013: 92). Vuonna 2009 tutkijat löysivät internetissä levinneen verkoston, joka yhdisti toisiinsa 1 295 palvelinta 103:ssa eri maassa. *GhostNet*iksi nimetty vakoiluverkosto oli levinnyt muun muassa suurlähetystöihin ja ulkoministeriöihin sähköpostin liitetiedoston välityksellä. Verkoston alkuperä paikannettiin Kiinaan. (Singer & Friedman 2013: 93.) Kenties maailman tunnetuin tiedustelurikos on Edward Snowdenin tapaus, jossa Snowden ei itse ollut vakoilijan asemassa, vaan sen sijaan hän paljasti Yhdysvaltojen pitkään jatkuneen systemaattisen kybervakoilun tuloksia. Kyseinen tapahtuma osoittaa, että fyysinen vakoilu ei ole katoamassa minnekään – siitä on tullut vain entistä moniulotteisempaa (Limnéll ym. 2014: 129).

2.4.3 Sota

Kybersodasta puhutaan paljon poliittisten päättäjien keskuudessa. Vaikka vain pienen osan kyberhyökkäyksistä katsotaan edustavan sotatoimia, kybersodalle annetaan puolustusstrategioita mietittäessä suuri merkitys. Limnéllin ym. (2014: 138–139) mukaan kybersodasta puhutaan liian heiveröisin perustein, mikä osaltaan johtuu siitä, ettei käsitettä ole määritelty riittävän selkeästi. Kybersotaa ”hypetetään” eli korostetaan liiallisuuksiin asti. Tietotekniikan tutkija Gary McGraw (2013: 111) on ylikorostamisesta samaa mieltä. Hän kuvailee sotaa vielä melko yksinkertaisesti: ”väkivaltainen konflikti, joka oikeutetaan poliittisin, taloudellisin tai ideologisin perusteluin”. Mutta kun ’sodan’ eteen lisätään liite ’kyber’, terminologia mutkistuu.

Singer & Friedmanin (2014: 121) mukaan hyökkäyksen määrittely kybersodaksi vaatii todellisen fyysisen seurauksen: kuolemantapauksia, väkivaltaa tai merkittävää fyysistä tuhoa. Toisin sanoen vaikka isku tapahtuisikin kybermaailmassa tai sen kautta, sen seurausten tulee olla fyysisiä. McGraw (2013: 112) puhuu kineettisestä vaikutuksesta tarkoittaessaan samaa asiaa. Kybersodaksi ei siis luokitella mitä tahansa kybermaailmassa tapahtunutta hyökkäystä. Valtiot esimerkiksi vakoilevat toisiaan jatkuvasti ja jäävät siitä kiinni, mutta yksikään valtio ei ole aloittanut sotatoimia varastettujen tiedostojen vuoksi. Tiedostot ovat voineet sisältää kriittistäkin informaatiota, mutta vasta kun tietoa hyödynnetään vieraan valtion sotaväen tappamiseen, voidaan puhua kybersodasta.

Kybermaailma voi toimia paikkana, jossa sota saa alkunsa tai se voi olla keino vaikuttaa sodankäyntiin. Moni länsimainen valtio on ottanut kyberulottuvuuden osaksi perinteisiä sodankäynnin muotoja: maa, meri, ilma, avaruus – ja uutuutena kyber. Tämä tulee muuttamaan ja on jo muuttanut valtioiden voimasuhteita. Pienet valtiot, joilla on osaamista ja resursseja panostaa kybertoimintaan, voivat nousta suurvaltojen rinnalle ja jopa ohi. Hyvänä esimerkkinä tällaisesta valtiosta on Viro, joka on yksi maailman kehittyneimmistä valtioista kybermaailmassa. (Limnéll ym. 2014: 142.)

Kybersodan tunnetuimpia esimerkkejä ovat Venäjän hyökkäys Georgiaan vuonna 2008 ja Stuxnet-vakoiluohjelma, jonka Yhdysvallat syötti Iranin tietojärjestelmään. Vuoden 2008 tapahtumat perustuvat Georgian sisäisiin konflikteihin armeijan ja separatistien välillä. Konfliktissa separatistien puolella ollut Venäjä reagoi lähettämällä omat joukkonsa Georgian rajojen yli päivä sen jälkeen, kun maan tietoverkot oli ensin kaadettu palvelinestohyökkäyksellä. Tutkijat eivät ole pystyneet osoittamaan, että Venäjä olisi ollut iskun takana, mutta median uutisoinnin seurauksena kyberhyökkäys on pantu Venäjän nimiin. (Tikk, Kaska, Rünnimeri, Kert, Talihärm & Vihul 2008: 4, 12.) Georgian ja Venäjän konfliktissa voidaan puhua kybersodasta, sillä ensin maan tietoverkot kaadettiin, minkä jälkeen fyysiset asevoimat marssivat laittomasti toisen valtion alueelle sotatoimiin. Lähtökohta on ollut kybermaailmassa, minkä lisäksi fyysisen seurauksen ehto on toteutunut.

Stuxnet ei varsinaisesti aiheuttanut sotatoimia, mutta on erinomainen osoitus kyberaseesta ja siitä, kuinka sitä voitaisiin hyödyntää kybersodassa. Stuxnet on Yhdysvaltojen

ja Israelin yhteistyönä toteutettu haittaohjelma, joka aiheutti hankaluuksia Iranin ydinaseohjelmalle. Haittaohjelma sai ydinreaktorit toimintakyvyttömiksi, mistä seurasi säteilyuhka ja pelko ydinvoimalan räjähtämisestä. Stuxnet aiheutti sen, etteivät ohjauslaitteet ymmärtäneet, milloin reaktorit olivat ylikuumentumassa. Vaarallisen kyberaseen Stuxnetin kaltaisista haittaohjelmista tekee se, että niillä pystytään syöttämään virheellistä dataa infrastruktuurin kriittisten osa-alueiden lamaannuttamiseksi ja että ne on verrattain helppo toteuttaa teknisesti. (McGraw 2013: 112, 115.) Tämän lisäksi kyberaseiden käyttö on valtioille edullista. Stuxnetin hinnaksi arvioidaan 10 miljoonaa dollaria, kun taas hävittäjälentokone maksaa valtiolle jopa kymmenen kertaa enemmän. (Limnéll ym. 2014: 140.)

Tulevaisuudessa jokainen sota tulee sisältämään jonkinlaisen kyberkomponentin. Tietotekniikan avulla annetaan jo nyt käskyjä toisella puolella maailmaa sijaitseville joukoille tai ohjataan miehittämättömiä hävittäjälennokkeja. Fyysinen toimintamuoto tulee säilymään sodankäynnissä myös tulevaisuudessa – aivan kuten kybervakoilussakin. Kyberaspekti antaa niille vain uusia muotoja ja vaikuttamiskeinoja. (Limnéll ym. 2014: 141.)

2.5 Valtio kybermaailmassa

Kuten edellisessä luvussa esitin, kyberuhkia yhdistää niiden monimuotoisuus. Kybertoimintaympäristöön vaikuttavat sekä luonnonkatastrofit, teknologian kehitys että ihminen itse. Uhkilla on omat erityispiirteensä, mutta samalla ne myös linkittyvät toisiinsa. Kybervakoilu on rikollista toimintaa ja erilaisten laitteiden häirintä rikollisin menetelmin voidaan katsoa sotatoimiksi. Toisaalta kybersodassa pyritään hankkimaan tietoa vastapuolen toimista erilaisin vakoiluohjelmin. Vakoilu eroaa rikollisuudesta ja sodasta siinä, että se ei itsessään pyri tuhoamaan, vaan hankkimaan tietoa. Vakoilun keinoin hankittua tietoa voidaan tosin käyttää tuhoamisen välineenä. Uhkiin vastaaminen jää käytännössä valtion tehtäväksi, sillä sen vastuulla on rangaista rikollista toimintaa. Tähän valtiot ovat kehittäneet avukseen kyberturvallisuusstrategiat.

Valtio on olennainen osa kybertoimintaympäristöä kahdesta syystä: sen täytyy suojata 1) oma digitaalinen toimintansa ja 2) kansalaisten tarvitsemat elämisen mahdollistavat palvelut (Singer & Friedman 2014: 197). Internetin yksityistyttyä valtio on yrittänyt pysytellä mukana teknologisessa kehityksessä, mikä on johtanut siihen, että valtaosa valtionhallinnon asiakirjoista, viestinnästä ja päätöksenteosta tapahtuu verkossa. Lisäksi valtion rajojen sisäpuolella on vesi- ja sähkölaitoksia, liikennettä ja maanviljelyä, jotka kaikki ovat jollakin tavalla yhteydessä verkkoon. Valtio on tahtomattaankin osa kybertoimintaympäristöä, eikä sen vuoksi voi toimia siellä ilman strategista suunnitelmaa.

Kybertoimintaympäristössä vaikuttaminen ei ole valtiolle helppoa. Ensinnäkin valtio on täynnä byrokratiaa ja siksi hidas (Singer & Friedman 2014: 198). Valtio ei pysty vastaamaan kybermaailman nopeuteen, jossa hyökkäykset tapahtuvat ilman ennakkovaroitusta. Fyysisessä maailmassa käytössä olevat keinot, joilla toimintoja jäljitetään, eivät välttämättä toimi kybermaailmassa. (Choucri, Madnick & Ferwerda 2014: 98.) Tämän vuoksi isojen strategisten päätösten tekeminen vie aikaa, ja lopulta kun päätös valmistuu, sen sisältö on ehtinyt vanhentua.

Toisekseen valtio joutuu miettimään puolustuspolitiikkansa uudelleen. Perinteiseen puolustukseen verrattuna toimiva kyberturvallisuus vaatii yhteistyötä sekä kansallisella, kahdenvälisellä että globaalilla tasolla (Choucri ym. 2014: 104). Fyysisessä maailmassa on paljon yksinkertaisempaa osoittaa maiden väliset rajat ja niitä puolustavat sotavoimat. Valtiot pystyvät esimerkiksi asettamaan toisensa kauppasaartoon tai määrätä muita pakotteita, jos toinen maa vahingoittaa maiden välistä suvereniteettia. Kybermaailmassa vastustajaa ei kuitenkaan aina tunneta tai hyökkäyksen taustalla on jokin muu toimija kuin valtio. Kyberrikollisuus ei pysyttele maiden rajojen sisäpuolella, mikä tekee siitä valtioiden yhteisen uhan. Siksi rangaistusten asettaminen on hankalampaa.

Kansainvälinen yhteistyö ei myöskään jakaudu tasa-arvoisesti maiden kesken. Viestinnän tutkija Ellada Gamreklidzen (2014: 203–204, 214) mukaan *digitaalinen kahtiajako* vaikuttaa myös kyberturvallisuusyhteistyöhön. Digitaalisella kahtiajaolla tarkoitetaan perinteisesti ihmisten, yritysten ja maantieteellisten alueiden välistä kuilua, joka erottaa osa-

puolet toisistaan mahdollisuuksissa päästä tai kyetä käyttämään tieto- ja viestintäteknologiaa. Valtiot, joilla ei ole kattavaa tietoverkkoinfrastruktuuria, ei ole myöskään keinoja puolustautua kyberhyökkäyksiä vastaan. Näiltä valtioilta puuttuvat kyberturvallisuusstrategiat, hallinnolliset elimet tai asiantuntevat ihmiset, jotka voisivat edistää kyberturvallisuutta. Rajallinen tietoverkkoinfrastruktuuri ei kuitenkaan poista sitä tosiasiaa, että näissä maissa kyberhyökkäykset kohdistuvat valtion kriittisimpään tietoliikenteeseen, kuten pankki- ja SCADA-viestintään[6].

Oletettavaa on, että yhteistyö vasta kehittyvien ja jo kehittyneiden kybervaltioiden välillä on melko vähäistä, sillä kehittyvillä valtioilla ei ole juurikaan annettavaa vastapuolelle. Informaatio- ja kommunikaatiotieteilijät Regner Sabillon ja Victor Cavaller sekä oikeustieteilijä Jeimy Cano (2016: 79) ovat tulleet samaan johtopäätökseen. Heidän mukaansa kansainvälisestä yhteistyöstä puhutaan kyllä paljon, mutta kybermaailmasta puuttuu kokonaan kansainvälinen standardi, jonka puitteissa kyberturvallisuus toteutettaisiin. Lisäksi maakohtaiset lainsäädännöt poikkeavat toisistaan, mutta sen sijaan, että ne yhtenäistettäisiin, Sabillon ym. ehdottavat, että kybertoimintaympäristölle luotaisiin oma kansainvälinen lakinsa. Globaalin standardin ja lainsäädännön luominen vaatii Sabillonin ym. mukaan kehittyneiden maiden panosta, jotta myös kehittyvät maat pääsisivät kiinni kyberaikakauteen.

Kolmas ja viimeinen valtion haaste kybertoimintaympäristön vaikuttajana on kysymys valtion oikeudesta määrätä yksityisen sektorin toiminnasta. Kybertoimintaympäristön perusarkkitehtuuria ylläpitää ei-hallinnolliset elimet (Choucri ym. 2014: 98), ei valtiot. Internet Engineering Task Force (IETF) on alkujaan vapaaehtoisista koostunut insinööri- ja tiedeyhteisö, joka kehittää internet-standardia ja -protokollia. IETF:n toiminnalle teknistä tukea antaa Internet Engineering Steering Group (IESG), joka taas keskustelee Internet Architecture Board (IAB) -organisaation kanssa. Nämä vastaavat toiminnastaan Internet Societylle (ISOC), joka on perustettu valvomaan avoimen lähdekoodin laillisia oikeuksia.

[6] SCADA (Supervisory control and data acquisition) -sovellus on teollisuuskäyttöön tarkoitettu kontrollijärjestelmä, jonka avulla yritys tai organisaatio voi valvoa, hallinnoida ja kerätä tietoa automatisoidusta laitteistostaan. SCADA-sovelluksia käytetään muun muassa sähkönjakelussa, ruokateollisuudessa ja liikenteenohjauksessa. (Inductive Automation 2017.)

Lisäksi internetissä on muitakin sen toiminnan kannalta oleellisia osia, kuten nimipalvelu, jota pyörittää Internet Corporation for Assigned Names and Numbers (ICANN). ICANN jakaa ja hallinnoi verkkosivujen IP-osoitteita. (Singer & Friedman 2014: 27–29.)

Edellä esitellyt organisaatiot ovat olemassa pelkästään siksi, että internet toimisi. Turvallisuudesta vastaamaan on perustettu CERT-toiminta (Compurter Emergency Response Teams). CERT-toiminnot on kehitetty kansainvälisessä yhteistyössä, mutta ne eivät kuitenkaan ole valtioiden hallinnan alaisia. CERTien tehtävä on ehkäistä kyberhyökkäyksiä, suositella turvallisimpia teknologioita ja varmistaa verkon jatkuvuus. Sen lisäksi, että on olemassa kansainvälinen niin sanottu globaali CERT, jokaisella maalla on omansa (esimerkiksi Suomella CERT-FI). CERTit ovat jakautuneet alueellisesti, mutta myös sillä perusteella, ketä ne on perustettu suojelemaan (mm. yliopisto, yksityinen sektori, pankkiviestintä) ja minkälaiselta uhalta (mm. virukset, vakoiluohjelmat, madot). (Choucri ym. 2014: 104–105.)

Tutkijat pohtivatkin sitä, onko valtiolla oikeus määrätä kybertoimintaympäristöstä, jos ne eivät ole sen varsinaisia ylläpitäjiä. Muun muassa turvallisuus- ja tietotekniikan tutkija Julian Richards (2014: 61) kyseenalaistaa valtion oikeuden säätää yrityksiä velvoittavia lakeja. Limnéllin ym. (2014: 46) mukaan valtio saa ohjeistaa yksityistä sektoria, mutta kybertoimintaympäristön turvaaminen ilman läheistä yhteistyötä yritysten kanssa ei ole mahdollista. Jos valtio ei hallinnoi kybertoimintaympäristöä, toinen vaihtoehto on jättää vastuu yrityksille. Loppujen lopuksi valtaosa valtioiden kybermääräyksistä ja -säädöksistä kuitenkin koskee yksityistä sektoria.

Vastaus kybertoimintaympäristön hallinnoijasta ei ole kuitenkaan niin yksiselitteinen. Richardsin (2014: 68) mukaan laajamittaisesta kyberrikollisuudesta rankaiseminen kuuluu kansainväliselle tuomioistuimelle. Silti valtiot pyrkivät kyberturvallisuusstrategioidensa mukaan kitkemään rikollisuuden itse. Ongelmana on, että strategiat on pääpiirteissään kehitetty kybersotia tai -terrorismia vastaan, ei niinkään rikollisuutta. Tämä liittyy aikaisemmin todettuun kybersodan ”hypettämiseen”, jota valtiot tapaavat tehdä. Lisäksi valtiot voivat itse olla kyberhyökkäysten tai muun kyberrikollisuuden takana, joten kybertoimintaympäristöstä päättäminen ei voi olla pelkästään yksityisen sektorin tehtävä.

Haasteiden ohella kybertoimintaympäristö tarjoaa myös mahdollisuuksia. Se, kuinka valtiot onnistuvat hyödyntämään muun muassa *big dataa*[7], pilvilaskentaa (engl. *cloud computing*) ja esineiden internetiä, on merkittävä kansallinen kilpailuvaltti tulevaisuuden kybermaailmassa (Min, Chai & Han 2015: 13). Kybermaailma on paikka, jossa valtio pystyy kohtaamaan kansalaiset ja muodostamaan selkeän kuvan heidän tarpeistansa ja oikeuksistansa. Palveluiden personointi tekee asioimisesta viiveettömämpää. (Sabillon, Cavaller & Cano 2016: 67.) On kuitenkin valtiosta itsestään kiinni, kuinka hyvin se tuntee omat resurssinsa ja onnistuu sisällyttämään ne kyberturvallisuusstrategiaansa. Ennen kuin pohdin, miten valtiot strategiansa tuottavat, tarkastelen sitä, mikä strategia on ja millaisen muodon se tekstilajina ottaa.

2.6 Strategia genrenä

Aikoinaan strategialla tarkoitettiin sodankäynnissä sotajoukkojen asemia, mutta sittemmin 1900-luvun alun Yhdysvalloissa modernien yritysten ja bisnesmallien kehittyessä strategioita alettiin tehdä yritysjohdolle selkiyttämään liiketoimintaa (Pälli, Vaara & Sorsa 2009: 304). Strategiat ovat siis ikään kuin ”oppaita tulevaan” (emt. 314) eli pitkäntähtäimen suunnitelmia ja päätöksentekovälineitä, joihin yrityksen toiminta pohjaa. Tekstinä strategialla – kuten kaikilla teksteillä – on kielellisiä erityispiirteitä, jotka tekevät siitä strategian.

Kun kategorisoidaan tekstejä erilaisiin tyyppeihin, puhutaan *genreistä*. Norman Faircloughin (1992: 126) mukaan genret ovat kokoelma suhteellisen muuttumattomia tekstuaalisia ja sosiaalisen vuorovaikutuksen käytänteitä, joita ovat esimerkiksi uutinen, runo ja romaani, mutta myös työhaastattelu, myyjän ja asiakkaan välinen ostotapahtuma tai tuttavien nopea rupattelu. Tekstityyppien kategorisoinnin lisäksi genrejä voidaan määri-

[7] *Big datalle* ei ole vakiintunut yhtenäistä määritelmää, mutta yleensä sillä viitataan erittäin suureen määrään strukturoimatonta dataa, jota tulee jatkuvasti lisää ja johon datan analysoijien on jatkuvasti reagoitava (Bigdata.fi 2017). *Big data* on muuttanut yritysten perinteistä tietojenhallintaa siten, että esimerkiksi pelkkien asiakasrekistereiden pitämisen sijasta *big datan* hallinnasta on tullut oma liiketoiminta-alueensa.

tellä tuottamisen, jakamisen ja kuluttamisen näkökulmasta. Toisin sanoen tiettyjen genrejen tekstit syntyvät erilaisissa olosuhteissa kuin toiset ja ne myös saatetaan yleisön tietoon eri kanavia pitkin. Myös lukemisen ja tulkitsemisen tavat genreissä eroavat toisistaan.

Strategiateksti on oma genrensä. Huolimatta siitä, onko strategia tehty yksityisen tai julkisen sektorin organisaatiolle, sillä on erityisiä sisällöllisiä samankaltaisuuksia muiden strategiagenreen kuuluvien tekstien kanssa. Strategiassa määritellään organisaation kompetenssit eli kyvyt sekä se, kuinka ne valjastetaan yrityksen käyttöön. Ihanteellinen strategiateksti noudattaa organisaation virallista linjaa. Lisäksi strategiassa osoitetaan organisaation sisäiset vastuut ja ajanjakso, jolloin strategiset toimenpiteet toteutetaan. (Paroutis, Heracleous & Anfwin 2016: 7.)

Strategiat syntyvät kahdella tapaa: joko autonomisesti organisaatiohierarkiassa alhaalta ylös tai strukturoidusti organisaatiojohdosta ylhäältä alaspäin. Autonomisen strategisen käytöksen seurauksena strategia syntyy ikään kuin itsestään useiden työntekijöiden kehittäessä toimintatapoja ja jopa ”kilpaillessa” keskenään parhaimmista tavoista optimoida resurssien käyttö. Strukturoidussa kontekstissa strategia näyttäytyy muodollisuuksien, kuten informaationjaon, arviointien ja palkkiojärjestelmien, välityksellä. Organisaatiojohto on strategian toimeenpanija. (Paroutis ym. 2016: 2). Tämä antaa myös vastaanottajalle aineksia siihen, kuinka strategiatekstiä tulisi tulkita. Strategia, jonka tekemisessä työntekijä tai kansalainen on ollut mukana, on todennäköisesti helpompi hyväksyä, kun taas ylhäältä annettu strategia voi aiheuttaa enemmän kielteistä suhtautumista.

Tekstin tasolla strategialle on tyypillistä, että se legitimoi (ks. luku 4.1) toisia ajattelutapoja ja sulkee samalla toiset ulkopuolelle. Pyrkiessään tuottamaan hyväksyvää suhtautumista strategia herättää myös vastarintaa ja levittää poliittisia tai ideologisia vaikutteita. (Vaara, Sorsa & Pälli 2010: 686.) Strategioiden päämäärät ovat usein tarkoituksella suostuttelevia (Williams 2009: 100). Tämä johtuu siitä, että niiden tavoitteena on rohkaista työntekijöitä ja muita yritysten jaostoja identifioitumaan organisaation päämääriin. Toisin sanoen strategiateksteillä on tietoisesti rakennettuja tavoitteita, minkä vuoksi myös niiden kielessä on käytetty paljon vakuuttavia ja suostuttelevia keinoja.

