Kyberpelotteen rakentuminen

Naton kyberpuolustuksen linjaukset Varsovan huippukokouksen oppaassa

Laura Penttilä

Pro gradu -tutkielma

Politiikan opintosuunta

Yhteiskuntatieteiden ja filosofian laitos

Jyväskylän yliopisto

Helmikuu 2019

Kyberpelotteen rakentuminen

Naton kyberpuolustuksen linjaukset Varsovan huippukokouksen oppaassa

Laura Penttilä
Politiikan opintosuunta
Pro gradu -tutkielma
Yhteiskuntatieteiden ja filosofian laitos
Jyväskylän yliopisto
Ohjaaja: Pekka Korhonen
Helmikuu 2019
Sivumäärä: 65 sivua

Tämän tutkimuksen taustalla on Naton yhteisen puolustuksen palautuminen liittouman keskeiseksi tehtäväksi. Yhteinen puolustus on toiminut Naton pelotteena vuodesta 1949 asti. Kyberympäristö on tuonut tähän oman ulottuvuutensa. Tutkimuksen pohjana on kyberympäristön ulottaminen yhteisen puolustuksen alle. Tutkimuksessa on tarkoitus selvittää, miten kyberpelotetta rakennetaan Varsovan huippukokouksessa. Tutkimuksessa esitetään niitä linjauksia, joita Nato on tehnyt kyberpuolustuksen suhteen. Lisäksi tutkimuksessa tarkastellaan, miten kyberpuolustus asettuu yhteisen puolustuksen alle.

Tutkimuksen aineisto on vuoden 2016 Varsovan huippukokouksen opas, jossa Nato käsittelee sen tulevien vuosien strategista suuntaa. Varsovan huippukokouksessa tehtiin keskeisiä poliittisia uudistuksia kyberpuolustuksen suhteen. Keskeisiä tapahtumia yhteisen puolustuksen vahvistamisen taustalla olivat Ukrainan kriisi ja Krimin valtaus. Aineistoa analysoidaan kahden eri teorian kautta. Tutkimuksessa on selvitetty skinneriläistä puheteon tulkintaa hyödyntäen, mitä tekoja Nato on tehnyt kyberpuolustuksen suhteen. Peloteteorian kautta tarkastellaan sitä, miten kyberhyökkäykset toimivat välineinä kyberpuolustuksen vahvistamiseksi, ja miten tämä asettuu yhteisen puolustuksen alle.

Tulokset osoittavat, että keskeisin tekijä oli tulkinnallinen muutos Naton kyberpuolustuksen suhteen. Tällä tarkoitetaan sitä, että kyberympäristö nähtiin operatiivisena osa-alueena maan, meren ja ilman ohella. Lisäksi tunnistettiin, että Nato on juuri niin vahva kuin sen heikoin lenkki. Tästä syystä jäsenvaltioiden kyberkyvykkyyttä on pyritty parantamaan harjoitustoiminnan, koulutuksen sekä poliittisten asiakirjojen kautta. Tutkimustuloksissa nousee esille, että kyberpelotteen kannalta keskeisiä tekijöitä olivat resilienssi, attribuutio, kyvykkyys sekä kyberosaaminen. Naton keskeisimmiksi haasteiksi esitettiin poliittinen päätöksenteko, kyberympäristön ja ajan välinen suhde sekä kyberympäristön monitahoisuus.

Avainsanat: Nato, kyberpuolustus, kyberpelote, puheteko, peloteteoria, kyberturvallisuus, kyberympäristö

Sisällys

1. Johdanto

Elämme nykyään aikaa, jossa digitaalinen maailma ja fyysinen maailma ovat tiiviissä vuorovaikutuksessa keskenään. Ne eivät ole toisistaan irrallisia, vaan ne ovat kietoutuneet toisiinsa yhä tiiviimmin. Mitä enemmän esineiden internetissä (IoT) on palveluita, joista ihmiset ovat riippuvaisia, sitä haavoittuvaisemmiksi ja riippuvaisemmiksi tästä ympäristöstä tulemme. Kyberuhkat voivat pahimmillaan aiheuttaa merkittävää haittaa niin yhteiskunnalle, yrityksille kuin yksittäisille kansalaisille. (Limnéll, Majewski & Salminen 2014, 9.) Uutisten otsikoissa näkyy mainintoja erilaisista haittaohjelmista ja tietomurroista. Yksi keskeinen vaikuttava tekijä on se, että nykyään noin puolet maapallon väestöstä on kytkeytynyt internetiin (Talous & Tekniikka 2017). Ihmiset pystyvät olemaan virtuaalihahmoja silloin kuin haluavat ja poistumaan sieltä, kun siltä tuntuu. Kybertoimintaympäristössä virtuaalihahmo pääsee Suomesta esimerkiksi Yhdysvaltoihin tai Australiaan hetkessä. Kyberympäristön muutos on vaikuttanut myös Natoon. Tämä tarkoittaa sitä, etteivät sen viholliset ole pelkästään valtiollisia toimijoita, vaan yhä enemmän niin rikolliset, terroristit, hakkerit kuin aktivistitkin käyttävät kybertoimintaympäristöä väylänä päämääriensä saavuttamiseksi. (Limnéll ym. 2014, 37.)

Nato järjestää joka toinen vuosi huippukokouksen, jossa käsitellään tulevan vuoden strategisia linjauksia yhdessä Nato-maiden johtajien kanssa. Naton perustamisen jälkeen huippukokouksia on pidetty yhteensä 28, joista viimeisin järjestettiin Brysselissä heinäkuussa 2018. Krimin valtaus ja Ukrainan kriisi olivat asioita, joiden vuoksi yhteinen puolustus palasi Naton keskeisimmäksi strategiseksi tehtäväksi. Walesissa vuonna 2014 järjestetyn huippukokouksen oppaassa sanotaan, että Venäjän toimet Ukrainassa ovat tehneet Euroopan rauhan ja vapauden kyseenalaisiksi. Venäjän toimet Barentsinmerellä, Välimerellä, Mustallamerellä sekä Itämerellä lisäävät epävarmuutta ja kireyttä ympäri Eurooppaa. Lähi-idän ja Afrikan kriisit tuovat mukanaan uusia uhkia myös Euroopan turvallisuudelle. Varsovassa pidetyssä huippukokouksessa vuonna 2016 nostettiin entistä vahvemmin esille Naton tarve sopeutua paremmin muuttuneeseen turvallisuustilanteeseen. Näkökulma on palannut kriisinhallinta-alueelta sen ydinalueelle eli yhteisen puolustuksen ja pelotteen vahvistamiseen. (Wales Summit Guide 2014 1-4; Warsaw Summit Guide 2016, 1-5; Suomen erityisedustusto Natossa 2017.)

Tämä tutkimus keskittyy Naton yhteisen puolustuksen ulottuvuuteen, ja tarkastelun kohteena on Naton kyberpuolustus Varsovan huippukokouksen oppaan näkökulmasta. Nato on sotilas- ja puolustusliitto, ja näin myös sen kyberpuolustus on saanut sotilaallisen ilmentymän. Naton yksi keskeisin strateginen tehtävä on yhteinen puolustaminen, joka toimii myös liittouman pelotteena (deterrence). Tutkimus jakaantuu kahteen erilliseen analyysiosioon. Ensimmäisessä osiossa tarkastellaan Naton kyberpuolustuksen rakentumista Skinnerin puheteko -metodologiaa apuna käyttäen ja toisessa osiossa keskitytään kollektiivisen puolustuksen ja kyberpelotteen väliseen suhteeseen. Olen pyrkinyt Varsovan huippukokouksen sekä muun lähdeaineiston avulla rakentamaan kuvauksen siitä, miten ymmärrän Naton kyberpuolustuksen ja pelotteen välisen yhteyden. Tutkimuksen tarkoitus on selvittää, miten Naton kyberpelotetta rakennetaan Varsovan huippukokousten linjausten mukaan. Pääkysymystä on tarkoitus täydentää seuraavilla kysymyksillä: mitä linjauksia Nato on tehnyt kyberpuolustuksen suhteen ja miten kyberpelote toimii yhteisen puolustuksen alla?

1.2. Tutkimusaineisto

Naton yhteinen pelote on perustunut yhteiseen johtorakenteeseen, yhteisiin harjoituksiin sekä puolustusrakenteen integroimiseen. Kylmän sodan jälkeen Venäjää ei koettu enää yhtä suurena uhkana kuin ennen. Tämä näkyi siinä, että Naton painopiste siirtyi yhteisestä puolustuksesta kriisinhallintatehtäviin. (Suomen erityisedustusto Natossa 2017.) Viimeistään Ukrainan kriisi, kuten tässä tutkimuksessa useaan otteeseen huomataan, on ollut yksi keskeisin syy sille, miksi Naton painopiste on siirtynyt kriisinhallintatehtävistä takaisin yhteiseen puolustukseen. Walesin huippukokouksessa aloitettiin Naton strategisen linjan muuttaminen. Huippukokouksessa konkretisoitiin valmiusohjelma (RAP), jonka avulla on tarkoitus pystyä vastaamaan nopeastikin ilmeneviin uhkiin. Varsovan huippukokouksessa painotus jatkui yhteisen puolustuksen vahvistamisessa. Yksi keskeisin päätös, joka Varsovan huippukokouksessa tehtiin, oli niin kutsuttu eteentyönnetty läsnäolo (Enhanced Forward Presence, EFP). (Warsaw Summit Guide 2016, 81.) Tällä tarkoitetaan monikansallisia taisteluosastoja, jotka ovat sijoitettu pysyvästi Naton itäisten jäsenvaltioiden alueille. Näin ollen hyökkäyksen kohdistuessa yhteen valtioon se koskettaa heti koko liittoumaa. Pelote on laajentunut koskemaan hybridi- sekä kyberuhkia varsinkin Ukrainan tapahtumien seurauksena. Vaikka pelote onkin nostettu esiin enemmän tavallisten

joukkojen, ohjelmien, ohjusten ja ydinohjusten kautta, niillä kaikilla on yhteys sähköiseen maailmaan tavalla tai toisella. (Suomen erityisedustusto Natossa 2017.)

Huippukokouksissa on tarkoitus käsitellä Pohjois-Atlantin neuvoston (North Atlantic Council, NAC) eli Naton pääasiallisen päätöksentekoelimen ja jäsenvaltioiden ylimmän johdon kanssa Naton seuraavien vuosien toimintalinjauksia. Nato järjesti ensimmäisen huippukokouksen Pariisissa vuonna 1957. Niitä on pidetty vuoteen 2019 mennessä yhteensä 28, viimeisin Brysselissä vuonna 2018. Tässä tutkimuksessa aineistona käytetään pääasiassa Varsovan huippukokouksen opasta vuodelta 2016. Valitessani aineistoa Varsovan huppukokous oli tuorein saatavilla oleva ylimmän tason huippukokous. Lisäksi tässä huippukokouksessa Nato nostaa ensimmäistä kertaa esille sen, että kansainvälinen oikeus pätee myös kybertoimintaympäristössä, joka on tämän tutkimuksen pohja. (Warsaw Summit Guide 2016, 124.)

Krimin valtaus ja Ukrainan kriisi olivat selkeä käännekohta myös Naton strategiselle suunnalle. Varsovan huippukokouksen pöytäkirjassa on yhteensä 315 sivua. Huippukokouksen suuret teemat on jaettu kansalaisten suojeluun modernilla pelotevaikutuksella (deterrence*)* ja puolustuksella (defence), vakauden säilyttämiseen, yhteistyöhön Euroopan unionin kanssa sekä yhteisten arvojen säilyttämiseen. Selkein painotus Varsovan huippukokouksessa on Naton itäisten jäsenmaiden turvallisuuden parantaminen Krimin valtauksen ja Ukrainan kriisin jälkeen. Tämä on lisännyt Naton harjoitustoimintaa alueella. Lisäksi Nato on työstänyt strategiaa, joka vastaisi paremmin nykyaikana ilmeneviin uhkiin, kuten kyberhyökkäyksiin tai hybridioperaatioihin. (Warsaw Summit Guide 2016, 1–5.)

Tässä tutkimuksessa kiinnostuksen kohde on siinä, miten näiden tapahtumien jälkeen Naton kyberpuolustamisen kuvaa on rakennettu Varsovan huippukokouksessa. Vaikka Skinner tunnetaankin klassikkotekstien tulkintametodologian asiantuntijana, viittaan häneen tässä työssä eri näkökulmasta. Skinnerin puhetekoa hyödynnetään ensimmäisessä analyysiosassa, jossa käytetään puheteon ajatusmallia analyysin työkaluna. Aineistosta esitetään lausuntoja siitä, mitä on sanottu (lokuutio), ja tämän jälkeen analysoidaan sitä, mitä tekoja näillä on tehty (illokuutio) Naton kyberpuolustamisen suhteen. Peloteteoria on valittu toiseksi teoriaksi siitä syystä, että Naton yksi keskeisin tehtävä on yhteinen puolustus, joka on ollut liittouman pelote jo vuodesta 1949. Peloteteoriaa käsitellään toisessa analyysiosassa, jossa tarkastellaan kybertoimintaympäristön toimivuutta Naton yhteisen puolustuksen alla. Näiden molempien analyysiosioiden tarkoitus on rakentaa kuva Naton kyberpuolustuksesta Varsovan huippukokouksessa sekä analysoida sitä, miten tehokas pelote yhteinen puolustus on kybertoimintaympäristössä.

Seuraavassa alaluvussa käsitellään tutkimuksen taustaa ja tuodaan esille tutkimuksen taustalla vaikuttaneita asioita. Tämän jälkeen alaluvuissa esitellään molemmat teoriat. Luku 2 keskittyy kyberkäsitteistöön ja etenkin siihen, mitä kyber-termillä tarkoitetaan tässä tutkimuksessa. Lisäksi tuodaan lyhyesti esille keskeisiä kybertoimintaympäristössä liikkuvia tekijöitä ja sitä, millaisia uhkia ne muodostavat. Tässä tutkimuksessa kyber-termi esiintyy sotilaallisen toiminnan yhteydessä, koska kyseessä on kyberpuolustus. Itse näen kybertoimintaympäristön sekä kyberturvallisuuden positiivisina ja mahdollistavina asioina. Tässä tutkimuksessa käsite saa negatiivisemman sävyn, koska tarkastelun kohteena on kyberpuolustuksen pelote kybertoimintaympäristössä.

1.3. Tausta

Nato perustettiin vuonna 1949 toisen maailmansodan jälkeen suojelemaan sen jäsenvaltioita Neuvostoliiton uhalta. Liittouman ensisijainen tarkoitus on ollut Euroopan turvallisuuden takaaminen, paremman yhteistyön mahdollistaminen sekä rauhan varmistaminen jäsenvaltioiden alueella (NATO 2017a). Puolustusliiton ytimessä on yhteinen puolustus, joka tarkoittaa oikeutta itsepuolustukseen. Tämä tarkoittaa sitä, että hyökkäys yhtä jäsenvaltiota vastaan voidaan tulkita hyökkäykseksi kaikkia jäsenvaltioita vastaan. Teknologisen kehityksen vauhdittamana esiin tulee uudenlaisia haasteita, jotka haastavat myös nykyisen 29 jäsenvaltion liittouman. Kybertoimintaympäristö on avannut toisenlaisen nopeamman ja arvaamattoman ympäristön, jossa päätöksentekijät, turvallisuuskulttuuri sekä Naton organisaatio haastetaan uudella tavalla.

Veenendaal, Kaska ja Brangetto (2016) tutkivat sitä, onko Nato valmis ottamaan suuren askeleen kyberpuolustamisessa, artikkelissa ”*Is Nato Ready to Cross the Rubicon on Cyber Defence*”. Siinä keskeiseksi teemaksi nousi ensinnäkin kybertoimintaympäristön tunnistaminen operatiiviseksi ulottuvuudeksi. Toiseksi painotettiin toimintaperiaatteen sisällön uusimista niin, että Nato pystyy sekä puolustamaan ja vastaamaan mihin tahansa uhkaan kybertoimintaympäristössä. Kolmanneksi painotus oli sellaisten toimenpiteiden kehittämisessä, jotka mahdollistavat kyberkyvykkyyksien hyödyntämisen myös sotilaallisesti. (Ibid, 7.) Lewis (2015) tutki hyökkäyksellisiä kyberoperaatioita yhteisessä puolustuksessa artikkelissaan ”*The Role of Offensive Cyber Operations in Nato’s Collective Defence*”. Artikkelissa keskeisenä kysymyksenä oli mahdolliseen hyökkäykseen tarkoitetut kyberoperaatiot. Kysymys oli siitä, pystyykö Nato riittävän hyvin puolustautumaan ilman

niitä. Tähän liittyen artikkelissa mainittiin toimintaperiaatteen päivittämisen tarve. Päivitystarve liittyi jäsenvaltioiden kyberoperaatioiden käyttöön sellaisessa tilanteessa, jossa näiden käyttö siirtyisi Natolle. (Lewis 2015, 1, 12.) Hunker (2010) kirjoittaa kybersodan ja kybervallan haasteista Natolle artikkelissa ”*Cyber war and Cyber power: Issues for Nato doctrine*”. Hän nostaa esiin kansojen kasvavan riippuvuuden sähköisistä järjestelmistä, joiden haavoittuvuudet ulottuvat kaikkialle. Sekä valtiolliset että ei-valtiolliset toimijat käyttävät kyberhyökkäyksiä näiden haavoittuvuuksien hyödyntämiseen. Hänestä Naton yksi keskeisimpiä kysymyksiä on kybertoimintaympäristön toiminta-alueen viitekehyksen hahmottaminen. Lisäksi Naton tulee luoda selkeä rakenne kyberpuolustukselle. (Ibid., 11–12.) Nato on niin Varsovan kuin Brysselinkin huippukokouksessa vahvistanut kyberpuolustuksen johtamisrakennetta verbaalisesti. Bendiek ja Metzger (2015) tutkivat artikkelissaan ”*Deterrence theory in cyber-century*” kyberpelotetta ja peloteteorioiden soveltuvuutta kyberympäristöön. Tässä tutkimuksessa kyberpelotteen rakentuminen on ymmärretty samalla periaatteella kuin rangaistuksen sekä vahvan puolustuksen pelote fyysisessä maailmassa. Tähän palataan tarkemmin luvussa 1.4.2.

Tutkimuksessa ei käsitellä Yhdistyneiden kansakuntien (YK) roolia syvemmin, mutta YK:n peruskirjan artiklat ovat oleellisia siitä syystä, että ne loivat mandaatin Naton perustamiselle. Nato ja YK ovat molemmat lupautuneet ylläpitämään ja edistämään kansainvälistä rauhaa ja turvallisuutta (NATO 2009). YK:n turvallisuusneuvostolla on ensisijainen rooli kansainvälisen turvallisuuden ja rauhan ylläpitämisessä. Turvallisuusneuvoston tehtävä on määritellä, mitkä tekijät ovat uhkaksi rauhalle ja turvallisuudelle. Heidän kuuluu määritellä, milloin ja missä tilanteissa on oikeutettua käyttää voimakeinoja rauhan ylläpitämiseen. YK:n artiklan 2 ja artiklan 51 välimaastoon sijoittuvaksi toiminnaksi nähdään ainakin sotilaiden siirtyminen rajan läheisyyteen, keskipitkän matkan ohjusten rakentaminen, tulenjohtotutkan käyttö sekä johtamisen tai ennakkovaroitusjärjestelmien häiritseminen. Jos valtiota vastaan kohdistuu mainittuja toimenpiteitä, on kyseinen valtio oikeutettu käyttämään vastatoimenpiteitä (counter measures), jotka muuten katsottaisiin laittomiksi. Vastatoimenpiteisiin ei kuitenkaan kuulu sotilaallisen voiman käyttö. (Tikk & Kerttunen 2018.) Tämän tutkimuksen tarkoitus on lähestyä näitä asioita kybertoimintaympäristöstä käsin. Keskeinen kysymys on se, milloin toiminta nähdään kybertoimintaympäristössä voimankäyttönä (use of force) ja milloin aseellisena hyökkäyksenä (armed attack) (Kerttunen 2018.)

Kansainvälisessä oikeudessa hyökkäys (attack) liitetään usein sotilaalliseen toimintaan. Geneven sopimuksessa protokollassa I (1977) määritellään säädöksiä, jotka koskevat kansainvälisiä konflikteja ja niiden uhrien suojelemista. Lisäpöytäkirjassa

todetaan, että hyökkäys tarkoittaa väkivaltaisia toimia vihollista vastaan, oli kyseessä hyökkäyksellinen tai puolustuksellinen toiminta (Finlex 1980, artikla 49). Tämäkin määritelmä on riippuvainen siitä, onko kyseessä hyökkääjä vai puolustaja. Aseellinen hyökkäys nähdään toimintana, joka antaa valtiolle oikeuden itsepuolustukseen ja käyttää voimakeinoja rauhan saavuttamiseksi, kun taas hyökkäys liittyy sotilaalliseen toimintaan aseellisen konfliktin yhteydessä. (Schmitt 2012, 285–286.) Aseellisen hyökkäyksen nähdään tyypillisesti aiheuttavan fyysistä vahinkoa, joko henkilövahinkoja, omaisuuden tai alueen tuhoamista. Keskeisin ero artiklan 2(4) ja artiklan 51 välillä on oikeutettu voimankäyttö. (Dev 2015, 385.) Valtio on oikeutettu käyttämään voimakeinoja, kun kyseessä on sodan julistaminen, aluevaltaus, saartaminen, ennakointijärjestelmien tuhoaminen, voimankäyttö aluetta, asevoimia tai siviilejä vastaan. (Tikk & Kerttunen 2018.)

Vuonna 2016 Varsovan huippukokouksessa Nato linjasi seuraavasti: ”NATO has affirmed that international law applies in cyberspace” (Warsaw Summit Guide 2016, 124). Tämä tarkoittaa sitä, että kybertoimintaympäristössä tapahtuva tietynasteinen ja vakavuudeltaan aseelliseen hyökkäykseen verrattavissa oleva hyökkäys voidaan nähdä aseellisena hyökkäyksenä ja voi käynnistää artiklan 5 toimeenpanon (Warsaw Summit Guide 2016, 124; Secretary General’s Annual report 2017, 20–21). Yhteinen puolustus on toiminut pelotteena, kun puhutaan fyysisen maailman toimintaympäristöstä. Kybertoimintaympäristössä tilanne on erilainen. Iranin uraanirikastamoa varten suunniteltu Stuxnet-haittaohjelma oli esimerkiksi Yhdysvaltojen kyvykkyyden osoittamista kyberympäristössä. (Limnéll ym. 2014, 67.) Stuxnet-haittaohjelmaan palataan tutkimuksen luvussa neljä. Kyberhyökkäysten vaikuttavuuden näkee vasta, kun hyökkäys aktivoituu. Käytännössä hyökkääjä ei itsekään tiedä sen vaikutuksia tarkasti, koska sen etenemistä on vaikea kontrolloida. (Moran 200, 285.) Haasteen tuo kybertoimintaympäristön rajattomuus. Se ei tunne valtioiden välisiä rajoja kuten fyysinen ympäristö. Mihin loppuu valtion raja ja mistä alkaa toisen? On haastavaa puolustautua ympäristössä, joka muuttuu jatkuvasti, jossa voi päästää kenet vain sisään tai ulos ja jossa pääsee kulkemaan virtuaalisesti minne vain. (Porche, Sollinger & McKay 2011, 2–3.) Kyberhyökkäysten kohdalla on hyvä pysähtyä miettimään, mikä on hyökkäyksen tarkoitus pelotteen kannalta.

Kyberpuolustus on aina kytkeytynyt myös kyberturvallisuuteen. Turvallisuus-sana liittyy tunteeseen siitä, miten turvallinen olo on. Turvallisuuteen vaikuttaa myös todellisuus eli se, miten asiat oikeasti ovat ympärillämme. Lisäksi kyse on arvoista ja kulttuurista eli siitä, miten tärkeänä pidämme turvallisuutta ja millaisia tapoja tai prosesseja meillä on kehittää sitä. Kyberturvallisuudessa nousee esiin käsite resilienssi, joka tarkoittaa sitä, miten hyvin pystymme sietämään ja palautumaan häiriötilanteista. Nykyään resilienssin taso

yhteiskunnissa on laskenut alhaiseksi, koska olemme riippuvaisia sähköstä ja sähköisestä maailmasta. Turvallisuuden tunteeseen vaikuttavat kaikki tasot eli todellisuus, tunne, kulttuuri ja sietokyky. Lisäksi kybertoimintaympäristössä ajan ja toiminnan suhde on kaventunut. Turvallisuuden tunteen ylläpitäminen vaatii ponnisteluja, koska koko ajan tulee olla tietoinen siitä, mitä ympärillä tapahtuu. Kyberhyökkäyksiä voidaan myös käyttää hyökkääjän toimien piilottamiseen. (Limnéll ym. 2014, 34–36.) Esimerkiksi haittaohjelma voi olla järjestelmässä vuosia ennen kuin se havaitaan. Tämän vuoksi kyberhyökkäyksen pelotetta on vaikea määritellä.

