Tampereen yliopisto

Roope Rannikko

# KYBERVALLAN KONSTITUOITUMINEN

## Euroopan unionin kybervallan identifiointia

Johtamisen ja talouden tiedekunta
Kandidaatintutkielma
Toukokuu 2020

# TIIVISTELMÄ

Roope Rannikko: Kybervallan konstituoituminen – Euroopan unionin kybervallan identifiointia
Kandidaatintutkielma
Tampereen yliopisto
Kansainvälinen politiikka
Toukokuu/2020

Tässä kandidaatintutkielmassa tutkitaan kyberturvallisuutta kybervallan näkökulmasta. Kybervallalla tarkoitetaan toimijan kykyä edistää strategisia ja poliittisia tavoitteita kyberfyysisessä toimintaympäristössä. Kyberfyysinen toimintaympäristö kattaa sekä kyberavaruuden että sen ulkopuolisen maailman, mitä hallinnoidaan poliittisin, sosiaalisin ja lainsäädännöllisin keinoin. Kyberfyysinen toimintaympäristö sulautuukin osaksi yksilöiden luonnollista ja yhteiskunnallista elämää esimerkiksi erilaisten päätelaitteiden avulla, kuten älypuhelimien, jotka mahdollistavat uudenlaisen tavan olla vuorovaikutuksessa ja toimia. Valtiot ovat viime vuosina kasvattaneet toimintakapasiteettiaan kyberympäristössä toimimiseksi. Kansainvälisessä politiikassakin kybervaltaa lähestytään asiana, joka muuttaa valtasuhteita maailmanpolitiikassa.

Yllä kuvattu määritelmä kybervallasta lähestyy kybervaltaa uudenlaisena aseena, ja sitä verrataankin 50 vuotta sitten kehittyneisiin ydinaseisiin, jotka mullistivat maailmanpolitiikan luonteen perustavanlaatuisesti. Kybervallasta on olemassa kolme erilaista määritelmää, jotka mukailevat realismia ja liberalismin variaatioita positivistisella tavalla. Kandidaatintutkielman kirjoittajan mielestä edellisen kaltaiset tavat katsoa kybervaltaa ovat kyseenalaisia, koska kyberympäristö rikkoo valtion väkivallan monopolin. Kyberhyökkäys voikin tulla mistä, milloin ja keneltä tahansa. Kandidaatintutkielmassa lähestytään kybervaltaa toisesta ääripäästä, joka konstituoituu osapuolten välisessä kanssakäymisessä. Työssä kerrotaan, mitä tarkoitetaan konstitutiivisella vallalla hyödyntäen konstruktivistisia ajatuksia diskursseista valtavälineenä ja todellisuuden muokkaajana. Konstitutiivisessa vallassa toimijat itse määrittelevät, miltä kybervallan tulisi osapuolten välillä näyttää. Edellisen kaltainen lähestymistapa suosii dekonstruktiivista selittämistapaa, joka määrittelee, mitä mahdollisuuksia ja rooleja toimijoille on muodostunut diskurssissa.

Esimerkkinä konstitutiivisesta vallasta käytetään Euroopan unionin kybervaltaa, koska unionin poliittinen järjestelmä suosii konstitutiivisia selityksiä. Tutkimuksessa dekonstruktoidaan Euroopan unionin kyberturvallisuusdiskurssi diskurssianalyysillä, tutkimalla unionin keskeisimpiä asiakirjoja tehokkaan kyberpuolustuksen ja siten kybervallan saavuttamiseksi. Tutkimuksessa tunnistetaan Euroopan unionilla olevan kuusi erilaista identiteettiä kybervallassa. EU:n tämänhetkinen rooli perustuu pääasiassa lainsäätäjän ja sääntelijän rooliin. EU:n kybervallassa korostuu sekä ylikansallinen että valtioidenvälinen yhteistyö, mutta EU pyrkii kasvattamaan kybervaltaansa turvallisuuskumppanin suuntaan. EU:n kyberturvallisuuden diskurssilla on inklusiivisia makrotason vaikutuksia, sillä kyberuhat uhkaavat valtiota laajempia maantieteellisiä alueita. Kybervallan tarkasteleminen konstitutiivisena johtaa toimijoiden väliseen tehokkaaseen yhteistyöhön, kun taas kybervallan näkeminen resurssina johtaa ankaraan kilpailuun toimijoiden välillä resurssin hallitsemiseksi.

Avainsanat: kybervalta, kyberturvallisuus, konstituoituminen, kybervaltaidentiteetti, dekonstruktio, diskurssivalta

# Sisällysluettelo

*1. Johdanto ..... 1*

*2. Turvallisuuspolitiikkaa vai politiikkaa turvallisuudesta? ..... 2*

**2.1. Valta ja turvallisuuden politisoituminen ..... 2**

**2.2. Diskurssit ja sanat todellisuuden luojana – dekonstruktiivinen lähestymistapa ..... 5**

**2.3. Kööpenhaminan koulukunnan näkökulma turvallisuuden poliittisesta konstruoitumisesta ..... 7**

*3. Mikä ihmeen kyberturvallisuus ja kybervalta? ..... 10*

**3.1. Hieman kyberturvallisuudesta ja kyberympäristöstä ..... 10**

**3.2. Kybervalta mahdollistaa toiminnan kyberfyysisessä toimintaympäristössä ..... 13**

*4. Diskurssianalyysi kybervallan rakentumisesta – EU:n kybervalta ..... 18*

**4.1. Dekonstruktiivisen diskurssianalyysin ja aineistolukutavan esittely ..... 18**

**4.2. Mitä kyberturvallisuuden diskurssit pitävät sisällänsä? ..... 24**

**4.3. Tutkimusaineiston esittely: EU:n keskeisimmät asiakirjat kyberturvallisuuspolitiikassa ..... 25**

**4.4. EU:n kyberturvallisuuden dekonstruktio ..... 27**

4.4.1. Predikointi ..... 27

4.4.2. Olettamus ..... 27

4.4.3. Subjektin paikannus: kybervallan identifiointia ..... 30

*5. Johtopäätökset ..... 33*

*Lähteet ..... 36*

*Liitteet ..... 41*

**Taulukko 6 tutkimusaineiston esittely ..... 41**

**Taulukko 5:n alkuperäiset lausumat ..... 43**

# 1. Johdanto

Kandidaatintutkielmassa tarkastellaan Euroopan unionin harjoittamaa kyberturvallisuuspolitiikka kybervallan näkökulmasta. Jotta kybervallan moniulotteisuutta voitaisiin ymmärtää, niin ensin tulee selvittää, mitä valta on. Valta onkin yksi politiikan tutkimuksen ja kansainvälisen politiikan peruskäsitteistä (Nye 2010, 2; Ruostesaari 2010, 28 & Van Haaster 2016, 8). Ensimmäiseksi tutkimuksessa väitetäänkin, että tämän hetkiset käsitykset kybervallasta mukailevat positivistisia turvallisuuskäsityksiä, jotka näkevät kansainvälisen anarkian luonteen konfliktisena ja, siten myös toimijoiden identiteetit itsestään annettuina (Fierke 2005). Toiseksi positivistinen tulokulma ei tarjoa tämän takia vaihtoehtoista tapaa selittää kybervaltaa, jolloin se ei onnistu uskottavalla tavalla kertomaan Euroopan unionin kybervallasta, tai integraatiosta tehokkaan kyberpuolustuksen aikaansaamiseksi. Tehokas kyberpuolustus on riippuvainen integroituneesta toimintamallista (*Integrated Capability Model)* (Klimburg 2011), jossa koko poliittinen järjestelmä pyrkii yhteistyössä aikaansaamaan onnistuneen kyberpuolustuksen kyberhyökkäyksiä vastaan. Kybervalta ja kyberturvallisuus sulautuvatkin tiiviisti toisiinsa integroituneessa toimintamallissa (Dunn Cavelty 2018, 309), sillä kybervallalla tarkoitetaan kykyä edistää itselleen mieluisia politiikkaetuja kyberavaruuden avulla.

Yhtenä tutkimuskysymyksenä onkin, *miten* Euroopan unioni muodostaa legitiimistä kyberturvallisuuden turvallistamisen diskurssia, jotta sen kybervalta integroituneen toimintamallin mukaisesti olisi hyväksyttävää? Lisäksi kun kybervalta sijoitetaan laajempaan keskusteluun vallan luonteesta, niin herää kysymys *missä olosuhteissa* kybervalta muuttuu poliittiseksi vallaksi ja, kuinka se voitaisiin käsitteellistää ja toteuttaa (Dunn-Cavelty 2019, 318). Kolmanneksi tutkimuksessa halutaan selvittää, *minkälaisena* kybervalta ilmenee konstitutiivisena, joka korostaa produktiivista ja diffuusiivista valtakäsitystä, jolloin valta ei varsinaisesti ole kenenkään hallinnoimaa (Barnett & Duvall 2005, 55). Aiemmat tutkimukset kybervallasta eivät ole tarkastelleet valtaa konstitutiivisesta näkökulmista (Dunn-Cavelty 2018, 309). Perinteisesti kybervallan tutkimukset ovat nähneet kybervallan hallittavana resurssina, joka muuttaa toimijoidenvälisiä valtasuhteita. Valta on silloin joko läsnä tai poissa, jonka seurauksena toimijalla on kybervaltaa tai sitten ei. Kandidaatintutkielman kirjoittajan mielestä edellisenkaltainen ajattelumalli on kyseenalaista, koska kybervalta on sitä, mitä toimijat tulkitsevat sen olevan. Kandidaatintutkielmassa pyritäänkin hahmottamaan yllä esiteltyjä kysymyksiä kybervallasta identiteetin rakentumisen kautta, jossa identiteetti toimii sekä poliittisen toiminnan perustana kuin tuotteenakin. Valtiolla on useita rooleja kyberturvallisuuspolitiikassa, jolloin valtion rooli kybervallan käyttäjänä on moniulotteisempi kuin mitä perinteiset kybervallan käsitteet olettavat.

Euroopan unionikin kybervallan käyttäjänä muodostaakin identiteettiään kybervallastaan suhteessa toisiin toimijoihin, erilaisissa yhdistelemisen ja erottelun prosesseissa, jossa yhdenlaista turvallisuusdiskurssia suositaan ennemmin kuin toista (Hansen 2006, 17-19). Tutkimuksessa osoitetaankin, miksi olisi tärkeätä kiinnittää huomiota erilaisiin kybervaltarooleihin, koska onnistunut kyberpuolustus ja siten kybervalta, ovat riippuvaisia monien erilaisten intressien yhteensovittamisesta parhaan yhteistyön saavuttamiseksi. Muutokset toimijoiden identiteeteissä muuttavat myös vallitsevia diskursseja ja myös käsityksiä ympäröivästä todellisuudestaan, jossa diskurssit syntyvät ja luovat itseään uudella tavalla.

Toisessa luvussa havainnollistetaan, kuinka positivistiset tulkinnat näkevät politiikan konfliktisena ja pyritään esittämään vaihtoehtoista tapaa ymmärtää politiikan luonnetta. Lisäksi luvussa kerrottaan turvallisuuden poliittisesta luonteesta ja, kuinka se voi johtaa yhdentyyppisen käsitykseen todellisuudesta. Luvussa kaksi havainnollistetaan, miten sanat muokkaavat käsityksiämme todellisuudesta sekä esitellään dekonstruktion keskeisimpiä ajatuksia. Kolmannessa luvussa esitetään kaikki tähän mennessä hahmotetut tavat ymmärtää kybervaltaa. Lisäksi luvussa kerrotaan lukijalle hieman kybertuvallisuudesta ja kyberfyysisestä toimintaympäristöstä. Luvussa osoitetaan, että konstruktiiviset tulkinnat turvallisuudesta voisivat myös täydentää integroitunutta toimintamallia. Neljännessä luvussa esitellään tutkimuksessa käytettävä aineisto, joiden pohjalta diskurssianalyysi tehdään. Esimerkkitapauksena tarkastellaan Euroopan unionin kyberturvallisuuden diskurssia, mikä suosii konstituoitunutta valtakäsitystä kyberturvallisuuden selittämiseksi. EU:n kybervalta dekonstruktioidaan Lynn Dotyn (1993) kehittelemän metodin mukaisesti predikoinnin, olettamuksen ja subjektin paikannuksen avulla. Kandidaatintutkielmassa huomataankin Euroopan unionilla voivan olla kuusi erilaista kybervaltaroolia taulukon viisi mukaisesti. Nykyisin Euroopan unionin kybervalta perustuu selkeimmin lainsäätäjän ja sääntelijän rooliin. Viidennessä luvussa esitellään tutkimuksen johtopäätökset sekä miksi olisi hyödyllistä pyrkiä tarkastelemaan kybervaltaa produktiivisen ja diffuusiivisen valtakäsityksen mukaisesti. Edellisessä tapauksessa valta konstituoituu osapuolten välillä ja määrittelee, mitä mahdollisuuksia toimijoille on muodostunut vuorovaikutuksessa.

# 2. Turvallisuuspolitiikkaa vai politiikkaa turvallisuudesta?

## 2.1. Valta ja turvallisuuden politisoituminen

Valta on yksi valtio-opin ja kansainvälisen politiikan keskeisimmistä käsitteistä, jolle ei olemassa yksinkertaista määritelmää (Nye 2010, 2 ; Ruostesaari 2010, 28 & Van Haaster 2016, 8). Yksi asia, josta kaksi edellä mainittua oppialaa ovat varmoja on, että vallalla ja politiikalla

on olemassa selkeä yhteys. Yksi määritelmä politiikalle onkin nähdä se vallan työkaluna, joka ulottuu kaikkialle yhteiskunnissamme ja kaikessa ihmistoiminnassa (Heywood 2013, 9). Jos politiikka ja valta nähdään yhtenä ja samana asiana, niin politiikka saa parhaimmillaan radikaalejakin ilmentymiä. Max Weber näkikin vallan väkivallan monopolina, joka yleensä kuuluu valtiolle eli suvereniteetille. Valta näyttäytyy silloin institutionaalisessa muodossaan, jossa valta on toimijoiden tavalla tai toisella omistamaa ja hallinnoimaa pääomaa (Ruostesaari 2014, 58). Heywood (2013, 10) kuvaileekin, silloin politiikassa olevan kyse ihmiselämään liittyvien resurssien tuottamisesta, jakamisesta ja niiden käytöstä. Politiikka näyttäytyy konfliktisena, koska resurssit ovat rajallisia, kun taas ihmishalu on rajaton. Politiikka on kamppailua rajallisista resursseista (Heywood 2013, 10), jossa valta liittyy resurssien hallintaan liittyvänä asiana. Vallan resursseja voivat olla muun muassa auktoriteetti, raha, väkivalta tai symbolinen suostuttelu, mutta institutionaalisessa muodossaan se ei kuitenkaan pelkisty mihinkään näistä, vaan vallanpitäjän kannalta valta on yleinen ja abstrakti asia (Ruostesaari 2014, 59).

Kansainvälisessä politiikassa puolestaan on tavallista puhua vallantasapainosta, jossa valta jakaantuu eri toimijoiden välillä. Vallantasapainossakin on kyse osapuolten välisestä riippuvuussuhteesta, koska muutoin valta lakkaisi olemasta kansainvälisessä ympäristössä, jos ei olisi toimijoita, joiden toiminnan ympärille se muodostuisi. Juuri ylemmän auktoriteetin puuttuminen kansainvälisessä järjestelmässä on johtanut anarkian määritelmään ja kansainvälisen suhteiden koulukuntien teoriakin rakentuu pitkälti anarkian määrittelylle. Nye (2010, 2) muistuttaa, koska vallalle ei ole olemassa yhdenlaista määritelmää, niin vallan tulkinta heijastelee osittain aina määrittelijän arvomaailmaa ja intressejä. Teoriatkin kansainvälisissä suhteissa ovat eräänlaisia yleistyksiä ihmisten ja valtioiden tavoista käyttäytyä erilaisissa tilanteissa. Esimerkiksi käsitykset sodasta ja orjuudesta ovat muuttuneet aikojen saatossa, jolloin ne eivät ole muuttumattomia asioita. Toisin sanoen ihmiskäyttäytyminen on avoin uudenlaisille habituksille ja normeille sen eksakteimmassa mielessä. (Fierke 2005, 1-4. & Waever 2011, 467.) Kansainvälisen politiikan realismin koulukunnalla on hyvin pessimistinen ihmisisolettamus, jolloin koulukunta näkee valtioiden välisen anarkian vihamielisenä. Realismin käsitykset ihmisluonteesta heijastuvat sen esittämissä teorioissa ja koulukunta korostaakin kuvailevansa maailmanpolitiikan ”objektiivista luonnetta”. Liberalismi puolestaan ei kiistä anarkian vihamielisyyttä, mutta uskoo esimerkiksi ihmisten rationaalisuuden ja taloudellisen tavoittelun mahdollistavan valtioiden välisen yhteistyön ja, siten vähentävän järjestelmän anarkiamaisuutta. Tieteessä metodologia voidaan mieltää tietyksi tavaksi tehdä, opiskella ja opettaa asioita. Vastaavasti maailma, mitä tutkimme (esim. kansainvälinen järjestelmä), liittyy tieteen epistemologiaan, kun taas ontologia vihjaa tuon tutkittavan maailman olemukseen (kansainvälisen järjestelmän

anarkian luonteeseen). Jos näemme kansainvälisen ympäristön realismin ja liberalismin eli tieteen positivistisella tavalla katsoa anarkian luonnetta, niin helposti voidaan päätyä lopputulokseen vallan, pahuuden, ahneuden ja konfliktien olevan pysyväluonteisia. (Fierke 2005, 5-9.)

Tutkiessamme ihmisten luomia asioita ja instituutiota, kuten sotaa, avioliitto, turvallisuutta tai valtiota, niin niille on hyvin vaikea löytää positivistista kaikenkattavaa teoriaa. Yksinkertaisesti, emme voisi positivistisesti mielekkäällä tavalla tutkia esimerkiksi avioliittoa ja verrata sitä havaintoihimme. Pystymme tunnistamaan avioliittoon liittyviä erilaisia ominaisuuksia, kuten neutraaliavioliitto, mies ja nainen, vihkiminen, perhe, pappi ja rakkaus muutamana esimerkkinä. Kaikki eroavaisuudet täydentävätkin siten avioliiton kokonaisvaltaista olemusta. Lisäksi avioliitto voidaan mieltää erilaisissa kulttuureissa eri tavoin, jolloin avioliitolle ei ole universaalista määritelmää. Pyrkiessämme selittämään avioliittoa meidän on siis *konstitutioitava (costitute)* käsitys avioliitosta eli toisin sanoen rakennettava riippuvuussuhteita asioiden välille. Ihmiset ovat vuorovaikutuksessa ympäristönsä, niin luonnollisen kuin rakennetun sekä toistensa kanssa. Ihmiset muokkaavatkin omaa maailmansa, jossa elävät koko ajan. Esimerkiksi käsitys suvereniteetista miellettiin aikoinaan ylivaltaa käyttäväksi monarkiksi, mutta nykyisin korkein valta kuuluu todennäköisesti valtion parlamentille. Vastaavasti suvereenius tunnustetaan toisten valtioiden toimesta eli kuka tahansa ei voi olla suvereeni. (Fierke 2005, 5-9.) Edellä olevan tarkoitus on osoittaa, ihmisten luomat asiat ovat usein historiallisia artefakteja ja niiden merkityksellisyydet ovat määrittelylle avoimia. Juuri konstruktivistiset tulkinnat ovat pyrkineet ymmärtämään, kuinka asioita määritellään ja niistä puhutaan eli sitä, miten ihmiset hahmottavat todellisuutensa. Konstruktivistiset tulkinnat lähtevätkin siitä olettamuksesta, ihmiset tekevät kielellä paljon muutakin kuin vain kuvailevat vallitsevia olotiloja. Konstruktivistiset teoriat eivät kiistä yhteiskunnallisten kausaalisten olosuhteiden olemassaoloa, mutta niitä ei monistikaan voida kuvailla sellaisenaan, kuten positivistiset teoriat toivoisivat (Fierke 2005, 14). Positivistiset teoriat saattavat antaa yleisiä luonnollisia olettamuksia asioiden olotiloista. Muun muassa realismissa valta nähdään taisteluna olemassaolosta ja samalla väkivaltaisuuden identiteetti otetaan itsestään annettuna, koska kansainvälinen ympäristö pakottaa tähän. Väkivalta voi olla luonnollinen ominaisuus, mutta konfliktit ja turvallisuus eivät ole luonnollisia asioita sellaisenaan, vaan riippuvaisia ihmismaailmasta.