2.7 Kansallinen kyberturvallisuusstrategia

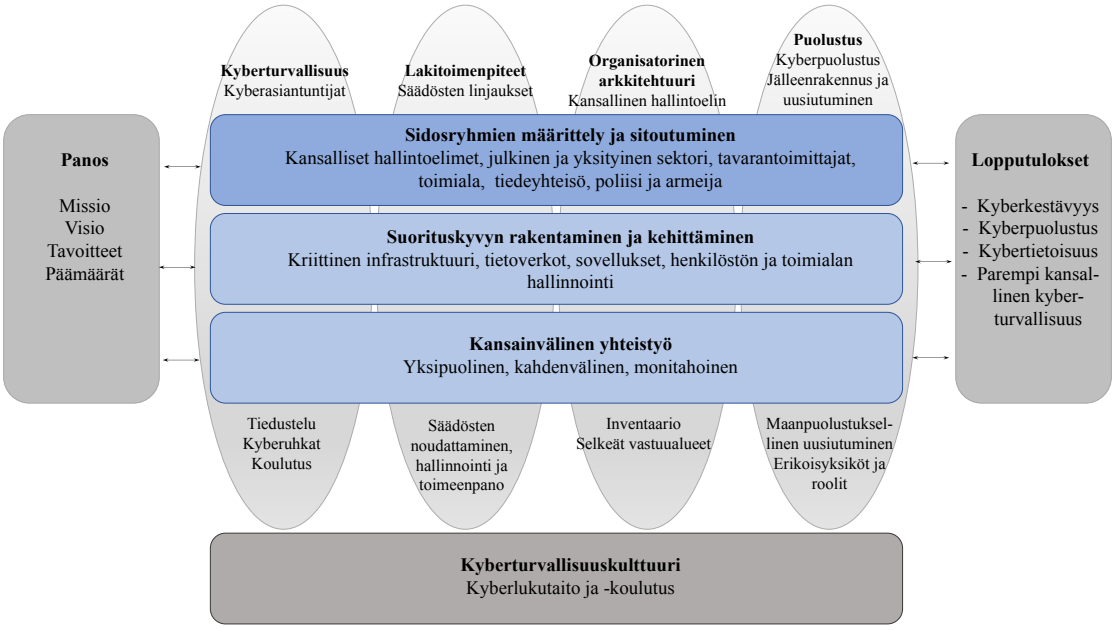
Valtioiden kiinnostus kyberturvallisuutta kohtaan näkyy muun muassa siten, että yli 80 valtiota on julkaissut tai on julkaisemassa kyberturvallisuusstrategian vuoden 2010 jälkeen. Kyberaikakausi on mennyt eteenpäin niin hurjaa vauhtia, että ensimmäisinä strategiansa julkaisseet ovat jo tekemässä niistä päivitettyjä versioita.

Kyberturvallisuusstrategia on valtion mahdollistamis- ja turvallisuussuunnitelma kybertoimintaympäristöä varten. Strategia koostuu sekä abstraktista visiosta että käytännön teknisestä toteutuksesta. Strategian tarkoitus on kartoittaa kybertoimintaympäristön tarjoamia pitkän aikavälin mahdollisuuksia riskit huomioiden. Mitä suuremmat visiot ovat, eli toisin sanoen mitä enemmän valtio näkee kybertoimintaympäristössä mahdollisuuksia, sitä laajemmaksi kasvavat myös riskit. (Limnéll ym. 2014: 157–158.) Strateginen toimintamalli on valtion kyberturvallisuuden elinehto (Gamreklidze 2014: 204).

Valtioiden kyberturvallisuusstrategiat on tehty melko pitkälti saman mallin mukaan. Yleisimmät kyberturvallisuusstrategioissa esitetyt toimenpiteet ovat 1) poikkihallinnollinen yhteistyö, jossa tieto kulkee hallintoyksiköstä toiseen ja kaikki ymmärtävät kokonaisturvallisuuden merkityksen, 2) kyberiskujen ennaltaehkäisy ja proaktiivinen toiminta, 3) kansainvälinen yhteistyö, 4) lainsäädännön saattaminen vastaamaan teknologista kehitystä, 5) tutkimus- ja kehittämistyö, 6) ensisijaisten kohteiden (kuten infrastruktuuri) turvaaminen sekä 7) kyberturvallisuuskeskuksen ja vastaavan poliittisen elimen perustaminen. (Limnéll 2014: 84).

Sabillon ym. (2016: 79) ovat luoneet kansallisen kyberstrategiamallin, joka perustuu Kansainvälisen televiestintäliiton (International Telecommunication Union), Naton, OECD:n ja EU:n suosituksiin. Sabillonin ym. mukaan paras mahdollinen kyberstrategia saavutetaan, kun valtio on tietoinen resursseistaan strategian toteuttamiseksi, onnistuu toteuttamaan suunnitelmansa käytännön tasolla ja lisäksi pyrkii kehittämään ja parantamaan toimintaansa entisestään. Kuviossa 3 *panos* vastaa tietoisuutta resursseista, keskimäiset pilarit käytännön toteutusta ja *lopputulokset* toiminnan kehittämistä ja paranta-

mista. Mallin mukaan strategian tulee nojata *kyberkulttuuriin*, joka on kaiken kybertoiminnan pohja. Kyberkulttuuri istutetaan kansalaisiin koulutuksen avulla. Se, kuinka paljon valtio panostaa strategiaan, määrittää *sidosryhmät*, *suorituskyvyn* ja *kansainvälisen yhteistyön*. Näiden tulisi olla prioriteettina valtion strategisessa kybertoiminnassa. Lisäksi onnistuneen strategian kannalta on olennaista, kuinka valtio tekee yhteistyötä *kyberyhteisön* kanssa, onnistuu kehittämään *lainsäädäntöään*, järjestää *hallinnolliset ja organisatoriset elimet* sekä *kyberpuolustuksen*. Lopputulemana on kyberturvallisuusstrategia, joka mahdollistaa nopean *palautumisen* kyberhyökkäyksistä, vahvan *kyberpuolustuksen* ja *tietoisuuden* sekä *kehittää* valtion kybertoimintaa entisestään.



Kuvio 3. Kansallinen kyberstrategia -malli (National Cyber Security Strategy Model NCCSM) (Sabillon ym. 2016: 79) [kääntänyt S.J.]

Sabillonin ym. mallista löytyvät melko pitkälle samat asiat, jotka Limnéll ym. ovat löytäneet jo olemassa olevista strategioista. Tämä ei ole mikään ihme, sillä kybermaailma on globaali ilmiö, jossa mahdollisuudet ja uhat ovat kaikille samat. Valtion sen hetkinen poliittinen, sotilaallinen tai vaikkapa maantieteellinen asema vaikuttaa siihen, millaisia

mahdollisuuksia se pystyy toteuttamaan tai millaisiin uhkiin se pystyy vastaamaan. Kyberturvallisuusstrategia luodaan sen hetkisen aseman pohjalta. Jos valtiolla ei ole resursseja, myös mahdollisuudet pysyvät pienimuotoisina. Sen sijaan johtavat kybervaltiot, kuten Yhdysvallat tai Iso-Britannia, pystyvät visioimaan strategioissaan laajempia kokonaisuuksia.

Valtiot myös ottavat kyberturvallisuusstrategioita luodessaan mallia toisiltaan. Kuten aikaisemmin olen todennut, kybermaailma on vielä uusi ja varsin tuntematon asia. Vaikka valtiot olisivat kiinnostuneita siitä, se ei vielä tarkoita, että ne todella tuntisivat sitä. Esimerkiksi maa, joka ei ole koskaan joutunut kyberhyökkäyksen kohteeksi, ei osaa arvioida omaa toimintakykyään iskun sattuessa yhtä hyvin kuin maa, joka on joutunut sellaista vastaan puolustautumaan. Samasta syystä strategioissa on toistuvasti epäjohdonmukaisuuksia tietoturvan ja kyberturvallisuuden käsitteiden käytössä (von Solms & van Niekerk 2013: 97). Niiden eroa ei osata selittää, koska kybermaailmaa ei ymmärretä. Strategioihin otetaan siis mukaan asioita, jotka toistuvat muilla, vaikkei niistä itsellä olisikaan kokemusta. Koska strategiat ovat vielä yleisesti kaikkien luettavissa, ne lainaavat ajatuksia ja ideoita toisiltaan.

Miksi strategiat sitten ovat yleisesti nähtävillä? Luultavampaa olisi, että valtiot pitäisivät strategiansa salaisina, koska ne pitävät sisällään paljon puolustuspoliittisia suunnitelmia. Richards (2014: 68) toteaa kuitenkin, että paras keino puolustautua kyberuhkia vastaan on informaation vapaa liikkuvuus. Kybermaailmassa onkin syytä hyväksyä se, että turvallisuus tulee väistämättä pettämään jossakin vaiheessa (Limnéll 2014: 159). Lisäksi se, että on valmis kertomaan kyberturvallisuussuunnitelmista iskuja ja hyökkäyksiä vastaan, luo pelotteen hyökkääjille. Tämän vuoksi strategioihin on usein liitetty kommentteja fyysisistä voimakeinoista esimerkiksi kybersodan yhteyteen. (Richards 2014: 63.) Pällin ym. (2009: 309) mukaan strategiatekstit on kirjoitettu niitä työstäneiden ja työssään tarvitsevien lisäksi laajalle sidosryhmäjoukolle, johon lukeutuvat muun muassa asukkaat, kansalaiset, turistit sekä muut samanarvoiset toimijat eli muut valtiot ja media. Strategiateksti on siis paitsi valtion sisäinen työväline, myös keino esitellä toimintaa muille.

Edellä esitellyt seikat ovat olennainen osa tässä tutkimuksessa analysoitavien kyberturvallisuusstrategioiden vakuuttamisen keinoja. Voimakeinojen ja muun informaation sijoittaminen strategiaan luo tietynlaista diskursiivista kybermaailmaa, jota ymmärtääkseen on syvennyttävä strategioihin tarkemmin. Tähän käytän apuna diskurssianalyysia. Esittelen kyseisen metodin seuraavaksi.

3 DISKURSSIT VAKUUTTAMISEN JA SUOSTUTTELUN VÄLINEENÄ

Menetelmänä diskurssianalyysi ei ole yksiselitteinen tai kaiken kattava, vaan yksi kvalitatiivisen tutkimuksen vaihtoehdoista. Diskurssianalyysissa kiinnostuksen kohteena on prosessi (Jokinen 1999/2006: 40), jossa kieli nähdään osana sosiaalista toimintaa. Tarkasteluun otetaan vallalla tai marginaalissa olevia merkityksiä ja pohditaan, mitä ne tarkoittavat ja miksi. Kieli toimii eri tavoin eri tilanteissa käyttäjiensä muokatessa sitä, mutta samalla kieli itsekin muokkaa käyttäjiään. (Pietikäinen & Mäntynen 2009: 13–14.) Arja Jokisen, Kirsi Juhilan ja Eero Suonisen (2016: 17) mukaan diskurssianalyysi on ”kielenkäytön ja muun merkitysvälitteisen toiminnan tutkimu[sta], jossa analysoidaan yksityiskohtaisesti sitä, miten sosiaalista todellisuutta tuotetaan erilaisissa sosiaalisissa käytännöissä”.

Tämän kappaleen tarkoituksena on perehtyä syvällisemmin diskurssianalyysiin – erityisesti kriittiseen sellaiseen – ja rajata siitä tähän tutkimukseen sopivat työkalut. Aluksi selitän tarkemmin, mikä diskurssi on ja mitä sillä tarkoitetaan kriittisessä diskurssianalyysissa. Sen pohjalta määrittelen tutkimukseni tärkeimmät käsitteet ja esittelen retoriikasta lainaamiani keinoja, joita kriittisessä diskurssianalyysissa voidaan käyttää diskurssien paikantamiseen.

3.1 Kriittinen diskurssianalyysi

Yhteiskuntatieteissä diskurssianalyysiteoriat nojaavat usein ranskalaisfilosofi Michel Foucault’n ajatuksiin. Tulkitessaan Foucault’ta kulttuurintutkija Stuart Hall (2001: 72–73) sanoo, että foucault’laisittain diskurssit ovat tapa puhua ja järjestää tietoa tai ymmärrystä (engl. *knowledge*) jostakin asiasta. Diskurssi tarkoittaa kielestä muodostuvaa merkityssysteemiä, eli kieli tarjoaa mahdollisuudet, joilla asioista voidaan puhua käyttämällä tiettyjä merkityksiä. Hall painottaa, että diskurssi on kielellisen ilmaisun ohella toimintaa, sillä merkitykset muodostuvat myös ihmisen teoissa. Kun merkityksen nähdään muodostuvan sosiaalisessa toiminnassa, puhutaan sosiaalisesta konstruktionismista. Diskurssilla pyritään häivyttämään kielen ja toiminnan välistä eroa. Kun tekstiä ja puhetta tuotetaan

vuorovaikutteisesti, syntyy merkityksiä. Tekstin ja puheen vuorovaikutuksesta muodostuu diskurssi. Esimerkiksi erityinen tervehdys ja käden liike ovat merkityksellisiä tietyssä diskurssissa vain, kun ne suoritetaan samanaikaisesti.

Kriittiselle diskurssianalyysille on tyypillistä, että diskursseja voidaan lähestyä kahdesta eri perinteestä. Yleisesti puhuttaessa diskurssilla (engl. *discourse*) tarkoitetaan koko tutkimusalan teoreettista lähtökohtaa eli kielenkäyttöä sosiaalisena toimintana. Tällöin tutkimus on vahvasti teoreettista ja kieleen pohjautuvaa, ja siitä käytetään nimitystä mikrotaso. Spesifeihin diskursseihin (engl. *a discourse*) viitattaessa tarkastelussa on kielen makrotaso eli historiallisesti vakiintuneet ja tunnistettavat tavat, joilla asioita tai ilmiötä merkityksellistetään ja kuvataan. Makrotason tutkimus yhdistetään tavallisesti foucault'laiseen diskurssiteoriaan, sillä Foucault oli kiinnostunut merkityksistä kielen taustalla. (Pietikäinen & Mäntynen 2009: 26–27.) Mats Alvesson & Dan Kärreman (2000: 1126–1127) puhuvat "aineksesta tekstin takana" viitatessaan makrotasoon. Heidän mukaansa haasteena makrotason tutkimuksessa on valjastaa tekstin takainen merkitysmaailma osaksi diskursseja niin, että ilmiöistä ja asioista voidaan puhua teoreettisen tason lisäksi myös konkreettisella tasolla. Toisin sanoen tutkimuksen perusteella halutaan sanoa jotakin todellisesta maailmasta – kriittisessä diskurssianalyysissa usein purkaa tai uusintaa vanhoja käytänteitä.

Käytännössä mikro- ja makrotasoa on kriittisessä diskurssianalyysissa mahdotonta erottaa toisistaan. Teksti toimii välineenä tunnistaa diskurssit, joiden pohjalta analysoidaan, miten sosiaalinen todellisuus kussakin diskurssissa toteutuu (Pynnönen 2013: 8). Tutkija perehtyy aluksi teksteihin eli mikrotasoon, josta hän etenee makrotasolle yhdistelemällä tekstistä nousseita diskursseja siihen sosiaaliseen todellisuuteen, jossa ne on tuotettu. Norman Fairclough (2003: 3, 16) painottaa, ettei tutkimuksessa pitäisi joutua valitsemaan mikro- ja makrotutkimuksen väliltä. Hänen mukaansa tekstuaalinen analyysi on olennainen osa diskurssien tutkimusta, mutta diskurssianalyysi on vain vähän lingvististä. Yksinään tekstuaalinen analyysi on melko rajoitettua, kun taas yhdistettynä makrotason tutkimukseen se toimii olennaisena lisäyksenä. Alvesson & Kärremanin (2000: 1134) mukaan oman haasteensa tällaiseen lähestymistapaan tuo se, että mikro- ja makrotason diskurssianalyysitavat käsittelevät diskursseja eri näkökulmista. Diskurssi yksikössä eli mikrotaso

on lähtökohtaisesti paikallisempaa, teoreettisempaa ja ei-fyysistä, kun taas diskurssit monikossa kytkeytyvät laajempiin ilmiöihin. Toisin sanoen tutkimuksen kannalta keskeistä on se, kuinka paljon *kontekstia* diskursseihin sisällytetään.

Kontekstin käsitteellä viitataan niihin tekijöihin, joiden pohjalta merkitykset muodostuvat ja jotka rajoittavat tai mahdollistavat merkityksen käyttöä (Pietikäinen & Mäntynen 2009: 30). Diskurssit eivät ikinä koostu vain yhdestä tekstistä, lausumasta tai teosta (Hall 2001: 72). Sen sijaan ne saavat merkityksensä suhteessa muihin teksteihin tai tekoihin sekä suhteessa sosiaaliseen todellisuuteen, josta ne saavat alkunsa (Phillips & Hardy 2002: 3, 82). Kyberturvallisuusstrategioita tutkittaessa diskurssit syntyvät paitsi tekstien suhteessa toisiinsa, myös niitä ympäröivään kontekstiin, jossa ne on tuotettu. Tässä tutkimuksessa konteksti ulottuu tutkittavien valtioiden maailman- ja geopoliittisiin asemiin sekä siihen, miten strategiat asemoituvat suhteessa toisiinsa ja siten tuottavat diskursseja. Sitä sosiaalista tilannetta, jossa strategiatekstiä on tuotettu, ei kuitenkaan ole tässä tutkimuksessa mahdollista tarkastella.

Kontekstin ohella olennainen osa kriittistä diskurssianalyysiä on diskurssin ja *representaation* suhde. Representaatiossa on kyse siitä, miten kielellä kuvataan maailmaa. Merkittävää on esimerkiksi se, mitä jätetään sanomatta tai sanotaan, kuka on äänessä ja kuka ei, millaisia nimityksiä käytetään ja mikä on niiden hierarkkinen suhde. Tutkimuksen kannalta kiinnostavaa on, mitkä asiat on valittu ja mitkä ei. Tämä asettaa myös diskurssit eriarvoiseen asemaan, kun toiset diskurssit representoivat todellisuutta äänekkäämmin kuin toiset. (Pietikäinen & Mäntynen 2009: 55–56, 70, 72.) Tällaiset epäsymmetrisyydet ovatkin kriittisessä diskurssianalyysissa keskiössä: analyysissa on ominaista pohtia väärinkäyttöä, dominointia ja epätasa-arvoisuutta, sekä sitä, kuinka ne syntyvät ja kuinka niitä toisaalta ylläpidetään ja vastustetaan sekä teksteissä että puheessa (van Dijk 2001: 352). Fairclough (1993: 135, 137) painottaa sitä, miten kriittisessä diskurssianalyysissa sosiaalisen toiminnan seuraukset – väärinkäyttö, dominointi, epätasa-arvo – luovat *valtasuhteita*.

Vallan käsite on tärkeä myös Foucault'n diskurssiteoriassa. Jos foucault'laisittain ajatellaan diskurssien syntyvän ymmärryksen ja tietämyksen järjestämisestä järkeväksi merkityskokonaisuudeksi, seurauksena syntyy käyttäytymismalleja, uskomuksia ja tapoja. Olennaista ei ole se, ovatko nuo mallit oikeita tai vääriä, sillä uskoessaan niihin ja käyttäytyessään niiden mukaisesti ihminen tekee niistä "tosia". Kun diskursiiviset käytänteet omaksutaan osaksi yhteiskuntaa ja niiden pohjalta aletaan säännellä ihmisten käytöstä, syntyy rajoituksia ja sääntöjä. Näin ollen diskurssit, jotka nousevat vuorovaikutteisesta toiminnasta, sisältävät valtaefektin. (Hall 2001: 76.) Käytännössä diskurssien valta ilmenee esimerkiksi siten, että kyberturvallisuusstrategioiden lukijat hyväksyvät niissä esiintyvät diskurssit eli tavan, jolla tieto on niissä järjestetty, ja alkavat toimia sen mukaisesti. Diskurssit eivät kuitenkaan ole ehdottomia ja muuttumattomia. Tiedon järjestäminen toisella tavalla – esimerkiksi tutkimusten tuodessa uutta tietoa – muokkaa ja uusintaa jo vakiintuneita diskursseja.

Kun tiettyjä diskursseja pyritään "istuttamaan" osaksi yhteiskuntaa ja ihmisten ajattelua, puhutaan *legitimoinnista*. Legitimointia tekevät yleensä eliitti- ja instituutioryhmittymät, joilla on valta-asema suhteessa muuhun yhteiskuntaan. (van Dijk 1993: 249–250.) Kriittisessä diskurssianalyysissa legitimointi toteutuu erilaisten argumentaatiostrategioiden kautta. Niillä oikeutetaan tai perustellaan tietynlaista sosiaalista toimintaa, kuten ideoita, ajatuksia, julistuksia ja käyttäytymistä. (Reyes 2011: 792.) Fairclough (2003: 98) erottaa neljä eri legitimoinnin muotoa: 1) *valtuuttaminen*, jolloin legitimaation voima perustuu perinteisiin, tapoihin, lakeihin ja instituutioihin; 2) *rationalisointi* eli institutionaalisen tai muun vastaavan toiminnan oikeuttaminen hyödyllä tai järjellä; 3) *moraaliin* perustuva legitimointi, jolloin toiminta oikeutetaan arvojärjestelmällä ja 4) *mythopoesis*, jossa legitimaatio tuotetaan tarinoiden ja myyttien avulla. Mukaillessaan Theo van Leeuwenin teoriaa legitimoinnista Reyes (2011: 785, 804) mainitsee legitimoinnin muodoiksi vielä *tunteisiin vetoamisen*, *hypoteettisen tulevaisuuden* ja *altruismin*.

Legitimoinnin tapoja on siis monia ja tutkijat määrittelevät niitä eri tavoin. Kootusti voidaan sanoa, että kaikilla legitimoinnin tavoilla eli oikeuttamisella pyritään suostuttelemaan ja vakuuttamaan toisia. (Pynnönen 2013: 21.) Legitimointi tuo kyberturvallisuusstrategioiden analysointiin arvokkaan lisän, sillä sen avulla on mahdollista löytää tekstistä

diskursiiviset valta-asetelmat ja siten valtion keinot pyrkiä vakuuttamaan strategioiden yleisö. Valtioiden legitimointiin pyrkivä toiminta voi olla joko tietoista tai tiedostamatonta, sillä kuten olen edellä todennut, diskurssit ovat usein historiallisesti vakiintuneita ja näin ollen syntyneet pitkän ajan kuluessa. Tuottaessaan jotakin tiettyä diskurssia valtio ei ilman muuta tee sitä tarkoituksenmukaisesti, vaan koska ”niin on aina tehty” (eli diskurssi on yleisesti hyväksytty ja tunnistettu yhteiskunnassa merkityssysteemiksi).

Legitimoinnin keinot ja diskurssien valta-asetelmat ovat paikannettavissa tekstistä retorisen analyysin avulla. Sen lähtökohtana on tutkia sitä, kuinka kielellä yritetään vakuuttaa toimijat jostakin tietystä todellisuuden versiosta. Jokinen (2016: 338–339) puhuu retoriikan yhteydessä argumentoinnista, joka pyrkii vahvistamaan omaa totuutta tai käsitystä siitä ja vakuuttamaan yleisön. Retoriset keinot toimivat siis diskurssien välittämisen työkaluina tekstissä. Poliittisissa teksteissä retorisia keinoja käytetään laajasti (Jokinen 1999/2006: 47), joten niiden tutkiminen kyberturvallisuusstrategioissa on perusteltua diskursiivisten valta-asetelmien jäsentämiseksi.