Yhteiskunta on yhä enemmän riippuvainen yrityksistä, jotka tuottavat yhteiskunnalle elintärkeitä palveluita. Elinkeinoelämä kytkeytyy yhteiskunnan toimintaan tiiviimmin kuin ennen. (Limnéll ym. 2014, 47.) Naton kannalta ei enää riitä, että se suojelee vain omia tietoliikenneverkkojaan ja palvelujaan, vaan se joutuu kannustamaan jäsenvaltioita huolehtimaan yhteiskunnan kriittisten toimintojen turvaamisesta ja tärkeiden toimijoiden kytkemisestä tähän kokonaisuuteen. Esimerkiksi Suomessa on käytössä kokonaisturvallisuuden varautumisen malli, jossa viranomaiset, elinkeinoelämä, järjestöt sekä kansalaiset huolehtivat yhteistyössä yhteiskunnan toimintaan vaikuttavien palveluiden ja rakenteiden toimivuudesta (Yhteiskunnan turvallisuusstrategia 2017, 7). Kokonaisturvallisuudesta on muodostunut yhteistoimintamalli, jossa turvallisuuteen liittyvää tietoa jaetaan ja analysoidaan keskeisten toimijoiden kesken. Lisäksi turvallisuusalan toimijat suunnittelevat sekä harjoittelevat yhdessä erilaisia skenaarioita (mt, 5). Siinä puhutaan yhden valtion mallista: se kytkee yhteiskunnan eri osa-alueet varautumisen malliin, joka on ottanut ennakoinnin ja varautumisen keskiöön. Turvallisuus ei ole kytkeytynyt vain sotilaalliseen ulottuvuuteen. Se kattaa jokaisen yhteiskunnan osa-alueen, ja sotilaallinen ulottuvuus on yksi niistä. Tämä tuo pohdittavaa myös sotilas- ja puolustusliitolle, jonka ensisijainen tehtävä on säilyttää rauha ja vakaus sen 29 jäsenmaiden alueella.

Tutkimuksen aiheen valintaa on ohjannut kiinnostus siihen, miten Nato pystyy vastaamaan uhkiin, jotka eivät ole enää vain sotilaallisia. Pelkästään valtion johdon sitoutuminen ei takaa turvallisuuden vahvistumista. Kuva on paljon kompleksisempi, koska siihen liittyy monta eri toimijaa ympäri maailmaa. Nato otti askeleen eteenpäin, kun se linjasi Varsovan huippukokouksessa, että kansainvälinen oikeus pätee myös kyberavaruudessa. Tutkimuksen painopiste tuleekin olemaan siinä, mitä tämä siirto on tarkoittanut Natolle ja miten se on vahvistanut Naton kyberpelotetta. Pystyykö 29 jäsenvaltion liittouma nykyiseen muutostahtiin?

1.4. Tutkimusmenetelmät

1.4.1 Puheteko

Puhetekoa ovat tulkinneet muun muassa John Austin, John Searle, Quentin Skinner ja Ludwig Wittgenstein. Puheteko liitetään perinteisesti Austinin ”How to do things with words” -ajatukseen, jossa keskeistä on se, että lauseet ja sanat nähdään poliittisina tekoina. Skinnerin mukaan John Austin sekä John Searle tutkivat kielen tarkoituksellista käyttämistä jonkin päämäärän saavuttamiseksi. Tällä viitataan siihen, että sanat ovat tällaisissa yhteyksissä samaan aikaan tekoja. (Skinner 2002, 2.) Niillä pyritään kertomaan tai osoittamaan jotain siitä ympäristöstä, jossa ne on kirjoitettu tai sanottu. Puheteossa keskeinen tutkittava kohde on lausunto ”A spoken word, statement, or vocal sound”. (Oxford Dictionaries 2019.) Tekstejä käsitellessään kirjoittajan pitää ensin selvittää, mitä tietyt sanat tarkoittavat tietyssä kontekstissa: ”What point a given expression might have had for the agents who used it” (Skinner 1969a, 38). Keskeisin asia ei kuitenkaan ole vain se, *mitä* on sanottu, vaan miten ja miksi jokin asia on sanottu. Lausunnot nähdään tarkoituksellisina tekoina, joiden tekemiseen liittyy motiivi. Tässä suhteessa tekstissä esiintyviä lausuntoja tulee tulkita argumenttien tavoin. Argumentointiin tarvitaan aina joku asia, jonka puolesta tai vastaan argumentoidaan, jolloin puhujalla tai kirjoittajalla on jokin näkökulma tekoon. Varsovan huippukokouksen oppaassa tämä tarkoittaisi sitä, että pyritään pääsemään kirjoitetun tekstin taakse ja löytämään tarkoitus sille, miksi lausunto on tehty: ”if we wish to understand what has been said, we shall have to identify what exact position has been taken up.” (Skinner 2002, 115.) Tästä syystä on tiedettävä jotain siitä taustasta ja poliittisesta ympäristöstä, jossa kirjoittaja on toiminut. Käsitteet muodostavat erilaisia tarkoituksia eri konteksteissa, ja käsitteiden tarkoitus muodostuu siitä, miten niitä käytetään. (Skinner 2002, 32.)

Wittgensteinin käsitteellisestä muutoksesta (conceptual change) Skinner sai vaikutusta omaan menetelmäänsä. Käsitteiden käyttö ja niiden tarkoitus on linkittynyt kielelliseen toimintaan. Tällaista toimintaa voidaan tarkastella esimerkiksi väittelytilanteissa. Esimerkiksi shakkipelissä pelaaja joutuu väistämättä muuttamaan toimintaansa tilanteiden muuttuessa, koska vastapuolen toiminta vaikuttaa siihen, miten oma strategia toimii. Skinneristä on oleellista takertua siihen, mikä sai tilanteen muuttumaan ja mikä sai pelaajan valitsemaan juuri kyseisen työkalun. (Palonen 2003, 37–40.) Skinnerin

mukaan Wittgenstein pyrki pois ajatusmallista, jossa ei keskitytä vain käsitteiden merkityksen analysoimiseen. Hän halusi keskittyä ennemmin siihen, miten käsitteitä käytetään eri tekojen suorittamiseen. (Skinner 2002, 2.)

Skinner käytti teoksessaan *Visions of Politics: Regarding method* lausetta ”The ice over there is very thin”, jonka poliisi sanoi jäällä luistelevalle henkilölle (Skinner 2002, 114). Tämän idea on se, että irrallisena lauseena emme voi ymmärtää lauseen merkitystä asettamatta sitä kontekstiin. Tutkijan tulisi lukea tekstiä siinä asiayhteydessä ja siinä ajassa, jossa se on kirjoitettu. Lauseita tai käsitteitä on vaikea ymmärtää puheakteina, ellemme ymmärrä niiden tarkoitusta. Tämä edellyttää ajan käytäntöihin, tapoihin sekä merkityksiin tutustumista. (Skinner 2002, 84.) Tiedämme historiasta sen, mitä meille on kerrottu, ja sen mukaan olemme maailmankuvamme sekä todellisuutemme rakentaneet. Haasteellista onkin selvittää, mitä kyseiset käsitteet ovat tarkoittaneet sen ajan kontekstissa olematta itse siinä.

Skinneriläisen lähestymistavan mukaan tekstin tarkoitus (*meaning*) on jotain, mikä on löydettävissä tekstistä. Henkilö, joka lukee teosta, ikään kuin löytää sen uudelleen. Siinä on esillä poliittisen toiminnan eri tasot: lokuutio, illokuutio sekä perlokuutio. Tekstin tarkoitus ja merkitys ovat ensin tekstin kirjoittajan käsissä. Lokuutio ilmaisee sen, mitä on sanottu. Illokuutio taas ilmaisee tekstin tai lauseen merkityksen ja funktion. Se on työkalu, jolla pyritään löytämään lausuntojen takana olevat teot. Perlokuutio viittaa viestin vastaanottamiseen ja yleisön reaktioon. Nämä tekijät muodostavat yhdessä puheteon. (Palonen 2003, 29–56.)

> Reflecting on the idea that speech is also action, I came to the conclusion that the theory of speech acts might have something to tell us about the philosophy of action more generally, and in particular about the role of causality in the explanation of behaviour (Skinner 2002, 4).

Skinner kritisoi lähestymistapaa, joka irrottaa argumentit kontekstistaan, ja liittää ne ”ajattomaan” kontekstiin. Vaikka kysymys olisi tänä päivänä sama kuin sata vuotta sitten, se ei tarkoita, että kysyjä ymmärtäisi tai tarkoittaisi kysymyksellä samaa asiaa, mitä sen kysyjä on tarkoittanut sata vuotta sitten. (Skinner 2002, 87–88.) Tämän koulukunnan ajattelijat ovat sitä mieltä, että vain tekstin kirjoittajat ovat tietoisia tekstin tarkoituksista ja merkityksistä ja vain he voivat olla tietoisia siitä, mitä teksteillä on haluttu sanoa. Tästä syystä ne, jotka lukevat tekstejä uudelleen, eivät voi olla huomioimatta tekstin laatinutta kirjoittajaa. (Ibid., 57–89.) Poliittisia teorioita tulee katsoa niiden historiallisessa ulottuvuudessa sekä ajan sosiaalisen ja poliittisen toiminnan kautta. Lauseita ei voi irrottaa kontekstista ja ymmärtää niiden tarkoitusperiä sellaisenaan. (Palonen 2003, 19–20.) Se vaatii

historian tuntemusta sekä ajan poliittista ymmärrystä. Tekstin tulkitsijat voivat kohdata tekstiä tulkitessaan ainakin kaksi eri ongelmaa. Ensimmäinen näistä on ironia, jossa tekstin tulkitsijan on vaikea erottaa käytettyjen käsitteiden ja lausuntojen sekä niiden tavoitteiden välistä yhteyttä. Toinen ongelma on se, ettei tulkitsija pääse käsiksi siihen, mitä lokuutioilla on tehty. Tästä syystä pelkästään kirjoittajien tärkeiden lausuntojen opiskelu ei ole riittävä polku, jotta voidaan ymmärtää, mitä niillä halutaan sanoa. (Skinner 2002, 80–82.)

Politiikan teoreetikot pyrkivät vastaamaan teorioillaan ajan poliittisiin kysymyksiin. Näitä kysymyksiä ei ole kirjoitettu ajattomassa tilassa, vaan puheet ja tekstit avaavat tien poliittiseen toimintaan. (Skinner 2002, 57–59, 79.) Toisen koulukunnan teoreetikot, muun muassa Ricoeur sekä Derrida, ajattelevat, että tekstin tulkitsijoiden tulisi ensisijaisesti keskittyä tekstin julkiseen tarkoitukseen. Ricoeur havainnollistaa asiaa niin, että kielellinen toiminta on monimerkityksellistä. Lisäksi se sisältää kielellisiä vertauskuvia, jolloin tekstit ikään kuin saavuttavat ajan saatossa itsenäisen tilan. Tällöin tekstin tarkoitus ei ole enää sama kuin se, mitä sen alkuperäinen kirjoittaja on sillä tarkoittanut. (Palonen 2003, 91–93.)

> As Derrida remarks, ‘Everyone knows what “I have forgotten my umbrella” means.’ Derrida’s objection is that we are still left without any means of recovering what I am calling meanings, that is, of recovering what Nietzsche may have meant by writing just those words. Perhaps, as Derrida concludes, he may have meant nothing at all. Derrida’s point is that we have no means of knowing, since we have no means of recovering meaning and hence no prospect of understanding what (if anything) Nietzsche may have meant. (Skinner 2002, 93.)

Derrida taas näkee, että tekstin alkuperäistä tarkoitusta on mahdoton tulkita uudelleen. Hänestä meillä ei ole välineitä eikä keinoja tuoda merkityksiä tekstistä uudelleen esiin. Hän ottaa esimerkiksi Nietzschen käyttämän sanonnan ”I have forgotten my umbrella”. (Skinner 2002, 93.) Eri koulukunnan edustajista Skinner (2002) tuo esiin Derridan, jonka mielestä emme voi tietää, mitä Nietzsche on tällä pohjimmiltaan tarkoittanut. (Skinner 2002, 93.) Myös Ricoeur näkee, että on oleellisempaa keskittyä siihen, mitä teksti tarkoittaa nykyään kuin pyrkiä etsimään tekstin kirjoittajan tarkoitusta: ”What the text says now matters more than what the author meant to say” (Ricoeur 1987, 201). Skinner ja muut tämän koulukunnan teoreetikot eivät usko, että pystymme ymmärtämään puhetekoa, jos emme edes yritä ymmärtää, mikä oli kirjoittajan motiivi. Skinner kritisoi Lovejoyn menetelmää, jonka mukaan tekstissä tulisi kiinnittää huomiota ainoastaan ajan käsityksiin ja mielikuviin eikä niiden käyttöön argumenteissa. Kritiikki kohdistuu siihen, että Lovejoyn History of ideas -konseptissa käsitteet eivät edusta kielellistä toimintaa monipuolisesti. Kielellistä ilmaisua pitäisi tarkastella sanaston, tyylin sekä tekstin eri ulottuvuuksien kautta. Käsityksiä

ja mielikuvia pitäisi tarkastella osana sitä, miten niitä on käytetty tai käytetään argumenteissa, eikä pelkästään tarkastella niitä omana yksikkönään. (Palonen 2003, 35–37.)

Wimsatt ja Beardsley ajattelevat, ettei kirjoittajan tarkoitukseen pääseminen ole relevanttia. Heistä kirjoittajan tarkoitus sekä motiivi lausunnolle ovat löydettävissä tekstin sisältä, eivätkä ne ole siitä irrallisia. Lisäksi argumentteja on esitetty sen puolesta, että kirjoittajan tarkoitus ja motiivi ovat irrallisia heidän työstään, ja siksi niihin ei pitäisi kiinnittää huomiota. Heistä on mahdotonta tietää kirjoittajan motiivia tai tarkoitusta, koska ne ovat vain kirjoittajan tiedossa. Toisaalta argumentteja on esitetty siitä lähtökohdasta, ettei kirjoittajan motiiveihin tai tarkoituksiin tarvitse päästä, kun yritämme ymmärtää tekstin tarkoitusta. (Skinner 2002, 94–95.) Skinnerin vastaus kriitikoille on se, että motiivien ja tarkoituksien tietäminen edellyttää sen ymmärtämistä, mikä suhde kirjoittajalla on siihen, mitä tämä on kirjoittanut. Lukijan tulee ymmärtää, oliko kirjoittaja vakavissaan vai vitsailiko hän kirjoittaessaan kyseessä olevan lausunnon. Skinnerin mielestä pystymme pääsemään kirjoittajan tarkoitukseen ja motiiviin, jos ymmärrämme, millainen puheteko oli kyseessä. Tämä edellyttää, että tiedämme, mitkä asiat innoittivat kyseisiin puhetekoihin: “an understanding of the illocutionary act performed by a speaker will be equivalent to understanding their primary intentions in issuing their utterance.” (Skinner 2002, 98.) Näin voimme havaita, oliko lauseen tarkoitus varoittaa, informoida tai tehdä lupaus ja niin edelleen (Skinner 2002, 96.)

> The lack of agency makes it impossible to understand ’what part, trivial or important, the given idea may have played in the thought of any individual thinker who happened to mention it , or what place, characteristic or unusual, it may have taken in the intellectual climate of any given period in which it appeared’ (Skinner 1970, 118).

Oleellisempaa on etsiä vastausta kysymykseen, miksi tuo siirto oli tärkeä tehdä, ja yrittää tarrata kiinni niihin vaikuttaviin tekijöihin, jotka siirron tekemiseen johtivat (Skinner 1988, 274). Skinner näkee argumentin muodostuvan kahdesta eri ulottuvuudesta, liikkeestä sekä käsitteistä. Liike voidaan nähdä Skinnerin mukaan shakkipelinä ja sitä kautta voidaan tarkastella, miten teoriat on ymmärretty kielellisessä toiminnassa. Shakkipeliä voidaan pitää metaforana käsitteiden käytölle: liikkeen tarkoitus on muuttaa nappuloiden eli käsitteiden ja lausuntojen ryhmittymää. Jokaisen siirron kohdalla joudutaan miettimään kaikki käytössä olevat mahdollisuudet, joita työkaluilla voi tehdä. Otetaan esimerkiksi aiemmin mainittu ”The ice over there is very thin” -lokuutio. Lokuutio edustaa tässä sitä, mitä on sanottu. Illokuutio pyrkii etsimään lokuution tarkoituksen, oliko tällä tarkoitus varoittaa, huomauttaa

vai todeta ja niin edelleen. (Skinner 2002, 108.) Tämä kuitenkin edellyttää sosiaalisten käytänteiden sekä sääntöjen tuntemista. Esimerkiksi eri kulttuureissa tietyt asiat tai sanat tarkoittavat eri asioita. Autolla ei voi ajaa liikenteessä, ellei tunne liikennesääntöjä. Työpaikoilla on omat käytänteet ja säännöt. Skinner käyttää esimerkkinä kokenutta kansanedustajaa, joka tietää ja tunnistaa tietyt käytänteet, joita kansanedustuslaitoksessa edellytetään ja käytetään. Tällaisia käytänteitä ei ole kirjoitettu, vaan ne on opeteltava joko lähteisiin tutustumalla tai historiallisista tutkimuksista. (Palonen 2003, 37.)

Muutos on ollut keskeisimpiä tekijöitä poliittisella kentällä, joka on ollut aina läsnä. Käsitteet, uskomukset, toiminta ja tavat kulkevat käsi kädessä ja muuttuvat yhdessä. Poliittinen muutos on läsnä myös käsitteellisessä muutoksessa (conceptual change) sekä toisinpäin. Käsitteellinen muutos on löydettävissä, kun löydämme muutoksia käsitteissä tai niiden käyttötavoissa. Kieli ja käsitteet ovat heijasteita siitä, miten koemme maailman. Ne muuttuvat, kun maailma muuttuu, ja toisinpäin. Käsitteiden käyttö on yksi tapa muuttaa tai ratkaista poliittisia ongelmia. Ristiriidat ja ongelmat pitää paikantaa historialliseen konseptiin. Kenen ristiriitoja tai ongelmia nämä ovat olleet – tai ovat yhä: ”Conceptual histories must explain the emergence and transformation of concepts as outcomes of actors using them for political purposes.” (Farr 1989, 38.) Tämä edellyttää itsestään selvinä pidettyjen asioiden kyseenalaistamista. Se edellyttää myös niiden palapelin palasten etsimistä, joita ei ole löydetty tai jotka on sijoitettu vääriin kohtiin. Toisaalta yritetään löytää myös se, mikä on jäänyt sanomatta. (Farr 1989, 24–40.)

Suurin haaste klassikkotekstejä luettaessa on syyllistyminen anakronismiin (Kanerva 2015, 4). Tämä tarkoittaa sitä, että tehdään väitteitä tai oletuksia asioista, joita emme siinä ajassa olisi voineet tehdä. Tällöin ikään kuin ”matkustetaan” ajassa taaksepäin ja tehdään havaintoja asioista, jotka ovat tapahtuneet omassa maailmankuvassamme. (Skinner 2002, 86–87.) Sen takia puheteon tarkoitus on pyrkiä löytämään teon tarkoitus sekä kirjoittajan motiivi.

1.4.2 Peloteteoria

Pelote on selitetty muun muassa seuraavasti: ”frighten from or away” ja ”to discourage and turn aside or restrain by fear” (Oxford English Dictionary 2014). Näiden idea on se, että pelon avulla vastustaja saadaan perääntymään. ”Deterrence is concerned with discouraging others from acting ways that advantage them but harm you” (Freedman 2004, 109). Pelotteeseen voidaan liittää niin taloudellisia, sosiaalisia, diplomaattisia tai sotilaallisiakin keinoja. Tutkimuksessa näkökulma painottuu sitovaan oikeuteen (hard law), koska painotus on artiklan 5 yhteisessä puolustuksessa (Scwarz 2005, 11). Keskeisintä on pohtia sitä, miten Nato lähestyy pelotetta kybertoimintaympäristössä. Naton määritelmän mukaan ”Deterrence, based on an appropriate mix of nuclear, conventional and ballistic missile defence, capabilities, remains a core element of NATO’s overall strategy” (Warsaw Summit Guide 2016, 55). Peloteteorian sotilaallinen näkemys liitetään usein ydinaseisiin. Nähtiin, että valtiot, joilla on ydinasevaltaa, eivät lähtisi sotaan toisiaan vastaan, koska ne pelkäävät niistä aiheutuvia seurauksia. Tässä tutkimuksessa peloteteoriaa sovelletaan sotilaallisessa kontekstissa, koska Nato on sotilas- ja puolustusliitto. Ydinaseet muodostivat keskeisen uhkakuvan, kun Nato luotiin pelotteeksi Neuvostoliitolle. (Schwarz 2005, 6.) Krimin valtauksen ja Ukrainan kriisin jälkeen Naton huomio on palannut takaisin yhteisen puolustuksen eli pelotteen vahvistamiseen. Ennen Krimin valtausta ja Ukrainan kriisiä Chicagon huippukokouksessa vuonna 2012 sana pelote esiintyi 15 kertaa, kun Varsovan huippukokouksessa vuonna 2016 sana esiintyi jo 77 kertaa. (Chicago Summit Guide 2012; Warsaw Summit Guide 2016.)

Pelotteella nähdään perinteisesti olevan kaksi lähestymistapaa. Ensimmäinen on rangaistuksen pelotevaikutus (deterrence by punishment) ja jälkimmäinen vahvan puolustuksen pelote (deterrence by denial). Ensimmäisellä viitataan pelotevaikutukseen, jossa vastustajan hyökkäys tehdään kannattamattomaksi. Pelote perustuu siihen, että vastustaja pyritään vakuuttamaan siitä, että sen hyökkäys on hyödytön, koska sitä vastaan kohdistettaisiin laajat vastatoimet. Jälkimmäisellä viitataan siihen, että alueellinen puolustus on niin vahva, ettei vastustaja pysty saavuttamaan operatiivisia tavoitteitaan. Tutkimuksessa näiden ero nähdään yhteisessä puolustuksessa sekä puolustuksessa alueellisella tasolla. Rangaistuksen pelotevaikutuksella viitataan tässä tutkimuksessa Naton yhteiseen puolustukseen. Vahvan puolustuksen pelotevaikutus liittyy taas Naton kyvykkyyteen puolustaa sen alueita operatiivisella tasolla. Esimerkiksi huippukokouksissa niin Walesissa kuin Varsovassakin Nato on vahvistanut valmiuttaan toimia nopeammin ja tehokkaammin esimerkiksi Baltian alueella valmiusohjelmalla (Readiness Action Plan, RAP) sekä

eteentyönnetyllä läsnäololla (Enhanced Forward Presence, EFP). (Bendiek & Metzger 2015, 5; Nato 2016; Schwarz 2005, 9; Warsaw Summit Guide 2016; Suomen erityisedustusto Natossa 2017.)

Snyder erottelee Bendiekin sekä Metzgerin tavoin peloteteoriasta kyvykkyyden torjua (denial) vastustajan muodostaman uhkan sekä kyvykkyyden aiheuttaa merkittävää (punishment) vahinkoa. Kun vihollinen miettii teosta aiheutuvaa hyötyä, se joutuu pohtimaan perinteisen sodankäynnin eri ulottuvuudet eli kokonaiskyvykkyyden niin maassa, merellä kuin ilmassa ottaen näin huomioon kaikki sen puolustushaarat. Se joutuu myös punnitsemaan, pystyykö vastustaja torjumaan sen taktiset siirrot. Tyypillisesti ydinasevaltiot käyttävät ydinaseita pelotteena, ja hyökkääjän uskotaan perääntyvän, sillä vahinko ja kokonaiskustannukset olisivat suuret. Torjuminen voi toimia hyvänä pelotteena, jos hyökkääjä kokee, että puolustajalla on hyvät mahdollisuudet saavuttaa osavoitto operatiivisella kentällä tai strateginen voitto koko sodasta. Riskianalyysi toimii suuntaa antavana tekijänä, mutta siinä on huomioitava se, että arvion tekee kumpikin osapuoli itse ja virhemarginaali on aina olemassa. (Snyder 2015, 4; Bendiek & Metzger 2015, 4-5.)

