UNIVERSITY OF
EASTERN FINLAND

Terrorismirikostunnusmerkistöjen kattavuus ja sovellettavuus kyberterrorismissa

Elina Rokka, 175159
Itä-Suomen yliopisto
Oikeustieteiden laitos
Pro gradu -tutkielma
01.05.2022
Ohjaajat: Matti Tolvanen ja Heikki Kallio

Tiivistelmä

ITÄ-SUOMEN YLIOPISTO

Tiedekunta	Yksikkö
Yhteiskuntatieteiden ja kauppatieteiden tiedekunta	**Oikeustieteiden laitos**
Tekijä: **Elina Rokka**	

Työn nimi: **Terrorismirikostunnusmerkistöjen kattavuus ja sovellettavuus kyberterrorismissa**			
Pääaine: **Rikosoikeus**	Työn laji: **Pro gradu -tutkielma**	Aika: **01.05.2022**	Sivuja: **xiv–85**

Tiivistelmä

Terrorismi on yksi vakavimmista henkeä, terveyttä ja turvallisuutta vaarantavista rikoksista, josta säädetään rikoslain 34 a luvussa. Rikoslain 34 a lukua on laajennettu kansainvälisten sopimusten myötä ja lukuun on sisällytetty vakaviin tietoverkkorikoksiin liittyvää sääntelyä. Tietoverkkoihin kohdistuva uhka on tällä hetkellä todellinen ja ajankohtainen, sillä Venäjän Ukrainaan aloittaman hyökkäyssodan myötä Suomen turvallisuustilanne on muuttunut ja Suomeen kohdistettavien kybertoimien uhka on kasvanut.

Tutkielma koostuu kahdesta varsinaisesta tutkimuskysymyksestä; ensinnäkin tuleeko rikoslain 34 a luku sovellettavaksi kyberterrorismissa ja toisekseen kattaako kyseinen luku kyberterrorismin, vai onko lainsäädännössä uudistamistarpeita tai puutteita? Tutkimuskysymyksiin edetään osakysymysten avulla, ensin määrittäen keskeiset käsitteet. Tutkimuskysymyksiä tarkastellaan lainopillisesti, mutta terrorismin luonteesta johtuen tutkielmassa on myös oikeus- ja yhteiskuntatieteellistä tutkimusta.

Rikoslain 34 a luku tulee sovellettavaksi kyberhyökkäyksissä, mikäli rikoksentekijällä on terroristinen tarkoitus ja teko on omiaan aiheuttamaan vakavaa vahinkoa. Lainsäädäntö kattaa palvelunestohyökkäykset ja haittaohjelmat, mutta kybervaikuttamisen osalta lainsäädännössä ei ole olemassa määritelmää. Kybervaikuttamiseen liittyvä edeltävä teko on kriminalisoitu RL 34 a luvussa (esim. kiristyshaittaohjelmat), mutta vaikuttamisesta itsessään ei ole säädetty RL 34 a luvussa. Kybervakoilusta säädetään RL 34a:4:ssä, jos vakoilua harjoitetaan osana terroristiryhmää, mutta yksin tai kaksin toteutetusta kybervakoilusta terroristisessa tarkoituksessa ei ole säädetty RL 34 a luvussa. Rikoslain 34 a lukuun tulisi lisätä kybervaikuttamista koskeva säännös ja kybervakoilu yksittäisen henkilön toimesta tulisi saattaa rangaistavaksi.

Tällä hetkellä lainsäädäntö kattaa tyypillisempiä tietoverkkorikoksia, mutta teknologian ja terrorismin nopeasta kehityksestä johtuen lainsäädäntöä tulisi tarkastella säännöllisesti, jotta ilmiöön pystytään vastaamaan oikea-aikaisesti. Rikoslain 34 a luku on kokonaisuutena tarkastellen haastava ja epäselvä kokonaisuus, joka vaatii säädöksen yksinkertaistamiseksi kokonaisuudistuksen.

Avainsanat: Kyberterrorismi, terrorismi, tietoverkkorikollisuus, abstraktinen vaarantamisrikos, tietoturvallisuus, kyber, kyberhyökkäys, kybervaikuttaminen, kybersota, kansallinen turvallisuus, kybertoimintaympäristö, kybervakoilu, hybridivaikuttaminen, kyberrikollisuus, kyberuhka, kriittinen infrastruktuuri

SISÄLLYS

LÄHTEET

KIRJALLISUUS

Aarnio, Aulis, Mitä lainoppi on? Tammi Helsinki 1978.

Cassese, Antonio, International Criminal Law, 2nd edition. Oxford University Press 2008.

Esko, Anna, Kansainvälinen oikeus, terrorismi ja sodankäynti. Defensor Legis N:o 1/2017, s. 102–107.

Ferm, Tiina, Artikkeleita Eurooppa oikeudesta. Ajankohtaista EU:n hybridiuhkien torjunnasta. Defensor Legis N:o 3/2018, s. 404–419.

Hanhimäki, Jussi – Blumeneau Bernhard, An International History of Terrorism: Western and Non-Western Experiences. Taylor & Francis Group 2013.

Härkönen, Henrik, Terroristiryhmän rikosoikeudellinen sääntely. Lakimies 2/2006 s. 216–235.

Jansson, Saara – Sihvonen Tanja, Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. Media ja Viestintä 41/2018. [https://journal.fi/mediaviestinta/article/view/69950]

Järvinen, Petteri, Kyberuhkia ja somesotaa. Digiaikana sinäkin olet etulinjassa. Docendo Oy Jyväskylä 2018.

Korkka-Knuts, Heli – Helenius Dan – Frände Dan, Yleinen rikosoikeus. Otavan Kirjapaino Oy Keuruu 2020.

Laari, Tommi – Flyktman, Jouni – Härmä, Katriina – Timonen, Jussi – Tuovinen, Jussi, Kyberpuolustus, kyberkäsikirja Puolustusvoimien henkilöstölle 2019. Maanpuolustuskorkeakoulu Julkaisusarja 3: Työpapereita nro 12, Sotataidon laitos Helsinki. [https://www.doria.fi/handle/10024/173254]

Lappi-Seppälä, Tapio – Hakamies, Kaarlo – Helenius, Dan – Koskinen, Pekka – Majanen, Martti – Melander, Sakari., … Rautio, Ilkka, Rikosoikeus. Alma Talent Helsinki 2009.

Limnèll, Jarno – Majewski, Klaus – Salminen, Mirva, Kyberturvallisuus. Docendo Oy Jyväskylä 2014.

Limnèll, Jarno – Iloniemi, Jaakko, Uhkakuvat. Docendo Oy Jyväskylä 2018.

Lohse, Mikael, Terrorismirikoksen valmistelu ja edistäminen. Oy Nord Print Ab, Helsinki 2012.

Lohse, Mikael, Terroristinen edistäminen ja sitä lähellä olevat osallisuusmuodot. Referee-artikkeli. Edilex-sarja 2011/18. [www.edilex.fi/artikkelit/8043]

Lohse, Mikael – Meriniemi, Marko – Honkanen Kosti, Tiedustelumenetelmät. Alma Talent Oy 2019.

Lohse, Mikael – Viitanen Marko, Johdatus tiedusteluun. Alma Talent Oy 2019.

Malkki, Leena, Mitä tiedämme terrorismista. Kustannusosakeyhtiö Otava Keuruu 2020.

Melander, Sakari, EU-rikosoikeus (2. uud. p.). Helsinki: Talentum Media 2015.

Minkkinen, Panu, Oikeus- ja yhteiskuntatieteellinen tutkimus – suuntaus, tarkastelutapa, menetelmä? Lakimies 7–8/2017 s. 908–923.

Määttä, Tapio, Oikeudellisen ajattelun perusteita: oikeustieteiden pääsykoekirja 2012. Joensuu: University of Eastern Finland 2012.

Määttä, Tapio – Tolvanen, Matti – Kolehmainen, Antti – Kosonen, Jonna – Väätänen, Ulla – Keinänen, Anssi, Oikeudellisen ajattelun perusteita. Joensuu: University of Eastern Finland 2018.

Nevalainen, Sami, Kyberrikokset ja Suomen rikosoikeus. Defensor Legis N:o 2/2019, s. 131–148.

Oikeusministeriö, Lainkirjoittajan opas 37/2013. [https://julkaisut.valtioneuvosto.fi/handle/10024/76493] (15.3.2022)

Paasonen, Jyri – Aaltonen, Mikko – Luomala, Mikko, Kyberrikokset tuomioistuimisissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset. Referee-artikkeli, Defensor Legis 4/2021, s. 966–987.

Pihlajamäki, Antti, Tietojenkäsittelyrauhan rikosoikeudellinen suoja. Datarikoksia koskeva sääntely Suomen rikoslaissa. Gummerus Kirjapaino Oy Jyväskylä 2004.

Schneier, Bruce, Klikkaa tästä ja tapa kaikki. Suojaus ja eloonjääminen hyperkytkeytyneessä maailmassa. Painoliber Oy Helsinki 2020.

Sirjonen, Roni, Oikeutettua sotaa verkossa: Milloin kyberhyökkäys täyttää aseellisen voimankäytön vaatimukset., Acta Legis Turkuensia 1/2018.

Sisäministeriö, Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14/2017. [https://julkaisut.valtioneuvosto.fi/handle/10024/79866] (01.04.2022)

Sisäminiteriö, Varautuminen muuttoliikettä hyväksikäyttävään hybridivaikuttamiseen. Selvitys lainsäädännön muutostarpeista. Sisäministeriön julkaisuja 2022:20. [https://julkaisut.valtioneuvosto.fi/handle/10024/163861] (03.04.2022)

Tapani, Jussi – Tolvanen, Matti, Rikosoikeus: Rangaistuksen määrääminen ja täytäntöönpano 2. uudistettu painos. Juridica-kirjasarja No. 12. Helsinki, Talentum 2011.

Tapani, Jussi – Tolvanen, Matti, Rikosoikeuden yleinen osa – Vastuuoppi. Alma Talent Oy 2019.

Tiilikainen, Heikki, Hybridisota: rintamaraportti. Helsinki, Auditorium 2015.

Traficom, Kyberturvallisuus ja yrityksen hallituksen vastuu. Traficomin julkaisuja 02/2020. [https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas] (23.03.2022)

Turvallisuuskomitea, Kyberturvallisuuden sanasto. Sanastokeskus TSK ry, Helsinki 2018. [http://www.tsk.fi/tsk/fi/kyberturvallisuuden_sanasto_tsk_52-1125.html] (25.4.2022)

Virtanen, Vesa – Salmi, Ilkka – Penttilä, Teemu – Ossa, Jaakko – Nurmi, Veli-Pekka – Aine, Antti, Moderni kriisilainsäädäntö. Talentum Media Helsinki 2011.

Weimann, Gabriel, Terrorism in Cyberspace. New York: Columbia University Press 2015.

VIRALLISLÄHTEET

Euroopan unionin neuvosto., Neuvoston päätös unionia tai sen jäsenvaltiota uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä 7299/19. Bryssel 14.5.2019 (OR.en).

Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU 12.8.2013 tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta.

Euroopan parlamentin ja neuvoston direktiivi 2017/541/EU 15.3.2017 terrorismin torjumisesta sekä neuvoston puitepäätöksen 2002/475/YOS korvaamisesta sekä neuvoston päätöksen 2005/671/YOS muuttamisesta.

HE 1/1996 vp. Hallituksen esitys Eduskunnalle Suomen rikosoikeuden soveltamisalaa koskevan lainsäädännön uudistamisesta.

HE 44/2002 vp. Hallituksen esitys Eduskunnalle rikosoikeuden yleisiä oppeja koskevan lainsäädännön uudistamiseksi.

HE 188/2002 vp. Hallituksen esitys Eduskunnalle terrorismia koskeviksi rikoslain ja pakkokeinolain säännöksiksi.

HE 3/2008 vp. Hallituksen esitys Eduskunnalle valmiuslaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 289/2014 vp. Hallituksen esitys eduskunnalle Kansainvälisen rikostuomioistuimen Rooman perussääntöön vuonna 2010 Kampalan tarkistuskonferenssissa tehtyjen muutosten hyväksymisestä sekä laeiksi muutosten lainsäädännön alan kuuluvien määräysten voimaansaattamisesta sekä rikoslain ja pakkokeinolain muuttamisesta.

HE 30/2018 vp. Hallituksen esitys Eduskunnalle laeiksi rikoslain, pakkokeinolain 10 luvun ja poliisilain 5 luvun muuttamisesta.

Komiteanmietintö 2005:2. Ehdotus uudeksi valmiuslaiksi., Valmiuslakitoimikunnan mietintö. Oikeusministeriö Helsinki 2005.

Melander, Sakari 2016, Lausunto eduskunnan perustuslakivaliokunnalle 17.11.2016. Asia: Valtioneuvoston U-kirjelmä (U) 22/2015 vp eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi (terrorismin torjuminen). Helsingin yliopisto, oikeustieteellinen tiedekunta.

Melander, Sakari 2020, Lausunto eduskunnan perustuslakivaliokunnalle 12.11.2020. Asia: Hallituksen esitys (HE 135/2020 vp) eduskunnalle terrorismin rahoittamista koskevien säännösten muuttamiseksi.

Neuvoston puitepäätös (2002/475/YOS), 13.6.2002 terrorismin torjumisesta.

Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013. Turvallisuuskomitean sihteeristö. Forssa Print, 2013. [https://um.fi/julkaisut/-/asset_publisher/TVOLgBmLyZvu/content/suomen-kyberturvallisuusstrategia-] (22.3.2022)

Suomen kyberturvallisuusstrategia 2019, Valtioneuvoston periaatepäätös 3.10.2019. Turvallisuuskomitean sihteeristö 2019. [https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/] (22.03.2022)

Ulkoministeriö, Perusmuistio UM2020-00783. EU/YUTP/EDUSKUNNALLE TIEDOTTAMINEN/Unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaiset rajoittavat toimenpiteet. UTP40/2018vp.

INTERNETLÄHTEET

Helsingin Sanomat 8.4.2022. Valtion verkkosivut joutuivat verkkohyökkäyksen kohteeksi – Ulkoministeriö tekee asiasta rikosilmoituksen. [https://www.hs.fi/kotimaa/art-2000008738855.html] (14.4.2022)

Iltalehti 1.3.2022. Hakkeriryhmä estänyt Venäjän sotakuljetuksia – halvaannutti raideliikenteen. [https://www.iltalehti.fi/digiuutiset/a/471ecb18-1256-42d7-8088-61434f1f6341] (02.04.2022)

Ilta-Sanomat, 8.4.2022. Ulkoministeri Haavisto arvioi: hyökkäys ministeriöiden sivuille oli muistutus Venäjältä. [https://www.is.fi/politiikka/art-2000008740577.html] (17.04.2022)

Keski-Uusimaa, 18.3.2022. Tekoälyllä luodut deepfake -valevideot valjastettiin Ukrainan sodan propaganda-aseeksi – väärennettyä videota presidentti Zelenskyin antautumisesta levitettiin netissä. [https://www.keski-uusimaa.fi/uutissuomalainen/4518773] (03.04.2022)

Suojelupoliisi, 29.3.2022. Supon vuosikirja 2021: Suomalaisten on varauduttava Venäjän vaikuttamisyrityksiin Nato-keskustelun aikana. [https://supo.fi/-/supon-vuosikirja-2021-suomalaisten-on-varauduttava-venajan-vaikuttamisyrityksiin-nato-keskustelun-aikana] (1.5.2022)

Suojelupoliisi, kyberuhkat. [https://supo.fi/kyberuhkat] (03.04.2022)

Talouselämä, 28.2.2022. Venäjälle taas pettymyksiä – Hakkerit pysäyttelevät joukkoja liikuttavia junia matkalla rajalle. [https://www.talouselama.fi/uutiset/venajalle-taas-pettymyksia-hakkerit-pysayttelevat-joukkoja-liikuttavia-junia-matkalla-rajalle/ad67a279-754a-4cb1-861e-8270f6fb875c] (18.04.2022)

Tilastokeskus, Käsitteet – Väestö. [https://www.stat.fi/meta/kas/vaesto.html] (14.04.2022)

Valtioneuvosto, 8.12.2021. Valmiuslain uudistaminen käynnistyy. [https://valtioneuvosto.fi/-//1410853/valmiuslain-uudistaminen-kaynnistyy] (15.03.2022)

Yle Uutiset, 3.3.2022. Ukrainan puolesta taistelee ennennäkemätön hakkeriarmeija, mukana suomalainen ”Jouni” – asiantuntijat varoittavat: ”tämä ei ole leikkisotaa”. [https://yle.fi/uutiset/3-12338836] (17.03.2022)

Yle Uutiset, 13.2.2022. Putinin kaasupeli. Venäjän kaasuhanojen sulkeminen ajaisi Keski-Euroopan kriisiin. Temppu voisi silti kääntyä itseään vastaan. [https://yle.fi/uutiset/3-12307391] (17.03.2022)

Yle Uutiset, 28.2.2022. Hakkeriryhmä Anonymous julisti kybersodan Venäjää vastaan – väittää kaataneensa useita Venäjän hallinnon sivustoja. [https://yle.fi/uutiset/3-12336205] (02.04.2022)

Yle Uutiset, 1.11.2013. HS: Vinkki verkkovakoilusta tuli Ruotsista. [https://yle.fi/uutiset/3-6914048] (07.04.2022)

LYHENNELUETTELO

ETYJ	Euroopan turvallisuus- ja yhteistyöjärjestö
EN	Euroopan neuvosto
EU	Euroopan unioni
Deepfake	Video- tai kuvaväärennös
Hakkeri	Henkilö, joka tunkeutuu luvatta tietokoneeseen, -järjestelmään tai -verkkoon
HE	Hallituksen esitys
NATO	Pohjois-Atlantin puolustusliitto (North Atlantic Treaty Organisation)
NIS	EU:n verkko- ja tietoturvadirektiivi
OECD	Taloudellisen yhteistyön ja kehityksen järjestö (Organisation for Economic Co-operation and Development)
PolL	Poliisilaki
RL	Rikoslaki
SotTiedL	Laki sotilastiedustelusta
Supo	Suojelupoliisi
TtStL	Laki tietoliikennetiedustelusta siviilitiedustelussa
Telegram	Viestintäsovellus
Tietoverkkorikosdirektiivi	EU:n komission ja neuvoston direktiivi tietoverkkoihin kohdistuvista hyökkäyksistä 2013/40/EU. EUVL nro 218, 14.8.2013
Tietoverkkorikossopimus	Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus. CETS 185, Budapest 23.11.2001. SopS 60/2007
YK	Yhdistyneet kansakunnat

KUVIOT JA TAULUKOT

1 JOHDANTO

1.1 Johdatus aiheeseen

Terrorismi on yksi vakavimmista rikoksista ihmiskunnassa, joka uhkaa välittömästi ihmishenkeä, terveyttä ja turvallisuutta. Tämä vakavasti henkeä, terveyttä ja turvallisuutta vaarantava rikollisuus kehittyy ja hyödyntää yhä enenevissä määrin apunaan teknologiaa.[1] Terrorismirikoksista säädetään Suomen rikoslain 34 a luvussa (39/1889, RL) ja lukuun on nykyisin sisällytetty yhä enemmän vakaviin tietoverkkorikoksiin liittyvää sääntelyä.

Rikoslain 34 a luku on verrattain uusi ja lisätty rikoslakiin vuonna 2003 EU:ssa vuonna 2001 hyväksytyn terrorismin torjuntaa koskevan puitepäätöksen (2002/475/YOS) myötä. [2] Kyseinen terrorisimipuitepäätös korvattiin vuonna 2008 uudella puitepäätöksellä (2008/919/YOS), jolla velvoitettiin kaikkia jäsenmaita kriminalisoimaan mm. terroristisessa tarkoituksessa tehdyt tietoverkkorikokset. Lainsäädäntöä terrorismin osalta on myöhemmin laajennettu uusien kansainvälisten sopimusten myötä.[3] Terrorismiin liittyvä uhka on kasvanut viimeisten vuosikymmenten aikana ja rikoslain 34 a luvulle on olemassa selvä tarve. Rikoslain 34 a lukua on päivitetty vastaamaan nykymaailman turvallisuusuhkaa ja viimeisimmät lisäykset terrorismirikoslakiin on tehty vuonna 2021. Suomessa ei vielä toistaiseksi ole nähty rikoslain 34 a luvun mukaisia tietoverkkorikostapauksia, joten laki ei ole vielä tullut käytännössä sovellettavaksi. Tietoverkkoihin kohdistuva uhka on kuitenkin tällä hetkellä todellinen ja ajankohtainen, sillä Venäjän Ukrainaan aloittaman hyökkäyssodan myötä Suomen turvallisuustilanne on muuttunut ja Suomeen kohdistettavien kyberhyökkäysten uhka on kasvanut[4].

---

[1] Limnell – Majewski – Salminen 2014, s. 130–135.
[2] HE 188/2002 vp.
[3] Malkki 2020, s. 32. Puitepäätös hyväksyttiin syyskuussa 2001 Yhdysvalloissa tapahtuneiden iskujen jälkeen.
[4] Suojelupoliisi, 29.3.2022. Supon vuosikirja 2021: Suomalaisten on varauduttava Venäjän vaikuttamisyrityksiin Nato-keskustelun aikana. [https://supo.fi/-/supon-vuosikirja-2021-suomalaisten-on-varauduttava-venajan-vaikuttamisyrityksiin-nato-keskustelun-aikana]

Kyberterrorismi on terrorismin lailla jatkuvasti kehittyvä rikollisuuden muoto, joka vaatii lainsäädännön ajantasaisuutta sen torjumiseksi ja tekojen saattamiseksi rangaistavuuden piiriin. Lainsäädäntö edellyttää täsmällisiä kriminalisointeja, mutta toisaalta liian tarkka määritelmä voi luoda kielellisesti pitkiä ja monimutkaisia rikostunnusmerkistöjä. Tutkimuksen aihe sisältää paljon määritelmiä, joille ei ole kansainvälisesti onnistuttu sopimaan kaikkien hyväksymää kattavaa sisältöä[5]. Suomen terrorismirikoksia koskevan lainsäädännön on sanottu olevan monessa suhteessa poikkeuksellinen kokonaisuus, sillä sääntely on vaikeaselkoista ja monimutkaista sisältäen paljon viittauksia rikoslain muihin säännöksiin.[6] Kyberterrorismiin liittyvä säännös (RL 34a:1.1,4) on kokoelma rikoslaissa aiemmin säädetyistä teoista.

1.2 Tutkimuskysymykset ja rajaukset

Tutkielman aihe on ajankohtainen, sillä Suomi määrittää tällä hetkellä turvallisuuspolitiikkaansa uudelleen Venäjän Ukrainaan aloittaman hyökkäyssodan takia. Suomi tekee ratkaisua Natoon liittymisestä ja tämä tulee todennäköisesti lisäämään vakavien kyberiskujen todennäköisyyttä lähiaikoina. Tutkielma koostuu kahdesta varsinaisesta tutkimuskysymyksestä; ensinnäkin tuleeko RL 34 a luku sovellettavaksi kyberterrorismiin liittyvissä rikoksissa? Rikoslain 34 a luvun sovellettavuutta arvioidaan kyberhyökkäystä ja -vaikuttamista koskevien tekojen osalta ja lisäksi arvioidaan värväyksen (RL 34a:4c) ja terrorismirikoksiin liittyvän julkisen kehottamisen (RL 34a:5e) soveltuvuutta kyberterrorismirikoksissa. Sovellettavuuden arviointi kyberterrorismin osalta on valikoitunut tarkasteltavaksi edellä mainittujen tekojen osalta, sillä teot ovat ajankohtaisia uhkia yhteiskunnassamme. Tutkielmassa ei siten ole tarkoitus tehdä sovellettavuuden arviointia koko kyberterrorismiin liittyvän sääntelyn osalta.

Toisena tutkimuskysymyksenä on, kattaako lainsäädäntö tällä hetkellä kyberterrorismiin liittyvän rikollisuuden vai onko lainsäädäntö kyberterrorismin osalta joiltain osin puutteellinen? Arviointia on toteutettu rikoslain 34 a luvun näkökulmasta ja lisäksi on tarkasteltu muun lainsäädännön, eli

[5] Esko 2017, s. 106.
[6] Melander 2015, s. 416–420.

tiedustelulain, valmiuslain ja pakotejärjestelmän merkitystä kyberterrorismin torjunnan kannalta.

Tutkielmassa kyberterrorismilla tarkoitetaan tyypillisimpiä tekoja, jotka ovat yksittäisten henkilöiden tai valtioiden tekemiä ja jotka kohdistuvat yhteiskunnan kannalta elintärkeisiin toimintoihin tai infrastruktuuriin. Kyberterrorismilla ei tässä tutkielmassa tarkoiteta sotaa käyvien valtioiden välisiä kybersotatoimia, vaan kybersota jää tutkimuksen ulkopuolelle. Tutkielmassa kuitenkin käydään läpi kyberterrorismin ja kybersodan välistä rajanvetoa, mutta aiheesta ei ole tarkoitus tehdä kattavaa selvitystä. Aihetta on tutkimuksen kannalta tärkeää sivuta, sillä kybersodalla ja kyberterrorismilla on paljon yhteistä kosketuspintaa ja päällekkäisyyttä[7].

Tutkielma on rajattu koskemaan kyberterrorismin osalta vain kansallista lainsäädäntöä ja tästä syystä ei ole ollut relevanttia tehdä kansainvälistä oikeusvertailua. Lisäksi kyberterrorismiin liittyvässä tarkastelussa ei keskitytä varsinaisten tietojärjestelmien toimivuuteen, hyökkäyksen tekniseen toteutukseen tai tietyistä toimenpiteistä aiheutuviin seurauksiin, vaan tarkastelu toteutetaan tarkastelemalla yleisellä tasolla aktiivista tekovaihetta rikoslain 34 a luvun tunnusmerkistön avulla. Tutkielmassa kyberterrorismi rajataan koskemaan tyypillisimpiä vakavia tekoja, joilla voidaan lamauttaa yhteiskunnan elintärkeitä toimintoja. Näin ollen tutkielmassa ei keskitytä pienempiin terroristisiksi teoiksi luokiteltaviin tekoihin.

Tutkielmassa on esitettynä kyberterrorismin osalta keskeiset käsitteet ja niiden määritelmät, jotka liittyvät olennaisilta osin kyberterrorismin kokonaisuuden ymmärtämiseen. Tutkielman tutkimuskysymysten luonteesta johtuen määritelmien tarkoituksena ei ole ollut laatia käsitteistä kaiken kattavaa määritelmää, vaan tarkoituksena on ollut selvittää, mitä kullakin käsitteellä tänä päivänä tarkoitetaan ja miten ne tulisivat tunnusmerkistöjen osalta sovellettavaksi RL 34 a luvussa. Tarkoituksena on ollut tuoda esiin määrittelemiseen ja määrittelemättömyyteen liittyviä haasteita ja niistä aiheutuvia oikeudellisia ja poliittisia ongelmia.