Konstruktiivisessa selitystavassa valta voi saada sosiaalisissa suhteissa diffuusiivisempia ja konstitutiivisia muotojakin. Konstitutiivinen valta siis edeltää ennen sosiaalisia toimijoita ja myöskin siten määrittelee toimijoiden intressejä. Konstitutiiviset selitykset tutkivatkin, miten tietynlaiset sosiaaliset suhteet ovat tuottaneet tietyntyyppisiä toimijoita. Edellisen kaltaiset teoriat käsittelevätkin asioiden ominaisuuksia viitaten rakenteisiin, joiden nojalla ne ovat

olemassa. Sosiaaliset suhteet muokkaavatkin toimijoiden itseymmärrystä, jolla on myös vaikutuksia käyttäjän kykyyn muokata ympäristöään ja sen prosesseja. (Barnett & Duvall 2005, 46.) Konstitutiivinen valta osuvasti kuvastaakin, millaisia mahdollisuuksia toimijoille on muodostunut eikä niinkään, miten toimija hallitsee toista yksilöä tai resurssia. Vallalla on siten myös tuottavia ominaisuuksia konstruktiivisessa lukutavassa eli valta on produktiivista ja hajaantuneempaa. Produktiivinen valta muodostuu, siten kaikissa sosiaalisissa subjekteissa tietojärjestelmien ja laajempien diskursiivisten käytänteiden seurauksesta. Produktiivisessa vallassa on kyse merkityksistä ja tarkoituksista, mitkä ovat jäsenneltyjä, mutta eivät itsessään ole rakenteita. Valta nähdään sosiaalisten voimien verkostona, ikuisesti muokkaavana voimana ja menee yli vallitsevien rakenteiden. (Barnett & Duvall 2005, 55.)

## 2.2. Diskurssit ja sanat todellisuuden luojana – dekonstruktiivinen lähestymistapa

Konstruktivistiset tulkinnat liitetään usein valtio-opissa ja kansainvälisessä politiikassa kriittiseen teoriaan, joka tarkastelee valtavirtateorioita ja vakiintuneita käsitteitä kriittisesti. Jos oletetaan ideoiden olevan merkityksellisiä, niin tulee väittämiin kiinnittää erityistä huomiota (Risse 2009, 149). Yksinkertaisesti määriteltynä diskurssi voidaan ymmärtää ihmisten väliseksi vuorovaikutukseksi, jossa kommunikaatiota tutkimalla on mahdollistaa osoittaa ja paljastaa valtasuhteita osapuolten välillä (Heywood 2013, 18). Diskurssit perustavatkin hierarkioita ja valtasuhteita toimijoille, sillä toimijat antavat asioille tarkoituksia ja diskurssin konteksti määrittelee subjektin paikkaa (Foucault 2002, 57-58). Lingvistisestä käänteestä inspiroituneet suuntaukset ovat saaneet innoitteita Ferdinand de Saussuren oivalluksesta, jossa sanat koostuvat merkkijärjestelmistä, jotka voidaan rinnastaa todellisuudessa vallitseviin asioihin. Saussure ymmärsi merkkien merkityksellisyyden toimivan merkitsijän ja merkityn välillä sekä vertaamalla merkkejä todellisuudessa vallitseviin asioihin. (Derrida & Caputo 1997, 100-1.) Esimerkiksi on olemassa sana *hevonen* (merkitsijä), jolla tarkoitetaan konkreettista eläintä eli *hevosta* (merkitty). Saussurelle tämä mahdollisti kielen toiminnan. Pystymme erottamaan hevosen aasista ja seeprasta, niiden eroavaisuuksien ansiosta emmekä itse sanojen takia. Sanojen todelliset merkitykset ymmärretäänkin eroavaisuuksien ja toisten asioiden kautta (Wæver 2009, 166) muun muassa mies/nainen, hyvä/paha, kaunis/ruma ja kirjoittaminen/puhuminen.

Derridalainen *dekonstruktiivinen* lukutapa painottaakin merkityksien antamisen olevan loppumaton prosessi ja sanoilla on hierarkia toistensa välillä, jossa toista sanaa suositaan ennemmin kuin toista (Derrida & Caputo 1997, 103-5 & Wæver 2009, 166) muun muassa puhumista kirjoittamisen sijasta tai rationaalisuutta ennemmin kuin tunteellisuutta. Asioiden päättymätöntä merkityksettömyyttä voidaan havainnollistaa seuraavalla esimerkillä. Mietitään

esimerkiksi sana *leijona* (merkitsijä), jolla tarkoitetaan usein isoa *kissaeläintä* (merkitty). Kuitenkin leijona, joissain konteksteissa voidaan liittää myös *rohkeuteen* (merkitty) ja *hallitsijaan* (merkitty). Vastaavasti *hallitsija* voi symboloida *valtiota,* joka voidaan toisinaan liittää kokonaiseen *imperiumiin* (esim. kiinalainen tai brittiläinen imperiumi). Edellisen kaltaisessa jaottelussa sanat usein ymmärretäänkin eroavaisuuksien ja toisten asioiden kautta. Foucault (2002, 212) puhuikin, jokaiselle aikakaudella on omanlaisensa tiedollinen episteemi eli tietynlainen diskursiivinen muodostuma, mikä määrittää kielenkäytön ja ideoinnin rajat sekä yksilöiden tavan ymmärtää asioita. Diskurssit pyrkivätkin perustamaan transsendentaalisen viittauksen, eli jonkinlaisen havaintojen ulkopuolelle jäävän viittauksen kohteen, johon voimme perustaa lopullisen väittämämme, mutta tämäkin saa merkityksensä vasta muiden sanojen myötä (Wæver 2009, 166). Dekonstruktion (Derrida & Caputo 1997) avulla pyritään ymmärtämään eroavaisuuksia ja ristiriitoja erilaisten asioiden välillä. Esimerkiksi Lynn Dotty (1993) on hyödyntänyt dekonstruktiivista diskurssianalyysiä analysoidessaan Yhdysvaltojen 1950-luvun ulkopolitiikkaa sosiaalisesti rakentuneena philippiiniläisiä kapinoitsijoita kohtaan. Kanditutkielmassa käytetäänkin Lynn Dottyn kehittämää diskurssianalyysiä, jossa hyödynnetään predikointia, olettamusta ja subjektin paikantamista Euroopan unionin kybervallan selittämiseksi (luku 4).

Konstruktivistit uskovat todellisuutemme syntyvän ”sisältäpäin”, eräänlaisena intersubjektiivisena tietoisuutena, jossa subjektit rakentavat todellisuuttaan uskomuksien ja olettamuksien varassa (Heywood 2013, 16). Olettamukset ovat konstruktivistisissa selityksissä keskiössä silloin, kun ne ovat laajasti ymmärrettyjä ja, ne synnyttävät toimijoissaan identiteettejä ja intressejä. Tarpeeksi monen toimijan jakavan identiteettiin ja toimintaan liittyviä sääntöjä, vaikuttaa se myös ympäröivään sosiaaliseen maailmaan (Heywood 2013, 16). Konstruktivistiset selitysmallit mahdollistavat oppimisen ja toisen toimimisen mahdollisuudet esimerkiksi, jolloin käyttäjien identiteetit ja toimintamallit voivat muuttua tilanteesta riippuen. Konstruktivisti painottavat subjektien olettamuksien määrittyvän pääasiassa toimijoiden jaettujen käsityksien mukaan ennemmin kuin materiaalisten seikkojen. Toimijoiden identiteetit ja tarkoitukset muodostuvatkin, siten ideoiden rakentumisessa eikä toimijoiden oletetussa käyttäytymisessä (Wendt 1999, 1.)

Erityisenä huomiona dekonstruktiivisessa lukutavassa on pitää mielessä läsnäolevan (presence) ja poissaolevan (absence) välinen dynamiikka (Derrida & Caputo 1999, 79-80). Derrida oli hyvin kriittinen objektiivisen totuuden absoluuttisesta olemassaolosta, koska hänestä todellisuus oli liian monimutkainen, eikä yksikään konsepti onnistuisi tarpeeksi kokonaisvaltaisesti kuvailemaan vallitsevaa asiatilaa (Derrida & Caputo 1999, 31-2). Derridan mukaan, havaitsija kuvailee asian eroavaisuuksia ja asia saa merkityksensä vastakohdastaan.

Esimerkiksi läsnäoleva voidaan ymmärtää poissaolevan vastakohtana, mutta läsnäolevalle asialle on annettu etusija suhteessa poissaolevalle muun muassa tieteessä. Dekonstruktiossa uskotaankin havaitsijan tekevän asian näkyväksi olettamuksilla esimerkiksi, onko toimijalla valtaa tai ei. Absoluuttisen totuuden puuttuessa toimijoilla onkin vain totuudenkaltaisia olettamuksia ympäristöstään (Lynn Doty 1993, 306). Dekonstruktio painottaa asian olevan enemmän kuin vain läsnä tai poissa, jolloin asia voi saada monenlaisia muotoja muun muassa erilaisia vallan asteita. Esimerkiksi toimijoiden vaikutusvalta voi olla toimijoiden välillä vaihtelevaa, jolloin valta ei ole vain läsnä tai poissa absoluuttisessa mielessä. Dekonstruktiivinen lukutapa mahdollistaa uudenlaisen lukutavan, jolloin valta voi saada monenlaisia olemuksellisia muotoja jopa samanaikaisesti.

### 2.3. Kööpenhaminan koulukunnan näkökulma turvallisuuden poliittisesta konstruoitumisesta

Kuten yllä olevissa luvuissa pyritään havainnollistamaan positivististen suuntausten kausaalinen selittäminen saattaa johtaa hyvin pessimistiseen olettamukseen maailmanpolitiikan anarkian luonteesta ja siihen liittyvästä vallasta. Pessimistinen maailmankuva antaa myös tiettyjä olettamuksia toimijoiden luonteesta, jolloin positivistiset suuntaukset epäonnistuvat kuvailemaan toimijoiden identiteeteissä tapahtuvia muutoksia. Muun muassa kansainvälisten suhteiden perinteisimmät oppialat eivät kyenneet selittämään kylmän sodan loppumisessa tapahtunutta muutosta, jossa Yhdysvallat ja Neuvostoliitto lähentyvät toisiaan (Wendt 1992, 395-396 & Fierke 2005, 12).

Kansainvälinen järjestelmä asettaa valtiolle raamit, jonka sisällä ne toimivat. Yleisellä tasolla valtiot ovat ensisijaisesti vastuussa omasta ja kansalaistensa olemassaolosta. Yksinkertaisimmillaan voidaankin puhua eräänlaisista uhkakuvista, jotka uhkaavat edellä mainittujen olemassaoloa. Valtiot ovat kehittyneen aikoinaan yksilöiden suojelemiseksi eli turvaamiseksi ja valtiot voivat luoda myös itsekin uhkakuvia, luoden valtiolle olemassaolon tarkoituksen (Limnéll et al. 2018, 14). Kuten yllä mainitun avioliiton tapaa, turvallisuudella on olemassa useita erilaisia sen ominaisuuksia kuvaavia käsitteitä muun muassa *täydentäviä konsepteja*, jotka osoittavat tietyntyyppisiin kysymyksiin, esim. deterrenssi, strategia tai hallinta. Usein turvallisuudella on *rinnakkaisia konsepteja* poliittisesta teoriasta, jolloin siihen liittyviä termejä ovat valta, suvereniteetti ja identiteetti. Jotkut puhuvat turvallisuuden korvaamisesta kokonaan *vastakkaisilla käsitteillä* kuten rauhalla tai riskillä (Buzan & Hansen 2009, 14.) Ymmärrämme turvallisuuden sen eroavaisuuksien ja samankaltaisuuksien kautta, mutta samanaikaisesti turvallisuuden kokonaisvaltainen konsepti jää hieman tietoisuutemme ulottumattomiin

derridalaisessa mielessä. Liiallinen uhkakuvien maalailu voi aiheuttaa uhkakuvien inflaatiota, joka saattaa viedä huomion todellisista uhkaavista tekijöistä (Limnéll et al 2018, 15). Tällöin nouseekin muun muassa seuraavankaltaisia kysymyksiä kenen uhkakuvat tulisi ratkaista, mitkä lasketaan todellisiksi uhkakuviksi, kuka toimii turvaajana ja mikä tulisi turvata?

Turvallisuuteen liittyvää tietoteoreettisia seikkoja voidaan lähestyä ainakin kolmella tavalla. Ensimmäinen ja perinteisin tapa hahmottaa turvallisuus on nähdä se objektiivisena käsitteenä. Turvallisuutta lähestytään materialistisin seikoin ja konkreettiset uhkakuvat ovat joko läsnä tai poissa. Toiseksi turvallisuus voi näyttäytyä subjektiivisesti, eli toimijan näkökulmasta. Turvallisuus rakentuukin subjektin omista uhkakokemuksista ja näkökulma painottaakin turvallisuuteen liittyvää sosiaalista kontekstia sekä historiallista ja psykologista tuntemusta (väärin) havaitusta uhasta. Subjektiivinen turvallisuuskäsitys ylläpitää viittauksen myös objektiin, joka voi olla itse uhkaaja tai turvaaja. Viimeiseksi turvallisuus saatetaan mieltää diskursiivisena konseptina, mitä usein kriittiset teoriat painottavatkin omissa teorioissaan. Diskursiivisena käsitteenä turvallisuutta ei voida kuvailla objektiivisin termein, vaan turvallisuus rakentuu puheakteissa. Kriittiset teoriat painottavakin turvallisuuden olevan intersubjektiivinen kokemus, jossa uhkatekijä nousee poliittiselle agendalle turvallisuusongelmana. (Buzan & Hansen, 2009 34.) Turvallisuuden tutkimuksessa onkin alettua puhua laajasta ja kapeasta turvallisuuskäsityksestä, jossa kapeampi käsitys yhdistetään niin sanotusti ”kovaan turvallisuuteen” eli pääsääntöisesti turvallisuuden sotilaallisiin ja strategisiin seikkoihin. Laajempi turvallisuuskäsitys puolestaan pyrkii huomiomaan esimerkiksi ympäristöön, talouteen ja ihmisten sosiaalisen hyvinvointiin liittyviä uhkia. Kritiikkinä laajemmalle turvallisuuskäsitykselle esitetäänkin, että kaikkia uhkia ei voida ratkaista, vaan niiden ratkaisemissa on preferoitava ongelmia. Toiseksi, jos kaikki voidaan lukea turvallisuuden piiriin, niin turvallisuus menettää merkityksensä.

Kööpenhaminan koulukunta onkin pyrkinyt löytämään keskitietä *turvallistamisen teoriallaan* laajan ja kapean turvallisuuskäsityksien välille (Wæver 2011, 466-7). Koulukunta osoittaakin, miten yksilöt muodostavat uhkakuvia, tarjoten konstruktiiviselle perspektiiville vasta-argumentin objektiiviselle (materialismia painottavalle) turvallisuuskäsitykselle (Buzan & Hansen 2009, 36). Toiseksi koulukunta painottaakin teorioissaan, kaikkien kansainvälisen politiikan teorioiden olevan eräänlaisia kannanottoja maailmanpolitiikasta. Teoriat ovat vain reflektioita maailmanpolitiikasta, sillä ihmisillä on mahdollisuus valita mitä sanovat tilanteesta riippuen (Wæver 2011, 466). Kolmanneksi koulukunta ehdottaa kielen merkityksellisyyttä todellisuuden luojana. Esimerkiksi lingvistisestä käänteestä inspiroituneet tutkijat uskovat, akateemisessa maailmassakin analysoijan ja analysoitavan olevan jatkuvassa vuorovaikutuksessa luoden merkityksen tutkittavalle kohteelle (Waever 2011, 467). Neljänneksi sanoilla on

merkitystä ja niilläkin on seurauksia. Esimerkiksi erilaisilla väittämillä voidaan kuvailla asioiden olemuksia, mutta niillä voidaan ohjata ihmisten käyttäytymistä ja selvittää sanojan aikomuksia. Puheaktiteoria pohjautuu J. L. Austinin ajatuksiin lokuutio-, illokutiio- ja perlokuutiolausumista. Lokutionaariset lausumat pitävät sisällään asioiden luonnollista kuvailua, illokutionaarinen puheakti korostaa sanojan aikomuksia ja perlokutionaarinen väite määrittelee vastaanottajan reaktiota. (Vuori 2016, 28-31). Esimerkiksi Vuori (2016, 44-45) on tarkastellut artikkelissaan ydinasepelotteen vaikutuksia maailmanpolitiikassa ja todennut, toimivan ydinasepelotteen olevan perlokutionaarinen puheakti.

Turvallistaminen nähdään puheaktisuorituksen kaltaisena tekona, joka vaikuttaa toimijaan. Kööpenhaminan koulukunnalla onkin erilainen politiikkakäsitys kuin realismilla ja liberalismilla. Turvallistamisen kehittäjä Wæver (2011, 478) korostaa, hänen tapansa ymmärtää politiikka on arendtilainen. Arendt (2017) teoksessaan; ”*Vita activa — Ihmisenä olemisen ehdot”,* pyrkii tarjoamaan vaihtoehtoisen tavan mieltää politiikka perinteisen valtapolitiikan sijasta. Hän näkikin politiikan olevan luonnollista toimintaa ihmiselle ja politiikka syntyy ihmisten välisessä vuorovaikutuksessa. Hän korostaa ihmisen olevan ensisijaisesti poliittinen eläin, mikä erottaa ihmisen muista eläimistä. Näin hän rinnastaa inhimillisyyden ja politiikan toisiinsa, sillä ihmiset kohtaavat toisensa tasavertaisina yksilöinä politiikassa. (Arendt 2017.) Arendtilainen politiikkakäsitys pohjautuu antiikin kreikkalaisten *klassiseen demokratiamalliin* (Held 2006, 18-33), jossa kansalaisuuden saaneilla oli tasavertainen mahdollisuus osallistua *polisen* hoitamiseen. Wæver (2011, 468) kirjoittaakin Arendtin vaatineenkin politiikan olevan tuottavaa, peruuttamatonta ja tapahtuvan ihmisten välillä odottamattomina tapahtumaketjuina. Politiikka ei ikinä ota tällöin sellaista muotoa, jossa joku nappaisi vallan itselleen ja tuottaisi ennalta-arvatun lopputuloksen. Politiikassa toiminta on aina riippuvainen muiden toiminnasta, joka määrittelee politiikan lopputulosta. Toiminnan tiettyä ”tarkoitusta”, tai ”hyvyyttä” ei voida tietää ennalta kuin vasta myöhemmin historiassa. (Waever 2011, 468.)

