EUROOPAN UNIONIN KYBERTURVALLISUUSTOIMIJUUS

Kokonaisvaltaisesta lähestymistavasta kohti yksilötasoa uhkakuvia arkipäiväistämällä

Rauha-Maija Rannikko

Pro gradu -tutkielma

Valtio-oppi

Turun yliopisto

Kevät 2022

TURUN YLIOPISTO
Filosofian, poliittisen historian ja valtio-opin laitos / Yhteiskuntatieteellinen tiedekunta

RANNIKKO, RAUHA-MAIJA: Euroopan unionin kyberturvallisuustoimijuus. Kokonaisvaltaisesta lähestymistavasta kohti yksilötasoa uhkakuvia arkipäiväistämällä.

Pro-gradu -tutkielma, 96 s.
Valtio-oppi
Huhtikuu 2022

Tutkielma tarkastelee Euroopan unionia (EU) toimijana, joka on nopeasti nostanut kyberturvallisuuden keskeiseksi osaksi turvallisuuspolitiikkaansa. Aiemmin hyvin teknisenä käsitteenä ymmärretty kyberturvallisuus on EU:ssa noussut poikkihallinnolliseksi politiikka-alaksi, joka vaikuttaa niin yhteisiin sisämarkkinoihin, yksittäisen yksilön vapauksiin ja oikeuksiin kuin EU:n yhteisen turvallisuus- ja puolustuspolitiikan kehitykseen. Euroopan unioni on tunnetaan kompleksisena turvallisuuspolitiikan toimijana, mikä herättää kysymyksen siitä, millaisena kyberturvallisuuden toimijana EU puolestaan pyrkii itsensä esittämään ja millaisille tekijöille sen kyberturvallisuustoimijuus perustuu.

Tutkielma on teoriaohjaava laadullinen tutkimus, jossa kriittisen turvallisuustutkimuksen sekä kriittisen diskurssianalyysin teoretisointi ovat keskeisessä osassa. Kriittisen turvallisuustutkimuksen suuntauksista tutkielma nojaa niin kutsutun ’Pariisin koulukunnan’ ja Didier Bigon turvattomuuden politiikan elementtien tarkasteluun. Kriittisiä teoreettisia raameja tukee vahvasti kriittinen diskurssianalyysi, joka toimii aineiston analyysin metodina. Kriittisen diskurssianalyysin menetelmistä tutkielmassa hyödynnetään Norman Fairclough’n tulkintaa diskurssin ja kontekstin välisestä vuorovaikutuksesta sekä vallan paikantumisesta diskurssin takaa.

Tutkielman aineisto koostuu Euroopan unionin virallisista dokumenteista, jotka avaavat kuvaa siitä, millaisena kyberturvallisuustoimijana EU pyrkii itsensä esittämään. Lisäksi tukea-antavana aineistona toimivat Eurobarometrin tuottamat kyberturvallisuutta käsittelevät tilastoaineistot, jotka kertovat EU-kansalaisten suhtautumisesta kyberturvallisuuteen.

Tutkielman analyysi paljastaa mielenkiintoisesti sen, kuinka Euroopan unioni pyrkii esittämään itsensä auktoriteetin omaavana kyberturvallisuustoimijana, joka määrittelee kyberuhkakuvia kansainvälisen turvallisuuspolitiikan tasolta aina yksilötasolle asti. Uhkakuvia arkipäiväistämällä EU pyrkii osoittamaan EU-kansalaisille, kuinka kyberuhat ovat jatkuvasti läsnä ihmisten elämässä erilaisten verkkoon kytkettyjen laitteiden kautta. EU:n arkipäiväisiin asioihin liittyvä turvallisuusuhkien määrittely on turvallistamisen teko. Se mihin, EU kuitenkin turvallistamisellaan pyrkii on yksilöiden tietoisuuden parantaminen ja kouluttaminen kyberuhkiin varautumiseen. Tutkimus osoittaa myös, että kyberturvallisuustutkimusta on tehtävä lisää etenkin yhteiskuntatieteellisen tutkimuksen piirissä, jotta ihmislähtöisemmät näkökulmat aiheeseen lisääntyisivät.

Asiasanat: kyberturvallisuus, toimija, Euroopan unioni, kriittinen turvallisuustutkimus, kriittinen diskurssianalyysi, turvallisuuspolitiikka, uhkakuvien määrittely

KESKEISET LYHENTEET

CASE – Critical Approaches to Security in Europe Collective, Yhteisjulistus kriittisistä turvallisuuden suuntauksista Euroopassa

CERT – Computer Emergency Response Teams, toiminto tietoturvaloukkausten ehkäisemiseen ja tiedottamiseen

cPPP – contractual Public Private Partnership, sopimusluontoinen julkisen ja yksityisen sektorin kumppanuus

CSS – Critical Security Studies, kriittinen turvallisuustutkimus

DNS – Domain Name System, nimijärjestelmä

NATO/Nato – North Atlantic Treaty Organization, Pohjois-Atlantin puolustusliitto

NIS – Network and Information Security Directive, verkko- ja tietoturvadirektiivi

EC3 – European Cybercrime Centre, Euroopan kyberrikollisuuskeskus

ECSO – European Cybersecurity Organisation, Euroopan kyberturvallisuusorganisaatio

EDA – European Defence Agency, Euroopan puolustusvirasto

ENISA – European Union Agency for Cybersecurity, Euroopan unionin verkko- ja tietoturvavirasto/Euroopan unionin kyberturvallisuusvirasto

ESDC –European Security and Defence College, Euroopan turvallisuus- ja puolustusakatemia

EU – Euroopan unioni

EUH – Euroopan unionin ulkosuhdehallinto

J-CAT – Joint Cybercrime Action Taskforce, yhteinen kyberrikollisuuden erikoisyksikkö

YUTP – EU:n yhteinen ulko- ja turvallisuuspolitiikka (alk. engl. Common Foreign and Security Policy, CFSP)

YTPP – EU:n yhteinen turvallisuus- ja puolustuspolitiikka (alk. engl. Common Security and Defence Policy CSDP)

Sisällysluettelo

Kuviot ja taulukot

1. Johdanto

Sana kyber tulee kreikan kielen sanasta ”kybereo”, joka tarkoittaa ohjata, hallita ja opastaa (Turvallisuuskomitea 2018, 22). Sanan voisi helposti liittää merenkulkuun, mutta nykymerkityksessään sana on vakiintunut tarkoittamaan informaation käsittelyä digitaalisessa muodossa esimerkiksi tiedon jakamisena ja viestintänä. Samalla sana viittaa myös itse tietojärjestelmiin ja tietokoneisiin, jotka tietoa käsittelevät. (emt.) Kyber on monien tuttujen sanojen yhdyssanan määriteosana löytänyt nopeasti vakiintuneen paikkansa erityisesti valtioiden ja kansainvälisten organisaatioiden turvallisuuspolitiikasta. Miksi näin?

Viron infrastruktuuriin vuonna 2007 kohdistuneet laajat kyberhyökkäykset (Christou 2019, 282) aloittivat uuden aikakauden kybertoimintaympäristössä. Siitä lähtien kyberhyökkäykset ja -vaikuttaminen ovat yhä suoranaisempia iskuja kohdistettuna tiettyyn toimijaan tai yleisöön (Dunn Cavelty ja Wenger 2020, 5). Kyberoperaatiot ovat nykyään myös kalliimpia, strategisempia ja siten myös poliittisempia Yhdysvaltojen presidentinvaalien häirinnästä lähtien. Tämä selittää sitä, miksi kyberturvallisuus on nostettu niin kansalliselle kuin kansainväliselle turvallisuuspoliittiselle agendalle ja kiireesti (emt.).

Euroopan unioni (EU), kompleksisuudessaan ainutlaatuinen turvallisuuspolitiikan toimija, (Sperling & Webber 2019) on julkaissut jo useamman kyberturvallisuuteen liittyvän strategian sekä direktiivin 2010-luvulta lähtien. Teknisluontoisista tietoturvadirektiiveistä on siirrytty hiljattain kohti kokonaisvaltaisempaa ymmärrystä tehden kyberturvallisuudesta keskeisen osan EU:n turvallisuuspolitiikkaa. Tästä osoituksena toimii vuonna 2020 julkaistu Euroopan unionin turvallisuusunionistrategia, jossa kyberuhat nimetään ensimmäisenä EU:n turvallisuutta uhkaavana tekijänä ennen järjestäytynyttä rikollisuutta sekä terrorismia. Vielä 2010 julkaistussa EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelmassa järjestäytynyt rikollisuus sekä terrorismi mainitaan ensimmäisinä ennen tietoverkkorikollisuutta (EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelma 2010, 2). Kyberuhat koetaan siis nykypäivänä terrorismia ja järjestäytynyttä rikollisuutta suurempina uhkina EU:ssa. Toisaalta digitalisaation aikakaudella myös terrorismi ja järjestäytynyt rikollisuus vaikuttavat digitaalisessa maailmassa eli kybertoimintaympäristössä. Ei pidä siis vähätellä kyberturvallisuuden painoarvoa EU:n turvallisuuspolitiikassa.

Kybertoimintaympäristö on alusta asti nähty kaksiteräisenä miekkana sisältäen laajan mahdollisuuksien kentän, mutta samalla merkittävät riskitekijänsä (Dunn Cavelty 2018, 306-307; Bigo ja Bonelli 2019, 101). Ennakkotapauksia kyberulottuvuudessa toimimisesta ei ollut, minkä vuoksi jokaisen tavoitellun hyödyn mahdollisia negatiivisia seurauksia ei ole voitu etukäteen tietää. Lisäksi kybertoimintaympäristön toimijat ovat alusta asti olleet moninaisia, jolloin valtion tahon toimijoiden lisäksi ympäristössä on aina ollut ulkopuolisia toimijoita omine motiiveineen (Deibert 2018, 411). Toisaalta kaksipäisyytensä ansiosta se tarjoaa samat mahdollisuudet sekä haavoittuvuudet kaikille toimijoille esimerkiksi internetin käytön kautta. Yhdenvertaisuus tarkoittaa myös sitä, että niin yksittäisellä yksilöllä kuin suuremmalla organisaatiolla kuten EU:lla on lähtökohtaisesti täysin samat toimintaedellytykset kybertoimintaympäristössä niin mahdollisuuksien kuin haavoittuvuuksien porttien avaamiseen, mikäli kaikilla olisi käytössään samankokoiset resurssit. Huolimatta siitä, millaisin motiivein toimija kybertoimintaympäristössä toimii, on jokainen toimija autoritaarisista valtioista EU:hun sekä yksilöön riippuvainen kybertoimintaympäristön avoimuudesta (Deibert ja Pauly 2019, 81).

Kyberturvallisuus itsessään on tavoitetila. Tavoitteena on kybertoimintaympäristön luotettavuus ja toiminnan turvaaminen. Kyberturvallisuus on sekä ennakoivaa toimintaa, toimenpiteitä, joilla voidaan estää tai minimoida riskejä, mutta se on myös toimintaympäristön sietokyvyn kehittämistä kyberuhkia vastaan. (Turvallisuuskomitea 2018, 23.) Monien tietovuotojen kohdalla on huomattu, että niiden vaikutukset ovat saattaneet paljastua vasta kuukausien tai jopa vuosien päästä (Limnéll 2021, 8). Sen vuoksi kyberturvallisuuden kehittämisessä on tärkeää ennakoida mahdollisen uhan vaikutukset.

Koska nykypäivänä monet toiminnot kytkeytyvät tietojärjestelmiin ja tietoverkkoon, on sekä mahdollisuuksien että niitä seuraavien riskien määrä yhä suurempi. Riskit ovat vapaassa kybertoimintaympäristössä yhä näkymättömämpiä ja yllättävämpiä. Tämän vuoksi kyberuhkia vastaan pyritään varautumaan, mutta riskejä ei voida enää täysin poistaa. Kyberturvallisuudessa korostuukin riskien minimoimisen sijaan toimintaympäristön resilienssi, kyky sopeutua mahdolliseen kyberhyökkäykseen tai -vaikuttamiseen ja kyky kattavasti analysoida niiden vaikutuksia (Turvallisuuskomitea 2018, 14, 23). Resilienssi on sekä yhteisöjen että yksilöiden kykyä sopeutua muuttuneeseen tilanteeseen, jonka odottamaton uhka aiheuttaa (emt.).

Resilienssi painottuu myös Euroopan unionin tavassa luoda kyberturvallisuutta. Ymmärrys siitä, että jokainen yksilö on osa suurempaa turvallisuusratkaisua näkyy EU:n lähestymistavassa (EU:n turvallisuusunionistrategia 2020). Resilienssiä vaaditaan myös yksilöiltä ja yhteisöiltä turvallisuuspoliittisten kriisien puhjetessa. Keskinäisriippuvuuksien maailmassa kukaan ei ole irrallaan konfliktitilanteista, vaan nykyään kybertoimintaympäristö sitoo jokaisen osaksi konfliktitilanteiden seurantaa tai niihin vaikuttamista. Kyberulottuvuus on yhä vankemmin yksi taistelukenttä perinteisten sotatantereiden rinnalla.

Kyberturvallisuudesta jää helposti kuva kovan turvallisuuden aiheena, jota leimaa strategis-sotilaallinen ajattelu nollasummapeleineen. Tätä mielikuvaa haluan kuitenkin tässä tutkielmassa ravistella. Kyberturvallisuus tulisi ymmärtää kokonaisvaltaisempana käsitteenä etenkin, kun lähes jokainen yksilö on nykypäivänä kytköksissä kybertoimintaympäristöön. Tässä tutkielmassa pyrin tuomaan esille nimenomaan ihmislähtöisempää näkökulmaa tarkastella kyberturvallisuutta. Tämän lähtökohdan valossa esittelen seuraavaksi tutkielmani tavoitteet sekä tutkimuskysymykset.

1.1. Tutkielman tavoitteet ja tutkimuskysymykset

Tarkastelen pro gradu -työssäni sitä, millaisena kyberturvallisuuden toimijana Euroopan unioni pyrkii itsensä esittämään, millaista turvallisuutta se haluaa tuottaa ja kenelle sekä mihin EU:n kyberturvallisuustoimijuus perustuu. EU:ta sekä moititaan että ylistetään pehmeän vallan käyttäjäksi turvallisuuspoliittisissa kysymyksissä (Manners 2002). Ulottuuko samanlainen käyttäytyminen myös kyberulottuvuuteen? Entä mitä uutta EU:n kyberturvallisuustoimijuus voi tuoda sen perinteisen turvallisuuspoliittisen toimijuuden rinnalle?

Tutkielmani tavoitteena on tukea ihmislähtöisempää tapaa tarkastella kyberturvallisuutta sekä tukea kyberturvallisuustutkimuksen vakiinnuttamista suomenkielisessä kontekstissaan. Tutkielman tavoitteen kannalta Euroopan unioni osoittautuu tässä aihepiirissä mielenkiintoiseksi tarkastelukohteeksi, joka korostaa kokonaisvaltaista lähestymistapaa kyberturvallisuuteen pitäen sisällään myös ihmislähtöisen näkökulman. Missä määrin suuri organisaatio voi kokonaisvaltaisuudellaan kuitenkaan tukea

yksilötason kyberturvallisuuden toteutumista? Eikö kriittisen turvallisuustutkimuksen termein, joku jää aina turvallisuuden ulkopuolelle, turvattomuuden marginaaleihin?

Olen valinnut kriittisen turvallisuustutkimuksen suuntauksen teoreettiseksi kehikoksi tutkielmaani, sillä suuntaus näkee turvallisuuden terminä sekä toiminnan muotona olevan jatkuva kyseenalaistamisen kohde, jota tekijä haluaa merkittävästi kontrolloida (Bigo ja McCluskey 2018, 123). Pidän tätä merkityksellisenä siinä mielessä, että kyberturvallisuus on pakottanut vallanpitäjät näkemään turvallisuuden eri tavalla, perinteisestä turvallisuuspolitiikasta poikkeavana, vaikkakin osana sitä. Samalla tarkastelukohteena olevasta Euroopan unionista huokuu halu laajentaa kyberturvallisuustoimijuuttaan, eli politiikan keinoin kontrolloida kybertoimintaympäristössä tapahtuvaa toimintaa, joka on liitännäistä sen sisäiseen kyberturvallisuuteen, mutta kenties myös kansainväliseen turvallisuustoimijan rooliin (Dunn Cavelty 2018, 304).

Tarkoitukseni on tarkastella Euroopan unionia yhtenä kokonaisena instituutiona, ei sen yksittäisiä jäsenvaltioita. Tarkastelen ensisijaisesti sitä, millaisena kyberturvallisuustoimijana EU pyrkii itsensä esittämään ja millaisille seikoille sen kyberturvallisuustoimijuus perustuu. Toisaalta pidän tarkastelussa myös mukana ajatusta siitä, millaisena yksilöiden eli EU-kansalaisten rooli kyberturvallisuuspolitiikassa näyttäytyy. Kuljetan yksilötasoa mukana läpi tarkastelun, sillä kybertoimintaympäristössä toimiminen on yhtä aikaa rajat ylittävää ja kansainvälistä, mutta samalla kaikki toiminta on kosketuspinnassa yksilöön. Tämä onkin toimijoiden voimavara ja samalla suurin haaste kyberulottuvuudessa.

Tutkimuskysymykseni tässä tutkielmassa ovat seuraavat:

> Pääkysymys: *Millaisena kyberturvallisuuden toimijana Euroopan unioni pyrkii itsensä esittämään?*
>
> Alakysymys: *Millaisille tekijöille Euroopan unionin kyberturvallisuustoimijuus perustuu?*

Tutkimuskysymyksistä pääkysymys on keskeisin tässä tutkielmassa, ja pyrin aineiston analyysin avulla löytämään tähän kysymykseen vastauksia. Alakysymys on kytköksissä pääkysymykseen ja luo syvyyttä tarkastella Euroopan unionin

kyberturvallisuustoimijuuden rakenteita ja toisaalta samankaltaisuuksia sen perinteiseen turvallisuuspoliittiseen toimijuuteen.

Tutkielmassa on vahvaa teoriaohjaavuutta, sillä hyödynnän EU:n kyberturvallisuuden tarkastelussa kriittisen turvallisuustutkimuksen teoretisointia ja etenkin ’Pariisin koulukunnan’ suuntausta tarkastella turvattomuuden politiikan elementtejä. Lisäksi käytän aineiston analyysin menetelmänä kriittisen diskurssianalyysin teoretisointia, joka mahdollistaa vallan ja diskurssin suhteen tarkastelun. Vallan paikantuminen diskurssin takana avaa tulkintaa myös turvattomuuden politiikan elementtien tarkastelulle turvallisuuden ollessa yksi vallankäytön muodoista (Aradau ja van Munster 2016, 107).

Tutkielmani metodologisia lähtökohtia havainnoidessani, huomaan tutkijana olevani merkillisessä, mutta mahdollisuuksia luovassa tilanteessa, jossa omat arvoni sekä hyväksyvät että kritisoivat kriittisen turvallisuustutkimuksen katsantakulmaa. En halua väheksyä tämänhetkistä merkittävästi muuttunutta turvallisuuspoliittista tilannetta, jossa hybridi- ja kyberhyökkäysten määrä on enenevissä määrin lisääntynyt ja niitä käytetään todellisen sodan välineinä. Toisaalta haluan myös tuoda esiin asioiden toista puolta turvallisuuspolitiikassa, esimerkiksi sitä, kuinka Euroopan unioni turvallistaa uhkakuvamäärittelyllään, luo turvallisuuden kasvavilla menettelyillä turvattomuutta sekä ylläpitää myös kyberturvallisuuden piirissä omaa valta-asemaansa asiantuntijavallan turvin. Nämä ovat seikkoja, joita haluan tutkia, mutta samalla pidän mielessäni realistisemman turvallisuuspoliittisen näkökulman.

1.2. Tutkielman rakenne

Johdannossa olen esitellyt tiivistetysti kyberturvallisuuden keskeistä sanastoa ja luonut ymmärrystä sille, mitä kyberturvallisuudella ja -toimintaympäristöllä tarkoitetaan. Seuraavassa luvussa kaksi siirryn tarkastelemaan Euroopan unionin kyberturvallisuusinfrastruktuuria, joka pohjautuu vahvasti unionin turvallisuustoimijuudelle. Pyrin toisessa luvussa kuvaamaan myös EU:n haasteita ja keskeisiä kehityksen paikkoja kyberturvallisuuden rakentamiseksi ja ylläpitämiseksi.

Luvussa kolme paneudun kriittisen turvallisuustutkimuksen suuntauksiin, joista keskityn tarkastelemaan niin kutsutun ’Pariisin koulukunnan’ teoretisointia. Pohjustan kriittisen turvallisuustutkimuksen suuntauksia luvun kolme alussa lyhyesti kertomalla kriittisestä

teoriasta. Tämän jälkeen tarkastelen ensiksi eurooppalaisia kriittisen turvallisuustutkimuksen suuntauksia, ja viimeisessä luvussa keskityn tarkastelemaan ’Pariisin koulukunnan’ turvattomuuden politiikkaa. Kriittinen turvallisuustutkimus on lähtökohtaisesti eurooppalaiskeskeistä, ja koulukuntamäärittelyt väljiä. Tutkielmassa valittujen painotusten selkeyttämiseksi käytän termiä ’Pariisin koulukunta’, vaikka painotan kriittisen turvallisuustutkimuksen suuntausten väljyyttä.

Seuraavassa luvussa neljä esittelen tutkielmassa käytettävät metodit sekä aineiston. Esittelen ensiksi tutkimusaineiston analyysin vaiheet, kriittisen diskurssianalyysin teoretisointia sekä työkaluja, joita hyödynnän aineiston analyysissä. Esittelen myös turvattomuuden politiikan elementit, joiden paikantamista hyödynnän jatkoanalyysissä. Tämän jälkeen esittelen tutkielman aineistokappaleet, joista kolme on dokumentteja ja kaksi tilastoaineistokappaleita. Lopuksi käyn läpi vielä sen, miten käsittelen tutkimusaineistoani.

Luvut viisi, kuusi ja seitsemän ovat aineiston analyysilukuja. Luku viisi pohjustaa lukua kuusi keskittyen dokumenttiaineiston sekä tilastoaineistokappaleiden purkamiseen kriittisen diskurssianalyysin sekä tulkinnan keinoin. Luvussa viisi tuon esille dokumenttiaineistosta poimittuja keskeisiä kohtia ja tarkastelen etenkin tekstin ja kontekstin suhdetta sekä pyrin paikantamaan vallan ilmentymistä diskurssin takana. Tilastoaineistokappaleet ovat haastattelututkimuksena koottuja tilastoja Euroopan unionin kansalaisten mieltymyksistä ja tavoista. Tilastoaineistokappaleiden kysymyksiä voi analysoida diskurssin ja vallan näkökulmasta, kun taas tilastotuloksia voi analysoida tulkinnan ja vertailun keinoin.

Luvussa kuusi jätän tilastoaineiston hetkeksi sivuun ja jatkan analyysiä etsimällä dokumenttiaineistosta löytyviä hegemonisia diskursseja. Hegemoniset diskurssit ovat suuria, mutta eivät kaikista ilmeisimpiä temaattisia diskursseja, joita muut aineiston diskurssit tukevat (Jokinen ja Juhlia 1991, 69). Edellisessä luvussa viisi tehdyt havainnot vallan paikantumisesta diskurssin takaa auttavat hegemonisten diskurssien löytämisessä.

Viimeisessä aineistoanalyysiluvussa seitsemän analysoin aineistosta löytyviä turvattomuuden politiikan elementtejä. Tässä luvussa tuon yhteen sekä dokumenttiaineiston hegemoniset diskurssit että tilastoaineistokappaleiden tulkinnan tulokset. Määrittelen tarkasteltavat turvattomuuden politiikan elementit aiemmassa

luvussa neljä, ja pyrin tässä viimeisessä analyysiluvussa tuomaan esille aineistosta löytyviä yhtymäkohtia näihin elementteihin. Esittämäni turvattomuuden politiikan elementit eivät ole poissulkevia, eikä niitä tulisi ymmärtää liian ehdottomina.

Lopuksi kokoan yhteen analyysiluvuissa tekemiäni havaintoja ja pyrin kokoamaan yhteen vastauksen tutkimuskysymyksilleni. Johtopäätösluvussa tuon esille myös tulkinnan sudenkuppia tutkielmassani sekä esitän jatkokysymyksiä, joita tutkielman tuottamisprosessi on kirjoittajassa herättänyt.

2. Euroopan unionin kyberturvallisuuden ulottuvuudet

Tässä luvussa käsittelen Euroopan unionia kyberturvallisuustoimijana. Luku toimii pohjustavana kirjallisuuskatsauksena aineistonanalyysille. Euroopan unionin kyberturvallisuutta ja sen hallintaa (governance) on 2020-luvulle tultaessa tutkittu yllättävän vähän. Toisaalta tutkijoiden näkökulmat ovat hyvin monipuolisia, ja EU:n kyberturvallisuutta on tarkasteltu niin lainsäädännön, hallintoteorioiden kuin neorealistisempien näkökulmien kautta.

Käsittelen luvun alussa lyhyesti Euroopan unionia turvallisuustoimijana, mikä toimii pohjustavana tekijänä kyberturvallisuustoimijuuden ymmärtämiseksi. Tämän jälkeen käyn läpi kyberturvallisuuspolitiikan esillemarssia EU:n turvallisuuskontekstissa sekä viimeisessä alaluvussa syvennyn tarkastelemaan unionin kyberturvallisuuspolitiikan kolmea keskeistä ulottuvuutta.

2.1. Euroopan unioni turvallisuustoimijana

Euroopan unioni on tunnustettu kompleksiseksi toimijaksi turvallisuuden alalla (Sperling ja Webber 2019, 228). Kompleksisuudella viitataan EU:n ainutlaatuisuuteen kansainvälisenä turvallisuustoimijana, jollaisena sillä on valtaa sekä itsenäisenä toimijana nauttiessaan jäsenvaltioiden suosiota, mutta samalla sen jäsenvaltiot ovat omia turvallisuustoimijoitaan suvereniteettinsa turvin. EU:n kompleksisuuden kuvaa lisää se, että se pyrkii vastaamaan useisiin turvallisuusuhkiin samanaikaisesti laajan ja monipuolisen menettelytapapaletin avulla (emt). Vastaamalla turvallisuusuhkiin se pyrkii tuottamaan ja asettamaan yhteisiä turvallisuuspoliittisia raameja toiminnalle. Lisäksi EU:n pyrkimyksille kansainvälisesti tunnustettuna turvallisuuspoliittisena toimijana on asetettu aivan erityinen normatiivinen leima (Manners 2002).

Yhteinen ulko- ja turvallisuuspolitiikka (YUTP, alk. engl. Common Foreign and Security Policy, CFSP) toimii EU:n turvallisuuspolitiikan pohjana. Yhteinen ulko- ja turvallisuuspolitiikka määriteltiin vuonna 1992 solmitussa Maastrichtin sopimuksessa yhdeksi kolmesta keskeisestä yhteistyön pilarista yhdessä Euroopan taloudellisen yhteisön sekä rikosasioissa tapahtuvan poliisi- ja lainsäädännöllisen yhteistyön edistämisen kanssa (Gegout 2017, 3). YUTP sekä myöhemmin määritelty yhteinen turvallisuus ja puolustuspolitiikka (YTPP, alk. engl. Common Security and Defence Policy, CSDP) ovat tehneet Euroopan unionista kansainvälisen turvallisuuspolitiikan

toimijan (Renard 2016, 13-14). Vaikka turvallisuuspolitiikka on selkeästi määritelty Euroopan unionin keskeiseksi kokonaisuudeksi, se ei silti tarkoita, että turvallisuuspolitiikan toteuttaminen käytännössä ja jäsenvaltioiden yhteistyön kautta onnistuisi mutkattomasti EU:lta. Turvallisuuspolitiikan toteuttamisen haasteet Euroopan unionissa liittyvät pitkälti jäsenvaltioiden halukkuuteen pitää kiinni itsemääräämisoikeudestaan turvallisuuspoliittisissa asioissa, mikä tekee haasteelliseksi yhteisen päätöksenteon (Gegout 2017, 3-4). Schimmelfennigin (2003) mukaan turvallisuuspolitiikassa ennen kaikkea luottamus, ryhmäidentiteetti sekä sosiaalinen oppiminen määrittelevät sen, ryhtyykö valtio yhteistyöhön ja kenen kanssa. Luottamuksella saavutetaan parempaa yhteistyötä kuin painostuksella, mutta silti luottamuksen rakentaminen turvallisuuspolitiikassa jäsenvaltioidensa kesken tuntuu olevan EU:lle haasteellista.

Haasteistaan huolimatta, se mitä EU on kyennyt turvallisuustoimijana tekemään on identifioimaan uhkia ja sen kautta jopa turvallistamaan tiettyjä aiheita kuten terrorismin, maahanmuuton, energiantuotannon, terveyden, ilmastonmuutoksen sekä kybertoimintaympäristön. Tämä herättää kysymyksen siitä, pystyykö EU muotoilemaan jäsenvaltioidensa ymmärryksiä siitä, mikä koetaan turvallisuusuhkana (Sperling ja Webber 2019, 232)? Onko silloin kyse kollektiivisesta turvallistamisesta? Samalla edellä esitetyt turvallisuuspolitiikan kentälle nousseet aiheet ovat yhä useammin valtioiden rajat ylittäviä ongelmia, jolloin valtioiden on tukeuduttava ylikansalliseen päätöksentekoinstituutioon kuten EU:hun, Natoon tai Yhdistyneisiin Kansakuntiin (emt 2019, 232). Kybertoimintaympäristö on oiva esimerkki turvallisuuspolitiikkaan kuuluvasta kokonaisuudesta, joka omaa sekä ylikansallisen että hallitsemattoman luonteen.

Euroopan unionin uudet avaukset turvallisuuspolitiikassa ovat mahdollisia, koska EU pyrkii saavuttamaan legitimiteetin asiantuntijatietoon nojaamalla (Egeberg ja Trondal 2917, 677). EU tarvitsee jäsenvaltioidensa ja kansalaisten oikeutuksen toimilleen, mutta se ei voi saavuttaa sitä edustuksellisen demokratian kautta kaikissa instituutioissaan (Euroopan parlamentti on ainoa poikkeus) (Schmidt 2013). EU luottaa vahvasti tieteellisesti tuotettuun asiantuntijatietoon (Pérez-Durán ja Bravo-Laguna 2019, 973), joka muodostaa sille parhaat mahdolliset ratkaisut sekä käytänteet päätöksentekotilanteissa (Egeberg ja Trondal 2917, 677). Tällä tavoin se pystyy

oikeuttamaan toimintansa valtaapitävänä organisaationa ja lisäämään toimivaltaansa turvallisuuspolitiikan uusillakin aloilla esimerkiksi kyberturvallisuuspolitiikassa.

2.2. Kyberturvallisuuspolitiikan esillemarssi EU:n turvallisuuskontekstissa

EU:n kyberturvallisuuspolitiikkaa on luotu sekä erityisten tapahtumien että pidempiaikaisten trendien saattelemana (Christou 2019, 282). Tapahtumista merkittävämpiä ovat olleet Virossa 2007 tapahtuneet laajat tietomurrot valtion infrastruktuureihin kuten myös kyberhyökkäykset ja -häirintätapaukset EU:n instituutioihin (Benincasa 2021, 40, 49). Yksittäiset kyberhyökkäykset ovat herätelleet EU:ta keksimään nopeitakin *ad hoc* -ratkaisuja kyberturvallisuuden takaamiseksi (Carrapico ja Farrand 2020, 1111). Kyberturvallisuus on nopeasti kehittynyt EU:ssa pienistä käytännönläheisistä ratkaisuista suureksi poikkihallinnolliseksi turvallisuuspoliittiseksi kokonaisuudeksi, mikä tekee siitä myös osatekijän EU integraation syventämispyrkimyksissä (emt.).

EU luo omaa kyberturvallisuuspolitiikkaa vaiheittain ja pehmeästi. Se on päässyt laajentamaan vaikutusvaltaansa erityisesti niillä politiikka-aloilla, joissa kyberturvallisuuteen liittyvät uhat ovat käyneet ilmeisiksi kuten kyberrikollisuus ja Euroopan sisämarkkinat. Sen sijaan yhteisen turvallisuus- ja puolustuspolitiikan alle lukeutuvan kyberpuolustuksen luominen on yhä vaiheessa, juuri vapaaehtoisuuteen perustuvan yhteistyön vuoksi (Christou 2019, 291).

Carrapico ja Farrand (2020, 1115) argumentoivat, että kyberturvallisuuden alalla Euroopan unioni ei ole noudattanut mitään tiettyä turvallisuusfilosofiaa, vaan sen motiivit kyberturvallisuusvalmiuksien kehittämiseksi ovat olleet alun perin täysin taloudelliset. Christou (2019, 282-283) jakaa tämän käsityksen, sillä jo 1990-luvulla Euroopan taloudellinen yhteisö tunnusti tarpeen verkko- ja informaatioturvallisuuden parantamiselle yhteisten sisämarkkinoiden eteenpäin viemiseksi (Bangemann -raportti 1994; Carrapico ja Barrinha 2017, 1259).

Historiallisesti kolme elementtiä ovat kiihdyttäneet EU:n kyberturvallisuuspolitiikan institutionalisointia ja käytänteiden juurruttamista. Ensimmäinen on ollut käsitys siitä, että kyberrikollisuus on lisääntymässä, toisena elementtinä on ollut vastaaminen lisääntyneeseen internetin ja digitaalisten palveluiden käyttöön, sekä kolmantena tekijänä

reagointi kyberhyökkäyksiin ja niiden vaikutukset kohdemaahan (Carrapico ja Barrinha 2017, 1265). Kyberturvallisuuden tietoisuuden lisääntyminen erityisesti kansallisella tasolla EU-maissa on edesauttanut yhteiseurooppalaisen kyberturvallisuuden ja etenkin sen käytäntöjen muodostumista (emt). Merkittävänä tulisi pitää myös sitä, että Euroopan unioni näkee terrorismin lisäksi kyberuhat (kyberhyökkäykset ja kyberrikollisuus) sekä sisäisen turvallisuuden että ulkoisen turvallisuuden uhkina (Renard 2016, 11).

2010-luvulla lisääntynyt internetin ja digitaalisten palveluiden käyttö kiihdytti EU:n kiinnostusta muuttuvaan turvallisuusympäristöön. Vuonna 2013 Euroopan unioni julkaisi kyberturvallisuusstrategiansa (Euroopan komissio 2013) ja sitä seurasivat Euroopan turvallisuusagenda 2015 (Euroopan komissio 2015) verkko- ja informaatiojärjestelmien direktiivi 2016 (NIS, nykyään kutsutaan myös verkko- ja informaatioturvallisuusdirektiiviksi) (ENISA 2022), Yhteinen kehys hybridiuhkien torjumiseksi: Euroopan unionin toimet (Euroopan komissio 2016), EU:n globaalistrategia (EU:n ulkosuhdehallinto 2016) sekä sopimus sopimusluonteisesta julkisen ja yksityisen sektorin kumppanuudesta 2016 (alk. engl. contractual Public Private Partnership, cPPP) (ECSO 2022). Viimeisimmäksi mainittua sopimusta julkisen ja yksityisen sektorin kumppanuudesta on avattava tarkastelemalla yksityisen sektorin roolia EU:n kyberturvallisuuspolitiikan tekemisessä.

Yksityinen sektori on keskeinen toimija EU:n kyberturvallisuuspolitiikassa suhteessa EU-instituutioihin sekä jäsenvaltioihin, ja yksityisen puolen toimijoita pidetäänkin agendan määrittelijöinä, jotka nostavat esille esimerkiksi tiettyjä toiminnan trendejä kybertoimintaympäristössä (Carrapico ja Barrinha 2017, 1265). Yksityinen sektori myös omistaa ja operoi suurinta osaa verkko- ja informaatiojärjestelmistä tehden yksityisen ja julkisen sektorin yhteistyöstä ensiarvoisen tärkeää (Benincasa 2021, 49; Wessel 2015, 410), mikäli julkinen sektori haluaa asettaa jonkinlaisia turvallisuusraameja toiminnalle kyberulottuvuudessa. Yksityisen sektorin taloudellisten toimijoiden tulisi olla kiinnostuneita myös EU:n kyberturvallisuustoimintavalmiuksien kehittämisestä, sillä EU:n kehitellessä sisämarkkinoitaan digitaalisiksi (EU Digital Single Market) (Benincasa 2021, 39), kyberhyökkäykset voivat olla uhka myös yksityisen puolen toimijoille etenkin liikevoittoja mietittäessä.