Pelotteen luonne voi olla myös hyökkäyksellinen. Tällöin keinona käytetään painostusta vastustajaa kohtaan ja pyritään muuttamaan sopimaton käytös tai epätoivottu tilanne. Tällaisesta tilanteesta toimivat esimerkkeinä kriisit niin Kuubassa 1962, Falklandinsaarilla 1982 sekä Kuwaitissa 1999. Kuuban ohjuskriisissä Yhdysvallat vaati Neuvostoliittoa hylkäämään ohjusten sijoittamisen Kuubaan ja asetti saarron, joka esti ohjusten kuljettamisen Kuubaan. Kuuban kriisin taustalla oli Yhdysvaltojen sijoittamat ohjukset Turkkiin. Vastauksena Neuvostoliitto sijoitti ohjuksia Kuubaan, josta oli lyhyt kantomatka Yhdysvaltoihin ja sen keskeisimpiin strategisiin kohteisiin. (Schwarz 2005, 10; Schwarz 2013.)

2. Käsitteistöä

2.1. Tietoturvallisuus, digitaalinen turvallisuus ja kyberturvallisuus

Etuliite kyber tulee kreikankielisestä sanasta kybereo, ja sillä viitataan opastamiseen, ohjaamiseen ja hallintaan. Sen voidaan katsoa viittaavan virtuaalimaailman ja fyysisen maailman välimaastoon. Kyber-etuliitettä ei juuri käytetä yksittäisenä sanana, koska sen merkitys on riippuvainen sen perusosasta, johon se liitetään. Kyber-etuliite viitaa kuitenkin seuraavaan: ”Sanan merkityssisältö liittyy yleensä digitaalisessa muodossa olevan informaation käsittelyyn: tietotekniikkaan, digitaaliseen viestintään (tietoverkkoihin), tietojärjestelmiin tai tietokonejärjestelmiin” (Kyberturvallisuuden sanasto 2018, 30). Kybertoimintaympäristö muodostuu viestintäverkoista, joiden avulla informaatiota siirretään ja varastoidaan elektroniikkaa tai sähkömagneettista spektriä käyttämällä. Informaation ja datan käsittelyyn linkittyvät oleellisesti fyysiset rakenteet, kuten pankki- ja rahoitusjärjestelmät ja liikenteen ohjausjärjestelmät. (Kyberturvallisuuden sanasto 2018, 21.)

> Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber attack. (NATO 2014.)

Norbert Wiener (1948) keksi käyttää ensimmäistä kertaa 1940-luvulla sanaa kybernetiikka. Sen avulla pyrittiin hahmottamaan tietokoneita ohjaavia ohjausjärjestelmiä. Kybernetiikalla tutkitaan erilaisten järjestelmien välistä vuorovaikutusta sekä niiden ohjaamista: ”Se on systeemiteoriaan pohjaava poikkitieteellinen tutkimusala, jonka keskeisiä kysymyksiä ovat, mitä jokin asia tekee tai mitä se voi tehdä.” (Limnéll, Majewski & Salminen 2014, 30.) Kyse oli ennen kaikkea toiminnan ohjaamisen ja viestinnän välisestä suhteesta. Myöhemmin kybernetiikalla viitattiin tietokoneisiin, joissa järjestelmän toiminta ja toiminnan tulokset olivat laskettavissa, ja niistä voitiin rakentaa matemaattisia malleja. Merkittävin kyberneettinen saavutus oli 1990-luvulla internet, jolloin konkreettisesti nähtiin ihmisten ja koneiden välinen jatkuva yhteistyö. (Ibid., 30.)

Kriittinen infrastruktuuri nostetaan usein esille, kun puhutaan kybermaailmasta. Digitalisaation kehittyessä myös valtioiden kriittiset kohteet ovat kytkeytyneet kybertoimintaympäristöön. Tämä jakautuu yksityisten sekä julkisten instituutioiden verkostoihin, joista ovat riippuvaisia esimerkiksi pankki- ja rahoitusjärjestelmät, terveyspalvelut ja tietoliikennejärjestelmät (Lehto 2017). Pankki- ja rahoitusjärjestelmät

sekä sähköverkko ovat huoltovarmuuskriittisimpiä kohteita Suomessa (Suomi Areena 2018). Yhteiskunta on riippuvainen sen elintärkeistä toiminnoista, joita ovat esimerkiksi valtion johtaminen, sisäinen turvallisuus, puolustus, talous, infrastruktuuri, kriisinsietokyky, väestön sekä palveluiden toimintakyky, henkinen kriisinkestävyys sekä kansainvälinen toiminta (Yhteiskunnan turvallisuusstrategia 2017, 14).

Kyberavaruutta pidetään fyysisenä ja epäfyysisenä alueena, johon liittyy tietokonejärjestelmät, tietokone- sekä tietoliikenneverkot, erilaiset ohjelmistot, tietoliikenneverkoissa tai tietokoneissa liikkuva data, niiden sisältö ja liikenne sekä näiden kaikkien käyttäjät (Israel Government Decision no. 3611, 2011). Kyberavaruus on keskenään riippuvaisten informaatioteknologiaverkostojen ulottuvuus, johon internet, tietoliikenneverkot, tietokoneet, tieto- tai viestintäjärjestelmät sekä sulautetut järjestelmät kytkeytyvät (Cybersecurity Strategy 2018). Kyberavaruus on globaali informaatioympäristö, joka muodostuu informaatioteknologiasta ja siitä riippuvaisista verkostoista.

Naton omassa terminologiassa määritellään *computer network attack*, ja termin kohdalla mainitaan erikseen, että kyberhyökkäys on yksi tietokoneverkkohyökkäyksen tyyppi.

> Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber attack. (NATO 2018b, 31.)

Kyberhyökkäyksen nähdään kohdistuvan kriittiseen infrastruktuuriin (Valtiovarainministeriö 2018, 15). Sen nähdään heikentävän demokraattista järjestelmää ja sillä voidaan häiritä tai hankaloittaa sotilaallisia operaatioita. Naton pääsihteeri Jens Stoltenberg nosti esiin Varsovan huippukokouksessa kaksi askelta, jotka tehtiin kyberpuolustuksen parantamiseksi. Ensinnäkin kybertoimintaympäristö tunnistettiin operatiiviseksi alueeksi, joka vaatii puolustusta. Näin ollen Nato pystyy reagoimaan tilanteisiin, joihin se ei ennen kyennyt. Toiseksi jäsenvaltiot lupasivat kehittää kansallista kyberpuolustusta. Naton kyberpuolustus perustuu kansallisiin kehyksiin. (The Secretary General's Annual Raport 2016, 24.) Kyberhyökkäykset ovat kineettiseen hyökkäykseen verraten haasteellisia, sillä niitä ei välttämättä havaita heti. Se ei tarkoita sitä, etteikö niitä tapahtuisi jatkuvasti. Ne eivät vain välttämättä ole havaintokykymme ulottuvissa. (NATO 2018a.) Naton pääsihteerin vuosiraportissa 2016 todetaan, että Nato on käsitellyt noin 500 kybertapausta kuukaudessa, mikä tarkoitti 60 prosentin kasvua vuoteen 2015 verrattuna (The Secretary General's Annual Raport 2016, 6). Varsovan huippukokouksessa ja vuoden 2017

vuosiraportissa vastaavia lukuja ei ole ilmoitettu, mutta hypoteesi on, että lukumäärä on kasvanut. Kaksi vuotta sitten kyberhyökkäys onnistui estämään pääsyn Naton internetsivuille. Nykyään monia kyberhyökkäyksiä on kohdistettu esimerkiksi Saksan valtion tietokonejärjestelmiin pyrkimyksenä saada tietoa sen kriittisestä infrastruktuurista. Tämä on kuitenkin vain yksi esimerkki, jonka Naton internetsivusto ilmoitti. Näitä käytettiin esimerkkinä sille, miten valtiolliset sekä ei-valtiolliset toimijat käyttävät kybertoimintaympäristöä yhtenä väylänä toiminnalleen. Ukrainassa taas kyberhyökkäyksiä on käytetty osana tavanomaista sodankäyntiä. (NATO 2018a.)

> Cyberspace threats from state and non-state actors are a real and imminent danger to all operations. Information is a critical instrument of national power, thus the ability to achieve and maintain an advantage in cyberspace is crucial to national security. (Joint Communications System 2015, 5.)

Tiedosta on tullut merkittävä osa kansallista turvallisuutta, ja siitä on tullut vaihdon väline. Kyber nousi esiin käsitteenä, kun alettiin puhumaan liikkuvan datan ja informaation turvaamisesta. Informaatio on dataa, jota on kaikkialla, mutta sitä ei ole prosessoitu. Tietoturva liittyy läheisesti kyberturvallisuuteen, mutta tietoturva tarkoittaa jo varastoituneet tiedon turvaamista, kun taas kyberturvallisuus liittyy liikkuvan datan ja informaation turvallisuuteen. Tämä tarkoittaa niin toimijan oman kuin sen ulkopuolella olevien järjestelmien turvaamista. Siitä tuli käsite, joka kattoi fyysisen ja digitaalisen maailman rajapinnan. Se koskettaa tätä kyberfyysistä ympäristöä, joiden osaksi olemme jo kasvaneet. (Limnéll ym. 2014, 31.) Tietoturvallisuudella tarkoitetaan tiedon hallinnan ja sen jakamisen turvallisuutta teknisistä sekä hallinnollisista lähtökohdista käsin. Tietoturvalla tarkoitetaan sitä, että tietoa voidaan käyttää turvallisesti ja sen sisältöön luotetaan. Lisäksi tiedon saavutettavuus on turvattu, etteivät ulkopuoliset pääse tietoon käsiksi. Kyberturvallisuudella tarkoitetaan sitä tavoitetilaa, jossa eri tietojärjestelmistä koostuva toimintaympäristö on turvallinen. Sillä tarkoitetaan verkottuneen ja digitaalisen yhteiskunnan sekä siihen liittyvien keskeisten toimintojen turvallisuutta. Kyberturvallisuus liittyy pitkälti yhteiskunnan tai organisaation kriittisten ja välttämättömien järjestelmien ja verkkojen suojelemiseen, ehkäisyyn sekä tunnistamiseen. Digitaalinen turvallisuus toimii näiden kattokäsitteenä, joka sisältää kaikki digitaalisen toimintaympäristön turvallisuuteen liittyvät asiat. (Rousku 2018; Kyberturvallisuuden sanasto 2018, 21.)

Kybertoimintaympäristö on tuonut niin hyvässä kuin pahassa kaikki keskeiset tekijät sen vaikutuspiiriin. Naton sekä sen jäsenvaltioiden sotilaalliset järjestelmät ovat nykyään riippuvaisia informaatioteknologiasta. Tämä riippuvuus tekee Natostakin

haavoittuvaisemman. (Iaisello 2015, 24–25.) Mikäli joku onnistuu joko estämään, sabotoimaan, pysäyttämään tai anastamaan datavirtauksen, josta esimerkiksi Naton operaatiot ovat riippuvaisia, vaikutukset voivat olla hyvinkin haitallisia (Hunker 2010, 5). Tämä on vain yksi mahdollinen esimerkki monen joukossa. Kybertoimintaympäristön mahdollisuuksien kirjo on vielä näkemättä (Lewis 2015, 4).

ENISA (European Union Agency for Network and Information Security) on koostanut raportin keskeisimmistä kyberuhkista vuonna 2017. Ensimmäisenä mainitaan erilaiset haittaohjelmat, jotka ovat olleet kybertoimintaympäristössä kohdatuimpia vuoden 2017 aikana. Toisena mainitaan verkkohyökkäykset, joilla pyritään saamaan haittaohjelma loppukäyttäjän koneelle. Tällaisten uhkien odotetaan olevan yleisiä myös tulevaisuudessa, koska digitaalisessa maailmassa verkkosivustot ovat työkaluja, joilla pyritään johonkin tiettyyn päämäärään. Kolmanneksi on mainittu verkkosovellushyökkäykset, joilla pyritään vaikuttamaan verkkosovellusten sovellusohjelmointirajapintoihin. Neljäntenä on tietojen kalastelu, jota tehdään loppukäyttäjän manipuloimiseksi ja tiedon keräämiseksi kohteesta. Viidentenä mainitaan roskapostit, jotka ovat edelleen yksi keskeisin keino esimerkiksi haittaohjelmien välittämiseen. Kuudentena ovat palvelunestohyökkäykset, joilla pyritään tukkimaan käyttäjän pääsy sivustolle. Seitsemäntenä ovat kiristyshaittaohjelmat, joiden avulla kiristetään rahaa loppukäyttäjiltä. Kahdeksantena listataan botnetit eli ”tietokonearmeijat”, joita käytetään palvelunestohyökkäyksiin tai roskapostin levittämiseen. Yhdeksäs kyberuhka on sisäinen uhka eli organisaation työntekijän oikeuksien hyväksikäyttö organisaation turvallisuuden horjuttamiseksi. Kymmentenä mainitaan fyysisten laitteiden manipulointi tai varastaminen. Yhdenneksitoista mainittu uhka on tietomurto. Tietomurtojen haaste on se, että vahinko on jo tapahtunut, kun tietomurto havaitaan. Kahdenneksitoista on mainittu identiteettivarkaus, jossa käytetään jonkin toisen henkilökohtaisia tietoja välineenä päämäärän saavuttamiseksi. Kolmastoista uhka on tietovuoto, eli yrityksistä ja henkilöistä kerätään tietoja internetin välityksellä. Neljänneksitoista on mainittu ohjelmistoräjähteet. Niissä hyökkääjä muodostaa ohjelmistoräjähteitä haavoittuneita sovelluksia vastaan (F-secure 2019). Viidestoista uhka on kybervakoilu, jota pidetään globaaleissa organisaatioissa merkittävimpänä uhkana. (ENISA Threat Landscape Report 2017, 25–87.)

Caveltyn (2011, 15) esittää kyberuhkista mallin, joka voidaan jakaa viiteen eri portaaseen. Ensimmäisen tason muodostaa kybervandalismi, joka jakautuu hakkerismiin, haktivismiin ja kyberparveiluun. Näihin kuuluvat esimerkiksi verkkosivujen tiedon manipulointi tai palvelunestohyökkäykset. Nämä ovat vaikutuksiltaan suhteellisen lyhytaikaisia, eli suurempia vahinkoja tällaisten hyökkäysten kautta ei aiheudu. (Caveltyn

2008, 1.) Kyberparveilua käytetään esimerkiksi sotilasoperaatioiden yhteydessä, ja sen tarkoituksena on tehdä hyökkäyksiä taktisesti monesta eri suunnasta samaan aikaan. Tämä edellyttää, että kaikilla osapuolilla on sama tilannekuva. Informaatio- ja kommunikaatioteknologian hyödyntäminen ja tehokas käyttäminen ovat oleellisia tilannekuvan reaaliaikaistamiseksi (Lehto 2011). Toisen tason muodostaa kyberrikollisuus. Kyberrikolliseksi toiminnaksi nähdään toimet, jotka tehdään sähköisiä viestintäkanavia tai verkkoja hyväksi käyttäen. Tällaisia hyökkäyksiä ovat esimerkiksi tietomurrot, tietojen kaappaukset haittaohjelmien avulla tai hyökkäykset tietoverkoissa. (Poliisi 2018.)

Kolmannen tason muodostaa vakoilu, jossa tarkoituksena on kalastella arkaluontoista tai tietosuojaluokiteltua tietoa. Tutkimuksessani keskityn ainoastaan valtiolliseen tasoon, jolloin tarkoitetaan sotilaallisen, taloudellisen tai poliittisen edun tavoittelua käyttäen laittomia keinoja kyberavaruudessa. (Liaropoulos 2010, 181.) Tason neljä muodostaa kyberterrorismi, jolla pyritään kriittistä infrastruktuuria hyväksi käyttäen levittämään yleistä pelkoa kansalaisten keskuudessa ja saamaan näin poliittista painetta poliittisten päätöksentekijöiden harteille (Beggs 2009). Viides taso muodostuu kybersodankäynnistä, jolle on vaikea löytää selkeää määritelmää. Se kuitenkin edellyttää valtioiden välistä sotatilaa, jossa kyberoperaatiot toimivat yhtenä alueena osana maa-, meri- ja ilmaoperaatioita. (Lehto 2017, 11.)

Kansainvälinen asema pitää Natoa houkuttelevana kohteena rikollisille, jotka haluavat saada rahaa myymällä Naton tietoja. Rikollisten kohteena voi olla esimerkiksi Naton henkilöstö. Sähköpostin kautta voidaan lähettää saastuneita tiedostoja tai yrittää päästä käyttäjätietoihin käsiksi. Haittaohjelma pystyy aktivoiduttuaan pääsemään tietokoneen sisään ja tekemään sille määritettyjä toimenpiteitä, kuten lataamaan tiedostoja, anastamaan tietoja sekä levittäytymään muihin laitteisiin. (Fidler, Pregent & Vandurme 2013, 8–9.)

2.2. Kyberkäsityksen kehitys huippukokouksissa

Vuonna 2016 Nato nosti julkisesti esiin sen, että kansainvälinen oikeus pätee myös kyberavaruudessa. Tämä juontaa juurensa vuosien 2013 ja 2015 United Nationsin Group of Governmental Experts (GGE) -raporttien läpimurtoon tieto- ja viestintäteknologian ja kansainvälisen turvallisuuden välisessä suhteessa (Kerttunen 2018; Nato Cooperative Cyber Defence of Excellence 2015). Tämä voidaan nähdä hyvänä edistysaskeleena, kun viimein kyberavaruus tunnistettiin yhdeksi kaikkia koskevaksi ulottuvuudeksi ja se sai oikeudellisen ulottuvuuden. Vuonna 2016 Nato ilmoitti, että kyberavaruus kuuluu myös sen perustamissopimuksen artiklan 5 piiriin, jolloin tunnustettiin, että kyberhyökkäys voi myös toimeenpanna yhteisen puolustuksen. (Warsaw Summit Guide 2016, 124.)

> In the context of international law, the 2015 report draws heavily on 2013 report, taking as its starting point the earlier statement that international law applies to the 'use of ICTs'. It repeats that state sovereignty and related principles apply to state conduct of ICT-related activities and that states enjoy jurisdiction over ICT infrastructure within their territory. The references to human rights law are also not new, nor are the mentions of internationally wrongful acts, proxies, and non-state actors. (Nato Cooperative Cyber Defence Centre of Excellence 2015.)

Nato nosti ensimmäistä kertaa kyberpuolustamisen poliittiselle agendalleen 16 vuotta sitten Prahan huippukokouksessa 2002. Vasta viisi vuotta myöhemmin kansainvälisesti huomiota herättäneet kyberhyökkäykset Naton jäsenmaata Viroa vastaan osoittivat, että kyberpuolustamisen alueella on vielä kehitettävää. Vuonna 2008 Nato laati ensimmäisen kyberpuolustuksen toimintaperiaatteen (Policy on Cyber Defence). Georgian ja Venäjän välinen konflikti osoitti, että kyberhyökkäyksiä voidaan käyttää osana tavanomaista sodankäyntiä. Nato hyväksyi uuden strategisen konseptin vuonna 2010 Lissabonin huippukokouksessa näiden tapausten seurauksena. Strategiassa on linjattu, että Naton keskeiset strategiset tehtävät ovat kollektiivinen puolustus, kriisinhallinta sekä turvallisuusyhteistyö. (Warsaw Summit Guide 2016, 127; Strategic Concept 2010, 7-8.)

Kyberpuolustuksen toimintaperiaate ja lupaus kyberpuolustuksen vahvistamisesta ovat keskeisiä liittoumaa ohjaavia sopimuksia. Kyberpuolustamisen tunnustettiin kuuluvan yhteisen puolustuksen piiriin, jolloin hyväksyttiin, että kansainvälinen oikeus pätee myös kybertoimintaympäristössä. Tällöin kyberkysymykset nostettiin taktiselta ja operatiiviselta tasolta strategiselle tasolle, jolloin niistä tuli koko liittoumaa koskeva asia. Tämän lisäksi

Nato on uudistanut kyberpuolustamisen toimintaperiaatteensa vuonna 2011 turvallisuusympäristön tuodessa erilaisia haasteita teknologian nopean kehityksen myötä. (Warsaw Summit Guide 2016, 127–128.)

Käänteen tekevänä kohtana voidaan kuitenkin pitää Krimin valtausta ja Ukrainan kriisiä. Vuoden 2014 tapahtumien jälkeen Nato lanseerasi uuden, päivitetyn kyberpuolustamisen toimintaperiaatteen. Lisäksi Nato näki tarpeelliseksi uudistaa myös toimintasuunnitelman (*action plan*). Kyberpuolustaminen edellyttää myös Natolta yhteistyötä yksityisen sektorin kanssa, sillä yksityinen sektori on merkittävä toimija kybertoimintaympäristössä. Yksityinen sektori tuottaa yhä enemmän turvallisuuspalveluita loppukäyttäjille. Tämän johdosta Walesin huippukokouksessa 2014 Nato kannatti perustettavaksi teollisuusyhteistyöhön erikoistunutta organisaatiota, joka sai nimekseen Nato Industry Cyber Partnership (NICP). Lopuksi vuonna 2016 ennen Varsovan huippukokousta Nato ja Euroopan unioni allekirjoittivat teknisen sopimuksen kyberpuolustamiselle (*Technical Arragement on Cyber Defence*). Tämän sopimuksen tarkoitus on ollut välttää päällekkäistä työtä, ja molemmat voivat keskittyä omiin vahvuusalueisiinsa. (Warsaw Summit Guide 2016, 124–130.)

Varsovan huippukokouksen ensimmäinen askel kyberpuolustuksen parantamiseksi oli se, että kybertoimintaympäristö nähtiin yhtä lailla operatiivisena ympäristönä maan, meren ja ilman ohella. Se ei ole oma osa-alueensa, vaan digitalisaation kehityksen myötä se tulee osaksi kaikkia osa-alueita. Mitä enemmän digitalisoimme asioita, sitä enemmän siitä tulee osa elämäämme. Aiemmin sähköinen ja fyysinen maailma olivat toisistaan erillisiä, mutta nykyään ne linkittyvät toisiinsa ja ovat sulautuneet yhdeksi kokonaisuudeksi. On luonnollista, että kyberpuolustuksesta muodostui taktisen tason ohella strateginen uhka. (Brussel Summit Guide 2018, 74; Shea 2017, 167.)

> NATO will need to learn more from its allies who have already moved in this direction, such as the US, the UK, France and the Netherlands, how their models are working and how they are using cyber effects as part of their military operations. This is all the more important as NATO will not develop offensive cyber capabilities and would therefore need to be able to rely upon voluntary national capabilities (subject to political approval by NATO overall) in instances where NATO military commanders believe that a cyber effect rather than the use of a conventional weapon is the best way of producing a desired military outcome. (Shea 2017, 169.)

Nykyään haasteena on se, että saman pöydän ääressä toimijoita on enemmän kuin koskaan ennen. Lisäksi ennen käsiteltiin paljon rajatumpaa tapahtumakenttää. Kyberympäristö on kuitenkin erilainen. Innovaatioiden tahti on huomattavasti nopeampaa, ja teknologia on huomattavasti hajautetumpaa. Voimavarat jakautuvat monelle toimijalle, ja näitä tulee

soveltaa harkitusti. Kybertoimintaympäristö tuo kaikki osa-alueet yhteen, niin yksilöt, ryhmät kuin valtiotkin palvelurakenteineen, luoden erilaisia tasoja. Näiden uhka-arvio on huomattavasti haasteellisempaa kuin tavanomaisten tai ydinaseviholliston kanssa. (Shea 2017, 165–174.)

3. Kyberpuolustuksen pelikenttä

Tässä luvussa pääasiallisena analyysityökaluna on Skinnerin puheteon ajatusmalli. Pyrin tuomaan esiin, miten Nato rakentaa sen kyberpuolustusta Varsovan huippukokouksen oppaassa. Skinneriläisen lähestymistavan mukaan tarkoituksena on yrittää ymmärtää kirjoittajan tarkoitus. Puheteon lokuutiot edustavat Varsovan huippukokouksesta otettuja sitaatteja. Illokuution avulla aineistosta pyritään nostamaan esiin, mitä tekoja Nato on näillä tehnyt, ja vastaamaan siihen, miten ne muuttavat nykytilaa. (Skinner 2002, 104–105.) Perlokuutio jää tämän tutkimuksen ulkopuolelle, sillä aineistosta ei selviä, mikä on Naton jäsenvaltioiden reaktio kyberpuolustamiseen. Tarkastelun kohteena on Varsovan huippukokouksen kyberpuolustusta käsittelevä osio, josta on tarkoitus nostaa esiin keskeisiä kyberpuolustuksen linjausten lokuutioita. Näiden lokuutioiden perusteella pyrin selvittämään, mitkä ovat keskeisiä toimijoita Naton kyberpuolustamisessa, mitkä ovat keskeiset välineet sen vahvistamiseksi sekä mikä on taustalla oleva ympäristö, jota varten teko on laitettu liikkeelle.