[7] Esko 2017, s. 111–112.

1.3 Tutkimusmenetelmä

Tutkielmassa tarkastellaan tutkimuskohdetta ja siihen liittyviä tutkimuskysymyksiä rikoslainopillisesti eli oikeusdogmaattisesti. Rikoslainopin tehtävänä on voimassa olevien rikosoikeudellisten säännösten tulkinta ja systematisointi. Rikoslainopin voidaan katsoa olevan lainopillisten ongelmien uudelleenmuotoilua, uudenlaista systemaattisten yhteyksien osoittamista ja relevanttien näkökohtien jäsentämistä. Rikosoikeudellinen materiaali pyritään jäsentämään rationaaliseksi kokonaisuudeksi ja tarkoituksena on helpottaa rikoslain normien käytännön sovellettavuutta. Tutkielmassa käytetään rikoslainopillisen tutkimuksen tavoin lähteinä säädöstekstejä, hallituksen esityksiä ja oikeuskirjallisuutta.[8] Lisäksi ilmiöiden selittämisen tueksi on esitetty esimerkkitapauksia uutisartikkeleista.

Lainoppi jaetaan tyypillisesti käytännölliseen ja teoreettiseen lainoppiin. Käytännöllisestä lainopista käytetään myös termiä tulkintajuridiikka, jonka keskeisin tehtävä on tuottaa suosituksia siitä, miten lakia tulisi soveltaa. Käytännöllisestä lainopista voidaan myös puhua tulkintatieteenä, joka ei tutki säännönmukaisuuksia eikä lainopin tulkintatuloksia empiirisesti. Sen sijaan lainopin kohteena ovat juridiset tekstit ja niiden merkityssisällöllinen täsmentäminen. Menetelmän ydin koostuu oikeuslähde-, tulkinta- ja argumentaatio-opeista, jolloin tutkija toimii ja ajattelee konkreettisen lainsoveltajan (viranomainen, tuomioistuin) tavoin.[9]

Käytännöllinen lainoppi tarvitsee oikeusjärjestyksen ymmärtämiseen teoreettista tausta-ainesta ja systematisointia, jotta käytännön lainopin avulla on mahdollista syventyä oikeudellisten ilmiöiden ydinkysymyksiin. Oikeustosiseikkojen ja oikeudellisten seuraamusten välistä suhdetta ei käytännön lainoppi kykene tunnistamaan, mikäli käsitteistö on muotoiltu liian epämääräisesti ja abstraktisti. Teoreettisen lainopin avulla voidaan luoda uudenlaisia systematisointitapoja, joilla on määräävää vaikutusta käytännön lainoppiin.[10] Tulkintakannanottojen perusta toteutetaan

[8] Määttä – Tolvanen ym. 2018, s. 72.
[9] Määttä 2012, s. 17–18.
[10] Aarnio 1978, s. 98.

teoreettisen lainopin tuottamien ja kehittämien yleisten oppien (käsitteiden, periaatteiden ja teorioiden) avulla. Yleisillä opeilla tarkoitetaan oikeustieteen luomaa, johdonmukaista oppijärjestelmää, joka toimii lainsoveltajan apuvälineenä ja jolla jäsennetään ja tehdään ymmärrettäväksi oikeuden ulkoisia suhteita. Lainsäätämisen kannalta yleisillä opeilla on tärkeä merkitys, sillä uudet säännökset sijoittuvat osaksi aiempaa oikeudellista järjestelmää.[11]

Nykyisin oikeustieteelliselle tutkimukselle on ominaista käyttää erilaisten menetelmien ja näkökulmien moninaisuutta ja rinnakkaisuutta. Oikeustiedettä ei voida kuvata enää vain lainopiksi ja sitä täydentäviksi oikeuden yleistieteiksi sen laaja-alaistumisesta ja monipuolistumisesta johtuen.[12] Tässä tutkielmassa ei keskitytä pelkästään voimassa olevan oikeuden systematisointiin, vaan tarkoituksena on tarkastella kriittisesti säännöksen (RL 34 a) rikosoikeudellista sovellettavuutta. Tutkielma ei myöskään ole täysin puhtaasti lainopillinen tutkimus, sillä terrorismirikoksia rinnastetaan toisinaan myös poliittisiin rikoksiin[13]. Tästä syystä terrorismirikoksilla on olemassa oikeudellisen näkökulman lisäksi vahva suhde politiikkaan. Oikeutta voidaan tarkastella siten myös yhteiskunnallisessa ja poliittisessa yhteydessä, jolloin puhutaan oikeus- ja yhteiskuntatieteellisestä tutkimuksesta. Kyse ei kuitenkaan ole lainopista poikkeavasta ulkoisesta tutkimusmenetelmästä, vaan oikeus- ja yhteiskuntatieteellisessä tutkimuksessa voidaan tutkia kaikkia perinteisiä oikeudellisia aiheita.[14]

Tutkielmassa esiintyy yhteiskuntatieteellistä näkökulmaa käsitteiden määrittelyn yhteydessä, jolloin tarkastellaan oikeudellista ja poliittista näkökulmaa sekä niiden välistä suhdetta. Tutkielmassa on myös oikeusteoreettista pohjaa, jonka avulla tarkastellaan oikeuskäsitteitä. Lisäksi lainopilliselle tutkimukselle luontevana sivutuotteena voidaan nähdä lain kehittämistä koskevien de lege ferenda -suositusten esittäminen. Tutkielmassa tehdään lainopillisen tulkintasuositusten

[11] Määttä 2012, s. 17–18.
[12] Määttä 2012, s. 23.
[13] Lohse 2012, s. 68.
[14] Minkkinen 2017, s. 915.

lisäksi havaintoja lainsäädännön puutteista ja aukoista sekä esitetään lainsäädännön konkreettisia kehittämistarpeita.[15]

1.4 Tutkielman rakenne

Tutkimuskysymyksiä lähestytään osakysymysten kautta, joiden avulla saavutetaan varsinaiset tutkimuskysymykset. Tutkielman aluksi käydään läpi tutkimuksen kannalta keskeisiä käsitteitä, jotka määrittävät tutkittavaa aihetta ja lisäksi muodostavat tärkeää pohjaa tutkimukselle. Tämän jälkeen syvennytään tarkemmin kyberterrorismin määritelmään, joka on tutkimuksen kannalta keskeisin käsite. Tarkoituksena on selvittää mitä tarkoitetaan, kun puhutaan kyberterrorismista. Määritelmien eri teorioiden lisäksi tarkastellaan kyberterrorismin ja kybersodan välistä rajapintaa, joka on keskeistä aiheen moniulotteisuuden hahmottamisen ja rajanvedon kannalta.

Neljännessä luvussa tarkastellaan terrorismirikosten kansallisen lainsäädännön taustaa, tämänhetkistä sääntelyä ja tunnusmerkistöjä kyberterrorismin osalta. Tämän jälkeen tarkastellaan laajemmin lainsäädännön sovellettavuutta kyberterrorismiin, joka on yksi tämän tutkielman tutkimuskysymyksistä. Rikoslain 34 a luvun sovellettavuuden arviointia tehdään kyberhyökkäyksiä ja kybervaikuttamista koskevien rikosten osalta, jotka voidaan nähdä yleisimpinä kybertoiminnan muotoina. Lisäksi rikoslain 34 a luvun sovellettavuuden arviointi laajennetaan koskemaan värväystä (RL 34a:4c) ja julkista kehottamista (RL 34a:5e) kyberterrorismirikoksissa. Säännökset valikoituivat tarkastelun kohteeksi siitä syystä, että Venäjän ja Ukrainan välisen sodan myötä kyseisiin säännöksiin liittyvää kybertoimintaa on nähty kyberhyökkäysten, vaikuttamiskeinojen, erilaisten värväysten ja julkisten kehottamisten osalta. Luvun 5 tarkoituksena ei ole tehdä sovellettavuuden arviointia kaikkiin kyberterrorismia koskeviin säännöksiin, vaan tarkastella tilannetta valittujen tekojen kautta.

[15] Määttä 2012, s. 18.

Luvussa 6 syvennytään kansallisen lainsäädännön kattavuuden arviointiin, joka on toinen tämän tutkielman tutkimuskysymyksistä. Tarkoituksena on selvittää, kuinka kattavalla tasolla kyberterrorismiin liittyvä sääntely on tällä hetkellä ja havaitaanko siinä lainsäädännöllisiä puutteita. Lainsäädännön kattavuuden arviointiin on tuotu tarkasteltavaksi kyberterrorismin kannalta oleellista muuta lainsäädäntöä. Tutkielman lopussa esitetään olennaisilta osin tiivistetysti tämän tutkielman johtopäätökset.

2 KESKEISET KÄSITTEET

2.1 Kyberturvallisuus

Nyky-yhteiskunnassa tietoteknologiasta on tullut erottamaton osa arkipäivää. Yhteiskunnan tärkeät toiminnot ja maailmantalous ovat riippuvaisia bittien toimivuudesta. Digitaalinen rajaton maailma tarjoaa mahdollisuuksia ajallisesti ja rajattomasti. Näillä mahdollisuuksilla on kuitenkin olemassa kääntöpuolensa, jolla tarkoitetaan sitä, että yhteiskuntien haavoittuvuus lisääntyy. Kyberturvallisuus koskettaa lähtökohtaisesti kaikkia yhteiskuntia ja yksilöitä. Yleisimmät ongelmat kyberturvallisuudessa liittyvät siihen, että yksilötasolla kyberturvallisuuden katsotaan kuuluvan vain alan asiantuntijoille eikä tavallisille kansalaisille. Käytännössä kuitenkin yksittäinen internetin tai älypuhelimen käyttäjä taistelee kyberturvallisuuden eturintamassa. Kyberturvallisuus on myös strateginen ja poliittinen asia, jossa uhkat ovat todellisia ja vaikutuksiltaan vakavia. Hinta välinpitämättömyydestä voi nousta korkeaksi.[16]

Sanalla kyber (kreik. kybereo) tarkoitetaan digitaalista maailmaa eli bittien maailmaa, joka ympärillämme vallitsee. Käsitteenä se usein rinnastuu kybertoimintaympäristöön tai kybermaailmaan, mutta harvoin sitä kuitenkaan käytetään yksittäisenä sanana. Sana kyber toimiikin kuvaavana yhdyssanan etuliitteenä, joka saa varsinaisen merkityksensä, kun sanaan liitetään tarvittava loppuosa esim. kyberrikollisuus, kyberhyökkäys, kyberterrorismi tai kyberturvallisuus.[17]

Kyberturvallisuus on terminä vielä suhteellisen uusi ja sisällöltään vakiintumaton. Käytännössä sillä yleensä tarkoitetaan organisaatioiden ja yhteiskunnan digitalisoitumisen aiheuttamia uudenlaisia turvallisuushaasteita. Kyberturvallisuudella voidaan tarkoittaa myös suojaustoimenpiteitä, joilla turvataan mm. tietoliikenneyhteydet kyberuhkilta.[18] Kyberuhkia on olemassa monen-

[16] Limnell – Majewski – Salminen 2014, s. 13–15.
[17] Limnell – Majewski – Salminen ym. 2014, s. 29.
[18] Traficom 2020, s. 4.

laisia, joilla pyritään vaikuttamaan organisaatioiden tai valtioiden toimintaan, talouteen tai hallussa oleviin tietoihin. Kyberuhkia ovat mm. tietojenkalastelut, haittaohjelmat ja palvelunestohyökkäykset.[19]

Kyberturvallisuudella tarkoitetaan tietoturvan ulottamista yhteiskunnan peruspalveluihin kuten energiahuoltoon (mm. sähkön ja veden jakelu), yleiseen terveydenhuoltoon, maanpuolustukseen ja tietoliikenneyhteyksien toimimiseen. Huomioitavaa on tehdä ero termien välillä, sillä termejä kyberturvallisuus ja tietoturvallisuus käytetään usein sekaisin. Tietoturvallisuudella tarkoitetaan myös datan suojaamista ja tietojärjestelmien toiminnan varmistamista. Tietoturvalla pyritään yksittäisten koneiden suojaamiseen.[20] Termeillä on siten eroavaisuutta kyberturvallisuuden kanssa, sillä kyberturvallisuudella tarkoitetaan tietoturvan ulottamista laaja-alaisesti yhteiskunnan toimintoihin.

Tarkasteltaessa kybermaailman ajankohtaisuutta ja sen merkittävyyttä, voidaan havaita neljä tekijää. Ensinnäkin yhteiskunta ja yritykset ovat entistä riippuvaisempia digitaalisesta maailmasta, ja bittien toimimattomuus voi hidastaa tai pahimmillaan lamauttaa toimintoja. Toisekseen valtiot ovat yhä voimakkaammin kytköksissä kybermaailmaan, johon on suhtauduttu yhtenä strategisena sodankäynnin ulottuvuutena ja jota voidaan hyödyntää laajempien strategisten päämäärien tavoittelussa. Valtiot ovat strategisessa kyberturvallisuudessa tärkeimpiä ja isoimpia tekijöitä ja uskottavuuden takia valtioiden edellytetään olevan vahvoja toimijoita. Monien maiden asevoimissa puhutaankin kybermaailmasta sodankäynnin viidentenä ulottuvuutena maan, meren, ilman ja avaruuden ohella. Kolmantena kohtana voidaan havaita kybermaailmassa käynnissä oleva kiihtyvä kamppailu kyberpuolustuksen ja -hyökkäyksen välillä. Kybermaailmassa pyritään jatkuvasti kehittämään tehokkaampia puolustusmekanismeja, mutta samaan aikaan kyberrikolliset pyrkivät löytämään haavoittuvuuksia ja aukkoja puolustuksessa. Neljäntenä tekijänä nähdään kybermaailman kustannustehokkuus (vrt. fyysiset aseet) ja matala kiinnijäämisen riski.[21]

---

[19] Traficom 2020, s. 4.
[20] Järvinen 2018, s. 14.
[21] Limnell – Majewski – Salminen ym. 2014, s. 20–23.

Kyberturvallisuudesta on tullut yksi näkyvä poliittinen väline, ja valtiot ovat kiinnostuneita kybermaailman strategisista mahdollisuuksista. Monissa maissa kyberturvallisuus on puolustuspolitiikan kulmakivi ja yksi sodankäynnin ulottuvuuksista. Vuonna 2013 Yhdysvallat ilmoitti, että heidän suurimmiksi kansallista turvallisuutta uhkaaviksi tekijöiksi terrorismin sijasta ovat nousseet kyberuhkat.[22] Huomioitavaa kyberturvallisuuden osalta on, että valtio saattaa myös muodostua uhkaksi kansalaisten kyberturvallisuudelle liiallisen tiedonkeruun ja valvonnan myötä.[23]

Kyberturvallisuudelle tärkeänä asiana nähdäänkin luottamuksen vahvistaminen ja sen rakentaminen yhteiskunnassa. Kyberturvallisuudella pyritään siihen, että sen toimivuuteen voidaan luottaa tai muutoin se lisää haavoittuvuuden riskiä.[24] Turvallisuus on yksi perustarpeista, joka valtion on turvattava. Lainsäädännön kyberrikosten osalta on oltava kattava, oikeusjärjestelmän kyberrikollisuuden torjumiseksi on oltava toimiva ja valtioiden välillä tulee olla kansainvälistä yhteistyötä. Yhteiskunnassa on oltava riittävää osaamista kyberturvallisuudesta ja yhteiskunnallisen toimintaympäristön ja -kulttuurin on tuettava teknologiaosaamista. Lisäksi on oltava toimiva ja tunnustettu koulutusjärjestelmä, joka kykenee tuottamaan osaavaa työvoimaa. Varautumissuunnitelmien on oltava kansallisen kriittisen infrastruktuurin osalta hyvällä tasolla ja kansallisen kyberrikollisuuden vähäistä.[25] Edellä kuvattujen tekijöiden voidaan katsoa lisäävän ennakoitavuutta kyberrikollisuuden torjumiseksi.

Yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisempiä tehtäviä. Suomi on laatinut oman kyberturvallisuusstrategian, jossa asetetaan keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi. Digitaalisen toimintaympäristön kehitys ja siellä tapahtuvat merkittävät muutokset lisäävät kyberturvallisuusstrategian päivittämistarvetta.[26] Uusin kyberturvallisuusstrategia on laadittu vuonna 2019.

---

[22] Jansson – Sihvonen 2018, s. 6.
[23] Limnell – Majewski – Salminen 2014, s. 60.
[24] Limnell – Majewski – Salminen 2014, s. 40–41.
[25] Limnell – Majewski – Salminen 2014, s. 61–62.
[26] Suomen kyberturvallisuusstrategia 2019, s. 4.

Kansainvälinen yhteistyö on Suomen kyberturvallisuudelle ensiarvoisen tärkeää. Yhteistyö koskee teknisen ja poliittisen tason yhteistyötä. Kansainvälinen oikeus, kansainväliset sopimukset ja ihmisoikeussopimukset ovat yhteistyön perusta myös kybertoimintaympäristössä. Euroopan unionin päätökset ja yhteistyö EU:ssa muodostavat Suomen kansalliselle kyberturvallisuuspolitiikalle ja sen kehittämiselle selkärangan. EU:n keskeiset lainsäädäntöhankkeet mm. EU:n verkko- ja tietoturvadirektiivi (NIS) ja EU:n kyberturvallisuusstrategia vaikuttavat kansallisella tasolla kyberturvallisuuden kehittämiseen. Lisäksi Suomi vaikuttaa EU:ssa ja keskeisissä kansainvälisissä järjestöissä (YK, ECD, ETYJ, EN ja Nato) aktiivisesti kyberturvallisuusagendaan.[27]

2.2 Kybertoimintaympäristö

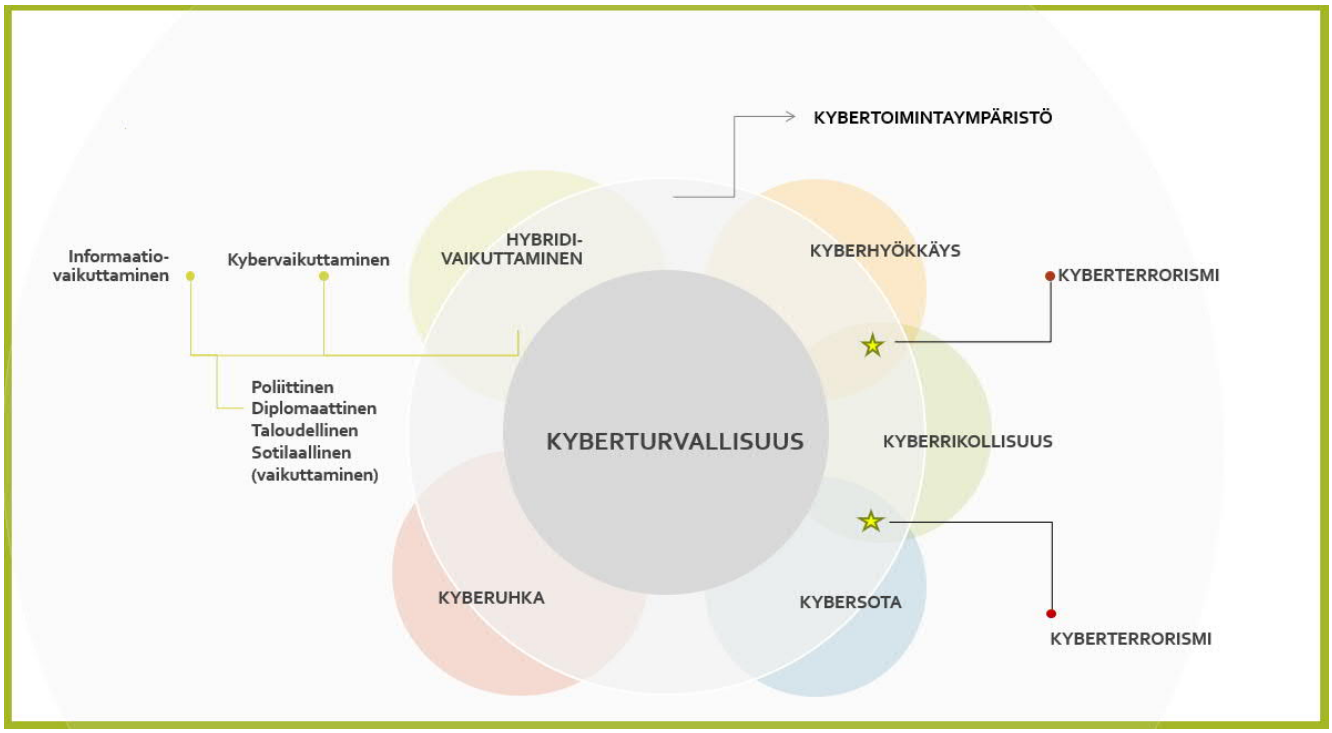
Kybertoimintaympäristö on yksi keskeisimpiä käsitteitä, jonka ymmärtäminen mahdollistaa kyberturvallisuuteen liittyvän kokonaisuuden hahmottamisen. Kybertoimintaympäristö on keskeinen myös siinä mielessä, että se luo kyberterrorismille laaja-alaiset mahdollisuudet. Kybertoimintaympäristöllä tarkoitetaan useita toisiinsa yhdistyneitä tietoverkkoja, joissa tietoa siirtyy maailmanlaajuisesti digitaalisessa muodossa käyttäjältä tai laitteelta toiselle. Tietoa siirtyy tietoliikennetekniikasta, tietokoneista, datasäiliöistä, reitittimistä ja palvelimista. Ihminen on yksi olennainen osa kybertoimintaympäristöä vastaamalla verkon ylläpidosta ja sen toimintaedellytyksistä.[28]

Turvallisuuskomitean laatiman kyberturvallisuuden sanaston mukaan kybertoimintaympäristön määritelmä on seuraava: ”yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö. Kybertoimintaympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet.” Esimerkkeinä kybertoimintaympäristöstä on mainittu tietojärjestelmiin perustuvat

[27] Suomen kyberturvallisuusstrategia 2019, s. 5.
[28] Jansson – Sihvonen 2018, s. 2.

ydinvoimalan ohjausjärjestelmät, elintarvikkeiden kuljetus- ja logistiikkajärjestelmät, liikenteen ohjausjärjestelmät sekä pankki- ja maksujärjestelmät.[29]

Kyberturvallisuuden työelämäprofessori **Jarno Limnéll** puolestaan määrittelee kybertoimintaympäristön ”kattavan kaikki palvelut, toiminnot ja muut asiat, jotka tapahtuvat bittien maailmassa”.[30] Kybertoimintaympäristö koostuu laajasta ja moninaisesta kokonaisuudesta, jonka ymmärtäminen on toisinaan haasteellista. Alla on esitettynä kuvio, joka kuvaa kybertoimintaympäristöä ja siinä ilmeneviä toimintoja. Kuvio kuvaa kyberhyökkäyksen, kyberrikollisuuden ja kybersodan välistä suhdetta kyberterrorismiin. Kybertoimintaympäristö voidaan nähdä olevan kaiken kybertoiminnan mahdollistaja ja siten muut toiminnot ovat tämän ympärillä. Kyberturvallisuus on sijoitettu kuvion keskelle esittämään turvallisuuden ydintä, jonka reunoilla tapahtuu rikollista toimintaa.



Kuvio 1. Kybermaailma kiteytettynä

[29] Turvallisuuskomitea 2018, s. 22.
[30] Limnéll – Majewski – Salminen 2014, s. 240.

Kybertoimintaympäristön fyysisiä ulottuvuuksia on myös pohdittu ja osa tutkijoista on tullut siihen tulokseen, ettei kybertoimintaympäristö ole maantieteellisesti tai millään muullakaan määritelmällä rajaton. Valtiot hallinnoivat toimintaympäristöä maiden rajojen sisäpuolella ja ei-valtiolliset organisaatiot taas jotakin muuta globaalin verkon osa-aluetta. Kybertoimintaympäristöä määrittää myös jatkuva muutos ja laajeneminen. Aiemmin se nähtiin pelkkänä tiedonsiirron välineenä ja nykyään kaikki valtioiden kriittisimmät infrastruktuurit (sähkö- ja vesilaitokset, liikenteenohjaus) toimivat kybermaailmassa.[31]

Toisaalta taas kybertoimintaympäristö voidaan nähdä globaalina rajattomana järjestelmänä, joka kasvaa ja kehittyy koko ajan. Se muodostuu valtiollisesta ja yksityisestä informaatiostruktuurista, keskenään vuorovaikuttavista organisaatioista, yksilöistä, prosesseista ja teknologioista sekä niistä ympäristöistä ja olosuhteista, jotka vaikuttavat kyberturvallisuuteen.[32]

Kybertoimintaympäristö on kehittynyt huimasti viime vuosikymmenten aikana ja kuuluisimmat kyberhyökkäykset ja haittaohjelmat sijoittuvatkin viimeisen vuosikymmenen ajalle. Kybertoimintaympäristöön ja -turvallisuuteen liittyy internet, joka on konkreettinen väline ja keino toimenpiteille. Internetin kautta kybertoimintaympäristö tulee olemassa olevaksi. Kyberturvallisuuden ylläpitämisessä valtiolla on merkittävä rooli. Suomessa tehtävää hoitaa Viestintävirasto, Kyberturvallisuuskeskus ja kriittisen tietoverkkoinfrastruktuurin osalta Suomen Erillisverkot Oy.[33] Kybertoimintaympäristö on jatkuvasti alttiina viruksille, haittaohjelmille, identiteettivarkauksille, luonnonkatastrofeille, fyysisen maailman ongelmille (mm. sähkökatkokset), kyberrikollisten hyökkäyksille ja vakoilulle.[34]

Valtiot harjoittavat tiedustelutoimintaa, kybervakoilua ja toteuttavat vastaiskuja kyberhyökkäyksiin.[35] Valtio on kybertoimintaympäristön olennaisin osa, sillä sen tulee pystyä suojaamaan oma

[31] Jansson – Sihvonen 2018, s. 5.
[32] Limnell – Majewski – Salminen 2014, s. 74.
[33] Jansson – Sihvonen 2018, s. 7.
[34] Jansson – Sihvonen 2018, s. 9.
[35] Jansson – Sihvonen 2018, s. 10.

digitaalinen infrastruktuurinsa, yhteiskunnan elintärkeät tehtävät ja kansalaisten tarvitsemat elämisen palvelut. Valtio on myös vastuussa kokonaisturvallisuudesta ja laeista (mm. yksityisyyden suoja), joilla kybertoimintaympäristöä säädellään. Huomattavaa on, että kybermaailmasta puuttuvat kansainväliset standardit, joiden puitteissa kyberturvallisuutta toteutetaan. Lisäksi maakohtaiset lainsäädännöt poikkeavat toisistaan, joka osaltaan luo haasteita kansainvälisessä yhteistyössä. Kybertoimintaympäristölle on ehdotettu oman kansainvälisen lain luomista yhtenäistämisen sijaan.[36]

Kybermaailmassa monet lainalaisuudet ovat erilaisia suhteessa fyysiseen maailmaan. Välttämätöntä on ymmärtää bittien tuomat lainalaisuudet, jotta pystytään torjumaan uhkia sekä hyödyntämään tehokkaasti kybermaailman mahdollisuuksia. Kybertoimintaympäristön muuttuvista lainalaisuuksista on mahdollista muodostaa kaava nimeltään ”ATTAT”. Tällä tarkoitetaan aikaa, tilaa, tunnistamattomuutta, asymmetrisyyttä ja tehokkuutta.[37]

Kybermaailmassa ajalla (A) on erilainen merkitys verrattuna fyysiseen maailmaan. Asiat voivat bittien maailmassa tapahtua välittömästi ja yhtäkkiä. Aika menettää merkityksensä, sillä ei ole väliä toteutetaanko hyökkäys viereisestä rakennuksesta vai toiselta puolelta maapalloa, toiminta on välitön. Toisaalta taas bittien maailmassa aika pitenee, sillä välittömästi toteutettaviin hyökkäyksiin tarvitaankin pitkäaikaista valmistelua.[38]

Aika ja tila ovat tiiviissä yhteydessä toisiinsa. Tilalla (T) tarkoitetaan rajattomuutta, etäisyyksien häviämistä, jonka seurauksena tila itsessään häviää. Asioiden toteuttamiseksi ei tarvitse olla fyysisesti erillisessä tilassa vaan digitaalisessa maailmassa esim. kyberhyökkäys voidaan toteuttaa maantieteellisesti mistä tahansa ja se voidaan kohdistaa mihin tahansa.[39]

---

[36] Jansson – Sihvonen 2018, s. 14.
[37] Limnell – Majewski – Salminen 2014, s. 63.
[38] Limnell – Majewski – Salminen 2014, s. 63–64.
[39] Limnell – Majewski – Salminen 2014, s. 65–66.

