Tommi Laari

KYBERTERRORISMIN UHKA EUROOPASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Laari, Tommi
Kyberterrorismin uhka Euroopassa
Jyväskylä: Jyväskylän yliopisto, 2018, 80 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Kyberterrorismi on nimetty yhdeksi maailman vakavimmista tulevaisuuden turvallisuusuhkista. Terrorihyökkäykset Euroopassa ja taistelu terroristijärjestö ISIS:iä vastaan ovat lisänneet kyberterrorismin saamaa huomiota Euroopassa ja lisääntyneen huomion myötä kyberterrorismin käsite on muuttunut vaikeammin ymmärrettäväksi. Tämän tutkimuksen tavoitteena on ollut selittää kyberterrorismia, sen muodostamaa uhkaa ja sitä, millaisena tämä uhka koetaan eurooppalaisten valtioiden näkökulmasta. Tutkimuksen päätutkimuskysymyksenä on ollut: Millaisena uhkana kyberterrorismia pidetään Euroopassa?

Tutkimus on toteutettu laadullisena tutkimuksena. Tutkimuksessa kyberterrorismia on pyritty kuvaamaan mahdollisimman kokonaisvaltaisesti ja tutkijan parhaan ymmärryksen mukaan. Lähdeaineistoa on analysoitu aineistolähtöisen sisällönanalyysin avulla. Rajauksina tutkimuksessa on keskitytty alueellisesti Eurooppaan ja lähdemateriaalin osalta on pyritty käyttämään maksimissaan kymmenen vuotta vanhaa materiaalia.

Tutkimuksen tärkeimpinä johtopäätöksinä voidaan todeta, että kyberterrorismia pidetään hyvin mahdollisena, mutta ei kovinkaan todennäköisenä uhkana Euroopassa. Yleisesti hyväksyttyä määritelmää kyberterrorismille ei ole olemassa, ja sen käyttämistä on pyrittävä välttämään aina, kun mahdollista. Käsitteen ristiriitaisuus ei kuitenkaan poista sitä tosiasiaa, että kyberterrorismi on yksi kybertoimintaympäristön merkittävistä uhkista. Vaikkakin terrorismi on voimakkaasti esillä jokapäiväisessä uutisoinnissa, eurooppalaisten valtioiden kyberturvallisuusstrategioissa terrorismia ja kyberterrorismia käsitellään hyvin rajatusti. Viime vuosina tapahtuneet terrori-iskut ovat saaneet viranomaiset kuitenkin huolestumaan entistä enemmän tästä terrorismin kehittyvästä osa-alueesta, kyberterrorismista.

Asiasanat: kybertoimintaympäristö, kyberturvallisuus, terrorismi

ABSTRACT

Laari, Tommi
Threat of Cyberterrorism in Europe
Jyväskylä: University of Jyväskylä, 2018, 80 p.
Information Systems, Master's Thesis
Supervisor: Lehto, Martti

Cyberterrorism has been named one of the world's most serious security threats in the future. Terrorist attacks in Europe and the struggle against the terrorist organization ISIS have increased the attention of cyber terrorism in Europe and as a result of increased attention the concept of cyber terrorism has become more difficult to understand. The aim of this study was to explain the cyberterrorism, the threat it poses, and how this threat is perceived from the point of view of European states. The main research question has been: What kind of threat is cyber terrorism in Europe?

The research has been carried out as a qualitative study. The aim of the study is to describe the cyberterrorism as comprehensively as possible and according to the best understanding of the researcher. The source material has been analyzed by means of content-based content analysis. As a limitation, the research has focused on Europe on a regional basis. Also the aim for the research has been using material of no more than ten years old for the source material.

As main conclusions of the study, it can be said that cyberterrorism is considered a very potential, but not a very likely threat to Europe. A generally accepted definition of cyber terrorism does not exist and its use must be avoided wherever possible. However, the contradiction of the concept does not eliminate the fact that cyber terrorism is one of the major threats of the cyberspace. Though terrorism is strongly exposed in daily news coverage, terrorist and cyber terrorism in the European states' cybersecurity strategies is handled very narrowly. However, terrorist attacks in recent years have led the authorities to worry more about this emerging terrorist sector, cyberterrorism.

Keywords: cyberspace, cybersecurity, terrorism

KUVIOT

SISÄLLYS

1 KYBERTERRORISMIN UHKA JA HAASTEET

1.1 Aihepiirin kuvaus ja keskeiset käsitteet

Maailman johtavat valtiot ovat nimenneet kyberterrorismin yhdeksi lähitulevaisuuden vakavimmaksi turvallisuusuhkaksi (HM Government, 2015), (Clapper, 2016). Viimeaikaisten, eri puolilla maailmaa tapahtuneiden terrorihyökkäysten sekä taistelun The Islamic State of Iraq and the Levant (ISIL)/ISIS -järjestöä vastaan arvioidaan lisänneen kyberterrorismin uhkaa. Silti toisaalla on esitetty voimakkaita väitteitä siitä, että kyberterrorismi ei ole realistinen uhka lainkaan ja sen vakavuutta liioitellaan (Veerasamy & Grobler, 2015). Tämän kaltaisen keskustelun myötä kyberterrorismi on saanut osakseen lisääntyvän määrän huomiota, ja samanaikaisesti koko kyberterrorismin käsite on muuttunut yhä vaikeaselkoisemmaksi ja helpommin väärin ymmärretyksi.

Swansean yliopiston tutkija Andrew Whiting esitteli vuonna 2013 kyberterrorismia käsittelevässä konferenssissa näkemyksensä siitä, että vaikkakin kyberterrorismi on käsitteenä tullut yhä tunnetummaksi viime vuosien aikana, on käsitteen sisältö muuttunut yhä kiistanalaisemmaksi (MacDonald, Jarvis & Chen, 2013). Kyberhyökkäykset aiheuttavat edelleen vain harvoin fyysisiä vahinkoja ja näin ollen niiden käyttö terrori-iskuissa on ollut vähäistä. (Denning, 2011). On myös väitetty, että kyberterrorismin uhka ei ole todellinen, koska ei ole olemassa tunnettuja tai kirjattuja tapauksia, joissa informaatioteknologian avulla olisi aiheutettu hengenvaaraan tai kuolemaan johtaneita tilanteita. (Veerasamy & Grobler, 2015).

Toisaalta on arvioitu, että kyberterrorismin lisääntyminen ja sen myötä lisääntynyt julkisuus uhkaavat mitätöidä informaatioteknologian kehityksen mukanaan tuomia hyötyjä, mikäli tähän ei varauduta asianmukaisesti (Samuel, Osman, Al-Khasawneh & Duhaim, 2014). Vuonna 2015 julkaistussa Iso-Britannian kansallisessa turvallisuusstrategiassa sekä kyber että terrorismi olivat nimetty kuuden suurimman lähitulevaisuuden uhkan joukkoon. (HM Government, 2015)

Tämän tutkimuksen keskeisimpiä käsitteitä ovat kybertoimintaympäristö, kyberterrorismi ja kyberturvallisuusstrategia. Kybertoimintaympäristö (englanniksi cyberspace) muodostaa perustan tutkimuksen toteutukselle. Kybertoimintaympäristöstä puhuttaessa tarkoitetaan monimutkaista ja -kerroksista informaatioverkostoa, johon kuuluu kansallisia julkishallinnon, yritysmaailman ja turvallisuusviranomaisten tiedonsiirtoverkkoja, informaatiojärjestelmiä ja digitaalisia palveluita ja -palvelualustoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta- ja ohjausjärjestelmiä. Nämä järjestelmät ja palvelut muodostavat internetin välityksellä maailmanlaajuisen verkoston, joka tässä tutkimuksessa ymmärretään kybertoimintaympäristönä. (Lehto, ym., 2017). Tarkemmin kybertoimintaympäristöä on tarkastelu tutkimuksen luvussa kaksi.

Kyberterrorismi (englanniksi cyberterrorism) on tämän tutkimuksen avainkäsite. Sen määrittely on hyvin haastavaa ja tähän problematiikkaan on paneuduttu tarkemmin tutkimusraportin luvussa neljä. Tässä tutkimuksessa kyberterrorismi on yksilöiden tai ryhmien kybertoimintaympäristössä tai sen avulla harjoittamaa poliittisesti, uskonnollisesti tai ideologista motivoitua väkivaltaa häiriön, tuhon ja pelon saavuttamiseksi kohteissaan.

Tutkimuksen kolmas keskeinen käsite on kyberturvallisuusstrategia (englanniksi cyber security strategy). Kyberturvallisuusstrategioita on tarkastelu tutkimusraportin luvussa viisi. Kansalliset kyberturvallisuusstrategiat ovat työkaluja, joiden avulla pyritään parantamaan valtion ja yhteiskunnan turvallisuutta sekä lisäämään valtion palveluiden ja infrastruktuurin sietokykyä. Kyberturvallisuusstrategia on ylätason lähestymistapa kyberturvallisuuteen ja se muodostaa strategisen viitekehyksen valtioiden kyberturvallisuudelle (ENISA, 2012).

1.2 Tutkimuksen motiivit

Tutkimuksen motiivina on tutkia aiemman koulutuksen ja ammattiosaamisen pohjalta ajankohtaista ja mielenkiintoista aihealuetta oman ammattitaidon ja ymmärryksen lisäämiseksi. Tutkimusaiheena kyberterrorismi on herättänyt kiinnostusta muuallakin, mikä on näkynyt kyberterrorismi käsitteen saaman julkisuuden lisääntymisenä. Lisäksi tutkimuksen aihealueesta on olemassa riittävästi, mutta ei kuitenkaan liikaa, lähdemateriaalia, jonka avulla laadukkaan tutkimuksen läpivieminen on mahdollista.

Tutkimusaiheena kyberterrorismi on mielenkiintoinen myös sen takia, että kybertoimintaympäristö on erittäin houkutteleva toimintakenttä tulevaisuuden terroristeille. Kyberterrorismi ei välttämättä edellytä oman henkensä uhraamista aatteen vuoksi ja jopa kiinni jäämisen riski on hyvin laadituissa teoissa suhteellisen pieni. Sen lisäksi tekoja on mahdollista toteuttaa hyvin vähäisillä resursseilla ja kuitenkin aiheuttaa valtavaa vaikutusta oman aatteen nimissä. Tämän kaltaisen kyberterrorismin lisääntyminen on uhka, joka voi oleellisesti heikentää teknologian kehityksen kautta saatavien hyötyjen saavuttamista (Samuel, Osman, Al-Khasawneh & Duhaim, 2014).

Perinteisestä terrorismista on olemassa paljon erilaisia tutkimuksia. Myös kybertoimintaympäristön uhkia on kartoitettu ja tutkittu, mutta jo huomattavasti pienemmissä määrissä. Varsinaisia kyberterrorismiin keskittyviä tutkimuksia ja niistä kirjoitettuja tieteellisiä artikkeleita on myös olemassa jo useita, mutta pääosa niistä keskittyy lähinnä tarkastelemaan ja pohtimaan kyberterrorismia käsitteenä. Useita tällaisia artikkeleita käytetään tämän tutkimuksen lähdemateriaalina. Suomenkielistä materiaalia kyberterrorismista on olemassa toistaiseksi melko vähän.

1.3 Tutkimusongelma

Päätutkimuskysymys on:

- Millaisena uhkana kyberterrorismia pidetään Euroopassa?

Siihen vastausta haetaan alatutkimuskysymysten avulla, jotka ovat:

- Mitä on kyberterrorismi?
- Miten Euroopan valtioiden kyberturvallisuusstrategiat painottavat kyberterrorismia ja sen muodostamaa uhkaa?
- Miten USA:n kyberturvallisuusstrategiat painottavat kyberterrorismia?
- Millainen on ollut viimeaikainen kyberterrorismin kehitys?

Tutkimuksen tarkoituksena on selittää kyberterrorismia, sen muodostamaa uhkaa ja sitä, millaisena tämä uhka koetaan eurooppalaisten valtioiden näkökulmasta. Eurooppalaisten valtioiden näkökulmaa on pyritty selvittämään valtioiden kyberturvallisuusstrategioiden avulla. Tutkimus on luonteeltaan selittävä ja sen avulla pyritään löytämään niitä toimintoja ja asenteita, jotka ovat vaikuttaneet kyberterrorismin ja sen uhkan muodostumiseen. Lisäksi tutkimuksessa pyritään selittämään, kuinka nämä tekijät ovat vuorovaikutuksessa toisiinsa. Tutkimus toteutetaan laadullisena tutkimuksena, jossa kyberterrorismia pyritään tutkimaan mahdollisimman kokonaisvaltaisesti ja todellisuutta pyritään kuvaamaan tutkijan parhaan ymmärryksen mukaisesti. (Hirsjärvi, Remes & Sajavaara, 2005).

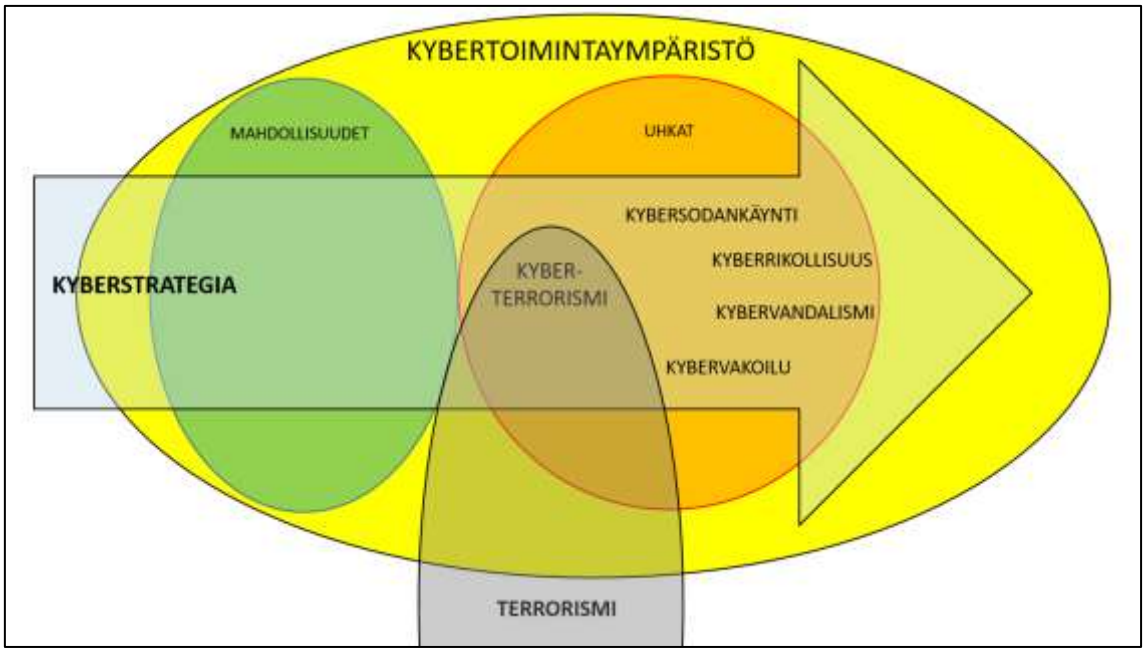
1.4 Näkökulma ja rajaus

Tutkimuksessa kyberterrorismia ja sen muodostamaa uhkaa tarkastellaan eurooppalaisten valtioiden näkökulmasta. Tätä kansainvälisen diplomatian nä-

kökulmaa kyberterrorismiin täydennetään tutkimuksessa tarkastelemalla kyberterrorismin käsitettä myös tieteellisten julkaisujen näkökulmasta. Tutkimuksen näkökulman muodostaminen tapahtuu siten, että tutkimuksen alussa kyberterrorismi pyritään määrittämään käsitteenä. Siinä tarkastelu tapahtuu tieteellisten julkaisujen näkökulmasta. Varsinaisessa tutkimuksessa kyberterrorismia tarkastellaan eurooppalaisten valtioiden kyberturvallisuusstrategioiden avulla eli kansainvälisen diplomatian näkökulmasta.

Tutkimus on rajattu usealla eri tavalla. Lähdemateriaalin osalta tavoitteena on ollut käyttää alle kymmenen vuotta vanhaa materiaalia. Tämän rajauksen osalta joitain poikkeuksia on olemassa, mutta ne perustuvat erityistarpeisiin, jotka on tuotu esille tämän kaltaisia lähteitä käytettäessä. Alueellisesti tarkastelu on rajattu Eurooppaan ja Euroopan ulkopuolisia asioita kuten Yhdysvaltojen kyberstrategioita tai terroristijärjestö ISIS:iä käsiteltäessä on nimenomaan pyritty löytämään näiden vaikutuksia Euroopassa. Kybertoimintaympäristön ja siinä esiintyvien muiden uhkien varsinainen käsittely on rajattu tämän tutkimuksen ulkopuolelle. Muut uhkat on kuitenkin esitelty lyhyesti luvussa kaksi tutkimuksen viitekehyksen muodostamiseksi ja kyberterrorismin asemoimiseksi tässä kehyksessä. Tutkimuksessa käytettävien eurooppalaisten valtioiden kyberturvallisuusstrategiat on rajattu englanninkielisiksi julkaisuiksi. Kyberterrorismin osalta sen varsinainen sosiaalinen ja psykologinen tarkastelu on rajattu tutkimuksen ulkopuolelle.

Tutkimuksessa kyberterrorismia käsitellään kybertoimintaympäristön muodostamassa viitekehyksessä. Viitekehys on esitelty kuviossa 1. Tutkimus rakentuu kybertoimintaympäristöstä, joka tarjoaa sekä mahdollisuuksia että uhkia. Kyberterrorismi arvioidaan osaksi terrorismia, mutta samalla se on yksi kybertoimintaympäristön uhkista. Kybertoimintaympäristön mahdollisuuksia ei tässä tutkimuksessa ole tarkasteltu, mutta ne on haluttu tuoda näkyviin tutkimuksen viitekehyksessä, jotta lukijoille ei jää väärää käsitystä kybertoimintaympäristön luonteesta ja jotta kyberturvallisuusstrategiat on helpommin miellettävissä viitekehykseen. Kyberturvallisuusstrategioiden arvioidaan pääasiassa käsittelevän laaja-alaisesti kybertoimintaympäristöä ja näin ollen ne käsittelevät useissa tapauksissa sekä uhkia että mahdollisuuksia. Tutkimuksen viitekehyksen ja siitä laaditun kuvion tavoitteena on selkeyttää tutkimuksen kokonaisuutta, siinä esiintyviä käsitteitä ja niiden vuorovaikutussuhteita. Lisäksi sen tarkoituksena on tuoda esille se, kuinka tutkija hahmottaa tutkimaansa kokonaisuutta.



KUVIO 1: Tutkimuksen viitekehys

1.5 Tutkimuksen raportointi

Tutkimuksen toteutus ja tulokset on esitetty seitsemään lukuun jaetussa tutkimusraportissa. Tutkimusraportin alussa on johdantoluku, jossa on lyhyesti kuvattu tutkimuksen aihepiiri, tutkimusongelma ja -tavoitteet sekä tutkimuksen näkökulma ja rajaukset. Seuraavassa luvussa, kybertoimintaympäristö ja terrorismi, on muodostettu tutkimukselle viitekehys. Lisäksi lyhyellä terrorismin tarkastelulla on pyritty luomaan edellytykset kyberterrorismin käsitteen määrittelylle neljännessä luvussa. Kolmannessa luvussa on kuvattu tutkimuksessa käytetyt tutkimusmenetelmät. Neljännessä luvussa käsitellään kyberterrorismia käsitteenä. Luvun avulla on pyritty vastaamaan tutkimuksen ensimmäiseen alatutkimuskysymykseen: mitä on kyberterrorismi? Tässä luvussa kyberterrorismin käsitettä on tarkasteltu tieteellisten julkaisujen näkökulmasta ja niiden avulla on kyberterrorismille pyritty muodostamaan tässä tutkimuksessa käytettävä määritelmä. Viidennessä luvussa on esitetty eurooppalaisten valtioiden kyberturvallisuusstrategioiden tutkimus. Sen avulla on muodostettu myös tutkimuksessa käytetty kansainvälisen diplomatian näkökulma kyberterrorismille. Tätä näkökulmaa on täydennetty Yhdysvaltojen kyberstrategioiden tarkastelulla. Luku pyrkii vastaamaan tutkimuksen alatutkimuskysymyksiin kyberturvallisuusstrategioista ja kyberterrorismin uhkasta. Tutkimuksen kuudennessa luvussa vastataan viimeiseen alatutkimuskysymykseen ja kerrotaan kyberterrorismin viimeaikaisesta kehityksestä Euroopassa. Tutkimuksen johtopäätökset ja tutkimusongelman vastaus on esitelty viimeisessä eli seitsemännessä luvussa.

2 KYBERTOIMINTAYMPÄRISTÖ JA TERRORISMI

Kybertoimintaympäristö ja terrorismi -luvun tarkoituksena on luoda viitekehys tutkimukselle. Samalla luku on yleinen kuvaus siitä toimintaympäristöstä, missä kyberterrorismia tässä tutkimuksessa käsitellään. Lisäksi luvun tavoitteena on tuoda esille se, kuinka tutkija hahmottaa tutkimaansa kokonaisuutta. Luvussa esitellään myös muut kybertoimintaympäristön uhkat ja hahmotellaan sitä, kuinka ne eroavat kyberterrorismista. Terrorismin osalta tarkoituksena on osoittaa, kuinka se liittyy kyberterrorismiin sekä muodostaa kyberterrorismin käsitteelle osa, jonka varaan käsitettä voidaan tutkimuksen edetessä rakentaa.

2.1 Kybertoimintaympäristö

Suomen kyberturvallisuusstrategiassa on arvioitu, että Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Samankaltainen trendi on nähtävissä muissakin kehittyneissä valtioissa. Tästä keskinäisriippuvaisesta ja moninaisesta sähköisessä muodossa olevan tiedon käsittelyyn tarkoitetusta ympäristöstä on kansainvälisesti ryhdytty käyttämään termiä kybertoimintaympäristö. Suomessa kybertoimintaympäristöllä tarkoitetaan sähköisessä muodossa olevan informaation käsittelyyn tarkoitettua, yhdestä tai useammasta tietojärjestelmästä muodostuvaa toimintaympäristöä. (Valtioneuvosto , 2013a.)

Kansainvälinen kybertoimintaympäristön määrittely noudattaa samaa linjaa aihealueen muiden käsitteiden kanssa eikä ole mitenkään yksiselitteinen. Kybertoimintaympäristön englanninkielinen käännös voidaan lähteistä riippuen tulkita olevan kyberavaruus (cyberspace) tai kybermaailma (cyberworld) tai kyberdomain (cyberdomain). Tässä tutkimuksessa olen päätynyt johtopäätökseen,

että koska käsitteiden kybermaailma ja kyberdomain käyttö on ollut tutkimusmateriaalissa kovin vähäistä, suomenkielinen kybertoimintaympäristö voidaan ymmärtää englanninkielisen cyberspace käsitteen synonyyminä. Valtaosa tutkimuksen käytössä olevista lähteistä tukee näkemystäni ja lisäksi esimerkiksi NATO:n Cooperative Cyber Defence Centre of Excellence:n määritelmien mukaisesti Suomen kyberturvallisuusstrategiassa määritelty kybertoimintaympäristö, vaikkakin suoran käännöksen mukaisesti voidaan ymmärtää käsitteellä cyberdomain, kuuluu kuitenkin cyberspace käsitteiden joukkoon (CCDCOE, 2017a). Käsitteelle cyberspace ei ole myöskään olemassa yksiselitteistä määritelmää, vaan esimerkiksi edellä mainitulla sivustolla sille on löydettävissä 36 erilaista määritelmää, ja jos käsitteen kirjoitusasu muutetaan muotoon cyber space, löytyy määritelmiä vieläkin lisää (CCDCOE, 2017a). Kansainvälisesti tunnustetun Oxfordin sanakirjan mukaan sanan cyberspace määritelmä on ”käsitteellinen ympäristö, missä kommunikaatio tapahtuu tietoverkkojen avulla” (Oxford Dictionary, 2017). Vastaavasti Tallinn manuaalista löytyvän kansainvälisten lakiasiantuntijoiden määritelmän mukaisesti cyberspace on fyysisistä ja ei-fyysisistä osista muodostuva ympäristö, jolle on ominaista tietokoneiden ja elektromagneettisen spektrin käyttäminen sekä datan tallentaminen, muokkaaminen ja vaihtaminen tietokoneverkkojen avulla (Schmitt, 2013). Yhdysvaltojen puolustusministeriön sanakirjan mukaan käsitteellä cyberspace tarkoitetaan informaatiotoimintaympäristön sisällä olevaa maailmanlaajuista toimialuetta, joka muodostuu toisistaan riippuvista informaatioteknologian infrastruktuurin ja siellä olevan datan muodostamista verkoista, joihin kuuluvat internet, telekommunikaatioverkot, tietokonejärjestelmät ja sulautetut prosessorit sekä ohjaimet (US Department of Defense, 2017). Kaikissa esimerkkinä olevista määritelmistä löytyy painotus toimintaympäristöön, joten tässä tutkimuksessa kybertoimintaympäristö voidaan mieltää lähtökohtaisesti englanninkielisen termin cyberspace synonyyminä, vaikkakin asia on jokaisen tutkimusmateriaalin kohdalla pyritty vielä varmistamaan erikseen.

Tässä tutkimuksessa puhutaan siis kybertoimintaympäristöstä. Tutkimuksessa on käytetty suomalaista kyberturvallisuusstrategian taustamuistiosta löytyvää ja vuonna 2017 Suomen kyberturvallisuuden nykytila -tutkimuksessa päivitettyä määritelmää kybertoimintaympäristölle. Tässä tutkimuksessa kybertoimintaympäristö määritellään seuraavasti:

> Globaali kybertoimintaympäristö muodostuu monimutkaisista ja -kerroksisista informaatioverkostoista, joihin kuuluu kansallisia julkishallinnon, yritysmaailman ja turvallisuusviranomaisten tiedonsiirtoverkkoja, informaatiojärjestelmiä ja digitaalisia palveluita ja palvelualustoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta ja ohjausjärjestelmiä, mitkä internetin välityksellä muodostavat maailmanlaajuisen verkoston”. (Lehto, ym., 2017).

Tälle kybertoimintaympäristölle ominaista on se, että siinä tapahtuvat muutokset ovat nopeita ja vaikutuksiltaan vaikeasti ennakoitavia (Valtioneuvosto, 2013a). Sen lisäksi kybertoimintaympäristö on muuttanut perinteisiä kansainvälisiä valta-asetelmia. Se antaa myös pienille valtioille ja ei-valtiollisille toimijoille

mahdollisuuden toimia tehokkaasti. Tässä kybertoimintaympäristössä fyysinen koko ja massa eivät enää ole hallitsevia, vaan osaaminen. (Valtioneuvosto, 2013b). Lisäksi tämän tutkimuksen kannalta oleellista on mieltää, että tämä kybertoimintaympäristö on muutakin kuin pelkästään internet (MacDonald, Jarvis & Chen, 2013).

2.2 Uhkat kybertoimintaympäristössä

Kehittyvä kybertoimintaympäristö tarjoaa valtavasti mahdollisuuksia. Toisaalta ja valitettavasti myös uhkat ovat osa kybertoimintaympäristöä ja ne aiheuttavat erilaisia haasteita siinä toimimiselle. Kybertoimintaympäristön uhkista käytetään usein termiä kyberuhka. Yleisesti kyberuhka voidaan määritellä tahallisesti tai tahattomasti digitaalisessa maailmassa tapahtuvaksi turvattavan kohteen turvallisuutta heikentäväksi tekijäksi (Limnéll, Majewski & Salminen, 2014). Suomen kyberturvallisuusstrategian mukaan kyberuhkalla tarkoitetaan mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon. Lisäksi kyberturvallisuusstrategia tarkentaa, että nämä kyberuhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan. (Valtioneuvosto, 2013a).

Kybertoimintaympäristön uhkia voidaan käsitellä ja jaotella useilla eri tavoilla, samoin kuin myöhemmin esiteltävää terrorismia. Lähestyttäessä kybertoimintaympäristön uhkia nimenomaan terrorismin avulla voidaan huomioida, että esimerkiksi julkisessa keskustelussa terrorismista puhutaan usein kuin se olisi yhtenäinen ilmiö. Siinä terrorismi liitetään voimakkaasti tietyn toimijan, esimerkiksi terroristiliikkeen ominaisuudeksi, vaikka suurin osa tutkimuksessa käytetyistä määritelmistä perustuu siihen, että terrorismin katsotaan olevan toimintatapa. Eli vaikka useimmat terrorisminmääritelmät on rakennettu vastamaan kysymykseen mitä terrorismi on, julkisessa keskustelussa kysymys on usein ollut pikemminkin kuka on terroristi. (Malkki, 2014). Samalla tavoin voidaan myös lähestyä kybertoimintaympäristön uhkia. Pääosin tutkimuksissa, kuten myös tässäkin tutkimuksessa, on pyritty määrittämään mitä kybertoimintaympäristön uhkat ja erityisesti kyberterrorismi ovat. Sen lisäksi tarkastelemme asiaa lyhyesti myös toimijoiden näkökulmasta. Oleellista on myös huomioida se, että uhkien luokittelu riippuu aina tarkastelijan käyttämästä näkökulmasta. Näin ollen myös tässä uhkatarkastelussa on syytä muistaa se, että mikä toisesta suunnasta katsottuna vaikuttaa terroristilta, voi toisesta suunnasta katsottuna vaikuttaa vapaustaistelijalta.

Suomessa kyberturvallisuusstrategian taustamuistiossa kyberuhkien on arvioitu voivan kohdistua suoraan tai välillisesti suomalaisen yhteiskunnan elintärkeitä toimintoja, kansallista kriittistä infrastruktuuria tai kansalaisia vastaan maan rajojen sisältä tai ulkopuolelta. Taustamuistiossa kyberuhkat on jaettu viiteen luokkaan, jotka ovat:

- Kyberaktivismi (kybervandalismi, haktivismi)
- Kyberrikollisuus
- Kybervakoilu
- Kyberterrorismi
- Kyberoperaatiot; painostus, sotaa alempi konflikti tai sotaan liittyvä kyberoperaatio (Valtioneuvosto, 2013b.)

Kyberaktivismi ei käsitteenä ole lähtökohtaisesti kielteistä toimintaa ja vaikka se taustamuistiossa uhka käsitteenä tuodaankin esille, niin tässä tutkimuksessa kuten pääosassa sen lähdeaineistoa, käytetään jatkossa termiä kybervandalismi.

Kansainvälisesti uhkien jaotteluun on käytetty hyvin samankaltaista tapaa. Myriam Dunn Cavelty esitteli vuonna 2010 samankaltaisen viisiportaisen jaottelun ja seuraavana vuonna Debi Asheden(2011) jakoi kybersodankäyntiä käsittävän ylimmän tason vielä kahtia päätyen esittämään kyberuhkien jaottelua kuuteen eri tasoon. Tässä jaottelussa kaksi ensimmäistä tasoa muodostuvat kybersodankäynnistä (cyber war) siten, että ensimmäisellä tasolla kybersodankäyntiä käsitellään irrallisena ja strategisena uhkana ja toisella tasolla kyseessä on taas kybersodankäynti ja siihen kuuluvat tietoverkkohyökkäykset taktisena uhkana. Kolmas taso on kyberterrorismi. Loput kolme tasoa ovat kybervakoilu (cyber espionage), kyberrikollisuus (cyber crime) ja kybervandalismi (cyber vandalism/hactivismi.

Kotimaisissa tieteellisissä määrittelyissä professori Martti Lehdon (2015) kyberuhkien rakennemalli mukailee sekä Myriam Dunn Caveltyn vuonna 2010 esittämää että Valtioneuvoston vuonna 2013 kyberturvallisuusstrategian taustamuistiossa esittelemää jäsentelyä. Pieniä eroja toki löytyy, mutta ne ovat pääosin terminologisia. Lehdon mallissa kyberuhat on jaettu viiteen osaan. Nämä osat ovat kybersodankäynti, kyberterrorismi, kybervakoilu, kyberrikollisuus ja kybervandalismi.

Tyypillistä kaikille yllä esitetyille kyberuhkien jaotteluille on se, että kyberterrorismi, kybervakoilu ja kyberrikollisuus sijoittuvat niissä kaikissa ääripäiden väliin eli keskelle. Eroavaisuudet on löydettävissä uhkamallien ääripäistä eli kybersodankäynnin osalta ja toisaalta kybervandalismin osalta. Näin ollen kyberterrorismin näkökulmasta voidaan todeta, että kyberterrorismi on yksi kybertoimintaympäristön uhkista ja sen sijoittumisesta uhkamalleihin voidaan arvioida sen olevan vaikuttavuudeltaan yksi kybertoimintaympäristön vakavimmista uhkista kybersodankäynnin jälkeen.

Kyberuhkien jaottelu on kuitenkin teoreettista ja sen takia onkin syytä huomioida, että jotkin uhkat voivat sopia useampaan luokkaan samanaikaisesti. Lisäksi on tarpeen muistaa, että kybertoimintaympäristön uhkat voivat esiintyä myös muissa ulottuvuuksissa samanaikaisesti. Professori Lehto (2015) mainitsee esimerkkinä tällaisista toimista tavanomaiseen sodankäyntiin liitetyt kyberoperaatiot ja vastustajan talouden romahduttamiseen tähtäävät toimet sekä terrorismin, johon fyysistä tuhoa aiheuttaviin iskuihin liitetään erilaisia operaatioita kybermaailmassa ja talousjärjestelmässä.

Toimijoiden näkökulmasta kybertoimintaympäristön uhkien aiheuttajat voidaan jakaa samalla tavoin myös viiteen eri luokkaan. F-Securen tutkimusjohtaja Mikko Hyppönen (2017) esitteli seuraavan kaltaisen jaottelun. Ensimmäisen luokan muodostavat penetraatiotestaukseen erikoistuneet eettiset hakkerit, englanniksi white hat hackers, joiden ei varsinaisesti pitäisi aiheuttaa uhkaa kybertoimintaympäristölle, mutta jotka voivat joskus näin toimiessaan kuitenkin vahingossa tehdä. Toisen luokan muodostavat haktivistit, jotka hakkeroivat protestiksi tai omien päämääriensä puolesta. Kolmannen luokan muodostavat rikolliset. Tämä ryhmä aiheuttaa valtaosan haittaohjelmista, mutta ei siitäkään huolimatta ole vaikutuksiltaan vaarallisin. Neljännen ja samalla vaarallisimman luokan muodostavat valtiolliset toimijat. Näitä toimijoita on kokonaisuuteen nähden vähän, mutta nämä ryhmät toimivat ainoastaan valikoituja kohteita vastaan ja niiden aiheuttamat toimet ovat aina vakavia, pääosin tiedustelutoimia. Viimeisen eli viidennen ryhmän muodostavat terroristit ja ääriryhmät. Pääosin kybertoimintaympäristö tarjoaa näille terroristiryhmille keinon rekrytoida ihmisiä ja levittää ideologiaa. Varsinaista kyberterrori-iskua, jossa olisi yhdistetty fyysinen väkivalta ja kyberhyökkäys ei kuitenkaan vielä ole nähty. Hyppösen (2017) arvion mukaan terroristijärjestöistä ainoastaan ISIS olisi kykenevä sen kaltaisen iskun toteuttamiseen ja sen kyberosaajat ovat joutuneet viimeaikoina useasti Yhdysvaltojen lennokkihyökkäysten kohteiksi.

Tässä tutkimuksessa on paneuduttu kyberterrorismiin, mutta sen käsittelyn helpottamiseksi myös muut kyberuhkat on syytä kuvata lyhyesti kokonaiskuvan ja tutkimuksen viitekehyksen muodostamiseksi. Kybertoimintaympäristön uhkien jaottelussa on hyödynnetty aiemmin esitettyä professori Martti Lehdon kyberuhkien rakennemallia. Tämän lisäksi joitain rajoja ja eroavaisuuksia eri kyberuhkien välille on pyritty löytämään, mutta tarkkojen rajojen määrittely on muodostunut tutkimuksen aikana hyvin vaikeaksi.

