Markus Vaija

KYBERTERRORISMI – TODELLINEN ILMIÖ VAI TULEVAISUUDEN UHKA?

TIIVISTELMÄ

Vaija, Markus
Kyberterrorismi – todellinen ilmiö vai tulevaisuuden uhka?
Jyväskylä: Jyväskylän yliopisto, 2023, s.50
Turvallisuus ja strateginen analyysi, Pro Gradu tutkielma
Ohjaaja(t): Lehto, Martti

Kyberterrorismi on usein tunnistettu uhka, mutta siltä puuttuu yhteisesti hyväksytty ja eri toimijoiden jakama määritelmä. Tämä jo pitkään tiedostettu problematiikka haastaa sekä akateemista keskustelua että viranomaisyhteistyötä uhkaan vastaamisessa. Tässä tutkimuksessa perehdyttiin tapoihin, joilla kyberterrorismia on aiemmin pyritty määrittelemään, ja minkälaisia lähestymistapoja on koetettu. Tutkimus toteutettiin alkuvaiheen kirjallisuuskatsauksena ja myöhemmin teorialähtöistä sisällönanalyysiä hyödyntäen. Kirjallisuuden joukosta valittiin parhaaksi ja kattavimmaksi todettu määritelmä, jonka avulla lähestyttiin viimeisen vuoden aikana tapahtuneita tosimaailman kyberhyökkäyksiä. Teorialähtöisen sisällönanalyysin avulla pyrittiin selvittämään, toimiiko tämä valittu määrittelytapa tapausten luokittelemiseen kyberterrorismiksi, tai voidaanko sen avulla aiemmin haastavat rajatapaukset sulkea määritelmän ulkopuolelle. Tutkimuksessa löydettiin tapauksia, jotka sopivat määritelmän mukaiseen käsitykseen kyberterrorismista, mutta valitun taksonomian käyttöön liittyi myös merkittäviä haasteita. Eräs suurimmista haasteista oli toimijoiden tunnistaminen kyberhyökkäysten taustalla, ja etenkin ei-valtiollisen toiminnan erottaminen valtiollisesta. Toinen merkittävä haaste liittyi hyökkäysten aikomuksen, eli tavoitteen arviointiin, joka usein edellytti varsin korkeaa tulkinnanvaraisuutta. Kokonaisuudessaan kuitenkin taksonomian voitiin todeta olevan toimiva tunnistamaan kyberterrorismin määritelmään sopivia tapauksia ja että ilmiön erottaminen muista kyberuhista on mahdollista, joskin haastavaa. Jatkotutkimusaiheiksi esitetään etenkin kyberterrorismikäsitteen laajentamista koskemaan myös mahdollisen valtiollisen taustan tai motiivin omaavia hyökkäyksiä sekä luopumista vaatimuksesta, että tullakseen määritellyksi kyberterrorismiksi, tulee kybertapahtuman johtaa kineettisiin, eli fyysisen maailman seurauksiin.

Asiasanat: Kyberterrorismi, kyberuhat, terrorismi,

ABSTRACT

Vaija, Markus
Cyberterrorism – a real phenomenon or a threat of the future?
Jyväskylä: University of Jyväskylä, 2023, 50 pp.
Security and strategic analysis, Master's Thesis
Supervisor(s): Lehto, Martti

Cyberterrorism is an often identified threat, but one that lacks a commonly agreed definition shared by different actors. This problem, which has been recognised for a long time, challenges both academic discussion and cooperation between authorities in responding to the threat. This study explored the ways in which cyberterrorism has been defined in the past and what approaches have been tried. The study was carried out as an initial literature review, and later using theory-based content analysis. Among the literature, the best and most comprehensive definition of cyberterrorism was selected and applied to real-world cyberattacks that have occurred in the past year. The purpose of theory-based content analysis was to find out whether this chosen definition method works for classifying cases as cyberterrorism, or whether it can be used to exclude previously challenging borderline cases from the definition. The study found both cases that fit the definition of cyberterrorism, but there were also significant challenges associated with the use of the chosen taxonomy. One of the major challenges was related to difficulties in differentiating between non-state and state supported actors behind the attacks. Another encountered issue had to do with need of assessing the intent, i.e. objective, of the cyberattacks, which often came with a high degree of ambiguity. However, the taxonomy overall was found to be effective in identifying cases that fit the definition of cyberterrorism, and that distinguishing the phenomenon from other cyber threats is possible, albeit challenging. Suggested further research topics include expanding the concept of cyber terrorism to include attacks with a possible state background or motive, and waiving the requirement that in order to be defined as cyberterrorism, a cyber event must lead to kinetic, i.e. physical, consequences.

Keywords: cyberterrorism, cyberthreats, terrorism,

KUVIOT

SISÄLLYS

1 JOHDANTO

1.1 Kyberterrorismi – uhka vailla määritelmää

Kybermaailman uhista puhutaan jatkuvasti enemmän, ja niihin suhtaudutaan entistä vakavammin. Näitä uhkia on paljon erilaisia, ja se huoli, joka niitä kohtaan osoitetaan kasvaa samaa tahtia kuin riippuvuus erilaisista digitaalisista järjestelmistä ja sovelluksista eri yhteiskunnan osa-alueilla korostuu. Eräs uhka, josta jonkin verran puhutaan ja joka kenties nimensä perusteella vaikuttaa jopa muihin kyberuhkiin verrattuna korostuneen huolestuttavalta on kyberterrorismi. Tässä termissä yhdistyy kaksi usein uhkaavaksi koettua ilmiötä, eli luonnostaan pelottava terrorismi ja usein ainakin asiaan perehtymättömälle tuntematon ja siten uhkaavaksi mielletty kyberympäristö. Kyberterrorismista puhutaan jonkin verran, mutta hämmentävää kyllä, ei sille tunnu löytyvän selkeää määritelmää. Entistä haastavamman, ja toisaalta mielenkiintoisemman, ilmiöstä tekee edelleen se, että monet asiantuntijat tuntuvat olevan eri mieltä onko se todellinen ilmiö ollenkaan, tai lähinnä että onko kyberterrorismiksi miellettäviä tapahtumia vielä tähän mennessä tapahtunut yhtäkään (Kenney, 2015, Plotnek & Slay 2021).

Kuitenkin kyberterrorismi, tai ainakin terroristisen toimijoiden kyberympäristön käyttö, on monen turvallisuusviranomaisen toteama uhka, ja vieläpä sellainen, joka on sekä ollut ja jonka oletetaan yhä jatkavan kasvamistaan. Esimerkiksi Suomessa Suojelupoliisi toteaa kansallisen turvallisuuden katsauksessa, että Suomen rajojen sisällä tapahtuvasta terrorismiin liittyvästä toiminnasta merkittävä osa tapahtuu kyberympäristössä (Suojelupoliisi, 2022). Samoin kansainvälisesti on terroristisen toimijoiden kyberympäristön kasvavan hyödyntämisen muodostama uhka huomattu, ja vaikka tarkkaa tietoa tai esimerkkejä tunnettujen terroristiryhmittymien kyberpotentiaalista ei ole ovat useat tunnetut terroritoimijat selvästi tunnistaneet ja myös julkisesti ilmaisseet tavoitteensa oman kyberpotentiaalinsa lisäämiseen. Esimerkiksi tunnettuun terrorijärjestö ISIS:iin liitetty United Cyber Caliphate (UCC), ajaa ryhmittymän etuja kybertoiminnan keinoin

ja on tunnistettu merkittäväksi uhkatoimijaksi toimijaksi kyberympäristössä. (Blanning, 2017).

Näissäkään ulostuloissa ei kuitenkaan yleisesti ole määritelty sitä mitä kyberterrorismi varsinaisesti on, tai vaihtoehtoisesti määritelmät eri toimijoiden välillä poikkeavat toisistaan huomattavasti. Kyberterrorismi on siis tunnistettu ja kasvava uhka, jolta kuitenkin puuttuu selkeä määritelmä. Tämä on toisaalta luonnollista, sillä yhteisesti sovittua ja hyväksyttyä kategorisointia ei löydy edes pelkän ”tavallisen” terrorismin kohdalla, ja termin tuominen kyberympäristöön on luonnollisesti myös osoittautunut haastavaksi (Plotnek & Slay 2021).

Onkin hieman ristiriitaista, että termi on toisaalta laajalti ja kasvavasti käytetty, mutta ilman varsinaista ja yhteisesti sovittua määritelmää. Kuten todettua, sama pitää toki paikkansa myös ”perinteisen” terrorismin kohdalla, eli myöskin siitä on olemassa kilpailevia määritelmiä ja yhteisesti hyväksytty käsitys puuttuu (Chenoweth, English, Gofas & Kalyvas, 2019 s. 34-37). Silti kyberterrorismi eroaa tässä suhteessa ilmiöstä, josta se on johdettu, sillä kuten todettua toisin kuin perinteisen terrorismin kohdalla on jonkin verran kiistanalaista, että tapahtuuko kyberterrorismia lainkaan. Vaikka perinteistä terrorismia siis määritellään eri tavoin, lähes poikkeuksetta kuitenkin määritelmää vastaavaa toimintaa voidaan tunnistaa ja käsitellä. Tämä ei kuitenkaan toteudu kyberterrorismin kohdalla ja se on merkittävä ero siinä suhteessa, että luonnollisesti ilmiön käsittely ja jäsentäminen on helpompaa, jos se voidaan sitoa konkreettisiin tapahtumiin, kuin jos puhutaan pelkästä teoreettisesta uhasta tai potentiaalisesta toiminnasta.

Ongelma määritelmän haastavuuden suhteen ei suinkaan ole uusi. Ensimmäiset maininnat kyberterrorismista, ja yritykset muodostavat sille selkeä määritelmä ovat peräisin jo vuosituhannen vaihteesta (Denning, 2000). Akateemisessa keskustellussa etenkin on pitkään kuitenkin vaikuttanut ajatus, että kyberterrorismia ei varsinaisesti ole olemassa, tai sen ei ole ainakaan vielä havaittu olevan todellinen ilmiö (esim. Abdulrahman 2015, Kenney 2015, Dogrul et al. 2011). Tämä ajatusmalli perustuu jo ensimmäisiin ilmiön määrittelytapoihin sisältyneeseen vaatimukseen, että ollakseen kyberterrorismia, tulee kybermaailmassa tapahtuneen ideologisesti motivoituneen toiminnan johtaa fyysisen maailman seurauksiin, eli yleisesti joko ihmisten loukkaantumiseen tai jonkin laitteen pysyvään vaurioitumiseen (Denning, 2000). Tämän lisäksi toinen oleellinen komponentti on ollut toiminnan ”terroristinen motivaatio” eli taustalla vaikuttava pyrkimys tuottaa pelkoa ja epäjärjestystä, sekä edistää toimijan poliittista tai ideologista agendaa (Plotnek & Slay, 2021). Sikäli kun fyysisen maailman seurauksiin johtavat kyberhyökkäykset ovat ainakin vielä olleet suhteellisen harvinaisia ei toisaalta ole yllättävääkään, että tämän vaatimuksen toteuttavaa kyberterrorismiksi miellettävää toimintaa ei ole toistaiseksi havaittu. Kuitenkin ideologisen ja poliittisesti motivoituneen kybertoiminnan on arvioitu merkittävästi kasvaneen muutaman viimeisen vuoden aikana, ja poliittista agendaa edistäviä ja epäjärjestystä tuottavia hyökkäyksiä on sitäkin enemmän (Thomas, Collier, Hutchings, Clayton & Anderson,). Onkin kenties siis asiallista haastaa nämä vallitsevat käsitykset kyberterrorismista, selvittää miksi näihin ajatuksiin ilmiöstä

on päädytty, ja onko olemassa määrittelytapoja kyberterrorismista, joiden mukaista toimintaa voitaisiin todellisuudessa tunnistaa ja siten helpommin käsitellä.

Tämän tutkimuksen tarkoituksena on selvittää, voidaanko kyberterrorismia siis määritellä tavalla, joka mahdollistaa sen käsittelyn omana, muista kyberuhista irrallisena ilmiönä, mutta jota vastaavaa toimintaa voidaan konkreettisesti tunnistaa todellisen maailman tapahtumista. Tutkimus on toteutettu kahdessa vaiheessa, josta ensimmäinen koostui kirjallisuuskatsauksena, jonka tarkoituksena oli saavuttaa ymmärrys siitä, miten kyberterrorismia on aiemmin pyritty määrittelemään. Huomio kiinnittyi tekijöihin, jotka ovat olleet erityisen haastavia määrittelyn kannalta, ja mitkä ovat kenties osaltaan johtaneet tilanteeseen, jossa kilpailevia määritelmiä on niin paljon. Ensimmäisen työvaiheen pohjalta valittiin kirjallisuudesta löydetty parhaaksi koettu olemassa oleva tapa jäsentää kyberterrorismia, ja tätä määrittelytapaa testattiin lähestymällä vertaamalla sitä todellisen maailman tapahtumiin. Käytännössä tämä toteutettiin teorialähtöisen sisällönanalyysin keinoin, jossa ohjaavana teoriana toimi valittu kyberterrorismin määrittelytapa, ja aineistoksi kerättiin viimeisen kahden vuoden ajalta esimerkkitapauksia kybermaailman tapahtumista, jotka intuitiivisesti ilman ennakkokäsityksiä voitaisiin mieltää terrorismiksi.

Tämän tutkimuksen tavoitteena ei ole siis kehittää uutta määritelmää kyberterrorismista, vaan selvittää miksi käsitettä on ollut niin vaikea määritellä, ja kuinka pitkällä tässä työssä tällä hetkellä ollaan. Vastaavanlaista tutkimusta, jossa valittua määritelmää verrataan käytännön tapahtumiin ei ainakaan suurissa määrin ole tehty, ja tämänkaltainen lähestymistapa voi tuottaa uudenlaista ymmärrystä siitä, miten ilmiötä tulisi kenties jatkossa lähestyä.

Työ koostuu alussa olevista käsitteiden, ja aiheen esittelyyn keskittyvistä luvuista, joiden lopuksi tutkimuskysymys ja aiheen rajaus esitellään tarkemmin. Tämän jälkeen luvussa 4 avataan tutkimuksen ensimmäisen vaiheen, eli kirjallisuuskatsauksen löydöksiä ja luvussa 5 tuloksia, jotka saatiin, kun valittua määritelmää verrattiin todellisuuteen. Viimeisessä luvussa 6 puolestaan esitellään johtopäätöksiä, joita tästä tutkimuksesta saatiin ja pohditaan mitä ne merkitsevät kyberterrorismiin liittyvälle tutkimukselle tulevaisuuden suhteen.

2 TUTKIMUKSEN TAUSTAA

Tässä alaluvussa esitellään tutkimuksen kannalta oleellisimpia käsitteitä ja miten niitä on hyödynnetty tämän työn kontekstissa. Koska käsiteltävänä aiheena olevan ilmiön eli kyberterrorismin itsensä määrittely on yksi tutkimuksen kohteena olevista ongelmista, siihen palataan vasta myöhemmissä luvuissa. Luvun lopussa myös esitetään tämän tutkimuksen varsinainen tutkimuskysymys, sekä siten miten aihetta on rajattu.

2.1 Miksi kyberterrorismin määrittely on ongelma

Kyberterrorismin koetaan olevan kasvava ja uhkaa tuottava toiminnan muoto, jonka tarkkaa määrittelyä ei kuitenkaan tunnu löytyvän niistäkään julkaisuista, joissa sen tuomaa uhkaa esitellään (Burak Bicak & Bogdanova, 2018). Seuraavassa luvussa käsitellään tarkemmin, miten kyberterrorismia on määritelty ja miten määritelmät ovat kehittyneet vuosien saatossa. On kuitenkin hyvä ymmärtää taustalla vaikuttava motivaatio siihen, miksi kyberterrorismin käsitettä on ylipäänsä pyritty jäsentämään ja miksi yleisesti hyväksytyn määritelmän kehittäminen olisi tärkeää.

Viranomaisteksteissä terroristien usein tunnistetaan hyödyntävän kybertoimintaympäristöä eri keinoin, mutta tarkkaa määrittelyä kyberterrorismille ei silti tehdä. Esimerkiksi Suomessa Suojelupoliisi julkaisee vuosittain kansallisen turvallisuuden katsauksen, jossa terrorismin tuottamaa uhkaa ja sen kehitystä arvioidaan vuositasolla. Viimeisimmässä, vuonna 2022 ilmestyneessä katsauksessa terrorismin uhka määritellään neliportaisen asteikon toiselle tasolle ja lisäksi todetaan että

> *”merkittävä osa (terroristisesta) toiminnasta, kuten verkostoituminen, tapahtuu internetissä ja viestintäsovelluksissa” (Suojelupoliisi 2022).*

Kuitenkaan sanaa kyberterrorismi ei mainita katsauksessa kertaakaan. Vaikka terroristisen toiminnan onkin siis todettu tuottavan uhkaa, ja kyberympäristön näyttelevän tässä merkittävää roolia, ei kyberterrorismista ole mainintaa (Suojelupoliisi 2022). Viestintäviraston Turvallisuuskomitean julkaisemassa Kyberturvallisuuden sanastossa termi puolestaan käsitetään määrittämään suhteellisen laajasti

> *"terroristista toimintaa, jossa hyökätään tietojärjestelmien kautta kansalaisia, liikeelämää yhteiskunnan elintärkeitä toimintoja, kriittistä infrastruktuuria tai muuta kohdetta vastaan" (Viestintävirasto 2018).*

Tämän kaltainen määrittely jättää huomattavasti tulkinnanvaraa, ja eroja eri instituutioiden ja etenkin eri valtioiden välillä on paljon (Burak Bicak & Bogdanova, 2018).

Käsitteen käyttöä on kenties vältelty juuri, sen monitulkintaisuuden ja vaihtelevan määrittelyn vuoksi. Kyberterrorismista on puhuttu sekä akateemisessa ympäristössä että sen ulkopuolella jo vuosia, ja kun konsensusta määrittelystä ei ole syntynyt on se johtanut entistä sekavampaan kenttään ja keskenään kilpaileviin lähestymistapoihin (esim. Kenney 2015, Plotnek & Slay 2021). Kun yhteistä tapaa puhua ilmiöstä ei ole haastaa se luonnollisesti tutkijayhteisöä, mutta myös turvallisuusviranomaisia. Etenkin kansainvälisen yhteistyön on todettu olevan haasteellista, kun jokainen toimija tuntuu määrittelevän kyberterrorismin (tai siihen kuuluvat komponentit) omalla tavallaan (M. Dogrul, A. Aslan, & E. Celik, 2011). Kansainvälisen yhteistyön kehittäminen olisi kuitenkin erittäin oleellista kasvavaan uhkaan vastaamisessa.

Terrorismi yleisesti on varsin kansainvälinen ilmiö, ja toimintana äärimmäisen kohdistuu saman valtion rajojen sisälle kuin missä toimija itse on (Chenoweth et al. s. 34-37). Tämä pätee ja haastaa viranomaisia myös kyberterrorismiin varautumisen suhteen. Kohdevaltion lainsäädäntö ja rikollisten seuranta on siis usein hyödytöntä ulkomailta tulevan iskun tekijöiden rankaisemiseksi tai toiminnan rajoittamiseksi. Tarve kansainväliselle yhteistyölle onkin suuri ja vaikka erilaisia kansainväliseen kyberrikollisuuteen keskittyviä toimijoita on ja niiden resurssit kasvavat jatkuvasti, vaikuttaa silti siltä, että yhteistyön kehittyminen on hidasta. (M. Dogrul, A. Aslan, & E. Celik, 2011).

Yksi suurimmista seikoista, jonka voi nähdä jarruttavan kyberterrorismin torjuntaan liittyvän kansainvälisen toiminnan kehittymistä, on yhteisen ilmiön määritelmän (ja sen myötä yhteneväisen lainsäädännön) puutteen lisäksi kyberterrorismin kohdistuminen kansallisiin järjestelmiin, joiden suojaus ja sen eri osien kattavuus on erittäin salaista. Kyberterrorismin kannalta houkuttelevimpien kohteiden joukkoon kuuluvat valtion kannalta elintärkeiden kyberinfrastruktuurin osiin kohdistuvat iskut. Näiden ollessa myös valtioiden välisen kybertiedustelun ja jopa kybersodankäynnin kohteita, ei tietoja omasta puolustuskyvystä, tai varsinkaan siinä olevista aukoista, mielellään julkaista (Chaturvedi, Unal, Aggarwal, Bahl, & Malik. 2014).

Kuitenkin olisi sekä viranomaistyön että akateemisen tarkastelun kannalta oleellista saavuttaa yhteinen ja jaettu ymmärrys siitä mitä kyberterrorismi on.

Tiedeyhteisöllä tuntuu olevan jaettu käsitys siitä miksi terroristisesti motivoituneet toimijat kyberympäristöä haluavat tai pyrkivät hyödyntämään, mutta silti tämän toiminnan kokonaisuus eli kyberterrorismi on vailla yleisesti hyväksyttyä määritelmää. Tämä on johtanut tilanteeseen, jossa kyberterrorismista käytävä akateeminen keskustelu on pirstaleista ja muiden tekemän työn päälle on vaikea rakentaa määritelmien ja lähestymistapojen vaihdellessa (Kenney, 2015).