Pyrkimyksenä on päästä siihen asiayhteyteen, jossa kyseinen lausunto on muodostettu. ”It is certainly an implication of my approach that our main attention should fall not on individual authors but on the more general discourse of their times.” (Skinner 2002, 118.) Vaikka kyseessä onkin kirjoittajan tarkoituksen löytäminen lausunnosta (utterance), tarkastelun kohteena ei ole kirjoittaja itse. Tarkoitus on tarkastella ajan yleistä keskustelua. Tähän yritetään päästä seuraavan esimerkin avulla. Kirjoittajan ottaessa aseman A voimme olettaa tämän silloin vastustavan sen vastakohtaa B. Tai kirjoittajan suositellessa teosta X voimme olettaa kirjoittajan kritisoivan teosta, joka on teoksen X vastakohta, ja niin edelleen. (Skinner 2002, 115–119.) Naton painottaessa tiettyä kantaa voimme olettaa sen vastustavan asian vastakohtaa. Kirjoittajan tarkoitus on läheisesti kytkeytynyt tämän motiiveihin (Skinner 2002, 120). Näin voimme ymmärtää, miksi kirjoittaja on muodostanut kyseisen lausunnon, ja päästä käsiksi siihen ympäristöön, jossa kirjoittaja on toiminut. Osiossa on tukeuduttu Varsovan huippukokouksen oppaan lisäksi aihetta käsittelevään lähdeaineistoon. Näiden avulla on tarkoitus saada mahdollisimman tarkka kuvaus siitä, mitä kyseisillä illokuutioilla tarkoitetaan.

3.1. Muuttuva turvallisuusympäristö

> Cyber threats and attacks are becoming more common, sophisticated and damaging. The Alliance is faced with an evolving complex threat environment. State and non-state actors can use cyber attacks in the context of military operations. In recent events, cyber attacks have been part of hybrid warfare. (Warsaw Summit Guide 2016, 124.)

Lainauksessa todetaan, että kyberhyökkäykset ovat yleistyneet ja niistä on tullut hienovaraisempia sekä vahingoittavampia. Siinä hyväksytään, ettei turvallisuusympäristö ole enää yhtä tuttu kuin ennen. Nato myöntää, että turvallisuusympäristö on muuttunut monimutkaisemmaksi eivätkä sen vihollisia ole ainoastaan valtiolliset toimijat vaan myös ei-valtiolliset toimijat. Ei-valtiolliset toimijat ovat myös osa sotilaallisia operaatioita. Nato liittää kyberhyökkäykset osaksi hybridisodankäyntiä, jonka yhteydessä niitä on esiintynyt viime aikoina. Taustalla voi olettaa olevan Krimin valtausta edeltäneet informaatiovaikuttamisen tapahtumasarjat. Ennen Krimin valloitusta hyökkäyksessä käytettiin laajaa informaatio-operaatiota, jota hyödynnettiin propagandan ja virheellisen tiedon levittämiseen. (Pietilä 2017, 55.) Hybridisodankäynnissä hyödynnetään molempia, sotilaallisia sekä ei-sotilaallisia toimia, joita käytetään tietyn päämäärän saavuttamiseksi. Tällaisia keinoja ovat muun muassa kyberhyökkäykset, taloudellinen painostus, valeuutiset, sotilaallisten joukkojen käyttö sääntöjen vastaisesti sekä asevoimien käyttö. (Ibid.) Näillä pyritään hämärtämään sodan ja rauhan välistä rajaa sekä luomaan epävarmuutta yhteiskunnassa. Näin ollen on yhä vaikeampi tiedostaa, missä menee sodan ja rauhan välinen raja. (NATO 2018.)

Käsitteiden käyttö ja niiden tarkoitus on löydettävissä kielellisestä toiminnasta (Palonen 2003, 37). Kyberpuolustuksen osion alussa on kuva, johon on sijoitettu sanat *worm*, *malware*, *virus*, *trojanhorse*, *spyware* ja *phishing* (Warsaw Summit Guide 2016, 124). Nämä kaikki ovat erilaisia haittaohjelmia. Ne luokitellaan sen mukaan, mitä ne tekevät ja mitä niillä halutaan saavuttaa. Kaikki, jotka liittyvät virtuaalimaailmaan, ovat sen toimijoita tavalla tai toisella, mutta toimijan päämäärä tai tavoite määrittää sen, mihin kategoriaan toimijat sijoittuvat. (Limnéll ym. 2014, 113.) Kyberhyökkääjiksi voidaan tämän väittämän perusteella nähdä valtiollisten toimijoiden lisäksi ei-valtiolliset toimijat, kuten terroristit, rikolliset, haktivistit ja yritykset (Suomen kyberturvallisuusstrategia 2013, 18). Nato määrittelee karkeasti, että valtiolliset sekä ei-valtiolliset toimijat voivat käyttää kyberhyökkäyksiä sotilaallisen operaation yhteydessä: ”State and non-state actors can use

cyber attacks in the context of military operations." (Warsaw Summit Guide 2016a, 124). Tällä viitataan kyberhyökkäysten sotilaalliseen ulottuvuuteen. Mikä tahansa näistä toimijoista voi olla Natolle uhka kybertoimintaympäristössä. Hyökkääjän motiivi ja toisaalta kybertoimintakyky voivat antaa viitteitä siitä, onko kyseessä valtiollinen toimija vai ei. Valtiollisilla toimijoilla on enemmän resursseja, jolloin valtioiden harjoittamat hyökkäykset ovat jo lähtökohtaisesti pidempikestoisia. (Ottis 2008, 1–6.)

> NATO has been increasingly targeted with cyber-attacks over the past decade. The majority of targeted attacks against NATO networks originate from state actors. Suspicious events are detected every day. Most of these are dealt with automatically. Some require analysis and response by NATO's cyber defence experts. In 2016 NATO experienced an average of 500 incidents per month – an increase of roughly 60% over 2015. (NATO 2018c, 1.)

Lainauksessa otetaan kantaa Naton kyberpuolustuksen menettelytapoihin. Vastaavia lukuja ei ole nostettu esiin Varsovan huippukokouksen oppaassa, ja siitä syystä lähde on otettu Naton omista julkaisuista. Lainauksessa todetaan, että toistaiseksi kybertoimintaympäristössä suurimmat uhkat muodostavat valtiolliset toimijat. Kyberhyökkäyksien määrä on kasvanut 60 prosenttia vuodesta 2015 vuoteen 2016 verrattuna. Tämä on yksi esimerkki siitä, että toimijat tekevät yhä enemmän kyberhyökkäyksiä kybertoimintaympäristöä hyödyntäen. Kyberhyökkäysten avulla voidaan painostaa valtio tai organisaatio myönnytyksiin, joita hyökkääjä vaatii. (Suomen kyberturvallisuusstrategia 2013, 17.) Lisäksi hyökkäyksillä pystytään aiheuttamaan fyysistä vahinkoa laitteille ja järjestelmille (Ibid., 18). Syynä tälle voi olla esimerkiksi se, että kyberhyökkäyksiä voidaan ostaa internetistä tai pienemmän kynnyksen hyökkäykset ovat helppoja ja halpoja tuottaa (Limnéll 2017). Kyberhyökkäyksien kohdalla puhutaan paljon kuitenkin attribuutio-ongelmasta. Tällä tarkoitetaan sitä, että hyökkäyksen varsinaista tekijää on vaikea saada selville tai todisteiden kerääminen voi olla haastavaa. (Fidler, Pregent & Vandurme 2013, 21.) Oman arvioni mukaan attribuutio-ongelma on myös poliittista toimintaa. Esimerkiksi valtiolla voi olla tiedustelun avulla tuotettua tietoa vastapuolesta, joten kyberhyökkäyksistä ei välttämättä kerrota. Valtio ei välttämättä joudu hyökkäyksistä vastuuseen, jos vastustajalla on jotain sellaista tietoa, jota ei haluta julkisuuteen.

Lisäksi lainauksessa mainitaan, että suurin osa hyökkäyksistä käsitellään automaattisesti. Osa hyökkäyksistä vaatii kuitenkin asiantuntijoiden tarkastelua ja toimenpiteitä. Kyberuhkien kannalta keskeinen toimija on NCIRC (Nato Computer Incident Response Capacity). Se on Naton keskeinen asiantuntija teknisellä, toiminnallisella ja

ennaltaehkäisevällä tasolla, sillä se vastaa Naton tietoverkkojen, toimistojen sekä operaatioiden turvallisuudesta. Nato pyrkii vahvistamaan sen kyberpuolustusta määrittelemällä mahdollisia järjestelmien haavoittuvuuksia esimerkiksi penetraatiotestauksilla. Harkituilla järjestelmään tehdyillä iskuilla haavoittuvuudet pystytään löytämään ja korjaamaan. Tätä kautta pystytään havaitsemaan hyökkäyksen laajuus ja luonne sekä vastaamaan niihin. Toisaalta Nato pyrkii kasvattamaan henkilöstönsä tietämystä erilaisilla harjoituksilla, koulutuksilla ja valmennuksilla. Sillä on myös käytössä järjestelmien havainnointilaitteita, jotka tarkkailevat mahdollisia merkkejä tunkeutujista ja haittaohjelmista tarkistamalla sähköposteja tai nettisivustoja. (Fidler, Pregent & Vandurme 2013, 10.)

> The policy establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO's cooperation with industry. The top priority is the protection of the communications systems owned and operated by the Alliance. (Warsaw Summit Guide 2016, 125.)

Yllä oleva lainaus nostaa esiin kolme keskeistä tekijää kyberpuolustuksen toimintaperiaatteesta (Policy on Cyber Defence). Nämä asiat ovat yhteinen puolustaminen, kansainvälinen oikeus sekä teollisuusyhteistyö. Lisäksi lainauksessa painotetaan, että yksi keskeisin tehtävä on Naton tietoliikenneverkoston ja tietojärjestelmien suojaaminen. Ensinnäkin Naton jokaisella jäsenmaalla on oma kyberturvallisuusstrategiansa, jossa määritellään kansallisella tasolla kyberturvallisuuden sekä sen kehittämisen vaatimukset. Nämä löytyvät Naton kyberpuolustuksen kehitys- ja harjoituskeskuksen sivuilta (NATO Cooperative Cyber Defence Centre of Excellence). Strategioissa esitellään jäsenvaltioiden kyberturvallisuuden näkemys, siihen tarkoitukseen luotu toimintamalli sekä strategiset linjaukset näiden päämäärien saavuttamiseksi. Kyberpuolustuksen toimintaperiaatteen avulla jäsenvaltiot tunnistavat Naton menettelytavat kyberturvallisuuden parantamiseksi. Natolla on myös toimintasuunnitelma (*action plan*), joka helpottaa toimintaperiaatteen toimeenpanoa käytännön tasolla. Linjauksen tarkoitus on ensisijaisesti keskittyä siihen, että Nato pystyy suojaamaan sen omat kommunikaatio- ja informaatiojärjestelmänsä. Nato on korostanut myös sen strategisessa konseptissaan, että sen tulee pystyä havaitsemaan, ehkäisemään ja puolustautumaan kyberhyökkäystä vastaan sekä palautumaan niistä mahdollisimman nopeasti. (Nato Policy on Cyber Defence 2011; Strategic Concept 2010, 16.) Keskeisintä toimintaperiaatteessa on se, että siinä painotetaan kyberpuolustuksen tärkeyttä yhteisessä puolustuksessa. Tämä juontaa juurensa vuosien 2013 ja 2015 GGE

(United Nations Group of Governmental Experts) -raporttien läpimurtoon tieto- ja viestintäteknologian ja kansainvälisen turvallisuuden välisessä suhteessa (Kerttunen 2018). Raportin läpimurto voidaan nähdä hyvänä edistysaskeleena, koska viimein kybertoimintaympäristö tunnistettiin yhdeksi kaikkia koskevaksi ulottuvuudeksi, jolloin se sai myös oikeudellisen ulottuvuuden. Kansainvälisillä areenoilla viimein tunnistettiin myös kirjallisesti, että sähköisiä menetelmiä hyödynnetään toimijoiden päämäärien saavuttamiseksi. Raportilla pyrittiin siihen, että valtioilla olisi ensisijainen rooli valvoa väärinkäytöksiä, joita pyrittäisiin tekemään tietoteknisiä menetelmiä hyödyntäen. (General Assembly 2015, 2.)

Miksi tuo siirto oli niin tärkeä tehdä ja mitkä olivat taustalla vaikuttavat tekijät, jotka siirron tekemiseen johtivat? (Skinner 2002, 104.) Krimin valtauksen yhteydessä käytettiin hybridisodan menetelmiä, kuten informaatio-operaatioita, kyberhyökkäyksiä sekä sotilaallisia toimia huomion siirtämiseksi johonkin muuhun kuin siihen, mitä todellisuudessa tapahtui. Kyberhyökkäyksien sekä muiden ei-sotilaallisten toimien, kuten informaatio-operaatioiden, hyödyntäminen tehdään sellaisella tasolla, etteivät ne ylitä artiklan 5 rajaa. (Pietilä 2017, 54.) Oletetaan, että tällä tapahtumasarjalla on ollut vaikutus myös Naton kyberpuolustuksen vahvistamiseen. Tämä hypoteesi muodostuu siitä, että näiden tapahtumien jälkeen Nato tunnisti kansainvälisen oikeuden kybertoimintaympäristössä. Tällä pyritään siihen, että valtiot pystyisivät ylläpitämään rauhaa, turvallisuutta sekä vakautta myös digitaalisessa ympäristössä. (General Assembly A/70/174 2015, 12.) Tarkoitus on mahdollistaa valtioiden reagointia hyökkäyksiin, joita niitä vastaan tehdään.

> We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales[…] (NATO 2016a.)

Vuotta 2016 on pidetty Naton toimintalinjauksien aikana. Yksi keskeisimpiä toimintalinjauksia oli lupaus kyberpuolustamisesta (Cyber Defence pledge). (Shea 2017, 169.) Tässä lupauksessa jäsenvaltiot lupautuvat huolehtimaan valtion tietoliikenneverkkojen päivittämisestä. Tämänkin yhteydessä painotetaan yhteistä puolustusta, jolla voitaisiin viitata siihen, että kyberpuolustusta pidetään erottamattomana osana yhteistä puolustusta. Naton jäsenvaltiot ovat vastuussa niiden omien verkkojen suojelemisesta, ja suojaustasojen tulee olla yhdenmukaiset. (Brussels Summit Guide 2018, 35.) Lupauksen päätavoitteita ovat muun muassa pysyä teknologisen kehityksen mukana sekä kehittää kyberpuolustusta kaikilla yhteiskunnan tasoilla niin taktisesti, operatiivisesti kuin strategisestikin. Sillä

pyritään yhteiseen käsitykseen kyberpuolustuksesta, jossa sen nähdään liittyvän kaikkeen liittouman toimintaan. Lisäksi painopisteenä on Euro-Atlantin alueen resilienssin parantaminen. (NATO 2016a.) Lupauksessa voi nähdä epäsuoran viittauksen turvallisuuden tunteeseen, resilienssiin, sekä Naton kulttuuriperinteeseen yhteisestä puolustamisesta. Lisäksi huomion kohteena on jäsenvaltioiden kansallinen infrastruktuuri sekä tietoliikenneverkosto. Kyberpuolustus on tiiviisti linkittynyt sen jäsenvaltioiden kyvykkyyteen tällä alueella. Keskeinen muutos Naton toiminnassa olikin sen painopisteen siirtyminen verkkojen suojelemisesta laajemmin Nato-maiden yhteiskunnan eri osa-alueiden suojelemiseen. Niillä pyrittiin vaikuttamaan poliittisiin järjestelmiin, jolloin kyberhyökkäysten konkreettinen vaikutus yhteiskunnan toimintaan huomattiin. Vuoden 2016 jälkeen kyberuhkat eivät olleet pelkästään yksittäisten yhtiöiden, yritysten tai palveluntarjoajien ongelma, vaan niistä tuli koko yhteiskuntaa koskettava asia. Nato on jokaisella osa-alueella riippuvainen sen kansallisista voimavaroista, koska liittoumalla ei ole yhteisesti omistettua omaisuutta lukuun ottamatta AWACS-lentokonetta. Näin ollen sen kyvykkyys toimia kybertoimintaympäristössä on riippuvainen sen jäsenmaiden kyvykkyyksistä: ”[…] Our interconnectedness means that we are only as strong as our weakest link […].” (NATO 2016a.) Edellä sanotaan, että Nato on juuri niin vahva kuin sen heikoin lenkki. Näin ollen kyse on Naton kyvystä asettaa tarpeeksi kunnianhimoiset tavoitteet sen jäsenvaltioille, jos se haluaa olla kyberpuolustuksen keihäänkärki liittoumana (Shea 2017, 165–174).

> Allies are committed to enhancing information-sharing and mutual assistance in preventing, mitigating and recovering from cyber attacks (Warsaw Summit Guide 2016, 125; Brussels Summit Guide 2018, 36).

Lauseen teko (illokuutio) on selvästi toimeksi antava. Siinä todetaan, että jäsenvaltiot ovat sitoutuneet informaation jakamiseen kyberpuolustuksen vahvistamiseksi. Mielestäni keskeistä on se, miten Nato saa jäsenvaltiot sitoutumaan tähän. Naton vahva kyberpuolustuksen lähtökohta on siinä, että sen jäsenvaltiot ovat kyberturvallisia. Naton kapasiteetti koostuu nimenomaan sen jäsenvaltioiden kyvykkyyksistä. Natolla on hyvät edellytykset olla kyberpuolustamisen keihäänkärki, sillä ainakin Yhdysvallat, Iso-Britannia, Ranska ja Saksa on nimetty ”kybervaltioiksi” ja näistä jokainen on myös Naton jäsenvaltio. (NATO Cooperative Cyber Defence Centre of Excellence 2015.) Kyberturvallisuuden keskeisin asia on luottamus. Kyberpuolustus voi olla ainoastaan silloin vahva, jos luotamme kybertoimintaympäristön toimivuuteen. (Limnéll ym. 2014, 40; Suomen

kyberturvallisuusstrategia 2013, 1.) Valitettavaa on se, että nykyään turvallisuuden tunne alkaa kääntymään meitä itseämme vastaan, vaikka asian pitäisi olla toisin päin. Tämä johtuu informaation paljoudesta. Jos avoimuus ja kriittinen suhtautuminen asioihin puuttuvat, alamme uskomaan siihen todellisuuteen, joka meille on kuvitettu. Tämä on merkittävää siksi, että menettäessämme turvallisuuden tunteen menetämme myös luottamuksen, avoimuuden sekä kriittisen arviointikyvyn sen suhteen. Näin alamme uskomaan asioita, joita ei oikeasti ole. (Limnéll ym. 2014, 40–41.)

> NATO is also helping member countries by sharing information and best practices, and by conducting cyber defence exercises to help develop national expertise. Similarly, individual Allied countries may, on a voluntary basis and facilitated by NATO, assist other Allies to develop their national cyber defence capabilities. (Warsaw Summit Guide 2016, 125.)

Nato on painottanut informaation jakamisen tärkeyttä osana vahvempaa kyberpuolustusta. Kyberturvallisuus ja sitä kautta kyberpuolustus lähtevät Natossakin ensin kansalliselta tasolta. Informaatiolla on nykyään paljon painoarvoa, joten ovatko yksittäiset, varsinkin kybervaltiot, valmiita jakamaan arkaluontoista informaatiota muille? (Fidler ym. 2013, 18.) Nato-maiden informaation jakamisen kannalta yksi keskeisimmistä alustoista on Smart Defence, jonka tarkoitus on tuoda Naton jäsenvaltiot yhteen tekemään yhteistyötä vahvemman puolustuksen mahdollistamiseksi. Tämän idea on, että jäsenvaltiot voivat kehittää yhteistyössä ja ylläpitää sellaisia voimavaroja, joihin heillä ei yksittäisinä jäsenvaltioina olisi mahdollisuutta. Alustan avulla voidaan esimerkiksi jakaa tietoa erilaisiin haittaohjelmiin liittyen. Tätä kautta jäsenet kehittävät kyberpuolustuksen toimintakykyä sekä panostavat koulutukseen sekä harjoitustoimintaan erilaisten projektien kautta. Näiden avulla pyritään siihen, että Nato pystyy mahdollisimman hyvin ylläpitämään sen yhteisen puolustuksen tehtävää. (NATO 2017c.) Päätelaitteita käyttävä henkilöstö tarvitsee koulutusta kyberhyökkäysten perinteisistä menettelytavoista. Portugali on ottanut vastuun tällaisesta koulutuksesta, mutta lisäksi se on vastuussa tieto- ja viestintäopetuksesta. Tämä oppilaitos toimii samaan aikaan harjoituskeskuksena kuin foorumina Naton henkilöstön, akatemian sekä teollisuudenalan välillä. Belgia taas on onnistunut luomaan haittaohjelmiin liittyvän informaatioalustan, joka on otettu Naton jäsenmaiden lisäksi käyttöön Euroopan unionissa. Lisäksi Romania ja Alankomaat ovat ottaneet käyttöön järjestelmän, joka keskittyy tilannekuvan parantamiseen sekä tapahtumien koordinoimiseen. Nato on

lupautunut avustamaan maita, jotka suostuvat johtamaan kyberpuolustukseen liittyviä projekteja. (Shea 2017, 170–171.)

Kyberpuolustus on yksi kiinteä osa muuta puolustusta eikä oma erillinen puolustuksen osa-alue. Yhteiskunnan elintärkeiden toimintojen ja toimijoiden toiminta pystytään turvaamaan myös poikkeusoloissa. (Turvallinen Suomi 2018, 9; Valmiuslaki 1552/2011.) Kyberhyökkäyksiä käytetään, kun halutaan testata vastustajan kohteen haavoittuvuutta ja reagointikykyä, hankkia kohteesta informaatiota, lamaannuttaa vastustajan toimintaa tai hämätä sitä. Kyberhyökkäyksiä käytetään pääsääntöisesti työkaluina jonkun tietyn päämäärän saavuttamiseksi. Kuitenkin digitalisaation kasvun myötä myös tavalliset kansalaiset, yritykset, järjestöt sekä viranomaiset ovat osa haavoittuvuutta, johon kyberhyökkäyksillä voidaan vaikuttaa. Kyberhyökkäyksien haaste on se, että ne voidaan toimeenpanna salassa ja huomaamatta. Toisinaan tarkoitus onkin, ettei vastustaja tiedä hyökkäyksistä mitään. Haasteellista tämän huomioimisessa on se, että hybridivaikuttamisen komponentit pystytään pitämään varsin pitkään salassa. Hyökkäyksiä voidaan ostaa rikollisilta, huomio voidaan kiinnittää muualle ja toisaalta toiminta voidaan kieltää, mikäli vastustaja ei pysty hyökkäyksiä todistamaan. (Hyytiäinen 2018, 27–29.)

> Recognising that cyber defence is as much about people as it is about technology, NATO continues to improve the state of its cyber defence education, training, exercises and evaluation (Warsaw Summit Guide 2016, 126; Brussels Summit Guide 2018, 37).

Tässä lausunnossa tunnistetaan, että kyberpuolustus on yhtä paljon kiinni ihmisistä kuin teknologiasta. Naton suorituskyky perustuu kolmeen keskeiseen tekijään eli harjoitustoimintaan, koulutukseen sekä valmennustoimintaan. Kyberpuolustuksen kannalta keskeisiä harjoituksia ovat Cyber Coalition Exercise sekä Nato Cyber Range. Näiden harjoitusten tarkoituksena on integroida kyberpuolustukseen liittyvät toiminnot yhteen sekä huomioida nämä myös muussa harjoitustoiminnassa. Tilannekuvan parantamiseksi kaikki Naton jäsenvaltiot ovat allekirjoittaneet asiakirjan MOU (Memorandum of Understanding on Cyber Defence), jotta informaatio kulkisi paremmin jäsenvaltioiden välillä. (Brussel Summit Guide 2018, 37.) Se on yksi työkalu, jolla jäsenmaat voivat kehittää niiden kyberkyvykkyyttä, tuoda esiin jo havaittuja kyberhyökkäysten muotoja sekä parantaa informaation kulkua ja jakamista.