Käsitteille kybersodankäynti ja kybersota ei ole yleisesti hyväksyttyä määritelmää, vaan eri valtiot ja organisaatiot määrittelevät kybersodankäynnin eri tavalla. Yhdysvaltojen puolustusministeriön määritelmän mukaan kybersodankäynti on aseellinen konflikti, joka käydään osittain tai kokonaan kyberkeinoin. Sotilasoperaatioiden tarkoituksena on estää vastustajan kyberjärjestelmien ja -aseiden tehokas käyttö konfliktissa. Kybersodankäyntiin kuuluvat kyberhyökkäykset, kyberpuolustus ja niitä mahdollistavat toimenpiteet. (US Department of Defense, 2010). Professori Limnéll (2015) arvioi, että kybersodankäynti tulee olemaan osa jokaista tulevaisuuden sotaa.

Kyberterrorismia on käsitelty laajalti tässä tutkimuksessa. Tutkimuksen viitekehyksen hahmottamiseksi voidaan tässä vaiheessa todeta, että tässä tutkimuksessa kyberterrorismilla tarkoitetaan yksilöiden tai ryhmien kybertoimintaympäristössä tai sen avulla harjoittamaa poliittisesti, uskonnollisesti tai ideologisesti motivoitua väkivaltaa häiriön, tuhon ja pelon saavuttamiseksi kohteissaan.

Sanakirjan mukaan kybervakoilulla tarkoitetaan sitä, kun tietoverkkojen käytön avulla hankitaan laiton pääsy hallinnon tai organisaation luottamukselliseen tietoon (Oxford Dictionary, 2017). Tallinn manualin ja samalla myös NATO CCDCOE määritelmän mukaan kybervakoilulla tarkoitetaan salaa tai vilpillisesti

toteutettua konfliktin osapuolen kontrolloimalla alueella tehtyä tekoa, jossa käytetään kyberkykyjä tiedon keräämiseen tarkoituksena välittää se vastapuolelle (Schmitt, 2013).

Kyberrikollisuudelle ei ole olemassa yksiselitteistä kansainvälisesti hyväksyttyä määritelmää. INTERPOL:in (2017) näkemyksen mukaan kyberrikollisuus voidaan jakaa kahteen päätyyppiin. Kehittyneellä kyberrikollisuudella tarkoitetaan pitkälle kehitettyjä kyberhyökkäyksiä tietolaitteistoa ja ohjelmistoa vastaan. Kybertoimintaympäristön mahdollistamalla rikollisuudella puolestaan tarkoitetaan perinteistä rikollisuutta, joka on ottanut internetin mukaan toimintaan. Tällaista rikollisuutta on mm. lapsiin kohdistuvat rikokset, talousrikollisuus ja jopa terrorismi.

Suomessa tietoverkkorikoksen ja kyberrikoksen määritelmät ovat moninaiset ja termien käyttö on usein kontekstiriippuvaista sekä osin päällekkäistä. Poliisihallituksen mukaan kyberrikos ja tietoverkkorikos ovat toistensa synonyymeja ja niillä tarkoitetaan sellaisten rikosten tekomuotoja, joita esiintyy ainoastaan tietojärjestelmissä, kuten hakkerointi, hyökkäykset tietojärjestelmiä vastaan, haittaohjelmien avulla tehdyt identiteettivarkaudet ja palvelunestohyökkäykset. (Leppänen, Lindenborg & Saarimäki, 2016.)

Kybervandalismi on ideologialähtöistä toimintaa ja sillä tarkoitetaan hakkerointia, haktivismia ja kyberparveilua. Sen ilmenemismuotoja ovat mm. erilaiset tietomurrot, tietovuodot ja palvelunestohyökkäykset. Ne saavat julkisuudessa paljon näkyvyyttä, mutta ovat yleensä vaikutuksiltaan suhteellisen lyhytaikaisia ja osin vaarattomia. Arabi-kevään tapahtumissa julkisuuteen on noussut myös kyberparveilu, jossa internetin ja matkapuhelinten avulla on koottu ja johdettu usein väkivaltaisia mielenosoituksia. Tätä toimintaa ei voida ainakaan Lähi-Idän osalta pitää vaikutuksiltaan vähäisenä. Lisäksi yksittäisen yrityksen tai yksilön tasolla kybervandalismi saattaa aiheuttaa merkittäviäkin taloudellisia vahinkoja. (Lehto, 2015.)

Erilaisten kyberuhkien erottaminen toisistaan ja tarkkojen rajausten löytäminen niiden välillä on haastavaa. Yksi tapa on pyrkiä tarkastelemaan uhkien eroja mahdollisten tekijöiden kautta. Mahdollinen löydettävissä oleva ero kyberrikollisen, kybertaistelijan ja kyberterroristin välillä voi löytyä tarkastelemalla toimijan motivaatiota ja tavoitteita. Kyberrikollinen tavoittelee taloudellista hyötyä, kybertaistelija toimii sotilaallisten tavoitteiden saavuttamiseksi ja kyberterroristi omien, poliittisten, uskonnollisten tai ideologisten, tavoitteidensa saavuttamiseksi.(Lehto, 2015.)

Todellisen elämän esimerkeissä myöskään toimijoiden tarkastelu ei aina välttämättä yksinkertaista asiaa. Kybertaistelijat tai kybersotilaat ovat yleensä kansallisesti motivoituneita ja ryhmittymät voivat toiminnassaan siirtyä kyberterroristien, aktivistien sekä kybervakoilun välimaastoon. Esimerkkinä tällaisesta kybertaitelijoiden ryhmästä on Syrian Electronic Army, jonka avainhenkilöillä on tai on ollut läheiset suhteet Syyrian hallitukseen. Muita esimerkkejä tällaisista ryhmittymistä ovat Yemen Cyber Army ja Iranian Cyber Army. Toisaalta terroristihyökkäys Pariisissa Charlie Hebdo -lehden toimitukseen, jolla on ollut

suuri vaikutus myöhemmin esiteltävään Ranskan kyberstrategiaan, on myös esimerkki kyberterroristien sekä kybersotilaiden välimaastossa toimivasta ryhmästä. (Lehto, ym., 2017.)

Kyberuhkien luokittelusta riippumatta tyypillistä on, että usein niihin kuuluu jonkinlainen kyberhyökkäys. Espanjan kyberturvallisuusstrategiassa kyberhyökkäyksille on määritetty yleisiä piirteitä. Ne toimivat hyvänä lähtökohtana kyberhyökkäyksen tarkastelulle ja hyökkäyksen eri piirteiden painotusten muutoksia voidaan hyödyntää tarkasteltaessa mihin mahdolliseen kyberuhkaluokkaan kyseinen hyökkäys voisi kuulua. Kyberhyökkäyksen yleisiä piirteitä ovat:

- Edulliset kustannukset: valtaosa käyttöön tarvittavista työkaluista on saatavilla joko ilmaiseksi tai erittäin halvalla.
- Kaikkialla läsnä oleva toimintaympäristö ja toteuttamisen helppous: hyökkäykset eivät ole riippuvaisia hyökkääjän fyysisestä sijainnista ja useissa tapauksissa hyökkäykseen ei tarvita todellista teknistä osaamista.
- Tehokkuus ja vaikutus: hyvin suunnitellulla hyökkäyksellä voidaan saavuttaa asetetut tavoitteet. Lisäksi kyberturvallisuuden puutteelliset ohjeet ja laitteisto sekä puutteet tiedoissa ja taidoissa voivat edesauttaa hyökkäyksen onnistumista.
- Pieni riski hyökkääjälle: kyberhyökkäysten salaaminen on helppoa ja tekijän tai tekijöiden löytäminen vaikeaa. Lisäksi vähäisen tai puutteellisen oikeudenhoidon- ja lakimääritelmien takia kyberhyökkäyksiin syyllistyneitä on vaikea saada tuomioistuimen eteen vastaamaan teoistaan. (Presidency of the Government of Spain, 2013.)

Onnistuneella kyberhyökkäyksellä voi olla yllättäviä seurauksia muillakin kuin hyökkäyksen kohdistamalla osa-alueella. Tästä syystä laaja-alainen terroristityyppinen kyberhyökkäys voisi aiheuttaa yllättäviä ja jopa katastrofaalisia seurauksia muilla osa-alueilla ja mahdollisesti myös pitkäaikaisia vaikutuksia valtion talouteen. (Ahmad, Yunos & Sahib, 2012.)

Nopeat ja vaikeasti ennakoitavat kybertoimintaympäristössä tapahtuvat muutokset ja kyberhyökkäysmuotojen ja haittaohjelmien nopea kehityssykli asettavat kasvavan haasteen yhteiskunnan kyvylle varautua erilaisiin kyberuhkiin. Samanaikaisesti uhkat ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmiksi yksittäisten ihmisten, yritysten sekä koko yhteiskunnan kannalta ja uhkia muodostavat toimijat ovat ammattimaisempia kuin ennen. Kyberuhkiin varautuminen ja niiden torjuminen edellyttää yhteiskunnan kaikilta osapuolilta entistä nopeampaa, läpinäkyvämpää ja paremmin koordinoitua toimintaa, sekä erikseen että yhdessä. (Valtioneuvosto , 2013a.)

On myös syytä muistaa, että kyberuhkiin voi liittyä myös muita uhkia. Esimerkiksi perinteisessä terrorismissa voidaan fyysistä tuhoa aiheuttaviin iskuihin liittää erilaisia operaatioita kybertoimintaympäristössä. Kybertoimintaympäristön luonteen vuoksi uhkien syitä, niiden taustalla olevia toimijoita, täsmällisiä

kohteita ja tavoitteita, ilmenemisen laajuutta tai vaikutusten seurannaisvaikutuksia on vaikea tulkita ja ennustaa. (Valtioneuvosto, 2013b.)

2.3 Perinteinen terrorismi kyberterrorismin taustalla

Kyberterrorismia ei voi käsitellä ilman, että törmätään tarpeeseen verrata sitä niin sanottuun perinteiseen terrorismiin. Yleisesti terrorismia, josta tässä tutkimuksessa käytetään väärinkäsitysten välttämiseksi termiä perinteinen terrorismi, on tutkittu runsaasti ympäri maailmaa ja tämän tutkimuksen osalta ei ole ollut tarkoitus tai edes mahdollista laaja-alaisesti perehtyä kaikkeen tähän tutkimusmateriaaliin. Sen sijaan tässä tutkimuksessa perinteistä terrorismia on pyritty tarkastelemaan lyhyesti kyberterrorismin näkökulmasta. Tämän tarkastelun tarkoituksena on ollut löytää yhteys näiden kahden terrorismin muodon välille ja osoittaa ne perusteet perinteisestä terrorismista, joiden varaan kyberterrorismi rakentuu. Tämän tutkimuksen käyttöön on valittu perinteisen terrorismin määritelmä, jonka on arvioitu parhaiten tukevan tutkimusta ja siinä erityisesti kyberterrorismin käsitteen määrittelyä. Terrorismin määritelmä on esitetty luvun lopussa. Tutkimuksen lähtökohtana ja johtopäätöksenä on, että perinteinen terrorismi on laajempi käsite, jonka osa kyberterrorismi on. Terrorismin eri muotojen käytön myötä on korostunut tarve myös pyrkiä ymmärtämään niitä. Paronen ja Teirilä (2014) ovat arvioineet terrorismia ilmiönä käsittelevässä teoksessaan, että terroristi pyrkii saavuttamaan tavoitteensa äärimmäisellä väkivallalla ja tuhovoimalla luomansa pelkotilan avulla. Tällaisen ilmiön ymmärtäminen on tarpeen sen vaikutusten arvioimiseksi ja niiden vähentämiseksi.

Perinteisen terrorismin määritelmiä ja sen osatekijöitä on hyödynnetty kyberterrorismin määrittelemisen apuna myös aiemmin. Esimerkiksi Gordonin ja Fordin (2003) julkaisema kyberterrorismia käsittelevä paljon lainattu julkaisu on pyrkinyt hyödyntämään terrorismista tunnistettavia osatekijöitä ja aiemmin tapahtuneita terrori-iskuja. Tutkijat ovat pyrkineet liittämään löytämiään osatekijöitä ja tapahtumia kybertoimintaympäristöön pyrkimyksenä muodostaa laajempi ja käyttökelpoisempi arvio kybertoimintaympäristössä toimivista terroristeista.

Terrorismille on olemassa satoja erilaisia määritelmiä laatijan näkökulmasta ja terrorismin analysointitavasta riippuen (US Army TRADOC, 2007). Perinteisen terrorismin käsite tuli aktiiviseen käyttöön nykymerkityksessään ja kansainväliseen huomion kohteeksi vuonna 1972 Münchenin olympialaisiin tehdyn iskun myötä. Tällöin termille vahvistui voimakkaan kielteinen lataus ja se tuli käyttöön nimityksenä väkivallan teoille, joiden katsottiin olevan jollain tavalla poikkeuksellisia ja uudenlaisia. (Malkki, 2014.)

Yhteisesti hyväksyttyä määritelmää perinteiselle terrorismille on haettu 1970-luvulta asti sekä kansainvälisen diplomatian että akateemisen terrorismin tutkimuksen parissa. Siitä huolimatta yhteisesti jaettua määritelmää ei pitkällisistä keskusteluista huolimatta ole, vaikkakin vaikuttaa siltä, että jonkinlainen yksimielisyys vallitsee terrorismin keskeisistä piirteistä. Tämän lisäksi vaikuttaa

myös siltä, että yhdestä terrorismin ominaisuudesta vallitsee kiistaton yhteisymmärrys: terrorismi on erittäin tuomittavaa. Hyvänä esimerkkinä perinteisen terrorismin määrittelyongelmista kertoo se, että edes Yhdistyneiden kansakuntien (YK:n) turvallisuusneuvostossa pian syyskuun 11. päivän iskujen jälkeen hyväksytyssä ja kansainvälisen yhteistyön kannalta merkittävässä terrorismin vastaista toimintaa käsittelevässä päätöslauselmassa 1373 terrorismia ei määritellä. Tämä johtuu juuri siitä, että määritelmästä ei olisi saavutettu yksimielisyyttä. (Malkki, 2014.)

Terrorismille on kuitenkin olemassa useita eri valtioiden ja organisaatioiden käyttöön hyväksyttyjä määritelmiä. Veerasamyn ja Groblerin (2015) mukaan tänä päivänä edelleen käytössä olevan vuonna 1983 laaditun yhdysvaltalaisen määritelmän mukaan terrorismi on alueellisten tai luvattomien ryhmien ja toimijoiden ei-sotilaallisia kohteita kohtaan harjoittamaa harkittua poliittista väkivaltaa, jonka tavoitteena on vaikuttaa kohteisiinsa. Yhdysvaltojen puolustusministeriö puolestaan määrittelee terrorismin olevan laitonta uskonnollisesti, poliittisesti tai ideologisesti motivoitua väkivaltaa tai sillä uhkaamista pelon luomiseksi ja hallinnon tai väestön pakottamista pääosin poliittisiin tavoitteisiin (US Department of Defense, 2017). Yhdysvaltojen liittovaltionpoliisin (FBI) määritelmän mukaan terrorismi on laitonta henkilöihin tai omaisuuteen kohdistuvaa voimankäyttöä ja väkivaltaa, jonka tavoitteena on pelotella tai pakottaa hallintoa, siviiliväestöä tai niiden kaltaisia toimijoita poliittisten tai sosiaalisten tavoitteiden edistämiseksi (US Army TRADOC, 2007).

Kaikesta aiheeseen liittyvästä ristiriitaisuudesta huolimatta Yhdistyneet kansakunnat (YK) on vuonna 1992 kyennyt luomaan kuvauksen terrorismille. Kuvauksen mukaan terrorismia on levottomuus, joka inspiroi toistuvaan väkivallan käyttöön osin laittomia yksilöitä, ryhmiä tai valtiollisia toimijoita omaperäisistä, rikollisista tai poliittista syistä siten, että vastakohtana salamurhille, väkivallan kohteet eivät ole toiminnan pääkohteita. Täytyy kuitenkin edelleen painottaa, että YK:lla ei ole olemassa kansainvälisesti hyväksyttyä määritelmää perinteiselle terrorismille. (US Army TRADOC, 2007.)

Kaikkein yksinkertaisimmillaan Yhdysvaltain armeija on määritellyt terrorismin olevan väkivaltaa, joka tapahtuu normaalin lainsäädännön määräämien rajojen ja tavanomaisen sotilaallisen käyttäytymisen ulkopuolella (US Army TRADOC, 2007).

Charles Rubyn (2002) esittämän määritelmän mukaan perinteinen terrorismi keskittyy kolmeen kriittiseen näkökohtaan: terrorismin motivaatio on poliittinen, terrorismin kohteena on siviilihenkilöitä, jotka eivät kuulu tai osallistu sotilasoperaatioihin sekä terroritekojen tekijöinä ovat luvattomat alueelliset järjestöt tai henkilöt. Tämän määritelmän mukaan voisi tulkita, että valtiot eivät voi syyllistyä terrorismiin.

Terrorismiin liittyvän kysymyksen asettelun lisäksi suhtautuminen terrorismiin on myös näkökulmakysymys. Terrorismi voidaan nähdä rikollisena toimintana, epäsymmetrisenä sodankäynnin muotona tai vaikkapa sosiaalisena ongelmana, jolloin sen katsotaan olevan yhteiskunnasta syrjäytyneiden pahoinvoinnin kanavoitumista (Paronen & Teirilä, 2014).

Terrorismin käsitteellinen epäselvyys on lisännyt käsitteen poliittista käyttöä. Siitä onkin tullut yksi käytetyimmistä negatiiviseen leimaamiseen ja mustamaalaamiseen liittyvistä käsitteistä monien maiden sisäpolitiikassa ja myös kansainvälisissä suhteissa. Erityisesti käsitteen laaja-alaisuus ja epämääräisyys vaikeuttaa ilmiöstä muodostettavan kokonaiskuvan hahmottamista. Näin ollen jonkun toimijan leimaaminen terroristiksi mahdollistaa kaikkien käytössä olevien vastakeinojen käyttämisen. (Raitasalo, 2014.)

Swansean yliopiston tutkija Andrew Whiting toi kyberterrorismia käsittelevässä konferenssissa esille näkemyksen siitä, että perinteinen terrorismi ja sen ymmärrys ovat kehittyneet huomattavasti ajan myötä. Näin ollen tuntuisi erikoiselta väittää, että kybertoimintaympäristössä tapahtuvat aktiviteetit eivät mahtuisi mukaan tähän kategoriaan. Veerasamyn ja Groblerin (2015) mukaan uusi osa tätä terrorismin kehitystä on terroristien uusi sukupolvi, jotka toimivat tehokkuutta, helppoutta ja saavutettavuutta parantavassa digitaalisessa maailmassa. Toisaalta samanaikaisesti hallitseva näkemys terrorismista väkivallan ja huomion välineenä vaikeuttavat kybertoimintaympäristön salaperäisyyden liittämistä tähän näkemykseen (MacDonald, Jarvis & Chen, 2013).

Perinteisessä terrorismissa ja kyberterrorismissa on olemassa samoja yhteisiä piirteitä sekä luonnollisesti yhteisenä tekijänä nimenomaan terrorismi (Flemming & Stohl, 2001). Toisaalta juuri kyber-etuliite vahvistaa entisestään terrorismin moniin erilaisiin määritelmiin liittyviä väärinkäsitysten mahdollisuuksia (Limnéll, Majewski & Salminen, 2014). Pahimpien arvioiden mukaan tulevaisuuden terroristi kykenee voittamaan sotia ampumatta laukaustakaan tuhoamalla kriittisen kansallisen infrastruktuurin, jos tällaiseen kyberhyökkäyksen uhkaan ei ole ennalta osattu varautua (Bogdanoski & Petreski, 2013).

Perinteisen terrorismin ja kyberterrorismin raja on hämärtymässä. Nykyään lähes kaikki terroristiset teot sisältävät tietoteknologian hyödyntämistä jossain muodossa. Lisäksi uudet terroristiorganisaatiot voivat olla hyvin rahoitettuja ja teknologisesti osaavia ryhmittymiä, joiden kohdeyleisönä on koko maailma ja joilla on kyky tuottaa huomattavaa vahinkoa suuressa määrässä kohteita. Samanaikaisesti webbisivuista on tullut voimakas strategisen kommunikaation väline. Perinteisten joukkotiedotusvälineiden sijaan terroristiset ryhmittymät voivat nyt tuoda viestinsä globaalin yleisön eteen ilman hallinnon sensuuria ja välikäsiä. (Limnéll, Majewski & Salminen, 2014.)

Kybertoimintaympäristössä internet on ideaalinen toimintaympäristö terroristijärjestöille. Veerasamyn ja Groblerin (2011) mukaan terroristit käyttävät internettiä rekrytointiin, harjoitteluun, kommunikaatiovälineenä, operaatioidensa toteuttamiseen, propagandaan, rahoituksen hankintaan ja psykologiseen sodankäyntiin. Käytännössä kansainväliset terroristijärjestöt käyttävät internettiä kaikkiin päivittäisiin toimintoihinsa.

Tässä tutkimuksessa terrorismin määritelmänä kyberterrorismin taustalla käytetään Yhdysvaltain armeijan hyvin yleistä määritelmää terrorismille. Sen mukaan terrorismi on väkivaltaa, joka tapahtuu normaalin lainsäädännön määräämien rajojen ja tavanomaisen sotilaallisen käyttäytymisen ulkopuolella. (US

Army TRADOC, 2007). Tämä määritelmä kuvaa hyvin terrorismin yleistä luonnetta kuitenkin rajaamatta liian tarkasti siihen kuuluvia tekijöitä ja näin ollen mahdollistaa kyberterrorismin käsitteen määrittelyn painopisteen muodostamisen nimenomaan kybertoimintaympäristöön. Samalla käsite terrorismi ei rajoita kyberterrorismin määrittelyä muuten kuin sillä edellytyksellä, että teon tulee kuitenkin olla luonteeltaan väkivaltainen.

3 TUTKIMUSMENETELMÄN ESITTELY

Tutkimuksen tutkimusmenetelmä on pyritty valitsemaan tutkimuksen tavoitteiden, tutkimusongelman ja käytössä olevan aineiston kannalta mahdollisimman optimaalisesti. Lisäksi tutkimusmenetelmän valintaan ovat vaikuttaneet laaditun tutkimuksen laajuus opinnäytetyönä, siihen käytössä oleva aika sekä taloudelliset resurssit. Myös tutkijan aiemmat kokemukset ovat vaikuttaneet tutkimusmenetelmän valitsemiseen. Valitun tutkimusmenetelmän on edellä mainittujen tekijöiden mukaisesti arvioitu olevan hyvin soveltuva tähän tutkimukseen. Tutkimuksessa käytetty tutkimusmenetelmä on pyritty kuvaamaan sellaisella tarkkuudella, että sen avulla tutkimus olisi mahdollista suorittaa haluttaessa uudelleen. Erityisesti tutkimuksesta on pyritty kuvaamaan kuinka sen aineisto on hankittu ja kuinka sitä on analysoitu.

3.1 Tieteellinen lähestymistapa

Tutkimus on toteutettu laadullisena eli kvalitatiivisena tutkimuksena. Laadullinen tutkimus on tieteellisen tutkimuksen menetelmäsuuntaus, jossa pyritään ymmärtämään kohteen laatua, ominaisuuksia ja merkityksiä kokonaisvaltaisesti (Humanistinen tiedekunta, Jyväskylän yliopisto, 2017b).

Laadullisessa tutkimuksessa lähtökohtana on todellisen elämän kuvaaminen. Tähän sisältyy ajatus, että todellisuus on moninainen. Tutkimuksessa on kuitenkin otettu huomioon, että tätä todellisuutta ei voi pirstoa mielivaltaisesti osiin. Tapahtumat muovaavat samanaikaisesti toinen toistaan, ja onkin mahdollista löytää monensuuntaisia suhteita. Tässä laadullisessa tutkimuksessa on pyritty tutkimaan kohdetta eli kyberterrorismia mahdollisimman kokonaisvaltaisesti. (Hirsjärvi, Remes & Sajavaara, 2016.)

Tarkemmin kvalitatiivista tutkimusta jaoteltaessa voidaan arvioida, että tässä tutkimuksessa pyritään nimenomaan kyberterrorismin toiminnan ja siitä

kirjoitetun tekstin merkityksen ymmärtämiseen. Näin ollen muunlaiset kvalitatiivisen tutkimuksen tyypit, kuten kielen piirteet, säännönmukaisuuksien etsiminen ja reflektio voidaan rajata tutkimuksen ulkopuolelle. Tämän jaottelun avulla voidaan arvioida tutkimuksen kuuluvan fenomenologis-hermeneuttiseen perinteeseen liittyväksi tutkimukseksi. (Hirsjärvi ym., 2016.)

Tämän tutkimuksen mielenkiinnon kohteena on ilmiön eli kyberterrorismin ymmärtäminen, kuvaaminen ja selittäminen. Näin ollen laadullisen tutkimustradition mukaisesti sen tutkimusstrategia on fenomenologis-hermeneuttinen (Metsämuuronen, 2006). Tässä yhteydessä tutkimusstrategia tarkoittaa tutkimuksen menetelmällisten ratkaisujen kokonaisuutta (Hirsjärvi ym., 2016).

Tutkimuksen tarkoituksena on selittää kyberterrorismia, sen muodostamaa uhkaa sekä millaiseksi tämä uhka koetaan. Tutkimus on siis luonteeltaan selittävä ja sen avulla pyritään löytämään niitä toimintoja ja asenteita, jotka ovat vaikuttaneet kyberterrorismin ja sen uhkan muodostumiseen. Lisäksi tutkimuksessa pyritään selittämään kuinka nämä tekijät ovat vuorovaikutuksessa toisiinsa. Tämä selittävä tutkimusote on valittu siksi, että sen avulla saadaan parhaiten luotua vastaukset asetettuun tutkimusongelmaan.

3.2 Tiedonkeruumenetelmä

Tutkimuksessa käytettävän aineiston hankinta eli tiedonkeruu on tapahtunut useissa eri vaiheissa. Tutkimuksen suunnittelun ja hahmottelun aikana aineistoa on hankittu tarkastamalla jo muussa opiskelukäytössä olevasta kirjallisuudesta viittauksia ja määritelmiä kyberterrorismiin. Lisäksi kyberterrorismin määritelmiä ja siihen liittyviä aineistoja on haettu internetistä yleisten hakukoneiden kuten Googlen avulla. Tämän tiedonkeruuvaiheen tarkoituksena on ollut luoda yleissilmäys tutkimuksen kohteeksi aiottuun aihealueeseen sekä varmistua siitä, että alustavasti edellytykset tutkimukselle ovat olemassa.

Alustavan kartoituksen jälkeen syntyi päätös kyberterrorismiin liittyvän tutkimuksen toteuttamisesta. Sen jälkeen alkoi tutkimussuunnitelman laatiminen. Tutkimussuunnitelman laatimiseen liittyen tiedonkeruuta oli mahdollista yhdistää informaatioturvallisuuden jatkokurssin opintoihin. Tiedonkeruu tapahtui hankkimalla kyberterrorismia ja myös kybertoimintaympäristöä käsittelevää kirjallisuutta Maanpuolustuskorkeakoulun kirjastosta sekä Tuusulan pääkirjastosta. Näiden kirjojen avulla luotiin näkemystä tutkimuksen viitekehyksen muodostamiseen, parannettiin kybertoimintaympäristön ymmärrystä sekä luotiin edellytyksiä tieteellisten artikkeleiden keräämiselle. Tämä tieteellisten kyberterrorismia käsittelevien artikkelien haku toteutettiin Jyväskylän yliopiston kirjaston internet-hakukoneiden avulla. Löydetty artikkelien ja tutkimusten määrä oli suurempi kuin tutkimuksen tässä vaiheessa oli ajankäytöllisesti mahdollista käsitellä. Näin ollen ainoastaan osa artikkeleista valittiin perehdyttäviksi tässä vaiheessa tutkimussuunnitelmaa ja informaatioturvallisuuden jatkokurssin tavoitteita varten. Loput arkistoitiin tutkimuksen myöhempää vaihetta varten.

Tutkimussuunnitelman laatimisen jälkeen tutkimuksessa havaittiin, että kyberterrorismia käsittelevää aineistoa oli tutkimuskäyttöön melko laajalti ja tiedonkeruun painopiste siirtyi muualle. Seuraavaksi lisää aineistoa hankittiin tutkimusmenetelmistä. Tämä aineisto koostui pääosin Maanpuolustuskorkeakoulun kirjastosta lainatusta laadullista tutkimusta käsittelevästä kirjallisuudesta sekä muutamista aihealueeseen kuuluvista internetin kautta löydetyistä artikkeleista ja julkaisuista. Lisäksi tässä vaiheessa aineistonkeruuvuorossa olivat myös eurooppalaisten valtioiden ja Yhdysvaltojen kyberturvallisuusstrategiat, jotka olivat löydettävissä julkaisuina internetin avulla. Myös muutamia täsmennyksiä terrorismiin liittyen oli tarve hankkia Maanpuolustuskorkeakoulun kirjaston ja internetin avulla. Tässä vaiheessa tutkimuksen osalta pääosa aineistosta oli saatu kerättyä ja edellytykset siirtyä toteuttamaan varsinaista tutkimusta olivat olemassa. Luonnollisesti lähdemateriaalia on jouduttu hieman täydentämään tutkimuksen edetessä, mutta pääosin tutkimus pystyttiin toteuttamaan varsinaisen aineistonkeruun aikana löydetyn materiaalin avulla.

Tutkimuksen lähdeaineisto on siis koostunut kyberterrorismiin liittyvistä tutkimuksista ja artikkeleista sekä valtioiden kyberturvallisuusstrategioista. Niistä saatuja havaintoja on täydennetty aihealuetta käsittelevällä kirjallisuudella, jota on myös käytetty tutkimuksen viitekehyksen muodostamiseen. Tämän lisäksi tutkimuksen toteutuksen tukena ovat olleet laadullisen tutkimuksen toteuttamista opastavat kirjat.

Tutkimuksen lähdeaineiston osalta kritiikkiä voi oikeutetusti esittää ainakin kyberterrorismin viimeaikaista kehitystä käsittelevän kuudennen luvun lähdemateriaalista. Luvun lähdeaineistossa on käytössä tieteelliseen tutkimukseen suhteellisen paljon lehtiartikkeleita. Niitä on käytetty siitä syystä, että tutkittaessa uutta ja melko ajankohtaista asiaa, on ollut tärkeää saada yleinen näkemys tapahtumaan, niin sanottu ensikäsitys asiasta. Lisäksi uusista ja ajankohtaisista asioista ei yleensä tieteellisiä artikkeleita ja lähdeaineistoa ole edes saatavilla. Käytetyt lehtiartikkelit soveltuivat hyvin tähän tutkimukseen ja juuri sen uusimpia asioita käsittelevään osa-alueeseen. Uusien lehtiartikkeleiden käytössä olevat riskit on pyritty tunnistamaan ja niiden sisältämiä faktoja on tarkastettu ristiin useista eri lähteistä. Lisäksi niin sanottu keltainen lehdistö on jätetty käyttämättä ja kaikissa tilanteissa on pyritty löytämään kansainvälisesti tunnettuja ja arvostettuja julkaisijoita.

3.3 Aineiston analysointimenetelmä

Aineiston analyysimenetelmänä on käytetty aineistolähtöistä sisällönanalyysia. Sen tarkoituksena on ollut luoda sanallinen ja selkeä kuvaus tutkittavasta ilmiöstä eli kyberterrorismista. Suoritettu tutkimus on laadullinen tutkimus ja kokonaisuus, jossa aineisto kuvaa tutkittavaa ilmiötä eli kyberterrorismia ja sisällönanalyysillä pyritään järjestämään aineisto tiiviiseen ja selkeään muotoon kadottamatta sen sisältämää informaatiota. Laadullisena tutkimuksena aineiston

analysoinnin tarkoituksena on ollut informaatioarvon lisääminen, jossa hajanaisesta aineistosta on pyritty luomaan mielekästä, selkeää ja yhtenäistä informaatiota. (Tuomi & Sarajärvi, 2013.)

Sisällönanalyysi on menettelytapa, jolla voidaan analysoida dokumentteja systemaattisesti ja objektiivisesti. Lisäksi sen avulla pyritään saamaan tutkittavasta ilmiöstä kuvaus tiivistetyssä ja yleisessä muodossa. Aineistolähtöinen sisällönanalyysi muodostuu kolmesta vaiheesta. Ensimmäinen vaihe on aineiston redusointi eli aineiston pelkistäminen. Siinä pyritään karsimaan aineistosta pois kaikki epäolennainen ja tiivistämään informaatiota. Toisessa vaiheessa vuorossa on aineiston klusterointi eli ryhmittely. Sen aikana aineisto ryhmitellään ja yhdistellään luokiksi. Kolmannessa eli viimeisessä vaiheessa vuorossa on abstrahointi eli käsitteellistäminen. Sen aikana pyritään luomaan teoreettisiä käsitteitä ja yhdistelemään luokkia. Ainestolähtöisen sisällönanalyysin ideana on siis yhdistellä käsitteitä ja näin saada vastaus tutkimusongelmaan. Se perustuu tulkintaan ja päättelyyn. (Tuomi & Sarajärvi, 2013.)

Tässä tutkimuksessa edellytykset analyysille luotiin jo ennen varsinaisten analyysivaiheiden alkua tutkimusongelmaa ja rajauksia asetettaessa. Näiden lähtökohtien myötä muodostuivat edellytykset analyysille. Tässä tutkimuksessa aineiston analysointi eli aineistolähtöinen sisällönanalyysi toteutettiin edellä esitetyn esimerkin mukaisesti kolmessa vaiheessa. Ensimmäisessä vaiheessa tapahtui aineiston redusointi eli pelkistäminen. Siinä aineistosta pyrittiin karsimaan pois epäolennainen ja erityisesti mielenkiintoiset, mutta tutkimuksen kannalta epäoleelliset sivujuonteet. Aineistoa käytiin läpi nimenomaan tutkimuskysymysten avulla ja tärkeimpänä analyysiyksikkönä toimi käsite kyberterrorismi. Lisäksi tässä vaiheessa myös tutkimuksen rajauksen mukaisesti liian vanhaksi arvioitu aineisto rajattiin pääosin tutkimuksen ulkopuolelle. Seuraavana vuorossa oli aineiston klusterointi eli luokittelu. Esimerkiksi kyberturvallisuusstrategiat luokiteltiin aluksi kahteen osaan eli niihin, jotka eivät millään lailla käsitelleet kyberterrorismia tai terrorismia, ja niihin, jotka käsittelivät. Sen jälkeen terrorismia ja kyberterrorismia käsitelleet kyberturvallisuusstrategiat teemoiteltiin eli jaettiin aihepiirien mukaisesti. Aihepiirit eli teemat muodostuivat yleisestä terrorismista sekä kyberterrorismista. Samankaltaista luokittelua ja teemoittelua käytettiin myös kyberterrorismia käsittelevän aineiston osalta. Siinä käytettyjä luokkia, teemoja ja tyypittelyä on esitelty tarkemmin kyberterrorismia käsitelevässä luvussa. Erityisesti pyrittiin löytämään eroavaisuuksia tutkimuksen aineiston ja tutkimuksen oman kyberterrorismin määritelmän osalta. Tutkimuksen kannalta haastavin vaihe oli analyysin viimeinen eli kolmas vaihe. Siinä vuorossa oli aineiston abstrahointi eli käsitteellistäminen. Tavoitteena oli löytää tutkimuksen kannalta olennainen tieto, muodostaa teoreettisia käsitteitä ja löytää vastaukset tutkimusongelmaan. Johtoajatuksena kolmannessa vaiheessa oli Tuomen ja Sarajärven (2013) opastus siitä, että järjestetty aineisto ei riitä sellaisenaan tutkimuksen tuloksiksi vaan siitä on kyettävä muodostamaan edelleen johtopäätöksiä.

Sisällönanalyysiä olisi voitu jatkaa luokittelun ja kategorioiden muodostamisen jälkeen vieläkin pidemmälle kvantifioimalla aineisto (Tuomi & Sarajärvi,

2013). Se olisi voitu toteuttaa vaikkapa laskemalla esiintyvien sanojen määrää käsitteissä. Tässä tutkimuksessa näin ei kuitenkaan tehty, koska tutkija arvioi, että kattavan, mutta edelleen suhteellisen pienen aineiston kvantifiointi ei tosiasiassa olisi tuonut tutkimukselle todellista lisätietoa tai antanut erilaista näkökulmaa tutkimustuloksiin.