2.2 Käytettäviä käsitteitä

2.2.1 Terrorismi

Terroristisen toiminnan määrittely itsessään on lähes yhtä haastavaa kuin kyberterrorisminkin ja tapoja jäsentää ilmiötä on olemassa satoja (Plotnek & Slay 2021). Tämän tutkimuksen tarkoituksena on tarkastella kyberympäristön hyödyntämistä terroristisen toiminnan tukemisena, joten on oleellista määritellä myös käsiteltävän ilmiön taustaetermi eli terrorismi itsessään. Tässä tutkimuksessa fokus ei kuitenkaan ole itse terrorismin käsitteessä, joten terroristisen toiminnan määrittelyyn on valittu myös laaja ja paljon vapauksia antava käsitteistö. Käytettäväksi valittu määritelmä on hyvin löyhä ja laaja tapa määritellä terrorismia, koska kerättävää aineistoa ei rajata liikaa.

Terrorismia käytetään terminä usein strategisen viestinnän työkaluna, kun hyökkäyksen toteuttanut taho pyritään kuvaamaan mahdollisimman negatiiviseen sävyyn ja toiminta kehystämään mahdollisimman tuomittavaksi (Burak Bicak & Bogdanova 2018). Jotta vältyttäisiin analysoimasta vain toimintaa, joka on haluttu kehystää terrorismiksi informaatiovaikuttamistarkoituksessa, laaja ja tutkijariippuvainen määritelmä on pakollinen.

Terroristisen toiminnan tunnistaminen on myös varsin haastavaa, ja attribuutioon liittyy merkittäviä ongelmia (Agrafiotis et al. 2018). Tästäkin syystä on päädytty käyttämään laajaa ja tulkinnan varaista määritelmää aineiston suppeuden välttämiseksi. Tutkimuksessa aineistoon haluttiin hyväksyä toimintaa, joka on määriteltävissä terroristiseksi ja tapahtuu pääosin tai kokonaan kyberympäristössä. Yleinen tapa määritellä terrorismia on sen motivaatioon tai tavoitteeseen perustuen (Chenoweth et al. s. 34-37) ja se toimii myös tämän tutkimuksen kontekstissa. Koska tutkimuksessa käsitellään terroristista kybertoimintaa, on hyvä tapa määritellä terrorismia sen motivaatioon perustuen.

Käytännössä hyödynnetään Suomen rikoslain luvun 34a kuudennesta momentista löytyvää terroristisen toiminnan määrittelyä. Suomen rikoslaissa ei varsinaisesti ole määritetty erillisiä terrorismirikoksia, vaan ”tavallisia” rikoksia tulkitaan eri tavalla, mikäli niillä voidaan todeta olevan terroristinen tarkoitus. Tarkoituksella tarkoitetaan toiminnan motivaatiota, ja jotta rikos voitaisiin määritellä terroristiseksi, tulee toiminnan tavoitteena olla

1) aiheuttaa vakavaa pelkoa väestön keskuudessa;

2) pakottaa oikeudettomasti jonkin valtion hallitus tai muu viranomainen taikka kansainvälinen järjestö tekemään, sietämään tai tekemättä jättämään jotakin;

3) oikeudettomasti kumota jonkin valtion valtiosääntö tai muuttaa sitä tai horjuttaa vakavasti valtion oikeusjärjestystä taikka aiheuttaa erityisen suurta vahinkoa valtiontaloudelle tai valtion yhteiskunnallisille perusrakenteille; tai

4) aiheuttaa erityisen suurta vahinkoa kansainvälisen järjestön taloudelle tai sellaisen järjestön muille perusrakenteille. (Suomen rikoslaki 2021/281 34a § 6).

Rikoslaissa lisäksi määritellään terroristiryhmän olevan vähintään kolmen henkilön muodostama tietyn ajan koossa pysyvä yhteenliittymä, joka toimii yhteisen (terroristisen) tavoitteen edistämiseksi.

2.2.2 Kyberympäristö ja kybertoiminta

Tässä tutkimuksessa käsitellään toimintaa ja tapauksia kyberympäristössä. Kyberympäristö, tai kybertoimintaympäristö, joita tässä tutkimuksessa käytetään synonyymeina koostuvat tietoverkoista, sekä niiden käyttöön suunniteltavista laitteista ja teknologiasta. Kybertoimintaympäristöä voidaan määritellä monella eri tavalla, mutta tässä tutkimuksessa hyödynnetään Turvallisuuskomitean kyberturvallisuuden sanaston tarjoamaa määritelmää, jossa kybertoimintaympäristö ymmärretään tarkoittamaan

> *”elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet.” (Viestintävirasto, 2018)*

Samassa lähteessä kybertoimintaympäristössä tapahtuva operaatio, eli kyberoperaatio puolestaan on

> *”suunnitelmallinen ja johdettu sarja pääosin kybertoimintaympäristössä tapahtuvia toimintoja, joilla pyritään hankkimaan tietoa kohteesta tai vaikuttamaan sen toimintaan” (Viestintävirasto, 2018)*

Tässä tutkimuksessa kuitenkin kybertoimintana tai kyberoperaationa pidetään mitä tahansa kyberympäristössä tapahtuvaa tai sieltä lähtöisin olevaa toimintaa, jonka vaikutukset ulottuvat myös sen ulkopuolelle. Käsittelyn ulkopuolelle jää siis esimerkiksi ”perinteisin” menetelmin toteutettu tuhoamispyrkimyksessä toteutettu terrori-isku, jonka tarkoituksena on lamauttaa tai tuhota kybertoimintaa mahdollistavaa teknologiaa tai infrastruktuuria. Mikäli tähän tavoitteeseen

pyritään kuitenkin kyberhyökkäyksen keinoin, tai toimintaa tuetaan kyberympäristön avulla, on se mahdollista ottaa mukaan käsittelyyn.

Kuten seuraavasta luvusta tarkemmin selviää, on kyberterrorismin käsitettä yleisesti määriteltäessä esitetty vaatimus, että toiminnan tulee tapahtua kyberympäristössä, mutta sen vaikutusten tulee olla havaittavissa myös sen ulkopuolella. Fyysisen maailman seurauksiin pääseminen on kyberhyökkäyksillä vielä suhteellisen harvinaista (Agrafiotis et al. 2018) joten tässä tutkimuksessa vaatimusta kybertoiminnan fyysisille seurauksille ei ole, jotta käsiteltävä aineisto ei rajaudu liikaa.

2.2.3 Kyberuhat

Kybermaailmasta lähtöisin olevia, tai siihen kohdistuvia uhkia kutsutaan yleisesti nimellä kyberuhat. Kyberuhka voi olla luonteeltaan joko tahallinen tai tahaton, mutta tullakseen määritellyksi uhaksi tulee sen heikentää jonkin tunnistetun kohteen turvallisuutta (Limnell, Majewski & Salminen, 2015). Turvallisuuskomitean kyberturvallisuuden sanaston mukaan puolestaan kyberuhka on

> *"mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon." (Viestintävirasto 2018)*

Kyberuhkia voidaan jaotella ja luokitella eri tavoin, ja usein yhtenä tämän jaottelun kategoriana on hieman hämmentävästi kenties ollut myös kyberterrorismi. Esimerkiksi Suomen kyberturvallisuusstrategian jo jokseenkin vanhoissa taustamuistoissa kyberuhkat on jaettu viiteen luokkaan, jotka ovat:

- Kyberaktivismi
- Kyberrikollisuus
- Kybervakoilu
- Kyberterrorismi
- Kyberoperaatiot; painostus, sotaa alempi konflikti tai sotaan liittyvä kyberoperaatio

(Valtioneuvosto 2013)

Akateemisissa lähteissä puolestaan on usein suosittu kuusiluokkaista jaottelutapaa, jossa kyberuhkien tyypit ovat:

- Kybervandalismi
- Kyberrikollisuus
- Kybervakoilu
- Kyberterrorismi
- Kybersabotaasi
- Kybersota

(Lehto, 2022)

Kyberterrorismin käyttö yhtenä jaottelun kategoriana on siinä mielessä mielenkiinoista, että kuten aiemmin todettiin, puuttuu tältä uhkakategorialta yhteinen hyväksytty määritelmä ja lisäksi monen asiantuntijan käsityksen mukaan tämän kategorian ilmiöitä ei ainakaan vielä ole tapahtunut. Usein kuitenkin sitä käytetään uhkien jaottelussa yhtenä kategorioina muiden joukossa, ja etenkin ei-akateemisissa lähteissä itse kategorian sisällön määrittely on suppeahkoa tai epäselvää. Tämä tuntuu olevan jonkin verran suosittu ajatusmalli kyberterrorismin ja kyberuhkien suhteeseen liittyen; Kyberterrorismi tunnistetaan kyberuhaksi, mutta sen määrittelemisen hankaluuden vuoksi käsitettä ei avata kovinkaan paljoa, tai siihen viitataan nimenomaan vielä toteutumattomana uhkakuvana (Abdulrahman 2015).

Yksi tämän tutkimuksen tavoitteista on selvittää, miksi kyberterrorismi on tämän kaltaisessa tunnistetun, mutta määrittämättömän uhan asemassa. Se siis tunnistetaan yhdeksi kyberuhaksi muiden joukossa, jonka määrittelytapa on yksi tutkimuskohteista. Tässä tutkimuksessa viitataan myös jonkin verran muihin kyberuhkakategorioihin tai kybermaailman operaatioihin, joista puhuttaessa käytetään alla olevia Turvallisuuskomitean kyberturvallisuuden sanaston mukaisia määritelmiä.

- **Kyberrikollisuus**: Rikollisuus, joka muodostuu viestintäverkkoja ja tietojärjestelmiä hyödyntäen tehdyistä sekä niihin kohdistuvista rikoksista.
- **Informaatiovaikuttaminen:** Toiminta, jossa informaatiota tuottamalla, muokkaamalla tai sen saatavuutta rajoittamalla muutetaan kohteen käsityksiä tai toimintaa informaatio- ja mielipideympäristön kautta.
- **Palvelunestohyökkäys**: tietoverkkohyökkäys, jolla pyritään kuormittamaan ja siten lamaannuttamaan jokin palvelu tai tietojärjestelmä tai hajautettu palvelunestohyökkäys, jolloin samaan kohteeseen hyökätään yhtä aikaa useista eri lähteistä. (Viestintävirasto 2018)

Näiden lisäksi poliittisesti tai ideologisesta kybertoiminnasta puhutaan jonkin verran, ja tätä verrataan usein kyberterrorismiin. Tässä tutkimuksessa kyberaktivismi- termin sijaan käytetään sanaa haktivismi, ja sen suhdetta kyberterrorismiin esitellään tarkemmin seuraavaksi.

2.2.4 Kyberterrorismi ja haktivismi

Vuoden 2022 helmikuussa alkaneen Ukrainan sodan myötä maailmassa on todistettu jonkinnäköistä murrosta ideologisesti tai poliittisesti motivoituneessa kybertoiminnassa (Vu et al. 2023). Tätä toimintaa ovat harjoittaneet kasvavissa määrin yksilöt, ja usein vaikuttaminen on ollut globaalia (Vu et al. 2023). Hyvä esimerkki tästä on Ukrainan puolesta toimiva Ukrainan IT-armeija, joka rekrytoi ja hyödyntää vapaaehtoisia kybertoimijoita ympäri maailmaan. Toisaalta yhtä

lailla samassa konfliktissa Venäjän puolella toimivia kyberrikollisia, jotka iskuillaan tukevat tai edistivät valtion agendaa, on tunnistettu jatkuvasti enemmän. Monessa lähteessä on puhuttu ideologisesti tai poliittisesti motivoituneen kybertoiminnan räjähdysmäisestä kasvusta, tai yllättävästä esiinnoususta. Ideologinen hakkerointi, eli haktivismi on ilmiönä suhteellisen lähellä kyberterrorismia, ja eron tekeminen etenkin näiden kahden kyberuhkakategorian välille onkin hankalaa. Haastetta luonnollisesti lisää se, että kyberterrorismilta puuttuu tarkka määritelmä, joten eron tekeminen sen kanssa luonnollisesti paljon päällekkäisyyksiä omaavan ilmiön kanssa on vaikeaa.

Kyberterrorismi ja haktivismi ovat lähes kaikissa lähteissä molemmat ajateltu olevan poliittisesti tai ideologisesti motivoitunutta kybertoimintaa, merkittävimpien erojen ollessa tyypillisesti operaatioiden luonteessa, toteutustavassa, tai siinä minkälaisin konkreettisin keinoin tavoitteiseen pyritään. Kyberterrorismin on tyypillisesti ajateltu olevan ”vakavampi” muoto haktivismista, eli vaikutuksiltaan merkittävää ja toteutustavaltaan todellista vahinkoa aiheuttavaa (Denning 2000, Kenney 2015). Haktivismi puolestaan vaikuttaa aiemmin olleen mielletty lähinnä matalan tason aktivismiksi kybermaailmassa, jolla ei useinkaan ole merkittäviä vaikutuksia (Denning, 2001). Ukrainan sodan myötä kiihtyneen ideologisen kybertoiminnan kasvun myötä on kuitenkin jouduttu toteamaan, että haktivismi tai sellaiseksi miellettävät teot voivat olla vaikutukseltaan merkittäviä, ja ilmiön räjähdysmäinen kasvu on pakottanut lähestymään ilmiötä uudenlaisella vakavuudella. On olemassa vaihtelevia arvioita siitä, kuinka merkittävää tämä haktivismitoiminta on sodan kulun kannalta ollut, mutta selvää on se, että aktiivisuus tämänkaltaisessa toiminnassa on kasvanut (Vu et al. 2023).

Tämä tutkimus ei sinänsä käsittele haktivismia, mutta koska se omaa huomattavan paljon samaa kyberterrorismin kanssa, on näiden kahden ilmiön suhdetta käsiteltävä joka tapauksessa. Koska tämä tutkimus pyrkii kuitenkin lähestymään kyberterrorismia suhteellisen avoimesta lähtökohdasta, ei haktivismiakaan johon kyberterrorismia myöhemmin verrataan määritellä etukäteen kovinkaan tarkasti. Tässäkin tapauksessa soveltuu käytettäväksi Turvallisuuskomitean sanastosta löytyvä kuvaus haktivismista:

> *” yksittäisen henkilön tai ryhmän kybertoimintaympäristössä harjoittama tavoitteellinen tai aatteellinen toiminta”* (Viestintävirasto 2018).

Tämä vastaa myös useimpia akateemisissa lähteissä käytettäviä määritelmiä, joissa toistuvia teemoja ovat edellisen tavoin vaatimukset poliittisesta tai ideologisesta motivaatiosta, toimijan ei-valtiollisuudesta ja toiminnan tapahtumisesta kyberympäristössä (Ussath et al 2016). Siihen miten hyvin tässä tutkimuksessa valittu lähestymistapa onnistuu erottamaan nämä kaksi ilmiötä toisistaan, palataan luvussa 6, jossa esitellään työn tuloksista tehtäviä johtopäätöksiä.

2.2.5 Hakkerijengit

Tässä tutkimuksessa viitataan jonkin verran kybermaailman rikosten toteuttajiin, eli hakkereihin tai hakkeriryhmiin. Hakkereiden toiminta ja ryhmäytyminen on

jo itsessään mielenkiintoinen ilmiö, jota on tutkittu jo pidemmän aikaa (Perkins, Oullet, Howell & Maimon 2023). Tämän tutkimuksen tarkoituksena ei ole analysoida sitä, miten eri kybermaailman terroristisesti motivoituneet uhkatoimijat löytävät toisensa tai muodostavat kollektiiveja, vaikka esimerkiksi juuri kyberterrorismiksi miellettävään toimintaan liittyen tämänkaltainen selvitys oli mielenkiintoinen. Tämän tutkimuksen kontekstissa riittää todeta, että kybermaailmassa yleisesti samanmieliset toimijat löytävät toisensa, ja yhteisten intressien myötä muodostetaan löyhästi toisiinsa sitoutuneita ryhmiä, jotka muodostavat ja pyrkivät toteuttamaan yhteisiä tavoitteita (Perkins et al. 2023). Tämänkaltaista ryhmää tai ryhmittymää kutsutaan nimellä hakkerijengi.

Kybermaailman uhkatoimijoita on myös usein jaettu valtiollisiin ja ei-valtiollisiin toimijoihin (Chen, Desmet & Huygens 2014). Tämän tutkimuksen myöhemmissä luvuissa palataan jonkin verran tämän jaottelun haasteisiin kyberterrorismia tarkasteltaessa, sillä se on oleellinen osa ilmiöiden tarkastelua ja arviointia. Kuitenkin tutkimuksessa yleisesti puhuttaessa hakkerijengeistä, ei tätä jaottelua erikseen tehdä, eli hakkerijengeistä puhuttaessa kyse voi olla sekä tiedossa olevasta valtiollisesti tuetusta ryhmittymästä tai aiemmin kuvaillusta löyhästi toisiinsa sitoutuneista samat intressit jakavista rikollisista. Kuten todettua, tämä jaottelu ei potentiaalisia kyberterroristisia tapahtumia arvioitaessa kuitenkaan ole merkityksetön, ja sekä jaottelun järkevyyteen että valtiollisen tunnistamisen erottamiseen ei-valtiollisesta palataan sekä tutkielman luvuissa 5 että 6.

2.3 Tutkimuskysymys ja aiheen rajaus

Kyberterrorismi on siis monella tavalla haastava ilmiö. Se on tunnistettu kehittyväksi ja kasvavaksi kyberuhaksi, mutta siltä puuttuu tyydyttävä ja yhteisesti hyväksytty määritelmä. Haastetta luo etenkin se seikka, että monen käytettävän määrittelytavan mukaan kyberterrorismia ei sinänsä ole olemassa, eli määritelmän täyttämästä toiminnasta ei ole käytännön esimerkkejä. Tämän työn tarkoituksena on tarkastella, löytyykö tämän hetken kirjallisuudesta määritelmää, jonka avulla kyberterrorismi voidaan:

a) Todeta olemassa olevaksi toiminnaksi
b) Erottaa tyydyttävästi muista kyberuhista

Tutkimuksen tavoitteena ei kuitenkaan ole pyrkiä mittaamaan tai arvioimaan kuinka paljon kyberterrorismia ilmenee, tai kuinka merkittävä sen muodostama uhka on muihin kyberuhkiin verrattuna. Tarkoituksena on sen sijaan selvittää, onko käsitettä mahdollista määritellä tavalla, joka mahdollistaa lähestyminen tunnistettavana ja muista eroteltavan uhkana. Tutkimuskysymys, johon pyritään vastaamaan on:

Onko kyberterrorismi ilmiö, joka voidaan tyydyttävästi määritellä erottumaan muista kyberuhista, ja jonka voidaan havaita olevan todellisuudessa tapahtuvaa toimintaa?

Jotta tähän kysymykseen pystyttäisiin vastaamaan, on tässä tutkimuksessa valittava jokin kilpailevista tavoista määritellä kyberterrorismi, jotta tätä määrittelytapaa voidaan sitten verrata todellisuuteen. Tästä syystä varsinaista tutkimuskysymystä tukemaan muodostettiin alakysymyksiä, joiden tavoitteena on selvittää, miten ilmiötä on pyritty määrittelemään, ja mikä määrittelytapa soveltuu parhaiten tässä tutkimuksessa käytettäväksi. Alakysymykset ovat muotoiltu seuraavasti:

a) **Miten kyberterrorismia on pyritty määrittelemään?**
b) **Mitkä ovat olleet määrittelyn haasteet?**
c) **Mikä on tämän tutkimuksen kannalta paras tapa määritellä kyberterrorismi?**

Luvussa 4 pyritään vastaamaan näihin alakysymyksiin, tarkastelemalla miten ilmiöön liittyvä akateeminen työ on kehittynyt ja mitä haasteita määrittelemisessä on tunnistettu. Luvun lopussa esitellään tähän työhön valittu tapa määritellä kyberterrorismia, jonka soveltuvuutta testataan vertaamalla määritelmää käytännön tapauksiin viimeisen vuoden ajalta, jotka intuitiivisesti saattaisivat vaikuttaa kyberterrorismilta. Tällä prosessilla pyritään siis vastamaan varsinaiseen tutkimuskysymykseen. Aineiston keräämistä ja tutkimusmenetelmää kuvataan tarkemmin seuraavassa luvussa 3. Tutkimus rajataan käsittelemään kyberterrorismia lähestymällä sitä vain havaittujen tapausten, eli tyypillisesti kyberhyökkäysten tai hyökkäyskampanjoiden kautta. Rajauksen ulkopuolelle siis jää esimerkiksi terroristien kyberympäristön hyödyntäminen kommunikointiin ja rekrytointiin. Edellä mainitut ovat tunnistettuja tapoja, joilla terroristiset toimijat hyödyntävät kyberympäristöä (ks. Kenney 2015), mutta niiden analysointi tämän tutkimuksen kontekstissa ei ole mahdollista. Luotettavaa ja ajankohtaista tietoa terrorijärjestöjen sisäisestä tai ulkoisesta viestinnästä ei julkisista lähteistä löydy tarpeeksi, ja viestinnän sisällön analysointi ei muutenkaan toisi merkittävää lisää tämän tutkimuksen tutkimuskysymyksiin vastatessa. Vaikkakin siis kybertoiminnanmuodot kuin suorat hyökkäykset tai niiden uhka voidaan tunnistaa kyberterrorismiksi, tässä työssä käsitellään nimenomaan kyberhyökkäyksiä ja niiden määrittelemistä kyberterrorismiksi.