Kybermaailmassa tunnistamattomuus (T) on avainasemassa ja toimijan tunnistaminen onkin haasteellista lukemattomien identiteettien ansiosta. Kiinnijäämisen riski täten pienenee, joka houkuttaa toimijoita rikolliseen toimintaan. Toimijan osoite on mahdollista selvittää, mutta haasteeksi osoittautuu yhteyden todellisen käyttäjän määrittäminen. Toimija pyrkii pysymään tunnistamattomana aina silloin, kun se edistää käyttäjän tavoitteita. Ainoa varma keino tunnistaa toimija onkin toimijan oma ilmoittautuminen.[40]

Asymmetrisyydellä (A) tarkoitetaan toimijoiden suhteellisen voiman ja strategian sekä taktiikan poikkeamista toisistaan merkittävästi. Sillä tarkoitetaan esim. välinettä tai toimintoa, jota voimasuhteiltaan merkittävästi heikompi käyttää suhteessa vahvempaan. Esimerkkinä voidaan mainita al-Qaidan toteuttama hyökkäys Yhdysvaltoihin (9/11), joissa aseina käytettiin kaapattuja lentokoneita. Kybermaailmassa kyberhyökkäyksiä on mahdollista toteuttaa rajattomasti ilman, että se vähentäisi hyökkääjän resursseja. Täten fyysisen maailman perusperiaate ”hyökkääjällä oltava kolminkertainen ylivoima suhteessa puolustajaan” ei päde. Bittien maailmassa puhutaan onnistuneesta hyökkäyksestä, jos yksi miljoonasta tunkeutumisyrityksestä onnistuu. Tämä asymmetrinen luonne tekee monimutkaiseksi, ellei miltei mahdottomaksi voiton, häviön ja vahingon arvioimisen.[41]

Viimeisenä kaavan osana on tehokkuus (T). Tehokkuuden mittarina toimii hyökkääjän kyky tehdä montaa asiaa samaan aikaan, toistensa yhteydessä, eri ulottuvuuksilla ja nopeasti. Kybermaailma mahdollistaa kybertoimintaympäristön käytön samanaikaisesti moneen eri tarkoitukseen esimerkiksi propagandaan, vakoiluun ja kriittisen infrastruktuurin vahingoittamiseen tai suojaamiseen. Tehokkuus on yksi kybermaailman vaikuttavimpia lainalaisuuksia.[42]

---

[40] Limnell – Majewski – Salminen 2014, s. 67.
[41] Limnell – Majewski – Salminen 2014, s. 68–69.
[42] Limnell – Majewski – Salminen 2014, s. 69–70.

2.3 Kyberhyökkäys

Maailma on mitä enenevissä määrin riippuvainen erilaisista tietoverkoista ja niiden informaatioista. Tietoverkkojen laajeneminen on luonut maailman, joka ylittää perinteiset valtiorajat ja niiden merkitys ihmisten toiminnassa on vähentynyt. Rajaton ja verkostoitunut maailma on avannut laajemman toimintakentän rikollisuudelle ja sodankäynnille.[43] Tilanne tietoteknisesti merkittävästi muuttuvasta maailmasta luo juridisesti paljon haasteita, sillä lainsäädännön tulisi olla jatkuvasti ajan tasalla tai jopa yhden askeleen edellä. Rajat ylittävä tietoverkkojen kautta tapahtuva rikollisuus tai sodankäynti vaatii kansainvälistä yhteistyötä lainsäädännöllisesti. Kyberuhkille on tyypillistä rajattomuus, kyberhyökkäysten toteuttajien vaihtuvuus ja haasteellinen tunnistettavuus[44]. Venäjän ja Ukrainan välisestä sodasta vuonna 2022 huomataan, että erilaiset kyberhyökkäykset ja -vaikuttamiset ovat mahdollisia tiettyyn valtioon myös muista valtioista ja yksityisten tahojen toimesta. Tällaista kybertoimintaa ovat harjoittaneet erilaiset hakkeri- ja aktivistiryhmät, joista yksi on nimeltään Anonymous-liike[45]. Kyseinen liike on ilmoituksiensa mukaan toteuttanut monia kyberhyökkäyksiä Venäjää vastaan ja keinoina on pääsääntöisesti käytetty palvelunestohyökkäyksiä[46].

Valtioiden osuus kyberhyökkäyksissä on suuri ja niitä voidaan toteuttaa suoraan tai epäsuorasti. Kyberhyökkäykset ovat liittyneet tiedustelutoimintaan, poliittiseen painostamiseen tai propagandan jakamiseen. Esimerkiksi vaalituloksiin tai kohdemaan sisäisiin asioihin, kuten sisäpolitiikkaan ja demokraattisen yhteiskuntajärjestelmän uskottavuuteen, on yritetty vaikuttaa. Uutisia on manipuloitu, julkisia palveluita on lamautettu kyberhyökkäyksin ja yhteiskunnan elintärkeisiin toimintoihin sekä kriittiseen infrastruktuuriin on kohdistettu hyökkäyksiä. Etenkin telealan ja energiasektorin yritykset, teollisuusyritykset ja julkinen sektori ovat joutuneet hyökkäysten kohteeksi.[47]

---

[43] Sirjonen 2018, s. 188.
[44] Suomen kyberturvallisuusstrategia .2013, s. 33.
[45] Limnell – Majewski – Salminen 2014, s. 233.
[46] Yle Uutiset 28.2.2022. Hakkeriryhmä Anonymous julisti kybersodan Venäjää vastaan – väittää kaataneensa useita Venäjän hallinnon sivustoja. [https://yle.fi/uutiset/3-12336205]
[47] Ferm 2018, s. 404.

Suomen turvallisuusstrategiassa tai sen taustamuistioissa ei ole erikseen määritelty kyberhyökkäystä. Turvallisuuskomitean kyberturvallisuuden laatimassa sanastossa tietoverkkohyökkäyksellä, verkkohyökkäyksellä ja kyberhyökkäyksellä tarkoitetaan seuraavaa: ”tietoverkon kautta tapahtuva teko tai toiminta, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön. Tietoverkkohyökkäys voidaan tehdä esim. palvelunestohyökkäyksenä tai haittaohjelman avulla. Termi kyberhyökkäys viittaa tietoverkkohyökkäystä laajempaan käsitteeseen, sillä kyberhyökkäys voidaan tehdä myös muilla tavoin kuin tietoverkon kautta.”[48]

Nato (North Atlantic Treaty Organization, Pohjois-Atlantin puolustusliitto) puolestaan määrittelee kyberhyökkäyksen verkossa tapahtuvaksi hyökkääväksi tai puolustavaksi toiminnaksi, joka oletettavasti johtaa omaisuuden vahingoittumiseen tai tuhoutumiseen tai ihmishenkien tai terveyden menetykseen.[49] Tutkijoiden mukaan kyberhyökkäys voidaan määrittää myös olevan bittien kautta toteutettava hyökkäys, jolla voidaan tuottaa haittaa, vahinkoa tai tuhoa niin fyysiseen kuin tietoverkkomaailmaankin. Tarkoituksena voi olla myös tiedon varastaminen, laitteiden tai järjestelmien käytön estäminen.[50] Euroopan unionin neuvoston päätöksen 1 artiklassa todetaan kyberhyökkäyksien olevan toimia, joihin liittyy pääsy tietojärjestelmiin, tietojärjestelmien häirintä, tietojen vahingoittaminen tai niiden sieppaus. Lisäksi kyberhyökkäyksien todetaan olevan kaikkia niitä toimia, joihin ei ole järjestelmän tai muun oikeudenhaltijan asianmukaista lupaa tai, jotka eivät ole sallittuja Euroopan unionin oikeuden tai jäsenvaltion lainsäädännön nojalla.[51]

Euroopan unionin neuvoston päätöksen artiklan 1 mukaan kyberhyökkäykset voivat kohdistua elintärkeään infrastruktuuriin, johon kuuluu myös vedenalaiset kaapelit ja ulkoavaruuteen lähetetyt esineet, jotka ylläpitävät yhteiskunnan välttämättömiä toimintoja, terveydenhuoltoa, turvallisuutta, turvatoimia, väestön taloudellista ja sosiaalista hyvinvointia. Tällaisia toimintoja on ener-

[48] Turvallisuuskomitea 2018, s. 31.
[49] Sirjonen 2018, s. 192.
[50] Limnéll – Majewski – Salminen 2014, s. 240.
[51] Euroopan unionin neuvosto, Neuvoston päätös 7299/19 s. 8.

gia (sähkö, öljy, kaasu), liikenne (lento-, rautatie-, vesi- ja tieliikenne), pankkitoiminta, terveydenhuolto, juomaveden toimittaminen ja jakelu, digitaalinen infrastruktuuri ja muu valtiolle elintärkeä ala. Valtioiden elintärkeitä tehtäviä on erityisesti seuraavilla aloilla: puolustus, instituutioiden hallinto ja toiminta (sisältäen vaalien järjestämisen tai äänestysmenettelyn), talous- ja siviili-infrastruktuurin toiminta sekä sisäisen turvallisuuden ja ulkosuhteet kuten diplomaattiedustustot. Hyökkäys voidaan kohdistaa turvallisuusluokiteltujen tietojen säilyttämiseen ja käsittelyyn tai valtionhallinnon kriisiryhmiin.[52]

Kyberhyökkäysten tekniikat ovat moninaisia ja jatkuvasti muuntuvia sekä kehittyviä. Valtioiden on mahdollista käyttää välillistä toimijaa verkossa ja kyberhyökkäyksissä. Välillisellä toimijalla tarkoitetaan ei-valtiollisia toimijoita toteuttamaan kyberhyökkäyksiä. Välillisen toimijan käytöllä mahdollistetaan valtion anonymiteetti, jolloin toiminta saadaan näyttämään kyberterrorismilta tai kyberrikollisuudelta, mutta tosiasiassa valtio voi kuitenkin olla hyökkäyksen toimija. Verkossa toteutettavat hyökkäykset ovat todellisia ja hyvin potentiaalisia valtioiden hyödyntämiä terrorismin välineitä.[53]

Suomi ja Eurooppa kaipaavat vielä yhtenäistä poliittista mallia, miten kyberhyökkäyksiin ja kybervaikuttamisiin vastattaisiin. Iso-Britannia on valmis vastaamaan kyberhyökkäyksiin kovalla sotilaallisella voimalla kuten ilmaiskuilla. Nato on myös todennut, että kyberhyökkäys voisi johtaa viidennen artiklan aktivointiin. Tällainen teko voisi olla esimerkiksi kyberhyökkäys sairaalaympäristöön, joka johtaisi ihmishenkien menetykseen.[54]

2.4 Kybervaikuttaminen

Kyberhyökkäykset tulevat olemaan keskeisessä roolissa tulevissa vaikutustavoissa ja sodankäynneissä. Tätä kehitystä vauhdittaa digitalisaation vahvistuminen ja riippuvuuden kasvaminen. Vaikuttamisella pyritään pysymään sodan julistamisen kynnyksen alapuolella ja valtiot testaavatkin

[52] Euroopan unionin neuvosto, Neuvoston päätös 7299/19 s. 8.
[53] Sirjonen 2018, s. 201.
[54] Limnèll – Iloliemi 2018, s. 171.

yhä rohkeammin kybertaistelukentän poliittisia rajoja uusilla vaikuttamisen keinoilla. Vastatoimet ovat tähän mennessä osoittautuneet hyvin vaatimattomiksi, ellei jopa olemattomiksi. Tämä johtaa jatkossa yhä aggressiivisempaan ja vaikuttavampaan kybervaikuttamiseen. Esimerkiksi Ranskan poliittinen johto ilmoitti vastaavansa presidentinvaaleihin kohdistuneeseen vaikuttamiseen, mutta julkisesti vastatoimia ei ole nähty.[55]

Kybervaikuttaminen liittyy yhtenä osana hybridivaikuttamista. Hybridivaikuttamisella ei ole olemassa vakiintunutta määritelmää, mutta yleensä sillä tarkoitetaan valtiollisen tai muun ulkoisen toimijan pyrkimystä vaikuttamaa kohteen haavoittuvuuksiin samanaikaisesti tai jatkumona, suunnitelmallisesti ja eri keinoja käyttäen. Toimija pyrkii tavoitteisiinsa hyödyntämällä hybridivaikuttamisen laajaa keinovalikoimaa. Keinoja voivat olla mm. poliittiset, diplomaattiset, taloudelliset ja sotilaalliset toimet sekä informaatio- ja kybervaikuttaminen. Vaikuttaminen voi olla erittäin vahingollista ja siinä usein käytetyt kolmannet toimijat mahdollistavat tekojen kiistettävyyden. Vaikuttaminen voi olla hyvin laaja-alaista, suunnitelmallista ja pitkäkestoista. Vaikuttamisessa hyödynnetään yhteiskunnan haavoittuvuuksia jo normaalioloissa, joten sitä voi olla vaikeaa tunnistaa.[56]

Kybertoimintaympäristö tarjoaa laaja-alaisen soveltuvuuden hybridivaikuttamiselle. Ensinnäkin tekijää on vaikea tunnistaa, poliittiset riskit kybervaikuttamisen vastatoimista näyttäytyvät pieninä, kansainvälisen lainsäädännön osalta kyberasiat ovat harmaata aluetta, lisääntyvä valtioiden kyberoperaatioiden ulkoistaminen ei-valtiollisille toimijoille sekä ei-kineettisten kohteiden merkityksen ja vaikuttavuuden kasvu.[57]

Kybervaikuttaminen on osittain käsitteenä ja toiminnoiltaan vielä jäsentymätön, mutta tiivistetysti voidaan todeta sen tarkoittavan digitaalisen toimintaympäristön käyttämistä hyväksi eri motiivein ja tarkoitusperin.[58] Käytännössä voidaan yksinkertaisimmallaan puhua vaikuttamisesta,

---

[55] Limnèll – Iloniemi 2018, s. 169–170.
[56] Sisäministeriön julkaisuja 2022:20, s. 10.
[57] Limnèll – Iloniemi 2018, s. 169–170.
[58] Limnèll – Iloniemi 2018, s. 169.

jota toteutetaan verkon välityksellä. Internetin kehitys on mahdollistanut uuden strategisen välineen terrorismille, jolloin terroristiset ryhmittyvät voivan ilman hallinnon sensuuria tai joukkotiedotusvälineitä tuoda viestinsä suoraan julkisuuteen. Näin terroristeilla on mahdollisuus tuoda ideologiansa ja tavoitteensa näkyville. Tällaisen toiminnan vaikutusta yhteiskuntaan on mahdotonta arvioida.[59]

Jäsentymättömästä käsitteestä johtuen kybervaikuttamisen kenttä on laaja ja havaintoja kybervaikuttamisen keinoista sekä uhkakuvista tuleekin etsiä useista eri kanavista. Suomen suojelupoliisi (Supo) on kansallisturvallisuuden katsauksessa ilmoittanut tämänhetkiseksi kyberuhkaksi mm. kybervaikuttamisen. Supossa tällaisella kybervaikuttamisella tarkoitetaan taloudellisesti motivoitunutta kiristysrikollisuutta, jolla voidaan vaarantaa Suomen kansallista turvallisuutta.[60]

Kiristyshaittaohjelmia käytetään digitaalisen vaikuttamisen keinoina ja yhtenä kohteena voidaan nähdä terveydenhuoltoala. Arvokkaat potilastiedot yhteiskunnan avainhenkilöistä mahdollistavat keinot poliittiselle vaikuttamiselle ja kiristykselle. Viime vuosina sairaaloihin on kohdistettu kiristyshaittaohjelmahyökkäyksiä, joilla voidaan estää pääsy potilastietoihin tai resepteihin. Potilastietojärjestelmät ovat elintärkeitä sairaaloiden toiminnalle, kuten myös lääkintälaitteet, jotka ovat pääsääntöisesti kytkettyinä verkkoon. Turvallisuushaasteet lisääntyvät jatkuvasti ja tiedon sisällöllisestä oikeellisuudesta joudutaan yhtä tarkemmin huolehtimaan, sillä kybervaikuttamisen keinona on esiintynyt myös tietomanipulaatiota. Tämä ilmiö on nostettu yhdeksi keskeisemmäksi turvallisuutta uhkaavaksi tekijäksi, sillä manipulaatiolla pyritään vaikuttamaan yhteiskunnan luottamukseen. Sairaaloissa tällä voitaisiin tarkoittaa tietojärjestelmissä olevien laboratoriotulosten vääristämistä. Toimintatapa manipulaatioon on tehokas ja pitkäkestoinen, jolloin pidemmän ajan kuluessa voidaan saastuttaa myös varmennukset ja varmuuskopiot.[61]

Kiristyshaittaohjelmien käyttäminen on esitetyn perusteella mahdollista toteuttaa kybervaikuttamisen keinona myös muualla kuin terveydenhuollossa. Se voidaan kohdistaa hallinnollisiin tai

---

[59] Limnéll – Majewski – Salminen 2014, s. 133.
[60] Suojelupoliisi, ajankohtaista 3.4.2022. Kyberuhkat. [https://supo.fi/kyberuhkat]
[61] Limnéll – Iloniemi 2018, s. 196–198.

julkisiin laitoksiin, liikennejärjestelmiin, kriittiseen infrastruktuuriin, energiahuoltoon, maanpuolustukseen tai muihin yhteiskunnan tärkeisiin toimintoihin. Tällä voidaan saattaa vaaraan ihmishenkiä, aiheuttaa suuria taloudellisia menetyksiä tai saada aikaan halutunlaista vaikutusta poliittisessa päätöksenteossa. Kiristystä voidaan kohdistaa ja todennäköisesti kohdistettaisiinkin näissä laitoksissa työskenteleviin henkilöihin. Kiristyksessä käytettävänä materiaalina voidaan hyödyntää siten muutakin kuin potilastietoja. Materiaaliksi voitaisiin täten nähdä käyvän minkä tahansa, jolla mahdollistetaan halutun päämäärän saavuttaminen.[62] Tällainen kybervaikuttamisen keino on erittäin vakava ja yhteiskuntaa uhkaava ilmiö, jonka torjumiseksi tulee kohdistaa oikeasuhtaisia keinoja etenkin lainsäädännön keinoin.

Lisäksi yhtenä merkittävänä kasvavana tekijänä digitaalisessa ympäristössä voidaan nähdä internetin algoritmit. Algoritmeilla tarkoitetaan tietokoneohjelmia, jotka pystyvät käsittelemään suuren määrän tietoa. Ihminen jättää yhä enemmän tietoa itsestään digitaalisessa ympäristössä toimiessaan. Algoritmit kokoavat nämä tiedot yhteen, profiloivat sen ja tämän jälkeen tekevät päätöksen siitä, mitä sisältöä ihmisille tarjotaan. Algoritmit ovat sinnikkäitä ja väsymättömiä ohjelmoituja tekijöitä kybermaailmassa, jotka keräävät kaiken digitaalisen tiedon mitä ihmisestä jää.[63]

Algoritmien voidaan nähdä olevan yksi tehokkaimmista kybervaikuttamisen keinoista, joiden avulla ihmismieleen saadaan syötettyä disinformaatiota. Mikäli algoritmi havaitsee henkilön kiinnostuneen esim. salaliittoteorioista, tarjoavat internetin uutissivustot toivotunlaista sisältöä henkilölle. Huomaamattaan henkilö voi alkaa uskomaan tarjottua informaatiota ja häntä on tätä kautta helppo manipuloida. Algoritmeilla voidaan pyrkiä saavuttamaan myös poliittisia tai ideologisia päämääriä. Tästä syystä tulevaisuudessa lähdekriittisyyden merkitys korostuu entisestään, sillä informaatiolla voidaan joko viestittää relevantteja asioita, tai sitten niillä pyritään vaikuttamaan mielipiteeseen. Keskeisimpänä tämänhetkisenä turvallisuuspoliittisena aiheena on Suomen mahdollinen Nato jäsenyys, johon Venäjä pyrkii tekemään vaikuttamista.

---

[62] Limnéll – Iloniemi 2018, s. 196–198.
[63] Limnéll – Iloniemi 2018, s. 194.

Algoritmeja voidaan käyttää myös syväoppimisen työkaluina, joilla voidaan luoda ”deepfake” -kuvia ja videoita. Kyseessä on uudenlainen ilmiö kuva- tai videoväärennöksestä, jossa menneiden tapahtumien materiaalia uusiokäytetään ja hyödynnetään valheellisessa kontekstissa. Tekoälyn avulla tuotettu video saadaan näyttämään aidolta, jossa videolla esiintyvälle henkilölle saadaan muokattua halutunlainen valheellinen sisältö. Menetelmä mahdollistaa vaikuttavan ja uskottavan disinformaation välittämisen ja vaikuttamisen keinon. Esimerkkinä voidaan mainita deepfake video Ukrainan presidentti Volodymyr Zelenskyistä, jossa algoritmeja hyödyntämällä luotiin video käyttäen Zelenskyin ääntä ja kasvoja. Videolla kerrottiin valeuutinen, jossa Ukrainan presidentti Zelenskyin nähdään antavan antautumiskäskyä sotilailleen.[64] Deepfake -videolla pyrittiin mahdollisesti vaikuttamaan sotilaiden taistelumoraaliin ja sodan kulkuun. Voidaan havaita, että käsillä on uudenlaista teknologiaa hyödyntävä kybervaikuttamisen keino. Käytännössä kybermaailmassa tapahtuvalle vaikuttamiselle vain mielikuvitus on rajana. Tietotekniikka kehittyy ja muuntautuu vauhdilla, jonka takia tulevaisuuden kybervaikuttamisen keinoja on erityisen vaikeaa ennustaa.

2.5 Vakavat kyberuhkat

Edellä on esitetty käsitteistöä tutkimusaiheeseen liittyen. Jotta käsillä olevan aiheen vakavuus on mahdollista ymmärtää, on tässä kohdin syytä käydä läpi, millaisia konkreettisia vakavia seurauksia toiminnoilla voidaan aiheuttaa. Teknologian kehityksen myötä, turvallisuuden ja sodankäynnin toimijoiden kyvykkyys ja monipuolisuus kasvaa. Uhkaavina tekijöinä voidaan nähdä niin terroristit, poliittiset ja taloudelliset vakoojat, rikolliset, aktivistit, yksilöt kuin valtiotkin. Arvaamattomasti käyttäytyvät yksilöt saattavat päätyä kansallisesta turvallisuudesta vastaavien viranomaisten tarkkailuun ja seurantaan.[65]

---

[64] Keski-Uusimaa 18.3.2022. Tekoälyllä luodut deepfake -valevideot valjastettiin Ukrainan sodan propaganda-aseeksi – väärennettyä videota presidentti Zelenskyin antautumisesta levitettiin netissä. [https://www.keski-uusimaa.fi/uutissuomalainen/4518773]

[65] Limnéll – Iloniemi 2018, s. 174.

Kyberhyökkäykset voivat viestittää vääränlaista vaikutelmaa myös teon vakavuudesta, sillä ihmishenkiä ei välttämättä menetetä. Hyökkäykset yhteiskunnan kriittiseen infrastruktuuriin voivat kuitenkin aiheuttaa ihmishenkien menetyksiä aineellisten tappioiden ohella.[66] Yhteiskunnan elintärkeinä toimintoina voidaan nähdä talous, puolustuskyky, johtaminen, infrastruktuuri, huoltovarmuus, väestön toimintakyky ja palvelut. Valtiosääntöisesti toiminnot voidaan jakaa intresseihin, joita ovat elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen.[67] Näihin toimintoihin on kyberhyökkäyksellä mahdollista kohdistaa laajamittaista datamanipulaatiota tai valtionhallinnon organisaation ja yhteiskunnan toimivuuden kannalta erilaisia tietovuotoja.[68]

Kyberhyökkäys rahoitusmarkkinainfrastruktuuriin voi lamauttaa maksuliikenteen ja horjuttaa rahoitusmarkkinoiden vakautta. Vakavat häiriötilanteet voivat laajentua talouskriiseiksi, jotka uhkaavat koko kansantaloutta. Valtioiden tai yritysten luottokelpoisuus voi romahtaa, jolloin koko yhteiskunnan toiminta voi joutua kaaokseen.[69] Energiahuoltoon voidaan kohdistaa myös erinäisiä hyökkäyksiä. Energiahuolto on yksi oleellisimmista yhteiskunnan elintärkeistä toiminnoista, jota turvataan eritoten sähkön keskeytyksettömällä saannilla. Suomi on energiataloudessaan vahvasti riippuvainen energian tuonnista, sillä kaksi kolmasosaa energiasta tulee Suomen rajojen ulkopuolelta ja tästä tuontienergiasta kaksi kolmasosaa Venäjältä. Öljy, hiili, kaasu ja ydinpolttoaine ovat täysin tuontitavaraa. Energian suhteen riippuvuus toiseen valtioon voi olla riski, sillä energian saatavuuteen voidaan kohdistaa poliittista vaikuttamista normaaliolojenkin aikana.[70] Tällaisen haavoittuvuuden takia valtioiden ei tulisi olla energiasaannissaan täysin riippuvaisia, vaan energiaa tulisi pystyä tuottamaan mahdollisimman paljon itse. Tällä hetkellä Venäjä uhkaa Eurooppaa kaasuhanojen sulkemisella kostotoimena lännen asettamia pakotteita vastaan[71]. Toimenpide on Eurooppaa vakavasti uhkaava ja tällä Venäjä pyrkii vaikuttamaan Euroopassa tehtäviin päätöksiin.