Aineistolähtöisen sisällönanalyysin yhtenä tavoitteena on ollut myös tutkimuksen luotettavuuden varmistaminen. Tämän takia aineistoa analysoitaessa on pyritty hyödyntämään myös diskurssianalyysin peruskysymyksiä. Eli artikkeleita ja kirjallisuutta tarkasteltaessa on mietitty kysymyksiä: kuka sanoi, mitä sanoi, mitä tarkoitti, miksi sanoi, mihin pyrki ja kehen pyrki vaikuttamaan (Metsämuuronen, 2006).

Kyberterrorismia käsitteenä käsittelevässä luvussa aineistolähtöisen sisällönanalyysin lisäksi on täydentävänä menetelmänä käytetty käsiteanalyysiä (Nuopponen, 2009). Siinä kyberterrorismin käsitteen erilaisia määritelmiä on haettu tieteellisistä julkaisuista ja muusta lähdeaineistosta. Tämän jälkeen löydettyjen määritelmien tulkintoja kyberterrorismi käsitteen sisällöstä on vertailtu ja luokiteltu. Samanaikaisesti määritelmiä on myös verrattu tutkimuksen käyttöön muodostamaan omaan kyberterrorismin määritelmään.

Lopullisten johtopäätösten ja tutkimusongelman vastausten löytämiseksi aineiston tulkintamenetelmänä on hyödynnetty laadullisen tutkimuksen tyypillisten piirteiden mukaisesti induktiivista päättelyä, jossa päättelyä pyritään laajentamaan yksittäisistä tapauksista yleisiin (Grönfors, 2011).

Aineistolähtöisen tutkimuksen haasteena on se, että ei ole olemassa objektiivisia ja puhtaita havaintoja sinällään, vaan käytetyt käsitteet, tutkimusasetelma ja menetelmät ovat tutkijan asettamia ja vaikuttavat aina tuloksiin. Fenomenologis-hermeneuttisessa perinteessä haaste on pyritty ratkaisemaan siten, että tutkijan tulee kirjoittaa auki omat ennakkokäsityksensä ilmiöstä ja suhtautua tietoisesti niihin analyysin aikana. (Tuomi & Sarajärvi, 2013.)

Tässä tutkimuksessa tunnistettuja ennakkokäsityksiä kyberterrorismista on ollut kolme. Ensimmäisenä ennakkokäsityksenä on ollut ajatus siitä, ettei kyberterrorismille ole olemassa yhteisesti hyväksyttyä määritelmää. Toinen ennakkokäsitys on ollut se, että kyberterrorismi käsitettä käytetään hyvin laaja-alaisesti ja pääasiassa sen esittäjän haluamassa muodossa tai tavoitteita tukien. Kolmantena ennakkokäsityksenä on ollut ajatus siitä, että kyberterrorismi on yksi osa perinteistä terrorismia.

3.4 Raportointimenetelmä

Tutkimuksen tulokset on raportoitu Jyväskylän yliopiston raportointiohjeen mukaisesti (Pirhonen & Jauhiainen, 2017). Tutkimuksen kulku, tutkimuksen viitekehys ja raportin jaottelu on löydettävissä alla esitetystä tutkimusasetelmasta.

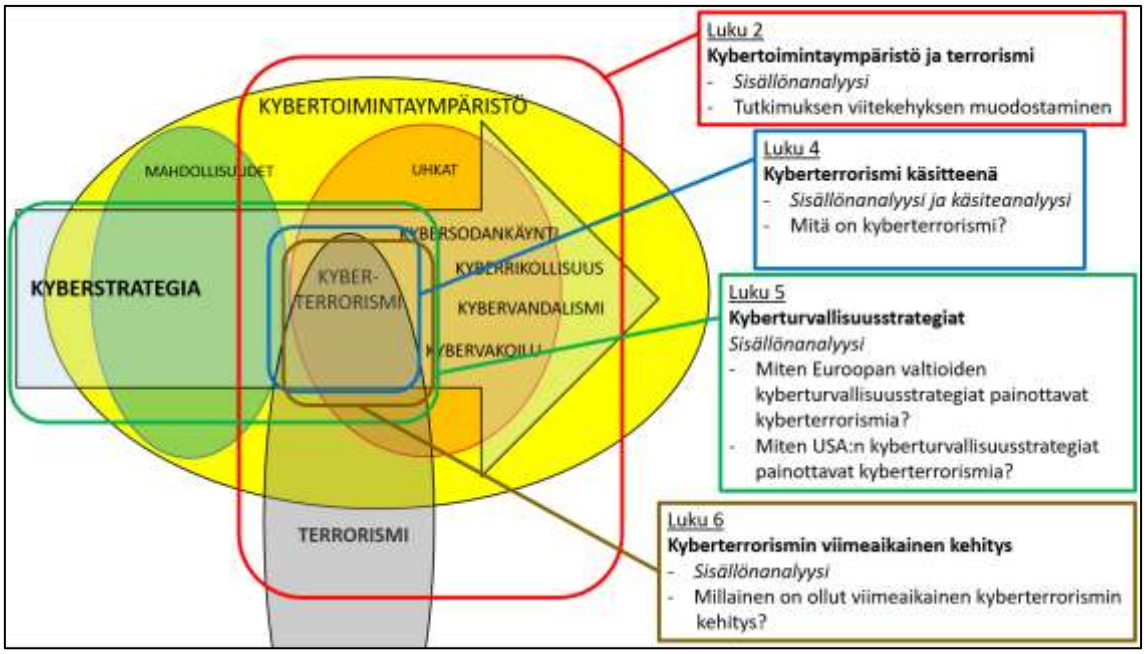
Tutkimus ja sen raportointi on valittu toteutettavaksi suomenkielisenä, vaikkakin valtaosa lähdeaineistosta on englanninkielistä. Tutkimuksen aikana

tämä on pyritty ottamaan huomioon siten, että käsitteitä tulkittaessa kielellisten eroavaisuuksien lisäksi myös kulttuurillisia eroja on pyritty huomioimaan mahdollisuuksien mukaan ja väärinymmärtämisen riski tiedostaen. Yksi tutkimuksen tavoitteista on kuitenkin ollut suomenkielisen materiaalin tuottaminen tutkimuksen aihealueesta.

Tutkimusraportin runko-osa alkaa johdantoluvulla kyberterrorismin uhka ja haasteet. Sen tarkoituksena on tutkimusraportin alkuun lyhyesti kuvata tutkimuksen aihepiiri, tutkimusongelma ja -tavoitteet, käytetyt menetelmät sekä saavutetut tulokset. Seuraavassa luvussa, kybertoimintaympäristö ja terrorismi, on muodostettu tutkimukselle viitekehys. Kolmannessa luvussa on kuvattu tutkimuksessa käytetyt tutkimusmenetelmät.

Tutkimuksen neljännessä luvussa käsitellään kyberterrorismia käsitteenä. Siinä sisällönanalyysiä on täydennetty käsiteanalyysin avulla. Luvun avulla on pyritty vastaamaan tutkimuksen ensimmäiseen alatutkimuskysymykseen: mitä on kyberterrorismi? Luvussa kyberterrorismia on käsitelty vielä pääosin tieteellisten tutkimusten näkökulman avulla. Viidennessä luvussa kyberterrorismia käsitellään koko tutkimuksen varsinaisen näkökulman eli kansainvälisen diplomatian näkökulman mukaisesti. Luvussa valtioiden kyberturvallisuusstrategioita tutkitaan sisällönanalyysin avulla. Luku pyrkii vastaamaan ensisijaisesti siihen, miten Euroopan valtioiden kyberturvallisuusstrategiat painottavat kyberterrorismia. Lisäksi luvun sisältöä täydennetään etsimällä vastausta alatutkimuskysymykseen, miten USA:n kyberturvallisuusstrategiat painottavat kyberterrorismia.

Kuudennessa luvussa on vastattu tutkimuksen viimeiseen alatutkimuskysymykseen ja tarkasteltu kyberterrorismin viimeaikaista kehitystä Euroopassa. Tutkimuksen johtopäätökset on esitelty viimeisessä eli seitsemännessä luvussa. Johtopäätökset on pyritty muodostamaan tulkitsemalla aiempien lukujen tuloksia laadullisen tutkimuksen piirteiden mukaisesti induktiivista päättelyä hyödyntämällä. Lisäksi luvun lopussa on pohdintaosuus, jossa tutkija on arvioinut tutkimuksen onnistumista ja mahdollisia tutkimuksen aikana esiin tulleita jatkotutkimustarpeita.



KUVIO 2: Tutkimusasetelma

4 KYBERTERRORISMI KÄSITTEENÄ

Kyberterrorismi käsitteenä -luvun tarkoituksena on luoda perusteet kyberterrorismin tutkimukselle määrittämällä vastaus alatutkimuskysymykseen: mitä on kyberterrorismi? Luvussa kyberterrorismia tarkastellaan tieteellisten julkaisujen näkökulmasta. Samalla se on myös tutkimuksen kirjallisuuskatsaus, jonka tarkoituksena on näyttää, mistä näkökulmista ja miten kyberterrorismia on aiemmin tutkittu ja miten nyt tehty tutkimus liittyy jo olemassa oleviin tutkimuksiin. Lisäksi luku kuvaa, miten aiempi tutkimustieto on merkityksellistä nyt suoritetun tutkimustehtävän kannalta. (Hirsjärvi, Remes & Sajavaara, 2005.)

Kyberterrorismia käsitteenä voidaan lähestyä useista erilaisista näkökulmista. Voidaan esimerkiksi arvioida sitä, onko kyberterrorismissa kyseessä erillinen ilmiö vai onko kyseessä ainoastaan yksi informaatiosodankäynnin muoto, jota terroristit käyttävät (Lehto, 2015). Tässä tutkimuksessa lähtökohtana on kuitenkin ollut se, että aiemmin esitettyjen kybertoimintaympäristön uhkamallien mukaisesti kyberterrorismi on erotettu sodankäynnistä, ja sitä käsitellään erillisenä ilmiönä. Tässä luvussa kyberterrorismia on tarkasteltu nimenomaan akateemisen tutkimuksen näkökulmien avulla, vaikkakin myös muunlaisista näkemyksistä on mainittu esimerkkejä. Myöhemmin tutkimusraportin viidennessä, kyberstrategioita käsittelevässä luvussa kyberterrorismia on tarkasteltu kansainvälisen diplomatian näkökulmia hyödyntäen. Luvun viisi tarkastelun näkökulma on myös samalla tämän tutkimuksen tarkastelun näkökulma, jolle luodaan perusteita tämän luvun tarkastelun avulla.

Tutkijan ennakkokäsityksen mukaan kyberterrorismin määritelmä vaihtelee tilanteen ja määrittelijän mukaan. Tutkimuksen aikana tämä on käynyt hyvin selville ja on ollut helppo yhtyä aiempiin näkemyksiin siitä, että kyberterrorismia on määritelty useiden eri tutkijoiden ja organisaatioiden toimesta useilla eri tavoilla määrittelijöiden oman tarpeen mukaisesti (Samuel, Osman, Al-Khasawneh & Duhaim, 2014).

4.1 Kyberterrorismi erilaisissa lähteissä

Kyberterrorismi on melko uusi käsite. Siitäkin huolimatta ensimmäiset määritelmät kyberterrorismille on löydettävissä jo 1980-luvulta. Yleisen näkemyksen mukaan kyberterrorismi käsitteen on määritellyt ensimmäistä kertaa vuonna 1982 Barry Collin. Hänen määritelmänsä perustui fyysisen ja kybermaailman yhdistämiseen (Samuel ym., 2014).

Sen jälkeen kyberterrorismia on käsitelty ja määritelty useissa kirjoissa ja artikkeleissa pienenä osana laajempaa kokonaisuutta. Esimerkkinä tämän kaltaisesta teoksesta voidaan pitää Bel G Raggadin (2010) kirjoittamaa kirjaa Information Security Management. Kyseinen kirja on käytössä Jyväskylän yliopistossa informaatioturvallisuuden hallinnan opintojaksoilla ja se määrittelee kyberterrorismin hyökkäykseksi henkilöä tai tietoverkkoja vastaan pääasiassa internetin kautta tavoitteena aiheuttaa haittaa tai vahinkoa terroristien päämäärän saavuttamisen tueksi.

Nykyisin on löydettävissä myös kirjoja, jotka käsittelevät ensisijaisesti kyberterrorismia. Haifan yliopiston professorin, Gabriel Weimannin (2015) teos Terrorism in Cyberspace on yksi tällaisista kirjoista. Teoksessaan professori Weimann määrittelee, että yleisesti kyberterrorismilla tarkoitetaan tietokoneiden ja tietoverkkojen käyttämistä kansallisen kriittisen infrastruktuurin tai valtion operaatioiden sabotoimiseen. Lisäksi hän määrittelee, että yksinkertaisimmillaan kyberterrorismi on kyberteknologian käyttämistä terrorismissa.

Tieteellisten julkaisujen lisäksi kyberterrorismia on käsitelty ansiokkaasti myös kybertoimintaympäristöä käsittelevillä internet-sivustoilla ja niillä esiintyvissä blogikirjoituksissa. Esimerkkinä tällaisesta toimii Paul Curranin (2016) kirjoitus kyberterrorismin uhkan todellisuudesta. Curranin (2016) näkemyksen mukaan kyberterrorismia on mikä tahansa internet-terrorismin toimi, johon liittyy tahallinen ja laaja hyökkäys ja tietoverkkojen häirintä tietokonevirusten avulla tai fyysinen hyökkäys haittaohjelmien avulla yksilöitä, hallintoa tai organisaatioita kohtaan. Curran (2016) arvioi, että kyberrikollisia motivoi taloudellinen hyöty, hakkerointia ja internetvandalismia tehdään usein tyydyttämään hakkerin egoa, mutta kyberterrorismin polttoaineena toimii ideologia. Terrorismin tavoitteena on luoda pelon tunne kohteisiinsa. Tämä periaate huomioiden on helpompi erotella kyberterrorismiin kuuluvat vahinkoa ja tuhoa tavoittelevat kyberhyökkäykset sellaisista, joiden tavoitteena on taloudellinen tai maineellinen hyöty.

Valtaosa kyberterrorismia käsittelevästä aineistosta muodostuu kuitenkin erilaisista artikkeleista, joista pääosa on julkaistu joko tieteellisissä lehdissä tai tutkimuksiin liittyvien konferenssien julkaisuissa. Esimerkkejä tämän kaltaisesta lähdeaineistosta on tämänkin luvun sisällä lukuisia.

4.2 Kyberterrorismin osatekijät

Kyberterrorismin käsitteen tarkastelussa on pyritty löytämään erilaisia tapoja, joiden avulla käsitettä voidaan jakaa pienempiin osakokonaisuuksiin. Vanhin jaottelu on löydettävissä Gordonin ja Fordin (2003) laatimasta Symantecin raportista. Raportti on valittu mukaan tutkimuksen lähdeaineistoon, koska sen sisältöä on lainattu useissa uudemmissa aihealuetta käsittelevissä tutkimuksissa. Symantecin raportin mukaan kyberterrorismi on jaoteltu seitsemään osaan, jotka ovat: tekijä, tekopaikka, toiminta, työkalut ja välineet, kohde, kuuluminen organisaatioon ja motivaatio.

Seuraava tutkimukseen valittu kyberterrorismi-käsitteen jaottelu osakokonaisuuksiin oli löydettävissä noin kymmenen vuotta uudemmasta materiaalista. Vuodelta 2012 löytyi artikkeli, jossa kyberterrorismi oli jaettu viiteen kriittiseen osatekijään. Ne olivat hyökkäyksen kohde, hyökkäyksen motivaatio ja tavoitteet, vaikutus, käytetyt keinot ja välineet sekä hyökkäyksen toimialue, jolla voidaan tarkoittaa hyökkäyksen ympäristöä tai toimintamenetelmää. Kyberterrorismia voidaan määritellä myös tunnistamalla hyökkäyksen profiili tai motivaatio. Artikkelin laatinut tutkijaryhmä täsmentää kuitenkin, että kaikki edellä mainitut osatekijät on löydettävä arvioitavasta teosta, jos teko halutaan luokitella kyberterrorismiksi. (Ahmad, Yunos & Sahib, 2012.)

Samalta vuodelta eli vuodelta 2012 on löydettävissä myös Veerasamy, Groblerin ja Von Solmsin (2012) jaottelu kyberterrorismin pääosista. Heidän mielestään kyberterrorismi koostuu tekijästä, kybertapahtumasta, tavoitteesta, motivaatiosta, suoritetuista toimenpiteistä, vaikutuksista ja kohteesta. Tutkijaryhmän mukaan on tärkeää kyetä erottamaan, onko teko kyberterrorismia vai onko kyseessä kybertoimintaympäristössä tapahtuva tapahtuma, joka yleisesti tukee terrorismia. Tähän tekojen luokittelemiseen tutkijat käyttävät määrittelemistään kyberterrorismin osista motivaatiota, tavoitetta, kohdetta, vaikutusta ja suoritettuja toimenpiteitä.

Uusin tutkimuksessa käytetty kyberterrorismin jaottelu ja samalla yksi tuoreimmista kyberterrorismin määritelmistä oli löydettävissä International Journal of Cyber Warfare and Terrorism –aikakausilehdestä. Lehdestä löytyi tutkijaryhmän vuonna 2016 laatima artikkeli, jossa pyrittiin luokittelemaan kyberterrorismia ja siihen kuuluvia osakokonaisuuksia. Artikkelissa kyberterrorismi koostui viidestä osasta, jotka olivat kohde, motiivi, keinot, vaikutus ja tarkoitus. Näiden myötä artikkelin määritelmän mukaan kyberterrorismin kohteena on kriittinen kansallinen infrastruktuuri tai muu valtion hallinnon omaisuus. Kyberterrorismilla on psykologinen, sosiaalinen, poliittinen tai uskonnollinen motiivi ja se käyttää keinoinaan tietokoneita, tietoverkkoja ja teknologiaa. Kyberterrorismin vaikutuksena ja tarkoituksena on aiheuttaa vahinkoa yksittäisille henkilöille tai ryhmille sekä fyysisesti vahingoittaa infrastruktuuria ja omaisuutta. (Al Mazari, Anjariny, Habib & Nyakwende, 2016.)

Ahmad, Yunos ja Sahibin (2012) esittämä jaottelu poikkesi hieman uudemmasta, ja sen avulla kyberterrorismin määritelmä voisi muodostua erilaiseksi

kuin uudemman, vuoden 2016 artikkelin jaottelun mukaan. Pääosin jaottelut ovat samanlaisia, mutta vanhemmassa Ahmadin ja kumppaneiden esittämässä jaottelussa kyberterrorismin varsinaista tarkoitusta ei erikseen tarkastella, vaan se kuuluu kohtaan, jossa tarkastellaan motivaatiota ja tavoitteita. Lisäyksenä uudempaan jaotteluun sen sijaan löytyy hyökkäyksen toimialueen tarkastelu, jota vuoden 2016 jaottelussa ei varsinaisesti erillisenä ole, mutta joka voitaisiin laveasti tulkittuna arvioida löytyvän kohdasta keinot. Toisaalta on kuitenkin huomioitava, että Ahmadin ja kumppaneiden (2012) esittämässä jaottelussa keinot ja välineet tarkastellaan jo omana erillisenä kohtanaan, joten täysin samankaltaisesta asiasta ei siis ole kyse.

Uusimman Al Mazari ja kumppaneiden (2016) esittämä kyberterrorismin määritelmä on tutkimuksen aikana osoittautunut hyvin haasteelliseksi. Kyseessä on hyvin lavea tulkinta kyberterrorismista ja kyseisen määritelmän mukaan kaikki kyberhyökkäykset ovat samalla myös kyberterrorismia. Tämä näkemys ei kuitenkaan saa kannatusta monissa muissa tutkimusartikkeleissa. Esimerkiksi Veerasamyn ja Groblerin (2015) mukaan usein kyberhyökkäykset luokitellaan kyberterrorismiksi ilman, että hyökkäysten motiivia ja tavoitetta on tosiasiallisesti edes tarkasteltu.

4.3 Erilaisia lähestymistapoja kyberterrorismiin

Denningin (2000) esittämän näkemyksen mukaan kyberterrorismi on terrorismin ja kybertoimintaympäristön lähentymistä. Lisäksi Denning täsmentää, että jotta voisimme ymmärtää kyberterrorismin uhkaa, tulee meidän tarkastella kahta sen osatekijää. Ensimmäisenä täytyisi kyetä tunnistamaan sellaiset hyökkäyksen kohteet, jotka ovat haavoittuvia ja joiden avulla voisi aiheutua vakavia vahinkoja tai väkivaltaa. Toiseksi tulisi tunnistaa sellaiset toimijat, joilla olisi sekä kapasiteettia että motivaatiota toteuttaa tämän kaltaisia hyökkäyksiä. Tämä tutkimuksen pääasiallista lähdemateriaalia vanhempi lähde on valittu käyttöön myös tähän tutkimukseen, koska se on tullut tutkimuksen aikana vastaan alkuperäisenä lähteenä useissa eri artikkeleissa.

Denningin (2012) näkemyksen mukaan poliittisesti motivoitua kyberhyökkäystä voidaan pitää kyberterrorismina siinä tapauksessa, että se herättää pelkoa samalla tavalla kuin fyysiset ja väkivaltaiset terrorihyökkäykset kuten pommiiskut. Esimerkkinä tämän kaltaisista kyberhyökkäyksistä Denning mainitsee suuret sähkökatkot, kaasuputkien räjähtämiset, junien raiteilta suistumiset, lento-onnettomuudet ja kyberhyökkäykset, jotka aiheuttavat huomattavat taloudelliset vahingot. Sen sijaan internetsivujen käyttöhäiriöt ja –katkokset eivät Denningin näkemyksen mukaan ole kyberterrorismia.

Rollins ja Wilson (2007) määrittelivät kyberterrorismin kahdella erilaisella lähestymistavalla eli perustuen teon vaikutuksiin ja tavoitteisiin. Vaikutuksiin perustuvassa määritelmässä kyberterrorismia ovat tietokonehyökkäykset, joiden seuraamukset ovat niin laajoja, että ne aiheuttavat perinteisten terrori-iskujen

kaltaista pelkoa, vaikkakin toteuttajana olisivat rikolliset. Tavoitteisiin perustuvassa määritelmässä kyberterrorismia ovat laittomat tai poliittisesti motivoidut tietokonehyökkäykset, joiden tavoitteena on aiheuttaa pelkoa ja pakottaa hallintoa tai ihmisiä hyökkääjien poliittisiin tavoitteisiin tai aiheuttaa vakavaa haittaa tai vakavia taloudellisia vahinkoja.

Talihärm (2010) pitää kuitenkin Rollinsin ja Wilsonin esittämiä määritelmiä liian pitkälle yksinkertaistettuina. Hänen mukaansa erityisen mielenkiintoista on se, että vaikutuksiin perustuvassa määritelmässä ei ole minkäänlaista mainintaa poliittisesta tai sosiaalisesta teon motiivista. Talihärmin näkemyksen mukaan tällä hetkellä kyberterrorismin käsitteen teoreettinen määritelmä eroaa siitä, kuinka terroristit hyödyntävät internettiä. Talihärm arvioi että, vaikkakin kyberhyökkäykset muodostavat kasvavan kiusan, niistä yksikään ei ole aiheuttanut yleisesti kyberterrorismin käsitteissä asetettuja vaatimuksia aiheutetuista vahingoista. Huolimatta väitteistä, joiden mukaan kyberterrorismi on ainoastaan median jatkuvan esilletuonnin ja liioittelun tuote, se on ideana ollut olemassa julkisuudessa jo vuosikymmeniä. Hänen näkemyksensä mukaan kyberterrorismi käsitteen käyttöä yksittäisten kybertapahtumien kuvaamiseen kannattaisi välttää, kunnes sille on olemassa todelliset perusteet niin poliittisen tai sosiaalisen motivaation kuin vahinkojen ja pelon aiheuttamisen suhteen.

Luokiteltaessa kyberterrorismia tekijän suhteen, tarkastelun kohteena ovat muun muassa se, onko teon tekijä tehnyt teon yksin vai toiminut osana ryhmää, onko kyseessä siviili vai sotilas ja onko teko kansallinen vai kansainvälinen. Tekopaikkaa tarkasteltaessa teko voi käytännössä olla kolmea eri tyyppiä. Se voi olla toteutettu digitaalisessa maailmassa siellä sijaitsevaa kohdetta vastaan. Kyseessä voi olla myös teko, jossa digitaalisesta maailmasta hyökkäys kohdistetaan fyysistä kohdetta vastaan. Lisäksi on myös mahdollista, että teko tehdään vaikuttamalla fyysisellä kohteella digitaaliseen maailmaan. Jo aiemmin esitetyn Denningin (2000) näkemyksen mukaan kyberterrorismi on kybertoimintaympäristön ja terrorismin lähentymistä tai yhdistymistä. Tässä tutkimuksessa se tarkoittaa käytännössä sitä, että jotta teko voisi olla kyberterrorismia, täytyy se tapahtua kybertoimintaympäristössä.

Kyberhyökkäyksiin ja näin ollen myös kyberterrorismiin käytettyjen työkalujen ja välineiden kirjo on valtava. Näiden järjestelmällinen luokittelu ja tutkiminen vaatisivat oman erillisen tutkimuksen. Tämän tutkimuksen osalta on noudatettu Ahmadin, Yonusin ja Sahibin (2012) esittämää näkemystä siitä, että tietokoneiden rooli terrorihyökkäyksen kokonaisuutta arvioitaessa on tärkeä osatekijä arvioitaessa onko teko kyberterrorismia. Ahmadin ja kumppaneiden näkemyksen mukaan terrorihyökkäysten osana voivat olla kaikki mahdolliset kyberhyökkäysten muodot madoista palvelunestohyökkäyksiin ja bottiverkkojen hyödyntämiseen. Myös Limnell ja kumppanit (2014) painottavat tietokoneiden roolia kyberterrorismissa. Heidän mukaansa kyberterrorismin todennäköisin ase on tietokone, jota voidaan käyttää joko suoran tai epäsuoran vahingon aiheuttamiseen tai tukemaan muuta toimintaa.

Yleinen käytetty tapa kyberterrorismin määrittelyyn on tehdä se hyökkäysten kohteiden ja aiheutettujen vahinkojen avulla. Hyökkäyksen kohteiden näkökulmasta kyberterrorismi voidaan määritellä kybertoimintaympäristön käyttämiseksi hyökkäyksiin sellaista kriittistä infrastruktuuria kohtaan, jota ilman valtio tai organisaatiot eivät voi toimia (Samuel ym., 2014). Toisen samankaltaisen määritelmän mukaan kyberterrorismi voitaisiin ymmärtää laittomiksi hyökkäyksiksi tai niiden uhaksi tietokoneita, tietoverkkoja ja niiden sisältämää informaatiota kohtaan hallinnon tai väestön uhkailemiseksi tai pakottamiseksi terroristien sosiaalisten tai poliittisten tavoitteiden edistämistä varten. Tällaisessa muodossa määritelmä ei juurikaan eroa sen yllä olevasta. Kun määritelmään lisätään vaatimus siitä, että ollakseen kyberterrorismia hyökkäyksen tulee olla väkivaltainen hyökkäys joko ihmisiä tai omaisuutta kohtaan ja sen tulee aiheuttaa riittävästi vahinkoa pelon lietsomiseen, se muuttuu luonteeltaan oleellisesti aiemmasta (Denning, 2000).

Denningin (2000) määritelmän mukaan aiheutetut vahingot ja hyökkäyksen tulokset ovat siis avainasemassa kyberterrorismia määriteltäessä. Vieläkin laajemmassa määritelmässä voidaan kyberterrorismista puhua internetin käytöllä lisätyn perinteisen terrorismin määritelmän avulla. Tämän kaltaisen määritelmän mukaan kyberterrorismia on mikä tahansa poliittisesti tai sosiaalisesti motivoitu informaatioteknologian avulla toteutettu tietokoneita, tietoverkkoja tai informaatiojärjestelmiä vastaan kohdistettu hyökkäys, jonka seurauksena on ei-sotilashenkilöihin kohdistuvaa väkivaltaa, josta heille koituu vammoja, verenvuodatusta, vakavia loukkaantumisia tai pelkoa (Samuel ym., 2014). Tämän kaltaisessa kyberterrorismin määritelmässä aiheutetut vahingot ja hyökkäyksen kohteet ovat määriteltyjä. Lisäksi sen mukaan kyberterrorismin ensisijainen hyökkäyksen kohde on nimenomaan tietokoneet, tietoverkot ja erilaiset informaatiojärjestelmät, joiden avulla vahinkoa ihmisille aiheutetaan.

Perinteistä terrorismia arvioidaan usein hyökkääjän motivaation ja tavoitteiden kautta. Ahmadin ja kumppaneiden näkemyksen mukaan kyberterrorismin näkökulmasta hyökkääjän tai hyökkäävän ryhmän motivaatio tulee olla selkeästi poliittinen tai voimakkaasti ideologinen, jotta teko voitaisiin mieltää kyberterrorismiksi. (Ahmas ym., 2012). Veerasamy kumppaneineen (2012) puolestaan määrittelee, että teon motivaation tulee olla vahvasti uskonnollinen, sosiaalinen tai poliittinen. Tavoitteiden osalta tarkasteltaessa kyberterroristien hyökkäyksen varsinaisia tavoitteita voivat olla mm. tuhoaminen, häiriön tai pelon aiheuttaminen ja vaikkapa protestointi. Sen lisäksi hyökkäyksellä voi olla varsinaisia tavoitteita tukevia tavoitteita, kuten tiedon- tai rahoituksen hankinta, propaganda, harjoittelu ja uusien jäsenien rekrytoiminen.

Kyberterrorismia voidaan arvioida myös teon vaikutusten kautta. Vaikutuksia voidaan arvioida esimerkiksi vaikutusten suuruuden kautta tai tarkastelemalla fyysisiä, tietoteknisiä tai psykologisia vaikutuksia. Veerasamy ja kumppanit (2012) käyttivät vaikutuksien suuruuden jaotteluun neljäasteista taulukkoa, jossa heikoin taso ei aiheuttanut lainkaan vaikutusta, sen jälkeen aiheutui pieniä vaikutuksia, joista kuitenkin kyettiin palautumaan. Kolmas taso on huomattavat vaikutukset, joita ovat suuret taloudelliset tappiot tai maineen menettäminen.

Neljäs taso on katastrofaaliset vaikutukset, jotka estävät kohteen toiminnan pysyvästi. Lisäksi tutkijat arvioivat, että ainoastaan kolmannen tai neljännen tason eli huomattavat tai katastrofaaliset vaikutukset aiheuttava teko voidaan määritellä kyberterrorismiksi.

Myös kyberterrorismin ja kyberhyökkäysten välistä eroa on pyritty tutkimaan ja yritetty määritellä. Yhdessä tällaisessa tutkimuksessa pyrittiin muodostamaan looginen testaustyökalu, jolla kyettäisiin tunnistamaan sellaiset kyberhyökkäykset, jotka ovat myös kyberterrorismia. Yksinkertaisuudessaan tämä työkalu määrittelee yksittäiset tapaukset annettujen ohjeiden avulla kyberterrorismiksi tai sitten ei. (Veerasamy & Grobler, 2015.) Haasteellisen tämän työkalun käyttämisestä tekee kuitenkin se, että sen määrittely perustuu täysin käyttöön annettuun kyberterrorismin määritelmään.

Warwickin yliopiston tutkijan Yaroslav Shiryaevin mukaan kyberterrorismilla tarkoitetaan valtioiden, ei-valtiollisten ryhmien, yhtiöiden ja yksilöiden toteuttamia kyberhyökkäyksiä, jotka rikkovat nykyisiä lakeja ja sääntöjä (MacDonald, Jarvis & Chen, 2013). Tyypillistä kaikelle terrorismille, niin perinteiselle kuin kyberterrorismille, on se, että se tapahtuu yleisesti hyväksyttyjen yhteiskunnan sääntöjen ulkopuolella. Tämä osaltaan vaikeuttaa yksittäisten tekojen määrittelyä terrorismiksi (Veerasamy & Grobler, 2015).

Gordon ja Ford (2003) tuovat esille, että laajan tulkinnan mukaan myös Yhdysvaltoja vastaan syyskuun 11. päivä vuonna 2001 tehdyt iskut olisivat kyberterrorismia, sillä tietokoneilla ja erityisesti internetillä oli merkittävä rooli hyökkäysten suunnittelussa, valmistelussa ja toteutuksessa. Tämä näkemys eroaa kuitenkin nykyisin pääasiassa käytössä olevasta käsityksestä siitä, mikä on kyberterrorismia.

Kyberterrorismi tarkoittaa eri asiaa eri ihmisille. Tässä tutkimuksessa kyberterrorismi on määritelty siten, ettei kaikkia kybertoimintaympäristön toimia voida pitää kyberterrorismina. Lisäksi lähtökohtana määrittelyssä on ollut se, että myöskään kaikki kyberhyökkäykset eivät ole välttämättä kyberterrorismia (Veerasamy & Grobler, 2015). Tässä tutkimuksessa kyberterrorismi on yksilöiden tai ryhmien kybertoimintaympäristössä tai sen avulla harjoittamaa poliittisesti, uskonnollisesti tai ideologisesti motivoitua väkivaltaa häiriön, tuhon ja pelon saavuttamiseksi kohteissaan.

4.4 Puhdas kyberterrorismi

Puhdas kyberterrorismi, eli terroristiset toimet, jotka toteutetaan kokonaan kybertoimintaympäristössä, on se kyberterrorismin muoto, jota useimmat aihealueesta kirjoittavat henkilöt tarkoittavat tarkastellessaan kyberterrorismin aiheuttamia uhkia (Gordon & Ford, 2003).

Kyberterrorismi käsitettä on käytetty kuvaamaan kaikkea yksinkertaisista hakkerointi yrityksistä vaarallisiin taloudellista vahinkoa ja verenvuodatusta tavoitteleviin kyberhyökkäyksiin. Käsitteelle on olemassa useita erilaisia määritelmiä, jotka voidaan jakaa kuitenkin kahteen pääryhmään. Ensimmäinen ryhmä määrittelee kyberterrorismin poliittisesti ja sosiaalisesti motivoiduiksi hyökkäyksiksi tietokoneita, tietoverkkoja ja informaatiota kohtaan. Hyökkäykset voidaan toteuttaa joko tietokoneiden avulla tai fyysisellä väkivallalla, ja ne aiheuttavat henkilövahinkoja, vakavaa tuhoa ja pelkoa. Toinen ryhmä määrittelee puolestaan kyberterrorismiksi kaikki toimet, joissa internetiä tai tietokoneita käytetään terrori-iskujen organisoimiseen ja toteutukseen. (Talihärm, 2010)

Vastaavanlaisen jaottelun esittelevät myös Limnéll ja kumppanit (2014). Myös he käyttävät kyberterrorismi-käsitteen rinnalla käsitettä puhdas kyberterrorismi, jolla tarkoitetaan sellaista kyberterrorismin muotoa, jossa tietoteknologia on joko ase tai hyökkäyksen kohde. Limnéll ja kumppanit painottavat, että joidenkin tutkijoiden mielestä tämä varsinainen kyberterrorismi on tärkeää erottaa tietoteknologian käyttämisestä terroristisiin toimiin tai niiden edesauttamiseen.

Kontselidzen (2015) näkemys kyberterrorismista on hyvin puhtaan kyberterrorismin suuntainen, joskin siinä on määritelty poikkeuksellisen tarkasti kyberterrorismin vaikutuksia. Kontselidzen mukaan kyberterrorismina voidaan pitää tietokonehyökkäyksiä, joista aiheutuu tuhoa, kuolemia, laaja-alainen sähkökatkos, lento-onnettomuus, laaja-alainen veden saastuminen tai luottamuksen romahtaminen yleistä taloutta kohtaan.

Kyberterrorismina voidaan pitää ihmisten motiivien ja informaatioteknologian yhdistämistä terroristisiin toimiin kybertoimintaympäristössä. Samankaltainen ja jo aiemmin esitelty määritelmä on löydettävissä Gordonin ja Fordin tekemästä Symantecin raportista käsitteelle puhdas kyberterrorismi. (Bogdanoski & Petreski, 2013.)