Naton valtuuttama kehitys- ja harjoituslaitos (Nato Cooperative Cyber Defence Centre of Excellence, CCDCOE) sijoitettiin Viroon vuoden 2007 pronssisoturikiistan jälkeen. Siellä keskitytään kyberpuolustamisen opetukseen, konsultointiin, arviointiin, tutkimukseen ja kehitykseen. Vaikka se ei ole Naton hallintorakenteen virallinen oppilaitos,

se tuo arvokasta asiantuntijuutta ja kokemusta Naton oppilaitosten rinnalle. Saksassa Naton oppilaitos tarjoaa tukea Naton kyberpuolustuksen eri osa-alueisiin. Italian ensimmäisessä oppilaitoksessa tarjotaan koulutusta Naton tieto- ja viestintäjärjestelmien toiminnoista sekä niiden ylläpitoon niin Naton henkilöstölle kuin sen jäsenmaille. Toisessa oppilaitoksessa opetetaan strategista johtamista niin poliittisissa kuin sotilaallisissa tilanteissa. (Warsaw Summit Guide 2016, 125–126.) Nämä yllä mainitut asiat nousevat huippukokouksen oppaassa keskeisimmiksi, kun tarkastellaan sitä, mitä Nato on tehnyt kyvykkyyden vahvistamiseksi. Lopulta ihminen on heikoin lenkki myös kyberpuolustuksessa, sillä aina joku menee hyökkääjien ansaan. McAfee labsin uhkaraportti varoittaa, että yksi kymmenestä lähetetystä tietojenkalastelusähköpostista on onnistunut. Eli kaikki palaa lopulta ihmiseen, minkä takia myös Naton tulee panostaa koko Naton henkilökunnan koulutukseen, ei pelkästään kyberpuolustamisen kannalta keskeiseen hallintorakenteeseen. (Shea 2016, 171.)

Tässä alaluvussa Naton kyberpuolustuksen kuva on rakentunut harjoitustoiminnan, informaation jakamisen, kriittisen infrastruktuurin, ihmisten kyvykkyyden, yhteisen puolustuksen sekä kansallisen että kansainvälisen asiantuntijuuden ympärille. Kyberpuolustus on monen tekijän summa. Muuttunut turvallisuusympäristö edellyttää näitä asioita, jotta kyberpuolustus toimii. Eniten se kuitenkin edellyttää poliittista tahtoa, jota käsitellään seuraavaksi.

3.2. Onko vahvaa kyberkyvykkyyttä ilman poliittista tahtoa?

> The NATO Policy on Cyber Defence is implemented by NATO's political, military and technical authorities, as well as by individual Allies. The North Atlantic Council (NAC) provides high-level political oversight on all aspects of implementation. The NAC is apprised of major cyber incidents and attacks, and it exercises principal authority in cyber defence-related crisis management. (Warsaw Summit Guide 2016, 126.)

Pohjois-Atlantin neuvosto (NAC) on liittouman pääasiallinen päätöksentekoelin. Sen alainen neuvosto on kyberpuolustuksesta vastaava valiokunta (Cyber Defence Committee), joka toimii keskeisenä koordinoijana Naton sotilaallisen komento-osaston sekä edustustojen välillä, ja se on tärkeä linkki teknisen toimintaosaston, toimintaperiaate- ja päätöksentekoprosessien eri tasoilla. Naton kyberpuolustuksesta vastaava neuvosto (CDMB) tuo kaikki keskeiset tekijät yhteen arvioimaan ja vastaamaan osaan kyberhyökkäyksistä. Naton komento- ja hallintoyksikkö (NC3) on vastuussa Naton

operaatioiden ja muun toiminnan teknisestä toteutuksesta. Naton sotilasviranomaiset (NMA) vastaavat Naton operatiivisesta valmiudesta sekä sen käyttöönotosta. Naton yhdestä suurimmasta kyberharjoituksesta (Cyber Coalition Exercise) on vastuussa Naton transformaatio-osasto (ACT). Naton tieto- ja viestintävirasto (NCIA) on vastuussa kyberturvallisuuspalveluiden tuottamisesta Natolle. Naton tietoturvahaavoittuvuuksista vastaava tekninen keskus (NCIRC Computer Incident Response Capacity, NCIRC Technical Centre) vastaa kaikesta liittoumaan kohdistuneista kybertapauksista, joista se raportoi sekä levittää tietoa johdolle ja käyttäjille. (Shea 2017, 171–172; Warsaw Summit guide 2016, 127; Brussels Summit Guide 2018, 38.)

Kyberpuolustus tarvitsee ympärilleen vahvan yhteisön, jossa jokaiseen ketjun jäseneen pitää pystyä luottamaan. Esimerkkejä sopimuksista ovat jo aiemmin mainitut lupaus kyberpuolustuksesta (cyber defence pledge) sekä muistio kyberpuolustuksen tietoisuuden parantamisesta (Memorandum of Understanding Cyber Defence). Mikäli näillä sopimuksilla ei ole riittävästi painoarvoa tai jokaisella hallintorakenteen tasolla ei ole luottamusta, jäsenvaltiot ovat todennäköisesti haluttomia jakamaan asiantuntijuutta ja tietoa toisilleen. Toisaalta, kun kyberhyökkäyksiä on alettu käyttämään enenevissä määrin tavanomaisen sodankäynnin instrumentteina, tämä luo paineita myös toisille valtioille pärjätä tällä osa-alueella. (Lewis 2015, 4.) Viimeisimmäksi Brysselin huippukokouksessa Nato-maat tekivät julistuksen, jossa he lupautuivat käyttämään kaksi prosenttia bruttokansantulosta puolustuksen vahvistamiseen. Nykyinen kyberpuolustuksen lupaus velvoittaa jäsenvaltioita käyttämään osan tästä kyberpuolustamisen vahvistamiseen. Jäsenvaltiot ovat haluttomia jakamaan arkaluontoista aineistoa sellaisten jäsenvaltioiden kanssa, jotka eivät ole tuoneet kansallista kyberpuolustustaan vähimmäisvaatimusten tasolle. Läpinäkyvyys tulee olemaan Natolle tärkeä tekijä, jotta se pystyy tunnistamaan aukot ja priorisoimaan liittouman tarpeita. (Shea 2017, 171–172.)

Natolla tulee olemaan haasteita sen päätöksenteossa kybertoimintaympäristössä, sillä sen päätöksenteko perustuu yksimielisyyteen. Tämä tarkoittaa sitä, että Naton kaikki päätökset perustuvat jokaisen jäsenmaan hyväksyntään. Keskusteluja päätöksistä käydään siihen asti, kunnes yhteinen ymmärrys on saavutettu. (Nato 2016b.) Esimerkiksi kyberpuolustamisen kannalta haasteelliseksi muodostuu kysymys, kuinka aktiivinen Naton tulisi olla kyberpuolustamisessa. Kun päätökseen tarvitaan jokaisen jäsenvaltion hyväksyntä, voi päätökseen pääsemiseen mennä aikaa. Kybertoimintaympäristö edellyttää huomattavasti nopeampaa reagointia. (Fidler ym. 2013.) Tässä ympäristössä tapahtuvat asiat tapahtuvat jopa huomaamatta. Nykyään päätöksenteko ei voi pohjautua ainoastaan niihin tapauksiin, jotka ovat jo tapahtuneet. Enenevissä määrin tarvitaan ennakointia ja

varautumista sekä mielikuvitusta siihen, mitä tulevaisuudessa voi tapahtua. Naton kannalta varautuminen tässä yhteydessä tarkoittaa esimerkiksi harjoitus- sekä koulutustoimintaa. Lisäksi varautumiseen liittyväksi toiminnaksi määritellään valmiussuunnittelu sekä jatkuvuuden hallinta. Varautumisen tarkoitus on toimia ennaltaehkäisevänä toimintana, jonka avulla pyritään tehtävien mahdollisimman normaaliin toimintaan (Yhteiskunnan turvallisuusstrategia 2017, 9). Ennakoinnin merkitys on aina ollut tärkeä, sillä kaikki strategiset linjaukset tai yksittäiset strategiat kirjoitetaan ennakointilähtöisesti: ”Ennakointi antaa tulevaisuuden koko kirjon, strategia antaa fokuksen ja doktriini kertoo, miten fokuksessa toimitaan.” (Kuusisto 2018, 12.) Sen tarkoituksena on pyrkiä kuvaamaan tulevaisuutta mahdollisimman tarkasti saatavilla olevan tiedon kautta. Voidaan sanoa, että joku ilmestyy aina jostakin, mutta ei kuitenkaan tyhjästä. Toimintaympäristö on tila, joka ilmestymisen mahdollistaa (Ibid., 13). Turvallisuuskulttuurin ilmentyminen vaihtelee jäsenvaltioiden välillä. Nämä asiat vaikuttavat myös siihen, mitä asioita Nato painottaa kyberpuolustamisessa (Palonen 2003, 37). Jäsenvaltioita on yhteensä 29, joten näiden turvallisuuskulttuurien integroiminen on oma tehtävänsä. Kybertoimintaympäristö on ennen kaikkea poliittinen. Se vaatii vahvaa poliittista tahtoa ja johtajuutta, jotta kyberhyökkäyksiin pystytään vastaamaan. Miten kyberpelotetta rakennetaan poliittisesti? Tämä edellyttää selviä pelisääntöjä siitä, miten tietyissä tilanteissa tulee toimia. (Limnéll 2017.)

> […]The Alliance also welcomed efforts undertaken in other international fora to develop norms of responsible state behaviour and confidence-building measures to foster a more transparent and stable cyberspace for the international community. As most crises and conflicts today have a cyber dimension, treating cyberspace as a domain would enable NATO to better protect its missions and operations. (Warsaw Summit Guide 2016, 128.)

Skinner edustaa sitä koulukuntaa, jossa lukija ei voi olla huomioimatta tekstin kirjoittajaa, koska tekstin tarkoitus on löydettävissä kirjoittajan perusteella (Skinner 2002, 57). Sen takia tulee ottaa huomioon ympäristö, johon teksti on kirjoitettu (Palonen 2003, 20). Vaalivaikuttamisen nousu oli myös yksi keskeinen tekijä siihen, miksi myös Naton jäsenmaat huolestuivat demokratian ytimeen kohdistuvista hyökkäyksistä. Siitä tuli selkeästi poliittinen asia. Hyökkäyksiä havaittiin Yhdysvaltojen lisäksi myös esimerkiksi Saksassa, Itävallassa, Alankomaissa sekä Ranskassa. Kyberhyökkäykset osana hybridisodankäyntiä toivat myös valtiot jatkuvan uhkan kohteiksi. (Shea 2017, 166–167.) Venäjän kyky ja uhka hyödyntää kyberhyökkäyksiä demokraattisia instituutioita kohtaan ja sen vaikutus demokratian ytimeen eli päätöksentekoon nousivat keskeisiksi huolenaiheiksi. Lisäksi sähköverkon häiriö Ukrainassa, huhut Pohjois-Korean ydinaseohjelmasta sekä terroristeille

mahdollistuneet keinot internetin välityksellä lisäsivät kyberhyökkäysten tietoisuutta. (Shea 2017, 165.)

Voimme havaita käsitteellisen muutoksen poliittisen muutoksen yhteydessä ja toisinpäin. Tämä viittaa siihen, millaiseksi Nato kokee kyberpuolustuksen aseman maailmassa. Lausuntojen avulla pyritään näkemään, miten Nato ratkaisee kyberpuolustuksen poliittisia ongelmia ottamalla huomioon sen toimintaympäristön. (Farr 1989, 38.) Naton kyberpuolustus jakaantuu teoreettisesti kybertoimintoihin, hallintoon sekä kehitykseen. Selkeä painotus on nähtävissä mainittuun toiminnot-osioon, jossa painotuksena ovat kyberpuolustuksen menettelytavat, kyberkyvykkyys, kybertoiminta sekä yhteistyö niin teollisuuden kuin Euroopan unioninkin kanssa. Tulkintani mukaan painotus on näissä sen takia, että niillä pyritään osoittamaan Naton kyky, voima ja potentiaali toimia tehokkaasti myös kybertoimintaympäristössä. Käänteentekevä asia oli jo aiemmin mainittu tulkinnallinen muutos kybertoimintaympäristöön, eli kyberpuolustusta ei nähty enää pelkästään tietoliikenneverkon tai digitaalisten laitteiden suojelemisena, vaan se nähtiin ennemminkin Nato-maiden demokraattisten instituutioiden autonomian turvaamisena. Toisin sanoen kyberpuolustus sai myös teknisen käsityksen sijaan poliittisen merkityksen. Kyberhyökkäykset nähtiin yksittäisen verkkoon tunkeutumisen sijaan pyrkimyksenä vaikuttaa poliittisiin päätöksiin ja väylänä poliittiseen painostukseen tai pelotteluun. (Shea 2017, 166.) Naton viesti Varsovan huippukokouksen oppaassa oli se, että Nato voi vastata artiklan 5 edellytyksin myös kybertoimintaympäristön iskuihin. Kyse on poliittisen kyberpelotteen luomisesta (Limnéll 2017). Sopimukset kyberpuolustuksen parantamiseksi, harjoitustoiminta, tiedottaminen ja opetus ovat Naton kyberkyvykkyyden osoittamista. On toinen asia, miten hyvin näihin pystytään vastaamaan poliittisin keinoin.

4. Pelotteen rakentuminen kybertoimintaympäristössä

Tässä luvussa käsitellään peloteteorian kahta näkökulmaa, jotka ovat pelote rangaistuksesta (deterrence by punishment) ja pelote vahvasta puolustuksesta (deterrence by denial). Vuosien 2014 ja 2016 aikana Naton painopiste siirtyi pelkästä verkkojen suojelemisesta kyberpuolustukseen yhtenä operatiivisena osa-alueena niin maan, meren ja ilman rinnalla. Lisäksi vahva kyberpuolustus on nykyään oleellinen osa näiden operatiivista valmiutta. Tässä luvussa pelote rangaistuksesta (deterrence by punishment) ymmärretään Naton yhteisen puolustuksen tuomana pelotteena. Vahva puolustus (deterrence by denial) nähdään Naton kyvykkyytenä vastata kyberpuolustukseen tietyllä operatiivisella alueella.

Tämä luku keskittyy kyberpuolustuksen ja yhteisen puolustuksen väliseen tarkasteluun. Varsovan huippukokouksen opas luo pohjan tälle osiolle, vaikka painopiste on Naton perustamissopimuksen artiklan 5 ja tätä kautta myös YK:n peruskirjan artiklan 2(4) sekä 51 välisessä rajapinnassa. Varsovan huippukokouksen oppaassa todetaan, että kansainvälinen oikeus pätee myös kybertoimintaympäristössä. Tämä tarkoittaa teknologianeutraalin lähestymistavan ottamista kyberpuolustukseen, jolloin kyberhyökkäyksen voidaan nähdä täyttävän aseellisen hyökkäyksen tavoin artiklan 5 ehdot.

Luvussa esitellään Viron pronssisoturikiistaa vuodelta 2007 sekä Iranin ydinvoimalaan kohdistunutta Stuxnet-haittaohjelmaa vuodelta 2010. Viron pronssisoturikiista on valittu tähän sen takia, että Viro oli jo tuolloin Naton jäsenvaltio. Näin voidaan tämän esimerkin ja siihen tueksi otetun lähdeaineiston avulla tarkastella, mitä tekoja Nato on tehnyt kyberpuolustuksen suhteen. Stuxnet on valittu tähän siitä syystä, että sen jälkeen alkoi uusi aikakausi. Haittaohjelman merkittävin saavutus oli se, että sillä pystyttiin aiheuttamaan fyysistä vahinkoa sähköisiin järjestelmiin ja laitteisiin (Suomen kyberturvallisuusstrategia 2013, 18). Näistä esimerkeistä saatujen havaintojen perusteella luvussa tarkastellaan tarkemmin sitä, mitä aseellinen hyökkäys tarkoittaa kybertoimintaympäristössä. Koska artiklan 5 mukaan aseellinen hyökkäys oikeuttaa itsepuolustukseen, pyritään hakemaan selvyyttä siihen, mitä se tarkoittaa kybertoimintaympäristössä. Kyberpuolustuksessa on havaittavissa käsitteellinen muutos vuosien 2014 ja 2016 aikana. Tässä luvussa tarkastellaan Naton rakentaman kuvan perusteella kyberpuolustuksen merkittävyyttä yhteisessä puolustuksessa. Kaikki lainaukset on otettu Skinnerin puheteon mallia hyödyntämällä, eli lainaukset edustavat tässäkin sitä, mitä on sanottu (lokuutio). Tarkoitus on niiden avulla selvittää, miten artiklan 5 alla kyberhyökkäykset toimivat pelotteena eli mitä tekoja lainauksissa on tehty (illokuutio).

4.1. Pronssisoturikiista

Viroa vastaan tehtiin sarja kyberhyökkäyksiä 27.4.–18.5.2007. Tämä sarja sai alkunsa, kun Viron hallitus päätti siirtää pronssisen soturipatsaan, joka oli pystytetty Tallinnan Tõnismäelle. Kyberhyökkäysten taustalla oli pronssisoturikiista etnisten venäläisten sekä virolaisten välillä. Pronssisoturi sijoitettiin Tallinnan keskustaan toisen maailmansodan jälkeen symboliksi natsi-Saksan voitosta. Tilanne kuitenkin kärjistyi provosoitumisten ja mellakoinnin takia, ja patsas päätettiin siirtää uuteen paikkaan 26. huhtikuuta 2007. Tästä seurannut mellakointi ja väkivalta saivat jatkoa kybertoimintaympäristössä, jossa hyökkäykset kestivät melkein kuukauden. Kohteina olivat valtiolliset ja poliittiset kohteet, kuten valtion laitokset sekä verkkopalvelut. (Tikk, Kaska & Vihul 2010, 20.) Ei ole siis yllättävää, että kohteena olivat valtion instituutiot, koska Viron hallitus päätti siirtää patsaan, joka kosketti sekä virolaisia että venäläisiä.

Hyökkäysmuotoina käytettiin palvelunesto- (denial of service, DoS) sekä hajautettua palvelunestohyökkäystä (distributed denial of service, DDoS). Palvelunestohyökkäys kohdistetaan esimerkiksi palvelimille tai verkkosivustoille, ja sillä pyritään estämään pääsy kyseiselle palvelimelle. Hajautetussa palvelunestohyökkäyksessä taas käytetään useista tietokoneista koostuvia botnetteja. Niiden avulla muodostetaan ”tietokonejoukkoja”, joiden avulla osallistutaan palvelunestohyökkäykseen. Hajautetussa palvelunestohyökkäyksessä tällaisen botnetin voi luoda esimerkiksi roskasähköpostilla. Viesti sisältää esimerkiksi linkin, jonka kautta laitteen käyttäjä osallistuu hajautettuun palvelunestohyökkäykseen. Usein käyttäjä ei tiedä, että tietokone osallistuu tällaiseen. Kohteina näille hyökkäyksille olivat muun muassa Viron kahden suurimman pankin verkkopankkisivustot, internetin palveluntarjoajat, mediayritykset sekä webhotellit. Lisäksi hyökkäysten kohteina olivat muun muassa valtiolliset ja poliittiset nettisivustot. (Tikk, Kaska & Vihul 2010, 20–22.)

Hyökkäykset eivät ainoastaan vaikuttaneet niiden kohteisiin, vaan ne vaikuttivat myös keskisuuriin ja pieniin yrityksiin kuin myös tavallisiin kansalaisiin. Tämä johtuu siitä, että hyökkäyksen kohteeksi joutuivat suuret yritykset ja organisaatiot, joilla on vaikutusta monen muun yrityksen ja yksittäisten henkilöiden toimintaan. Kuitenkin hyökkäysten vaikutuksista on epäselvää tietoa, ja on vaikea sanoa, kuinka suuri vaikutus niillä esimerkiksi yhteiskunnallisesti loppujen lopuksi oli. (Tikk, Kaska & Vihul 2010, 20–22.) Hyökkäykset, jotka kohdistuivat valtiohallinnon verkkosivuille, eivät aiheuttaneet merkittävää yhteiskunnallista vahinkoa, koska pääsyn esto näille sivustoille ja niiden sisältöön oli lyhytaikaista. Lisäksi palvelimien tietosisältö on hajautettu. Tällä varmistetaan, että tieto on

tallennettu useaan eri kohteeseen, eli se ei häviä, jos yksi palvelin kaatuu. Hyökkäysten vaikutukset, jotka kohdistuivat valtion verkkopalvelun eesti.ee palveluihin, ovat epäselvät. Näitä palveluita osa väestöstä käyttää esimerkiksi veroilmoitusten tekemiseen ja valtion etuuksien sekä tukien hakemiseen, joten hyökkäyksen aikana tehdyt ilmoitukset ja hakemukset hidastuivat, mutta niiden haittavaikutuksista ei ole selvyyttä. Virossa ei ole maailmanlaajuisia suuria uutistoimistoja, joten tiedon saanti Virosta hyökkäysten aikana vaikeutui, ja koska hyökkäysten aikana kaadettiin palvelimet, joiden kautta tietoa oli aiemmin jaettu. Lopuksi psykologisena vaikutuksena voidaan todeta, että varsin pienellä vaivalla voidaan saada näin suuri iskusarja aikaiseksi ja aiheuttaa epävarmuuden tunnetta sekä vahinkoa koko yhteiskunnalle. (Tikk, Kaska & Vihul 2010, 21–25.)

Yleisesti on pidetty varmana, että Venäjän valtio on tukenut iskuja Viron hallintoa vastaan. Todisteita on löytynyt siitä, että tuona aikana tehdyt hyökkäykset on tehty Viron alueen ulkopuolelta. Kyberhyökkäyksillä voidaan sanoa olleen selkeä poliittinen motivaatio, ja ne sisälsivät selvän vihjeen venäjänkielisestä taustasta. Ohjeita hyökkäyksiin levitettiin monille venäjänkielisille foorumeille ja verkkosivustoille. Lisäksi ne sisälsivät yksityiskohtaiset ohjeistukset, miten hyökkäys Viron eri palvelimille tehdään. (Ottis 2008, 1–6.) Kyberhyökkäyksien alkuperästä on kiistoja, mutta voidaan kuitenkin pitää selvänä, että hyökkäyksillä oli yhteys Viron ja Venäjän väliseen konfliktiin pronssisoturipatsaasta (Ibid.). Tämän tapauksen seurauksena Nato päätti perustaa 2007 Tallinnaan NATO Cooperative Cyber Defence Centre of Exellence -yksikön, johon kuuluu asiantuntijoita niin tekniikan, strategian, operaatioiden sekä lain tieteenaloilta. (Warsaw Summit Guide 2016, 126.)

4.2. Stuxnet-haittaohjelma

Stuxnet oli kohdistettu Iranin viiden eri tehtaan tietokonejärjestelmiin. Mato ehti vaikuttaa järjestelmissä kesäkuusta 2009 toukokuuhun 2010. Mato ohjelmoitiin vahingoittamaan Siemensin kehittämää teollisuuden valvonta- ja tiedonhankinnan ohjausjärjestelmää, Supervisory Control And Data Acquisitiota (SCADA). Se oli suunniteltu muuttamaan Natanzin uraanirikastamon sentrifugien ohjauslogiikkaa hidastamalla tai kiihdyttämällä tehtaiden taajuusmuuttajan ohjausjärjestelmiä. Mato piilotti nämä muutokset laitteiden käyttäjiltä. (Ziolkowski 2012, 3–4.)

Taajuusmuuttajat saavat sentrifugit pyörimään tietyllä nopeudella tiettyyn suuntaan. Näitä taajuusmuuttajia ohjaa Siemensin ohjauslogiikka Siemens Simatic Step 7, joka on

maailmanlaajuisesti käytetyin ohjauslogiikka. Mato osasi tunnistaa Siemens Simatic Step 7 -ohjauslogiikkajärjestelmän, johon liittyy tietyt taajuusmuuttajat ja sentrifugit. Kun mato tunnisti olevansa oikeassa kohteessa, se aktivoitui ja alkoi käyttämään näitä taajuusmuuttajia virheellisillä asetuksilla. Stuxnet onnistui vahingoittamaan Natanzin tehtaan 5000 sentrifugista 1000. Merkittävää oli se, että mato levisi maailmalla satoihin tuhansiin tietokoneohjelmiin, mutta ei aktivoitunut niissä, koska se tunnisti, ettei kyseessä ollut iranilainen uraanirikastamo. Se olisi voitu uudelleenohjelmoida ja näin olisi onnistuttu aktivoimaan mato myös maailmanlaajuisesti. (Moilanen 2017; Ziolkowski 2012.)