3.2 Vakuuttaminen ja argumentointi

Retoriikka on kielenkäytön keino, jolla pyritään vakuuttamaan yleisö ja argumentoimaan oma näkökulma mahdollisimman pätevästi. Kaikki teksti ja puhe sisältävät väistämättä retoriikkaa. Kriittisen diskurssianalyysin puitteissa retoriikka toimii työkaluna. Sen avulla tekstistä etsitään keinoja, joilla puhuja tekee argumentaatiostaan uskottavaa. Tällaisia keinoja voivat olla esimerkiksi syy-seuraussuhteet, rinnastukset, metaforat ja vastakkainasettelut. Päämääränä on vastata sellaisiin kysymyksiin, kuten kuinka merkityksiä tuotetaan, kategorisoidaan ja oikeutetaan teksteissä. Siinä missä retoriikka tutkimusmenetelmänä huomioi kielen muotoilua sekä puhujan ja yleisön välistä suhdetta, kriittinen diskurssianalyysi tutkii, miten merkitykset muotoutuvat retoristen keinojen kautta. (Jokinen 1999/2006: 46–47.) Keskiössä on siis tarkastella teksteissä ja puheessa sitä, mitä retorisilla keinoilla argumentoidaan ja tehdään siinä hetkessä, kun ne tuotetaan. (Jokinen 2016: 338).

Retorisilla keinoilla ”tekeminen” linkittyy Foucault’n diskurssiteoriaan, jossa toiminta ja kieli ovat samanarvoisia diskurssien muodostajia. Myös retorisilla keinoilla tehdään – vakuutetaan, oikeutetaan, dominoidaan – ja siten rakennetaan diskursseja. Jokisen (2016: 339) mukaan diskurssianalyysissa retorisiin keinoihin ja argumentointiin liittyvät käsitteet tulisikin määritellä uudelleen toiminnallisuuden näkökulmasta. Jos perinteisessä retoriikan tutkimuksessa asenne ymmärretään staattisesti ihmisen sisäiseksi mielentilaksi, sen toiminnallinen merkitys näyttäytyy siinä, kuinka henkilö on puhuessaan *asemoitunut.* Asemoituminen on sosiaalista toimintaa, jossa puhuja on paitsi jotakin mieltä asiasta, hän myös konkreettisesti asettuu julkisessa keskustelussa jonkin kannan taakse (Billig 1987: 177; 1991: 43). Diskurssianalyysin kannalta tämä tarkoittaa sitä, että kieltä tutkiessa tutkijan täytyy huomioida, millaisesta kontekstista (eli asenteesta) käsin se on tuotettu ja minkälaiseen keskusteluun se on tarkoitettu (eli asemoitu). Kyberturvallisuusstrategioita analysoitaessa on oleellista määrittää konteksti ja puhujan asemoituminen, sillä vaikka strategioiden teksti ei sinänsä ole asenteellista, ne on tuotettu tietystä asemasta käsin. Tuo asema voi olla itse otettu tai jonkun toisen määrittämä. Joka tapauksessa analyysin lähtökohtana on strategian asemointi.

Asemoitumista määrittää myös se, kenelle puhe on suunnattu. Jotkin retoriset keinot toimivat eri tilanteissa paremmin kuin toiset. Argumentoinnin onnistumista mittaa lopulta yleisön hyväksyntä. Jokinen (2016: 340) kirjoittaa, että tekstejä tutkittaessa yleisösuhteen analysointi on haastavaa, koska vastaanottajan reaktio ei välttämättä ole näkyvissä. Tällöin puhujan asemoituminen voi paljastaa, kenelle tekstit on suunnattu. Omassa tutkimuksessani yleisösuhdetta ei juuri pysty analysoimaan, sillä kyberturvallisuusstrategioiden teksteissä ei ole näkyvää vuorovaikutusta. Sen sijaan retoristen keinojen käyttäminen voi paljastaa, kuka on strategian oletettu yleisö.

Perinteisessä retoriikassa vakuuttava argumentointi voi perustua tosiasioihin. Kriittisessä diskurssianalyysissa palataan jälleen kielen ja toiminnan yhteisvaikutukseen (Jokinen 2016: 341), ja tosiasioiden sijasta siinä tutkitaan asian todeksi tekemisen *prosessia* eli *faktan konstruointia*. Olennaista ei ole se, onko fakta tosi vai epätosi, vaan kuinka puhuja on tuottanut faktan – eli toiminta faktan määrittämisen takana. (Potter 1996: 112.) Sa-

malla tavoin voidaan tehdä ero retoriikan ja diskurssianalyysin välille todellisuuden *kategorisoinnissa.* Kun retoriikka määrittelee, millaisia kategorioita puheessa on, kriittisessä diskurssianalyysissa ihminen on tuottanut kategoriat kielen ja toiminnan välisessä sosiaalisessa vuorovaikutuksessa (Potter 1996: 111).

Edellä olen selvittänyt retoriikan ja kriittisen diskurssianalyysin eroja retoristen keinojen analysoimiseen. Vaikka kriittinen diskurssianalyysi onkin lainannut käsitteitä ja analyysimenetelmiä retoriikasta, lähestymistavat eroavat toisistaan. Retorisessa tutkimuksessa kieltä tutkitaan staattisempana merkityssysteeminä kuin mitä diskurssit ovat. Kriittisessä diskurssianalyysissa painopiste on kielen ja toiminnan vuorovaikutuksessa, jolloin kieltäkin tutkitaan toimintana.

Aluksi diskurssianalyyttinen tutkimus, jossa käytetään retoriikan menetelmiä, voi vaikuttaa retoriikan tutkimukselta, mutta tämä on vasta analyysin ensimmäinen vaihe. Fairclough'n teorian perusteella voitaisiin puhua kriittisen diskurssianalyysin tekstuaalisesta mikrotason tutkimuksesta. Kun retoriset keinot on paikannettu selonteoista, tutkija syventyy niiden käyttökontekstiin eli makrotasolle. Tässä vaiheessa tutkimusta kielestä löytyneet diskurssit sidotaan kontekstiinsa, jolloin ne ovat vuorovaikutussuhteessa toimintaan eli strategioiden tuottamishetkeen. Tämän avulla on mahdollista löytää diskursiiviset todellisuudet, jotka tekstin – tässä tapauksessa kyberturvallisuusstrategian – taustalla vaikuttavat. Analyysin pohjustamiseksi esittelen vielä lyhyesti strategioissa eniten käytettyjä retorisia keinoja ja osoitan, kuinka ne on strategioista paikannettu.

3.3 Kyberturvallisuusstrategioiden retoriset keinot

Retorisilla keinoilla pyritään uskottavuuteen. Puhuja yrittää vakuuttaa kuulijoilleen esittämänsä asian olevan totta. Osa keinoista pyrkii tekemään väitteen esittäjästä uskottavamman, kun taas toisten tarkoituksena on saada asia näyttämään todelta ja siten myös luotettavammalta. Olen listannut Jokisen (2016: 345–367) mainitsemat yleisimmät vakuuttamisen keinot taulukkoon 4. *Esittäjän uskottavuutta* tukevat keinot liittyvät puhujan ase-

maan ja läheisyyteen suhteessa yleisöön sekä puhujaa tukeviin tahoihin. Näiden paikantaminen kielestä voi osoittautua haastavaksi, sillä ne vaativat syvempää tulkintaa. Sen sijaan *väitteen uskottavuutta* perustellaan näkyvämmillä kielen keinoilla, joita ovat esimerkiksi ääri-ilmaisut ja listat, määrällistäminen ja toisto.

Jokinen (2016: 343–344, 351–353) painottaa, ettei keinojen löytäminen ja tyypittely ole diskurssianalyysissa olennaisinta, vaan tarkoitus on tutkia sitä, mitä niiden käyttämisestä seuraa. Esimerkiksi se, onko retoriikka kielessä tietoista vai ei, on tutkimuksellisesti sivuseikka. Kaikki keinot eivät myöskään aina toimi kaikissa vuorovaikutustilanteissa, joten toiset keinot ovat toisinaan merkityksellisempiä kuin toiset. Poliittisissa teksteissä on tyypillistä käyttää konsensusta yhtenäisyyden luomiseen tai tosiasiapuhetta vasta-argumenttien välttämiseksi.

Taulukko 4. Yleisimmät vakuuttamisen keinot (ks. Jokinen 2016: 345–367)

Esittäjän uskottavuus	**Väitteen uskottavuus**	
Etäännyttäminen omista intresseistä	Tosiasiat ja vaihtoehdotto-muuspuhe	Metaforat
Puhujan kategorinen asema	Kategorioilla oikeuttami-nen tai kritisoiminen	Ääri-ilmaisut
Puhujan liittoutumisaste lukijaansa	Yksityiskohdat ja kertomukset	Kolmen lista
Konsensus ja asiantuntija-lausunnot	Numeerinen ja ei-numeeri-nen määrällistäminen	Kontrastiparit
	Toisto	Vasta-argumentteihin varautuminen

Oletan, että myös kyberturvallisuusstrategioissa toiset keinot ovat näkyvämpiä ja yleisempiä kuin toiset, kun taas toisia käytetään huomattavasti hienovaraisemmin ja määrällisesti vähemmän. Sen vuoksi esittelen tässä tutkimuksessa tarkemmin vain ne retoriset keinot, joilla on ollut olennainen osa diskurssien muodostumista analyysivaiheessa (ks. luku 4). Joitakin yksittäistapauksia muista keinoista nostan esiin, jos ne ovat olleet merkittäviä diskurssien kannalta. Havaintojeni perusteella strategioissa yleisimmin käytetyt

retoriset keinot ovat *puhujan kategorinen asema*, *konsensus*, *tosiasiat*, *yksityiskohdat*, *määrällistäminen* ja *metaforat*.

3.3.1 Puhujan kategorinen asema

Puhujakategorialla tarkoitetaan sitä, millaisesta kulttuurisen tietämyksen asemasta toimija puhuu. Toiset puhujakategoriat ovat arvostetumpia kuin toiset, koska niillä odotetaan olevan sellaista tietoa, jota voi hankkia ainoastaan asiaan perehtymällä. Esimerkiksi lääkärin asema on tällainen. (Potter 1996: 114.) Puhujakategoriat eivät ole muuttumattomia, vaan samalla henkilöllä voi olla niitä useita (Jokinen 2016: 347). Lääkäri voi puhua myös äitinä tai puolisona tai muutoin yhteiskunnallisena vaikuttajana vaikkapa kunnallispolitiikassa.

Bronwyn Davies ja Rom Harré (1991/2001: 263) linkittävät puhujakategorian asemoitumiseen. Puhuessaan jostakin asemasta käsin puhuja tulee samalla sulkeneeksi ulkopuolelle monia muita asemia, joista käsin hän kenties olisi voinut puhua, tai hän joutuu tekemään näin, sillä asema ei ole hänen ulottuvillaan. Esimerkiksi puhuessaan miehenä hän ei voi olla samanaikaisesti nainen. Asemoitumalla johonkin tiettyyn kategoriaan puhuja osallistuu myös noiden kategorioiden diskursseihin.

Puhujakategoria on annettu asema eikä itse valittu. Diskurssit kertovat ihmiselle kuka hän on ja mikä on hänen suhteensa todellisuuteen (Törrönen 2000: 250). Niinpä esimerkiksi kyberturvallisuusstrategioissakin puhujakategoriat ovat ikään kuin määräytyneet tekstin luonteen ja sen tuottaneen instituution seurauksena. Kansallisissa poliittisissa teksteissä on todella rajallista, miten puhuja voi asemoitua. Strategioissa puhujakategoria on yleensä valtio, jonka tavoitteena on turvata talouspolitiikka ja kansalaistensa hyvinvointi. Usein puhe vielä henkilöityy hallitukseen tai ministeriin, mutta siitä huolimatta puhujakategoria on tavalliseen kansalaiseen nähden institutionaalisessa asemassa, jonka diskursiivisia käytänteitä voi olla vaikea tavoittaa.

3.3.2 Konsensus

Konsensus tarkoittaa yleisesti hyväksyttyä tai jaettua mielipidettä jostakin asiasta. Jos asialle on saatu hyväksyntä usealta eri taholta, voidaan saavuttaa vastaanottajan luottamus (Potter 1996: 159). Tällöin asia ei näyttäydy vain puhujan omana mielipiteenä, vaan joku muukin on vahvistanut sen. Mitä arvovaltaisempi vahvistava taho on, sitä suurempi vaikutus ulkopuolisella hyväksynnällä on asian uskottavuuden kannalta. Esimerkiksi tutkimustulokset tai asiantuntijat tuovat väitteille hyväksyntää. (Jokinen 2016: 350.)

Konsensusta voidaan luoda myös me-retoriikan käytöllä. Tuolloin puhuja esiintyy laajan joukon puolesta puhujana, mutta asettumalla jonkin ryhmän edustajaksi hän tekee samalla erottelun ”meihin” ja ”muihin” (Billig 1987: 89). Me-retoriikassa on siis aina implisiittisenä jako kategorioihin. Me-retoriikka on näkyvin vakuuttamisen muoto, sillä sen tunnistaa jo itse sanasta. Lisäksi sen käyttö on yleistä poliittisessa puheessa ja tekstissä (Billig 1987: 89; Jokinen 2016: 351), mikä on kiinnostavaa tämän tutkimuksen kannalta.

Kyberturvallisuusstrategioissa me-retoriikkaa käytetään laajasti. Tuolloin pyrkimyksenä voi olla esimerkiksi luoda kansalaisista yhtenäinen joukko, jonka kaikilla osapuolilla on samanlaiset intressit (Jokinen 2016: 351). Asiantuntijalausunnot ja muut ulkoisten tahojen vahvistukset ilmenevät strategioissa erityisesti suorilla lainauksilla, jotka Robin Wooffitin (1992: 155–177) mukaan toimivat konkreettisena keinona asiantuntijuuden esittelemiseksi.

3.3.3 Tosiasiat ja vaihtoehdottomuuspuhe

Tosi-asia ja vaihtoehdottomuuspuhe ovat retorisia keinoja, joiden tehtävä on vahvistaa väitteen uskottavuutta esittäjän sijasta. Poliittisessa puheessa asiat esitetään usein totuuksina, joihin kukaan ei voi vaikuttaa (Wooffit 1992: 102–103). Asia on ikään kuin hyväksyttävä sellaisenaan, eikä sille esitetä muita rationaalisia vaihtoehtoja. Kun tällainen väite esitetään, kuulijalle tulee tunne, että hänen on hyväksyttävä se näyttäytyäkseen loogisena. Vastuu asiasta siirretään vastaanottajan ymmärryksen varaan. Lisäksi tällaiset ”toteen”

perustuvat ehdottomat väitteet vähentävät moraalista pohdintaa, sillä asian suhteen ei yksinkertaisesti ole muita toimintatapoja. Vaihtoehdottomuuspuheen tunnistaa usein siitä, että lauseessa ei ole tekijää, jolloin syiden etsimisestäkin tulee mahdotonta. (Jokinen 2016: 352–353.)

Kyberturvallisuusstrategioissa tosiasia- ja vaihtoehdottomuuspuhetta käytetään muun muassa valtion sen hetkisen tilanteen selittämiseen. Valtio ei esimerkiksi ole pystynyt panostamaan kybertoimintaansa enempää, sillä se on ”jätetty asian kanssa yksin”. Asia on ilmaistu ikään kuin valtion tila on jonkin kausaali-ilmiön tulos, eikä sille ole voitu tehdä mitään muuta. Tutkija voi tällöin kyseenalaistaa, onko väittämä todella ainoan mahdollisen vaihtoehdon tulos, vai kenties retorinen ilmaus, jolla halutaan puolustella tai oikeuttaa aikaisempaa vähäistä panostusta kybermaailmaan.

3.3.4 Yksityiskohdat ja kertomukset

Yksityiskohtainen tarinankerronta luo väitteelle autenttisuuden ja todenmukaisuuden tunnun. Kun tapahtumat kerrotaan osana isompaa kertomusta, kuulija osaa odottaa tiettyä lopputulemaa ja rakentaa lopullisen tulkintansa itse. Tällöin väite tuntuu todelta, sillä kuulija luottaa omaan ymmärrykseensä väitteestä, mikä tekee siitä uskottavamman. (Potter 1996: 117–118.) Puhuja ei ole myöskään velvollinen puheistaan, jos kuulija on tehnyt virheellisen tulkinnan (Jokinen 2016: 357).

Yksityiskohtia ja tarinoita käytetään kyberturvallisuusstrategioissa erityisesti silloin, kun halutaan korostaa tai nostaa esiin jokin tietty seikka. Tuolloin asia on erotettu varsinaisesta tekstistä ”tietoiskuksi”. Käsitteitä tai aikaisempia kyberiskuja selitetään tarkemmin omissa tekstiosioissaan, jolloin niille kasautuu enemmän painoarvoa. Uhkista ja haavoittuvuuksista kerrotaan usein laajemmin, sillä vaikka ne ovat yleisesti ottaen mielenkiintoisia ja kansantajuisia, luovat ne samalla sen verran pelkoa, että ihminen alkaa huolehtia omasta toiminnastaan ja muuttaa käytöstään halutunlaiseksi.

3.3.5 Määrällistäminen

Kvantifioimalla eli määrällistämällä vakuuttamista on yleensä numeroiden, taulukoiden, prosenttien, osuuksien ja laatusanojen käyttö. Tarkoituksena voi olla esimerkiksi väitteen merkityksen oikeuttaminen tai sillä syyttäminen tai kehuminen. Väitteen perustuessa numeroihin unohdetaan usein se, että puhuja on itse valinnut perustelunsa jostakin kokonaisuudesta. Tuolloin tietyt numerot voivat puhetilanteessa kuulostaa merkittäviltä, mutta todellisuudessa ne ovat vain pieni osa suurempaa joukkoa. Näin ollen kvantitatiivinen aineisto on pääpiirteissään vahvasti tulkinnallista, vaikkei sitä yleensä mielletä sellaiseksi. (Jokinen 2016: 358–360.)

Retorisena keinona määrällistäminen erottuu tekstistä varsin helposti. Kyberturvallisuusstrategioissa määrällistämisellä ilmaistaan kybertoimintaympäristön laajuutta ja käyttäjämäärää, tehtyjä kyberiskuja ja siitä seuranneita kustannuksia sekä mahdollisia taloudellisia hyötyjä. Kybertoimintaympäristön taloudellisia kustannuksia on kuitenkin lähes mahdoton laskea, joten lukujen vertailukelpoisuus jää melko vähäiseksi. Lisäksi taloudellisista intresseistä puhuttaessa voisi olettaa, että valtio on valinnut strategioihin tietyt luvut, jotka tuovat sille hyötyä.

3.3.6 Metaforat

Metafora on ilmaisu, jossa sanotulla ei ole samanlaista merkitystä kuin sen kirjaimellisella määritelmällä. Metaforan tarkoitus on tehdä jokin outo tai tuntematon asia tutuksi toisesta yhteydestä lainatuilla ilmaisuilla. Retorisesti metaforien käyttö on tehokasta, sillä vastaanottajalle syntyy ilmaisusta konnotaatio, joka vahvistaa väitettä. Tällöin puhuja ei välttämättä joudu turvautumaan muuhun argumentaatioon. Niin sanotut piilevät metaforat ovat erityisen vakuuttavia. Väitteeseen kätkeytyvä metafora saa aikaan samanlaisen efektin kuin vaihtoehdottomuuspuhe: asiat vain johtuvat niiden luonteesta, jolle ihminen ei voi mitään. (Jokinen 2016: 360–362.)

Kyberturvallisuusstrategioissa oman haasteensa metaforien paikantamiseen tuo englannin kieli, jonka kaikki vivahteet eivät aukea ei-natiiville lukijalle. Esimerkiksi sanontoja

käytetään strategioissa paljon, ja niillä voi olla erilainen kirjaimellinen vastine suomeksi. Metaforat on usein lainattu arkikielestä, mikä tuo niihin kansanomaisuutta ja tekee siten teksteistä helposti lähestyttävämpää. Urheilutermien ja -metaforien käyttö tuo asiat lähelle lukijaa, jolloin tämä hyväksyy sanotun helpommin.

3.3.7 Muita vakuuttamisen keinoja

Kyberturvallisuusstrategioissa vähemmän käytettyjä, mutta kuitenkin merkittäviä vakuuttamisen keinoja edellisten lisäksi, ovat *ääri-ilmaisut* ja *toisto*. Ääri-ilmaisuilla maksimoidaan tai minimoidaan kuvauksen kohdetta. Kun asia esitetään ääri-ilmaisuin, asiasta tehdään kiistaton, eikä siitä ole helppo väitellä, onko se totta vai ei. Ääri-ilmaisuja voidaan käyttää myös oikeuttamaan oma toiminta esimerkiksi normalisoimalla jokin tekeminen: ”jos kaikki tekevät niin, minäkin voin”. (Jokinen 2016: 363.) Toiston käyttäminen vastapuolen vakuuttamiseksi perustuu siihen, miten muotoilua käytetään osana omaa argumentointia. Toistolla voidaan rakentaa uudenlaisia merkityksiä muun muassa viittaamalla toisiin teksteihin ja asettaa sama asia eri yhteyteen. (Jokinen 2016: 363, 366.) Kyberturvallisuusstrategioissa ääri-ilmaisuilla perustellaan jonkin ajatuksen yleisyyttä (”kaikki ajattelevat näin”), kun taas toiston tehtävä on mainosmaailman tapaan iskostaa jokin asia vastaanottajan päähän.

Edellä olen määritellyt kyberturvallisuusstrategioissa eniten käytettyjä vakuuttamisen keinoja. Niistä puhujakategorian ja konsensuksen tavoitteena on kasvattaa puhujan uskottavuutta, kun taas tosiasioilla, yksityiskohdilla, määrällistämällä ja metaforilla tehdään luotettava itse väitteestä. Kun vakuuttamisen eri keinoja käytetään samanaikaisesti, tekstin ja sen esittäjän uskottavuus korostuu entisestään. Vakuuttamisen keinojen tunnistaminen tekstistä on olennaista diskurssien muodostamiseksi. Analyysivaiheessa keinot toimivat työkaluina, joilla tekstistä etsitään vakuuttavien diskurssien kannalta merkittäviä kohtia lähempään tarkasteluun. Seuraavassa kappaleessa esitän analyysini kyberturvallisuusstrategioissa käytetyistä diskursseista, jotka olen paikantanut vakuuttamisen keinoja hyödyntämällä.

4 KYBERSTRATEGIOIDEN VAKUUTTAVUUS JA KONTEKSTOINTI

Diskurssien tunnistaminen ja analysointi ovat monivaiheisia prosesseja. Koska kyseessä on laadullinen tutkimus, tarkoituksena on pelkistää alkuperäiset havainnot suppeammiksi havaintoryhmiksi (Alasuutari 2011: 43). Tämä tarkoittaa sitä, että aluksi käytössä on ollut suuri määrä aineistoa, josta haarukoimalla olen rajannut tutkmuksen kannalta olennaiset diskurssit lähempää analyysia varten. Työkaluina minulla on ollut edellisessä luvussa käsittelemäni kriittisen diskurssianalyysin käsitteet ja retoriset keinot.

Tässä luvussa analysoin kyberturvallisuusstrategioiden diskursseja kokonaisvaltaisesti. Aluksi asetan strategiat kontekstiinsa. Tämän jälkeen selvennän analyysin vaiheita, minkä jälkeen tarkastelen yksityiskohtaisesti strategioiden diskursseja nojautumalla aineistostani esiin nostamiini esimerkkeihin. Lopuksi peilaan diskursseja valtioiden todelliseen tilanteeseen ja kokoan analyysini löydökset yhteen.

4.1 Analysoitavat strategiat

Kuten olen aikaisemmin todennut strategiatekstiä käsitellessäni, jokainen tässä tutkimuksessa analysoimani kyberturvallisuusstrategia edustaa strategian genreä. Strategiat pitävät sisällään valtion vision ja suunnitelmat kyberturvallisuudesta. Yhteisestä genrestä huolimatta strategioilla on myös omia erityispiirteitä, jotka johtuvat strategian syntykontekstista. Eri maiden strategiset lähtökohdat ja tavoitteet voivat poiketa toisistaan paljon, minkä lisäksi strategioiden sisältöön vaikuttavat kulttuuriset tekijät. Seuraavaksi esittelen lyhyesti analysoimani kyberturvallisuusstrategiat ja valtioiden tilanteen kyberturvallisuuden saralla.