Bogdanoskin ja Petreskin (2013) mukaan hyvin yleisiä ovat väitteet siitä, että kyberterrorismia ei ole olemassakaan ja kyseessä on tosiasiassa hakkerointi ja haitalliset hyökkäykset. Kyberterrorismin vastustajien mukaan todennäköisyys pelon, vakavien fyysisten vahinkojen tai jopa kuoleman tuottamiseen elektronisten apuvälineiden avulla on hyvin pieni, otettaessa huomioon nykyiset ennalta ehkäisyyn ja huolenpitoon varatut teknologiat.

Bogdanoskin ja Petreskin (2013) näkemyksen mukaan kyberterrorismi on tehokkaimmillaan yhdistettynä fyysiseen terrorismiin. Tämä voisi tarkoittaa esimerkiksi sitä, että ensiapujärjestelmiä vastaan kohdistetaan hyökkäys, joilla niiden toimintakyky lamautetaan juuri silloin kun fyysinen terroristihyökkäys on aiheuttanut niille suuren käyttötarpeen. Toisaalta tutkijat kuitenkin arvioivat, että useimmiten terroristijärjestöt käyttävät informaatioteknologiaa ja internettiä rahoituksen hankkimiseen, propagandan levittämiseen ja turvattuun yhteydenpitoon

Kyberterrorismin käsitteen rajaaminen ainoastaan puhtaaseen kyberterrorismiin heikentää kykyämme puolustautua kyberterrorismin aiheuttamilta uh-

kilta. Gordonin ja Fordin (2003) mukaan suurimman uhkan aiheuttavat kuitenkin puhdas kyberterrorismi-käsitteen ulkopuolelle jäävät, useat muut tietokoneiden hyväksikäytön ja terrorismin yhdistelmät.

4.5 Kyberterrorismin haasteet

Yhteinen kyberterrorismin luonteenpiirteiden ymmärryksen puute on estänyt tehokkaan vuoropuhelun aiheesta ja lopulta johtanut kyberterrorismia koskevien käsitteiden sekasotkuun. Talihärmin (2010) esittämän näkemyksen mukaan maailma ei ole vielä kokenut selvää kyberterrori-iskua ja sen takia kyberterrorismin käsitteet ja lähestymistavat ovat teoreettisia. Käytännössä tapahtuneet kyberhyökkäykset ovat ainoastaan sisältäneet joitain kyberterrorismin osatekijöitä kuten poliittinen motivaatio tai pelon ja vahinkojen aiheuttaminen. Tämän lisäksi terroristit ovat käyttäneet internettiä tukemaan ja toteuttamaan tavoitteitaan.

Hyvänä esimerkkinä erilaisista tulkinnoista kyberterrorismin ja kyberhyökkäyksien suhteen voidaan pitää vuonna 2000 Australiassa tapahtunutta viemäröintijärjestelmää vastaan tehtyä hyökkäystä, jossa entinen työntekijä pumppasi miljoonia litroja puhdistamatonta viemärivettä vesistöön aiheuttaen huomattavia vahinkoja. Talihärmin (2010) esittämän näkemyksen mukaan tekoa ei voida luokitella kyberterrorismiksi ainoastaan sen takia että se on toteutettu internetin välityksellä ja se on aiheuttanut huomattavia vahinkoja. Sen sijaan Veerasamy ja kumppanit (2012) arvioivat kaksi vuotta myöhemmin, että kyseessä olisi kyberterrorismi. Heidän perusteluiden mukaan teko oli sosiaalisesti motivoitu, se aiheutti huomattavaa vahinkoa, teko kohdistui yhteiskunnan kriittisiin rakenteisiin ja sen pyrkimyksenä oli nimenomaan haitan aiheuttaminen. Myös Bogdanoski ja Petreski (2013) käyttävät kyseistä tapausta esimerkkinä kyberterrorismista.

Kyberterrorismin määrittelyssä erimielisyyttä on aiheuttanut se, tuleeko teon aiheuttaa fyysistä vahinkoa, jotta se voidaan määritellä kyberterrorismiksi. Fyysistä vahinkoa kannattavien mielipiteiden ajatuksena on se, että fyysistä vahinkoa tarvitaan todellisen pelon aiheuttamiseen. Näiden näkemysten mukaan terrorismi aiheuttaa psykologisesti pelon, kauhun ja surun tuntemuksia juuri sen takia, että siviileihin kohdistetut väkivaltaiset terroriteot vaikuttavat sattumanvaraisilta ja järjettömiltä (Veerasamy & Grobler, 2015). Lisäksi Denning (2012) on esittänyt näkemyksen siitä, että jotta poliittisesti motivoitu hyökkäys voitaisiin määritellä kyberterrorismiksi, tulisi sen aiheuttaa väkivaltaisen fyysisen hyökkäyksen kaltaista pelkoa. Denningin uudemman näkemyksen mukaan fyysinen väkivalta itsessään ei ole välttämättömyys, mutta samankaltaisen pelon aiheuttaminen on. Samankaltaista ajatusmaailmaa tukee myös ajatus siitä, että kyberterrorismi ei aina tarvitse toteutettua hyökkäystä osakseen vaan joissain tapauksissa kyberterrorismiksi voidaan määritellä jopa pelkkä hyökkäyksen uhka (Veerasamy & Grobler, 2015).

Vuonna 2013 pidetyssä kyberterrorismia käsitelleessä konferenssissa Alexandros Kyriakidis Sheffieldin yliopistosta toi esille myös sen, että kyberterrorismilla ei ole olemassa määritelmää kansainvälisissä lakisäädöksissä. Hän myös kertoi lukuisista mahdollisuuksista, joissa kyseinen käsite olisi voitu määritellä esimerkiksi Yhdistyneiden kansakuntien (YK), Pohjois-Atlantin liiton (NATO) tai jonkin muun kansainvälisesti tunnustetun organisaation toimesta. Näin ei kuitenkaan ole tapahtunut. (MacDonald, Jarvis & Chen, 2013.)

Valtion roolilla voi olla merkitystä myös kyberterrorismin määrittelyssä, aivan kuten Ruby (2002) käytti valtion roolia yhtenä merkitsevänä tekijänä perinteisen terrorismin määrittelyssä päätyen johtopäätökseen, että valtio ei voi syyllistyä terrorismiin. Elizaveta Huttenlocher (2016) on esittänyt näkemyksen, jonka mukaan juuri valtion rooli määrittää eron kybersodankäynnin ja kyberterrorismin välillä. Hänen mukaansa kybersodankäynti on kyseessä tilanteessa, jossa valtio virallisesti liittää kybertoimijat osaksi asevoimiaan. Sen sijaan tilanteissa, joissa valtiot rekrytoivat kybertoimijoita toimimaan epävirallisesti valtion asialla, kyseessä on kyberterrorismi. Huttenlocher ei esitä muuta keinoa kybersodankäynnin ja kyberterrorismin erottamiseen. Sen lisäksi hän ei myöskään ota kantaa siihen, miten kyberhyökkäykset asemoituisivat osaksi tätä jaottelua.

Kyberterrorismia ei kuitenkaan aina verrata kybersodankäyntiin tai kyberhyökkäyksiin. Yksi tapa määritellä kyberterrorismia on Yhdysvaltojen liittovaltion rikospoliisin eli FBI:n käyttämä määritelmä kyberterrorismista rikollisena toimintana. FBI:n määritelmän mukaan kyberterrorismi on rikollista toimintaa tietokonejärjestelmiä ja tietoliikenneverkkoja hyödyntäen, minkä seurauksena syntyy väkivaltaa, tuhoa ja häiriöitä erilaisille palveluille tavoitteena aiheuttaa hämmennystä ja epävarmuutta kohteena olevaan ryhmään tai väestöön. Kaiken tämän tavoitteena on motivoida hallintoa tai muuta väestöä mukautumaan kyberterroristien poliittiseen, sosiaaliseen tai ideologiseen päämäärään. (US Army TRADOC, 2006.)

Kansainvälisen yhteisön taistelussa kyberterrorismia vastaan todella tärkeänä tekijänä on kyberterrorismin määritteleminen osana kansainvälistä lainsäädäntöä. Lisäksi kehittyneet käyttötapaohjeet ja strategiat muodostavat tehokkaan vastapelotteen kyberterrorismin aiheuttamia uhkia kohtaan. (Ahmad, Yunos & Sahib, 2012.) Mikäli kyberterrorismi katsotaan rikolliseksi toiminnaksi, palataan taas siihen faktaan, ettei kyberterrorismille ole olemassa määritelmää kansainvälisessä lainsäädännössä. Näin ollen kyberterrorismia tarkastellaan kansallisten rikoslainsäädäntöjen valossa, ja se taas johtaa ilmiön erilaiseen tulkintaan eri viitekehyksissä. (Limnéll ym., 2014.)

Aiemmin esitellyistä perinteisen terrorismin määrittelyn haasteista huolimatta, Limnéll ja kumppanit (2014) arvioivat, että mikäli kyberterrorismi rinnastetaan terrorismiin, se viittaa vain hyökkäyksiin, jotka uhkaavat elämää tai omaisuutta, ja joilla vaikutetaan hyökkäyskohteen tietojärjestelmiin tai niiden sisältämään informaatioon fyysisen vahingon aikaansaamiseksi. Heidän lähtökohtanaan on näkemys siitä, että terrorismi on määritelmällisesti yleensä väkivaltaista tai sisältää väkivallan uhkan. Limnéll ja kumppanit kuitenkin painottavat, että ei

ole kuitenkaan yksiselitteistä, mitä väkivallalla virtuaalisena ilmiönä tarkoitetaan.

Kyberterrorismin määrittelyä, kuten perinteistä terrorismiakin, voidaan lähestyä myös sosiaalisesta ja kulttuurillisesta näkökulmasta väkivallan sijaan. Tällöin kyberterrorismiksi voidaan määritellä esimerkiksi organisaation verkkosivujen turmeleminen, sekä sähköpostin ja sosiaalisen median avulla väärien huhujen levittäminen valituista sosiaalisista kohteista (Jalil, 2003). Erään uuden tutkimuksen mukaan juuri kyberhyökkäykset, joiden tavoitteena on pilata kohteeksi valitun yksilön, organisaation, yhteisön tai kulttuurin imagoa ja mainetta, ovat yksi aliarvioitu kyberterrorismin muoto (Al Mazari, Anjariny, Habib & Nyakwende, 2016).

Kyberterrorismin käsite menettää merkityksensä, jos sillä viitataan mihin tahansa tietoteknologiapohjaiseen toimintaan hallintoa tai muuta auktoriteettia vastaan. Limnéll ja kumppanit (2014) liittävät kyberterrorismin terrorismiin ja painottavat, että siihen kuuluu olennaisena osana jonkinlainen näyttävyys ja julkisuushakuisuus. Heidän mukaan kyberterrorismia määriteltäessä onkin syytä muistaa, että hyökkäykset ovat etukäteen suunniteltuja, tavoitteiltaan poliittisia, sosiaalisia, uskonnollisia tai ideologisia, useimmiten pienten ryhmittymien suorittamia, ja niiden tarkoitus on kiinnittää huomiota johonkin asiaan, levittää pelkoa tai vaikuttaa väestöön ja päätöksentekijöihin.

4.6 Johtopäätöksiä eli mitä on kyberterrorismi?

Kyberterrorismi tarkoittaa tilanteesta ja olosuhteista riippuen eri asiaa eri ihmisille. Se voidaan määritellä useilla eri tavoilla ja sen määrittelyssä voidaan painottaa useita eri osatekijöitä tilanteesta ja tarpeesta riippuen. Käsitteen epämääräisyyden ja väärinymmärrysten välttämiseksi käsitettä ei tulisi joko käyttää tai sitten se tulisi tarkkaan määritellä ennen käyttämistä. Monissa tilanteissa kyberterrorismi käsitteen käyttämisen sijaan asia voidaan kuvata kyseiseen tilanteeseen liittyen jollakin aiheeseen liittyvällä tarkemmalla ja helpommin ymmärrettävällä käsitteellä.

Tässä tutkimuksessa kyberterrorismi on yksi kybertoimintaympäristön uhkista ja erotettavissa kybersodankäynnistä, kyberrikollisuudesta, kybervakoilusta ja kybervandalismista, vaikkakin tarkkojen rajojen määrittäminen näiden välille voi olla haastavaa. Kyberterrorismia on käsitelty useissa erilaisissa lähteissä ja käsiteltävän lähteen taustat ja tavoitteet voivat myös osaltaan määrittää kyberterrorismi käsitteen määrittelyä. Tässä tutkimuksessa valtaosa lähdemateriaalista muodostuu tieteellisistä artikkeleista, joissa lähes poikkeuksetta on määritelty kyberterrorismi käsitteenä, vaikkakin nämä määritelmät poikkeavat jopa huomattavasti toisistaan eri julkaisujen välillä.

Tässä tutkimuksessa Yhdysvaltain armeijan määritelmää perinteiselle terrorismille on käytetty kyberterrorismin määritelmän taustalla sekä vertailtaessa erilaisia lähdeaineistoista löytyviä kyberterrorismin määritelmiä. Sen mukaan

terrorismi on väkivaltaa, joka tapahtuu normaalin lainsäädännön määräämien rajojen ja tavanomaisen sotilaallisen käyttäytymisen ulkopuolella (US Army TRADOC, 2007). Tässä tutkimuksessa tätä määritelmää on täsmennetty kyberterrorismiksi siten, jotta teko voisi olla kyberterrorismia, täytyy se tapahtua kybertoimintaympäristössä.

Erilaisista tutkimuksessa käytetyistä lähteistä useissa kyberterrorismin määrittelyn taustalla on hyödynnetty joko Denningin (2000) Yhdysvaltain kongressille pitämää todistusta aihealueesta tai Gordonin ja Fordin (2003) julkaisemaa Symantecin raporttia. Kuten jo aiemmin todettu nämä kaksi lähdettä on valittu mukaan tutkimukseen juuri niiden alkuperäislähteenä toimimisen yleisyyden takia, vaikkakin ne ovat ajallisesti selkeästi tutkimukseen rajattua tutkimusaineistoa vanhempia.

Kyberterrorismin käsittely ja rajaaminen ainoastaan puhtaaseen kyberterrorismiin ei tutkimuksen näkemyksen mukaan vastaa tämän päivän käsitystä kyberterrorismista tai sen todennäköisestä ilmenemismuodosta. Toisaalta myöskään liian lavea määritelmä ei ole käyttökelpoinen, vaan se päätyy määrittämään kaikki kybertoimintaympäristön toimet kyberterrorismiksi, mikä ei myöskään ole tarkoitus. Tässä tutkimuksessa kyberterrorismi on yksilöiden tai ryhmien kybertoimintaympäristössä tai sen avulla harjoittamaa poliittisesti, uskonnollisesti tai ideologisesti motivoitua väkivaltaa häiriön, tuhon ja pelon saavuttamiseksi kohteissaan.

5 KYBERTURVALLISUUSSTRATEGIAT JA KYBERTERRORISMIN UHKA

Kyberturvallisuusstrategiat ja kyberterrorismin uhka luvun tavoitteena on tarkastella kuinka eurooppalaisten valtioiden kyberturvallisuusstrategiat painottavat kyberterrorismia ja millaisen uhkan kyberterrorismi niiden mukaan Euroopassa muodostaa. Eurooppalaisten kyberturvallisuusstrategioiden lisäksi luvussa on tarkasteltu myös Yhdysvaltojen kyberturvallisuusstrategioita ja verrattu sitä, kuinka niiden kyberterrorismin painotus eroaa eurooppalaisista painotuksista. Tässä luvussa kyberterrorismia on tarkasteltu tämän tutkimuksen varsinaisesta eli kansainvälisen diplomatian näkökulmasta.

Kyberterrorismi muodostaa kansallisen turvallisuusriskin valtioille, ja tällä hetkellä olemassa olevat strategiat eivät pelotteena ole riittäviä sitä estämään. Valtioiden ja kansainvälisten organisaatioiden tulisi yhteistoimin pyrkiä lieventämään kyberterrorismin uhkaa ja vähentämään sen vaikutuksia. (Al Mazari ym., 2016.)

Selvitäkseen kybertoimintaympäristön haasteista ja riskeistä sekä saadakseen parhaan mahdollisen hyödyn sen tarjoamista mahdollisuuksista, valtiot pitävät kyberturvallisuutta erottamattomana osana kansallista turvallisuutta ja taloudellista kehitystä (Tatar, Calik, Celik & Karabacak, 2014). Lisäksi kyberturvallisuus koetaan yhä lisääntyvissä määrin valtion strategisena asiana, jolla on vaikutusta yhteiskunnan kaikille osa-alueille. Kansalliset kyberturvallisuusstrategiat ovat työkalu, joiden avulla voidaan parantaa valtion ja yhteiskunnan turvallisuutta sekä lisätä valtion palveluiden ja infrastruktuurin sietokykyä. Kyberturvallisuusstrategia on ylätason, hierarkiassa ylhäältä alaspäin suunnattu lähestymistapa kyberturvallisuuteen, jonka avulla voidaan määritellä kansallisia tavoitteita ja prioriteetteja sekä aikataulu niiden saavuttamiseksi. Sellaisenaan kyberturvallisuusstrategia muodostaa strategisen viitekehyksen valtioiden kyberturvallisuudelle. (ENISA, 2012.)

Viimeisen vuosikymmenen aikana erityisesti kolme tapahtumaa ovat alkuun panneet ja kiihdyttäneet valtioiden kyberturvallisuusstrategioiden laatimista. Ensimmäinen tapahtuma on vuonna 2007 Viroa ja sen infrastruktuuria vastaan tehty kyberhyökkäys, joka muutti käsitystä kyberhyökkäysten mahdollisista vaikutuksista. Toisena kyberturvallisuusstrategioiden kehittymiseen vaikuttavana tekijänä voidaan pitää vuonna 2008 tapahtunutta Georgian sotaa. Ensimmäistä kertaa fyysistä sodankäyntiä edelsi ja myös sen aikana käynnissä oli myös kybersodankäynti. Kolmas kehitykseen vaikuttava tapahtuma on vuonna 2010 julkisuuteen tullut Stuxnet hyökkäys Iranin Natanzin ydinvoimalaa kohtaan. Hyökkäyksen monimutkaisuus viittasi siihen, että sen taustalla olisi valtiollinen toimija ja näin ollen kyberhyökkäykset eivät enää olleetkaan ainoastaan hakkereiden ja erilaisten pienten ryhmien aikaansaannoksia. (Tatar ym., 2014.)

Sekä Euroopassa että maailmanlaajuisesti kyberturvallisuudelta puuttuu yhtenäinen selkeä määritelmä. Kyberturvallisuuden ja siihen liittyvien tärkeimpien käsitteiden kuten kybertoimintaympäristö ja kyberhyökkäys määritelmät vaihtelevat voimakkaasti eri valtioiden välillä (ENISA, 2012).

Tutkimuksessa mukana ovat olleet englanniksi käyttöön saatavilla olevia kyberturvallisuusstrategioita tai niihin liittyviä muita virallisia asiakirjoja. Keskeneräiset strategiat tai sellaiset joista ei ole olemassa virallista englannin kielistä käännöstä on jouduttu jättämään tämän tutkimuksen ulkopuolelle. Lisäksi myös sellaiset kyberturvallisuusstrategiat, joista saatavilla on ollut ainoastaan englanninkielinen tiivistelmä, on jätetty pois. Tästäkin huolimatta tutkimuksen käytössä on ollut riittävästi kyberturvallisuusstrategioita ja muutamia niitä tukevia asiakirjoja. Tukena kyberturvallisuusstrategioiden valitsemisessa ja etsimisessä ovat toimineet European Union Agency for Network and Information Security (ENISA, 2017) ja NATO:n Cooperative Cyber Defence Centre of Excellence (CCDCOE, 2017b) internet-sivuilta löytyvät koosteet kansallisista kyberturvallisuusstrategioista.

Professori Lehdon (2013) tekemän tutkimuksen mukaan kahdeksasta tutkimastaan kyberturvallisuusstrategiasta useimmat strategiat mainitsevat kyberterrorismin. Lehdon arvion mukaan kyberterrorismia ei ole käsitelty omana erillisenä uhkana vaan pikemminkin osana perinteistä terrorismia.

Tässä tutkimuksessa on käyty läpi kaksikymmentäkaksi kappaletta Eurooppalaisten maiden kyberturvallisuusstrategiaa tai siihen rinnastettavaa asiakirjaa mukaan lukien Euroopan Unionin kyberturvallisuusstrategia (2013) ja European Network and Information Security Agencyn (ENISA, 2012) julkaisema kansallisia kyberturvallisuusstrategioita ohjaamaan tarkoitettu kyberturvallisuusstrategia. Näistä strategioista neljässätoista mainittiin terrorismi tai kyberterrorismi jollain tavalla. Usein näissä maininnoissa kyseessä oli ainoastaan yksittäinen käsite tekstin osana ilman asian sen syvällisempää tarkastelua tai johtopäätöksiä. Yllättävää oli se, että ainoastaan kolmessa kyberturvallisuusstrategiassa oli löydettävissä jonkinlainen määritelmä kyberterrorismille.

5.1 Kyberterrorismi eurooppalaisissa kyberturvallisuusstrategioissa

Iso-Britannian kyberturvallisuusstrategia (2016) nimeää terroristiorganisaatiot uhkakseen heti johdannossa. Sen arvion mukaan terroristit ja heidän kannattajansa toteuttavat pienimuotoisia kyberhyökkäyksiä ja pyrkivät jatkuvasti saamaan aikaan suuremman mittakaavan vaikutusta. Iso-Britannian kyberturvallisuusstrategia on määritellyt terroristit yhdeksi viidestä määrittelemästään kyberuhkasta. Strategiasta ei löydy määritelmää käsitteelle kyberterrorismi. Uhka-arvion mukaan terroristit pyrkivät Iso-Britanniaa ja sen etuja vahingoittavaan toimintaan kyberympäristössä, mutta terroristien tekninen kyvykkyys arvioidaan kuitenkin vähäiseksi. Kaikesta huolimatta pienetkin terroriteot kybertoimintaympäristössä ovat saaneet aikaan suhteettoman paljon vaikutusta. Pienimuotoisten hyökkäykset internet-sivustojen ulkonäön tai sisällön muuttamiseksi tai mustamaalaamiseksi (website defacements) ja yksityisten tietojen julkaiseminen (doxing) ovat saaneet paljon mediahuomiota ja onnistuneet pelottelemaan uhrejaan. (HM Government, 2016.)

Iso-Britannian Kyberturvallisuusstrategia painottaa kuitenkin ENISA:n lausuntoa siitä, että terroristit, jotka käyttävät internettiä ovat edelleen eri asia kuin kyberterrorismi. Toisaalta terroristien lisääntynyt kybertoimintaympäristön hyödyntäminen ja fakta siitä, että kyberhyökkäyksiä voi ostaa jo valmiina palveluina, antavat olettaa että terroristit ovat kykeneviä myös kyberhyökkäyksiin. (ENISA, 2016.)

Iso-Britannian kyberturvallisuusstrategian arvio on, että perinteinen fyysinen terrorismi on kyberterrorismia todennäköisempi terroristiryhmien käyttämä hyökkäysmuoto myös lähitulevaisuudessa. Arvion mukaan uuden tietotekniikkaa paremmin hallitsevan terroristisukupolven kasvaessa melko yksinkertaisten palvelunestohyökkäysten ja internet-sivustojen muokkaamisen kaltaisten häiriötä aiheuttavien hyökkäysten määrä Iso-Britanniaa vastaan tulee lisääntymään. Tämän lisäksi kasvaa todennäköisyys sille, että aatteelleen lojaalit yksittäiset osaajat suorittavat omia hyökkäyksiään tai se, että terroristijärjestöt pyrkivät saamaan sisäpiiriläisiä mukaan tehostamaan hyökkäyksiään. Terroristien arvioidaan käyttävän mitä kybertoimintaympäristön keinoja tahansa saadakseen aikaan maksimaalisen vaikutuksen teoilleen. Kyberturvallisuusstrategiassa huomautetaan myös, että jo vähäinenkin lisäys terroristien kyvyissä voi aiheuttaa huomattavaa uhkaa Iso-Britannialle ja sen eduille. (HM Government, 2016.)

Iso-Britannian kyberturvallisuusstrategia ei kuitenkaan ainoastaan tyydy esittelemään terrorismin ja kyberterrorismin uhkaa vaan esittää myös toimenpiteitä, joilla tätä uhkaa vastaan voidaan toimia. Esimerkiksi tiedustelua ja poliisiviranomaisten panosta terrorismin vastaiseen taisteluun lisätään, jotta ne kykenevät aiempaa tehokkaammin tunnistamaan, ennakoimaan ja estämään vieraiden valtioiden, kyberrikollisten tai terroristien kyberhyökkäykset. Lisäksi kyberturvallisuusstrategian lähtökohtana on ajatus siitä, puolustautuminen ja suojautuminen alkavat pelotteen luomisella. Terroristeja vastaan tämä pelote pyritään

luomaan tunnistamalla ja estämällä Iso-Britannian kansallista turvallisuutta vastaan suunnitteilla olevat terroriteot. Kaiken kaikkiaan kyberterrorismin uhka pyritään pitämään mahdollisimman alhaisena etsimällä ja jäljittämällä mahdolliset terroristit sekä tutkimalla ja estämällä mahdolliset terroristien suunnittelemat kyberhyökkäykset myös yhteistyössä kansainvälisten kumppaneiden kanssa. Lainsäädännön avulla halutaan myös huolehtia siitä, että kyberterroristeilla ei ole mahdollisuutta piiloutua mm. uusien jatkuvasti kehittyvien salausjärjestelmien taakse viranomaisten saavuttamattomiin. Myös jatkuva tehokas teknologian kehityksen seuraaminen koetaan tärkeänä osana taistelussa kyberrikollisuutta ja -terrorismia vastaan. (HM Government, 2016.)

Iso-Britannian kyberturvallisuusstrategian lopussa olevassa toimeenpanoohjelmassa on nimetty useita keinoja, joiden avulla Iso-Britannia saavuttaa kyvyn tehokkaasti löytää, tutkia ja vastata sen vastustajien muodostamiin kyberuhkiin. Kyberterrorismiin liittyen yhdeksi keinoiksi mainitaan puolustukseen ja pelotteen luomiseen liittyvät toimenpiteet, joiden avulla pienennetään kyberterroristien onnistumismahdollisuuksia ja saadaan Iso-Britannia vaikeammaksi kohteeksi hyökkäyksille. Toisena keinona tunnistamalla ja tutkimalla kyberterrorismin Iso-Britannialle aiheuttamaa uhkaa, pyritään lisäämään ymmärrystä tätä uhkaa kohtaan. Ja kolmantena keinona halutaan varmistua siitä, että terroristien kyky toimia kybertoimintaympäristössä pysyy alhaisena myös tulevaisuudessa. Tähän pyritään tarkalla kyvykkyyksien monitoroinnilla sekä estämällä terroristien kyvykkyyksien ja aktiivisuuden kehittyminen mahdollisimman aikaisessa vaiheessa. (HM Government , 2016.)

Iso-Britannian kyberturvallisuusstrategia käsittelee terrorismia ja kyberterrorismia sen osana monipuolisesti niin uhkan kuin myös vastatoimien kannalta. Strategiasta jää selkeästi näkemys, että terrorismi kokonaisuudessaan koetaan vakavana uhkana ja kyberterrorismi on osa terrorismin nykypäivän ilmenemismuotoja. Lisäksi kyberterrorismin uhka koetaan realistisena ja sen arvioidaan jopa todennäköisesti lisääntyvän tulevaisuudessa. Varsinaista erillistä määritelmää käsitteelle kyberterrorismi ei strategiasta löydy.

Italian kyberturvallisuusstrategia on nimeltään kansallinen strateginen viitekehys kybertoimintaympäristön turvallisuudelle. Siinä uhkat on luokiteltu neljään kategoriaan, jotka ovat kyberrikollisuus, kybervakoilu, kyberterrorismi ja kybersodankäynti. Kyberterrorismi on määritelty ideologisesti motivoiduksi järjestelmien heikkouksien hyväksikäyttämiseksi tavoitteena vaikuttaa valtioon tai kansainväliseen organisaatioon. Strategian mukaan digitaalinen toimintaympäristö tarjoaa loistavan mahdollisuuden maailmanlaajuiseen yhteydenpitoon. Samalla kuitenkin muodostuu riski siitä, että tämän nimettömyyttä suosiva toiminta-alusta joutuu radikaalin vihan, laittoman materiaalin ja rikollisten tai terroristien suunnitelmien levitysvälineeksi. Strategiassa arvioidaan, että on hyvin mahdollista, että tulevaisuuden terroristit tai terroristijärjestöt hyödyntävät kybertoimintaympäristön tarjoamia mahdollisuuksia hyökkäykseen sotilas- tai siviilikohteisiin. Käytettävät kyberaseet ovat terroristien saatavilla joko suoraan verkosta rikollisia välineitä tarjoavista kauppapaikoista tai ne voivat olla myös

terroristien itsensä kehittämiä kyberaseisiin liittyvän jo olemassa olevan osaamisen, takaisinmallinnuksen (reverse engineering) ja tiedon avulla. Onneksi tämän kaltainen uhka on edelleen ainoastaan hypoteettinen, mutta on kuitenkin tärkeää pyrkiä varmistamaan se, että potentiaalisesti tuhoa aiheuttavat kyberaseet ovat jatkossakin vaarallisten käyttäjien ulottumattomissa. (Presidency of the Council of Ministers of Italy, 2013.)

Italian kyberturvallisuusstrategian esittämiin haasteisiin on pyritty myös löytämään ratkaisuja ja määrittämään vastuita. Italian sisäministeriön ja siihen kuuluvien poliisiviranomaisten vastuulle on määritetty osallistua työhön, jonka avulla ennaltaehkäistään ja estetään kybertoimintaympäristössä tapahtuvaa terrorismia ja sen tukemista. Puolustusministeriön vastuulla on ennaltaehkäistä ja toimia vastavoimana asevoimiin suunnattua kybertoimintaympäristössä tapahtuvaa terrorismia vastaan. (Presidency of the Council of Ministers of Italy, 2013.)

Italian kyberturvallisuusstrategia arvioi kyberterrorismin laatimishetken sijaan pikemminkin tulevaisuuden uhkakuvaksi. Strategiasta jää käsitys, että laatimisajankohtana kyberterrorismin uhkaa ei pidetä kovinkaan todennäköisenä, mutta aihe koetaan kuitenkin erittäin tärkeäksi tulevaisuudessa ja toimenpiteet tämän mahdollisen tulevaisuuden uhkan ennaltaehkäisemiseksi ja pienentämiseksi on kuitenkin käynnistettävä välittömästi.

Itävallan kyberturvallisuusstrategia arvioi, että kybertoimintaympäristössä tapahtuvat hyökkäykset muodostavat suoran uhkan sekä turvallisuudelle että valtion, talouden, tieteen ja yhteiskunnan toimivuudelle. Näin ollen nämä hyökkäykset vaikuttavat ihmisten joka päiväseen elämään. Strategian arvion mukaan sekä ei valtiolliset toimijat kuten rikolliset, järjestäytynyt rikollisuus ja terroristit että valtiolliset toimijat kuten turvallisuuspalvelut ja asevoimat voivat käyttää kybertoimintaympäristöä omiin tarkoituksiinsa ja häiritä sen varsinaista toimintaa. Kyberturvallisuusstrategian riskimatriisin mukaan kyberterrorismi on arvioitu hyvin samankaltaiseksi uhkaksi kuin kybersodankäynti. Sen todennäköisyyttä pidetään keskitasoisena ja vähäisempänä kuin esimerkiksi kyberrikollisuuden osalta. (Federal Chancellery of the Republic of Austria, 2013.)

Itävallan kyberturvallisuusstrategian mukaan kyberterrorismi on valtiollisten ja ei-valtiollisten toimijoiden poliittisesti motivoitunutta rikollisuutta tietokoneita, tietoverkkoja ja niihin tallennettua informaatiota kohtaan. Kyberterrorin tavoitteena on:

- Provosoida vakavia tai pitkäkestoisia häiriöitä ihmisten elämään.
- Aiheuttaa vakavia taloudellisia vahinkoja tavoitteena pelotella väestöä, viranomaisia tai kansainvälisiä organisaatioita, jotta nämä tekisivät, sietäisivät tai jättäisivät pois haluttuja levottomuutta aiheuttavia toimia.
- Tuhota valtioiden tai kansainvälisten organisaatioiden poliittisia, perustuslaillisia, taloudellisia tai sosiaalisin rakenteita.

Nämä poliittis-fundamentalististen ryhmien ja rikollisten yksilöiden tekemät teot muodostavat organisoitua kybersabotaasia tai kyberhyökkäyksiä valtiota, organisaatioita ja yrityksiä kohtaan. (Federal Chancellery of the Republic of Austria, 2013.)

Itävallan kyberturvallisuusstrategia arvioi kyberterrorismin sekä erittäin vakavaksi koko yhteiskuntaan koskevaksi uhkaksi että myös erittäin realistiseksi uhkaksi. Strategiassa arvioidaan myös sitä, miksi kyberterrorismia mahdollisesti tapahtuu ja mitkä voivat olla sen tavoitteita.

Saksan kyberturvallisuusstrategia on esimerkiksi aiemmin esiteltyä Iso-Britannian vastaavaa dokumenttia huomattavasti lyhempi ja tiiviimpi. Tiiviin olemuksensa mukaisesti myös kyberuhkat on esitelty strategiassa lyhyesti yhdellä sivulla. Kyberturvallisuusstrategian mukaan kyberhyökkäykset ovat viime vuosien aikana lisääntyneet ja muuttuneet monimutkaisemmiksi sekä niiden tekijät kehittyneet yhä ammattitaitoisemmiksi. Näiden hyökkäysten tekijöiksi nimetään rikolliset, terroristit sekä vakoilijat ja niiden ominaispiirteenä on se, että ne eivät ole sidoksissa valtioiden fyysisiin rajoihin. Tämä on kuitenkin ainoa viittaus kyberterrorismiin koko strategian osalta. Strategia toki määrittelee, että valtiolla tulee olla käytössään työkaluja, joiden avulla kyberhyökkäyksiä vastaan voidaan toimia ja tässä määrittelyssä kyberhyökkäysten lähtökohdan voidaan arvioida nimenomaan olevan edellä mainittuja toimijoita. Myöskään erillistä määritelmää kyberterrorismille ei Saksan kyberturvallisuusstrategiassa ole. (German Federal Ministry of the Interior, 2011.)

Ranskan kyberturvallisuusstrategia on nimetty Ranskan kansallisen digitaalisen turvallisuuden strategiaksi. Myöskään siinä ei ole määritelmää tai selitettä kyberterrorismille. Sen sijaan strategiassa arvioidaan että kybertoimintaympäristöstä on muodostunut uusi toimialue epäreilulle kilpailulle, vakoilulle, disinformaatiolle ja propagandalle sekä terrorismille ja rikollisuudelle. Terrorismin näkökulmasta Ranskan kyberturvallisuusstrategiassa näkyvät voimakkaasti vuoden 2015 alussa tehtyjen terroristi-iskujen vaikutukset. Näihin terrori-iskuihin liitetään niiden jälkeen tapahtuneet kyberhyökkäykset useiden ranskalaisten internet-sivustojen ulkonäön tai sisällön muuttamiseksi tai mustamaalaamiseksi (website defacements). Näiden hyökkäysten arvioidaan olleen teknisesti melko vaatimattomia, mutta symbolisesti ne varmastikin saavuttivat terroristien tavoittelemat huomattavat vaikutukset. Samoin myös ranskalaista kansainvälistä mediaa vastaan suunnattuja kyberhyökkäyksiä kyberturvallisuusstrategia arvioi yritykseksi vaikuttaa voimakkaasti mielipiteisiin ja edesauttaa radikalisoitumista, jonka tavoitteena ovat terroriteot. Lisäksi tämän mediaa vastaan suunnatun kyberhyökkäyksen arvioidaan osoittaneen hyökkääjien kyvyn vaikuttaa ja häiritä erittäin symbolisen infrastruktuurin osa-alueen toimintaa. (French Government, 2015.)