Yksityisen ja julkisen puolen (EU) yhteistyössä voidaan puhua vertikaalisesta yhteistyöstä, mutta samalla korostuu myös yksityisen puolen toimijoiden välinen

keskinäinen yhteistyö, joka puolestaan on horisontaalista yhteistyötä (Carrapico ja Barrinha 2017, 1263). ENISA eli Euroopan unionin kyberturvallisuusvirasto (2015) näkee keskeisenä, että yksityisen sektorin toimijat pystyisivät jakamaan tietoa keskenään kybertoimintaympäristössä toimimisesta ja kehittämään yhdessä keinoja kyberturvallisuuden parantamiseksi. Yksityisellä puolella yritysten kyberturvallisuusvalmiuksien taso kuitenkin vaihtelee (Carrapico ja Barrinha 2017, 1265), ja tiukemman yhteistyön esteenä tuntuu olevan myös yrityskilpailu (emt.; Giacomello 2014).

CPPP -sopimuksen mukaisia julkisen ja yksityisen sektorin välisiä kumppanuuksia on solmittu laajasti EU:n kyberturvallisuuden eri politiikka-aloilla. EU:n yhteistyö yksityisen sektorin kanssa pitää kuitenkin sisällään omat haasteensa. Yksityisen ja julkisen sektorin tarpeet ja toiveet toistensa toiminnasta eivät aina kohtaa (Carrapico ja Barrinha 2017, 1266). Julkisen sektori haluaa priorisoida turvallisuusaspektia, joskaan se ei halua antaa liikaa vastuuta yksityisen sektorin toimijoille kansalaisten turvallisuuden takaamiseksi (Dunn Cavelty ja Suter 2009, 181). Samalla kun julkisella sektorilla on vain vähän tarjottavaa yksityiselle sektorille, yksityisellä sektorilla on myös omat ennakkoluulonsa syvemmän luottamuksen rakentamisen suhteen. Keskinäisen luottamuksen rakentaminen kumppanien välillä vaatisi laajaa tietojen vaihtoa puolin ja toisin, mutta usein yksityinen puoli pelkää tietoturvaloukkauksia järjestelmiinsä, mikäli he jakavat laajemmin tietoa verkko- ja informaatiojärjestelmistään (Bossong ja Wagner 2016, 272-237). Bossongin ja Wagnerin (2016, 237) mukaan haasteet julkisen ja yksityisen sektorin kumppanuuksissa ovat johtaneet siihen, että kumppanuudesta on siirrytty enemmin kohti pakollista julkista sääntelyä, jonka alla yksityisen sektorin toimijoiden on ilmoitettava heihin kohdistuneista kybertapauksista (esim. kybervaikuttaminen, -rikos, -hyökkäys, tietomurto).

EU:n yksityisen sektorin kumppanuuksien lisäksi jäsenvaltioilla on keskeinen rooli unionin kyberturvallisuusvalmiuksien kehittämisen ja ylläpitämisen kannalta. Myös jäsenvaltioiden kohdalla voidaan puhua vertikaalisesta ja horisontaalisesta yhteistyöstä, sillä jäsenvaltiot osallistuvat EU:n kyberturvallisuustoimintaan vertikaalisen yhteistyön nimissä, mutta EU haluaa painottaa myös horisontaalista yhteistyötä jäsenvaltioiden välillä EU:n kokonaisvaltaisen kyberturvallisuuden vahvistamiseksi (Carrapico ja Barrinha 2017, 1264). Jäsenvaltiot tuntuvat jakavan samat uhkakuvat heihin kohdistuvista mahdollisista kyberuhista ja tunnustavat niiden ylikansallisen luonteen

(emt. 2017, 1266-1267), mutta ne eivät jaa samoja ratkaisuvaihtoehtoja uhkien torjumiseksi tai ylipäänsä jaa samanlaista käsitystä siitä, mitä turvallisuus tässä yhteydessä tarkoittaa. Tämä johtuu etenkin siitä, että jäsenvaltioiden kybertoimintavalmiudet voivat olla täysin eri tasoilla, minkä lisäksi turvallisuuspolitiikkaan kuuluva kyberturvallisuus koetaan kansallisesti herkäksi aiheeksi, ja luottamusta valtioiden välillä on näissä kysymyksissä vaikea rakentaa (emt. 2017, 1263; Christou 2019, 280). Kyberturvallisuuspolitiikan tiiviimpään toteuttamiseen pätevät siis samankaltaiset haasteet, kuin kollektiivisen turvallisuuspolitiikan toteuttamiseen yleisestikin EU:ssa, kun jäsenvaltiot haluavat pitää kiinni itsemääräämisoikeudestaan turvallisuuspoliittisissa asioissa (Gegout 2017, 3-4). Jäsenvaltiot ovat siis epäluuloisia sekä Euroopan unionia että toisia jäsenvaltioita kohtaan turvallisuuspoliittisissa kysymyksissä.

Euroopan unionin kyberturvallisuuspolitiikassa korostuu moninaisten alojen sekä toimijoiden joukko, joka muodostaa kompleksisen toiminnan verkoston kyberturvallisuuden kehittämiseksi ja ylläpitämiseksi. Toimintaperiaatteita luodaan edelleen käytännön tapahtumien kautta, mutta kyberturvallisuus on vakiinnuttanut asemansa EU:n turvallisuuspoliittisella kartalla, mikä näkyy kasvavissa määrin EU:n hallintokoneiston tuottamissa, jäsenvaltioiden toimintaa ohjaavissa strategioiden, kommunikeoiden sekä direktiivien määrässä.

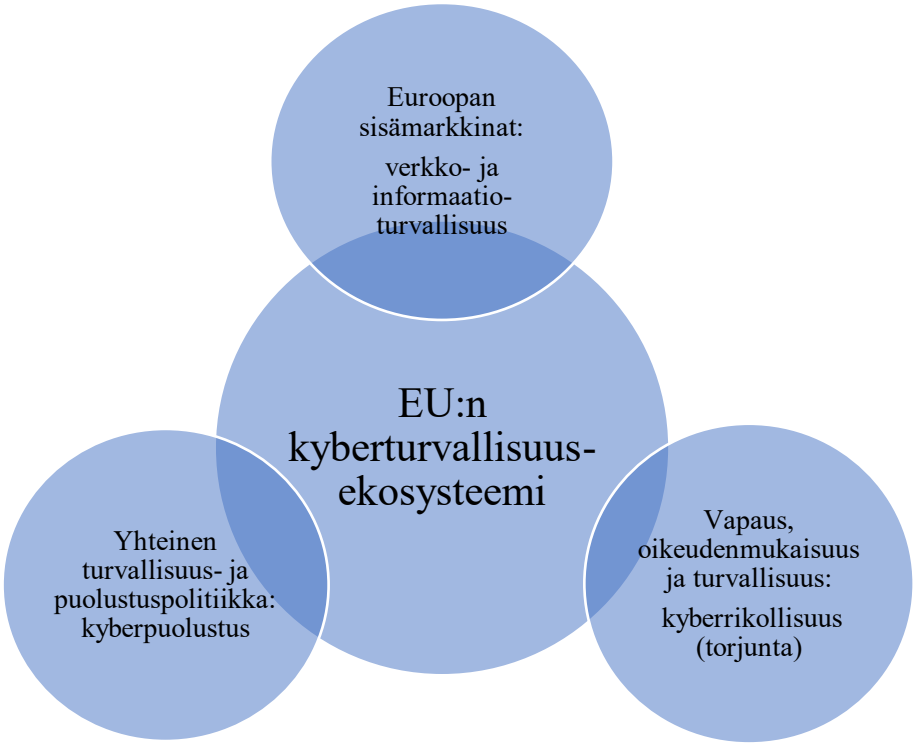
Seuraavassa alaluvussa paneudun vielä tarkemmin Euroopan unionin kyberturvallisuuspolitiikan ulottuvuuksiin. Kyse on eri aihepiireistä, jotka ovat havaittavissa EU:n harjoittamasta kyberturvallisuuspolitiikasta. Kutsun kokonaisuutta EU:n omin sanoin kyberturvallisuusekosysteemiksi.

2.3. Euroopan unionin kyberturvallisuusekosysteemi

Aiemman alaluvun perusteella on identifioitavissa kolme EU:lle keskeistä politiikkaulottuvuutta, joissa kyberturvallisuuden harjoittaminen on olennaista. Näissä kolmessa ulottuvuudessa harjoitettavat käytännön toimet ottavat kuitenkin toisistaan eriäviä muotoja, vaikka uhkakuvat olisivat osittain päällekkäisiä.

Esittelen George Christoun (2019) mallinnukseen perustuen Euroopan unionin kyberturvallisuusekosysteemin kolme keskeisintä ulottuvuutta ja niissä harjoitettavat

kybertoimet. Ulottuvuudet kytkeytyvät keskenään toisiinsa toimien kansallisella, paikallisella sekä globaalilla tasolla, ja auttavat hahmottamaan EU:n kannalta kriittisimmät alueet kyberturvallisuuden toteuttamiselle (emt. 2019, 279). Christou ei käytä ekosysteemi -sanaa omassa jaottelussaan, vaan ekosysteemi sana on poimittu EU:n turvallisuusunionistrategiasta (2020, 10). Lisäksi Christou on mallintanut kolmea ulottuvuutta sanoin, ei kuvin, joten oheinen kuvio 1. on tässä tutkielmassa omaa tulkintaani.



Kuvio 1. EU:n kyberturvallisuusekosysteemin ulottuvuudet ja niissä harjoitettavat kybertoimet (mukaillen Christou 2019).

2.3.1. Euroopan (digitaaliset) sisämarkkinat: verkko- ja informaatioturvallisuus

EU:n tuorein kyberturvallisuusstrategia (2020) mainitsee sisämarkkinoiden suojelun tärkeänä kriittisenä infrastruktuurina unionin toiminnan edellytyksille. Vuonna 2016 annettu direktiivi verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi (Network and Information Systems (NIS) Directive) on ensisijaisesti suunnattu juuri toimimaan yhteisten sisämarkkinoiden kyberturvallisuuden ohjenuorana (EU kyberturvallisuusstrategia 2020, 5). NIS saa siis mandaattinsa sisämarkkinoilta (Christou

2019, 291) ja siten kaikki sen raameissa toteutettu toiminta pyrkii suojelemaan ja vahvistamaan digitaalisten sisämarkkinoiden resilienssiä.

Euroopan digitaaliset sisämarkkinat on tässä yhteydessä erotettu omaksi kokonaisuudekseen kyberrikollisuuden torjuntaa toteuttavasta vapauden, oikeudenmukaisuuden ja turvallisuuden -ulottuvuudesta, sillä vaikka kyberrikollisuus on sisämarkkinoille aivan yhtä olennainen uhka, tärkeää olisi myös vahvistaa ja ylläpitää kansalaisten luottamusta käyttämiinsä teknologioihin ja digitaalisiin palveluihin (Wessel 2015, 403) niin tietojärjestelmien valvonnan kuin kansalaisten koulutuksen avulla. EU on siis ymmärtänyt, että yksilötasolla tietoisuus tietoturvariskeistä ja teknologian oikeaoppinen käyttö suojaavat myös kaikista parhaiten digitaalisia sisämarkkinoita.

Tämä ulottuvuus kuvaa myös sitä, että kyberuhkia ei voida supistaa vain ja ainoastaan kyberrikollisuuteen (Christou 2019, 284), vaikka se edelleen onkin EU:lle yksi merkittävä uhka. Esimerkiksi kaikista palvelunestohyökkäyksistä ei puhuta kyberrikoksina, koska niin tekijä kuin teon motiivit saattavat olla hämärän peitossa. Viron kriittiseen infrastruktuuriin vuonna 2007 kohdistunut laaja kyberhyökkäysten sarja on oiva esimerkki kokonaiseen valtioon kohdistuvasta hyökkäyksestä, jossa tekijää voidaan vahvasti epäillä toisen (vihamielisen) valtion toimijaksi, vaikka tekijää ei ole voitu varmuudella vahvistaa (McGuinness 2017).

Kenties kaikista keskeisin toimija EU:n kyberturvallisuuspaletissa on Euroopan verkko- ja tietoturvavirasto (ENISA), jota nykyisin myös Euroopan Unionin kyberturvallisuusvirastoksi kutsutaan. ENISA perustettiin 2004 tuottamaan tietoa ja ymmärrystä tietoturvariskeistä (Euroopan parlamentti ja Eurooppa-neuvosto 2004). 2010 ENISA:n rooli laajeni löytämään ratkaisuja kyberturvallisuusresilienssin kehittämiseksi, parantamaan alan yhteistyötä eri toimijoiden välillä sekä luomaan sääntöleviä mekanismeja eurooppalaisille toimijoille kyberulottuvuudessa (Christou 2019, 285). EU:n kyberturvallisuusvirasto koordinoi lisäksi kansalliselle tasolle perustettujen CERT -yksiköiden (Computer Emergency Response Teams) toimintaa, joiden tehtävänä on jäsenvaltioiden tasolla varoittaa häiriöistä ja tietoturvariskeistä sekä toimia kyberhäiriötilanteissa (Carrapico ja Farrand 2020, 1116). ENISA:n toiminta perustuu siis nimenomaan tiedontuottamiseen ja CERT-yksiköiden kautta tietoturvariskeistä ilmoittamiseen kansalaisille. Tätä kautta parannetaan kansalaisten tietoisuutta ja varautumista heidän omissa teknologisissa laitteissaan piileviin tietoturva-aukkoihin.

ENISA:n yhä korostetummasta roolista EU:n sisällä kielii se, että vuonna 2015 ENISA:n vuosittainen budjetti oli 10 miljoonaa euroa kun vuonna 2020 se oli jo lähes 20 miljoonaa euroa (Merino 2021). ENISA:n toimintaa rahoittavat Euroopan komission lisäksi Euroopan talousalueeseen (EEA) kuuluvat Islanti, Liechtenstein, Norja ja Sveitsi (emt.).

Digitaalisten palveluiden ja sosiaalisen median käytön lisääntyessä kansalaisten keskuudessa EU on ottanut aktiivisemmin huomioon myös käyttäjän tietosuojaan liittyvät seikat (Christou 2019, 285). Tällä tavoin Euroopan unioni on pystynyt siirtymään yhä lähemmäksi yksilötasoa huomioiden yksilöön kohdistuvat informaatio- ja kommunikaatioverkoissa piilevät riskit. EU:n sääntö- ja normiverkosto tässä ulottuvuudessa ei ole läheskään valmis, mutta se on saanut kyberturvallisuuspolitiikassa tapahtuvan orastavan jäsenmaiden välisen yhteistyön käynnistettyä parhaiten juuri tässä ulottuvuudessa (emt. 2019, 286). Merkittävimpänä EU lainsäädäntönä on pidettävä toukokuussa 2018 voimaan tullutta yleistä tietosuoja-asetusta (alk. engl. General Data Protection Regulation, GDPR), joka asettaa vaatimukset organisaatioille ja yrityksille henkilötietojen keräämiseen, hallinnointiin ja säilytykseen (Europa 2021). Tämä takaa yksilölle paremman tiedon siitä, milloin yritys tai organisaatio käsittelee hänen henkilötietojaan ja yksilöltä kysytään myös suostumusta aina kun henkilötietoja pyydetään luovuttamaan. Tällä tavoin varmistetaan, että yksilön tietoja käsitellään lainmukaisesti, ne on kerätty laillista tarkoitusta varten ja niitä käsitellään vain ja ainoastaan tätä tarkoitusta varten (emt.).

2.3.2. Vapaus, oikeudenmukaisuus ja turvallisuus: kyberrikollisuus

Vapauden, oikeudenmukaisuuden ja turvallisuuden ulottuvuus kyberturvallisuushallinnossa viittaa EU:n tekemään asetus-, direktiivi- ja lainsäädäntötyöhön kyberturvallisuuden parantamiseksi (Christou 2019, 280). Euroopan Unioni on toiminut aktiivisimmin etenkin kyberrikollisuuden selvittämisen ja kitkemisen mahdollistamiseksi, ja se on merkittävä prioriteetti sille edelleen (emt. 2019, 288). Kyberturvallisuuden toteuttamiseen kytkeytyy myös EU:n normatiivisen luonteen esille tuominen, jota korostetaan aktiivisesti asetus-, direktiivi- ja lainsäädäntötyössä. Esimerkiksi vuoden 2013 EU:n kyberturvallisuusstrategiassa todetaan, että ”[p]erusoikeuksia, demokratiaa ja oikeusvaltioperiaatetta on suojeltava myös kyberavaruudessa” (Euroopan komissio 2013). Vapaus ja oikeudenmukaisuus ovat

EU:lle tärkeitä arvoja, joita muun muassa perusoikeuksien, demokratian ja oikeusvaltioperiaatteen suojelulla toteutetaan.

Kyberrikollisuutta kuvaillaan niin rajat ylittäväksi kuin alat ylittäväksi rikollisuudeksi, jossa EU joutuu yhdistelemään sekä sisä- että ulkopolitiikan elementtejä keskenään (Wessel 2015, 404, 405). Kyberrikollisuus ei tapahdu ainoastaan valtion rajojen sisällä vaan on usein paikasta riippumatonta rikollisuutta, joka kytkeytyy muuhun rikollisuuteen kuten terrorismiin, järjestäytyneeseen rikollisuuteen ja laittomaan maahanmuuttoon. Euroopan unionin sisällä on perustettu hallintoelimiä kyberrikollisuuden kitkemiseksi sekä parantamaan nimenomaan kansainvälistä koordinaatiota ja yhteistyötä rajat ylittävän kyberrikollisuuden selvittämiseksi (Christou 2019, 280). Europolin yhteydessä toimiva European Cybercrime Centre (EC3) (Carrapico ja Barrinha 2017, 1263) sekä sen alla toimiva Joint Cybercrime Action Taskforce (J-CAT) (Christou 2018) ovat merkittävimmät toimielimet kyberrikollisuuden torjunnassa. EC3 omaa samankaltaisen muodollisen rakenteen kuin useat muutkin EU instituutiot, kun taas J-CAT:n toimintaa on kuvailtu joustavan hallinnon toiminnaksi yksikön ollessa oman erityisen lainsäädännöllisen paletin alainen (Christou 2019, 292-293; 2018, 365). J-CAT:n kohtelu oman erityisen lainsäädännön alaisena toimijana tarjoaa sille joustavuutta ja nopeutta reagoida kybertoimintaympäristön nopeasti muuttuviin tilanteisiin ilman ylimääräisiä hallinnollisia tai laillisia esteitä (emt. 2019, 293). Tällainen lainsäädännön kiertäminen on poikkeuksellista EU:lle, ja herättää toki kysymyksiä hallinnon läpinäkyvyydestä ja tilivelvollisuudesta, vaikka toimintaa tehtäisiinkin kyberrikollisuuden torjunnan nimissä.

EU on kyberturvallisuuden lisäämiseksi ja ylläpitämiseksi ottanut käyttöön kaksihaaraisen toimintapaletin, jossa se pyrkii yhtä aikaa liittämään kyberturvallisuuden osaksi sen olemassa olevia kyvykkyyksiä eri sektoreilla, mutta samanaikaisesti se pyrkii pehmeän lainsäädännön instrumentein houkuttelemaan jäsenvaltiot ja muut toimijat toimeenpanemaan strategioissa määriteltyjä toimintaperiaatteita (Wessel 2015, 405). Kyberrikollisuuden torjunta tarjoaa tästä ilmeisen esimerkin, jossa kyberturvallisuutta institutionalisoidaan ja käytänteitä luodaan yhdenmukaisiksi EC3:n, J-CAT:n ja ENISA:n kaltaisten elinten kautta, kun taas CERT -toiminnan avulla pyritään osallistamaan jäsenvaltioita ja sitä kautta toteuttamaan yhteiseen kyberstrategiaan kirjattuja toiminnan tavoitteita. EU jakaa siis vastuutaan kyberturvallisuudessa aktiivisesti jäsenmaille sekä pyrkii itse koordinoimaan toimintaa johdonmukaisemmaksi.

Kyberrikollisuudesta puhuttaessa on lisäksi sivuttava aiheen lainsäädännöllistä puolta. Kyberrikollisuus asettaa aivan erityisiä haasteita perinteiselle rikoslainsäädännölle sekä rikostuomioistuinten käytänteille (Calderoni 2010, 340). Tähän liittyy erityisesti kyberrikollisuuden rajat ylittävä ja hallitsematon luonne sekä rikosten kirjo ja sidonnaisuus muihin rikoksiin. Kybertoimintaympäristö ei esimerkiksi istu perinteisen rikoslainsäädännön muottiin ilman suvereniteetin ja territoriaaliperiaatteen kriteereitä (emt. 2010, 341). Suomessa poliisi (2022) jakaa kyberrikokset erikseen tietoverkkoavusteisiin ja tietoverkkosidonnaisiin rikoksiin. Kyberrikosten kirjo on laaja, ja se voi olla niin yksityisen henkilön luottokorttitietojen varastamista, tietojärjestelmän tuhoavan viruksen asentamista, laittoman materiaalin kuten lapsipornografian levittämistä kuin laittomasti hankitun tietokoneohjelmiston myymistä (Calderoni 2010, 341). Kyberrikoksen selvittämistyötä hankaloittaa attribuutio-ongelma eli se, että tekijää ei voida paikantaa tai tunnistaa (Norilo 2021, 21-22). Mikäli tekijä tai tekijöiden joukko tunnistetaan, usein valtioiden erilaiset oikeudelliset käytänteet haastavoittavat heidän saamista oikeudelliseen vastuuseen teoistaan, jos kyseessä on rajat ylittävä kyberrikollinen toiminta (Turvallisuuskomitea 2018, 27). Euroopan neuvoston Budapestin sopimus koskien kyberrikollisuutta (alk. engl. Budapest Convention: The Council of Europe Convention on Cybercrime) on keskeisin kansainvälisesti sitova lainsäädännöllinen instrumentti, joka toimii sekä alan kansainvälisen yhteistyön runkona että tarjoaa ohjeistusta kansallisen lainsäädännön parantamiselle kyberrikollisuutta koskevissa asioissa (Wessel 2015, 418). Euroopan unionin jäsenvaltiot ovat Budapestin sopimuksessa mukana (emt.).

2.3.3. Euroopan yhteinen turvallisuus- ja puolustuspolitiikka: kyberpuolustus

EU:n päivitetyssä kyberpuolustuskehyksessä (2018) mainitaan kyberavaruuden olevan yksi viidestä sotilaallisten operaatioiden ulottuvuudesta yhdessä maa-, meri-, ilma- sekä avaruusulottuvuuksien kanssa (Eurooppa-neuvosto 2018). Huomionarvoista on kuitenkin se, että EU tähtää kyberpuolustuksella nimenomaan ulkoisten uhkien torjuntaan, kun muiden kyberturvallisuuden politiikkaulottuvuuksien kohdalla kyse on ensisijaisesti sisäisen turvallisuuden takaamisesta kuten sisämarkkinoiden ja kansalaisten suojelusta. EU:n kyberpuolustuskehyksessä (2018) mainitaan tavoitteita kyberpuolustuksen menetelmien kehittämiseksi. Jäsenvaltioiden koulutuksen ja menetelmien kehittäminen on yksi ensisijaisista tavoitteista, mutta kehyksessä mainitaan myös Nato yhteistyön tiivistäminen EU:n kyberpuolustuksen kasvattamiseksi. (emt.)

Yhteisen turvallisuus- ja puolustuspolitiikan ulottuvuus on haasteellisin ylikansallisen yhteistyön toteuttamisen kannalta (Christou 2019, 291). Vahva kansallisen turvallisuuden leima kyberturvallisuuden puolustusulottuvuudessa rajoittaa EU:n jäsenvaltioiden halukkuutta ylikansalliseen yhteistyöhön aiheen parissa sen vaatiessa esimerkiksi arkaluontoisten kansallista turvallisuutta koskevien tietojen luovuttamista. Samalla tässä ulottuvuudessa korostuu jäsenvaltioiden kyberturvallisuusvalmiuksien ja -osaamisen vaihteleva taso. (Carrapico ja Barrinha 2017, 1263.) EU on pyrkinyt suhtautumaan yhteistyön edistämiseen pehmittelevästi korostaen vapaaehtoista osallistumista esimerkiksi Euroopan Puolustusviraston (European Defence Agency, EDA) kyberturvallisuusharjoituksiin ja projekteihin (emt. 2017, 1266). EDA:n lisäksi EU:n ulkosuhdehallinto (EUH) on keskeisesti mukana EU:n kyberpuolustuskomponentin rakentamisessa (Christou 2019, 291).

Kybertoimintaympäristössä selkeä trendi valtiollisten toimijoiden keskuudessa on se, että omia kybertoimintakyvykkyyksiä kuten hyökkäys- tai puolustuskykyjä ei julkisesti paljasteta (Keinonen 2021). Samalla kyvykkyyksien mittaaminen itsessään on haasteellista, kukaan ulkopuolinen ei voi nähdä hyökkäykseen tai puolustukseen käytettyjä virtuaalisia aseita, minkä lisäksi niitä ei voida johdonmukaisesti laskea yhteen kuten esimerkiksi ydinaseet voidaan (Borghard ja Lonergan 2018). Kyseiset seikat haastavoittavat entisestään EU:n jäsenvaltioiden välisen yhteistyön tiivistämistä tässä ulottuvuudessa luottamuspulan vuoksi.

Miksi sitten Euroopan unioni ylipäänsä panostaa kyberpuolustukseen? Kybertoimintaympäristössä attribuutio-ongelmat johtavat usein siihen, että rangaistus ei ole toimiva mekanismi, eikä sillä ole edes pelotevaikutusta (alk. engl. *deterrence by punishment*) (Nye 2016/17, 56). Tämän vuoksi hyvin suunniteltu ja toteutettu puolustusjärjestelmä voi toimia parempana pelotteena tai esteenä vastapuolen hyökkääjälle (Benincasa, 2021, 46), koska hyökkääjällä on usein rajalliset ajalliset ja taloudelliset resurssit hyökkäyksen tekemiseen, ja kovan puolustusjärjestelmän kohdatessaan kustannushyötysuhde on heikko hyökkääjän kannalta (Nye 2016/17, 56). Toimivaksi kyberpuolustukseksi voidaan tulkita myös alueellisen yhteistyön ja kyberresilienssin rakentaminen (Benincasa 2021, 46), jolloin voidaan palata takaisin EU:n vahvuusalueille. Nye (2016/17, 56) näkee etenkin resilienssin eli kyvyn sopeutua sekä kyvyn palautua nopeasti kyberhäirinnän tai -hyökkäyksen jälkeen tärkeänä

kyberpuolustuksellisena mekanismina. Kyberresilienssi voi tarkoittaa niin sotilaallisen kyvykkyyksien kehittämistä ja harjoittamista, mutta se on myös yhtä olennaista yhteiskunnan kriittisen infrastruktuurin suojelemiseksi esimerkiksi huoltovarmuuden kehittämistä (emt.). EU:n kannalta kyberpuolustuksen voidaan siis tulkita tarkoittavan nimenomaan kyberresilienssin kehittämistä ja ylläpitämistä, jossa yhteiskunnan kriittisen infrastruktuurin suojelu on keskeisessä osassa.

EU:n ja Naton välistä yhteistyötä on puolestaan pyritty lisäämään muun muassa kolmannen osapuolen kautta. Vuonna 2016 julkaistu *Yhteinen kehys hybridiuhkien torjumiseksi: Euroopan unionin toimet* esitti hybridiuhkien torjunnan osaamiskeskuksen perustamista, joka toimisi tiiviisti yhdessä EU:n ja Naton kanssa. Kehyksessä mainitaan tiiviin yhteistyön hyötynä erityisesti eri näkökulmien esille tuominen esimerkiksi kyberpuolustuksesta ja kriisitoiminnasta (2016, 5-6). Euroopan hybridiuhkien torjunnan osaamiskeskus perustettiin vuonna 2017 yhteisellä EU:n ja Naton välisellä julistuksella (Hybrid CoE 2022). EU-Nato yhteistyön lisääminen on yksi erityisimmistä haasteista EU:n kollektiivisen kyberturvallisuuden kasvattamiselle jäsenmaiden jakaessa erilaisen suhtautumisen Natoon yhteistyökumppanina. Sen sijaan yhteistyötä voidaan tehdä yhteisten harjoitusten sekä tietotaidon kehittämisen parissa. Lisäksi EU ei velvoita, mutta kannustaa jäsenmaitaan osallistumaan Euroopan hybridiuhkien torjunnan osaamiskeskuksen toimintaan tehden jälleen kerran osallistumisesta vapaaehtoista.

Vaikka EU:lla riittää haasteita yhteisen turvallisuus- ja puolustuspolitiikan ulottuvuudessa etenkin kollektiivisen turvallisuuden rakentamiseksi, jäsenvaltioiden välillä on nähtävissä jossain määrin ainakin halukkuutta yhteiselle harjoittelulle sekä tietotaidon kehittämiselle. Lähes kaikki jäsenmaat ovat Euroopan hybridiuhkien torjunnan osaamiskeskuksen osallistujamaita (Hybrid CoE 2022) ja kyberresilienssikyvykkyyksiä kehitetään myös ENISA:n ja sen alaisten CERT-yksiköiden harjoitusten ja koulutusten avulla (Carrapico ja Farrand 2020, 1116). Euroopan unioni on kehittänyt toimivan kyberturvallisuuskehyksen (Benincasa 2021) pyrkien vastaamaan ja ennakoimaan kyberuhkia ja -heikkouksia monella politiikka-alalla. Nopeasti muuttuvassa turvallisuusympäristössä kyvykkyydet ja heikkoudet vaativat jatkuvaa uudelleen arviointia, ja EU pyrkii ainakin tarjoamaan parhaimmat mahdolliset työkalut tähän omille jäsenvaltioilleen koulutuksen ja harjoittelun avulla. Seuraavaksi siirryn eteenpäin Euroopan unionin kyberturvallisuuspolitiikasta ja keskityn tarkastelemaan tutkielmassani hyödyntämääni teoretisointia.

3. Teorialuku

Käytän tutkielmassani kriittisen turvallisuustutkimuksen turvallistamisen ja turvattomuuden teoretisointia. Seuraavissa alaluvuissa avaan ensinnäkin sitä, mitä kriittisyys tarkoittaa yhteiskuntatieteellisessä tutkimuksessa ja sen jälkeen tarkastelen kriittisen turvallisuustutkimuksen haaraa. Viimeisessä alaluvussa käsittelen 'Pariisin koulukuntaa', joka on keskittynyt tarkastelemaan turvattomuuden politiikan elementtejä.

3.1. Kriittisyyden juuret yhteiskuntatieteellisessä tutkimuksessa

Yhteiskuntatieteiden alalla kriittisyyden juuret löytyvät saksalaisen politiikan filosofian debateista ja etenkin Frankfurtin koulukunnasta. Koulukunnan suurnimien Max Horkheimerin ja Theodor Adornon kritiikki kapitalismin ylivoimaa vastaan sekä kokemukset totalitaristisesta hallinnosta saivat heidät suuntamaan tutkimuksensa valtavirran ilmiöitä vastaan (Roach 2016, 147). Koulukunta kritisoi Max Horkheimerin johdolla niin Karl Marxia kuin valistuksen ajan filosofeja luokkayhteiskunnan ja sen lieveilmiöiden synnyttämisestä (Abromeit 2018, 26). Vuonna 1937 julkaistussa julistuksessaan *Traditional and Critical Theory* Horkheimer ilmoitti, että on olemassa tarve uudelleen ajatella suunta, johon teoreettinen mallinnus on menossa. Julistus oli sekä kritiikki Euroopan älymystöpiireissä vallallaan ollutta uuskantilaista suuntausta kohtaan että pragmatismia, positivismia, fenomenologiaa ja sosiologian suuntauksia kohtaan. (Macdonald 2017, 511.)

Kriittisen teorian diskurssi yhdistelee empiriaa, käytäntöä ja normatiivisuutta pyrkien ymmärtämään hyväksikäytön, riistämisen ja sorron olosuhteita (Macdonald 2017, 514). Kriittisen teorian ilmentymänä on vapauttamisen ajatus, joka näkyy alan tutkijoiden halukkuudessa osoittaa sinne suuntaan, missä väärinkäytöstä tapahtuu (Roach 2016, 145-146). Huomionarvoista on se, että kriittinen teoria on lähtenyt elämään omaa elämäänsä vasta 1900-luvun viimeisinä vuosikymmeninä, ja kriittisen näkökulman omaavien tutkimustraditioiden määrä ovat suorastaan räjähtänyt 2000-luvulla, jolloin vanhoista käytänteistä halutaan pyristellä irti emansipatorisella tavalla (Macdonald 2017, 514).

Kriittisen teorian sijaan voidaan siis nykyään puhua monien kriittisten teorioiden diskursseista, joita yhdistää metateorian tasolla ajatus historian autenttisuudesta, jännitteinen konfliktinomainen tilanne vallan subjektin kanssa sekä halu sosiaaliseen ja

poliittiseen muutokseen ihmisten onnellisuuden ja oikeudenmukaisuuden nimissä (Macdonald 2017, 514). Historian autenttisuus oli tärkeää Max Horkheimerille, joka jakoi samanlaisen näkökannan Karl Marxin kanssa luokkajakoa vastaan, mutta ei pitänyt Marxin historianäkemystä *bourgeois*-luokan vallasta tarpeeksi valistuneena (Abromeit 2018, 29). Kriittisen teorian monet diskurssit ymmärtävät valtaa pitävän talousjärjestelmän myös kulttuuria hallitsevana kokonaisuutena, joka oikeuttaa tahtomattaan myös materialistiseen epätasa-arvoon (Gartman 2013, 131). Massakulttuurin aikakaudella kriittiset näkökulmat talousjärjestelmämme ylivaltaa kohtaan ovat nostaneet päätään (mm. Pierre Bourdieu). Kriittisen näkökulman kuvaillaan toimivan myös välikappaleena teorian ja empirian välissä. Jos tutkimuksen empiirinen virta keskittyy liikaa metodeihin ja tutkimuksen teknisiin ulottuvuuksiin, kriittinen näkökulma saattaa tutkijan näkemään jälleen teorian ja empirian välisen yhteyden (Guillaume 2013, 92).

Frankfurtin koulukunnalla ja positivismin jälkeisellä suuntauksella kansainvälisten suhteiden tutkimuksen parissa on eittämättä suuret vaikutukset kriittisen turvallisuustutkimuksen kehittymiseen (Mutimer 2016, 81). Ensimmäiset kriittisen turvallisuustutkimuksen pariin liitetyt tutkijat kuten Ken Booth, Michael Williams, Richard Wyn Jones ja Keith Krause osoittivat, kuinka turvallisuus oli konseptina muotoutunut statistiseksi ja sotilaallisesti suuntautuneeksi (CASE Collective 2006, 448). Turvallisuuden alle voitiin liittää muitakin tekijöitä kuin pelkkä sotilaallinen turvallisuus ulkoista uhkaa vastaan. Seuraavassa alaluvussa käsittelen kriittisen turvallisuustutkimuksen eurooppalaisia traditioita.

3.2. Eurooppalaisen kriittisen turvallisuustutkimuksen perinteet

Kriittinen turvallisuustutkimus (Critical Security Studies, CSS) on tutkimussuuntaus, joka yhdistelee politiikan tutkimuksen ja sosiologian elementtejä (Hendershot ja Mutimer 2018, 60). Kylmä sodan päättyminen 1990-luvulla tarjosi turvallisuustutkimuksen parissa tilaa uusille teoreettisille suuntauksille, kun poliittisen realismin teorioiden nähtiin tulleen tiensä päähän (Mutimer 2016, 82). Vahvasti eurooppalainen suuntaus ei halua lukeutua turvallisuustutkimuksen tai kansainvälisten suhteiden tutkimuksen alalajiksi, vaan suuntauksen tutkijat näkevät itsensä heterogeenisenä joukkona, joka tarkastelee turvallisuuden ilmiöitä monipuolisesti tavanomaisista menetelmistä ja näkökulmista poiketen (CASE Collective 2006).

Yhtenä kriittisen turvallisuustutkimuksen lähtökohtana on valtion roolin kriittinen tarkastelu turvallisuuskontekstien tuottajana (Vuori 2014, 26). Valtion sijaan suuntaus haluaa nostaa esiin yksilön turvallisuuden todellisena kohteena osoittaen, että on paljon paikallisia turvallisuuteen liittyviä ymmärryksiä, jotka länsimaisessa valtiokeskeisissä näkökulmissa jäävät huomioimatta (Buzan ja Hansen 2009, 200). Kriittisyys viittaa siis siihen, että tutkija pystyy tarkastelemaan konseptia eri tavalla, toisesta näkökulmasta kuin miten valtio, valtion päättäjä asiaa tarkastelisi (Guillaume 2013, 91-92).