3 TUTKIMUSAINEISTO JA -MENETELMÄ

Tämän työn tarkoitus on tarkastella, voidaanko lähihistoriasta löytää tapauksia, jotka vastaavat edellisessä luvussa esitellyn Plotnekin ja Slayn määritelmää kyberterrorismista, eli onko kyberterrorismi siis todellinen ja havaittavissa oleva ilmiö. Tavoitteena oli myös selvittää mitkä ovat näitä tapauksia kuvaavia tekijöitä, sekä onko havaittavissa että jokin komponentti osoittautuu muita karsivammaksi kyberterrorismia määriteltäessä. Aineistona käytetään avoimista lähteistä saatavilla olevia tietoja viimeisen vuoden aikana tapahtuneista kyberhyökkäyksistä, eikä tapauksia rajattu niiden maantieteellisen sijainnin mukaan. Tavoitteena on lähestyä mahdollisimman laajaa kirjoa erilaisia kybertapahtumia, ja pyrkiä selvittämään voidaanko niitä määritellä kyberterrorismiksi Plotnekin ja Slayn mallia käyttäen. Kuten aiemmin todettua tavoitteena ei ole niinkään selvittää kuinka paljon kyberterrorismia tapahtuu, vaan tarkastella yksittäisiä tapauksia tarkemmin, jotta määritelmää saadaan paremmin testattua. Aineiston keräys rajattiin tapahtumiin, joista on saatavilla tarpeeksi luotettavaa tietoa eri lähteistä, ja jotka ovat tapahtuneet vuoden 2022 alun jälkeen. Suhteellisen lyhyt aikaikkuna valittiin, sillä näin aineistoa saatiin tehokkaasti rajattua, ja kyberympäristön ollessa toimintakenttänä varsin nopeasti muuttuva ja uudistuva ei vanhempia tapauksia haluttu ottaa mukaan käsittelyyn.

Käytännössä aineiston keräys tapahtui eri medialähteitä, ja tietoturvatoimijoiden julkaisuja seuraamalla. Näistä etsittiin kuvauksia tapahtuneista kyberhyökkäyksistä, tai iskukampanjoista, jotka ensisilmäyksen perusteella voisivat vaikuttaa sopivan kyberterrorismin määritelmään. Kun seurannasta nousi esiin mielenkiintoinen tapaus, selvitettiin ensin, kuinka paljon tietoa on saatavilla ja vaikuttaako sen analysointi kyberterrorismin taksonomian kautta järkevältä. Tässä työssä sanalla tapaus, viitataan kybermaailman tapahtumaan, joka voi olla luonteeltaan yksittäinen kyberhyökkäys tai pidempi useita päiviä jatkunut hyökkäyskampanja, mikäli sen yhteydessä oli löydettävissä jokin tunniste, jonka avulla tapahtumat voitiin liittää toisiinsa. Yleensä tämä tunniste oli esimerkiksi hakkeriryhmien julkaisussaan käyttämä hashtag, eli #-kuvio, jolla samaan kampanjaan kuuluvat hyökkäykset voitiin yhdistää toisiinsa. Käytännössä tässä vaiheessa arvioitiin nopeasti, ilman syvempää analyysiä onko mahdollista, että

tapaus olisi miellettäväksi kyberterrorismiksi lähemmän tarkastelun myötä. Monen tapauksen kohdalla siihen liittyvää uutisointia ja julkaisuja seurattiin pidemmän aikaa, sillä suurimassa osasta tapauksia lisää luotettavaa tietoa tuli usein vasta kuukausien kuluttua itse tapahtumasta. Tämän työvaiheen tarkoituksena ei ollut analysoida jokaista seurannasta noussutta tapausta Plotnekin ja Slayn taksonomiaa hyödyntäen, vaan tavoitteena oli kerätä mahdollisimman kirjava ja rikas aineisto, josta voidaan havaita sekä kyberterrorismin määritelmään sopivia tapauksia, että määritelmän ulkopuolelle jääviä. Tämä oli tavoitteena siksi, että teorian testaamisen kannalta todettiin hyödylliseksi, mikäli aineistoon kuuluu sekä tapauksia, jotka vastaavat määritelmää, että sellaisia, jotka jäävät sen ulkopuolelle. Näin saadaan parempi käsitys siitä mitkä tekijät vaikuttavat siihen tuleeko tapaus määritellyksi kyberterrorismiksi taksonomian kautta.

Kun seurannasta löydettiin esitarkastuksen läpäissyt tapaus, siitä kerättiin mahdollisimman paljon tietoa eri lähteistä hyödyntäen usein hyökkääjien omia somekanavia, joilla iskuista tiedotettiin. Tarkoituksena oli kerätä mahdollisimman paljon tietoa esivalinnan läpäisseistä tapauksista, jotta niiden arviointi työn seuraavassa vaiheessa oli hedelmällisempää. Monen tapauksen kohdalla arviointi jätettiin kesken ja yleisin syy tähän oli, että kyseistä tapauksesta oli saatavilla liian vähän luotettavaksi todetuista lähteistä peräisin olevaa tietoa. Lähempään tarkasteluun valikoitui lopulta yhteensä 15 tapausta, ja näitä lähestyttiin tarkemmin Plotnekin ja Slayn kyberterrorismin taksonomiaa hyödyntäen.

Tutkimusmenetelmäksi valikoitui varsin luonnollisesti teorialähtöinen sisällönanalyysi. Teorialähtöinen sisällönanalyysi on sisällönanalyysin muoto, jossa tavoitteena on tutkia kerättyä aineistoa ennalta valittua teoriaa tai mallia hyödyntäen. Teorialähtöistä sisällönanalyysiä käytetään tutkimuksissa, joissa on tavoitteena esimerkiksi testata kehitettyä teoriaa, tai sen soveltuvuutta tiettyyn ympäristöön. (Jouni & Sarajärvi 2018). Menetelmän valinta tähän tutkimukseen oli varsin luontevaa, sillä tutkimuksen tavoitteena on selvittää miten Plotnekin ja Slayn mallin mukaista kyberterrorismia ilmenee.

Tässä työssä siis verrattiin Plotnekin ja Slayn määritelmää kyberterrorismista aineiston tapauksiin. Tavoitteena ei ollut arvioida sitä kuinka hyvä, tai käyttökelpoinen malli on esimerkiksi kyberterrorismia koskevan lainsäädännön muokkaamisen suhteen, vaan ylipäätään selvittää minkälaisia tapauksia malli määrittelee kyberterrorismiksi. Kuten jo aiemmin todettua, tavoitteena ei myöskään ollut mitata tai arvioida sitä kuinka paljon kyberterrorismia tapahtuu, tai onko sen ilmentymisessä maantieteellisiä eroja. Päätavoite oli pyrkiä selvittämään, onko valittu määrittelytapa käytännöllinen kyberterrorismin erottamiseen muista uhista, ja voidaanko määritelmään sopivaa toimintaa edes ylipäätään tunnistaa aineistosta.

Käytännössä työ eteni tarkastelemalla ensin jokaista tapausta yksittäin kaiken saatavilla olevan tiedon avulla ja vertaamaan sen osatekijöitä Plotnekin ja Slayn mallin komponentteihin. Saatavilla olevan tiedon perusteella pyrittiin siis selvittämään tapaukseen liittyvä toimija, motiivi, aikomus, keinot, vaikutus sekä kohde. Joissain tapauksissa näiden määritteleminen perustui suhteellisen paljon tulkinnanvaraisuuteen ja jossain tapauksissa komponentit olivat helpommin

havaittavissa. Tuloksia esitellessä selvitetään myös se, kuinka tulkinnanvaraisena komponentin hyväksymistä määritelmään sopivaksi pidetään.

Komponenttien analysoinnin perusteella tapausten joko todettiin vastaavan määritelmää kyberterrorismista, tai jäävän tämän ulkopuolelle. Seuraavaksi etsittiin yhdistäviä tekijöitä niistä tapauksista, jotka jäivät määritelmän ulkopuolelle sekä yhdenmukaisuuksia niiden tapauksien välillä, jotka sopivat määritelmään. Analyysin tulokset ovat tarkemmin esiteltynä seuraavassa luvussa, ja luvussa 6 tehdään tarkempia johtopäätöksiä siitä mitä tämän tutkimuksen perusteella voidaan sanoa käytettävästä kyberterrorismin määritelmästä.

4 MITEN KYBERTERRORISMIA ON MÄÄRITELTY

Tässä luvussa esitellään kyberterrorismin käsitettä yleisesti, sekä sen määrittelyyn liittyviä haasteita. Luku toimii sekä tutkielman kirjallisuuskatsauksena, että tutkimusongelmaa edelleen havainnollistavana aiheen esittelynä. Luvun tarkoituksena on esitellä sekä miten määrittelyä on tehty, mutta myös korostaa siihen liittyviä haasteita.

Luvun lopussa esitellään laajemmin kirjallisuuskatsauksessa löydetty ajallisesti uusin, ja luonteeltaan tähän mennessä kattavin tapa jäsentää kyberterrorismin ilmiötä. Tässä taksonomisessa lähestymisessä hyödynnetään aiemman tutkimuksen tuottamaa ymmärrystä, kun ilmiötä pilkotaan pienempiin kategorioihin, joiden avulla se pyritään määrittelemään entistä tarkemmin ja rajatummin. Taksonomia esitellään tässä laajasti, sillä se edustaa tutkijan käsityksen mukaan uusinta ja parhaiten aiempaa kokoavana ja hyödyntävänä tapana jäsentää kyberterrorismin ilmiötä, ilman että oleellisia toiminnan muotoja jää tarkastelun ulkopuolelle.

4.1 Kyberterrorismin määrittelyä

4.1.1 Määrittelyn lähtökohtia

Vaikka miellettävissä varsin moderniksi, ja monessa tapauksessa jopa vasta tulevaisuuden ilmiöksi, kyberterrorismi on ollut akateemisessa keskustelussa käytettävä termi jo vuosikymmenten ajan. Ensimmäisiä merkittäviä kyberterrorismiin liittyviä julkaisuja löytyy jo viime vuosisadan puolelta ja ensimmäiseksi termin käyttäjäksi onkin usein mainittu Barry Collin jo 1980-luvulla, jolloin hän käsitti termin olevan yksinkertaisesti terrorismin ja tietoverkkojen yhdistymistä (Denning 2001, Abdulrahman 2015). Ennen digitalisaation vallankumousta ja tietoverkkojen yleistymistä ei kyberympäristössä tapahtuvasta terrorismista luonnollisestikaan puhuttu juurikaan tätä laajemmin, tai sen potentiaalia voitu edes teoriassa ymmärtää. Tästä on tultu reilusti eteenpäin, ja vuosien saatossa kymmenet akateemikot ovat pyrkineet muodostamaan käsitteelle tyydyttävää määritelmää.

Määritelmää on yritetty rakentaa pohjaten etenkin motivaatioon ja toiminnan seurauksiin (Kenney, 2015). Seuraavissa alaluvuissa tarkastellaan, miten käsitteen määrittelyssä on edetty vuosituhannen vaihteesta eteenpäin.

Eräs lainatuimmista eniten huomiota herättäneistä määritelmistä on jo vuodelta 2001. Dorothy Denning määrittelee kyberterrorismin koostuvan laittomista kybertoimista, joiden tavoitteena on tuottaa pelkoa ja edistää poliittista agendaa. Denningin mukaan kyberterrorismiin kuuluu siis terroristisen motivaation yhdistäminen rikolliseen kybertoimintaan. Määritelmään kuuluu myös ajatus siitä, että vaikka terroristi toimisikin kyberympäristössä, täytyy toiminnalla olla myös kineettisiä tosimaailman seurauksia (Denning, 2001). Tarkemmin, toiminnan tulee johtaa väkivaltaan, tai henkilöiden loukkaantumiseen. Denningin määritelmää on vuosien saatossa pidetty yleisesti melko hyvänä ja sitä lainattu hyvinkin laajasti (Kenney 2015, Plotnik & Slay 2021).

Kuitenkin toisin kuin kirjoittaja kenties pari vuosikymmentä sitten arveli, määritelmän mukaisesta kyberterrorismista ei ole saatu esimerkkejä, eikä siihen sopivaa toimintaa siten ole ollut olemassa (Denning 2007). Kybertoiminnan kineettiset seuraukset ovat yleisestikin olleet suhteellisen harvinaisia oli puhe sitten valtiollisesta vaikuttamisesta tai kyberrikollisuudesta (Agrafiotis et al. 2018). Ei sikäli ole ihme, että esimerkkejä kyberterrori-iskusta, joka olisi johtanut loukkaantumisiin tai fyysisiin vaurioihin ei ole olemassa.

Denningin määritelmä on kuitenkin ollut hyödyllinen sen tehdessä selvän eron kyberterrorismin ja muunlaisen rikollisen kybertoiminnan välillä. Etenkin sen erottaminen haktivismista, eli poliittisesti motivoituneesta hakkeritoiminnasta on selkeyttänyt keskustelua erotellen nämä kaksi ilmiöitä toisistaan. Haktivismi poikkeaa Denningin mukaan kyberterrorismista siten, että vaikka molemmissa tapauksissa toimijalla saattaisikin olla poliittinen tai ideologinen motivaatio, haktivisti ei pyri toiminnallaan tuottamaan vahinkoa vaan motivaatio on enemmän huomion saanti ideologialle (Denning, 2001).

Denningin muodostama määritelmä oli luontihetkellä selkeästi tulevaisuuten katsova, ja hän myös toteaa tavoitteisekseen tarkastella miten terroristit potentiaalisesti tulevat tai voivat hyödyntää kyberympäristöä toiminnassaan. Ajatukset kybertoiminnan vähäisemmästä riskistä, pienemmästä kynnyksestä ja taloudellisista kustannuksista ovat vielä nykypäivänäkin pitkälti nähty syiksi, joiden vuoksi terroristit kyberympäristöä hyödyntävät (Liang, 2017, Chaturvedi et al. 2014). Eli vaikka luodun määritelmän voisi tulkita olevan liian poissulkeva on Denningin työllä silti ollut selkeästi arvoa sekä ensimmäisenä suunnannäyttäjänä ilmiön pohdintaan ja pohjaymmärryksen luojana.

4.1.2 Kohti ymmärrystä

Vuosituhannen ja digitalisaation edetessä akateeminen huomio terroristien kyberympäristön hyödyntämiseen jatkui ja kasvoi. Päällimmäisenä haasteena vaikuttaa kyberterrorismin määrittelyä tehneille olleen sen Denningin aloittaman tien mukaisesti sen erottaminen muista kyberuhista (Lewis 2002). Terroristinen motivaatio eli pelon tai kauhun herättäminen on ollut oleellinen osa lähes kaikkia määritelmiä, ja monessa toistetaan Denningin esittämä vaatimus, että ollakseen

kyberterrorismia, tulee kybertoiminnan johtaa todellisen maailman seurauksiin (Weimann, 2004, Czerpak 2005). Kaikissa ei kuitenkaan näin tehdä, ja myös laajempia määritelmiä on kehitetty (Mantel 2009). Näissä mikä tahansa terroristisesti motivoitunut kybertoiminta voidaan periaatteessa mieltää kyberterrorismiksi, oli se sitten viestinvaihtoa terroristiryhmän sisällä tai varainhankintaa kyberrikollisuuden keinoin. Luonnollisesti tämän kaltaista määrittelyä haastaa liian suppean määrittelyn vastakohta. Jos käytännössä kaikki verkkotoiminta voidaan mieltää kyberterrorismiksi, jos siihen vain voidaan jollain tasolla liittää terroristinen motivaatio, ei määritelmästä juuri ole hyötyä sen sisältäen niin laajan kirjon erilaista toimintaa (Plotnik & Slay 2021). Toiminnan akateeminen tarkastelu tämänkaltaisen määritelmän kautta on vähintäänkin hankalaa, sillä huomio ohjautuu niin laajalle, että toiminnan eri muotojen tunnistaminen ja erottelu vie huomion itsen ilmiön käsittelyn sijaan.

Selkeästi toistuvia tekijöitä eri tavoissa jäsentää kyberterrorismin ilmiötä on pelon herättämisen ja ideologisen motivaation lisäksi luonnollisesti toiminnan tapahtuminen kyberympäristössä. Kuten aiemmin todettua, usein todetaan, että kyberterrorismi ei ole vielä uhkana realisoitunut, sillä tosimaailman esimerkkejä kyberterrori-iskuista, joilla olisi ollut tosimaailman seurauksia ei ole. 2010-luvulle tultaessa alettiin selvästi tunnistaa määritelmän ongelmallisuus, etenkin kun kasvavaksi koettu terrorismin uhka lisäsi keskustelua kyberympäristön hyödyntämisestä terroristisessa toiminnassa (Kenney 2015).

Ongelmallisuuden julkisessa keskustelussa ja akateemisen käsitteen erossa toi esille myös Michael Kenney vuonna 2015 artikkelissaan *Cyber-Terrorism in a Post-Stuxnet World.* Kenneyn mukaan keskustelu kyberterrorismista ja sen tuottamista uhkakuvista on karannut kauas todellisuudesta, ja kyberterrorismin uhkaa korostetaan liikaa etenkin Yhdysvaltojen viestinnässä. Kenneyn mukaan käsite on usein väärin ymmärretty, ja akateemisessakin ympäristössä keskenään kilpailevat käsitykset tekevät ilmiön tulkinnasta sekavaa. Kenney pyrkii selkiyttämään mitä kyberterrorismi todellisuudessa on, ja miten se eroaa muista samankaltaisista mutta erillisistä ilmiöistä, kuten aiemmin mainitusta haktivistmista ja valtiollisista kyberhyökkäyksistä. Tuloksena muodostuu taksonomia, jossa kyberterrorismi käsitetään koostuvan neljästä elementistä, joiden kaikkien tulee olla havaittavissa, jotta toiminta voidaan määrittää kyberterrorismiksi:

1) Tietokonelähtöisyys (engl. computer generation) – Toiminnan on tapahduttava ja sen on myös kohdistuttava digitaalisiin järjestelmiin tai tietoverkkoihin.
2) Poliittinen motivaatio (engl. political motivation) – Toiminnan on oltava poliittisesti tai ideologisesti motivoitunutta, eikä tavoitteena voi olla esimerkiksi taloudellinen hyöty.
3) Fyysinen väkivalta (engl. physical violence) – Jotta toiminta on kyberterrorismia, on sen johdettava kybermaailman ulkopuolella tapahtuvaan ihmisiin tai infrastruktuuriin kohdistuvaan vahinkoon.
4) Psykologinen pakottaminen (engl. psychological coercion) – Toiminnan lopullisen tavoitteen on oltava tarkoituksellinen pelon herättäminen - terrorismin on luotava terroria. (Kenney 2015).

Kenneyn määritelmä yhdistelee ja selkiyttää aiemmin sekavaa tutkimuskenttää aiheeseen liittyen. Se nojaa pitkälti Denningin alkuperäiseen määritelmään, pitäen mukana fyysisen väkivallan vaatimuksen, mutta ottaa mukaan uudemman ajatuksen psykologisesta pakottamisesta, tai tavoitteesta saada kohde toimimaan pelon avulla halutulla tavalla. Tämä toimintaan pakottamisen intressi on läsnä monessa modernimmassa tavassa määritellä kyberterrorismia ja näkyy myös esimerkiksi tässä tutkimuksessa käytettävässä terroristisen toiminnan määrittelyssä. Terroristien tavoitteiden on nähty kehittyneen siis kauhun ja pelon herättämisestä sekä huomion hakemisesta omalle agendalle, kyberhyökkäyksen hyödyntämiseen informaatiovaikuttamisen työkaluna tavoitteena saada kohde käyttäytymään toivotulla tavalla. Kenneyn mukaan terrorismiin kuuluu oleellisesti toiminnan saaman huomion johtaminen siitä kuulevan yleisön pelkoon ja tämän on toteuduttava myös kyberterrorismissa. (Kenney 2015).

Mielenkiintoisesti Kenney tulee Denningin kanssa samaan tulokseen, jossa kyberterrorismia ei todellisuudessa ole vielä tapahtunut. Tämä huolimatta siitä, että artikkelissa käsitellään tunnistettujen terrorijärjestöjen kuten Al-Qaidan toteuttamia kyberhyökkäyksiä. Tämäkään toiminta ei täytä kyberterrorismin määritelmää, sillä sen vaikutukset ovat usein jääneet häirinnän tasolle, eikä väkivaltaisia seurauksia kybermaailman ulkopuolelle ole tapahtunut (Kenney 2015). Kenney toteaa monen akateemikon kanssa yhteisen mielipiteen, että lähitulevaisuudessa varsinainen kyberterrori-isku on epätodennäköinen, ja terroristisen toimijoiden kyberympäristön hyödyntäminen keskittyy perinteisten operaatioiden tukemiseen tai niiden valmisteluun. Kyberympäristö näyttäytyy terrorismia mahdollistavana, ja operaatioita tukevana kenttänä, mutta puhtaasta kyberterrorismista ei voida vielä puhua. Määritelmän poissulkeva luonne kuitenkin jälleen voidaan tulkita sen käytettävyyttä rajoittavaksi, sillä akateemisen maailman ulkopuolella lainsäädäntöä tai varautumista on vaikea kohdistaa ilmiöön, jota ei todellisuudessa, tai ainakaan vielä, ole olemassa.