---

[66] Limnéll – Iloniemi 2018, s. 174.
[67] Lohse – Meriniemi – Honkanen 2019, s. 76.
[68] Limnéll – Iloniemi 2018, s. 174.
[69] Lohse – Meriniemi – Honkanen 2019, s. 75.
[70] Lohse – Meriniemi – Honkanen 2019, s. 75.
[71] Yle uutiset. Putinin kaasupeli. Venäjän kaasuhanojen sulkeminen ajaisi Keski-Euroopan kriisiin. Temppu voisi silti kääntyä itseään vastaan. 13.2.2022. [https://yle.fi/uutiset/3-12307391]

Kyberhyökkäys voi kohdistua myös sähkönjakeluinfrastruktuuriin, eritoten ohjaus- ja valvontajärjestelmiin.[72] Tämä tarkoittaisi mm. vakavia ongelmia asuntojen lämmityksiin, lämpimän veden tuloon sekä muihin elämisen kannalta kriittisiin asioihin. Lisäksi sähköenergian varassa on yhteiskunnan johtamiseen ja väestön varoittamiseen käytettäviä tieto- ja viestintäjärjestelmiä. Kyseisiin sähköpalveluihin voidaan kohdistaa erilaisia hyökkäyksiä, jotka voivat pahimmillaan johtaa kriittisen tietoverkkoinfrastruktuurin tuhoamiseen.[73]

Suomen huoltovarmuus on vahvasti riippuvainen logistiikasta ja kansainvälisistä yhteyksistä, joita toteutetaan merikuljetuksina. Euroopan turvallisuuspoliittinen muutos voisi johtaa logistiseen häiriöön, jolloin se heijastuisi välittömästi Suomen talouteen ja yhteiskuntaan.[74] Lisäksi koko Suomi on riippuvainen tietoverkkojen- ja järjestelmien toiminnasta, joten kyberuhkat muodostavat kokonaisturvallisuuden kannalta hyvinkin merkittävän tekijän. Odottamattomiin vaikutuskeinoihin ja hyökkäyksiin tulee osata varautua. Pelkästään internetin katkeaminen tekee kolmasosan suomalaisista yrityksistä toimintakyvyttömiksi.[75] Käytännössä tällä tarkoitetaan sitä, että monet elintärkeät toiminnot vaarantuisivat kuten kaupassa maksaminen, polttoaineen ostaminen ja käteisen rahan nostaminen.

Yhtenäistä valtioita sitovaa valtiosopimusta, joka kattaisi kaikki kyberuhkatilanteet, ei ole olemassa. Kansainvälisessä oikeudessa kyberuhkatilanteita on käsitelty eri näkökulmista hyvin hajanaisesti. Kansainvälisellä tasolla asiakokonaisuuden oikeudellinen keskustelu on vilkastunut[76] ja voidaan olettaa Venäjän ja Ukrainan välisen sodan vauhdittaneen keskustelua tulevaisuudessa vielä enemmän. Keskusteluilla on tarkoitus luoda oikeudellisia tulkintoja kyberuhkatilanteiden arvioinnissa eri tahoilla valtioiden välillä tai kansainvälisissä yhteisöissä. Todennäköistä on, ettei

[72] Lohse – Meriniemi – Honkanen 2019, s. 75.
[73] Lohse – Meriniemi – Honkanen 2019, s. 75.
[74] Lohse – Meriniemi – Honkanen 2019, s. 75.
[75] Limnéll – Iloniemi 2018, s. 175.
[76] Suomen kyberturvallisuusstrategia .2013, s. 33.

keskusteluilla saavuteta valtioita oikeudellisesti sitovia tulkintoja, vaan ennemminkin tavoitteita joihin järjestelyissä mukana olevat valtiot ovat valmiita yhtymään.[77]

[77] Suomen kyberturvallisuusstrategia 2013, s. 33.

3 KYBERTERRORISMIN MÄÄRITELMÄ

3.1 Terrorismin määritelmä

Terrorismin määritelmä ei ole vielä saavuttanut kansainvälisesti hyväksyttyä yleismaailmallista virallista määritelmää. On esitetty, ettei terrorismi -sanan merkityksestä ole tarkoituksenmukaistakaan löytää yhtä ja oikeaa määritelmää. Tämä ajatus johtuu siitä, ettei viimeisintä totuutta asiassa ole, sillä käsite on sosiaalinen konstruktio. Tämä tarkoittaa sitä, että merkitys syntyy siitä, miten sanaa käytetään ja miten se määritellään. Käsitteiden merkitykset eivät ole yksiselitteisiä ja ne ovat taipuvaisia muovautumaan poliittisten suhdanteiden mukana. Haastetta merkityksen luomiseen tuo myös se, ettei poliittisesti ole aina onnistututtu muodostamaan yksimielisyyttä siitä kuka on terroristi, sillä ensin pitäisi pystyä määrittelemään kuka on vihollinen ja kuka ystävä. Terrorismi sanaa käytetään eri yhteyksissä, eri merkityksissä ja eri tarkoituksissa. Terminä se saattaa herättää poliittista ja moraalista paheksuntaa ja se voi olla myös oikeudellinen käsite sekä akateemisen tutkimuksen kohde.[78]

Joidenkin määritelmien mukaan terrorismi on tarkoitettu aiheuttamaan kauaskantoisia psykologisia vaikutuksia. Terrorismi on suunniteltu luomaan valtaa siellä, missä sitä ei ole tai vahvistamaan valtaa siellä missä sitä on hyvin vähän. Väkivallalla tuotetun julkisuuden avulla terroristit pyrkivät saamaan vaikutusvaltaa poliittisten muutosten aikaansaamiseksi, joko paikallisella tai kansainvälisellä tasolla. Monen tutkijan tekemässä määritelmässä toistuu kuitenkin muutama sama seikka. Ensinnäkin terrorismille selvää on väkivallan käyttö tai sillä uhkailu, uhrit valitaan sattumanvaraisesti, aikomus aiheuttaa laajalti psykologisia vaikutuksia ja tekoa seuraa poliittinen muutos. Määrittelykysymyksessä usein piilee myös umpikuja. Tämä tarkoittaa sitä, että monet maat haluavat tehdä selvän eron terrorismin ja aseellisen taistelun välille, jossa pyritään vastustamaan vierasta miehitystä. Yksinkertaistettuna yhden terroristi on toisen vapaustaistelija.[79]

---

[78] Malkki 2020, s. 18.
[79] Hanhimäki – Blumeneau 2013, s. 4–5.

Ulottuuko terrorismin määritelmä valtioiden toimintaan vai ei? Tämä on kysymys, jonka vastauksesta on pitkään kiistelty. Kolmannet maat ovat sitä mieltä, että valtioiden harjoittama terroritoiminta tulisi sisällyttää kansainvälisen terrorismin määritelmään ja asettaa se huomion keskipisteeksi. Länsimaiden mukaan valtioiden väkivallan käyttöä säännellään jo useilla muilla kansainvälisen oikeuden instrumenteilla, joten tätä ei tulisi sisällyttää kansainvälisen terrorismin määritelmään. YK:n turvallisuusneuvoston terrorismin vastaista toimintaa käsittelevässä päätöslauselmassa 1373 terrorismia ei ole määritelty. Tämä asettaa jäsenmaille erilaisia velvoitteita terrorismin torjunnan suhteen, koska ei välttämättä ymmärretä torjunnan kohdetta. Ilman kansainvälistä määritelmää jokainen valtio voi käyttää terrorismin määritelmää haluamallaan tavalla.[80]

Terrorismin käsite on saanut kansainvälisen oikeuden myötä tapaoikeudellisen sisällön. Tapaoikeuden mukaan terrorismilla tarkoitetaan tekoja, jotka ovat normaalisti kriminalisoituja kansallisessa rikoslainsäädännössä tai tällaisten rikosten avustamisessa rauhan aikana. Näiden tekojen tarkoituksena on aiheuttaa kauhua väestön keskuudessa tai pakottaa valtio tai kansainvälinen yhteisö ryhtymään tietynlaisiin toimiin. Teot ovat poliittisesti ja ideologisesti motivoituneita, eivätkä perustu yksityisten päämäärien tai hyötyjen tavoitteluun.[81]

Euroopan unioni on yksi harvoista kansainvälisistä toimijoista, jotka ovat onnistuneet yksimielisesti saavuttamaan sitovan terrorismin määritelmän. Euroopan parlamentin 13.6.2002 hyväksymä puitepäätös (2002/475/YOS) sisältää terrorismirikosten määritelmän ja siihen liittyvän kriminalisointivelvoitteen, joka on sitä myöden kirjattu myös kansalliseen lainsäädäntöön. Puitepäätöksen 1 artiklan 1 kappaleessa terrorismirikoksen määritelmä on kaksiosainen. Ensinnäkin se koostuu rikosluettelosta rikoksista, jotka tulisi katsoa terrorismirikoksiksi ja toisaalta siinä on yleisen terrorismirikoksen määritelmä. Terrorismirikos määritellään ”rikollisuudeksi, jonka tar-

[80] Malkki 2020, s. 36–37.

[81] Cassese 2008, s. 163. “i) acts normally criminalized under national penal system, or assistance in the commission of such acts whenever they are performed in time of peace; ii) and those acts must be intended to provoke a state of terror in the population or to coerce state or international organization to take some sort of action; iii) and finally are politically or ideologically motivated; that is, are not based on the pursuit of private ends”.

koituksena on pelotella vakavasti väestöä, pakottaa aiheettomasti viranomaiset tai kansainvälinen järjestö johonkin tekoon tai pidättäytymään jostakin teosta taikka horjuttaa vakavasti jonkin maan tai kansainvälisen järjestön poliittisia, perustuslaillisia, taloudellisia tai sosiaalisia perusrakenteita tai tuhota ne."[82] Neuvoston puitepäätöksen (2002/475/YOS) mukaan terrorismirikoksesta on kyse, jos "aiheuttaa hallinnollisille tai julkisille laitoksille, liikennejärjestelmille, infrastruktuureille atk-järjestelmät mukaan luettuina –– suuria tuhoja, jotka voivat saattaa vaaraan ihmishenkiä tai aiheuttaa huomattavia taloudellisia menetyksiä".[83] Puitepäätöksen määritelmässä terrorismi määritellään siis teon tarkoituksen kautta.

Huomioita oikeudellisessa määritelmässä herättää se, että määritelmässä ei ole käsitelty poliittista tai uskonnollista motiivia. Kyseisiä motiiveja on kuitenkin laajasti tunnistettu kansainvälisestikin ja nämä motiivit pääsääntöisesti erottavat terrorismirikoksen tavallisesta väkivaltaisesta teosta. Esimerkiksi Iso-Britannian terrorismilainsäädäntö (Terrorism Act) sisältää terroriteon määritelmän, jossa toiminnalta edellytetään lisäksi aina poliittisten, uskonnollisten tai ideologisten tarkoitusperien edistämistä. Samoin Kanadassa terrorismilainsäädäntö (Anti-Terrorism Act) edellyttää terroriteon olleen kokonaan tai osittain poliittinen, uskonnollinen tai ideologinen.[84] Suomen rikoslain näkökulmasta on toissijaista, millainen laajempi tavoite teon taustalla on, sillä tällä on vältetty mahdolliset poliittiset kiistat[85]. Tosiasiassa kuitenkin motiivit vaikuttavat tekojen moitittavuusarvioinnissa ilman lakiin kirjoitettua mainintaa.[86] Syyllisyysarvostelussa arvotetaan teon motiivit, jolla on merkitystä tahallisuuden arvioinnissa jäsennettäessä tekijän tarkoitusperiä ja niiden selityksiä.[87] Voidaan siis todeta, että vaikka poliittista tai uskonnollista motiivia ei ole oikeudelliseen määritelmään kirjoitettu, sen nähdään vaikuttavan syyllisyysarvostelussa.

[82] HE 188/2002 vp, s. 3.
[83] Neuvoston puitepäätös (2002/475/YOS), s. 2.
[84] HE 188/2002 vp, s. 14–15.
[85] Malkki 2020, s. 33.
[86] HE 44/2002, s. 181.
[87] Tapani – Tolvanen 2011, s. 23–24.

3.2 Tietoteknologia osana terrorismia

Internet toimii tehokkaana välineenä terrorismirikosten valmistelulle ja toteuttamiselle. Internetin välityksellä on mahdollista esittää uhkavaatimuksia, tehdä ideologiaa tunnetuksi, järjestää virtuaalisia koulutusleirejä, hankkia rahoitusta ja rekrytoida terrori-iskujen tekijöitä.[88] Tietoteknologia voidaan käyttää myös hyökkäysten organisoimiseen, toteuttamiseen tai ryhmittymän järjestäytymiseen, kommunikoimiseen ja tiedon välittämiseen eri ryhmittymien välillä. Lisäksi sen avulla voidaan muodostaa kyberuhka.[89]

Toisaalta taas tietojärjestelmät- ja verkot tai yleinen tietoliikenneinfrastruktuuri voivat olla terrorismihyökkäysten kohteena[90]. Verkon välityksellä tapahtuva terroristinen toiminta kiehtoo tekijöitään rajattomuudellaan ja kustannustehokkuudellaan. Terrorismiin liittyviä nettisivuja on arvioitu olevan satoja ja käyttäjäkuntaa tuhansia ympäri maailmaa.[91] Kyberterrorismin todennäköisenä aseena voidaan nähdä tietokoneet, joita voidaan käyttää suoran tai epäsuoran vahingon aiheuttamiseen tai tukemaan muuta toimintaa. Kybermaailma voidaan nähdä myös tärkeänä radikalisoitumisen ja rekrytoimisen kanavana.[92]

Kyberterrorismiin käytettäviä toimintatapoja on arvioitu olevan ainakin seuraavat toimet: propagandan levittäminen, vandalismi, palvelunestohyökkäykset, vakoiluohjelmat, ohjelmien tai ohjelmistojen käskyjen muuttaminen, kyberhyökkäykset siviili- tai sotilasinfrastruktuuria vastaan ja fyysiset hyökkäykset siviili- tai sotilasinfrastruktuurin keskeisiä laitteistoja kohtaan. Internet tarjoaa myös terrorismille koulutus- ja harjoitusalustoja sekä lisäksi kasvavan määrän sivustoja, jotka sisältävät käytännön ohjeita, videoharjoituksia, tietoja ja neuvoja.[93]

---

[88] Lohse 2012, s. 22.
[89] Limnell – Majewski – Salminen 2014, s. 132.
[90] Limnell – Majewski – Salminen 2014, s. 132.
[91] Lohse 2012, s. 22–23.
[92] Limnell – Majewski – Salminen 2014, s. 134.
[93] Limnell – Majewski – Salminen 2014, s. 135.

3.3 Kyberterrorismin määritelmän taustaa

Kyberterrorismilla ei ole olemassa yksiselitteistä lainsäädännöllistä määritelmää, vaikka käsite on ollut käytössä kolmisenkymmentä vuotta. Yhdysvaltalainen entinen tiedustelu-upseeri **Barry Collin** on 1980-luvulla käyttänyt termiä viitatessaan fyysisen ja digitaalisen maailman sulautumisesta aiheutuneisiin muutoksiin terrorismissa. Collin oli sitä mieltä, että kyberhyökkäyksillä saavutettiin samankaltaisia vaikutuksia kuin fyysisen väkivallan käytöllä. Nykypäivän kyberterrorismille on olemassa monta erilaista määritelmää.[94]

Ensinnäkin tulee ymmärtää, että kyberterrorismilla ei voi viitata mihin tahansa tietoteknologiapohjaiseen toimintaan hallintoa tai muuta auktoriteettia vastaan, sillä silloin käsite menettää merkityksensä. Määritelmää laadittaessa onkin muistettava, että hyökkäykset ovat etukäteen suunniteltuja, tavoitteeltaan poliittisia, sosiaalisia, uskonnollisia tai ideologisia. Useimmiten niitä suorittavat ovat pienryhmittymiä, joiden tarkoitus on kiinnittää huomiota haluttuun asiaan, levittää pelkoa tai vaikuttaa väestöön tai päätöksentekijöihin. Terrorismille ominaista on tietynlainen julkisuushakuisuus.[95]

Kyberterrorismia määriteltäessä voi luontevasti lähteä liikkeelle olemassa olevan terrorismimääritelmän kautta. Täten looginen kaava olisi seuraava; terrorismi on X ja kyberterrorismi on KX. Tilanne ei kuitenkaan ole niin yksiselitteinen, sillä kyseinen lähestymistapa ilmiön moniulotteisuudesta johtuen johtaa käytännön ongelmiin. Terrorismi voidaan lukea osaksi rikollisuutta, epätavanomaista sodankäyntiä tai omanlaatuiseksi ilmiöksi. Terrorismin monitulkinnaisuudesta johtuen sana ”kyber” vahvistaa vielä entisestään väärinkäsitysten mahdollisuutta. Määriteltäessä kyberterrorismia terrorismin kautta, tulee tarkasteltavaksi, millä ehdoin teot katsotaan terroristisiksi ja mitkä tavat käyttää teknologiaa täyttävät nämä kriteerit. Huomiota tulisikin kiinnittää toiminnan tarkoitukseen, motiiviin ja vahingollisuuteen. Yleisesti katsottuna terrorismilla viitataan

[94] Limnell – Majewski – Salminen 2014, s. 131.
[95] Limnell – Majewski– Salminen 2014, s. 131.

laittomaan siviilikohteisiin kohdistuvaan väkivaltaiseen uhkaan tai toimintaan. Terroristinen toimija voi olla yksityinen henkilö, ryhmittymä tai valtio. [96]

Kyberterrorismin määritelmä ei ole yksiselitteistä, sillä kansainvälisen lainsäädännön puuttuessa määritelmää tulee tarkastella kansallisen rikoslainsäädännön valossa. Tämä johtaa ilmiön erilaiseen tulkintaan eri viitekehyksissä.[97] Toisaalta taas esimerkiksi tiedustelun asiayhteydessä kapea tulkinta terrorismirikoksesta olisi se, miten siitä säädetään lainsäädännössä. Terrorismia kehotetaan enemmänkin ymmärtämään ilmiönä, sillä ilmiötasolla terrorismia voidaan kuvailla toiminnaksi, jonka tarkoituksena on mm. aiheuttaa pelkoa.[98]

Huomionarvoista tutkimuskysymyksen kannalta on huomata se, että terrorismi yleensä määritellään väkivaltaiseksi tai se sisältää väkivallan uhkaa. Kuten voidaan edellä esitetystä havaita, väkivalta on vahvasti ollut läsnä tutkijoiden tekemissä terrorismin määritelmissä. Tämä mahdollisesti juontaa juurensa maailmalla tapahtuneisiin fyysisiin terrori-iskuihin. Puitepäätöksen määritelmässä ei ole kuvattu terrorismia väkivallan kautta tai sen uhkana. Kyberterrorismissa nimittäin ei välttämättä harjoiteta väkivaltaa tai ei ainakaan ole yksiselitteistä, mitä tietoverkkovälitteisesti toteutettavalla väkivallalla tarkoitetaan[99]. Kyberterrorismissa iskuja toteutetaan siis bittien välityksellä, joka voi tietysti johtaa silmittömään väkivallan tekoon. Esimerkiksi ilmailuun kohdistettavat GPS-häirinnät voivat pahimmillaan johtaa lentokoneen maahan syöksymiseen ja aiheuttaa kuolonuhreja. Toisaalta kyberterroristinen isku voi kohdistua vesilaitokseen ja lamauttaa tai saastuttaa veden jakelun. Tällöin iskusta aiheutuneita ihmismenetyksiä ei ole samalla tavalla välittömästi havaittavissa, kuten aiemmassa esimerkissä. Täten määritelmän sisältämä *pelotella vakavasti* väestöä voidaan nähdä olevan kyberterrorismin määritelmän kannalta paremmin kuvaavana.

---

[96] Limnell– Majewski– Salminen 2014, s. 131–132.
[97] Limnell – Majewski– Salminen 2014, s. 131.
[98] Lohse – Meriniemi– Honkanen 2019, s. 30.
[99] Limnell – Majewski– Salminen 2014, s. 132.

Terrorismille on aiemmin ollut tyypillistä radikaali-islamistinen ajatusmaailma, joka on ollut selvästi havaittavissa ISIS- ja al-Qaida-ryhmittymien toiminnassa[100]. Kyberterrorismin kannalta olennaista on huomata se, että kyberterrorismissa ei välttämättä ole kyse jihadistisesta ideologiasta vaan kyberterrorismiin voi liittyä jokin muu poliittinen tai ideologinen tavoite. Ryhmittymääkään ei välttämättä tarvita, vaan teko voidaan toteuttaa yksittäisen henkilön tekemänä. Venäjän ja Ukrainan välinen sota vuonna 2022 osaltaan myös vahvistaa tätä väitettä, sillä esimerkiksi hakkeriryhmä Anonymous koostuu kansainvälisistä toimijoista ympäri maailmaa ja tämä ryhmä on osaltaan osallistunut tukemaan Ukrainaa erilaisin toimin tekemällä erilaisia kyberhyökkäyksiä Venäjää vastaan[101]. Mielenkiintoista ilmiössä on huomata se, että ryhmällä on täysin toisenlainen poliittinen tavoite kuin terrorismille tyypillinen ääri-islamistinen. Kokoavasti voidaan todeta, että käsillä on uudenlainen terrorismin muoto, mihin on aikaisemmin totuttu.

3.4 Kyberterrorismin määritelmän eri teoriat

Kyberterrorismi on verrattain uusi ilmiö. Kyberterrorismilla voidaan tarkoittaa tietokoneiden ja tietoverkkojen käyttämistä kansallisen infrastruktuurin tai valtion operaatioiden sabotoimiseen. Yksinkertaisimmillaan kyberterrorismista on kyse, kun tietoteknologiaa käytetään terroristisen tavoitteiden edistämiseen.[102] Kyberterroristisilla teoilla on myös tarkoitus pelotella tai pakottaa hallintoa tai muuta tahoa toimimaan tiettyjen poliittisten tai sosiaalisten päämäärien edistämiseksi. Toisaalta kyberterrorismi voidaan määritellä tarkoittavan terrorismin ja kyberavaruuden yhdistymistä toisiinsa.[103]

Kyberterrorismi ymmärretään yksinkertaisimmillaan laittomiksi tietokoneisiin, tietoverkkoihin ja varastoituihin tietoihin kohdistuviksi hyökkäyksiksi tai niillä uhkaamiseksi. Terrorismiin rinnastettavassa määritelmässä kyberterrorismilla taas viitataan vain hyökkäyksiin, jotka uhkaavat elämää

[100] Malkki 2020, s. 20.
[101] Iltalehti 1.3.2022. Hakkeriryhmä estänyt Venäjän sotakuljetuksia – halvaannutti raideliikenteen. [https://www.iltalehti.fi/digiuutiset/a/471ecb18-1256-42d7-8088-61434f1f6341]
[102] Weimann 2015, s. 46.
[103] Limnell – Majewski – Salminen 2014, s. 132.

tai omaisuutta, ja joilla vaikutetaan kohteen tietojärjestelmiin tai niiden sisältämään informaatioon fyysisen vahingon aiheuttamiseksi.[104]

Terrorismin tutkijat ovat antaneet kyberterrorismille määritteleviä piirteitä, joita ovat poliittinen tai ideologinen tavoite, digitaalisuus (kohteet, keinot), toiminnasta aiheutuva pelko, väkivalta ihmisiä tai omaisuutta kohtaan, rikollisuus, laittomuus, siviilikohteet, toiminnan performatiivisuus, ei-valtiolliset toimijat, ryhmittymän tai organisaation muoto sekä sattumanvaraisesti kohdistuva toiminta. Näiden lisäksi tutkijat ovat nostaneet esiin kyberterrorismille ominaisia seikkoja kuten infrastruktuurille tehtävän vahingon, valtiolliset toimijat, pakottamisen tai pelkoa herättävän väkivaltaisen sorron laajemmassa joukossa, terroristisen kyvykkyyden esittelemisen, vahingon tai vaaran aiheuttamisen sekä kustannustehokkuuden.[105]

Tietoteknologian käyttäminen terroristisiin toimiin ja varsinainen kyberterrorismi on tutkijoiden mukaan tärkeää erottaa toisistaan. Kyberterrorismista on kyse silloin, kun tietoteknologiaa käytetään aseena tai hyökkäyksen kohteena (ns. ”puhdas terrorismi”). Puhtaasta kyberterrorismista puhuttaessa on kyse teoista, jotka toteutetaan suoraan, kokonaan tai pääosin bittien maailmassa. Kybermaailma avaa ovia uudenlaisille terroristisille toimille, sillä toiminta ei vaadi suurta rahallista panostusta, samanmieliset löytävät toisensa ja voivat kokoontua yhteen nopeasti sekä turvallisesti. Käytännössä terroristit hyödyntävät kybermaailmaa samalla tavalla kuin kaikki muutkin ja tietoteknologia jatkuvasti muovaa terroristista toimintatapaa.[106]

Kyberterrorismia ei tulisi kuitenkaan rinnastaa pelkästään terrorismiin eikä sitä tulisi rajata pelkkään toimintaan, joka käyttää aseena tai kohteena tietoteknologiaa. Kyberterrorismi voidaan nähdä uuden terrorismin ilmentymänä, joka hyödyntää tietoteknologiaa toiminnassaan. Uudet terroristiorganisaatiot saattavat olla hyvinkin vauraita, rahoitettuja ja teknologisesti kykeneviä, jolloin ryhmittymällä on kyky tuottaa huomattavaa vahinkoa suuremmassa mittakaavassa ja useammassa kohteessa. Toisaalta taas terrorismia ja kyberterrorismia ei tule erottaa toisistaan, sillä