Kriittinen turvallisuustutkimus haluaa sekä kyseenalaistaa ne kysymykset, joita turvallisuuteen liittyen esitetään, että vastaukset, joita niihin annetaan (Hendershot ja Mutimer 2018, 62). Kriittiseen turvallisuustutkimukseen liitetään usein myös vapauttamisen (emansipaation) leima. Tarkastelu pyritään suuntaamaan siihen kohteeseen, joka on aiemmin ollut turvallisuustutkimuksen piirissä näkymätön. Tämä normatiivinen lähestymistapa on etenkin ominaista niin kutsutulle ’Aberystwythin koulukunnalle’, joka näkee emansipaation todellisena turvallisuutena vallan ja järjestyksen sijaan. (CASE Collective 2006, 455-456.)

Vaikka kriittinen teoria vierastaa vahvasti ongelmanratkaisuteoretisointia, kriittiselle turvallisuustutkimukselle ongelmanratkaisu on tästä huolimatta olennainen (Vuori 2014, 10). Robert Coxin (1981, 128-129) määritelmän mukaan ongelmanratkaisuteorioita voi hyödyntää tilanteissa, joissa kaikkia tilannetta rajoittavia tekijöitä voidaan tarkastella tasapuolisesti, ja ratkaisu on siten löydettävissä. Erityisesti käytännön turvallisuuspolitiikassa on yhdisteltävä sekä ongelmanratkaisua että teoriaa (Vuori 2014, 10).

Kriittinen teoria ei ole ainoa kriittisen turvallisuustutkimuksen taustalla vaikuttava kansainvälisten suhteiden tutkimuksen suuntaus. Konstruktivismin teorialla ja erityisesti sen ydinajatuksella todellisuuden sosiaalisesta rakentumisesta on ollut vaikutusta kriittisen turvallisuustutkimuksen kehittymiseen (Buzan ja Hansen 2009, 199-200; Vuori 2014, 12-13.) Englantilaisen koulukunnan suuntaus kansainvälisten suhteiden teorioista on myös vaikuttanut osaltaan kriittisen turvallisuustutkimuksen kehitykseen tukien erityisesti ’Kööpenhaminan koulukunnan’ turvallistamisen teorian kehittelyä (CASE Collective 2006, 452.)

Kriittinen turvallisuustutkimus jaetaan helposti kolmeen eurooppalaiseen koulukuntaan: Kööpenhamina, Aberystwyth ja Pariisi (Vuori 2014, 27-28). Koulukunnat ovat muotoutuneet kaupunkien nimien mukaisesti sillä tutkimus on kehittynyt pääosin näiden kaupunkien yliopistoissa. ’Koulukunnat’ leimataan herkästi toistensa kilpailijoiksi ja ne erotellaan toisistaan kertomalla niiden erilaisista piirteistä (Bigo ja McCluskey 2018, 116.) Tutkijat itse pitävät koulukuntiin määrittelyä liian kapea-alaisena, ja haluavat painottaa tutkijoidensa monialaisuutta sekä keskinäistä vuorovaikutusta. Vuonna 2006 julkaistu C.A.S.E. Collective: Critical Approaches to Security in Europe Manifesto (tästä eteenpäin CASE) on useiden eri kriittisen turvallisuustutkimuksen suuntauksia edustavien tutkijoiden yhteinen julistus, jolla he haluavat hälventää ulkopuolisten tekemiä vahvoja rajauksia koulukuntiin sekä tuoda esille kriittisen turvallisuustutkimuksen moninaisuutta ja akateemisen dialogin tärkeyttä.

Niin kutsuttujen kriittisen turvallisuustutkimuksen ’koulukuntien’ välillä on toki eroja tutkimuspainotuksissa sekä teoreettisissa mallinnuksissa. ’Koulukuntien’ tutkijat ottavat kuitenkin aktiivisesti vaikutteita toisiltaan yli koulukuntarajojen ja moni teoreettinen oivallus on syntynyt juuri akateemisen ajatustenvaihdon sekä debatin seurauksena (CASE Collective 2006, 444). Kyseenalaistamisen ja debatin perinne ovat olleet tutkimusalan voimavara viimeisen 30 vuoden aikana (Hendershot ja Mutimer 2018, 62).

CASE Collective -julistuksen takana on myös ajatus tuoda vahvemmalla voimalla esille eurooppalaista turvallisuustutkimusta. Turvallisuuden tutkimusta on pitkään leimannut yhdysvaltalaisuus ja etenkin vanhojen, kylmän sodan aikana turvallisuuspolitiikassa meritoituneiden mieshenkilöiden ylivalta. CASE Collectiven avulla on pyritty nostamaan eurooppalaista kriittistä turvallisuustutkimusta omalle erilliselle jalustalleen, ilman, että sen eri koulukunnat nähdään toistensa kilpailijoina. (CASE Collective 2006, 444.)

Käytän tässä tutkimuksessa eurooppalaisen kriittisen turvallisuustutkimuksen koulukuntajakoa, kuitenkin painottaen sen väljyyttä. ’Koulukunnat’ on ymmärrettävä suuntaa-antavina ei absoluuttista jakoa edustavina. Todellissudessa määrittelyt ja lokeroinnit helpottavat ihmisten hahmottamiskykyä etenkin monivivahteisten teorioiden kohdalla.

’Koulukunnista’ Kööpenhaminalla ja Aberystwythillä on juuret politiikan teoriassa ja kansainvälisten suhteiden tutkimuksen alan debateissa. Molemmat koulukunnat ovat

muotoutuneet rauhan ja konfliktin tutkimuksen sekä strategisen tutkimuksen välimaastossa uudelleen asemoiden itsensä (CASE 2006, 446). ’Pariisin koulukunta’ on puolestaan muotoutunut monien eri tieteenalojen fuusiona ja sen tutkijat yhdistelevät edelleen sosiologian, kriminologian, politiikan tutkimuksen, oikeustieteen ja manner-eurooppalaisen hallintotieteen tutkimussuuntauksia (Bigo ja McCluskey 2018, 117).

Hedershot ja Mutimer (2018, 66) huomauttavat, että vaikka kriittinen turvallisuustutkimus voi kritisoida perinteisiä turvallisuuden tutkimuksen suuntauksia, ei kriittinen turvallisuustutkimus vastusta tai pyri muuttamaan nollasummapelin, sotilaallisen tai strategisen turvallisuuden luomia teoreettisia mallinnuksia. Kriittinen turvallisuustutkimus haluaa yksinkertaisesti paljastaa ne kohdat, ryhmittymät ja näkökulmat, jotka perinteinen turvallisuustutkimus sivuuttaa.

Pariisin ja Kööpenhaminan ’koulukunnat’ ovat nousseet kahdeksi keskeisimmäksi teoretisointia luovaksi suuntaukseksi turvallisuustutkimuksen alalla (Vuori 2014, 28-29). Näiden kahden välillä on myös nähty kiivain kriittinen dialogi etenkin turvallisuuden ja turvallistamisen termien ympärillä (Bigo ja McCluskey 2018, 117). Ole Wæverin johdolla muodostunut ’Kööpenhaminan koulukunta’ sai vastapainokseen *Cultures et Conflits* -lehden ympärille muodostuneen monitieteellisen tutkijoiden joukon, jota alettiin kutsua ’Pariisin koulukunnaksi’. (Bigo ja McCluskey 2018, 117.)

Seuraavassa alaluvussa keskityn tarkastelemaan ’Pariisin koulukunnan’ ajatuksia ja turvattomuuden politiikan teoretisointia. ’Pariisin koulukunta’ tukee monia ’Kööpenhaminan koulukunnan’ teoriamalleja, mutta luo myös omia tulkintojaan niiden pohjalta.

3.3. ’Pariisin koulukunta’: turvattomuuden politiikka ((in)security, (in)securitization)

Usein ajatellaan että, turvattomuus ja turvallisuus toimivat vastakohtina toisilleen. Valtion turvallisuusanalyyseissä kuten myös akateemisessa kirjallisuudessa voidaan usein nähdä ajatusmalli siitä, että turvallisuuden lisääminen vähentää turvattomuutta. Ajatus on paradoksaalinen, sillä jos ymmärtää turvallisuuden olevan päättymätöntä ja päämäärätöntä ei sen lisäämisen koskaan poista turvattomuutta. Turvattomuus on poliittinen arvio tilanteesta, jota verrataan menneeseen ja nykyiseen (Bigo ja McCluskey

2018, 125-126.) Turvattomuus on siis tilannekohtaista. Uudet ja ajankohtaiselta tuntuvat turvallisuusuhat ja riskit oikeuttavat myös uusien turvallisuusrakenteiden muodostamiseen (Bigo 2000, 171). Sekä turvallisuuden että turvattomuuden määrittely on poliittinen teko. Molemmat ovat osa laajempaan turvallistamisen/epäturvallistamisen prosessia. Turvallistaminen puolestaan tarkoittaa tekoja (päätöksiä, uhrauksia, symbolisen valta-aseman ottamista), joilla päätökset turvallisuuden luomiseksi oikeutetaan. (Bigo ja McCluskey 2018, 126.)

Turvattomuuden politiikka ((in)security ja (in)securitization) on yksi keskeisimmistä jälkistrukturalistisen kriittisen turvallisuustutkimuksen käsitteistä, jonka avulla tarkastellaan turvallisuuden diskursiivista toimintaa samalla kiinnittäen huomiota siihen, kuka turvallisuuden narratiiveja muodostaa osana arkipäiväistä työtään (Bigo ja McCluskey 2018, 119). ’Pariisin koulukunnan’ lähestymistapa korostaa laajasti erilaisia elementtejä teknologian käytöstä hallinnon rationaalisuuteen ja byrokratiaan turvallisuuden tekemisessä (Vuori 2014, 37). Turvallisuuden tulkitaan siis olevan yksi vallankäytön muodoista (Aradau ja van Munster 2016, 107).

Michel Foucault’n vallan määritelmällä on ollut suuri vaikutus kriittisen turvallisuustutkimuksen turvattomuuden ((in)security) käsityksen muodostamiseen. Foucault’n keskeisillä käsitteillä kuten kurinpitovallalla, biovallalla sekä hallitsemisajattelulla (*gouvernamentalité*) on ollut vaikutusta ’Pariisin koulukunnan’ turvallisuusnäkökulman muodostumiseen.

Michel Foucault johtaa kurinpitovallan historiallisesta kontekstista suvereenivallan ajoilta. Kurinpitovallassa valta keskittyy yksilöön, kun taas biovallassa koko väestö ja ihmisten elämä otetaan hallinnan kohteeksi. Biovalta ulottuu kaikkialle ihmisen elämän vivahteisiin, mutta on usein näkymätöntä ja rajatonta valtaa, joka ei perustu mihinkään keskitettyyn legitiimiin vallankäyttäjään. (Aradau ja van Munster 2016, 110-111.) Olennaista on ymmärtää Foucault’n käsitys vallasta ketjumaisena elementtinä, jossa valta ei ole kenenkään toimijan käsissä, vaan toimijat ovat vain vallan johdattimina (Vuori 2014, 37).

Foucault’lle turvallisuus kytkeytyy ’normaalioloihin’ ja vapauteen: ”*Turvallisuus voi toimia sääntelevänä tekijänä, mutta se ei kiellä tai määrää mitään kuten laki ja kurivalta tekevät* ” (Foucault 1978). Turvallisuus kytkeytyy siis ennemmin biovallan muotoon edustaen vapaata rauhallista elämää, ei sodan tai valvonnan elementtejä (Bigo 2008, 107).

Hallitsemisajattelu on puolestaan tapa hallita väestöä kokonaisuudessaan, jossa turvallisuuden dispositiivi eli vallan strategia on kaiken mahdollisen, ihmisten, kulutushyödykkeiden ja talouden vapaata kiertoa yhteiskunnassa. Tähän liittyy tilastollisen mallintamisen elementti, jonka avulla pystytään kartoittamaan turvallisuuteen liittyviä uhkia ja riskitekijöitä. (Foucault 1978.)

Didier Bigo (2008, 105), 'Pariisin koulukunnan' edustaja ja yksi Foucault'n merkittävimmistä tulkitsijoista huomauttaa, että Michel Foucault'n turvallisuuden käsite jää vajaaksi niin sisällöiltään kuin ratkaisuiltaan. Tämän vuoksi kriittisen turvallisuustutkimuksen tutkijoiden tekemiä tulkintoja ei tulisi ymmärtää suoraan Foucault'n käsityksinä turvallisuudesta vaan kriittisen turvallisuustutkimuksen suuntauksen omana kehityskulkuna.

Turvallisuuden dispositiivi kaiken vapaasta kierrosta yhteiskunnassa korostuu 'Pariisin koulukunnan' näkökulmassa turvallisuudesta. Koulukunnan tutkijat haluavat korostaa vapautta, sen edistämistä ja suojelua sen sijaan, että turvallisuus ymmärrettäisiin puhtaasti pelkästään fyysisten maa-alueiden suojeluna. Ajatus tukee liberaalien, demokraattisten yhteiskuntien toimintamallia, jossa juuri vapaus ja kaiken vapaa kierto ovat yhteiskunnan toiminnan edellytyksiä. Turvallisuudella viitataan näiden toimintojen suojeluun. (Bigo 2008, 96-97.)

Turvallisuus itsessään aiheuttaa turvattomuutta turvallistamisen avulla. Kun yhteiskunta hyväksyy turvallisuuden nimissä keinot turvallisuusuhkien torjumiseksi, riskeistä, vaaroista ja jopa kuolemasta tehdään normaali asia. Usein turvattomuus kohdistuu kuitenkin yhteiskunnan marginaaleihin, niihin ihmisryhmittymiin, jotka eivät ovat osa 'tavallisten kansalaisten' joukkoa. (Bigo 2008, 105.) Esimerkiksi pakolaispolitiikkaa voidaan kiristää turvallisuuden nimissä, mutta tässä yhteydessä kyse on yhteiskunnan 'tavallisten ihmisten' turvallisuudesta, sillä kiristyvät toimet voivat aiheuttaa turvattomuutta esimerkiksi pakolaisille, jotka anovat turvapaikkaa valtiosta.

Turvattomuuden politiikka jakaa 'Kööpenhaminan koulukunnan' turvallistamisen konseptin diskursiivisen muodon, mutta haluaa painottaa puheaktin lisäksi turvallistettavan aiheen vakiinnuttamista turvallisuuden kentälle valtiohallinnon byrokraattisilla ja rationaalisilla toimintamenetelmillä (Buzan ja Hansen 2009, 217). Lisäksi uusi ilmiö tai aihe ei aina vaadi suurta 'spektaakkelia' noustakseen turvallisuuspoliittiselle agendalle (Vuori 2014, 37). Turvallistamisen sijaan 'Pariisin

koulukunnan' tutkijat käyttävät termiä "(in)securitization", jonka voisi suomeksi kääntää turvattomuuden luomiseksi. Turvattomuuden luominen liitetään kiinteästi vapauteen ja sen kiertoon ja sen kuvaillaan olevan kontingenssin muoto (Bigo 2008, 105). Samalla turvattomuuden luominen on osa turvallistamista: kun turvallistetaan, asetetaan tietty joukko turvattomuuden piiriin.

Kyberturvallisuus tarjoaa tässä oivallisen tarkastelukohteen, sillä rajatonta kokonaisuutta, eli kybertoimintaympäristöä pyritään monin keinoin rajaamaan ja ehdollistamaan, mikä on puolestaan synnyttänyt jälleen uusia turvallisuusuhkia. Esimerkiksi tietomurrot ja verkkohyökkäykset osoittavat, kuinka teknologisten laitteidemme tietoturvallisuutta pyritään jatkuvasti parantelemaan ohjelmistopäivitysten avulla. Loppujen lopuksi tietojärjestelmä ei koskaan ole aukoton, koska ohjelmointivirheet ja siten ohjelmiston haavoittuvuus niissä huomataan vasta kun tietomurto on päässyt jo tapahtumaan (Norilo 2021, 22).

Lisäksi voidaan nähdä, että kyberturvallisuuden ehtoja määrittelevät pitkälti teknologian ammattilaiset ja politiikan toimijat sekä itse teknologia. Teknologia ohjaa ja ehdollistaa toimintaa nyky-yhteiskunnissa. Vaikka turvallisuutta määrittelevät edelleen valtioiden ylimmät päätöksentekijät puheaktin kautta turvallistaen tiettyjä aiheita, pelkät suvereenit käskyt eivät välttämättä ole nykyään enää yhtä tehokkaita kuin teknologian hallinnan keinot (Vuori 2014, 38). Kybertoimintaympäristössä teknologia on keskeisessä asemassa, mutta lähes yhtä keskeisiä ovat sen käyttäjät eli yksilöt. Yksilöllä on lopulta kaikki valta käsissään kybertoimintaympäristössä myös turvallisuuden näkökulmasta.

***

Tarkastelen tutkielmassani 'Pariisin koulukunnan' turvattomuuden politiikan näkökulmasta Euroopan unionin harjoittamaa kyberturvallisuuspolitiikkaa. Keskityn tarkastelussa analysoimaan turvallisuuden diskursiivista toimintaa samalla kiinnittäen huomiota siihen, miten turvallisuuden narratiiveja muodostaa osana arkipäiväistä työtään EU:ssa. Kriittisen diskurssianalyysin keinoin pyrin erottelemaan Euroopan unionin virallisista dokumenteista turvallistamisen ja turvattomuuden politiikan elementtejä.

Seuraavaksi siirryn tarkastelemaan tutkielman metodeja ja esittelemään aineiston, jonka tulkitsemisessa hyödynnän kriittisen diskurssianalyysin työkaluja sekä turvattomuuden politiikan elementtejä.

4. Metodit ja aineiston esittely

4.1. Kriittisen turvallisuustutkimuksen menetelmistä

Kriittisen turvallisuustutkimuksen parissa menetelmät painottuvat laadullisiin ja usein diskursiivisiin muotoihin. Alan tutkijat ovat kuitenkin kokeilunhaluisia ja erilaisia menetelmällisiä työkaluja yhdistellään kuten sopivaksi nähdään (Salter ja Mutlu 2018, 169). Tämä luo vapautta niin aineiston keräämiseen kuin analysointiin. Kriittisen turvallisuustutkimuksen parissa teoreettiset suuntaviivat eriävät toisistaan, mutta menetelmissä tutkimusalan haarat ovat lähellä toisiaan (emt.).

Tutkijan oma positio on hyvä ottaa huomioon tutkimuksen metodologisia lähtökohtia määriteltäessä (Juhila 2016). Kriittisen turvallisuustutkimuksen näkökulma on vahva tutkielmassani, mutta oma henkilökohtainen katsantokantani puoltaa myös realismiin taipuvan reaalipoliittisen turvallisuustilanteen kantaa, jossa turvallisuusuhkiin on suhtauduttava vakavuudella. Tämä näkyy myös aineistovalinnoissani, sillä käytän pääaineistonani Euroopan unionin virallisia dokumentteja, jotka korostavat juuri turvallisuusuhkien vakavuutta. Tärkeää on kuitenkin tarkastella dokumenttien sisältöä kielellisestä näkökulmasta, pohtia niiden välittämää kuvaa kriittisesti sekä tuoda esiin erilaisia vivahteita EU:n kyberturvallisuuspolitiikasta.

Kuten useissa yhteiskuntatieteellisissä tutkimuksissa tämänkin tutkielman osalta kirjoittaja on tietoinen tutkielman subjektiivisesta luonteesta. Aineiston kerääminen, valitseminen ja luokittelu on tapahtunut kirjoittajan omien valintojen perusteella, eikä perustu objektiiviseen totuuteen asioista. Tutkielman menetelmät edellyttävät asioiden tulkintaa, minkä vuoksi tutkimuksen tulokset ovat alttiita kyseenalaistamiselle ja kritiikille.

4.2. Aineiston analyysin vaiheet

Kuvio 2. Tutkimusaineiston analyysin vaiheet.

Tutkielmani aineiston analyysi etenee kuvion 2 mukaisessa järjestyksessä. Aloitan aineiston analyysin kriittisen diskurssianalyysin työkaluilla, jotka esittelen seuraavassa alaluvussa 4.3. Kriittisen diskurssianalyysi mahdollistaa tekstistä löytyvien eri temaattisten diskurssien eli hegemonisten diskurssien havainnoimisen. Tässä tutkielmassa aineiston temaattinen erittely tapahtuu löydettyjen diskurssien avulla. Kun hegemoniset diskurssit on eritelty, pyrin etsimään turvattomuuden politiikan elementtejä näistä diskursseista. Esittelen turvattomuuden politiikan elementit alaluvussa 4.4.

Hyödynnän tutkimusaineistona dokumenttien lisäksi tilastoaineistokappaleita, joiden kohdalla käytän kriittisen diskurssianalyysin menetelmiä vain kysymyksien analysointiin ja vallan paikantamiseen diskurssin takana. Tilastoaineistokappaleiden analysoinnissa hyödynnän muuten sisällönanalyysin ja tulkinnan menetelmiä. Tilastoaineisto toimii tässä yhteydessä dokumenttiaineistoa tukevana aineistona, jonka avulla pyrin muun muassa edesauttamaan turvattomuuden politiikan elementtien havainnollistamista.

4.3. Kriittinen diskurssianalyysi

Hyödynnän tutkielmassani kriittisen turvallisuustutkimuksen relatiivista vapautta käyttää niitä menetelmiä, jotka kokee sopiviksi. Tutkimusaineistoni on tekstipainotteista, minkä vuoksi päätyökalunani käytän kriittistä diskurssianalyysiä. Kriittinen diskurssianalyysi on kriittisen sosiaalianalyysin muoto (Fairclough 2018, 13), jossa yhdistyy diskurssiin kohdistuvan normatiivisen kritiikin esittäminen sekä sen suhteen selittäminen sosiaaliseen todellisuuteen (Fairclough 2015, 6, 48). Diskurssin analysoinnilla tarkastellaan tekstin ja kontekstin vuorovaikutusta (Flowerdew 2018, 165).

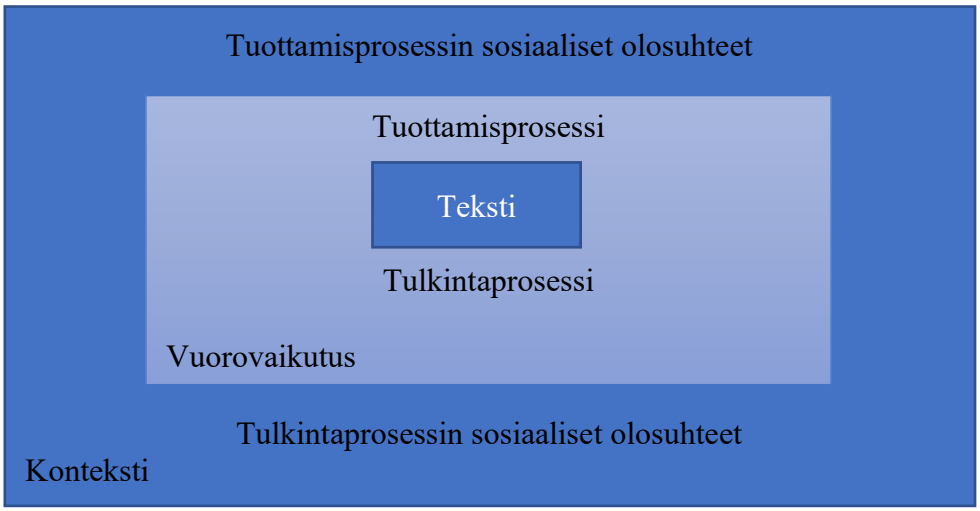
Kriittisen diskurssianalyysin tarkoituksena on osoittaa epäkohdat ihmisten sosiaalisissa käytänteissä ja löytää mahdolliset ratkaisut epäkohtien korjaamiseen (Fairclough 2018, 13). Kriittinen diskurssianalyysi pitää siis sisällään muillekin kriittisille teorioille ominaisen emansipatorisen agendan eli pyrkimyksen osoittaa sinne, missä nähdään epäkohta sosiaalisessa tai poliittisessa elämässä ja tuoda parannus tilanteeseen. (mm. Fairclough 2001a, 26; McKinlay ja McVittie 2008, 12.)

Tämän tutkielman teoreettinen tausta nojaa vahvasti kriittisen turvallisuustutkimuksen turvattomuuden politiikan elementteihin, joten keskityn hyödyntämään kriittistä diskurssianalyysiä menetelmällisenä työkaluna. Sekä teoreettista että metodologista suuntausta tutkimuksessani nivoo yhteen kriittinen suuntaus, jonka pohjana toimii kriittinen teoria.

Sosiaalista todellisuutta välitetään diskurssin ja ideoiden avulla. Sosiaaliset kokonaisuudet kuten ihmiset, tapahtumat, instituutiot ja tavat tuovat esille uskomuksiaan ja ideoitaan representaation muodossa. Analyysin tehtävänä on sisäistää nämä molemmat ja etenkin sosiaalisen kokonaisuuden ja sen representaation suhde. (Fairclough 2018, 14.) Kirjoitettu tekstikin on viestintää, joka tapahtuu tietyssä paikassa sekä ajassa ja on siten sosiaalisen vuorovaikutuksen muoto (Metsämuuronen 2008, 33-34). Tekstiä analysoidessa on huomioitava sosiokulttuurinen konteksti, mitä tietyllä sanalla on tässä yhteydessä tarkoitettu ja onko se kenties suunnattu vain jollekin ihmisryhmälle, joka ymmärtää sanan sen siinä merkityksessä. Tärkeää on lisäksi pohtia kuka puhuu, mikä on puhujan näkökulma, mihin pyritään vetoamaan ja miten kertoja tai puhuja pyrkii vakuuttamaan lukijan tietystä totuudesta tai epätotuudesta (emt. 2008, 33-34).

Vaikka diskurssianalyysille on ominaista olettaa kielenkäytön sosiaalista todellisuutta rakentava luonne (Jokinen, Juhila ja Suoninen 2016; Young ja Harrison 2004), kriittinen diskurssianalyysi hiukan vierastaa ajatusta siitä, että tutkimuskohteet olisivat sosiaalisesti rakentuneita. Toisin sanoen kriittinen diskurssianalyysi näkee sosiaaliset ilmiöt ennemmin todellisina sosiaalisina objekteina. Diskursiiviset tavat eivät kuitenkaan ole erillään todellisesta maailmasta, tärkeämpää on vain osoittaa, millaisia toimia ihmiset voivat saavuttaa kielen avulla. (McKinley ja McVittie 2008, 12.)

Kriittisen turvallisuustutkimuksen teoretisoinnin kannalta pidättäydyn tässä tutkielmassa selkeästi perinteisen diskurssianalyysin tulkinnassa siitä, että kieli ei pelkästään kuvaa maailmaa vaan luo myös uusia merkityksiä siten, että se samalla uusintaa, järjestää ja rakentaa sosiaalista todellisuutta. Kielen merkitys muodostuu suhteessa toisiin, ja kieltä voidaan siten jäsentää merkityssysteemien avulla. (Jokinen, Juhila ja Suominen 2016.) Myös Norman Fairclough'n valtatulkinta olettaa diskurssin olevan sosiaalinen harjoite, joka samalla osallistuu sosiaalisten rakenteiden tuottamiseen (Fairclough 2015, 98). Sanoista muodostuvat diskurssit ilmentävät ideoita, arvoja ja tapoja, jotka ovat todellisen maailman objekteja (Salter ja Mutlu 2018, 172). Täten myös kieli palvelee tiettyjä intressejä ja sitä käytetään tarkoituksenmukaisesti (emt. 2018, 172). Kriittisen turvallisuustutkimuksen näkökulmasta asiantuntijat ja poliitikot käyttävät tietynlaista kieltä tarkoituksenmukaisesti, jotta voivat saavuttaa auktoriteetin tietyllä osa-alueella (Bigo 2002).



Kuvio 3. Diskurssin, vuorovaikutuksen ja kontekstin suhde (Fairclough 2015, 58).

Oheinen kuvio 3 havainnollistaa Norman Fairclough'n (2015, 57-58) tulkintaa diskurssista sosiaalisen toiminnan muotona. Teksti on tuote, ja siksi se saa paikan suorakulmion keskeltä. Diskurssilla viitataan tässä yhteydessä koko sosiaalisen vuorovaikutuksen prosessiin, jonka yksi osa teksti vain on. Prosessiin sisältyy itse tuottamisprosessi, mutta myös tulkintaprosessi, jolle teksti on voimavara. Tekstin analysointi on vain yksi osa diskurssianalyysiä, sillä yhtä lailla oleellista on *tekstin tuottamisprosessin jälkien* sekä *tulkinnallisen prosessin merkkien* havainnointi (Fairclough 2015, 57). Tekstin tuottamisprosessin jäljet sekä tulkinnallisen prosessin merkit sekä syntyvät että niitä tulkitaan aina vuorovaikutuksessa ihmisen omiin arvoihin,

mielleyhtymiin, olettamuksiin ja tapoihin tulkita maailmaa sekä tekstiä. Fairclough (2015, 57) kutsuu näitä ’jäsenten resursseiksi’ (’members’ resources’, MR), kun taas Eero Suoninen (2016) puhuu ihmisen yksilöllisistä mielleyhtymistä, myyttisistä merkityksistä tai tunnemerkityksistä.

Tekstin tulkitsijana toimivan ihmisen omat ajatukset vaikuttavat tekstin tulkintaan kuten myös erilaiset kognitiiviset strategiat, esimerkiksi erilaiset tavat, joilla ihmisen odotetaan tulkitsevan runoa ja verkkouutista. Nämä ovat osa ennalta määrättyjä sosiaalisia olosuhteita, jotka on hyvä huomioida tulkittaessa tekstiä kriittisesti. (Fairclough 2015, 57.) Diskurssi siten pitää sisällään sekä tulkinnan että tuottamisen sosiaaliset olosuhteet, jotka on kuvattu kuvion ulommaisessa suorakulmiossa.

Tulkinnan ja tuottamisen sosiaaliset olosuhteet on huomioitava tekstiä analysoidessa. Kriittisessä diskurssianalyysissä tekstin analysoimiseen tarvitaan kuitenkin muitakin analyysityökaluja. Käytän tutkielmassa James Geen (1996) kriittisen diskurssianalyysin kehikkoa apuvälineenä dokumenttiaineiston analysoinnissa. Geen malli on toki vain yksi monista kriittisen diskurssianalyysin ’muistilistoista’ (Locke 2004, 53), minkä vuoksi tämänkin tutkielman analyysi on tulkintaa, ja siten altis kritiikille sekä kiistämiselle.

Prosodia: Millä nuotilla sekä tavalla sanat ja lauseet tekstissä ilmaistaan. Miltä teksti kuulostaa.
Kontekstualisoivat signaalit: Merkit, joita kirjoittaja tai puhuja antaa, jotka kertovat jotain tekstin tuottamistilanteesta. Voivat olla esimerkiksi vahvistussanoja, jotka indikoivat kiireestä tai stressistä (’paljon’, ’merkittävä’).
Koheesio: Millä tavoin lauseet on liitetty tekstissä yhteen kielellisten keinojen kuten konjunktioiden, sidesanojen avulla.
Diskurssien rakenne: Millä tavoin lauseet on rakennettu ja yhdistetty. Muodostaako teksti tarinan vai onko se kokoelman pieniä argumentteja perustellakseen yhden ison argumentin.
Temaattiset rakenteet: Millaisia teemoja teksti viestittää ja muodostaa.

Taulukko 1. James Geen (1996, 94) viisi analyysin muotoa.

Geen viisi analyysin muotoa painottuvat diskurssin lingvistisiin seikkoihin, mutta rakentavat samalla siltaa tekstin ja kontekstin välillä esimerkiksi kontekstualisoivien signaalien ja temaattisten rakenteiden avulla. Viidettä analyysin muotoa eli temaattisten rakenteiden havainnointia on mahdollista hyödyntää eri temaattisten ryhmien jäsentämiseen.

Geen mallin sekä Fairclough'n tekstin tulkinnan suorakulmion (Kuvio 3) lisäksi hyödynnän aineiston tulkinnassa Fairclough'n määritelmää vallan ja diskurssin suhteesta. Geen malli toimii sopivana 'muistilistana' kriittisen diskurssianalyysin harjoittamiseen, kun taas Fairclough'n vallan määritelmän avulla voidaan tarkastella sitä, miten valitut diskurssit ilmentävät vallankäyttöä. Fairclough'n (2015, 98) mukaan valtaa harjoitetaan ja toteutetaan diskurssissa, mutta diskurssin takana piilee myös vallan erilaisia suhteita. Jos vallan ymmärretään olevan diskurssissa, silloin diskurssi on valtataisteluiden näyttämö. Jos taas vallan ajatellaan olevan diskurssin takana, silloin diskurssi itsessään on valtataisteluiden panoksena. Se joka hallitsee diskurssin järjestystä, voittaa ja ylläpitää valtaa sosiaalisessa järjestelmässä. (emt. 2015, 98.)

Mikäli vallan ajatellaan olevan diskurssin takana ja siten diskurssin olevan valtataisteluiden panoksena, on sosiaalisen järjestelmän taisteluilla diskursiivisesta vallasta myös pidempiaikaisia ja pysyvämpiä vaikutuksia (Fairclough 2015, 98). Valtaa käyttävä diskurssiin osallistuva voi asettaa rajoitteita muille (ei valtaapitäville) osallistujille kolmella tavalla. Seuraava taulukko esittelee Fairclough'n (2015, 99) mallia mukaillen nämä kolme rajoitettavaa tekijää sekä niiden rakenteelliset seuraukset.

Rajoitettava tekijä	Rakenteellinen seuraus
Sisältö	Osaaminen ja uskomukset
Suhde	Sosiaaliset suhteet
Subjekti	Sosiaaliset identiteetit

Taulukko 2. Diskurssin ilmentämät rajoitteet ja niiden rakenteelliset seuraukset (Fairclough 2015, 99).

Taulukossa 2 kuvatut osaaminen ja uskomukset, sosiaaliset suhteet sekä sosiaaliset identiteetit ovat Fairclough'n (2001b, 62) mukaan missä tahansa yhteiskunnassa koordinoinnin ja yhtenäistämisen kohteita. Koordinointia ja yhtenäistämistä voidaan

toteuttaa kolmella tavalla. Ensinnäkin on olemassa universaaleja käytänteitä ja diskurssin muotoja, joita harjoitetaan ja ne on hyväksyttävä sellaisinaan, koska ei ole tarjolla muitakaan parempia vaihtoehtoja. Toisekseen koordinointia voidaan soveltaa osana vallan harjoittamista, kuten diskurssin takana. Fairclough (2001b, 62) kutsuu tätä mielen teroittamiseksi. Kolmantena koordinoinnin työkaluna toimii tiedonvälitys. Kaikki kolme koordinoinnin mekanismia vaikuttavat yhteiskunnissamme, mutta lopullinen taistelu käydään mielen teroittamisen ja tiedonvälityksen välillä. Vallankäyttäjä, joka halua ylläpitää olemassa olevia valtasuhteita, jopa luokkajakoja ja herruuksia, hyödyntää mielen teroittamisen mekanismia ylläpitääkseen universaalisti hyväksyttyjä käytänteitä ja diskurssin muotoja. Tiedonvälitys puolestaan toimii mekanismina emansipaatiolle ja taistelulle vallan ylivaltaa vastaan. (emt. 2001b, 62.) Kriittinen diskurssianalyysi on siis kiinnostunut siitä, sovelletaanko rajoitettaviin sisällön, suhteen ja subjektin tekijöihin mielen teroittamisen kautta valtaa vai koordinoidaanko niitä tiedonvälityksen kautta.

Vallan paikantamisessa apuna käytetään puheaktin teoriaa. Puheaktin (alk. engl. *speech act*) avulla pystytään identifioimaan se, mitä tekstin tuottaja pyrkii tekstin nojalla tuottamaan, onko kyse esimerkiksi uhkauksesta, lupauksen tekemisestä, julkilausumasta vai käskyn antamisesta (Fairclough 2001b, 129). Tuottaja voi tuottaa montaa puheaktin arvoa samanaikaisesti (emt.). Samalla tilannekohtaiset ja kontekstiin liittyvät tulkinnat sekä jäsenten resurssit, tai kuten Eero Suoninen (2016) niitä kutsuu, ihmisen yksilölliset mielleyhtymät vaikuttavat puheaktin arvojen tunnistamiseen (Fairclough 2001b, 129). Puheaktia tulkittaessa on tunnusteltava puhujaa ja vastaajaa, mitä tiedämme puheen tuottajasta ja vastaajasta heidän sosiaalisessa kontekstissaan. Jos kyse on esimerkiksi poliisin ja kuulusteltavan välisestä keskustelusta, poliisin voidaan olettaa käyttävän suoraa kieltä, mikä indikoi hänen auktoriteettiaan ja vallan käyttöään.