4.2 Moderni taksonomia

Kenneyn tavoin taksonomian kautta kyberterrorismin määritelmään on pyritty myös muiden toimesta, ja sitä voidaan pitää lupaavana tapana saavuttaa paremmin jäsennelty ymmärrys ilmiöstä. Merkittävän työn tämä eteen ovat tehneet Jordan Plotnek ja Jill Slay vuoden 2021 artikkelissaan *Cyber terrorism: A homogenized taxonomy and definition.* Työssään he ovat koonneet laajasti aiemmin kehiteltyjä tapoja määritellä kyberterrorismia, ja pyrkineet yhtäläisyyksiä ja toistuvia sanoja etsimällä yhdistelemään vuosien saatossa kasvaneen ymmärryksen yhdeksi kattavaksi mutta tarkaksi taksonomiseksi määrittelyksi. Tuloksena kehitettyä taksonomiaa voidaan pitää edistyneempänä kuin aiempia yrityksiä (Kenney 2015, mutta ks. myös myös Al Mazari et al 2015) sen pystyessä sekä olemaan tarpeeksi tarkka sulkeakseen pois rinnakkaisilmiöt, mutta tarpeeksi laaja jotta sitä voidaan hyödyntää tarkastelemaan kyberterrorismia kokonaisuudessaan. Olemassa olevia jäsentelyjä hyödyntämällä, sekä ammentaen jo saavutetusta ymmärryksestä

ilmiön suhteen he kehittivät tavan määrittää kyberterrorismia perustuen toimijaan, motiiviin, aikomukseen, keinoihin, vaikutukseen ja kohteeseen. (Plotnek & Slay 2021)

Pyrkiessään määrittämään ensin minkälainen on luonteeltaan kyberterroristinen toimija, Plotnek ja Slay tulivat tulokseen, että aiemmassa tutkimuksessa toimijaa on pyritty määrittelemään kolmella eri tavalla. Toimija on joko ollut määritetty suoraan terroristiksi, perustuen johonkin olemassa olevaan perinteisen terrorismin määritelmään, yleisesti ei-valtiolliseksi toimijaksi tai yksinkertaisesti salassa tai luvatta (eng. clandestine) toimivaksi tahoksi. Heidän mukaansa perinteisestä terrorismin määrittelystä riippuvainen tapa ei ole kannattava, sillä kyberterrorismi voi sisältää toimintaa, joka ei välttämättä sisälly siitä käytettäviin määritelmiin, ja salassa tai luvatta toimimisen kautta määrittely jäisi liian laajaksi rajaamatta käytännössä mitään toimijaa pois. Lopputulemana todetaan, että paras tapa saada laaja, mutta käyttökelpoinen määritelmä kyberterrorismiin liittyvälle toimijalle on sen käsittäminen ei-valtiolliseksi toimijaksi. (Plotnek & Slay 2021).

Seuraava kategoria, jonka kautta ilmiötä pyritään selkeyttämään, on motiivi. Motiivi on aiempaan tutkimukseen perustuen ollut joko ideologinen, sosiaalinen, taloudellinen ja ennalta suunniteltu. Ideologinen motivaatio on tässäkin työssä jo monesti vastaan tullut taustalla vaikuttava ideologia tai poliittinen pyrkimys. Sosiaalisen motivaation käsitettiin tarkoittavan rodullista tai tiettyyn sosiaaliseen ryhmään liittyvää motivaatiota. Taloudellinen motivaatio päädyttiin jättämään jäsentelyn ulkopuolelle sen ollessa mainittuna vain yhdessä aiemmassa tutkimuksessa, ja vaikka sen todetaan olevan mahdollinen vaikuttaja etenkin tulevaisuuden kyberterroristisen toiminnan taustalla, päädyttiin se vähäisen ilmenevyyden takia jättämään pois jäsentelystä. Yhdistelemällä ajatusmallit ideologisesta ja sosiaalisesta motivaatiosta ja liittämällä niihin vaatimus toiminnan olemisesta ennalta suunniteltua ja harkittua saadaan katettua laaja kirjo erilaisia kyberterroristisen toiminnan mahdollisuuksia kuitenkin säilyttäen rajaukset muihin lieve ilmiöihin. (Plotnek & Slay 2021).

Kolmas taksonomian kategoria on toimijan aikomus. Aikomus eroaa motiivista sen tarkoittaessa keinoa, jolla motiivi pyritään saavuttamaan. Aikomusta oli aiemmassa tutkimuksessa kuvattu yhteensä yhdeksään eri kategoriaan jaetusti, mutta samankaltaisuuksia poistamalla tai liian suppeat tai laveat määritelmät ohittamalla aikomukseksi voidaan tiivistäen todeta olevan joko pelon herättäminen, tai jonkin tai jonkun toimintaan pakottaminen. Käytännössä toiminnan ollakseen kyberterrorismiksi määriteltävissä on keinona motiivin toteuttamisen siis oltava yleisesti pelon herättäminen tai ulkopuolisen toimijan pakottaminen haluttuun toimintaan. (Plotnek & Slay 2021).

Seuraava kategoria on toiminnan keinot. Keinoilla tarkoitetaan käytännön toimia, joilla aiottuun tavoitteeseen pyritään, ja luonnollisesti keinovalikoima on suhteellisen laaja. Aiemmasta tutkimuksesta tunnistettiin yhteensä 17 eriteltyä kyberterrorismissa hyödynnettävää keinoa, mutta yhdistävänä tekijänä näissä kaikissa oli varsin luonnollisesti toiminnan tapahtuminen kyberympäristössä. Aiemmista tässä tekstissä esitellyistä keinoista poiketen, myös toiminnalla

uhkaaminen tunnistettiin osaksi kyberterroristin keinovalikoimaan, joten keinot voidaankin tiivistää kyberympäristössä tapahtuvaan hyökkäykseen tai sen uhkaan. (Plotnek & Slay 2021).

Aiempaa tutkimusta on kenties eniten haastanut ristiriita liittyen seuraavan kategorian sisältöön, eli toiminnan vaikutuksiin. Vaihtelevat vaatimukset kyberympäristön ulkopuolelle laajentuvista vaikutuksista ovat vaihdelleet, usein sisältäen termejä kuten väkivalta tai palveluhäiriö. Yhteisenä vaatimuksena on kuitenkin yleisesti pidetty sitä, että kyberterrorismilla on jonkinlainen havaittavissa oleva vaikutus myös kyberympäristön ulkopuolella, oli se sitten vaikutus väestöön, palvelujen saatavuuteen tai infrastruktuurin tai henkilöiden vahingoittumiseen. Toiminnan vaikutusten ollessa kenties tähän mennessä suurimman haasteen aiheuttanut yksittäinen tekijä Plotnek ja Slay päätyvät jäsentelyssään sen varsin laajaan määrittelyyn. Taksonomiassa kyberterrorismin vaikutusten todetaan olevan kybermaailman ulkopuolella tapahtuvia seurauksia, jotka voivat luonteeltaan olla sosiaalisia, psykologisia, sosiaalisia, poliittisia, fyysisiä, taloudellisia tai ekologisia. (Plotnek & Slay 2021).

Viimeinen kategoria on kyberterrorismin toiminnan kohde. Tähänkin liittyen aiemmassa tutkimuksessa oli listattu varsin laajasti eri potentiaalisia kohteita, ja yli kahdestakymmenestä havaitusta kohteesta päädyttiin tiivistämään ne kolmeen. Kohteen määrittelyssä poikkeuksellinen haaste on myös, että toiminnalla voi samaan aikaan olla useita tai päällekkäisiä kohteita, ja kohteen roolia toiminnan määrittelyyn ei myöskään koeta yhtä tärkeänä kuin muita kategorioita. Jäsentelyssä päädyttiin siis tiivistykseen, jossa kyberterrorismin kohteita ovat yksinkertaisesti, siviilit, valtiohallinto tai sen osa sekä ei-valtiollisen organisaatiot. Kyseessä on jälleen melko laaja tapa jäsentää ilmiötä, mutta kun useat laajasti määritellyt kategoriat yhdistellään, saadaan suhteellisen kuvaava ja monia uniikkeja aspekteja huomioon ottava tapa jäsentää ilmiötä. (Plotnek & Slay 2021).

Koottuna Plotnekin ja Slayn määrittelyn mukaisesti kyberterrorismi koostuu seuraavista osatekijöistä:

- Toimija: Ei-valtiollinen
- Motiivi: Ennalta suunniteltu ideologinen tai sosiaalinen
- Aikomus: Pelon herättäminen tai toimintaan pakottaminen
- Keinot: Kyberympäristössä tapahtuva hyökkäys tai sen uhka
- Vaikutus: Kybermaailman ulkopuolinen psykologinen, sosiaalinen, poliittinen, fyysinen, taloudellinen tai ekologinen seuraus
- Kohde: Siviilit, valtiohallinto tai ei-valtiolliset organisaatiot

Auki kirjoitettuna kehitetyn taksonomian perusteella muodostettava kyberterrorismin määritelmä on siis:

> *”ei valtiollisen toimijan harkittuja ja suunniteltuja hyökkäyksiä tai niillä uhkaamista aikomuksena hyödyntää kyberympäristöä pelon herättämiseen tai siviilien, valtioiden tai ei-valtiollisten organisaatioiden toimintaan pakottamiseen sosiaalisten tai ideologisten tavoitteiden vuoksi (Plotnek & Slay 2021).”*

Kaiken kaikkiaan vaikkakin pitkä ja osin vaikeaselkoinen, on taksonomian avulla onnistuttu kehittämään laajasti erilaisia toiminnan muotoja huomioon ottava, mutta muista ilmiöstä erottelemaan kykenevä kyberterrorismin määrittely. Siinä näkyy selvästi tutkimustyöllä aiemmin saavutettu ymmärrys, ja siitä on havaittavissa tuttuja aspekteja kuten vaatimus kybermaailman ulkopuolisille seurauksille tai pelon käyttäminen toimintaan painostamiseen tai pakottamiseen. Toisin kuin monet muut aiemmat lähestymistavat, sisältyy määritelmään esimerkiksi terroristisessa mielessä harjoitettava informaatiovaikuttaminen tai propagandan levitys olettaen, että se sisältää jonkinnäköisen uhkauksen hyökkäysten toteuttamiseen. Toisaalta ulkopuolelle jää yhä varsin laajalti perinteisen terrorismin tukena harjoitettava kybertoiminta, kuten rekrytointi, viestintä tai varainhankinta (ks. Kenney 2015). On huomioitava, että kyseessä on suhteellisen uusi tapa jäsentää ilmiötä, eikä sitä ole ainakaan vielä yleisesti todettu parhaaksi tai järkevimmäksi tavaksi määritellä se.

Kyberterrorismin määrittelyn haasteita kuvaa, että suhteellisen laajasta, nyt jo vuosikymmeniä jatkuneesta panostuksesta huolimatta, ei yhteisesti sovittua ja hyväksi todettua tapaa määritellä ilmiötä ole vielä onnistuttu tuottamaan. Tämän luvun tarkoituksena oli ennen kaikkea kuvata näitä haasteita, sekä sitä miten määrittelyyn on tähän mennessä pyritty. Plotnekin ja Slayn taksonomia esiteltiin muita määritelmiä tarkemmin sen ollessa tämän tutkimuksen kannalta huomattavasti oleellisin. Tätä taksonomiaa, ja sen osatekijöitä eli komponentteja tullaan hyödyntämään sekä tarkasteltavaa aineistoa kerätessä että sitä analysoitaessa. Tutkimuksen ei ole tarkoitus todistaa kehitettyä teoriaa oikeaksi tai vääräksi, vaan arvioida mitä sen avulla tarkasteltuna voidaan sanoa kyberterrorismin ilmentymisestä viimeisen vuoden aikana.

5 TUTKIMUKSEN TULOKSET

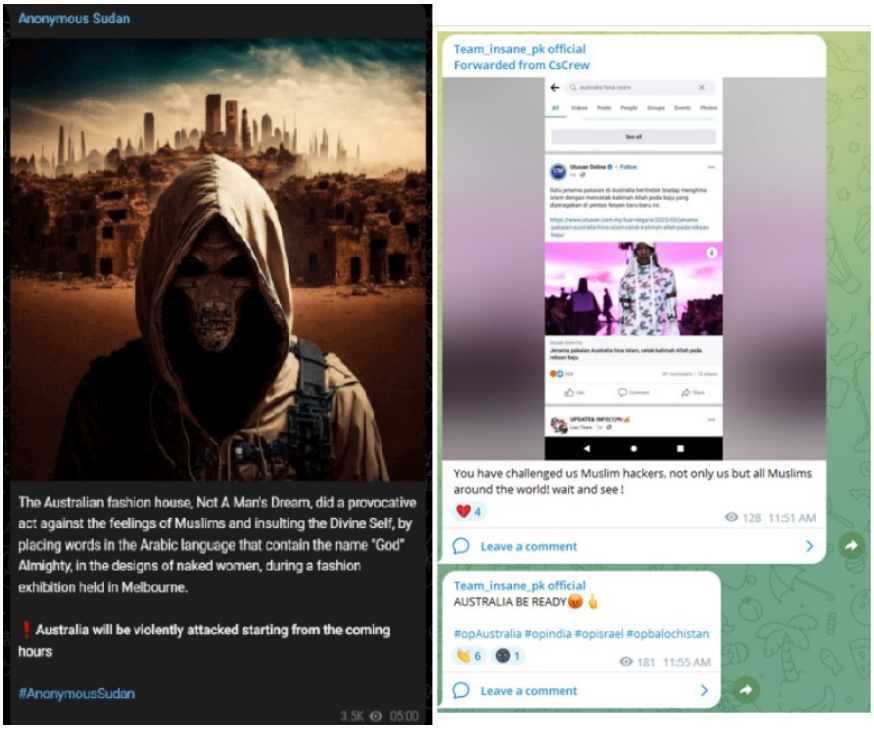
Tässä luvussa esitellään havaintoja, jota kerätystä aineistosta tehtiin, kun eri tapauksia pyrittiin vertaamaan Plotnekin ja Slayn kyberterrorismin taksonomian komponentteihin. Yhteensä viidestätoista analysoidusta tapauksesta, kolmen tunnistettiin täyttävän kaikki taksonomian komponentit ja olivat siten määriteltävissä kyberterrorismiksi. Muiden kohdalla yhden tai useamman komponentit kohdalla todettiin, että ne eivät sovi määritelmään, ja etenkin toimijan komponentti osoittautui tässä suhteessa karsivaksi. Tässä luvussa esitellään laajemmin tapauksia, joiden voitiin todeta vastaavan määritelmän mukaista kyberterrorismia, ja käsitellään tekijöitä, mitkä olivat tyypillisimpiä syitä, että tapaus jäi tulkitsematta kyberterrorismiksi. Kaikkia analysoituja tapauksia ei käsitellä, vaan käsittely on rajattu tapauksiin, jotka olivat joko luonteeltaan merkittäviä tai kuvastivat aineistossa toistuvia havaintoja tehokkaasti. Seuraavat alaluvut noudattavat pääosin rakennetta, jossa ensin esitellään käsiteltävä tapaus laajemmin, ja sen jälkeen sen eri osatekijöitä verrataan Plotnekin ja Slayn taksonomian komponentteihin ja pyrkimyksenä selvittää sopiiko se määritelmään kyberterrorismista, vai jääkö sen ulkopuolelle.

5.1 #OpAustralia – kyberiskut työkaluna ja kosto motiivina

Maaliskuussa 2023 australialainen muotitalo Not A Man's Dream järjesti Melbournen muotifestivaaleilla muotinäytöksen, jossa esitellyissä vaatekappaleissa kahdessa oli kirjoitettuna arabiankielinen lause "Allah kävelee kanssani". Kuvat sekä videot näytöksestä saivat pian islaminuskoisten muotimaailman seuraajien huomion. Tietoisuus levisi tehokkaasti etenkin, kun eri sosiaalisen median kanavilla suosittu malli ja muotibloggaaja Mona Khalifa nosti asian keskiöön pitäen vaatteita loukkaavina uskonnollisista syistä. Vastauksena syntyi ensin sosiaalisen median raivo, joka levisi islaminuskoisten keskuudessa ympäri maailman, ja vaikka muotitalo kiirehti pyytämään anteeksi ja poistamaan kuvat vaatteista omilta sosiaalisen median kanaviltaan vahinko oli jo tapahtunut. Useat

hakkeriryhmittymät ilmoittivat kanavillaan kostavansa kokemansa uskonnollisen halvennuksen kyberhyökkäyksillä Australiaan. Iskut kohdistuivat aluksi muotitaloon itseensä, mutta levisivät pian muihin australialaisiin kohteisiin, ja hyökkäyskampanja laajeni ja jatkui useita päiviä.

Mielenkiintoista tapauksesta tekee etenkin sen hyvin selkeä uskonnollinen motiivi, mutta myös se, että iskujen taustalla ei tunnistettu vain yhtä ryhmää tai ryhmittymää, vaan iskuja Australiaan tekivät useat toisistaan erilliset hakkerijengit. Plotnekin ja Slayn mukaisen mallin mukainen ennalta suunnittelu ja harkinta on selkeästi havaittavissa, sillä moni hyökkäyskampanjaan osallistunut ryhmä julkaisi etukäteen ilmoituksen aikeistaan iskeä Australiaan (Kuvio 1)[1]. Viestiä levitettiin ryhmien somekanavilla käyttäen hashtageja #OpAustralia ja #opsjentik ja eri arvioiden mukaan kampanjaan liittyi useita kymmeniä hakkerijengejä.



KUVIO 1 Kuvakaappaukset Anynomous Sudan ja Team_insane hakkerijengien sosiaalisen median kanavilta

Käytännössä hyökkäyskampanja toteutui palvelunestohyökkäyksien, tai hajautettujen palvelunestohyökkäyksien muodossa. Kuten aiemmin todettiin, kohteena oli aluksi itse näytöksen järjestänyt muotitalo sekä Melbournen muotifestivaalien muut osallistuja- ja järjestäjätahot, mutta hyökkäykset levisivät pian myös kohdistumaan myös muihin australialaisiin kohteisiin. Hyökkäysten kohteeksi joutui sekä australialaisia yliopistoja, pankkeja että viranomaistahoja, mutta myös yksityisiä yrityksiä toimialaan katsomatta.

[1] Haettu lähteistä https://socradar.io/hacktivism-on-the-rise-killnet-anonymous-sudans-cyber-campaign-targets-australia ja https://www.radware.com/security/threat-advisories-and-attack-reports/opaustralia-opsjentik/ 23.05.2023

Kyberterrorismin malliin sopii siis ennalta suunnitellun lisäksi selvästi taustalla vaikuttava uskonnollinen motivaatio. Plotnekin ja Slayn mallissa kyberterrorismin motivaatio on joko ideologinen tai sosiaalinen. Sosiaalisen motivaation kuvataan olevan tiettyyn rotuun tai väestöryhmään kohdistuva motivaatio, ja tässä tapauksessa se on sekä selkeä että monen hyökkäyksiä tehneen tahon itsensä ilmaisema motivaatio vastata islaminuskoa, ja -uskovaisia loukkaavaan tai halventavaan toimintaan.

Toisaalta taksonomian kannalta oleellinen aikomus on ensisilmäyksellä vaikeampi sovittaa malliin. Aikomuksena monen hakkerijengin mainitsema kosto on taksonomian kannalta hankala, sillä kostaminen on luonteeltaan reaktiivista toimintaa, eikä sillä välttämättä ole konkreettisia tavoitteita. Kosto on vastaus koettuun vääryyteen, eikä sen tarkoitus välttämättä, kuten ei tässäkään tapauksessa, ole pakottaa kohdettaan toimintaan. Kostolla voidaan yleisesti ajatella olevan tavoite saada kohde lopettamaan toteuttajaa loukanneen toiminnan, mutta kyseisessä tapauksessa tämäkään ei toteudu. Koska kyseessä oli yksittäinen tapahtuma, eli muotinäytös, jossa esiteltiin loukkaavia vaatteita, jonka ei voida olettaa toistuvan, ja koston kohteilla sinänsä ei välttämättä ollut mitään tekemistä koston aiheena olevan toiminnan kanssa ei kostomotiivilla voida nähdä olevan taksonomiassa mainittua tarkoitusta pakottaa tai painostaa kohde toimimaan halutulla tavalla. Plotnekin ja Slayn mallissa aikomuksena voi kuitenkin haluttuun toimintaan pakottamisen tai painostamisen sijaan olla myös yleinen pelon herättäminen kohteessa.