Kööpenhaminan koulukunnan käsitykset tarjoavat vaihtoehtoisen tavan ymmärtää kansainvälistä politiikkaa kuin, miten positivistiset suuntaukset sen olettavat. Mikään itsessään ei päädy turvallisuuden piiriin, vaan kyse on uhkakuvien hallitsemisesta (Wæver 2011, 468) eli politisoimisesta. Turvallisuus ei itsessään tarkoita mitään, vaan se saa merkityksensä vasta käyttöyhteydessään kuten uhatkin (Limnéll et al, 2018 15). Turvallisuus funktiona tarvitsee myös viittauksen toiseuteen. Turvallisuuslausumissa toimijat eivät vain kuvaile vain itseään ja muita, mutta myös määrittelee havaitun asian piirteitä. Turvallisuuden merkitys perustuukin vahvasti asioiden eroavaisuuksien ja yhtäläisyyksien tunnistamiseen (Hansen 2012, 530). Turvallisuuden absoluuttista olemusta ei voida saavuttaa, koska esimerkiksi ilmastonmuutoksen

uhkaa ei pystyisi käsittämään, jos ei sitä ei yhdistettäisi ilmastonlämpenemiseen, hiilidioksidipäästöihin, lämpimiin ja kylmempiin ajanjaksoihin tai lajien sukupuuttoon. Myös ilmastonmuutoksen vastainen tila on derridalaisesti implisiittisesti läsnä, jolloin ilmastonmuutos saa olemuksellisen merkityksensä.

Turvallistaminen tulisikin nähdä prosessina, joka koostuu neljästä osasta. Turvallistaminen pitää sisällään turvallistajatoimijan (esim. komissio), joka tekee ”turvallistavan” lausunnon. Toiseksi turvallistaminen tarvitsee eksistentiaalisen uhan eli objektin, jota pidetään potentiaalisesti harmillisena (esim. kyberrikolliuus). Kolmanneksi turvallistamisisessa viitataan aina asiaan, jota pitää suojella (esim. EU:n sisämarkkinoita). Lopuksi yleisön on hyväksyttävä jokin asia turvallisuusuhkana, koska vasta silloin turvallistaminen on onnistunut (esim. jäsenvaltiot integroituvat tehokkaamman kyberpuolustuksen saavuttamiseksi). Perinteisesti politiikassa asioita voidaan pyrkiä politisoimaan tai epäpolitisoimaan asioita. Kuitenkin turvallistamisen prosessi on kyse äärimmäisestä poliittisesta toimenpiteestä, jossa jokin asia nostetaan julkisen keskustelun yläpuolelle ”turvallisuuden nimissä”. Turvallisuuden nimissä asiasta ei väitellä poliittisena asiana, vaan asia käsitellään nopeasti päätöksenteossa, mikä voi puolestaan vahingoittaa normaaleja laillisia ja sosiaalisia sääntöjä. Kööpenhaminan koulukunta korostaakin asioiden epäturvallistamista (*desecuritization)*, jolloin asia pyritään palauttamaan takaisin normaaliseen poliittiseen keskusteluun. (Buzan & Hansen 2009, 213-14; Hansen 2009, 1158-60.). Turvallistamisessa on myös kyse tietyntyyppisestä diskursseista ja pätevyydestä puhua asioista. Esimerkiksi sotatieteissä on erilainen tyyli puhua sodasta kuin konfliktin- ja rauhantutkimuksessa. Tietynlainen alakohtainen koulutus johtaa tietyntyyppiseen tapaa puhua asioista normaalisesti (Vuori 2016, 39). Normaalistumisen prosessissa ulkoa annettu ideaali johtaa ”normaalisena” pidettyyn asiaan esimerkiksi ympäröivän maailman hahmottamiseksi.

# 3. Mikä ihmeen kyberturvallisuus ja kybervalta?

## 3.1. Hieman kyberturvallisuudesta ja kyberympäristöstä

Kyberturvallisuudesta ja kyberulottuvuudesta on tullut osa arkipäiväämme ja tämä näkyy siinä, että EU on jo vuonna 2013 julkaissut kyberturvallisuutta käsittelevän strategiansa; ” *Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö”*. Vielä ennen 2010-lukua Euroopan unioni on viitannut hyvin epäsuoranaisesti kyberulottuvuudessa esiintyviin uhkakuviin (Carrapico & Barrinha 2017, 1259-60 & Dunn-Cavelty 2018, 312). 2010-luvulla myös kansallisvaltiot ovat alkaneet määrittelemään kyberturvallisuutta koskevia strategioita enimmissä määrin (ks. Dunn-Cavelty 2018; Lehto et al. 2017; Limnéll et al.

2018, 164-180 & Kello 2018, 58-59). Suomessakin ”kyber”-käsite esiintyi ensimmäisen kerran suomalaisissa turvallisuusstrategioissa vasta vuonna 2010 (Limenèll et al. 2018). Kybersanana on kuitenkin vanhempi, sillä onhan Internetkin ollut jo olemassa 1990-luvulta alkaen. Esimerkiksi Euroopan unioni on korostanut informaatio- ja kommunikaatioteknologian roolia omien sisämarkkinoiden edistämiseksi jo 1990-luvulla julkaistuissa asiakirjoissaan (Carrapico & Barrinha 2017, 1259). Kyberturvallisuusala kattaakin monenlaisia asioita ja toiminnan muotoja. Muun muassa kyberturvallisuuden piiriin voidaan lukea kybersota, kyberterrorismi, kybervakoilu, kyberrikollisuus, haktivismi ja hakkerointi (Limnéll et al. 2014, 113). Lisäksi EU on alkanut harjoittaa kyberdiplomatiaa (Komissio cybersecurity 2020) virallisesti vuodesta 2017 alkaen sekä Suomenkin ulkoministeriöönkin on perustettu kybersuurlähettilään (Lehto et al 2017, 205) virka. Huolimatta kyberturvallisuuden kasvaneesta merkityksestä yhteiskunnissamme, niin kyberturvallisuudelle tai kyberympäristölle, ei ole löydetty yksiselitteistä määritelmää. Kyberala voidaan nähdä sekä laaja-alaisesti että kapealla sektorilla.

Alkujaan kyberturvallisuus liitettiin vahvasti tietoteknillisiin käsityksiin virtuaalimaailmasta, jolla tarkoitettiin datan suojelemista haluamattomilta paljastuksilta, tiedon muuntelulta, tai tuhoamiselta sekä itse tietojärjestelmien suojelemista (Hansen & Nissenbaum 2009, 1160). Kyber-sanan etymologia on peräisin antiikin Kreikasta (*cybernetice*), jolla tarkoitetaan ohjausta ja hallintaa. Ohjauksen kohteena saattoi olla kansa, jolloin sanalla viitattiin esimerkiksi valtion hallintakoneistoon. Kyber-sanan merkitys onkin siis muuttunut ja tavallisesti tietoturva liitetäänkin tietojen, tiedostojen ja yksittäisten koneiden suojaamiseen. Kyberturvallisuus tarkoittaa puolestaan tietoturvan ulottamista yhteiskunnan peruspalveluihin muun muassa sähkön- ja vedenjakeluun sekä tietoliikenneyhteyksien toimimiseen koko yhteiskunnassa. (Van Haaster 2016, 13 & Järvinen 2018, 13-14.) Lyhyesti sanottuna huolimatta kyberturvallisuuden ”tietoteknillis-painotteisuudesta” kyberturvallisuudella on myös vahvoja yhteiskunnallisia ja poliittisia ulottuvuuksia ja osittain ”kyber-sanan” epämääräisyys on varjostanut sanan tietoteoreettista viitekehystä. Tärkeää onkin, riippuen tutkimuksesta määritellä, mitä kyberturvallisuuden osa-aluetta tutkimuksessa tarkastellaan sekä myös, millä tavoin kyberympäristö hahmotetaan. Juuri yhteiskunnallisen merkityksen kasvun seurauksena ja globaaliluonteisuutensa takia kansallisvaltiot ovat kiinnostuneita hallitsemaan kyberympäristöä (Limnéll et al. 2018,165 & Kello 2018, 1-3). Kybertilaa halutaan luonteensa vuoksi hallita ylikansallisvaltiorajojen ja EU korostaakin unionin roolia (Strategia 2013 & Resilienssi 2017) kyberasioiden koordinoimisessa. Keskeisimpiä ylikansallisia viranomaisia kyberturvallisuuden hoitamisessa ovatkin Europolin alainen Euroopan kyberturvallisuuskeskus (EC3), Euroopan unionin verkko- ja

tietoturvavirasto (ENISA) sekä Computer Emergency Response Team (CERT-EU) (Carraprico et al. 2017, 1263).

Tieteessä pyritään tarkkoihin määritelmiin, mutta kyberturvallisuudelle ja kyberympäristölle ei ole annettu kaiken kattavaa määritelmää. Kuten jo ylempänä todettua kyberympäristö voidaan mieltää sekä laaja-alaisesti tai kapea-alaisesti. Esimerkiksi *kyberavaruus* (*cyber space)* voidaan nähdä pelkästään koostuvan kaikista verkoista ja tietokoneista, jotka ovat olemassa. Kyberavaruus koostuisi silloin kolmesta erilaisesta kerroksesta. Ensimmäinen kerros kattais Internetin ja siihen yhdistyvät päätelaitteet. Toinen kerros pitäisi sisällään kaikki ne solmukohdat, joilla on mahdollista liittyä World Wide Webiin (WWW). Kolmas kerros puolestaan rakentuisi omista itsenäisistä verkoista, jotka eivät ole yhteydessä Internetiin. Vastaavasti *kyberpiirin* (*cyber domain*) luettaisiin kaikki ne toimijat ja instituutiot, jotka hallinnoivat ja operoivat kyberavaruutta. Edellisen kaltaisella jaottelulla halutaan painottaa kahden eri ympäristön hallitsemiskeinoja. Kyberavaruutta hallitaan koodien avulla, kun taas kyberpiiriä kontrolloidaan poliittisin ja sosiaalisin keinoin, jolloin ne ovat alttiita sosiaalisille normeille. (Kello 2018, 45-46.) Tämänkaltainen jaottelu tuntuu myös hassulta. Esimerkiksi kyberavaruudella on vahva geopoliittinen ulottuvuus, sillä kyberavaruus on olemassa fyysisten asioiden muun muassa kaapeleiden, satelliittien ja verkkokeskuksien ansioista. Edelliset asiat ovat alttiita fysikaalisille luonnonlaeille eli, kos satelliitti lakkaisi toimimasta, niin sillä olisi vaikutusta myös kyberavaruuden toiminnalle. (Sheldon 2014, 287-88.) Toiseksi sotatieteissä kyberympäristö hahmotetaankin yhtenä sodankäynnin viidentenä ulottuvuutena, joka osittain sivuaa maa-, meri-, ilma- ja avaruussodankäyntiä (Limnéll et al. 2014, 141). Myös Euroopan unioni tarkastelee puolustusstrategioissaan kyberympäristöä kokonaisvaltaisesti, joka muokkaa edellä mainittuja sodankäynnin osa-alueita (CSDP 2017, 37).

Tässä tutkimuksessa kyberympäristö mielletäänkin kyberfyysisenä toimintaympäristönä. Kyberfyysisellä toimintaympäristöllä viitataan muotoutumassa olevaan ympäristöön, jossa digitaalinen ja fyysinen maailma ovat kietoutuneet tiivisti yhteen. Ihmisten elämismaailmassa tietoteknologia kytkeytyy näin ”luonnolliseksi”, huomaamattomaksi osaksi arkipäiväämme. (Salminen 2018, 266.) Määritelmä kattaa sekä kyberavaruuden että kyberpiirin. Kyberfyysistä toimintaympäristöä tulisi lähestyä kuin luonnollista ja yhteiskunnallista ympäristöäkin. Luonnollinen ja yhteiskunnallinen maailma elävät rintarinnan, jolloin ihminen pystyy muokkaamaan molempia ympäristöjään. Ihmisen toiminta kahdessa edellä mainitussa ympäristössä on erilaista, aivan kuten kybermaailman ympäristössäkin. Kybermaailma muuttaa esimerkiksi aika- ja tilakäsityksiä, mutta kyberympäristö on silti loppupeleissä ihmisen rakentama ympäristö ja avoin ihmisten määrittelemille säännöille. Kyberfyysinen toimintaympäristö on

maailma, jossa kyberoperaatiot kohdistuvat virtuaalimaailmaan ja fyysiseen laitemaailmaan, liittäen kyberavaruuden osaksi globaalia ympäristöä (Lehto & Limnéll 2017, 195-6). Kybervallassa onkin kyse kyberfyysisen toimintaympäristön lainalaisuuksien ymmärtämisestä. Ympäristönä se tuleekin asettamaan haasteita tieteelle ja tutkimukselle, sillä se tarvitsee poikkitieteellistä lähestymistapaa. Artech (2011, 5-6) esittääkin, että kyberfyysisen toimintaympäristön tekniikan hallitsemiseksi tarvitaan koneinsinöörien, sähköinsinöörien ja tietojenkäsittelytieteiden yhteistyötä. Kuitenkin, jotta kyberfyysisestä toimintaympäristöstä voidaan saada koko sen potentiaali hyödyksi, niin tarvitaan myös taloustieteiden ja yhteiskuntatieteiden apua edellä mainittujen tieteen alojen lisäksi (Acatech 2011, 5-6.)

### 3.2. Kybervalta mahdollistaa toiminnan kyberfyysisessä toimintaympäristössä

Jarno Limnéll et. al. (2014, 39) antavat kyberturvallisuudelle seuraavanlaisen määritelmän; ”Kyberturvallisuus tarkoittaa digitaalisen maailman tilaa, jossa vallitsee sekä ymmärryksen myötä tunnettu luottamuksen tunne että käytännön toimenpitein saavutettu kyky ennakoivasti hallita sekä sietää kyberuhkia ja niiden vaikutuksia”. Kyberturvallisuudella pyritään varautumaan kybermaailmassa tapahtuviin uhkiin eli kyberhyökkäyksiin. Kyberhyökkäyksillä tarkoitetaan tietokoneiden tietojärjestelmien häiritsemistä koodien avulla poliittisten ja strategisten tavoitteiden saavuttamiseksi. Kyberhyökkäys koostuukin hyökkääjän halusta ja kyvystä häiritä tietokoneiden toimintoja, tai tuhota fyysisiä resursseja kyberavaruuden kautta. (Kello 2018, 51.) Juuri kyberturvallisuuteen liittyvien uhkien hallinnan seurauksena Nye (2010) on kehitellyt kybervallan käsitteen.

Kybervallalla Nye (2010) tarkoittaa kykyä saavuttaa haluttuja lopputuloksi käyttäen kyberpiirin tarjoamia toisiinsa kytkeytyneitä informaatioresursseja. Kybervalta perustuukin tietokoneisiin liittyvien tietojen kontrollointiin, luomiseen ja kommunikaatioon sekä infrastruktuuriin, verkkoihin, ohjelmointiin ja ihmistaitoihin liittyviin asioihin. Kybervalta on siis kykyä käyttää kyberavaruutta luomaan etuja ja vaikuttamaan tapahtumiin muissa operationaalisissa ympäristöissä erilaisilla valtavälineillä. Kybervalta kattaa lisäksi sekä kyberavaruuden että sen ulkopuoliset ympäristöt. (Nye 2010, 3-4.) Tämänkaltainen tulkinta kybervallasta pitääkin sisällään poliittisen, hallinnollisen, taloudellisen ja sosiaalisen ulottuvuuden. Kybervaltaa voidaan käyttää suoraan (esimerkiksi kyberhyökkäys ja kyberpuolustus) tai epäsuorasti (esimerkiksi maine tai tietovalta) (Limnéll et al. 2014. 240).

Kybervallasta onkin kehitelty kolme erilaista variaatiota, jotka ovat Nyen (2010, 7) kybervallan kolme osa-aluetta, Betzn and Stevensn neljä kybervaltatyyppiä (Dunn-Cavelty 2018, 309) sekä Klimburgin integroitunut toimintamalli (Kilmburg 2011; Dunn-Cavelty 2018, 301).

Nyen (taulukko 1) pyrkiikin tarkastelemaan kybervaltaa puhtaasti ikään kuin mitattavana valtaresurssina, josta häntä on myös kritisoitu. Kybervaltaa tulisikin lähestyä enemmän suhteellisesti (*relationally*), joka aktualisoituu toimijoiden välisissä suhteissa. (Van Haaster 2016, 10-11.) Vallan suhteellisella ajattelutavalla korostetaan, kybervallan vaikutusvallan olevan riippuvainen kontekstistaan ja kaiken kaltaiset kyberhyökkäykset eivät ole kybervallan näkökulmasta tehokkaita.

Taulukko 1: Kybervallan kolmet kasvot

| Vallan muoto | Kova valta | Pehmeä valta |
|---|---|---|
| A estää B:tä tekemästä jotain, mitä B ei muutoin tekisi. | palvelunestohyökkäykset<br><br>haittaohjelmien syöttäminen<br><br>SCADA-häiriöt<br><br>bloggaajien pidätykset. | Tiedotuskampanja hakkereiden alkuperäisten mieltymysten muuttamiseksi<br><br>Terroristijärjestöjen jäsenten rekrytointi |
| Agendavalta: (A tekee B: n valinnan mahdottomaksi, sulkemalla sen B:n vaihtoehdoista pois). | Palomuurit<br><br>Tietojen suodattaminen<br><br>yrityksien painostaminen joidenkin ideoiden poisjättämiseksi. | Internet-palveluntarjoajien ja hakukoneiden omavalvonta<br><br>Verkkotunnusten ICANN-säännöt<br><br>Laajalti hyväksytyt ohjelmistostandardit. |
| A muokkaa B: n mieltymyksiä siten, että joitain strategioita B ei edes tule koskaan harkinneen | Uhkailu bloggaajien rankaisemiseksi, jotka levittävät sensuroitua materiaalia | Taipumuksia muokkaava informaatio (esim. nationalismin stimulointi ja ”isänmaalliset hakkerit”)<br><br>Normien kehittäminen, jotka herättävät inhoa (esim. lapsipornografia) |

Lähde: Nye, Joseph Jr. (2010, 7).