Pyrin tämän tutkielman diskurssianalyysissä tarkastelemaan sitä, millaista valtaa rajoitettaviin tekijöihin pyritään soveltamaan, ja hyödynnetäänkö niissä mielen teroittamisen tekniikkaa valtarakenteiden ylläpitämiseksi. Vallan paikantaminen diskurssissa on olennaista myös kriittisen turvallisuustutkimuksen turvattomuuden politiikan elementtien löytämisen kannalta, sillä elementit kytkeytyvät asiantuntijavallan ja kielen tarkoituksenmukaisen käytön taakse (Bigo 2002).

Kriittinen diskurssianalyysi ja Geen (1996) analyysityökalujen käyttö mahdollistaa tekstin jaottelun eri temaattisiin diskursseihin. Seuraavassa alaluvussa kerron tutkielmani

aineiston analyysin seuraavasta vaiheesta, aineiston jaottelusta ja turvattomuuden politiikan elementtien tarkastelusta.

4.4. Aineiston jaottelu temaattisiin diskursseihin ja turvattomuuden politiikan elementit

Kriittisen diskurssianalyysin avulla tekstiä on mahdollista jäsennellä eri diskursseihin eli ikään kuin teemoihin, jotka perustuvat aineistossa valitseviin piileviin merkityssysteemeihin. Jokisen, Juhilan ja Suonisen (2016) mukaan kielen jäsentäminen tapahtuu sosiaalisesti jaettujen merkityssysteemien avulla. Teemme päivittäin merkityseroja esimerkiksi mies ja nainen, esihenkilö ja alainen tai sininen ja punainen. Jäsennämme maailmassa erilaisia asioita suhteessa johonkin toiseen, ja merkitys muodostuu suhteessa toiseen.

Diskurssien tunnistamiseen vaikuttavat myös mielleyhtymät, myyttiset merkitykset tai tunnemerkitykset, joiden tunnistamiseen vaikuttaa tulkitsijan omat ajatukset (Suoninen 2016). Sekä tekstin tuottaminen että analysointi ovat luonteeltaan tulkinnallista (Fairclough 1989, 80). Erilaisten diskurssien esiin nostaminen tekstistä on siis tutkijan tulkintaa, ja eri tulkitsijat voivat nostaa tekstistä esille erilaisia diskursseja. Paikannetut keskeiset temaattiset diskurssit ovat niin kutsuttuja hegemonisia diskursseja. Jokinen ja Juhila (1991, 69) kuvaavat hegemonista diskurssia sellaiseksi, joka on olemassa ainoastaan puheiden ja tekojen kautta, mutta on samalla paljon enemmän kuin yksittäiset teot ja puheet. Hegemoninen diskurssi ilmentää siis yleisempää tyyliä, tapaa tai teemaa suuremmassa sosiaalisessa kokonaisuudessa.

Paljastan aineistosta löytyvät hegemoniset diskurssit vasta analyysiluvussa kuusi, sillä diskursseihin jaottelu vaatii tulkinnan johdonmukaista avaamista aineistoon nojaten. Teemoihin jaottelu ei ole etukäteisesti mahdollista hegemonisia diskursseja paikannettaessa. Tämän vuoksi en vielä tässä luvussa kerro tarkemmin diskurssien jaottelusta. Tutkielmani noudattaa siis erityistä järjestystä, jossa analysoin tekstiä ensiksi kriittisen diskurssianalyysin menetelmin ja sen pohjalta jaottelen tekstiä teemoittain. Tämän jälkeen analysoin turvattomuuden politiikan elementtejä dokumenttiaineistojen ilmentämissä hegemonisissa diskursseissa sekä tilastoaineistossa.

Turvattomuuden politiikan elementit:
-turvallistaminen
-turvallisuuden dispositiivi
-turvallisuuden arkipäiväisyys
-hallinnon rationaalisuus ja byrokratia, asiantuntijavallan korostaminen
-turvallisuuden parantaminen turvattomuuden vähentämiseksi

Taulukko 3. Turvattomuuden politiikan elementtejä.

Yllä olevassa taulukossa näkyvät turvattomuuden politiikan elementit, joita pyrin tekstistä löytyneistä temaattisista diskursseista etsimään. Käsittelen turvattomuuden politiikkaa ja ’Pariisin koulukunnan’ teoriaa tarkemmin luvussa kolme. Oheiseen taulukkoon 3 olen kerännyt ’Pariisin koulukunnan’ ja muiden kriittisen turvallisuustutkimuksen tutkijoiden yleisimmin esittämiä turvattomuuden politiikkaan liittyviä elementtejä. Ensimmäinen elementti eli turvallistaminen tarkoittaa tekoja (uhrauksia, päätöksiä tai symbolisen valta-aseman ottamista), joilla päätökset turvallisuuden luomiseksi oikeutetaan (Bigo ja McCluskey 2018, 126). Turvallisuuden dispositiivi viittaa puolestaan Foucault’n (1978) ajatukseen kaiken vapaasta kierrosta yhteiskunnassa, ja jota turvallisuus suojelee länsimaisissa liberaaleissa yhteiskunnissa (Bigo 2008, 96-97). Ideana on siis tarkastella elementtejä, jotka viittaavat aineistossa ’länsimaisen vapauden suojeluun’ turvallisuuden keinoin. Turvallisuuden arkipäiväisyys taas tarkoittaa sen toimijan tunnistamista, joka luo turvallisuuden narratiiveja osana arkipäiväistä työtään (Bigo ja McCluskey 2018, 119). Asiantuntijavallan korostaminen, hallinnon rationaalisuus ja byrokratia ovat puolestaan elementtejä, joita ’Pariisin koulukunnan lähestymistapa korostaa turvallisuuspolitiikan luomisessa, koska aihe ei välttämättä tarvitse enää suurta ’spektaakkelia’ noustakseen turvallisuuspoliittiselle agendalle (Vuori 2014, 37). Näiden lisäksi havainnoin aineistosta kohtia, joissa turvallisuutta pyritään parantamaan tai tiukentamaan turvattomuuden vähentämiseksi, vaikka turvallisuus ja turvattomuus eivät ole toistensa vastakohtia (Bigo ja McCluskey 2018, 125-126). Tämä avaa mahdollisuuden tulkita, kuka tai ketkä voivat mahdollisesti jäädä turvallisuuden ulkopuolelle ja turvattomuuden marginaaleihin EU:n kyberturvallisuuspolitiikassa.

Seuraavaksi esittelen tutkielman aineiston, joka koostuu kolmesta päädokumentista sekä kahdesta tukea antavasta tilastonaineistokappaleesta.

4.5. Tutkielman aineisto

Tutkielman aineisto muodostuu Euroopan unionin keskeisistä kyberturvallisuuteen liittyvistä dokumenteista: *EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle 2020*, *Euroopan unionin turvallisuusunionistrategia 2020* sekä EU:n ulkosuhdehallinnon uuden *Strategisen kompassin esipuhe*, jonka on laatinut ulkosuhdehallinnon korkea edustaja Josep Borrell. Strategista kompassia ei itsessään ole vielä julkaistu aineiston analyysivaiheessa, minkä vuoksi tarkastelussa on pelkästään esipuhe.

Keskeisten dokumenttien lisäksi hyödynnän aineistona Eurobarometrin tuottamia tilastoja, eurooppalaisten suhtautumisesta kyberturvallisuuteen sekä verkkoturvallisuuteen: *Erityiseurobarometri: Eurooppalaisten asenteet verkkoturvallisuutta kohtaan 2019* (alk. engl. *Europeans attitudes towards Internet security, special Eurobarometer*) ja *Erityiseurobarometri: Eurooppalaisten suhtautuminen kyberturvallisuuteen (kyberrikollisuus) 2020* (alk. engl. *Europeans attitudes towards cybersecurity (cybercrime), special Eurobarometer*).

Keskeiset dokumentit tuovat esille EU:n nykyhetken turvallisuuspoliittisen näkökulman, kun taas tilastoiksi kootut kyselyt tarkastelevat ruohonjuuritasolla sitä, millaisena kansalaiset itse mieltävät kyberturvallisuuden ja siihen liittyvät uhat. Otan tilastot mukaan tarkasteluun myös sen vuoksi, että ne tuovat esille niitä piirteitä, jotka ovat kriittisen turvallisuustutkimuksen kannalta olennaisia. Kriittinen turvallisuustutkimus pyrkii aina viemään näkökulmaa pois valtiollisesta toimijasta kohti pienempää toimijaa, joka tässä tutkimuksessa on tavallinen EU:n jäsenvaltion kansalainen.

4.5.1. Euroopan unionin turvallisuusunionistrategia 2020

Euroopan unionin turvallisuusunionistrategia on julkaistu heinäkuussa 2020 ja se kattaa aikavälin 2020-2025. Strategia on pantu täytäntöön, ja komissio on julkaissut kolme seurantaraporttia aiheesta. Strategia koostuu neljästä pääpilarista, jotka ovat ”*tulevaisuudenkestävä turvallisuusympäristö*, *muuttuvien uhkien torjunta*,

eurooppalaisten suojelu terrorismilta ja järjestäytyneeltä rikollisuudelta sekä vahva ja eurooppalainen turvallisuusekosysteemi". (Euroopan komissio 2022.)

Turvallisuusunionistrategian nimetyt neljä pääpilaria ovat helposti nostettavissa strategiasta esille. Ekosysteemi -sanan käyttö on mielenkiintoinen valinta turvallisuusstrategiassa, sillä sana kumpuaa pikemminkin biologiasta. Siitä on mitä ilmeisemmin tullut jonkinlainen trendisana Euroopan unionin virkakielessä, sillä Euroopan komission vuonna 2021 päivitetyssä teollisuuspolitiikkastrategiassa puhutaan myös teollisista ekosysteemeistä[1].

Turvallisuusunionistrategian osalta keskityn tarkastelemaan asiakirjan kohtia, joissa puhutaan kyber- tai hybridiuhista, muuttuvista uhista digitaalisen ympäristön yhteydessä tai kyberrikollisuudesta. Jätän pois luvut, joissa käsitellään terrorismia ja fyysisten, paikkasidonnaisten terrori-iskujen uhkaa (sivut 10-11 ja 17-19) sekä järjestäytyneen rikollisuuden muita muotoja kuin kyberrikollisuutta (sivut 19-23). Nykyään terrorismikaan ei kuitenkaan ole digitaalisesta ympäristöstä irrallaan, eivätkä kyberuhat täysin terrorismista eroteltavissa. EU:n turvallisuusunionistrategiassa (2020, 10-11) terrorismista kuitenkin puhutaan julkisten tilojen suojelemisen yhteydessä ja sen vuoksi jätän sen pois tarkastelusta.

4.5.2. Euroopan unionin kyberturvallisuusstrategia digitaaliselle vuosikymmenelle 2020

EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle (tästä lähtien EU:n kyberturvallisuusstrategia 2020) on julkaistu joulukuussa 2020, ja se on merkittävä osa Euroopan digitaalisen tulevaisuuden rakentamissuunnitelmaa[2], Euroopan elpymissuunnitelmaa[3] sekä EU:n turvallisuusunionistrategiaa. Kyberturvallisuusstrategian ovat tuottaneet Euroopan komissio yhdessä EU:n ulkosuhdehallinnon korkean edustajan kanssa. (Euroopan komissio 2021.) Tämä kertoo siitä, että kyberturvallisuuteen ei suhtauduta EU:ssa pelkästään sisäisen turvallisuuden

[1] Euroopan komissio 2021: Euroopan teollisuusstrategia ja neljätoista teollista ekosysteemiä: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_fi.
[2] Euroopan digitaalista tulevaisuutta rakentamassa ja sen prioriteetit: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_fi.
[3] Euroopan komission elpymissuunnitelma: https://ec.europa.eu/info/strategy/recovery-plan-europe_fi.

asiana vaan kyse on globaalin merkityksen saaneesta turvallisuuspoliittisesta aiheesta. EU:n kyberturvallisuusstrategiassa (2020, 5) toinen luku on otsikoitu ”Globaali näkökulma, Euroopan tason toiminta”, joka viittaa niin EU:n toiveisiin maailmanlaajuisesti avoimesta kybertoimintaympäristöstä, kansainväliseen yhteistyöhön sekä uhkien ehkäisemiseen, torjumiseen ja niihin vastaamiseen globaalilla toimintakentällä.

EU:n kyberturvallisuusstrategia 2020 seuraa aiempien kyberturvallisuusstrategioiden saavutettuja tavoitteita, mutta asettaa myös konkreettisia ehdotuksia. Strategia nimeää kolme pääinstrumenttia, joilla konkreettisia toimia voidaan saavuttaa kyberturvallisuuden saralla. Nämä kolme instrumenttia ovat regulaatio, investoinnit ja aloitteet. Instrumenttien avulla EU tavoittelee resilienssiä, teknologista suvereniteettia ja johtajuutta, operationaalisia kykyjä ehkäistä, torjua ja vastata kyberuhkiin sekä lisätä yhteistyötä globaalin ja avoimen kyberavaruuden mahdollistamiseksi. (Euroopan komissio 2020.)

4.5.3. Euroopan unionin Strateginen kompassi 2022: esipuhe

Kolmantena dokumenttiaineistokappaleena käytän Euroopan unionin ulkosuhdehallinnon (EUH) vuonna 2021 julkaisemaa esipuhetta, joka tulee vuonna 2022 julkaistavaan Euroopan unionin Strategiseen kompassiin (alk. engl. *A Strategic Compass for the EU*). Strategisesta kompassista on julkaistu EU:n ulkosuhdehallinnon korkean edustajan Josep Borrellin esipuheen lisäksi lyhyt tietoisku. Analyysin fokus on tässä tutkielmassa korkea edustaja Borrellin esipuheessa, mutta hyödynnän tietoiskua taustoittavana elementtinä, sillä muuta tietoa Strategisesta kompassista ei ole vielä julkaistu tutkielman analyysivaiheessa. Nämä esitiedot uudesta Strategisesta kompassista on otettu mukaan tutkielman aineiston analyysiin, sillä nämä ovat aineiston ainoat osat, jotka EU:n ulkosuhdehallinto on pelkästään tuottanut. Turvallisuusunionistrategia ja kyberturvallisuusstrategia ovat Euroopan komission johdolla muodostettuja strategioita. EU:n ulkosuhdehallinto vastaa kuitenkin yhtä lailla turvallisuuspolitiikasta, ja etenkin tämä strateginen kompassi painottuu turvallisuus- ja puolustuspolitiikan tiivistämiseen EU:ssa (EU:n ulkosuhdehallinto 2021), mikä on keskeistä EU:n kyberturvallisuuspolitiikan kannalta. Lisäksi Strategisen kompassin toivotaan tekevän Euroopasta turvallisuuden tuottajan, tai ainakin otsikkotasolla asia näin ilmaistaan (alk. engl. *A Strategic Compass to make Europe a Security Provider*) (Borrellin esipuhe 2021).

4.5.4. Tilastoaineisto

Erityiseurobarometri 480 eurooppalaisten asenteista verkkoturvallisuutta kohtaan (alk. engl. *Europeans attitudes towards Internet security*, *special Eurobarometer*) on päivätty vuodelle 2019, mutta haastattelut on toteutettu kasvotusten vuoden 2018 loka- ja marraskuussa (Data Europa 2019). Tilastotutkimukseen on haastateltu yhteensä 27 339 EU-kansalaista (emt.), ja tutkimus ei erottele eri jäsenvaltioiden kansalaisia, vaan EU-kansalaisia tarkastellaan yhtenä joukkona. Mukana tarkastelussa on 28 jäsenvaltiota, eli Iso-Britannia, joka sittemmin on eronnut EU:sta, on ollut vielä mukana tässä kyselyssä.

Erityiseurobarometri 499 eurooppalaisten suhtautuminen kyberturvallisuuteen (kyberrikollisuus) 2020 (alk. engl. *Europeans attitudes towards cybersecurity (cybercrime), special Eurobarometer*) on puolestaan toteutettu haastatteluiden muodossa lokakuussa 2019. Tutkimuksessa on haastateltu yhteensä 27 607 henkilöä EU-maista sekä Iso-Britanniasta. Suurin osa haastatteluista, noin 13 prosenttia on tehty Ranskassa, Länsi-Saksassa sekä Iso-Britanniassa. Saksa on mielenkiintoisesti eroteltu tutkimuksessa Itä- ja Länsi-Saksaan.

4.6. Aineiston käsittely

Aineiston käsittely tapahtuu lukemalla yksityiskohtaisesti aineiston dokumentit sekä tilastot läpi. Aineisto on kohtuullisen kokoinen ja teksti helppolukuista. Kriittisen turvallisuustutkimuksen teoretisointia hyödyntäessä ja turvallistamisen ja turvattomuuden elementtejä etsiessä tekstiä on luettava huolella keskittyen kokonaisten virkkeiden ja kappaleiden sanomaan. Kriittinen diskurssianalyysi vaatii myös tekstin läpikotaista lukemista niin, että tekstin osaa liittää oikeaan kontekstiin, ja ymmärtää samalla ne arvot, kuten esimerkiksi vallan, joka on piilotettu tekstin taakse (Fairclough 2018, 14).

Koodaan ja jäsentelen tekstiä oman analyysiprosessin helpottamiseksi. Tässä käytän hyödyksi Pdf-dokumenttien lukuohjelmaan valmiiksi asennettua alleviivaus sekä sanahaku -työkaluja. Sanahaku -työkalu toimii tilanteissa, joissa etsin tiettyä sanaa tai sanaparia kuten ”kyberturvallisuusekosysteemi”, ”kokonaisvaltainen lähestymistapa” tai ”resilienssi”. Sanahaku sekä alleviivaus -työkalut helpottavat dokumentin työstämistä ja etenkin sitä, että olennaiset asiat tekstistä muistuvat yhä uudelleen mieleen.

Aineistoni dokumenteista EU:n turvallisuusunionistrategia sekä kyberturvallisuusstrategia on saatavissa suomenkielisinä. EU:n ulkosuhdehallinnon strategiseen kompassin esipuhetta tarkastelen englanninkielisenä. Sisällönanalyysin kannalta suomenkielisten dokumenttien analyysi on sujuvampaa ja laatu parempaa, kun analysoin tekstiä diskursiivisin keinoin suomeksi. Käytän tarpeen tullen englanninkielisiä strategioita kielen tarkastuksessa, koska olen huomannut, että suomenkielisissä dokumenteissa on pieniä käännösvirheitä[4]. Euroopan ulkosuhdehallinnon strategista kompassia koskevan aineistokappaleen kohdalla käännän tarvittavat kohdat itsenäisesti englannista suomeksi kriittistä diskurssianalyysiä varten.

Eurobarometrin tilastoaineistojen kieli on englanti sekä ranska, ja tulkitsen molempia kieliä sujuvasti. Pyrin analysoimaan diskursiivisesti tilastojen tekemisessä käytettyjä kysymyksiä sekä analysoimaan kyselyiden perusteella tuotettuja mittaustuloksia tavallisin sisällönanalyysin ja tulkinnan keinoin. Tilastoaineistot toimivat dokumenttiaineistoa tukevana aineistona tässä tutkielmassa.

***

Olen tässä luvussa avannut kriittisen diskurssianalyysin työkaluja, joita hyödynnän aineiston analyysissä. Olen lisäksi eritellyt keskeisimmät turvattomuuden politiikan elementit, joita tule aineistossa tarkastelemaan vallan ja diskurssin suhteen paikantuessa. Seuraavassa luvussa viisi siirryn aineiston analyysiin. Analyysiluvut noudattavat tässä luvussa esitettyjä aineiston analyysin vaiheita.

[4] Esimerkiksi Euroopan unionin turvallisuusunionistrategiassa (2020) englanninkielinen *policy* -sana on toistuvasti käännetty suomeksi *poliitikoksi*, kun tarkoitus olisi käyttää sanamuotoa *harjoitettu politiikka*.

5. Vallan kontekstualisointi

Tässä luvussa käyn läpi tutkimusaineistoa kriittisen diskurssianalyysin sekä sisällönanalyysin keinoin. Aloitan Euroopan unionin turvallisuusunionistrategian (2020), kyberturvallisuusstrategian (2020) sekä EU:n ulkosuhdehallinnon korkean edustajan Josep Borrellin strategisen kompassin esipuheen (2021) kontekstualisoinnilla ja diskursiivisten rakenteiden purkamisella. Käsittelen dokumenttien sisältöjä ensiksi erillisinä, ja temaattisten diskurssien analysoinnissa yhdistelen teksteistä löytyviä elementtejä.

James Geen (1996) kriittisen diskurssianalyysin työkaluja (prosodia, kontekstualisoivat signaalit, koheesio, diskurssin rakenne ja temaattiset rakenteet) hyödyntäen pyrin purkamaan dokumenttien diskursiivista rakennetta sekä tarkastelemaan Norman Fairclough'n ajatusten mukaisesti diskurssin kontekstia sekä vallan ja diskurssin suhdetta strategioissa ja esipuheessa. Dokumentteja on kokonaisuudessaan mahdollista analysoida diskursiivisin menetelmin, mutta poimin strategioista ja esipuheesta ne kohdat, jotka ovat olennaisia tutkimukseni kannalta. Seuraavassa luvussa kuusi paneudun tarkemmin temaattisiin diskursseihin, joita tekstistä on havaittavissa.

Lisäksi tarkastelen tässä luvussa tutkimusaineiston tilastoaineistoa sisällönanalyysin ja tulkinnan keinoin. Tuon tilastoaineiston analyysin mukaan tarkasteluun kontekstualisoidessani tutkimusaineiston muita kappaleita. Tarkastelen myös sitä, miten uhkakuvia tuodaan esille tilastoaineiston kautta. Tilastoaineiston analyysi toimii tässä tutkielmassa muuta aineiston analyysiä tukevana elementtinä, ja tilastoaineiston tulkinta tuo lisää syvyyttä turvattomuuden politiikan elementtien tarkasteluun luvussa seitsemän.

5.1. Mitä aineistokappaleet tavoittelevat?

Euroopan unionin vuonna 2020 julkaiseman turvallisuusunionistrategian johdannossa määritellään tavoite EU:n turvallisuusunionista: "*taata turvallisuus sekä fyysisissä että digitaalisissa ympäristöissä*" ja kansalaisten suojelun on tapahduttava yhteistyöllä. Lisäksi mainitaan, että EU:n tehtävänä on varmistaa, että "*turvallisuuspolitiikka perustuu yhteisiin eurooppalaisiin arvoihin – oikeusvaltioperiaatteen, tasa-arvon ja perusoikeuksien kunnioittamiseen ja vaalimiseen sekä avoimuuden, vastuuvelvollisuuden ja demokraattisen valvonnan takaamiseen*". Strategian kerrotaan luovan raamit

toimintaperiaatteille vuosille 2020-2025, ja se esittelee ”koko yhteiskunnan kattavan lähestymistavan”.

> ”(1) *Komission poliittisissa suuntaviivoissa tehtiin selväksi, että meidän on tehtävä kaikkemme unionin kansalaisten suojelemiseksi.* (2) *Turvallisuus on ensiarvoisen tärkeää henkilötasolla, mutta se suojelee myös perusoikeuksia sekä luo perustan taloutemme, yhteiskuntamme ja demokratiamme luottamukselle ja dynaamisuudelle.* (3) *Euroopan turvallisuusympäristö on muutostilassa.* (4) *Syynä tähän ovat muuttuvat uhat sekä muut tekijät, kuten ilmastonmuutos, väestönkehityksen suuntaukset ja poliittinen epävakaisuus rajojemme ulkopuolella.*” (EU:n turvallisuusunionistrategia 2020, 1.)

Me -muodon käyttö heti EU:n turvallisuusunionistrategian alussa: ”*meidän on tehtävä kaikkemme unionin kansalaisten suojelemiseksi*”, luo mielikuvaa siitä, että kyse on yhteisestä asiasta, että turvallisuus Euroopassa on meidän kaikkien yhteinen asia. Samoin toisessa virkkeessä puhutaan monikossa ”[*t*]*urvallisuus…luo perustan taloutemme, yhteiskuntamme ja demokratiamme luottamukselle ja dynaamisuudelle*”. Tällä pyritään vahvistamaan mielikuvaa siitä, että tarvitsemme turvallisuutta, jotta *meidän* taloutemme, yhteiskuntamme ja demokratiamme säilyisivät. Me -muodon käyttö myös hämää, sillä se vie lukijan ajatukset siihen, mikä kaikki on eurooppalaisille yhteistä. Sen sijaan kirjoittajat pyrkivät perustelemaan, miksi turvallisuus on tärkeää, koska se mahdollistaa nykyisenkaltaisen talouden, yhteiskunnan ja demokratian *luottamuksen* ja *dynaamisuuden*, ja sen vuoksi turvallisuuttamme on suojeltava. Me -muodon käytöllä myös pyritään perustelemaan sitä, että turvallisuuden suojelua on toteutettava yhteisesti. Prosodian näkökulmasta johdanto kuulostaa samaan aikaan uhkaavalta, mutta dynaamiselta. Sanat ja virkkeet on tarkoin harkittuja siten, että lukija saadaan pelästymään välittömiä uhkia ja turvallisuusympäristön muutostilaa. Samalla luodaan uskoa *me*-hengellä, etenkin sillä, *integroitujen ratkaisujen* avulla EU pystyy auttamaan jäsenvaltioita sekä ”*tarjoaa tarvittavia välineitä ja tietoa*” turvallisuusuhkien kohtaamiseen.

EU:n kyberturvallisuusstrategia digitaaliselle vuosikymmenelle (2020) keskittyy puolestaan määrittelemään toiminnan tavoitteet kyberturvallisuuden kokonaisvaltaiseksi toteuttamiseksi. Kun turvallisuusunionistrategiassa korostuu ”*meidän Eurooppa*” -dialogi, kyberturvallisuusstrategiassa puhutaan maailmasta ja globaalitasosta: ”*vihamieliset hyökkäykset ovat maailmanlaajuinen riski*” (EU:n kyberturvallisuusstrategia 2020, 2). Kyberturvallisuusstrategian tavoite määritellään luvussa kaksi: ”*tavoitteena on varmistaa maailmanlaajuinen ja avoin internet, jossa*

eurooppalaisten turvallisuutta ja perusoikeuksia ja -vapauksia voidaan tehokkaasti suojella niihin kohdistuvilta riskeiltä" (EU:n kyberturvallisuusstrategia 2020, 5). Strategian luvataan sisältävän myös konkreettisia ehdotuksia sääntelyn, politiikan ja investointien välineistöä hyödyntäen (emt.). Kyberturvallisuusstrategia eroaakin tässä juuri turvallisuusunionistrategiasta, sillä kyberturvallisuusstrategia on sisällöltään teknisempi ja konkreettisiin ratkaisuehdotuksiin paneutuva. Turvallisuusunionistrategia puhuu turvallisuusuhista ja niihin vastaamisesta ylätasolla ja yleisemmin. Sen vuoksi kyberturvallisuusstrategia täsmentää turvallisuusunionistrategiassa määriteltyjä tavoitteita muun muassa johdonmukaisesta lähestymistavasta (EU:n kyberturvallisuusstrategia 2020, 6).

Kyberturvallisuus nimetään heti kyberturvallisuusstrategian alussa "*olennaiseksi osaksi eurooppalaisten turvallisuutta*". *Olennaiseksi* toteaminen tekee asiasta kuin asiasta painavan, mutta turvallistaa samalla kyberturvallisuuden konseptin määrittelemällä sen osaksi turvallisuusulottuvuutta (Vuori 2014; Buzan ja Hansen 2009, 217). Strategiassa käytetään yleisestikin paljon vahvistussanoja kuten *erityisen* tai *olennaisen tärkeää*, *välttämätöntä*, *elintärkeää* ja *ennennäkemätöntä*. Vahvistussanat luovat tekstin tuntuvuutta ja saavat aiheen kuulostamaan vakavammalta.

> "(1) *Kyberturvallisuus on olennainen osa eurooppalaisten turvallisuutta.* (2) *Olipa kyse sitten verkkoon liitetyistä laitteista, sähköverkoista, pankkipalveluista, lentokoneista, julkishallinnosta tai sairaaloista, ihmisten on voitava luottaa siihen, että heitä suojellaan kyberuhkilta.* (3) *EU:n talous, demokratia ja yhteiskunta ovat ennennäkemättömän riippuvaisia turvallisista ja luotettavista digitaalisista välineistä ja yhteyksistä.* (4) *Kyberturvallisuuden varmistaminen onkin välttämätön osa selviytymiskykyisen, vihreän ja digitaalisen Euroopan rakentamista*." (EU:n kyberturvallisuusstrategia 2020, 1.)

Oheinen kappale on kyberturvallisuusstrategian alusta. Ensimmäistä kappaletta on mielenkiintoista tarkastella, sillä se kertoo paljon koko dokumentin sisällöstä, ja pyrkii sitomaan lukijan mielenkiinnon aiheeseen. Prosodian näkökulmasta tämä ensimmäinen kappale kuulostaa itsevarmuutta uhkuvalta, mutta samaan aikaan vakavalta, onhan kyseessä haastava eurooppalaisten turvallisuuteen liittyvä aihe. Itsevarmuuden tuntu tulee etenkin pienestä sanaparista "*olipa kyse sitten*" toisessa virkkeessä, ja kun se liitetään luetteloon asioista, jotka ovat meille eurooppalaisille arkipäivää kuten digitaaliset verkkopalvelut, lentokoneet ja lentäminen, sairaaloiden toiminta ja ylipäänsä talouden, demokratian ja yhteiskunnan toimintakyky. Toisessa virkkeessä luetellut asiat ovat arkipäivää eurooppalaisille, mutta ne eivät ole arkipäivää kaikilla maapallon mantereilla.

Vakavuutta luodaan sillä, että uhkakuvia on olemassa, ja digitaalinen ympäristö on riippuvainen turvallisuudesta. Tämä ensimmäinen kappale kyberturvallisuusstrategiassa on tarinamainen ainakin ensimmäisen ja toisen virkkeen osalta. Kolmannen ja neljännen virkkeen osalta on huomattavissa käännös tarinallisuudesta argumentaation pienellä sanakäänteellä *onkin* neljännessä virkkeessä. Kolmas virke siis tekee väitteen, jonka vuoksi kyberturvallisuus on esille nostamisen arvoinen aihe, ja neljäs virke tuo aiheen esille nostamiselle perustelun.

Talouden, yhteiskunnan ja demokratian turvallisuudesta tai suojelusta puhutaan turvallisuusunionistrategiassa. Tämä on toistuva elementti myös kyberturvallisuusstrategiassa näkyen heti ensimmäisen kappaleen neljännessä virkkeessä. EU:n arvomaailmaa kuvaa myös ”*osa selviytymiskykyisen, vihreän ja digitaalisen Euroopan rakentamista*”. Vihreys liittyy EU:n talouteen, ei millään lailla turvallisuuteen, mutta kyberturvallisuus sitoo yhteen sekä talouden että turvallisuuden politiikka-alat. Mielenkiintoista on lisäksi *Eurooppa* -sanan käyttö *Euroopan unionin* sijasta. Tätä on huomattavissa melko usein EU:n virallisissa teksteissä. Kyse voi olla joko siitä, että halutaan välttää toistoa, mutta kyse voi olla myös siitä, että EU näkee muidenkin kuin sen jäsenvaltioiden nauttivan Euroopan alueella sen tuottamasta taloudellisesta ja sosiaalisesta hyvinvoinnista sekä turvallisuudesta.

Kolmas dokumenttiaineiston kappale, Josep Borrellin esipuhe vuonna 2022 julkaistavaan Strategiseen kompassiin puolestaan määrittelee selkeästi julkaisunsa syyn heti ensimmäisessä kappaleessa: ”*…tarjota operationaalisia suuntaviivoja, jotta Euroopan unionista voi tulla turvallisuuden tuottaja kansalaisilleen samalla suojaten omia arvojaan ja intressejään.*”[5]. Samalla esipuheen toisessa kappaleessa puhutaan ’*strategisen arvon alennuksesta*’ (alk. engl. ’*strategic shrinkage*’). Käsitettä avataan sivun kaksi lopussa, jossa puhutaan strategisen ympäristön heikentyneestä tilanteesta ja siitä, että eurooppalaiset ajautuvat usein käsitteellisiin tai institutionaalisiin keskusteluihin, kun pitäisi löytää strategiset ja operationaaliset keinot toiminnalle (Borellin esipuhe 2021, 2). Vaikka strategisen kompassin tavoite määritellään sanallisesti

[5] “*…propose operational guidelines to enable the European Union to become a security provider for its citizens, protecting its values and interests*.” (Borellin esipuhe 2021, 1)

heti esipuheen alussa, EU:n '*strategisen arvon alennuksen*' välttäminen tuntuu kuitenkin olevan se keskeisin tavoite, josta kompassin avulla pyritään suunnistamaan ulos.

Strateginen kompassi liittyy vahvasti siihen, että EU kokee strategisen kilpailun kiihtyneen ja turvallisuusuhkien, konfliktien ja epävakauden siementen olevan yhä kompleksisempia (Euroopan unionin ulkosuhdehallinto 2021). EU pelkää, että sen *strateginen arvo ja osaaminen* olisi jollain uhattuna, ja sen vuoksi se tarvitsee uuden strategisen kompassin yhteisten toiminnan raamien kehittämiseksi kohdatessaan näitä uusia ja moninaisia uhkia sekä haasteita (Borrellin esipuhe 2021).

Vaikka '*strategisen arvon alennuksesta*' puhuminen Borrellin esipuheessa tuntuukin kritiikiltä eurooppalaisia kohtaan, läpi koko esipuheen toistuva *me*-dialogi sitoo tekstin tuottajan yhteen ja osaksi eurooppalaisia: "…*meidän pitäisi olla tulosorientoituneita ja välttää meidän tavanomaista eurooppalaista tapaa ajautua käsitteellisiin tai institutionaalisiin keskusteluihin*…"[6] Tekstin tuottajan voidaan olettaa olevan Josep Borrell, ainakin hänet mainitaan tekstin tuottajana. Vahva *me*-dialogin esille tuominen on siis yhteistä Borrellin esipuheelle ja EU:n turvallisuusunionistrategialle.

Tutkimusaineiston tilastoaineistokappaleet, Erityiseurobarometri eurooppalaisten asenteista verkkoturvallisuutta kohtaan (2019) ja Erityiseurobarometri eurooppalaisten suhtautumisesta kyberturvallisuuteen (2020) tavoittelevat kattavaa läpileikkausta eurooppalaisten mielipiteistä. Kuten EU:n turvallisuusunionistrategialla ja kyberturvallisuusstrategialla, eurobarometreillä ei ole selkeää strategian kaltaista tavoitetta, vaan Euroopan komission rahoittamina (Tietoarkisto 2022) ne pyrkivät tuottamaan tietoa päätöksenteon tueksi. Pohdin kyselyiden tavoitteita vielä tarkemmin purkaessani tilastoaineistokappaleissa esiintyvää uhkakuvamäärittelyä.

5.2. Kontekstualisointi

Norman Fairclough'n (2015, 57-58) tulkintaa diskurssista sosiaalisen toiminnan muotona avataan tekstiä ympäröivän kontekstin paikantamisella. Kontekstista antavat viitteitä niin tuottamisprosessin kuin tulkinnallisen prosessin jäljet. Myös James Gee (1996) pitää diskurssianalyysissä keskeisenä niiden viitteiden löytämistä tekstistä, jotka kertovat jotain siitä hetkestä, kun tekstiä on muodostettu. Tässä alaluvussa havainnollistan aineistosta löytyvien viitteiden avulla tekstin kontekstin paikantamista. Lisäksi on hyvä

[6] "…we should be result-oriented and avoid our usual European tendency to go for conceptual or institutional discussions…" (Borrellin esipuhe 2021, 2)

pitää mielessä, että niin aineistokappaleiden tuottajien yksilölliset mielleyhtymät kuin tämän tutkielman tekijän omat mielleyhtymät vaikuttavat tekstin kontekstualisointiin.