Tässä yhteydessä kohteeksi onkin miellettävä itse kyberiskujen kohteiden sijaan laajempi kokonaisuus, johon ne kaikki kuuluvat. Plotnekin ja Slayn mallissa kyberterrorismin kohde on joko siviilit, ei-valtiolliset organisaatiot tai valtionhallinto. Hyökkäyskampanjan tarkoituksena, motiivina tai aikomuksena ei ollut alkuvaiheen jälkeen iskeä mihinkään tiettyyn kohteeseen, vaan ylipäätään mihin tahansa australialaiseen toimijaan. Iskujen kohteet olivat ne sitten julkishallinon osia tai yksityisiä yrityksiä, olivat enemmän välineitä, joiden kautta Australiaan ja australialaisiin pyrittiin vaikuttamaan. Kun tapausta lähestytään tältä näkökannalta, on havaittavissa tavoite herättää pelkoa australialaisessa yhteiskunnassa, ja tätä tukee myös kyberhyökkäyksille tyypillinen retostelu onnistuneista iskuista sekä toisaalta myös niiden ennakkoon ilmoittaminen.

Pelkoa pyrittiin herättämään luomalla turvattomuuden tunnetta väestössä, ja vaikka myös ”suorempia” vaikutuksia väestöön saattoikin yksittäisistä hyökkäyksistä pienissä määrin seurata, voidaan toiminnan laajempana tavoitteena nähdä olevan pelon herättäminen ja sen kautta huomion saanti australialaisessa yhteiskunnassa. Monessa kampanjaan liittyvässä hyökkäyksiin osallistuneen hakkerijengin julkaisussa on suoraan havaittavissa tavoite herättää pelkoa tai epävarmuutta (ks. Kuvio 1). Myös sekä toteutuneiden iskujen, että aikeiden ilmaiseminen julkisilla sosiaalisen median kanavilla itsessään voidaan tulkita osaksi tavoitteita herättää pelkoa

Iskujen vaikutus ei konkreettisesti ollut merkittävä. Pysyvää tai edes kovin pitkäkestoista vaikutusta ei monellakaan kampanjan hyökkäyksellä ollut, mutta Plotnekin ja Slayn malli on tältä osaltaan varsin lavea. Taksonomiassa

kyberterrorismin vaikutuksia kuvataan olevan käytännössä mikä tahansa kybermaailman ulkopuolinen seuraus oli se sitten luonteeltaan sosiaalinen, psykologinen, taloudellinen, fyysinen tai ekologinen. Vaikka yksittäisiä nostoja tiettyjen kampanjaan liittyvien hyökkäyksien merkittävistä vaikutuksista ei löydykään, voidaan jo pelkän nousseen mediahuomion ja tulkita indikoivan jonkinlaista reaktiota kohdeyhteiskunnassa. Lisäksi taksonomiassa vaikutusten koolla ei sinänsä ole väliä, joten lyhyetkin toimintakatkokset ja niiden aiheuttama taloudellinen haitta ovat myös tulkittavissa kyberympäristön ulkopuolisiksi vaikutuksiksi.

On huomioitava, että vaikka tässä tekstissä kampanjaa käsitellään yhtenä laajan operaationa, ei taustalla ainakaan julkisten lähteiden valossa voida tulkita olevan vain yhtä toimijaa, jonka aikomusta tai tavoitteita voitaisiin analysoida. Vaikka on todisteita siitä, että eri kampanjaan osallistuneet hakkerijengit tukivatkin toisiaan vähintäänkin jakamalla omilla kanavillaan postauksia myös muiden suorittamista iskuista (ks. Kuvio 1), ei varsinaista koordinaatiota voida varmasti sanoa taustalla olevan.

Kaikesta huolimatta #OpAustralia hyökkäyskampanja tuntuu sopivan Plotnekin ja Slayn taksonomian mukaiseen määrittelyyn kyberterrorismista. Siinä on selkeä sosiaalinen motivaatio, toimijana on useat ei-valtiolliset hakkerijengit, aikomus on pelon herättäminen kohdeyhteiskunnassa, keinona toimii kyberympäristössä tapahtuva hyökkäys, vaikutukset (joskaan ei vakavat) ovat havaittavissa kyberympäristön ulkopuolella ja kohteena voidaan tulkita olevan sekä australialaiset siviilit, valtiohallinto tai ei-valtiolliset organisaatiot. Mielenkiintoista tarkastelusta tekee etenkin juuri toiminnan kohteen olevan eri kuin itse hyökkäysten kohteen. Koska aikomuksena oli herättää pelkoa yleisesti yhteiskunnassa ei itse hyökkäysten kohteilla sinänsä ollut väliä, vaan tärkeämpää oli mahdollisimman moneen kohteeseen iskeminen ja sitä kautta huomion saanti. Kampanjan tavoitteiden kannalta oleellista ei ollut varsinaisesti yksittäisten iskujen tuomat vaikutukset vaan enemmänkin hyökkäyskampanjan saama huomio ja sen laajuuden korostaminen.

5.2 #OpSweden ja pelotevaikutuksen kyseenalainen teho

#OpAustralian kanssa hyvin verrannollinen tapaus oli Ruotsissa tapahtunutta Koraanin polttoa seurannut kyberhyökkäysaalto. Vuoden 2023 tammikuussa ruotsalainen äärioikeistopoliitikko Rasmus Paludan poltti Koraanin Turkin suurlähetystön lähistöllä poliittisena mielenilmauksena. Mielenilmaukseen oli pyydetty lupaa Ruotsin viranomaisilta, jota ei kuitenkaan saatu, mutta Koraani paloi tästä huolimatta. Tämän tutkimuksen kannalta ei ole niinkään mielenkiintoisia ne syyt, jotka johtivat kirjan polttoon, tai diplomaattiset seuraukset Ruotsin ja Turkin välille, vaan tarkastelun kohteena on kybermaailmassa tapahtunut reagointi, jossa Ruotsille päätettiin kostaa pyhän kirjan halventaminen. #OpSweden nimellä kulkeva kyberhyökkäyskampanja oli monella tapaa hyvin

samankaltainen #OpAustralian kanssa ja siinäkin motiivina oli uskonnollisen loukkauksen kostaminen.

Kuviossa 2 on kuvakaappaus Ghost Killer hakkeriryhmän Twitter-julkaisusta, jossa luvataan kostaa Koraanin poltto kyberhyökkäyksillä.[2]

KUVIO 2 Kuvakaappaus Ghost Killer hakkeriryhmän Twitter-julkaisusta.

Samoin kuin esitellyn Australian tapauksen kanssa, myös Ruotsiin kohdistui seurauksena muutamia päiviä kestänyt kyberhyökkäysten aalto, jonka kohteiksi joutui niin valtiohallinnon osia kuin yksityisiä yrityksiä. Plotnekin ja Slayn mallin mukaiset motivaatio, toimija, aikomus, keinot, vaikutukset ja kohde löytyvät myös tästä tapauksesta, tosin jälleen aikomuksen tulkinta pelon herättämiseen yhteiskunnassa on jokseenkin tulkinnanvarainen ja perustuu ajatukseen, että kyberhyökkäyksillä ruotsalaisiin organisaatioihin tavoitellaan pelon herättämistä yhteiskunnassa.

Luvussa 3 esitellyssä Michel Kenneyn kyberterrorismin määritelmässä (Kenney, 2015) pelon herättämisellä ajatellaan usein olevan taustatavoite pakottaa pelon keinoin kohde toimimaan halutulla tavalla. #OpAustraliaan verrattuna Ruotsin tapauksessa on kenties helpommin havaittavissa ajatusmalli, jossa väestössä herätetyn pelon avulla pyritään painostamaan viranomaisia ja päättäjiä haluttuun toimintaan, sillä käynnissä oli samanaikaisesti myös diplomaattinen konflikti, jossa Turkki pyrki painostamaan Ruotsia toimimaan haluamallaan tavalla. Australian tapaukseen verrattuna #OpSwedenillä vaikutti myös olevan huomattavasti konkreettisempia seurauksia, sen johtaessa sekä laajaan

[2] Haettu lähteestä https://twitter.com/thtghostkiller/status/1638259824432410655 22.05.2023

kansainväliseen huomioon, että konkreettisiin diplomaattisiin seurauksiin Ruotsin ja Turkin välillä. Kuitenkin on vaikea nähdä, että edellä mainitut seuraukset olisivat johtuneet itse kyberhyökkäyksistä, ja niiden vaikutus kokonaisuudessaan on varsin tulkinnanvarainen. Lisäksi, jotta nämä seuraukset voitaisiin mieltää vaikutuksiksi kyberterrorismiksi määriteltävästä toiminnasta, olisi toimijaksi miellettävä Turkin valtio, eikä siitä irralliset hakkerijengit, kuten nyt on tehty. Plotnekin ja Slayn mallissa kyberterrorismin toimijan on oltava ei-valtiollinen, ja tähän haasteeseen palataan myöhemmin enemmän. Siis vaikka kyberhyökkäyskampanja tapahtui samanaikaisesti diplomaattisen selkkauksen kanssa, ei sillä ainakaan selvästi voida nähdä olleen merkittävää vaikutusta tähän, ja myös pelotevaikutuksesta tuntuu jääneen tässäkin tapauksessa vähäiseksi. Kyberhyökkäykset eivät aiheuttaneet merkittäviä tai pitkäkestoisia toimintahäiriöitä ruotsalaisessa yhteiskunnassa, eikä niillä onnistuttu tarpeeksi konkreettisesti uhkaamaan Ruotsin väestöä, jotta pelotevaikutus olisi ollut merkittävä.

Sekä #OpAustralian että #OpSwedenin kohdalla Plotnekin ja Slayn taksonomian osista eniten haasteita tuottaa aikomuksen tulkinta. Molemmissa tapauksissa pelon herättämisen tavoite on tulkinnanvarainen, ja etenkin sen teho kyseenalainen. On vaikea arvioida, milloin pelon herättäminen on onnistunut, eikä se varsinaisesti ollut tämän tutkimuksen tavoitteena, mutta kummassakaan tapauksessa ei niitä käsittelevissä media-artikkeleissa tilannetta kuvattu uhkaavana, tai merkkejä siitä, että kohdemaan väestö (henkilöt tai organisaatiot) olisi todella ollut peloissaan ei löydetty. Määritelmässä ei kuitenkaan ole väliä sillä kuinka tehokkaasti kyberterroristinen toiminta onnistui saavuttamaan siihen liittyvän aikomuksen ja tässä suhteessa molemmat tapauksesta ovat miellettävissä teorian mukaisista vaikkakin konkreettisilta vaikutuksiltaan vähäisiksi esimerkeiksi kyberterrorismista.

Mielenkiintoinen tapa ajatella pelkovaikutusta on myös sen lähestyminen Plotnekin ja Slayn taksonomian keinon, eikä aikomuksen kautta. Määritelmässä hyökkäyksen toteuttamisen keinona voi olla myös kyberhyökkäyksen sijaan pelkkä sen uhka, ja etenkin jatkuvan hyökkäyskampanjan yhteydessä voidaan helposti nähdä miten pelkovaikutus perustuu pitkälti myös uhkaan jatkuvista tai tulevista iskuista. #OpAustralian ja #OpSwedenin kaltaisiin hyökkäyskampanjoihin pelon herättäminen liittyy siis sekä aikomuksen, että keinon komponenttiin.

5.3 Charlie Hebdo ja kostomotiivi

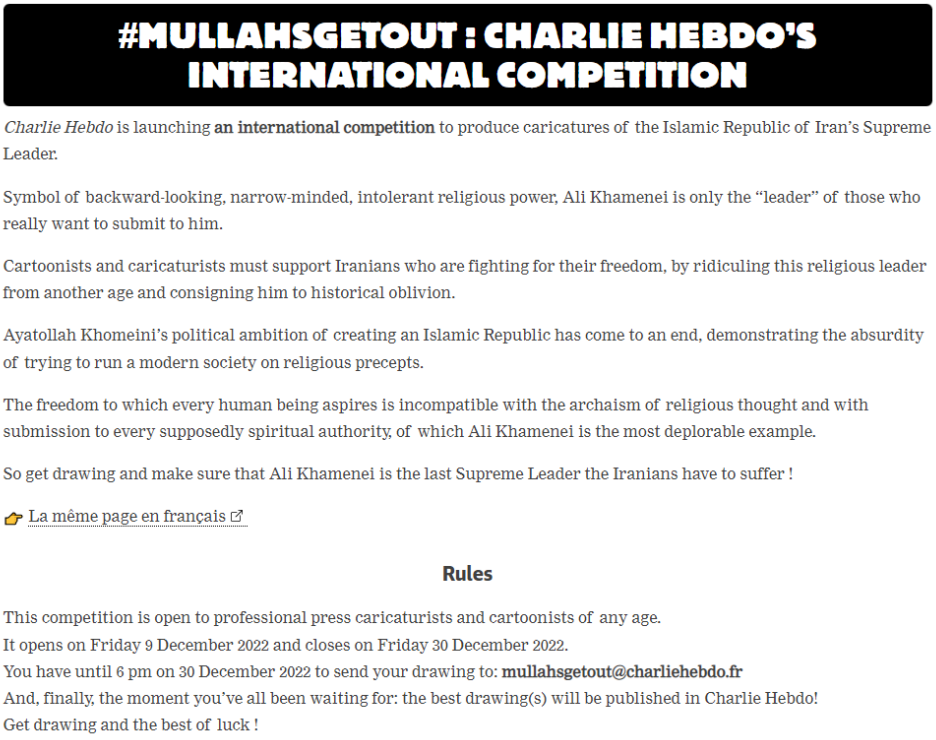
#OpAustralia ja #OpSweden ovat parhaiten Plotnikin ja Slayn taksonomiaan sopivia tapauksia, joissa selvästi on havaittavissa kaikki määritelmän mukaiset kyberterrorismin komponentit. Ne ovat myös monella muulla tavalla kuvaavia esimerkkejä aineistossa havaittuihin toistuviin ilmiöihin. Yksi näistä, joka toistui myös monen huonommin taksonomiaan sopivan tapauksen kanssa, on motiivina tai aikomuksen toiminut kostaminen. Monessa tapauksessa hakkeriryhmien itse ilmoittava motivaatio, eli taksonomian mukainen aikomus, oli kostaa koettu

vääryys tietylle taholle tai toimijalle. Tämänkaltaisia tapauksia oli esimerkiksi ranskalaislehti Charlie Hebdoon tammi-helmikuussa 2023 tehty tietomurto. Vaikka tapaus ei välttämättä muilta osin vastaakaan teorian mukaista kyberterrorismia, on siinä silti piirteitä, jotka tekevät siitä mielenkiintoisen tarkastelun kohteen taksonomian avulla lähestyen. Kosto oli motiivina myös moneen muuhun tarkasteltuun kyberhyökkäykseen, mutta näistä yksikään ei täyttänyt kaikkia muita taksonomian vaatimuksia tullakseen määritetyksi kyberterrorismiksi ja yleisimpiin syihin miksi tapaukset jäivät määritelmän ulkopuolelle, palataan myöhemmässä alaluvussa.

Charlie Hebdo muistetaan sen toimitukseen vuonna 2015 tehdystä terrori-iskusta, jossa 12 henkilöä menetti henkensä. Lehti on siis ollut aiemmin ”perinteisen” terrori-iskun kohteena, ja sen kautta onkin mielenkiintoista vertailla sen aiemmin kokemaa perinteistä iskua vuoden 2023 alussa tapahtuneeseen kyberhyökkäykseen. Vaikka aiempi tapaus tunnetaan yhtenä konkreettisimmista modernin maailman terrori-iskuista Euroopassa, ei taustavaikuttimiltaan hyvinkin samankaltaista kyberiskua ole laajasti leimattu terrorismiksi.

Vuoden 2015 terrori-iskun taustalla oli lehden julkaisemat satiiriset kuvat islaminuskolle tärkeästä profeetta Muhammedista, joiden myötä lehteä syytettiin uskon halventamisesta. Vuoden 2022 lopulla lehti ilmoitti järjestävänsä piirustuskilpailun, johon osallistuvia pyydettiin tuottamaan pilkkaavia tai halventavia kuvia Iranin hengellisestä johtajasta Ali Khameneista (Kuvio 3).[3]

[3] Haettu lähteestä https://web.archive.org/web/20230109230442/https:/charliehebdo.fr/mullahsgetout-international-competition/ 23.05.2023



#MULLAHSGETOUT : CHARLIE HEBDO'S INTERNATIONAL COMPETITION

Charlie Hebdo is launching **an international competition** to produce caricatures of the Islamic Republic of Iran's Supreme Leader.

Symbol of backward-looking, narrow-minded, intolerant religious power, Ali Khamenei is only the "leader" of those who really want to submit to him.

Cartoonists and caricaturists must support Iranians who are fighting for their freedom, by ridiculing this religious leader from another age and consigning him to historical oblivion.

Ayatollah Khomeini's political ambition of creating an Islamic Republic has come to an end, demonstrating the absurdity of trying to run a modern society on religious precepts.

The freedom to which every human being aspires is incompatible with the archaism of religious thought and with submission to every supposedly spiritual authority, of which Ali Khamenei is the most deplorable example.

So get drawing and make sure that Ali Khamenei is the last Supreme Leader the Iranians have to suffer !

La même page en français

Rules

- This competition is open to professional press caricaturists and cartoonists of any age.
- It opens on Friday 9 December 2022 and closes on Friday 30 December 2022.
- You have until 6 pm on 30 December 2022 to send your drawing to: **mullahsgetout@charliehebdo.fr**
- And, finally, the moment you've all been waiting for: the best drawing(s) will be published in Charlie Hebdo!
- Get drawing and the best of luck !

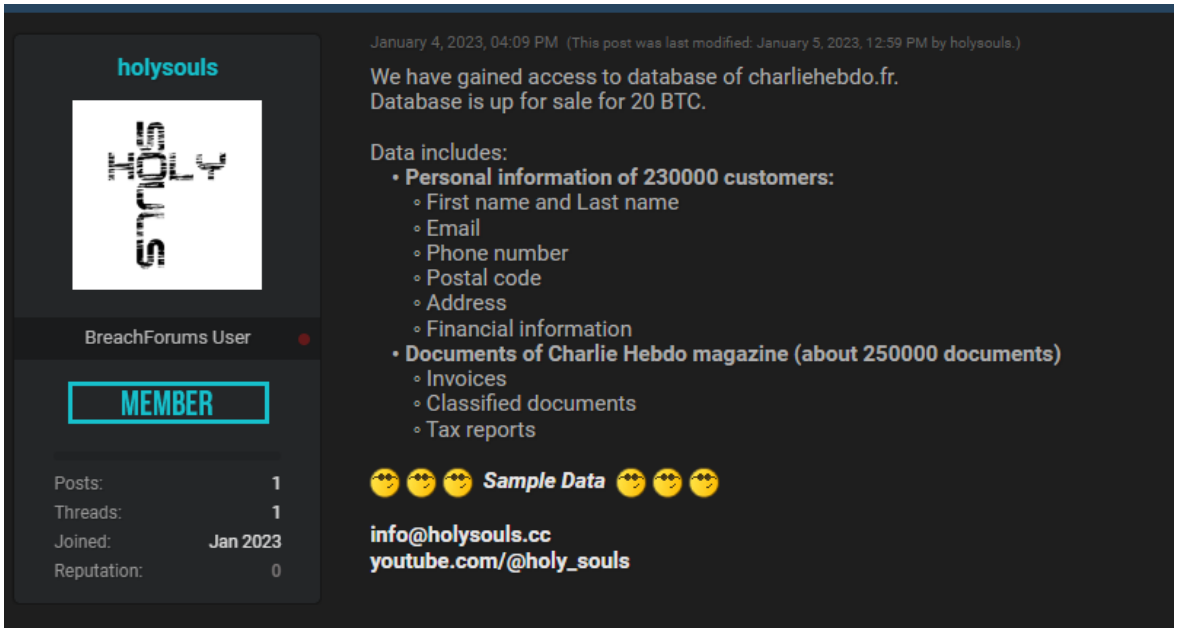
KUVIO 3. Kuvakaappaus Charlie Hebdon julkaisemasta ilmoituksesta piirustuskilpailusta.

Kuten kuviosta 3 nähdään, ilmoitettuna syynä kilpailun järjestämiseen oli Iranin hallintoa vastustavien aktivistien tukeminen ja toive kuvatun vanhoillisen hallintomuodon kaatamisesta. Luonnollisesti tähän Iranin valtio reagoi tähän negatiivisesti, ja kun muutaman viikon kuluttua aiemmin tuntematon Holy Souls- niminen hakkeriryhmä ilmoitti toteuttaneensa onnistuneen kyberhyökkäyksen lehteä kohtaan, olivat iranilaiset toimijat luonnollisia epäilyksen kohteita. Holy Souls paljastuikin myöhemmin olevan itsenäisen hakkerijengin sijaan hyvin todennäköisesti Iranin valtion kontrolloima ryhmä, ja tähän muutokseen toimijan luonteessa palataan myöhemmin.

Kyberhyökkäyksestä ilmoitettiin jälleen sen toteuttaneen ryhmittymän toimesta, tällä keltaa sosiaalisen median sijaan ajanhetkellä aktiivisella ja yleisesti tunnetulla hakkerien käyttämällä keskustelupalstalla (Kuvio 4).[4] Ryhmä kertoi saaneensa haltuun Charlie Hebdon tietokannan, joka sisälsi yli 230 000 lehden tilaajan henkilötietoja, sekä noin 250 000 toimituksen sisäistä tiedostoa. Kuten tietomurtojen kohdalla on tyypillistä, viestin yhteydessä julkaistiin näyte haltuun saadusta datasta, ja ranskalaislehden Le Monden analysoiman näytteen

[4] Haettu lähteestä https://web.archive.org/web/20230109230105/https://breached.vc/Thread-Personal-information-of-230000-customers-of-charliehebdo-fr 23.05.2023

perusteella voitiin todeta, että näytteen sisältämät tiedot olivat aitoja ja peräisin Charlie Hebdolta (Le Monde).