Kyberturvallisuusstrategiassaan Ranska nimeää valtion vastuulle kansalaisilleen tiedottamisen siitä, millainen on internetissä tapahtuvan manipuloimisen riski ja minkälaisia propaganda tekniikoita siihen on käytössä. Tähän liittyen vuoden 2015 tapahtuneiden terrori-iskujen jälkeen hallitus perusti tietopisteen tiedottaakseen juuri sähköisessä tiedonvälityksessä tapahtuvan islamilaisen radikalisoitumisen riskistä. Kyseinen ranskankielinen sivusto on löydettävissä osoitteessa www.stop-djihadisme.gouv.fr. Kyberturvallisuusstrategian mukaan vastaavanlaista toimintamallia voidaan hyödyntää muissakin tapauksissa tilan-

teen näin vaatiessa. Viimeisenä terrorismiin liittyvänä asiana strategiassa tuodaan esille terroristijärjestöjen sosiaalisen median jatkuvan näkyvyyden hyödyntäminen. Terroristijärjestöt hyödyntävät sosiaalista mediaa sekä uusien jäsenten hankintaan suunnatun propagandan levittämiseen että valtaväestön pelottelemiseen. (French Government, 2015.)

Alankomaiden kyberturvallisuusstrategia on jakautunut useaan osaan. Vuodelta 2012 on olemassa kyberturvallisuusstrategian ensimmäinen osa eli *the Defence Cyber Strategy*, joka täydentää Alankomaissa annettuja aiempia ohjeita ja pyrkii ohjaamaan kokonaisvaltaisen lähestymistavan kybertoimintaympäristössä toimivan sotilaallisen kapasiteetin kehittämiseen. Strategiassa arvioidaan, että terrorihyökkäysten tapaan kyberhyökkäykset voivat aiheuttaa suuria mullistuksia ja laaja-alaisia sosiaalisia häiriöitä. Muutoin terrorismi mainitaan asiakirjassa ainoastaan käsitteellä vastaterrorismi ja se tapahtuu kohdissa, joissa jaettaessa vastuita ja tehtäviä kansalliselle vastaterrorismin ja turvallisuuden koordinaattorille. (The Netherlands Ministry of Defence, 2012.)

Alankomaiden kansallisessa kyberturvallisuusstrategia 2:ssa, ei kyberterrorismia tai terrorismia ole mainittu lainkaan vaikka se on nimenomaan kansallisen turvallisuuden ja vastaterrorismin koordinaattorin laatima asiakirja. (The National Coordinator for Security and Counterterrorism of The Netherlands, 2013.)

Slovakian kyberturvallisuusstrategian ainoa maininta terrorismista on löydettävissä johdannosta, jossa kyberuhat, kansainvälinen terrorismi ja joukkotuhoaseiden leviäminen nimetään tulevaisuuden kansainvälisiksi uhkakuviksi. (National Council of the Slovak Republic, 2016.)

Norjan kyberturvallisuusstrategiassa on esitelty turvallisuushaasteita ja trendejä lyhyesti. Niiden joukkoon on nimetty mm internetin lisääntyvä käyttö, yhteiskunnan lisääntynyt riippuvuus toimivista tietoverkoista, kasvava markkina rikollisuudelle sekä tiedustelun ja sabotaasin lisääntyminen. Sen lisäksi strategiassa todetaan, että turvallisuushaasteet ja trendit esitellään yksityiskohtaisemmin hallituksen informaatioturvallisuuden toimintasuunnitelmassa. Terrorismi on mainittu yhtenä osana ilkeämielistä toimintaa, jota vastaan Norjassa rakennetaan toimintavalmiutta. Tämä vastuu määritetään kyberturvallisuusstrategiassa Norjan kansalliselle turvallisuusviranomaiselle (The Norwegian National Security Authority, NSM). Muutoin strategiassa ei terrorismia tai kyberterrorismia käsitellä. (Norwegian Ministries, 2012.)

Kyberterrorismi on hyvin pienessä roolissa Kroatian kyberturvallisuusstrategiassa. Siinä kyberterrorismi ja muut kansalliseen turvallisuuteen liittyvät kybernäkökohdat jätetään muutamien asiaa hallitsevien turvallisuus- ja tiedustelupalveluiden henkilöiden vastuulle. Strategian mukaan edellä mainitut haasteet vaativat erillistä lähestymiskulmaa ja myös sitä, että strategiassa esitetyt muut tarpeelliset osa-alueet huomioidaan siinä. Erillistä määritelmää kyberterrorismille ei esitetä. (Republic of Croatia, 2015.)

Tšekin kyberturvallisuusstrategia esittelee kyberterrorismin heti strategian alussa jo ennen varsinaista johdantoa yhdeksi kyberturvallisuuden haasteista yhdessä kyberhyökkäysten, kyberrikollisuuden ja kybervakoilun kanssa. Hetkeä

myöhemmin johdannossa määritellään kybertoimintaympäristön suurimpia riskejä ja arvioidaan että kyberterrorismista voi muodostua sellainen tulevaisuudessa. Tämän enempää Tšekin kyberturvallisuusstrategia ei kuitenkaan kyberterrorismia käsittele ja siitä ei ole myöskään löydettävissä määritelmää kyberterrorismille. (Czech National Security Authority , 2011.)

Espanjan kyberturvallisuusstrategiassa kansallisiin kyberuhkiin ja –riskeihin on määritetty terrorismi sekä terroristijärjestöt. Strategiassa on määritetty kuusi tavoitetta, joiden avulla pyritään saavuttamaan Espanjan kyberturvallisuudelle määrittämä kokonaistavoite. Yksi näistä kuudesta tavoitteesta keskittyy parantamaan kybertoimintaympäristössä tapahtuvien terroristisen toimien ja rikollisuuden ennaltaehkäisyä, tunnistamista, reagoimista, analysointia, palautumista, vastatoimenpiteitä, tutkintaa ja koordinaatiota. Tämän lisäksi kyberturvallisuusstrategiassa on määritetty kahdeksan toimintalinjaa, joiden avulla tavoitteisiin pyritään. Yhden toimintalinjan ajatuksena on kehittää kyberterrorismin ja kyberrikollisuuden tutkinta- ja syyttämiskapasiteettia. Toisessa puolestaan pyritään edesauttamaan kansainvälistä poliisin ja oikeuslaitosten yhteistoimintaa sekä yhtenäistämään lainsäädäntöä kyberrikollisuutta ja kyberterrorismia vastaan käytävän taistelun tukemiseksi. (Presidency of the Government of Spain, 2013.)

Puolan kyberturvallisuusstrategia on nimeltään Puolan tasavallan kybertoimintaympäristön suojauspolitiikka. Se määrittelee kyberterrorismin terrorismin luonteiseksi kybertoimintaympäristössä tapahtuvaksi hyökkäykseksi. Strategiassa määritetään strategisia tavoitteita ja erityistavoitteita, joiden toimeenpano toteutetaan mm kybertoimintaympäristön uhkia ja hyökkäyksiä, mukaan lukien terrorismin luonteiset hyökkäykset, vastaan toimivan koordinaatiosysteemin avulla. Kaiken tämän toiminnan avulla tavoitellaan sitä, että Puolaa vastaan suunnatun kyberterrorismin vaikutukset pienenevät ja nämä vaikutukset voidaan poistaa tai korjata vähäisemmillä kustannuksilla. (Republic of Poland, 2013.)

Valtioiden lisäksi myös Euroopan Unioni on luonut kyberturvallisuusstrategian vuonna 2013, jonka avulla tavoitellaan avointa, suojattua ja turvallista kybertoimintaympäristöä. Strategia nimeää kybertoimintaympäristön uhkiksi rikollisuuden, poliittiset motivaatiot, terroristit ja valtioiden tukemat hyökkäykset sekä luonnon katastrofit ja tahattomat virheet. Kyberrikollisuutta on käsitelty strategiassa enemmälti, mutta kyberterrorismista on vain muutama maininta. Yhtenä niistä on ajatus siitä, että tukirahastojen avulla toimivalla tutkimus- ja kehittämistoiminnalla pyritään luomaan työkaluja kyberrikollisuuden ja kyberterrorismin vastaiseen taisteluun. Lisäksi strategiassa tuodaan esiin ajatus siitä, että yhteistoiminnassa jäsenvaltioiden, komission ja Euroopan unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustajan kanssa kyetään kehittämään yhteistoimintaa kansainvälisten kumppaneiden ja organisaatioiden, yksityissektorin ja siviiliyhteiskunnan kanssa tukemaan kybertoimintaympäristön rakentumista kehittyvissä maissa. Tämän toiminnan tavoitteena on parantaa pääsyä avoimeen internettiin ja informaatioon sekä ennaltaehkäistä ja estää kyberuhkia kuten on-

nettomuudet, kyberrikollisuus ja kyberterrorismi. Lisäksi samalla pyritään kehittämään rahoituksen koordinointia näiden valmiuksien luomiseen liittyen. (European Commision, 2013.)

5.2 Kyberturvallisuusstrategioita ilman kyberterrorismia

36 prosenttia eli kahdeksan kappaletta 22:sta tutkimukseen valituista eurooppalaisten valtioiden kyberturvallisuusstrategioista oli sellaisia, ettei niissä ole mainittu sanallakaan terrorismia tai kyberterrorismia. Kaikkia kyberturvallisuusstrategioita, joissa terrorismista tai kyberterrorismista ei ole mainintaa, ei kuitenkaan ole tarkoituksen mukaista esitellä tässä tutkimusraportissa. Kaikki tutkitut kyberturvallisuusstrategiat on kuitenkin mainittu luvun lopussa. Sen sijaan alle on kirjattu muutamia havaintoja neljästä valitusta yllä mainittuun kategoriaan kuuluvasta kyberturvallisuusstrategiasta sekä lyhyesti esitelty havaintoja syistä tai yhteyksistä, joita kyseisillä kyberturvallisuusstrategioilla on löydettävissä kyberterrorismiin.

Suomen kyberturvallisuusstrategiassa ei ole mainintaa terrorismista tai kyberterrorismista (Valtioneuvosto, 2013a). Sen sijaan kyberturvallisuusstrategian taustamuistiossa, kyberuhkamallissa, kyberterrorismi on nimetty yhdeksi viidestä kyberuhkasta (Valtioneuvosto, 2013b). Tutkimuksessa käyttöön valitut kyberturvallisuusstrategiat olivat kuitenkin jo aiempien perusteluiden mukaisesti valittu mukaan nimen omaan englanninkielisten virallisten kyberturvallisuusstrategioiden tai niitä vastaavien asiakirjojen mukaisesti, ja näillä tutkimusperusteilla myös Suomi kuuluu näin ollen niiden maiden joukkoon, joilla ei ole mainintaa terrorismista tai kyberterrorismista kyberturvallisuusstrategiassaan. Kyberturvallisuusstrategian taustamuistion näkemyksiä kyberterrorismista on esitelty tässä tutkimuksessa jo aiemmin.

Viron kyberturvallisuusstrategiassa ei ole mainintaa terrorismista tai kyberterrorismista. Strategian mukaan suurin uhka muodostuu kyberrikollisuudesta, jonka kasvu heijastuu sekä kyberrikollisten kykyjen ja osaamisen merkittävästä kehityksestä että kyberrikollisten kehittyneestä kyvystä toteuttaa organisoituja kyberhyökkäyksiä. Sen lisäksi Viron kyberturvallisuusstrategia arvioi, että kyberhyökkäyksiin kykenevien valtioiden määrä ja aktiivisuus ovat lisääntyneet. Kyberterrorismia ei Viron kyberturvallisuusstrategiassa mainita käsitteenä laisinkaan. Lähimmät viittaukset kyberterrorismiin on löydettävissä arvioista, joiden mukaan poliittisesti motivoitujen ja rajallisia keinoja käyttävien yksilöiden tai ryhmien sosiaalisen median hyödyntäminen, palvelunesto- ja muiden kyberhyökkäysten määrä on myös lisääntymässä. Toisena asiana, joka laveasti tulkittuna voidaan kokea olevan liitettävissä kyberterrorismiin, on arvio siitä, että kyberrikollisuus voi pahimmillaan aiheuttaa tilanteita, joissa ihmishenkiä menetetään. Tässäkin näkemyksessä painotus on kuitenkin selkeästi kyberrikollisuudessa ja mitään varsinaista viittausta tai liittymäpintaa kyberterrorismiin ei ole löydettävissä. (Estonian Ministry of Economic Affairs and Communication, 2014.)

Tanskan kyber- ja informaatioturvallisuudenstrategia on vuodelta 2015. Se on tiivis seitsemän sivua pitkä asiakirja, jossa terrorismia tai kyberterrorismia ei mainita lainkaan. Muutoinkin kybertoimintaympäristön haasteita ja uhkia on strategiassa käsitelty hyvin lyhyesti ja ne eivät ole selkeästikään olleet keskiössä kyberturvallisuusstrategiaa laadittaessa. (Centre for Cyber Security of Denmark, 2015.)

Irlannin kyberturvallisuusstrategiassa tuodaan esille World Economic Forumin näkemys vuodelta 2013, jonka mukaan kybertoimintaympäristöön liittyvät uhkat ovat yksiä maailman suurimpia riskejä niin vaikutusten kuin todennäköisyydenkin suhteen. Strategiassa kyberuhkiksi nimetään hakkerointi, kyberrikollisuus, haktivismi ja kybervakoilu. Sen lisäksi strategia korostaa äärimmäisistä sääilmiöistä johtuvien, ihmisten tekemien, ohjelmistosta tai laitteistosta johtuvien virheiden aiheuttamaa suurta riskiä yksilöille, yrityksille ja yhteisölle. Strategiassa ei mainita terrorismia tai kyberterrorismia sanallakaan. (Irelands Department of Communications, Energy & Natural Resources, 2015.)

Näiden neljän edellä lyhyesti esitellyn kyberturvallisuusstrategian lisäksi tutkimuksessa todettiin, että Unkarin (Government of Hungary, 2013), Latvian (Latvian Ministeriön kabinetti nro 40 , 2014), Liettuan (Government of the Republic of Lithuania, 2011) ja Alankomaiden toisessa (The National Coordinator for Security and Counterterrorism of The Netherlands, 2013) kyberturvallisuusstrategioissa ei terrorismia tai kyberterrorismia käsitellä lainkaan.

5.3 Yhdysvaltojen kyberturvallisuusstrategia

Yhdysvalloilla on olemassa useita erilaisia virallisia asiakirjoja, jotka käsittelevät kybertoimintaympäristöä. Samankaltainen tilanne on toki myös joillain eurooppalaisilla valtioilla, mutta ero löytyy Yhdysvaltojen erilaisten kyberstrategioiden suuresta määrästä. Tähän tutkimukseen vertailukohdaksi eurooppalaisille kyberturvallisuusstrategioille valikoitui kaksi amerikkalaista kyberturvallisuusstrategiaa. Ensimmäinen valittu strategia on *The National Strategy to Secure Cyberspace* (The White House, 2003). Se on valittu käyttöön sen takia, että se on hieman vanhempi jo pidempään käytössä ollut strategia, joka on olemassa ololla todennäköisesti ollut vaikuttamassa useisiin sen jälkeen laadittuihin strategioihin niin Yhdysvalloissa kuin Euroopassakin. Lisäksi sen avulla saadaan hieman näkemystä tutkimukseen siitä, onko viimeisen kymmenen vuoden aikana ajatusmaailmassa tapahtunut merkittäviä muutoksia. Toinen valittu strategia on *The Department of Defence Cyber Strategy* (US Department of Defense, 2015). Tämä strategia eroaa tyyliltään pääosasta eurooppalaisista kyberturvallisuusstrategioista ollen hyvin konkreettinen. Tähän tutkimukseen se on kuitenkin valittu, koska strategia on melko uusi eli vuodelta 2015, siinä hyödynnetään samankaltaista jaottelua kuin eurooppalaisissa vastineissaan ja vaikkakin kyseessä on puo-

lustusministeriön strategia, on se kuitenkin laadittu käsittelemään koko Yhdysvaltojen puolustamista kybertoimintaympäristössä tapahtuvia hyökkäyksiä vastaan.

Tässä tutkimuksessa Yhdysvaltojen kyberturvallisuusstrategioita oli tarkoituksena ensin vertailla toisiinsa ja pyrkiä löytämään niiden tärkeimmät yhteneväisyydet ja ristiriidat. Sen jälkeen tätä vertailun tulosta oli tarkoituksena käyttää vertailussa eurooppalaisten kyberturvallisuusstrategioiden kanssa. Tutkimuksen aikana kävi kuitenkin selväksi, että mitään yhteneväistä eurooppalaista kyberturvallisuusstrategiaa ei ollut olemassa vertailukohteeksi, vaan vertailu tulisi suorittaa jokaista 22 kyberturvallisuusstrategiaa kohtaan. Tämä taas ei tutkimuksen tavoitteiden ja ajankäytön kannalta ollut kuitenkaan järkevää, ja näin ollen laaja jokaista yksittäistä eurooppalaista kyberturvallisuusstrategiaa kohtaan tehty vertailu jätettiin tekemättä. Tärkeimmät havainnot Yhdysvaltojen kyberturvallisuusstrategioista sen sijaan haluttiin tutkimuksen kannalta tuoda esille ja yleisiä vertauksia eurooppalaisiin kyberturvallisuusstrategioihin ja asenteisiin on esitetty Yhdysvaltojen kyberturvallisuusstrategioiden esittelyn yhteydessä.

Vuodelta 2003 olevan Yhdysvaltojen kybertoimintaympäristön turvallisuusstrategian tavoitteena on sitouttaa ja valtuuttaa amerikkalaiset turvaamaan se osa kybertoimintaympäristöstä, jonka he omistavat, jossa he toimivat, jota he operoivat tai jossa he vuorovaikuttavat. Strategian mukaan kybertoimintaympäristön terve toiminta on olennaista niin taloudelle kuin Yhdysvaltojen kansalliselle turvallisuudelle. Strategia arvioi, että kyberhyökkäysten nopeus ja nimettömyys tekevät niihin syyllistyneiden terroristien, rikollisten ja valtioiden erottelun vaikeaksi ja usein vasta jälkikäteen tapahtuvaksi, jos edes silloinkaan. Strategia kuitenkin painottaa, että kyberhyökkäysten ennaltaehkäisy ja torjunta on koko kansakunnan ja sen yksilöiden yhteinen ponnistus, ei ainoastaan hallinnon asia. (The White House, 2003.)

Samainen kybertoimintaympäristön turvallisuusstrategia mainitsee, että aiemmin merentakaiset terroristiverkostot ovat aiheuttaneet ainoastaan hyvin rajallisia vahinkoja Yhdysvalloissa. Tämä kaikki muuttui kuitenkin syyskuun 2001 terrorihyökkäyksessä. Strategia mainitsee, että vaikkakin vuoden 2001 terrori-iskut tapahtuivat fyysisesti, tulevaisuuden uhkat esiintyvät lisääntyvissä määrin kybertoimintaympäristössä. Näihin kybertoimintaympäristön ilkeämielisiin toimijoihin arvioidaan kuuluvaksi yksilöitä, rikollisjärjestöjä, terroristeja ja vihamielisiä valtioita. Strategiassa ei kuitenkaan tätä tarkemmin nimetä tai luokitella näitä toimijoita tai sitä, mitä niillä tarkoitetaan, vaan pikemminkin pyritään nimeämään muutamia erilaisia uhkia niin sodan kuin rauhan ajalle. Strategiassa ei mainita tai ole käytössä käsitettä kyberterrorismi. Pääosin vastuu kybertoimintaympäristön turvallisuudesta on määritetty hieman ennen strategian ilmestymistä eli vuoden 2002 marraskuussa perustetulle Department of Homeland Security (DHS). Strategia kuitenkin arvioi, että pääosa kyberhyökkäyksistä voidaan arvioida rikolliseksi toiminnaksi ja näin ollen niiden osalta vastuuta on annettu myös oikeuslaitoksen tietokonerikollisuuden osastolle (Justice Department's Computer Crime and Intellectual Property Section), liittovaltion poliisin

kyberdivisioonalle (the FBI's Cyber Division) ja salaiselle palvelulle (the U.S. Secret Service). Strategia arvioi myös, että koska nimenomaan valtiot ja terroristit pyrkivät kehittämään kyberhyökkäyskykyä, on tärkeää ymmärtää millaisiin vaikutuksiin sellaisilla hyökkäyksillä pystytään ja miten näitä hyökkäysten vaikutuksia on mahdollista pienentää. (The White House, 2003.)

Vuoden 2003 kybertoimintaympäristön turvallisuusstrategia näkee Yhdysvaltojen kybertoimintaympäristön osana maailmanlaajuista kybertoimintaympäristöä, jossa valtioiden rajoilla ei ole merkitystä ja reaaliaikainen vihamielisten toimijoiden luokittelu rikollisiin, terroristeihin ja valtioihin on hyvin vaikeaa. Nämä kybertoimintaympäristön vihamieliset toimijat kuten valtiot ja terroristit kykenevät etsimään heikkouksia järjestelmistä sekä suorittamaan kyberhyökkäyksiä. Jo rauhan aikana Yhdysvaltojen viholliset pyrkivät vakoilemaan ja valmistelemaan hyökkäyksiä Yhdysvaltojen hallintoa, tutkimusta ja yksityisiä yrityksiä vastaan. Kriisitilanteissa nämä viholliset voisivat aiheuttaa pelotetta hyökkäämällä kriittistä infrastruktuuria tai tärkeimpiä talouden toimintoja vastaan sekä heikentämällä väestön uskoa erilaisten informaatiojärjestelmien toimintaan. Yhdysvallat varaakin strategiassa itselleen oikeuden vastata näitä mahdollisia vihamielisiä toimia vastaan millä tahansa sopivaksi katsomallaan tavalla. (The White House, 2003.)

Kaksitoista vuotta myöhemmin ilmestynyt Yhdysvaltojen puolustusministeriön kyberstrategia on tyyliltään hieman erilainen kuin osa edellisissä alaluvuissa käsitellyistä eurooppalaisten valtioiden kyberturvallisuusstrategioista. Kuten jo aiemmin on lyhyesti mainittu, se on lähestymistavaltaan useita eurooppalaisia vastineita konkreettisempi nimeten tarkasti toimijoita, toimintoja ja vastuita. Toisaalta tämän tapaisia vastuunjakoja on löydettävissä myös eurooppalaisista kyberturvallisuusstrategioista, jotta sen osalta Yhdysvaltojen puolustusministeriön kyberstrategia oli mahdollista valita tutkimusmateriaaliksi ja vertailukohdaksi eurooppalaisille strategioille. Tämän lisäksi strategia on melko uusi eli vuodelta 2015 eli hyvinkin samaa ikäluokkaa kuin osa eurooppalaisista uusimmista strategioista. Lisäksi, vaikkakin kyseessä on puolustusministeriön strategia, on se kuitenkin laadittu yhteistoiminnassa muiden valtiollisten toimijoiden kanssa ja siinä yhtenä tärkeimpänä osa-alueena on nimenomaan Yhdysvaltojen kotimaan ja etujen puolustaminen myös kybertoimintaympäristössä tapahtuvia hyökkäyksiä vastaan (US Department of Defense, 2015). Sen lisäksi puolustusministeriö tukee Department of Homeland Securitya (DHS) ja liittovaltion poliisia (FBI) uhkien tarkastelussa esimerkiksi, kun arvioidaan potentiaaliseen hyökkäykseen viittaavia teknisiä indikaatioita. Näin ollen puolustusministeriön laatimaa kyberstrategiaa voidaan pitää tältä osin valtion kyberstrategiana, varsinkin kun mitään vastaavaa kilpailevaa strategiaa ei Yhdysvalloissa ole tarjolla.

Yhdysvaltojen puolustusministeriön kyberstrategian mukaan internetin nopean leviämisen mahdollistaneet avoimuus ja dynaamisuus ovat samalla luoneet keinoja vaarallisille valtiollisille ja ei-valtiollisille toimijoille Yhdysvaltojen etujen vähentämiseksi. Kybertoimintaympäristössä vihamieliset toimijat voivat varastaa informaatiota ja yksityistä omaisuutta omia taloudellisia tai poliittisia

päämääriä varten. Sen lisäksi toisella puolella maailmaa toimiva alueellinen toimija voi kybertoimintaympäristön avulla iskeä suoraan tietoverkkoihin tuhansien kilometrien päässä ja sen avulla tuhota informaatiota, häiritä liiketoimintaa tai jopa sulkea kriittisiä järjestelmiä. Tänä päivänä valtiolliset ja ei-valtiolliset toimijat toteuttavat kyberoperaatioitaan omien poliittisten, taloudellisten tai sotilaallisten päämäärien saavuttamiseksi. (US Department of Defense, 2015.)

Strategiassa ei käytetä termiä kyberterrorismi, eikä terrorismia ole rajattu ainoastaan ei-valtiollisten toimijoiden keinoksi. Esimerkkinä tästä on annettu Pohjois-Korean vuonna 2014 marraskuussa toteuttama kyberhyökkäys Sony Pictures Entertainment – yhtiötä vastaan. Hyökkäyksen syyksi arvioitiin esitykseen tulossa olevan satiirisen elokuvan vastustaminen. Pohjois-Korean kyberhyökkäys sisälsi pakottamista, pelottelua ja terrorismilla uhkaamista. Strategiassa tarkoitetaan todennäköisesti nimen omaa fyysisen terrorismin uhkaa, mutta sitä ei tämän tarkemmin kuitenkaan kuvata. Strategiassa ei mainita, että kyseessä olisi ollut kyberterrorismi vaan siinä puhutaan ainoastaan valtiollisen toimijan kyberhyökkäyksestä. Sen sijaan strategiassa tuodaan esille se, että kyberhyökkäysten käyttö poliittisena instrumenttina on lisääntynyt kansainvälisessä kanssakäymisessä. Tähän liittyen haavoittuvat datajärjestelmät muodostavat kiehtovan mahdollisuuden Yhdysvaltoja tai sen etuja vastaan hyökkäystä aikoville valtiollisille tai ei-valtiollisille toimijoille. Näiden lisäksi kehittynyt hyökkääjä voisi toimia joko teollisia kontrollijärjestelmiä vastaan vaikuttaen yleiseen turvallisuuteen tai murtautua tietoverkkoihin ja muokata vaikkapa henkilöiden terveystietoja ja näin ollen vaikuttaa ihmisten hyvinvointiin. Manipuloiva tai häiriötä tai tuhoa aiheuttava kyberhyökkäys voisi aiheuttaa merkittävän riskin Yhdysvaltojen taloudelle ja kansalliselle turvallisuudelle, jos ihmishenkiä menetetään, omaisuutta tuhoutuu, poliittisia tavoitteita vahingoitetaan tai taloudellisiin kohteisiin vaikutetaan. (US Department of Defense, 2015.)

Strategia linjaa, että Yhdysvallat voi toteuttaa rajoitettuja kyberoperaatioita varmistaakseen, että internet säilyy avoimena, turvallisena ja taloudellisesti menestyvänä ja estääkseen ihmishenkien menetykset tai vahingot omaisuudelle. Päätökset tilanteista, joissa kyberoperaatio suunnataan puolustusministeriön verkon ulkopuolelle, tehdään huolellisesti ja harkiten erehdysten välttämiseksi sotilaallisia konflikteja koskevan lainsäädännön mukaisesti. Tähän liittyen vaikkakin investoinnit ja puolustusministeriön kyberkykyjen rakentaminen tehdään Yhdysvaltojen kansallisten etujen näkökulmasta, puolustusministeriö seuraa tarkkaavaisesti valtiollisten ja ei-valtiollisten toimijoiden käytöstä ja sen vaikutuksia kybertoimintaympäristöön. (US Department of Defense, 2015.)

Vuonna 2013 kansallisen tiedusteluyhteisön johtaja nimesi kyberuhkan Yhdysvaltojen suurimmaksi strategiseksi uhkaksi terrorismin sijaan ensimmäistä kertaa sitten vuoden 2001 syyskuun terrori-iskujen. Potentiaaliset valtiolliset ja ei-valtiolliset vastustajat toteuttavat ilkeämielisiä kybertoimintoja maailmanlaajuisesti Yhdysvaltojen etuja vastaan ja testaavat samalla Yhdysvaltojen ja kansainvälisen yhteisön sietokykyä. Nämä vastustajat voivat tunkeutua Yhdysvaltojen tietoverkkoihin ja –järjestelmiin useista eri syistä kuten varastaakseen informaatiota, häiritäkseen organisaatioiden toimintaa tai toteuttaakseen sotilaallisiin

tavoitteisiin pyrkivän häiriötä ja tuhoa aiheuttavan hyökkäyksen. Valtiollisten uhkien lisäksi ei-valtiolliset toimijat kuten Islamic State in Iraq and the Levant -järjestö (ISIL/ISIS) käyttävät kybertoimintaympäristöä taistelijoiden rekrytoimiseen ja propagandan levittämiseen. Tämän lisäksi ISIS-järjestö on julistanut tavoitteekseen hankkia häiriöitä ja tuhoa aiheuttavan kyberkyvykkyyden. Rikolliset toimijat aiheuttavat huomattavan uhkan kybertoimintaympäristössä etenkin talouden toimijoille ja ideologiset ryhmät käyttävät usein hakkereita omien poliittisten näkökulmien esille tuomiseen. Valtiollisten ja ei-valtiollisten toimijoiden aiheuttamat uhkat voivat myös sekoittua keskenään. Isänmaalliset yhteisöt voivat toimia valtioiden kybertoimijoiden korvikkeena ja ei-valtiollisten toimijoiden taakse voidaan kätkeä valtion kyberoperaatio. Tämä aiheuttaa sen, että oikeiden kybertoimijoiden nimeäminen on entistä vaikeampaa ja riski väärille tulkinnoille lisääntyy. (US Department of Defense, 2015.)

Valtiolliset tai ei-valtiolliset toimijat sekä yksiöt voivat hankkia tuhoa aiheuttavia haittaohjelmia ja muita vastaavia kyvykkyyksiä pimeiltä markkinoilta. Tämän lisäksi valtiolliset ja ei-valtiolliset toimijat maksavat asiantuntijoille haavoittuvuuksien löytämisestä ja niiden hyväksikäyttömahdollisuuksien kehittämisestä. Tämä kysyntä on luonut vaaralliset ja hallitsemattomat markkinat, jotka palvelevat useita kansainvälisen tason toimijoita erilaisissa kilpailutilanteissa. Puolustusministeriö arvioi, että markkinoiden laajentuessa valtiolliset ja ei-valtiolliset toimijat pyrkivät etsimään ja kehittämään Yhdysvaltojen etuja vastaan suunnattuja kyberkykyjä. Lisääntynyttä valtiollisten ja ei-valtiollisten toimijoiden uhkaa vastaan Yhdysvaltojen puolustusministeriö pyrkii kehittämään ja saamaan käyttöön kokonaisvaltaisen kyberpelotestrategian, jonka avulla kyetään rakentamaan todellinen pelote Yhdysvaltojen etuja vastaan kyberhyökkäyksiä suorittaville toimijoille. Tässä onnistuakseen, tehokas kyberpelotestrategia vaatii useita erilaisia menettelytapaohjeita ja kyvyn vaikuttaa valtiollisten ja ei-valtiollisten toimijoiden käytökseen. Lisäksi lisääntyneet kyberkyvyt mahdollistavat valtiollisille ja ei-valtiollisille toimijoille hyökkäyksen Yhdysvaltojen etuja kohtaan tavalla, johon ei voida vastata suoraan sotilaallisilla keinoilla, mutta joka kuitenkin aiheuttaa merkittävän uhkan Yhdysvaltojen kansalliselle turvallisuudelle ja voi mahdollistaa jonkinlaiset ei-sotilaalliset vastatoimet. Tällaisissa tilanteissa Yhdysvallat voi käyttää keinoinaan diplomatiaa, oikeudenhoitotoimia tai harkita taloudellisia sanktioita. (US Department of Defense, 2015.)

Valtiolliset ja ei-valtiolliset toimijat uhkaavat Yhdysvaltoja häiriötä ja tuhoa aiheuttavilla kyberhyökkäyksillä, varastavat älyllistä pääomaa ja samalla pienentävät Yhdysvaltojen teknologista ja sotilaallista etumatkaa. (US Department of Defense, 2015.)

Vaikkakaan Yhdysvaltojen puolustusministeriön kyberturvallisuusstrategiassa ei puhuta sanallakaan käsitteestä kyberterrorismi, on kybertoimintaympäristön uhkat voimakkaasti esillä. Erityisesti valtiolliset toimijat, joina mainitaan esimerkiksi Pohjois-Korea, sekä ei-valtiolliset toimijat kuten ISIS-järjestö ovat voimakkaasti esillä tässä strategiassa. Painotus onkin nimenomaan valtiollisten ja ei-valtiollisten toimijoiden aiheuttamiin uhkiin ja yksilöt sekä kyberrikollisuus on jätetty pienemmälle painotukselle. Tämä on tietysti hyvin ymmärrettävää, jos

strategian tarkoituksena on pohtia koko Yhdysvaltoja ja sen etuja vastaan suuntautuvia uhkia. Toisaalta ei-valtiollisten toimijoiden, jotka ymmärrän käsittävän nimenomaan terroristijärjestöjä, suuri painotus kertoo siitä, kuinka vakavana uhkana kybertoimintaympäristössä tapahtuvaa terrorismia Yhdysvalloissa pidetään. Mielenkiintoisena sattumana pidän myös sitä, että aiemmin tutkimuksessani päädyin tulokseen, että termiä kyberterrorismi ei kannata käyttää jos sen voi jotenkin välttää. Mielestäni puolustusministeriön kyberturvallisuusstrategiassa on toimittu juuri tuolla tavoin. Kyseessä on siis tutkimuksen kannalta ainoastaan mielenkiintoinen sattuma, joka mielestäni kuitenkin tukee myös aiempia omia havaintojani kyberterrorismi-käsitteen käytöstä.

Kuten jo aiemmin on tuotu esille, tutkimuksen alussa ajatuksena oli, että Yhdysvaltojen kyberturvallisuusstrategioita vertailtaisiin eurooppalaisiin kyberturvallisuusstrategioihin ja näiden välisiä eroja ja yhteneväisyyksiä pyrittäisiin löytämään. Tutkimuksen aikana kävi kuitenkin selväksi, että mitään yhteneväistä eurooppalaista kyberturvallisuusstrategiaa ei ollut olemassa vertailukohteeksi, vaan vertailu tulisi suorittaa jokaista 22 kyberturvallisuusstrategiaa kohtaan. Tämä taas ei ollut tutkimuksen tavoitteiden ja ajankäytön kannalta kuitenkaan järkevää, ja näin ollen laaja, jokaista yksittäistä eurooppalaista kyberturvallisuusstrategiaa kohtaan tehty vertailu jätettiin tekemättä. Sen sijaan tutkimuksen kannalta oli hyödyllistä jättää kuitenkin näkyviin edellä esitellyt kaksi Yhdysvaltojen kyberturvallisuusstrategiaa sekä niiden näkemykset kyberterrorismiin. Niiden tavoitteena on antaa kaksi esimerkkiä siitä, miten kyberturvallisuusstrategia voidaan laatia ja millä tavoin kyberterrorismi siinä ilmenee. Tämän lisäksi *The National Strategy to Secure Cyberspace* vuodelta 2003 strategian havainnot on haluttu jättää näkyviin sen takia, että sillä on todennäköisesti ollut vaikutusta useisiin sen jälkeen laadittuihin strategioihin Euroopassa. Lisäksi tutkimuksessa oli ajatus siitä, että Yhdysvaltojen kyberturvallisuusstrategioista voisi olla löydettävissä myös viitteitä siitä, mihin suuntaan eurooppalaiset kyberturvallisuusstrategiat ovat kehittymässä nimenomaan kyberterrorismin näkökulmasta.