5.2.1. Tekstin ja kontekstin suhde dokumenttiaineistossa

Euroopan unionin turvallisuusunionistrategia (2020) on julkinen strategia, jonka lukijakuntana voidaan pitää niin jäsenvaltioiden julkishallinnon työtekijöitä kuin kansalaisia. Dokumentin kieli on tehty helposti ymmärrettäväksi, mikä voisi viitata siihen, että lukijakunnan toivotaan olevan tavallisia kansalaisia. Monet lyhenteet on kirjoitettu auki, mikä kertoo strategian luonteesta julkisena asiakirjana, eikä kyse ole pelkästään asiantuntijoiden kesken vaihdettavasta dokumentista. Koska kyse on kirjoitetusta tekstistä, sekä sen *tuottamisprosessi* että *tulkintaprosessi* ovat olennaisia diskurssin kannalta (Fairclough 2015, 58). Tuottamisprosessin sosiaalisista olosuhteista tiedämme vain sen verran, että tarve uuden turvallisuusstrategian luomiselle on mitä ilmeisimmin ollut jonkin suuruinen EU:ssa. EU:n tiedetään tuottavan tasaisin väliajoin uusia strategioita, kun edellisten strategioiden tavoitteet saavutetaan tai koetaan tarvetta muokata tavoitteita. Sosiaalisen tuottamisprosessin sekä tulkintaprosessin piiriin voisi myös liittää sen, kenen uskotaan lukevan kyseistä dokumenttia. Koska kyse on turvallisuuspoliittisesta strategiasta, dokumentilla voisi ajatella olevan myös sellaisia lukijoita, jotka ovat kiinnostuneita Euroopan unionin heikkouksista ja kyvykkyyksistä suhteessa omiin turvallisuuspoliittisiin tavoitteisiinsa. Strategiassa ei mainita Kiinaa tai Venäjää sanallakaan, mutta yhteistyö puolustusliitto Naton kanssa mainitaan. EU on kuitenkin tietoinen esimerkiksi kyberympäristössä tapahtuvasta tietoisen aktiivisesta disinformaation levittämisestä Venäjän erinäisten toimijoiden toimesta (Carrapico ja Farrand 2020, 1118). Venäjän puolestaan tiedetään suhtautuvan kriittisesti Natoon, ja se vastustaa etenkin Naton laajentumisaikeita (Husu 2022). Todellisten turvallisuuspoliittisten realiteettien vuoksi strategia on hiottu ympäripyöreäksi ulostuloksi, jossa EU:n omat vahvuudet ja heikkouksien paikkaamiset tuodaan esiin parhain päin.

Turvallisuusunionistrategiassa on paljon toistuvia elementtejä, joista on mainittava erityisesti dialogi *eurooppalaisten elämäntapaan kohdistuvien välittömien uhkien* toteamisesta sekä *Euroopan turvallisuusympäristön muutostilan toteaminen*. Näillä halutaan korostaa sitä, että uhat ovat täällä, meidän keskuudessamme ja osa arkipäiväämme. Arkipäiväisyyttä ei sanana mainita dokumentissa kertaakaan, mutta

siihen vahvasti viitataan, kun puhutaan ihmisille arkipäiväisistä asioista kuten kahvinkeittimistä. Kirjoittajat haluavat siis korostaa sitä, että uhat eivät ole enää vain jossain tuolla kaukana vaan ihan lähellä, keskellä jokapäiväistä arkeamme, kiitos digitalisaation. Toinen merkittävä teema, joka turvallisuusunionistrategiassa mainitaan peräti 14 kertaa on perusoikeudet. Usein se mainitaan sanaparina *perusoikeuksien suojeleminen*, *kunnioittaminen* tai *vaaliminen*. Tämä on viittaus EU:lle tärkeään arvomaailmaan, ja tuo heti mieleen Ian Mannersin (2002) kuuluisaksi tekemän normatiivisen vallan Euroopan (Normative Power Europe). Olisiko kyse jonkinlaisesta arvodiskurssista? Palaan tähän pohdintaan seuraavassa luvussa kuusi.

Vuonna 2020 julkaistussa kyberturvallisuusstrategiassa puolestaan viitteitä kontekstista, jossa tekstiä on tuotettu ja tulkittu, antavat lauseet ”[*m*]*aailmassa on jo enemmän verkkoon liitettyjä laitteita kuin ihmisiä, ja niiden määrän odotetaan kasvavan 25 miljardiin vuoteen 2025 mennessä*” (s.1), ”[*k*]*oronaviruspandemia on vauhdittanut työskentelymallien digitalisoitumista entisestään*” (s.1), ”[*u*]*hkia pahentavat geopoliittiset jännitteet*” (s.2) ja ”[*s*]*amaan aikaan viimeaikaiset tapahtumat osoittavat, että EU:n on nostettava tavoitetasoaan ja valmiuttaan selviytyä kyberuhkaympäristössä*” (s.15-16). Tekstin tuottajat ovat tulkinneet verkkoon liitettyjen laitteiden määrän kasvun olevan kriittistä myös kyberturvallisuuden kannalta sekä näkevät geopoliittisten jännitteiden pahentavan uhkakuvia myös kybertoimintaympäristössä ja viittaavat *viimeaikaisiin tapahtumiin*, joiden vuoksi tavoite- ja valmiustasoa pitäisi nyt tässä hetkessä nostaa. Lisäksi tekstiä on tuotettu ainakin osin koronavirsupandemian alettua, ja pandemian vaikutuksia tulkitaan varovaisesti myös tässä strategiassa. Tämä ilmentää selkeästi tekstin *tulkintaprosessia* (Fairclough 2015, 58).

EU:n turvallisuusunionistrategiassa yksilökeskeinen näkökulma on vahvasti läsnä läpi strategian kaikissa kohdissa, joissa puhutaan kyberturvallisuudesta. Yksilökeskeisyydellä tarkoitan tässä yhteydessä sitä, että uhkien korostetaan kohdistuvan digitaalisessa ympäristössä yhä herkemmin yksilöön todeten: ”[*t*]*urvallisuus on ensiarvoisen tärkeää henkilötasolla, mutta se suojelee myös perusoikeuksia sekä luo perustan taloutemme, yhteiskuntamme ja demokratiamme luottamukselle ja dynaamisuudelle*” (EU:n turvallisuusunionistrategia 2020, 1). Euroopan unionin kyberturvallisuusstrategiassa ei nosteta eurooppalaisia yksilöinä samalla tavalla esille. Tämä korostaa kyberturvallisuusstrategian byrokraattisempaa ja teknisempää luonnetta, eikä haluta tuoda esille esimerkiksi tunteisiin vetoavampaa puhetta yksilöön kohdistuvista

kyberuhista. Samalla vahvistuu mielikuva siitä, että kyberturvallisuusstrategian kohdeyleisöksi ei ole ajateltu tavallista EU jäsenvaltion kansalaista, vaan kohderyhmänä olisi nimenomaan EU:n toimielinten sekä jäsenvaltioiden virkahenkilöt, joiden tehtävänä on toimeenpanna strategiassa esitettyjä toimenpiteitä.

Josep Borrellin esipuhe vuonna 2022 julkaistavaan Strategiseen kompassiin taas on luonteeltaan erilainen kuin EU:n turvallisuusunionistrategia ja kyberturvallisuusstrategia. Esipuhe on kuin tehty luettavaksi puheeksi. Strategisen kompassin luonnosversio on esitelty jäsenmaille marraskuussa 2021 (EU:n ulkosuhdehallinto 2021), ja voisi hyvin kuvitella, että Borrell olisi puhunut tämän esipuheen esittelyn yhteydessä. Kieli on hyvin voimakasta ja persoonallista, minkä lisäksi lauseiden väliset tauot ovat kuultavissa. Esipuhe alkaa uhkaavalla sävyllä: ”*Eurooppa on vaarassa*”[7]. Tämä antaa viitteitä kontekstista, jossa puhetta on tuotettu ja tulkittu, nimittäin kiristyneeksi koetusta maailmanpoliittisesta tilanteesta. Euroopan unionin korkea johtaja ei pelottelisi vaaralla lämpimikseen.

5.2.2. Kontekstin paikantaminen tilastoaineistossa

Tuon tässä kohtaa mukaan tarkasteluun tilastoaineistokappaleet tukevana osana muuta tutkimusaineistoa. Tilastoaineiston kontekstualisointi tapahtuu analysoimalla kysyttyjä kysymyksiä ja annettuja vastausvaihtoehtoja. Koska tilastoaineistokappaleita on kaksi, pystyy tarkastelussa hyödyntämään vertailua. Tilastoaineiston kontekstualisointi on olennaista, kun halutaan tarkastella sitä, mihin tilastoaineistokappaleista saatavilla tuloksilla pyritään vaikuttamaan.

Erityiseurobarometri eurooppalaisten asenteista verkkoturvallisuutta kohtaan (2019) on kattava läpileikkaus ihmisten arkipäiväiseen käyttäytymiseen internetissä. Haastatteluina toteutettu kyselytutkimus purkaa yksityiskohtaisesti kansalaisten internetin käyttöön liittyviä tilanteita, huolenaiheita sekä kertoo kattavasti myös kyselyyn vastanneiden poliittisista, sosiaalisista ja taloudellisista taustoista. Koska kyselyssä tarjotaan vastausvaihtoehdot jokaisen kysymyksen kohdalla, vastaajan on täytynyt pohtia, mikä annetuista vastauksista vastaa hänen tilannettaan tai hänen tuntemuksiaan. Näin ollen vastaamista ei voi kuvata spontaaniksi vastauksen antamistilanteeksi, jossa vastaaja kertoisi ensimmäisestä mielikuvasta, mikä hänelle tulee kysymyksestä mieleen. Ainoa

[7] ”*Europe is in danger*” (Borrellin esipuhe 2021, 1).

poikkeus tehdään kysymyksessä kuusi, jossa vastaajaa pyydetään pohtimaan alle 16-vuotiaiden lasten kokemaa ahdistelua verkossa (esim. kiusaaminen tai seksuaalinen hyväksikäyttö), ja mitä tai onko mitään tehty omassa kotitaloudessa lasten suojelemiseksi internetissä. Tämän kysymyksen kohdalla kyselyn tekijää pyydetään erityisesti jättämään näyttämättä vastausvaihtoehdot. Vaihtoehdot on kuitenkin lopulta koodattu kahdeksaksi eri vastausvaihtoehdoksi tämänkin kysymyksen kohdalla. Joka tapauksessa kyselyn tuloksiin on suhtauduttava tietyllä varovaisuudella juuri sen vuoksi, että vastausvaihtoehdot on esitetty annettuina vastaajille vastaustilanteessa.

Toinen kysely, Erityiseurobarometri eurooppalaisten suhtautumisesta kyberturvallisuuteen (2020) noudattaa kysymysten suhteen samanlaista kaavaa kuin vuotta aiemmin suoritettu kyselytutkimus eurooppalaisten asenteista verkkoturvallisuutta kohtaan. Kysymyspatteristo on lähes sama, pienillä nyanssieroilla, mutta vastausvaihtoehdot tarjotaan jälleen, ja ne ovat samat. Yhtenä eroavaisuutena tutkimusten välillä voisi mainita ensimmäisen kysymyksen, jossa tiedustellaan, mitä laitetta vastaaja käyttää päästäkseen internetiin. Tuoreemmassa, suhtautumista kyberturvallisuuteen mittaavassa tutkimuksessa on eroteltu pöytätietokone ja kannettava tietokone toisistaan, kun vuotta vanhemmassa tutkimuksessa puhuttiin vain tietokoneesta. Tämän takia vuotta vanhemmassa verkkoturvallisuutta käsittelevässä tutkimuksessa 85 prosenttia vastaajista sanoo käyttävänsä tietokonetta päästäkseen internetiin, kun uudemmassa kyberturvallisuutta käsittelevässä tutkimuksessa 41 prosenttia sanoo käyttävänsä pöytätietokonetta ja 51 prosenttia kannettavaa tietokonetta. Tämä antaa viitteitä kontekstista, jossa kyselyn tekijät ovat selkeästi halunneet täsmentää vastausvaihtoehtoa tietokoneen käytöstä, koska teknologia kehittyy koko ajan ja käyttäjien laitteetkin muuttavat muotoaan. Myös älypuhelimen käytön voidaan päätellä yleistyneen internetin käytön laitteena, sillä 2019 kyselyssä 79 prosenttia vastaajista käytti älypuhelinta internetin selaamiseen, kun 2020 julkaistussa kyselyssä osuus oli jo 85 prosenttia.

Molemmat kyselyt keräävät tarkkoja tietoja myös vastaajien sosiaalisista taustoista, kuten kotitalouksien koosta, perhesuhteista sekä poliittisista mielipiteistä. Verkkoturvallisuutta käsittelevä Eurobarometri (2019) pyytää vastaajia nimeämään itsensä johonkin yhteiskuntaluokkaan kuuluvaksi kun taas kyberturvallisuutta käsittelevä Eurobarometri (2020) on tiedustelee vastaajilta, miten paljon he seuraavat ja keskustelevat lähipiirissään niin kansallisesta kuin eurooppalaisesta politiikasta. Tässä kyselyssä tiedustellaan myös vastaajan suhtautumista Euroopan unioniin. Verkkoturvallisuutta käsittelevä Eurobarometri (2019) jaottelee vastauksia iän ja sukupuolen mukaan sekä tarjoaa

vastausten tarkastelun myös eri yhteiskuntaluokkien välillä. Kyberturvallisuutta käsittelevä Eurobarometri puolestaan jaottelee vastaukset prosenttiosuuksineen EU:n jäsenvaltioiden mukaisesti.

Kyselyt paljastavat hyvinkin yksityiskohtaisia tietoja EU-kansalaisten verkkokäyttäytymisestä, muun muassa siitä, millaisia laitteita ja mihin tarkoituksiin internetiä käytetään. Lisäksi kyselyissä käsitellään kansalaisten kokemia huolenaiheita, joita heillä liittyy internetin ja verkkopalveluiden käyttöön, ja pelkäävätkö he esimerkiksi joutuvansa kyberhyökkäyksen tai kyberrikollisuuden uhriksi. On hyvä, että tämän kaltaista yksityiskohtaista tietoa kerätään, se hyödyttää viranomaisia, kun he pohtivat toimia kyberturvallisuuden parantamiseksi. Toisaalta tämän tyyppinen yksityiskohtainen tieto voi yhtä lailla hyödyttää myös sellaisia tahoja, jotka haluavat hyödyntää kybertoimintaympäristössä käyttäjien heikkouksia. Molemmissa kyselyissä esimerkiksi kysytään (kysymys neljä), mihin palveluun vastaaja on vaihtanut vai onko vaihtanut ollenkaan salasanaansa viimeisen 12 kuukauden aikana. Vastausprosentit ovat verkkoturvallisuutta käsittelevässä Eurobarometrissä (2019) jokaisen eri vastausvaihtoehdon kohdalla alle 50 prosenttia, jopa alle kymmenen prosenttia on vaihtanut salasanan viimeisen 12 kuukauden aikana julkishallinnon verkkopalvelutileille. Tämä on tärkeää tietoa sellaisille tahoille, kuten verkkorikollisille, jotka pyrkivät varastamaan verkkopalveluiden käyttäjien tietoja tai hyödyntämään heidän laitteitaan tai tilejään oman toimintansa salaamiseksi. Lisäksi tietynlaisten kyberturvallisuuteen liittyvien huolenaiheiden tiedustelu kansalaisilta voi hyödyttää enemmän niitä, jotka haluavat tehdä tavallisille verkkoalustojen käyttäjille hallaa.

Yleisesti voidaan valittujen tilastoaineistojen pohjalta todeta, että eurooppalaiset kokevat jollain tasolla olevansa huolissaan erilaisista kyberuhista niin palvelunestohyökkäyksistä, identiteettivarkauksista kuin kyberrikollisuudesta ylipäänsä. Molemmat Eurobarometrikyselyt paljastavat, että osa kokee olevansa heikosti informoitu kyberrikollisuuden rikseistä. Verkkoturvallisuutta käsittelevässä Eurobarometrissä (2019) peräti 51 prosenttia vastaajista koki olevansa ”*heikosti informoitu*” (alk engl. ”*not well infomed*”, alk. ransk. ”*pas bien informé*”) ja kyberturvallisuutta käsittelevässä Eurobarometrissä (2020) 47 prosenttia koki olevansa ”*heikosti informoitu*” kyberrikollisuuden riskeistä. Tämän voisi tulkita viittaavan siihen, että niin kansallisen tason kuin EU-tason viesti kyberturvallisuuspolitiikasta ei ole täysin tavoittanut kansalaisia. Heikko informaation taso näkyy esimerkiksi siinä, että kansalaiset eivät aina tienneet, keneen ottaa yhteyttä, jos saavat epäilyttävän sähköpostiviestin tai soiton

kysellen henkilökohtaisia tietoja. Kyseisessä tilanteessa vain 38 prosenttia vastaajista olisi yhteydessä poliisiin (Erityiseurobarometri eurooppalaisten suhtautuminen kyberturvallisuuteen 2020).

5.3. Uhkakuvien määrittely

Uhkakuvien määrittely on leimallista turvallisuuspoliittisille strategioille. Samalla uhkakuvien määrittelyä voi tulkita kriittisen turvallisuustutkimuksen näkökulmasta. Tässä alaluvussa käyn läpi aineistokappaleista löytyviä esimerkkejä uhkakuvien esille tuomisesta. Jatkan samalla kriittisen diskurssianalyysin työkalujen käyttöä dokumenttien analysoimiseen. Dokumenttikappaleissa uhkakuvamäärittely on suorempaa, mutta myös tilastoaineistokappaleet paljastavat toisenlaista uhkakuvien esittelyä.

5.3.1. Uhkakuvien esittely dokumenttiaineistossa

Euroopan unionin turvallisuusunionistrategiassa (2020) nimetään hyvinkin avoimesti ne uhat, jotka esimerkiksi kansalaisiin arkipäiväisessä elämässä saattavat kohdistua: ”*Kun jopa pienet verkkoon yhteydessä olevat kodinkoneet (esimerkiksi jääkaappi ja kahvinkeitin) voivat aiheuttaa tietoturvariskin.*” (EU:n turvallisuusunionistrategia 2020, 5). Kyseisellä esimerkillä jääkaapista ja kahvinkeittimestä turvallisuuteen liittyvät uhkakuvat tuodaan hyvin lähelle ihmisen arkipäiväisiä tilanteita. Tämä korostaa sitä seikkaa, että tavallinen kansalainen, joka turvallisuusunionistrategiaa lukee, saadaan kiinnostumaan omasta turvallisuustilanteestaan ja toivomaan parannuksia heikentyneelle tai murroksessa olevalle tilanteelleen. Kriittisen turvallisuustutkimuksen näkökulmasta tämä on yksi keino luoda ja vakiinnuttaa turvallisuuskäytänteitä ja etenkin luoda oikeutus uusien turvallisuutta lisäävien mekanismien käyttöönottamiselle (Vuori 2014, 37, Buzan ja Hansen 2009, 217).

Mielenkiintoa herättää myös *voida* -sanan indikatiivin käyttö toistuvasti pitkin turvallisuusunionistrategiaa: EU *voi* auttaa, EU *voi* muodostaa, EU *voi* tarjota, EU *voi* näyttää. Tämä luo kuvaa Euroopan unionista, jolta kyllä löytyy keinoja niin turvallisuusuhkien torjumiseen, uusien innovaatioiden kehittämiseen kuin tulevaisuuden turvaamiseen. Onko tämä viesti kenties niille tahoille, jotka eivät ole turvallisuuspolitiikassa Euroopan unionin kumppaneita?

Sen lisäksi, että turvallisuusunionistrategissa puhutaan suhteellisen suoraan uhkista ja nimetään niitä, strategiassa nimetään myös kyberhyökkäysten tekijöitä:

> ”(1) *Hyökkäykset ovat kehittyneempiä kuin koskaan, ne ovat peräisin useista eri lähteistä EU:ssa ja sen ulkopuolella, ja niitä kohdistetaan erityisen haavoittuviin alueisiin.* (2) *Niiden taustalla on usein valtioita tai valtion tukemia toimijoita, jotka valitsevat kohteikseen keskeisiä digitaalisia infrastruktuureja, kuten suuria pilvipalvelujen tarjoajia.*” (EU:n turvallisuusunionistrategia 2020, 8.)

EU:n turvallisuusunionistrategia nimeää *valtiot* tai *valtion tukemat toimijat* todennäköisiksi kyberhyökkäysten tekijöiksi, ja kohteina ovat usein ”*keskeiset digitaaliset infrastruktuurit*”. Tämän perusteella vaikuttaa siltä, että EU on hyvin tietoinen, kuka senkin kriittiseen infrastruktuuriin kyberoperaatioita kohdistaa. Toisaalta valtiollisten tahojen tuki useimmille merkittävimmille kyberoperaatioille on toki yleinen olettamus, ja näin oletettiin esimerkiksi Viroon kohdistuneen laajan kyberhyökkäyksen kohdalla, jolloin epäilyt kohdistuivat vihamielisesti käyttäytyvään Venäjään (McGuinness 2017).

> ”(1) *Teknologia luo yhteiskunnalle uusia mahdollisuuksia.* (2) *Se myös tarjoaa uusia välineitä oikeuslaitoksen ja lainvalvonnan käyttöön.* (3) *Samalla se kuitenkin avaa ovia rikollisille.* (4) *Haittaohjelmat, henkilö- tai yritystietojen varastaminen hakkeroimalla ja digitaalisen toiminnan katkaiseminen aiheuttavat taloudellista vahinkoa tai tahraavat mainetta.* (5) *Vahvan kyberturvallisuuden tarjoama selviytymiskykyinen ympäristö on paras puolustus näitä vastaan*.” (EU:n turvallisuusunionistrategia 2020, 12.)

Oheinen kappale on EU:n turvallisuusunionistrategian neljännen luvun toisesta alaluvusta ”*Reagointi muuttuviin uhkiin – Kyberrikollisuus*”. Jos kappaletta kuuntelee, kuulostaa ensimmäinen sekä toinen lause positiiviselta, mahdollisuuksia luovalta, kun taas kolmas ja neljäs lause tuovat tumman pilven aiempien virkkeiden ylle. Viimeinen virke tuo jälleen toivon pilkahduksen. Kappale vaikuttaa imitoivan hampurilaistekniikkaa, jossa ikävä asia on puettu keskelle virkkeisiin kolme ja neljä, ja esitetään kahden positiivisen asian jälkeen. Ensimmäiset kaksi lausetta ovat lyhyitä, vaikka ne voisi hyvin yhdistää yhdeksi virkkeeksi. Lauseiden lyhyydellä terävöitetään ilosanomaa teknologian luomista mahdollisuuksista kuten myös ovien avaamisesta rikollisille. Lyhyet lauseet luovat selkeyttä. Hampurilaisesimerkissä on havaittavissa koheesion piirteitä. Lyhyet lauseet liittyvät yhteen sidossanoilla *myös* ja *samalla*. Sen sijaan itse liima virkkeiden välillä tuntuu kuitenkin olevan useammin asioiden merkityksissä, jotka liittyvät jollakin tavalla toisiinsa, eikä itse sidossanoilla ole kovin suurta merkitystä kyseisessä asiatekstissä.

Oheisessa turvallisuusunionistrategian kappaleessa kontekstualisoivat signaalit *vahva kyberturvallisuus*, *selviytymiskykyinen* ja *paras* kertovat siitä, että EU on jo kehittänyt tai kehittämässä keinoja, joilla kyberrikollisuuteen voidaan puuttua, ja kyberturvallisuuden vahvistaminen on yksi niistä keinoista. Yleisesti kontekstualisointia on havaittavissa turvallisuusunionistrategiassa esimerkiksi viitauksilla siihen, että turvallisuusuhat ovat yhä lähempänä ihmisten arkipäiväistä elämää. Tällä pyritään luomaan kiireen tuntua (Locke 2004, 59), että nyt on toimittava nopeasti, koska tavallinen arkipäiväinen elämäkin on uhattuna.

Diskurssien rakenne, Geen (1996) analyysikehikon mukaisesti muodostuu turvallisuusunionistrategiassa hampurilaistekniikan avulla. Olennaista on tässä kohtaa huomioida dokumentin luonne, eli kyse on strategiasta. Strategia on toimintasuunnitelma, jonka avulla pyritään luomaan raamit toiminnalle tai ongelmatilanteelle (Kielitoimiston sanakirja 2022a). Tämän strategian tehtävä on alleviivata muuttunutta turvallisuustilannetta, antaa työkalut sekä toiminnan raamit muuttuneessa tilanteessa selviämiseksi. Strategian merkitys ohjaa tämän dokumentin rakentumista. Sama pätee kyberturvallisuusstrategian kohdalla.

Euroopan unionin kyberturvallisuusstrategiassa (2020) uhkakuvien määrittely on toisaalta samanlaista, mutta myös erilaista kuin turvallisuusunionistrategiassa. Oheinen kappale mukailee diskursiivisesti turvallisuusunionistrategian kaltaista uhkakuvamäärittelyä, mutta omaa sisällöllisesti erilaiset tavoitteet:

> ”(1) *Uhkia pahentavat geopoliittiset jännitteet, joita liittyy maailmanlaajuiseen ja avoimeen internetiin ja teknologian hallintaan koko toimitusketjussa.* (2) *Nämä jännitteet näkyvät siinä, että yhä useammat valtiot rakentavat digitaalisia rajoja…* (3) *Kybertoimintaympäristöä käytetään yhä enemmän poliittisiin ja ideologisiin tarkoituksiin, ja lisääntyvä polarisoituminen kansainvälisellä tasolla haittaa tehokasta monenvälisyyttä.*” (EU:n kyberturvallisuusstrategia 2020, 2.)

Ensinnäkin on erityisen mielenkiintoista, että kyberturvallisuusstrategia nimeää geopoliittiset jännitteet kyberuhkia pahentaviksi, mutta jättää tekstin lukijan tulkinnan varaan sen, mistä geopoliittisista jännitteistä on kyse. Tämä kertoo kuitenkin jotain tekstin tuottajan tulkintaprosessista ja lukija voi tehdä omia mielleyhtymiä peilatessaan tekstiä todelliseen sosiaaliseen maailmaan. Digitaalisten rajojen rakentaminen tuntuisi viittaavan esimerkiksi Kiinaan, joka on rakentanut oman digitaalisen muurin (alk. engl. Great Firewall of China), jonka avulla valtio kontrolloi ja säätelee kansalaistensa toimintaa

kyberulottuvuudessa (Griffiths 2019, 8). Kiinalaisilla ei ole pääsyä esimerkiksi länsimaisiin viestipalveluihin kuten Twitteriin (Horng-En Wang, Lee, Wu ja Shen 2020, 472). EU pyrkii selkeästi tällä strategialla toimimaan päinvastaisesti Kiinaan verrattuna, sillä kyberturvallisuusstrategian tavoitteena on ”*varmistaa maailmanlaajuinen ja avoin internet*” (s.5). Tekstin viimeistä virkettä tarkasteltaessa huomio kiinnittyy ”*poliittisiin ja ideologisiin tarkoituksiin*” sekä ”*lisääntyvään polarisaatioon kansainvälisellä tasolla*”.

Diskursiivisesta näkökulmasta tarkasteltuna oheinen kappale EU:n kyberturvallisuusstrategiassa ikään kuin lisää yhden kerroksen uhkakuvien päälle kertoen, mitkä tekijät pahentavat ja lisäävät uhkien painavuutta. Teksti on hyvin painavaa ja realistiseen näkökulmaan taipuvaista. Kontekstualisoivana signaalina toimii itse sana geopoliittiset jännitteet viitaten joihinkin turvallisuuspoliittisiin tapahtumiin, joita ei tarkemmin tässä yhteydessä avata. Kappaleessa diskurssin rakenne on kuitenkin erilainen kuin turvallisuusunionistrategiassa paikannettu hampurilaistekniikka. Tässä kappaleessa ei leivota ikävää asiaa keskelle, eikä tarjota ratkaisuja ikäville uhkille.

Josep Borrellin strategisen kompassin esipuheessa (2021) puolestaan uhkakuvien määrittely on avointa, mutta abstraktia:

> ”(1) *Strategisen kompassin aloituspiste on se, että Eurooppa on vaarassa.* (2) *Se kohtaa uudenlaisia uhkia, jotka eivät ole pelkästään sotilaallisia tai alueellisia*. (3) *Näemme voimapolitiikan ja nollasummakonfliktien paluun, kun valtioiden välinen kilpailu kiihtyy.* (4) *Samanaikaisesti keskinäisriippuvuudesta on tulossa kasvavissa määrin konfliktinomaista ja pehmeän vallan käyttökin aseistetaan*.”[8]

Yllä olevaa kappaletta analysoitaessa diskursiivisesti on huomattavissa, että prosodian kannalta teksti kuulostaa uhittelevalta ja raskaan negatiiviselta. Tilanne ei suoraan sanottuna kuulosta kovin hyvältä. Kappaleessa määritellään selkeästi uhkakuvatilanne, vaikka ei sen tarkemmin indikoida, millaisia nämä *uudenlaiset uhat* ovat. Kontekstualisoivina signaaleina toimivat sanat kuten *uudenlaisia*, *näemme* (alk. engl. *we are seeing*) ja *samanaikaisesti*. Tekstin tuottaja ja tulkitsija on elänyt tai elää sosiaalisissa olosuhteissa, joissa kokee turvallisuusuhkien muuttuneen ja voimapolitiikan palanneen kansainvälisiin suhteisiin. Tekstin konteksti on tekstiä analysoidessa myös tulkitsijalle hyvin tuttu, sillä turvallisuuspoliittisen tilanteen kiristymistä etenkin länsimaiden ja

[8] ”*The starting point of the Strategic Compass is to recognize that Europe is in danger. It faces new threats that are not just military or territorial. We are seeing the return of power politics and zero sum conflicts with competition between states intensifying. At the same time, interdependence is becoming increasingly conflictual and soft power is weaponized*.”

Venäjän välillä ei voi olla huomaamatta päivittäisiä uutisia lukiessa (Helsingin Sanomat pääkirjoitus 4.2.2022). Esipuheen kappaleessa koheesiota luovat sanat *se* virkkeiden yksi ja kaksi välissä sekä *samanaikaisesti* virkkeiden kolme ja neljä välissä. Tämä tekee diskurssista sulavaa. Sisällöllisesti oheisen kappaleen tarkoituksena on perustella Strategisen kompassin tarkoitusta, ja teksti on perustelevaa samalla tavoin, kuin turvallisuusunionistrategian ja kyberturvallisuusstrategian kohdalla. Kokonaisuudessaan tämän Strategisen kompassin esipuheen diskursiivinen rakenne on tarinamaisempi kuin aiemmin analysoitujen strategioiden. Esipuhe kuitenkin eroaa luonteeltaan strategioista, sillä esipuhe toimii julkaistun teoksen saatesanoina (Kielitoimiston sanakirja 2022b). Esipuheen tehtävänä on siis pohjustaa itse teosta, joka voi hyvin olla niin kaunokirjallinen teos kuin viranomaistekstikin. Se selittää osin esipuheen vapaampaa kirjoitusotetta verrattuna strategioihin, ja strategisen kompassin varsinainen sisältö tulee varmasti olemaan myös strategian omainen.

5.3.2. Millä tavalla uhkakuvia tuodaan esille tilastoaineistossa?

Kansalaisten kyberturvallisuuteen liittyviä pelkoja tunnutaan testaavan vahvasti sekä Erityiseurobarometrissa eurooppalaisten asenteista verkkoturvallisuutta kohtaan (2019) että Erityiseurobarometrissa eurooppalaisten suhtautumisesta kyberturvallisuuteen (2020). Voisiko kyselyiden kysymysten ohjaavalla luonteella olla myös toinenkin merkitys, nimittäin tietoisuuden lisääminen kansalaisten keskuudessa kybertoimintaympäristöön liittyvistä riskeistä? EU:n turvallisuusunionistrategia (2020) kuin kyberturvallisuusstrategia (2020) painottavat kattavaa lähestymistapaa kyberturvallisuuteen, jossa halutaan tuoda kansalaiset ja heidän kybertoimintansa osaksi kyberturvallisuuden kokonaisvaltaista ymmärrystä: ”*yksityishenkilö on osa ratkaisua, jolla varmistetaan kyberturvallinen digitaalinen siirtymä*” (EU:n kyberturvallisuusstrategia 2020, 28). Kenties kyseinen ajattelutapa heijastuu jo tarkasteluun valituissa kyselyissä, jotka on suoritettu ennen turvallisuusunioni- ja kyberturvallisuusstrategioiden laatimista. Toinen vaihtoehto on, että kyselyiden perusteella on huomattu, että kansalaisten tietoisuus kybertoimintaympäristön tietoturvariskeistä on heikkoa.

Jos tarkastelee molempien Erityiseurobarometrien keskeisiä kysymyksiä (kysymyksen kahdeksan alakysymykset), joissa vastaajia pyydetään kertomaan ”*miten huolissaan olet*

henkilökohtaisesti seuraavanlaisen tilanteen kokemisesta tai sen uhriksi joutumisesta"[9] ja valitsemaan vastausvaihtoehdoista itselleen sopivin, suurta hajontaa ei ole löydettävissä vastauksissa eri ammattikuntien, eri sosiaaliseen luokkaan itsensä luokittelevien kuin eri jäsenvaltioidenkaan välillä. Prosentuaalisesti juuri missään tarkastellussa ryhmässä, tai kaikki vastaajat yhteen laskettuina, ensimmäinen vastausvaihtoehto "*erittäin huolissaan*" (alk. engl. *very concerned*, alk. ransk. *très inquiet*/i*nquiète*) ei ylitä 50 prosenttia. Pieni poikkeus on molemmissa kyselyissä alakysymys 8.9, joka tiedustelee sitä, *miten huolissaan vastaaja on henkilökohtaisesti pankkikortin tai verkkopankkitunnusten varastamisesta*[10]. Tämän kysymyksen kohdalla kyberturvallisuutta käsitelevässä eurobarometrissa (2020) latvialaisten vastaajien vastausosuus "*erittäin huolissaan*" -vastausvaihtoehdolle on 55 prosenttia, ja espanjalaisista sekä irlantilaisista 49 prosenttia vastaa olevansa "*erittäin huolissaan*". Taulukko kuusi havainnollistaa vastaustuloksia kyseisen kysymyksen kohdalla.

[9] alk. engl.:*How concerned are you personally about experiencing or being a victim of the following situations?*" (Erityiseurobarometri eurooppalaisten suhtautuminen kyberturvallisuuteen 2020).
[10] Kysymys 8.9 alk. engl: *Bank card or online banking fraud* (Erityiseurobarometrit eurooppalaisten asenteet verkkoturvallisuutta kohtaan 2019 ja eurooppalaisten suhtautuminen kyberturvallisuuteen 2020).

Erityiseurobarometreissä esitetty kysymys (8.9): ***Miten huolissaan olet henkilökohtaisesti seuraavanlaisen tilanteen kokemisesta tai sen uhriksi joutumisesta: pankkikortin tai verkkopankkitunnusten varastaminen.***			
”*Erittäin huolissaan*” -vastausvaihtoehdon vastausprosentit	Vastaajien määrä yhteensä (EU28)	Prosenttiosuus (EU28)	Latvia
Erityiseurobarometri eurooppalaisten asenteet verkkoturvallisuutta kohtaan (2019)	7058	32%	
Erityiseurobarometri eurooppalaisten asenteet kyberturvallisuutta kohtaan (2020)	7455	32%	462, 55%

Taulukko 4. Vastaukset yhteensä ”Erittäin huolissaan” -vastausvaihtoehdolle molemmissa Erityiseurobarometreissa kysymykselle pankkikortin tai verkkopankkitunnusten varastamisesta.