4.1.1 Australia

Australian kyberturvallisuusstrategia (2016) on valtion toinen julkaistu strategia. Julkaisuajankohtanaan strategia noteerattiin Australian uutismediassa erityisesti budjetin osalta, minkä lisäksi mediaa kiinnosti strategiassa määritellyt uudet tehtävänkuvat, kuten

kyberturvallisuusministerin ja kyberturvallisuuslähettilään toimet. Strategian mukaan valtaosa Australiaan kohdistuneista hyökkäyksistä tulee ulkomailta ja etenkin Kiinasta. (Karp 2016.) Syksyllä 2015 paljastui laaja kyberhyökkäys, jossa havaittiin Australian ilmatieteenlaitoksen kaikkien käyttäjätilien salasanojen vaarantuneen. Merkittävää tämä on siksi, että ilmatieteen laitos toimittaa dataa puolustusjoukoille. Iskun tekijät paikannettiin Kiinaan. (ACSC 2016: 11; Uhlmann 2015.) Australialaisten asiantuntijoiden mukaan Australia tulee vielä selkeästi perässä monia muita kybermaita, kuten Yhdysvaltoja, ja heidän toiveenaan onkin saattaa kyberturvallisuus osaksi Australian puolustusjoukkoja (Austin 2016). Vastikään nimetty Australian kybersuojelija Gideon Creech sen sijaan haluaisi panostaa enemmän opetukseen ja yritysyhteistyöhön (Brause 2016).

Australian kyberturvallisuusstrategiasta selviää, että valtio haluaisi kasvaa paikallisesti merkittäväksi toimijaksi Kaakkois-Aasian ja Tyynenmeren alueella. Hallitus panostaa erityisesti kansainväliseen yhteistyöhön sekä vastustuskykyiseen kybertoimintaympäristöön ja sen nopeaan palautumiseen. Haasteita tuo moniääninen asiantuntijajoukko, jonka mielestä kyberturvallisuutta pitäisi viedä enemmän puolustuspoliittiseen suuntaan viestintäpoliittisen sijasta ja toisaalta panostaa australialaisten kouluttamiseen, mikä itsessään vaatisi suurempaa kulttuurista muutosta yksityisyydestään tarkkojen australialaisten keskuudessa. Strategiasta välittyy vahva me-henki, jonka tavoittamiseksi se on osaltaan tuotettukin.

4.1.2 Iso-Britannia

Kuten Australian, myös Iso-Britannian kyberturvallisuusstrategia (2016) on varsin tuore. Kun se julkaistiin syksyllä 2016, media otti strategian vastaan melko ristiriitaisesti. Toisaalta kasvanutta puolustusbudjettia kiiteltiin, toisaalta se koettiin edelleen liian vähäiseksi valtion puolustuksen kokonaisturvallisuusbudjettiin verrattuna. Kyberturvallisuusbudjetin kasvattamisen sijasta sanomalehti *The Guardian* toivoi hallitukselta lainsäädännön uudistusta: tietoturva-asetusten käyttämistä pakolliseksi ja ohjelmistoyrityksiä vastuuseen haitallisten sovellusten jakamisesta. (Naughton 2016.) Eniten kyberhyökkäyksiä Iso-Britanniaan tulee Venäjältä ja Kiinasta. Alkuvuodesta 2017 Iso-Britannian

kyberturvallisuuskeskus raportoi lähes 200:sta korkean tason hyökkäyksestä kolmen kuukauden ajalta. (Grierson 2017.) Uudessa kyberturvallisuusstrategiassa on huomioitu myös Iso-Britanniaan kohdistuneisiin kyberhyökkäyksiin vastaaminen, mikä osaltaan huolestuttaa mediaa. Vastaiskujen tekeminen vaatii hyökkäyksen alkuperän eksaktia paikantamista, mistä hallituksella ei median mielestä ole vielä tarpeeksi kokemusta. (Schwartz 2016.)

Iso-Britannian kyberturvallisuusstrategia on varsin mahtipontinen esitys, jonka tavoitteena on tehdä Iso-Britanniasta maailman turvallisin valtio yritystoiminnan harjoittamiseen. Strategiassa esitetään varsin selvästi, että Iso-Britannian asema antaa sille vapauden harjoittaa verrattain aktiivista kyberpuolustusta. Hallitus painottaa, että vain sillä on vastuu ja riittävät resurssit puuttua maan sisäisiin kyberturvallisuuspuutteisiin. Tämä tarkoittaa sitä, että hallitus voi halutessaan pakottaa yrityksen tai organisaation muuttamaan toimintatapojaan. Syitä tälle ei tarvitse etsiä kaukaa, sillä maailmanpoliittisesti johtavana suurvaltana Iso-Britannian ei juuri tarvitse varoa tuomasta mahtiaan esille, eikä se strategiassaan sitä edes yritä.

4.1.3 Nigeria

Nigerian kyberturvallisuusstrategia (2015) eroaa muista tutkimistani strategioista eniten. Sen sijaan, että maa pyrkisi maailmanlaajuiseen kyberherruuteen, Nigeria lähtee liikkeelle perusasioista: kansalaisten turvaaminen, lainvalvonnan saattaminen kyberaikakauteen sopivaksi ja infrastruktuurin suojaaminen. Lisäksi strategiaan on lisätty oma lukunsa lasten ja nuorten suojelemiseksi. Myös poliisin ja tuomareiden kouluttaminen kyberrikollisuustapauksissa – erityisesti lapsiin liittyvissä – on isossa osassa strategiaa.

Nigerialle kyberturvallisuus on erityisen tärkeää, sillä maahan on kohdistunut huomattava määrä kyberhyökkäyksiä viime vuosina. Vuonna 2015 onnistuneita iskuja oli 2 175, joista 587 tehtiin hallituksen sivuille. Internetkäyttäjistä 15 prosenttia kärsi iskujen seurauksista. (Tarpael 2017.) Rahalliset tappiot ylsivät yli 450 miljoonaan dollariin (Shaban 2016). Yleisesti ottaen Nigeria oli 20:ksi alttein kyberhyökkäysten kohde vuonna 2015 (It News Africa 2015). Nigeria ei ole pelkästään iskujen kohde, vaan usein myös niiden

lähde. Valtion asemaa kybertoimintaympäristössä vahingoittaa maan nimeen liitettävät nigerialaiskirjeet, joiden tarkoituksena on huijata rahaa sähköpostin tai sosiaalisen median kautta. Nimensä mukaisesti nigerialaiskirjeiden alkuperä on Nigeriassa. (Halminen 2014.) Ei ole siis mikään ihme, että Nigeria haluaa panostaa kyberturvallisuuteensa ja osoittaa aktiivisuutensa muille valtioille.

4.1.4 Singapore

Rikas ja pieni Singapore on Kaakkois-Aasian maista yksi teknologisesti kehittyneimmistä. Tämän perusteella voisi luulla, että sillä olisi myös vahvaa osaamista kyberturvallisuuden saralla. Tutkimusten mukaan Singapore on kuitenkin Aasian maista viiden haavoittuvimman ja kyberhyökkäyksille altteimman maan joukossa (Parameswaran 2016). Singapore kärsii Nigerian tavoin taloudellisista menetyksistä. Arvioiden mukaan kyberhyökkäysten kustannukset nousevat Singaporessa vuosittain 820 miljoonaan euroon. Iso ongelma kyberhyökkäysten pysäyttämiseksi on työvoiman puute. (Lim 2016.)

Singaporen kyberturvallisuusstrategia (2016) keskittyy koulutuksen lisäämiseen ja alan henkilöstön kasvattamiseen. Singaporella on merkittävä asema lentoliikenteen ja laivarahdin kauttakulkumaana, minkä lisäksi maan sisäisen liikenteen matkustajamäärät ovat huimia, sillä kaupunkivaltion alueella asuu 5,4 miljoonaa asukasta. Maan rahoituspalveluissa liikkuu biljoonia dollareita vuosittain. Eniten menetettävää Singaporella on, jos muut valtiot siirtyvät käyttämään samoja palveluita jonnekin muualle. Huomionarvoista on se, että Singaporen kyberturvallisuusstrategian on julkaissut maan viestintäministeriö eikä esimerkiksi puolustusministeriö tai pääministerin kanslia, kuten Australian, Iso-Britannian ja Yhdysvaltojen tapauksessa. Strategiassa ei viitata ollenkaan puolustuspoliittisiin uhkiin, mikä kertoo siitä, että Singaporen prioriteetit kyberturvallisuuden suhteen ovat jossain muualla.

4.1.5 Yhdysvallat

Yhdysvaltojen panostus kyberturvallisuuteen on alkanut jo 2000-luvun alussa. Vuonna 2003 Yhdysvallat julkaisi ensimmäisen varsinaisen kyberturvallisuusstrategiansa, johon

on tehty lisäyksiä muutaman vuoden välein. Lisäykset liittyvät muun muassa toimintatapoihin, kansainväliseen kyberturvallisuuteen, infrastruktuuriin ja presidentin kommentteihin. Viimeisin vuonna 2015 julkaistu versio on puolustusministeriön kyberturvallisuusstrategia. Tämä kertoo siitä, että Yhdysvalloissa kybermaailma on liitetty yhä enemmän osaksi puolustusvoimia tietoliikenne- ja viestintäministeriöiden sijasta.

Yhdysvaltoihin tehdään vuosittain lukemattomia kyberiskuja. Monet globaalit yritykset ovat kärsineet taloudellisia tappioita iskujen seurauksena. Vuonna 2016 kyberhyökkäyksistä raportoivat ainakinLinkedIn, MySpace, Yahoo, Dropbox, Dyn, FBI ja Yhdysvaltojen valtiovarainministeriö (Walters 2016). Yhdysvallat on kybermaailmassa paitsi houkutteleva kohde, myös vahva puolustaja ja vastaiskujen tekijä. Maalla on pitkät perinteet laajamittaisessa kybervakoilussa. Media uutisoi jatkuvasti Yhdysvaltojen ja Venäjän välisistä kyberkiistoista. Yhdysvallat toteaa kyberturvallisuusstrategiassaan oikeudekseen lopettaa konfliktit omilla ehdoillaan.

4.2 Strategioiden vakuuttamisen diskurssit

Analyysin ensimmäinen vaihe on ollut aineiston lukeminen ja rajaaminen, minkä jälkeen olen etsinyt strategioista vakuuttamisen keinoja. Tarkoituksenani on ollut paikantaa retoriset keinot luvussa 3.3 tekemieni määritelmien perusteella. Keinot paikannettuani olen valinnut strategioista sellaisia tekstikohtia, joissa keinot ovat erityisen näkyviä tai joissa useita keinoja on käytetty samanaikaisesti. Jokaisesta strategiasta olen rajannut noin 20 lyhyttä tekstikohtaa lähempään tarkasteluun.

Yleisimmät strategioissa esiintyvät vakuuttamisen keinot ovat puhujan kategorinen asema, konsensus, tosiasiat, yksityiskohdat, määrällistäminen ja metaforat (ks. luku 3.2). Jotkut strategiat rakentavat vahvaa yhteishenkeä, kun taas toiset pyrkivät vakuuttamaan lukijansa esimerkiksi pelottelemalla. Vakuuttamista analysoidessani olen tarkastellut toimintaa retoristen keinojen takana ja sen perusteella muodostanut diskursseja. Strategioissa diskurssit määrittyvät siis siten, mikä on sanojen toiminnan tavoite eli mistä todellisuudesta käsin puhuja pyrkii vakuuttamaan lukijansa.

Diskursseja määritellessäni olen yhdistänyt aikaisemmin valikoituneita tekstikohtia toisiinsa etsien yhtäläisyyksiä puhetapojen väliltä. Tässä vaiheessa eri valtioiden strategiat ovat sekoittuneet toisiinsa ja moni tekstikohta jäänyt pois. Lopullisessa analyysissa on yhteensä 49 lainausta kyberturvallisuusstrategioista. Diskurssien rajat ovat häilyviä, ja kutakin tekstiä voisi tarkastella useammasta diskurssista käsin. Analyysin pitämiseksi selkeänä olen kuitenkin analysoinut tekstejä vain yhden ja mielestäni selkeimmän diskurssin kautta. Strategioista nousi esiin viisi erityistä diskurssia, joista jokainen pitää sisällään 10–15 tekstipätkää useammasta eri strategiasta. Näille diskursseille olen antanut nimet *yhteishenki*, *kiiltokuva*, *pakotettu kontrolli*, *varallisuus* ja *itseoikeuttaminen.* Nimillä viitataan siihen, mitä kullakin diskurssilla pyritään konkreettisesti saavuttamaan: yhteishenkeä, kiiltävää ulkokuorta, kontrollia, varallisuutta ja omien toimien oikeutusta.

4.2.1 Yhteishenki

Ensimmäinen diskursiivinen piirre kyberturvallisuusstrategioissa on *yhteishengen* luominen. Yhteishengellä tarkoitan keskinäistä samaistumista ja yhteistä kokemuspohjaa, jonka kautta yksilöt tuntevat kuuluvansa samaan yhteisöön. Tämän seurauksena yksilöt alkavat toimia yhteisen päämäärän hyväksi. Yhteishengen tunnetta voisi verrata Benedict Andersonin (1983/2007: 39) käsitteeseen *kuviteltu yhteisö*, jonka jäsenet kokevat edustavansa samaa kansallista ideologiaa. Todellisuudessa he eivät välttämättä koskaan tapaa kaikkia yhteisönsä jäseniä, mutta mielessä syntynyt ajatus ideologisesta samankaltaisuudesta pitää yhteisöä koossa.

Kuviteltu yhteisö on ideologinen käsite, eikä sitä välttämättä ole edes olemassa tekstin ja puheen ulkopuolella. Yhteisön jäsenet voivat kokea yhtenäisyyttä, joka perustuu samaan kokemuspohjaan ja historiaan eli yhteiseen todellisuuteen, mutta aivan yhtä hyvin kuviteltu yhteisö voi olla olemassa vain tekstissä tai puhetavassa. Esimerkiksi kyberturvallisuusstrategioissa luotu yhteisö on syntynyt tiettyä tarvetta varten. Kybermaailman turvaaminen ei onnistu niin kauan kuin yksilöt toimivat omien intressiensä mukaisesti, joten ajatus samaan päämäärään pyrkimisestä on perusteltua. Kyberturvallisuusstrategioissa yhteishengen diskurssi on suunnattu pääosin kansalaisille ja se ilmenee muun muassa vahvan me-retoriikan kautta.

(1) Ultimately, all of us – governments, businesses, communities and individuals – need to tackle cyber security threats to make the most of online opportunities. (Australia 2016: 5.)

(2) Finally, we will step up partnerships and international engagement to manage the rapidly evolving nature of cybercrime and tackle cross-border issues. (Singapore 2016: 23.)

(3) The UK is one of the world's leading digital nations. Much of our prosperity now depends on our ability to secure our technology, data and networks from the many threats we face. -- The cyber threat impacts the whole of our society, so we want to make very clear that everyone has a part to play in our national response. (Iso-Britannia 2016: 6.)

(4) The strategic environment can change quickly. That is especially true in cyberspace. We must be dynamic, flexible, and agile in this work. We must anticipate emerging threats, identify new capabilities to build, and determine how to enhance our partnerships and planning. As always, our women and men – both uniformed and civilian personnel – will be our greatest and most enduring strength and a constant source of inspiration. By working together we will help protect and defend the United States and its interests in the digital age. (Yhdysvallat 2015: 33.)

Esimerkeissä puhutaan paljon *meistä*, *meidän vauraudestamme* ja *kyvyistämme*, *meidän vastuustamme.* Kansalaisille syntyy vahva tunne mahdollisuudesta vaikuttaa siihen, että jokaisen toiminnalla on merkitystä koko kansakunnan turvallisuuteen. Strategiat rakentavat kuvan, että kansalaiset ja hallitus ovat samanarvoisia. Esimerkissä 1 painotetaan yhdessä tekemistä ja ”yhteen hiileen puhaltamista”. Sen mukaan kaikki ovat velvollisia osallistumaan kyberturvallisuuden parantamiseen. Eri toimijoiden mainitseminen nimeltä osoittaa, että strategia pyritään kohdistamaan yhteiskunnan toimijoille tasapuolisesti. Näistä toimijoista on koottu joukkue, joka pyrkii ”kampittamaan” tai ”taklaamaan” (*tackle*) vastustajansa. Urheiluun viittaaminen on keino luoda kyberturvallisuuden kehittämisestä urheilutapahtuman kaltainen ilmiö, jossa joukkue taistelee yhdessä voiton puolesta. Myös esimerkissä 2 lainataan puhetapaa urheilusta yhteishengen nostattamiseksi.

Esimerkissä 3 korostetaan yhteisen kansakunnan tavoitetta melkeinpä nationalistisesti. Kansakunta kohtaa uhat yhdessä, kasvotusten. Ilmaisu ”*we want to make very clear*” voitaisiin tulkita jopa käskyksi, ellei sitä olisi pehmitetty vetoamalla kansalliseen vastuuseen sekä toisaalta vaihtoehdottomaan tilanteeseen, jossa ei ole muuta tehtävissä. Esimerkin 4

mukaan halu kyberturvallisuuteen nousee kansalaisista eli yksilöistä inspiraation lähteenä. Ilmauksen tarkoituksena on saada lukija tuntemaan olevansa tärkeä, mutta toisaalta hän on velvollinen ”antamaan takaisin” valtiolle, joka ponnistelee hänen puolestaan.

Me-retoriikan lisäksi yhteishengen diskurssia määrittävät metaforat. Metaforilla vaikeasti hahmotettavat asiat tuodaan lähelle kansalaista ilmaisemalla asia niin, että siihen on helppo samaistua.

> (5) Cyberspace is their nervous system – the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security. (Yhdysvallat 2003: vii.)

Esimerkissä 5 kyberturvallisuutta verrataan hermostoon, jonka tehtävä on kontrolloida ihmisen ruumista. Tässä tapauksessa ruumiin sijasta kontrolloitavana on valtio. Kun hermojärjestelmä levittyy ihmiskehon joka puolelle ja lähettää viestejä kehon eri osista, kybertoimintaympäristö on verkottunut kokonaisuus, jossa tietokoneet, palvelimet, reitittimet ja kaapelit mahdollistavat viestien välittymisen laitteelta ja ihmiseltä toiselle. Verkottunut kybertoimintaympäristö on yhtä tärkeä valtion hallinnolle kuin hermojärjestelmä ihmiskeholle. Esimerkin kautta välitetään kuva, että kyberverkosta tulisi huolehtia kuin omasta kehosta. Tässä tapauksessa keho vain on kaikkien yhteinen. Kansalaiset tunnistavat metaforan helposti ja pystyvät siksi samaistumaan siihen. Metaforan tehtävänä kyseisessä esimerkissä onkin yhteisen kokemuspohjan ja sitä kautta yhteishengen luominen.

Myös yksityiskohdilla ja tapausesimerkeillä viitataan yhteiseen perinteeseen tai kokemusmaailmaan. Esimerkissä 6 viitataan Yhdysvaltoja kollektiivisesti järkyttäneeseen 9/11–terrori-iskuun. Sen lisäksi, että kansalaiset tunnistavat tapahtuman ja kokevat vuosikymmenen takaiset tunteet uudelleen, he ovat paljon vastaanottavaisempia asialle, jota esimerkki pohjustaa. Koska kyseinen terrori-isku oli ja on edelleen tunteita herättävä tapahtuma, tekstissä sitä seuraava me-retoriikka on huomattavan voimakkaasti latautunutta yhteishengen luomista. Lisäksi esimerkin lopussa muistutetaan siitä, kuinka tietynlaista

elämäntapaa, *meidän* elämäntapaa*mme*, on pyritty terroristi-iskulla vahingoittamaan, jolloin yhtenäinen kansakunta kokee oikeudekseen harjoittaa kyberturvallisuutta omilla ehdoillaan.

> (6) The terrorist attacks against the United States that took place on September 11, 2001, had a profound impact on our Nation. The federal government and society as a whole have been forced to reexamine conceptions of security on our home soil, with many understanding only for the first time the lengths to which self-designated enemies of our country are willing to go to inflict debilitating damage. We must move forward with the understanding that there are enemies who seek to inflict damage on our way of life. (Yhdysvallat 2003: 5.)

Esimerkeissä 7 ja 8 yksityiskohdat on esitetty hieman eri tavoin. Sen sijaan, että vedottaisiin tunteisiin ja muistoihin, esimerkissä 7 painotetaan konkreettisia toimenpiteitä, joilla kyberturvallisuustaso saadaan riittävän korkeaksi kansalaisten intressien ja arvojen mukaisesti. Ehdotuksena on kansainvälinen yhteistyö, jonka keskiössä on kansakunnan hyöty. Myös esimerkissä 8 kerrotaan konkreettisista uudistuksista kyberturvallisuuden parantamiseksi, sillä sitä vastaan puolustautuminen on rajallista. Uudistuksiksi esitetään muun muassa säännöllisiä harjoituksia, validointia ja jatkuvaa arviointia.

> (7) Australia needs to partner internationally to ensure our cyber engagement advances our security and economic interests, as well as our values. (Australia 2016: 40.)

> (8) However, we recognise that no system is 100 per cent fool-proof and breaches may still occur even despite the best of our efforts. We will continue to hold regular cybersecurity exercises to stress test our procedures and capabilities for a realistic evaluation of our proficiency, and conduct red-teaming sessions to validate the security of our systems. (Singapore 2016: 21.)

Esimerkeissä 7 ja 8 on käytetty me-retoriikkaa esimerkkien 1–4 tavoin. Erona on kuitenkin se, että jälkimmäisissä esimerkeissä me-retoriikalla kuvailtiin yleisöä eli kansakuntaa, sekä kerrotaan sille sen yhteiset mahdollisuudet ja velvollisuudet. Sen sijaan esimerkeissä 7 ja 8 kansakuntaa rauhoitellaan konkretialla ja yksityiskohtaisilla kuvailuilla, ja me-retoriikka toimii vain tukevana vakuuttamisen keinona. Mitä useampia keinoja tekstissä käytetään, sitä vakuuttavampi se on.

Huolimatta siitä, mitä vakuuttamisen keinoja tekstissä on käytetty, yhteishengen diskurssille on tyypillistä, että se kohdistetaan suoraan kansalle. Kansalaisia voimaannutetaan puheella yhteisestä päämäärästä tai urheilutermein, samaistetaan yhteisen kokemuspohjan ja kulttuurin perusteella sekä luodaan turvallisuuden tunnetta konkreettisilla esimerkeillä. Nämä saavat lukijan tuntemaan olevansa yksi ”meistä”. Yhteishenkeä voidaan kuitenkin luoda myös hyvin erilaisesta puhujakategoriasta käsin, nimittäin kohdistamalla puhe yhteisön ulkopuolelle.

(9) Thousands participated in the town hall meetings and provided comments online. (Yhdysvallat 2003: 2.)

(10) The level of skills, capabilities and expertise possessed by the personnel that will be charged with the responsibility of securing the nation's cyberspace, who will essentially be Nigerian citizens, will go a long way in determining how well it will be done. (Nigeria 2015: 7.3.)