KUVIO 4. Kuvakaappaus Holy Souls ryhmän viestistä BreachForums keskustelupalstalla.

Tapaus eroaa muista tässä tutkimuksessa tähän mennessä esitellyistä kyberhyökkäyksistä sen suhteen, että siinä toimijana on monen eri hakkeriryhmän sijaan vain yksi toimija, ja kyseessä oli useita päiviä jatkuneen kampanjan sijaan yksittäinen isku. Tapauksen taustalla oli aiempien kanssa samanlainen uskonnollinen motiivi ja aikomus aiheuttaa pelkoa, mutta sekä keinot, niiden vaikutukset, että iskun takan oleva tekijä olivat erilaiset.

Keinona oli aiemmista tapauksista poiketen tietomurto, ja sitä seurannut lunnasvaatimus. Kuten kuviosta 4 nähdään, ryhmä ilmoitti kaapattujen tietojen olevan myynnissä 20 Bitcoinin hintaan. Itse tapaa, jolla tietomurto toteutettiin ei julkisista lähteistä ole varmasti pääteltävissä, mutta taksonomian kannalta tällä ei niinkään ole väliä, sillä kyseessä voidaan varmuudella silti sanoa olleen kyberympäristössä tapahtunut isku.

Iskun vaikutukset puolestaan olivat selkeästi muihin esiteltyihin tapauksiin verrattuna konkreettisemmat ja selkeämmät. Vaikka jälleen pelotevaikutuksen teho on vaikeatulkintainen tällä kertaa iskun takia kymmenien tuhansien yksittäisten henkilöiden tietoja, päätyi kyberrikollisten käsiin, johtaen sekä kasvaneeseen riskiin joutua identiteettivarkauksien tai muiden kyberuhkien kohteeksi. Lisäksi vaikkakaan tietoa siitä, että vaadittuja lunnaita tietojen palauttamiseksi olisi maksettu, tai kukaan olisi ylipäätään kaapattua dataa ostanut, voidaan taustalla nähdä silti olevan myös taloudellisen hyödyn tavoittelu, eli taksonomiaan sopivien taloudellisten vaikutusten tavoittelu.

Mielenkiintoisin, ja taksonomian kannalta hankalin komponentti on kuitenkin itse hyökkäyksen tekijä. Kuten aiemmin mainittu, Holy Souls oli entuudestaan tuntematon hakkeriryhmittymä, mutta Microsoftin Digitaalisten uhkien analyysikeskuksen (engl. Microsoft Threat Analysis Center, DTAC) mukaan

kyseessä on todellisuudessa jo entuudestaan tunnettu Emennet Pasargard- niminen uhkatoimija, jonka on jo aiemmin tunnistettu olevan tuttu Iranin valtion kontrolloima ryhmä. Attribuutio, eli ryhmän tunnistaminen ennalta tunnetuksi perustui keskuksen omaan *DTAC Framework of Attribution*- malliin ja sitä voidaan pitää luotettavana. Mallissa attribuutio tehdään sekä avoimesti saatavilla olevaan tietoon ja arvioitavan kohteen toimintatapoihin, joita verrattaan tunnistettuihin tapauksiin, mutta myös ei-julkiseen telemetriatietoon[5]. Vaikka Iran ei virallisesti tunnustakaan iskun tekemistä, on tämä varsin tyypillistä valtiollisten hakkeriryhmien käytössä (Lemay, Calvet, Menet & Fernandez, 2018 s. 34–40). Lisäksi attribuutiota tukee myös Iranin vallankumouskaartin komentajan kenraali Hossein Salamin lausunto piirustuskilpailuun liittyen, jossa hän kertoo koston lehteä kohtaan olevan taattu.

Koska kyseessä voidaan siis suhteellisen luotettavasti todeta olevan valtiollinen toimija, ei tapaus sovi Plotnekin ja Slayn kyberterrorismin malliin. Vaikka muut taksonomian komponentit ovatkin havaittavissa, ja tapaus etenkin historiallisen kontekstin vuoksi voi intuitiivisesti tuntua ennemmin terroriteolta ei se sitä määritelmän mukaisesti ole. Aiempiin esiteltyihin tapauksiin verrattuna on tapauksessa myös konkreettisempi ja kenties tehokkaampi pelotevaikutus, ja toisin kuin #OpSwedenin ja #OpAustralian tapauksissa, myös useat viranomaistahot ilmaisivat huolen siitä mitä voi seurata, että lehden tilaajien tietoja on päässyt vihamielisten tahojen käsiin tehostaen pelon syntymistä. Valtiollinen attribuutio kuitenkin sulkee tapauksen kyberterrorismin määritelmän ulkopuolelle, ja sama todettiin myös usean muun tutkimuksessa käsitellyn tapauksen kohdalla.

5.4 Toimijan tunnistaminen haasteena

Kaikista Plotnekin ja Slayn taksonomian komponenteista tekijän sovittaminen kyberterrorismin malliin osoittautui kaikista hankalimmaksi. Hyvin monen käsitellyn tapauksen kohdalla kaikki muut taksonomian edellyttämät komponentit voitiin suhteellisen helposti löytää, mutta tekijää ei joko voitu tarkasti määrittää, tai Charlie Hebdon tapauksen tavoin tekijäksi voitiin tunnistaa valtiollinen toimija. Toimijan tunnistaminen ja etenkin valtiollisten ja ei-valtiollisten ryhmien erottaminen toisistaan on yleinen kyberuhkien tulkintaan liittyvä haaste, joka käy jatkuvasti vaikeammaksi. Monella suurvallalla on käytössään, joko suoraan niiden ohjauksessa olevia hakkeriryhmiä, tai heikommin sidottuja, mutta silti valtiollista agendaa toteuttavia toimijoita (Ussath, Jaeger, Feng Cheng & Meinel 2016). Kuten aiemmin todettua, näitä irrallisia ryhmiä kontrolloivat valtiot äärimmäisen harvoin tunnustavat niiden toiminnan, ja yksi oleellisimmista syistä käyttää näitä ryhmiä onkin attribuution välttäminen (Lemay & al. 2018).

[5] https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/02/DTAC-Attribution-Framework.pdf luettu 23.05.2023

Valtiollisista hakkerijengeistä käytetään yleensä nimitystä Advanced Persisten Threat- eli ATP-ryhmä.

Tässä tutkimuksessa tuli vastaan useita tapauksia, jotka muuten olisivat vastanneet valitun määritelmän mukaista kyberterrorismia, mutta yhden tai useamman luotettavana pidetyn tason tekemän analyysin myötä taustalla paljastui olevan johonkin valtioon liitettävissä oleva ATP-ryhmä. Etenkin Iraniin ja sen vallankumouskaartiin (Islamic Revuliotanary Guard Corps, IRGC) yhdistettiin paljon tapauksia, jotka muuten olisivat vastanneet kyberterrorismin määritelmää. Näitä tapauksia olivat esimerkiksi Albaniaan kesä- ja syyskuussa kohdistuneet kyberhyökkäykset, Israeliin kohdistunut vuosittain toistuva #OpIsrael hyökkäysaalto, ja jo esitelty Charlie Hebdon kokema tietomurto.

Mielenkiintoisen asetelmasta tekee se, että Iranin vallankumouskaarti mielletään itsessään monessa länsimaassa terroristijärjestöksi, ja se löytyy esimerkiksi Yhdysvaltojen *Foreign Terrorist Organizations* listalta[6]. Plotnekin ja Slayn malli kuitenkin sulkee nämä, vaikkakin tunnistetun terroristiorganisaation suorittamat kyberhyökkäykset kyberterrorismin ulkopuolelle, sillä Iranin vallankumouskaarti on selvästi valtiollinen, eli valtiohallinnon alaisuudessa oleva toimija. Tämä on mielenkiintoinen asetelma, sillä intuitiivisesti voisi ajatella, että jos puhutaan tunnetun terroriorganisaation suorittamista kyberhyökkäyksistä kyse olisi automaattisesti kyberterrorismista. Plotnekin ja Slayn mallissa tunnistetut terroristitoimijat rajattiin kuitenkin taksonomian ulkopuolelle, sillä terroristiorganisaatioillekaan ei ole olemassa yksiselitteistä määritelmää, ja eri toimijoiden muodostamat tai ylläpitämät listat terroristeista ovat vahvasti subjektiivisia (Plotnek & Slay 2021). Tätä rajausta perustellaan myös toisaalta sillä, että suurin osa terroristiorganisaatioista on samaan aikaa myös ei-valtiollisia toimijoita, joten näiden suorittamat operaatiot olisivat miellettäväksi kyberterrorismiksi huolimatta siitä, oliko niitä vai ei etukäteen todettu terroritoimijoiksi. Iranin vallankumouskaartia voidaan siis poikkeustapauksena, jossa on kyse samaan aikaan usean tahon määrittämästä terroristijärjestöstä ja valtiollisesta toimijasta, joten tähän liittyvät haasteet ovat luonnollisia.

Monessa analysoidussa tapauksessa kyberterrorismin määritelmä jäi myös täyttymättä yksinkertaisesti siitä syystä, että toimijaa ei voitu luotettavasti tunnistaa. Plotnekin ja Slayn taksonomiassa kyberterroristisen toimijan tulee olla tunnistettu ei-valtiollinen toimija, ja mikäli tätä ei voitu luotettavalla varmuudella tehdä, jäi tapaus tunnistamatta kyberterrorismiksi. Toimijan komponenttia esitellessä Plotnek ja Slay mainitsevat, että jossain aiemmissa ilmiön määrittelyissä toimija oli yksinkertaisesti nimetty salassa, tai luvatta toimivaksi eikä näissä lähestymistavoissa varsinaista tunnistamista tai attribuutiota olisi vaadittu. Kuten tutkijat toisaalta toteavatkin, mikäli toimijuus määritellään pelkästään salassa tai luvattomasti toimimisella, olisi lopputulos lähes sama kuin määritelmää ei olisi lainkaan. Kun puhutaan kyberhyökkäyksistä, joita yritetään määritellä kyberterrorismiksi, puhutaan jo lähtökohtaisesti toiminnasta, joka on

[6] https://www.state.gov/foreign-terrorist-organizations/ luettu 23.05.2023

vähintäänkin luvatonta, ja yleensä toiminta itse myös toteutetaan salassa, vaikka sillä etukäteen uhattaisiinkin tai myöhemmin retosteltaisiin.

Toimijan tunnistaminen on siis oleellinen osa taksonomian toimintaa. On huomioitava, että vaikka tässä tutkimuksessa toimijan komponentti oli selkeästi eniten tapauksia kyberterrorismin määritelmän ulkopuolelle rajaava, oli syynä tähän pitkälti se, että valtioiden käyttämät ja niille selkeästi attribuoidut hakkeriryhmät tulkittiin valtiollisiksi toimijoiksi, eikä ei-valtiollisiksi, jolloin ne olisivat määritelmään sopineet. Kuten aiemmin todettua, valtioiden käyttämät hakkeriryhmät ovat monimutkainen ja heterogeeninen kokonaisuus, ja rajanveto siihen missä menee valtiollisen ja ei-valtiollisen toimijan raja on häilyvä. Tämä haastaa myös valtiollisuuteen perustuvan komponentin käyttöä kyberterrorismin määrittelemisessä.

5.5 Iranin terästeollisuus ja tulkinnanvarainen motiivi

Vaikka toimijuuden komponenttiin liittyvät haasteet olivat yksittäinen merkittävin syy, jonka myötä käsitellyt tapaukset rajattiin kyberterrorismin määritelmän ulkopuolelle ei se ollut ainoa laatuaan. Kuten mainittua, toimijuuden komponentti sisälsi jonkin verran tulkinnanvaraisuutta siitä milloin kyse on valtiollisesta ja milloin ei-valtiollisesta toimijasta, mutta tämä tulkinnanvaraisuuden haaste oli kenties vielä enemmän läsnä muihin komponentteihin perustuvissa rajauksissa.

Yksi muuten mielenkiintoinen ja monella tavalla poikkeava tapaus, jonka taksonomiaan sovittaminen tuotti haasteita etenkin aikomuksen ja motivaation komponenttien osalta oli Iranin terästeollisuuteen heinäkuussa 2022 kohdistunut kyberhyökkäys. Kolmeen tuotantolaitokseen kohdistuneessa iskussa hyökkääjät onnistuivat hallintajärjestelmät lamauttamalla aiheuttamaan tulipalon ainakin yhdellä kohteena olleista laitoksista. Kyseessä on sikäli harvinainen tapaus, että kyberhyökkäyksillä hyvin harvoin onnistutaan aiheuttamaan fyysistä tuhoa kohteessa, ainakaan suoraan ja pelkästään kyberympäristössä tapahtuvalla hyökkäyksellä. Valvontakameravideot tehtaalta kuitenkin todistavat, että tulipalo todella syttyi, ja myös henkilövahingot olisivat olleet mahdollisia.

Tapaus on siis monelta osin varsin poikkeuksellinen ja sopii usean komponentin osalta myös Plotnekin ja Slayn taksonomiaan kyberterrorismista. Kuten jo todettua, kyseessä on kyberhyökkäystä keinona hyödyntävä, vaikutuksiltaan hyvin konkreettisesti kybermaailman ulkopuolella, Iranin valtion omistamiin tehtaisiin, eli siten valtiolliseen organisaatioon kohdistuva isku. Kuitenkin tekijän sovittaminen tuottaa haasteita malliin, ja motivaation sekä aikomuksen kohdalla tämä on vielä hankalampaa.

KUVIO 5. Kuvakaappaus Predatory Sparrow ryhmän viestistä hyökkäyksen jälkeen

Iskun tekijäksi ilmoittautui Predatory Sparrow- nimellä tunnettu hakkeriryhmä, joka käyttää itsestään samaa tarkoittavaa Persian kielen nimitystä Gonjeshke Darande (Kuvio 5), joka tunnetaan jo entuudestaan etenkin Iraniin kohdistuneista hyökkäyksistä.[7] Aiemmat ryhmälle attribuoidut operaatiot ovat kohdistuneet julkisen liikenteen häirintään ja hallinnon kyvyttömyyden pilkkaamiseen. Ryhmä liitetään hyvin vahvasti Israeliin, joka käy jatkuvaa kyberkamppailua Iranin kohtaan, ja monen kontekstuaalisen todisteen perusteella voidaan jopa suhteellisen luottavaisesti väittää ryhmän olevan joko israelilainen, tai ainakin sen agendaa edistävä ryhmittymä. Tästä ei kuitenkaan ole varmuutta, eli luotettavan kolmannen osapuolen tekemää faktoihin pohjautuvaa analyysia ja sekä ryhmä itse että Israelin valtio ovat kieltäneet yhteyden. Joten toisin kuin Charlie Hebdoon iskeneen Holy Souls- ryhmän kohdalla, ei tässä kohdassa voida tulkita tekijän olevan valtiollinen kiistattomien todisteiden puuttuessa. Holy Soulsin kohdalla ryhmän voitiin todeta olevan Iranin valtion alainen toimija perustuen tarkkaan analyysiin sen toimintamenetelmistä ja käytetyistä tekniikoista ja Predatory Sparrow:n kohdalla vastaavaa analyysiä ei löydy, vaan attribuutio perustuu siihen, että ryhmän toiminta on tukenut Israelin valtiollisia motiiveja haitaten Iranin toimintaa, ja siihen että ryhmä on vahvasti resursoitu. Tästä johtuen tässä tutkimuksessa päädyttiin hyväksymään Predatory Sparrow ei-valtiolliseksi toimijaksi, jolloin toimijan komponentti vastaa Plotnekin ja Slayn taksonomiaa.

Aikomus ja motiivi ovat kuitenkin vaikeammin määritelmään sovitettavissa. Kuten kuviosta 5 nähdään, ryhmän ainoa itse ilmoittamansa motiivi iskulle

[7] haettu kohteesta https://www.nejatngo.org/en/posts/14305, 26.05.2023.

on kohteena olleiden iranilaisten tehtaiden toiminta niihin kohdistuneista kansainvälisistä sanktioista huolimatta. Kyseessä voitaisiin nähdä olevan ideologiaan, eli tässä tapauksessa Iranin hallinnon vastustukseen perustuva motiivi, tai toisaalta sosiaalisuuteen eli viestissä mainittujen viattomien siviilien suojeluun perustuva motiivi. Monessa lähteessä kuitenkin mainittiin, että taustalla vaikutti todennäköisesti Israelin valtion motiivi heikentää Iranin terästeollisuuden tuotantokykyä, ja vaikka tämäkin tulkinta perustuu vain oletukseen siitä, että ryhmä todella ajaa Israelin etuja on motiivin kohdalla silti tulkinnanvaraisuutta ja hyvin vähän konkretiaa mihin tarttua. Jälleen kuitenkin varmojen todisteiden puuttuessa, ryhmän toiminnan motiiviksi tulkittiin sen oman viestinnän perusteella olevan ideologinen Iranin hallinnon vastustaminen, joten myös motiivin komponentin todettiin vastaavan Plotnekin ja Slayn mallia.

Sama pitää paikkansa myös aikomuksen komponentin kohdalla. Jälleen on tulkittavissa, että iskulla haluttiin herättää pelkoa etenkin liittyen konkreettisen tuhovaikutuksen saavuttamiseen, ja toisaalta kenties tämän tutkimuksen tapauksista parhaiten se myös pakotti kohteensa toimintaan, eli vähintäänkin sammuttamaan tulipalon ja korjaamaan vahingot. Plotnekin ja Slayn mallissa kuitenkin toimintaan pakottamisella tarkoitetaan, että kohde pakotetaan toimimaan hyökkääjän haluamalla tavalla, eli tässä tilanteessa pitäisi tulkita, että hyökkääjä on toivonut kohteensa sammuttavan tulipalon ja korjaavan lattioita. Toisaalta, mikäli toiminnaksi, johon pakotetaan, on toiminnan puute, eli hyökkäystä seurannut tuotantokatko sopisi se tämän tulkinnan kautta malliin. Taksonomiassa ei kuitenkaan suoraan oteta kantaa, onko toiminnan estäminen tulkittavissa haluttuun toimintaan pakottamisella, ja määritelmää muodostaessaan aikomuksen komponentista jätettiin tietoisesti pois useammassa määritelmän muodostamisessa käytetyssä tutkimuksessa mainittu estämisen tai häirinnän tavoittelu (engl. interfere). Tähän päädyttiin, sillä toiminnan estäminen tai häirintä ei Plotnekin ja Slayn mukaan kuulu yksinomaan kyberterroristin toiminnan aikomuksiin, ja se saattaa hyvinkin esiintyä muunlaisenkin kyberuhkatoimijan tavoitteena. Pelon herättämisen aikomus on myös tulkinnanvarainen, sillä tätä ei voida päätellä ryhmän omasta viestinnästä, vaikka todennäköisesti tämän iskun pelkovaikutus oli tässä tutkimuksessa käsittelyistä tapauksista merkittävin aiheutetun fyysisen tuhon myötä. Aikomuksen tulkittiin kuitenkin loppujen lopuksi vastaavan taksonomiaa, sillä viestinnässä on havaittavissa merkkejä uhkaamisesta, eli tavoittelusta herättää pelkoa ja sitä kautta vaikuttaa kohteen toimintaa.

On mielenkiintoista, että monessa aiemmassa tavassa määritellä kyberterrorismia varsin konkreettisessa roolissa oli vaatimus aiheuttaa fyysistä tuhoa kyberiskulla. Kuitenkin tässä tutkimuksessa Iranin terästeollisuus oli ainoa tallaisen piirteen omaava tapaus, ja sen voitiin tulkita vastaavan Plotnekin ja Slayn määritelmää vain hyvin tulkinnanvaraisesti. Se kuitenkin päädyttiin hyväksymään yhdeksi esimerkiksi kyberterrorismista, mutta määrittely tehtiin varauksella, sillä luotettavaa tietoa tapauksesta ja etenkin sen taustalla vaikuttavasta toimijasta oli suhteellisen vähän. Tapausta haluttiin kuitenkin käsitellä sen mielenkiintoisen ominaispiirteen, eli fyysisen vahingon aiheuttamisen vuoksi.

6 JOHTOPÄÄTÖKSET JA POHDINTA

6.1 Taksonomian toimivuus

Tässä tutkimuksessa käsiteltiin yhteensä viittätoista tapausta, joista vain kolme loppujen lopuksi sopivat valittuun kyberterrorismin määritelmään. Vaikka luku saattaa ensisilmäyksellä vaikuttaa vähäiseltä, on hyvä muistaa, että suhteellisen yleisen käsityksen mukaan näitä tapauksia tulisi olla nolla, sillä kyberterrorismista ei monen tutkijan mukaan ole olemassa vielä ainakaan konkreettisia esimerkkejä. Plotnekin ja Slayn taksonomiaan sopivia tapauksia löydettiin kuitenkin, ja niiden ominaisuudet vastasivat suhteellisen hyvin määritelmän eri komponentteja.