[104] Limnèll – Majewski – Salminen 2014, s. 132.
[105] Limnèll – Majewski – Salminen 2014, s. 132–133.
[106] Limnèll – Majewski – Salminen 2014, s. 133.

se vaikeuttaa terrorismin kokonaisuhkan arvioimista ja siihen vastaamista. Tämä taas antaa terroristisen teon tekijälle selvää etua. Haittapuolena kyberterrorismissa voidaan nähdä tietojärjestelmien tietoverkkojen monimutkaisuus, jonka vuoksi hyökkäyksen hallittavuus kärsii. Täten hyökkääjällä on haasteita halutun tuhotason määrittelemisessä ja isku voi olla hallitsematon. Myöskin tekojen performatiivisuus kärsii, jos ihmisiä ei kuole tai loukkaannu siinä mittakaavassa kuin oli suunniteltu.[107]

3.5 Määritelmän merkitys lainsäädännössä

Tutkielmassa on useita mainintoja määritelmien puutteesta tutkittavaan aiheeseen liittyen. Mitä merkitystä lainsäädännöllisesti on, että jokin määritelmä ei ole vakiintunut tai ei sisällä yksiselitteistä lainsäädännöllistä määritelmää? Lainsäädännöllisesti katsottuna määritelmien tarkoituksena on jäntevöittää ja tiivistää säädöstekstiä, sillä yhdellä lyhyehköllä termillä voidaan korvata pitkät ja monisanaiset ilmaisut. Määritelmät eivät kuitenkaan ole välttämättömiä ja niihin tulisikin suhtautua pidättyvästi. Mikäli ajatellaan lainsäädäntöä, niin määritelmällä on sitova vaikutus, joten siitä on oltava hyötyä, sen on oltava looginen eikä saa sisältää aineellisia säännöksiä.[108]

Rikosoikeudelliseen laillisuusperiaatteeseen sisältyy epätäsmällisyyskielto, joka edellyttää lainsäätäjältä suppeita ja täsmällisiä kriminalisointeja. Täten tunnusmerkistöjen kirjoitusasuun asetetaan kielellisiä vaatimuksia, jotta vältytään liian laajoilta ja epätäsmällisiltä kriminalisoinneilta. Epätäsmällisyyskiellon rikkomista on vaikea havaita pelkästään sanamuotoja tarkastelemalla, sillä sanat ja sanojen sisällöt ovat usein monimerkityksellisiä. Valvonnan vastuu kuuluukin perustuslakivaliokunnan tehtäväksi, mutta myös lakivaliokunta huolehtii rikoslain täsmällisyydestä. Epätäsmällisyyskiellolla pyritään varmistamaan, että kansalaisten olisi mahdollista ennakolta tietää mikä yhteiskunnaassa on rikosoikeudellisesti kiellettyä ja mikä puolestaan sallittua. Tämä ei kuitenkaan käytännössä toteudu monenkaan lain kohdalla ja tunnusmerkistöt ovat kieliasultaan liian avoimia. Kuitenkin liian tiukat täsmällisyysvaatimukset johtaisivat taas kasuistisiin, kielelli-

[107] Limnell – Majewski – Salminen 2014, s. 134.
[108] Oikeusministeriö 2013, s. 431.

siesti pitkiin ja monimutkaisiin rikostunnusmerkistöihin ja tästä syystä Euroopan ihmisoikeustuomioistuimen ratkaisukäytäntö hyväksyy kohtalaisen epätäsmällisenkin rikosoikeudellisen sääntelyn.[109]

Perustuslakivaliokunta tasapainotteleekin tarkkarajaisuuden ja tarvittavan avoimuuden välimaastossa ja on painottanut useaan otteeseen, että täysin avoimet tekotapakuvaukset ovat lähtökohtaisesti ongelmallisia. Toisaalta jotkut kriminalisoinnit ovat luonteensa takia sellaisia, että avoimet tekotapakuvaukset tulee hyväksyä, joista esimerkkinä voidaan mainita vainoaminen.[110] Tämän perusteella voidaan ajatella, että kyberhyökkäykset ja -vaikuttamiset ovat luonteeltaan vainoamisen kaltaisia tekoja, joiden tekotapakuvaus laajana tulee hyväksyä, jotta lainsäädäntö pysyy muuntuvan ilmiön johdosta ajantasaisena. Lakivaliokunta on vainoamisrikoksen kohdalla katsonut, että vainoamisrikoksen erityisluonteeseen kuuluu vainoamistekojen monityyppisyys sekä teknisen kehityksen vaikutus mahdollisiin toteuttamistapoihin[111]. Tämä pätee myös osaltaan kyberterrorismirikoksiin.

3.6 Kyberterrorismia vai kybersotaa

Kybersodalle ei ole olemassa varsinaista määritelmää, mutta sen voidaan katsoa olevan määrätietoista ja vihamielistä verkkoihin tunkeutumista, joiden kautta pyritään pääsemään käsiksi valtion elintärkeisiin toimintoihin.[112] Myös kyberterrorismin voidaan katsoa täyttävän samat kriteerit. Ongelmana on, että erilaiset teoriapohjat kybersodasta ovat keskeneräisiä ja näkemyseroja käsitteestä on eri tahoilla. Kybersodan käsitteen voidaan katsoa syntyneen jo 1970-luvulla modernin informaatiosodankäynnin yhteydessä. Viime vuosisadan lopulla oli yleisesti hyväksytty käsite informaatiosodankäynnistä, jonka lopulta kybersodan käsite syrjäytti 2010-luvulla. On sanottu, että kybersodankäynti on toisille sotaa digitaalisessa maailmassa ja toisille se on vastakohta fyysiselle sodankäynnille.[113]

---

[109] Tapani – Tolvanen 2019, s. 131.
[110] Tapani – Tolvanen 2019, s. 132.
[111] Tapani – Tolvanen 2019, s. 133.
[112] Tiilikainen 2015, s. 88.
[113] Sirjonen 2018, s. 191.

Kybersodankäynnin voidaan katsoa olevan oikeudellisesti haastava sodankäynnin muoto, sillä kyberhyökkäyksetkin voivat olla tuhovoimaltaan yhtä massiivisia ja vakavia kuin perinteisessä sodankäynnissä ja hyökkäysten vaikutukset voivat kohdistua siviiliväestöön.[114] Kansainvälisen oikeuden mukaan kybersota ja kyberhyökkäykset vastaavat aseellista voimankäyttöä, mikäli niissä voidaan toteuttaa kansainvälisessä oikeudessa määriteltyjä sotarikoksia. Väkivalta välillisesti kybersotaan osallistumattomia tahoja kohtaan on yksi kybersodankäynnin luonteenomaisista piirteistä verkkoympäristöön kohdistettujen iskujen rajattomuudesta ja hallitsemattomuudesta johtuen.[115]

Terrorismia voidaan luonnehtia superrikokseksi, joka sisältää sodankäynnin ominaisuuksia. Luonnehdinta johtuu osittain siitä, että terrorismia on vaikeaa luokitella sillä ei voida varmuudella vastata onko kyse sodasta, rikoksesta vai terrorismista. Lisäksi kysymykseen tulee minkä kategorian välinein tekoa vastaan tulisi toimia? **Lohse** väitöskirjassaan on kuvannut sodan ja rikoksen välistä suhdetta neljällä eri tavalla: ”1) ne kattavat toisensa 2) ne ovat erillisiä, yhteisen rajapinnan omaavia kategorioita 3) ne ovat erillisiä, keskinäistä rajapintaa vailla olevia luokkia tai 4) kyse on joiltain osin päällekkäisistä ja selvästi erillään olevista kategorioista.” Lohse on sitä mieltä, että ”erityisesti kolmas vaihtoehto on terrorismin vastaisen sodan paradigman ymmärtämisen kannalta selitysvoimaisin”.[116]

Terminä kyber laajentaa taistelukenttää, mikäli asiaa katsotaan sotilaallisesta näkökulmasta. Valtioiden rajoja ei tunnusteta samaan tapaan kuin fyysisessä maailmassa ja tämä voidaankin nähdä kyberin erityispiirteenä. Sotaa käyvien maiden väliset taistelut saadaan ulottumaan fyysisten rajojen ulkopuolelle eivätkä taistelut verkossa rajoitu vain sotaa käyviin maihin, vaan ne kohdistuvat myös verkkojen ulkopuolelle siviileihin. Pian huomataan, että kyberympäristössä kaikista tulee osallisia. Tästä johtuen kybermaailma kyseenalaistaa perinteisen sodankäynnin käsit-

[114] Sirjonen 2018, s. 195.
[115] Sirjonen 2018, s. 200.
[116] Lohse 2012, s. 40–41.

teen. Varsinaista ”puhdasta kybersotaa”, jota toteutetaan digitaalisessa ympäristössä ei ole koskaan nähty ja tutkijoiden mukaan tuskin tullaan koskaan näkemään.[117] Ennemminkin näköpiirissä on hybridisota, jossa sotaa käydään monella eri tavalla hyödyntäen sotilaallisen voiman lisäksi myös kybertaistelukenttää. Myöskään kaikki kyberoperaatiot eivät ole sotaa.[118] Yleisesti sitovaa hyväksyttyä määritelmää kybersodankäynnille tai kyberterrorismille ei ole luotu ja yhtenä syynä voidaan nähdä nykyaikaisen tietoverkon hyödyntämisen olevan uusi ilmiö terroristisessa tai sotilaallisessa tarkoituksessa. Käsitteiden määrittelemättömyys mahdollistaa valtioille laajemman ja vapaamman toimimisen verkossa oikeudellisia rajoja rikkomatta.[119]

Voidaanko sanoa, että hakkeriryhmä Anonymous ja muut hakkerit harjoittavat tosiasiassa kyberterrorismia hyökätessään muualta kuin sotaa käyvistä valtioista Venäjää vastaan Venäjän käydessä sotaa Ukrainan kanssa? Vai onko kyseessä kybersota, johon on liittynyt mukaan joukko vierastaistelijoita muista maista? Valtiot tasapainottelevat jatkuvasti sen välillä ovatko teot tarkasteltavissa sodan oikeussääntöjen kautta, onko kyse jonkin oikeutuksen omaavasta taistelijasta vai sovelletaanko tekoon rikoslainsäädäntöä. Joissain tapauksissa kyse voi toisaalta olla sekä sota- että terrorismirikoksesta ja tällaisessa tilanteessa tulisi arvioida vahvemmin läsnä olevia piirteitä. Terrorismirikokset ovat hyvin moniulotteisia rikoksia ja terrorismia voi esiintyä niin rauhan kuin konfliktinkin aikana. Kansainvälisen oikeuden mukaan osallistuminen vihollisuuksiin ulkomailla ei ole oikeudenvastaista ja taistelijoihin saa kohdistaa väkivaltaa osana laillisia sotatoimia. Kansainvälinen yhteisö ei myöskään ole yksimielinen siitä, missä kulkee terrorismin raja aseellisen konfliktin yhteydessä.[120]

Kuten voidaan havaita, esitettyyn kysymykseen vastaaminen ei ole niin yksiselitteistä ja edellä esitetyn valossa tarkastelu vaatisi laajempaa analyysia, joka ulottuisi pitkälle tämän tutkimuksen ulkopuolelle. Todettakoon siis, että edellä esitetyn perusteella on selvää, että sotarikoksilla ja ter-

[117] Limnéll – Iloniemi 2018, s. 168.
[118] Tiilikainen 2015, s. 88.
[119] Sirjonen 2018, s. 191.
[120] Esko 2017, s. 115–117.

rorismilla on paljon yhteistä kosketuspintaa ja päällekkäisyyttä. Tästä syystä sotarikosten ja terrorismin käsitteet sekä humanitaarisen oikeuden periaatteet sekoittuvat. Arvioitaessa rikosten luonnetta sota- tai terrorismirikoksina tulee oikeudellinen punninta toteuttaa kumpaakin rikosta koskevan sääntelyn valossa sekä kansainvälisen humanitaarisen oikeuden nojalla.[121]

[121] Esko 2017, s. 111–112.

4 KANSALLINEN LAINSÄÄDÄNTÖ KYBERTERRORISMISSA

4.1 Terrorismilainsäädännön taustaa

Rikosoikeutta on perinteisesti käsitelty pelkästään kansallisesta näkökulmasta, jossa lähtökohtana on pidetty rikoksen toteuttamista kotimaassa ja kaikkien osallisten olevan kotimaan kansalaisia. Tästä näkökulmasta katsottuna rikos ei siten koskettaisi ulkomaisia intressejä ja olosuhteita. Ympäriltämme voidaan kuitenkin havaita, ettei tämä mielikuva vastaa todellisuutta. Kotimaan kansalaiset syyllistyvät rikoksiin ulkomailla ja terrorismi kansainvälistyy. Tästä syystä myös rikosoikeuden tulisi kansainvälistyä, sillä rajat ylittävää rikollisuutta toteutetaan mitä enenevissä määrin.[122]

Terrorismilainsäädännön kerrotaan saaneen alkunsa New Yorkiin 11.9.2001 kohdistetusta terrori-iskusta. Samana vuonna joulukuussa 2001 EU:ssa hyväksyttiin terrorismin torjuntaa koskeva puitepäätös (2002/475/YOS). Puitepäätöksen valmistelu oli kuitenkin aloitettu jo ennen iskuja, mutta iskut vauhdittivat puitepäätöksen valmistelua. On sanottu, että puitepäätöksestä olisi tullut sisällöltään johdonmukaisempi ja laadukkaampi, jos sen valmisteluun olisi käytetty enemmän aikaa. Kyseinen puitepäätös on yksi EU:n rikosoikeudellisesti merkittävimpiä puitepäätöksiä ja sen vaikutus kansallisiin rikoslakeihin on ollut suuri, varsinkin Pohjoismaissa.[123] Puitepäätöksen tarkoituksena on torjua terrorismia, varmistaa terrorismirikosten johtaminen tehokkaisiin syytetoimiin ja puuttua yhä löyhemmin organisoituihin terroristijärjestöihin sekä internetin käyttöön terroristien koulutuskenttänä.[124]

Terrorismipuitepäätöstä muutettiin vuonna 2008 annetulla uudella puitepäätöksellä (2008/919/YOS). Tällä korvattiin aiemmin vuonna 2002 tehty terrorismirikoksia koskeva puitepäätös (2002/475/YOS). Muutospuitepäätös liittyi Euroopan neuvoston terrorismin ennaltaeh-

---

[122] Korkka-Knuts – Helenius – Frände 2020, s. 25.
[123] Melander 2015, s. 414.
[124] Melander 2015, s. 417–418.

käisyä koskevaan yleissopimukseen (CETS No. 196, SopS 49/2008), jolla täydennettiin eräitä puitepäätöksen artikloita. Komissio katsoi turvallisuusstrategiaa koskevassa tiedonannossa, että terrorismiin tulee EU:ssa vastata vankoin rikosoikeudellisin keinoin ja terrorismia koskeva rikosoikeudellinen kehys tuli saattaa ajan tasalle korvaamalla puitepäätös terrorismirikoksia koskevalla direktiivillä.[125]

Terrorismirikoksista säädetään nykyisin Suomen rikoslain (39/1889, RL) 34 a luvussa. Kyseinen 34 a luku on sisällytetty Suomen rikoslakiin vuonna 2003, eikä sitä ennen Suomessa ollut erikseen terrorismia koskevaa lainsäädäntöä.[126] Puitepäätöksen voimaansaattamisen seurauksena kyseinen muutos rikoslainsäädäntöön oli merkittävä lainsäädäntötoimi säännösten määrään suhteutettuna. Lisäksi puitepäätöksen voimaansaattamista koskevasta hallituksen esityksestä (HE 188/2002) tuli puitepäätöksen artiklojen implementoinnin kannalta merkittävä asiakirja.[127] Rikoslain 34 a luvun 1 § noudattaa puitepäätöksen 1 artiklaa siinä mielessä, että Suomessa omaksuttiin näkemys, jonka mukaan puitepäätöksen terrorismikäsite on tekninen. Tällä tarkoitetaan sitä, että ei ole olemassa erillistä terrorismirikosten rikoslajia. Voimassa olevasta rikoslajista tehdään terroristisessa tarkoituksessa, moitittavuudeltaan ja rangaistusasteikoltaan perusrikosta poikkeavampi, jonka rangaistusta on korotettu.[128]

Euroopan parlamentin ja neuvoston direktiivi (2013/40/EU) artiklan 1 kohta edellytti, että jäsenvaltioiden tuli tehdä tarvittavat toimenpiteet varmistaakseen, että tietyt rikokset tulee olla lainsäädännössä terrorismirikoksina rangaistavia. Tarkoituksena oli myös ottaa käyttöön yhteinen määritelmä tietojen laittomasta hankkimisesta, jolla tarkoitetaan laitonta tunkeutumista tietojärjestelmään, laitonta järjestelmän häirintää, laitonta datan vahingoittamista ja viestintäsalaisuuden loukkaamista.[129] Terroristisessa tarkoituksessa tehtyjä rikoksia koskevia säännöksiä muutettiin rikoslaissa siten, että törkeä datavahingonteko, törkeä tietoliikennehäirintä ja törkeä tietojär-

[125] Melander 2015, s. 416.
[126] HE 188/2002, s. 16.
[127] Melander 2015, s. 416.
[128] Melander 2015, s. 420.
[129] Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, s. 12.

jestelmän häirintä lisättiin terrorismirikoslainsäädäntöön (RL 34a:1.1,4), joka vahvistettiin rikoslaissa hallituksen esityksen (HE 30/2018 vp) pohjalta vuonna 2018. Kyseiset teot ovat olleet aiemmin säädettyinä perusmuotoisina rikoslain 35 ja 38 luvuissa.

Samaan aikaan lukuisia muita rikoslain 34 a luvun säännöksiä muutettiin siten, että niissä otettiin huomioon terroristisessa tarkoituksessa tehtyjä rikoksia koskevat vakaviin tietoverkkorikokseen liittyvät muutokset. Muutokset ovat koskeneet terroristisessa tarkoituksessa tehtävän terroristiryhmän johtamista (34a:3.1), terroristiryhmän toimintaan osallistumista (34a:4.1), koulutuksen antamista terrorismirikoksen tekemistä varten (34a:4a), kouluttautumista terrorismirikoksen tekemistä varten (34a:4b), värväystä terrorismirikoksen tekemiseen (34a:4c), terrorismin rahoittamista (34a:5.2), matkustamista terrorismirikoksen tekemistä varten (34a:5c.1) ja terroristiryhmän määritelmää (34a:6.2).[130] Kyseisissä säännöksissä on siten huomioitu tietoverkkorikokset ja täten säännökset voivat tulla sovellettavaksi kyberterrorismiin liittyvissä rikoksissa. Lisäksi rikoslain 34 a lukuun on tehty muutos, jossa sana ”valtio” on korvattu ”maalla”, jolla korostetaan sitä, että terrorismirikokset ovat laajasti yhteiskuntaan kohdistuvia rikoksia eivätkä pelkästään aiheuta vahinkoa valtion rakenteille ja viranomaisille vaan teko on omiaan aiheuttamaan vahinkoa koko maalle.[131]

Yhteiskunta teknistyy ja kansainvälistyy nopeasti ja nämä muutokset ovat asettaneet rikoslainsäätäjät uusien haasteiden äärelle. Uusista ilmiöistä mm. terrorismi edellyttää uudenlaista rikosoikeudellista kontrollia, joka on johtanut rikostunnusmerkistöjen ohentumiseen. Liian avoimet rikostunnusmerkistöt eivät ole hyväksyttäviä, mutta liikaa täsmällisyyttä rikoslailta ei myöskään voida edellyttää.[132] Nykyistä terrorismilainsäädäntöä onkin kritisoitu, sillä rikoslain 34 a luku on monessa suhteessa poikkeuksellinen kokonaisuus. Sääntely nähdään vaikeaselkoisena sisältäen paljon luvun sisäisiä viittauksia ja viittauksia rikoslain muihin säännöksiin. Myöskään terrorismin määritelmäsäännöstä ei voida pitää yksinkertaisena. Sääntelyn haastavuutta lisää se, että terrorismirikoksia koskevien säännösten taustalla on monia kansainvälisiä oikeudellisia velvoitteita,

[130] HE 30/2018 vp, s. 8.
[131] HE 30/2018 vp, s. 99.
[132] Tapani – Tolvanen 2019, s. 132.

jotka tulee ottaa huomioon sääntelyä sovellettaessa. Lisäksi terrorismirikoksiin liittyvässä sääntelyssä on otettava huomioon perus- ja ihmisoikeudet, jotta terrorismin torjuntaan liittyvät toimet eivät loukkaisi näitä oikeuksia perusteetta.[133]

Rikoslain 34 a luku on vierasperäinen, joka tarkoittaa sitä, että luvun säännökset perustuvat EU:n oikeuteen ja myös Euroopan neuvostossa syntyneeseen normistoon. YK:n turvallisuusneuvoston päätöslauselman 1373 aiheutuvat velvoitteet ovat panneet alulle EU:n terrorismipuitepäätöksen ja Euroopan neuvoston terrorismiyleissopimuksen (SopS 48/2002). Oikeudellisessa harkinnassa tulee hallita sekä EU-oikeuden, että valtiosopimusten tulkinta.[134] Terrorismirikosten jäsentelyä voidaan toteuttaa monin eri tavoin. Rikoslain 34 a luvussa säädetään erilaisia toiminnan kokonaisuuksia, jonka ytimen muodostavat terroristisessa tarkoituksessa tehdyt rikokset (RL 34a:1).[135] Lainsäädäntöä on viime vuosien aikana päivitetty ja sääntely koskee yhä laajemmin terroristisessa tarkoituksessa tehtyjä rikoksia.

4.2 Yleistä terrorismirikoksista

Terrorismirikoksissa on kyse kansainvälisistä rikoksista. Kansainvälisellä rikosoikeudella ei ole yksiselitteistä määritelmää, vaan sitä käytetään eri yhteyksissä eri tavalla. Käsitettä voidaan perinteisesti käyttää kuvailemaan normikokonaisuutta, joka säätelee valtion rikosoikeudellista soveltamisalaa tai sitä voidaan käyttää luonnehtimaan sellaisia normeja, jotka luovat välittömän rikosvastuun suoraan kansainvälisen oikeuden nojalla. Laajassa mittakaavassa voidaan puhua eräänlaisesta kattokäsitteestä, mutta tässä yhteydessä on syytä ymmärtää, että normien alkuperä voi olla kansallinen, valtioiden välinen tai kansainvälinen. Täten käsitteen alle voidaan sijoittaa prosessioikeudellisia ilmiöitä kuten rikoksen johdosta tapahtuva rikoksentekijän luovuttaminen toiseen valtioon tai muu kansainvälinen oikeusapu rikosasioissa. Kansainvälinen rikosoikeus voidaankin jakaa neljään eri osa-alueeseen: 1) rikosoikeuden soveltamisalaa koskeviin normeihin

[133] Melander 2016, s. 2.
[134] Lohse 2012, s. 52.
[135] Lappi-Seppälä ym. 2009, s. 1163.

2) kansainväliseen oikeusapuun rikosasioissa 3) ylikansalliseen eurooppalaiseen rikosoikeuteen ja 4) kansainväliseen rikosoikeuteen suppeassa merkityksessä.[136]

Terrorismirikoksissa on kyse abstraktisista vaarantamisrikoksista. Vaaran toteaminen edellyttää aina seurauksen syntymisen mahdollisuutta. Abstrakteissa vaarantamisrikoksissa riittää varteenotettava mahdollisuus vaaran syntymisestä, ei tarvitse osoittaa jonkun olleen vaaran piirissä. Abstraktin vaaran kriminalisoinnilla ylläpidetään kansalaisten luottamusta siihen, ettei henkeen ja terveyteen liittyviä turvallisuusodotuksia horjuteta.[137] Turvallistamisdoktriinin tuottamaa käsitteistöä ja argumentointitapaa hyödynnetään terrorismikontekstin hahmottamisessa. Terrorismiin liittyvää ympäristöä voidaan lähestyä neljän kysymyksen avulla 1) miltä turvataan 2) mikä turvataan 3) kuka osoittaa uhan 4) miten turvataan.[138]

Oikeuskäytännössä terrorismirikoksia rinnastetaan toisinaan poliittisiin rikoksiin, joka on lähes poikkeuksetta ongelmallista. Poliittisista rikoksista ei ole muodostunut yhtenäistä kansainvälistä soveltamiskäytäntöä, ja terrorismirikokset jäävät poliittisia rikoksia koskevan doktriinin ydinalueen ulkopuolelle. Terrorismirikoksilta ei myöskään välttämättä edellytetä poliittisesti motivoituneen väkivallan käyttämistä tai sillä uhkaamista. Lisäksi rikoslain 34 a luvun edistämisrikoksissa ei edellytetä terroristista tarkoitusta, mikä voidaan nähdä ainoana poliittisena elementtinä terrorismirikoksiin kanavoivana vastuukriteerinä. Selvästi poliittisluonteisia terroristisen tarkoituksen omaavia tekoja voidaan nähdä vain RL 34a:6.1:n 2 ja 3 kohdassa.[139]

Sota- ja terrorismirikokset ovat kansainvälisiä rikoksia, jotka ovat tyypillisesti kollektiivisia rikoksia, joissa erilaiset osallistumisen muodot ja roolit on mahdollista erottaa. Terrorismirikokset kuuluvat siis henkilökohtaiseen rikosoikeudelliseen vastuun muotoon nimeltään Joint Criminal Enterprise (JCE). Vastuu ulottuu kaikkiin niihin, joita epäillään osallisiksi yhteiseen rikolliseen pää-

[136] Korkka-Knuts – Helenius – Frände 2020, s. 28.
[137] Tolvanen – Tapani 2019, s. 248.
[138] Lohse 2012, s. 67.
[139] Lohse 2012, s. 68.

määrään tekotapaan tai rooliin katsomatta. JCE-malli on käytössä rikosvastuun liittämisen välineenä esimerkiksi puolisotilaallisissa yhteenliittymissä ja rikollisjärjestöissä.[140] Lainsäädännön mukaan terrorismirikoksille ominaista on terroristinen tarkoitus (RL 34a:6). Terrorismirikokset ovat myös kansainvälisiä rikoksia ja ”Suomen lainsäädäntöä sovelletaan tekopaikan laista riippumatta myös Suomen ulkopuolella (RL 1:7.3)”, kun kyseessä on rikoslain 34 a luvussa tarkoitettu rikos. Lainkäyttövalta on siten Suomella riippumatta tekopaikasta, sen lainsäädännöstä tai tekijästä universaaliperiaatteen nojalla[141].