(11) The government will need to interface with ordinary citizens engaging online on protection awareness, safety consciousness, learning materials, security tools and tips shall be articulated, localized and transmitted online to safeguard the most critical asset of the nation, i.e. her people. (Nigeria 2015: 11.1.)

Esimerkki 9 on yleisluontoinen kuvaus strategian tekovaiheesta, jolloin esimerkin mukaisesti tuhannet kaupunginvaltuuston kokouksiin osallistuneet pääsivät vaikuttamaan lopulliseen strategiaan. Vaikka esimerkin yleisönä ei ensisijaisesti ole kansakunta, vaan esimerkiksi media tai muut valtiot, sen on tarkoitus välittää kuva yhtenäisestä ja aktiivisesta kansasta, joka yhdessä haluaa panostaa kyberturvallisuuteensa. Myöskään esimerkissä 10 ei puhutella kansalaisia suoraan, mutta toteamus siitä, että kyseisen valtion kybermaailman turvaajaksi halutaan ensisijaisesti oman maan kansalaisia, on luottamuksenosoitus kansalaisia kohtaan. Samalla kun esimerkki on viesti muille valtioille, että Nigeria pärjää omalla väellään, mikä kenties luo valtiosta sisäänpäin kääntyneen kuvan ulkopuolisille, kansalaiset se saa tuntemaan itsensä arvokkaaksi voimavaraksi. Tämä tulkinta vahvistuu esimerkissä 11, jossa hallituksesta puhutaan erillisenä, yhteisöstä irrallisena toimijana, joka kuitenkin kokee tärkeimmäksi voimavarakseen kansalaisensa.

Yhteishenki-diskurssi on kenties helpoimmin näkyvä diskurssi tekstissä. Yhteishenki on vahvimmillaan silloin, kun tekstissä käytetään me-retoriikkaa, metaforia ja yksityiskohtaista kuvailua. Myös puhujan kategorisoidessaan itsensä osaksi vastaanottajien joukkoa yhteishenki on vahva. Kyberturvallisuuden kannalta yhteishengen luominen on olennaista vastaanottajien saamiseksi ”omalle puolelleen”, sillä kuten myöhemmissä diskursseissa tulemme huomaamaan, strategioissa on yhteisönkin kannalta joitain varsin ongelmallisia kohtia.

4.2.2 Kiiltokuva

Siinä missä yhteishenki-diskurssi kohdistetaan pääasiassa suoraan kansalaisille, *kiiltokuva*-diskurssin tarkoitus on näyttää valtion mahtia ulkopuolisille toimijoille. Kiiltokuva-diskurssilla tarkoitan sellaista puhetta, jossa valtio pyrkii luomaan itsestään mahdollisimman hyvän kuvan, eli se niin sanotusti ”kiillottaa ulkokuortaan”. Sillä, miltä maan ulkokuori näyttää, on iso rooli kyberturvallisuusstrategioissa. Kiiltokuva-diskurssissa maat korostavat ylivertaisuuttaan, kykyjään ja resurssejaan sekä rakentavat kilpailuasetelmia. Diskurssin sävy ei kuitenkaan ole uhkaava tai luo pelkoa, vaan siitä välittyy pikemminkin ylpeys ja ylemmyydentunto. Kiiltokuva-diskurssi ilmenee muun muassa lupauksilla tulevasta:

> (12) In the next few years, Nigeria will become a broadband economy where every individual and corporate citizens will have unhindered wholesome access to the internet. (Nigeria 2015: 1.4.3.)
>
> (13) Australia will raise the bar on cyber security performance. (Australia 2016: 7.)

Esimerkeistä käy ilmi, että kyseiset valtiot rakentavat kilpailuasetelmia. Esimerkissä 12 luvataan, että jokaisella kansalaisella on vapaa pääsy internetiin viiden vuoden kuluttua. Ottamatta kantaa siihen onko tämä konkreettisesti mahdollista toteuttaa, lupauksella pyritään luomaan kuva valtiosta teknologisen kehityksen kärjessä. Länsimaissa tämä ei välttämättä herätä suuriakaan tunteita, mutta Afrikassa, jossa ihmisten pääsy internetiin on huomattavasti rajallisempi, lupaus on houkutteleva kuvaus tulevaisuuden Nigeriasta ja voi siten herättää kilpailua valtioiden välille. Ääri-ilmaisujen käyttö (*every, unhindered*

wholesome) korostaa väitteen vakuuttavuutta. Myös esimerkissä 13 luodaan kilpailuasetelma. Vaikka kyseessä ei ole mikään selkeä tai näkyvä tavoite, väite kuitenkin viittaa tulevaan kyberturvallisuusrooliin, johon valtio pyrkii. Metaforan (*raise the bar*) käyttö tekee väitteestä kilpailuhenkisen, ja samalla valtio ilmoittaa olevansa varteenotettava vastustaja.

Kilpailuasetelman lisäksi kiiltokuva-diskurssi näkyy kansalaisista huolehtimisena:

(14) We will preserve and protect UK citizens' privacy. (Iso-Britannia 2016: 25.)

(15) We seek to be open and transparent with the American people and the world about our capabilities and plans. (Yhdysvallat 2015: esipuhe.)

(16) All intelligence collection will follow the law and guidance outlined in executive orders. (Yhdysvallat 2015: 24.)

Esimerkeissä 14–16 puhutaan yksityisyyden tärkeydestä ja suojaamisesta sekä lainmukaisesta toiminnasta. Valtiot esittäytyvät ikään kuin vanhemman roolissa vakuuttamalla muille, että ”lapset ovat turvassa isänsä kanssa”. Esimerkissä 14 luvataan säilyttää ja suojella isobritannialaisten yksityisyys. Vaikka kohdan puhujakategoria viittaisi siihen, että puhujana on kansalaisista muodostunut yhteisö, tällä kertaa äänessä on hallitus. Teksti on suunnattu muille kuin kansalaisille, sillä siinä puhutaan Iso-Britannian kansalaisista – ei esimerkiksi meidän kansalaisista*mme*, tai jos hallitus puhuisi kansalle, teidän turvallisuudestanne. Sen sijaan Iso-Britannian hallitus kertoo muulle maailmalle turvaavansa isobritannialaisten yksityisyyden. Esimerkki 15 toimii edellisen tavoin siten, että puhujakategorian ja kansalaisista puhumisen tavan suhde on samanlainen. Jälleen hallitus vakuuttaa olevansa läpinäkyvä toimistaan amerikkalaisille ja muulle maailmalle. Tekstikohta osoittaa, että avoimuus on hyve, johon tulee pyrkiä. Esimerkissä 16 korostetaan lisäksi, että valtio noudattaa lakia ja toimii oikein. Vakuuttavuutta lisää ääri-ilmaisu ”kaikki” (*all*). Valtiot siis lupaavat strategioissaan kehittää maansa kybertuvallisuutta sekä suojella kansalaisiaan. Sen lisäksi ne kehuvat itseään monilla yksityiskohtaisilla kuvauksilla merkityksestään kybermaailmalle:

(17) It has been established that we have the contemporary four (4) domains of land, Sea, Air and Space, Nigeria recognizes Cyberspace as the fifth (5th)

domain for driving critical national functions such as economic development, commerce and transactions, social interactions, medical and health, government operations, national security and defense. (Nigeria 2015: 1.4.6.)

(18) The Singapore Port and Changi Airport are among the world's busiest. The Port is a major transhipment hub that handles more than 130,000 vessels and 30 million containers each year. The Airport sees more than 340,000 flights, 55 million travellers, and 1.8 million tons of cargo annually. Our public transport system handles 7.5 million passenger trips per day. (Singapore 2016: 11.)

(19) Singapore is a major financial centre that processes massive amounts of transactions every second. For example, our local inter-bank payment systems handle millions of transactions totalling trillions of dollars annually. Many of our public services – government transactions, healthcare, emergency services – are increasingly reliant on complex underlying computer systems to serve millions of users each year. (Singapore 2016: 10.)

Kohta 17 on esimerkki siitä, että valtio on kiinni ajassaan ja ymmärtää teknologian mukanaan tuomat uudet toimintaympäristöt. Kybermaailmasta on tullut samanarvoinen muiden ympäristöjen – maa, meri, ilma ja avaruus – kanssa, ja sen toteaminen osoittaa valtiolta edistyksellisyyttä. Merkittävää tekstikohdassa on myös se, että puhujana toimii jälleen valtio ikään kuin se olisi itsenäinen toimija, vaikka todellisuudessa ihmiset kyseisen oivalluksen ovat tehneet. Kun maan nimeä käytetään tällä tavoin metonymiana[8] henkilölle, sillä on ikään kuin laillinen oikeus puhua koko maan puolesta (vrt. Pälli ym. 2009: 309).

Esimerkit 18 ja 19 ajavat keskenään samaa asiaa: mitä suurempaa osaa yhteiskunnan toiminnoista ylläpidetään kybermaailman avulla, sitä isompi merkitys on valtion kyberturvallisuudella. Asioiden määrällistäminen on tuolloin keino vakuuttaa vastaanottajat. Esimerkissä 18 korostetaankin sitä, kuinka valtavia liikennöinti- ja ihmismääriä valtio onnistuu käsittelemään vuosittain tai päivittäin. Kaikki toimii niin kuin pitääkin, mikä johtuu onnistuneesta kyberturvallisuudesta. Liikennöinti ja logistiikka vaativat sähköä, joka

[8] Metonymiaa käytetään korvaamaan sana jollakin samankaltaisella ilmaisulla. Sanojen välisen yhteyden tulee olla jo entuudestaan tunnettu. (Tieteen termipankki 2017.) Esimerkissä 17 strategisen havainnon tehneet ihmiset on korvattu valtion nimellä.

ylläpitää lukuisia tietokonejärjestelmiä. Ne taas huolehtivat siitä, että laitteet ja asiat liikkuvat oikeassa järjestyksessä oikeaan aikaan eikä satu onnettomuuksia. Esimerkki 19 kuvaa samaa asiaa, mutta ihmisten fyysisen turvallisuuden sijasta siinä on kyse talouden turvallisuudesta ja yksityisyydestä. Digitaalisessa muodossa oleva raha pitää suojata vahvasti hyökkääjiä vastaan. Myös arkaluontoista dataa kerätään yhä enenevissä määrin, joten sekin pitää pystyä turvaamaan. Kun valtio onnistuu toteuttamaan kyberturvallisuutta niin, etteivät riskialttiit kohteet kärsi, se haluaa ilman muuta kertoa onnistumisistaan muille.

Toisinaan kehumista esiintyy myös ylemmyydentunnon muodossa. Kohdassa 20 valtio – todennäköisesti omasta mielestään oikeutetusti – puhuu itsestään huomattavasti kyberturvallisuusasioissa kehittyneempänä kuin muut maat. Esimerkin tarkoituksena voisi olla välittää isällistä roolia aikaisempien esimerkkien 14–16 tavoin, mutta koska tekstissä on eroteltu isobritannialaiset ”meistä”, se on suunnattu valtion ulkopuolelle. Metaforana ”vain kourallinen” on vahva ja konkreettinen ilmaisu siitä, kuinka vähäinen määrä maita edes nähdään potentiaalisina kilpakumppaneina. Valtio tietää, että se on kybermaailmassa merkittävä toimija, eikä se pelkää tuoda sitä esille.

(20) Only a handful of states have the technical capabilities to pose a serious threat to the UK’s overall security and prosperity. (Iso-Britannia 2016: 18.)

(21) Digital technology works because it is open, and that openness brings with it risk. What we can do is reduce the threat to a level that ensures we remain at the vanguard of the digital revolution. (Iso-Britannia 2016: 6.)

Esimerkin 21 puhujakategoria on mielenkiintoinen. Puhujana voisi olla sekä hallitus että kansalaisista muodostuva yhteisö. Lopulta sillä ei kuitenkaan ole suurta merkitystä, sillä tärkeämpää tässä kohdassa on huomata puhujan tavoite: ”laskea uhka sellaiselle tasolle, että se varmasti pitää meidät digitaalisen vallankumouksen etujoukoissa”. Toisin sanoen puhujan mielestä sillä on valta vaikuttaa uhkaan valinnoillaan ja resursseillaan. Puhuja näkee olevansa jo nyt ”digitaalisen vallankumouksen etujoukoissa” ja haluaa säilyttää paikkansa siellä. Esimerkki 21 on siis viesti muille valtioille, että Iso-Britannialla on kybermaailmassa valtaa tehdä asioita melko vapaasti.

Kiiltokuva-diskurssi esiintyy strategioissa lupauksina ja vastuullisuutena, mutta myös itsekehuna ja ylemmyydentuntona. Näkyvimpiä retorisia keinoja tässä diskurssissa ovat puhujakategoria, määrällistäminen ja metaforat. Kiiltokuva-diskurssissa kerrotaan paljon omasta osaamisesta ja tulevaisuudensuunnitelmista, mistä voisi päätellä, että valtioiden tavoitteena on löytää muista valtioista uusia yhteistyökumppaneita. Toki omaa osaamista markkinoidaan myös kilpailumielessä, joten kehua vain sen itsensä vuoksi esiintyy myös paljon. Kiiltokuva-diskurssi on kuitenkin valtioille hyödyllinen, koska jos muut haluavat solmia kumppanuuksia tai muutoin vaikuttuvat lukemastaan, sillä voi olla isokin merkitys valtioiden talouskasvulle.

4.2.3 Varallisuus

Yksi kyberturvallisuusstrategioiden isoimmista teemoista on varallisuus. Kybertoimintaympäristön mahdollisuudet voivat kasvattaa valtion taloutta merkittävästi, mutta toisaalta kyberrikollisuus on monen miljardin bisnes vuosittain. *Varallisuus*-diskurssi onkin pääpiirteissään jakautunut kahtia: toisaalta kybertoimintaympäristöä halutaan hyödyntää, mutta toisaalta pelätään, että varallisuus menetetään kybermaailman vuoksi. Tulevaisuuteen positiivisesti suhtautuvissa tekstikohdissa pyritään herättämään kansalaisten luottamusta, jotta he hyväksyisivät kyberturvallisuusstrategian toimeenpanon:

> (22) The Government will spare no effort in safeguarding its systems and networks. The Government has undertaken, in this current term, to work towards a goal of setting aside 8 per cent of its ICT expenditure on cybersecurity. (Singapore 2016: 20.)

Esimerkissä 22 hallitus lupaa tekevänsä kaikkensa, jotta sen järjestelmät ja verkostot olisivat turvallisia. Todisteeksi tästä hallitus pohtii, kuinka se voisi säästää lisää rahaa kyberturvallisuuden kehittämiseksi. Varallisuus-diskurssille on tyypillistä, että siinä esitetään paljon lukuja eli määrällistetään asioita. Lisäksi puhujakategorialla on iso rooli. Kyseisessä esimerkissä puhuu hallitus, jonka kohderyhmänä ovat kansalaiset. Luottamuksen kannalta sillä on suuri merkitys, että hallitus kirjaimellisesti lupaa sitoutuvansa säästämään ja miettimään talouttaan uudelleen. Jos puhujaksi olisi merkitty vaikkapa valtion

nimi, lupaus ei olisi yhtä uskottava. Hallitus on yksilöidympi ja konkreettisempi puhuja kuin valtio.

Kybertoimintaympäristön mahdollisuuksia esitetään konkretian kautta. Tuolloin kansalaisille kerrotaan numeroin ja yksityiskohdin, kuinka varallisuutta voidaan lisätä:

> (23) With skilled professionals, technologically-advanced companies and strong research collaborations, Singapore can be at the global forefront of cybersecurity innovation and create economic opportunities for Singaporeans and the industry. (Singapore 2016: 5.)
>
> (24) Within the U.S. economy alone, anywhere from three to 13 percent of business sector value-added is derived from Internet-related businesses. Over the last ten years Internet access increased by over two billion people across the globe. (Yhdysvallat 2015: 1.)
>
> (25) Ensuring the CNI [critical national infrastructure] is secure and resilient against cyber attack will be a priority for the Government. -- They include the jewels in our economic crown – the UK's most successful companies and also those that hold our future economic strength in the value of their research and intellectual property. (Iso-Britannia 2016: 40.)

Esimerkin 23 mukaan teknologia-alan kehittäminen nostaisi valtion kyberasioiden kärkimaaksi ja toisi uusia työmahdollisuuksia kansalaisille. Kyseessä ei kuitenkaan ole lupaus, vaan pikemminkin tavoite. Sitä ei perustella laskelmilla, vaan konsensuksella, jolloin alan ammattilaiset, yritykset ja tutkijat ovat avainasemassa. Sen sijaan esimerkissä 24 kansalaisia vakuutetaan määrällistämisellä. Internet-bisneksen kasvu kuvataan prosentuaalisesti ja verkon kehitystahti käyttäjämäärän kasvulla. Kyseisessä tekstikohdassa avainasemassa on ilmaisu ”yksistään” (*alone*), sillä se kertoo, että kyseessä on vain yksi esimerkki ja että todellisuudessa kasvu on vieläkin nopeampaa. Tämä tekee muistakin maista tavoiteltavia markkina-alueita. Esimerkissä 25 kuvataan hieman tarkemmin, keneltä kasvua odotetaan. Kriittiseen infrastruktuuriin sisällytetään kyseisessä valtiossa myös talouden tärkeimmät yritykset. Hallitukselle ne ovat prioriteettilistan kärjessä, sillä ne tulevat olemaan vaikutusvaltaisia myös tulevaisuudessa. Kansalaisille kyseisten yritysten tärkeyttä korostetaan metaforalla ja me-retoriikalla. ”Talouden kruununjalokivet” on vahva ilmaus

varsinkin Iso-Britanniassa, jossa todelliset kuningattaren kruununjalokivet ovat kansallinen aarre. Kun yrityksiä verrataan näin vahvaan kulttuuriseen esineistöön, syntyy luottamus, jota me-retoriikka vain vahvistaa.

> (26) Eight in ten Australians access the Internet daily. -- In 2014 alone, the Internet vase economy contributed $79 billion to the Australian economy (or 5.1 per cent of GDP). This amount could grow to $139 billion annually (7.3 per cent of GDP). (Australia 2016: 14.)

Vieläkin konkreettisemmaksi talouskasvu ja varallisuus tulevat, kun esitetään todellisia summia ja aikamääreitä. Esimerkissä 26 määrällistämistä on käytetty useita kertoja: kahdeksalla kymmenestä australialaisesta on pääsy nettiin päivittäin, ja vuonna 2014 internet-bisnes oli laajuudeltaan 79 miljardia dollaria. Kasvupotentiaaliksi on laskettu vielä 139 miljardia dollaria joka vuosi. Myös internetbisneksen osuus bruttokansantuotteesta on ilmoitettu. Päällisin puolin luvut ovat vakuuttavia. Määrällistäminen on kuitenkin vahvasti subjektiivinen vakuuttamisen keino, sillä puhuja on itse päättänyt, millaisia lukuja tekstissä on ilmoitettu ja mihin niitä verrataan. Esimerkiksi internet-bisneksen osuus bruttokansantuotteesta ei vielä kerro mitään, ellei vastaanottaja tiedä, mikä todella on iso prosentti bruttokansantuotteesta puhuttaessa. Kahdeksan kymmenestä kuulostaa murtolukuna isolta, mutta prosenteiksi muutettuna se on 80 prosenttia. Globaalisti luku on korkea, kun mitataan pääsyä internetiin, mutta yltääkö se esimerkiksi länsimaissa – joihin Australiakin voidaan lukea – keskitasoa korkeammalle? Toisin sanoen olennaista on, mitä lukujen perusteella voidaan todella sanoa varallisuudesta.

> (27) The S$130 million NCR [national cyber security R&D -program] was launched in 2013 by the National Research Foundation (NRF). This was further topped up in 2016 by an additional S$60 million as part of the Research, Innovation and Enterprise 2020 Plan (RIE 2020). (Singapore 2016: 40.)

Myös esimerkissä 27 käytetään määrällistämistä vakuuttamaan lukija. Lisäksi tekstissä viitataan tutkimus- ja kehitysohjelmiin ja rahastoon, mikä tuo lisäarvoa luvuille. Isojen tukijoiden mainitseminen nimeltä luo sellaisen kuvan, että kybermaailmaa todella halu-

taan kasvattaa ja kehittää, ja että hallitus on konkreettisesti siinä mukana. Tämän tekstikohdan ongelma on silti sama kuin edellisen esimerkin: onko rahasumma kyseisen valtion budjetissa iso tai riittävä siihen, että kehitystyö tuottaa tulosta.

Varallisuus-diskurssia käytetään kyberturvallisuusstrategioissa myös huomattavasti negatiivisemmassa mielessä. Tuolloin pelkona on varallisuuden menettäminen. Kuten edellisissä esimerkeissä, myös menettämisen pelon teemassa varallisuudessa puhutaan numeroin ja rahayksiköin:

> (28) Cybercrime is estimated to cost Australians over $1 billion each year. (Australia 2016: 15.)
>
> (29) Recently, a total of $388billion USD was estimated as the approximate total financial loss to cybercrime in more 24 countries in the last six years. The global black market in marijuana, cocaine and heroin combined ($288bn) and approaching the value of all global drug trafficking ($411bn). At $388bn, cybercrime is more than 100 times the annual expenditure of UNICEF ($3.65 billion). (Nigeria 2015: 2.2.6.)

Esimerkissä 28 kybertoimintaympäristöä lähestytään siitä näkökulmasta, kuinka paljon tappiota ja menetyksiä se voi tuoda mukanaan. Kyberrikollisuuden hinta on esimerkin mukaan miljardi dollaria joka vuosi. Kuten aikaisemmin olen todennut, kyberrikollisuuden todellisia kustannuksia on vaikea määrittää ja arvioita liikkuu aina miljardista satoihin miljardeihin. Arvio on siihen nähden melko alhainen. Ääri-ilmaisu ”yli” (*over*) viittaa siihen, että summa voisi olla enemmänkin. Tekstissä sanotaan myös, että ”hinta on kansalaisille” (*Australians*), eikä esimerkiksi ”valtiolle”, mikä antaa ymmärtää, että asian halutaan koskettavan jokaista yksittäistä australialaista. Näin luodaan myös pelkoa siitä, että oma varallisuus voi huveta.

Esimerkin 29 mukaan kyberrikollisuuden hinta arvioidaan epämääräisemmin: summaksi on ilmoitettu 388 miljardia Yhdysvaltojen dollaria 24 maassa viimeisen kuuden vuoden aikana. Maakohtaisesti tämä voi tarkoittaa mitä tahansa. Sen lisäksi kyberrikollisuutta verrataan huumekauppaan, jonka summat liikkuvat 100 miljardia dollaria kyberrikollisuusarvion ylä- ja alapuolella. Lopuksi kyberrikollisuutta verrataan vielä hyväntekeväi-

syysjärjestö UNICEF:in vuotuisiin menoihin. Vaikka määrällistämistä onkin tässä esimerkissä käytetty paljon ja siten pyritty vakuuttamaan lukija, antaa teksti myös ristiriitaisen kuvan siitä, onko kyberrikollisuudessa liikkuvat rahat isoja vai eivät. Kyberrikollisuutta verrataan ääriesimerkkeihin – hyväntekeväisyyteen ja huumekauppaan – joten todennäköisemmin tarkoituksena on herättää lukijassa tunteita. Huumekauppaa stereotyyppisesti pidetään huonona asiana, kun taas hyväntekeväisyyttä hyvänä. Kun kansalainen kokee, että kyberrikollisuus tuo maalle yhtä suuret tappiot kuin huumekauppa, hän todennäköisesti hyväksyy monet strategian ehdotukset helpommin.