6 KYBERTERRORISMIN VIIMEAIKAINEN KEHITYS

Kyberterrorismin viimeaikaisen kehityksen tarkastelun tavoitteena on ollut löytää terrorismin kehityksen trendejä ja niiden kautta vertailla sitä, kuinka aiemmin kyberturvallisuusstrategioissa arvioitu uhkakuva on edelleen paikkaansa pitävä ja ajankohtainen. Tässä tutkimuksessa kyberterrorismin viimeaikaista kehityksen tarkastelu on aloitettu tarkastelemalla Euroopassa viime aikoina tapahtuneita perinteisiä terrori-iskuja. Tämä perinteisen terrorismin tarkastelu on tehty, jotta kyberterrorismille muodostuu selkeä vertailupari. Samalla on pyritty kartoittamaan myös sitä, kuinka kyberterrorismi liittyy fyysisiin terroristihyökkäyksiin ja minkälaisia yhteneväisyyksiä näiden kahden terrorismimuodon välillä on löydettävissä. Lisäksi tutkimuksen aikana kävi selväksi, että perinteisestä terrorismista ja siihen liittyvistä terroristihyökkäyksistä on paljon helpommin tietoa saatavilla kuin esimerkiksi terroristien toteuttamista kyberhyökkäyksistä. Toisaalta, kuten jo aiemmin tutkimuksessa on käynyt selville, kyberterrorismin tekopaikka ei ole samalla tavalla riippuvainen fyysisestä sijainnista kuin perinteinen terrorismi ja sen osalta tarkasteluun olisi ollut valittavissa myös muualla tehdyt, eurooppalaisia valtioita kohtaan suunnatut terroristihyökkäykset. Tutkimuksen selkeyden ja johdonmukaisuuden takia fyysinen rajaus Euroopassa tapahtuviin terrori-iskuihin oli kuitenkin tarkoituksenmukainen, ja se pyrittiin mahdollisuuksien mukaan ulottamaan myös kyberterrorismin tarkasteluun.

Kyberterrorismin viimeaikaisen kehityksen tutkimus on kuvattu tässä tutkimusraportissa siten, että ensin on esitetty kuolemia aiheuttaneet Euroopassa vuoden 2016 alun ja vuoden 2017 syyskuun välisenä aikana tapahtuneet terrori-iskut. Sen jälkeen on esitelty kyberterrorismia Euroopassa samaiselta ajanjaksolta ja tarkastelu sitä, millainen on ollut kyberterrorismin osuus edellä esitellyissä perinteisissä terrori-iskuissa. Luvun lopuksi on vertailtu aiemmin esiteltyjen kyberturvallisuusstrategioiden näkemyksiä terrorismiin ja kyberterrorismiin viime vuosina tapahtuneisiin tapahtumiin ja pyritty löytämään yhteneväisyyksiä ja eroavaisuuksia tutkimuksen johtopäätösten tueksi.

6.1 Terrori-iskut Euroopassa vuosina 2016 – 2017

Kyberterrorismin tarkastelun lähtökohtana ja tukena on käytetty Euroopassa vuoden 2016 alun ja vuoden 2017 syyskuun välisenä aikana tapahtuneita useita terrorihyökkäyksiä ja -iskuja, joiden seurauksena on ollut ihmishengen menetys. Lähes poikkeuksetta kuolonuhrien joukkoon on laskettu hyökkääjät, jotka siis pääasiassa ovat menettäneet terrori-iskuissa henkensä iskun tyypistä riippumatta. Tähän tutkimukseen tarkasteltavaksi on valittu ainoastaan iskut, jotka ovat aiheuttaneet ihmishengen menetyksiä. Myöskin sellaiset iskut, joissa ainoa kuolonuhri on ollut hyökkääjä itse, on rajattu tarkastelun ulkopuolelle. Huomioitavaa kuitenkin on, että tutkimuksessa esille tuotujen lisäksi on olemassa useita erilaisia terrori-iskuja, jotka ovat aiheuttaneet merkittäviä, mutta vähäisempiä vahinkoja tai jotka ovat epäonnistuneet tavoitteissaan, mutta ovat kuitenkin saaneet osakseen julkisuutta. Lisäksi terrorismia tutkittaessa ei myöskään saa väheksyä sellaisia terrori-iskujen suunnitelmia, jotka on pystytty estämään viranomaisten toimesta, mutta niitä ei ole käytetty eikä ole ollut mahdollista käyttää tämän tutkimuksen lähdeaineistona. Pääasiassa tällaisista suunnitelmista ei ole olemassa julkista saatavilla olevaa lähdeaineistoa.

Tässä tutkimuksessa lähestymistapa perinteiseen terrorismiin on esitelty jo luvussa kaksi. Kertauksena on kuitenkin syytä tuoda esille, että tässä tutkimuksessa perinteinen terrorismi on määritelty seuraavalla tavalla: Terrorismi on väkivaltaa, joka tapahtuu normaalin lainsäädännön määräämien rajojen ja tavanomaisen sotilaallisen käyttäytymisen ulkopuolella. (US Army TRADOC, 2007.)

Seuraavassa on lyhyesti kuvattu Euroopassa viime aikoina tapahtuneet tämän tutkimuksen kannalta merkittävimmät terrorihyökkäykset. Terrorihyökkäysten kuvausten runkona on käytetty internetistä, wikipediasta löytyvää luetteloa (Islamic terrorism in Europe (2014 - present), 2017). Wikipedian luetteloa on käytetty mahdollisimman vertailukelpoisen näkemyksen muodostamiseen tapahtuneista terrori-iskuista ja niiden aiheuttamista henkilövahingoista. Wikipedian luoma kooste antaa riittävän tarkkuuden henkilövahingoista, sillä ne eivät ole millään lailla tämän tutkimuksen tärkeintä sisältöä vaan niitä on hyödynnetty ainoastaan terrori-iskujen luokittelussa ja tutkijan aihealueeseen liittyvän laajemman ymmärryksen muodostamisessa. Tutkimuksen aikana on pyritty tarkkaan arvioimaan, millä perusteilla kyseiset iskut on määritelty terrorismiksi ja tarkastamaan muista lähteistä, onko jotain tutkimuksen kannalta oleellisia tapahtumia jätetty pois luettelosta ja millä perusteella. Viimeaikaiset terrorihyökkäykset Euroopassa:

Vuosi 2016:

- Tammikuussa 2016 Turkissa Istanbulissa tapahtui turisteja vastaan suunnattu itsemurhapommi-isku. Sen seurauksena 14 henkilöä kuoli ja 9 loukkaantui. (Yackley, 2016.)

- Maaliskuu 2016 Turkissa Istanbulissa Beyoglu alueen kuvernöörin toimiston edessä tapahtui itsemurhapommi-isku, joka oli myös todennäköisesti suunnattu turisteja vastaan. Sen seurauksena 5 henkilöä kuoli ja 36 loukkaantui. (Istanbul bombing: At least five killed in Turkish city, 2016.)
- Maaliskuussa 2016, vain kolme päivää Istanbulin pommi-iskun jälkeen, tapahtui Belgiassa koordinoitu terrorihyökkäys. Terrorihyökkäys koostui kolmesta itsemurhapommi-iskusta, joista kaksi toteutettiin Brysselin lentokentällä ja kolmas Maalbeekin metroasemalla Brysselissä. Tämän hyökkäyksen seurauksena 35 henkilöä kuoli ja 340 loukkaantui. ISIS ilmoittautui tämän hyökkäyksen tekijäksi. (Brussells explosions: What we know about airport and metro attacks, 2016.)
- Kesäkuussa 2016 tapahtui Magnanvillessä Ranskassa terrorihyökkäys, jossa jo aiemmin terrorismista tuomittu ja ISIS kannattajaksi julistautunut mies hyökkäsi poliisin kotiin surmaten hänet ja hänen puolisonsa puukolla. (French police officer and partner murderd in 'odious terrorist attack', 2016.)
- Kesäkuussa 2016 tapahtui Turkissa Istanbulissa Ataturkin lentoasemalla terrorihyökkäys. Kolme terroristia hyökkäsi automaattiaseilla ampuen ja lopulta itsensä räjäyttäen. Iskun seurauksena oli 45 kuollutta ja 230 loukkaantunutta. Turkin viranomaisten arvion mukaan tekijänä on ISIS. (Istanbul Ataturk airport attack: 41 dead and more than 230 hurt, 2016.)
- Heinäkuussa 2016 kuorma-auto ajoi tarkoituksella väkijoukkoon Nizzassa, Ranskassa. Hyökkäyksen seurauksena 87 ihmistä kuoli ja 458 loukkaantui. ISIS ilmoittautui teon tekijäksi. (Truck Attack in Nice, France: What We Know, and What We Don't, 2016.)
- Heinäkuussa 2016 kaksi veitsin aseistautunutta miestä hyökkäsi kirkkoon Saint-Etienne-du-Rouvrayssa, Normandiassa, Ranskassa. Hyökkääjät surmasivat papin ja saivat itse surmansa poliisien luodeista. Tämän lisäksi yksi ihminen loukkaantui. ISIS ilmoittautui teon tekijäksi. (McAuley & Myrphy, 2016.)
- Elokuussa 2016 tapahtui terrorihyökkäys Shchelkovo poliisiasemalle Moskovan lähellä. Kaksi tsetseenialaista syntyperää olevaa terroristia hyökkäsi poliisiasemalle ampumalla ja kirveiden kanssa, vahingoittaen kahta poliisia, joista toinen kuoli myöhemmin saamiinsa vammoihin. Molemmat hyökkääjät saivat surmansa hyökkäyksen yhteydessä. ISIS ilmoittautui teon tekijäksi. (Islamic State claims responsibility for attack on Russian traffic police, 2016.)
- Joulukuussa 2016, Berliinin joulumarkkinoilla Saksassa, kuorma-auto ajoi tahallaan väkijoukkoon surmaten 12 henkilöä ja aiheuttaen 56 henkilön loukkaantumisen. ISIS ilmoitti olevansa teon takana. Teon tekijä pääsi aluksi karkuun, mutta kuoli neljä päivää myöhemmin pidätyksen yhteydessä Italiassa. (Automatic brakes stopped Berlin truck during Christmas market attack, 2016.)

Vuosi 2017:

- Tammikuussa 2017 kesken uuden vuoden juhlinnan terroristi hyökkäsi ampumalla Besiktasin alueella Istanbulissa sijaitsevaan yökerhoon. Hyökkäyksen seurauksena 39 henkilöä kuoli ja 70 loukkaantui. ISIS ilmoitti olevansa hyökkäyksen tekijä. Tavanomaisesta poiketen hyökkääjä ei saanut surmaansa vaan hänet pidätettiin. (Istanbul new year Reina nightclub attack 'leaves 39 dead', 2017.)
- Maaliskuussa 2017 tapahtui Westminster sillalla Lontoossa, Iso-Britanniassa terrori-isku. Hyökkääjä ajoi henkilöauton väkijoukkoon ja onnistui sen jälkeen vielä puukottamaan aseistamatonta turvamiestä ennen kuin sai itse surmansa. Terrorihyökkäyksen seurauksena 6 henkilöä sai surmansa ja 49 loukkaantui. (U.K. Parliament attack: Five dead and 40 injured in 'sick and depraved terrorist incident' at Westminster, 2017.)
- Huhtikuussa 2017 Venäjällä Pietarin metrossa tapahtui itsemurhapommi-isku, jonka seurauksena 16 henkilöä menetti henkensä ja 87 loukkaantui. Räjähtäneen pommin lisäksi läheiseltä metroasemalta löytyi toinen pommi, joka kuitenkin saatiin puretuksi. ISIS arvioitiin olevan terrori-iskun taustalla. (Pinchuk, 2017.)
- Huhtikuussa 2017 uzbekistanilaissyntyinen ja todennäköisesti myös ISIS-järjestöön liittynyt turvapaikanhakija ajoi kuorma-auton tahallaan väkijoukkoon Tukholman keskustassa Ruotsissa. Terrorihyökkäyksen seurauksena 5 ihmistä kuoli ja 14 loukkaantui. Tekijä jäi henkiin ja pidätettiin myöhemmin. (Masters, Said-Moorhouse & Sanchez, 2017.)
- Huhtikuussa 2017 terroristi ampui rynnäkkökiväärillä Pariisissa Ranskassa Champs-Elysees ostoskadulla saaden lopulta itse surmansa. Ammunnan seurauksena 2 ihmistä kuoli ja 3 loukkaantui. Iskun jälkeen hyökkääjä ilmoitettiin kuuluneeksi ISIS-järjestöön. (Paris: French police officer killed in terrorist shooting on Champs Elysees, 2017.)
- Toukokuussa 2017 terroristi räjäytti kotitekoisen pommin Manchester Areenalla Iso-Britanniassa pop-konsertin ollessa meneillään. Itsemurhapommi-iskun seurauksena oli 23 kuollutta ja 120 loukkaantunutta. ISIS ilmoittautui teon tekijäksi. (Manchester attack: 22 dead and 59 hurt in suicide bombing, 2017.)
- Kesäkuussa 2017 kolme hyökkääjää ajoi pakettiauton väkijoukkoon Lontoon sillalla, Iso-Britanniassa. Tämän jälkeen terroristit jatkoivat hyökkäystään puukottamalla ihmisiä läheisellä torilla saatuaan lopulta surmansa poliisien luodeista. Terrorihyökkäyksessä sai surmansa 11 henkilöä ja 48 loukkaantui. Hyökkäys on liitetty osaksi ääri-islamilaista terrorismia. (The Guardian, 2017.)
- Elokuussa 2017 Espanjassa tapahtui terrorihyökkäysten sarja. Siihen kuului pakettiauton ajaminen väkijoukkoon ja puukotus Las Rambla –kadulla Barcelonassa, henkilöauton ajaminen väkijoukkoon Cambrilsissa sekä rä-

> jähdys Alcanarissa. Terrorihyökkäykselle tunnistettiin 8 tekijää, ja sen seurauksena 24 ihmistä kuoli ja 152 loukkaantui. ISIS ilmoittautui teon tekijäksi. (Gonzales, Berwick & Ruano, 2017.)

Eniten ihmishenkiä vaatineita terrori-iskuja on tutkimukseen valittuna ajankohtana tapahtunut Turkissa, Ranskassa ja Iso-Britanniassa. Tarkasteluajanjakson alkupuolella tapahtumat ovat olleet Turkissa ja vuoden 2017 puolella niiden painopiste on vaihtunut Iso-Britanniaan. Terrorihyökkäysten tekotavoista voidaan todeta, että perinteisten itsemurhapommi-iskujen ja ampumisten rinnalle ovat nousseet ajoneuvolla väkijoukkoon ajaminen ja puukotukset. Nämä uudet menetelmät ovat yhä vaikeampia viranomaisille ennalta havaita ja estää. Tämän tutkimuksen osalta yllä esitetyn kaltaisen kehityksen voidaan arvioida olevan osa terrorismin kehittymistä uhrien ja heidän yhteiskunnan heikkouksien ja haavoittuvuuksien hyväksikäyttämiseksi. Toisaalta tämä samanaikaisesti siirtää perinteistä terrorismia kauemmas tässäkin tutkimuksessa esitetyistä näkemyksistä puhtaasta kyberterrorismista, jossa kybertoimintaympäristön avulla ja välityksellä aiheutetaan fyysisiä vahinkoja. Näyttääkin siltä, että terrorismin kehitys ja kyberterrorismi eivät olekaan ottaneet niin voimakkaita askelia kehittyvän teknologian hyväksikäytössä kuin hurjimmissa ennusteissa on odotettu ja annettu ymmärtää.

Huolimatta siitä, että tutkimukseen valitut terrorihyökkäykset olivat rajattu sekä alueellisesti että ajallisesti ja aiheutettujen vahinkojen osalta, voidaan niiden lukumäärää silti pitää merkittävänä. Eniten julkisuutta ovat saaneet ja saavat iskut, joissa on eniten uhreja. Lisäksi, jos näiden hyökkäysten vaikutuksia arvioidaan puhtaasti menetettyjen ihmishenkien näkökulmasta, voidaan näitä terrorihyökkäyksiä pitää huomattavina ja erittäin merkityksellisinä uhkina Euroopan, sen valtioiden ja kansalaisten turvallisuudelle. Lähes poikkeuksetta kaikki viimeisten vajaan kahden vuoden aikana Euroopassa tapahtuneet ja kuolemaan johtaneet terrori-iskut on liitetty islamilaiseen terrorismiin. Pääasialliseksi tekijäksi on julistautunut tai arvioitu terroristijärjestö ISIS.

EUROPOLI:in (2016) raportin mukaan ISIS on todistanut kykynsä hyökätä halutessaan useita kertoja eri tyyppisiä kohteita vastaan Euroopassa. ISIS:n voidaan arvioida ottaneen johtavan aseman maailmanlaajuisessa islamilaisessa pyhässä sodassa (global jihad), kuitenkin poistamatta muiden toimijoiden aiheuttamia riskejä. Erityisen suuren riskin ISIS:in osalta muodostavat taistelukentiltä palaavat sotilaat, jotka muodostavat uhkan tulevien terrorihyökkäysten tekijöinä.

Esitellyt teot täyttävät tämän tutkimuksen määritelmän terrorismista. Terrorihyökkäyksiin liittyvät pienet tulkinnalliset erot eri lähteiden välillä eivät ole oleellisesti vaikuttaneet tapahtumien käsittelyyn tässä tutkimuksessa. Jokaisen terrorihyökkäyksen osalta on esitelty niiden päälähde, vaikkakin jokainen teko on tarkastettu vähintään kolmesta eri lähteestä.

6.2 Kyberterrorismin raportointia 2016 - 2017

Viimeaikaisen Euroopassa tapahtuneen kyberterrorismin ja siihen liittyvän lähdeaineiston löytäminen osoittautui perinteiseen terrorismiin verrattuna hyvin hankalaksi ja sitä oli löydettävissä vain vähän. Euroopassa vuosina 2016-2017 tapahtuneista kyberterrorismihyökkäyksistä tällaista lähdeaineistoa ei lähtökohtaisesti ollut saatavilla. Yleisesti kyberterrorismia ja sen kehitystä oli kuvattu ENISA:n (The European Union Agency for Network and Information Security) ja EUROPOL:in (European Police Office) vuosittaisissa terrorismiraporteissa ja israelilaisen ICT:n (International Institute for Counter-Terrorism) neljännesvuosikatsauksissa.

Kyberterrorismiin liittyvän lähdeaineiston löytymisen vaikeus herätti myös kysymyksiä tutkimuksen aikana. Ensimmäiseksi heräsi kysymys siitä, tulisiko tiedonkeruu toteuttaa jollain eri tavalla kuin aiemmissa luvuissa. Kartoituksen jälkeen tähän ei kuitenkaan ollut todellista tarvetta eikä sen enempää ajallisia kuin taloudellisia mahdollisuuksia. Näin ollen tutkimuksen tiedonkeruuta jatkettiin aiempia menetelmiä tehostaen. Samanaikaisesti muodostui kuitenkin myös näkemys siitä, että lähdemateriaalia oli selkeästi vähemmän saatavilla kuin perinteisestä terrorismista. Tämä herätti tutkijassa kysymyksen siitä, eikö kyberterrorismia ja sen elementtejä kyetä tunnistamaan vai eikö kyberterrorismista haluta kertoa ja tällä tavoin antaa sille sen mahdollisesti kaipaamaa julkisuutta. Varmaa kuitenkin on se, että internet, joka on kybertoimintaympäristön yhteen sitova elementti, on toiminut tiedonhankinta-, rekrytointi- ja mahdollistamiskanavana myös kaikille aiemmin esitetyille terroristihyökkäyksille. Tämä ei kuitenkaan tee niistä kyberterrorihyökkäyksiä sen enempää kuin vuoden 2001 iskut New Yorkin tornitaloihin. Pikemminkin se kuvaa nykyaikaisen elämän riippuvuutta digitaalisesta maailmasta.

Vuonna 2016 toteutuneesta kyberterrorismista oli löydettävissä kolmenlaisia toisiaan tukevia ja osin toistavia raportteja. Raporttien laatijoina olivat ENISA, EUROPOL ja ICT.

ENISA:n vuoden 2016 Threat Landscape -raportin mukaan tapahtuneiden terroristihyökkäysten, mediahuomion ja kansainvälisen yhteisön taistelu ISIS:ia vastaan ovat kääntäneet kyberturvallisuuden huomion ja painopisteen kyberterrorismiin. Vaikkakaan minkäänlaista suoraa uhkaa ei voida liittää kyberjihadisteiksikin kutsuttuihin kyberterroristeihin, joitain hakkeriryhmiä on liitetty tukemaan samankaltaisia tavoitteita ja ISIS:iä. Toisaalta kyberterrorismiin ja erityisesti myös kyberjihadiin kuuluu paljon muitakin terroristijärjestöjä ISIS:in lisäksi kuten al-Qaeda tai Boko Haram. Kyberturvallisuusyritysten laatiman arvion mukaan kyberterroristien kyvyt ovat tietojärjestelmiin murtautuminen, sivustojen mustamaalaaminen ja sosiaalisen median käyttäjätilien kaappaukset. Raportissa kerrottiin myös ISIS:in kyberterroristien paikannuksista, seurannasta ja eliminoimisista. Tämä todistaa sen, että turvallisuusviranomaiset seuraavat tarkasti näitä korkean profiilin ja kyvykkyyden omaavia yksilöitä tavoitteena heidän eliminoi-

misensa. Vuoden 2017 alussa laaditun arvion mukaan kyberterroristien suorituskyky osoittaa, että terroristit hyödyntävät anonymiteettia suojaavia työkaluja ja toimintatapoja sekä hyödyntävät darknettiä. Laaditun arvion mukaan kyberterroristit omaavat yleisen tason osaamisen kybertoimintaympäristössä, vaikkakin he samanaikaisesti pyrkivät löytämään uusia kohteita esineiden internetin (Internet of Things, IoT) yleistyessä. Lisäksi kyberterroristien kyvykkyyksien kehittymistä rajoittaa kilpailevien terroristijärjestöjen vastenmielisyys yhteistoimintaan. Tästäkin huolimatta, internetistä ostettavissa olevat rikokset (Crime-as-a-service, CaaS) mahdollistavat terroristijärjestöille laajatkin hyökkäykset valittuja kohteita vastaan. (ENISA, 2017.)

EUROPOL:in (2016) raportin mukaan kyberterrorismilla on korkea potentiaali mutta alhainen todennäköisyys. Raportin mukaan internet ja sen tarjoamat palvelut voivat toimia sekä hyökkäyskanavina että hyökkäyksen kohteina. Internetin anonymiteetin ja salaustekniikoiden kehittyminen ovat monimutkaistaneet terrorismin valvontaa. Jatkuvasti kehittyvä kyberrikollisuus tarjoaa kyberterroristeille edullisia ja pienen kiinnijäämisriskin sisältäviä palveluita, joiden avulla on saavutettavissa huomattavasti suurempia vaikutuksia kuin mitä terrorismijärjestöjen omat tekniset kyvyt mahdollistaisivat.

ICT toi vuoden 2016 alussa raportissaan esille, että Euroopassa tapahtuneiden terroristihyökkäysten seurauksena Euroopan Unioni joutui arvioimaan uudelleen ISIS:n Euroopalle aiheuttamaan uhkaa. Lähes samanaikaisesti Yhdysvallat aloitti helmikuussa 2016 ISIS:ia vastaan suunnatun kyberoperaation, jonka tavoitteena oli häiritä ja jopa rajoittaa ISIS:in kykyä toimia internetissä. (ICT - International Institute for Counter-Terrorism, 2016a.)

ICT:n kyberterrorismiraporteista ei ollut löydettävissä yhtäkään Euroopassa vuonna 2016 tapahtunutta kyberhyökkäystä, joka olisi selkeästi ollut liitettävissä jonkin terroristijärjestön toimintaan. Huomioitavaa kuitenkin on se, että useissa kyberhyökkäyksissä ei hyökkääjää kyetty tunnistamaan ainakaan hyökkäystä seuraavien viikkojen aikana. Tämä viittaa siihen, että hyökkäyksen takana on jokin muu taho ja motivaatio kuin terrorismi. Tässä tutkimuksessa käytössä olevien määritelmien mukaisesti terrorismissa toimijat mielellään tuovat esille oman osuutensa tapahtumiin ja saamansa julkisuuden kautta tehostavat pelon lietsomista yleisöön eli omaa terrorismiaan. Esimerkkejä tämän kaltaisista kyberhyökkäyksistä ovat mm. vuoden vaihteessa 2015 – 2016 BBC:n internet-sivustoa vastaan suunnattu palvelunestohyökkäys, jonka seurauksena internet-sivusto oli poissa käytöstä parin tunnin ajan (ICT - International Institute for Counter-Terrorism, 2016a) tai huhtikuussa 2016 Saksassa Gundremmingenissa ydinvoimalaa vastaan tapahtunut haittaohjelmahyökkäys (ICT - International Institute for Counter-Terrorism, 2016b).

Myös vuonna 2017 toteutuneesta kyberterrorismista oli löydettävissä useita toisiaan tukevia raportteja, vaikka huomioitavaa on se, että tutkimusta toteutettaessa vuosi oli edelleen meneillään. Raporttien laatijoina olivat EUROPOL ja ICT kuten aiemminkin, mutta sisällöissä ja rakenteissa oli löydettävissä huomattavia poikkeuksia. ENISA:n raporttia vuodelle 2017 ei ollut vielä saatavilla.

EUROPOL:in (2017) raportin sisältö poikkeaa kyberterrorismin osalta huomattavasti edellisen vuoden raportista. Vuoden 2017 raportissa ei ollut enää lainkaan mainintaa kyberterrorismista tai kybertoimintaympäristöstä. Mielenkiintoisen asiasta tekeekin se, onko kyseessä unohdus, uusi linjaus vai osaamattomuus. Syytä voi osaltaan selittää rakenteiden muutokset ja tammikuussa 2016 käynnistynyt European Counter Terrorism Centre (ECTC). On mahdollista, että vastuuta sekä terrorismista että kyberterrorismista on siirretty uudelle keskukselle, mutta toisaalta EUROPOL on edelleen koonnut samalla nimellä olevan terrorismiraportin, joten uuden keskuksen vastuulle puutetta ei voi ainakaan sälyttää.

EUROPOL:in (2017) raportissa on kuitenkin löydettävissä muutamia mielenkiintoisia asiakokonaisuuksia kybertoimintaympäristöön liittyen. Yksi tällainen huomio on se, että sota-alueilla käytettyjä improvisoituja räjähteitä (Improvised Explosive Devices, IED) on alettu käyttää myös Euroopassa. Syynä tähän arvioidaan olevan sota-alueelta palaavat taistelijat, mutta myös aktiivisessa terroristien käytössä oleva sosiaalinen media sekä muut verkon yli tapahtuvat kommunikaatioyhteydet.

International Institute for Counter-Terrorism (ICT) -raportin nimi vaihtui kevään 2017 aikana cyber terrorism activities raportista cyber report -muotoon. Sisällön osalta rakenne säilyi kuitenkin suurin piirtein samana. Suurin muutos oli se, että vuoden 2017 alusta sisällöstä puuttuivat luettelot tärkeimmistä kyberterrorismitapahtumista, joita ei vuoden 2016 aikana kuitenkaan oltu juurikaan kyetty tunnistamaan. Propaganda sen sijaan on vahvasti esillä ja näyttää olevan isossa osassa.

International Institute for Counter-Terrorism (ICT) raportin mukaan vuoden 2017 keväällä kybertoimintaympäristössä tiedossa olevista toimijoista aktiivisia olivat mm. the Popular Front for the Liberation of Palestine, the United Cyber Caliphate (UCC) ja the Caliphate Cyber Terrorism Army (CCTA). Pääosin verkkohyökkäykset on toteutettu murtautumalla sosiaalisessa mediassa oleville käyttäjätileille ja mustamaalaamalla yksityisten internetsivujen sisältöä. Lisäksi vaikuttaa myös siltä, että kohteeksi on valittu nimenomaan helposti murrettavissa olevia kohteita. (ICT - International Institute for Counter-Terrorism, 2017d.)

Yksi vuoden 2017 aikana terroristien käyttämistä toimintatapamalleista on se, että avointa internettiä käytetään rekrytointiin ja sen jälkeen toiminnot siirtyvät salauksen taakse darknetin puolelle, koska tämän koetaan olevan yksityisyyden säilyttämisen kannalta parempi vaihtoehto. (ICT- International Institute for Counter-Terrorism, 2017c.)

Kesällä 2017 lainsäädäntö ja lakien toimeenpano saivat huomiota osana kansainvälistä kyberterrorismin vastaista taistelua. Uutta aihealueeseen liittyvää lainsäädäntöä hyväksyttiin mm. Saksassa, Venäjällä ja Israelissa. Tämä toteutettiin erityisesti lisäämällä viranomaisille keinoja puuttua terroristijärjestöjen sosiaalisen median käyttöön. Toisaalta samanaikaisesti aihealueeseen otettiin täysin vastakkainen lähestymistapa, kun Euroopan parlamentissa laadittiin uusi lakiluonnos tavoitteena parantaa yksityisyyden suojaa elektronisessa viestinnässä (ICT - International Institute for Counter-Terrorism, 2017b.)

6.3 Yhdistävänä tekijän terroristijärjestö ISIS

Tutkimuksen lähdeaineiston mukaan kyberterrorismi ei ole ollut juurikaan osana edellisessä luvussa esitetyissä Euroopassa tapahtuneissa terrorihyökkäyksissä, muutoin kuin internetissä levitetyn propagandan ja rekrytointiin tarkoitetun sisällön osalta. Yhdistävänä tekijänä sen sijaan oli se, että lähes kaikissa Euroopassa tapahtuneissa terrorihyökkäyksissä hyökkääjäksi on epäilty tai nimetty terrorijärjestö ISIS. Vuosina 2016 – 2017 tapahtuneissa iskuissa oli poikkeuksellista, jos tekijöitä ei joillain tavoin yhdistetty ISIS:iin.

ISIS eroaa perinteisistä terroristijärjestöistä usealla eri tavalla. Ensimmäiseksi ISIS:in tavoitteena on ollut valtion eli islamilaisen kalifaatin rakentaminen. Toiseksi ISIS on kyennyt ylläpitämään oman taloutensa ja keräämään suuremman pääoman kuin mikään terroristijärjestö aiemmin. Kolmanneksi ISIS:llä on ollut aiempia terroristijärjestöjä globaalimmat ja samalla myös maailmanlopun haluisemmat tavoitteet. Neljänneksi ISIS:illa on olemassa kehittynyt ja tehokas viestintästrategia, joka käyttää erilaisia verkosta löytyviä mediatyökaluja levittääkseen moniulotteista propagandaa. Sen avulla ISIS on järjestänyt hyvin tehokkaan kampanjan sosiaalisessa mediassa ympäri maailma ja onnistunut rekrytoimaan yli 18 000 ulkomaalaista taistelijaa yli 90 eri maasta. (Schori Liang, 2015.)

Jo ennen tutkimukseen valittua ajanjaksoa tapahtuneita terrorihyökkäyksiä eli vuoteen 2015 mennessä, ISIS oli onnistunut nostamaan kybertoimintaympäristössä tapahtuvan islamilaisen pyhän sodan eli kyberjihadin aivan uudelle tasolle. Siihen kuuluivat vaikuttaminen perinteisten internet-sivustojen lisäksi chat-foorumeissa sekä verkkojulkaisujen interaktiivisissa ja jatkuvasti muuttuvissa sosiaalisen median alustoissa. Näiden avulla ISIS on mahdollistanut ideologiansa levittämisen reaaliajassa ympäri maailmaa. Toiminnallaan ISIS on muuttanut nykyisen terrorismin toteutustapoja. Kyberjihad ja strateginen viestintä ovat modernin terrorismin levittämisen uusia menestyskeinoja, joilla on mahdollista myös yhdistää terroristijärjestöjä toisiinsa. (Schori Liang, 2015.)

Merkityksellistä kyberterrorismin kannalta tästä tekee sen, että tietoturvayhtiö F-Securen tutkimusjohtajan Mikko Hyppösen julkisuudessakin paljon huomiota saaneen näkemyksen mukaan ISIS järjestö on ensimmäinen terrorijärjestö, joka omaa huomattavia kykyjä myös kyberterrorismiin. (Chmielewski, 2015) Myös vastaväitteitä Hyppösen näkemykselle on esitetty, mutta Hyppösen väitteitä tukevat samana vuonna eli 2015 Yhdysvaltojen asevoimien tekemät lennokki-iskut, joiden avulla näkyviä ISIS:in kyberterroristeja kuten Junaid Hussain on surmattu. (Starr, 2015). Tämän kaltaisen toiminnan voidaan arvioida osoittavan sen, että ainakin vuonna 2015 Yhdysvallat arvioi ISIS kyberterrorismin olevan kehittymässä tai muodostavan tarpeeksi merkittävän riskin, jotta sitä vastaan täytyi toimia äärimmäisillä keinoilla.

Voimakkaiden vastatoimien ja ISIS:in vaikutusvallan vähenemisen myötä myös sen kyberterrorismikykyjen arvioidaan heikentyneen. Vuonna 2017 tietoturva-asiantuntija Kyle Wilhoit arvioi DerbyCon konferenssissa, että ISIS on lopettanut omien haitta- ja kommunikaatio-ohjelmien kehittämisen ja siirtynyt etsimään korvaavia tuotteita kybertoimintaympäristöstä rikollisten tarjoamista palveluista. Lisäksi Wilhoit arvioi, että ISIS:sin kyvyt ja osaaminen kyberterrorismiin on heikko. (Paganini, 2017.)

ISIS:in halusta ja kyvystä toimia ja vaikuttaa kybertoimintaympäristössä kertoo joka tapauksessa jotain sen organisaatioon yhdistetyt erilaiset kybertoimintaympäristöön keskittyvät toimijat. Tällaisia hakkeriryhmiä on eri lähteistä löydettävissä useita. Wilhoit on jaotellut näitä ryhmiä ja niiden toimia seuraavaasti:

- The Caliphate Cyber Army on keskittynyt ensisijaisesti mustamaalaamaan internet-sivustoja
- The Islamic State Hacking Divisionin on väitetty murtautuneen valtionhallinnon järjestelmiin Yhdysvalloissa, Iso-Britanniassa ja Australiassa kerätäkseen järjestelmistä tietoa, niistä sotilashenkilöistä jotka ovat osallistuneet ISIS:ia vastaan tehtyihin lennokki-iskuihin Syyriassa ja Irakissa. Toukokuussa 2016 ryhmä ilmoitti murtautuneensa Iso-Britannian puolustusministeriön sivuille, mutta näytöt ryhmän teknisestä osaamisesta ovat vähäisiä.
- The Islamic Cyber Army keskittyy energiateollisuuden kohteisiin tarkoituksenaan kerätä tietoja, joiden avulla hyökkäykset erilaisia energia-alan laitoksia vastaan olisivat mahdollisia. Onnistumisista tämän kaltaisissa toimissa ei ole kuitenkaan näyttöä.
- The Sons of the Caliphate Army -niminen ryhmä on myös tunnistettu, mutta sen toiminnasta ei ole mitään näyttöä. (Paganini, 2017.)

6.4 Salaaminen, propaganda ja kyberrikollisuus osana kyberterrorismia

Terroristijärjestöt ovat ymmärtäneet, että samalla kun kybertoimintaympäristö tarjoaa heille mahdollisuuksia, tarjoaa se niitä myös terroristijärjestöjen vastustajille. Sen seurauksena terroristijärjestöt ovat ohjeistaneet toimintatapojaan jäsenilleen ja siirtäneet toimiaan julkisesta internetistä darknetin puolelle tavoitteenaan suojata viestiliikennettään ja parantaa jäsentensä anonymiteettia. Näillä toimilla terroristijärjestöt pyrkivät välttämään mm. turvallisuuspalveluiden käyttämiä seurantaan tarkoitettuja ohjelmistoja ja erityisesti sosiaalisessa mediassa toimivia terroristien etsimiseen ja tarkkailuun erikoistuneita toimijoita. (ICT - International Institute for Counter-Terrorism, 2016b.)

ISIS:in kaltaisilla terroristijärjestöillä on korkeatasoinen ymmärrys siitä, kuinka salaustekniikoita ja internetin anonymiteettia voidaan hyväksikäyttää.

Esimerkkejä tällaisesta toiminnasta myös muiden terroristijärjestöjen toimesta ovat Al-Qaedan kehittämä ja käyttämä salaamisohjelmisto Asrar ak-Mujahedeen ja Anders Breivikin manifesti virtuaaliverkkojen (Virtual Private Network, VPN) ja TOR-selaimen (The Onion Router, TOR) parhaista käytänteistä. ISIS suosii julkisesti saatavilla olevia salattuja sovelluksia kuten Telegram sekä hyödyntää darknettiä mm. tuliaseiden hankkimisessa. Tämän lisäksi terroristit hyödyntävät salaustekniikoita ja anonymiteettiä terrorihyökkäysten valmisteluissa kaukana itse kohteesta ja vähentävät paljastumisen riskiä välttämällä turhaa matkustamista ja fyysisiä valmisteluita. Tämä on selkeä osoitus siitä, että terroristit kehittävät jatkuvasti toimintatapojaan ja kybertoimintaympäristön rooli tulee lisääntymään myös terrorismin mahdollistajana tulevaisuudessa. Ainakin terroristijärjestöt ovat selvästi osoittaneet halunsa kehittää kybertoimintaympäristöön liittyviä teknisiä kykyjään. (EUROPOL, 2016.)