4.3 Kyberterrorismiin liittyvä rikoslain 34 a luvun mukainen tunnusmerkistö

4.3.1 Terroristisessa tarkoituksessa tehdyt rikokset

Rikoslain 34a:1:ssä on säädetty terroristisessa tarkoituksessa tehdyistä rikoksista. Tarkoituksena on tässä kohdin nostaa tarkastelun kohteeksi vain tietoverkkorikollisuuteen kohdistuvat säännökset. Täten muut kyseisen luvun rikokset jätetään tarkastelun ulkopuolelle. Hallituksen esityksessä esitettiin muutettavaksi Suomen rikoslain 34 a lukua siten, että RL 34a:1.1,4 kattaisi RL 35:3b.1,4 kohdassa tarkoitetun törkeän datavahingonteon, RL 38:6.1,3,5 tai 6 kohdassa tarkoitetun törkeän tietoliikennehäirinnän ja RL 38:7b.1,1,3 ja 5 kohdassa tarkoitetun törkeän tietojärjestelmän häirinnän.[142]

Rikoslain säännös (34a:1.1,4) tietoverkkorikoksista on siis kokoelma rikoslaissa aiemmin muissa luvuissa (RL 35 ja RL 38) säädetyistä rikoksista, joista on myöhemmin säädetty myös terrorismirikoksissa. Säännös kuuluu avatusti seuraavalla tavalla[143]: ”Joka terroristisessa tarkoituksessa siten, että teko on omiaan aiheuttamaan vakavaa vahinkoa jollekin maalle tai kansainväliselle järjestölle,

---

[140] Lohse 2011, s. 10.
[141] HE 1/1996 vp, s. 22.
[142] HE 30/2018 vp, s. 1.

- tekee törkeän datavahingonteon kohdistamalla rikoksen tietojärjestelmään, jonka vahingoittaminen vaarantaisi energianhuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon (RL 35:3b1,4)
- tekee törkeän tietoliikenteen häirinnän, jossa tietoliikennehäirinnässä rikos tehdään osana toimintaa, jossa on vaikeutettu merkittävään määrään tietojärjestelmiä käyttäen sellaisen laitteen tai tietokonehaittaohjelman taikka ohjelmakäskyjen sarjaa, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa taikka murtaa tai purkaa sähköisen viestinnän teknisen suojauksen taikka tietojärjestelmän toiselle kuuluvaa salasanaa, pääsykoodia tai muuta vastaavaa tietoa (RL 38:6.1,3,5 tai 6)
- tekee törkeän tietojärjestelmän häirinnän, jos tietojärjestelmän häirinnässä aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa tai rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon (RL 38:7b.1,1,3 tai 5), on tuomittava vankeuteen ––”.

Säännös kvalifioi perusrikoksia, jolla tarkoitetaan sitä, että teosta tuomitaan rangaistukseen ankaramman asteikon puitteissa, mikäli tekijällä on ollut terroristinen tarkoitus. Huomioitavaa on, että kuitenkaan pelkkä tarkoitus ei riitä, vaan tekijän on syyllistyttävä säännöksessä mainittuun rikokseen, eikä yritys ole rangaistavaa.[144] Lain tulkinnassa on oleellista ymmärtää mitä tarkoitetaan, jos rikoksen tekijällä on terroristinen tarkoitus. Terrorismirikokset erottuvatkin muista niitä muistuttavista rikoksista RL 34a:6,1 nojalla. Kyseisessä lainkohdassa säädetään terroristisesta tarkoituksesta, joka liittyy joko suoraan tai välillisesti kaikkiin terrorismirikoksiin[145].

[144] Lappi-Seppälä ym. 2009, s. 1170 (kirjailija päivittänyt tekstin 7.12.2021).
[145] HE 30/2018 vp, s. 80.

Rikoslain 34 a luvun 6 §:n mukaan ”rikoksentekijällä on terroristinen tarkoitus, jos hänen tarkoituksenaan on 1) aiheuttaa vakavaa pelkoa väestön keskuudessa; 2) pakottaa oikeudettomasti jonkin valtion hallitus tai muu viranomainen taikka kansainvälinen järjestö tekemään, sietämään tai tekemättä jättämään jotakin; 3) oikeudettomasti kumota jonkin valtion valtiosääntö tai muuttaa sitä tai horjuttaa vakavasti valtion oikeusjärjestystä taikka aiheuttaa erityisen suurta vahinkoa valtiontaloudelle tai valtion yhteiskunnallisille perusrakenteille; tai 4) aiheuttaa erityisen suurta vahinkoa kansainvälisen järjestön taloudelle tai sellaisen järjestön muille perusrakenteille.” Edellä luetellut tekotavat ovat vaihtoehtoisia eli yksikin teon tarkoitus riittää osoittamaan terroristisen tarkoituksen[146]. Teon tarkoituksen määritelmä on luvun kannalta keskeinen, sillä sen olemassaolo tekee tietoverkkorikoksista sellaisia, että niistä tulee rangaista ankarammin kuin ilman tällaista tarkoitusta.

Lainsäädännössä käytetty kirjoitustapa ”siten, että teko on omiaan ––” osoittaa sen, että kyse on abstraktin vaarantamisen rikoksesta. Abstrakteissa vaarantamisrikoksissa ei tarvitse osoittaa teon aiheuttaneen vakavaa vahinkoa tietyssä tilanteessa vaan riittää, että teko tekotyyppinä kokemusperäisesti aiheuttaisi sellaista vahinkoa. Huomioitavaa on, että terrorismirikoksilta edellytetään, että teko on omiaan aiheuttamaan tällaista vahinkoa, muutoin tekoa ei ole pidettävä terroristisessa tarkoituksessa tehtynä rikoksena, vaikka tekijällä olisi ollut terroristinen tarkoitus ja vaikka teko olisi pykälän sisältämän rikostunnusmerkistön mukainen.[147]

Maan ja kansainvälisen järjestön määritelmä on määritetty RL 34a:6.3:ssa, jossa alkuperäisessä säännöksessä oli kyse valtiosta eikä maasta. Kyse on ollut käännösvirheestä, sillä puitepäätös ja direktiivi käyttää valtion sijasta ”maata”, jolloin tekojen piiriin saadaan myös kansaan ja kansalaisyhteiskuntaan kohdistuvat teot.[148]

---

[146] HE 188/2002 vp, s 57.
[147] HE 188/2002 vp, s.33.
[148] Lappi-Seppälä 2009, s. 1170.

Vakavalla vahingolla (RL 34a:1.1) tarkoitetaan jäsenvaltioiden määritelmää vakavasta vahingosta kansallisen lain ja käytännön mukaan. Tällä tarkoitetaan sitä, että rikoslaissa (34a:1.1,4) on viitattu 38 luvun 7 b §:n ja 6 §:n sisältämään kvalifiointiperusteeseen, joka kattaa tilanteet, joissa aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa.[149] Vakavalla pelolla puolestaan tarkoitetaan hallituksen esityksen (188/2002) mukaan väestön keskuudessa syntyvää perusteltua vakavaa pelkoa siitä, että yksityiset edut kuten henki, terveys, vapaus, ruumiillinen koskemattomuus, omaisuus, kotirauha tai yhteisön edut kuten valtion valtiosääntö tai ympäristö ovat vaarassa.[150]

Hallituksen esityksen mukaan tietoverkkorikoksia koskeva säännös (RL 34a:1.1,4) on rajattu koskemaan direktiivin 3 artiklan 1 kohdan i alakohdan edellytyksiä, joissa kyseessä ovat törkeät datavahingonteot, törkeät tietoliikenteen häirinnät tai törkeät tietojärjestelmän häirinnät, jotka ovat laajamittaisia, erityisen tuntuvaa haittaa tai taloudellista vahinkoa aiheuttavia tai yhteiskunnan tärkeän toiminnan vaarantavia tekijöitä.[151] Lisäksi teon voi tehdä törkeäksi se, että rikos kohdistuu laitteeseen, tietojärjestelmän tai viestintään, joka voi vahingoittuessaan vaarantaa energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon.[152]

Euroopan parlamentin ja neuvoston direktiivin (2013/40/EU) 2 artiklan a kohdan mukaan tietojärjestelmällä tarkoitetaan laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu tietojenkäsittelyä varten. Lisäksi sillä tarkoitetaan dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään sen tai niiden toimintaa, käyttöä tai suojausta tai huoltoa varten. Datalla puolestaan tarkoitetaan tietojärjestelmässä käsiteltäväksi soveltuvaa tosiseikkojen, tietojen tai käsitteiden esitystä, jotka mahdollistavat tietojärjestelmän suorittamaan joitain toimintoja.[153]

---

[149] HE 232/2014 vp, s. 23.
[150] HE 188/2002 vp, s. 58–59.
[151] HE 30/2018 vp, s. 110.
[152] HE 30/2018 vp, s. 31.
[153] HE 232/2014 vp, s.9.

4.3.2 Terroristiryhmän johtaminen

”Joka johtaa terroristiryhmää, jonka toiminnassa on tehty 1 §:n 1 momentin 2–8 kohdassa –– tarkoitettu rikos –– on tuomittava terroristiryhmän johtamisesta vankeuteen –– (RL 34 a luku 3 §)”. Terroristiryhmällä tarkoitetaan RL 34a:6.2 mukaan ”vähintään kolmen henkilön muodostamaa tietyn ajan koossa pysyvää rakenteeltaan jäsentynyttä yhteenliittymää, joka toimii yhteistuumin tehdäkseen 1 tai 1 a §:ssä tarkoitettuja rikoksia”. Johtamista sen sijaan ei ole määritelty lain tasolla, mutta lain esitöiden mukaan se voi ilmetä ryhmän hierarkiasta. Tyypillisesti terroristiryhmän ei kuitenkaan katsota organisoituvan siten, että siellä vallitsisi selkeät vastuu- ja toimivaltasuhteet ja ryhmä voikin jakautua useaan eri soluun. Perinteisellä tasolla johtajuuden voidaan katsoa perustuvan käskyjen ja ohjeiden antamiseen.[154]

Tuomitsemisen osalta todettakoon, että johtaja tulee tuomituksi sekä johtamisesta, että siitä rikoksesta johon terrorismiryhmässä syyllistytään. Johtajan vastuu on laajempaa kuin normaali osallisuuteen perustuva vastuu ja täten riittää, että hän tiesi tai hänen olisi pitänyt tietää rikoksen tekeillä olosta. Vastuu perustuu ryhmän valvontavelvollisuuteen eikä johtaja vastaa sellaisten henkilöiden rikoksista, joihin häneltä puuttuu johtajasuhde. Myöskään johtaja ei vastaa ryhmän ulkopuolisten tekemistä rikoksista eikä sellaisista rikoksista, joista hän ei tiedä tai joita hän on pyrkinyt estämään.[155] Kyseisen pykälän nojalla tietoverkkorikollisuuteen kytkeytyvän terroristiryhmän johtaminen on rangaistavaa.

4.3.3 Terroristiryhmän toimintaan osallistuminen

”Joka edistääkseen terroristiryhmän 1, 1 a tai 2 §:ssä tarkoitettua rikollista toimintaa taikka tietoisena siitä, että hänen toimintansa edistää sitä,
1) varustaa tai yrittää varustaa terroristiryhmää räjähteillä, aseilla, ampumatarvikkeilla tai niiden valmistamiseen tarkoitetuilla aineilla tai tarvikkeilla taikka muilla vaarallisilla esineillä tai aineilla,

[154] Lappi-Seppälä ym. 2009, s. 1174 (kirjailija päivittänyt tekstin 7.12.2021).
[155] Lappi-Seppälä ym. 2009, s. 1174 (kirjailija päivittänyt tekstin 7.12.2021).

2) hankkii tai yrittää hankkia taikka luovuttaa terroristiryhmälle toimitiloja tai muita sen tarvitsemia tiloja taikka kulkuvälineitä tai muita ryhmän toiminnan kannalta erittäin tärkeitä välineitä,
3) hankkii tai yrittää hankkia tiedon, jonka tuleminen terroristiryhmän tietoon on omiaan aiheuttamaan vakavaa vahinkoa maalle tai kansainväliselle järjestölle, taikka välittää, luovuttaa tai ilmaisee terroristiryhmälle sellaisen tiedon ––.” (RL 34 a luku 4 §)

Jotta henkilö voitaisiin saattaa säännöksen tarkoittamasta rikoksesta vastuuseen, tulee edistämisen olla suoranaista tai tietoista menettelyn edistämistä terroristiryhmän rikollista toimintaa kohtaan. Edistäminen edellyttää aina aktiivista toimintaa, jolla pyritään edistämään terrorismirikoksen toteuttamista, eikä täten pelkkä kannattaminen ole toiminnan rangaistavaa edistämistä.[156] Edistäminen ja avunanto ovat toisiaan hyvin lähellä olevia myötävaikuttamisen muotoja. Tärkeää on kuitenkin niiden erottaminen toisistaan, sillä rangaistuksen määräämisen kannalta avunanto on rangaistuksen vähentämisperuste (RL 6:8). Edistämisen ja avunannon tärkein rajanveto on **Lohsen** mukaan siinä, että ”terroristisen edistämisrikossäännösten soveltamisala kattaa vain ne teot, joiden yhteys terroristiseen päärikokseen ei ole kiinteässä yhteydessä terroristiseen päärikokseen tai sen valmisteluun siten, että vastuusubjektia voitaisiin pitää avunantajana tällaiseen rikokseen”.[157]

Toisekseen edistämisrangaistavuus ei edellytä pääteon tai sen yrityksen tekemistä, toisin kuin avunanto. Edistämisrikossäännökset ovat siten sovellettavissa, vaikka päärikosta ei edes valmistella eikä rangaistavuus ole kytköksissä terroristiseen päärikokseen. Täten edistämistoimet ovat rangaistavissa ennen päärikosta, sen aikana tai sen jälkeen. Edistämisrikossäännös kattaa avunantoa varhaisemman menettelyn.[158]

Kyberterrorismin kannalta merkitystä voidaan katsoa olevan sillä, mitä säännöksellä (RL 34a:4.1,2) tarkoitetaan ”muiden erittäin tärkeiden välineiden hankkimisella terroristiryhmälle”.

---

[156] Lappi-Seppälä ym. 2009, s. 1175 (kirjailija päivittänyt tekstin 7.12.2021).
[157] Lohse 2012, s. 108.
[158] Lohse 2012, s. 109.

Tällaisia välineitä voivat olla tietojenkäsittely- tai viestitysvälineet kuten tietokoneet, matka- ja radiopuhelimet sekä muut yhteydenpitovälineet. Välineen tärkeyden määrittää se, estääkö välineen puutuminen terrori-iskun tekemisen tai lykkää sen tekemistä.[159] Esimerkiksi tietokoneen puuttuminen kyberterrorismi-iskun tekemisessä estää toiminnan kokonaan. Toisaalta taas välineen tärkeydestä viestittää myös terrorismiryhmän toistuva pyrkimys saada haltuunsa tietty väline[160].

Toisena seikkana kyberterrorismin kannalta säännöksestä voidaan ottaa tarkasteluun tietojen hankkimiseen käytettävät keinot. Säännös on jätetty avoimeksi lain esitöissä siten, että siinä ei varsinaisesti ole otettu kantaa tietojen hankkimisen keinoista. Toisaalta säännös kattaa teknisin keinoin tapahtuvan tahallisen ja oikeudettoman tietojen hankinnan tietojärjestelmistä tai datan siirroista.[161] Säännös voisi tulla sovellettavaksi kyberterrorismiin liittyvissä rikoksissa tietojen hankkimiseen liittyvän tunnusmerkistön osalta. Säännöstä on tarkemmin määritelty ja sovellettu tutkielman myöhemmässä vaiheessa kybervakoiluun liittyvässä terrorismirikoksen muodossa.

4.3.4 Terrorismiin liittyvä koulutus

Koulutuksen antamisesta terrorismirikoksen tekemistä varten säädetään RL 34 a luvun 4 a §:ssä, ”joka edistääkseen 1 §:ssä –– tarkoitettua rikollista toimintaa taikka tietoisena siitä, että hänen toimintansa edistää sitä, –– taikka muulla vastaavalla tavalla toimeenpanee, yrittää toimeenpanna tai antaa koulutusta ––”.

Kouluttautumisesta terrorismirikoksen tekemistä varten säädetään RL 34 a luvun 4 b §:ssä: ”joka tehdäkseen 1 §:n 1 momentin 2–8 kohdassa –– tarkoitetun rikoksen kouluttautuu räjähteiden, ampuma-aseiden tai muiden aseiden taikka myrkyllisten tai haitallisten aineiden valmistuksessa tai käytössä taikka muiden näihin merkitykseltään rinnastuvien erityisten menetelmien tai tekniikoiden käytössä ––.”

---

[159] Lohse 2012, s. 151 ja HE 188/2002, s. 52.
[160] Lohse 2012, s. 151.
[161] HE 232/2014 vp, s. 15. ks. 6 artikla viestintäsalaisuuden loukkaus (tietojen laiton hankkiminen)

Terrorismirikosdirektiivin (EU 2017/541) 3 artiklan 1 kohta on laajennettu rikoslakiin kattamaan myös vakaviin tietoverkkorikoksiin liittyvää koulutuksen antamista ja kouluttautumista ja tästä syystä teko on lisätty kyseisiin säännöksiin viittauksella rikoslain 34 a luvun 1 §:ään.[162] Internetistä on tullut terroristisen erityistaitojen levityskanava ja anonymiteetin suoja. Online-ohjeiden lataaminen tietokoneelle ei kuitenkaan täytä RL 34a:4a tunnusmerkistöä, vaikka toiminnassa olisi kyse virtuaalisesta etäkouluttautumisesta vaan kyseessä on RL 34a:4b liittyvä teko.[163] Täten direktiivin mukaan itseopiskelu terrorismirikoksen tekemiseen ja sen edistämiseen katsotaan olevan kouluttautumista terrorismiin. Toisaalta taas hallituksen esityksessä korostetaan, että kouluttautumisen tulee tapahtua koulutuksen antajan ohjauksessa ja itseopiskelu internetin tietoja hyödyntämällä ei olisi kouluttautumista terrorismirikoksen tekemistä varten[164]. Myöhemmin lain esitöiden mukaan on säännöksestä poistettu viittaus ”4 a §:ssä tarkoitetulla tavalla” joka tarkoittaa sitä, että RL 34a:4b säännös kattaa nyt paremmin itsekouluttautumistilanteet.[165]

Säännöksissä ei ole epätäsmällisyyskiellosta huolimatta kuvattu kouluttautumistapoja esimerkein, joka täsmentäisi nykyistä säännöstä. Toki tyhjentävää tekotapaluetteloa ei ole mahdollista saavuttaa jatkuvasti muuttuvien kouluttautumistapojen takia eikä siihen ole aiheellista myöskään pyrkiä.[166] Kyseisten säännösten tämänhetkinen luonne mahdollistaa paremman sovellettavuuden ja rangaistavuuden esimerkiksi kyberterrorismiin liittyvässä kouluttautumisessa tai kouluttamisessa. Hallituksen esityksessä on mainittu, että näytön arviointi koulutuksen tai kouluttautumisen tilanteissa saattaa osoittautua haasteelliseksi, samoin kuin tapausten paljastuminen[167]. Kaiken kaikkiaan kyseessä voidaan katsoa olevan sovellettavuuden kannalta haasteellinen kokonaisuus varsinkin kyberterrorismirikoksissa, joissa anonymiteetti ja kyberympäristö luovat erinomaiset puitteet koulutuksen antamiselle ja kouluttautumiselle.

---

[162] HE 30/2018 vp, s. 41.
[163] Lohse 2012, s. 160.
[164] HE 18/2014 vp, s. 14–15.
[165] HE 30/2018 vp, s. 42.
[166] HE 30/2018 vp, s. 44.
[167] HE 30/2018 vp, s. 44.

4.3.5 Värväys terrorismirikoksen tekemiseen

”Joka edistääkseen 1 §:ssä –– tarkoitettua rikollista toimintaa taikka tietoisena siitä, että hänen toimintansa edistää sitä, perustaa tai organisoi terroristiryhmän taikka värvää tai yrittää värvätä väkeä terroristiryhmään tai muuten tekemään mainituissa pykälissä tarkoitetun terrorismirikoksen on tuomittava –– vankeuteen (RL 34 a luku 4 c §)”.

Kyseinen säännös liittyy perustamis- ja organisoimistoimia koskeviin tekoihin, joilta vaaditaan aktiivisuutta. Värväystapoihin ei liity ajallisia rajoitteita ja organisointiin liittyvät toimet voivatkin olla pitkäkestoisia. Terroristiseksi värväykseksi voidaan katsoa terroristikokelaiden tai sellaisiksi haluavien kokoaminen yhteen erilaisin keinoin. Värväämisen oivalliseksi kanavaksi on nykypäivänä osoittautunut internet, joka ulottuu kaikkialle maailmaan.[168] Täten kyberterrorismiin liittyvään rikollisuuteen on luontevaa värvätä tekijöitä internetin avulla. Tutkielmassa jäljempänä on käyty tarkemmin esimerkin avulla läpi säännöksen sovellettavuutta kyberterrorismiin liittyvässä rikollisuudessa.

4.3.6 Terrorismiin liittyvä rahoittaminen

Terrorismirikoksen rahoittamisesta säädetään rikoslain 34 a luvun 5 §:ssä, ”joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan jotakin 1 §:ssä –– tarkoitettua rikosta ––. Terrorismirikoksen rahoittamisesta tuomitaan myös se, joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan –– sellaista tuhotyötä, törkeää tuhotyötä tai yleisvaarallisen rikoksen valmistelua, jota on pidettävä terroristisen pommi-iskujen torjumista koskevassa kansainvälisessä yleissopimuksessa (SopS 59–60/2002) tarkoitettuna rikoksena ––.”

[168] Lohse 2012, s.163–164.

Terroristin rahoittamisesta on säädetty rikoslain 34 a luvun 5 a §:ssä, ”joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan henkilöä, joka tekee 1 §:ssä –– tarkoitettuja rikoksia tai osallistuu niiden tekemiseen 5 luvun 3–6 §:ssä tarkoitettuna rikokseen osallisena, on tuomittava terroristin rahoittamisesta vankeuteen ––.”

Terroristiryhmän rahoittamisesta säädetään rikoslain 34 a luku 5 b §:ssä: ”joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan 6 §:n 2 momentissa tarkoitettua terroristiryhmää, on tuomittava terroristiryhmän rahoittamisesta vankeuteen ––.”

Terrorismin rahoittamisessa on kyse kaikista suorimmasta rahoittamiseen liittyvästä kriminalisoinnista, jolla rahoittaja antaa tai kerää varoja terrorismirikoksen tekemistä varten. Kyseinen lainkohta perustuu YK:n terrorismin vastaiseen yleissopimukseen. Sääntelyn merkitys on erityinen, sillä rahoittamisella on selvä suoranainen vaikutus luoda edellytyksiä terroristiseen toimintaan. Terroristin rahoittamiseen liittyvä säännös on lisätty terrorismin rahoittamisrikoksiin viimeisimmässä uudistuksessa ja toimii rinnakkaissäännöksenä terroristiryhmän rahoittamissäännökselle. Kummassakaan tapauksessa ei tarvitse osoittaa rahoituksen kohdentuvan tietyn rikoksen tekemiseen eikä myöskään tarvitse osoittaa rahoittamisen yhteyttä nimenomaisen terrorismirikoksen tekemiseen.[169]

Rangaistavuuden raja on säännöksissä hankala, sillä varojen antaja ei voi kontrolloida mihin toimintaan varoja tosiasiassa käytetään ja esimerkiksi humanitaariseen tukeen osoitetut varat voivat kohdistua terroristiseen toimintaan. Rahoittamista koskeva kriminalisointi on ollut tarpeellinen, sillä rahoittaja ei pääsääntöisesti tiedä rikoksia, joita terroristiryhmässä tehdään ja ilman kyseisiä säännöksiä rahoittaminen voisi olla rankaisematonta.[170]

Säännöksessä (RL 34a:5) mainitun tuhotyön voidaan katsoa liittyvän olennaisilta osin kyberterrorismiin. Nimittäin tietoliikenteen, tietojärjestelmän häirinnän ja datavahingonteon kohdistuessa

[169] Lappi-Seppälä ym. 2009 s. 1177 (kirjailija päivittänyt tekstin 7.12.2021)
[170] Lappi-Seppälä ym. 2009 s. 1177–1179 (kirjailija päivittänyt tekstin 7.12.2021)

elintärkeään infrastruktuuriin kuuluvaan tietojärjestelmään saattaa useimmissa tapauksissa täyttyä RL 34:1:ssä tarkoitettu tuhotyön tunnusmerkistö. Tuhotyön tunnusmerkistö edellyttää vakavan vaaran täyttymistä.[171] Tuhotyötä koskeva kriminalisointi saattaa olla toisinaan päällekkäistä törkeän tietoliikennehäirinnän ja törkeän tietojärjestelmähäirintää koskevan kriminalisoinnin kanssa. Eroavaisuutena näissä on, että datavahingonteko, tietojärjestelmän häirintä ja tietoliikenteen häirintä edellyttävät tuhotyöhön verrattuna erityistä tahallisuutta tai tekotapaa ja voivat tulla sovellettavaksi tuhotyön sijasta, vaikka vakavaa vaaraa olisi aiheutunutkin. Tuhotyön säännöstä voidaan soveltaa tilanteissa, joissa erityinen tahallisuus ja tekotapa eivät täyty, mutta kuitenkin aiheutetaan vakavaa vaaraa.[172]

Kuten aiemmin tutkielmassa on todettu, kyseiset säännökset soveltuvat kyberterrorismiin siinä mielessä, että esimerkiksi valtiot voivat harjoittaa kyberterrorismia välillisesti. Täten terrorismitoimen rahoittajana toimii valtio, jolloin terrorismilla on käytössä varallisuutta aivan eri mittakaavassa kuin, että kyseessä olisi yksittäinen tekijä tai ryhmittymä. Kyberhyökkäyksiin on tänä päivänä liittynyt paljon valtioiden intressien sisältämää poliittista sanomaa, jota on esimerkin tavoin esitelty tarkemmin tutkimuksessa. Kyberympäristön tarjoaman anonymiteetin ansiosta hyökkäysten todellisia tekijöitä ei kaikissa tapauksissa ole mahdollista edes selvittää.

4.3.7 Matkustaminen terrorismirikoksen tekemistä varten

”Joka matkustaa toiseen valtioon tehdäkseen siellä 1 §:ssä –– tarkoitetun rikoksen, on tuomittava, jollei teko ole jonkin mainitun pykälän mukaan rangaistava, matkustamisesta terrorismirikoksen tekemistä varten sakkoon tai vankeuteen –– (RL 34a luku 5 c §).”