Betzllä ja Stevensllä (taulukko 2) on käsitteellisempi tapa lähestyä kybervaltaa verrattuna Nyen, sillä he kiinnittävät huomiota vallan eri muotoihin. Van Haaster (2016, 15) toteaakin, Betz ja Stevens pyrkivät hahmottamaan areenan, josta vallasta kamppaillaan, kun taas Nye kuvailee enemmän niitä aseita, joilla kamppailua harjoitetaan. Toisaalta Betz ja Stevens eivät kauheasti kerro esimerkkejä, kuinka rakenteellista ja produktiivista kybervaltaa voitaisiin hyödyntää (Krzysztof 2014, 16-18 & Dunn Cavelty 2018).

| Taulukko 2: Neljä kybervallan valtatyyppiä | | |
|---|---|---|
| Valtatyyppi | Määritelmä | Esimerkkejä |
| **Pakottava** (suoramaista, vuorovaikutuksessa tiettyjen toimijoiden kanssa) | Toimija käyttää pakottavaa valtaa kyberavaruudessa yrittäessä muuttaa toisen toimijan käyttäytymistä | Anonyymit hyökkäykset (esim. HBGary Federal)<br><br>Ei-aineellisten (symbolisten) resurssien hyödyntäminen, mitkä voivat vaikuttaa suoraan muiden toimintaan (esim. rangaistusuhat) |
| **Institutionaalinen** (diffuusiivinen, vuorovaikutuksessa tiettyjen toimijoiden kanssa) | Kyberavaruuden hallinta, pääasiassa virallisten ja epävirallisten instituutioiden välityksellä | Yhdysvaltojen pyrkimyksenä pitää hallussaan ICANN<br><br>Yhdysvaltojen pehmeämmät muodot ”kyberpelotteen” luomiseksi |
| **Strukturaalinen** (suoramaista, sosiaalisten suhteiden muodostuminen) | Liittyy siihen, kuinka kyberavaruuden (rakenne) voi helpottaa tai rajoittaa kahden toimijan välistä suoraa yhteyttä | Yrityksenä luoda kulttuurisia muutoksia (esim. kuinka Information Assurance sovelletaan)<br><br>Arabikevät ja ihmisten mobilisoiminen sosiaalisen median avulla |
| **Produktiivinen** (diffuusiivinen, sosiaalisten suhteiden muodostuminen) | Sosiaalisten subjektien muodostaminen kyberavaruuden diskursseissa, jotka määrittelevät ”mahdollisuuksien kentät”. Mahdollisuuksien kentät myös rajoittavat ja helpottavat sosiaalista kanssakäymistä | Julkinen diplomaattinen ja strateginen kommunikaatio<br><br>Uhkakuvien rakentuminen<br><br>Olemassa olevien ja syntyvien narratiivien levittämistä sekä edistämistä |

Lähde: Dunn-Cavelty (2018, 309)

Kahta edellä esitettyä kybervallan käsitettä yhdistää se, että ne näkevät kybervallan voimapolitiikan mukaisesti. Kumpikaan teorioista eivät tarkastele valtaa konstitutiivisena. Klimburgn integroituneessa toimintamallissa (taulukko 3) kybervalta nähdään hajautetun vallan perspektiivistä, jossa erilaiset yksilöt ja organisaatiot elävät tiiviissä suhteessa toisiinsa nähden. Kybervalta ei ole silloin kenenkään hallinnoimaa pääomaa. Lyhyesti ilmaistuna integroitunut toimintamalli korostaa sisäänpäin suuntautunutta pehmeää valtaa (an inward-focused soft-power approach). (Dunn-Cavelty 2018, 309.) Kilmburgn (2011, 171-73) mukaan onnistuneessa kyberpuolustuksessa kansallisvaltion pitää pystyä motivoimaan ja vetämään puoleensa muita toimijoita ja organisaatiota. Kyberpuolustuksessa kansallisvaltiot ovat riippuvaisia yksityisistä toimijoista, jotka tarjoavat kyberavaruuden. Kansalaisyhteiskunnan toimijat puolestaan määrittelevät ja ohjelmoivat kyberpiirin (esim. ohjelmistojen protokollat). (Klimburg 2011, 173 & 175.) Integroitunut toimintamalli pyrkii yhdistämään kansallisvaltion turvallisuusintressejä ja hahmottelemaan siten tehokasta kyberpuolustusmallia (Dunn-Cavelty 2018, 309). Kansallisvaltion onkin käytettävä niitä keinoja, joilla saa muut kyberpiirin toimijat yhteistyöhön kanssaan (Klimburg 2011, 175). Klimburg (2011, 175) näkee, valtioilla olevan kolme erilaista tapaa saada toimijat yhteistyöhön ja nämä ovat pakottaminen, tarjoamalla yhteistyövaihtoehtoja tai vakuuttamalla toimijat yhteistyön kannalle. Liberaalidemokratiat eivät voi pakottaa tai lahjoa,

Kiinan ja Venäjän tavoin (ks. Klimburg 2011, 175), saadakseen kansalaisyhteiskunnan ja yritykset toimimaan haluamallaan tavalla. Liberaalidemokratioille ei jää juuri muita vaihtoehtoja, kuin yrittää saada muut toimijat vakuuttuneiksi kansallisvaltioiden uhkakuvien relevanttisuudesta, jotta ne alkaisivat tukemaan valtioiden turvallisuusintressejä. (Klimburg 2011, 175-76.)

Taulukko 3: Integroitu toimintamalli

| Valtatyyppi | Määritelmä | Esimerkkejä |
|---|---|---|
| **Integroitu hallitusvalmius** | Hallituksella kyky toteuttaa yhteisiä toimia, erityisesti kyky hyökätä ja puolustaa kyberavaruudessa, laatia poliittisia kantoja ja jakaa operatiivisia resursseja | USA:n kybertapauksien torjuntasuunnitelman (NCIRP)<br><br>Yhdysvaltain kansallinen kyberturvallisuus- ja viestintäintegraatiokeskus (NCCIC) |
| **Integroitu systeemi kyvykkyys** | Valtion kyky toimia kansainvälisten liittojen ja kumppanuuksien kautta | Kansainväliset liitot ja kumppanuudet, kuten Nato tai YK<br><br>Valtiosta riippumattomat horisontaaliset kumppanuudet, kuten FIRST<br><br>Hybridiorganisaatiot, kuten ICANN<br><br>Kybersuhteiden toimisto ulkoministeriöissä |
| **Integroitu kansallinen kyvykkyys** | Valtion kyky käyttää yksityisen ja kolmannen sektorin toimijoita politiikan välittömässä tukemisessa (liberaalien demokratioiden osalta: yhteistyön kautta ennemmin kuin pakottamalla/vaihtoehtoja tarjoamalla | Julkisen ja yksityisen sektorin kumppanuusohjelmat<br><br>Kansalaisyhteiskunnan hyödyntäminen valvonnassa ja opettaa yksilöt oikeanlaiseen verkkokäyttäytymiseen (Klimburg 2011, 176). *Tämänkaltaisesta toiminnasta käytetään myös nimitystä kyberhygienia toisinaan (Ks. Dunn-Cavelty 2013, 115)* |

Lähde: Dunn-Cavelty (2018, 310)

Kandidaatintutkielmassa lähestytäänkin kybervaltaa Klimburgn (2011) integroituneen toimintamallin mukaisesti, jossa koko poliittinen järjestelmä tekee yhteistyötä uskottavan kybervallan savuttamiseksi. Käsitys korostaa kybervallan ja kyberturvallisuuden olevankin tiivisti kytkeytyneitä toisiinsa (Dunn-Cavelty 2018, 309). Esimerkiksi Dunn-Cavelty (2018) on tutkinut EU:n kybervaltaa kaikkien kolmen yllä esiteltyjen mallien näkökulmasta. Hänen (2018, 315) mielestä paras tapa kuvata unionin kybervaltaa onkin tarkastella sitä integroituneen toimintamallin kautta (Taulukko 4).

| Taulukko 4 EU:n kybervalta integroituneen toimintamallin mukaisesti | | |
|---|---|---|
| Valtatyyppi | Määritelmä | esimerkki |
| **Integroitu hallitus-valmius** | Kyky toteuttaa yhteisiä toimia, erityisesti kyky hyökätä ja puolustaa kyberavaruudessa, laatia poliittisia kantoja ja jakaa operatiivisia resurs-seja | ENISA<br><br>EC3<br><br>Kyberpuolustuksen kehittäminen |
| **Integroitu systeemi kyvykkyys** | Kyky toimia kansainvälisten liittojen ja kump-panuuksien kautta | EU:n kyberdiplomatia<br><br>Bilateraaliset sopimukset (esim. USA tai Kiina)<br><br>EU:n yhteistyö NATO:n kanssa (ja muiden organisaatioiden) |
| **Integroitu kansalli-nen kyvykkyys** | Käyttää ei-valtiollisia toimijoiden tarjoamia kyberelementtejä politiikan tukemiseksi | Eurooppalainen Julkinen-Yksityi-nen-Kumppanuus Resilienssin pa-rantamiseksi (EP3R)<br><br>R&D Horizon 2020 -tutkimusoh-jelma |

Lähde: Dunn-Cavelty, (2018, 315)

Kaikkia yllä esiteltyjä käsityksiä kybervallasta yhdistää se, että ne tarkastelevat valtaa positivistisella tavalla. Nyen tapa mieltää kybervalta noudattaa realismia, kun taas Betzn ja Stevensn sekä Klimburgn hahmotustavat kybervallasta edustavat liberalismin variaatioita (Dunn-Cavelty 2018, 310). Realismin ja liberalismin tavat ymmärtää kyberavaruutta on nähdä se ympäristönä, joka kumoaa kansainvälisen politiikan valtasuhteita ja tuottaa uudenlaisen tavan hallita valtaa. Muutkin toimijat, kuten yksilöt ja pienemmät valtiot (ks Nye 2010, 10) voivat silloin haastaa suurempiaan. Kyberturvallisuus muokkaakin kansainvälisen politiikan anarkian luonnetta perustavanlaatuisesti. EU:n kyberturvallisuuspolitiikan kohdalla perinteinen tarkastelutapa kybervallasta ei ole sopivaa, koska EU:n poliittinen järjestelmä on sekä valtioiden välistä että ylikansallista päätöksentekoa riippuen politiikka-alasta (Hix et al. 2011 17-19). Esimerkiksi EU:n turvallisuuspolitiikka perustuu toiselle ja kolmannelle peruspilarille, jossa päätökset perustuvat hallitustenväliseen yhteistyöhön eikä ylikansalliseen päätöksentekoon (Hix et. al 2011 11). Euroopan unionin toisella pilarilla tarkoitetaan EU:n yhteistä ulko- ja turvallisuuspolitiikkaa. Kolmas pilari liitetäänkin poliisityöhön ja oikeudelliseen yhteistyöhön rikosasioissa eli sisäpolitiikkaan. (Maastricht 1992.) Kyberturvallisuus liitetään EU:n sisäpolitiikkaan vahvasti, vaikka sen hallinnoimiseksi korostetaan ulko- ja turvallisuuspolitiikan merkitystä (Strategia 2013 & Resilienssi 2017). EU ei toisin sanoen voi pakottaa jäsenvaltioita edistämään ylikansallisia kyberturvallisuuskäytäntöjä ilman jäsenvaltioiden suostumusta kybervaltansa kehittämiseksi. EU:n kybervaltaa tulisikin lähestyä konstitutiivisena, jossa valta operoi

laaja-alaisesti. Euroopan unioni pyrkiikin turvallistamaan kyberympäristöä esimerkiksi uhkana, joka voi aiheuttaa hallitsemattomana taloudellisia haittoja koko Euroopalle (Strategia 2013, 2-3).

Perinteisemmät tavat tarkastella kybervaltaa ovat soveltuvaisempia kansallisvaltioille kuin ylikansallisille organisaatioille. Esimerkiksi EU:n päätöksentekoa koskevissa teorioissa painotetaan usein päämies-agentti-ongelmaa (Principal–agent problem). Dilemma syntyy silloin kun yksi toimijoista (agentti) on kykeneväinen tekemään päätöksiä, toteuttamaan toimintoja toisen agentin puolesta tai toimijan päätöksellä on vaikutuksia muihin osapuoliin (päämieheen). (Hix et.al. 2011, 24.) Päämies-agentti-ongelma korostaa, agenttien olevan motivoituneita toimimaan omien intressiensä mukaan, mitkä voivat olla päämiehen intressien vastaisia. Euroopan unionissa päämies-agentti-ongelma korostuu erityisesti, koska aloiteoikeus on delegoitu Komissiolle, joka pyrkii oletetusti edistämään itselleen mieluisia politiikkaetuja. Kun aloite tulee valtioiden ja (mahdollisesti Euroopan parlamentin käsiteltäväksi), niin ne pyrkivät muokkaamaan alkuperäistä ehdotusta itselleen sopivaksi, jolloin komission idea saattaa muuttua alkuperäisestä ehdotuksesta. (Hix et. al. 2012 23-27.) Ylikansallinen päätöksenteko ja laajempi mandaatti toimia Euroopan unionin kyberturvallisuuden edistämiseksi tekisi unionista paremman kybervallan käyttäjän, mutta tämä ei ole välttämättä mahdollista juuri EU:n toisen ja kolmannessa pilarissa sovellettavien päätöksentekomenetelmien vuoksi. EU:n kybervallan ymmärtämiseksi tulee tutkia diskurssia, jolla unioni lisää vaikutusvaltaansa kybervallan kasvattamiseksi. Euroopan unionilla on kybervaltaa, mutta se ei varsinaisesti pelkisty mihinkään aiemmin esiteltyihin tapoihin ymmärtää sitä. Kaikki kybervallan konseptit onnistuvat kuvailemaan EU:n kybervallan olemusta, mutta vain siten että kybervalta on joko läsnä tai poissa derridalaisessa mielessä. Ne eivät kerro mitään EU:n kybervallan vaikutusvallasta. Seuraavassa luvussa dekonstruktioidaan Euroopan unionin kybervalta, joka mahdollistaa valtaidentiteetin ymmärtämisen laaja-alaisemmin. Kandidaatintutkielmassa ei yritetä tarjota vaihtoehtoista kybervaltakäsitystä, vaan ideana on pyrkiä täydentämään integroitunutta toimintamallia dekonstruktion hengessä. Dekonstruktiivinen lähestymistapa huomio EU:n poliittisen järjestelmän integraation, jossa toimijat määrittelevät unionin roolia kyberturvallisuudessa.

# 4. Diskurssianalyysi kybervallan rakentumisesta – EU:n kybervalta

## 4.1. Dekonstruktiivisen diskurssianalyysin ja aineistolukutavan esittely

Dekonstruktiivisella lukutavalla voidaan konstruktoida Euroopan unionin kybervalta, hyödyntäen Kööpenhaminan koulukunnan käsityksiä turvallisuusdiskursseista. Kybervaltaa

lähestytään integroituneen toimintamallin näkökulmasta, joka painottaa usean eri toimijan välistä yhteistyötä tehokkaan kyberpuolustuksen saamiseksi. Ideana onkin ymmärtää, miten Euroopan unioni pyrkii rakentamaan itselleen tehokasta kyberpuolustusta eli kasvattamaan kybervaltaansa kyberfyysisen toimintaympäristön hallitsemiseksi. Edellisen kaltainen näkökulma pyrkii täydentämään integroituneeseen toimintamalliin liitettyjä yhteistyökaluja, tarjoten erilaisen tavan selittää kybervallan muodostumista. Valta ei ole silloin vain läsnä tai poissa, vaan muodostuu toimijoiden välillä. Kööpenhaminan koulukunnan käsitykset turvallisuusdiskursseista mukailevat vahvasti Derridan dekonstruktion lähestymistapaa, jossa asiat saavat merkityksensä yhtäläisyyksien ja eroavaisuuksien kautta, mutta samalla erilaisten konseptien välillä ilmenee hierarkia. Derridalainen diskurssianalyysi perustuukin diskurssin rakentumisen tarkasteluun erottelun ja yhdistelemisen prosesseissa, jotka määrittelevät toimijoiden identiteettejä. Derridalaisen diskurssianalyysin etuna on myös se, että se näkeekin identiteetin rakentuvan käytäntöjen kautta esimerkiksi politiikanteossa. Politiikkadiskurssit eivät vain kuvaile objekteja ja subjekteja, vaan määrittelevät tarvittavia toimenpiteitä asioiden hallitsemiseksi. Poliittisen diskurssin avulla muodostetaan hyväksytynlaista todellisuutta. Identiteetit siis artikuloidaan politiikan perusteeksi, mutta identiteettiä luodaan ja uusinnetaan samalla diskurssissa. Identiteetti on samanaikaisesti diskurssin perusta ja tuote, jolloin muutokset vallitsevassa diskurssissa voivat johtaa myös toimijoiden identiteetin uudenlaiseen muodostumiseen ja käyttäytymiseen. (Hansen 2006, 19; Wæver 2009, 174.)

Turvallistamisen prosessi on jo itsesään omanlaista diskurssianalyysiä, koska diskurssin analyysi kohdistuu puheaktien tarkastelemiseen turvallistamisen ja epäturvallistamisen väliselle (desecuritization) binääriselle akselille. Epäturvallistamisen prosessi noudatteleekin dekonstruktion logiikkaa, jossa uhkakuvan välille muodostuu binäärinen jaottelu ystävän ja vihollisen välillä. (Hansen 2012, 530.) Turvallisuuslausumat myös tarvitsevat epäturvallisuuslausumia täydentämään puheaktia, koska muutoin lausumat jäisivät vain kuvailun tasolle (Hansen 2012,530-1). Turvallisuuslausumia voitaisiin verrata sanakirjoihin, jotka pitävät sisällään määritteleviä täydennyslauseita, koska muutoin sanakirjan funktio ei toteudu oikealla tavalla. Kolmanneksi turvallisuuslausumat eivät sisällä vain *minuuden* ja *toiseuden* määrittelyä, vaan kuvailee myös *mitä* objektit itsessään ovat, luoden samalla olettamuksia miten toiseutta tulisi lähestyä. (Hansen 2012, 533.)

Tutkimuksessa noudatetaankin Lynn Dotyn (1993, 306) soveltamaa dekonstruktiivista diskurssilukutapaa, joka erottelee lausahduksia *olettamuksien* (*presupposition*), *predikoinnoin (predication)* ja *subjektin paikannuksen (subject positioning*) kategorioihin. Kaikenlaiset väittämät sisältävät, jonkun asteisia olettamuksia asioiden luonteesta ja riippuvuussuhteista.

Esimerkiksi kysymyslauseet ovat olettamuksellisia usein luonteeltansa; ”oletko käyttänyt koiran ulkona?”. Kysymyksestä voidaan tehdä oletuksia, että on olemassa koira, joka sinä omistat ja sinun pitäisi viedä se ulos. Toiseksi väittämät rakentavat riippuvuussuhteita asioiden välille predikoinnin keinoin, jossa lauseenjäsenet ilmaisevat asian ominaisuuden, tilan, toiminnon ja luokan. Toteamus; ”Suomi on mahtava maa, jolla on tapana noudattaa kansainvälisiä lakeja ja ihmisoikeuksia”. Toteamus siis kuvailee Suomen subjektiivisuutta, piirteitä ja toiminnan tapoja. Olettamukset ja predikointi luikittelevat siten asioiden olotiloja. Asioiden välille syntyy subjektin ja objektin välinen olotila, jota voidaan kutsua subjektin paikantamiseksi. Subjektin paikantamista määrittelevät muun muassa vastakkaisuus, identiteetti, samankaltaisuus ja toisiaan täydentävät asiat. (Lynn Dotyn 1993, 306.)