Propaganda on ollut tärkeässä roolissa terroristijärjestöjen kybertoimintaympäristön käytössä ja terroristijärjestöt ovat jatkaneet verkkopalveluiden hyödyntämistä kohdistetusti ja monimuotoisesti. Kaikkien merkittävien jihadististen terroristijärjestöjen alkuperä on Euroopan ulkopuolella. Internetin välityksellä tapahtuva propaganda on yksi näiden järjestöjen tärkeimmistä keinoista tavoittaa Euroopassa olevaa kohdeyleisöä. Sen avulla terroristijärjestöt pyrkivät tuomaan esille epäkohtia Euroopassa asuvien ihmisten elämän ja eurooppalaisten valtioiden sotatoimien operaatioalueilla aiheuttamien kärsimysten välillä. Propagandan levittämiseen käytettiin ensisijaisesti sosiaalisen median palveluita sekä tiedostojen jakopalveluita. Laajasti saatavilla olevat ilmaiset, salatut ja anonymiteetin takaavat palvelut mahdollistivat propagandan levittämisen itseään paljastamatta. Toisaalta joidenkin sosiaalisen median palveluiden tiukentuneet käytännöt ovat rajoittaneet ja vähitellen vähentäneet erityisesti ISIS-kommunikaatiota. (EUROPOL, 2017.)

International Institute for Counter-Terrorism (ICT) -raportin mukaan terroristijärjestöt jatkoivat propagandansa levittämistä tavoittaakseen kannattajansa ja potentiaaliset uudet jäsenet. ISIS keskittyi rohkaisemaan yksittäisiin terroristihyökkäyksiin ympäri maailmaa hyödyntämällä aiemmin onnistuneita terroristihyökkäyksien tapoja, kuten Ranskassa Nizzassa oli toteutettu. (ICT - International Institute for Counter-Terrorism, 2016c.)

ISIS:in menestyksen hiipuminen ja taistelukentällä kärsimät tappiot heijastuivat myös järjestön toimintaan kybertoimintaympäristössä. Esimerkiksi järjestön viestinnässä painopiste siirrettiin kertomaan operaatioalueella tehdyistä terroristihyökkäyksistä ja yksittäisiä terroristeja kannustettiin hyökkäyksiin ISIS:ia vastaan taistelevan liittouman jäsenmaissa. ICT:n arvion mukaan tämän kaltaisen propagandan tavoitteena oli kääntää huomio pois ISIS:in taistelukentillä kärsimistä tappioista. Samanaikaisesti yleisesti terroristijärjestöjen toimet kybertoimintaympäristössä kuvastivat hyvin järjestöjen teknologisia kykyjä. Tällaisiin toimiin kuuluivat lähinnä yksittäisiä internetsivustoja vastaan suunnatut hyökkäykset ja niiden mustamaalaaminen. (ICT - International Institute for Counter-Terrorism, 2016d.)

Samoilla ajatuksilla jatkaa myös vuoden 2017 International Institute for Counter-Terrorism (ICT) -raportti, jonka mukaan yksi kyberterrorismin trendeistä on internetin hyödyntäminen propagandan välineenä. ISIS julkaisee ja jakaa internetissä tietoa sotilaallisista saavutuksistaan, vähätelläkseen järjestön kärsimiä menetyksiä alueiden, johtajien, tulojen ja uusien jäsenten suhteen. Samanaikaisesti ISIS on käyttänyt minilennokkeja terroristihyökkäyksissään sekä niiden videokuvaamiseen propagandakäyttöä varten. Lisäksi ISIS on lanseerannut internetissä käyntiin uuden kampanjan "#Demolishing_Fences", jonka tavoitteena on kannustaa kyberhyökkäyksiin yksityisiä tietoverkkoja kohtaan ja yksittäisten terroristien tekemiin terroristi-iskuihin. (ICT- International Institute for Counter-Terrorism, 2017c.)

ICT arvioi raportissaan, että viimeisten vuosien aikana poliittisia kohteita, kriittistä infrastruktuuria ja kaupallisten yritysten verkkosivuja vastaan kohdistetut kyberhyökkäykset ovat lisääntyneet. Tällaisten, yhä lisääntyvissä määrin julkisuutta saavien, kyberhyökkäysten tekijöinä ovat valtiolliset toimijat, hakkeriryhmät kuten Anonymous, järjestäytynyt rikollisuus sekä yksittäiset hakkerit. ICT:n arvion mukaan terroristijärjestöt toimivat läheisessä yhteistyössä järjestäytyneen rikollisuuden kanssa sekä kehittääkseen omaa osaamistaan että palkatakseen käyttöönsä omia tavoitteita tukevia palveluita. Tämän takia myös kyberterrorismin kannalta on tärkeää seurata kyberrikollisuuden tapahtumia ja kehitystä. (ICT - International Institute for Counter-Terrorism, 2016b.)

Terroristien teknisten kykyjen kehittyessä ja ymmärryksen teknisistä tutkimusmenetelmistä ja –tavoista lisääntyessä, on hyvinkin mahdollista, että myös terroristit ryhtyvät hyödyntämään verkossa ostettavissa olevia rikoksia (Crime-as-a-Service (CaaS) (EUROPOL, 2016).

Viimeaikaisen kehityksen valossa, verkossa toimivien kehittyneiden ja todennäköisesti valtioiden rahoittamien Advanced Persistent Threat (APT) -ryhmien ja taloudellista voittoa tavoittelevien kyberrikollisten käyttämät työkalut ja toimintatavat ovat lähentyneet toisiaan. Tämän perusteella voidaan olettaa myös, että kyberterroristeilla on lähitulevaisuudessa kykyjä kehittyneempien ja vaikeammin torjuttavien ja havaittavien kyberhyökkäysten toteuttamiseen. Tämä huolestuttava kehityssuunta koskee erityisesti valtioiden kriittistä infrastruktuuria ja sille muodostuvaa uhkaa. Vaikuttakin siltä, että terroristijärjestöt hyötyvät erityisesti verkossa myynnissä olevista rikollisista palveluista (Crime-as-a-Service, CaaS), joiden avulla terroristit kykenevät hankkimaan aiempaa kehittyneempiä työkaluja, palveluita sekä löytämään uudenlaisia hyökkäysvektoreita kriittistä infrastuktuuria vastaan suunnattujen hyökkäysten toteuttamiseksi. Yhden arvion mukaan hyökkäys kriittistä infrastruktuuria vastaan voitaisiin toteuttaa laajalla palvelunestohyökkäyksellä (Distributed Denial of Service (DDoS)) kiristämistarkoituksessa. (EUROPOL, 2016.)

International Institute for Counter-Terrorism (ICT) arvion mukaan rikollisuus ja terrorismi kulkevat käsi kädessä. Useammin kuin kerran terroristit ovat hyväksikäyttäneet rikollisuutta rahoittaakseen terrorihyökkäyksiään fyysisessä maailmassa. Kybertoimintaympäristössä tämä kyberrikollisuuden ja kyberterro-

rismin välinen ero on hyvin pieni, sillä kyberrikollisuudessa käytettäviä työkaluja, toimintatapoja ja -menetelmiä voidaan hyödyntää myös kyberterrorismissa. Tämä erotuksena fyysisestä maailmasta, jossa perinteisillä rikoksilla kuten murrot, varkaudet ja ryöstöt, ei ole suoraa käyttöä terrorismissa. Haittaohjelmien kehityksen seuraaminen ja niiden mahdollisesti aiheuttamien vahinkojen arvioiminen ovat tärkeitä toimenpiteitä, joiden avulla on samalla mahdollista seurata kyberrikollisuuden ja kyberterrorismin kehitystä ja näiden välistä suhdetta. (ICT - International Institute for Counter-Terrorism, 2017d.)

Kiristyshaittaohjelmien käytön leviäminen ja sillä tehdyt osittain onnistuneet hyökkäykset ovat rohkaisseet terroristijärjestöjä imitoimaan ja hankkimaan kiristyshaittaohjelmia käyttöönsä. Viime aikoina kiristyshaittaohjelmat ovat olleet kyberrikollisten suosiossa ja keväällä 2017 maailmalla koettiin tähän mennessä suurin tai vähintäänkin eniten huomiota saanut kiristyshaittaohjelmalla tehty kyberhyökkäys nimeltään ”WannaCry”. Tällä maailmanlaajuisella kyberhyökkäyksellä oli kahden tyyppisiä vaikutuksia terroristijärjestöjen toimintaan. Samankaltaisia haittaohjelmia pyrittiin joko imitoimaan tai ostamaan omaa käyttöä varten. Onkin syytä huomioida, että myyntipalveluna terroristeille tarjottavan kiristyshaittaohjelma tarjoaa kahdenlaisia mahdollisuuksia terroristeille. Ensinnäkin se tarjoaa keinon hankkia tuloja terroristihyökkäysten rahoittamiseen ja toiseksi sillä on mahdollista aiheuttaa taloudellisia vahinkoja hyökkäyksen uhreille. (ICT - International Institute for Counter-Terrorism, 2017a.)

Kirjatut havainnot tukevat aiempia analyyseja kyberterrorismista. Jo Denningin (2011) laatiman arvion mukaan terroristijärjestöt eivät ole olleet kiinnostuneita kybertoimintaympäristön käytöstä väkivallan ja pelon välineenä. Sen sijaan Denning arvioi, että terroristijärjestöt ovat olleet erittäin kiinnostuneita hyödyntämään kybertoimintaympäristöä viestiensä levittämiseen ja löytämään sieltä uusia tapoja tukea tavoitteidensa saavuttamista. Lisäksi Denning arvioi, että vuonna 2011 al-Qaeda ja muut terroristijärjestöt ovat edelleen paljon kiinnostuneempia perinteisistä pommeista kuin biteistä, ja kyberterrorismi säilyy hypoteettisena uhkana, vaikkakin yleiset uhkat kybertoimintaympäristössä ovat lisääntyneet.

Toisaalta uudemmissa arvioissa on tuotu esille, että kybertoimintaympäristön ja erityisesti sitä yhdistävän internetin rooli nyt ja tulevaisuudessa on paljon monimuotoisempi kuin esimerkiksi useissa vanhemmissa lähdemateriaaleissa on ennakoitu. Kuten jo aiemmin mainittu, kyberhyökkäysten lisäksi terroristit hyödyntävät internettiä ja kybertoimintaympäristöä rekrytoinnissa, omassa propagandassaan sekä rahoituksen keräämisessä. Tämän lisäksi terroristit voivat hyödyntää kybertoimintaympäristöä tiedon keräämiseen, psykologiseen sodankäyntiin, salattuihin viestiyhteyksiin, sovellusten jakamiseen, väärennettyjen dokumenttien hankkimiseen sekä koulutukseen. (Paganani, 2016.)

International Institute for Counter-Terrorism (ICT) tekemän arvion mukaan terroristijärjestöt pyrkivät edelleen kehittämään omia kykyjään kyberhyökkäysten tekemiseen, mutta keväällä 2016 laaditun arvion mukaan järjestöjen teknologisista kyvyistä ei ole olemassa minkäänlaisia näyttöjä. Näin ollen uhkan voivat

muodostaa terroristijärjestöjen palkkaamat järjestöjen ulkopuoliset, mutta samankaltaista ideologiaa kannattavat toimijat tai jopa sitä tukevat valtiot. Esimerkkinä ISIS:in yrityksistä vaikuttaa voidaan mainita internetissä julkaistu video, jossa ISIS:n hakkerit väittävät murtautuneensa Twitterin ja Facebookin tileille ja uhanneensa palveluiden ylläpitäjiä ja omistajia, jos nämä jatkavat ISIS:iin liittyvien sisältöjen poistamista. Samankaltaisia kykyjä on esittänyt myös Al-Qaeda, joka on julkaissut yksityiskohtia Windowsin etäsovelluksista löytyvistä haavoittuvuuksista. (ICT - International Institute for Counter-Terrorism, 2016b.)

Toisaalta on myös oikeutettua kysyä, että jos vuosina 2016-2017 Euroopassa on tapahtunut lukuisia kyberhyökkäyksiä, niin miksi osa niistä ei voisi olla myös kyberterrorismia? Tässä tutkimuksessa on käynyt selville, että monesti on hyvin vaikeaa, ellei jopa mahdotonta erotella, mitkä kybertoimintaympäristössä tapahtuneet hyökkäykset liittyvät kyberterrorismiin. Tätä eroteltavuutta vaikeuttaa entisestään se, että kyberrikoksia on entistä helpompi ostaa internetin välityksellä ja luonnollisesti myös terroristijärjestöt pyrkivät hyödyntämään näitä ostopalveluita oman toimintansa osana. Toisaalta tutkimuksessa on käynyt myös selville, että käytetty kyberterrorismin määritelmä rajaa aiemmin esille tuodut kyberhyökkäykset kyberterrorismin ulkopuolelle. Terrorismin motivaatio ei näy ja jos hyökkäyksellä ei ole näkyvyyttä, ei synny pelkoa eli hyökkäys ei täytä terrorismin vaatimuksia. Asiaa voidaan tarkastella hieman samaan tapaan kuin vertausta yksinään metsässä kaatuvasta puusta ja siitä syntyvästä äänestä. Onko ääntä, jos kukaan ei ole sitä kuulemassa ei kuitenkaan tässä tapauksessa ole oleellinen kysymys, vaan sen sijaan jos kuulijoita ei ole, ei puun kaatumisellakaan ole merkitystä. Näin ollen osa kyberhyökkäyksistä voi olla ollutkin kyberterroristien tekemiä, mutta ne eivät ole onnistuneet tämän tutkimuksen mukaisen kyberterrorismin määritelmän mukaisesti ja niitä ei näin ollen ole luokiteltu sen enempää tässä tutkimuksessa kuin esimerkiksi julkisuudessa tai yleisen käsityksen mukaan kyberterrorismiksi.

7 JOHTOPÄÄTÖKSET JA POHDINTA

Tutkimuksen päätutkimuskysymyksenä oli selittää, millaisena uhkana kyberterrorismia pidetään Euroopassa. Tähän tutkimuskysymykseen on rakennettu vastausta läpi tutkimuksen erityisesti alatutkimuskysymysten ja niihin perustuvien tutkimusraportin lukujen avulla. Tähän mennessä kaikkiin alatutkimuskysymyksiin on jo vastattu ja tämän viimeisen luvun tavoitteena on kerrata kaikkien alatutkimuskysymysten vastaukset sekä muodostaa niistä johtopäätöksiä, joiden avulla vastaus yllä esitettyyn päätutkimuskysymykseen on muodostettu.

Kyberterrorismia pidetään hyvinkin mahdollisena, mutta ei kovinkaan todennäköisenä uhkana Euroopassa. Erityisesti tahtoa kyberterrorismihyökkäykseen voisi olla, mutta terroristijärjestöjen potentiaali ei tällä hetkellä sitä vielä mahdollista. Eurooppalaisten valtioiden laatimista kyberturvallisuusstrategioista valtaosa nimeää terrorismin ja kyberterrorismin jonkinlaiseksi uhkaksi, mutta jopa kolmannes ei tunnista tai nimeä tällaista uhkaa millään tavalla. Kyberterrorismin viimeaikainen kehitys on painottunut kybertoimintaympäristön käyttöön propagandan, rekrytoinnin ja viestinnän välineenä. Varsinaista kyberterrorismiin liitettävissä olevaa kyberhyökkäystä ei tutkimuksessa ole tunnistettu, vaikkakin joitain spekulointeja sellaisista on ajoittain esiintynyt.

7.1 Kyberterrorismi osana terrorismia

Johtopäätöksissä voidaan lähteä liikkeelle siitä, että tässä tutkimuksessa kyberterrorismi on yksilöiden tai ryhmien kybertoimintaympäristössä tai sen avulla harjoittamaa poliittisesti, uskonnollisesti tai ideologisesti motivoitua väkivaltaa häiriön, tuhon ja pelon saavuttamiseksi kohteissaan. Tämä määritelmä toimii myös tutkimusten johtopäätösten tukena.

Kybertoimintaympäristö voidaan ymmärtää englanninkielisen cyberspace käsitteen synonyyminä. Cyberspace-käsitettä on käytetty hyvin monissa eri yhteyksissä ja eri tarkoituksissa. Eri lähteistä löytyvät hienot ja monimutkaiset määritelmät kybertoimintaympäristölle eivät pääasiassa lisää sen ymmärrystä, vaan pikemmin monimutkaistavat aihealueen käsittelyä. Kybertoimintaympäristön riittävän laaja-alainen ja monipuolinen ymmärtäminen on tärkeää esimerkiksi sen erilaisia uhkia tarkasteltaessa. Kybertoimintaympäristön liiallinen rajaaminen, esimerkiksi ainoastaan internettiin, voisi vääristää ja yksipuolistaa uhkien kuten kyberterrorismin tarkastelua. Kybertoimintaympäristö muodostuu siis monimutkaisista ja -kerroksisista informaatioverkoista. Kybertoimintaympäristöksi voidaan ymmärtää myös yksinkertaisesti digitaalinen maailma. Toiseksi kyber-käsite ei yksinään juurikaan tarkoita mitään, vaikkakin joissain tilanteessa sillä voidaan nimenomaan tarkoittaa kybertoimintaympäristöä kokonaisuutena. Suurin hyöty kyber-käsitteen käytöstä tulee kuitenkin, kun se yhdistetään johonkin fyysisessä maailmassa olemassa olevaan käsitteeseen. Tällöin kyber-käsite siirtää tämän fyysisestä maailmasta tutun käsitteen kybertoimintaympäristöön ja antaa sille uudenlaisen merkityksen.

Kyberuhkien ja näin ollen myös kyberterrorismin teoreettisessa tarkastelussa joudutaan aina määrittämään lähestymistapa. Tässä tutkimuksessa ja pääosassa siinä käytettyä lähdeaineistoa kyberterrorismia on pyritty määrittelemään selvittämällä, mitä se on. Kuitenkin usein julkisuudessa ja myös tässäkin tutkimuksessa aihetta on lähestytty myös toimijoiden näkökulmasta. Usein selvittämällä, kuka on kyberterroristi, voidaan kyberterrorismin määrittelyä edesauttaa ja se on helpommin erotettavissa esimerkiksi kyberikollisuudesta. Jaottelutavoista riippumatta, tutkimuksen johtopäätös on, että kyberterrorismia voidaan pitää yhtenä kybertoimintaympäristön uhkista. Sen lisäksi useiden erilaisten tutkimuksessa esitettyjen uhkamallien mukaisesti kyberterrorismin voidaan arvioida sijoittuvan lähimmäksi kyberrikollisuutta ja -sodankäyntiä, vaikkakin kyberterrorismin rajanveto kybervandalismiin vaikuttaa usein myös haastavalta.

Kyberhyökkäys ei ole sama asia kuin kyberterrorismi. Jossain tapauksissa kyberhyökkäykset ovat myös kyberterrorismia, mutta läheskään aina näin ei voida suoraan olettaa. Kyberhyökkäykset voivat olla osa jotain muuta kybertoimintaympäristön uhkaa, kuten kybersodankäynnin osana toteutettavaa kyberoperaatiota tai siihen kuuluvaa harhautusta. Asian tarkastelu muuttuu entistä monimutkaisemmaksi, jos sitä tarkastellaan vastakkaisesta suunnasta eli kyberterrorismin suhdetta kyberhyökkäyksiin. Tutkimuksessa esitettyjen useiden näkemysten mukaisesti teon tulee sisältää jonkinlainen kyberhyökkäys, jotta se voidaan määritellä kyberterrorismiksi. Voisiko kuitenkin olla niin, että myöskään kyberterrorismi ei aina tarvitse osakseen kyberhyökkäystä, vaan jossain tilanteissa kyberterrorismiksi riittää hyökkäyksen uhka ja sen aiheuttama pelko. Tutkimuksen aikana tämän kaltaista esimerkkiä ei lähdeaineistosta ollut tunnistettavissa, mutta en pitäisi ajatusta täysin poissuljettuna keinona tulevaisuuden terroristeille.

Kyberterrorismi on osa terrorismia. Pääasiassa kyberterrorismin voidaan määritellä lisäävän terroristien toimintatapoja ja vaikutuskanavia. Kyberterrorismin ja niin sanotun perinteisen terrorismin yhteisiä piirteitä ovat myös termeihin iskostettu kielteinen lataus ja se, että ne molemmat koetaan voimakkaasti tuomittavina toimintamuotoina. Kaikessa yksinkertaisuudessa kyberterrorismia voidaan pitää terrorismin kehityksenä nopeasti kehittyvässä ja lisääntyvässä määrin digitalisoituvassa maailmassa.

Kyberterrorismin määritelmät vaihtelevat paljon määrittelijän ja tilanteen mukaan. Lisäksi kyberterrorismi-käsitteen lisääntynyt käyttö julkisissa tiedotusvälineissä melko vapaamuotoisesti ja mielikuvituksellisesti ovat edesauttaneet käsitteen ymmärryksen jakautumista useisiin eri suuntiin. Tutkimuksen myötä useimmat parhaimmat määrittelyt ovat samalla myös olleet yksinkertaisimpia. Tällaisia ovat muun muassa arvio siitä, että kyberterrorismi on terrorismia kybertoimintaympäristössä. Tämän kaltaisen hyvin laajan määritelmän etuna voidaan pitää sitä, että se ei yksinkertaisuudessaan määrittele juurikaan kyberterrorismia ja näin ollen samalla voimakkaasti rajaa lukijoidensa näkemyksiä aihealueeseen. Toisaalta juuri samainen rajauksen puute on myös määritelmän heikkous, sillä se mahdollistaa jokaiselle lukijalle täysin oman käsityksensä kyberterrorismista. Laaja-alaista määritelmää voisi kuitenkin hyödyntää esimerkiksi arvioitaessa kyberterrorismin uhkaa ja siihen liittyviä vastatoimia, jolloin on tärkeää yrittää tarkastella aihealuetta mahdollisimman laaja-alaisesti ja aiempia luokitteluja vältellen.

Äskeisen jaottelun perusteella voidaan määritellä, että kyberterrorismi on kybertoimintaympäristöön kuuluvaa terrorismia. Tämän kaltainen määritelmä käsitteelle on kuitenkin niin ylimalkainen, että se ei joko tarkoita mitään tai sitten se tarkoittaa tilanteesta ja ihmisistä johtuen niin erilaisia asioita, ettei sitä voida käyttää. Tästä on kuitenkin muodostettavissa yksi tutkimuksen tärkeimmistä johtopäätöksistä. Kyberterrorismi käsitettä ei kannatta käyttää, jos ei siihen ole pakottavaa syytä. Suositeltavaa olisi sen sijaan puhua joko terrorismista tai kybertoimintaympäristössä tapahtuvista toimista, joilla on liittymiä terrorismiin. Johtopäätöksen yhtenä tärkeimpänä perusteluna voidaan pitää myös sitä, että käsitteellä terrorismi ei ole yksiselitteistä hyväksyttyä määritelmää olemassa. Näin ollen epämääräisen käsitteen siirtäminen uuteen toimintaympäristöön ei valitettavasti selkeytä sitä lainkaan, vaan päinvastoin.

Yleisesti hyväksyttyä yhteistä määritelmää kyberterrorismille ei ole olemassa. Tämä aiheuttaa sen, että monissa tilanteissa kyberterrorismi helposti ymmärretään väärin ja käsitteen käyttäminen on vaikeaa. Kyberterrorismi tulee aina määritellä asiayhteyteensä liittyen, jotta voidaan tosiasiallisesti varmistua siitä että ihmisillä on samankaltainen ymmärrys sen sisällöstä. Kyberterrorismin määrittelyn lähtökohtana tulisikin ensin kyetä määrittelemään, onko kyberterrorismin tärkein ominaisuus sen kohde, käytetyt keinot vai kenties aiheutetut vahingot. Monissa tilanteissa on syytä myös kriittisesti tarkastella, onko käsitteen kyberterrorismi käytölle tosiasiallista tarvetta vai voisiko asian ilmaista yksiselitteisempien termien avulla selkeämmin. Tämä ei kuitenkaan poista sitä tosiasiaa, että kyberterrorismin kaltainen kybertoimintaympäristön uhka on olemassa ja

todennäköisesti lisääntymässä lähitulevaisuudessa. Ja se aiheuttaa voimakkaan tarpeen varautumiseen ja valmistautumiseen niin valtioiden, yritysten kuin yksilöiden tasolla.

Tutkimuksen aikana on lähdeaineistossa esiintynyt paljon myös erilaisia hyvinkin tarkkoja määritelmiä kyberterrorismille. Lisäksi on löydettävissä kyberterrorismin tarkasteluja erilaisiin osatekijöihin jakamisen avulla. Tutkimuksen lähdeaineistosta löydetyt osatekijäluettelot vaikuttivat tutkimuksen alussa hyvin loogisilta ja asiaa tukevilta, mutta toimivat pääasiassa juuri päinvastoin. Niitä voidaan hyödyntää arvioitaessa jotain jo tapahtunutta yksittäistä tapahtumaa, mutta niiden avulla on vaikeaa löytää selkeää vastausta siihen, mitä kyberterrorismi on. Lisäksi aiemmin tutkimusraportissa esitettyjen esimerkkien valossa voidaan havaita, että osatekijöitä vaivaa aivan samankaltainen käsitteiden sekasotku kuin kyberterrorismi-käsitteellä. Näin ollen samaa esimerkkiä on arvioitu hyvin eri tavoin eri tutkijoiden toimesta.

Puhdas kyberterrorismi on käsite, joka on tullut esille useissa tutkimuksen lähdemateriaaleissa. Tutkijalle yllättävää oli monien lähdemateriaalissa olevien tutkimusten painotus ja etsintä tämän puhtaan kyberterrorismin suuntaan. Monilla tutkijoilla on ollut voimakas tahto irrottaa kyberterrorismi perinteisestä terrorismista ja määritellä se vain ja ainoastaan kybertoimintaympäristöön liittyväksi tavalla tai toisella. Tutkimuksen lähdeaineiston pohjalta käsitettä voidaan kuitenkin pitää hyvin teoreettisena, ja tutkimuksen aikana muodostui näkemys siitä, että puhdas kyberterrorismi on lähinnä akateemista pohdintaa, joka on vieraannuttanut kyberterrorismin käsitettä tosielämän tapahtumista. Tutkimuksen päättyessä puhtaan kyberterrorismin kaltaisia toimia ei ollut löydettävissä lähdeaineistosta tai julkisuudesta. Tämän kaltaisen tiukasti rajatun määritelmän käyttöä tulisi välttää kyberterrorismin yleistä määritelmää voimakkaammin. Perusteluna voidaan pitää jo aiemmin esille tullutta näkemystä siitä, että usein määritelmä toimii lähtökohtana terrorismin suojautumista suunniteltaessa ja toteutettaessa. Näin ollen teoreettinen ja voimakkaasti normaalista arkielämästä löydetyistä tapahtumista poikkeava määritelmä saattaa ohjata ajattelua väärään suuntaan tai vähintään rajoittaa sitä. Puhdas kyberterrorismi rajaa tiukimmillaan kaikki lähdeaineistosta löydetyt esimerkkitapaukset käsitteen ulkopuolelle ja on näin ollen ollut käyttökelvoton määritelmä vaikkapa suojautumisen kannalta.

Tutkimuksen yhtenä tärkeimpänä johtopäätöksenä voidaan pitää ajatusta siitä, että kyberterrorismi-käsitettä ei kannata käyttää. Useissa tapauksissa käsitteen käytölle ei edes ole todellista tarvetta, ja jos sellainen ilmenee, on käsite kyettävä määrittelemään sen verran hyvin, että väärinkäsitysten määrä saadaan minimoitua. Yleisenä määritelmänä voisi esittää vaatimuksen siitä, että jotta teko voidaan määritellä kyberterrorismiksi, tulisi sen jollain lailla tapahtua kybertoimintaympäristössä. Tästä voidaan puolestaan tehdä aiemmin lähdeaineistossakin esiintynyt johtopäätös siitä, että tietokone on kyberterroristin todennäköisin ase.

Tutkimuksen aikana esille tulleet väitteet siitä, ettei kyberterrorismia ole olemassa sen takia, ettei se olisi mahdollista tai sen uhka olisi niin pieni, kuulos-

tavat tutkimuksen lopussa erittäin omituisilta ja huolestuttavilta. On täysin ymmärrettävää pohtia asioiden nimiä ja määritelmiä, mutta niiden ristiriitaisuus tai puutteet eivät kuitenkaan poista kybertoimintaympäristön kehityksen myötä syntyneitä uhkia. Myöskään teknologian ja sen turvallisuuden kehitys eivät valitettavasti kykene täysin poistamaan tämän kaltaisten uhkien, joita tässä tutkimuksessa on kutsuttu kyberterrorismiksi, olemassa oloa.

Toisaalta tutkimuksen edetessä on ollut helppo yhtyä näkemykseen siitä, että pahimman uhkan kyberterrorismi muodostaa tilanteessa, jossa se onnistutaan liittämään yhteen perinteiseen fyysiseen terrorismiin. Juuri tämän kaltainen yhdistelmä tulee tulevaisuudessa muodostamaan uhkan niin kybertoimintaympäristön turvallisuudelle kuin myös yleiselle turvallisuudelle. Johtopäätöksenä voidaan todeta, että kyberterrorismi ei ole erillinen kybertoimintaympäristössä toimiva terrorismin osa, vaan osa tämän päivän terrorismia.

7.2 Kyberturvallisuusstrategiat ja kyberterrorismin viimeaikainen kehitys

Tässä tutkimuksessa tutkittiin kaksikymmentäkaksi eurooppalaisten maiden kyberturvallisuusstrategiaa tai siihen rinnastettavaa asiakirjaa mukaan lukien Euroopan Unionin kyberturvallisuusstrategia vuodelta 2013 (European Commision, 2013) ja European Network and Information Security Agencyn (ENISA) vuonna 2012 julkaisema, kansallisia kyberturvallisuusstrategioita ohjaamaan tarkoitettu kyberturvallisuusstrategia (ENISA, 2012). Näistä strategioista neljässätoista mainittiin terrorismi tai kyberterrorismi jollain tavalla. Usein näissä maininnoissa kyseessä oli ainoastaan yksittäinen käsite tekstin osana ilman asian sen syvällisempää tarkastelua tai johtopäätöksiä. Yllättävää oli se, että ainoastaan kolmessa kyberturvallisuusstrategiassa oli löydettävissä jonkinlainen määritelmä kyberterrorismille.

Se, että lähes kaikilta eurooppalaisilta valtioilta löytyy jonkinlainen kyberturvallisuusstrategia osoittaa, että valtiot uskovat sen olevan hyvä ja kokonaisvaltainen keino sekä kertoa ulospäin valtion näkemys kyberturvallisuuteen että jakaa vastuuta monialaisesti valtion sisällä eri toimialojen toimijoiden kesken. Toisaalta tämä kyberturvallisuusstrategioiden laaja-alaisuus tarkoittaa sitä, että ne ovat hyvin yleisesti kirjoitettuja ja eivätkä juuri ota kantaa tosielämän kyberturvallisuuden toimeenpanoon. Eli tämän tutkimuksen johtopäätöksenä voidaan todeta, että valtioiden kyberturvallisuusstrategiat ovat erittäin tärkeitä asiakirjoja, jotka viestivät isoista linjoista ja tavoitteista, mutta jättävät vielä käytännön työn ja tavoitteiden toteutuksen avoimeksi.

Kyberterrorismin viimeaikaisesta kehityksestä lähdeaineistoa oli oletettua vähemmän löydettävissä. Johtopäätöksenä voidaan todeta, että kyberterrorismia on ajoittain vaikea kyetä tunnistamaan ja toisaalta on myös ymmärrettävää jos siitä ei haluta kertoa tai antaa sille julkisuutta. Selvää on kuitenkin se, että inter-

net on toiminut tiedonhankinta-, rekrytointi- ja mahdollistamiskanavana kaikissa viimeaikaisissa terroristihyökkäyksissä tekemättä niistä kuitenkaan kyberterrorismia. Kuten jo aiemmin on tuotu esille, tämä ilmiö kuvaa pikemminkin nykyaikaisen elämän riippuvuutta digitaalisesta maailmasta eli kybertoimintaympäristöstä.

Viime vuosina Euroopassa on tapahtunut lukuisia kyberhyökkäyksiä, joista yhtäkään ei kuitenkaan voida suoraan määritellä kyberterrorismiksi. Tässä tutkimuksessa perustelu on ollut yksinkertainen, sillä tutkimuksessa käytetty kyberterrorismin määritelmä rajaa ne pois tästä kategoriasta. Tutkimus ei kuitenkaan väitä, etteikö osa kyberhyökkäyksistä voisi olla ollut kyberterroristien tai terroristijärjestöjen tekemiä, mutta ne eivät ole onnistuneet tämän tutkimuksen kyberterrorismin määritelmän mukaisesti.

Toinen huomioitava asia on se, että läheskään kaikkia kyberhyökkäyksiä ei tuoda julkisuuteen, vain isot ja mediaseksikkäät kyberhyökkäykset näkyvät ja saavat julkisuutta. Hyvällä syyllä voi kuitenkin epäillä, että näiden lisäksi on tapahtunut paljon muitakin kyberhyökkäyksiä. Toivottavasti useimmat näistä eivät ole tulleet julkisuuteen sen takia, että ne ovat olleet niin pieniä tai niiden aiheuttamat seuraukset ovat olleet niin vaatimattomia. Huolestuttavampia ovat kyberhyökkäykset, joita hyökkäyksen kohde ei ole itse kyennyt tunnistamaan tai joita kohde on salaillut, tavoitteenaan säilyttää esimerkiksi yrityksen imago ja asiakkaiden luottamus. Tällaisista kyberhyökkäyksistä ja niihin liittyvistä asenteista tulisi olla huolissaan, sillä kyvyttömyys ja vääränlainen asenne voivat tarjota juuri sellaisen hyökkäysvektorin, jota kyberterroristit ovat odottaneet.

Asiaa monimutkaistaa edelleen se, että nykyisin on yhä vaikeampaa ellei jopa mahdotonta erotella, mitkä kybertoimintaympäristössä tapahtuneista hyökkäyksistä liittyvät kyberterrorismiin ja mitkä ovat puhtaasti taloudellista hyötyä tavoittelevaa kyberrikollisuutta. Tätä eroteltavuutta vaikeuttaa entisestään se, että kyberrikoksia on entistä helpompi ostaa internetin välityksellä ja luonnollisesti myös terroristijärjestöt pyrkivät hyödyntämään näitä ostopalveluita oman toimintansa osana.

Kyberterrorismin viimeaikaisessa raportoinnissa on myös havaittu tutkimuksen aikana muutoksia ja jopa epäjohdonmukaisuutta. Esimerkiksi EUROPOL:in (2017) raportin sisältö poikkeaa kyberterrorismin osalta huomattavasti edellisen vuoden raportista, ja vuoden 2017 raportissa ei ole enää lainkaan mainintaa kyberterrorismista tai kybertoimintaympäristöstä. Tämä voi johtua uudesta vastuunjaosta tai sitten se kuvastaa sitä epäkypsyyttä, mikä valitettavan useilla organisaatioilla on olemassa liittyen kybertoimintaympäristöön ja siihen liittyviin aihealueisiin.

Iso-Britannian (2016) julkaistu kyberturvallisuusstrategia käsittelee terrorismia ja kyberterrorismia sen osana monipuolisesti. Strategian esittämät näkemykset ovat lähes täysin samanlaisia kuin tutkimuksessa käytetyissä kyberterrorismia vuosina 2016-2017 kuvanneissa raporteissa löytyvät. Yhtäläisyydet Iso-Britannian kyberturvallisuusstrategian ja lähdeaineiston välillä löytyvät siitä, että ne ovat samanaikaisesti ja samalla kielellä laadittuja. On jopa mahdollista,

että ENISA:n ja EUROPOL:in raportteja on ollut laatimassa samoja henkilöitä kuin Iso-Britannian kyberturvallisuusstrategiaa.