Matkustamista koskeva kriminalisointi liittyy vierastaistelijoiden ongelmaan, jossa konfliktialueille siirrytään osallistumaan koulutukseen tai muuhun toimintaan. Matkustamisen voidaan kat-

[171] HE 232/2014 s. 23
[172] HE 232/2014 vp, s. 25.

soa olevan eräänlainen valmistelutoimi, joka ei ollut ennen tämän säännöksen voimaan astumista rangaistavaa ja joihin viranomaisilla ei ollut mahdollisuutta puuttua.[173] Toisaalta taas hallituksen esityksessä (30/2018) on todettu, että matkustaminen koskee kaikkia matkustamistilanteita, myös niitä tilanteita, joissa Suomeen matkustavat terroristisessa tarkoituksessa saatetaan rangaistusvastuun piiriin.[174]

Mielenkiintoista tutkimusaiheen kannalta on, mistä syystä matkustamisen säännökseen on liitetty myös tietoverkkorikollisuuteen liittyvä kriminalisointi. Kyberympäristö tarjoaa rajattomat mahdollisuudet kyberterrorismin harjoittamiseen maailmanlaajuisesti, joten konkreettinen matkustaminen ei kaikissa tapauksissa ole välttämätöntä. Lain esitöistä ei suoranaista vastausta kysymykseen löydy, mutta sääntelyä voitaisiin soveltaa tutkimuksessa aiemmin mainittuihin merenpohjassa kulkeviin tietoliikennekaapeleihin. Näihin tietoliikennekaapeleihin kohdistuva hyökkäys voidaan tutkielmassa esitetyn tiedon valossa nähdä kyberhyökkäyksenä. Hyökkäys voidaan toteuttaa siten, että kaapelit fyysisesti katkaistaan, jolloin tekijän tulisi matkustaa kaapeleiden luokse. Vaihtoehtoisesti matkustaminen voisi tulla kyseeseen muissa tilanteissa, joissa kyberiskun toteuttaminen vaatisi henkilön matkustamista lähemmäksi kohdetta.

[173] Lappi-Seppälä ym. 2009, s. 1180 (kirjailija päivittänyt tekstin 7.12.2021).
[174] HE 30/2018 vp, s. 55.

5 RIKOSLAIN 34 a LUVUN SOVELLETTAVUUDEN ARVIOINTI KYBERTERRORISMISSA

5.1 Yleistä lain soveltamisesta kansainvälisissä rikoksissa

Ylikansallinen rikosoikeus on järjestelmä, joka on olemassa kansallisen järjestelmän rinnalla tai sen yläpuolella, jonka rikos- ja rangaistussäännökset ovat suoraan sovellettavissa kaikissa jäsenvaltioissa. Nämä ylikansalliset säännökset tulevat sovellettavaksi suoraan jäsenvaltioiden tuomioistuimissa. EU-rikosoikeus on luonnehdittavissa ylikansalliseksi rikosoikeudeksi, mutta mitään suoraa sovellettavaa EU-rikoslakia ei tällä hetkellä ole olemassa. Asetukset ja direktiivit ovat rikosoikeuden kannalta tärkeimmät sekundäärioikeudelliset instrumentit. Asetuksia voidaan suoraan soveltaa, mutta direktiivien soveltaminen edellyttää aina implementoinnin kansalliseen lainsäädäntöön. Direktiivi velvoittaa jokaista jäsenvaltiota toteuttamaan saavutettavaan tulokseen nähden tarvittavat toimet, mutta harkintavara direktiivin voimaansaattamisessa, muodoissa ja keinoissa on kansallisella lainsäätäjällä. Direktiivit myös helpottavat ja tehostavat jäsenvaltioiden välistä rikosprosessuaalista yhteistyötä sekä lähentävät jäsenvaltioiden lainsäädäntöä. Terrorismi on yksi näistä rikostyypeistä, johon kriminalisointien lähentäminen EU:ssa kohdistuu.[175]

Kansainväliset sopimukset eivät ole suoraan sovellettavia, vaan ne tulee implementoida kansalliseen lainsäädäntöön saadakseen rikosoikeudellisen vaikutuksen. Sopimusten tarkoituksena on tunnusmerkistöjen yhdenmukaistaminen sekä yhteisten keinojen ottaminen käyttöön rikostyyppien torjumiseksi. Sopimukset koskevat rajat ylittäviä rikoksia, kuten terrorismia (RL 34a) ja rikokset käsitellään kansallisissa tuomioistuimissa.[176]

Ensinnäkin, jotta voidaan ottaa kantaa tietyn teon rangaistavuuteen, tulee ensin varmistaa asianomaisen valtion rikosoikeuden sovellettavuus kyseisessä teossa. Rikosoikeudellinen toimivalta

[175] Korkka-Knuts – Helenius – Frände 2020, s. 32.
[176] Korkka-Knuts – Helenius – Frände 2020, s. 38.

on lähtökohtaisesti jokaisella valtiolla omalla alueellaan. Valtiot voivat ulottaa rikosoikeudellisen toimivaltansa myös ulkomailla tehtyihin rikoksiin, mutta teon ja toimivaltaa harjoittavan valtion välillä on oltava hyväksyttävä liittymä. Tällainen vaadittava liittymä ilmaistaan rikosoikeuden toimivaltasäännöissä rikoslain 1 luvun 1 §:ssä.[177]

Valtiosuojeluperiaatteen (RL 1:3) mukaan rikoslakia voidaan soveltaa Suomeen kohdistuneisiin Suomen ulkopuolella tehtyihin rikoksiin.[178] Tällaisia rikoksia voitaisiin nähdä olevan kyberterrorismiin liittyvät rikokset, sillä kyse on rajat ylittävistä rikoksista. Säännöksen tarkoituksena on muodostaa ns. valtiollinen hätävarjeluoikeus eli oikeus puolustautua rikoksilta, jotka kohdistuvat valtioon tai sen intresseihin. Säännöksen mukaan ”rikoksen katsotaan kohdistuneen Suomeen, jos 1) kyseessä on maan- tai valtiopetosrikos 2) teolla on muutoin vakavasti loukattu tai vaarannettu Suomen valtiollisia, sotilaallisia tai taloudellisia oikeuksia tai etuuksia 3) teko on kohdistunut Suomen viranomaiseen”.[179]

Lakitekstiä tulkittaessa apuna käytetään oikeuslähteitä niiden etusijajärjestyksen mukaisesti. Velvoittavuuden osalta oikeuslähteet voidaan jakaa kahteen ryhmään eli velvoittaviin ja sallittuihin lähteisiin. Velvoittavat oikeuslähteet ovat lähtökohtaisesti sovellettavia ja niihin luetaan lain kotimaiset esityöt sekä korkeimman oikeuden ratkaisukäytännöt. Lisäksi EU-oikeuteen kuuluvat direktiivit ja puitepäätökset ovat esitöihin verrattavia velvoittavia lähteitä, jotka implementoidaan Suomen lainsäädäntöön. Implementointilainsäädäntöä tulkittaessa tulee ottaa huomioon kotimaisen lainsäädännön taustalla olevat EU-säädökset, eikä suomalainen rikosoikeus voi olla ristiriidassa EU-oikeuden kanssa. Tulkinnassa voidaan käyttää apuna myös EU-tuomioistuimen ja EIT:n yksittäisiä tuomioita. [180]

[177] Korkka-Knuts – Helenius – Frände 2020, s. 28–29.
[178] Korkka-Knuts – Helenius – Frände 2020, s. 434.
[179] Korkka-Knuts – Helenius – Frände 2020, s. 434.
[180] Korkka-Knuts – Helenius – Frände 2020, s. 75.

Lainsäädännön tulkinnassa muiden lähteiden käyttö on sallittua eikä niiden käyttämättä jättämistä tarvitse perustella. Rikostunnusmerkistön sisältämä kriminalisointi eli tulkinnan kohteeseen liittyvä muu lainsäädäntö, siihen liittyvät esityöt ja oikeuskäytäntö, jäävät velvoittavien ja sallittujen oikeuslähteiden välimaastoon. Rikosoikeuden ulkopuolinen lainsäädäntö auttaa toisinaan tietyin rajoituksin tunnusmerkistön tulkitsemisessa ja siinä miten samankaltaiset tilanteet on muualla lainsäädännössä säännelty. [181]

Rikosoikeudellisen tulkinnan tavoitteena on antaa lakitekstille objektiivisesti perusteltu merkityssisältö, vaikka tulkinta on väistämättä myös subjektiivista. Laillisuusperiaate ja tulkintalähteet sekä lainopin metodiset suositukset ohjaavat rikosoikeudellista tulkintaa. Käytännössä yksittäisessä soveltamistilanteessa on kuitenkin kyse siitä, miten kukin lainsoveltaja ryhmittelee asioita ja mieltää käsillä olevia tilanteita. Lainkäyttäjän oikeudenmukaisuuskäsitys vaikuttaa näihin soveltamistilanteisiin.[182]

Laillisuusperiaatteesta säädetään perustuslain 2 luvun 8 §:ssä (731/1999, PL) ja se toimii rikosoikeudellisen oikeuslähdeopin tukirankana, jonka mukaan rangaistukseen voidaan tuomita vain teosta, joka on laissa säädetty rangaistavaksi (nulla poena sine lege). Täten PL 2:8 nojalla ”ketään ei saa pitää syyllisenä rikokseen eikä tuomita rangaistukseen sellaisen teon perusteella, jota ei tekohetkellä ole laissa säädetty rangaistavaksi”. Lisäksi RL 3:1.1 mukaan ”rikokseen syylliseksi saa katsoa vain sellaisen teon perusteella, joka tekohetkellä on laissa nimenomaan säädetty rangaistavaksi”. Kiellettyä on siten perustaa rangaistusvastuuta tekoon, josta laissa ei säädetä ja tästä johtuu kirjoitetun lain vaatimus.[183]

[181] Korkka-Knuts – Helenius – Frände 2020, s. 75.
[182] Korkka-Knuts – Helenius – Frände 2020, s. 42.
[183] Korkka-Knuts – Helenius – Frände 2020, s. 44–46.

5.2 Sovellettavuuden arviointi kyberhyökkäyksissä

5.2.1 Palvelunestohyökkäys terroristisessa tarkoituksessa

Tässä kappaleessa on tarkoitus selvittää, voidaanko kyberhyökkäystä pitää rikoslain 34 a luvun mukaisena terroritekona. Kysymystä tulee tutkimuksen kannalta lähestyä tyypillisimpien kyberhyökkäysten kautta, jotka kohdistuvat yhteiskunnan kriittiseen infrastruktuuriin tai muuhun vastaavaan elintärkeään toimintoon. Tyypillisimpinä tekoina pidetään tässä tarkastelussa palvelunestohyökkäyksiä ja haittaohjelmia.

Tyypillisin kyberhyökkäyksen toimintamalli on palvelunestohyökkäys, joka kohdistuu internetsivuja välittävään palvelimeen. Palvelunestohyökkäyksessä palvelin ylikuormitetaan yhdellä kohdistetulla komennolla, jolloin palvelimelle lähetetään lukuisia palvelinpyyntöjä.[184] Käytännössä tällä tarkoitetaan samaa asiaa kuin, että suuri joukko yksittäisiä ihmisiä vierailisi samanaikaisesti jollakin palvelimella, kuten esimerkiksi konserttilippujen sivustoilla. Sivujen runsas samanaikainen käyttö aiheuttaa palvelimen kaatumisen toimintakapasiteetin ylittyessä. Tällainen sivujen samanaikainen käyttö ei ole rangaistavaa toisin kuin palveluestohyökkäyksessä, jossa sivut kuormitetaan tarkoituksella. Suomessa vastikään kohdistettiin palvelunestohyökkäys ulkoministeriön, puolustusministeriön ja valtioneuvoston verkkosivuille, joka esti sivustoille pääsyn kokonaan[185]. Tämä puolestaan oli tahallinen ja siten rangaistava teko.

Palvelunestohyökkäys on laaja tekokokonaisuus, jossa tunkeudutaan tietojärjestelmiin, käytetään tietojärjestelmien resursseja oikeudettomasti tai hankitaan, levitetään tai käytetään haittaohjelmia[186]. Tapausten tarkempi lainopillinen analyysi edellyttäisi tapauskohtaista tietoa hyök-

[184] Jansson – Sihvonen 2018, s. 10.
[185] Helsingin Sanomat 8.4.2022. Valtion verkkosivut joutuivat verkkohyökkäyksen kohteeksi – Ulkoministeriö tekee asiasta rikosilmoituksen, [https://www.hs.fi/kotimaa/art-2000008738855.html]
[186] Nevalainen 2019, s. 144.

käyksen kohteena olevasta tietojärjestelmästä ja tosiasiallisista seurauksista, sillä palvelusestohyökkäyksiin voivat soveltua useatkin rikossäännökset.[187] Tarkastelu tässä kohdin rajataan koskemaan aktiivista hyökkäysvaihetta, jolloin tavallisesti sovellettaisiin RL 38:6 ja RL 38:7b. Tekoon lisätään terroristinen tarkoitus ja vakavan vahingon aiheuttaminen, jolloin tarkastellaan RL 34 a luvun sovellettavuutta.

Rikoslain 34a:1.1,4 kohdassa säädetään törkeästä tietojärjestelmän häirinnästä (RL 38:7b). Säännös kattaa myös palvelunestohyökkäyksen (Denial of Service, DoS), jolla tahallisesti ylikuormitetaan tietojärjestelmä estäen sen toiminta tai aiheuttaen sille haittaa. Kvalifiointiperusteina on mainittu tuntuva tai taloudellinen haitta. Tuntuvalla haitalla tarkoitetaan muuta haittaa kuin rahassa mitattavaa vahingollista vaikutusta, kun taas taloudellisella vahingolla tarkoitetaan rahassa mitattavia vaikutuksia tietojärjestelmän haltijalle. Lisäksi teko voi kohdistua tietojärjestelmään, jolla vaarannettaisiin energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun yhteiskunnan tärkeän toiminnon. Yhteiskunnan tärkeinä toimintoina voidaan pitää hyödykkeitä, järjestelmiä tai niiden osia, jotka ovat keskeisiä yhteiskunnan välttämättömien toimintojen ylläpitäjiä kuten esimerkiksi energialaitokset, liikenneverkot tai julkiset verkot. Näiden toimintojen vahingoittaminen voisi johtaa tilanteeseen, jossa toimintoja ei pystytä ylläpitämään.[188]

Jotta teko voitaisiin katsoa terroristisessa tarkoituksessa tehdyksi rikokseksi, edellytetään kahden kvalifikaation täyttymistä. Ensinnäkin rikoksentekijällä on tullut olla tekohetkellä terroristinen tarkoitus (RL 34a:6), ja toiseksi teon tulisi olla omiaan aiheuttamaan vakavaa vahinkoa jollekin maalle tai kansanväliselle järjestölle (RL 34a:1.1)[189]. Lisäksi terroristisessa teossa kysymys on korotetusta tahallisuusvaatimuksesta, joka ylittää normaalin tahallisuuden ja tahallisuusvaatimus koskee vain RL 34a:1:ssä tehtyjä rikoksia.[190]

---

[187] Nevalainen 2019, s. 144.
[188] HE 232/2014 vp, s. 23.
[189] Ks tarkemmin tämän tutkielman luku 4.3.1, jossa terroristisesta tarkoituksesta ja abstraktisesta vaarantamisrikoksesta.
[190] Melander 2015, s. 420.

Palvelunestohyökkäysten voidaan katsoa kuuluvan RL 34a:1.1,4 soveltamisen piiriin, mikäli teko on tehty terroristisessa tarkoituksessa, teko on ollut omiaan aiheuttamaan vakavaa vahinkoa, tekomuoto on ollut törkeä, teko on tehty tahallisena ja tietokonejärjestelmän käyttöä on vaikeutettu käyttämällä ohjelmakäskyjen sarjaa, joka on suunniteltu vahingoittamaan tietojärjestelmän toimintaa.[191] Hallituksen esityksen mukaan palvelunestohyökkäys on rangaistavaa RL 38:7b mukaisesti[192], joten lisäämällä tekoon terroristinen tarkoitus, vakavan vahingon aiheuttaminen ja törkeä tekomuoto olisi teko siten rangaistavaa RL 34a:1.1,4 mukaisesti.

Jotta palvelunestohyökkäyksessä rikoksen tekijällä olisi terroristinen tarkoitus, tulisi teon rikoslain 34 a luvun 6 §:n mukaisesti esimerkiksi aiheuttaa vakavaa pelkoa väestön keskuudessa. Hallituksen esityksen (188/2002) mukaan vakavalla pelolla tarkoitetaan väestön keskuudessa syntyvää perusteltua vakavaa pelkoa siitä, että henki, terveys tai vapaus ovat vaarassa.[193] Mikäli palvelunestohyökkäys kohdistettaisiin voimalaitokseen, eikä elämisen kannalta välttämättömiä toimintoja kuten asuntojen lämmitystä kyetä ylläpitämään, voisi aiheutua perusteltua pelkoa siitä, että henki ja terveys ovat vaarassa.

Toisaalta vakavalla pelolla voidaan myös tarkoittaa väestön keskuudessa syntyvää perusteltua vakavaa pelkoa siitä, että yksityisistä eduista esimerkiksi omaisuus on vaarassa.[194] Hallituksen esityksessä ei ole tarkemmin mainittu mitä tässä kohdin tarkoitetaan omaisuuden vaarantumisella. Mikäli omaisuuden vaarantumiseen liittyvä teko olisi palvelunestohyökkäys kohdistettuna talousjärjestelmään, joka keskeyttäisi verkkopankkien toiminnan sekä maksunvälityksen ja aiheuttaisi väestössä pelkoa omaisuuden vaarantumisesta, niin kyseessä voisi olla terroristinen teko.

Ongelmallista sovellettavuuden osalta on, kuinka mitata oikeudellisesti niinkin abstraktia käsitettä kuin pelko. Voidaanko ajatella palvelunestohyökkäyksen keston lisäävän väestössä pelkoa,

---

[191] ks. Paasonen – Aaltonen – Luomala 2021, s. 974 jossa palvelunestohyökkäysten katsottu kuuluvan RL 38:5–7 säädösten piiriin.
[192] HE 232/2014 vp, s. 21.
[193] HE 188/2002, s. 58-59.
[194] HE 188/2002 vp, s. 58–59.

jos kansalaisten kyky asioida ruokakaupassa estyy pidemmäksi aikaa tai asuntojen lämmitys ei palaudu kohtuullisessa ajassa? Milloin palvelunestohyökkäyksissä pelko ylittää terrorismirikoksen kynnyksen? Lisäksi kysymykseen tulee kuinka moneen henkilöön pelon tulisi ulottua, jotta se täyttäisi lain edellyttämän määritelmän? Määritelmän mukaan ”aiheuttaa pelkoa väestön keskuudessa” viittaisi väestön määritelmän mukaan alueella (koko maa, lääni, kunta) asuvaan väestöön[195]. Hallituksen esityksessä (188/2002) on todettu, että tapauskohtaisesti tulee harkittavaksi kuinka yleistä pelon tulisi olla väestön keskuudessa, jotta kyseessä voitaisiin katsoa olevan väestön keskuudessa syntyvä perusteltu vakava pelko[196].

5.2.2 Haittaohjelmien käyttö terroristisessa tarkoituksessa

Toinen tyypillinen kyberhyökkäyksen muoto on erilaiset haittaohjelmat, joita voidaan kohdistaa yhteiskunnan elintärkeään infrastruktuuriin. Haittaohjelma on käsitteenä määrittelemätön, mutta voidaan yleisesti mieltää kaiken tyyppisten kyberrikosten työkaluksi. Haittaohjelmilla pyritään häiritsemään tietojärjestelmän toimintaa, hankkimaan luottamuksellista tietoa ja vahingoittamaan tai muokkaamaan dataa.[197] Ulkomaisessa kielenkäytössä haittaohjelman sijaan käytetään yleistermiä ”virus”, jolla tarkoitetaan kaikkia vahingollisia ja haitallisia ohjelmia. Tällaisille haittaohjelmille on ominaista, että ne tarvitsevat isännäkseen toisen ohjelman eivätkä siten kykene toimimaan itsenäisesti. Leviäminen tietokoneessa ohjelmasta toiseen ja tietoverkon välityksellä tapahtuu itsestään eikä käyttäjän toimia siten tarvita.[198]

Haittaohjelmisto on siitä erikoinen, ettei se vaadi käyttäjältään kovinkaan vaativia taitoja, vaan taidot on sisällytetty ohjelmaan ja sitä voidaan jakaa laajamittaisesti. Tilannetta voidaan hahmottaa fyysiseen maailmaan siten, että maailman paras murtovaras jakaisi välineen, jolla keskinker-

---

[195] Tilastokeskus, Käsitteet – Väestö, [https://www.stat.fi/meta/kas/vaesto.html]
[196] HE 188/2002, s. 59.
[197] Nevalainen 2019, s. 144.
[198] Pihlajamäki 2004, s. 224–226.

tainen varas voisi murtautua haluamaansa paikkaan. Tämän ymmärtäminen hahmottaa haittaohjelman vaarallisuutta ja tieto siitä, että kyseisiä välineitä jaetaan Internetissä kaiken aikaa, luo huolta turvallisuudesta.[199]

Rikoslain 34a:1.1,4 kohdassa säädetään törkeästä tietoliikenteen häirinnästä, joka sisältää haittaohjelman määritelmän; ”jossa tietoliikennehäirinnässä rikos tehdään osana toimintaa, jossa on vaikeutettu merkittävään määrään tietojärjestelmiä käyttäen sellaisen laitteen tai tietokonehaittaohjelman taikka ohjelmakäskyjen sarjaa, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa – – (RL 38:6.1,3)”. Viruksista säädetään myös rikoslain 34 luvussa yleisvaarallisissa rikoksissa, sillä virukselle ominaista on sen sattumanvarainen ja toisaalta hallitsematon leviäminen, eikä levittäjä itsekään tiedä minne virus lopulta päätyy. Yleensä viruksella ei tähdätä tietyn tietokoneen tai tietyllä tietovälineellä olevan informaation vahingoittamiseen ja täten on yleistä vaaraa aiheuttava rikos.[200]

Haittaohjelmaa voidaan rikosoikeudellisesti tarkastella määritelmän ja käytön perusteella, mutta tässä kohdin haittaohjelmaa tarkastellaan kyberrikosvälineenä, jolloin keskeisimmät sääntelyt olisivat vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a) ja tietoverkkorikosvälineen hallussapito (RL 34:9b).[201] Mikäli kriminalisoinnin keskiössä on väline, kuvataan sitä rikossäännöksen tunnusmerkistössä käsitteiden laite, tietokoneohjelma ja ohjelmakäsky avulla. Rangaistavuuden alat ovat kuitenkin laajoja ja niihin kuuluvat erilaiset kyberrikosvälineet riippumatta objektiivisesta käyttötarkoituksesta, joten ne kattavat myös ns. kaksikäyttöiset välineet, jos niitä käytetään rikossäännösten edellyttämässä haittaamis- ja vahingoittamistarkoituksessa.[202]

Rikoslain 34a:2.1,2 ja 3 kohdassa säädetään vaarallisten esineiden ja lähinnä aseiden hankkimisesta, valmistuksesta tai hallussapidosta. Rikoslain 34 a luvussa ei ole erikseen säädetty terroristisessa tarkoituksessa käytettävien muiden välineiden kriminalisoinnista, johon haittaohjelman

[199] Schneier 2020, s. 41.
[200] Pihlajamäki 2004, s. 228.
[201] Nevalainen 2019, s. 145.
[202] Nevalainen 2019, s. 145.

voitaisiin katsoa sisältyvän. Sen sijaan RL 34a:1.1,4 kohtaan on sisällytetty RL 38:6.1,3,5 ja 6 kohta, joiden mukaan kyse on törkeästä tietoliikenteen häirinnästä, jos rikos tehdään käyttäen tietokonehaittaohjelmaa vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa. Toisaalta säännöksessä ei säädetä haittaohjelman hallussapidosta ja täten haittaohjelman hallussapito terroristiseen tarkoitukseen ja vaaran aiheuttamiseen ei olisi rikoslain 34 a luvun mukaisesti rangaistavaa. Perusmuotoisesta tietoverkkorikosvälineen hallussapidosta säädetään erikseen RL 34:9b:ssä.

Haittaohjelman käytössä rikoslain 34 a luvun sovellettavuuden osalta tulee myös arvioitavaksi tämän tutkielman aiemmassa kappaleessa (4.3.1) käydyt kvalifikaatioiden perusteiden täyttyminen terroristisesta tarkoituksesta ja, että teko on ollut omiaan aiheuttamaan vakavaa vahinkoa. Mikäli nämä edellytykset täyttyvät, tulee rikoslain 34 a luku sovellettavaksi.

5.3 Sovellettavuuden arviointi kybervaikuttamisessa

Kybervaikuttaminen on merkittävä osa kyberterrorismia, jossa digitaalista toimintaympäristöä käytetään hyväksi erilaisin keinoin, motiivein ja tarkoitusperin. Edellä käsiteltyä kyberhyökkäystä voidaan käyttää vaikuttamisen eri keinona, jolloin kybervaikuttamista pyrittiin mahdollisesti tekemään palvelunestohyökkäyksenä, joka kohdistettiin ulkoministeriön, puolustusministeriön ja valtioneuvoston verkkosivuille, joka esti kokonaan sivustoille pääsyn. Hyökkäyksen ajankohta oli osuva, sillä samoihin aikoihin Ukrainan presidentin oli määrä puhua Suomen eduskunnalle.[203] Ajankohdan optimoinnilla voidaan tämän esimerkin valossa katsoa olevan merkitystä vaikuttamisen kannalta, sillä palvelunestohyökkäys sivustoille muuna ajankohtana ei välttämättä olisi yhtä merkittävää vaikuttamista. Nyt mahdollisena motiivina oli tehdä poliittista vaikuttamista Suomeen varsinkin, kun päätös Nato-jäsenyydestä on edelleen avoinna. Tarkasteltavaksi tuleekin, voidaanko edellä esitettyä kybervaikuttamisen keinoa pitää rangaistavana tekona rikoslain 34 a luvun nojalla.

[203] Ilta-Sanomat 8.4.2022. Ulkoministeri Haavisto arvioi: hyökkäys ministeriöiden sivuille oli muistutus Venäjältä. [https://www.is.fi/politiikka/art-2000008740577.html]

Edellä esitetyssä kappaleessa on käsitelty rikoslain 34 a luvun soveltuvuutta palvelunestohyökkäykseen, joten tarkastelu tässä kohdin keskitetään pelkästään kybervaikuttamiseen. Edellä mainittu esimerkkitapaus Suomeen kohdistuneesta palvelunestohyökkäyksestä tulisi rangaistavaksi RL 38 luvun palvelunestohyökkäyksen osalta, mutta vaikuttamisen rangaistavuutta tulee tarkastella erikseen. Lähtökohtaisesti vaikuttamisen tavoitteena on aiheuttaa valitulle kohteelle painetta, vahinkoa, epävarmuutta ja epävakautta[204]. Tarkoituksena on vaikuttaa valtiolliseen päätöksentekoon esimerkiksi järjestäytyneen rikollisuuden soluttautumisella valtiohallinnon merkittäviin virkoihin ja sitä kautta altistamalla valtiota korruptiolle[205]. Tiedustelulainsäädännön myötä järjestäytyneen rikollisuuden soluttautumisen torjumiseksi on mahdollista kohdistaa tiedustelutoimia (PolL 5a:3,11 ja TtStL 3 § 11).