Varallisuuden menettämisen pelko esitetään myös suoranaisten uhkakuvien kautta. Esimerkki 30 perustelee paljon toistolla ja vaihtoehdottomuuspuheella sitä, miksi teknologia-ala ei ole kehittynyt odotetusti. Toiston merkitys on tässä tapauksessa painottaa asiaa niin, että se todella vakuuttaa lukijan. Markkinat toimivat ikään kuin itsestään ihmisistä irrallaan, minkä vuoksi myös kyberuhkien hallinnointi kärsii. Yritykset eivät panosta kyberturvallisuuteen tarpeeksi ja karkottavat sijoittajat. Myös valmistuvia opiskelijoita ja asiantuntijoita on liian vähän. Esimerkkikohta ikään kuin oikeuttaa sitä, minkä vuoksi hallituksen pitäisi puuttua kybermaailman toimintaan ja kehittämiseen. Näkymät eivät kyseisen tekstin perusteella ole kovin hyvät, ja jos samanlainen meno jatkuu, ne eivät siitä parane. Strategian onkin tarkoitus olla vastaus varallisuuden kasvattamiseen sen menettämisen sijasta.

> (30) Too many networks, including in critical sectors, are still insecure. The market is not valuing, and therefore not managing, cyber risk correctly. Too many organisations are still suffering breaches at even the most basic level. Too few investors are willing to risk supporting entrepreneurs in the sector. Too few graduates and others with the right skills are emerging from the education and training system. (Iso-Britannia 2016: 27.)
>
> (31) The Australian Cyber Security Centre Threat Report 2015 says cyber threat is undeniable, unrelenting and continues to grow. If an organisation is connected to the Internet, it is vulnerable to compromise – and the malicious cyber activities in the public eye are just the tip of the iceberg. (Australia 2016: 15.)

Esimerkissä 31 luodaan pelkokuvia yrityksille niiden kyberhyökkäysalttiudesta. Yritykset ovat elintärkeitä valtiontaloudelle, minkä vuoksi juuri niille suunnattuna uhkakuva

linkittyy myös talouteen ja varallisuuteen. Metaforien käyttö antaa esimerkille enemmän vakuuttavuutta, sillä se luo konnotaation suunnattomasta määrästä kyberiskuja, joista valtaosasta ei edes tiedetä mitään ja joista tiedetyt ovat vain ”jäävuoren huippu” (*the tip of the iceberg*). Lisäksi väite nojaa tutkimustuloksiin, mikä tekee siitä entistä vakuuttavamman – joskin vakuuttavuutta voi hieman laskea se, että kyseessä on valtion hallinnon alainen organisaatio eikä esimerkiksi täysin hallinnon ulkopuolinen tutkimus.

Kuten edellä olen esittänyt, varallisuus-diskurssi jakautuu kyberturvallisuusstrategioissa kahteen pääteemaan. Esimerkeissä varallisuuden tavoittelusta rakennetaan vastaanottajan luottamusta konkreettisilla esimerkeillä, yksityiskohdilla, rahasummilla ja aikamääreillä. Sen sijaan varallisuuden menettämisen pelko ilmenee vertailuna, ristiriitoina ja uhkakuvina. Vakuuttava puhetapa rakennetaan määrällistämällä, vaihtoehdottomuuspuheella ja puhujakategorialla. Myös muita keinoja käytetään pienimuotoisesti, kuten toistoa ja ääri-ilmaisuja. Varallisuus-diskurssille on ominaista, että vastaanottajana ovat valtion kansalaiset ja puhujana hallitus. Uhkakuvista huolimatta tekstin sävy on tiedottavaa ja lukijaa ”herättelevää”, mikä eroaa huomattavasti pakotetun kontrollin -diskurssista, jota käsittelen seuraavaksi.

4.2.4 Pakotettu kontrolli

Jos varallisuus-diskurssia havainnoivat uhkakuvat, *pakotetun kontrollin* diskurssissa ne on viety kenties vieläkin pidemmälle. Pakotetulla kontrollilla tarkoitan sitä, että valtio pyrkii tietoisesti kontrolloimaan kansalaistensa käyttäytymistä oman etunsa mukaisesti. Puhe on siis ensisijaisesti suunnattu valtion sisäisille toimijoille. Diskurssissa lukija saatetaan tietoiseksi kybermaailman tuomista ongelmista ja vakuutetaan siitä, että toisenlainen käytös poistaisi ongelmat. Diskurssia ilmennetään muun muassa vetoamisella, uhkailulla ja vaihtoehtoja tarjoamalla. Myös esimerkkejä ja tarinankerrontaa käytetään lukijan vakuuttamiseksi:

> (32) The recent revelations of American whistle-blower Edward Snowden has significantly raised awareness of the need for nations to put in place appropriate measures to protect the personal information, and privacy of its citizens. -- The revelations also identified the need to protect and secure

communications of not only high ranking government and high profile individuals from mobile phone tapping but also ordinary individuals from their everyday non-criminal conversations being intercepted and analysed by law enforcement agencies, organisations and foreign countries. (Nigeria 2015: 4.4.1.)

(33) As the Snowden disclosures demonstrate, often the most damaging risk to government or business online security is not 'malware' but 'warmware': the ability of a trusted insider to cause massive disruption to a network or to use legitimate access to obtain classifies material and then illegally disclose it. (Australia: 3.)

(34) As one example, in November, 2014, likely in retaliation for the planned release of a satirical film, North Korea conducted a cyberattack against Sony Pictures Entertainment, rendering thousands of Sony computers inoperable and breaching Sony's confidential business information. In addition to the destructive nature of the attacks, North Korea stole digital copies of a number of unreleased movies, as well as thousands of documents containing sensitive data regarding celebrities, Sony employees, and Sony's business operations. (Yhdysvallat 2015: 2.)

Esimerkissä 32 viitataan yhdysvaltalaisen Edward Snowdenin paljastuksiin maansa tiedustelupalvelujen toiminnasta. Snowdenista puhutaan melko negatiivissävytteisellä sanalla *whistle-blower*, mistä voi päätellä, että Snowdenin tekoja halveksutaan ja ne tuomitaan. Tekstissä kerrotaan myös tarkemmin tietovuodon seurauksista eli siitä, että ihmiset ja hallitukset tiedostavat nyt paremmin, kuka heitä kuuntelee ja miten. Lukija halutaan saada ymmärtämään, että tietoturvasta huolehtiminen nostaa yksityisyydensuojaa.

Samalla tavoin esimerkissä 33 ei varsinaisesti tuomita Snowdenia itseään, vaan hänen laiton tekonsa. Tapahtuma halutaan nostaa esiin, jotta kansalaisille olisi selvää, millaiset seuraukset vastaavasta toiminnasta koituisi heille itselleen. Ottamatta kantaa itse Snowdenin tapaukseen tekstissä todetaan, että ihminen on usein kyberhyökkäysten pahin aiheuttaja, ja tuomitaan salaiseksi luokitellun tiedon vuotaminen laittomaksi. Snowdenin tapaus paljasti kansalaisille huomattavan laajasti sen, kuinka paljon Yhdysvaltojen hallitus kuuntelee ja hallitsee maan tietoverkkoa. Tapahtuma sai ihmiset varpailleen ja he tulivat tietoisemmiksi omasta toiminnastaan verkossa. Pelkkä tieto siitä, että joku jossakin saattaa kuulla tai lukea dataa, jota verkon kautta lähetetään, saa ihmisen tarkkailemaan itse itseään, kuten Foucault'n valtateoria osoittaa (ks. luku 3.1). Myös esimerkki 34 on

yksityiskohtainen kuvaus siitä, millaisia ongelmia kybermaailmasta sen käyttäjille koituu. Tässä tekstikohdassa uhka tulee valtion ulkopuolelta. Tarinana sillä on kuitenkin samanlainen merkitys kuin sitä edeltävillä esimerkeillä, joiden tavoitteena on kontrolloida kansalaisia heidän kyberturvallisuusasioissa sekä toisaalta varoittaa seurauksista, joita heihin itseensä voisi kohdistua, jos he toimisivat samoin. On kyseessä sitten tietojen vuotaminen ulkopuolelle tai arkaluontoisen datan lataaminen verkkoon, vuoto on aina mahdollinen.

Vastaanottajille ei kuitenkaan tehdä itsestään selväksi sitä, kuinka vahvasti valtion on tarkoitus heidän toimintaansa kontrolloida. Asiat esitetään tarjoamalla vaihtoehtoja:

> (35) The level to which all citizens of the country become aware of, and educated about cybersecurity issues will to a large extent determine how strong the cybersecurity efforts of the nation will be. As security is only as strong as its weakest link. (Nigeria 2015: 7.3.)
>
> (36) Consumers will be empowered to choose products and services that have built-in security as a default setting. Individuals can switch off these settings if they choose to do so but those consumers who wish to engage in cyberspace in the most secure way will be automatically protected. (Iso-Britannia 2016: 36.)

Molemmissa esimerkeissä vaihtoehdot ovat kuitenkin näennäisiä. Esimerkissä 35 kyberturvallisuustason sanotaan riippuvan siitä, kuinka tietoisia ja koulutettuja käyttäjät ovat. Mitä enemmän heillä on osaamista, sitä enemmän he myös panostavat kyberturvallisuuteen. Lisäksi esimerkissä todetaan, että ”turvallisuus on vain niin vahvaa kuin sen heikoin lenkki”. Kansalainen ei kuitenkaan välttämättä voi itse vaikuttaa siihen, kuinka paljon hän asioista tietää tai mitä hän voi opiskella. Jos valtio ei tarjoa mahdollisuuksia kouluttautumiseen, kuinka kukaan voi kehittyä? Toisin sanoen valtio ikään kuin siirtää vastuun kyberturvallisuudesta vastaanottajalle ja pyrkii siten muokkaamaan tämän käytöstä kenties kyberturvallisuudelle vastaanottavaisemmaksi.

Esimerkki 36 ei ole yhtä hienovarainen, vaan siinä hallitus ilmaisee suoraan käyttäjän vastuun kyberturvallisuusasetusten käyttämisessä. Tekstin mukaan kuluttajia rohkaistaan valitsemaan palveluita, joissa turvallisuus on kytketty oletuksena päälle. Niitä kuluttajia,

jotka eivät asetuksiin koske, suojellaan automaattisesti. Kuluttajalle jätetään siis kaksi vaihtoehtoa: käyttää yritysten tai hallituksen hyväksymiä tietoturva-asetuksia tai suojautua itse. Mielenkiintoista on pohtia, kuinka monella on mahdollisuus tai osaamista toteuttaa itse esimerkiksi kyberturvallisuutensa. Jos kykyä ei ole, miksi käyttäjä ei ottaisi automaattista turvaa? Kummassakaan esimerkissä ei siis ole kyseessä todellinen vaihtoehtojen tarjoaminen, vaan tarkoituksena on ohjata vastaanottaja toimimaan hallituksen oman toiveen mukaisesti.

Edellä esitettyjen yksityiskohtaisten esimerkkien tai vaihtoehtojen lisäksi hallitus käyttää kontrollointikeinonaan vetoamista ja uhkailua. Vetoavassa kontrolloinnissa käytetään paljon metaforia vakuuttamisen keinoina:

> (38) The Government cannot do it alone. Businesses are responsible for protecting customers' personal data. Individuals need to practise good cyber hygiene to keep personal devices and data safe. If we each do our part to use our systems and devices responsibly, then collectively we can help to protect Singapore's cyberspace. (Singapore 2016: 1.)
>
> (39) The increasing number of infected machines spewing malicious traffic into the Internet has made cyberspace less safe for everyone. Just as we would stop people who eject sewage into clean water pipes, we will also have to block users who may be unwittingly polluting the Internet pipeline and alert them on measures for cleaning up their machines. (Singapore 2016: 31.)

Esimerkissä 38 vastaanottajalle luodaan kuva, että hallitus ei pärjää yksin ja tarvitsee siksi kansalaistensa apua. Jokainen kansalainen halutaan värvätä toimintaan mukaan. Tekstissä verrataan turvallista verkon käyttöä ”kyber hygieniaan” (*cyber hygiene*), millä on tarkoitus luoda selkeämpi kuva vastaanottajille, millaisia toimenpiteitä kyberturvallisuus pitää sisällään. Tätä samaa metaforaa jatketaan esimerkissä 39, joskin vielä värikkäämmin. Kyberhyökkäykselle altistuneita koneita kutsutaan ”saastuneiksi” (*infected*). Verkon ”likaamista” (*polluting*) verrataan siihen, että ihmiset laskevat jätevetensä puhtaisiin vesiputkiin – samalla tavoin huonolla kyberhygienialla ihmiset saastuttavat ”internetputkistoa” (*Internet pipeline*). Esimerkeissä siis vedotaan yhteisen hyvän puolesta taistelemiseen arkipäiväisillä metaforilla, joihin jokainen kansalainen voi varmasti samaistua. Samaistumisen myötä myös ihmisten käytös muuttuu halutunlaiseksi.

Jos vetoavaa kontrollointitapaa ei koeta riittävän tehokkaana, valtio voi esittää uhkauksia:

> (40) Recognizing that cybercrime can impact both private and public sector environments, the legal strategy is to adopt processes for both public and private sector collaboration in combating cybercrime. As an example relationships between Communication Service Providers in assisting law enforcement agencies in preserving communications data for specified periods as dictated by the Data Retention legislations will be encouraged and forged. (Nigeria 2015: 4.3.4.)
>
> (41) For the CNI, they must do this with government bodies and regulators so we can be confident that cyber risk is being properly managed and – if it is not – intervene in the interests of national security. The Government will, therefore, understand the level of cyber security across our CNI and have measures in place to intervene where necessary to drive improvements that are in the national interest. (Iso-Britannia 2016: 41.)

Molemmissa esimerkeissä hallitus ilmoittaa, että jos sopivia toimintatapoja kybermaailman turvaamiseen ei löydy tai niitä ei noudateta, sillä on oikeus pakottaa kansalaiset ja yritykset muuttamaan toimintaansa. Esimerkissä 40 uhkaus esitetään viestintäpalveluiden tarjoajille, joiden on autettava lainvalvojia säilyttämään dataa. Uhkausta tosin lievennetään sanalla ”rohkaista” (*encouraged*). Sitä seuraava ilmaisu ”pakottaa” (*forged*) ei kuitenkaan jätä epäselväksi, mitä hallitus todella haluaa. Esimerkki 41 on kohdistettu kriittisen infrastruktuurin yrityksille, joiden tulisi tehdä yhteistyötä valtion organisaatioiden kanssa kyberturvallisuuden takaamiseksi. Jos he eivät näin tee, hallituksella on oikeus sekaantua yrityksen toimintaan kansallisen turvallisuuden nimissä. Kummassakin esimerkissä on jätetty hieman epäselväksi se, mitä tarkoitetaan oikeanlaisella yhteistyöllä ja toimintatavoilla. Kun asia ilmaistaan suurpiirteisesti, tarkoituksena on hämärtää rajaa, jonka puitteissa hallitus voi valtaansa käyttää (ks. Pälli 2009: 310).

Viimeinen pakotettu kontrolli -diskurssin muoto on puhe yksityisyydestä. Kun kansalaiset tietävät tarpeeksi tai liikaa siitä, kuinka valtio tarkkailee tieto- ja viestiliikennettä, he alkavat salata viestinsä. Tämä asettaa hallituksen ongelmalliseen tilanteeseen. Halutessaan suojella ja turvata viestiliikenteensä hallitus kokee, että sillä on kansallisen turvallisuuden nimissä oikeus tarkkailla verkkoliikennettä.

(42) The technical environment is becoming more complex. -- For example, as encryption technology becomes cheaper and more widely available, there is an opportunity for all users to access this technology to secure information and improve their cyber security. However, there is also a growing trend for groups and individuals to use encryption to hide illegal activity and motivate others to join their cause. -- The Government supports the use of encryption to protect sensitive personal, commercial and government information. However, encryption presents challenges for Australian law enforcement and security agencies in continuing to access data essential for investigations to keep all Australians safe and secure. Government agencies are working to address these challenges. (Australia 2016: 33.)

(43) The abuse of cyberspace infringes on our privacy and our liberty. It is incumbent on the federal government to avoid such abuse and infringement. Cybersecurity and personal privacy need not be opposing goals. Cyberspace security programs must strengthen, not weaken, such protections. Accordingly, care must be taken to respect privacy interests and other civil liberties. (Yhdysvallat 2015: 14–15.)

Esimerkissä 42 hallitus ilmoittaa tukevansa salaustekniikoiden käyttämistä arkaluontoisen tiedon piilottamiseksi. Sen sijaan lainvalvojat ja tiedustelupalvelut ovat jatkuvasti haasteen edessä, kun ne pyrkivät pääsemään käsiksi olennaiseksi oletettuun dataan. Hallitus on tässä kohdassa erotettu lainvalvojista ja tiedustelupalveluista ja asemoitu ikään kuin kansalaisten rinnalle: kansalaiset ja hallitus yhdessä haluavat tukea salattua viestiliikennettä. Ilmaisemalla asemansa näin hallitus pyrkii estämään mahdollisen vastarinnan, joka voisi kansalaisten keskuudessa liian suorasukaisen puheen perusteella nousta.

Kontrolli näkyy siinä, että kansalaiset halutaan saada tuntemaan myötätuntoa hallitusta kohtaan. Olemalla yhtä kansalaisten kanssa hallitus pyrkii luomaan yhtenäisyyden tunnetta ja saavuttamaan kansalaisten luottamuksen, jolloin satunnaiset salattujen viestin tarkistamiset eivät olisi niin iso ongelma. Lainvalvojat ja tiedustelupalvelu kuitenkin toimivat jo hallituksen alaisuudessa, eikä hallitus voi irrottaa itseään niistä. Kansalaisia siis todennäköisesti kuunnellaan joka tapauksessa – suostuivat he siihen tai eivät. Esimerkki 43 vakuuttaa, että yksityisyys on jokaisen oikeus ja hallituksella on lain tuoma velvollisuus taata se. Samalla kun kyberturvallisuutta kehitetään, tulee myös kansalaisten oikeuksia kunnioittaa. Tässä tekstikohdassa on olennaista se, että kyseessä on Yhdysvaltojen kyberturvallisuusstrategia, ja Yhdysvaltojen tiedetään kuuntelevan maailman valtioista

laaja-alaisimmin sekä omia kansalaisiaan että muuta maailmaa. Esimerkissä siis vakuutetaan, että näin ei enää jatkossa toimittaisi. Vastaanottaja halutaan vakuuttaa ja saada uskomaan, että valtio on muuttanut tapansa ja että jatkossa hänen yksityisyytensä on turvattu. Kyseenalaista on, ettei tiedetä, onko muutoksia todella tapahtunut vai onko kyseinen kohta ainoastaan keino rauhoitella kansaa.

Pakotetun kontrollin diskurssilla on strategioissa monta ilmenemismuotoa: todelliset esimerkit, vaihtoehtojen tarjoaminen, vetoaminen, uhkailu ja yksityisyys. Diskurssi vakuuttaa lukijansa erityisesti metaforien ja konsensuksen kautta pyrkimällä rakentamaan luottamusta ja uskoa siihen, että valtio toimii oikein. Silti asiat jätetään toisinaan avoimiksi, jotta hallitus ei rajoittaisi itseään liikaa. Vaikka kontrollointi onkin rakennettu melko hienovaraisesti, se on tietoista. Tämä herättää kysymyksiä siitä, mitkä ovat valtion todelliset aikomukset. Joitakin niistä ne kertovat suoraan oikeuttamalla itse oman valtansa.

4.2.5 Itseoikeuttaminen

Itseoikeuttamisen diskurssi on pienempi kuin muut edellä käsittelemäni. Sitä kuitenkin esiintyy vain sellaisilla valtioilla, joiden maailmanpoliittinen vaikutus on suuri. Siksi diskurssi on olennainen myös tämän tutkimuksen kannalta. Itseoikeuttamisen diskurssi tarkoittaa sitä, että valtio kokee voivansa tehdä päätöksiä itse huolimatta siitä, onko se onnistunut vakuuttamaan muut kansalaiset tai valtiot vai ei. Kyseistä diskurssia käyttävät analysoimistani valtioista Yhdysvallat ja Iso-Britannia. Itseoikeuttamista perustellaan muun muassa hyödyllä:

> (44) For many, industry will be designing and leading implementation, with the Government's critical contribution being expert support, advice and thought-leadership. (Iso-Britannia 2016: 34.)
>
> (45) On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques, and procedures. Attrib-

> ution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack. (Yhdysvallat 2015: 11–12.)

Esimerkissä 44 hallituksen osallistuminen teknologia-alan kehittämiseen nähdään oikeutettuna, sillä hallitus tuo valtion varat ja resurssit mukanaan innovointiin. Hallituksesta on siis hyötyä yrityksille. Olennaista itseoikeuttamisen kannalta tässä kohdassa on se, että valtio nimittää itsensä mielipidejohtajaksi. Sen kontribuutio kehittämiselle on kriittinen eli hallitus saa kommentoida kehitystyötä vahvoinkin sanankäänteín. Hallitus ikään kuin legitimoi asemansa teknologia-alan kehitysjohtajana, vaikka moni näkisi sen olevan yksityisten toimijoiden vastuulla.

Seuraava tekstikohta, esimerkki 45, liittyy tiedusteluun. Tiedusteluun käytetyt investoinnit vähentävät anonyymiutta ja siten helpottavat tunnistamaan hyökkääjät iskujen takana. Kun iskun tekijät voidaan määrittää ja asettaa syytteeseen, myös vastavakoilu ja vastaiskut ovat oikeutettuja. Todellisuudessa hallitus tekee tätä jo, eikä ole siihen aikaisemmin pyytänyt lupaa kansalaisilta. Teksti on pikemminkin tiedottavaa: hallitus on aikaisemmin jo tehnyt näin, mistä on seurannut asia *x*, jonka perusteella hallitus saa käyttää vastatiedustelua ja -hyökkäyksiä varsin vapaasti. Molemmissa esimerkeissä hallitus kyllä perustelee toimintansa vakuuttamisen keinoilla ja legitimoimalla, mutta toisaalta asiat ovat sellaisia, joille ei enää voi juuri mitään.

> (46) If we can succeed in mainstreaming cyber security across all parts of our society, it could mean that Government itself can step back from such a prominent role, allowing the market and the technology to drive the evolution of cyber security across the economy and society. (Iso-Britannia 2016: 71.)

> (47) There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military- related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests. (Yhdysvallat 2015: 5.)

Toisaalta hallitus voi luo hypoteettista kuvaa todellisuudesta, minkä seurauksena kyberturvallisuus voi kehittyä tiettyyn suuntaan. Esimerkissä 46 hallitus lupaa, että jos kyberturvallisuus saadaan valtavirtaiseksi yhteiskunnassa, hallitus voi siirtyä syrjään hallitsevasta roolista ja antaa markkinoiden kehittää kyberturvallisuutta vapaasti. Ilmaus ”se voisi tarkoittaa” (*it could mean*) ei kuitenkaan takaa mitään, vaan jättää tulevaisuuden avoimeksi. Pikemminkin esimerkki luo yrityksille houkuttelevan kuvan tulevasta, mikä on todennäköisesti hallituksen tavoite. Itseoikeutettu rooli näkyy siten, että valtio tietää olevansa dominoivassa asemassa, josta sillä on valta pitää kiinni tai luopua. Jos valtio siis menettäisi valtansa kyberturvallisuusasioissa, se olisi hallituksen oma valinta.