Tämän Erityiseurobarometrien tarjoaman esimerkin avulla ei voi tehdä täysin aukottomia johtopäätöksiä. Sen voisi kuitenkin päätellä, että yleisesti eurooppalaiset eivät vaikuta olevan kovin huolissaan muun muassa pankkikortin tai verkkopankkitunnustensa varastamisesta digitaalisia palveluita käyttäessään. Vastausprosentti ”*erittäin huolissaan*” -vastausvaihtoehdolle on lähes samaa 30 prosentin luokkaa yhteensä myös muiden ”*miten huolissaan olet*” -alakysymysten kohdalla. Toki jos pankkikortin ja verkkopankkitunnusten varastamista koskevat vastausvaihtoehdot ”*erittäin huolissaan*” ja ”*melko huolissaan*” (alk. engl. *fairly concerned*, alk. ransk. *plutot inquiet/inquiète)* lasketaan yhteen, kyberturvallisuutta käsittelevässä Eurobarometrissa (2020) vastaustulos nousee 67 prosenttiin (15544 vastaajaa). Annettujen vastausvaihtoehtojen takia hämärtyy kuitenkin se, ovatko kansalaiset todella huolissaan pankkikortin tai

verkkopankkitunnustensa varastamisesta digitaalisia palveluita käyttäessään vai liittyykö asiaan esimerkiksi tietämättömyyttä tietoturvaan ja tietoturvariskeihin liittyvistä asioista. Toisaalta uhista ollaan huolissaan, mutta ovatko kansalaiset tarpeeksi huolissaan heihin kohdistuvista uhista kyberympäristössä vai luottavatko he viranomaisiin muun muassa avun tarjoajina hädän hetkellä? Ainakin lähes puolet koki molemmissa Eurobarometreissä olevansa ”*heikosti informoitu*” kyberrikollisuuden riskeistä (verkkoturvallisuutta käsittelevässä Eurobarometrissä (2019) peräti 51 prosenttia vastaajista ja kyberturvallisuutta käsittelevässä Eurobarometrissä (2020) 47 prosenttia vastaajista). Tällä saralla on siis selvästi vielä tehtävää, mikäli Euroopan unioni haluaa, että ”*tavallisten kansalaisten pitäisi tuntea edes perusasiat kyberturvallisuudesta, jotta he voisivat suojautua näiltä uhilta*” (EU:n turvallisuusunionistrategia 2020, 5).

5.4. Millaista vallankäyttöä aineistokappaleissa on havaittavissa?

Tässä viidennen luvun viimeisessä alaluvussa havainnollistan, millä tavalla valta ilmenee diskurssin takana valituissa aineistokappaleissa. Vallan ja diskurssin suhteen paikantaminen on olennaista myös seuraavassa luvussa kuusi tarkasteltavien hegemonisten diskurssien kannalta.

Jotta voi analysoida vallan luonnetta kahdessa virallisessa strategiassa sekä yhdessä esipuheessa, on nostettava esille jälleen strategian kaltaisen dokumentin luonne sekä aineistoon valikoituneiden dokumenttien konteksti. Ensinnäkin strategiaa voi pitää vakiintuneena ja globaalina sosiaalisena rakennelmana samalla tavalla kuin lehtiuutinen rakentuu lukijalle ennalta ennakoitavalla tavalla (Fairclough 2001b, 114-115). Strategiaa lukiessa lukijan tulisi siis tietää, mihin dokumentilla pyritään johtuen siitä, että sosiaalisen vuorovaikutuksen muodostamat rakennelmat odottavat tietyiltä teksteiltä tietynlaista ulosantia (emt.). Tekstin argumentoivan ja toiminnalle perusteluita hakevan luonteen ei siis pitäisi tulla lukijalle yllätyksenä, mikäli on tietoinen strategian merkityksestä osana sosiaalista rakennelmaa. Kun Euroopan unionin turvallisuusunionistrategiassa (2020, 12) todetaan, että ”[*k*]*yberrikollisuus on maailmanlaajuinen haaste*” lukija myös ottaa tämän toteamuksen annettuna ja etsii jo strategian seuraavasta virkkeestä esitettyä ratkaisuvaihtoehtoa tälle haasteelle. Tämä on eräänlaista vallankäyttöä, jota tekstin tuottaja harjoittaa. Samalla tekstin tuottaja ylläpitää olemassa olevia, *universaaleja käytänteitä* ja *diskurssin muotoja* Fairclough’n (2001b, 62) sanoin, *mielen teroittamisen* kautta. Lukija ymmärtää tekstin sellaisena kuin se on kirjoitettu, hyväksyen strategialle ominaisen luonteen, mikä edelleen ylläpitää ja samalla

rajoittaa osaamisia ja uskomuksia, sosiaalisia suhteita sekä sosiaalisia identiteettejä yhteiskunnassamme.

Tarkastelen seuraavaksi EU:n kyberturvallisuusstrategian (2020) sivulta neljä löytyvää väittämien sävyttämää kappaletta. Kyseinen kappale on diskursiivisesti sekä valtasuhteiden näkökulmasta mielenkiintoinen.

> ”(1) *EU:lla ei ole yhteisiä tilannetietoja kyberuhkista.* (2) *Tämä johtuu siitä, että kansalliset viranomaiset eivät kerää ja jaa järjestelmällisesti tietoja, esimerkiksi yksityiseltä sektorilta saatavia tietoja, jotka voisivat auttaa arvioimaan kyberturvallisuuden tilaa EU:ssa.* (3) *Jäsenvaltiot ilmoittavat vain murto-osasta poikkeamia, eikä tietojen jakaminen ole järjestelmällistä eikä kattavaa.* (4) *Kyberhyökkäykset saattavat olla vain yksi osa keskitettyjä vihamielisisiä hyökkäyksiä eurooppalaisia yhteiskuntia vastaan.* (5) *Tällä hetkellä jäsenvaltiot antavat toisilleen vain vähän operatiivista apua, eikä jäsenvaltioilla ja EU:n toimielimillä, virastoilla ja elimillä ole yhteistä operatiivista mekanismia laajamittaisten rajat ylittävien kyberturvallisuuspoikkeamien tai -kriisien varalta*.” (EU:n kyberturvallisuusstrategia 2020, 4.)

Prosodian näkökulmasta oheinen kappale kuulostaa negatiivissävytteiseltä, jopa syyttelevältä: ”*kansalliset viranomaiset eivät kerää*”, ”*jäsenvaltiot antavat toisilleen vähän operatiivista apua*” ja ”*ei ole yhteistä operatiivista mekanismia*”. Samalla virkkeet 1-3 muodostavat argumentin perusteluineen ja seurauksineen. Ensimmäinen virke on argumentti, toinen virke perustelee sitä ja antaa samalla ratkaisun ongelmaan ja kolmas vielä syventää esitettyä ongelmaa. Tämä kertoo oheisen kappaleen diskursiivisesta rakenteesta. Samalla sanat *tämä* ja *tällä* luovat koheesiota virkkeiden välille. Kontekstualisoivina signaaleina voisi pitää sanoja kuten ”*tällä hetkellä*”, ”*vain vähän*”. ”*Tällä hetkellä*” viittaa ainakin vallitseviin sosiaalisiin olosuhteisiin siinä ympäristössä, jossa teksti on tuotettu ja tulkittu. ”*Tällä hetkellä*” voi olla asia, joka nostetaan turvallisuusunionistrategiassa jossain muussa kohtaa esille, esimerkiksi kyse voi olla geopoliittisista jännitteistä, jotka vaikuttavat siihen, että ”*tällä hetkellä jäsenvaltiot antavat toisilleen vian vähän operatiivista apua*”. Mielenkiintoista on, että kyseiseen tilanteeseen viitataan, mutta tilanteen taustoja ei tarkemmin avata.

Oheista kappaletta voidaan tarkastella vallan ja diskurssin vuorovaikutuksen näkökulmasta. Vallan käyttäminen strategiassa on ilmeistä, mutta kyseisessä kappaleessa on paikannettavissa vallanpitäjän suhde vallan kohteeseen. Puheaktin avulla paikannetaan se, mitä tekstin tuottaja pyrkii tekstin nojalla tuottamaan, ja voiko kyse olla monesta puheaktin arvosta samanaikaisesti (Fairclough 2001b, 129). Samalla

tilannekohtaiset ja kontekstiin liittyvät tulkinnat sekä jäsenten resurssit, eli yksilölliset mielleyhtymät vaikuttavat puheaktin arvojen tunnistamiseen (Eero Suoninen 2016; Fairclough 2001b, 129). Puheaktia tulkittaessa on tunnusteltava puhujaa ja vastaajaa, ja sitä, mitä tiedämme heidän sosiaalisesta kontekstistaan.

EU:n kyberturvallisuusstrategian (2020) sivun neljä kappaleesta on paikannettavissa EU:n päälle painava ja jäsenvaltioita kohtaan syyttelevä rooli. EU:sta puhutaan tässä yhteydessä yhtenä instituutiona, sillä tiedossa ei ole tarkalleen ottaen, kuka tai ketkä strategian tekstejä ovat kirjoittaneet. Kyseessä on Euroopan komission tiedonanto Euroopan parlamentille ja Eurooppa-neuvostolle, jotka ovat myös antaneet omat kommenttinsa strategiaan. Puheaktina teksti on kuitenkin syyttelevä jäsenvaltioita kohtaan sen suhteen, että he eivät jaa tietoa tarpeeksi EU:lle kansalliselta tasolta, eivätkä he myöskään tarjoa toisilleen, jäsenvaltiotasolla apua. Tulkintaan puheaktin arvosta vaikuttaa toki tutkielman tekijän ennakkokäsitys siitä, että yhteistyö kyberturvallisuuden parissa on haasteellista EU:ssa sekä horisontaalisesti että vertikaalisesti aiemman tutkimuskirjallisuuden perusteella (mm. Christou 2019 ja Carrapico ja Barrinha 2017).

Tämä tekstin pätkä EU:n kyberturvallisuusstrategian (2020) sivulla neljä puhuttelee kuitenkin lukijaansa poikkeuksellisen napakasti strategian muihin osiin verrattuna. Kun EU (yhtenä instituutiona) toimii puheaktin tuottajana ja oletettavasti jäsenvaltion valtionhallinnon virkamies tekstin lukijana eli tuotteen vastaanottajana, diskurssi kertoo subjektien ideologisesta representaatiosta sekä niiden välisestä sosiaalisesta suhteesta (Fairclough 2001b, 131). Tässä on kyse opitusta käytänteestä ja diskurssin muodosta, joka EU:n ja sen jäsenvaltioiden välillä vallitsee: Euroopan unionilla on institutionaalinen valta, jota se käyttää suhteessa jäsenvaltioihin. Lisäksi on kuitenkin huomioitava, että tekstin tuottajat eivät syytä vain jäsenvaltioita, vaan kuten viidennestä virkkeestä huomataan, EU itsessään ja sen toimielimet joutuvat myös kritiikin kohteeksi. Euroopan unioni syyttää itse itseään luoden puheaktille myös toisenlaisen, itsetutkiskelevan arvon.

Kyberturvallisuusstrategiassa (2020, 15-16) todetaan EU:n halukkuudesta muodostaan yhteinen kyberturvallisuusyksikkö, joka koordinoisi operatiivisesti ja teknisesti merkittävien rajat ylittävien kyberuhkien kyberturvallisuuspoikkeamien torjumista. Yksikön perustamisen kohdalla todetaan, että EU ja sen toimielimet haluavat yhteistyössä jäsenvaltioiden ja muiden asiaankuuluvien kanssa edistää ”*vaiheittaista ja osallistavaa lähestymistapaa kunnioittaen kaikilta osin kaikkien asianosaisten toimivaltuuksia ja toimeksiantoja*” (s.16). Tämä viittaa selkeästi Carrapicon ja Barrinhan (2017, 1266) sekä

Christoun (2019, 291) identifioimiin haasteisiin EU:n kollektiivisen kyberturvallisuuspolitiikan luomiseksi. EU siis todella kokee haasteelliseksi uuden toimielimen (kyberturvallisuusyksikön) luomisen, mikä vaatisi tiiviimpää yhteistyötä ja tiedonvaihtoa jäsenvaltioilta ja muilta toimijoilta. Sen vuoksi se pyrkii jäsenvaltioita kunnioittavasti luomaan edellytyksiä uuden instituution rakentamiselle pehmittelevän *vaiheittaisesti* ja *osallistavasti* (Carrapico ja Barrinha 2017,1266). Jos kyseistä lausetta analysoi puheaktin kautta, paljastaa se erilaisen puheaktin arvon, kuin mitä se aiemmassa esimerkissä paljasti Euroopan unionin ja jäsenvaltioiden välisestä valtasuhteesta. Valta ei ole kuitenkaan poistunut tästä diskurssista, vaan EU edelleen tunnistaa ylläpitävänsä valtaa ja hakee vuorovaikutteisempaa suhdetta vallan alla oleviin tehden puheaktin arvosta sovittelua hakevan.

Euroopan ulkosuhdehallinnon korkea edustaja Borrellin esipuheessa valta piiloutuu mielenkiintoisen kappaleen taakse:

> ”(1) *Euroopan kansalaiset ovat myös tietoisia tästä uudesta kontekstista.* (2) *Useiden mielipidemittausten perusteella, he haluavat EU:n osallistuvan aktiivisemmin heidän turvallisuutensa sekä koko maailman turvallisuuden takaamiseen.* (3) *He haluavat, että EU suojelee heitä tältä vaaralliselta maailmalta, jossa asumme.* (4) *He ymmärtävät, että meidän on yhdistettävä jäsenmaiden puolustukselliset pyrkimykset, vältettävä toiston ja aukkojen vaarat kriittisissä kyvykkyyksissämme, jotta voimme olla tehokkaampia tässä suojelun tuottamisessa*.”[11]

Oheisessa kappaleessa Borrell haluaa tuoda esille EU kansalaisten näkökulmaa turvallisuuspoliittiseen tilanteeseen. Hän väittää kansalaisten olevan tietoisia ”*tästä uudesta kontekstista*”, joka viittaa muuttuneeseen turvallisuustilanteeseen ja geopoliittisiin tapahtumiin. Tämän jälkeen Borrell väittää virkkeissä kaksi ja kolme EU kansalaisten haluavan EU:lta turvallisuuden takaamista ja suojelua. Väitteidensä pohjana hän käyttää ”*useita mielipidemittauksia*”, mutta lukijalle jää epäselväksi, mitä nämä mielipidemittaukset ovat. Tämä ei tee väittämistä kovin päteviä todistuspohjan puuttuessa. Neljäs virke on kenties yllättävin, sillä se menee askeleen pidemmälle ja

[11] ”European citizens are also aware of this new context. According to many opinion polls, they want the EU to contribute in a more active way to their security and that of the world. They want the EU to protect them from the dangerous world we live in. They understand that we must connect the defence efforts of the Member States, avoiding duplications and gaps in our critical capabilities, to be more efficient in providing this protection. And they know that our security starts away from our borders. So we need to project our presence in the world, promoting security in our neighbourhood and with our partners.” (Borrellin esipuhe 2021, 1)

väittää EU-kansalaisten ymmärtävän tarpeen EU:n yhteisille puolustuspyrkimyksille. Tilanne on hullunkurinen, jos EU-kansalaisen itse ajatellaan lukevan tätä esipuhetta. Ikään kuin Borrell EU:n korkean johtajan asemassa sanoisi EU-kansalaiselle: ”*sinähän ymmärrät kuinka vakava tämä tilanne on, joten ymmärrät ja annat hyväksynnän myös sille, että jäsenvaltiot yhdistävät puolustukselliset voimavaransa*”. Tässä yhteydessä *puolustukselliset voimavarat* (alk. engl. *defence efforts*) voidaan ymmärtää nimenomaan EU:n yhteisen turvallisuus- ja puolustuspolitiikan eteenpäin viemisenä, joka on tämän strategisen kompassin keskeinen tavoite.

Valta diskurssin takana ilmenee oheisessa kappaleessa poikkeuksellisesti. Valta-asetelma on selvä, vaikka emme tietäisi, kuka tekstin lukijana ja tulkitsijana toimii. Josep Borrell EU:n ulkosuhdehallinnon korkeana edustajana on vallanpitäjä, joka puhuu vallan kohteelle. Edellä käsitellyssä kappaleessa hän kuitenkin hakee oikeutusta vallalleen toteamalla vallan kohteen eli kansalaisten olevan hänen kanssaan samaa mieltä. Luettuna tekstinä tällainen legitimiteetin hakeminen poliittisille toimille tuntuu vieraalta, universaaleista käytänteistä poikkeavalta, sillä hyväksynnän saaminen todetaan hyvin suoraan tekstissä. Tosiasiassa tämä kuitenkin juuri ylläpitää niitä rajoitettavia tekijöitä (sisältöä, suhdetta ja subjektia) sen kautta (Fairclough 2001b, 62), että vallankäytölle on haettava ainakin näennäisesti jonkinlainen oikeutus, ja tässä oikeutusta haetaan kansalaisten mielipiteiden kautta.

Palaan lopuksi vielä tutkielman tilastoaineistokappaleisiin, sillä yhtä lailla niissä on paikannettavissa vallankäyttöä. Erityiseurobarometrissa eurooppalaisten asenteista verkkoturvallisuutta kohtaan (2019) ja Erityiseurobarometrissa eurooppalaisten suhtautumisesta kyberturvallisuuteen (2020) kysymykset ja vastausvaihtoehdot on määritelty ennakkoon ja ne on esitetty kyselytutkimusta tehtäessä vastaajalle. Tämän voisi katsoa luovan valtasuhteen kyselyn tekijän ja vastaajan välille (Fairclough 2001b, 131), jossa vastaajan vastausvaihtoehdot ovat rajoitetut ja kysymykseen tunnutaan hakevan ohjatusti haluttua vastausta. Kun vastaaja ei saa vastata haluamallaan tavalla, hän on väistämättä kyselyn tekijän vallan alainen. Lisäksi tilastoaineistoiksi koottuihin kyselytutkimuksen tuloksiin ja niiden tulkintaan voi katsoa kohdistuvan vallan käyttöä siinä mielessä, että mihin tarkoitusperiin aineistoja hyödynnetään. Kuten Borrellin esipuheessa (2021) näkyi viittaus ’kansalaisten mielipiteeseen’, yhtä lailla näitä aineistokappaleiksi valittuja Eurobarometrejä saatetaan käyttää päätösten legitimoimiseksi EU:ssa etenkin kun Euroopan komissio rahoittaa Eurobarometrien tuottamisen (Tietoarkisto 2022).

***

Kriittisen diskurssianalyysin työkalut ovat paljastaneet aineistosta kiinnostavia yksityiskohtia niin sisällöllisesti kuin tulkinnan kautta. Kyseisessä luvussa viisi olen tarkastellut aineiston kolmea dokumenttia kriittisen diskurssianalyysin menetelmin sekä kahta tilastoaineistokappaletta sisällönanalyysin ja tulkinnan keinoin. Tässä luvussa olen pyrkinyt avaamaan aineistokappaleiden tavoitteita, kontekstualisoimaan ne sekä esittämään huomioita vallan ilmentymisestä diskurssin takana dokumenteissa sekä tilastoaineistossa. Seuraavassa luvussa kuusi käsittelen keskeisiä hegemonisia diskursseja, joiden löytäminen on ollut mahdollista kriittisen diskurssianalyysin työkalujen avulla ja erityisesti vallan paikantamisella diskursseista. Seuraavassa luvussa jätän tilastoaineistokappaleiden tulkinnan hetkeksi syrjään ja keskityn dokumenttiaineistoon.

6. Hegemoniset diskurssit

Tässä luvussa tarkastelen tutkimusaineiston dokumenteista löytyviä keskeisiä temaattisia diskursseja. Luvussa viisi tarkastelin Euroopan unionin turvallisuusstrategiaa, kyberturvallisuusstrategiaa sekä strategisen kompassin esipuheen kontekstia, tekstien tarkoitusta sekä luonnetta vallan näkökulmasta. Tässä luvussa jatkan vallan analysointia sekä pyrin sitomaan aineistot tiiviimmin yhteen niistä löytyvien diskurssien avulla. Dokumenteissa on paljon samankaltaisia elementtejä, mutta ne ovat tyyliltään ja painotuksiltaan erilaisia, mikä näkyy myös siinä, että niistä löytyy myös erilaisia diskursseja.

Valta sekä vallan käyttö kytkeytyy aina jollakin tavalla keskeisiin diskursseihin, joita myös hegemonisiksi diskursseiksi kutsutaan (Jokinen ja Juhlia 1991, 69). Hegemoninen diskurssi ilmentää yleisintä teemaa tai tapaa suuremmassa sosiaalisessa kokonaisuudessa. Seuraavaksi tarkastelen aineistosta löytyviä hegemonisia diskursseja.

6.1. Uhkakuva- ja arvodiskussin arkipäiväistäminen

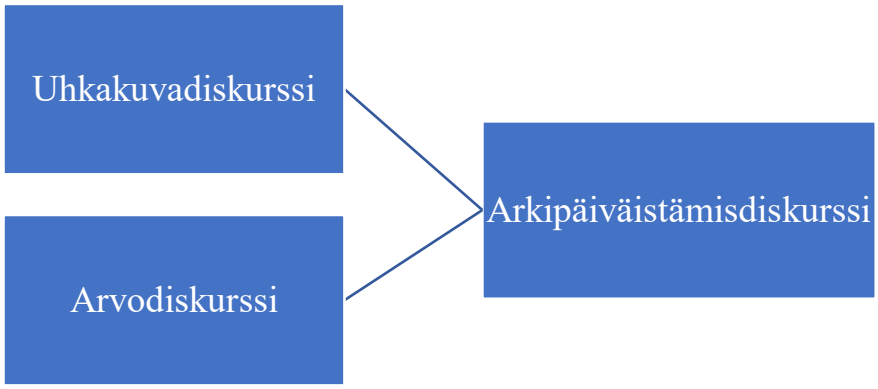
Euroopan unionin turvallisuusunionistrategiassa (2020) sekä kyberturvallisuusstrategiassa (2020) ilmeisin temaattinen diskurssi on uhkakuvadiskurssi. Turvallisuusstrategioina molemmat pyrkivät uhkakuvien määrittelyyn ja määrittelevät toiminnalle tavoitteita uhkakuvien torjumiseksi. Tämä diskurssi on löydettävissä myös Josep Borrellin EU:n Strategisen kompassin esipuheesta. Uhkakuvadiskurssi on paikannettavissa dokumenteissa läpi koko tekstin lauseilla kuten ”[*k*]*yberriskeistä on tullut merkittävä uhka myös rahoitusjärjestelmälle*” (EU:n turvallisuusunionistrategia 2020, 8), ”[*h*]*aittaohjelmat, henkilö- tai yritystietojen varastaminen hakkeroimalla ja digitaalisen toiminnan katkaiseminen aiheuttavat taloudellista vahinkoa tai tahraavat mainetta*” (EU:n turvallisuusunionistrategia 2020, 12), ”*vihamieliset hyökkäykset ovat maailmanlaajuinen riski*” (EU:n kyberturvallisuusstrategia 2020, 2) ja ”*Eurooppa on vaarassa*” (Borellin esipuhe 2021, 1). Samalla uhkakuvadiskurssi on juuri se temaattinen diskurssi, jonka tekstin tuottaja haluaa näistä strategioista ja esipuheesta lukijalle välittää. Valtaa käytetään diskurssin takana siinäkin mielessä, että määrittelemällä tietynlaiset uhat, määrittelijä oikeuttaa myös teot uhkien torjumiseksi (mukaillen Buzan ja Hansen 2009, 217). Uhkakuvadiskurssi antaa turvallisuuspoliittisille strategioille niiden merkityksen tukien ja ylläpitäen niiden ympärille rakennettuja universaaleja käytänteitä ja diskurssin

rakenteita *mielen teroittamisen* logiikalla (Fairclough 2001b, 62). Tämän vuoksi uhkakuvadiskurssia on tulkittava syvemmälle.

Uhkakuvadiskurssin lisäksi toinen ilmeinen diskurssi, joka aineistosta löytyy on arvodiskurssi. Tämä on Euroopan unionin teksteissä yleisesti esiintyvä diskurssi, joka tuottaa ja ylläpitää EU:n normatiivista valtaa (Manners 2002). Arvodiskurssia ilmentävät esimerkiksi seuraavat tekstiosuudet: *"...eurooppalaisten turvallisuutta ja perusoikeuksia ja -vapauksia voidaan tehokkaasti suojella niihin kohdistuvilta riskeiltä*" (EU:n kyberturvallisuusstrategia 2020, 5), "[*i*]*nternetin ja sen käytön rajoitukset uhkaavat paitsi maailmanlaajuista ja avointa kybertoimintaympäristöä myös oikeusvaltioperiaatetta, perusoikeuksia, vapautta ja demokratiaa, jotka ovat EU:n keskeisiä arvoja*" (EU:n kyberturvallisuusstrategia 2020, 2) sekä "[*t*]*urvallisuus on ensiarvoisen tärkeää henkilötasolla, mutta se suojelee myös perusoikeuksia sekä luo perustan taloutemme, yhteiskuntamme ja demokratiamme luottamukselle ja dynaamisuudelle*" (EU:n turvallisuusunionistrategia 2020, 1). Lisäksi arvodiskurssia tukee yleinen *me*-dialogi, jota oli havaittavissa sekä turvallisuusunionistrategiassa (*meidän taloutemme, yhteiskuntamme ja demokratiamme*) että Borrellin esipuheessa (*meidän eurooppalainen tapa*). Kuten uhkakuvadiskurssi turvallisuuspoliittisissa teksteissä, arvodiskurssi on EU:lle keskeinen diskurssi, jonka se haluaa lukijalle välittää. Sen vuoksi kumpikaan näistä diskursseista ei ole niin sanottu hegemoninen diskurssi valitussa aineistossa. Hegemoninen diskurssi on itsestään selvä, mutta piilevämpi kuin tekstissä useammin nähtävillä olevat diskurssit (Jokinen ja Juhila 2016).

Uhkakuvadiskurssi ja arvodiskurssi ilmentävät osittain samankaltaisia piirteitä tarkastellussa aineistossa. Nämä kaksi yleisemmin toistuvaa diskurssia luovat oikeutusta lopulta itseään suuremmalle diskurssille (Jokinen ja Juhila 2016), jota kutsun arkipäiväistämisdiskurssiksi. Arkipäiväistämisdiskurssi ilmenee siinä, että dokumenteissa arkipäiväistetään niin turvallisuusuhkia kuin arvoja. Uhkat tuodaan lähelle (Euroopan) kansalaista kertomalla päivittäin käytettävien digitaalisten laitteiden sisältämistä tietoturvariskeistä: "[*k*]*un jopa pienet verkkoon yhteydessä olevat kodinkoneet (esimerkiksi jääkaappi ja kahvinkeitin) voivat aiheuttaa tietoturvariskin.*" (EU:n turvallisuusunionistrategia 2020, 5) sekä puhumalla meille eurooppalaisille arkipäiväisistä asioista "*verkkoon liitetyistä laitteista, sähköverkoista, pankkipalveluista, lentokoneista, julkishallinnosta tai sairaaloista*" (EU:n kyberturvallisuusstrategia 2020, 1), jotka ovat kiinteästi osa kybertoimintaympäristöä. Uhkakuvia arkipäiväistetään myös Borrellin strategisen kompassin esipuheessa (2021) esittämällä väitteitä ihmisten peloista

ja toiveista turvallisuuden suojelun suhteen. Arvojen arkipäiväistämistä puolestaan tapahtuu, kun puhutaan *meidän eurooppalaisten arvoista ja intresseistä, perusoikeuksistamme ja -vapauksistamme, demokratiastamme, taloudestamme ja yhteiskunnastamme* tavallisina, jokapäiväisinä asioina, jotka ovat itsestäänselvyyksiä monelle eurooppalaiselle. Tätä arvojen arkipäiväistämisdiskurssia on havaittavissa kaikissa aineiston dokumenteissa.



Kuvio 4. Arkipäiväistämisdiskurssin muodostuminen.

Arkipäiväistämisdiskurssi	
Uhkakuvadiskurssi	”*Eurooppa on vaarassa*”, kyberuhat osana arkipäiväistä elämää digitaaliset laitteiden ja yhteiskunnan kriittisten digitaalisten palveluiden kautta
Arvodiskurssi	”*Meidän taloutemme, yhteiskuntamme ja demokratiamme*”, meille arkipäiväisten arvojen kuten perusoikeuksien ja -vapauksien, demokratian ja oikeusvaltioperiaatteen suojelu

Taulukko 5. Arkipäiväistämisdiskurssin ilmentyminen uhkakuva- ja arvodiskurssin kautta.

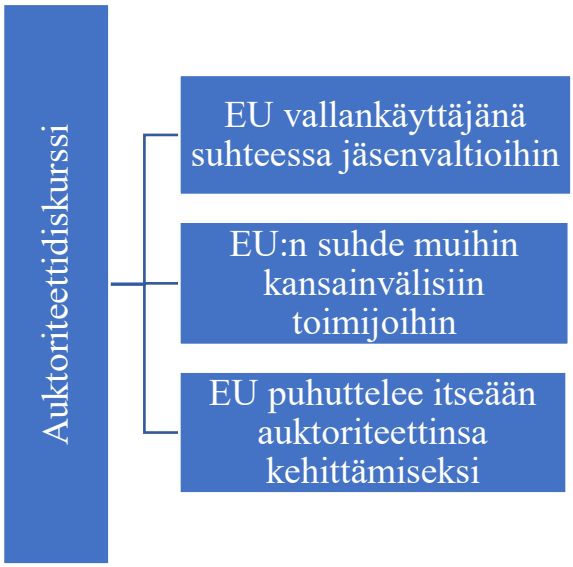
Vaikka uhkakuva- ja arvodiskurssi ovat helposti paikannettavissa teksteistä, ne eivät ole hegemonisia diskursseja. Pidän juuri arkipäiväistämisdiskurssia hegemonisena, sillä molemmat uhkakuva- ja arvodiskurssi tukevat sitä. Arkipäiväistämisdiskurssilla viittaa uhkien ja arvojen arkipäiväseksi tekemiseen lukijalle eli Euroopan unionin kansalaiselle.

Toisaalta, jos tekstejä lukee joku muu kuin EU-kansalainen, ne puolestaan kertovat siitä, mikä on *tavallista* ja *arkipäiväistä* eurooppalaisille: perusoikeudet sekä demokratia ja toisaalta kybertoimintaympäristön mukana tulleet kyberuhat, jotka ovat läsnä ihmisten arkipäiväisessä elämässä digitaalisten laitteiden kautta.

Euroopan unioni pyrkii esittämään itsensä arkipäiväistämisdiskurssin kautta toimijana, joka osaa määritellä kyberturvallisuuteen liittyvät uhat sekä pyrkii etsimään niihin ratkaisuja. Samalla EU haluaa näyttäytyä *eurooppalaisten arvojen* ja *yhteiskunnan puolustajana*, joka suojelee kansalaistensa arkipäiväistä elämää jopa kybertoimintaympäristössä. Uhkakuvien osoitetaan olevan lähellä tavallista kansalaista yhtä lailla, kuin eurooppalaisille tärkeä arvomaailma on kiinteä osa arkipäiväistä eurooppalaista elämää. EU haluaa suojella kansalaisiaan ja kansalaistensa elämää sellaisena kuin se on totuttu tuntemaan. Samalla se haluaa tuoda kansalaiset ja heidän kybertoimintansa osaksi kyberturvallisuuden kokonaisvaltaista ymmärrystä.

6.2. Auktoriteettidiskurssi

Arkipäiväistämisdiskurssin lisäksi aineistosta on paikannettavissa toinen keskeinen temaattinen diskurssi, jota nimitän auktoriteettidiskurssiksi. Auktoriteettidiskurssi on myös moniulotteinen diskurssikokonaisuus, sillä se kuvaa EU:n suhdetta kyberturvallisuuspolitiikassa niin jäsenvaltioihin, muihin kansainvälisiin toimijoihin kuin EU:hun itseensä turvallisuustoimijana, ja millaisena vallankäyttäjänä hän itse toivoo toimivansa. Auktoriteetilla tarkoitan tässä yhteydessä sekä toimijoita että institutionaalisia tekijöitä kuten kansainvälisesti sitovia sopimuksia. Auktoriteettidiskurssia havainnollistaa seuraava kuvio 5.



Kuvio 5. Auktoriteettidiskurssin kolme ulottuvuutta.

Auktoriteettidiskurssin kolmea ulottuvuutta yhdistää ajatus siitä, miten Euroopan unioni näkee itsensä toimijana, suhteessa toiseen toimijaan tai toiminnan kohteeseen. Euroopan unioni saattaa nähdä, että sillä on auktoriteettiasema suhteessa jäsenvaltioihin, kun taas suhteessa muihin kansainvälisiin toimijoihin saattaa EU nähdä itsensä kenties tasavertaisena tai hakea auktoriteetilleen tukea näiltä muilta toimijoilta. Samalla aineistosta on havaittavissa EU:n puhuttelua myös itselleen auktoriteettiaseman kehittämiseksi, tukevoittamiseksi ja parantamiseksi. Oheinen kappale havainnollistaa EU:n valtaa suhteessa jäsenvaltioihin:

> ”*EU:lla ei ole yhteisiä tilannetietoja kyberuhkista. Tämä johtuu siitä, että kansalliset viranomaiset eivät kerää ja jaa järjestelmällisesti tietoja, esimerkiksi yksityiseltä sektorilta saatavia tietoja, jotka voisivat auttaa arvioimaan kyberturvallisuuden tilaa EU:ssa. Jäsenvaltiot ilmoittavat vain murto-osasta poikkeamia, eikä tietojen jakaminen ole järjestelmällistä eikä kattavaa.* (EU:n kyberturvallisuusstrategia 2020, 4.)

Analysoin yllä olevaa kappaletta vallan näkökulmasta aiemmassa luvussa. Teksti paljastaa puheaktin kautta, että EU puhuttelee tässä kappaleessa jäsenvaltioita tietyllä sävyllä, koska kokee, että sillä on vallankäyttäjänä oikeus torua vallan kohdetta eli jäsenvaltiota. Samalla tavoin EU:n ulkosuhdehallinnon korkean edustajan Josep Borrellin strategisen kompassin esipuheen (2021, 1, 2) voidaan tulkita puhuttelevan toruvasti niin EU:n jäsenvaltioita kuin EU:ta kokonaisuutena esipuheen varoitellessa eurooppalaisten ’*strategisen arvon alennuksesta*’ (alk. engl. ’*strategic shrinkage*’).

Toisaalta Euroopan unionin sävy jäsenvaltioita kohtaan ei aina ole moittiva tai määräilevä kuten EU:n kyberturvallisuusstrategiassa (2020) esitetty toive yhteisestä kyberturvallisuusyksiköstä ilmentää:

> ”*Jotta yhteisestä kyberturvallisuusyksiköstä saataisiin tehtyä EU:n operatiivisen kyberturvallisuusyhteistyön ydin, komissio tekee yhteistyötä jäsenvaltioiden ja asiaankuuluvien EU:n toimielinten, elinten ja virastojen, kuten ENISA:n, CERT-EU:n ja Europolin, kanssa edistääkseen vaiheittaista ja osallistavaa lähestymistapaa kunnioittaen kaikilta osin kaikkien asianosaisten toimivaltuuksia ja toimeksiantoja*” (EU:n kyberturvallisuusstrategia 2020, 16).

Vaikka sävy on kunnioittavampi muita osapuolia, myös jäsenvaltioita kohtaan, EU:n ja jäsenvaltioiden suhde ei kuitenkaan muutu yllä olevassa kappaleessa millään lailla tasavertaiseksi. Kun EU:n valtaa pitävä toimija eli ”*komissio tekee yhteistyötä jäsenvaltioiden ja muiden asiaankuuluvien*” kanssa, komissio asetetaan tässä johtotehtävään yhteisen kyberturvallisuusyksikön muodostamiseksi.

Toisena auktoriteettidiskurssin ulottuvuutena on havaittavissa Euroopan unionin toiminta kansainvälisessä ympäristössä sekä EU:n vetoaminen johonkin kansainvälisesti merkittävään auktoriteettiin:

> ”*EU tekee edelleen yhteistyötä kansainvälisten kumppaneiden kanssa edistääkseen maailmanlaajuista, avointa, vakaata ja turvallista kybertoimintaympäristöä, jossa noudatetaan kansainvälistä oikeutta, erityisesti Yhdistyneiden kansakuntien (YK) peruskirjaa*” (EU:n kyberturvallisuusstrategia 22-23).

Tässä merkittävä kansainvälinen auktoriteetti on Yhdistyneiden kansankuntien peruskirja. ”*Maailmanlaajuinen, avoin, vakaa ja turvallinen kybertoimintaympäristö”* on EU:n määrittelemä tavoite. Oheinen virke ei sinällään kerro, jakavatko EU:n kansainväliset kumppanit saman tavoitteen. EU:n voidaan tulkita pitävän tavoitettaan linjassa YK:n peruskirjan kanssa, ja samalla YK:n peruskirjan noudattamisen takaavan EU:n haluaman kybertoimintaympäristön.

Dokumenteissa mainitaan useasti *Budapestin yleissopimus* (EU:n turvallisuusunionistrategia 2020, 12, 14; EU:n kyberturvallisuusstrategia 2020, 24, 26), joka on Euroopan neuvoston kyberrikollisuutta koskeva sopimus. Kyberturvallisuuspolitiikassa kyseinen sopimus on oikeudellinen auktoriteetti, jonka perusteella toimintaa voidaan valtiontasolla ohjata kyberrikollisuuden torjumiseksi ja selvittämiseksi.