4.3. Kyberpelotteen rakentuminen

Oleellisin ero kyberhyökkäyksen ja aseellisen hyökkäyksen välillä on se, miten määritellään voimankäyttö ja aseellinen hyökkäys (Kerttunen 2018). Varsovan huippukokouksessa Nato vahvisti: ”NATO has affirmed that international law applies in cyberspace.” (Warsaw Summit Guide 2016, 124.) YK:n turvallisuusneuvoston tehtävä on määritellä, mitkä tekijät ovat uhkaksi kansainväliselle rauhalle ja turvallisuudelle. Luvussa 1.1. esiteltiin toimet, jotka voivat uhata kansainvälistä rauhaa ja turvallisuutta. Lisäksi neuvoston kuuluu määritellä, milloin ja missä tilanteissa on oikeutettua käyttää voimakeinoja rauhan ylläpitämiseen ja säilyttämiseen. (Tikk & Kerttunen 2018.) YK:n perustuskirjan artikla 51 luo mandaatin myös Naton yhteiselle puolustukselle. Naton pelote on ollut vuodesta 1949 asti sama, eli aseellisen hyökkäyksen kohdistuessa Naton jäsenvaltiota vastaan se katsotaan hyökkäykseksi kaikkia jäsenvaltioita vastaan. Tämä oikeuttaa jäsenvaltiot käyttämään myös sotilaallista voimaa rauhan saavuttamiseksi liittouman alueella. Tänä päivänä se tarkoittaa sitä, että hyökkäys yhtä jäsenvaltiota vastaan on hyökkäys 29 jäsenvaltiota vastaan. (NATO 2018c.)

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.
>
> Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security. (The North Atlantic Treaty 1949, article 5.)

Lausunto on selkeä julistus ja lupaus, jossa painotetaan sitä, että aseellinen hyökkäys oikeuttaa käyttämään itse- tai yhteistä puolustusta rauhan ylläpitämiseksi Nato-maiden alueella. Näin ollen se on myös varoitus Naton vihollisille (Skinner 2002, 96–98). Aseellisella hyökkäyksellä on kaksi määritelmää kansainvälisessä oikeudessa: jus ad bellum ja jus in bello. Jus ad bellum viittaa tilanteeseen, jossa sota on oikeutettua, eli voimakeinot sallitaan osana itsepuolustusta. Tässä luvussa YK:n artikla 51 ja Naton artikla 5 käsittää jus ad bellumin eli oikeuden yhteiseen puolustukseen. (Schmitt 2012, 283.) Jus in bello tarkoittaa taas sitä, miten sotaa tulee laillisesti käydä. Tällöin viitataan tilanteeseen, jossa jus ad bellum on jo otettu käyttöön. (International Committee of the Red Cross 2014, 1.) Kyberhyökkäyksien haaste jus ad bellumille sekä jus in bellolle esitetään tässä luvussa. Tarkoitus on tässä viitekehyksessä huomioida myös pelotteen tehokkuus kyberpuolustuksen yhteydessä.

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations (UN Charter, article 2(4)).

YK:n peruskirjan artikla 2(4) on varoitus siitä, ettei kukaan saa uhata voimakeinoin toisen valtion alueellista koskemattomuutta tai poliittista itsemääräämisoikeutta. Valtioilla on oikeus käyttää voimakeinoja rikkomatta artiklaa 2(4), jos sitä vastaan kohdistetaan aseellinen hyökkäys. Kun valtio on oikeutettu itsepuolustukseen, sen ei tarvitse odottaa turvallisuusneuvoston hyväksyntää vastatoimenpiteisiin. (Schmitt 2012, 285.) Aseelliseksi hyökkäykseksi nähdään yleensä toimet, kuten sodan julistaminen, alueen miehitys, sotatoimet, saartaminen, kriittisten järjestelmien tuhoaminen, voimakeinot aluetta vastaan sekä vihamielinen toiminta. Yleisesti nähdään, että aseellinen hyökkäys on toimintaa, joka aiheuttaa merkittävää haittaa ja tuhoa vastapuolelle. (Tikk & Kerttunen 2018.) Kybertoimintaympäristö kyseenalaistaa mielestäni tämän lausunnon jatkuvasti. Tämä johtuu ensinnäkin siitä, että kyberympäristö ei tunne valtioiden rajoja. Kybertoimintaympäristön poliittisuus nousee esiin etenkin Venäjän operaatiossa Yhdysvaltain presidentin kampanjaa vastaan. Se oli yksi esimerkki siitä, miten kyberhyökkäyksiä käytetään poliittista itsemääräämisoikeutta vastaan (Shea 2017, 173). Viron soturipatsaskiistaa voisi myös pitää artiklan 2(4) kyseenalaistamisena, sillä hyökkäyksillä oli selkeä poliittinen konteksti, jolla pyrittiin vaikeuttamaan Viron yhteiskunnan toimintaa palvelunestohyökkäyksillä.

Geneven lisäpöytäkirjan artiklan 49 mukaan hyökkäys on väkivallan käyttöä vihollista vastaan niin hyökätessä kuin puolustaessakin: ””Attacks” means acts of violence

against the adversary, whether in offence or in defence.” (International Committee of the Red Cross 1977.) Naton määritelmän mukaan hyökkäys muodostuu sotilaallisista operaatioista, jotka ovat luonteeltaan hyökkäyksellisiä: ”In military operations, to take offensive action against a specified objective.” (NATO 2018b, 16.) Aseellinen hyökkäys on aina voimankäyttöä, mutta kaikki voimankäyttö ei ole luettavissa aseelliseksi hyökkäykseksi (Schmitt 2012, 286).

Yksimielisyyttä ei ole saavutettu siitä, mikä on täysin pätevä määritelmä aseelliselle hyökkäykselle. YK:n yleiskokouksen hyväksymän päätöslauselman artikla 3 johtaa siihen lopputulokseen, että aseellinen hyökkäys viittaa fyysiseen voimankäyttöön asevoimia tai sotavoimia käyttäen valtiota vastaan. (Ziolkowski 2012, 8–10.) Aseellinen hyökkäys on kuitenkin aina voimankäyttöä. YK:n yleiskokouksen päätöslauselman artikla 3 näkee aseellisen hyökkäyksen fyysisenä asevoimien tai sotavoimien käyttönä toista valtiota vastaan (United Nations 1974). Melkein jokainen 3. artiklan kohta viittaa siihen, että asevoimien käyttö nähdään aggressiivisena toimintana, joka voi eskaloitua sotatoimiksi. Aseellinen hyökkäys nähdään kaikista vakavimpana voimankäyttönä, josta aiheutuu merkittävää haittaa toiselle osapuolelle. Toiminta voidaan luokitella aseelliseksi hyökkäykseksi, kun se kykenee aiheuttamaan ihmisuhreja tai omaisuuden tuhoamista. (Geneva Academy 2014, 10). Aseellinen hyökkäys nähdään tahallisena puuttumisena toisen valtion toimintaan joko alueen sisällä tai ulkopuolella. Tällä tarkoitetaan esimerkiksi lähetystöjä tai kansalaisia ulkomailla. Lisäksi aseellinen hyökkäys edellyttää asevoimien käyttöä tietyn päämäärän saavuttamiseksi (Wilmshurst 2005, 6).

Voiman käyttö edellyttää aseen käyttöä. Perinteisesti aseellisella hyökkäyksellä on viitattu sotavoimiin ja niihin kuuluvaan varustukseen, joiden käytöstä seuraa kineettisiä eli liikkeestä aiheutuvia vaikutuksia (Ziolkowski 2012, 8–10). Tähän tuli kuitenkin muutos, kun ymmärrettiin, etteivät esimerkiksi kemialliset tai biologiset aseet täyttäneet tätä kriteeriä. Muun muassa Ian Brownlie siirsi näkökulman toiminnasta aiheutuneeseen seuraukseen. Hän keskittyi siihen, onko toiminnan seurauksena esimerkiksi tullut ihmisuhreja tai aiheutunut omaisuuden tuhoutumista. Hänestä sillä ei ole merkitystä, millä teko on tehty, vaan sillä, onko teosta seurannut merkittävää tuhoa. (Brownlie 1963, 362.) Vaikutukseen perustuva (effect based approach) lähestymistapa tarkoittaa sitä, että kyberhyökkäys voidaan nähdä aseellisena hyökkäyksenä, jos sen vaikutukset ovat verrattavissa kineettisen, biologisen tai kemiallisen hyökkäyksen vaikutuksiin. (Barkham 2001, 72.) Tällaisilla vaikutuksilla viitataan henkilövahinkoihin, fyysiseen vahinkoon tai omaisuuden tuhoamiseen. Viron tapahtumat voitaisiin nähdä vakavimmillaan artiklan 2(4) mukaisena voimankäyttönä Viron valtiota vastaan, mutta vaikutuksiltaan hyökkäys ei ollut aseelliseen hyökkäykseen

verrattavissa. Stuxnetin tapauksessa kysymykseen tulisi se, aiheuttiko haittaohjelma 1000 sentrifugin tuhoutumisen vai hetkellisen häiriötilan. Kysymys olisi silloin siitä, vahingoittiko mato merkittävästi Iranin kriittistä infrastruktuuria, kuten energiatuotantoa, vai aiheutuiko hyökkäyksestä henkilövahinkoja. Tällainen voisi olla vaikutukseltaan sellainen, joka täyttäisi vaikutukseen perustuvassa lähestymistavassa aseellisen hyökkäyksen kriteerin. (Ziolkowski 2012, 11.) Tällaisesta ei ole kuitenkaan raportoitu, eli tämä perustuu hypoteettiseen pohdintaan.

Viron soturikiista on hyvä esimerkki attribuutio-ongelman tuomasta haasteesta. Vaikka Venäjää pidetäänkin syyllisenä hyökkäyksiin, sitä ei kuitenkaan pystytty osoittamaan riittävin perustein. Venäjä ei ole myöntänyt osallisuuttaan tapaukseen (Tikk & Kerttunen 2018). Kyberhyökkäyksistä on tullut yksi voimankäytön tapa. Tässä tutkielmassa pelote rangaistuksesta (deterrence by punishment) ja pelote vahvasta puolustuksesta (deterrence by denial) ovat esitetyssä kehyksessä kykenemättömiä vastaamaan näihin esimerkkeihin. Tilanne näiden käsitteiden luomisen aikana oli maailmassa toisenlainen. Lisäksi kyber- ja hybridiuhat tuovat oman ulottuvuutensa tähän.

> Russia has become more assertive with the illegal annexation of Crimea and destabilisation of eastern Ukraine, as well as its military build-up close to NATO's borders. In parallel, to the south, the security situation in the Middle East and Africa has deteriorated due to a combination of factors that are causing loss of life, fuelling large-scale migration flows and inspiring terrorist attacks in Allied countries and elsewhere. (Warsaw Summit Guide 2016, 53.)

> Collective defence is the Alliance's greatest responsibility and deterrence remains a core element of NATO's overall strategy – preventing conflict and war, protecting Allies, maintaining freedom of decision and action, and upholding the principles and values it stands for – individual liberty, democracy, human rights and the rule of law. NATO's capacity to deter and defend is supported by an appropriate mix of capabilities […] (Warsaw Summit Guide 2016, 53–54.)

Tässä lainauksessa Nato painottaa Venäjän kasvanutta uhkaa niin Nato-maille kuin Naton ulkopuolisillekin valtioille. Skinnerin metodologiaa hyödyntäen Nato edustaa näissä lainauksissa Venäjän vastakohtaa. Tässä myös painotetaan yhteistä puolustusta Naton tärkeimpänä tehtävänä, ja pelote pysyy keskeisimpänä elementtinä yhteisen puolustusstrategian ylläpitämisessä. Ensimmäisen lainauksen voi tulkita varoituksena Venäjän toimista. Toinen lainaus perustuu enemmän lupaukseen. Siinä todetaan, että yhteinen puolustus on yhä Naton strategian keskiössä ja liittouman tärkein velvollisuus. (Skinner 2002, 96–98.) Nato käyttää Venäjän toiminnasta Krimin valtauksen ja Ukrainan kriisin yhteydessä sanaa vakuuttava. Mielestäni tällä viitataan siihen, että Venäjän pelote on

toiminut. Lainauksessa huomioidaan myös venäläisten sotilaiden siirtyminen Naton rajan läheisyyteen, mikä YK:n artiklan 2(4) mukaan nähdään voimankäyttönä.

Turvallisuustilanteet Lähi-idässä sekä Afrikassa ovat lisänneet pakolaisaaltojen määrää, mitä myös terroristit ovat käyttäneet hyväksi. Nato painottaa, että sen ensisijainen tehtävä on ehkäistä konflikteja, säilyttää sen jäsenvaltioiden autonomia niin päätöksenteossa kuin muussa toiminnassa. Lisäksi Nato pitää tärkeänä yksilön vapautta, demokratiaa, ihmisoikeuksia sekä laillisuusperiaatetta. Tämän lausunnon perusteella voidaan olettaa, että Nato tuomitsee Venäjän toimet, jotka rikkovat näitä arvoja. (Skinner 2002, 120.) Natolla on kyvykkyys vastata Venäjän uhkaan ydinaseiden, ohjustorjunnan sekä perinteisen sodankäynnin ulottuvuuksien yhdistelmällä. Brysselin huippukokouksen oppaasta löytyy seuraava lause: ”NATO Cyber Rapid Reaction teams are on standby to assist Allies, 24 hours a day, if requested and approved.” (Brussels Summit Guide 2018, 35.) Varsovan huippukokouksessa Naton pelotetta vahvistettiin konseptilla Readiness Action Plan (RAP), jonka tarkoitus on ollut vahvistaa Naton keski- sekä itäisen alueen puolustusta. Se muodostuu kahdesta eri osa-alueesta. Ensimmäinen osa-alue muodostuu pyrkimyksestä varmistaa näiden alueiden turvallisuus (assurance measure), ja toinen muodostuu rakenteellisista toimenpiteistä (adaptation measure). Varmistaviin toimenpiteisiin on kuulunut harjoitustoiminnan lisääminen sekä kaluston ja joukkojen asettaminen näille alueille. Rakenteellisilla toimenpiteillä tarkoitetaan Naton pidemmän ajan rakenteellista muutosta. Tähän kuuluvat muun muassa nopean toiminnan joukot, joiden kautta Nato pystyy nopeammin vastaamaan yllättäviinkin uhkiin. Näiden toimenpiteiden voidaan sanoa olevan suora vastaus Venäjälle sen toimista Krimillä ja Itä-Ukrainassa. (Warsaw Summit Guide 2016, 81–82.) Näillä toimenpiteillä vahvistettiin Naton pelotetta Varsovan huippukokouksen oppaassa. Brysselin huippukokouksessa Nato on ottanut saman askeleen myös kyberpuolustuksen suhteen, sillä se on perustanut nopean toiminnan joukot myös verkkohyökkäyksiä varten. Nämä joukot ovat valmiudessa 24 tuntia vuorokaudessa, ja ne avustavat jäsenvaltioita kyberhyökkäyksiä vastaan. (Brussels Summit Guide 2016, 35.)

> The Alliance’s actions are defensive in nature, proportionate and in line with international commitments given the threats in the changed and evolving security environment, and the Alliance’s right to self-defence. NATO also remains fully committed to non-proliferation, disarmament, arms control and confidence- and security-building measures to increase security and reduce military tensions […]. (Warsaw Summit Guide 2016, 54.)

Tässä lainauksessa kerrotaan Naton toiminnan luonteesta. Naton toiminta on yhdenmukaista kansainvälisten sopimusten kanssa. Silloin sen vastakohtana voidaan nähdä kaikki se

toiminta, joka rikkoo kansainvälistä oikeutta, kuten Venäjän toimet Krimillä ja Ukrainassa, terroristien toiminta Lähi-idässä ja Afrikassa tai hyökkäykset, joilla pyritään estämään vastustajan toimintaa kybertoimintaympäristössä. Nato on pyrkinyt myös vahvistamaan sen toimintaa kybertoimintaympäristössä. Kansainvälisen oikeuden tunnistaminen kyberavaruudessa on myös yksi keino vahvistaa sen asemaa kyseisessä ympäristössä. Tällöin Natolla on samat edellytykset vastata uhkiin kuin fyysisessäkin todellisuudessa, jolloin se pyrkii informoimaan sen vastustajaa omasta kyvykkyydestään myös kybertoimintaympäristössä. (Warsaw Summit Guide 2016; Skinner 2002, 120.) Kuten huomattiin esimerkiksi Stuxnetin ja soturikiistan kohdalla, kyberhyökkäysten tarkoitus ei ole ylittää aseellisen hyökkäyksen kynnystä. Niillä yritetään estää vastustajan toimintaa, jolloin niiden idea on pysyä matalan intensiteetin hyökkäyksinä, jolloin vastustaja ei voi käyttää esimerkiksi asevoimia niitä vastaan. (Pietilä 2017, 54.)

> More specifically, NATO's strengthened deterrence and defence posture will focus on areas such as conventional forces, forward presence, joint air power and maritime forces, as well as cyber defence, civil preparedness and countering hybrid threats, including in cooperation with the European Union (Warsaw Summit Guide 2016, 54).

Lainauksesta nousee esille, että Naton puolustuksen painopiste on säilynyt perinteisessä sodankäynnissä eikä sen painoarvo ole hävinnyt. Toisaalta tuskin koskaan perinteinen sodankäynti häviää. Fyysisen ja sähköisen maailman yhteen kietoutuminen on jo tapahtunut. Tämä tarkoittaa sitä, että myös Nato on tunnistanut, että kybertoimintaympäristön tapahtumat vaikuttavat suoraan fyysiseen maailmaan. Nykyään yhteiskunnat eivät toimi, mikäli digitaalinen maailma ei toimi. Tämä johtuu siitä, että yhteiskunnan kriittinen infrastruktuuri – sähkönjakelu, terveydenhuolto, rahoitusjärjestelmät sekä elintarvikelogistiikka – on kytkeytynyt digitaaliseen maailmaan. Haastavaa tässä on se, että näiden tiivis kietoutuminen toisiinsa muuttaa myös kulttuuriamme. Elämme tällä hetkellä käsi kädessä teknologian kanssa, vaikka emme välillä tiedä, mitä se on. Mitä syvemmälle menemme tässä kehityksessä, sen vaikeampi meidän on myös tiedostaa, missä kybermaailma sijaitsee, mistä se alkaa ja mihin se päättyy. Olemme riippuvaisia sellaisesta, jonka toimintaa emme pysty täysin ymmärtämään tai edes hallitsemaan. (Limnéll ym. 2014, 33–34.)

Kyberhyökkäyksiä käytetään epävarmuuden tunteen ja hämmennyksen vahvistamiseen, ja niillä pyritään vaikuttamaan ihmisten turvallisuuden tunteeseen (Limnéll ym. 2014, 34). Toisaalta niitä käytetään osana muita operaatioita ja pyritään vaikuttamaan vastustajan yhteiskunnan kannalta keskeisiin ja kriittisiin kohteisiin, kuten yllä todettiin.

Sodan ja rauhan rajapinta on hämärtynyt ja limittynyt yhteen. Nykyään on yhä vaikeampi havaita, missä vaara piilee ja onko vaara todellinen. Hybridivaikuttamiselle on tyypillistä, että eri keinoja hyödynnetään epäsymmetrisesti ja niiden avulla pyritään tiettyyn päämäärään. Vaikuttaminen voi kestää vuosia, koska lyhyellä aikavälillä vaikuttaminen olisi helposti huomattavissa. Haaste on eri vaikuttamisen keinojen yhdistämisessä ja näiden liittämisessä yhteiseen päämäärään samalla, kun vastustaja pyrkii vaikuttamaan huomaamattomasti. Missä vaiheessa Naton kohdalla aseellisen hyökkäyksen raja on ylitetty? Hybridioperaatio on voinut kohdistua valtiota kohtaan jo pitkään ennen kuin se huomataan. (Hyytiäinen 2018, 116–118.) Historian tutkimus ei yksin auta selvittämään asioiden syy- ja seuraussuhteita, vaan joudumme koko ajan tekemään uusia riskiarviointeja tulevaisuudesta sekä ennakoimaan sitä. Olemmehan itse nykyisen kybertoimintaympäristön luoneet, jossa melkein mikä tahansa on mahdollista. Tämä kaikki on siirtänyt painopistettä ihmisten mieleen, jossa vain mielikuvitus on rajana. Tästä syystä esimerkiksi hybridivaikuttamiseen liittyvässä skenaariopohdinnassa joudutaan varautumaan myös pahimpiin uhkakuviin. (Kinnunen 2018; Limnéll ym. 2014, 85.) Skinnerin metodologia liittyy vahvasti kirjoittajan intentioon sekä ajan poliittisen toimintaympäristön hahmottamiseen (Skinner 2002, 80–82). Mielestäni oleellista ei ole keskittyä pelkän teknologian parantamiseen ja mahdollisimman vaikeisiin uhkakuviin. Skinnerin metodologiaa hyödyntämällä voimme nähdä myös sen, mikä ei muutu. Emme voi mennä tulevaisuuteen tietämättä historiaa. On täysin mahdollista, että ajattelemme jonkun asian olevan liian itsestään selvää, jolloin sokeudumme sille emmekä näe sitä, mikä on silmiemme edessä. Tämä ei kuitenkaan riitä ainoaksi tarkastelutavaksi, vaan tarvitsemme tulevaisuuden ennakointia ja siihen varautumista. (Kuusisto 2018, 10; Hyytiäinen 2018, 140–142.)

Kyberhyökkäyksiä käytetään nykyään eniten hybridivaikuttamisen yhteydessä, ja se on operatiivisen toiminnan yksi osa-alue. Haittaohjelma saattaa olla järjestelmän sisällä vuosia ennen kuin se havaitaan. Tästä syystä sillä on varsin alhainen pelote, koska sen vaikuttavuus selviää vasta sitten, kun se löydetään (zero day vulnerability). (Bendiek & Metzger 2015, 7.) Lisäksi ydinaseet ja kyberhyökkäykset muodostavat toisistaan hyvin poikkeavat pelotteet. Ydinaseet ovat niin tuhoisia, että niiden käyttö on sen takia kannattamatonta, eivätkä valtiot halua ydinhyökkäyksen kohteeksi tai olla vastuussa sellaisesta (NATO 2016c). Niiden vaikutukset on todistettu jo 1945 Hiroshimassa sekä Nagasakissa.

Yksi keskeisin pelote onkin siinä, että niin kyberhyökkäyksillä kuin hybridivaikuttamisellakin pyritään horjuttamaan ihmisten luottamusta esimerkiksi valtion viranomaisia kohtaan. Toisaalta se voi olla sitä, että pyritään saamaan ihmiset

kyseenalaistamaan se, mikä tieto on totta ja mikä ei, esimerkiksi informaatio-operaatioita hyväksi käyttäen (Puistola 2018). Nykyään kybertoimijat pyrkivät myös vaikuttamaan demokratian ytimeen eli vaaleihin (Shea 2017, 166). Nato painotti Varsovan huippukokouksessa vaalimia arvojaan: ”individual liberty, democracy, human rights and the rule of law” (Warsaw Summit Guide 2016, 1). Tällä se erottaa itsensä niistä, jotka rikkovat näitä arvoja (Skinner 2002, 120). Venäjä edustaa Naton vastakohtaa, kuten voimme hyvin nähdä erilaisten tapahtumien, esimerkiksi Krimin valtauksen, Ukrainan kriisin ja Yhdysvaltojen presidentinvaaleihin sekaantumisen, yhteydessä. Tulevaisuutta pitää pystyä arvioimaan ja ennakoimaan, koska ”tulevaisuus tehdään joka kerta” (Kuusisto 2018, 10). Nykyään haaste onkin siinä, tiedämmekö edes olevamme jo hybridivaikuttamisen kohteena ja milloin ja missä kohtaa voidaan sanoa, että olemme kriisissä tai sodassa toisten valtion kanssa.

Kaikista merkittävin eroavaisuus tavanomaisessa kineettisessä hyökkäyksessä verrattuna kyberhyökkäykseen on se, että kybertoimintaympäristössä pelotteen voidaan sanoa epäonnistuvan jatkuvasti. Kybertoimintaympäristössä joudutaan alusta asti työskentelemään siitä lähtökohdasta, että vihollinen on jo päässyt sisään, koska muuten haavoittuvuuksia käytettäisi hyväksi. (Bendiek & Metzger 2015, 7.) Peloteteorian osa-alueiden eli rangaistuksen pelotteen (deterrence by punishment) ja puolustuksen pelotteen (deterrence by denial) soveltuvuus kybertoimintaympäristöön on heikko myös attribuutio-ongelman takia. Attribuutio-ongelman, eli syyksiluettavuuden ongelma onkin yksi keskeinen haastava tekijä kybertoimintaympäristössä, koska teon alkuperää ja tekijää voi olla vaikea selvittää. (Fidler ym. 2013, 21). Artikla 5 ja 51 toimivat pelotteena siitä syystä, että ainoastaan ääritilanteissa harkitaan niiden käyttöönottoa.