Aineistoa luettiin yllä esitettyjen kategorioiden mukaisesti yhdistäen väittämiä yksitellen Dunn-Cavelty & Egloff (2019, 37) tunnistamalle kuudelle erilaiselle valtion roolille kyberympäristössä. Jaottelua mukautettiin kuitenkin EU:n poliittinen järjestelmä huomioiden, esimerkiksi siten, että turvallisuuskumppanina Euroopan unionin päätöksenteko kyberturvallisuudessa olisi vahvasti liittovaltion kaltaista ylikansallista päätöksentekoa. Turvallisuuskumppanina EU:n poliittinen järjestelmä olisi siten hyvin integroitunut. Vastaavasti uhkakuvan ääripäässä Euroopan unionin poliittinen järjestelmä muistuttaisi enemmän konfederaatiomaista valtioidenvälistä yhteistyötä, jossa EU:n poliittinen järjestelmä ei olisikaan kovin integroitunut kybervallan näkökulmasta. Ylikansallisen ja valtioidenvälisen yhteistyön aksiooma syntyi yhtenä tutkimuksen taustaolettamuksista, jotka määrittelivät diskurssien tunnistamista. Tutkimuksen empiirinen aineisto on peräisin kymmenestä eri asiakirjasta, jotka esitellään taulukossa kuusi (liitteet). Taulukon viisi sulkeissa oleva numero ilmaisee, mistä asiakirjasta lausahdus on peräisin. Numeron viereinen roomalainen numero kertoo, jos kanditutkimuksen kirjoittaja on muokannut alkuperäistä lausumaa esimerkiksi lyhentämällä tai kääntämällä tekstiä englannista suomenkielelle. Alkuperäiset lausumat löytyvät kanditutkielman lopusta loppuviitteinä (liitteet). Aineisto rajattiin kymmeneen asiakirjaan, koska EU (Komissio cybersecurity) nostaa itse kyseiset asiakirjat keskeisimmiksi kybertuvallisuudessaan. Kaikista asiakirjoista tehtiin muistiinpanot, pyrkien tiivistämään asiakirjojen diskursiivisia väittämiä. Tiivistykset mahdollistivat aineiston käsittelemisen hallittavalla tavalla, minkä seurauksena samanoloisia väittämiä liitettiin tietyn kybervallan identiteetin piiriin. Identifioidessa olen pyrkinyt tunnistamaan tekstin välisiä sisäisiä jännitteitä, etsimään näiden jännitteiden välille ratkaisuja sekä tunnistamaan erilaisia identifioinnin tapoja perustuen tekstistä syntyneiden olettamuksien mukaisesti. Taulukkoon viisi päätyneet väittämät perustuivat esitettyjen lausumien johdonmukaisuuksien idealle, jotka toistuivat kaikissa asiakirjoissa. Johdonmukaisuudella pyritäänkin osoittamaan niin

sanotusti merkitykseltään hallitsevin diskurssi yllä esitellyn dekonstruktiivisen diskurssianalyysin mukaisesti. Vaikka väittämät eivät esiinny kaikissa asiakirjoissa samankaltaisina identtisinä lausumina, niin lausumia lähestyttiin intertekstuaalisesti. Intertekstuaalinen lähestymistapa olettaa erilaisten tekstien, huolimatta julkaisuajankohdasta, pitävän sisällään sekä eksplisiittisiä että implisiittisiä viittauksia toisiin teksteihin. Intertekstuaalisen lukutavan mukaan tekstit eivät synny tyhjiössä, vaan laajentavat merkityksellisyyksien verkostoa, koska erilaiset tekstit viittaavat toisenlaisiin teksteihin (Lynn Dotty 1993, 302). Intertekstuaalisuus on myös havaittavissa EU:n asiakirjoissa, sillä asiakirjoissa viitattiin monesti toisiin asiakirjoihin kuten strategiaan (2013), direktiiviin (2016) tai resilienssiin (2017). Tekstien kerronnallinen jatkuvuus näyttää diskurssin olemassaolon eräänlaisena jatkumona ja, osoittaa diskurssin olevan läsnä kaikkialla toimijoiden kanssakäymisessä (Lynn Dotty 1993, 302). Vaikka väittämät olisivatkin erilaisia eri teksteissä, niin ne voivat välittää samakaltaista ideaa ja tarkoitusperiä. Taulukossa 5 on pyritty havainnollistaan tekstien sidonnaisuuksia nostettujen väittämien perusteella.

Yksinkertaisesti sanottuna taulukossa viisi aineistolle on annettu ääni puhua dekonstruktiivisten ideoiden mukaisesti. Dekonstruktiivisen lukutavan mukaan tekstien lukija ei voi ikinä saavuttaa kirjoittajan alkuperäisiä tarkoitusperiä. Oletuksena onkin analysoijan tietoisuuden syntyneen erilaisessa historiallisissa aikahorisonteissa kuin alkuperäisen asiakirjojen kirjoittajan. Sen seurauksena kandidaatintutkielman kirjoittaja antaa EU:n asiakirjoille merkityksen omien taustaolettamuksien ja tietoisuutensa perustella, jona Euroopan unioni ilmenee hänelle. EU:n asiakirjoista on siis mahdollista muodostaa myöskin erilaisia olettamuksia, jotka eivät mukaile kirjoittajan havaintoja Euroopan unionin kybervallasta. Dekonstruktiivinen lukutapa on samanaikaisesti myöskin hyvin subjektiivinen lukutapa. Dekonstruktiossa ei oleteta löytävän oikeanlaista tai vääränlaista tulkintaa havaitusta asiasta. On olemassa parempia ja huonompia tulkintoja, mutta dekonstruktiossa minkään niistä ei oleteta olevan epätotta. Edellinen seikka kannattaa pitää mielessä, kun tulkitsee taulukkoa viisi alla olevien alalukujen mukaisesti.

Taulukko 5: Euroopan unionin kyberturvallisuuden diskurssin predikaatit ja praktisuudet [i]

*Euroopan unionin kybervalta*

| Ylikansallista | | Yhteistyötaso | | Valtioidenvälistä yhteistyötä | |
|---|---|---|---|---|---|
| **Turvallisuuskumppanina** | **Turvallisuuden takaajana** | **Tukijana ja edustajana** | **Lainsäätäjänä ja sääntelijänä** | **Tiedon luojana ja levittäjänä** | **Uhkana ja vihollisena** |
| *julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden perustamiseen* (6)<br><br>*Rikosten tutkiminen ja syyttäminen säilyy jäsenvaltioiden yhteisenä tavoitteena (8)*[ii]<br><br>*Kolmenvälistä yhteistyötä Euroopan komission, jäsenvaltioiden ja teollisuuden välillä (6)*<br><br>*luodaan yhteydet yritysmaailmaan, korkeakouluihin, tutkimusalaan ja kuluttajiin (6)*<br><br>*EU:n laajuinen kriisi, johon liittyy kyberturvallisuustekijöitä, vastatoimia koordinoi unionin poliittisella tasolla neuvosto käyttäen poliittisen kriisitoiminnan integroituja järjestelyjä (IPCR) (4)*<br><br>*edistettävä "kyberhygieniaa" (10)* | *konfliktien ehkäisy, kyberturvallisuusuhkien lieventäminen (8)*[iii]<br><br>*EU muistuttaa sen ja sen jäsenvaltioiden pyrkimyksiä parantaa kyberresilenssiä (8)*[iv]<br><br>*unionista olisi tehtävä "kyberturvallisuusalan maailmanlaajuinen johtaja vuoteen 2025 mennessä (6)*<br><br>*EU:n ulkopuolisista maista peräisin olevat yritykset, jotka ovat jo pitkään toimineet Euroopan maaperällä ..., voisivat olla EU:n hankkeiden kannalta erittäin hyödyllisiä (6)*[v]<br><br>*Kyberturvallisuuspoikkeama voi laukaista laajemman kriisin (4)*<br><br>*Perusoikeuksia, demokratiaa ja* | *EU: n lähestymistapa kyberdiplomatiaan (8)*[ix]<br><br>*kansainvälistä yhteistyötä kyberturvallisuusstandardien parantamiseksi (10)*<br><br>*kansainvälisten kumppanien ja kansainvälisten organisaatioiden, kuten Euroopan neuvosto, OECD, ETYJ, NATO ja YK, kanssa (1)*<br><br>*ylläpitää toimivia yhteyksiä teollisuuteen ja julkiseen sektoriin (6)*<br><br>*Kriisit voivat vaikuttaa taloudellisen toiminnan kaikkiin sektoreihin sisämarkkinoilla, kuten myös unionin turvallisuuteen ja kansainvälisiin suhteisiin sekä toimielimiin itseensä (4)*<br><br>*ylikansallisen luonteen vuoksi näiden järjestelmien merkittävät häiriöt ... voivat vaikuttaa yksittäisiin jäsenvaltioihin ja koko unioniin (3).*[x] | *Erityisesti toimeenpanemalla NIS-direktiivi (9)*<br><br>*Jäsenvaltioilla on vähimmäisvalmiudet ja strategia, joilla varmistetaan korkeatasoinen verkko- ja tietojärjestelmien turvallisuus niiden alueella (3)*<br><br>*keskeisten palvelujen tarjoajalla' julkista tai yksityistä toimijaa… (energia, liikenne, pankkiala, finanssimarkkinoiden ja digitaalinen infrastruktuuri, terveydenhuolto ja juomaveden jakelu) säädetyt kriteerit (3)*[xii]<br><br>*Budapestin sopimus ... kolmannetkin maat ...sitoutua…mallina…verkkorikoslainsäädännölle (1)*[xiii]<br><br>*Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ....eurooppalaisiin tai kansainvälisiin standardeihin perustuvia, paitsi jos kyseiset standardit ovat tehottomia tai epäasianmukaisia unionin* | *osaamiskeskus kykenee edistämään huipputason yleissivistävää ja ammatillista koulutusta (6)*<br><br>*uhkaympäristö ja hiljattaiset kyberturvallisuuspoikkeamat ovat osoitus siitä, että unionia uhkaava riski on kasvussa (4)*<br><br>*Nykyiset valmiudet eivät riitä varmistamaan korkeatasoista verkko- ja tietojärjestelmien turvallisuutta unionissa (3)*<br><br>*ENISA on tästä syystä järjestänyt vuodesta 2010 alkaen säännöllisiä yhteiseurooppalaisia kyberturvallisuusharjoituksia (4)*<br><br>*Yliopistoilla ja tutkimuskeskuksilla on ratkaiseva rooli tutkimuksen, kehityksen ja innovoinnin vauhdittamisessa (3)*<br><br>*ENISAn olisi avustettava jäsenvaltioita ja komissiota tarjoamalla asiantuntemusta ja neuvontaa (3)* | *Keskellä täysimittaista kybersodankäyntiä (6)*<br><br>*Kyberkonsultaatio ... aloitettu USA:n, Kiinan, Japanin, Intian, Etelä-Korean ja Brasilian kanssa (9)*[xviii]<br><br>*Terrorismin vastainen taistelu (9)*[xix]<br><br>*Autoritaaristen hallintojen valvontaan tai sensuuriin (9)*[xx]<br><br>*Kyberkapasiteetin kehittämisen merkitys kolmansissa maissa (8)*[xxi].<br><br>*EU on huolestunut valtiollisten ja valtiosta riippumattomien toimijoiden lisääntyneestä kyvystä ja halusta pyrkiä tavoitteisiinsa (8)*[xxii]<br><br>*EU on kyberturvallisuustuotteiden ja -ratkaisujen nettotuoja, mikä on ongelmallista taloudellisen kilpailukyvyn sekä siviili- ja sotilaallisen turvallisuuden kannalta (6)* |

| | | | | | |
|---|---|---|---|---|---|
| *EU, jäsenvaltiot, teollisuus ja yksityishenkilöt – antamaan kyberturvallisuudelle etusija (2).*<br><br>*Sisämarkkinoiden asianmukaisen toiminnan varmistamiseksi, pyrkien samalla saavuttamaan kyberturvallisuuden, kyberresilienssin ja luottamuksen korkean tason unionissa, tässä asetuksessa (10)* | *oikeusvaltioperiaatetta on suojeltava myös kyberavaruudessa (1)*<br><br>*EU:n ulkopuolisissa maissa hallitukset voivat myös väärinkäyttää verkkoa omien kansalaistensa tarkkailuun ja valvontaan (1)*<br><br>*Uhkien motiivi … rikollisen voiton tavoittelu … myös poliittisia ja strategisia (2)*[vi]<br><br>*uhkatoimijat, erityisesti EU: n ulkopuoliset valtiot tai valtion tukemat toimijat (7)*[vii]<br><br>*2019 ovat ensimmäiset Euroopan parlamentin vaalit muuttuneessa turvallisuusympäristössä (5)*[viii] | *välttämätön väline demokratian säilyttämisen kannalta (6)*<br><br>*Vastuu verkko- ja tietojärjestelmien turvallisuuden varmistamisesta lankeaa suurelta osin keskeisten palvelujen tarjoajille ja digitaalisen palvelun tarjoajille (3)*<br><br>*EU:n ydinarvot pätevät yhtä hyvin digitaalisessa kuin fyysisessäkin maailmassa (1)*<br><br>*Viidennen sukupolven (5G) televerkoilla … on keskeinen rooli… Euroopan yhteiskunnassa ja taloudessa (7)*[xi] | *oikeutettujen tavoitteiden saavuttamiseksi.*[xiv] *(10)*<br><br>*Eurooppalaista kyberturvallisuussertifikaattia olisi pidettävä vahvistuksena siitä, että kyseinen arviointi on tehty asianmukaisesti. (10)*<br><br>*Euroopan unionin perusoikeuskirjan 8 artiklalla, Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklalla ja Euroopan parlamentin ja neuvoston asetuksella (EU) 2016/67913 taataan luonnollisten henkilöiden suojelu suhteessa heidän henkilötietojensa käsittelyyn… (5)*[xv] | *CSIRT-verkostoon osallistuvia … tietoja julkaistavaksi ... vapaaehtoisuuteen perustuen (3)*[xvi]<br><br>*ENISAn on tarpeen analysoida nykyisiä ja kehittymässä olevia kyberturvallisuusriskejä (10)*<br><br>*3 miljardin euron investoinnit kyberturvallisuustekniikkaan seuraavassa EU: n talousarviossa 2021-27 (7)*[xvii] | *Kolmenvälisen yhteistyön tapauksessa on tärkeää kiinnittää huomiota kolmansista maista peräisin oleviin yrityksiin (6)*<br><br>*direktiivi (2016) ei rajoita toimia....kansallisen turvallisuuden… (ja tietojen) suojaamiseksi (3.)*[xxiii]<br><br>*asetus (2019) ei rajoita turvallisuutta, puolustusta, kansallista turvallisuutta tai yksittäisen valtion toimia rikosoikeuden alalla. (10)*[xxiv]<br><br>*Yksityiset yritykset ovat haluamattomia jakamaan tietoja kyberhaavoittuvuuksistaan ja niistä seuraavista tappioistaan, koska … liitetoimintatietoja, vaarantavansa maineensa tai rikkovansa tietosuojasääntöjä (2)*[xxv] |

## 4.2. Mitä kyberturvallisuuden diskurssit pitävät sisällänsä?

Kööpenhaminan koulukunta on määritellyt, mitä tunnusmerkkejä kyberturvallisuuden turvallisuusdiskursseilla on. Ensimmäiseksi kyberturvallisuuden diskurssit sisältävät hyperturvallistamista (*hypersecurization)*, joka liioitelee uhkien luonnetta ja, niihin tarvittavia vastatoiminpiteitä. Hyperturvallistamisessa korostuu uhkien nopeus ja keskinäisvaikutus, sillä verkossa tapahtuva toiminta nopeuttaa aika- ja tilakäsityksiä. Toiseksi kyberturvallisuusdiskursseissa ilmenee arkipäiväisiä turvallisuusuhkia ennemmin kuin pahemmat turvavallisuusskenaariot, missä esimerkiksi voimalaitoksen sammuminen johtaa koko yhteiskunnan pimenemiseen. Yleensä kyberturvallisuuden vaaroja kuvataan arjessa yksilöille tapahtuvaksi, kuten identiteetti- tai verkkopankkivarkauksina. Toisaalta kyberturvallisuuden diskursseissa painottuu uhkakuvien kaksiluonteisuus, koska uhat sijaitsevat aineettomassa verkossa, mutta niiden vaikutukset heijastuvat aineelliseen maailmaan. Kolmanneksi kyberdiskurssit ovat erittäin teknillispainotteisia. Lähtökohtaisesti kyberdiskursseista puhuminen suosii teknillistä asiantuntijuutta, mikä vaikuttaa siihen, kuka saa määritellä, mitä uhkakuvia kyberturvallisuuden tulisi pitää sisällään. (Hansen& Nissenbaum 2009, 1163-69.)

Kyberturvallisuuden uhkakuvien esittäminen rajoittaakin sitä, kuka saa osallistua kyberturvallisuusdiskurssin määrittelemiseen. EU:n kohdalla ENISA on keskeinen toimia kyberturvallisuuden määrittelemiseksi. Kyberturvallisuuden uhkakuvat mukailevat luonnontietieteitä, yhdistäen ne samalla tietotekniikan piiriin. Esimerkiksi uhkakuvia ovat muun muassa madot ja tietokonevirukset, mitkä olivat alkujaan peräisin populäärikirjallisuudesta. Myöhemmin ne ovat levinneet armeijan niin virallisiin strategioihin kuin tieteeseenkin (Dunn-Cavelty 2013, 110-1.) Uhkakuvia yritetään ratkaista luonnontieteistä ja terveydestä johdetuilla sanoilla. Diskurssissa puhutaankin kyberhygieniasta, kyberresilienssistä ja järjestelmän immuunisuojasta. kyberturvallisuusdiskurssien uhkakuva esitetäänkin usein digitaalisina onnettomuuksina. Kyber-etuliite kuvastaa vaarojen tapahtuvan tietokoneen välityksellä. Kyberturvallisuus sanaan liittyy mystisiä piirteitä muun muassa hakkereiden takia ja heidän kyvykkyydestään aiheuttaa vahinkoa toisille niin halutessaan. Hakkerit ovat muuttuneet tavallisista nuorista poikateineistä rikollistoimijoiksi, jotka voidaan liittää pahimmillaan terroristiseen toimintaan. (Dunn-Cavelty 2013, 112.) Kuten jo aiemmin ylempänä mainittua, niin kybertekijöiden identiteettiä on vaikea hahmottaa kyberavaruudessa, mikä lisää hakkereihin liittyvää mystiikkaa pahoina toimijoina. Kyberturvallisuutta yritetään hallita kuten mitä tahansa sodankäynnin osa-aluetta, missä kuitenkin koko yhteiskunnallinen systeemi (yleinen termi on puhua ”ekosysteemistä”) on vaarassa. Systeemivaarojen vakavuutta saatetaan lisätä, kuvaamalla niitä ”kriittisinä”, sillä niiden toimimattomuus saattaa aiheuttaa yhteiskunnalle merkittäviä haittoja. Teknologiaa ei voi siis

erottaa diskurssista, vaan ovat osa yksilöiden subjektiivisuutta ja yhteiskunnan arkea. Informaatiorakenteiden vaarat ovat samanaikaisesti siten uhka koko modernille elämälle. Lisäksi informaatiorakenteiden uhkakuvien tapahtumaketjut esiintyvät ryöppyävinä ja yhtäkkisinä, mikä voi uhata laajojakin maantieteellisiä alueita. Kolmas mielenkiintoinen seikka kuvastaa kyberuhkien sisältä-ulospäin suuntautuneisuutta, eikä niinkään ulkoa-sisäänpäin tulevaa vaaraa, kuten perinteiset vaarat (terrorismi, sota ja yms.) saattavat aiheuttaa yhteiskunnalle. (Dunn-Cavelty 2013, 114-5.)

### 4.3. Tutkimusaineiston esittely: EU:n keskeisimmät asiakirjat kyberturvallisuuspolitiikassa

Taulukossa kuusi (liitteet) esitellään koostetusti Euroopan unionin keskeisimmät asiakirjat (ns. cybersecurity package) tehokkaan kyberpuolustuksen järjestämiseksi. Olennaista Euroopan unionin kyberturvallisuuspaketissa on turvata tietoverkossa tapahtuvan talouden sujuvuus sekä vaurauden lisääntyminen koko unionin alueella. Euroopan unionin kyberturvallisuuden keskiössä on edistää kyberresilenssiä. (Komissio cybersecurity 2020.) Kyberresilienssillä tarkoitetaan järjestelmän toipumista iskusta, joko palautumalla kokonaan alkuperäiseen tilaansa tai toisenlaiseen kontrolloituun vaiheeseen. Resilienssistä on tullut kyberturvallisuuden saralla keino hallita kompleksisia ja ennustamattomia tapahtumaketjuja. Resilienssissä hallinta perustuu enemmän itseohjautuvien toimijoiden väliseen yhteistyöhän (governance) kuin hierarkkiseen komentoketjuun. Resilienssiä voitaisiin siten verrata itseparantuvaan immuunijärjestelmään. Euroopan unionin kybervallalla on resilienssin takia hyvin konstitutiivinen luonne toimijoiden välillä. (Dunn-Cavelt 2013, 116.)