EU:n ja Naton välinen yhteistyö mainitaan myös toistuvasti dokumenteissa: ”*EU:n olisi jatkettava…annettujen yhteisten julkilausumien pohjalta EU:n ja Naton yhteistyön edistämistä erityisesti kyberpuolustuksen yhteentoimivuusvaatimusten osalta*” (EU:n kyberturvallisuusstrategia 2020, 24) ja ”[*t*]*avoitteena on maksimoida EU:n toimien vaikutus kokoamalla nopeasti yhteen alakohtaiset ratkaisut ja varmistamalla saumaton yhteistyö kumppaneiden, ensi sijassa Naton, kanssa*” (EU:n turvallisuusunionistrategia 2020, 17). Lisäksi Borrell (2020, 1) viittaa muihin EU:n ja sen jäsenvaltioiden johtajien sekä Yhdysvaltojen presidentti Joe Bidenin puheisiin omassa esipuheessaan, ja nostaa esille ”*transatlanttisen yhteistyön*” merkityksen ”*Euroopan puolustusunionin*” rakentamiseksi. Pitääkö EU Natoa auktoriteettina suhteessa itseensä? Vaikuttaa siltä, ettei EU pidä Natoa itseään ylempiarvoisena vaan ennemmin samanarvoisena yhteistyökumppanina. Sen sijaan EU näkee yhteistyönsä Naton kanssa luovan sille lisää painoarvoa kansainvälisissä suhteissa. Kuten Josep Borrellin esipuheessa viitataan ”*uuteen uhkien maailmaan*”[12] EU näkee puolustuksen, strategisesti ja sotilaallisesti ymmärrettynä, sen selviytymiskeinoksi *uhkaavaksi* muuttuneessa maailmassa, ja mikä sen parempi yhteistyökumppani, kuin sotilaalliseen puolustautumiseen erikoistunut puolustusliitto Nato.

Euroopan unioni tuo auktoriteettiaan kansainvälisissä suhteissa esille myös toisella tavalla:

> ”*Edistääkseen ja puolustaakseen kybertoimintaympäristöä koskevaa visiotaan kansainvälisellä tasolla EU:n on tehostettava osallistumistaan kansainvälisiin standardointiprosesseihin ja johtajuuttaan niissä sekä lisättävä edustustaan kansainvälisissä ja eurooppalaisissa standardointielimissä sekä muissa standardointiorganisaatioissa*” (EU:n kyberturvallisuusstrategia 2020, 22).

Euroopan unioni haluaa aktiivisesti tuoda esille omaa visiotaan kybertoimintaympäristöstä, mikä tarkoittaa ”*maailmanlaajuista, avointa, vakaata ja turvallista kybertoimintaympäristöä*”. EU haluaa olla aktiivinen ja tunnustettu toimija kansainvälisissä pöydissä. Samalla oheinen teksti tuo esille toisenlaisen puolen auktoriteettidiskurssista, jossa EU patistaa itseään toiminnan tehostamiseen. Tässä yhteydessä toiminnan tehostaminen tarkoittaa *EU:n johtajuuden tehostamista* ja

[12] ”A new world of threats” (Borrellin esipuhe 2020, 2).

edustuksen lisäämistä kansainvälisissä ja eurooppalaisissa standardointielimissä. EU puhuttelee itseään toivoen auktoriteettinsa vahvistumista, mikä on kolmas havaittu auktoriteettidiskurssin ulottuvuus.

Dokumenttien tuottajat, jotka edustavat EU:ta kokonaisuudessaan (Euroopan komission ja ulkosuhdehallinnon edustajat tuottajina) luovat tekstillään kuvaa siitä, että EU:lla on valtaa, mutta valta-asemaa olisi yhä kehitettävä. Tästä muodostuu auktoriteettidiskurssi, jossa EU puhuttelee itseään kuten ”*EU:n olisi edelleen edistettävä jäsenvaltioiden välistä yhteistyötä kyberpuolustuksen tutkimuksessa, innovoinnissa ja voimavarojen kehittämisessä*” (EU:n kyberturvallisuusstrategia 2020, 20). Virkkeessä puhutaan jäsenvaltioiden välisen yhteistyön edistämisestä, mutta toiminta viittaa vahvemmin EU:n suuntaan. EU:n on tehostettava toimintaansa, EU puhuttelee itse itseään, vaikka virkkeessä on viitteitä myös EU:n ja jäsenvaltioiden välisen auktoriteettidiskurssin muodosta.

Samanlaista itsensä puhuttelua on havaittavissa virkkeessä: ”*EU:n olisi jatkossakin johdettava ihmisoikeuksien ja perusvapauksien suojelua ja edistämistä verkossa*” (EU:n kyberturvallisuusstrategia 2020, 23). Konditionaalimuoto *olisi* toistuu tässäkin yhteydessä, kuten myös ajatus toiminnan tehostamisesta, joka tässä tapauksessa on *johtamisen* tehostamista. Tässä virkkeessä myös arvodiskurssi näyttäytyy tutussa muodossaan, ja toimii auktoriteettidiskurssia tukevana diskurssina (Jokinen ja Juhlia 2016). Tämän ja edellisen kappaleen virkkeiden samankaltaisuus saa pohtimaan sitä, voiko tekstin tuottajan vaikutus olla niin suuri tekstin rakentumiseen, että hänen kirjoitustyylinsä on nähtävissä läpi toisiaan muistuttavien lauseiden kautta? Onko esimerkiksi konditionaalimuoto vai osa tekstin tuottajan tyylillisiä keinoja? Strategian kaltainen teksti on kuitenkin niin hiottua, joten tuskin on sattumaa, tämä tyyli, jolla EU puhuttelee itse itseään.

Dokumenteista löytyy myös toisenlaisia tapoja joilla, EU pyrkii auktoriteettinsa vahvistamiseen kuten: ”[*k*]*omission yksiköt ja Euroopan ulkosuhdehallinto tarkastelevat tilannetietoisuuden parantamiseksi mahdollisuuksia virtaviivaistaa tiedonkulkua eri lähteistä*” (EU:n turvallisuusunionistrategia 2020, 16-17). Tässä toiminnan tehostamista jaetaan komission yksiköiden ja ulkosuhdehallinnon vastuulle. Samalla tavoin tässä on kyse tilanteesta, jossa EU puhuttelee itse itseään, sillä turvallisuusunionistrategian on laatinut itse Euroopan komissio.

	Auktoriteettidiskurssi
EU vallankäyttäjänä suhteessa jäsenvaltioihin	Jäsenvaltioiden moittiminen, ja toisaalta yhteistyöhön kannustaminen *vaiheittain* ja *osallistavasti*
EU:n suhde muihin kansainvälisiin toimijoihin	Vetoaminen kansainvälisiin sopimuksiin ja yhteistyöhön: YK ja sen peruskirja, Budapestin sopimus, Nato
EU puhuttelee itseään auktoriteetin kehittämiseksi	*Johtajuuden* tehostaminen ja ylläpitäminen, tarvittavien toimien kehittäminen kyberturvallisuuden takaamiseksi

Taulukko 6. Auktoriteettidiskurssin kolme ulottuvuutta esimerkkeineen.

Auktoriteettidiskurssi ottaa siis erilaisia muotoja tarkastelussa aineistossa. Samalla diskurssit ovat usein limittäisiä, kuten edellisistä esimerkeistä on huomattavissa. Auktoriteettidiskurssi ilmentää arkipäiväistämisdiskurssin lisäksi toista tapaa, jolla EU pyrkii itsensä kyberturvallisuustoimijana esittämään: EU haluaa esittää itsensä auktoriteetin omaavana toimijana kyberturvallisuuden alalla.

***

Aineiston analyysin perusteella on selvää, että kyseisissäkin aineistossa kieli palvelee tiettyjä intressejä ja sen käyttö on tarkoituksenmukaista (Salter ja Mutlu 2018, 172). Diskurssit ilmentävät valtaa, jonka rakenteita Euroopan unioni toimijana haluaa ylläpitää ja rakentaa. Molemmat hegemoniset diskurssit, arkipäiväsitämis- ja auktoriteettidiskurssi ilmentävät sitä valtaa, joka EU:lla on sekä kertovat, millaisena toimijana EU haluaa kyberturvallisuuspolitiikassa näyttäytyä.

Seuraavassa luvussa siirryn tarkastelemaan turvattomuuden politiikan elementtejä aineiston analyysin pohjalta. Syvennän arkipäiväistämis- ja auktoriteettidiskurssin tarkastelua turvattomuuden politiikan elementtien kautta tuoden tilastoaineistojen tarjoamat esimerkit mukaan tarkasteluun.

7. Turvattomuuden politiikka

Tässä luvussa tarkastelen turvattomuuden politiikan elementtejä, joita on mahdollista tulkita vallan eri diskurssien alla sekä tilastoaineiston tulkintojen perusteella. Luvun alussa tarkastelen turvattomuuden politiikkaa hegemonisissa diskursseissa. Tuon tarkasteluun mukaan myös tilastoaineistoissa ilmeneviä turvattomuuden politiikan elementtejä. Lopuksi tarkastelen sitä, kuka mahdollisesti jää turvallisuuden ulkopuolelle ja turvattomuuden marginaaleihin EU:n kyberturvallisuuspolitiikassa.

7.1. Havaitut turvattomuuden politiikan elementit

Aineiston hegemonisia diskursseja, arkipäiväistämisdiskurssia ja auktoriteettidiskurssia voi tarkastella turvattomuuden politiikan näkökulmasta. Turvallistamisen havainnointi on ensisijaista muiden turvattomuuden elementtien paikantamiselle. Turvallistamista on ollut havaittavissa aineistossa useissa kohdin niin Borrellin (2021, 1) lausahduksella ”*Eurooppa on vaarassa*” kuin hienovaraisella turvallisuusuhkien määrittelyllä ”k*un jopa pienet verkkoon yhteydessä olevat kodinkoneet voivat aiheuttaa tietoturvariskin*” (EU:n turvallisuusunionistrategia 2020, 5). Bigo ja McCluskey (2018,126) argumentoivat, että turvallistaminen on tekoja, joilla päätökset turvallisuuden luomiseksi oikeutetaan. Virallisissa Euroopan unionin julkaisuissa kuten kyseisissä strategioissa ja esipuheessa turvallistamisen teko on turvallisuusuhkien määrittely.

Turvattomuus on aina poliittinen arvio tilanteesta, ja siinä nykyistä verrataan usein menneeseen (Bigo ja McCluskey 2018, 125-126). Arkipäiväistämisdiskurssissa tämä on havaittavissa siinä, että uhkakuvien kentän kuvaillaan muuttuneen, minkä lisäksi uudet kyberuhat voivat olla vaaraksi eurooppalaisten arvoille ja normeille, joita täytyy suojella. Eurooppalainen yhteiskunta, talous ja demokratia nähdään strategioiden perusteella nykyhetkessä uhattuina, kun vertailua tehdään menneeseen. Tämän vuoksi niiden suojelua pidetään oikeutettuna, jotta eurooppalaiset voisivat jatkaa elämäänsä ’ihan niin kuin ennenkin’. Eurooppalaisten liberaaleissa ja demokraattisissa yhteiskunnissa vapaus ja kaiken tavaran, ihmisten ja massan vapaa kierto ovat yhteiskuntien toiminnan edellytyksiä ja siksi suojelemisen arvoisia. Tätä kutsutaan kriittisen turvallisuustutkimuksen parissa turvallisuuden dispositiiviksi, jossa ’länsimaisen vapauden suojelun’ ajatus korostuu (Bigo 2008, 96-97).

Yhtä lailla auktoriteettidiskurssin kautta Euroopan unioni tekee poliittisia arvioita omasta tilanteestaan suhteessa jäsenvaltioihin, muihin toimijoihin ja kansainväliseen areenaan. Kybertoimintaympäristö on globaali ja rajat ylittävä kokonaisuus, jossa jokainen verkkoon liittynyt ihminen on osa suurta kokonaisuutta mahdollisuuksineen ja uhkineen. Turvattomuutta luodaan tämän diskurssin kautta siten, että tilanteen koetaan myös kansainvälisesti muuttuneen turvallisuustoimintaympäristön uudistuessa, kun ”*kybertoimintaympäristöä käytetään yhä enemmän poliittisiin ja ideologisiin tarkoituksiin”* (EU:n kyberturvallisuusstrategia 2020, 2).

Tässä kohtaa on hyvä selkeyttää merkityksiä *arkipäiväistämisdiskurssin* ja turvattomuuden politiikan elementin, *turvallisuuden arkipäiväisyyden* välillä. Turvallisuuden arkipäiväisyys tarkoittaa sitä, että tarkastellaan toimijaa, joka muodostaa turvallisuuden narratiiveja osana arkipäiväistä työtään (Bigo ja McCluskey 2018, 119). Hegemonisella arkipäiväistämisdiskurssilla ei suoranaisesti viitata toimijoihin, jotka muodostavat turvallisuuden narratiiveja työkseen ja päivittäin, vaan arkipäiväistämisdiskurssi viittaa EU:n tapaan tuoda uhkakuvien ja arvojen kautta turvallisuus lähelle kansalaisten arkipäivää. Toisaalta arkipäiväistämisdiskurssi on turvallisuuden narratiivi, jota EU toimijana muodostaa ja ylläpitää joka päivä, ja sen virkamiesten tehtävä on kirjoittaa ja tuottaa kyseistä vallan diskurssia osana arkipäiväistä työtään esimerkiksi strategioiden muodossa.

Myös tutkielman tilastoaineistot paljastavat mielenkiintoisesti turvattomuuden politiikan elementtejä. Erityiseurobarometri eurooppalaisten asenteista verkkoturvallisuutta kohtaan (2019) ja Erityiseurobarometri eurooppalaisten suhtautumisesta kyberturvallisuuteen (2020) tiedustelevat kattavasti eurooppalaisten huolenaiheita liittyen erilaisiin kyberuhkiin. Uhat on vielä erikseen nimetty, ja vastaajaa pyydetään asteikolla nimeään ”*miten huolissaan olet henkilökohtaisesti seuraavanlaisen tilanteen kokemisesta tai sen uhriksi joutumisesta*”[13]. Kuvattu tilanne voi olla henkilön sähköpostiin tai sosiaalisen median tileille hakkeroiminen tai verkkopankkitunnusten kalastelu. Kyselyn kysymykset ovat ohjaavia ikään kuin tiedustellen kansalaiselta ”*mitä sinä pelkäät*”. Tätä voisi kuvailla turvattomuuden politiikan elementiksi, jossa turvallisuuden narratiiveja muodostetaan ihmisille arkisia asioita turvallistaen (Bigo ja McCluskey 2018, 119, 126). Etenkin se, että vastaajien vastauksia ohjaillaan kysymällä,

[13] alk. engl.: “*Cybercrimes include many different types of criminal activity. How concerned are you personally about experiencing or being a victim of the following situations?*” (Erityiseurobarometri eurooppalaisten suhtautuminen kyberturvallisuuteen 2020).

asioista tietyllä sävyllä (miten huolissaan) ja antamalla valmis aihe vastausvaihtoehtoineen, aihe on helppo turvallistaa, kun moni vastaaja voi helposti todeta, että on ainakin hiukan huolissaan sosiaalisen median tilinsä hakkeroimisesta tai verkkopankkitunnusten kalastelusta.

Kielen käytön tarkoituksenmukaisuus Eurobarometrien tilastokyselyissä tukee myös turvattomuuden politiikkaa, sillä asiantuntijoiden kuvataan käyttävän tietynlaista kieltä tarkoituksenmukaisesti (Bigo 2002). Kysymysten ohjailevuus on tarkkaan harkittua ja perustuu asiantuntijoiden tekemille havainnoille kyberrikollisuuden ja tietoturvariskien erilaisista haitoista. Kun vastaaja vastaa kyselyyn vastauksia myötäilevästi, hän tulee samalla tukeneeksi asiantuntijoiden auktoriteettia, sillä osoittaa asiantuntijoiden kysymykset ja vastausvaihtoehdot aiheellisiksi. Tämän voidaan samalla tulkita ilmentävän *mielen teroittamisen* taktiikkaa, jolla vallan rakenteita ylläpidetään (Fairclough 2001b, 62). Vastaaja omaksuu kysymyksen ja sen vastausvaihtoehdot sellaisina kuin ne on annettu, eikä kyseenalaistamiselle ole sijaa.

Dokumenttiaineistosta paikannettu auktoriteettidiskurssi ilmentää puolestaan vahvimmin EU:n hallinnon teknis-byrokraattista luonnetta, joka on yksi turvattomuuden politiikan elementti (Vuori 2014, 37). Asiantuntijatiedon korostaminen vahvistaa EU:n legitimiteettiä (Egeberg ja Trondal 2017, 677), ja asiantuntijatietoa kerätään niin omien toimielinten kuin muiden kansainvälisten toimijoiden kautta:

> ”*Kyberriskeistä on tullut merkittävä uhka myös rahoitusjärjestelmälle. Kansainvälinen valuuttarahasto on arvioinut, että kyberhyökkäysten aiheuttamat vuotuiset tappiot ovat 9 prosenttia pankkien maailmanlaajuisista nettotuloista, eli noin 100 miljardia dollaria*.” (EU:n turvallisuusunionistrategia 2020, 8.)

Asiantuntijavallan korostamista hyödynnetään strategioissa turvallisuustekojen oikeuttamiseksi. Kansainvälisen valuuttarahaston arvion esille tuomisella halutaan korostaa tarvetta tehostaa EU:n lähestymistapoja kyberuhkiin sekä toivotaan, että kaikki tahot yksityishenkilöistä, toimielimiin ja tiedemaailmaan asettaisivat kyberturvallisuuden etusijalle (EU:n kyberturvallisuusstrategia 2020, 9). Asiatuntijavaltaan vetoamisella tehostetaan turvallisuuden narratiivia kyberturvallisuudesta. Asiantuntijavallan esille tuomista on havaittavissa aineistossa myös kohdissa, joissa EU arvioi omaa toimijuuttaan ja esittää parannusehdotuksia niin johtajuuden tehostamisessa kuin jäsenvaltioiden välisen yhteistyön tiivistämisessä *vaiheittain* ja *osallistavasti*.

Asiantuntijavallan näkökulmasta voi myös tarkastella Borrellin strategisen kompassin esipuheessa (2021) mielenkiintoista Euroopan kansalaisten mielipidemittausten esille nostamista. Borrell käyttää ikään kuin kansalaisten mielipiteitä asiantuntijamielipiteinä tekstissään todistaakseen tavallisten kansalaisten ymmärryksen ”*uudesta kontekstista*” ja siitä, että ”*kansalaiset haluavat, että EU suojelee heitä tältä vaaralliselta maailmalta jossa asumme*”[14]. Kuten on jo aiemmin todettu, *joihinkin mielipidemittauksiin* viittaaminen, on Borrellin esipuheen yhteydessä hyvin epämääräinen käsite, ja siten hänen väitteiltään puuttuu todistusarvo. Borrell osaa tekstin tuottajana ovelasti hyödyntää kansalaisiin vetoamista, tekemällä kansalaisista turvallisuuden asiantuntijoita, joiden tuntemuksia on kuunneltava. Tässä esipuheen tekstipätkässä kansalaiset toimivat asiantuntijatiedon tuottajana auktoriteetille eli EU:lle, joka pystyy oikeuttamaan tekonsa puolustusyhteistyön tiivistämisestä sen perusteella, että ”*kansalaiset odottavat EU:n suojelevan heitä*”. Sen sijaan, että kansalaiset olisivat tässä yhteydessä ’todellisia asiantuntijoita’, kansalaisten mielipidemittaustulokset valjastetaan osaksi turvallisuuden määrittelyä antaen ymmärtää, että kansalaiset kokevat turvattomuutta.

Tutkimusaineiston strategiat ja erityisesti kyberturvallisuusstrategia (2020) pitävät sisällään huomattavan määrän lyhenteitä, joita ei juurikaan avata lukijalle. Lyhenteet kuten CCCN, DNS, IPv6, DNS4EU ja CyCLONe korostavat jo entisestään teknispainotteista tekstiä edistäen mielikuvaa Euroopan unionista teknis-byrokraattisena kokonaisuutena. Teknisyys kumpuaa Euroopan unionin legitimiteetin rakentumisesta. Mikäli EU:n toimijuus ymmärretään monikansallisena (alk. engl. transnational) rakennelmana, jossa vastuu jakautuu löysästi EU-instituutioiden ja kanallisten toimielinten välille, EU:n legitimiteetti perustuu teknokraattisille arvoille ja asiantuntijuuden erinomaisuudelle (Egeberg ja Trondal 2017, 677). Teknokraattisten arvojen pohjalta EU näkee keskeisenä informaation välittämisen sekä ’paras käytäntö’ -menettelytavan (alk. engl. ’best practice’) (emt.). Muun muassa teknisten lyhenteiden käytön avulla EU siis vahvistaa oman asiantuntijuutensa auktoriteettia. Byrokraattisuus eli virkavaltaisuus (Kielitoimiston sanakirja 2022c) nostaa päätään puolestaan siinä, että kyseisiä teknisiä lyhenteitä muodostetaan menettelytapojen helpottamiseksi, mutta samalla rationaalisuus on osa sääntöjen noudattamisen takkaa (Bozeman 2000, 12).

[14] ”European citizens are also aware of this new context… They want the EU to protect them from the dangerous world we live in.” (Borrellin esipuhe 2021, 1)

Turvallisuuden parantamista tai tiukentamista turvattomuuden vähentämiseksi voidaan tulkita myös turvattomuuden politiikan elementiksi. Se on osittain päällekkäistä turvallistamisen kanssa, mutta ajatuksena on se, että, mikäli turvallisuus ymmärretään päämäärättömäksi kokonaisuudeksi, silloin turvallisuutta ja turvattomuutta ei voi tulkita toisilleen vastakkaisina asioina (Bigo ja McCluskey 2018, 125-126). Todellisuudessa kuitenkin turvallisuuden narratiiveja juuri luodaan sillä ajatuksella, että turvallisuus poistaisi turvattomuutta. Koska valittu aineisto huokuu vahvasti turvallisuusuhkien määrittelyä ja niiden kohtaamista, voisi jokaisen aineistokappaleen kuvailla vaativan turvallisuustilanteen parantamista turvattomuuden vähentämiseksi. Kenties räikeimmin tämä nousee esille Borrellin esipuheessa (2021, 1), jossa hän toteaa *"kansalaiset haluavat, että EU suojelee heitä tältä vaaralliselta maailmalta jossa asumme"*. Lauseessa tunnistetaan kasvanut turvattomuus ja tarve suojelulle eli turvallisuuden lisäämiselle.

Turvattomuuden politiikan elementtejä aineistossa:	
Turvallistaminen	Turvallisuusuhkien määrittely: "*Eurooppa on vaarassa*", "*miten huolissaan olet verkkopankkitunnusten varastamisesta?*"
Turvallisuuden dispositiivi	Kansalaisten 'länsimaalaisten' vapauksien ja oikeuksien suojelu
Turvallisuuden arkipäiväisyys	Strategiat itsessään ovat turvallisuuden narratiiveja, joita virkamiehet arkipäiväisessä työssään muodostavat
Asiantuntijavallan korostaminen, teknisyys ja byrokratia	EU toimii itse asiantuntijana ja korostaa muiden kansainvälisten toimijoiden sekä tahojen asiantuntijuutta, lyhenteiden käyttö toimii teknisyyttä korostavana elementtinä.
Turvallisuuden parantaminen turvattomuuden vähentämiseksi	Aineistokappaleet itsessään tavoittelevat tätä, ja se on etenkin turvallisuusstrategioiden olemassaoloa selittävä tekijä.

Taulukko 7. Havaitut turvattomuuden politiikan elementit aineistossa.

Oheinen taulukko seitsemän kokoaa vielä yhteen aineistossa havaitut turvattomuuden politiikan elementit. Turvattomuuden politiikan elementit näkyvät niin yksittäisissä virkkeissä valitussa aineistossa, mutta aineisto kokonaisuudessaan heijastelee myös

turvattomuuden politiikan elementtejä kuten turvallisuuden arkipäiväisyyttä ja käsitystä siitä, että turvallisuuden parantamisella saavutettaisiin turvattomuuden vähentyminen.

7.2. Kuka jää turvallisuuden ulkopuolelle?

Kuka tai ketkä sitten jäävät turvattomuuden piiriin ja turvallisuuden ulkopuolelle EU:n kyberturvallisuuspolitiikassa? Voiko tavallinen kansalainen tai kansalaisten joukko jäädä turvattomuuden piiriin? 'Pariisin koulukunnan' tulkinnan mukaan turvattomuus piilee marginaaleissa, ja se koskettaa vain tiettyä ihmisjoukkoa (Bigo 2008, 105).

Ainakin nimellisesti tutkimusaineiston analyysin perusteella yksilö pyritään huomioimaan ja yksilöiden merkitys kyberturvallisuuden kokonaispaletissa ymmärretään ensiarvoisen tärkeänä. Jos palaa Bigon ja McCluskeyn (2018, 125-126) ajatukseen siitä, että turvallisuus on päättymätöntä ja päämäärätöntä, silloin myöskään turvattomuus ei koskaan poistu. Mikäli EU pyrkii sanojensa mukaisesti "*varmistamaan maailmanlaajuisen ja avoimen internetin*" (EU:n kyberturvallisuusstrategia 2020, 5) se toteuttaa turvallisuuden dispositiivia (Bigo 2008, 96-97), mutta ei pysty koskaan sisällyttämään jokaista yksilöä turvallisuuden piiriin. Tällöin turvattomuuden puolelle jäävät kybertoimintaympäristössä yksittäiset yksilöt, jotka voivat nauttia internetin vapaudesta, ja samalla altistavat itsensä yhä uusille ja moninaisille uhille. Käytännöllisesti katsoen mikään tietojärjestelmä ei ole koskaan aukoton, kun ohjelmointivirheet ja ohjelmiston haavoittuvuus huomataan usein vasta tietomurron tapahtuessa (Norilo 2021, 22). Tämä tarkoittaa myös sitä, että Euroopan unioni, kuten kukaan muukaan toimija, ei pysty koskaan aukottomasti suojelemaan yksilöitä kyberuhilta, koska nykyhetkessä ei pystytä tunnistamaan kaikkia uhkia ennen kuin kyberoperaatio on tapahtunut. Kybertoimintaympäristö muuttaa muotoaan jatkuvasti, jolloin määrittelemättömät uhkakuvat tekevät turvattomuuden tunteesta päättymätöntä ja päämäärätöntä. EU:n vahva diskurssi kansalaisten tietoisuuden parantamisesta, "*koko yhteiskunnan kattavasta lähestymistavasta*" ja siitä, että "*EU:n toimielimet, virastot ja elimet, jäsenvaltiot, teollisuus, tiedemaailma ja yksityishenkilöt asettavat kyberturvallisuuden etusijalle*" (EU:n kyberturvallisuusstrategia 2020, 9) kielii siitä, että EU todella tunnustaa voimavarojensa rajallisuuden, ettei se yksin pysty tuottamaan kaikille, ja jokaiselle yksilölle tarvittavaa suojaa kyberuhkia vastaan. Turvattomuus vie väistämättä voiton yksilöiden kohdalla.

Kyberturvallisuuden parissa voisi helposti ajatella, että turvattomuuden piirissä on usein kerrallaan tietty joukko ihmisiä joiden laitteissa on tietoturvahaavoittuvuus, ja he ovat

alttiita mahdollisille uhille. Suomessa vuonna 2020 tapahtunut tietomurto psykoterapiakeskus Vastaamoa kohtaan antaa turvattomuudesta ikävän esimerkin. Vastaamon tietomurrossa kiristäjä onnistui saamaan käsiinsä satoja potilastietoja, joilla hän kiristi henkisesti ja psyykkisesti haavoittuvassa asemassa olevia yksilöitä (Rimpiläinen 2020). Vastaamo yrityksenä joutui tietomurron kohteeksi, koska sen tietoturvakäytänteissä oli merkittäviä heikkouksia (Koskinen 2020). Vaikka yrityksellä tulisi olla kaikki vastuu arkaluontoisten potilastietojen salaamisesta ja tietoturvallisesta käsittelystä, joutuivat sen asiakkaat kaikista turvattomimpaan tilanteeseen, kun henkilökohtaisia tietoja henkilötunnuksista alkaen julkaistiin pimeässä Tor-verkossa (Rimpiläinen 2020). Jo muutenkin yhteiskunnan syrjällä taistelevat henkisesti ja psyykkisesti haastavassa tilanteessa olevat yksilöt joutuivat tämän tietomurron kohdalla ikävästi turvattomuuden marginaaliin. Tietomurron tekijälle oli varmasti myös selvää, että tällainen ihmisryhmä on haavoittuvuutensa takia oivallinen kohde, mikä edelleen sementoi kyseisten yksilöiden asemaa turvattomuuden marginaalissa. Kybertoimintaympäristö on kuitenkin jatkuvassa muutoksen tilassa, mikä tarkoittaa, että myös uhkien kohteet vaihtelevat tietämättä ja ennakoimatta. Tämä asettaa aina uudelleen ja uudelleen jonkun uuden ihmisryhmän turvattomuuden piiriin siten, etteivät yksilöt itse edes välttämättä tiedosta omaa turvattomuuden tilaansa.

***

Turvattomuuden politiikan elementit eivät ole muita näkökulmia poissulkevia, mutta ne pyrkivät nostamaan esille piilevämpää tapaa tarkastella turvallisuuden ja vallan yhteenkietoutumia. Kyberturvallisuus on kokonaisuus, jossa turvallisuuden ja turvattomuuden rajat hämärtyvät niin konkreettisesti kuin kuvainnollisellakin tasolla, ja sen vuoksi kokonaisuudesta paikantuu varmasti vielä monia turvattomuuden politiikan elementtejä.

Seuraavassa luvussa palaa johtopäätösten muodossa tutkielman viitekehykseen sekä pohdin analyysilukujen tarjoamien tulkintojen merkitystä.

8. Johtopäätökset

8.1. Millaisena Euroopan unionin kyberturvallisuustoimijuus näyttäytyy aineiston analyysin valossa?

Kriittisen diskurssianalyysin kautta paljastuneet hegemoniset diskurssit arkipäiväistämisdiskurssi ja auktoriteettidiskurssi avaavat keskeisesti tutkielman alussa esitettyä tutkimuskysymystä, millaisena kyberturvallisuuden toimijana Euroopan unioni pyrkii itsensä esittämään. Hegemonisten diskurssien kautta on tulkittavissa myös se, millaisille tekijöille EU:n kyberturvallisuustoimijuus perustuu. Tämän toisen tutkimuskysymyksen kohdalla kaksi seikkaa nousee esiin yli muiden: turvallisuusuhkien arkipäiväisyyden turvallistaminen ja legitimiteetin hankinta asiantuntijavallan avulla.

Hegemonisista diskursseista arkipäiväistämisdiskurssissa kohtaavat EU:lle tärkeä normatiivinen arvomaailma (Manners 2002) sekä turvallisuusuhkien tuominen lähelle ihmisten jokapäiväistä elämää. EU pyrkii ylläpitämään kuvaa siitä, että EU-kansalaisille tärkeät arvot perusoikeuksien vaalimisesta aina *meidän* taloutemme, demokratiamme ja yhteiskuntamme suojeluun on jollakin tavalla uhattuina ja uhkakuvilta on suojauduttava. Uhkakuvadiskurssi tuodaan lähelle kansalaista kertomalla, kuinka jopa oma kahvinkeitinkin voi aiheuttaa tietoturvariskin. Tämä on osoitus turvallisuuspoliittisille strategioille tyypillisestä turvallistamisesta, jolla uhkakuvien määrittelijä pystyy myös oikeuttamaan halutut teot uhkien torjumiseksi (mukaillen Buzan ja Hansen 2009, 217; Bigo ja McCluskey 2018,126). Samalla strategiat todistavat sitä, että yhtä lailla kun EU on pystynyt identifioimaan terrorismin uhkana ja jopa turvallistamaan sen (Sperling ja Webber 2019, 232), pyrkii se myös turvallistamaan kybertoimintaympäristöön liittyviä elementtejä. Kyberturvallisuuden toimijana EU haluaa siis näyttäytyä turvallisuusuhkien määrittelijänä, joka haluaa löytää myös keinot uhkiin vastaamiseen.

Arkipäiväistämisdiskurssin kautta Euroopan unioni haluaa suojella *eurooppalaista elämäntapaa*, jossa perusoikeudet, taloudellinen hyvinvointi ja demokratia näyttelevät keskeistä roolia. Tätä *länsimaisen vapauden suojelua* kutsutaan ’Pariisin koulukunnan’ piirissä turvallisuuden dispositiiviksi (Bigo 2008, 96-97). Turvallisuuden dispositiivia ei saisi tulkita pelkästään negatiiviseksi asiaksi, vaan vapaus ja kaiken vapaa kierto ovat edellytyksiä yhteiskunnan toimivuudelle (emt.). Vapauksia on suojeltava turvallisuudella, mutta turvallisuuden takaamisen keinot eivät toisaalta saa itse olla vapauksia rajoittava tekijä.

Auktoriteettidiskurssi ilmentää toisella tavalla sitä, millaisena kyberturvallisuuden toimijana EU pyrkii itsensä esittämään: se haluaa tuoda esille auktoriteettiaan suhteessa jäsenvaltioihin, se haluaa olla tunnustettu taho kansainvälisessä kyberturvallisuuspolitiikassa ja se haluaa kehittää omaa johtajuuttaan paremman auktoriteetin saavuttamiseksi jäsenvaltioidensa keskuudessa kuten myös kansainvälisillä areenoilla. Entä onko EU:lla jo auktoriteettia kyberturvallisuuspolitiikassa vai ei? Ainakin *jäsenvaltioiden moittiminen* sekä *johtajuuden tehostaminen* ja *ylläpitäminen* viittaavat siihen, että jonkin tasoinen auktoriteettiasema on saavutettu, mutta sitä on lujitettava. EU:n yhteistä ulko- ja turvallisuuspolitiikkaa sekä yhteistä turvallisuus- ja puolustuspolitiikkaa voi pitää tekijöinä, jotka ovat nostaneet EU:n auktoriteettiasemaa turvallisuuspolitiikassa etenkin, kun ne ovat tehneet siitä kansainvälisen turvallisuuspolitiikan toimijan (Renard 2016, 13-14). Toinen merkittävä tekijä, joka vahvistaa EU:n auktoriteettia on juuri asiantuntijatietoon nojaaminen (Egeberg ja Trondal 2017, 677). Koska EU instituutioiden (muiden kuin Euroopan parlamentin) toiminta ei voi saavuttaa legitimiteettiään edustuksellisen demokratian turvin, EU:n on turvauduttava parhaimpaan mahdolliseen asiantuntijatietoon, joka sen päätöksentekijöillä on käytössä (Pérez-Durán ja Bravo-Laguna 2019, 973). Tämä lisää teknokraattisten elementtien olemassaoloa ja käytön arvostusta EU instituutioissa (emt.). EU:n legitimiteetti kokonaisuutena pohjautuu vahvasti sille, että EU pystyy tekemään parhaimmat mahdolliset ratkaisut nojaten parhaaseen mahdolliseen asiantuntijatietoon, joka on usein vielä tieteellistä tutkimustietoa (Lundin ja Öberg 2014, 27). EU:n auktoriteettiasema perustuu siis kyberturvallisuuden allakin vahvasti asiantuntijatietoon nojaamiseen, koska sen kautta EU voi ainoastaan saavuttaa legitimiteetin.

Samalla kriittisen turvallisuustutkimuksen näkökulmasta asiantuntijavallan korostamista voi pitää yhtenä turvattomuuden politiikan elementtinä etenkin hallinnon rationaalisuuden ja byrokratian elementtien korostuessa turvallisuuden tuottamisessa (Vuori 2014, 37). Rationaalisuus ja teknis-byrokraattinen ilme ovat läsnä EU:n kyberturvallisuusekosysteemissä yhtä lailla kun ne ovat muillakin hallinnon aloilla näkyvissä. Rationaalisuuteen liittyy EU:n halu edistää kokonaisvaltaista kyberturvallisuutta niin horisontaalisen kuin vertikaalisen yhteistyön kautta (Carrapico ja Barrinha 2017, 1263). Myös tutkimusaineisto antoi viitteitä siitä, että yhteistyön mahdollisuuksia on edistettävä niin yksityisen sektorin toimijoiden kanssa kuin jäsenvaltioiden kanssa. Lyhenteiden viljely ja kyberturvallisuusekosysteemin kokoaminen palapelin lailla tukevat EU:n teknis-byrokraattista ilmettä.