Suurin rajaava tekijä, jonka perusteella toiminta päädyttiin rajaamaan kyberterrorismin määritelmän ulkopuolelle, oli sekä ainestoa kerätessä että sitä analysoitaessa toimijuus, mutta myös motiivi ja aikomus rajasivat hyvin monet kyberhyökkäykset määritelmän ulkopuolelle. Tapaukset, joissa motiivina toimi nimenomaan ideologinen tai sosiaalinen vaikutin olivat suhteellisen harvassa ja esimerkiksi voittoa tavoitteleva kyberrikollisuus rajautui näin ulkopuolelle. Toisaalta kyberhyökkäysten motiivit ovat usein päällekkäiset (Lemay & al. 2018) ja esimerkiksi tässäkin tutkimuksessa käsitellyissä Iranin vallankumouskaartin ja Holy Souls hakkeriryhmän iskuissa mukana oli myös taloudellisen hyödyn tavoittelun motiivi, sosiaalisen tai ideologisen yhteydessä. Taksonomia ei kuitenkaan sulje näitä päällekkäin motivoituneita tapauksia pois, ja mikäli sulkisi olisi käsiteltävien tapauksien määrä ollut huomattavasti vähäisempi.

Merkittävä ongelma, joka taksonomian käytössä havaittiin, on monen eri komponentin arviointiin liittyvä tulkinnanvaraisuus tai epävarmuus. Lähes kaikkien käsiteltyjen tapausten kohdalla jonkin komponentin kohdalla jouduttiin tekemään selvästi tutkijasta riippuvainen ja lähdemateriaaliin hatarasti perustuva tulkinta tai oletus siitä, mikä oli esimerkiksi teon motivaationa, tai voidaanko toimija määritellä valtiolliseksi vai ei-valtiolliseksi. Tähän syynä on

suuressa määrin käytetyn aineiston laatu, ja kenties viranomaislähteitä tai muita ei-julkisia dokumentteja mukaan ottamalla tulkinnanvaraisuudesta johtuvaa epävarmuutta voitaisiin vähentää. Kuitenkin tämänkaltainen ongelma on huomionarvoinen, sillä kybermaailman ilmiöitä ja tapahtumia tarkastellessa epävarmuus jonkin tapahtumaketjun osasta on varsin yleinen ilmiö ja on vaikea kuvitella tarkastelutilannetta, jossa kybertapahtumasta voitaisiin varmuudella ja täysin ilman tulkinnanvaraisuutta määrittää kaikkiin taksonomian komponentteihin vastaus. Lisäksi mallin komponenteista toiset havaittiin selvästi enemmän tulkinnanvaraisiksi kuin toiset, sillä esimerkiksi keinojen ja kohteiden analysointi edellyttää huomattavasti vähemmän tulkintaa tai arviointia kuin esimerkiksi aikomuksen tai motiivin.

Toinen esille nostettava komponentti on toimija. Tämän komponentin ongelmallisuutta käsiteltiin jo hieman luvussa 5.4. On kuitenkin syytä pohtia minkä vuoksi taksonomiassa on päädytty rajaamaan valtiolliset toimijat määritelmän ulkopuolelle, ja mitä seuraisi, mikäli tämä vaatimus poistettaisiin. Plotnek ja Slay artikkelissaan, jossa taksonomian esittelevät, mainitsevat että toimijan komponentiksi määriteltiin ei-valtiollinen, sillä se on tarpeeksi laaja mutta käyttökelpoinen kyberterrorismin määrittelyyn (Plotnek & Slay, 2021). Kuitenkin tässäkin tutkimuksessa tuli vastaan kybermaailmassa jatkuvasti yleistyvä haaste liittyen rajanvetoon valtiollisen ja ei-valtiollisen toimijan välille. Kuten aiemmin todettua, erot näiden toimijoiden välillä eivät ole selkeitä, ja valtiollista tukea yritetään usein kyberhyökkäyksissä tarkoituksellisesti peitellä (Ussath et al 2016). Lisäksi on mahdollista, että sama toimija toimii sekä valtiollisesti tuettuna, mutta myös täysin itsenäisesti operaation mukaan, joten tämän komponentin tulkinta voi muodostua erittäinkin haastavaksi. Tätä ongelmaa ei kuitenkaan tässä tutkimuksessa laajalti kohdattu, mutta mikäli taksonomiaa olisi tarkoitus käyttää laajemmin kyberterrorismin tunnistamiseen on huomioitava, että tämän komponentin määrittäminen voi vaatia huomattavasti työtä. Mielenkiintoinen jatkoajatus tästä on koko tämän komponentin poistaminen mallista. Tällöin mukaan tulisi, että valtiot voivat harjoittaa kyberterrorismia. Tämä ajatus on mielenkiintoinen, sillä aineiston keruussa vastaan tuli useita tapauksia, joissa valtiot syyttelivät toisiaan kyberterrorismista, tai ilmoittivat joutuneensa valtiollisesti tuetun kyberterrorismin kohteeksi. Nämä tapaukset eivät pääsääntöisesti kuitenkaan vastanneet muilta osin valittua kyberterrorismin määritelmää, mutta olisi mielenkiistoista tarkastella olisiko mahdollista löytää tapauksia, joissa voidaan selvästi tunnistaa valtion harjoittama kyberterrorismi. Ainoa asia mikä sulkee tämän pois nyt Plotnekin ja Slayn mallissa on juuri toimijan komponentti, sillä sekä keinot, kohde, motiivi, vaikutus ja aikomus ovat sovitettavissa myös valtiolliseen kybertoimintaan.

Kolmas ongelma, joka taksonomiassa tunnistettiin, mutta joka ei kuitenkaan merkittävästi vaikuttanut tämän tutkimuksen toteutukseen oli vaatimus, että ollakseen kyberterrorismia tulee toiminnan olla suoraan hyökkäyksen toteuttamista tai sen uhkaa lisäävää. Tämä rajaa merkittävän osan esimerkiksi tunnistettujen terrorijärjestöjen kybertoiminnasta määritelmän ulkopuolelle, sen ollessa joko viestintään tai rekrytointiin keskittyvää. Tähän ongelmaan ja siihen

miksei se kuitenkaan tässä tutkimuksessa ollut merkittävä haaste palataan luvussa 6.4.

Kaiken kaikkiaan Plotnekin ja Slayn tapa määritellä kyberterrorismia, vaikuttaa kuitenkin jokseenkin toimivalta sillä sekä määritelmään sopivia, että sen ulkopuolelle jääviä tapauksia löydettiin tässä tutkimuksessa. Merkittävä haaste liittyy kuitenkin myös luvussa 2 esitettyyn ongelmaan, eli kyberterrorismia on suhteellisen vaikea erottaa ideologisesti motivoituneesta hakkeroinnista, eli haktivismista. Tässä työssä esiteltyihin #OpSweden ja #OpAustralia hyökkäyskampanjoihin viitattiin lähdeaineistossa useimmiten juuri haktivismina ja erottelu tämän ilmiön ja kyberterrorismin välillä on hankalaa myös Plotnekin ja Slayn mallia käyttäen.

6.2 Kyberterrorismi - muutakin kuin hyökkäyksiä

Tämän tutkimuksen tarkoitus oli selvittää, voidaanko modernia kyberterrorismin käsitteistöä käyttäen tunnistaa lähihistoriasta tapauksia jotka, vastaisivat valitun määritelmän mukaista kyberterrorismia. Tätä tutkimusta ei kuitenkaan tule ymmärtää analyysiksi siitä, kuinka paljon kyberterrorismia tapahtuu, tai kuinka yleistä se on. Tutkimuksen aineistoon pyrittiin tarkoituksen mukaisesti keräämään tapauksia, jotka sekä sopisivat valittuun taksonomiaan, mutta myös sellaisia, jotka haastaisivat sitä. Tavoitteena oli nimenomaan testata, kuinka hyvin valitun määrittelytavan avulla voidaan luokitella tosimaailman tapauksia, ja voidaanko sen avulla tunnistaa kyberterroristisia tapahtumia. Vastaus tähän kysymykseen on varovainen kyllä. Kyllä siksi, sillä kuten edellisessä luvussa esiteltiin, havaittiin useita tapauksia, joissa kaikki Plotnekin ja Slayn kehittämän taksonomian komponentit voitiin tunnistaa valituista tapahtumista, mutta varovaisuus johtuu edellisessä luvussa esitellyistä haasteista tulkinnanvaraisuuden ja epävarmuuden suhteen. Joka tapauksessa tämän tutkimuksen perusteella vaikuttaa siltä, että kyberympäristössä todella tapahtuu kyberterrorismiksi miellettäviä tapahtumia, ja näitä voidaan jäsentää ja lähestyä Plotnekin ja Slayn käyttämää taksonomiaa hyödyntäen.

Vaikka tulos onkin näennäisen positiivinen, ei se silti tarkoita, että kyberterrorismiin liittyvässä tutkimuksessa oltaisiin lähellä läpimurtoa. Toinen tämän tutkimuksen tutkimuskysymyksistä oli, onko kyberterrorismi todellinen ilmiö, joka voidaan erottaa muista kyberuhista. Tässä kysymyksessä nimenomaan sivulauseessa oleva kysymys erottelusta nousi tärkeäksi. Kyberterrorismiin liittyvässä keskustelussa ei kirjallisuuskatsauksen perusteella niinkään ole ollut kysymys siitä onko kyberterrorismia olemassa, vaan enemmänkin juuri siitä miten se voidaan tehokkaasti tunnistaa ja erotella muista kybermaailman uhista (Kenney 2015). Vaikka tässä tutkimuksessa löydettiinkin yksittäisiä tapauksia, joiden voitiin määritellä olevan kyberterrorismia ei se tuota vastausta tähän ongelmaan. Se, että ilmiö voidaan määritellä kuuluvan tiettyyn kategoriaan ei tarkoita sitä, etteikö sama ilmiö voitaisi määritellä kuuluvan myös toiseen. Käytännössä siis, vaikka tässä tutkimuksessa onnistuttiinkin tunnistamaan ilmiöitä, jotka sopivat

kyberterrorismin määritelmään, ei tämä sulje pois mahdollisuutta, että nämä ilmiöt voisi mieltää esimerkiksi haktivismiksi tai valtiollisesti tuetuksi kyberrikollisuudeksi.

Moni käsitellyistä tapauksista, ainakin käytetyissä medialähteissä nimenomaan miellettiin haktivismiksi, ja kuten jo luvussa 2 todettiin, erottelu näiden kahden ilmiön välillä on vaikeaa. Tässä suhteessa myös Plotnekin ja Slayn malli jokseenkin epäonnistuu, sillä sen komponenteista vain yksi vaikuttaa tekevän merkittävää erottelua haktivismin ja kyberterrorismin välille: Samoin kuin kyberterrorismissa, myös haktivismissa voidaan nähdä olevan poliittinen tai ideologinen motiivi, sen toteuttajan toimii ei-valtiollinen toimija, keinona tyypillisesti on kyberympäristössä tapahtuva hyökkäys ja myös sekä vaikutuksen että kohteen komponentit ovat helposti sovitettavissa Plotnekin ja Slayn malliin. Ainoaksi erottelevaksi komponentiksi jää siis aikomus. Haktivismin tavoitteena ei välttämättä ole herättää pelkoa tai pakottaa toimintaan, mutta kuten edellisessä luvussa todettiin, juuri aikomuksen komponentti on mallin osista kaikkein hankalin, sillä sen kohdalla vaadittiin yleensä selvästi eniten tulkinnanvaraisuutta. Aikomus on luonteeltaan tyypillisesti ääneen lausumaton, ja parhaimmillaan se voi olla jopa tarkoituksenmukaisesti peitelty tehden sen objektiivisesta arvioimisesta hyvin hankalaa. Kun siis yksi merkittävimmistä haasteista on nimenomaan kyberterrorismin erottaminen haktivismista, ja Plotnekin ja Slayn mallissa sen tekeminen vaatii joko sisäpiirin tietoa tapahtumasta ja sen taustoista, tai jonkin verran tulkinnanvaraisuutta, voidaan mallin sanoa olevan melko huono erottelemaan näiden kahden ilmiön välillä. Tyypillisesti kirjallisuudessa näiden kahden ilmiön välille eroa tekee, joko toiminnan vakavuus tai sen seuraukset, jotka kyberterrorismissa ovat tyypillisesti väkivaltaan johtavia (Denning, 2007). Plotnekin ja Slayn mallissa näin ei kuitenkaan ole, sillä vaikutuksen komponentti jättää paljon avoimeksi tehden erottelusta haastavaa.

Olisi toki myös mahdollista ajatella, että kyberterrorismin ja haktivismin välinen erottelu ei todellisuudessa ole mikään ongelma: Kyseessä on kaksi hyvin samankaltaista toiminnan muotoa, joissa usein taustalla on samankaltainen motivaatio, joten kuinka tärkeää on pystyä erottelemaan ne määritelmällä toisistaan. Luvussa kaksi todettiin, miksi kyberterrorismin määrittely itsessään on tärkeää, ja periaatteessa kaikki samat syyt pätevät myös siihen, miksi sen toimiva erottelu haktivismista olisi tarpeen. Niin lainvalvonnan, kansainvälisen yhteistyön kuin myös akateemisen työn kannalta olisi erittäin hyödyllistä, mikäli keskustelua voitaisiin selkiyttää käyttökelpoisten ja yleisesti hyväksyttyjen käsitteiden avulla.

6.3 Miksi kyberterrorismia?

Tämän tutkimuksen tavoitteena ei niinkään ollut jäsentää mitä kyberterroristinen toiminta itsessään on, tai miksi sitä harjoitetaan. Kuitenkin aineistoa tarkastellessa voitiin tunnistaa muutamia selkeitä piirteitä, joko toiminnan muotoja tai sen syitä, jotka yleisesti liitetään oleellisesti kyberterrorismiin. Havainnoissa korostui etenkin paljon kirjallisuudessa esiin noussut teema kybertoiminnan

houkuttelevuudesta terroristisesti motivoituneelle toimijalle tai ryhmälle. Tyypillisesti kybertoiminnan on ajateltu olevan houkuttelevaa terroristille sen matalan kynnyksen ja edullisen toteutuksen myötä (Burak Bicak & Bogdanova, 2018, Kenney 2015). Tässäkin tutkimuksessa käsitellyt kyberterrorismiksi määritellyt tapaukset voidaan mieltää suhteellisen helposti ja edullisesti toteuttavaksi toiminnan muodoksi. Kirjallisuudessa (esim. Denning, 2000; Dogrul et al. 2011) kyberterrorismin eduiksi katsotaan myös sen maantieteellinen riippumattomuus, ja myös tämä sopii tässä tutkimuksessa tehtyihin havaintoihin. Tässä tutkimuksessa kyberterrorismiksi määritellyt tapaukset kaikki tapahtuivat huomattavan välimatkan päästä, lähes aina eri mantereelta kuin missä kohde sijaitsi. Vaikkakin globaali ilmiö sekin, perinteisen maailman terrorismi on kuitenkin yhä suhteellisen rajoittunut maantieteellisesti, ja etenkin länsimaissa onnistuneet terrori-iskut ovat yhä verraten harvinaisia (Chenoweth et al. s. 34-37). Kyberterrorismin kohdalla tämä on kuitenkin toisin, sillä tässäkin tutkimuksessa käsitellyistä kyberterrorismiksi miellettävistä tapauksista kaksi kolmesta (#OpSweden ja #OpAustralia) tapahtui länsimaaksi miellettävän valtion maaperällä. Lisäksi molemmat näistä tapauksista vastasivat yleistä käsitystä kyberterrorismin houkuttelevuudesta siten, että ne olivat todennäköisesti suhteellisen helppoja ja edullisia toteuttaa. Molemmissa kyse oli pääosin palvelunesto- tai hajautetusta palvelunestohyökkäyksestä, ja tämä hyökkäysmuoto ei edellytä sen enempää korkeaa teknologista osaamista kuin korkeaa budjettiakaan.

Ainoa kyberterrorismiksi mielletty tapaus, joka poikkeaa tässä suhteessa edullisesta ja helposti toteuttavasta on Iranin terästeollisuuteen kohdistettu iskusarja. Tässä tapauksessa iskun toteuttanut taho on verrattain korkean teknologisen osaamisen omaava ja todennäköisesti myös hyvin resursoitu. Mitään varsinaisia päätelmiä tästä ei voida tehdä, sillä kyse on yksittäistapauksesta muutenkin hyvin pintaraapaisuksi jäävässä tutkimuksessa, mutta on silti mielenkiintoista tarkastella sitä esimerkkinä siitä, minkälaisena kyberterrorismi voisi näyttäytyä taloudellisen panostuksen ja korkean osaamistason myötä.

Mielenkiintoinen tarkasteltava tapaus edullisuuden ja helppouden perspektiivistä on myös Charlie Hebdoon tehdyt iskut. Vaikkakin tässä tutkimuksessa vuoden 2023 kyberhyökkäys jäi kyberterrorismin määritelmän ulkopuolelle, on sitä silti mielenkiintoista tarkastella verraten sitä saman lehden aiemmin kokemaan fyysisen maailman terrori-iskuun. Vuoden 2015 fyysiseen terrori-iskuun verrattuna, sekä toiminnan motivaatio ja toteuttajat olivat jokseenkin samoja. Molemmissa tapauksissa lehden toiminta oli islamilaisessa maailmassa koettu loukkaavana, ja vastauksena lehteen kohdistettiin aggressiota. Luonnollisesti, toiminnan laatu, vaikutukset ja vakavuus olivat merkittävästi erilaiset, ja on mielenkiintoista, pohtia miksi vastaus oli tuoreemmassa tapauksessa niin erilainen. Eräs mahdollinen selitys tähän on, että fyysisen maailman terrori-iskun suorittaminen Ranskassa vaikuttaa muuttuneen huomattavasti vuoden 2015 jälkeen. [8] Ensimmäinen Charlie Hebdo isku toimi Ranskassaa eräänlaisena

[8] https://www.france24.com/en/france/20210905-how-the-november-2015-attacks-marked-a-turning-point-in-french-terror-laws

laukaisimena lakimuutoksiin, ja entistä suurempaan resurssipanostukseen kotimaan terrorismin torjuntaan liittyen. On siis mahdollista, että Charlie Hebdoon liittyvän kostoiskun siirtyminen fyysisestä maailmasta kyberiin kuvaa sitä, miten terroristisesti motivoituneet toimijat ovat joutuneet etsimään uusia toimintatapoja perinteisten muuttuessa haastavimmiksi. Toisaalta ilmiön voi yhtä hyvin tulkita olevan esimerkki siitä, miten nykyään voidaan huomattavasti helpommin ja pienemmällä riskillä toteuttaa ideologisesti motivoituneita kostoiskuja.

Tässä tutkimuksessa tehtyjen havaintojen perusteella vaikuttaa siis siltä, että tutkimuskirjallisuudessa esiintyneet syyt terroristisen kybertoiminnan nousuun ja ennakoinnit sen entistä suuremmasta roolista tulevaisuudessa vaikuttavat pitävän paikkansa. Kyberiskujen suorittaminen terroristisin motivaatioin on helpompaa, siihen liittyy pienempi kiinni jäämisen riski ja se voidaan toteuttaa mistä päin maailmaa tahansa. Vaikka tämä havainto ei sinänsä ole uusi, on se oleellinen. Tämä siksi, että sen tekeminen tässä tutkimuksessa vahvistaa käsitystä, että vaikka kyberterrorismin määrittelemiseen liittyy vielä merkittäviä haasteita, ilmiön itsensä ymmärtäminen ja terroristisen kybertoiminnan taustat ovat suhteellisen hyvin ymmärretty tutkimuskirjallisuudessa. Luvussa 2 käsiteltiin sitä, miten viimeisen vuoden aikana ideologisesti motivoitunut kybertoiminta on merkittävästi kasvanut, ja vaikka vielä ei kenties voidakaan puhua vastaavasta räjähdyksestä kyberterrorismiksi määriteltävässä toiminnassa, on myös tämän mahdollisuus tunnistettava. Kyberhyökkäykset vaikuttavat nykyään saavan enemmän huomiota osakseen kuin aiemmin, ja tämä voi houkutella myös terroristisesti motivoituneet toimijat hakemaan huomiota tai pyrkimään pelon herättämiseen kohteissaan kyberiskun keinoin. Kasvavan huomion voi myös arvioida vaikuttavan siihen miten suuri potentiaalinen pelotevaikutus onnistuneella kyberhyökkäyksellä voi olla.

On mahdollista, että tulevaisuudessa nimenomaan pelon herättäminen korostuukin terroristisesti motivoituneiden toimijoiden kyberoperaatioissa. Aiempi ajatus terroristien tavoittelemasta fyysisestä vahingosta tai ihmisuhreista vaikuttaa muuttuvan yhä hankalammin saavutettavaksi ja siten epätodennäköiseksi. Tässä tutkimuksessa havaittiin vain yksi tapaus, jossa kyberhyökkäyksellä onnistuttiin aiheuttamaan fyysistä vahinkoa, ja kyberterrorismin ulkopuolellakin tarkasteltuna tämänkaltaiset tapaukset ovat harvinaisia (Agrafiotis et al. 2018). Lisäksi, kuten tässäkin tutkimuksessa käsitellyn Iranin terästeollisuuteen kohdistuneen iskun kohdalla havaittiin, fyysistä vahinkoa tuottavan iskun toteuttaminen vaatii yleensä suhteellisen korkeaa teknologista osaamistasoa, suunnittelua ja resursseja toteuttajaltaan. Tämä vaatimus oleellisesti poikkeaa niistä luetelluista hyödyistä, joita kyberympäristön hyödyntämisellä terroritoiminnassa on todettu olevan.