Taulukko kuusi kertoo kootusti Euroopan unionin kyberturvallisuuden raamit, joiden avulla unioni yrittää kehittää kybervaltaansa. Tutkimuksessa olisi voinut keskittyä tiettyyn osa-alueeseen esimerkiksi siihen, kuinka Euroopan unioni torjuu kyberrikollisuutta, varmistaa tieto- ja informaatioverkkojen turvallisuuden tai ylläpitää tarvittavaa kyberpuolustusta (ks. Christou 2019, 281). Edellisellä jaottelulla painotetaan muun muassa erilaisten toimijoiden roolia, mahdollisia uhkaavia tekijöitä sekä, millä tavoin niihin tulisi reagoida. Esimerkiksi kyberrikollisten motiivina kyberhyökkäyksillä on saavuttaa taloudellisia hyötyjä, kun taas valtiollisilla toimijoilla kyberpuolustuksessa ohjaavat todennäköisesti poliittiset ja strategiset motiivit. Voisi myös varovaisesti olettaa, kolmella osa-alueella diskursiivisten käytäntöjen ja uhkakuvien olevan myös vaihtelevia alasta riippuen. Kandidaatintutkielmassa ollaan kiinnostuneita EU:n kybervallasta kokonaisvaltaisena ilmiönä ja, siten unionin pyrkimyksestä kehittää

omaa kybertoimijuuttansa. EU:n kybertoimijuus on vaihtelevaa, riippuen kybertuvallisuuden osa-alueesta.

Muun muassa sisämarkkinoiden suojelemiseksi Euroopan unioni on onnistunut tekemään kyberturvallisuutta koskevaa lainsäädäntöä (Direktiivi 2016 & Asetus 2019), mutta kybersotilaallisen puolustuksen kohdalla unioni etsii vasta suuntaviivojansa. Euroopan unionin toiminta on ollut kyberturvallisuuden saralla enemmän reagoivaa kuin proaktiivista vielä toistaiseksi, vaikka unionin valmiudet vastata kyberturvallisuusuhkiin ovat kasvaneet. Muun muassa NATO muutti turvatakuunsa kattamaan myös kyberavaruudessa tapahtuvat hyökkäykset, pian Viroon vuonna 2007 kohdistuneen kyberhyökkäyksen jälkeen (Hansen & Nissenbaum 1168-71, 2009), kun taas unioni julkaisi varsinaisen kyberstrategiansa vasta vuonna 2013 ja vielä toistaiseksi EU ei ole julkaissut merkittäviä politiikkasuuntaviivoja sotilaskyberpuolustuksen saralla (Cristou 2019, 281).

Perinteisesti EU:ta koskevassa turvallisuus- ja ulkopolitiikassa jäsenvaltiot ovat olleet halukkaita kehittämään enemmän instituutioita, kuin varsinaisia kapasiteetteja itse päätösten varsinaiseen toteuttamiseen (Hix & Høyland 2011, 330). Esimerkiksi Euroopan unionilla on kahdeksan ongelmaa, jotka vaikeuttavat yhteisen kyberpuolustuspolitiikan muodostumista. Ensimmäinen koskee jäsenvaltioiden suvereniteettia ja EU:n ylikansallisten instituutioiden välistä toimintavastuita. Toinen vaikeus liittyy puolestaan ylikansallisten toimijoiden väliseen toimintaa. Kolmantena EU pitää ongelmana kyberavaruuden toimintaympäristöä ja siihen sovellettavaa aseellisiin konflikteihin liittyvää olemassa olevaa lainsäädäntöä. Neljäs haaste liittyy hybriditeknologiaa, kuten droneiden käyttöön konflikteissa. Viides vaikeus koskee kyberturvallisuuden määritelmättömyyttä, eli sitä mitä pidetään kybersodankäyntinä. Kuudenneksi monien toimijoiden sisällyttäminen yhteiseen kyberpuolustukseen tuo omat haasteensa. Seitsemänneksi sotilaallinen ja siviilinen toiminta kietoutuvat yhteen kyberpuolustuksessa vahvasti. Kahdeksanneksi EU:n toimintaa rajoittaa saatavilla olevan tiedon määrä, sillä EU:n lainsäädäntö (esim. NIS-direktiivi 2016/(8)) ei velvoita jäsenvaltioita luovuttamaan tilannetietoa, jos se on niiden kansallisen turvallisuuden vastaista. (CSDP 2017, 7.) Juuri unionin kyberturvallisuuspolitiikan pirstaloisuuden takia ja erilaisten integraatiovaiheiden vuoksi, kandidaatintutkimuksessa keskitytäänkin havaitsemaan yleisiä suuntaviivoja, kuinka unioni näkee kybertoimijuutensa. Toisin sanoen tutkimuksessa tarkastellaan relevantilla tavalla Euroopan unionin kybervallan rakentumista ja identifioitumista, eli pyrkimystä saavuttaa haluamiansa tavoitteita niin kyberavaruudessa kuin sen ulkopuolellakin kyberfyysisessä toimintaympäristössä.

## 4.4. EU:n kyberturvallisuuden dekonstruktio

### 4.4.1. Predikointi

Taulukossa viisi on esitelty Euroopan unionin kyberturvallisuuspolitiikan predikaatiot ja käytännöt. Toteamukset on johdettu tutkimalla lausahdusten piirteitä, adverbeja, taipumuksia, mitkä ovat vaikuttaneet kybervallan subjektimuotoihin. Taulukko viisi ei esitä diskurssiin osallistuneiden subjektiivisia kognitioita, vaan oletuksena on diskurssin itsessään muokkaavan subjektin käsityksiä ympäröivästä maailmastaan (Lynn Doty 1993, 310). Taulukkoa viisi tutkittaessa on hyvä pitää myös mielessä, vallitsevan diskurssin edustavan vain *Euroopan unionin* diskurssia. Diskurssi ei kerro mitään toisenlaisista ja kilpailevista vastadiskursseista, joita voisivat olla muun muassa yritysmaailman, yksittäisten jäsenvaltioiden, tiedemaailman tai kolmansien maiden diskurssit. Vaikka eri predikaation ja käytännön muodot eivät ole identtisiä, voidaan niiden välillä löytää yhtäläisyyksiä. Esimerkiksi Euroopan unionin kybervalta uhkana ja vihollisena esittää kaikkein selkeimmin, kuinka EU:n kohtaamat kyberuhat tulevat unionin ulkopuolisista maista. Myöskään jäsenvaltiot eivät välttämättä luota unionin kybervaltaan kansallisen turvallisuuden vuoksi. Yritysmaailmakin voi nähdä unionin kybervallan aiheuttavan yrityksille taloudellisia tappioita, jos ne luovuttavat EU:lle tietojansa. Euroopan unioni toteaakin; ” *Kolmenvälisen yhteistyön tapauksessa on tärkeää kiinnittää huomiota kolmansista maista peräisin oleviin yrityksiin”,* mutta vain jos*;” EU:n ulkopuolisista maista peräisin olevat yritykset, jotka ovat jo pitkään toimineet Euroopan maaperällä… voisivat olla EU:n hankkeiden kannalta erittäin hyödyllisiä”.* Edellisen kaltaisessa tilanteessa kolmansista maista peräisin olevat yritykset ovat eurooppalaistuneet, sisäistäen *eurooppalaisen kybersertifikaatin* ”luotettavuuden vaatimukset”, jolloin ne eivät ole vaaraksi unionille.

Yhtä todennäköisesti kyberhyökkäys voisi tulla Euroopan unionin sisältä, koska kyberhyökkäys voi tulla mistä, milloin ja keneltä tahansa. Euroopan unioni pyrkii turvallistamaan sisämarkkinansa ja määrittele omaa rooliaan sen suojelemiseksi. EU kuvailee, miten kolmannet maat ovat epäluotettavia, kun taas EU:n instituutiot ja jäsenvaltiot ovat luonnollisia yhteistyökumppaneita. Uhkakuva nähdäänkin tulevan unionin ulkopuolelta eikä niinkään jäsenvaltioiden yhteiskuntien sisäpuolelta kuten perinteisesti kyberturvallisuuden diskursseissa korostetaan. Taulukosta viisi huomataan, Euroopan unionin kybervallan muodostuminen noudattaakin turvallistamisen prosessia, kun se pyrkii identifioimaan itseänsä.

### 4.4.2. Olettamus

Taulukkoa viisi analysoidessa voidaankin huomata, merkitykset ovat riippuvaisia binäärisistä vastakkaisuuksista. Juuri erilaisten vastakkaisuuksien prosesseissa syntyy myös EU:n

kybervallan muoto, mihin vaikuttaa ulkopuoliset rajoitteet esimerkiksi lainsäädäntö, päätöksentekomenettely, mielikuvat sekä periaatteet. Lähtökohtaisesti tutkimuksessa oletuksena onkin unionin muokkaavan itselleen mieleistä diskursiivista ympäristöä, eli toisin sanoen muovaamaan sosiaalisten suhteiden rakenteita. Taulukko viisi perustuukin kolmelle olettamukselle, jotka antavat asioille niiden merkityksellisyyden. Alla olevat olettamukset ja havainnot perustuvatkin kirjoittajan valintoihin ja aineistosta syntyneeseen mielikuvaan unionin toimijuudesta kyberturvallisuuspolitiikassa. Toisaalta dekonstruktion etymologia korostaa havaitsijan luovan merkityksiä asioille, jolloin tutkimusfaktat eivät kerro itsessään vielä mitään, vaan niiden merkitys muodostuu eroavaisuuksien johdosta.

*Turvallinen/turvaton*. Ensimmäinen olettamus perustuu turvallisuuden ja turvattomuuden väliselle olotilalle. Kyberavaruus luo toimijoille uudenlaisia liiketoiminnan mahdollisuuksia ja luo unionin sisämarkkinoille uusia vaaroja. EU:n uskoo esineiden internetiin olevan kytkettyinä vuoteen 2020 mennessä kymmeniä miljardeja laitteita, mutta kyberturvallisuutta ei ole vielä asetettu laitteiden suunnittelussa etusijalle (Resilienssi 2017, 2). Lisäksi luomalla toimivat sisämarkkinat unioni voisi kasvattaa Euroopan bruttokansantuotetta lähes 500 miljardilla eurolla vuodessa. Erityisesti 5G-verkot luovat taloudellisia mahdollisuuksia liikenteen, energian, tuotannon, terveyden, maanviljelyn ja median saralla. (Strategia 2013, 2; 5G 2020, 1.) Kyberympäristö tuo mukanaan omat haasteensa, joihin EU:n on pyrittävä varautumaan. Euroopan kyberturvallisuutta koskevissa diskursseissa voidaankin havaita hyperturvallistamisen piirteitä, missä korostuu kyberuhkien arvaamattomuus ja tuntemattomuus. Lisäksi kyberuhat uhkaavat yhteiskunnan heikommassa asemassa olevimpia erityisesti lapsia (Asetus 2019, (3)). Kyberuhkia lähestytäänkin arkisten asioiden avulla, jotka toimivat diskurssissa retorisina tehokeinoina turvallisen ympäristön rakentamiseksi. Kyberturvallisuusdiskurssin pääviittauskohteena on suojata EU:n kriittistä infrastruktuuria. Unionin kyberturvallisuuden diskurssit noudattelevat jonkin verran myös teknillistämistä, mutta pääsääntöisesti diskursseissa kyberympäristö nähdään strategisesta näkökulmasta hallittavana asiana. Kyberympäristöä pyritäänkin turvallistamaan, jossa unioni määrittelee omat intressinsä ja arvonsa suojelemisen arvoiseksi. Turvallistaminen suosiikin sotilaallista asiantuntijuutta, ja siten samalla epäpolitisoi kyberturvallisuuden diskurssia. Pahin uhka unionin diskursseissa ilmenneenikin kybertilannetietoisuuden tiedottomuutena ja, jos EU ei pysy teknologisen kehityksen mukana, niin sisämarkkinoiden toimivuus on vaarassa. Uniolla ei ole siis muuta vaihtoehtoa kuin pyrkiä kehittämään omaa kyberturvallisuuspolitiikkaansa, mistä päästään tutkimuksen toiseen olettamukseen.

*Ylikansallinen yhteistyö/valtioidenvälinen yhteistyö*. Toinen oletus liittyy Euroopan unionin ja jäsenvaltioiden väliseen rooliin kyberpuolustuksen varmistamiseksi. Parhaan

kybervallan savuttamiseksi oletuksena on unionin suosivan ylikansallista yhteistyötä ennemmin kuin valtioidenvälistä yhteistyötä. EU on onnistunut kehittämään omaa kybertoimijuutta, mikä näkyy esimerkiksi ENISA:n roolin merkityksen kasvuna (Asetus 2019) ja Euroopan kattavan CSIRT-verkoston perustamisella (Direktiivi 2016). Vaikka kyberpuolustuksen fyysinen infrastruktuuri on jäsenvaltioilla, niin puolustusta tulisi hallita ja koordinoida enemmän unionin tasolla. Toisaalta unionin kybervaltaa rajoittaa EU:n oma institutionaalinen rakenne, jossa ulko- ja turvallisuuspolitiikka sekä sisäinen turvallisuus perustuvat enemmän valtioiden väliseen yhteistyöhön, jossa komission roolina on toimia koordinoijana jäsenvaltioille. EU:n institutionaalinen rakenne rajoittaa diskurssin kehittymistä, jolloin diskurssitkaan eivät operoi ilman rajoitteita. Muun muassa direktiivissä (2016) ja asetuksessa (2019) valtioiden ei tarvitse luovuttaa tietoja, jotka ovat niiden kansallisen turvallisuuden vastaisi. Komissio painottaa suunnitelmissaan unionille isompaa roolia, yrittäen muuttaa vallitsevaa sosiaalista ympäristöä unionille edullisemmaksi. Osittain kyse on myös identifikaatiosta, jossa EU:n instituutioiden oletetaan omaavan arvoja ja normeja, mitkä erottavat ne osittain kansallisvaltioista. Komissiolla onkin myönteisempi asenne ylikansallista toimijuutta kohtaan kuin jäsenvaltioilla, jotka joutuvat joustamaan suvereeniudessaan ylikansallisen päätöksenteon vuoksi. Identifikaatiosta voidaan johtaakin kolmas olettamus tutkimukselle.

*Jäsenvaltio/ei-jäsenvaltio.* Kolmas olettamus perustui analyysissä siihen, että jäsenvaltioiden ja ei-jäsenvaltioiden välillä on myös hierarkia, jossa jäsenmaiden identiteetti korostuu enemmin kuin unionin ulkopuolisten valtioiden. Kolmas olettamus oli myös vahvin kahdesta yllä esitellystä olettamuksesta ja taulukosta viisi voidaan havaita, miten Euroopan unionin normit ja arvot, esiintyvät kaikissa kuudessa vallan subjektin muodossa jollain tasolla. Euroopan unionin poliittinen järjestelmä ei vain rajoita jäsenvaltioiden politiikkaa, vaan myös sitä miten ne määrittelevät intressejään ja jopa identiteettiään (Risse 2009, 148). Euroopan unionin poliittinen järjestelmä edustaakin kansainvälisen lainsäädännön näkökulmasta uudenlaista oikeusjärjestystä, jonka seurauksena jäsenvaltiot havainnoivat itseään ja toisia eri lailla. EU:n jäsenvaltiot eivät ole vain eurooppalaisia valtioita, vaan jäsenvaltioiden identifioituminen määrittyy Euroopan unionin jäsenyyden kautta (Risse 2009, 148). EU: arvot ja normit vaikuttavatkin diskurssiin ja käyttäytymiseen, jonka alla jäsenvaltiot operoivat. Esimerkiksi unionin perussopimukset muodostavat EU:lle perustuslaillisen aseman, vaikka unionilla ei virallisesti ole olemassa perustuslakia unionin toiminnasta. EU:n kyberdiskursseissakin oikeusvaltion, demokratian ja tasa-arvon periaatteet erottuvat ja kyberympäristö uhkaa edellä lueteltujen arvojen olemassaoloa. EU ei esimerkiksi puhu demokraattisen rauhanteorian mukaisesti demokratioiden hyökkäämättömyydestä, vaan myöntää kybersodankäynnin olevan läsnä, vaikka

kybersodan termiä pidetään jo itsessään ongelmallisena. Kellon (2018, 52) mukaan mikään tähän mennessä paljastuneista kyberhyökkäyksistä ei ole täyttänyt esimerkiksi sodan määritelmiä. Euroopan unioni muodostaa omaa toimijuuttaan kyberavaruuden hallitsemiseksi kokemalla muut ei-jäsenvaltiot uhkaksi omalle olemassaololollensa.

### 4.4.3. Subjektin paikannus: kybervallan identifiointia

*Turvallisuuskumppanina.* Euroopan unionin vahvin kybervallan muoto. Tällöin unionin politiikka kyberturvallisuuden saralla on täysin integroitunut toisiinsa nähden ja Euroopan unioni määrittelee täysin politiikan suuntaviivat. Integroituneen toimintamallin näkökulmasta EU:n kyberpuolustus on verrattavissa kansallisvaltion kyberpuolustukseen. Myös jäsenvaltiot ja yritykset ovat enimmissä määrin valmiita joustamaan omista turvallisuusintresseistään unionin hyväksi, mikä mahdollistaa järjestelmän saumattoman yhteistyön. Taulukossa viisi havaitaan, miten diskursseissa Euroopan unioni yrittää parantaa asemiaan kybervallan kehittämiseksi. Unioni korostaa muun muassa kyberturvallisuuden keittyminen on johtanut uudenlaiseen; ”julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden perustamiseen”. Lisäksi erilaiset koko Euroopan kattavan ”resilienssin” ja ”kyberhygienian” kehittäminen painottavat EU:n kybervallan ilmenevän kumppanuutena eurooppalaisen yhteiskuntaelämän suojelemiseksi. Kumppanuuden roolissa EU:n rooli näyttäytyy yhteiskunnassa julkisen-yksityisen-kumppanuutena (*public-private-partnership*), jossa teollisuus ja jäsenvaltiot vaihtavat informaatiota keskenään, mutta ilman yksityisen sfäärin kriittisen infrastruktuurin kansallistamista ( Dunn-Cavelty & Egloff 2019, 49). Euroopan kattavia uhkia ratkaistaisiin kansalaisyhteiskunnan, jäsenvaltioiden, yksityisen sektorin ja unionin välisellä yhteistyöllä tasa-arvoisesti.

*Turvallisuuden takaajana*. Toisena valtaidentiteettinä Euroopan unionin kybervalta esiintyy turvallisuuden takaajana, jossa unioni on vähemmän integroituneempi kuin mitä turvallisuuskumppanin tilassa. Turvallisuuden takaajana EU:n roolina on turvata kaikin keinoin omat siviili- ja armeijaverkot kyberhyökkäyksiltä (Dunn-Cavelty &Egloff 2019, 49). Euroopan unionin jäsenvaltiot olisivatkin kehittäneet EU:n kykyä reagoida voimakkaammin kyberuhkiin ja tarvittaessa jäsenvaltiot olisivat turvallisuuden nimissä valmiita rajoittamaan kansalaistensa ja yrityksien toimintaan kyberavaruudessa. Unionin kybervalta muistuttaisi vahvasti NATO:n kybervaltaa, joka on määritellyt kyberturvallisuuttaan enemmän sotilaallisesta näkökulmasta, pyrkien suojelemaan jäseniään kollektiivisen turvallisuuden avulla (Krzysztof 2014b, 470). NATO lähestyykin kyberturvallisuutta kapeammin kuin mitä unioni, mistä johtuen NATO:a pidetään kybervallan käyttäjänä vahvempana kuin EU:ta (ks. Krzysztof 2014b). Euroopan unioni huomiosi todennäköisesti vähemmän yksityisten yritysten ja kansalaistensa näkökulmia

kyberpuolustuksessaan kuin mitä turvallisuuskumppanina. EU:n tavoitteena olisi; ” konfliktien ehkäisy, kyberturvallisuusuhkien lieventäminen” sekä ” unionista olisi tehtävä ”kyberturvallisuusalan maailmanlaajuinen johtaja vuoteen 2025 mennessä”. Yhteistyömuodolla olisi enemmän sotilaallisia kuin siviilinomaisia piirteitä.