Tilastoaineistokappaleiden tarkastelu puolestaan osoitti vahvasti, että kansalaisten kyberturvallisuuteen liittyviä pelkoja halutaan kartoittaa. Erityiseurobarometrit eurooppalaisten asenteista verkkoturvallisuutta kohtaan (2019) ja eurooppalaisten suhtautumisesta kyberturvallisuuteen (2020) ovat tehneet kartoitusta ihmisten peloista ja huolenaiheista verkkokäyttäytymiseen liittyen, mutta kyselyillä on saattanut olla piilevä tarkoitus testata kansalaisten tietoisuutta ja lisätä ymmärrystä erilaisista kybertoimintaympäristön riskeistä. Kyselytutkimuksina toteutettujen Eurobarometrien kysymysten ja vastausten ohjailevuus voisi viitata siihen, että ihmisten tietoisuuden tasoa on haluttu testata ja samalla lisätä tietoisuutta. Kyselytutkimusten ohjailevuus on kuitenkin vallan käytön muoto (Fairclough 2001b, 62), ja se kertoo myös kielen käytön tarkoituksenmukaisuudesta (Salter ja Mutlu 2018, 172). Euroopan unioni pyrkii siis kyberturvallisuuden toimijana pitämään kansalaiset tietoisena kyberturvallisuuden uhista, joita tavalliset kansalaiset voivat kohdata arkipäiväisissä askareissaan verkossa. Tämän valossa EU näyttäytyy kyberturvallisuustoimijana edelleen turvallisuusuhkien määrittelijänä, mutta ratkaisukeskeisyyttä siirretään lähemmäs yksilötasoa tietoisuuden parantamisella: ”*tavallisten kansalaisten pitäisi tuntea edes perusasiat kyberturvallisuudesta, jotta he voisivat suojautua näiltä uhilta*” (EU:n turvallisuusunionistrategia 2020, 5).

Turvallisuusuhkien arkipäiväistyminen sekä toiminnan legitimointi asiantuntijavallalla näyttäytyvät leimallisina Euroopan unionin kyberturvallisuustoimijuudelle. Turvattomuuden politiikan elementtien tarkastelu aineiston hegemonisissa diskursseissa sekä tilastoaineistossa osoittaa, että kieltä käytetään tarkoituksenmukaisesti (Salter ja Mutlu 2018, 172). Turvattomuuden politiikan elementit vahvistavat ymmärrystä Euroopan unionista teknis-byrokraattisella rakennelmana, jossa asiantuntijavalta on legitimiteetin lähde. Tästä näkökulmasta Bigon (2002) väite siitä, että asiantuntijat käyttävät tietynlaista kieltä tarkoituksenmukaisesti saavuttaakseen auktoriteetin tietyllä osa-alueella pitää täysin paikkansa.

Tarkastelun tulokset osoittavat tässä tutkielmassa, kuinka perinteisen turvallisuuspolitiikan toimintakeinot ovat periytyneet myös EU:n kyberturvallisuuspolitiikkaan turvallisuusuhkien määrittelyn (Sperling ja Webber 2019, 232) ja asiantuntijavallan legitimiteetin muodossa (Egeberg ja Trondal 2017, 677). Samalla eroavaisuutena EU:n perinteisen turvallisuuspolitiikan ja kyberturvallisuuspolitiikan välillä on kuitenkin nähtävissä turvallisuusuhkien

arkipäiväistäminen ja yksilön toiminnan mukaan tuominen osaksi kyberturvallisuuden ratkaisuja. EU:n turvallisuuspolitiikka on jäsenvaltioiden yhteistyöhön perustuvaa (Gegout 2017, 3-4), mutta kuitenkin ylätasolla tehtävää politiikka, jossa EU:kin tukeutuu usein muihin ylikansallisiin päätöksentekoinstituutioihin (Sperling ja Webber 2019, 232). Kyberturvallisuuspolitiikka EU:n laajemman turvallisuuspolitiikan osana eroaa siinä, että ratkaisuja ei voida hakea pelkästään suurilla kansainvälisillä areenoilla, vaan toiminnan olisi oltava tietoista ja johdonmukaista jo jokaisen yksilön kohdalla, jokaisen kansalaisen kotona käyttämillä laitteilla. Tätä tavoitetta kohti EU kyberturvallisuustoimijana tuntuu pyrkivän.

8.2. Tulkinnan sudenkuopat

Tutkimusaineisto on avannut Euroopan unionin näkökulmaa omaan kyberturvallisuustoimijuuteensa. Samalla on todettava tutkimusaineiston kuvaavan vain yhtä tapaa tarkastella sekä tulkita EU:ta kyberturvallisuustoimijana. Aineiston perustuessa Euroopan unionin itse tuottamiin dokumentteihin sekä tilastoihin, korostuu tulkinnassa EU:n itsensä välittämä kuva itsestään kyberturvallisuustoimijana. Toisaalta tämä on juuri se kuva, mitä tässä tutkielmassa haettiinkin, ei *millaisena kyberturvallisuustoimijana EU pyrkii itsensä esittämään*. Ulkopuoliset EU:ta tarkastelevat näkökulmat olisivat varmasti tarjonneet erilaisia tulkinnan tuloksia.

Aineiston dokumenttien tulkintaa kriittisen diskurssianalyysin keinoin tasapainottaa tilastoaineistokappaleiden tulkinta. Vaikka tilastoainesto toimi tässä tutkielmassa tukea antavana aineistona, toi se syvyyttä tarkastella kriittisen turvallisuustutkimuksen hengessä turvattomuuden politiikan elementtejä, joissa turvallisuuden tarkastelu painottuu yksilötasolle. Tilastoaineistokappaleiden haastattelututkimuksina kerätty aineisto on kattavuudessaan sekä tarkkuudessaan merkittävä, mutta kyseisten Erityiseurobarometrien kysymysten ohjailevuutta on tässä tutkielmassa tulkittava kriittisesti, sillä se kertoo vallan rakenteista haastattelijan eli asiantuntijan ja vastaajan eli kansalaisen välillä (Fairclough 2001b, 62). Samalla tilastoaineistokappaleet tarjosivat kysymyksillä ja niistä kootuilla vastauksilla diskursiivisesti mielenkiintoisia tietoja, mutta itse vastausprosenteista ei ollut poimittavissa mitään erityisiä havaintoja. Tämän vuoksi tilastoaineiston rooli tässä tutkielmassa jäi dokumenttiaineistoa tukevaksi elementiksi.

Kriittisen diskurssianalyysin pohjalta tehdyt tulkinnat tutkimusaineistosta toivat esiin toisen näkökulman tarkastella Euroopan unionia kyberturvallisuustoimijana, kuin mitä aiempi tutkimuskirjallisuus on tarjonnut. Toisaalta tarkastelemani aiempi tutkimuskirjallisuus (mm. Carrapico, Farrand, Barrinha ja Christou) painottaa EU:n hallinnon ja hallintorakenteiden tutkimista. Hallinnolliset rakenteet kuten kyberturvallisuuden kokonaisvaltaisuus, horisontaalisen ja vertikaalisen yhteistyön tärkeys sekä Christoun (2019) kyberturvallisuusekosysteemin ulottuvuudet kyllä näkyvät tutkimusaineistossa ja ne ovat merkittäviä rakenteellisia tekijöitä, jotka on sisäistettävä toisenlaisten näkökulmien havaitsemiseksi EU:n kyberturvallisuustoimijuudessa. On esimerkiksi ymmärrettävä jäsenvaltioiden vastahakoisuus luovuttaa päätäntävaltaa EU-tasolle turvallisuus- ja puolustuspoliittisissa kysymyksissä sekä tasoerot jäsenvaltioiden kyberturvallisuusvalmiuksissa ja -kyvykkyyksissä (Christou 2019, 291; Carrapico ja Barrinha 2017, 1263).

Euroopan unionin kyberturvallisuusekosysteemiä esitellessä totesin Carrapicon ja Farrandin (2020, 1115) argumentointiin viitaten, että EU:n omaa heikon turvallisuusfilosofian ja sen kyberturvallisuusvalmiuksien kehittämisen perusteet ovat olleet alun perin täysin taloudelliset. Aineiston analyysin perusteella puhdas taloudellinen argumentointi jää hegemonisten diskurssien taakse pimentoon. Asia, joka sieltä tosin nousee esille on eurooppalaisen arvomaailman korostaminen, ja sen yhtenä elementtinä mainitaan taloudellinen hyvinvointi ja sen suojelu (EU:n turvallisuusunionistrategia 2020). Euroopan talous, mukaan lukien yhteiset (digitaaliset) sisämarkkinat voitaisiin siis dokumenttiaineiston perusteella tulkita osana EU:n arvomaailmaa. Tilastoaineistossa puolestaan kysymyksenasettelu molemmissa kyselytutkimuksissa tarjoaa viitteitä siitä, että ainakin on haluttu tehdä kansalaiset tietoisiksi kyberhyökkäysten ja -rikollisuuden liitännäisyydestä talouteen verkko-ostosten ja pankkitoimintojen sähköistymisen myötä (Erityiseurobarometri eurooppalaisten asenteista verkkoturvallisuutta kohtaan, 2019; Erityiseurobarometri eurooppalaisten suhtautumisesta kyberturvallisuuteen, 2020). Siinä mielessä tilastoaineistokappaleet korostavat kyberuhkien riskiä taloudellisille elementeille jopa enemmän kuin strategiat, jotka painottavat kokonaisvaltaisempaa kuvaa ja puhuvat jopa geopoliittisista jännitteistä (EU:n kyberturvallisuusstrategia 2020, 2). Toisaalta on huomioitava, että analyysi on tutkielman tekijän omaa tulkintaa ja toisenlaiset mielleyhtymät voisivat tuottaa erilaisia tulkinnallisia päätelmiä (Suoninen 2016). Talous, ei tämän tulkinnan perusteella näyttäydy keskeisenä EU:n kyberturvallisuuspolitiikan ajurina.

Kriittisen diskurssianalyysin työkalujen käyttöön tulkinnan tuottamisen välineenä on myös suhtauduttava tietyllä varauksella. Kuten ei mikään metodi, myöskään kriittinen diskurssianalyysi ei ole aukoton analyysin työkalu. Koska yksilölliset mielleyhtymät (Suoninen 2016), tai kuten Fairclough (2001b, 129) niitä kuvaa, *jäsenten resurssit* vaikuttavat merkittävästi tekstin ja kontekstin vuorovaikutuksen tarkasteluun (Flowerdew 2018, 165) sekä diskurssin kritiikin esittämiseen (Fariclough 2018, 13). Kriittistä diskurssianalyysiä käytettäessä on siis vilpittömästi aina todettava aineistonanalyysin omaavan vahvan tulkinnallisen pohjan. Toisaalta tulkinnan vapaus on myös keino vapauttaa tulkitsija tarkastelemaan muun muassa diskurssin ja vallan välistä suhdetta, joka on olennainen osa erilaisiin diskursseihin kohdistuvaa normatiivisen kritiikin esittämistä (Fairclough 2015, 6, 48; Fairclough 2001b, 62).

Eräänä tulkinnan sudenkuoppana tässä tutkielmassa on pidettävä myös itse kriittisen turvallisuustutkimuksen näkökulmia ja turvattomuuden politiikan elementtien tarkastelua. Turvattomuuden politiikan elementit eivät tarjoa yksinkertaista tai muita tulkintoja poissulkevaa lähestymistapaa tarkastella Euroopan unionin kyberturvallisuutta. Turvattomuuden politiikan elementit on ymmärrettävä havaintoina turvallisuuspoliittisen narratiivin kriittisestä tarkastelusta (Guillaume 2013, 91-92). Kriittisen turvallisuustutkimuksen hengessä turvattomuuden politiikan elementit tarjoavat keinon tarkastella turvallisuutta näkökulmasta, jonka valtiokeskeiset toimijat jättävät usein huomioimatta (Buzan ja Hansen 2009, 200). On suhtauduttava varauksella myös siihen, onko tutkielmassa irtauduttu tarpeeksi valtiokeskeisestä näkökulmasta ottaen huomioon aineistovalintojen ’valtiokeskeisyyden’. Toisaalta ainakin analyysin tulokset tuntuisivat esittävän mielenkiintoisia ja erilaisia näkökulmia Euroopan unionin kyberturvallisuustoimijuudesta, kuin mitä aikaisempi, hallinnolliskeskeinen kyberturvallisuustutkimus on kenties esittänyt. Kriittistä tarkastelua voisi aina toki olla lisää, mutta tämä on ollut tutkielman tekijän valinta kuljettaa tarkastelussa mukana, myös pieniä rippeitä realistisemmista ja geopoliittisemmista näkemyksistä.

8.3. Jatkokysymysideoita turvallisuuspolitiikan murrostilanteessa

Kyberturvallisuus kuuluu eittämättä turvallisuuden alana politiikan ja politikoinnin piiriin (mukaillen Bigo ja McCluskey 2018, 123). Kyberturvallisuuden toimintaympäristö on virtuaalisesti monialainen, mutta myös politiikassa moniulotteinen. Siinä liikutaan yksilötasolta kansainväliseen ulko- ja turvallisuuspolitiikkaan ja oman tietokoneen tietoturvasta valtion kyberpelotteen rakentamiseen. Kokonaisuus on tutkijalle vaikeasti

koossa pidettävä ja se on sitä varmasti myös Euroopan unionin kokoiselle organisaatiolle. Tutkimustietoa kyberturvallisuudesta tarvitaan lisää, minkä lisäksi ihmislähtöisempää näkökulmaa on korostettava alan tutkimuksessa. Ihmislähtöisempi näkökulma yhteiskuntatieteellisessä kyberturvallisuustutkimuksessa on tärkeää juuri sen vuoksi, että puhutaan turvallisuuspolitiikan alasta, jolla on suoria ja nopeitakin vaikutuksia yksittäisen ihmisen elämään. Sen lisäksi että yksilön tietoinen tai tiedostamaton toiminta kybertoimintaympäristössä voi vaarantaa hänet itsensä, kybertoimintaympäristön keskinäisriippuvuuksista johtuen yksi teko voi johtaa useampien ihmisten, jopa suurien infrastruktuurien toiminnan tuhoutumiseen. Ei siis pidä vähätellä yksilöiden kouluttamisen ja tietoisuuden parantamisen roolia osana kyberturvallisuuden ratkaisua.

Lisäksi olisi tärkeää tarkastella sitä, millaisia implikaatioita ylätasolla eli valtion tai EU-tason kyberturvallisuuspolitiikalla on yksilötason toiminnalle ja millaiseksi vuorovaikutus näiden kahden tason välillä tulee tulevaisuudessa muodostumaan. Etenkin geopoliittisten tilanteiden kiristyessä ja toimijoiden rakentaessa strategisia kyvykkyyksiään herää eräs tutkimisen arvoinen kysymys: tekeekö kybertoimintaympäristö yksilöistä ulko- ja turvallisuuspolitiikan välineitä? Kysymys on muuttunut yhä olennaisemmaksi, kun seuraamme modernia sotaa reaaliajassa.

Vuonna 2022 Venäjän aloittama hyökkäyssota Ukrainaan on muokannut eurooppalaisten turvallisuuspoliittisia raameja perustavanlaatuisesti. Sota on myös paljastanut kybertoimintojen roolin osana sotaa niin disinformaation levittämisen kuin kyberhyökkäysten muodossa. Disinformaatio ja kyberoperaatiot ovat myös ylittäneet kansallisuuksien ja sotaa käyvien valtioiden rajat. Lisäksi Ukrainan kyberhyökkäyksiä Venäjää vastaan tukevat ulkomaalaiset yksityiset hakkerit, jotka Ukrainan digiministeri Myhailo Fedorov on itse pyytänyt avuksi kyberhyökkäysten tekemiseen (Lappalainen 2022). Ovatko nämä toimijat jo osa kansainvälisen turvallisuuspolitiikan välineistöä? Sota sekä turvallisuuspoliittisen tilanteen kriisiytyminen tulevat varmasti opettamaan paljon käytännön toimista kybertoimintaympäristössä kybersodan aikana, mutta myös muuttamaan valtioiden tapaa tarkastella kyberturvallisuutta. Kenties nyt jos koskaan korostuu koulutetun ja tiedostavan yksilön rooli navigoida itse tiensä ulos sosiaalisen median disinformaation, kyberhyökkäysten sekä -vaikuttamisoperaatioiden maailmasta.

9. Aineistolähteet

Erityiseurobarometri: Eurooppalaisten asenteet verkkoturvallisuutta kohtaan 2019 (alk. engl. Europeans attitudes towards Internet security, special Eurobarometer). [Katsottu 29.1.2022] Saatavissa: https://data.europa.eu/data/datasets/s2207_90_2_480_eng?locale=fi.

Erityiseurobarometri: Eurooppalaisten suhtautuminen kyberturvallisuuteen (kyberrikollisuus) 2020 (alk. engl. Europeans attitudes towards cybersecurity (cybercrime), special Eurobarometer. [Katsottu 30.1.2022] Saatavissa: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en.

Euroopan unionin kyberturvallisuusstrategia digitaaliselle vuosikymmenelle 2020. 2020. [Katsottu: 11.1.2022] Saatavissa: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018&qid=1641904795619.

Euroopan unionin turvallisuusunionistrategia 2020. 2020. [Katsottu: 11.1.2022] Saatavissa: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605.

Euroopan unionin strateginen kompassi. 2021. EU:n ulkosuhdehallinnon korkean edustajan esipuhe sekä tietoisku. [Katsottu 3.2.2022] Saatavissa: https://eeas.europa.eu/headquarters/headquarters-homepage/106337/towards-strategic-compass_en.

10. Lähdekirjallisuus

Abromeit, John. 2018. Max Horkheimer and the Early Model of Critical Theory. Teoksessa Best, Beverly; Bonefeld, Werner; O'Kane, Chris (toim.) *The Sage handbook of Frankfurt School Critical Theory*. London; Thousand Oaks, CA: Sage Inc.

Aradau, Claudia ja van Munster, Rens. 2016. Poststructuralist approaches to security. Teoksessa Dunn Cavelty, Miriam ja Balzacq, Thierry (toim.) *Routledge Handbook of Security Studies*. Second Edition. London: Routledge.

Bangemann -raportti. 1994. Bangemann report: Europe and the global information society. Recommendation to the European Council, High Level Group on Information Society. [Katsottu 21.1.2022] Saatavissa: https://cordis.europa.eu/article/id/2730-bangemann-report-europe-and-the-global-information-society.

Benincasa, Eugenio. 2021. The Case for Cyber 'Disarmament' in the European Union. *The International Spectator* 56:1, 39-54.

Bigo, Didier ja Bonelli, Laurent. 2019. Digital data and the transnational intelligence space. Teoksessa Bigo, Didier; Isin, Engin ja Ruppert, Evelyn (toim.) *Data Politics: Worlds, Subjects, Rights*, 100-122. Abingdon, Oxon; New York, N.Y.: Routledge.

Bigo, Didier ja McCluskey, Emma. 2018. What is PARIS approach to (in)securitization? Political Anthropological Research for International Sociology. Teoksessa Gheniu, Alexandra ja Wohlforth William (toim.) *The Oxford Handbook of International Security*, 116-130. Oxford: Oxford University Press.

Bigo, Didier. 2010. Delivering Liberty and Security? The Reframing of Freedom when Associated with Security. Teoksessa Bigo, Didier; Walker, R.B.J.; Carrera, Sergio ja Guild, Elspeth (toim.) *Europe's 21st Century Challenge: Delivering Liberty*, 263-287. Farnham, Surrey, England: Taylor and Francis Group.

Bigo, Didier. 2008. Security, A Field Left Fallow. Teoksessa Dillon, Michael ja Neal, Andrew (toim.) *Foucault on Politics, Security and War,* 93-114. London: Palgrave Macmillan.

Bigo, Didier. 2002. Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives* 27: 63-92.

Bigo, Didier. 2000. When two become one: Internal and external securitization in Europe. Teoksessa Kelstrup Morten ja Williams Michael (toim.) *International Relations Theory and the Politics of European Integration: Power, Security and Community*. Abingdon, Oxon; New York, N.Y.: Routledge.

Borghard, Erica D. ja Lonergan, Shawn W. 2018. Why are there no cyber arms control agreements? Council on Foreign Relations. [Katsottu 26.1.2022] Saatavissa: https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements.

Bossong, Raphael ja Wagner, Ben. 2016. A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime Law & Social Change* 67:3, 265-288.

Bozeman, Barry. 2000. *Bureaucracy and Red Tape*. Upper Saddle River, NJ: Prentice Hall.

Buzan, Barry ja Hansen, Lene. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Calderoni, Francesco. 2010. The European legal framework on cybercrime: striving for an effective implementation. *Crime Law & Social Change* 54:5, 339-357.

Carrapico, Helena ja Farrand, Benjamin. 2020. Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration* 42:8, 1111-1126.

Carrapico, Helena ja Barrinha, André. 2017. The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies* 55:6, 1254-1272.

CASE Collective. 2006. Critical Approaches to Security in Europe: A Networked Manifesto. *Security dialogue* 37:4, 443-487.

Christou, George. 2019. The collective securitisation of cyberspace in the European Union. *West European Politics* 42:2, 278-301.

Christou, George. 2018. The challenges of cybercrime governance in the European Union. *European Politics and Society* 19:3, 355-375.

Cox, Robert. 1981. Social Forces, States and World Orders: Beyond International Relations Theory. *Millennium – Journal of International Studies* 10:2, 126-155.

Data Europa EU. 2019. Special Eurobarometer 480: Europeans' attitudes towards internet security. [Katsottu 29.1.2022] Saatavissa: https://data.europa.eu/data/datasets/s2207_90_2_480_eng?locale=fi.

Deibert, Ronald J. ja Pauly, Louis W. Mutual Entanglement and Complex Sovereignty in Cyberspace. Teoksessa Bigo, Didier; Isin, Engin ja Ruppert, Evelyn (toim.) *Data Politics: Worlds, Subjects, Rights*, 81-99. Abingdon, Oxon; New York, N.Y.: Routledge.

Deibert, Ronald J. 2018. Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs* 32: 4, 411-424.

Dunn Cavelty, Myriam ja Wenger, Andreas. 2020. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy* 41:1, 5-32.

Dunn Cavelty, Myriam ja Suter, Manuel. 2009. Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection* 2:4, 179-187.

ECSO – European Cybersecurity Organisation. 2022. Contractual Public-Private Partnership (cPPP). [Katsottu 24.1.2022] Saatavissa: https://www.ecs-org.eu/cppp.

Egeberg, Morten ja Trondal, Jarle. 2017. Researching European Union Agencies: What Have We Learnt (and Where Do We Go from Here)? *Journal of Common Market Studies* 55: 4, 675-690.

ENISA. 2016. European Union Agency for Cybersecurity. NIS Directive. [Katsottu 6.1.2022] Saatavissa: https://www.enisa.europa.eu/topics/nis-directive.

ENISA. 2015. Information security and privacy standards for SMEs. [Katsottu 24.1.2022] Saatavissa: https://www.enisa.europa.eu/publications/standardisation-for-smes.

Euroopan komissio. 2022. EU:n turvallisuusunioni. [Katsottu 14.1.2022] Saatavissa: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_fi.

Euroopan komissio. 2021. Euroopan unionin kyberturvallisuusstrategia. [Katsottu: 15.1.2022] Saatavissa: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

Euroopan komissio. 2016. Yhteinen kehys hybridiuhkien torjumiseksi: Euroopan unionin toimet. [Katsottu 24.1.2022] Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

Euroopan komissio. 2015. Euroopan turvallisuusagenda. [Katsottu 24.1.2022] Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52015DC0185&from=EN.

Euroopan komissio. 2013. Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö. [Katsottu 24.1.2022] Saatavissa: https://eur-lex.europa.eu/resource.html?uri=cellar:e8ab3970-f86e-41a6-8666-33e94614dcf2.0010.03/DOC_1&format=PDF.

Euroopan komissio. 2001. Communication on Network and Information Security: proposal for A European Policy Approach. [Katsottu 21.1.2022] Saatavissa: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF.

Eurooppa-neuvosto. 2018. Viitekehys 14413/18 EU Cyber Defence Policy Framework. [Katsottu 12.3.2021] Saatavissa: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf.

Euroopan parlamentti ja Eurooppa-neuvosto. 2016. Direktiivi 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. [Katsottu 12.3.2021] Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Euroopan parlamentti ja Eurooppa-neuvosto. 2004. *Asetus* (EC) No 406/2004 Euroopan parlamentin ja Eurooppa-neuvoston toimesta 10 maaliskuuta 2004 Euroopan verkko- ja tietoturvallisuusviraston perustamisesta.

Euroopan unionin ulkosuhdehallinto. 2016. A Global Strategy for the European Union's Foreign and Security Policy. [Katsottu 24.1.2022] Saatavissa: https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

Euroopan unionin ulkosuhdehallinto. 2021. A Strategic Compass for the EU. [Katsottu 3.2.2022] Saatavissa: https://eeas.europa.eu/headquarters/headquarters-homepage/106337/towards-strategic-compass_en.

Europa. 2021. Yleinen tietosuoja-asetus. [Katsottu 26.1.2022] Saatavissa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm.

Fairclough, Norman. 2018. CDA as dialectical reasoning. Teoksessa Flowerdew, John ja Richardson John E. (toim.) *The Routledge handbook of critical discourse studies*, 13-25. Milton Park, Abingdon, Oxon; New York, NY: Routledge.

Fairclough, Norman. 2015. *Language and Power*. Third Edition. Abingdon, Oxon; New York, N.Y.: Routledge.

Fairclough, Norman. 2001a. Critical Discourse Analysis As A Method in Social Scientific Research. Teoksessa Wodak, Ruth ja Meyer, Michael (toim.) *Methods of Critical Discourse Analysis*, 121-138. London: Sage publications.

Fairclough, Norman. 2001b. *Language and Power*. Second Edition. Essex, England: Pearson.

Fairclough, Norman. 1989. *Language and Power*. London: Longman.

Flowerdew, John. 2018. Critical discourse studies and the context. Teoksessa Flowerdew, John ja Richardson John E. (toim.) *The Routledge handbook of critical discourse studies*, 165-178. Milton Park, Abingdon, Oxon; New York, NY: Routledge.

Foucault, Michel. 1978. Security, *Territory and Population*. Luennot Collège de Francessa 1977-78. Luennot 11. ja 18. tammikuuta 1978.

Gartman, David. 2013. *Culture, Class, and Critical Theory: between Bourdieu and Frankfurt School*. New York: Routledge.

Gee, James. 1996. Social Linguistics and Literacies: Ideology in Discourses. New York, N.Y.: Routledge.

Gegout, Catherine. 2017. *European Foreign and Security Policy: State, Power, Institutions*. Toronto: University of Toronto Press.

Georgieva, Ilina. 2020. The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy* 41:1, 33-54.

Giacomello, Giampiero. 2014. Introduction: Security in Cyberspace. Teoksessa Giacomello, Giampiero (toim.) *Security in Cyberspace – targeting Nations, Infrastructures, Individuals*. London: Bloomsbury.

Griffiths, James. 2019. *The Greats Firewall of China: How to Build and Control an Alternative Version of the Internet*. London: Zed Books Ltd.

Guillaume, Xavier. 2013. Criticality. Teoksessa Mutlu, Can ja Salter, Mark (toim.) *Research methods in critical security studies*, 91-98.

Helsingin Sanomat pääkirjoitus 4.2.2022. 2022. *Ursula von der Leyen antoi poliittiset turvatakuut EU:n keskinäisestä avusta kriisissä*. [Katsottu 4.2.2022] Saatavissa: https://www.hs.fi/paakirjoitukset/art-2000008587482.html.

Hendershot, Chris ja Mutimer David Critical Security Studies.2018. Teoksessa (toim.) Gheniu, Alexandra ja Wohlforth William *The Oxford Handbook of International Security*, p. 60-70.

Horng-En Wang, Austin; Lee, Mei-chun; Wu, Min-Hsuan ja Shen, Puma. Influencing overseas Chinese by tweets: text-images as the key tactic of Chinese propaganda. *Journal of Computational Social Science* 3:2, 469-486.

Husu, Rikhard. 2022. Aukeaako Ukrainan umpisolmu? Nato-maat ja Venäjä kokoustavat Brysselissä – tästä tapaamisessa on kyse. Yle uutiset 12.1.2022. [Katsottu 12.1.2022] Saatavissa: https://yle.fi/uutiset/3-12266347.

Hybrid CoE. 2022. The European Centre of Excellence for Countering Hybrid Threats. Establishment. [Katsottu 27.1.2022] Saatavissa: https://www.hybridcoe.fi/establishment/.

Jokinen, Arja; Juhila, Kirsi ja Suoninen, Eero. 2016. *Diskurssianalyysi: teoriat, peruskäsitteet ja käyttö*. Tampere: Vastapaino.

Jokinen, Arja ja Juhila, Kirsi. 2016. Valtasuhteiden analysoiminen. Teoksessa Jokinen, Arja; Juhila Kirsi ja Suoninen, Eero (toim.) *Diskurssianalyysi: teoriat, peruskäsitteet ja käyttö*. Tampere: Vastapaino.

Jokinen, Arja ja Juhila, Kirsi. 1991. *Diskursseja rakentamassa*. *Näkökulma sosiaalisten käytäntöjen tutkimiseen*. Tampereen yliopisto, sosiaalipolitiikan laitos, Tutkimuksia, Sarja A, Nro 2. Tampere: Tampereen yliopisto.

Keinonen, Maria. 2021. 02 Kyber. Sotataidon ytimessä -podcast 2.12.2021. [Kuunneltu 14.1.2022] Saatavissa: Spotify, Sotataidon ytimessä -podcast.

Kielitoimiston sanakirja. 2022a. Strategia. Kotimaisten kielten keskus ja Kielikone Oy. [Katsottu 11.1.2022] Saatavissa: https://www.kielitoimistonsanakirja.fi/#/strategia?source=suggestion&searchMode=all.

Kielitoimiston sanakirja. 2022b. Esipuhe. Kotimaisten kielten keskus ja Kielikone Oy. [Katsottu 4.2.2022] Saatavissa: https://www.kielitoimistonsanakirja.fi/#/fulltext/esipuhe?order=entry&field=&baseforms=false.

Kielitoimiston sanakirja. 2022c. Byrokratia. Kotimaisten kielten keskus ja Kielikone Oy. [Katsottu 14.2.2022] Saatavissa: https://www.kielitoimistonsanakirja.fi/#/byrokratia?searchMode=all.

Koskinen, Anu Leena. 2020. Vastaamo lähettänyt henkilötunnuksia sähköpostissa suojaamatta laskun mukana – asiantuntija: ”Vastoin kaikkia sääntöjä”. Yle uutiset 28.10.2020. [Katsottu 10.2.2022] Saatavissa: https://yle.fi/uutiset/3-11617763.

Lappalainen, Elina. 2022. Ukrainan digiministeri teki Twitterin aseen ja valjasti kryptovaluutat ja hakkeriyhteisön maansa tueksi. Helsingin Sanomat 21.3.2022. [Katsottu 27.3.2022] Saatavissa: https://www.hs.fi/visio/art-2000008686788.html.

Limnéll, Jarno. 2021. Suomenkin pitää vastata kyberhyökkäyksiin poliittisesti. *Kanava* 7/2021, 6-11.

Locke, Terry. 2004. Critical Discourse Analysis: Critical Discourse Analysis As Research Method. London; New York: Continuum.

Lundin, Martin ja Öberg, Per Ola. 2014. Expert knowledge use and deliberation in local policy making. *Policy Sciences* 47:1, 25-49.

Macdonald, Bradley J. 2017. Traditional and Critical Theory Today: Toward a Critical Political Science. *New political Science* 39:4, 511-522.

Manners, Ian. 2002. Normative Power Europe: A Contradiction in Terms? *Journal of Common Market Studies* 40:2, 235-258.

Martinich, Aloysius P. 1977. Austin, Strawson and the Correspondence theory of Language. *Crítica: Revista Hispanoamericana de Filosofía* 9:26, 39-64.

McGuinness, Damien. How a cyber attack transformed Estonia. BBC News 27.4.2017. [Katsottu 26.1.2022] Saatavissa: https://www.bbc.com/news/39655415.

Mckinlay, Andrew ja McVittie, Chris. 2008. *Social Psychology and discourse*. Hoboken: John Wiley & Sons.

Merino, Álvaro. 2021. ENISA: The cornerstone of the EU’s cybersecurity strategy. European Data Journalism Network. [Katsottu 24.1.2022] Saatavissa: https://www.europeandatajournalism.eu/eng/News/Data-news/ENISA-The-cornerstone-of-the-EU-s-cybersecurity-strategy.

Metsämuuronen, Jani. 2008. Laadullisen tutkimuksen perusteet. Metodologia-sarja 4. Helsinki: International Methelp Ky.

Mutimer, David. 2016. Critical Security Studies. Teoksessa Dunn Cavelty, Miriam ja Balzacq, Thierry (toim.) *Routledge Handbook of Security Studies*. Second Edition. London: Routledge.

Norilo, Niko. 2021. Kyberturvallisuus alkaa ymmärryksestä. Sotilasaikakausilehti 3/2021.

Nye, Joseph S. Jr. 2016/17. Deterrence and Dissuasion in Cyberspace. *International Security* 41:3, 44-71.

Pérez-Durán, Ixchel ja Bravo-Laguna, Carlos. 2019. Representative bureaucracy in European Union agencies. *Journal of European Integration* 41:8, 971-992.

Poliisi (Suomi). 2022. Kyberrikokset. [Katsottu 25.1.2022] Saatavissa: https://poliisi.fi/kyberrikokset.

Renard, Thomas. 2016. Partnering for Global Security: The EU, Its Strategic Partners and Transnational Security Challenges. *European Foreign Affairs Review* 21:1, 9-33.

Rimpiläinen, Tuomas. 2020. Psykoterapiakeskus Vastaamon kiristäjä julkaisi yöllä lisää erittäin arkaluontoisia potilaskertomuksia. Yle uutiset 22.10.2020. [Katsottu 10.2.2022] Saatavissa: https://yle.fi/uutiset/3-11606925.

Roach, Steven C. 2016. Critical Theory. Teoksessa Dunne Timothy; Kurki, Milja; Smith, Steve (toim.) *International relations theories: discipline and diversity.* Fourth Edition. Oxford: Oxford University Press.

Salter, Mark B ja Mutlu, Can E. 2018. Methods in Critical Security Studies. Teoksessa (toim.) Gheciu Alexandra ja Wohlforth William C.: *The Oxford Handbook of International Security*. Oxford: Oxford University Press.

Schimmelfennig, Frank. 2003. *The EU, NATO and the integration of Europe: rules and rhetoric*. Cambridge: Cambridge University Press.

Schmidt, Vivien A. 2013. Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput'. *Political Studies* 61:1, 2-22.

Sperling, James & Webber, Mark. 2019. The European Union: security governance and collective securitisation. *West European Politics* 42: 2, 228-260.

Suoninen, Eero. 2016. Kielenkäytön vaihtelevuuden analysoiminen. Teoksessa (toim.) Jokinen, Arja; Juhila Kirsi ja Suoninen, Eero: Diskurssianalyysi: teoriat, peruskäsitteet ja käyttö. Tampere: Vastapaino.

Tietoarkisto. 2022. Kansainvälisiä aineistosarjoja: Eurobarometrit. [Katsottu 19.3.2022] Saatavissa: https://www.fsd.tuni.fi/fi/aineistot/kansainvalisia-aineistosarjoja/eurobarometrit/.

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. Turvallisuuskomitea Puolustusministeriö.

Von Solms, Rossouw ja Van Niekerk, Johan. 2013. From information security to cyber security. *Computers & Security* 38; 97-102.

Vuori, Juha A. 2014. *Critical Security and Chinese Politics: the Anti-Falungong Campaign*. Abingdon, Oxon: Routledge.

Wessel, Ramses A. 2015. Towards EU cybersecurity law: Regulating a new policy field. Teoksessa (toim.) Tsagourias, Nicholas ja Buchan, Russell: *Research Handbook on International Law and Cyberspace*, 403-425. Cheltenham, UK; Massachusetts, USA: Edward Elgar Publishing Inc.

Young, Lynne ja Harrison Claire. 2004. Systemic functional linguistics and critical discourse studies: Studies in social change. London; New York: Continuum.