Kyberhyökkäysten potentiaalia fyysisen vahingon aiheuttamiseen on muutenkin alettu arvioimaan uudestaan. Huhtikuussa 2023 pidetyssä Atlantic Councilin paneelikeskustelussa *On Melding cyber and kinetic conflict* [9]käsiteltiin sitä,

[9] https://www.youtube.com/watch?v=y3aYKSMjHfQ luettu 26.06.2023

miten vuonna 2022 alkanut Ukrainan konflikti on muuttanut käsitystä siitä, mitä kyberhyökkäyksillä voidaan sodan kontekstissa saavuttaa. Vaikka päähuomio keskustelussa onkin kyberympäristön käyttö osana valtioiden välistä konfliktia, on osa nousseista ajatuksista laajennettavissa koskemaan myös poliittisesti tai ideologisesti motivoituneita kyberhyökkäyksiä. Eräs teema, josta asiantuntijat tuntuivat olevan samaa mieltä, oli että kyberhyökkäykset eivät loppujen lopuksi vaikuta olevan kovinkaan tehokkaita pysyvästi vaurioittamaan tai tuhoamaan kohteitaan. Kyberhyökkäysten päähyöty on hetkellisten toimintakatkojen aiheuttamisessa, ja niihin usein liitetään myös merkittävä informaatiovaikuttamistavoite. Alun perin Denningin esittämä ajatus siis siitä (Denning, 2000), että jotta voitaisiin puhua kyberterrorismista, täytyy kyberhyökkäyksen myötä syntyä joko pysyvää fyysistä vahinkoa henkilöihin tai asioihin näyttää entistä kaukaisemmalta. Tästä fyysisen vahingon vaatimuksesta onkin sittemmin näennäisesti luovuttu pääosassa kyberterrorismia määrittelemään pyrkivässä kirjallisuudessa, ja se vaikuttaa järkevältä ratkaisulta (Plotnek & Slay, 2021). Luonnollisesti ei voida sulkea pois mahdollisuutta kyberterrori-iskusta, jonka myötä fyysistä vahinkoa tapahtuisi tai joka jopa johtaisi ihmishenkien menetykseen, mutta tätä voidaan yhä pitää suhteellisen epätodennäköisenä.

6.4 Tutkimuksen haasteet ja rajoitteet

Selkein tämän tutkimuksen ongelma liittyy käytössä olevaan lähdemateriaaliin. Tutkimuksessa käytettiin yksinomaan julkisista lähteistä saatavilla olevaa materiaalia, ja tämän myötä joidenkin tapauksien arvioinnin kohdalla jouduttiin turvautumaan verrattain vahvasti tulkintaan, toisen käden tietoon tai olettamuksiin. Mikäli käytössä olisi ollut kaikki saatavilla oleva materiaali eri tapauksista, olisi niiden arviointi voinut olla huomattavasti helpompaa. Esimerkiksi kyberhyökkäyksen motivaatiota tai aikomusta voi olla helpompi arvioida, jos on suora pääsy esimerkiksi hyökkääjän ja uhrin väliseen viestinvaihtoon, tai forensiikkadataa analysoimalla on mahdollista tarkemmin arvioida toimijan valtiollista tukea tai sen puutetta. Tämän tutkimuksen ei kuitenkaan ollut tarkoitus tarkasti pyrkiä määrittelemään tapauksia kyberterrorismin käsitteeseen sopivaksi tai sen ulkopuolelle jääviksi, vaan tavoitteena oli pikemminkin testata valitun määrittelytavan toimivuutta ja siihen liittyviä ongelmia. Lähteiden rajoittavuus ei siis sikäli ollut merkittävä ongelma tämän tutkimuksen tavoitteiden kannalta kovinkaan merkittävä, mutta taksonomian toimivuutta arvioitaessa on hyvä ottaa huomioon, että sen käyttöä testattiin tässä tutkimuksessa varsin rajattuun lähdemateriaaliin perustuen.

Toinen merkittävä rajoite tässä tutkimuksessa on jo aineiston keräystä aloitettaessa tehty tietoinen valinta, että kyberterrorismia käsiteltiin vain tapahtuneiden iskujen kautta. Kuten sekä viranomaiset (Suojelupoliisi, 2022) että akateemikot ovat todenneet, tällä hetkellä merkittävin kyberympäristön käyttötapa terroristeille on rekrytointi tai viestintä (Kenney 2015, ks. myös Putra 2016). Tässä tutkimuksessa ei kuitenkaan käsitelty mitään kyberhyökkäysten ulkopuolista

toimintaa. Tähän oli jälleen pääosin syynä käytössä oleva lähdemateriaali, mutta on syytä myös ottaa huomioon, että valittu kyberterrorismin määritelmä käytännössä sulkee tämänkaltaisen toiminnan käsitteen ulkopuolelle. Plotnekin ja Slayn mallissa kyberterrorismin keinon, eli toteutustavan on oltava kybermaailmassa tapahtuva hyökkäys, tai sen uhka, ja mikäli esimerkiksi tunnistetun terroriorganisaation viestinnän tai rekrytoinnin ei ajatella suoraan tuottavan kyberhyökkäyksen uhkaa jää se kyberterrorismin määritelmän ulkopuolelle. Mikäli tämänkaltainen toiminta haluttaisiin siis sovittaa Plotnekin ja Slayn mallin mukaiseen kyberterrorismiin, tulisi käytännössä kaiken terroristisesti motivoituneiden toimijoiden kybertoiminta mieltää suoraan itse hyökkäyksen uhkaa kohottavaksi. Lisäksi määritelmän mukaisesti hyökkäyksen pitäisi tapahtua nimenomaan kyberympäristössä, joten esimerkiksi terroristisolujen välinen salattu viestintä kyberympäristöä hyödyntäen jäisi joka tapauksessa määritelmän ulkopuolelle. Toisaalta taksonomia onkin nimenomaan tarkoitettu kyberhyökkäysten tarkasteltuun. Lisäksi tyypillisesti myös perinteisestä terrorismista puhuttaessa toiminta itse terroristisen toiminnan ajatellaan olevan juuri hyökkäysten toteuttamista tai niiden valmistelua (Chenoweth et al. s. 34-37). Kuitenkin on hyvä huomioida, että tässä tutkimuksessa käytetty taksonomia soveltuu huonosti kaiken terrorismiin liittyvän kybertoiminnan tarkasteluun, vaikka sitä onkin mahdollisuus hyödyntää kyberterrori-iskujen tai -operaatioiden lähestymisessä.

Kuten aikaisemmin todettua, tätä tutkimusta tai sen tuloksia ei tule ymmärtää tilastolliseksi tarkasteluksi kyberterrorismin yleisyydestä, tai edes tarkaksi selvitykseksi siitä ovatko käsitellyt tapaukset loppujen lopuksi kyberterrorismia vai ei. Päätavoite oli testata valittua määrittelytapaa, ja tästä johtuen myös aineiston keruuta ohjasi tavoite saada kokoon homogeeninen ja määritelmää haastava kirjo tapauksia. Tämä johti myös usean merkittävän ja paljon huomiota saaneen tapauksen jättämiseen analyysin ulkopuolelle, pienempien mutta joiltain osin paremmin tähän tutkimukseen sopivien tapausten edeltä. Tästä syystä tutkimusta ei tule ymmärtää analyysiksi siitä kuinka paljon kyberterrorismia on tapahtunut viimeisen vuoden aikana, sillä otanta tutkimukseen on ollut valikoivaa.

6.5 Jatkotutkimus

Kuten tämän tutkimuksen luvussa 4 mainittiin, kyberterrorismi on ilmiö, joka on saanut osakseen jonkin verran akateemista huomiota. Kuitenkin, mikäli tilannetta verrataan vuosituhannen alkuun, jolloin termin käyttö alkoi yleistyä, ei vaikuta siltä, että yleisesti hyväksytyn määritelmän muodostamisessa ei ole juurikaan päästy eteenpäin. Toisaalta, vaikka yleinen määritelmä vielä puuttuukin, on ilmiön ymmärtäminen selvästi kehittynyt vuosikymmenten kuluessa ja akateemisen työn edetessä. Missään tapauksessa ei siis tehtyä työtä tule ajatella turhaksi, vaikka varsinaisen maalin saavuttaminen vaikuttaakin vielä kaukaiselta. Tulevaisuudessa tutkimustyötä kyberterrorismin parissa tuleekin siis jatkaa, sillä kuten useaan kertaan todettua, ilmiön määrittelyn kehittyminen helpottaa sen käsittelyä sekä akateemisessa maailmassa että sen ulkopuolella. Eräs

mahdollisuus on edelleen jatkaa tässä työssä käsitellyn Plotnekin ja Slayn taksonomian kehittämistä. Tässä tutkimuksessa taksonomia osoittautui selvästi toimivaksi, mutta ongelmalliseksi todettuja komponentteja muokkaamalla voitaisiin viitekehystä kenties parantaa entisestään. Selvitystä tulisi etenkin tehdä, voidaanko toimijan komponentti laajentaa sisältämään myös valtiollisesti tuetut toimijat. Kenties liian avoimen määritelmän välttämiseksi esimerkiksi valtioiden viralliset viranomaistahot voidaan yhä jättää ulkopuolelle, jotta vältytään tilanteelta, että liian monet valtioiden kyberoperaatiot ymmärretään kyberterrorismiksi.

Taksonomian suhteen olisi erittäin hyödyllistä, mikäli sitä voitaisiin muokata suuntaan, jossa tulkinnanvaraisuus tai epävarmuus määrittelyssä vähentyisi. Tämä ei kuitenkaan ole helppo ongelma ratkaistavaksi, sillä loppujen lopuksi itse taksonomian sijaan, se kenties johtuu enemmänkin kybermaailman operaatioiden tarkasteluun yleisesti liittyvästä vaikeatulkintaisuudesta. Mahdollinen jatkotutkimuskohde on kuitenkin, voidaanko eri komponenttien sisältöä muokkaamalla vähentää tulkinnanvaraisuutta taksonomian käyttöön liittyen.

Eräs tutkimuslinja, joka tällä hetkellä vaikuttaa kyberterorrismin suhteen saaneen vielä suhteellisen vähäistä huomiota on itse iskujen, kampanjoiden ja operaatioiden ympärillä tapahtuva kybertoiminta. Monessa lähteessä on todettu terroristien tällä hetkellä hyödyntävän kyberympäristöä pääosin muuhun kuin varsinaisten iskujen toteuttamiseen, mutta tätä toimintaa käsitteleviä tutkimuksia ei ole paljoa. Toisaalta ymmärrettävästi tämänkaltaiseen tutkimukseen voi olla varsin hankala hankkia lähdemateriaalia, mutta tutkimuslinjana se on silti mielenkiintoinen ja sen seuraaminen voisi avartaa käsitystä siitä, mihin kaikkeen terroristisesti motivoitunut toimija voi kyberympäristöä hyödyntää.

Lopuksi todettakoon vielä, että tulevaisuuden tutkimuksissa ja etenkin kyberterrorismin määrittelyyn keskittyvässä työssä on tämän tutkimuksenkin perusteella järkevää luopua vaatimuksesta, että ollakseen todellinen ilmiö tulee kyberterrorismin johtaa fyysisen maailman väkivaltaan. Kyberympäristön on todettu olevan varsin monimuotoinen kenttä, jossa tehtävillä operaatioilla on vaihtelevia ja ei läheskään aina kybermaailman ulkopuolelle kantautuvia tavoitteita ja seurauksia. Mikäli kyberterrorismin tutkimus keskittyy fyysisten seurausten ympärille, on riskinä se, että paljon toiminnasta jää huomioimatta. Kyberhyökkäysten vaikutus usein jää joko pelkästään kyberympäristön sisälle, tai niiden leviäminen ulkopuolelle ei johda suoriin fyysisiin seurauksiin. Tässäkin työssä esimerkiksi havaittiin, kuinka usean kyberterrorismin määritelmään sopivan tapauksen taustalla vaikutti tavoite pelon ja huomion herättämiseen, ja tähän kybermaailman iskut vaikuttavat soveltuvan hyvin.

LÄHTEET

Abdulrahman Alqahtani. (2015). "Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: A quantitative study." Information & Computer Security, 23(5), 532-569.

Agrafiotis Ioannis, Nurse Jason, Goldsmith Michael, Creese Sadie & Upton David. (2018). "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate" Journal of Cybersecurity, Volume 4, Issue 1, 2018

Al mazari Ali, Anjariny Ahmed, Habib Shakeel, & Nyakwende Emmanuel. (2015). "Cyber terrorism taxonomies: Definition, targets, patterns and mitigation strategies" European Conference on Information Warfare and Security, ECCWS, 2015, 11-18.

Blannin Patrick. (2017). "Islamic State's Financing: Sources, Methods and Utilisation." Counter Terrorist Trends and Analyses, vol. 9, no. 5, 2017, pp. 13–22. JSTOR

Burak Bicak Melih, & Bogdanova Daria. (2018). "Fighting cyber terrorism: Comparison of turkey and russia." Paper presented at the - 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), 98-101.

Chaturvedi Manmohan, Unal Aynur, Aggarwal Preeti, Bahl Shilpa & Malik Sapna. (2014). "International cooperation in cyber space to combat cyber crime and terrorism." Paper presented at the - 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW), 1-4.

Chen Ping, Desmet Lieven & Huygens Christophe. (2014). "A Study on Advanced Persistent Threats" Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science, vol 8735. Springer, Berlin, Heidelberg.

Chenowth Erica, English Richard, Gofas Andreas & Kalyvas Stahis. (2019). "The Oxford Handbook of Terrorism" Oxford: Oxford University Press 2019

D'Amato Silvia. (2019). "Islamization of criminal behaviour: The path to terrorism? Terrorist threat and crime in French counterterrorism policy-formulation" European Journal of Criminology, 16(3), 332–350.

Denning Dorothy. (2000). "Information Warfare And Security" AddisonWesley Professional.

Denning Dorothy. (2001). "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, eds., *Networks and Netwars* (Santa Monica, Calif.: RAND, 2001), p. 241.

Denning Dorothy. (2007). “A view of cyberterrorism five years later” Internet Security: Hacking, Counterhacking, and Society, Jones and Bartlett, London (2007), pp. 123-140

Dogrul Murat, Aslan Adil, & Celik Eyyup. (2011). “Developing an international cooperation on cyber defense and deterrence against cyber terrorism.” Paper presented at the - 2011 3rd International Conference on Cyber Conflict, 1-15.

Endy Charles lim, Eng Kho & Nugroho Anto. (2010). “Implementation of intelligent searching using self-organizing map for webmining used in document containing information in relation to cyber terrorism” Paper presented at the - 2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies, 195-197.

Kenney Michael. (2015). “Cyber-terrorism in a post-stuxnet world” Orbis, 59(1), 111-128.

Lewis James. (2002). “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats” Center for Strategic and International Studies (2002)

Liang Christina. (2017). “Unveiling the "united cyber caliphate" and the birth of the E-terrorist” Georgetown Journal of International Affairs, 18(3), 11-20.

Limnéll Jarno. (2015). “The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War” International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(4): 521-532 521 The Society of Digital Information and Wireless Communications, 2015

Lehto Martti, Limnéll Jarno, Innola Eeva, Pöyhönen Jouni, Rusi Tarja & Salminen Mirva. (2017). ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saa-vuttamiseksi.” Valtioneuvoston selvitys- ja tutkimustoi-minnan julkaisusarja 30/2017. Valtioneuvoston kanslia; 2017.

Lehto Martti. (2022). “Cyber-Attacks Against Critical Infrastructure” kirjassa Lehto M. & Neittaanmäki P. (Edit.) Cyber Security -Critical Infrastructure Protection, Springer, Barcelona, 2022. ISBN 978-3-030-91292-5

Lemay Antoine, Calvet Joan, Menet François & Fernandez José. (2018). “Survey of publicly available reports on advanced persistent threat actors” Computers & Security, Volume 72, 2018, Pages 26-59, ISSN 0167-4048,

Mantel Barbara. (2009). "Terrorism and the internet. Should web sites that promote terrorism be shut down?." CQ researcher 3.1 (2009): 285-310.

Papathanasaki Maria, Dimitriou Georgios, Maglaras Leandros., Vasileiou Ismini & Janicke Helge. (2020). “From cyber terrorism to cyber peacekeeping: Are we there yet?” arXiv Preprint arXiv:2010.07041

Perkins Robert, Ouellet Marie, Howell Jordan & Maimon David. (2023). The Illicit Ecosystem of Hacking: A Longitudinal Network Analysis of Website Defacement Groups. Social Science Computer Review, 41(2), 390–409.

Plotnek Jordan & Slay Jill. (2021). “Cyber terrorism: A homogenized taxonomy and definition” Computers & Security, Volume 102, 2021, 102145, ISSN 0167-4048,

Putra Muhammad Deri. (2016). “New Media and Terrorism: Role of the Social Media to Countering Cyber Terrorism and Cyber Extremism for Effective Response” (March 24, 2016) Available at SSRN: https://ssrn.com/abstract=2754370 or http://dx.doi.org/10.2139/ssrn.2754370

Raggard Bel, G. (2010). “Information security management : Concepts and practice.” Boca Taylor & Francis.

Rikoslaki 2021/281 34a § 6 https://www.finlex.fi/fi/laki/alkup/2021/20210281

Suojelupoliisi. (2022.) Kansallisen turvallisuuden katsaus 2021. Suojelupoliisi

Tuomi Jouni & Sarajärvi, Anneli. (2018) ”Laadullinen Tutkimus Ja Sisällönanalyysi. Uudistettu laitos.” Helsinki: Kustannusosakeyhtiö Tammi, 2018

Ussath Martin, Jaeger David, Cheng Feng & Meinel Chrirstopher. (2016). "Advanced persistent threats: Behind the scenes," *2016 Annual Conference on Information Science and Systems (CISS)*, Princeton, NJ, USA, 2016, pp. 181-186

Valtioneuvosto. (2013). Suomen kyberturvallisuusstrategian taustamuistio. Forssa: Turvallisuuskomitean sihteeristö.

Viestintävirasto. (2018). ”KYBERTURVALLISUUDEN SANASTO” Sanastokeskus TSK ry 2018

Vu Anh, Thomas Daniel, Collier Ben, Hutchings Alice, Clayton Richard & Anderson Ross. (2022). “Getting Bored of Cyberwar: Exploring the Role of Civilian Hacktivists in the Russia-Ukraine Conflict” University of Cambridge, University of Strathclyde, University of Edinburgh. arXiv:2208.10629v4 [cs.CR] 16 Jun 2023

Weimann, Gabriel. (2014) “Cyberterrorism: the sum of all fears?” Stud. Conflict Terrorism, 28 (2) (2004), p. 130,

Wu Chunying & Wang Juan. (2019). “Analysis of cyberterrorism and online social media.” Paper presented at the 4th International Conference on Modern Management, Education Technology and Social Science (MMETSS 201, 925-927.

Zhang Lefeng, Zhu Tianqing, Hussain Farooksh Khadeer, Ye Dayong & Zhou Wanlei. (2023) "A Game-Theoretic Method for Defending Against Advanced Persistent Threats in Cyber Systems," in *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1349-1364, 2023,

VERKKOLÄHTEET & KUVIOT

Bureau of Counterterrorism: Foreign Terrorist Organizations https://www.state.gov/foreign-terrorist-organizations/ luettu 23.05.2023

Microsoft: DRAFT WHITE PAPER: An attribution model for influence operations https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/02/DTAC-Attribution-Framework.pdf. luettu 22.08.2023

France24: "How the November 2015 attacks marked a turning point in French terror laws" Issued on: 05/09/2021 https://www.france24.com/en/france/20210905-how-the-november-2015-attacks-marked-a-turning-point-in-french-terror-laws luettu 22.06.2023

Kuvakaappaukset Anynomous Sudan ja Team_insane hakkerijengien sosiaalisen median kanavilta https://socradar.io/hacktivism-on-the-rise-killnet-anonymous-sudans-cyber-campaign-targets-australia ja https://www.radware.com/security/threat-advisories-and-attack-reports/opaustralia-opsjentik/ haettu 23.05.2023

Kuvakaappaus Ghost Killer hakkeriryhmän Twitter-julkaisusta. https://twitter.com/thtghostkiller/status/1638259824432410655 haettu 22.05.2023

Kuvakaappaus Charlie Hebdon julkaisemasta ilmoituksesta piirustuskilpailusta. https://web.archive.org/web/20230109230442/https:/charliehebdo.fr/mullahsgetout-international-competition/ haettu 22.05.2023

Kuvakaappaus Holy Souls ryhmän viestistä BreachForums keskustelupalstalla. https://web.archive.org/web/20230109230105/https:/breached.vc/Thread-Personal-information-of-230000-customers-of-charliehebdo-fr haettu 22.05.2023

Kuvakaappaus Predatory Sparrow ryhmän viestistä hyökkäyksen jälkeen https://www.nejatngo.org/en/posts/14305, haettu 26.05.2023.