*Yhteisön tukijana ja edustajana*. Unionin kybervallassa on tällä hetkellä osittaisia piirteitä toimia yhteisön tukijana ja edustajana kyberturvallisuuden saralla. Kyberturvallisuuden globaaliluonteisuuden takia valtiot joutuvat tekemään yhteistyötä, erityisesti kansainvälisen rikollisuuden torjumiseksi. EU:n roolina on silloin toimia yhteisönsä edustajana, joka edistää taloudellisia ja kansalaisyhteiskuntansa intressejä kansainvälisessä ympäristössä. (Dunn-Cavelty & Egloff 2019, 49.) Euroopan unionilla on mandaatti harjoittaa diplomatiaa jäsenvaltioidensa puolesta, ja jo nykyisin EU:lla on valtuudet toteuttaa eurooppalaista turvallisuus- ja puolustuspolitiikka esimerkiksi kriisinhallinnan sekä siviili- ja poliisiyhteistyön muodossa. Kuitenkin yhteisön tukijana ja edustajana uniolla ei olisi samanlaisia valmiuksia toteuttaa eurooppalaista kyberpuolustusta kuin yllä olevissa kybervallan muodoissa. Euroopan unioni yrittäisi enemmän edistää oikeusvaltio- ja demokratiaperiaatteita verkkoympäristön hallitsemiseksi, muokaten siten kansainvälistä normistoa kyberavaruuden hallitsemiseksi. Unioni ajaa jäsenvaltioiden intressejä globaalilla agendalla ja EU tekeekin yhteistyötä; ” kansainvälisten kumppanien ja kansainvälisten organisaatioiden, kuten Euroopan neuvosto, OECD, ETYJ, NATO ja YK, kanssa”. Yhteisön tukijana ja edustajana Euroopan unionin kybervallassa yhdistyisi vahvasti ylikansallisen ja valtioidenvälisen yhteistyön piirteitä, mutta pääsääntöisesti yhteistyö tapahtuisi ylikansallisesti.

*Lainsäätäjänä ja sääntelijänä*. Euroopan unionin asema kybervallan käyttäjänä muistuttaa vahvinten lainsäätäjän ja sääntelijän roolia. Toisin sanoen Euroopan unioni on onnistunut kehittämään yhteistä lainsäädäntöä kyberpuolustuksensa parantamiseksi, mutta kybervallassa yhdistyy selvästi sekä ylikansallisen että valtioidenvälisen yhteistyön muotoja. Yhtäältä lainsäätäjän ja sääntelijän roolissa EU luo tarvittavan oikeusjärjestyksen, selkeyttääkseen hierarkiallista funktiotansa suhteessa talouteen ja kansalaisyhteiskuntaan esimerkiksi suojelemalla kriittistä infrastruktuuriaan kyberrikollisuudelta. Toisaalta EU asettaa myös lailliset raamit säädelläkseen kansalaisyhteiskuntaansa ja talouttansa. Näin tapahtuu muun muassa tuotesertifiointien turvallisuusmääräysten kohdalla tai valmistajien vastuukysymyksinä digitaalisia komponentteja koskevana lainsäädäntöinä. (Dunn-Cavelty & Egloff 2019, 49.) EU on saavuttanut kybervaltansa kohdalla eräänlaisen välietapin ylikansallisena toimijana kyberturvallisuuden varmistamiseksi. Syveneekö Euroopan unionin toiminta kyberturvallisuuden parantamiseksi, riippuu jäsenvaltioiden ja instituutioiden välisestä historiallisesta kehityksestä. Vielä

toistaiseksi kansallisvaltioiden ei tarvitse luovuttaa tietoja EU:lle, jotka ovat niiden kansallisen turvallisuuden intressien vastaisia. Erityisesti Ranskan-Saksan-yhteistyö tulee määrittelemään todennäköisesti, miten pitkälle Euroopan unionin kybervalta integroituu. Muussa tapauksessa Euroopan unionin kybervalta voi jäädäkin lainsäätäjän ja sääntelijän rooliin, missä komission roolina on toimia enemmän koordinoijina yhteisen politiikan saavuttamiseksi.

*Tiedon tuottajana ja levittäjänä*. Euroopan unionilla on myös iso rooli toimia kyberturvallisuutta koskevan informaation levittäjänä. Toisaalta lainsäätäjänä EU:lle on pitänyt kehittyä toimintakäytänteitä ja instituutioita, mitkä mahdollistavat toivotunlaisen tiedon tuottamisen. EU:n kohdalla ENISA:lla on isoin rooli tuottaa Eurooppaa hyödyttävää informaatiota koskien kyberturvallisuutta. EU:n yhtenä roolina kyberavaruudessa on mahdollistaa taloudelle ja kansalaisyhteiskunnalle luotettavaa tietoa kyberasioista. Luotettavuuteen vaikuttaa vahvasti se, kuinka historiallisesti yhteiskunnan toimijoiden ja valtion instituutiot ovat kehittyneet. EU:n roolina onkin toimia turvallistajana, hyödyntäen toimijoilta saamaansa luottamustaan, levittäessään kyberuhkia koskevaa informaatiota. (Dunn-Cavelty & Egloff 2019, 49.) Euroopan unionin kybervallassa jäsenvaltiot ovat olleet sitoutuneita kehittämään EU:n kybervaltaa tiedon tuottajan ja levittäjän saralla. Muun muassa asetuksen (2019) tavoitteena oli pyrkiä lisäämään ENISA:n kapasiteettia avustamaan unionia kyberpuolustuksessa; ” ENISAn on tarpeen analysoida nykyisiä ja kehittymässä olevia kyberturvallisuusriskejä”. EU:n jäsenvaltiot eivät ole täysin valmiita jakamaan kaikkea informaatiota kyberturvallisuusasioissa, mitkä liittyvät niin sanottuun ”kovaan turvallisuuteen”. Jos unionin kybervalta pelkistyisi vain tiedon tuottamiseen ja levittämiseen, olisi unionin rooli enemmän valtioidenvälistä yhteistyötä, jossa ylikansallinen toimija (todennäköisesti ENISA) pyrkisi tuottamaan neutraalia tietoa kyberturvallisuudesta. Euroopan unionin kybervalta on jo kuitenkin tähän mennessä integroitunut pidemmälle kuin vain tiedon levittäjäksi tai tuottajaksi, kuten taulukosta viisi voidaan nähdä.

*Uhkana ja vihollisena*. Tässä skenaariossa EU:n kybervalta on heikoimmillansa. Todennäköisesti EU:lla olisi aivan minimaalinen rooli eurooppalaisessa kyberturvallisuuskäytänteissä. EU:n kohdalla lisääntynyt riippuvuus kyberavaruudesta johtaa eräänlaiseen paradoksaaliseen tilanteeseen, jossa vapaampi Internet on sille uhka, mutta samalla EU:sta voi tulla vaaratekijä myös omalle taloudelleen ja kansalaisyhteiskunnalleen (Dunn-Cavelty & Egloff 2019, 48). EU:n kybervalta voi loukata esimerkiksi yksilöidensä oikeuksia, unionin pyrkiessä kehittämään omia tiedusteluvalmiuksiaan. Esimerkiksi autoritaariset valtiot voivat tästä perspektiivistä näyttäytyä enemmän uhkana kuin turvallisuuden lisääjänä. Myös unionin kasvaneet valmiudet suorittaa kyberoperaatioita voivat näyttäytyä uhkana esimerkiksi USA:n tiedusteluvalmiuksille, joka haluaa säilyttää asemansa johtavana tiedustelutoimijana (Krzysztof 2014b,

472). Yhdysvallat ei välttämättä ole valmis tekemään sellaisia sopimuksia EU:n kanssa, jotka loukkaavat sen kansallisia intressejä. Yhtä lailla Kiinaa pidetään myös merkittävänä tiedustelijana (Nye 2017,65-66), joka voi kokea EU:n kybervallan uhkaksi omaksi yhteiskuntajärjestyksellensä. Euroopan unionin kybervalta voi myös uhata jäsenvaltioiden suvereniteettia, mistä johtuen ne eivät haluaisi jakaa tietojaan unionille. Pitää myös muistaa, EU:n kybervalta uhkana ja vihollisena on myös hyvin epätodennäköisin, jos unioni korostaa enemmän puolustuksellista kyberkyvykkyyttä kuin kykyä suorittaa haluamiaan kyberoperaatioita kyberavaruudessa.

# 5. Johtopäätökset

Kandidaatintutkielmassa on pyritty havainnollistamaan, millainen valtaväline kybervalta on ja, kuinka sitä on tutkittu positiivisten tulkintojen valossa. Kybervalta on käsitteenä hyvin tuore ja tämänhetkiset ymmärrykset kybervallasta korostavat sitä eräänlaisena valtaresurssina (Van Haast 2016, 10-11), siinä missä esimerkiksi ydinaseet ovat. Ydinaseiden määrä ei takaa ydinasepelotetta, vaan konstruktivistiset tulkinnat (Vuori 2016) painottavat myös puheaktien merkitystä pelotevaikutuksen luomiseksi. Kybervallassa on kyse kyberfyysisen toimintaympäristön hallitsemisesta. Kyberturvallisuudella pyritäänkin suojelemaan kyberfyysistä toimintaympäristöä hyökkäyksiltä, joiden kohteena ovat kyberavaruudessa sijaitsevat tietovarannot. Kööpenhaminan koulukunta korostaa turvallisuuden poliittista luonnetta, jossa erilaisin turvallisuusdiskurssein pyritään vaikuttamaan turvallisuuspolitiikan sisältöön. Turvallisuusdiskurssit muokkaavat toimijoiden käsityksiä sosiaalisesta ympäristöstä ja pitävät sisällään erilaisia erottelun piirteitä. Kyberturvallisuuden uhkakuvat muodostetaan bittienmaailmassa, mutta niiden vaikutukset konkretisoituvat fyysisessä maailmassa (Limnéll 2014 et.al. 32-34). Esimerkiksi haittaohjelma voi lamaannuttaa tietojärjestelmän ja samalla kaupungin energiaverkkojärjestelmän. Edellisen kaltainen uhkakuva korostaa, miten fyysinen maailma ja virtuaalimaailma sulautuvat tiivisti yhteen muodostaen kyberfyysisen toimintaympäristön.

Tutkimuksessa dekonstruktoidaan Euroopan unionin kybervalta ja taulukosta viisi voidaan nähdä kybervallalla olevan kuusi erilaista identiteettiroolia Euroopan unionin diskurssissa. Dekonstruktiivinen selittämistapa täydentää integroitunutta toimintamallia, koska se mahdollistaa integraation selittämisen prosessiluonteisena. Kybervalta ei ole silloin joko läsnä tai poissa derridalaisessa mielessä, vaan voi saada monenlaisia ilmentymiä samanaikaisestikin. Kybervallan identiteettirajat ovat häilyväisiä, sillä sitä on vaikea sanoa, milloin EU:n kybervalta muuttuu, jolloin sen rooli kyberturvallisuuspolitiikassa muuttuu myös. Toimijoilla voi olla elämässäkin samanaikaisesti moniakin erilaisia rooleja konstruktiivisten tulkintojen mukaisesti. Nykyisin Euroopan unionin kybervalta näyttäytyy vahvinten lainsäätäjänä ja

sääntelijänä sekä osittain yhteisön tukijana ja edustajana. Euroopan unionin kybervallalla on siten vahvasti sekä ylikansallisen että hallitustenvälisiä yhteistyömuotoja. Kybervalta ilmenee diskurssissa osittain neutraalina asiana, jossa korostetaan kyberturvallisuuden puolustuksellisia näkökulmia, eikä niinkään hyökkäyksellisiä valmiuksia. Osittain tämä vastaa Dunn-Caveltyn (2019) kysymykseen, että missä olosuhteissa kybervalta muuttuu poliittiseksi vallaksi ja, miten se voitaisiin käsitteellistää ja toteuttaa? Tutkimuksessa dekonstruktoitiin diskurssianalyysillä Euroopan unionin kyberturvallisuusdiskurssi predikoinnin, olettamuksien ja subjektin paikannuksen avulla. Myös kuudella erilaisella kybervallan identifikaatiomuodolla välillä vallitsee hierarkia, jossa unioni pyrkii lisäämään omaa vaikutusvaltaansa turvallisuuskumppanin roolin suuntaan. Tiiviimmin integroitunut kybervalta mahdollistaa EU:lle tehokkaamman poliittisten intressien tavoittelemisen verrattuna mitä hallitustenvälisessä yhteistyössä. Konstruktivistinen selitysmalli painottaa enemmän tarkoituksenmukaisuuden logiikkaa kuin seuraamuksen logiikkaa. Eurooppalaisessa kyberturvallisuuspolitiikassa jäsenvaltiot ovat tavoitelleet oikeanlaista ratkaisua EU:n kybervallan kehittämiseksi ennemmin kuin omien etujensa maksimointia.

Toimijoiden identiteetit muuttuvat vuorovaikutuksessa ja konstitutiivinen valta painottaa toimijoiden intressien muodostuvan sosiaalisessa kanssakäymisessä. Toimijat siten itse määrittelevät, miten ne kiinnittyvät rakenteisiin, eikä toisinpäin (Wendt 1992, 394). Edellinen seikka mahdollistaakin sen, millaisena kybervalta ilmenee toimijoiden mielestä. Makrotason turvallisuusdiskursseilla voi siten olla inklusiivisia vaikutuksia, missä eksistentiaalinen vaara uhkaa laajempaa maantieteellistä aluetta tai parhaimmillaan uskonnon, sivilisaation ja ideologian olemassaoloa (Buzan & Wæver 2009, 260-1). Muun muassa regionaalinen turvallisuuskompleksiteoria korostaa uhkien olevan luonteeltaan enemmän alueellisia, jossa saman alueen valtiot kokevat tietyn asian yhteisesti uhkaavana niiden olemassaoloa, jolloin valtioiden keskinäinen vuorovaikutus on voimakkaampaan kuin mitä alueiden välinen on (Buzan & Wæver 2003, 41). Hyvä esimerkki makrotason turvallisuusdiskurssista liittyy kylmän sodan ilmentymään Euroopassa, joka voidaan nähdä Yhdysvaltojen ja Neuvostoliiton välisenä ideologisena taisteluna. Vastaavasti toisinaan puhutaan myös Euroopan olleen vain yksi näyttämö lännen (USA, Eurooppa ja Japani) ja idän (Neuvostoliitto, Jugoslavia ja Kiina) välisessä kamppailussa. Euroopalla oli kylmässä sodassa erilainen rooli, riippuen makrodiskurssista.

Diskurssit muokkaavat toimijoiden identiteettejä, jolloin turvallisuusuhat mahdollistavat legitiimisen politiikan. Euroopan unioni rakentaa kybervaltaansakin vertaamalla itseään muihin toimijoihin, mikä määrittelee EU:n kybervallan muotoa hyvin vahvasti alueellisesta näkökulmasta. Jatkotutkimuksena olisi hyvä tutkia tarkemmin, millaisia diskursseja yrityksillä on kyberturvallisuudessa, koska valtion takaama turvallisuus on niistä vahvasti riippuvainen

kyberturvallisuudessa. Toiseksi Euroopan unionin sisällä voitaisiin syventyä tarkemmin tiettyjen instituutioiden ja jäsenvaltioiden (erityisesti Saksan ja Ranskan) diskursseihin, mitkä määrittelevät unionin kybervallan suunnan. Kolmanneksi voitaisiin tutkia muun muassa Kiinan ja USA:n kybervaltaa, koska se vaikuttaisi myös EU:n käsityksiin omasta toimijuudestaan kyberturvallisuuspolitiikassa. Tärkeintä tulevien tutkimusten olisi lähestyä kybervaltaa konstitutiivisesta näkökulmasta, mitä kukaan toimija ei voi yksin hallita. Kybervaltaa ei tulisi missään nimessä nähdä valtaresurssina siinä missä ydinaseet ovat. Toimijan ei voida sanoa omaavan kybervaltaa, jolloin valta on joko läsnä tai poissa. Kybervallan voidaan sanoakin ennemmin olevan läsnä, mutta toimijan rooli kybervallan käyttäjänä on vaihteleva. Edellinen seikka pyrkii huomiomaan niitä kybervallan piirteitä, jotka eivät ole täysin läsnä, mutta eivät myöskään poissa kokonaan. Kybervaltaa voitaisiin tarkastella enemmän toimijoita muokkaavana, koska valtioiden on pyrittävä sopeuttamaan omaa rooliaan uudella tavalla kyberfyysisessä toimintaympäristössä. Kyberympäristö rikkoo valtion väkivallan monopolin niin sanotusti, koska kyberhyökkäys voi tulla mistä, milloin ja keneltä tahansa. Kyberympäristö, kuten ei myöskään kansainvälinen ympäristö, ei ole normeista tai säännöistä täysin vapaa, sillä loppujen lopuksi kyberfyysinen toimintaympäristö on ihmisten luoma maailma. Juuri edellisen seikan vuoksi kandidaatintutkielmassa kybervalta ymmärretään produktiivisena ja diffuusiivisena, mikä luo toimijoille mahdollisuuksia. Kybervallan ymmärtäminen konstitutiivisena johtaa toimijoiden väliseen yhteistyöhön, missä valtion rooli muistuttaa turvallisuuskumppania eikä vihollista ja uhkaa. Edellisen kaltainen valtakäsitys johtaa myös toimijoiden väliseen tehokkaaseen yhteistyöhön kyberturvallisuuden parantamiseksi, koska toimijat määrittelevät kybervallan olemuksen.

# Lähteet

**Primääriaineisto**

Tutkimusaineisto

Asetus (2019). *Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifi-oinnista sekä asetuksen (EU) N:o 526/2013 kumoa-misesta (kyberturvallisuusasetus)*. Euroopan parlamentti. Saatavissa < https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32019R0881&from=FI >, luettu 24.4.2020.

EU-vaalit (2018), *COMMISSION RECOMMENDATION, on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*. Komissio. Saatavissa < https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf >, luettu 24.4.2020.

Kyberdiplomatia (2015), *Council Conclusions on Cyber Diplomacy*. Euroopan unionin neuvosto. Saatavissa < http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf>, luettu 24.4.2020.

Kyberdiplomatia (2017), *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* Saatavissa < http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf>, luettu 24.4.2020.

NIS-direktiivi (2016), *EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2016/1148, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa*. Euroopan parlamentti. Saatavissa < https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=EN >, luettu 24.4.2020.

Resilienssi (2017), *YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle*. Komissio. Saatavissa < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450 >, luettu 24.4.2020.

Strategia (2013), *YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö.* Komissio. Saatavissa < https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:52013JC0001&from=EN >, luettu 24.4.2020.

Suunnitelma (2017), *KOMISSION SUOSITUS (EU) 2017/1584, koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin*. Komissio. Saatavissa < https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32017H1584&from=FI >, luettu 24.4.2020.