Esimerkin 47 tulevaisuuskuva on yhtä hienovarainen ja avoin kuin edellinenkin. Vaikka asia esitetäänkin esimerkein ja hypoteesein, se ei poista sitä asiaa, etteikö hallituksella olisi valta toimia niin kuin se tekstissä esittää. Hallitus voi siis presidentin tai puolustusministerin pyynnöstä käyttää puolustusvoimia valtion intressejä vastaaviin operaatioihin. Esimerkkinä tästä ovat konfliktin päättäminen valtion omilla ehdoilla tai hyökkääjän häiritseminen sotilaallisella vastaiskulla.

Tunteisiin vetoavaa oikeuttamista edustaa esimerkki 48. Sen alussa puhutaan jälleen 9/11–terroristi-iskusta, joka on joutunut väistymään suurimpana strategisena uhkana kyberhyökkäysten tieltä. Kyberuhkien nostamisella Yhdysvaltojen merkittävimmän terroristi-iskun yläpuolelle on tarkoitus saada kansalaiset ymmärtämään uhan todellinen suuruusluokka. Koska Yhdysvallat julistivat aikoinaan sodan terroristi-iskun perusteella, se vihjaa kyberturvallisuusstrategiassaan tekevänsä sen myös vastaavan tason kyberhyökkäysten kohdalla. Esimerkissä käytetään ilmaisua ”suvaita” (*tolerate*), jonka merkittävyys on siinä, että Yhdysvalloilla todella on mahdollisuus suvaita tietynlaisia iskuja ja poistaa sellaisten iskujen tekijät, jotka se katsoo liian voimakkaiksi.

> (48) From 2013-2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001. Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the United States and the international community will tolerate. (Yhdysvallat 2015: 9.)

Sen sijaan esimerkki 49 ei edes esitä perusteluja sille, miksi hallitus toimii niin kuin toimii. Tekstikohdan mukaan hallitus ilmoittaa valitsevansa itsenäisesti tavat, joilla se tekee yhteistyötä muiden valtioiden kanssa. Tämä herättää kysymyksen, miten hallitus voi tehdä niin, jos tarkoituksena on saavuttaa tasa-arvoinen yhteistyökumppanuus? Toisaalta tämä on myös yksi itseoikeuttamisdiskurssin erityispiirteistä: puhuja ei hae hyväksyntää toimilleen, sillä se kokee itsellään olevan siihen valmiiksi riittävä valta-asema.

> (49) We will select the means that allow us to share information effectively with our allies, and ensure that trusted information and information systems are available, when and where required. (Iso-Britannia 2016: 52.)

Itseoikeuttamisen diskurssi ilmenee siis hyödyn, hypoteettisen tulevaisuuden, tunteisiin vetoamisen ja valta-aseman kautta. Diskurssi on ominainen sellaisille valtioille, joilla on poliittista tai sotilaallista mahtia. Jos samankaltaista diskurssia käyttäisi maailmapolitiikassa pieni valtio, diskurssi voitaisiin tulkita uhittelevaksi. Nyt se on vain toteavaa, vaihtoehdotonta todellisuutta, joka ei perusteluja juuri kaipaa.

4.3 Yhteenveto

Tässä tutkimuksessa tekemäni kriittinen diskurssianalyysi paljastaa valtioiden kansallisista kyberturvallisuusstrategioista viisi erilaista vakuuttamisen diskurssia: yhteishenki, kiiltokuva, varallisuus, pakotettu kontrolli ja itseoikeuttaminen. Diskurssit paikantuvat retorisiin keinoihin, joista yleisimpiä ovat metafora, konsensus, puhujakategoria ja määrällistäminen. Lisäksi jokaisella diskurssilla on omat erityispiirteensä eli aiheet tai teemat, joiden yhteydessä retorisia keinoja käytetään. Retoriset keinot ja erityispiirteet muodostavat yhdessä puhetavan, joka määrittää kutakin diskurssia. Analyysin merkittävimmät löydökset ja diskurssien erot on koottu taulukkoon 5.

Yhteishenki-diskurssi (1) rakentaa kansalaisista kuviteltua yhteisöä ilmaisemalla asiat niin, että niihin on helppo samaistua. Yleisimmät retoriset keinot tässä diskurssissa ovat metaforat, me-retoriikka, yksityiskohdat ja puhujakategoria. Yhteishengen diskurssi on kohdistettu kansalaisille ja sitä käyttävät kaikki valtiot. Diskurssin tavoitteena on luoda

mielipiteiltään vahva yhtenäinen kansakunta. Kiiltokuva-diskurssin (2) tehtävänä on löytää uusia yhteistyövaltioita, joiden avulla tavoitellaan talouskasvua. Kiiltokuva-diskurssi näkyy erilaisten lupausten, vastuullisuuden, kilpailuhengen ja ylemmyydentunnon kautta. Diskurssi ei kuitenkaan ole tyylillisesti uhkaava, sillä tarkoituksena on houkutella muita valtioita – ei karkottaa niitä. Retorisesti kiiltokuva-diskurssissa käytetään puhujakategorian, määrällistämisen, metaforan ja ääri-ilmaisujen keinoja. Varallisuus-diskurssi (3) on ikään kuin jatkumoa kiiltokuvalle. Varallisuuden tavoitteena on hyödyntää kybertoimintaympäristön taloudellisia mahdollisuuksia. Diskurssi jakautuu kahtia: toisaalta diskurssilla tavoitellaan hyötyä, toisaalta siinä pelätään varallisuuden menettämistä. Varallisuus-diskurssissa tehdään paljon vertailuja ja maalataan uhkakuvia, jotka voivat olla hyvinkin ristiriidassa keskenään. Retoriikan keinoista eniten on käytetty puhujakategoriaa, määrällistämistä, vaihtoehdottomuuspuhetta, toistoa ja ääri-ilmaisuja. Diskursseista seuraava, pakotetun kontrollin diskurssi (4), on tullut tyylillisesti kauas yhteishenki- ja kiiltokuva-diskurssien optimistisesta puhetavasta. Pakotettu kontrolli käyttää todellisia esimerkkejä, vetoamista ja uhkailua kansalaisten vakuuttamiseksi. Metaforat ja konsensus toimivat tässä diskurssissa retorisina keinoina. Pakotetun kontrollin diskurssia käyttävät kaikki valtiot tavoitteenaan kansalaisten käytöksen kontrollointi. Kansalaiset halutaan saada toimimaan verkossa valtion intressejä edistävällä tavalla. Viimeistä diskurssia, itseoikeuttamista (5), käyttävät ainoastaan Iso-Britannia ja Yhdysvallat. Itseoikeuttamisessa valtiot rakentavat hypoteettisia tulevaisuusnäkymiä, joihin heillä itsellään on suuri vaikutus. Itseoikeuttamisen diskurssissa valtiot eivät pyydä hyväksyntää puheilleen, vaan nojaavat maailmanpoliittiseen asemaansa. Retorisesti tämä onnistuu tosiasioiden ja vaihtoehdottomuuspuheen avulla. Tavoitteena on tehdä valtioiden valta näkyväksi.

Yleisesti kyberturvallisuusstrategioiden diskurssit rakentavat merkitysmaailmoja, jotka muodostuvat sosiaalisessa kanssakäymisessä kyberturvallisuusstrategian ja sen vastaanottajan välillä. Strategioille on tyypillistä, että ne on suunnattu pääpiirteissään valtion sisäiselle yleisölle. Lukiessaan ja omaksuessaan strategiaa kansalainen osallistuu kuhunkin diskurssiin ja ylläpitää sitä. Kyseenalaistettaessa strategian diskursiivista puhetapaa diskurssi uusiintuu. Diskurssit eivät ole erillisiä kokonaisuuksia, vaan ne limittyvät toisiinsa. Esimerkiksi yhteishengen diskurssia voi seurata kappale, josta välittyy pakotetun kontrollin diskurssi, tai kiiltokuva-diskurssin itsekehuisen tekstin jälkeen valtio itseoikeuttaa

valtansa maailmanpoliittisella asemallaan. Tällä tavoin kepeämmät diskurssit pehmentävät jyrkempien diskurssien sanomaa. Diskurssit näin ollen perustelevat ja vahvistavat toinen toisiaan.

Taulukko 5. Kyberturvallisuusstrategioiden vakuuttamisen diskurssit

	1 Yhteishenki	**2 Kiiltokuva**	**3 Varallisuus**	**4 Pakotettu kontrolli**	**5 Itseoikeuttaminen**
Erityispiirteet	Kuviteltu yhteisö Nationalismi Samaistuminen	Lupaukset Vastuullisuus Kilpailu Ylemmyydentunto Ei uhkaa	a) Hyödyn tavoittelu b) Menettämisen pelko - Uhkakuvat - Vertailu Ristiriidat	Todelliset esimerkit Vaihtoehtojen tarjoaminen Vetoaminen Uhkailu Yksityisyys	Hyöty Hypoteettinen tulevaisuus Vetoaminen Valta-asema Ei hae hyväksyntää
Ilmeneminen tekstissä	Metafora Me-retoriikka Yksityiskohdat Puhujakategoria	Puhujakategoria Määrällistäminen Metafora Ääri-ilmaisut	Puhujakategoria Määrällistäminen Vaihtoehdottomuus Toisto Ääri-ilmaisut	Metaforat Konsensus	Tosiasiat Vaihtoehdottomuus
Ensisijainen vastaanottaja tai yleisö	Kansalaiset	Muut valtiot Media	Yritykset Kansalaiset	Kansalaiset Muut valtion sisäiset toimijat	Kansalaiset Muut valtiot
Valtiot, joissa diskurssi esiintyy	Australia Iso-Britannia Nigeria Singapore Yhdysvallat	Australia Iso-Britannia Nigeria Singapore Yhdysvallat	Australia Iso-Britannia Nigeria Singapore Yhdysvallat	Australia Iso-Britannia Nigeria Singapore Yhdysvallat	Iso-Britannia Yhdysvallat
Tavoitteet ja seuraukset	Yhtenäisesti vahvan kansakunnan luominen	Löytää uusia yhteistyökumppaneita Taloudellinen kasvu	Talouskasvu Kybertoimintaympäristön mahdollisuuksien hyödyntäminen	Ihmiset saadaan käyttäytymään valtion intressien mukaisesti	Todeta valtion valta

Vahvistusta diskurssit kaipaavatkin, sillä ne ovat kaikki lopulta sidoksissa toisiinsa. Esimerkiksi varallisuuden diskurssissa valtio on huolissaan taloudellisista menetyksistä. Jotta kyberturvallisuus saataisiin kuriin, kaikkien pitää tehdä oikeita valintoja verkossa. Pakotetun kontrollin diskurssissa valtio pyrkii muuttamaan kansalaistensa käytöstä intressiensä eli talouden turvaamisen vuoksi. Tämän onnistumiseksi kansalaisten pitää olla vastaanottavaisia ja tavoitella valtion kanssa samaa asiaa, mitä taas haetaan yhteishengen diskurssilla. Diskurssit ovat siis myös riippuvaisia toisistaan siltä osin, kun vastaanottaja täytyy saada vakuutettua.

Lähes kaikissa analysoimissani strategioissa on käytössä kaikki diskurssit. Isoimmat erot diskurssien ilmenemisessä ovat aiheissa tai teemoissa, mikä on toisaalta johdonmukaistakin, jos diskurssien ajatellaan pohjautuvan kulttuuriin. Tämä tarkoittaa sitä, että toisessa valtiossa sama diskurssi voi olla käskevämpi kuin toisessa, koska myös kulttuurinen tapa puhua on erilainen. Näkyvin esimerkki tästä on itseoikeuttamisen diskurssi, jota käyttävät ainoastaan Yhdysvallat ja Iso-Britannia. Niiden asema on globaalisti niin vahva, ettei niiden valtaa juuri kyseenalaisteta. Jos esimerkiksi Nigeria ilmoittaisi kyberturvallisuusstrategiassaan, että se aikoo päättää konfliktit omilla ehdoillaan (kuten Yhdysvallat tekee), väite tulkittaisiin huomattavasti aggressiivisempana. Yhdysvaltojen kohdalla vastaavaan puhetapaan on jo totuttu. Myös pakotetun kontrollin diskurssi osoittaa, että kulttuurisilla tekijöillä on merkitystä. Singapore pyrkii muuttamaan kansalaistensa käytöstä vetoamalla, mikä voidaan tulkita niin, että se antaisi kansalaisten näennäisesti päättää itse. Sen sijaan Iso-Britannian keinona on uhkailu. Yhdysvallat, jossa kansalaisten usko yksityisyyteen on joutunut tietovuotojen myötä koetukselle, ja Australia, jossa yksityisyydensuoja on muutoin mielipiteitä jakava asia, kontrolloivat kansalaisiaan vihjailuilla aiheesta.

Se, mitä diskursseilla tavoitellaan, linkittyy suoraan myös strategioiden tavoitteisiin. Yhteishengen diskurssilla rakennetaan kansalaisista kuviteltua yhteisöä, mutta sen lisäksi, että sen haluttaisiin toteutuvan vain diskurssin sosiaalisessa vuorovaikutuksessa eli lukuhetkessä, valtio haluaisi sen toteutuvan myös kybermaailmassa. Kiiltokuva-diskurssin tavoitteena on luoda kuva menestyneestä kybervaltiosta ja siten löytää todellisia yhteistyökumppaneita. Varallisuuden tavoittelussa pyritään paitsi kasvattamaan taloutta, myös suojelemaan sitä. Varallisuus-diskurssi selittää kiiltokuva-diskurssia, sillä se kertoo

muille valtioille, mitä konkreettista hyötyä valtioiden välisestä yhteistyöstä on. Pakotetun kontrollin diskurssi tavoittelee kansalaisen luottamusta, jotta tämä konkreettisesti muuttaisi käytöstään verkossa. Itseoikeuttamisen diskurssi eroaa muista siten, että se ei hae kansalaisiltaan mitään todellista: diskurssin tavoitteena on vain osoittaa valtion valta ja vahvistaa sitä. Hyväksymällä itseoikeutettu valta hyväksytään myös diskurssi.

Yhteenvetona voidaan todeta, että kyberturvallisuusstrategioiden diskurssit ovat tiukasti sidoksissa toisiinsa. Niitä yhdistää samat retoriset keinot ja kohderyhmät. Lisäksi diskurssit perustelevat ja vahvistavat toisiaan pyrkiessään vakuuttamaan. Lähes kaikki valtiot käyttävät samoja diskursseja, joskin diskurssin sisällä kulttuuri vaikuttaa siihen, miten diskurssia ilmennetään temaattisesti. Diskurssien tavoitteet eroavat sisällöllisesti toisistaan, mutta muut paitsi itseoikeuttamisen diskurssi pyrkivät konkreettiseen muutokseen, joka liittyy erityisesti kansakunnan tilaan. Talous on valtioille yksi merkittävimmistä motivaation lähteistä muutosten toteuttamiseksi.

5 PÄÄTÄNTÖ

Tässä tutkimuksessa olen osoittanut, että valtioiden kansallisissa kyberturvallisuusstrategioissa käytetään paljon vakuuttavaa retoriikkaa, mistä muodostuu erilaisia puhetapoja eli diskursseja. Tutkimus on toteutettu kvalitatiivisesti, mikä tarkoittaa, että aineisto on koostunut pienestä määrästä kyberturvallisuusstrategioita. Analysoimieni strategioiden valtiot ovat Australia, Iso-Britannia, Nigeria, Singapore ja Yhdysvallat.

Analyysissa olen käyttänyt metodina kriittistä diskurssianalyysia. Sen soveltaminen aineistoon on toiminut onnistuneesti, sillä tavoitteenani on alusta asti ollut tekstuaalista analyysia laajemman ilmiön tutkiminen. Diskurssianalyysi mahdollistaa analyysin ulottamisen tekstin taakse sen kontekstiin. Sitoessani strategiatekstejä valtioiden todelliseen tilanteeseen olen onnistunut löytämään strategioiden puhetavoista nyanssieroja, jotka voivat johtua vain kulttuurisista tekijöistä. Diskurssianalyysiin olen lainannut retoriikan tutkimuksesta työkaluiksi erilaisia argumentoinnin ja vakuuttamisen keinoja. Niiden tehtävä tässä tutkimuksessa on paikantaa strategioista sellaiset kohdat, joissa painottuu jokin erityinen diskurssi. Tämän avulla diskurssien muodostaminen on sujunut vaikeuksitta, mutta haasteena on ollut se, etten ole jättänyt analyysia vain retoristen keinojen paikantamiseen, vaan että olen osannut tulkita diskurssia keinojen takana.

Kyberturvallisuusstrategioista voisi löytää hyvinkin erilaisia diskursseja, jos tieteellisen viitekehyksen rakentaisi toisenlaiseksi. Diskurssianalyysi on niin monimuotoinen tutkimusmenetelmä, että valitsemalla toiset käsitteet tai teoriaperinteen tutkimustulokset poikkeaisivat varmasti omistani. Tämän on jo osoittanut Aleksi Saloharju (2015) pro gradu -tutkielmassaan, joka painottaa vahvemmin sosiaalista konstruktivismia ja yhdistää analyysiin alueellista turvallisuuskompleksiteoriaa yhteiskuntatieteiden puolelta. Toisaalta oma tutkimukseni on jo olemassa olevalle kyberturvallisuusstrategioiden tutkimukselle arvokas lisä, koska tutkin strategioita heikomman osapuolen näkökulmasta.

Kyberturvallisuusstrategioita ei kuitenkaan ole tutkittu vielä läheskään tarpeeksi. Tässä tutkimuksessa analysoimani aineisto on ollut puhtaasti tekstuaalista, mutta diskurssiana-

lyysia voisi laajentaa keskusteluihin kyberturvallisuuden toimeenpanosta. Näin ovat tehneet muun muassa Vaara ym. (2010) tutkiessaan Lahden kaupungin strategiaa. He haastattelivat tutkimukseensa strategian toimeenpanijoita ja sisällyttivät heidän kommenttinsa osaksi aineistoa. Tällä tavoin strategioista löydetyt diskurssit laajenevat todelliseksi puhetilanteeksi, jossa niiden uusintaminen ja omaksuminen näkyvät käytännössä.

Lisäksi havaitsin, että ainoastaan viiden kyberturvallisuusstrategian tutkiminen menetelmälläni on työlästä aineiston määrän vuoksi – puhumattakaan niistä tutkimuksista, joissa on käsitelty kymmenestä neljäänkymmeneen strategiaa (ks. esim. Saloharju 2015; Min, Chai & Han 2015). Jo yhden kyberturvallisuusstrategian analysoiminen tarkemmin kertoo enemmän siitä, kuinka valtiot kyberturvallisuuteen suhtautuvat, sillä maat usein lainaavat ajatuksia ja sisältöjä toisiltaan. Vertaileva tutkimus esimerkiksi vanhojen ja uusien kyberturvallisuusstrategioiden välillä osoittaisi, onko diskurssissa tapahtunut jonkinlainen muutos. Tällainen tutkimus joutuu kuitenkin vielä odottamaan, sillä kybermaailmassa kymmenen vuotta on lyhyt aika – diskurssien muuttumisessa vielä lyhyempi.

Se, mitä tutkimukseni pohjalta voidaan sanoa kyberturvallisuudesta yleisesti, linkittyy jo aikaisempaan kyberturvallisuuskeskusteluun. Viimeisen vuosituhannen alusta vellonut keskustelu on ajanut valtiot pohtimaan tarkemmin omaa rooliaan globaalissa kybertoimintaympäristössä. Kyberturvallisuusstrategioissaan valtiot määrittelevät toinen toistaan suurempia visioita ”kybervaltiosta”, joka tarjoaa parhaan mahdollisen suojan kansalaisille ja yrityksille kyberhyökkäyksiä vastaan. Visioissaan valtiot esittelevät itsensä varteenotettavimpana kumppanina, joka osaa parhaiten hyödyntää kybermaailman mahdollisuudet ja torjua uhat.

Uhkia kybermaailmassa riittää. Rikollisuus, vakoilu ja sota ovat niistä merkittävimpiä. Uhkilta suojautuakseen yksittäinen ihminen ei voi juuri muuta kuin muuttaa omaa käytöstään kybertoimintaympäristössä: varmistamalla sähköpostien olevan oikealta lähettäjältä ja vaihtamalla salasanansa riittävän usein. Tästä huolimatta kybermaailma on suoranainen anarkian ilmentymä. Valtiovallan tehtävä on pysäyttää tai saattaa kuriin rikollinen toiminta. Tehtävä ei kuitenkaan ole niin yksinkertainen, koska länsimaisissa demokrati-

oissa ei hyväksytä valtiovallan puuttumista kansalaisen yksityiseen verkkokäyttäytymiseen. Toisaalta valtiot voivat olla kansalaisilleen yhtä iso uhka kuin kuka tahansa muu kybermaailman toimija. Rikollista toimintaa voivat harjoittaa valtioiden tukemat yritykset, minkä lisäksi on yleisesti tiedossa, että maailmanpoliittisesti merkittävien maiden tiedustelupalvelut tarkkailevat yksityishenkilöitä heidän tietämättään.

Kyberturvallisuusstrategiat ovat keino hälventää ristiriitaista käsitystä valtioista kansalaisten valvojina. Tässä tutkimuksessa olen osoittanut strategioissa käytettyjen diskurssien tavoitteen olevan kansalaisten vakuuttaminen siitä, että valtion toimet kybermaailmassa ovat heidän parhaaksensa. Diskurssien avulla pyritään herättämään muun muassa kansallista yhtenäisyyden tunnetta ja ylpeyttä oman maan saavutuksista, mutta toisaalta niillä halutaan myös muokata kansalaisten käyttäytymistä valtion intressien mukaiseksi. Käyttämällä erilaisia retorisia keinoja moni suoranainen käsky tai ohje on kirjoitettu strategian sisään niin taidokkaasti, ettei sitä tavallinen kansalainen välttämättä tule edes huomanneeksi. Kun teksti ei herätä hämmennystä tai sitä ei kyseenalaisteta, diskurssi liitetään osaksi omaa ajatteluaan.

Voisi sanoa, että näin on jo jopa käynytkin. Kyberturvallisuusstrategioita on julkaistu lähes kymmenen vuoden ajan, mutta edelleen ne ovat vain korkean tason poliittisia asiakirjoja. Tutkimistani strategioista vain kaksi ovat herättäneet julkaisuajankohtanaan suurempaa keskustelua kotimaan mediassa eli näissäkin tapauksissa lokaalilla tasolla. Strategioiden diskurssit on kuitenkin suunnattu pääasiassa tavallisille kansalaisille, joten se, ettei heidän keskuudestaan ole noussut laajempaa keskustelua aiheesta, osoittaa, etteivät strategiat ole joko tavoittaneet heitä tai diskurssit on hyväksytty sellaisenaan. Tämä kertoo siitä, ettei yksittäinen internetkäyttäjä koe kybermaailman ongelmia niin vahvasti kuin kyberturvallisuusstrategioissa asiat esitetään.

Tulevaisuudessa ongelmia voi kuitenkin syntyä, vaikkei kyberkeskustelu juuri nyt vaikuttaisikaan niin kiinnostavalta. Valtioiden kyberturvallisuusstrategiat ovat yleisesti kenen tahansa saatavilla, joten jos valtio päättää toteuttaa strategioissaan esittämiään muutoksia ja kansalaiset osoittavat siitä eriävän mielipiteen, valtio voi vedota strategian jul-

kisuuteen: kansalaisen olisi pitänyt tietää, millaisia suunnitelmia valtiolla on kybermaailman suhteen ollut. Esimerkiksi lakimuutokset, jotka mahdollistavat laajamittaisemman tiedustelun tai tietoturvaohjelman asentaminen pakolliseksi internetiä käyttäviin laitteisiin, voivat olla tulevaisuudessa keskustelua herättäviä aiheita. Tämän vuoksi sen havaitseminen, mihin kyberturvallisuusstrategioiden diskursseilla pyritään, on tärkeää tavallisen kansalaisen näkökulmasta.