Kybertoimintaympäristön haasteena on myös lainvalvonta. Eri maissa sovelletaan eri lainsäädäntöä ja tällaiset aukot mahdollistavat tällaisen systeemin hyväksikäytön. Kyberhyökkäyksiä tehdään jatkuvasti, ja niiden tarkoitus on iskeä niihin kohtiin, jossa vastustajan toimintaa pyritään vaikeuttamaan. Haaste on se, ettei hyökkäyksiä välttämättä konkreettisesti heti havaita ja toisaalta vaikutuksia on vaikea ennakoida. Lainsäädäntö ei kaikkialla tunnista teknologisin menetelmin tehtyjä rikoksia. Tällaiset rikokset jäävät helposti ilman rangaistusta. (Bendiek & Metzger 2015, 7.) Jos teko tunnistetaan esimerkiksi voimankäytöksi artiklan 2(4) mukaan tai aseelliseksi hyökkäykseksi artiklan 5 mukaan, kuka päättää, kenen lainsäädäntöä noudatetaan, jos kyse on Naton agendasta? Naton pitää pystyä suunnistamaan tässä kompleksisessa ympäristössä, jossa pitää huomioida kansainvälinen oikeus, kansallinen lainsäädäntö sekä valtioiden rajat ylittävä lainsäädäntö EU-jäsenmaat huomioiden, jotta vältyttäisiin ristiriidoilta. Tämä on kyberpuolustuksen kannalta keskeinen

ongelma, koska kyberhyökkäykset ovat valtioiden rajat ylittävää toimintaa ja näin ollen niihin vastaamisenkin pitäisi olla. Loppujen lopuksi kyse on kuitenkin poliittisesta päätöksestä. Se määrittelee sen, milloin hyökkäyksen tai operaation katsotaan ylittäneen aseellisen hyökkäyksen rajan. Toisaalta kyse on poliittisen pelotteen rakentamisesta eli selvien pelisääntöjen luomisesta. Näin tehtiin Varsovan huippukokouksessa, kun kybertoimintaympäristö tunnistettiin operatiiviseksi ulottuvuudeksi. Lisäksi lupaus kyberpuolustamisesta (Cyber Defence Pledge) sekä kyberpuolustuksen toimintaperiaate (Policy on Cyber Defence) ovat tällaisia poliittisia linjauksia. (Fidler ym. 2013, 13; Limnéll 2017.)

Krimin valtauksesta ja Ukrainan kriisistä kesti noin kaksi vuotta ennen kuin todettiin, että kansainvälinen oikeus pätee myös kybertoimintaympäristössä. Vasta vuotta 2016 pidettiin toimenpiteiden kehitysvaiheena, toisin sanoen poliittisten tekojen vaiheena, vaikka nykyinen toimintaympäristö edellyttää tapahtumien ennakointia ja niihin varautumista. Se edellyttää sitä, että asioita toimeenpannaan jo etukäteen. Lainsäädännön prosessointi vie oman aikansa, joten tarpeet sen muuttamiseksi pitäisi pystyä ennakoimaan. Kybertoimintaympäristö muuttuu joka hetki, ja eilinen tieto voi olla jo huomenna vanhentunutta. Kuten Lehtomäki kirjoittaa Turvallisuuskomitean blogissa, ennakoinnissa kyse on siitä, että tilanteen tullen olemme mahdollisimman toimintakykyisiä (Lehtomäki 2019). Keskeinen kysymys onkin, miten nopeasti Nato pystyisi reagoimaan artiklan 5 ylittävään kyberhyökkäykseen. Keskeistä on myös se, miten jäsenvaltiot pyrkivät ratkaisemaan valtiota vastaan tehtyjä hyökkäyksiä. Entä onko Natolla tarkkaa tietoa siitä, miten paljon ja millaisia hyökkäyksiä sen jäsenvaltiot kohtaavat? Kun puhutaan kyberpuolustamisesta ja kyberturvallisuudesta, on ensisijaisen tärkeää, onko eri toimijoiden välillä luottamusta vai ei. Kuten luvussa kolme nostettiin esiin, Natolla on laajamittaista ja ympärivuotisia harjoituksia sekä toimintoja, joiden avulla se pystyy kehittämään sen jäsenvaltioiden kyberkyvykkyyttä. Lisäksi sillä on erilaisia alustoja, joiden avulla tietoa erilaisista haittaohjelmista pyritään levittämään. Valmiussuunnitelma sekä nopean toiminnan joukot niin fyysisessä kuin sähköisessäkin maailmassa ovat konkreettisia esimerkkejä, joita Nato on tehnyt sen jäsenmaiden turvallisuuden parantamiseksi. Näiden erilaisten keinojen kautta se yrittää vahvistaa myös jäsenvaltioiden luottamusta.

Kuten alaluvussa 1.4.1. esitettiin, Skinnerin mukaan lausuntoja pitää katsoa argumenttien tavoin. Hänestä lausunnon ymmärtämisen kannalta on tärkeä tiedostaa, oliko kirjoittajan tarkoitus puolustaa, kritisoida vai hyökätä jotain argumenttia vastaan. Ymmärrän tämän niin, että tulkitsemme tekoa, teon seurauksia ja sitä toimintaympäristöä, joka on toiminut kontekstina teolle. (Skinner 2002, 128.) Näiden teesien pohjalta Naton artikla 5 on

lupaus sen jäsenvaltioille sekä varoitus sen vihollisille. Se on ollut vuoteen 2014 asti sama, kunnes kyberpuolustuksen toimintaperiaatteessa vuonna 2014 tunnistettiin, että kansainvälinen oikeus pätee myös kyberavaruudessa. Sen konkreettinen merkitys huomattiin Krimin valtauksen ja Ukrainan kriisin yhteydessä (Shea 2017, 167). Tässä luvussa etsitään vastausta kysymykseen, miten kyberpelotetta rakennetaan yhteisen puolustuksen alla. Oman tulkintani mukaan ne eivät toimi pelotteena kuten ydinaseet. Ydinaseiden käyttöä harkitaan ainoastaan ääritilanteissa, ja niiden vaikutukset on todistettu historiassa (Schwarz 2005, 10). Kyberhyökkäyksiä taas tehdään jatkuvasti. Niitä on vaikea havaita ja konkreettisesti nähdä. Kyberhyökkäysten tyyppejä ja toimijoita niiden käyttäjiksi on digitalisaation edetessä yhä enemmän. Lisäksi niiden tarkkaa vaikuttavuutta ei voi edes hyökkääjä itse tietää. Ne kuitenkin toimivat hyvinä välineinä osana suurempaa kokonaisuutta. Missä vaiheessa pelote on riittävä? Kyberhyökkäyksillä voidaan heikentää vastustajan toimintaa. Joissain tapauksissa se voi olla jo riittävästi. Kysymykseen tulee silloin se, miten paljon voidaan aiheuttaa haittaa kohteelle. Kyberkyvykkyys vahvistaa pelotetta silloin, kun pystytään osoittamaan niiden vaikuttavuus osana muita toimenpiteitä. (Ibid., 9.) Varsovan huippukokouksessa Nato informoi sen vastustajia myös siitä, että hyökkäys kybertoimintaympäristössä voi johtaa toimenpiteisiin. Naton yhteinen puolustus on selkeä viesti ja pelote sen vastustajille. Kybertoimintaympäristön ongelmiksi muodostuvat kyberhyökkäysten intensiteetin määritteleminen, attribuutio-ongelma sekä poliittinen kyvykkyys.

Tästä syystä on hyvä kysyä, miten muodostetaan riittävän vahva pelote kybertoimintaympäristössä. Pelotteen pitäisi kybertoimintaympäristössä luonnollisesti vastata enemmän digitaalisiin haasteisiin ja mahdollisuuksiin. Mielestäni kyberhyökkäysten paras pelote on niiden tuoma epävarmuus ja levottomuus, jolla vaikutetaan ihmisten turvallisuuden tunteeseen (Limnéll ym. 2014, 34). Onhan ihminen jo antiikin Rooman ajoilta pelännyt sitä, mitä ei tiedetä (Porvali 2017). Kyberhyökkäykset koskettavat yhteiskunnan kaikkia osa-alueita, sillä sen vaikutuksen piirissä ovat nykyään niin yksilöt kuin valtiotkin. Jokainen meistä voi kuvitella, millainen vaikutus hyökkäyksellä olisi, jos pankkikortit eivät toimisi tai sähkönjakelu katkeaisi. Toisaalta kyberhyökkäyksiä ei välttämättä havaita heti. Silloin ne toimivat pelotteena myös siitä näkökulmasta, että ihminen alkaa pelkäämään jopa tilanteita, jotka vaikuttavat normaaleilta. Keskeinen ero kyberhyökkäysten ja ydinaseiden tuomassa uhkassa on se, että ydinaseet tuovat pelotteen, jonka avulla se pyrkii säilyttämään olemassa olevan nykytilan. Kyberhyökkäykset liittyvät usein laajempaan kokonaisuuteen, jossa niitä käytetään työkaluina jonkun tietyn päämäärän saavuttamiseksi, jopa muuttamaan nykytilaa. Peloteteorian tarkoitus on ollut osoittaa, etteivät ydinasevaltiot lähde toisiaan

vastaan sotaan, millä pyrittiin ehkäisemään sotia (Schwarz 2005, 6). Kyberhyökkäyksien kannalta tilanne ei ole niin yksinkertainen, koska niiden vaikuttavuus ei ole yhtä konkreettisesti havaittavissa. Pelotetta on vaikea hallita, koska hyökkääjä ei pysty ennakoimaan hyökkäyksen vaikutuksia tarkasti. (Ibid., 10-11). Kyberpelotteen kannalta keskeisiä tekijöitä ovat sietokyky, eli se miten hyvin pystyy toimimaan hyökkäyksen alla. Toiseksi pelotteen toimivuuden kannalta keskeistä on se, kuinka hyvin hyökkääjä pystytään paikantamaan. Kolmanneksi pelotetta vahvistetaan kyvykkyydellä vastata hyökkäyksiin myös poliittisella tasolla. Viimeiseksi pelotteen uskottavuuden kannalta keskeistä on se miten paljon valtiosta löytyy kyberosaamista. (Lehto & Limnéll 2017, 205.)

Alaluvussa 1.4.2. nostin esiin ajatuksen, että rangaistuksen pelotetta (deterrence by punishment) kuvataan tässä tutkimuksessa Naton yhteisenä puolustuksena, kun vahvan puolustuksen (deterrence by denial) tuoma pelote viittaa Naton kyvykkyyteen toimia ja vastata uhkiin tietyllä alueella. Yhdysvallat, Ranska, Iso-Britannia ja Saksa ovat Naton jäsenvaltioita, joilla on myös hyvä kyberkyvykkyys. Kysymys onkin, haluavatko jäsenvaltiot toimia Naton mandaatilla vai itsenäisesti. Entä pystyykö Nato reagoimaan yksimielisyyden periaatteella riittävän nopeasti kybertoimintaympäristössä olevaan uhkaan? Fyysisessä maailmassa ihmiset ovat tottuneet siihen, että asioiden valmisteluun ja niiden kehittämiseen menee aikaa. Esimerkkinä voidaan käyttää mannerten välisten ohjusten valmistamista ja niiden laukaisemista, josta voidaan saada ennakkovaroitus. Kybertoimintaympäristö on erilainen suhteessa fyysiseen aikaan. Tässä toimintaympäristössä asiat tapahtuvat nopeasti, ja asiat voivat tapahtua myös ilman ennakkovaroitusta. (Limnéll ym. 2014, 63–67.)

Nykyään nämä kaksi peloteteorian lähtökohtaa voidaan liittää samaan toimintaympäristöön, jossa valtioiden rajat eivät ole esteenä. Kybertoimintaympäristössä etäisyys ei ole enää ratkaiseva tekijä. Sama pätee ihmisiin, koska ihmiset voivat suunnitella ja toimeenpanna hyökkäyksen mistä vain. Lisäksi olemme kehittäneet ympäristön, jota pystymme itse muokkaamaan halutun laiseksi. Rangaistuksen (punishment) ja puolustuksen (denial) pelotevaikutus on ensisijaisesti suunnattu koskemaan valtioita ja fyysistä tilaa. Kybertoimintaympäristössä yksikin riittävän hyvä ja motivoitunut henkilö voi aloittaa hyökkäyksen. Haittaohjelmat voidaan uudelleenohjelmoida, ja verkottunut maailma mahdollistaa niiden kontrolloimattoman leviämisen. Näin se voi lopulta jopa aiheuttaa haittaa itse hyökkääjälle, koska sen leviäminen ja vaikutukset eivät ole hyökkääjän päätettävissä. Haasteen luo nimenomaan se, että hyökkäys ei ole fyysinen eikä sen määrittämä. Tämä tuo haasteen myös 29 jäsenvaltion liittoumalle ja sen kyberpuolustukselle, sillä sen on mietittävä uudestaan, mitä se pyrkii ensisijaisesti turvaamaan, mikä on sen

keskeinen uhka ja mitkä ovat kohteiden turvaamiskeinot. Entä miten toimitaan tilanteessa, jossa hyökkäys ylittää artiklan 5 rajan, mutta hyökkäyksen aiheuttajaa ei tunnisteta? (Limnéll ym. 2014, 37–38, 65–66.)

Suomessa on käytössä kokonaisturvallisuuden varautumisen malli, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen sekä kansalaisten yhteistyönä. Yhteiskunnan elintärkeiksi toiminnoiksi luokitellaan valtion johtaminen, kansainvälinen toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri, huoltovarmuus, väestön toimintakyky, palvelut sekä henkinen kriisinkestävyys. (Yhteiskunnan turvallisuusstrategia 2017, 7, 14.) Tällä tarkoitetaan sitä, että joka tilanteessa yhteiskunnan elintärkeiden toimintojen tulee olla turvattuja. Ratkaisevaa on yhteistyö yhteiskunnan eri osa-alueiden välillä. Jos yhteistyö viranomaisten välillä toimii, pystytään erilaisiin hyökkäyksiin vastaamaan nopeammin. Varautumisella pidetään huolta siitä, että elintärkeät toiminnot pysyvät hyökkäyksestä huolimatta toimintakykyisinä ja tällaisesta hyökkäyksestä pystytään palautumaan nopeasti. Kokonaisturvallisuuden varautumisen malli on tärkeä nykyisessä toimintaympäristössä siitä syystä, että kyberturvallisuus on enenevissä määrin riippuvainen myös yksityisen sektorin tuottamista palveluista. Sen takia on oleellista, että valtionhallinto, yrityselämä, järjestöt sekä kansalaiset ovat kaikki saman konseptin alla. (Ibid, 7, 14.) Kybertoimintaympäristö koskettaa jokaista informaatioyhteiskunnan jäsentä, eikä se ole ympäristö, johon liittyisi ainoastaan sotilaallinen ulottuvuus. Kokonaisturvallisuus on ”tila, jossa yhteiskunnan elintärkeisiin toimintoihin kohdistuviin uhkiin ja riskeihin on varauduttu”. (Kokonaisturvallisuuden sanasto 2017, 14.) Uhkakuvat ovat moninaistuneet, ja sotilaallinen uhka on vain yksi osa tätä. Nykyään voisi ennemmin puhua kokonaisturvallisuudesta, koska valtiot eivät kohtaa enää vain sotilaallista uhkaa, vaan yhteiskunnan jokainen osa-alue on tullut mukaan tähän pelikenttään. (Yhteiskunnan turvallisuusstrategia 2017, 7.)

Kylmään sotaan asti Naton ensisijainen uhka oli Neuvostoliitto. Kylmän sodan jälkeen painopiste siirtyi terrorismiin. Naton Varsovan huippukokouksen oppaan lainauksista saa edelleen sen käsityksen, ettei nykyisen Venäjän tai terrorismin uhka ole hävinnyt. Kyber- ja hybridiuhat ovat tuoneet haasteena entistä epäsymmetrisemmän ja vaikeaselkoisemman ympäristön, jossa niin valtiolliset kuin ei-valtiollisetkin toimijat liikkuvat. Kuinka hyvin Nato pystyy vastaamaan puolustusliittona uhkiin, jotka eivät ole välttämättä sotilaallisia? Entä jos vaikutetaan samaan aikaan siviiliväestöön ja samaan aikaan sotilaalliseen ulottuvuuteen? Esimerkiksi kyberhyökkäyksiä voitaisiin käyttää valtion sähköverkon lamaannuttamiseen, kuten Ukrainassa vuonna 2016 (Halminen 2016). Tällainen hyökkäys koskettaa välittömästi jo useampaa yhteiskunnan toimijaa. Missä

vaiheessa tällainen uhka siirtyy Naton agendalle? Entä missä vaiheessa tällainen uhka on sotilaallinen?

Tässä luvussa on tarkasteltu sitä, että kyberturvallisuus on kyberpuolustuksen edellytys. Kyberturvallisuus kattaa sotilaallista näkökulmaa laajemmin yhteiskunnan eri osa-alueet. Tämä tarkoittaa sitä, että pelkän valtionjohdon kytkeminen kyberpuolustuksen vahvistamiseen ei enää riitä. Lainauksissa on noussut esille se, miten Nato näkee sen pelotteen rakentuvan. Esitetyt lausunnot ovat heijasteita siitä maailmasta, jota niissä kuvaillaan. (Farr 1989, 38.) Nato on Varsovan huippukokouksessa painottanut yhteisen puolustuksen ja pelotteen vahvistamista. Nato tuntuu kuitenkin pitävän perinteisten joukkojen asemaa yhtä vahvana kuin ennenkin, eli siitä ei ole luovuttu digitalisaation merkityksen noustessa myös taistelukentillä. Pelote on pitänyt asemansa fyysisessä maailmassa, mutta nyt se ulottuu kybertoimintaympäristöönkin. Varsovan huippukokouksen selkein poliittinen muutos on ollut kyberpuolustuksen toimintaperiaatteen sekä lupauksen toimeenpaneminen. Näiden avulla Nato on pyrkinyt parantamaan sen kyberpuolustuksen pelotetta harjoitustoiminnan, koulutuksen sekä tiedotuksen parantamisen kautta. Näillä muutoksilla se on myös pyrkinyt informoimaan muita toimijoita sen kyvykkyydestä kybertoimintaympäristössä. Onhan Varsovan huippukokouksen pöytäkirja kaikkien saatavilla. Merkittävä edistysaskel oli se, että kansainvälinen oikeus tunnistettiin myös kyberavaruudessa. Nato vahvistaa, että riittävän vakava kyberhyökkäys voidaan myös tulkita aseellisena hyökkäyksenä, jolloin valtio on oikeutettu käyttämään itsepuolustusta hyökkääjää vastaan. (Warsaw Summit Guide 2016, 124-125; The North Atlantic Treaty 1949.)

Varsovan huippukokouksessa Nato tunnisti kyber- ja hybridiuhat entistä vahvemmin sen uhkiksi. Kansainvälisen oikeuden ulottaminen kybertoimintaympäristöön on yksi esimerkki siitä. Naton pääasiallinen päätöksentekoelin Pohjois-Atlantin neuvosto valvoo kyberpuolustuksen toimintaperiaatteen toimeenpanoa. Haasteelliseksi muodostuu se, että kuinka nopeasti Pohjois-Atlantin neuvosto pystyy vastaamaan yksimielisyysperiaatteella kybertoimintaympäristössä tapahtuviin asioihin. Toisaalta onko 29 jäsenen liittoumassa riittävästi poliittista tahtoa ja kyvykkyyttä vastata näihin? Varsovan huippukokouksessa keskeisiksi nähtiin kyberpuolustuksen poliittisen ja operatiivisen ulottuvuuden vahvistaminen ja kyberpuolustuksen pelotteen vahvistaminen harjoitustoiminnalla, koulutuksella sekä tiedotuksella. Oppaassa tunnistettiin myös, että kyberpuolustus on inhimillistä toimintaa. Kyberturvallisuuteen vaikuttavat yhtä lailla ihmiset kuin teknologiakin. Venäjä nostettiin sekä Walesin että Varsovan huippukokouksessa vahvasti esiin Krimin valtauksen ja Ukrainan kriisin takia. Natosta rakentuu kuva Venäjän

vastakohtana, joka kunnioittaa liittouman yhteisiä arvoja sekä kansainvälistä oikeutta. Nato on vahvistanut valmiussuunnitelman (RAP) sekä eteentyönnetyn läsnäololla (EFP) sen pelotetta Varsovan huippukokouksessa. Pelotetta vahvistettiin Brysselin huippukokouksessa perustamalla kyberympäristöön nopean toiminnan joukot. (Warsaw Summit Guide 2016, 82; Brussels Summit Guide 2018, 35.) Lisäksi Varsovan huippukokouksessa tunnistettiin jäsenvaltioiden asema vahvemmassa kyberpuolustamisessa. Näistä toimivat esimerkkeinä allekirjoitettu MOU sekä lupaus kyberpuolustuksen vahvistamisesta. Myös valtiollisten toimijoiden lisäksi ei-valtiollisten toimijoiden, kuten terroristien, haktivistien sekä rikollisten, toiminta on nähty uhkana kybertoimintaympäristössä.

5. Loppupäätelmät

Tutkimuksen tarkoitus oli selvittää, miten Naton kyberpelote rakentuu Varsovan huippukokouksessa. Tätä kysymystä tarkennettiin kysymyksillä, mitä linjauksia Nato on tehnyt kyberpuolustuksen suhteen ja miten kyberpelote toimii yhteisen puolustuksen alla. Tutkimus koostui kahdesta erillisestä analyysiosiosta, joissa molemmissa hyödynnettiin Varsovan huippukokouksen opasta vuodelta 2016. Aineistosta otettiin lainauksia skinneriläistä puhetekojen ajatusta hyödyntäen. Tutkimuksessa esitetyt lainaukset edustavat lokuutioita eli sitä, mitä asiasta on sanottu. Lokuutioiden avulla oli tarkoitus selvittää, mitä tekoja eli illokuutioita Nato on näillä lausunnoilla tehnyt ja miten se on näillä pyrkinyt muuttamaan nykytilannetta. Luvussa kolme pyrin rakentamaan kuvan Naton kyberpuolustuksen linjauksista. Luvussa tarkastelin kyberpuolustuksen pelotetta hyödyntäen peloteteorian kahta näkökulmaa, rangaistuksen (punishment) sekä vahvan puolustuksen (denial) pelotetta.

Luvussa kolme tarkasteltiin lausuntoja, jotka heijastivat kuvan Naton kyberpuolustuksen asemasta. Keskeisiä teemoja olivat ne poliittiset lausunnot, joilla se on pyrkinyt muuttamaan nykytilaa. Naton kyberpuolustus rakentuu oppaan mukaan kolmesta isosta osiosta. Ensimmäinen ja suurin osio koostuu kybertoiminnoista. Ensimmäisenä mainittiin kyberpuolustuksen toimintaperiaate (Policy on Cyber Defence), joka luo pohjan kaikille muille toiminnoille. Siinä painotetaan yhteistä kyberpuolustusta, kybertoimintaympäristön operatiivista ulottuvuutta sekä teollisuusyhteistyötä. Lisäksi toimintaperiaate luo mandaatin Naton kyberpuolustuksen menettelytapoihin. Jäsenvaltioiden sisäisiin menettelytapoihin on luotu tukevia toimenpiteitä puolustussuunnittelun kautta. Toimenpiteiden avulla on tarkoitus ensimmäiseksi selvittää Naton jäsenmaiden kyberkyvykkyydet. Toiseksi toimenpiteillä edistetään jäsenvaltioiden kyberkyvykkyyttä yhteistyössä. Naton kyberkyvykkyyttä kasvatetaan poliittisten toimenpiteiden, harjoitustoiminnan, koulutusten sekä yhteistyön kautta. Käänteentekevä asia oli tulkinnallinen muutos kybertoimintaympäristöön, eli kyberpuolustusta ei nähty pelkästään tietoliikenneverkon tai digitaalisten laitteiden suojelemisena, vaan ennemminkin Nato-maiden demokraattisten instituutioiden autonomian turvaamisena. Tällöin kybertoimintaympäristö nähtiin myös poliittisena ulottuvuutena. Keskeisin muutos oli Varsovan huippukokouksen oppaan linjaus kansainvälisen oikeuden laajentamisesta myös kybertoimintaympäristöön. Tätä kutsuttiin tässä tutkimuksessa poliittisen kyberpelotteen vahvistamiseksi. Taustalla olleita tekijöitä olivat muun muassa Krimin valtaus, Ukrainan

kriisi, vaalivaikuttamisen nousu sekä tapahtumat Barentsinmerellä, Välimerellä, Mustallamerellä ja Itämerellä. Näiden takana on ollut Venäjä, jonka toimilla on ollut selkeä vaikutus Varsovan huippukokouksen oppaan sisältöön. Lainauksista päätellen Nato on implisiittisesti edustanut Venäjän vastakohtaa. Esiin nousee Naton kunnioitus kansainvälisiä sopimuksia kohtaan. Lisäksi lainauksista nousi esiin yksilön vapauden, demokratian, ihmisoikeuksien sekä laillisuusperiaatteen verbaalinen painotus. Näin voidaan päätellä, että Venäjä edustaa retorisesti Naton vastakohtaa rikkoessaan näitä periaatteita toiminnallaan. Lisäksi Venäjä on kasvattanut kansainvälistä jännitettä toimillaan Nato-maiden läheisyydessä. Krimin valtauksen ja Ukrainan kriisin jälkeen Varsovan huippukokouksessa pyrittiin selvästi vahvistamaan Naton pelotetta valmiussuunnitelmalla (RAP) sekä eteentyönnetyllä läsnäololla (EFP). Sama painotus nousi esiin myös kyberpuolustusta koskevissa lainauksissa. Jäsenmaiden kyberkyvykkyyden kehittämistä painotettiin niin harjoitustoiminnan, koulutuksen kuin poliittisten asiakirjojen kautta. Tällaisia asiakirjoja olivat lupaus kyberpuolustuksesta (Cyber Defence Pledge) sekä kyberpuolustuksen toimintaperiaate (Policy on Cyber Defence), joiden avulla on ollut tarkoitus vahvistaa yksittäisten jäsenvaltioiden kyvykkyyksiä.