Italian kyberturvallisuusstrategia (2013) täsmää ideologialtaan myös viimeaikaiseen kyberterrorismin kehitykseen. Myös siinä arvioidaan, että kyberterrorismin uhka on mahdollinen, mutta ei ainakaan vielä vuonna 2013 kovinkaan todennäköinen. Itävallan kyberturvallisuusstrategian (2013) vakava arvio kyberterrorismista vuodelta 2013 ei ole onneksi ollut realismia viimeaikaisessa kyberterrorismissa. Tämä on tietysti hyvä asia, ja näin ollen voidaankin spekuloida sillä, olisiko tilanne näin hyvä Itävallassa tai Euroopassa, jos tätä uhkaa ei olisi muutama vuosi sitten otettu näin voimakkaasti esille strategiassa.

Saksan kyberturvallisuusstrategiassa (2011), kuten monissa muissa Euroopan valtioiden tai Euroopan Unionin kyberturvallisuusstrategioissa, kyberuhkat on kuvattu niin yleisesti, että niistä ei liittymää nykyisen kyberterrorismin kehittymiseen ole havaittavissa. Sen sijaan Ranskan kyberturvallisuusstrategiassa (2015) on onnistuttu kuvaamaan realistisesti kybertoimintaympäristön käyttäminen terroristijärjestöjen propagandan, viestinnän ja toiminnan organisoimisen välineenä.

Kuten jo aiemmin luvussa viisi kerrottiin, 36 prosenttia eli kahdeksan kappaletta 22:sta tutkimukseen valituista eurooppalaisten valtioiden kyberturvallisuusstrategioista oli sellaisia, ettei niissä ole mainittu sanallakaan terrorismia tai kyberterrorismia. Tällaisten kyberturvallisuusstrategioiden voidaan myös osaltaan arvioida onnistuneen analyysissään tähän saakka, kun mitään todella merkittävää kyberterrorismihyökkäystä ei Euroopassa ole havaittu. Toisaalta, kun tarkastellaan kyberterrorismin kehitystä tämän tutkimuksen lähdemateriaalin kannalta, olisi kyberterrorismin uhka syytä tunnistaa, vaikkakin sen todennäköisyys yksittäiselle valtiolle olisikin arvioitu vähäiseksi.

Tutkimuksessa tarkastelun kohteena olleista Yhdysvaltojen kyberturvallisuusstrategioista vanhemman eli jo vuonna 2003 laaditun voidaan arvioida olleen aikaansa edellä Euroopan näkökulmasta ja sillä on varmasti ollut merkitystä useita Euroopassa laadittuja kyberturvallisuusstrategioita tehtäessä. Uudemmassa vuoden 2015 strategiassa Yhdysvallat toi uhkina esille ISIS:in, mutta myös Eurooppaa voimakkaammin mahdolliset terrorismia tukevat valtiot ja niiden muodostaman uhkan. Yhdysvaltojen kyberturvallisuusstrategioista ei sen sijaan tunnistettu viitteitä siitä, mihin suuntaan eurooppalaiset kyberturvallisuusstrategiat ovat kehittymässä nimenomaan kyberterrorismin näkökulmasta. Esimerkkejä siitä, kuinka vakavasti Yhdysvallat suhtautuu kyberterroristien muodostamaan uhkaan kuvaa se, että terroristijärjestöjen johtavia henkilöitä ja parhaita asiantuntijoita pyritään eliminoimaan mm. lennokeista tapahtuvilla ohjusiskuilla.

7.3 Millainen on kyberterrorismin uhka Euroopassa?

Millaisena kyberterrorismin uhka sitten koetaan. Ensimmäisenä johtopäätöksenä täytyy todeta se, että osan tutkimuksen lähdeaineiston ja viimeaikaiseen

kyberterrorismiin keskittyvän aineiston välillä on kohtuullisen suuri välimatka. Erityisesti osa kyberterrorismia puhtaasti teoreettisesti käsittelevistä lähdemateriaaleista on joko tarkoituksella tai tieteellisen tutkimuksen vaatimuksista vienyt näkemyksen kyberterrorismista kauas siitä, mikä on viimeaikaista kyberterrorismin toteutumista käsittelevän lähdeaineiston näkemys tämän hetken todellisuudesta kyberterrorismissa ja sen muodostamassa uhkassa.

Toiseksi voidaan todeta, että tutkimuksen lähdeaineistoon kuuluvat kyberturvallisuusstrategiat käsittelevät terrorismia ja kyberterrorismia melko rajatusti. Sen sijaan fyysisen maailman viimeaikaiset tapahtumat tuovat terroristihyökkäykset ja terrorismin uhan voimakkaasti esille joka päiväisessä mediassa ja jopa ihmisten arjessa. Yleisesti voidaan arvioida uhkan muodostuvan kyvyistä ja tahdosta. Terroristien viimeaikaiset iskut eurooppalaisiin suurkaupunkeihin ovat osoittaneet, että tahtoa ja motivaatiota on olemassa, ehkä jopa liikaakin. Sen sijaan terroristien kyvystä toteuttaa kehittyneitä kyberhyökkäyksiä, fyysisten iskujen tueksi, on olemassa melko vähän näyttöä. Lisäksi esimerkiksi Lähi-Idässä ISIS:in riveissä toimineiden taitavimpien tietokoneasiantuntijoiden kohtalona on ollut fyysinen tuhoutuminen esimerkiksi lennokki-iskun seurauksena. Lähdeaineiston pohjalta voidaankin olettaa, että terroristijärjestöjen kyvyt kybertoimintaympäristöön vaikuttamiseen ovat rajalliset ja niiden kehittymistä seurataan sekä tarvittaessa rajoitetaan hyvinkin voimakkaasti useiden erilaisten toimijoiden suunnalta. Suurimmaksi haasteeksi kansainväliselle yhteisölle muodostuukin se, kyetäänkö kaikki potentiaaliset toimijat tunnistamaan ajoissa.

Tutkimuksen lähdeaineistona käytettyjen eurooppalaisten valtioiden kyberturvallisuusstrategioiden pohjalta voidaan arvioida, että kyberterrorismin uhka koetaan vähäisenä Euroopassa. Viime vuosina tapahtuneet terrori-iskut ovat saaneet viranomaiset Euroopassa huolestumaan myös tästä terrorismin kehittyvästä osa-alueesta, mutta kansallisiin strategioihin saakka se ei ole vaikuttanut.

Yleisesti voidaan todeta, että terrorismia kannattaa tutkia, jotta sitä voitaisiin paremmin ymmärtää ja sen myötä siltä voitaisiin tulevaisuudessa tehokkaammin suojautua. Tämän takia useita asioita johtopäätöksissä tulkitaan terrorismilta suojautumisen kannalta. Näkökulma tälle suojautumisen pohdinnalle on pyritty säilyttämään kansainvälisen politiikan tasolla valtioiden näkökulmana. Tässä tutkimuksessa terrorismilla on tarkoitettu poliittiseen, sosiaaliseen tai uskonnolliseen ideologiaan perustuvaa väkivaltaa, jonka tarkoituksena on aiheuttaa tuhoa ja lietsoa pelkoa ihmisiin. Tutkimuksen yhtenä johtopäätöksenä voidaan todeta, että terrorismin ja terroristien käyttämien keinojen kehittyminen ajan kuluessa on vaikeuttanut terrorismin yksiselitteistä määrittelyä. Valtiot ja järjestöt ovat pyrkineet löytämään keinoja, joiden avulla terrorismilta voidaan suojautua tai ainakin sen vaikutuksia voidaan vähentää. Tämän suojautumiskeinojen kehittämisen lähtökohtana on useimmiten ollut määritelmä siitä, mitä terrorismi on eli miltä suojaudutaan. Ja sen myötä suojautumiskeinojen kehittyessä terroristit ovat vastaavasti pyrkineet uudistamaan ajattelutapojaan ja löytämään uusia heikkouksia, joita vastaan hyökätä. Näin ollen suojautumisen suunnitelman pohjana ollut määritelmä vanhenee terrorismin kehittyessä. Terrorismin

luonteeseen kuuluu tavoite terrorisoida ihmisiä. Sen myötä toimintojen ja ihmisten siirtyessä yhä lisääntyvissä määrin kybertoimintaympäristöön, on luonnollista että terroristit seuraavat perässä. Samankaltainen siirtyminen on havaittavissa esimerkiksi rahaliikenteen siirtyessä kybertoimintaympäristöön, jolloin rikollisuus on valitettavasti seurannut perässä. On hyvinkin mahdollista, että kyberterrorismia ja niin sanottua perinteistä terrorismia ei voida enää lähitulevaisuudessa tosiasiallisesti erottaa toisistaan.

Yhtenä tutkimuksen aikana esille tulleena asiana voidaan pitää sitä, että kyberterroristien tekninen osaaminen ei ole kehittynyt yhtä voimakkaasti kuin pääosassa lähdemateriaalia on arvioitu tai jopa pelätty. Tähän johtavia syitä on esitetty tutkimuksessa useita, mutta niitä voivat olla mm. avainhenkilöstön eliminoiminen ja kybertoimintaympäristön nopea kehittyminen. Yhtenä kyberterroristijärjestöjen kyvykkyyksiä rajoittavana tekijänä voidaan pitää myös sitä, että todennäköisesti valtiolliset toimijat ovat ottaneet ennakoitua suuremman roolin kybertoimintaympäristössä, ja näin ollen pienemmät ja rajallisemmin resurssein toimivat terroristit ovat jäänet jalkoihin. Toisaalta kyberterrorismin kyvykkyyksiä ei saa tarkastella missään tapauksessa ainoastaan teknisenä asiana, vaan on pyrittävä löytämään laajempia kokonaisuuksia, joissa tekniikka on ainoastaan osa toteutusta. Tämän tutkimuksen osalta on kuitenkin huomioitava, että sosiaaliset syyt on tarkoituksella rajattu tutkimuksen ulkopuolelle. Lisäksi kyberterrorismin osalta sosiaalinen, poliittinen tai uskonnollinen ideologia motivaationa verrattuna kyberrikollisten taloudelliseen motivaatioon, voi aiheuttaa yllättävien ja erittäin vaarallisten kohteiden joutumisen kyberhyökkäysten uhreiksi tulevaisuudessa.

Tutkimuksen lähdemateriaalin valossa terrorismin siirtymistä kybertoimintaympäristöön voidaan pitää yhtenä valitettavana mutta luonnollisena kehitysvaiheena terrorismin kehityskaaressa. Näin ollen erilliselle kyberterrorismikäsitteelle ei varsinaisesti ole tarvetta. Käsitteellä voidaan laaja-alaisesti viitata kybertoimintaympäristöön ja terrorismiin, mutta muutoin sen käyttöä kannattaisi välttää. Joissain tapauksissa kyberterrorismi-käsitteen käyttö on perustelua, kunhan se on tarkkaan harkittua ja selkeästi määriteltyä.

Kyberterrorismin tulevaisuutta on vaikea ennustaa ja ennakoida, eikä se ole ollut tämän tutkimuksen tarkoituskaan. Kuitenkin lopuksi on hyvä tuoda esille, että esimerkiksi ISIS:in islamilaisen kalifaatin romahtaminen ja tappiot Lähi-Idässä taistelukentillä voivat jälleen kerran pakottaa terroristit kehittämään toimintatapojaan. Kysymys onkin, siirtyvätkö terroristien toiminnot yhä voimakkaammin kybertoimintaympäristöön. Kyseessähän voisi olla muutos, joka ei olisi tapahtunut muutoin kuin pakon edessä.

7.4 Tutkimuksen luotettavuus ja jatkotutkimus

Tutkimuksen luotettavuutta arvioidaan validiteetin ja reliabiliteetin avulla. Molemmille käsitteille on olemassa useita erilaisia määritelmiä. Tässä tutkimuksen validiteetti eli tutkimuksen pätevyys voidaan arvioida sillä, oikeuttavatko käytetty aineisto, tutkimusmenetelmät ja saadut tulokset esitetyt johtopäätökset. Tutkimuksen validiteetti on pyritty huomioimaan tarkasti koko tutkimuksen ajan. Alkuperäisiä tutkimuskysymyksiä on täsmennetty tutkimuksen aikana saadun palautteen perusteella vastaamaan tarkemmin tutkimusongelmaa. Tutkimuksen validiteetti on helposti todennettavissa tutkimusraportin rakenteesta, jonka avulla on pyritty selkeyteen ja johdonmukaisuuteen. Lisäksi tutkimuksessa käytetty lähdeaineisto on helposti lukijoiden saatavilla ja käyttöön valitut tutkimusmenetelmät osoittautuivat sopiviksi pro gradu -tutkimuksen laatimiseen. Lisäksi tutkimusmenetelmien käytössä ja yhdistämisessä on tutkimuksessa onnistuttu hyvin.

Tutkimuksen reliabiliteetilla arvioidaan tutkimustulosten ja johtopäätösten luotettavuutta. Kaiken kaikkiaan tutkimuksen laatiminen on ollut läpinäkyvää. Alatutkimuskysymykset käsitellään omissa luvuissaan ja niiden avulla on muodostettu vastaus tutkimuskysymykseen. Kaikki tutkimuksen johtopäätökset perusteluineen ovat löydettävissä tutkimusraportista. Kaikki tämä mahdollistaa alkuperäisen tutkimuksen toistettavuuden ja samankaltaisten tulosten tuottamisen tarvittaessa.

Tutkimuksen tekijän näkökulmasta tutkimusta voidaan pitää onnistuneena. Tutkimukselle asetetut tavoitteet on saavutettu ja kattava määrä lähdemateriaalia on saatu luotettavasti käsiteltyä. Tutkimuksen suurimpana onnistumisena voidaankin pitää aiemmin kovin vähäisen kyberterrorismia käsittelevän suomenkielisen lähdemateriaalin tuottamista. Lisäksi tutkimuksen onnistumiseksi voidaan arvioida myös tutkimuksen johtopäätösten koottua kirjallista esittämistä ja niihin vaikuttavien tekijöiden esille tuontia. Kokonaisuudessaan tutkimus luo hyvän perustan aihealueen jatkotutkimukselle.

Tutkimuksen aihealueeseen liittyviä jatkotutkimusaiheita on tutkimuksen aikana tullut esille useita. Kokonaisuudessaan aihealuetta voidaan edelleen pitää melko vähän tutkittuna ja etenkin tiedon syventäminen monien osa-alueiden osalta olisi tarpeellista. Esimerkkejä jatkotutkimuksen aiheista voisivat olla kyberterroristijärjestöjen organisoituminen ja rakenteet, kybertoimintaympäristön käyttäminen propagandan levittämiseen terrorismissa tai vaikkapa kyberrikollisuuden ja kyberterrorismin synergiaedut.

LÄHTEET

(a) Artikkeli tieteellisessä aikakausilehdessä

Ahmad, R., Yunos, Z. & Sahib, S. (2012). Understanding Cyber Terrorism: The Grounded Theory Method Applied. *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 323 - 328.

Al Mazari, A., Anjariny, A. H., Habib, S. A. & Nyakwende, E. (2016). Cyber Terrorism Taxonomies. *International Journal of Cyber Warfare and Terrorism*, 1 - 12.

Bogdanoski, M. & Petreski, D. (2013). Cyber Terrorism –Global Security Threat. *Contemporary Macedonian Defense-International Scientific Defense, Security and Peace Journal*, 59 - 73.

Denning, D. E. (2012). Stuxnet: What Has Changed. *Future Internet*, 672 - 687.

Kontselidze, A. (2015). Cyberterrorism- When Technology Became a Weapon. *European Scientific Journal April 2015*, 24 - 29.

Limnéll, J. (2015). The Reality of Cyberwar - Current Concepts and Future Trends. *European Cybersecurity Journal*, 39 - 45.

Ruby, C. (2002). The Definition of Terrorism. *Analyses of Social Issues and Public Policy*, 9 - 14.

Samuel, K., Osman, W., Al-Khasawneh, Y. & Duhaim, S. (2014). Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. *International Journal of Computer Science and Mobile Computing*, 1082 - 1090.

Talihärm, A.-M. (2010). Cyberterrorism: in Theory or in Practice? *Defence Against Terrorism Review, Vol.3, No.2*, 59 - 74.

Veerasamy, N. & Grobler, M. (2015). Logic Tester for the Classification of Cyberterrorism Attacks. *International Journal of Cyber Warfare and Terrorism*, 30 - 46.

(b) Artikkeli kokoomateoksessa

Flemming, P. & Stohl, M. (2001). Myths and Realities of Cyberterrorism. *Countering Terrorism Through International Cooperation* (ss. 70 - 105). Vienna: International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program.

Malkki, L. (2014). Toisen terroristi, toisen vapaustaistelija? Teoksessa A. Paronen & O. Teirilä, *Vihatkoon kunhan pelkäävät - näkökulmia terrorismiin ilmiönä* (ss. 15 - 35). Tampere: Maanpuolustuskorkeakoulu, Strategian laitos, Julkaisusarja 2, N:o 51, Juvenes Print.

Nuopponen, A. (2009). Käsiteanalyysia käsiteanalyysistä - kohti systemaattista käsiteanalyysiä. Teoksessa M. Enell-Nilsson;& N. (. Nissilä, *VAKKI-symposiumi XXIX - Kieli ja valta* (ss. 308 - 319). Vaasa: VAKKI ry.

Raitasalo, J. (2014). Terrorismi uhkakuvana. Teoksessa A. Paronen & O. Teirilä, *Vihatkoon kunhan pelkäävät - näkökulmia terrorismiin ilmiönä* (ss. 9 - 14).

Tampere: Maanpuolustuskorkeakoulu, Strategian laitos, Julkaisusarja 2, N:o 51, Juvenes Print.

(c) Artikkeli konfrenssijulkaisussa

Algahtani, A. (2013). The Potential Threat of Cyber-Terrorism on Natioanal Security of Saudi Arabia. *International Conference on Information Warfare and Security* (ss. 231 - VI). Denver: Academic Conferences International Limited.

Asheden, D. (2011). Cyber Security: Time for Engagement and Debate. Teoksessa R. Ottis, *Proceedings of the 10th European Conference on Information Warfare and Security* (ss. 11 - 17). UK: Academic Publishing Limited.

Huttenlocher, E. (2016). Cyber-Warfare and Cyber-Terrorism: Step to Learning to Knowing the Difference. *International Conference on Cyber Warfare and Security*, 391 - 398.

Lehto, M. (2013). The Ways, Means and Ends in Cyber Security Strategies. *European Conference on Information Warfare and Security* (ss. 182 - VIII). Jyväskylä: Academic Conferences International Limited.

MacDonald, S., Jarvis, L. & Chen, T. (2013). *A Multidisciplinary Conference on Cyberterrorism: Final Report.* UK: Swansea University.

Veerasamy, N. & Grobler, M. (2011). Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure. *International Conference on Information Warfare and Security* (ss. 260 - 267). Washington DC: Academic Conferences and Publishing International Limited.

Veerasamy, N., Grobler, M. & Von Solms, B. (2012). Building an Ontology for Cyberterrorism. *European Conference on Information Warfare and Security* (ss. 286 - 295). Laval: Academic Conferences International Limited.

Tatar, Ü., Calik, O., Celik, M. & Karabacak, B. (2014). A Comparative Analysis of the National Cyber Security Strategies of Leading Nations. *International Conference on Cyber Warfare and Security* (ss. 211 - 218). West Lafayette: Academic COnferences International Limited.

(d) Artikkeli internet-sivustolla

Chmielewski, D. (20. Lokakuu 2015). *recode*. Noudettu osoitteesta Cyber Security Expert Mikko Hyppönen Worries About Extremists With Computers: https://www.recode.net/2015/10/20/11619776/cybersecurity-expert-mikko-hyppnen-worries-about-extremists-with

Curran, P. (4. toukokuu 2016). *Cyber Terrorism - How Real is the Threat*. Noudettu osoitteesta https://www.checkmarx.com/2016/05/04/cyber-terrorism-real-threat-2/

Denning, D. E. (23. May 2000). *Cyberterrorism.* Noudettu osoitteesta Testimony before the Special Oversight Panel on Terrorism: http://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm

Denning, D. E. (19. Elokuu 2011). *Whither Cyber Terror?* Noudettu osoitteesta 10 Years after September 11, A Social Science Research Council Essay Forum: http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/

Gonzales, A., Berwick, A. & Ruano, C. (17. Elokuu 2017). *Barcelona van attacker may still be alive, on the run: police*. Noudettu osoitteesta Reuters: https://www.reuters.com/article/us-spain-barcelona/barcelona-van-attacker-may-still-be-alive-on-the-run-police-idUSKCN1AX1W6

Humanistinen tiedekunta, Jyväskylän yliopisto. (18. Huhtikuu 2017a). *Hermeneuttinen tutkimus*. Noudettu osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/hermeneuttinen-tutkimus

Humanistinen tiedekunta, Jyväskylän yliopisto. (18. Huhtikuu 2017b). *Laadullinen tutkimus*. Noudettu osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

INTERPOL. (20. Maaliskuu 2017). *Cybercrime*. Noudettu osoitteesta https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Jalil, S. (2003). *Countering Cyber Terrorism Effectively: Are We Ready to Rumble?* U.S.: System Administration, Networking, and Security Institute (SANS).

Masters, J., Said-Moorhouse, L. & Sanchez, R. (8. Huhtikuu 2017). *Stockholm truck attack kills 4; suspect held on suspicion of terror*. Noudettu osoitteesta CNN: http://edition.cnn.com/2017/04/07/europe/stockholm-truck-crash/index.html

McAuley, J. & Myrphy, B. (26. Heinäkuu 2016). *Islamic State says militant 'soldiers' carried out Normandy church attack*. Noudettu osoitteesta The Washington Post: https://www.washingtonpost.com/world/attackers-slit-french-priests-throat-in-church-shot-dead-by-police/2016/07/26/618a9600-5315-11e6-b7de-dfe509430c39_story.html?utm_term=.dc3e18e6d2a7

Oxford Dictionary. (21. Maaliskuu 2017). *Cyberespionage*. Noudettu osoitteesta https://en.oxforddictionaries.com/definition/cyberespionage

Oxford Dictionary. (20. Maaliskuu 2017). *Cyberspace*. Noudettu osoitteesta cyberspace: https://en.oxforddictionaries.com/definition/cyberspace

Paganani, P. (3. Helmikuu 2016). *Infosec Institute*. Noudettu osoitteesta The Role of Technology in Modern Terrorism: http://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/

Paganini, P. (25. Syyskuu 2017). *Security Affairs*. Noudettu osoitteesta Experts say United Cyber Caliphate hackers have low-level cyber capabilities: http://securityaffairs.co/wordpress/63389/terrorism/united-cyber-caliphate-capabilities.html

Pinchuk, D. (3. Huhtikuu 2017). *Eleven killed in suspected suicide bombing on Russian metro train*. Noudettu osoitteesta Reuters: https://www.reuters.com/article/us-russia-blast-metro/eleven-killed-in-suspected-suicide-bombing-on-russian-metro-train-idUSKBN17519G

Rollins, J. & Wilson, C. (22. Tammikuu 2007). *Terrorist Capabilities for Cyberattack: Overview and Policy Issues.* Noudettu osoitteesta Congressional Research Service Reports on Terrorism: https://fas.org/sgp/crs/terror/index.html

Schori Liang, C. (Helmikuu 2015). *Cyber Jihad: Understanding and Countering Islamic State Propaganda.* Noudettu osoitteesta GCSP Policy Paper 2015/2: http://www.gcsp.ch/News-Knowledge/Publications/Cyber-Jihad-Understanding-and-Countering-Islamic-State-Propaganda

Starr, B. (28. Elokuu 2015). *CNN Politics*. Noudettu osoitteesta Prominent ISIS recruiter killed in airstrike: http://edition.cnn.com/2015/08/26/politics/isis-recruiter-targeted-in-airstrike/index.html

Yackley, A. J. (12. Tammikuu 2016). *Suicide bomber kills 10 people, mainly Germans, in Istanbul*. Noudettu osoitteesta Reuters: https://www.reuters.com/article/us-turkey-blast/suicide-bomber-kills-10-people-mainly-germans-in-istanbul-idUSKCN0UQ0UJ20160112

(e) Esitys

Hyppönen, M. (5. Toukokuu 2017). *Cyber Arms Race.* (M. Hyppönen, Esiintyjä) F-Secure auditorio, Helsinki.

(f) Kirja

Grönfors, M. (2011). *Laadullisen tutkimuksen kenttätyömenetelmät.* Hämeenlinna: Sosiologi-Filosofiapu Vilkka.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2005). *Tutki ja kirjoita.* Jyväskylä: Kustanneosakeyhtiö Tammi.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2016). *Tutki ja kirjoita.* Porvoo: Kustanneosakeyhtiö Tammi.

Limnéll, J., Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus.* Jyväskylä: Docendo Oy.

Metsämuuronen, J. (. (2006). *Laadullisen tutkimuksen käsikirja.* Jyväskylä: Gummerus Kirjapaino Oy.

Paronen, A. & Teirilä, O. (2014). *Vihatkoon kunhan pelkäävät - näkökulmia terrorismiin ilmiönä.* Tampere: Maanpuolustuskorkeakoulu, Strategian laitos, Julkaisusarja 2, N:o 51, Juvenes Print.

Raggad, B. G. (2010). *Information security management.* Boca Raton: Taylor and Francis Group.

Schmitt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Tuomi, J. & Sarajärvi, A. (2013). *Laadullinen tutkimus ja sisällönanalyysi.* Vantaa: Kustanneosakeyhtiö Tammi.

US Army TRADOC. (2006). *DCSINT Handbook No 1.02: Critical Infrastructure Threats and Terrorism.* Fort Leavenworth: US Army Training and Doctrine Command.

US Army TRADOC. (2007). *US Army TRADOC G2 Handbook No 1: A Military Guide to Terrorism in the Twenty-First Century.* Fort Leavenworth: US Army Training and Doctrine Command.

Weimann, G. (2015). *Terrorism in Cyberspace.* New York: Columbia University Press.

(g) Kyberturvallisuusstrategia

CCDCOE. (9. Maaliskuu 2017b). *Cyber Security Strategy Documents*. Noudettu osoitteesta ccdcoe.org/cyber-security-strategy-documents.html

Centre for Cyber Security of Denmark. (2015). *The Danish Cyber and Information Security Strategy*. Denmark: Centre for Cyber Security.

Czech National Security Authority . (2011). *National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020.* Czech: National Security Authority (Czech).

ENISA. (2012). *National Cyber Security Strategies*. Heraklion: European Network and Information Security Agency (ENISA).

ENISA. (9. Maaliskuu 2017). *National Cyber Security Strategies*. Noudettu osoitteesta www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Estonian Ministry of Economic Affairs and Communication. (2014). *Cyber Security Strategy 2014 - 2017.* Estonia: Ministry of Economic Affairs and Communication.

European Commision. (2013). *Cybersecurity Strategy of the European Union.* Brussels: European Commision and High Representative of the European Union for Foreign Affairs and Security Policy.

Federal Chancellery of the Republic of Austria. (2013). *Austrian Cyber Security Strategy.* Vienna: Federal Chancellery of The Republic of Austria.

French Government. (2015). *French National Digital Security Strategy.* France: Premier Ministre.

German Federal Ministry of the Interior. (2011). *Cyber Security Strategy for Germany.* Berlin: Federal Ministry of the Interior.

Government of Hungary. (2013). *Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary.* Hungary: the Prime Minister's Office of Hungary.

Government of the Republic of Lithuania. (2011). *Resolution No 796: On the Approval of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011 - 2019 .* Vilna: Government of the Republic of Lithuania.

HM Government . (2016). *National Cyber Security Strategy 2016 - 2021.* The United Kingdom: HM Government (the United Kingdom).

Irelands Department of Communications, Energy & Natural Resources. (2015). *National Cyber Security Strategy 2015 - 2017.* Ireland: Department of Communications, Energy & Natural Resources.

Latvian Ministeriön kabinetti nro 40 . (2014). *Cyber Security Strategy of Latvia.* Latvia: Ministeriön kabinetti nro 40.

National Council of the Slovak Republic. (2016). *Cyber Security Concept of the Slovak Republic.* Slovakia: National Council of the Slovak Republic.

Norwegian Ministries. (2012). *Cyber Security Strategy for Norway.* Norway: Norwegian Ministries.

Presidency of the Council of Ministers of Italy. (2013). *National Strategic Framework for Cyberspace Security.* Italy: Presidency of the Council of Ministers.

Presidency of the Government of Spain. (2013). *National Cyber Security Stratategy 2013.* Spain: Gobierno de Espana.

Republic of Croatia. (2015). *The National Cyber Security Strategy of the Republic of Croatia.* Zagreb: Republic of Croatia.

Republic of Poland. (2013). *Cyberspace Protection Policy of the Republic of Poland.* Warsaw: Ministry of Administration and Digitalisation, Internal Security Agency.

The National Coordinator for Security and Counterterrorism of The Netherlands. (2013). *National Cyber Security Strategy 2 - From Awareness to Capability.* Den Haag: The National Coordinator for Security and Counterterrorism.

The Netherlands Ministry of Defence. (2012). *The Defence Cyber Strategy.* The Netherlands: Ministry of Defence.

The White House. (2003). *The National Strategy to Secure Cyberspace.* Washington: The White House (USA).

US Department of Defense . (2015). *The DoD Cyber Strategy.* Washington: The Department of Defense.

(h) Raportti

CCDCOE. (20. Maaliskuu 2017a). *Cyber Definitions*. Noudettu osoitteesta CCDCOE - NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/cyber-definitions.html

Clapper, J. R. (2016). *Worldwide Threat Assessment of the US Intelligence Community.* USA: Senate Armed Service Committee.

ENISA. (2016). *ENISA Threat Landscape 2015.* Heraklion: The European Union Agency for Network and Information Security (ENISA).

ENISA. (2017). *ENISA Threat Landscape Report 2016.* Heraklion: The European Union Agency for Network and Information Security (ENISA).

EUROPOL . (2016). *European Union Terrorism Situation and Trend Report 2016.* The Hague: European Police Office.

EUROPOL . (2017). *European Union Terrorism Situation and Trend Report 2017.* The Hague: European Union Agency for Law Enforcement Cooperation 2017.

Gordon, S. & Ford, R. (2003). *Cyberterrorism?* Mountain View, USA: Symantec Security Response - White Paper.

HM Government . (2015). *National Security Strategy and Strategic Defence and Security Review 2015.* London: HM Government (the United Kingdom).

ICT - International Institute for Counter-Terrorism. (2016a). *Cyber-Terrorism Activities, Report No. 16, January - March 2016.* Herzliya: ICT - International Institute for Counter-Terrorism.

ICT - International Institute for Counter-Terrorism. (2016b). *Cyber-Terrorism Activities, Report No. 17, April - June 2016.* Herzliya: ICT - International Institute for Counter-Terrorism.

ICT - International Institute for Counter-Terrorism. (2016c). *Cyber-Terrorism Activities, Report No. 18, July - September 2016.* Herzliya: ICT - International Institute for Counter-Terrorism.

ICT - International Institute for Counter-Terrorism. (2016d). *Cyber-Terrorism Activities, Report No. 19, October - December 2016.* Herzliya: ICT - International Institute for Counter-Terrorism.

ICT - International Institute for Counter-Terrorism. (2017a). *Cyber Report No.22, May 2017.* Herzliya: ICT - International Institute for Counter-Terrorism.

ICT - International Institute for Counter-Terrorism. (2017b). *Cyber Report no.23, June - August 2017.* Herzliya: ICT - International Institute for Counter-Terrorism.

ICT - International Institute for Counter-Terrorism. (2017d). *Cyber-Terrorism Activities, Report No. 21, April 2017.* Herzliya: ICT - International Institute for Counter-Terrorism.

ICT- International Institute for Counter-Terrorism. (2017c). *Cyber-Terrorism Activities, Report No. 20, January - March 2017.* Herzliya: ICT- International Institute for Counter- Terrorism.

Lehto, M. (2015). *Kybermaailman ilmiöitä ja määrittelyjä.* Jyväskylä: Informaatioteknologian tiedekunta, Jyväskylän yliopisto.

Lehto, M., Limnell, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. (2017). *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.* Suomi: Valtioneuvoston selvitys- ja tutkimustoiminta.

Leppänen, A., Lindenborg, K. & Saarimäki, J. (2016). *Tietoverkkorikollisuuden tilannekuva.* Suomi: Valtioneuvoston selvitys- ja tutkimustoiminta.

Pirhonen, M. & Jauhiainen, E. (26. Huhtikuu 2017). *Ohjeita pro gradu -tutkielmien tekijöille tietojenkäsittelytieteiden laitoksella.* Noudettu osoitteesta Jyväskylän yliopisto: https://www.jyu.fi/it/opiskelu-ohjeet/TKTL-ohjeet/opinnaytetyot/ohjeita-tutkielmien-tekijoille

US Department of Defense. (2010). *Joint Terminology for Cyberspace Operations.* Washington: The Vice Chairman of the Chiefs of Staff.

US Department of Defense. (22. Maaliskuu 2017). *Department of Defense Dictionary of Military and Associated Terms.* Noudettu osoitteesta www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Valtioneuvosto. (2013a). *Suomen kyberturvallisuusstrategia.* Forssa: Turvallisuuskomitean sihteeristö.

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

(i) Verkkosivu

Automatic brakes stopped Berlin truck during Christmas market attack. (28. Joulukuu 2016). Noudettu osoitteesta Deutsche Welle: http://www.dw.com/en/automatic-brakes-stopped-berlin-truck-during-christmas-market-attack/a-36936455

Brussells explosions: What we know about airport and metro attacks. (9. Huhtikuu 2016). Noudettu osoitteesta BBC news: http://www.bbc.com/news/world-europe-35869985

French police officer and partner murderd in 'odious terrorist attack'. (14. Kesäkuu 2016). Noudettu osoitteesta The Guardian: https://www.theguardian.com/world/2016/jun/14/french-police-officer-wife-murdered-larossi-abballa-isis

Islamic State claims responsibility for attack on Russian traffic police. (18. Elokuu 2016). Noudettu osoitteesta Reuters wolrd news: https://www.reuters.com/article/us-russia-islamic-state/islamic-state-claims-responsibility-for-attack-on-russian-traffic-police-idUSKCN10T25S

Islamic terrorism in Europe (2014 - present). (17. Marraskuu 2017). Noudettu osoitteesta Wikipedia: https://en.wikipedia.org/wiki/Islamic_terrorism_in_Europe_(2014%E2%80%93present)

Istanbul Ataturk airport attack: 41 dead and more than 230 hurt. (29. Kesäkuu 2016). Noudettu osoitteesta BBC News: http://www.bbc.com/news/world-europe-36658187

Istanbul bombing: At least five killed in Turkish city. (20. Maaliskuu 2016). Noudettu osoitteesta Aljazeera: http://www.aljazeera.com/news/2016/03/istanbul-taksim-square-area-hit-explosion-160319091702737.html

Istanbul new year Reina nightclub attack 'leaves 39 dead'. (1. Tammikuu 2017). Noudettu osoitteesta BBC News: http://www.bbc.com/news/world-europe-38481521

Manchester attack: 22 dead and 59 hurt in suicide bombing. (23. Toukokuu 2017). Noudettu osoitteesta BBC News: http://www.bbc.com/news/uk-england-manchester-40010124

Paris: French police officer killed in terrorist shooting on Champs Elysees. (20. Huhtikuu 2017). Noudettu osoitteesta The Local France: https://www.thelocal.fr/20170420/two-french-police-injured-in-shooting-on-champs-elysees

The Guardian. (5. kesäkuu 2017). *London terror attack: what we know so far*. Noudettu osoitteesta https://www.theguardian.com/uk-news/2017/jun/04/london-attacks-what-we-know-so-far-london-bridge-borough-market-vauxhall

Truck Attack in Nice, France: What We Know, and What We Don't. (15. Heinäkuu 2016). Noudettu osoitteesta nytimes, internet archieve: https://web.archive.org/web/20160717172843/http://www.nytimes.com/2016/07/16/world/europe/nice-france-truck-attack-what-we-know.html?ref=liveblog

U.K. Parliament attack: Five dead and 40 injured in 'sick and depraved terrorist incident' at Westminster. (22. Maaliskuu 2017). Noudettu osoitteesta National Post: http://nationalpost.com/news/world/several-injured-outside-british-parliament-house-on-lockdown-amid-reports-of-several-injuries-outside