Toinen syy olla kiinnostunut kyberkeskustelusta on internetin kasvavat käyttäjämäärät. Internetin suosio kasvaa globaalissa mittakaavassa vuodesta toiseen: vuonna 2016 internetkäyttäjiä oli maailmassa lähes 3,5 miljardia (Statista 2017). Sitä, millaisia seurauksia tällä tulee olemaan, on vielä mahdotonta tietää. Kyberturvallisuusstrategiat kuitenkin yrittävät esittää ratkaisuja, ja niin niiden tulee tehdä myös tulevaisuudessa, sillä kybermaailma ei ole katoamassa minnekään.

Kybertoimintaympäristö, joka koostuu ihmisistä, koneista ja niiden toiminnan mahdollistavista instituutioista, on modernin internetin koti. Internetin suosio piilee siinä, että sen ensisijainen tehtävä on tuoda ihmiset lähelle toisiaan koneiden sijasta. Varhainen moderni internet perustui luottamukseen, ei vain teknologiaan. Kehittäjäyhteisö luotti siihen, että käyttäjät olivat ”enemmän tai vähemmän kykeneviä ja sydämiltään riittävän puhtaita, etteivät he tarkoituksella tai huolimattomuuttaan häiritse verkkoa” (Zittrain 2008: 3). Internetin kehittivätkin sellaiset ihmiset, joilla oli itsellään mahdollisuus vaikuttaa kyseiseen teknologiaan. Se on myös osaltaan yksi merkittävimmistä syistä koko internetin ja kybermaailman menestykselle.

Sittemmin verkosta on tullut paljon suljetumpi. Internetin alkujaan generatiivinen luonne, eli vapaa muokattavuus, on lopulta kääntynyt itseään vastaan. Internet on täyttynyt nopeasti viruksista ja haittaohjelmista. Ottamatta sen enempää kantaa internetin tulevaisuuteen, yhdyn Jonathan Zittrainin (2008: 3) visioon siitä, että yhä useampi internetin käyttäjä kaipaa stabiiliutta verkkoon. Ainakin länsimaissa, joissa internetin historia on pidempi, on päästy tähän vaiheeseen. Teknologia on juossut nopeasti tavallisen kansalaisen

ymmärryksen ohi, puhumattakaan sen jatkuvasta kehittymisestä ja yhä uusista vahingon-aiheuttajista, joita internetiin päätyy päivittäin. Se, että edes ymmärrettäisiin, ketä tai mitä vastaan kyberturvallisuudessa suojaudutaan, vakauttaisi internetiä merkittävästi.

LÄHTEET

Aineisto

Australia 2016 = Commonwealth of Australia (2016). *Australia's Cyber Security Strategy. Enabling innovation, growth & prosperity.* [Lainattu 8.12.2016]. Saatavilla: https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf?q=270716.

Iso-Britannia 2016 = Her Majesty Government (2016). *National Cyber Security Strategy 2016–2021*. [Lainattu 8.12.2016]. Saatavilla: https://www.gov.uk /government/uploads /system/uploads/attachment_data/file/567242/ntional_cy-ber_security_strategy _2016.pdf.

Nigeria (2015). *National Cybersecurity Strategy*. [Lainattu 8.12.2016]. Saatavilla: https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURI-TY_STRATEGY.pdf.

Singapore 2016 = Cyber Security Agency of Singapore (2016). *Singapore's Cybersecurity Strategy*. [Lainattu 8.12.2016]. Saatavilla: https://ccdcoe.org/sites/default/files/documents/SingaporeCybersecurityStrategy.pdf.

Yhdysvallat (2003). *The National Strategy to Secure Cyberspace.* [Lainattu 8.12.2016]. Saatavilla: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Yhdysvallat (2015). *The Department of Defence Cyber Strategy.* [Lainattu 8.12.2016]. Saatavilla: http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf.

Kirjallisuus

ACSC (2016). Threat Report. [Lainattu 27.3.2016]. Saatavilla: https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf.

Alasuutari, Pertti (2011). *Laadullinen tutkimus 2.0*. 4. painos. Tampere: Vastapaino.

Alvesson, Mats & Dan Kärreman (2000). Varieties of Discourse: On the Study of Organizations through Discourse Analysis. *Human Relations* 53: 9, 1125–1149.

Anderson, Benedict (1983/2007). *Kuvitellut yhteisöt. Nationalismin alkuperän ja leviämisen tarkastelua.* (*Imagined Communities. Reflections on the Origin and Spread of Nationalism*, kääntänyt Joel Kuortti). Tampere: Vastapaino.

Aristoteles (2012). Retoriikka. (*Rhētorikē*, kääntänyt Hohti Paavo & Päivi Myllykoski). Helsinki: Gaudeamus.

Austin, Greg (2016). New Study: Australia Rearmed! Future needs for cyber-enabled warfare. *Australian Centre for Cyber Security* 19.1.2016. [Lainattu 27.3.2016]. Saatavilla: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/news/australia-rearmed.

BBC (2014). Sony PlayStation Network and other game services attacked. Julkaistu 25.8.2014. [Lainattu 20.1.2017]. Saatavilla: http://www.bbc.com/news/technology-28925052.

BBC (2016). Cyber attacks briefly knock out top sites. Julkaistu 21.10.2016. [Lainattu 18.11.2016]. Saatavilla: http://www.bbc.com/news/technology-37728015.

Bigdata.fi (2017). Big data -määritelmiä. [Lainattu 19.4.2017]. Saatavilla: http://www.bigdata.fi/big-data-maaritelma.

Billig, Michael (1987). *Arguing and Thinking. A Rhetorical Approach to Social Psychology.* Cambridge: Cambridge University Press.

Billig, Michael (1991). *Ideology and Opinions. Studies in Rhetorical Psychology*. Lontoo: Sage.

Braue, David (2016). Security community needs "cultural change", warns Australia's newest Cyber Guardian. *CSO for IDG Communications* 28.10.2016. [Lainattu 27.3.2016]. Saatavilla: http://www.cso.com.au/article/609281/security-community-needs-cultural-change-warns-australia-first-ever-cyber-guardian/.

Candolin, Catharina (2012). Saako sanoa kyber? *All Things Cyber* -blogi. [Lainattu 18.1.2017]. Saatavilla: http://kyberturvallisuus.blogspot.fi/2012/03/saako-sanoa-kyber.html.

CCDCOE (2016). Cyber Security Strategy Documents. [Lainattu 9.11.2016]. Saatavilla: https://ccdcoe.org/cyber-security-strategy-documents.html.

Choucri, Nazli, Stuart Madnick & Jeremy Ferwerda (2014). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development* 20: 2, 96–121.

Curran, James (2012). Rethinking internet history. Teoksessa: James Curran, Natalie Fenton & Des Freedman (toim.). *Misunderstanding the internet.* Lontoo & New York: Routledge. 34–65.

Davies, Bronwyn & Rom Harré (1990/2001). Positioning: The Discursive Production of Selves. Teoksessa: Wetherell, Margaret, Stephanie Taylor & Simeon J. Yates (toim.). *Discourse Theory and Practice. A Reader.* London: Sage. 261–271.

Dijk, Theo van (1993). Principles of critical discourse analysis. *Discourse & Society* 4: 2, 249–283.

Dijk, Theo van (2001). Critical Discourse Analysis. Teoksessa: Deborah Schiffrin, Deborah Tannen & Heidi E. Hamilton (toim.). *Handbook of Discourse Analysis*. Oxford: Blackwell. 352–372.

e-Estonia (2017). Estonian e-Residency. [Lainattu 15.2.2017]. Saatavilla: https://e-estonia.com/e-residents/about/.

Edwards, Julia, Eric Beech & Eric Walsh (2016). FBI investigating cause of cyber attacks: law enforcement official. *Reuters* 21.10.2016. [Lainattu 18.11.2016]. Saatavilla: http://www.reuters.com/ article/us-usa-cyber-fbi-idUSKCN12L2P2.

ENISA (2014). An evaluation Framework for National Cyber Security Strategies. ENISA, Heraklion.

Fairclough, Norman (1992). *Discourse and Social Change.* Lontoo: Polity Press.

Fairclough, Norman (1993). Critical discourse analysis and the marketization of public discourse: the universities. *Discourse & Society* 4: 2, 133–168.

Fairclough, Norman (2003). A*nalysing Discourse. Textual analysis for social research.* Lontoo & New York: Routledge.

Gamreklidze, Ellada (2014). Cyber security in developing countries, a digital divide issue. *The Journal of International Communication* 20: 2, 200–217.

Gellman, Barton, Aaron Blake & Greg Miller (2013). Edward Snowden comes forward as source of NSA leaks. *Washington Post* 9.6.2013. [Lainattu 7.11.2016]. Saatavilla: https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html.

Grierson, Jamie (2017). UK hit by 188 high-level cyber-attacks in three months. *The Guardian* 12.2.2017. [Lainattu 28.3.2017]. Saatavilla: https://www.theguardian.com/world/2017/feb/12/uk-cyber-attacks-ncsc-russia-china-ciaran-martin.

Hall, Stuart (2001). Foucault: Power, Knowledge and Discourse. Teoksessa: Wetherell, Margaret, Stephanie Taylor & Simeon J. Yates (toim.). *Discourse Theory and Practice. A Reader.* Lontoo: Sage. 72–81.

Halminen, Laura (2014). Liian helppoa rahaa ollakseen totta – näin toimii nigerialaiskirje ja neljä muuta huijausta. *Helsingin Sanomat* 26.10.2014. [Lainattu 28.3.2017]. Saatavilla: http://www.hs.fi/kotimaa/art-2000002772494.html.

Hamilton, Sheryl N. (1998). Incomplete Determinism: A Discourse Analysis of Cybernetic Futurology in Early Cyberculture. *Journal of Communication Inquiry* 22: 2, 177–204.

Holmgren, Pia (2016). *”Pelkästä tietoturvallisuudesta ei välttämättä enää seuraa kyberturvallisuutta”. Käsiteanalyysi kyberturvallisuudesta.* Julkaisematon viestintätieteiden pro gradu -tutkielma. Vaasan yliopisto.

Inductive Automation (2017). What is SCADA? [Lainattu 20.1.2017]. Saatavilla: https://inductiveautomation.com/what-is-scada#.

It News Africa (2015). African nations among 20 countries most targeted by cybercriminals. [Lainattu 28.3.2017]. Saatavilla: http://www.itnewsafrica.com/2015/11/7-african-nations-among-20-countries-most-targeted-by-cybercriminals/.

Johnson, Mark (2013). *Cyber Crime, Security and Digital Intelligence.* Lontoo & New York: Routledge.

Jokinen, Arja (1999/2006). Diskurssianalyysin suhde sukulaistraditioihin. Teoksessa: Arja Jokinen, Kirsi Juhila & Eero Suoninen (toim.). *Diskurssianalyysi liikkeessä.* 3. painos. Tampere: Vastapaino. 37–53.

Jokinen, Arja (2016). Vakuuttelevan ja suostuttelevan retoriikan analysoiminen. Teoksessa: Arja Jokinen, Kirsi Juhila & Eero Suoninen (toim.). *Diskurssianalyysi. Teoriat, peruskäsitteet ja käyttö.* Tampere: Vastapaino. 337–368.

Jokinen, Arja, Kirsi Juhila & Eero Suoninen (1993/2000). Diskursiivinen maailma: teoreettiset lähtökohdat ja analyyttiset käsitteet. Teoksessa: Arja Jokinen, Kirsi Juhila & Eero Suoninen (toim.). *Diskurssianalyysin aakkoset*. 2. painos. Tampere: Vastapaino. 17–47.

Jokinen, Arja, Kirsi Juhila & Eero Suoninen (2016). *Diskurssianalyysi. Teoriat, peruskäsitteet ja käyttö.* Tampere: Vastapaino.

Juhila, Kirsi (1999/2006). Tutkijan positiot. Teoksessa: Arja Jokinen, Kirsi Juhila & Eero Suoninen (toim.) *Diskurssianalyysi liikkeessä.* 3. painos. Tampere: Vastapaino. 201–232.

Karp, Paul (2016). Australia puts $230m towards fighting cybercrime, including 50 extra police. *The Guardian* 20.4.2016. [Lainattu 27.3.2017]. Saatavilla: https://www.theguardian.com/technology/2016/apr/21/australia-230m-fighting-cybercrime-50-extra-police.

Kähkönen, Virve (2016). Hillary Clintonin annettava kirjallinen todistus sähköpostiskandaalissa – kohu varjostaa vaalikampanjaa. *Helsingin Sanomat* 20.8.2016. [Lainattu 19.1.2017]. Saatavilla: http://www.hs.fi/ulkomaat/art-2000002916961.html.

Liimatainen, Karoliina (2016). CIA: Venäjä pyrki auttamaan Trumpia presidentin vaaleissa. *Helsingin Sanomat* 10.12.2016. [Lainattu 19.1.2017]. Saatavilla: http://www.hs.fi/ulkomaat/art-2000005001541.html.

Lim, Linette (2016). Singapore's cybersecurity skills shortage: Why it matters. *Channel News Asia* 14.10.2016. [Lainattu 28.3.2017]. Saatavilla: http://www.channelnewsasia.com/news/business/singapore-s-cybersecurity-skills-shortage-why-it-matters/3203182.html.

Limnéll, Jarno (2014). Kyber rantautui Suomeen. Aalto-yliopiston julkaisusarja Tiede + Teknologia No 12/2014. Helsinki: Unigrafia Oy.

Limnéll, Jarno, Klaus Majewski & Mirva Salminen (2014). *Kyberturvallisuus*. Saarijärvi: Docendo Oy.

Lin, Herbert S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy* 4: 63, 63–86.

Luiijf, Eric, Kim Besseling & Patrick de Graaf (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures* 9: 1, 3–31.

Luiijf, Eric, Kim Besseling, Maartje Spoelstra & Patrick de Graaf (2011). Ten National Cyber Security Strategies: A Comparison. Teoksessa: Sandro Bologna, Dimitris Gritzalis, Bernhard Hämmerli & Stephen Wolthusen (toim.). *Critical Information Infrastructure Security: 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers.* Lontoo: Springer. 1–17.

Mansikka, Ossi (2017). Hakkeriyhteisö sanoo löytäneensä puutteita autoihin asennettavan ”mustan laatikon” tietoturvasta – Trafi testannut vastaavia laitteita. *Helsingin Sanomat* 16.1.2017. [Lainattu 19.1.2017]. Saatavilla: http://www.hs.fi/kotimaa/art-2000005046813.html.

McGraw, Gary (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies* 36: 1, 109–119.

Menn, Joseph, Jim Finkle & Dustin Volz (2016). Cyber attacks disrupt PayPal, Twitter, other sites. *Reuters* 21.10.2016. [Lainattu 18.11.2016]. Saatavilla: http://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME.

Min, Kyoung-Sik, Seung-Woan Chai & Mijeong Han (2015). An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications* 9: 2, 13–20.

Mindell, David A (2003). *Between Human and Machine: Feedback, Control, and Computing before Cybernetics*. Baltimore: The Johns Hopkins University Press.

Naughton, John (2016). Britain’s cybersecurity policy needs common sense, not just cash. *The Guardian* 6.11.2016. [Lainattu 28.3.2017]. Saatavilla: https://www.theguardian.com/commentisfree/2016/nov/06/uk-cybersecurity-needs-common-sense-not-just-cash.

Niiniluoto, Ilkka (1989). *Informaatio, tieto ja yhteiskunta. Filosofinen käsiteanalyysi.* Helsinki: Valtion painatuskeskus.

OECD (2012). Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy. *OECD Digital Economy Papers*, No. 211, OECD Publishing.

Parameswaran, Prashanth (2016). Singapore Among Most Vulnerable to Cyberattacks in Asia: Report. *The Diplomat* 23.2.2016. [Lainattu 28.3.2017]. Saatavilla: http://thediplomat.com/2016/02/singapore-among-most-vulnerable-to-cyberattacks-in-asia-report/.

Paroutis, Sotirios, Loizos Heracleous & Duncan Angwin (2016). *Practicing Strategy. Text & Cases.* 2. painos. Lontoo: Sage.

Pelican, Luke (2012). Peacetime Cyber-Espionage: A Dangerous But Necessary Game. *CommLaw conspectus* 20: 2, 363–390.

Perelman, Chaïm (1996). *Retoriikan valtakunta*. (*L'empire rhétorique*, kääntänyt Leevi Lehto). Tampere: Vastapaino.

Phillips, Nelson & Cynthia Hardy (2002). *Discourse Analysis: Investigating Processes of Social Construction.* Sage University Papers Series on Qualitative Research Methods, Vol. 50. Thousand Oaks, CA: Sage.

Pietikäinen, Sari & Anne Mäntynen (2009). *Kurssi kohti diskurssia.* Tampere: Vastapaino.

Potter, Jonathan (1996). *Representing Reality. Discourse, Rhetoric and Social Construction.* Lontoo: Sage.

Pynnönen, Anu (2013). Diskurssianalyysi: Tapa tutkia, tulkita ja olla kriittinen. Jyväskylän yliopiston kauppakorkeakoulun Working Paper N:o 379. Jyväskylä: University of Jyväskylä.

Pälli, Pekka, Eero Vaara & Virpi Sorsa (2009). Strategy as text and discursive practice: a genre-based approach to strategizing in city administration. *Discourse & Communication* 3: 3, 303–318.

Reyes, Antonio (2011). Strategies of legitimization in political discourse: From words to actions. *Discourse and Society* 22: 6, 781–807.

Richards, Julian (2014). *Cyber-War: The Anatomy of the Global Security Threat.* Hampshire & New York: Palgrave Macmillan.

Saaranen-Kauppinen, Anita & Anna Puusniekka (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto, [Lainattu 9.11.2016]. Saatavilla: http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_6_1.html.

Sabillon Regner, Victor Cavaller & Jeremy Cano (2016). National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering* (IJCSSE) 5: 5, 67–81.

Saloharju, Aleksi (2015). *Kehitystä, epävarmuutta ja orastavaa alueellisuutta: Käsitykset kyberturvallisuudesta valtioiden kyberturvallisuusstrategioissa.* Julkaisematon yhteiskuntatieteiden pro gradu -tutkielma. Turun yliopisto.

Salter, Michael & Chris Bryden (2009). I can see you: harassment and stalking on the Internet. *Information & Communications Technology Law* 18: 2, 99–122.

Schwartz, Mathew J. (2016). UK's New Cybersecurity Strategy - No Strike-Back Required. *ISMG* 8.11.2016. [Lainattu 28.3.2017]. Saatavilla: http://www.bankinfosecurity.com/blogs/uks-new-cybersecurity-strategy-no-strike-back-required-p-2314.

Shaban, Abdur Rahman Alfa (2016). Nigeria suffered 3,500 cyber attacks in 2015, lost $450m. *Africa News* 10.11.2016. [Lainattu 28.3.2017]. Saatavilla: http://www.africanews.com/2016/11/10/nigeria-suffered-3500-cyber-attacks-in-2015-lost-450m/

Singer, P.W. & Allan Friedman (2014). *Cybersecurity and cyberwar. What Everyone Needs to Know®.* New York: Oxford University Press.

Solms, Rossouw von & Johan van Niekerk (2013). From information security to cyber security. *Computers & Security* vol. 3, 97–102.

Statista (2017). Number of internet users worldwide from 2005 to 2016 (in millions). [Lainattu 9.1.2017]. Saatavilla: https://www.statista.com/statistics/273018/number -of-internet-users-worldwide/.

Suomi.fi (2017) Sähköinen tunnistus ja allekirjoitus. [Lainattu 15.2.2017]. Saatavilla: https://www.suomi.fi/suomifi/suomi/asioi_verkossa/sahkoinen_tunnistus_ja_allekirjoitus/index.html.

Tamminen, Saara (2016). *Lo and Behold, Reveries of a Connected World* -elokuvan esittelyteksti. Helsinki Documentary Film Festival. [Lainattu 5.1.2017]. Saatavilla: http://docpoint.info/tapahtumat/elokuvat/lo-and-behold-reveries-of-a-connected-world-2/.

Tarpael, Fabian (2017). Nigeria hit by 2,175 cyber-attacks in one year. *The Guardian* 17.2.2017. [Lainattu 28.3.2017]. Saatavilla: https://guardian.ng/technology/nigeria-hit-by-2175-cyber-attacks-in-one-year/.

Thielman, Sam (2016). Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian* 15.12.2016. [Lainattu 20.1.2017]. Saatavilla: https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached.

Tieteen termipankki (2017). Kirjallisuudentutkimus: metonymia. [Lainattu 19.04.2017]. Saatavilla: http://www.tieteentermipankki.fi/wiki/Kirjallisuudentutkimus:metonymia.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm & Liis Vihul, 'Cooperative Cyber Defence Centre of Excellence' (2008). Cyber Attacks Against Georgia: Legal Lessons Identified. [Lainattu 8.1.2017]. Saatavilla: http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug2008.pdf.

Turunen, Petri (2016). Oletko havainnut hitautta netissä? Meneillään on suuri verkkohyökkäys. *Ilta-Sanomat* 21.10.2016. [Lainattu 18.11.2016]. Saatavilla: http://www.iltasanomat.fi/digitoday/art-2000001935958.html.

Törrönen, Jukka (2000). Subjektiaseman käsite empiirisessä sosiaalitutkimuksessa. *Sosiologia* 37: 3, 243–255.

Uhlmann, Chris (2015). China blamed for 'massive' cyber attack on Bureau of Meteorology computer. *ABC* 2.12.2015. [Lainattu 27.3.2017]. Saatavilla: http://www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278.

Vaara, Eero, Virpi Sorsa & Pekka Pälli (2010). On the force potential of strategy texts: a critical discourse analysis of a strategic plan and its power effects in a city organization. *Organization* 17: 6, 685–702.

Viestintävirasto (2016a). Haavoittuvuudet. [Lainattu 23.11.2016]. Saatavilla: https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet.html.

Viestintävirasto (2016b). Tietoturvaloukkaukset vuonna 2015. Julkaistu 28.4.2016. [Lainattu 19.1.2017]. Saatavilla: https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2016/tietoturvaloukkauksetvuonna2015.html.

Walters, Riley (2016). Cyber Attacks on U.S. Companies in 2016. The Heritage Foundation 2.12.2016. [Lainattu 28.3.2017]. Saatavilla: http://www.heritage.org/defense/report/cyber-attacks-us-companies-2016#_ftn37.

Williams, Linda S. (2008). The Mission Statement: A Corporate Reporting Tool With a Past, Present, and Future. *Journal of Business Communication* 45: 5, 94–119.

York, Kyle (2016). Dyn Statement on 10/21/2016 DDoS Attack. Dyn 22.10.2016. [Lainattu 23.11.2016]. Saatavilla: http://hub.dyn.com/static/hub.dyn.com/dyn-blog/dyn-statement-on-10-21-2016-ddos-attack.html.

Zittrain, Jonathan (2008). *The Future of the Internet – And How to Stop It*. New Haven & Lontoo: Yale University Press.