Luvussa neljä painotus oli peloteteoriassa. Sillä on perinteisesti nähty olevan kaksi eri lähestymistapaa, pelote rangaistuksena (punishment) ja pelote vahvana puolustuksena (denial). Merkittävin poliittinen muutos tapahtui kybertoimintaympäristössä vuonna 2016, kun yhteinen puolustus ymmärrettiin yhtä lailla operatiivisena osa-alueena maan, meren ja ilman ohella. Skinneristä lausunnon ymmärtämisen kannalta on tärkeää tiedostaa, oliko kirjoittajan tarkoitus puolustaa, kritisoida tai hyökätä jotain argumenttia vastaan. Naton artikla 5 on lupaus sen jäsenmaille, mutta samalla varoitus sen vihollisille. Yhteinen puolustus edustaa Naton pelotetta, mikä on pysynyt samana vuodesta 1949 asti. Varsovan huippukokouksessa Naton kyberpuolustusta vahvistettiin eniten poliittisella tasolla. Brysselin huippukokouksen oppaassa nostettiin esiin konkreettinen muutos kybertoimintaympäristössä eli kyberpuolustukseen erikoistunut keskus sekä nopean toiminnan joukot. Pystyykö Nato pitämään yllä yhtä vahvaa pelotetta kybertoimintaympäristössä? Kybertoimintaympäristö ei poista fyysisen maailman pelotetta, mikä tarkoittaa sitä, että kyberhyökkäykseen voidaan vastata myös fyysisellä voimalla. Kybertoimintaympäristön suurin haaste on sen suhde fyysiseen aikaan. Siinä toimintaympäristössä tapahtuvat asiat voivat tapahtua nopeasti ja ilman ennakkovaroitusta. Kyberhyökkäysten vahvin pelote muodostuu tutkimukseni perusteella sodan ja rauhan välisen rajan hämärtymisestä. Kyberhyökkäykset koskettavat helposti jokaista yhteiskunnan osa-aluetta. Kyberhyökkäysten vaikuttavuutta on vaikea ennakoida,

kybertoimintaympäristön mahdollistaessa niiden kontrolloimattoman leviämisen. Kyberhyökkäyksillä voidaan vaikuttaa laajemmin ihmisen turvallisuuden tunteeseen. Tutkimuksessa esitettiin neljä tekijää, resilienssi, attribuutio, kyvykkyys sekä kyberomavaraisuus, jotka vaikuttavat kyberpelotteen rakentamiseen. Kyberympäristö on sotilaallista ulottuvuutta laajempi ja kattaa toimijoita yhteiskunnan eri osa-alueilta. Kyberhyökkäyksillä voidaan vaikuttaa laajemmin ihmisen turvallisuuden tunteeseen. Kyberhyökkäyksien ei ole tarkoitus ylittää yhteisen puolustuksen kynnystä, vaan niillä pyritään ennemminkin lamaannuttamaan vastustajan toimintaa. Kyberhyökkäyksien yleisyys haastaa myös niiden pelotteen toimivuuden. Attribuutio-ongelma kybertoimintaympäristössä on myös todellinen. Se edellyttää sitä, että hyökkäykseen pystytään vastaamaan, vaikka hyökkäyksen tekijää ei tiedettäisikään. Lisäksi kybertoimintaympäristössä täytyy työskennellä siitä lähtökohdasta, että ympäristöön on jo murtauduttu. Tämä edellyttää myös kyberympäristössä turvallisuuskulttuurin muutosta, mikä edellyttää ennakointia ja varautumista uhkiin, joita ei välttämättä ole vielä tapahtunut.

Digitalisaation kehitys ei ole poistanut fyysisen maailman uhkia, päinvastoin. Kyber- ja hybridiuhat ovat tuoneet oman ulottuvuutensa tähän kokonaisuuteen, joka on nyt yhtä lailla sotilaallisesti operatiivinen alue siinä missä maa, meri ja ilmakin. Natolla on kyvykkyyttä vastata toimintaympäristössä esiintyviin uhkiin. On kuitenkin kokonaan toinen asia, miten paljon poliittista tahtoa ja kyvykkyyttä Natolla on vastata tilanteisiin, jotka vaativat nopeaa reagointia. Mielestäni tällaiselle tutkimukselle voisi olla tulevaisuudessa tarvetta, koska tämä ei ilmene aineistosta. Lisäksi mielenkiintoisia tutkimuskysymyksiä olisivat esimerkiksi, miten hyvin Nato pystyy vastaamaan uhkiin, jotka eivät välttämättä ole sotilaallisia. Missä vaiheessa jäsenvaltion sähköverkkoon vaikuttaminen siirtyy Naton agendalle? Missä vaiheessa kyberuhkasta tulee sotilaallinen uhka?

Tutkimuksen aineistona oli Varsovan huippukokouksen pöytäkirja. Aineiston analyysiin työkaluina käytettiin skinneriläistä puhetekojen tulkintaa sekä peloteteoriaa. Voi olla, että keskeisten toimijoiden haastattelu olisi tuottanut hedelmällisemmän aineiston analyysin, mutta sellaisia toimijoita ei ole helppo päästä haastattelemaan gradua varten, minkä takia vaihtoehto ei tullut kysymykseen tämän tutkimuksen osalta. Puheteoista tutkimuksessa käytettiin ainoastaan lokuutiota ja illokuutiota. Puheteon kolmas osa, perlokuutio, jäi tämän tutkimuksen ulkopuolelle, koska jäsenvaltioiden toimet kyberpuolustukseen eivät selviä aineistosta. Aineisto on julkinen pöytäkirja, joka on kaikkien saatavilla. Näin ollen pöytäkirja on pintaraapaisu siitä, mitä Varsovassa lienee kaikkiaan keskusteltu. Kysely- tai haastattelututkimuksella olisi voinut saada esiin näkökulmia, jotka ovat jääneet pöytäkirjaa koostaessa mainitsematta. Tämän tutkimuksen

ohella heräsi myös kiinnostus kyberpuolustukseen yrityksien näkökulmasta, koska yritykset tuottavat yhä enemmän myös yhteiskunnalle keskeisiä palveluita. Missä määrin yritykset tekevät yhteistyötä Naton kanssa ja mikä on niiden näkökulma Naton kyberkyvykkyyden kehittämiseksi? Entä mikä rooli yrityksillä on Naton kyberpuolustuksen kehittämisessä?

Lähdeluettelo

Tutkimusaineisto

NATO Warsaw Summit Guide (2016): An essential Alliance in a more dangerous world. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf, 11.12.2018

Lähdeaineisto

Barkham, Jason (2001): "*Information Warfare and International Law on the Use of Force*".

Benedikt, Michael (1991): "Introduction to Cyberspace: First Steps". MIT Press. https://pdfs.semanticscholar.org/8517/59b84ee29d8fd9ee66b90316e4bc08406e15.pdf, 25.5.2018.

Bendiek, Annagret & Metzger, Tobias (2015): "*Deterrence theory in the cyber-century. Berlin: Stiftung Wissenschaft un Politik German institute for international and security affais*." 2.5.2015. Berlin: SWP German Institute for International Security Affairs.

Beggs, Cristopher (2009): "*Safeguarding Australia from Cyber-terrorism:A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption*". Perth: Edith Cowan University. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1004&context=isw, 18.3.2018

Cavelty, Myriam (2008): "*The reality and future of cyberwar. Department of Social Sciences and Humanities*", Cyber-Security and Threat Politics. https://pdfs.semanticscholar.org/bbba/7d388cb67e0d2b2ca7d7b2ed60ca2de65b1c.pdf, 17.3.2018

Delpech, Thérèse (2012): "Space and Cyberdeterrence". Teoksessa: *Nuclear Deterrence in the 21st century*, 141-157. Santa Monica: RAND Corporation.

Department of Defence (2001): Dictionary of Military and Associated Terms. Joint Publication 1-02. http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(10-08).pdf, 12.12.2018

ThreatCloud Intelligence (2018): Live Cyber Attack Threat Map. https://threatmap.checkpoint.com/ThreatPortal/livemap.html, 12.12.2018

Dev, R. Priyanka (2015): "*Use of Force and Armed Attack Threshold in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. response*". TexaS International Law Journals, 50(2), 380-398.

Eneken Tikk & Mika Kerttunen (2018): Cyber World and International Law. "*Use of force, Self-Defence and Countermeasures*". Jyväskylän yliopisto: luentosarja.

ENISA (2017): Threat Landscape Report 2017 15 Top Cyber-Threats and Trends. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017, 11.12.2018

Farr, James (1989): "*Understanding conceptual change politically*". Teoksessa: Political innovation and conceptual change, 24-46. Cambridge: Cambridge University Press.

Finlex (1980): Geneven yleissopimuksen LISÄPÖYTÄKIRJA kansanvälisten aseellisten selkkausten uhrien suojelemisesta: IV Osa siviiliväestö I Osasto Yleinen suojelu vihollisuuksien vaikutuksia vastaan I luku perussääntö ja soveltamisala: artikla 49. http://www.finlex.fi/fi/sopimukset/sopsteksti/1980/19800082/19800082_2#idp447139824, 11.12.2018.

Fidler, P. David, Pregent, Richard & Vandurme, Alex (2013): "*NATO, Cyber Defence and International Law*". Bloomington: Indiana University Bloomington.

Freedman, Lawrence (2004): Deterrence. Cambridge: Polity Press.

F-Secure (2019): Exploit Kits. https://www.f-secure.com/en/web/labs_global/exploit-kits, 5.2.2019.

Geneva Academy (2014): "*The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict –Interrelated or Distinct?*" Genéve: Geneva Academy Of International Humanitarian Law And Human Rights. http://www.prix-henry-dunant.org/wp-content/uploads/2014_IRMAKKESEN_Paper.pdf, 5.2.2019

Halminen, Laura (2016): "*Poikkeuksellinen kyberhyökkäys onnistui sammuttamaan ukrainalaisten sähköt*". 6.1.2016. Helsingin sanomat. https://www.hs.fi/ulkomaat/art-2000002878434.html, 5.2.2019

Hunker, Jeffrey (2010): "*Cyber War and Cyber Power Issues For Nato Doctrine*". Nato Defence College, (No. 62), p. 1-12. Italy: Rome.

Hyytiäinen, Mika (toim.) (2018): Tuleva sota: nykyhetki ennakointien valossa. Sotataidon laitos, Maanpuolustuskorkeakoulu. Keuruu: Otavan kirjapaino. http://www.doria.fi/bitstream/handle/10024/156904/Tuleva_sota_2.pdf?sequence=1&isAllowed=y, 12.12.2018

Iaisello, Emilio (2015): "*Are Cyber Weapons Effective Military Tools? Military and Stratefic Affairs*", 7(1), 23-39.

International Committee of Red Cross (2004) What is international Humanitarian Law? https://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf, 25.5.2018

International Board of Auditors for NATO (2016): Summary note to Council on the need to improve NATO's capability package process. https://www.nato.int/issues/iban/performance_audits/170201-improve-capability-package-process-eng.pdf, 12.12.2018

International Committee of Red Cross (1977): Definition of attacks and scope of application. https://ihl-databases.icrc.org/ihl/WebART/470-750062?OpenDocument, 5.2.2019

International Committee of Red Cross (2015): "What are jus ad bellum and jus in bello?". https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0, 5.2.2019

Israel Government Resolution 3611 (2011): Advancing National Cyberspace Capabilities. http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf, 12.12.2018

Joint Chiefs of Staff (2015): Joint Communications system. Joint Publication 6-0. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0.pdf, 12.12.2018

Kanerva, Jonne (2015): Paperivaltikka: arkistolaitos ja asiakirjahallinto poliittisen vallan välineinä Preussissa 1848-1918. Yleisen historian ja arkistonhallinnan pro-gradu tutkielma, Historian ja etnologian laitos, Jyväskylä: Jyväskylän yliopisto. https://jyx.jyu.fi/bitstream/handle/123456789/48184/URN%3aNBN%3afi%3ajyu-201512184102.pdf?sequence=1&isAllowed=y, 12.12.2018

Kuusisto, Rauno (2018): "Luotailua teemaan ja sen taakse". Teoksessa: *Tuleva sota: nykyhetki ennakointien valossa*. Sotataidon laitos, Maanpuolustuskorkeakoulu. Keuruu: Otavan kirjapaino. http://www.doria.fi/bitstream/handle/10024/156904/Tuleva_sota_2.pdf?sequence=1&isAllowed=y, 12.12.2018

Lehto, Martti (2017): Kybermaailman ilmiöitä ja määrittelyjä. Informaatioteknologian tiedekunta. Jyväskylä: Jyväskylän yliopisto.

Lehto, Martti (2011): SAL 11/2011 Kyberparveilu kybermaailman uusin uhka. https://www.upseeriliitto.fi/lehti/paakirjoitus/sal_2011/sal_11_2011_kyberparveilu_kybermaailman_uusin_uhka, 11.12.2018

Lehto, Martti & Limnéll, Jarno (2017): "*Kybersodankäynnin kehityksestä ja tulevaisuudesta*". Julkaisussa Tiede ja Ase (75).

Lehtomäki, Paula (2019): Kokonaisturvallisuutta tulevaisuusnäkökulmasta. Turvallisuuskomitea (toim.) https://turvallisuuskomitea.fi/kokonaisturvallisuutta-tulevaisuusnakokulmasta/, 5.2.2019

Lewis, A. James (2015): "*The Role of Offensive Cyber Operations in Nato's Collective Defence. NATO Cooperative Cyber Defence Centre of Excellence*", No. 8), 1-12. Estonia: Tallinn.

Liaropoulos, Andrew (2010): "*War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory*". Greece: University of Piraeus. https://www.academia.edu/292652/War_and_Ethics_in_Cyberspace_Cyber-Conflict_and_Just_War_Theory_in_9th_European_Conference_on_Information_Warfare_and_Security_University_of_Macedonia_and_Strategy_International_Thessaloniki_Greece_1-2_July_2010, 11.12.2018

Limnéll, Jarno, Majewski, Klaus ja Salminen, Mirva (2014): Kyberturvallisuus. Jyväskylä: Dosenco.

Limnéll, Jarno (2017): *Kyberhyökkäyksiin on vastattava politiikalla, sanktioilla tai jopa voimankäytöllä*. 11.7.2017. Yle. https://yle.fi/uutiset/3-9715578, 6.2.2019

Mika Kerttunen (2018): Cyber World and International Law. Jyväskylä: Jyväskylän yliopisto.

Moilanen, Panu (2017): Uudet teknologiat yhteiskunnassa. Teknologia ja kriisit. Jyväskylä: Jyväskylän yliopisto.

NATO (2009): "NATO's relations with the United Nations". https://www.nato.int/summit2009/topics_en/20-nato-un_relations.html, 11.12.2018

NATO Strategic Concept (2010): Active Engagement, Modern Defence. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, 12.12.2018

NATO (2011): Defending the networks, the Nato Policy on Cyber Defence. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf, 12.12.2018

NATO Chigaco Summit Guide (2012): https://www.nato.int/cps/en/natolive/topics_89738.htm, 7.2.2019

NATO (2014): Glossary Of Terms And Definitions. http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf, 12.12.2018

NATO (2016a): Cyber Defence Pledge.

https://www.nato.int/cps/en/natohq/official_texts_133177.htm, 25.1.2019

NATO (2016b): Topic: Consensus decision-making at NATO. https://www.nato.int/cps/em/natohq/topics_49178.htm, 5.2.2019

NATO Review Magazine (2016c): NATO: changing gear on cyber defence. https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm, 11.12.2018

NATO (2016): Secretary General's Annual Report. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170313_SG_AnnualReport_2016_en.pdf, 11.12.2018

NATO (2017a): "Why was NATO founded?". https://www.nato.int/wearenato/why-was-nato-founded.html, 11.12.2018

NATO (2017b): Nato Defence Planning Process. https://www.nato.int/cps/ua/natohq/topics_49202.htm, 11.12.2018

NATO (2017c): Smart Defence. https://www.nato.int/cps/ua/natohq/topics_84268.htm#, 11.12.2018

NATO Brussels Summit Guide (2018): A stronger and more agile Alliance. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180718_180711-summit-guide-brussels.pdf, 12.12.2018

NATO Industry Cyber Partnership (2018a): NATO and Cyber: Time to Raise our Game. http://www.nicp.nato.int/nato-cyber-defence/, 11.12.2018

NATO (2018b): Nato Glossary of Terms and Definitions (AAP-06).

NATO (2018c): NATO Cyber Defence https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf, 5.2.2019

NATO Cooperative Cyber Defence Centre of Exellence (2018): Locked Shields. https://ccdcoe.org/gallery/set/72157690295698290.html, 12.12.2018

Ottis, Rain (2008): "*Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*". Tallinn: Cooperative Cyber Defence Centre of Excellence.

Palonen, Kari (toim.) (2003): Key Contemporary Thinkers: Quentin Skinner: History, Politics and Rhetoric. Cambridge: Polity.

Pietilä, Kari (2017): NATON HYBRIDISODANKÄYNNIN MALLIN ILMENEMINEN UKRAINAN SODASSA. Maasotalinjan diplomityö. Helsinki: Maanpuolustuskorkeakoulu. http://www.doria.fi/bitstream/handle/10024/144266/Pietil%C3%A4KJ_YEK58.pdf?sequence=1, 5.2.2019

Poliisi (2018): Rikokset: Kyberrikollisuus. http://www.poliisi.fi/rikokset/kyberrikollisuus, 11.12.2018

Porche, R. Isaac, Sollinger, M. Jerry & McKay Shawn (2011):"A Cyberworm That Knows No Boundaries". Teoksessa: *A Cyberworm That Knows No Boundaries*, 1-17. Santa Monica: RAND Corporation.

Porvali, Mikko (2017): Informaation hallinta ja tiedustelu I: Tiedustelun historiaa. Jyväskylä: Jyväskylän yliopisto.

Puistola, Juha-Antero (2018): Kokonaisturvallisuus ja hybridivaikuttaminen. https://puolustusvoimat.fi/documents/1951210/8529440/Strategia_Juha-Antero-Puistola/d4c9fced-1d2e-4f59-9fd4-945fbe19dd5f/Strategia_Juha-Antero-Puistola.pdf, 5.2.2019

Ricoeur, Paul (1981): Hermeneutics and the Human Sciences. Käännös: John B. Thompson. Cambridge: Cambridge University Press.

Rousku, Kimmo (2018): Mistä digiturvallisuudesta on kyse? https://www.linkedin.com/pulse/mist%C3%A4-digiturvallisuudessa-kyse-kimmo-rousku, 5.2.2019

Schmitt, N. Michael (2012): "*Attack" as a Term of Art in International Law: The Cyber Operations Context".* International Law Department. United States Naval War College. Newport, U.S.A.

Schmitt, N. Michael (2011): "*Cyber Operations and the Jud Ad Bellum Revisted".* Pennsylvania: Villanova University, 56(3), 568-605.

Schwarz, Klaus-Dieter (2005): The Future of Deterrence. Berlin: SWP Research Paper.

Schwarz, Benjamin (2013): *The Real Cuban Missile Crisis : Everything you think you know about those 13 days is wrong*. 2/2013. The Atlantic. https://www.theatlantic.com/magazine/archive/2013/01/the-real-cuban-missile-crisis/309190/, 6.2.2019

Shea, Jamie (2017): "NATO: Stepping up its game in cyber defence". Teoksessa: Beckett Simon (2017): Cyber Security: A Peer-Reviewed Journal (toim.) Henry Stewart Publications https://www.henrystewartpublications.com/sites/default/files/CSJ1_2_Shea.pdf, 11.12.2018

Skinner, Quentin (1970): "Conventions and the Understanding of Speech-Acts". *Philosophical Quarterly,* 20-(79), 118-138. Oxford: Oxford University Press.

Skinner, Quentin (2002): Visions of Politics: Volume 1, Regarding Method. New York: Cambridge University Press

Snyder, H. Glenn (1961): "*Deterrence and Defence*". Princeton: Princeton University Press.

Suomen erityisedustusto Natossa (2017): Yhteinen puolustus ja pelote. http://www.finlandnato.org/public/default.aspx?nodeid=49916&contentlan=1&culture=fi-FI, 5.2.2019

Talous ja Tekniikka (2017): "*Maapallon väestöstä yli puolet käyttää internetiä – sosiaalista mediaa 40 %".* 9.8.2017. https://www.tekniikkatalous.fi/tekniikka/ict/maapallon-vaestosta-yli-puolet-kayttaa-internetia-sosiaalista-mediaa-40-6667907, 6.2.2019

Tikk, Eneken, Kaska, Kadri & Vihul, Liis (2010): "*International Cyber Incidents: Legal Considerations."* Nato Cooperative Cyber Defence Centre of Excellence. Estonia: Tallinn. https://ccdcoe.org/publications/books/legalconsiderations.pdf, 25.5.2018

Turvallisuuskomitea (2018): Elintärkeät toiminnot. https://www.turvallisuuskomitea.fi/index.php/fi/turvallisuuskomitea/25-kokonaisturvallisuus/40-elintaerkeaet-toiminnot, 11.12.2018

Turvallisuuskomitea (2017): Yhteiskunnan turvallisuusstrategia. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Turvallisuuskomitea (2017): Kokonaisturvallisuuden sanasto. Helsinki: Sanastokeskus TSK ry. https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf, 15.12.2018

United Nations (1945): UN Charter.
http://www.un.org/en/sections/un-charter/un-charter-full-text/

United Nations General Assembly (2015): Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174.
http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174, 12.12.2018

United Nations (2008): Definition of Aggression: General Assembly Resolution 3314 (XXIX). http://legal.un.org/avl/pdf/ha/da/da_ph_e.pdf, 5.2.2019

U.S. Department of Homeland Security (2018): Cybersecurity Stategy.
https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf, 12.12.2018

Valtiovarainministeriö (2018): Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma. 32/2018.
http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161218/VM_32_2018_Julkisen_hallinnon_digitaalisen_turvallisuuden_kehittamisohjelma.pdf?sequence=1&isAllowed=y, 7.2.2019

Veenendaal, Matthijs, Kaska, Kadri & Brangetto, Pascal (2016): "*Is Nato Ready to Cross the Rubicon on Cyber Defence?"*. Nato Cooperative Cyber Defence Centre of Excellence. Estonia: Tallinn.

Vitel, Philippe (2014): Cyber Space and Euro-Atlantic Security. Science and Technology Committee. Nato Parliamentary Assembly.

Ziolkowski, Katharina (2012): Stuxnet: Legal Considerations. Defence?. Nato Cooperative Cyber Defence Centre of Excellence, p. 1-26. Estonia: Tallinn.

Wilmshurst, Elizabeth (2005): "*Principles of International Law on the Use of Force by States in Self-Defence*". London: The Royal Institute of International Affairs.