Tutkimuskeskus (2018), *Euroopan talous- ja sosiaalikomitean lausunto aiheesta "Ehdotus Euroopan parlamentin ja neuvoston asetukseksi Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta*" (COM(2018) 630 final — 2018/0328 (COD)). Euroopan talous- ja

sosiaalikomitea. Saatavissa < https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:52018AE4805&qid=1537349553647>, luettu 24.4.2020.

5G (2020), *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Secure 5G deployment in the EU - Implementing the EU toolbox.* Komissio. Saatavissa < https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission>, luettu 24.4.2020.

Euroopan unionin verkkosivut

Council of Europe (2020), *Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime*. Saatavissa < Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime >, luettu 6.4.2020.

Komissio cybersecurity (2020), *Cybersecurity*. Saatavissa < https://ec.europa.eu/digital-single-market/en/cyber-security >, luettu 6.4.2020.

NIS-direktiivin verkkosivu (2020), *The Directive on security of network and information systems (NIS Directive)*. Saatavissa < https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive >, luettu 6.4.2020.

Kyberturvallisuusasetuksen verkkosivu (2020), *The EU Cybersecurity Act*. Saatavissa < https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act >, luettu 6.4.2020.

Euroopan unionin instituutioiden tuottamat aineistot

CSDP (2017)*, Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and risks for the EU*. EPRS | European Parliamentary Research Service Scientific Foresight Unit (STOA). Euroopan parlamentti.

*Maastrichtin sopimus Euroopan unionista* (1992): Tiivistelmä asiakirjasta. Saatavissa < https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=LEGISSUM:xy0026&from=EN>, luettu 1.4.2020.

**Sekundaariaineisto**

Acatech (2011), *Cyber-Physical Systems*. Berlin, Heidelberg : Springer Berlin Heidelberg : Imprint: Springer. Saatavissa < https://link-springer-com.libproxy.tuni.fi/book/10.1007%2F978-3-642-29090-9>, luettu 13.3.2020

Arendt, Hannah, kirjoittaja.; Virtanen, Eija, kääntäjä.; Oittinen, Riitta, toimittaja. (2017), *Vita activa : ihmisenä olemisen ehdot*. Tampere : Vastapaino.

Barnett, Michael & Duvall, Raymond (2005) “Power in International Politics.” International Organization 59.(1) 39–75.

Buzan, Barry & Wæver, Ole. (2003) *Regions and powers : the structure of international security* . Cambridge: Cambridge University Press.

Buzan, Barry & Hansen, Lene (2009), *THE EVOLUTION OF INTERNATIONAL SECURITY STUDIES*. CAMBRIDGE: CAMBRIDGE UNIVERSITY PRESS.

Buzan, Barry. & Wæver, Ole (2009), ”Macrosecuritisation and security constellations: reconsidering scale in securitisation theory”. *Review of International Studies*. 35 (2), 253–276.

CARRAPICO, HELENA & BARRINHA, ANDRÉ (2017), ” The EU as a Coherent (Cyber)Security Actor?”, *JCMS 2017* Volume 55. Number 6. pp. 1254–1272.

Christou, George (2019) ”The collective securitisation of cyberspace in the European Union”, *West European Politics,* 42:2, 278-301, DOI: 10.1080/01402382.2018.1510195.

Derrida, Jacques & Caputo, John (1997). *Deconstruction in a Nutshell: a Conversation with Jacques Derrida*. Saatavissa < https://www-fulcrum-org.libproxy.tuni.fi/epubs/1z40kt24v?locale=en#/6/246[xhtml00000123]!/4/4/1:0>, luettu 31.3.2020.

Dunn-Cavelty, Myriam (2013), “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse.” *International Studies Review* 15.(1) :105–122

Dunn-Cavelty, Myriam (2018), ” Europe’s cyber-power”, *EUROPEAN POLITICS AND SOCIETY*, 2018 VOL. 19, NO. 3, 304–320.

Dunn-Cavelty, Myriam & Egloff, Florian. J (2019), “The Politics of Cybersecurity: Balancing Different Roles of the State.” *St Antony’s International Review* 15 no.1:37-57.

Fierke, K. M.(2005) *Diplomatic Interventions : Conflict and Change in a Globalizing World* . Basingstoke: Palgrave Macmillan,

Foucault, Michel (2002), *Archaeology of Knowledge* . London: Routledge.

Hansen, Lene. (2006) *Security as practice : discourse analysis and the Bosnian war* . London ;: Routledge

Hansen, Lene & Nissenbaum, Helen (2009), ” Digital Disaster, Cyber Security, and the Copenhagen School”, *International Studies Quarterly*, Vol. 53, No. 4, 1155-1175.

Hansen, Lene. (2012) ”Reconstructing desecuritisation: the normative-political in the Copenhagen School and directions for how to apply it”. *Review of International Studies*. 38 (3), 525–546.

Held, David (2006), *Models of democracy.* Cambridge ; Malden MA : Polity.

Heywood, Andrew (2013), *Politics*. UK: Palgrave Foundations 4th.edition.

Hix, Simon & Høyland, Bjørn (2011), *The Political System of the European Union*. UK: Palgrave Macmillan 3rd. edition.

Järvinen, Petteri (2018), *Kyberuhkia ja Somesotaa*. Jyväskylä: Docendo

Kello, Lucas (2018), *The Virtual Weapon And International Order*. New Haven & London: Yale University Press.

Klimburg, Alexander (2011), ” The Whole of Nation in Cyberpower”. *International Engagement on Cyber*, 171-179.

Krzysztof, Sliwinski (2014), ”European Union – cyber power in the making.”, *Asia-Pacific-Journa of EU Studies.* Vol. 12. No. 1. 1-22.

Krzysztof, Sliwinski (2014b) ”Moving beyond the European Union’s Weakness as a Cyber-Security Agent”. *Contemporary Security Policy.* 35 (3), 468–486. Saatavissa http://www.tandfonline.com/doi/abs/10.1080/13523260.2014.959261, luettu 17.4.2020.

Lehto, Martti & Limnéll, Jarno (2017)”Kybersodankäynnin kehityksestä ja tulevaisuudesta”, *Tiede ja Ase*, 179-212.

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

Limnéll, Jarno & Iloniemi, Jaakko (2018), *Uhkakuvat*. Jyväskylä: Docendo.

Lynn Doty, Roxanne. (1993) ”Foreign policy as social construction - a post-positivist analysis of U.S. counter-insurgency policy in the Philippines”. *International studies quarterly*. 37 (3), 297–320.

Nye, Joseph Jr. (2010), *Cyber Power*. Harvard Kennedy School: Belfer Center for Science and International Affairs.

Nye, Joseph Jr. (2017), ”Deterrence and dissuasion in cyberspace”. *International security*, 41(3), 44-71.

Risse, Thomas (2009) ” Social constructivism and European integration ”. Teoksessa Wiener, Antje ja Thomas Diez (toim.). *European Integration Theory*. 2nd ed. Oxford: Oxford University Press.

Ruostesaari, Ilkka (2010), *Energiavalta: eliitti ja kansalaiset muuttuvilla energiamarkkinoilla*. Tampere: Tampere University Press.

Ruostesaari, Ilkka (2014), *Vallan Sisäpiirissä.* Tampere: Vastapaino.

Sheldon, John B (2014) ” Geopolitics and Cyber Power: Why Geography Still Matters” *merican Foreign Policy Interests*, Vol.36(5), pp.286-293. Saatavissa http://web.a.ebscohost.com.libproxy.tuni.fi/ehost/detail/detail?vid=0&sid=32636298-86ef-4221-a276-98ceaf39e169%40sdc-v-sessmgr01&bdata=JkF1dGhUeX-BlPWNvb2tpZSxpcCx1aWQmc2l0ZT1laG9zdC1saXZlJnNjb3BlPXNpdGU%3d#AN=99208039&db=asn, luettu 13.3.2020.

Salminen, Mirva (2018), ”Kyber-Fyysinen Sota 2030 +: Yhteiskuntien kompleksisuus tuottaa yllätyksiä sodankäyntiin”. Teoksessa Rantapelkonen, Jari (toim.), *Tuleva sota: tulevaisuuden*

*sodan tulevaisuus*. Julkaisusarja 2: Tutkimusselosteita nro 5. Maanpuolustuskorkeakoulu: Edita Publishing Oy.

Van Haaster, Jelle (2016), ” Assessing Cyber Power”, *2016 8th International Conference on Cyber Conflict Cyber Power* N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.) 2016 © NATO CCD COE Publications, Tallinn.

Vuori, Juha (2016), ” Deterring Things With Words: Deterrence as a Speech Act1”, *New-Perspectives* Vol. 24,No. 2/2016.

Wæver, Ole (2009), ”Discursive approaches”. Teoksessa Wiener, Antje, ja Thomas Diez (Toim.) *European Integration Theory* . 2nd ed. Oxford: Oxford University Press.

Wæver, Ole (2011), ” Politics, security, theory”. Security Dialogue 42(4-5) 465– 480.

Wendt, Alexander (1992) ”Anarchy is what states make of it: the social construction of power politics”. *International Organization*. 46 (Spring 92), 391–425. Saatavissa http://search.proquest.com/docview/57876575/, luettu 7.5.2020.

Wendt, Alexander (1999) *Social theory of international politics*. Cambridge: Cambridge University Press.

# Liitteet

Taulukko 6 tutkimusaineiston esittely

| **Asiakirja** | **Selitys** |
|---|---|
| Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö (2013). (Myöhemmin tekstissä pelkkä *Strategia (1)*). | Euroopan unionin ensimmäinen virallinen strategia, joka käsittelee pelkästään kyberturvallisuutta. Strategiassa hahmotellaan EU:n visiota kyberturvallisuudesta, suuntaviivoja, rooleja, vastuita sekä määritellään toimet tehokkaan verkkoturvallisuusympäristön aikaansaamiseksi. (Strategia 2013). |
| Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle (2017). (Myöhemmin tekstissä pelkkä *Resilienssi (2)*) | Kyberuhkien kasvan määrän johdosta, unioni täydentää alkuperäistä strategiaansa, joka painottaa resilienssin merkitystä kyberuhkien hallitsemiseksi. Tällä tulokulmalla Euroopan unioni siirtyy reaktiivisesta tulokulmasta proaktiivisempaa suuntaan. (Resilienssi 2017, 2-3.) |
| EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2016/1148, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (2016). (Myöhemmin tekstissä pelkkä *NIS-direktiivi (3)*) | NIS-direktiivi on ensimmäinen koko EU:n kattava kyberturvallisuutta koskeva lainsäädäntö. Lain tavoitteena on kehittää unionin lainsäädäntöä kyberturvallisuuden saralla. Lain johdosta jäsenvaltiot perustavat CSIRT-osastoja sekä virallisen NIS-viranomaisen, esim. Suomessa Liikenne- ja viestintäviraston alainen kyberturvallisuuskeskus, joka koordinoi kansallista kyberturvallisuutta. Lisäksi direktiivissä luetellaan ne alat, jotka ovat erityisen alttiita kyberhyökkäyksille unionin sisämarkkinoilla. (NIS-direktiivin verkkosivu 2020.) |
| Komission suositus (EU) 2017/1584, koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (2017). (Myöhemmin tekstissä pelkkä *Suunnitelma (4)*). | Suunnitelma tarjoaa EU:n toiminalle raamit laaja-alaisten rajat ylittävien tietoverkossa tapahtuvien vaaratilanteiden tai kriisien varalta. Strategiassa asetetaan tavoitteet ja yhteistyötavat, jolla jäsenvaltiot ja EU:n instituutiot pyrkivät vastaamaan kyberuhkiin. (Komissio cybersecurity 2020.) |

| | |
|---|---|
| Komission suositus verkon turvallisuudesta vapaan ja läpinäkyvän Euroopan parlamenttivaalien järjestämiseksi;”election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament” (2018). (Myöhemmin tekstissä pelkkä *EU-vaalit (5)*) | Suosituksessa Komissio esittelee toimenpiteitä, millä voidaan tukea Euroopan unionin vaaleja. Suosituksessa kerrotaan muun muassa vaalien järjestämiseksi tarvittavasta yhteistyöstä, tietoverkon avoimuudesta, verkkoturvallisuustilanteiden suojaamisesta ja väärien tietokampanjoiden torjumisesta. (Komissio cybersecurity 2020.) |
| Ehdotus Euroopan parlamentin ja neuvoston asetukseksi Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta (2018). (Myöhemmin pelkkä *Tutkimuskeskus (6)*) | Kyberturvallisuusasetuksen johdosta Komissio ehdotti kyberturvallisuuden osaamiskeskuksen perustamista sekä kyberturvallisuuskeskusta, joka on erikoistunut teollisuuden ja teknologian tutkimukseen kyberturvallisuuden saralla. (Komissio cybersecurity 2020) |
| Komission tiedonanto vakaasta 5G-verkkoympäristö ”Secure 5G deployment in the EU - Implementing the EU toolbox” (2020). (Myöhemmin pelkkä *5G (7)*) | Tiedonannossa Komissio esittelee vaatimuksia vakaiden 5G-verkkojen järjestämiseksi jäsenvaltioissa. Tiedonannossa todetaan, että 5G-verkkoympäristöstä pyritään tekemään ensimmäistä kertaa unionin historiassa eurooppalaista yhtenäistä tietoverkkoa. (5G 2020, 2.) |
| Euroopan unionin kyberpuolustus; ”Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox) (2017) ” & ” Council Conclusions on Cyber Diplomacy (2015)”. (Myöhemmin pelkkä *Kyberdiplomatia* 2017 (8) tai *Kyberdiplomatia* 2015 (9) | Asiakirjoissa määritellään diplomaattisia keinoja haitallisille tietoverkkotoiminnoille unionin yhteisessä ulko- ja turvallisuuspolitiikassa. Asiakirjoissa esitellään esimerkiksi rajoittavia toimenpiteitä, joilla voidaan vahvistaa EU:n reagointia toimintaa, jotka vahingoittavat sen taloudellisia, poliittisia ja turvallisuusintressejä. (Komissio cybersecurity. 2020) |
| Euroopan unionin kyberturvallisuusasetus: ”Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus)” (2019). (Myöhemmin pelkkä *Asetus (10)*) | Kyberturvallisuusasetus vahvistaa EU:n pääkybertoimijan ENISA:n roolia kyberasioihin liittyen. Asetuksen johdosta perustettiin eurooppalainen kyberturvallisuussertifiointikehys, jolla varmistetaan ICT-tuotteiden, palveluiden ja prosessien oikeanlaiset turvallisuusvaatimukset. (Kyberturvallisuusasetuksen verkkosivu 2020) |

Lyhenteet:

CSIRT= Computer Security Incident Response Team

ENISA= European Union Agency for Cybersecurity; Euroopan unionin verkko- ja tietoturvavirasto

*Sulkeissa ilmenevä luku vastaa taulukossa 6 otettua totea*

## Taulukko 5:n alkuperäiset lausumat

[i] Katso esimerkkinä Lynn Doty (1993, 311)
[ii] investigation and prosecution of such crimes remains a common endeavour for Member State
[iii] conflict prevention, the mitigation of cybersecurity threats
[iv] EU recalls its and its Member States' efforts to improve cyber resilience
[v] EU:n ulkopuolisista maista peräisin olevat yritykset, jotka ovat jo pitkään toimineet Euroopan maaperällä ja jotka ovat täysipainoinen osa Euroopan teknologista ja teollista perustaa, voisivat olla EU:n hankkeiden kannalta erittäin hyödyllisiä
[vi] Uhkien motiivi usein rikollinen voiton tavoittelu, mutta ne voivat olla luonteeltaan myös poliittisia tai strategioita
[vii] As a result, ensuring the cybersecurity of 5G networks is an issue of strategic importance for the Union at a time when cyber-attacks are on the rise, more sophisticated than ever and coming from a wide range of threat actors, in particular non-EU state or state-backed actors.
[viii] 2019 will be the first European Parliament elections in the changed security environment
[ix] EU approach for cyber diplomacy
[x] ylikansallisen luonteen vuoksi näiden järjestelmien merkittävät häiriöt, olivatpa ne tahallisia tai tahattomia ja riippumatta siitä, missä ne tapahtuvat, voivat vaikuttaa yksittäisiin jäsenvaltioihin ja koko unioniin.
[xi] The fifth generation (5G) of telecommunication networks are set to play an essential role in the development of the European society and economy
[xii] (2016/4(4)) ’keskeisten palvelujen tarjoajalla’ julkista tai yksityistä toimijaa, joka on liitteessä II tarkoitettua tyyppiä ja täyttää 5 artiklan 2 kohdassa säädetyt kriteerit;
[xiii] Verkkorikollisuuden osalta taas Budapestin sopimus on sääntelyväline, johon kolmannetkin maat voivat vapaasti voivat vapaasti sitoutua. Se toimii mallina kansalliselle verkkorikoslainsäädännölle ja perustana alan kansainväliselle yhteisölle.
[xiv] (2019 (69)) Eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien olisi oltava syrjimättömiä ja eurooppalaisiin tai kansainvälisiin standardeihin perustuvia, paitsi jos kyseiset standardit ovat tehottomia tai epäasianmukaisia unionin oikeutettujen tavoitteiden saavuttamiseksi.
[xv] Article 8 of the Charter of Fundamental Rights of the European Union, Article 16 of the Treaty on the Functioning of the European Union and Regulation (EU) 2016/679 of the European Parliament and of the Council13 guarantee the protection of natural persons with regard to the processing of their personal data including when their personal data are processed in the context of elections.
[xvi] (2016 (40)) CSIRT-verkostoon osallistuvia CSIRT-toimijoita kannustetaan tarjoamaan tietoja julkaistavaksi tällä verkkosivustolla vapaaehtoisuuteen perustuen sisällyttämättä mukaan luottamuksellisia tai arkaluonteisia tietoja.
[xvii] The Commission has proposed close to 3 billion Euro of investments in cybersecurity technologies under the next EU budget 2021-27**.**
[xviii] RECALLS that structured and overarching EU strategic cyber consultations have already been launched with the US, China, Japan, India, South Korea and Brazil
[xix] The fight against terrorism
[xx] for surveillance or censorship by authoritarian regimes
[xxi] the importance of cyber capacity building in third countries.
[xxii] The EU is concerned by the increased ability and willingness of State and non-state actors to pursue their objectives
[xxiii] (2016/1(6)) Tämä direktiivi ei rajoita toimia, joita jäsenvaltiot toteuttavat keskeisten valtiolle kuuluvien tehtäviensä suojaamiseksi, erityisesti kansallisen turvallisuuden suojaamiseksi, mukaan lukien toimet sellaisten tietojen suojaamiseksi, joiden ilmaisemisen jäsenvaltiot katsovat keskeisten turvallisuusetujensa vastaiseksi, sekä yleisen järjestyksen ylläpitämiseksi, erityisesti rikosten tutkimisen, selvittämisen ja syytteeseenpanon mahdollistamiseksi.

[xxiv] (2019/1(2)) Tämä asetus ei rajoita jäsenvaltioiden toimivaltaa sellaisten toimien osalta, jotka koskevat yleistä turvallisuutta, puolustusta, kansallista turvallisuutta tai yksittäisen valtion toimia rikosoikeuden alalla.

[xxv] Yksityiset yritykset ovat haluamattomia jakamaan tietoja kyberhaavoittuvuuksistaan ja niistä seuraavista tappioistaan, koska ne pelkäävät paljastavansa arkaluonteisia liiketoimintatietoja, vaarantavansa maineensa tai rikkovansa tietosuojasääntöjä.