Rikoslain 34 a luvun 6 §:n määritelmän mukaan ”rikoksentekijällä on terroristinen tarkoitus, jos hänen tarkoituksenaan on pakottaa oikeudettomasti jonkin valtion hallitus tai muu viranomainen taikka kansainvälinen järjestö tekemään, sietämään tai tekemättä jättämään jotakin ––”. Käytännössä tämä soveltuisi kybervaikuttamiseen liittyviin rikoksiin, mutta varsinainen teko edellyttäisi, että teko olisi omiaan aiheuttamaan vakavaa vahinkoa. Ei siis riitä, että tekijällä on ollut terroristinen tarkoitus, vaan myös tahallisuuden tulee ulottua abstraktiin vaarantamiseen.[206] Vaikuttamiseen liittyvä teko saattaa kytkeytyä jonkin muun rikoksen yhteyteen kuten esimerkiksi kyberhyökkäykseen, jolloin RL 34a:6.1,2 kohta tulisi sovellettavaksi. Kybervaikuttamista on mahdollista tämän tutkielman mukaan toteuttaa kiristyshaittaohjelmien kautta[207], jolloin kiristys toimii vaikutuskeinona yhteiskunnan avainhenkilöön.

Demokratian kannalta uudet haasteet kohdistuvat kansainväliseen disinformaatioon ja epäasialliseen vaaleihin kohdistuvaan häirintään. Laittomin tietomurroin voidaan vaalitulosta manipuloi-

---

[204] Lohse – Viitanen 2019, s. 226.
[205] Lohse – Meriniemi – Honkanen 2019, s. 49.
[206] HE 188/2002 vp, s.33.
[207] ks. tarkemmin tutkielman kappale 2.4 kybervaikuttamisesta.

malla, heikentämällä vaalien luottamusta tai muilla tavoin pyrkiä vaikuttamaan kansalaisten äänestyskäyttäytymiseen.[208] Toisinaan rikoksen kohde asettaa rikoslain sovellettavuudelle rajoituksia tarkoittaen sitä, että niiden soveltamiseen vaaditaan erityinen liittymä Suomeen. Vaalirikos (RL 14:1) ja vaalituloksen vääristäminen (RL 14:4) edellyttävät, että kyseessä on Suomen lainsäädännön mukainen vaali eikä täten rikoslaki sovellu esimerkiksi Saksaan kohdistuviin vaalirikoksiin.[209] Kybervaikuttaminen vaaleissa ei edellä mainittujen pykälien tunnusmerkistöjen osalta tule sovellettavaksi, sillä rikoslain 14 luvun 1 §:ssä kyse on väkivallalla tai uhkauksella vaikuttamista äänestämiseen.

Sen sijaan, mikäli kybervaikuttamisessa on toteutettu tietomurto, voi rikoslain 34 a luku tulla sovellettavaksi sillä RL 34a:1.1,4 mukaan tietojärjestelmän murto terroristisessa tarkoituksessa on rangaistavaa. Sen sijaan varsinainen vaikuttaminen jää kuitenkin tämän säännöksen ulkopuolelle ja teko on rangaistavaa vain tietomurron osalta. Kootusti voidaan todeta, ettei kybervaikuttaminen ilman edeltävää kriminalisoitua tekoa ole rikoslain mukaan rangaistavaa. Suomessa on tällä vireillä lakiuudistus liittyen hybridivaikuttamiseen[210]. Kyseisen lainsäädännön muutoksen myötä hybridivaikuttamiselle saadaan mahdollisesti määritelmä ja sitä kautta myös rangaistussäännös, joka auttaa tulkitsemaan myös kybervaikuttamiseen liittyviä tilanteita.

5.4 Värväys kyberterrorismiin

Värväys voidaan nähdä yhtenä merkittävänä osana kyberterrorismia, joka on otettu huomioon myös terrorismilain uudistuksessa vuonna 2018 ja värväyksestä säädetään rikoslain 34 a luvun 4 c §:ssä. Uudistus on ollut tarpeellinen, sillä kyberhyökkäyksiin värvätään väkeä verkossa. On esitetty, että Venäjän ja Ukrainan välisessä sodassa vuonna 2022 on havaittu hakkeriryhmien perustaneen yhteisiä digitaalisia kokoontumisalustoja, joihin haetaan hakkereita ja joissa on sittemmin ilmoitettu hyökkäysten kohteet. Myös Ukrainan valtio on liittoutunut hakkereiden kanssa ja

[208] Lohse – Meriniemi – Honkanen 2019, s. 46.
[209] Korkka-Knuts – Helenius – Frände 2020, s. 447.
[210] Sisäministeriö 2022, s. 1.

pyytänyt ukrainalaisia verkko-osaajia liittymään IT-armeijaan (IT Army of Ukraine), johon on sittemmin liittynyt myös lukuisia ulkomaalaisia. Asiantuntijoiden mukaan tilanne on todella poikkeuksellinen.[211]

Tapausta olisi syytä analysoida tarkemmin Suomen lainsäädännön valossa. Kysymykseen tuleekin, voidaanko edellä esitettyä hakkeriryhmiä ja niiden perustamista pitää terrorismin mukaisena värväämisenä (RL 34a:4c)? Vai toisaalta järjestäytyneen rikollisryhmän toimintaan osallistumisella ja sitä kautta värväämisellä (RL 17:1a)? Vai kuitenkin hyökkäysrikoksen valmisteluna (RL 11:4b)? Vai terrorismirikoksiin liittyvänä julkisena kehottamisena (34a:5e)? Kysymys on relevantti, kun mietitään mikä on ulkomaalaisten osallistujien rooli sotaa käyvien maiden välisessä konfliktissa ja muuttuuko tilanne, jos pyyntö osallistua kyberhyökkäyksiin tuleekin sotaa käyvän valtion taholta? Tutkielman tutkimuskysymyksen kannalta edellä esitettyä laajaa kysymystä on syytä rajata koskemaan tutkimuksen aihetta ja tarkastella teon tunnusmerkkejä pelkästään RL 34a:4c:n osalta.

Hallituksen esityksen (HE 188/2002) mukaan värvääminen voi tapahtua kahdenkeskeisesti tai laajamittaisemmin, perustamisvaiheessa tai myöhemmin. Värvääminen on toteutettu, kun kohde on liittynyt ryhmään. Pykälässä mainitulla edistämisellä tarkoitetaan myös sellaista edistämistä, jonka tarkoituksena on johtaa ko. rikoksen tekemiseen. Euroopan neuvoston (EN) yleissopimuksen 6 artiklan 1 kappaleen mukaan värväyksellä terrorismiin tarkoitetaan ”toisen henkilön taivuttamista tekemään terrorismirikos tai osallistumaan terrorismirikoksen tekoon taikka liittymään yhteenliittymään tai ryhmään tarkoituksella myötävaikuttaa siihen, että kyseinen yhteenliittymä tai ryhmä tekee yhden tai useamman terrorismirikoksen.”[212]

Rikoslain 34 a luvun 4 c §:n soveltamisalaan ei kuulu rekrytointiin liittymätön toiminta, joten terroristiryhmän perustamis- ja organisoimistoimet vaativat aktiivisuutta. Pelkästään kokouksiin osallistuminen tai mielipiteiden esittäminen eivät ole sellaisiksi teoiksi luokiteltavia. Värväystavat

---

[211] Yle uutiset. 3.3.2022 Ukrainan puolesta taistelee ennennäkemätön hakkeriarmeija, mukana suomalainen ”Jouni” – asiantuntijat varoittavat: ”tämä ei ole leikkisotaa”. [https://yle.fi/uutiset/3-12338836]
[212] HE 30/2018 vp, s. 40.

eivät ole aikarajoitteisia, joten perustamistoimet voivat olla hyvin pitkäkestoisia. Terroristikokelaita voidaan koota yhteen erilaisin ilmoituksin, kiertämällä tilaisuuksissa ja internetin välityksellä. Rekrytoinnin kannalta internet on tärkein värväämisen kanava, sillä kiinnijäämisriski on siellä olematon. Internet on rajaton, nopea ja halpa sekä lisäksi mahdollistaa käyttäjiensä anonymiteetin.[213]

Terrorismiyleissopimuksen 6 artiklan 1 kappaleen mukaan värväyksellä terrorismiin tarkoitetaan väen rekrytoimista tekemään, osallistumaan tai myötävaikuttamaan yhden tai useamman terrorismirikoksen tekemiseen. Rikoksen täyttyminen edellyttää, että värvääjä onnistuu luomaan kontaktin värvättävään. Ei siis edellytetä värväyksen kohteen osallistumista varsinaiseen terrorismirikoksen tekemiseen tai sen liittymistä ryhmään. Kontaktivaatimus täyttyy, kun värväyksen kohde ilmaisee myöntävän vastauksen tai antaa itsensä tulla rekrytoiduksi terroristiseen tekoon. Myös yritys on värväämisessä rangaistavaa, vaikka varsinainen teko ei ole saanut aikaan vaaraa rikoksen täyttymisestä.[214]

Edellä esitetyn tiedon valossa internetin kautta toteutettu hakkeriryhmän itse toteuttama värvääminen Venäjän vastaisiin toimiin voidaan nähdä terroristisena. Kybervapaaehtoisia on koottu Telegram-viestiryhmiin, joissa on suunniteltu kyberhyökkäyksiä Venäjää vastaan sodan ulkopuolisista valtioista. Ryhmän motiivi on selvästi ollut poliittinen, sillä tarkoituksena on ollut tukea Ukrainaa Venäjän hyökkäyssodassa. Kyberhyökkäysten kohteet, vakavuus ja vahingon aiheuttaminen määrittelee myös sen, onko kyse terrorismista. Mikäli kyberhyökkäyksiä suunnitellaan kohdistettavan kriittiseen infrastruktuuriin, teoilla on aiheutettu vakavaa vahinkoa ja teoilla on aiheutettu perusteltua pelkoa, voidaan puhua terrorismista.

Toisaalta tilanne voi muuttua, jos pyyntö ryhtyä kyseisiin toimiin esitetään sotaa käyvän maan toimesta. Tällöin voitaisiin puhua ennemminkin hyökkäysrikoksen valmistelusta (RL 11:4b). Hyökkäysrikoksen valmistelusta tietoverkkovälitteisesti eivät lain esityöt anna suoranaista vastausta.

---

[213] Lohse 2012, s. 164.
[214] Lohse 2012, s. 165.

Sen sijaan tapaukseen voitaisiin esimerkin valossa soveltaa tavallisen hyökkäysrikoksen valmistelun määritelmää. Hyökkäysrikoksen valmistelussa on hallituksen esityksen mukaan kyse salahanketyyppisen rikoksen valmistelun muodosta, jossa osapuolet laativat yksityiskohtaisen suunnitelman hyökkäysrikoksen tekemisestä.[215] Valtio siis lähettää asevoimiin kuulumattomia joukkoja suorittamaan toista valtiota vastaan asevoimiin verrattavia toimia.[216]

5.5 Julkinen kehottaminen kyberterrorismiin

Edellä esitettyä tapausta (IT-Army of Ukraine) on mahdollista tutkia myös terrorismirikoksiin liittyvän julkisen kehottamisen kautta (RL 34a:5e). ”Joka joukkotiedotusvälinettä käyttäen tai julkisesti väkijoukossa taikka yleisesti tietoon saatetussa kirjoituksessa tai muussa esityksessä kehottaa tai houkuttelee värväytymiseen terroristiryhmään tai tässä luvussa rangaistavaksi säädetyn rikoksen tekemiseen siten, että kehotus tai houkuttelu on omiaan aiheuttamaan värväytymisen tai terrorismirikoksen tekemisen, on tuomittava terrorismirikoksiin liittyvästä julkisesta kehottamisesta ––.”

Puitepäätöksen (2002/475/YOS) mukaan julkisella kehottamisella terrorismirikokseen tarkoitetaan ”sellaisen viestin levittämistä yleisölle tai muuta yleiseen tietoisuuteen saattamista, jonka tarkoituksena on yllyttää joku ihmishenkeen kohdistuvaan rikokseen, henkilön ruumiillista koskemattomuutta loukkaavaan törkeään rikokseen, ihmisryöstöön tai panttivangin ottamiseen. Toisaalta tarkoituksena on aiheuttaa hallinnollisille tai julkisille laitoksille, liikennejärjestelmille, infrastruktuureille (mukaan lukien atk-järjestelmät), mannerjalustalle sijaitsevalle kiinteälle lautalle, julkisille paikoille tai yksityiselle omaisuudelle suuria tuhoja, jotka voivat vaarantaa ihmishenkiä tai aiheuttaa huomattavia taloudellisia menetyksiä. Tarkoituksena on ilma-alusten tai muiden joukkoliikenne- tai tavarankuljetusvälineiden haltuunotto. Aseiden, räjähteiden, atomiaseiden sekä biologisten ja kemiallisten aseiden valmistus, hallussapito, hankinta, kuljetus, toimitus tai käyttö sekä biologisten ja kemiallisten aseiden osalta tutkimus ja kehittäminen. Vaarallisten aineiden vapauttaminen taikka tulipalojen, tulvien tai räjähdysten aiheuttaminen siten, että

[215] HE 289/2014, vp s. 29.
[216] HE 289/2014, vp s. 17.

ihmishenkiä saatetaan vaaraan. Veden- tai sähkövoiman jakelun tai muun perusluonnonvaran toimittamisen häirintä tai keskeytys siten, että ihmishenkiä saatetaan vaaraan”.[217]

Täten edellä esitetty tapaus (IT Army of Ukraine) voidaan katsoa olevan rangaistavaa myös tämän säännöksen (RL 34a:5e) nojalla mikäli teon katsottaisiin olevan terroristista. Tapauksessa hakkereita kehotettiin tai houkuteltiin osallistumaan Telegram -viestisovelluksessa olevaan ryhmään, jossa annettiin lisäohjeita iskujen toteutuksia varten. Vahinkoa haluttiin aiheuttaa Venäjän Ukrainaan toteuttamassa hyökkäysoperaatiossa Venäjää vastaan. Hakkereiden toteuttamassa kyberoperaatiossa pyrittiin vaikeuttaman Venäjän etenemistä Ukrainassa pysäyttämällä Venäjän joukkoja liikuttava raideliikenne[218]. Tämän kaltaisessa kyberhyökkäyksessä ei aiheutettu vaaraa ihmishengille, eikä kyseessä olisi edellä kuvatun kaltainen teko. Toisaalta tapauksessa kysymykseen tulee, tulisiko tekoa arvioida sotaoikeudellisesta näkökulmasta. Ovatko hakkerit sodan osapuolia vierastaistelijoina vai onko kyseessä terrorismiin liittyvä teko? Tässä voisi olla tutkimuskysymys tämän tutkielman pohjalta tehtävään jatkotutkimukseen.

Kuten alussa on todettu, sotarikokset ja terrorismirikokset ovat toisiaan hyvin lähellä olevia ja osittain jopa päällekkäisiä rikoksia, joiden rajanveto ei ole niin yksiselitteistä. Ilmiöitä on mahdollista arvioida oikeudellisesti sekä sota- että terrorismirikoksina ja myös näiden sekoituksena.[219] Tästä syystä tapauksen analysoinnissa voitaisiin päästä useampaan eri lopputulemaan ja näkemykseen siitä, mitä terrorismilla tai sodankäynnillä kussakin tarkasteltavassa tapauksessa tarkoitetaan.

---

[217] kts. Puitepäätöksen 2002/475/YOS 1artikla 1 kohdan a-h alakohta.
[218] Talouselämä 28.2.2022. Venäjälle taas pettymyksiä – Hakkerit pysäyttelevät joukkoja liikuttavia junia matkalla rajalle. [https://www.talouselama.fi/uutiset/venajalle-taas-pettymyksiahakkerit-pysayttelevat-joukkoja-liikuttavia-junia-matkalla-rajalle/ad67a279-754a-4cb1-861e-8270f6fb875c]
[219] Esko 2017, s. 111–112.

6 KANSALLISEN LAINSÄÄDÄNNÖN KATTAVUUDEN ARVIOINTI KYBERTERRORISMISSA

6.1 Kyberterrorismin sääntelyn tasosta yleisesti

Lainsäädäntö kattaa tällä hetkellä tyypillisimpiä tietoverkkorikoksia, mutta sääntelyn tarkkarajaisuus jättää toisinaan joitain tekoja sen ulkopuolelle, joista edellä on käyty läpi esimerkkitapauksia. Tulevaisuus tulee näyttämään, minkälaiseksi ilmiöksi kyberterrorismi lainsäädännön näkökulmasta vielä kehittyy. Määritelmäkysymykset terrorismissa ja kyberterrorismissa luovat haasteita lain sovellettavuudelle ja myös lain kattavuuden arvioinnille. Epäyhteneväiset ja puutteelliset kansainväliset määritelmät aiheen ympärillä vaikeuttavat myös lainsäätäjän roolia, sillä lakiin ei voida kirjoittaa epätäsmällisiä kriminalisointeja.

Kyberrikosten ydinalueen muodostavat keskeisimmät ylikansalliset instrumentit kuten Euroopan tietoverkkorikollisuutta koskeva yleissopimus (ETS 185, SopS 59–60/2007, Budapestin sopimus) ja sen lisäpöytäkirja (ETS 189, SopS 83–84/2011) sekä Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä (2013/40/EU). Lisäksi niin kutsuttu ”kyberydin” koostuu kansallisesta rikoslainsäädännöstä tieto- ja viestintärikoksista (RL 38), yleisvaarallisista rikoksista (RL 34), datavahingontekorikoksista (RL 35), luvatonta käyttöä koskevista rikossäännöksistä (RL 28)[220] sekä terrorismirikoksista (RL 34a). Sovellettaviksi voivat edellä mainittujen lisäksi tulla myös perinteisemmät rikossäännökset, vaikka tunnusmerkistössä ei ole käytetty kyberiin liittyvää terminologiaa. Tämä osoittaa myös sitä, että kokonaisuus on hyvin hajanainen ja sisältää kriminalisointien osalta paljon päällekkäisyyttä.[221]

Melander on eduskunnan perustuslakivaliokunnalle antamassaan lausunnossa vuonna 2020 todennut Suomen terrorismirikoksia koskevan rikoslainsäädännön olevan monessa suhteessa

[220] Nevalainen 2019, s. 137.
[221] Nevalainen 2019, s. 137.

poikkeuksellinen kokonaisuus, sillä sääntely on huomattavan monimutkaista sisältäen vaikeaselkoisen määritelmäsäännöksen. Ongelmallista on myös se, että sääntelyä on useaan otteeseen laajennettu kattamaan tekoja, jotka ovat yhä etäämmällä oikeushyviä konkreettisesti loukkaavasta tai vaarantavasta toiminnasta. Rikoslain 34 a luvun laajentaminen ei tällaisenaan ole toivottavaa sääntelyn ennakoitavuuden ja selkeyden näkökulmasta. Valiokunta onkin todennut, että terrorismirikoksia koskevaa sääntelyn kokonaisuutta tulisi tarkastella ja pyrkiä yksinkertaistamaan. Nyt terrorismirikosten lisääntyminen rikoslain 34 a lukuun on johtanut tilanteeseen, jossa säännösten sisältämiä rangaistusasteikkojen suhdetta toisiinsa ei ole kokonaisvaltaisesti arvioitu.[222]

Edellä esitetyn perusteella terrorismirikosten kohdalla ei ole tarkoituksenmukaista, että rikoslain 34 a lukua päivitetään jatkuvasti ja jälkijättöisesti sitä mukaa, kun terrorismi kehittyy ja muuttuu. Toisaalta terrorismi-ilmiön monimuotoisuus saattaa johtaa siihen, että rikoslainsäädäntö ei pysy tämän ilmiön edellä, sillä tekojen toteutustavoissa ja muodoissa vain mielikuvitus on rajana. Tämän voidaan katsoa vaikeuttavan tekojen ennakoitavuutta. Terrorismirikoksista kyberterrorismi lisää ennestään vaikeaselkoiseen sääntelyyn määrittelemättömyytensä johdosta monitulkintaisuutta, joka haastaa lainsäätäjän kykyä pysyä lainsäädännöllisesti ilmiön vaatimalla tasolla.

6.2 Muun kansallisen lainsäädännön merkitys kyberterrorismissa

6.2.1 Tiedustelulainsäädäntö

Ennen vuotta 2019 Suomessa ei ollut tiedustelua koskevaa lainsäädäntöä. Lainsäädännön voidaan nähdä saaneen alkunsa valtioneuvoston vuonna 2013 antamasta periaatepäätöksestä Suomen kyberturvallisuusstrategiasta. Puolustusministeriön työryhmän tehtäväksi tuli arvioida, kuinka lainsäädäntöä tulisi kehittää, jotta Suomessa pystytään huolehtimaan kansallisesta turvallisuudesta tietoverkoissa esiintyvien uhkien torjumiseksi.[223]

---

[222] Melander 2020, s. 1–9.
[223] Lohse – Viitanen 2019, s. 20.

Valtioilla on puolustettavanaan turvallisuuteen ja kansainvälisiin suhteisiin liittyviä etuja. Varjeltavia ovat eritoten intressit, joihin kohdistuu sotilaallista tai muuta vakavaa uhkaa. Terrorismi on siitä haastava ilmiö, että sitä ei voida luokitella temaattiseksi tai alueelliseksi, sillä terrorismi ei rajoitu valtion rajoihin[224] ja tämä koskee erityisesti kyberterrorismia. Suomessa on lainsäädäntöä, joka mahdollistaa tiedon hankkimisen kaikesta sellaisesta toiminnasta, jonka tavoitteena on heikentää, keskeyttää tai tuhota yhteiskunnan elintärkeitä toimintoja. Näitä ovat poliisilain (872/2011, PoL) 5a luvun 3 §:n 1 ja 6 kohta, laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019, TtStL) 3 §:n 1 ja 6 kohta ja laki sotilastiedustelusta (590/2019, SotTiedL) 4 §:n 2 kohta. Kyseisiin säädöksiin ei ole erikseen lisätty vakavuuden kvalifikaatiota, sillä yhteiskunnan elintärkeitä toimintoja uhkaava toiminta on jo itsessään vakavaa.[225]

Tietoa voidaan hankkia suunnitelmista, tavoitteista ja iskujen toteuttamiskyvystä Suomea kohtaan (PolL 5a:3,1 ja TtStL 3,1). Lisäksi tietoa saadaan siitä ketkä kytkeytyvät terroristijärjestön ja terroristisen pienryhmän toimintaan ja myös millainen työn- tai roolijako eri maissa vaikuttavilla terroristisilla toimijoilla on.[226] Laittoman tiedustelutoiminnan torjumiseksi voidaan toteuttaa vastatiedustelua, jonka tarkoituksena on löytää tiedustelutoimintaa harjoittavat henkilöt, jotka toiminnallaan vakavasti uhkaavat kansallista turvallisuutta. Lisäksi tietoa saadaan vieraan valtion tiedustelun toimintaperiaatteista, tiedustelupalvelun lukuun toimivista henkilöistä ja tiedonhankintakeinoista ja -kohteista.[227]

Tiedonhankintaa voidaan tehdä haittaohjelmasta, jolla pyritään aiheuttamaan vahinkoa viranomaisten käyttämiin tietojärjestelmiin tai huoltovarmuutta vaarantavissa toiminnoissa, joissa vieraan valtion tarkoituksena on lamauttaa sähköverkko. Uhka yhteiskunnan kriittisiin toimintoihin voi muodostua myös laiminlyönnin seurauksena tai aktiivisen toiminnan sivuvaikutuksena.

---

[224] Lohse – Viitanen 2019, s. 97.
[225] Lohse – Meriniemi – Honkanen 2019, s. 75.
[226] Lohse – Meriniemi – Honkanen 2019, s. 31.
[227] Lohse – Meriniemi – Honkanen 2019, s. 35.

Tietoa olisikin syytä kerätä sekä aktiivisesta, että passiivisesta toiminnasta, jonka motiivina voidaan nähdä yhteiskunnan elintärkeiden toimintojen vaarantuminen.[228]

Tiedustelun tarkoituksena on suojata kansallista turvallisuutta ja täten ennakoida sekä selvittää kansalliseen turvallisuuteen kohdistuvia tietoturva- ja kyberuhkia.[229] Lisäksi tarkoituksena on hankkia ja käsitellä tietoa Suomeen kohdistuvasta sotilaallisesta tai muusta vieraan valtion toiminnasta, joka vakavasti uhkaa Suomen puolustusta tai yhteiskunnan elintärkeitä toimintoja.[230] Tiedustelulla voidaan täten saada tietoa esim. suunniteltavasta kyberterrorismihyökkäyksestä ja täten hyökkäys voidaan parhaimmassa tapauksessa estää kokonaan tai siihen osataan varautua ja tekijä on mahdollista selvittää. Tiedustelulainsäädäntö voidaankin nähdä yhtenä merkittävimmistä tekijöistä kyberterrorismin torjunnan kannalta.

6.2.2 Valmiuslainsäädäntö

Turvallisuudesta huolehtiminen on yksi julkisen vallan tärkeimmistä tehtävistä ja viranomaisen tuleekin huolehtia kaikista välittömistä uhkatilanteista sekä varautua ennalta erilaisiin kuvitteellisiin uhkiin. Teknologinen kehitys, verkottuminen ja teknisten järjestelmien riippuvuus ovat olleet vakavien häiriötilanteiden ja poikkeusolojen varautumisen lähtökohtia.[231] Kriisitilanteiden varautumisen kannalta Suomessa on olemassa valmiuslainsäädäntö, joka koostuu valmiuslaista (1080/1991) ja puolustustilalaista (1083/1991). Erityisen vakavissa kriisitilanteissa valmiuslain tarkoituksena on turvata väestön toimeentulo, maan talouselämä, ylläpitää oikeusjärjestystä, huolehtia perus- ja ihmisoikeuksista sekä turvata valtakunnan alueellinen koskemattomuus ja itsenäisyys.[232]

Valmiuslain säätämisvaiheessa vuonna 2005 on todettu, että terroriteko saattaa johtaa tilanteeseen, jolloin valmiuslaki tulisi sovellettavaksi. Poikkeusolojen tunnusmerkistö täyttyisi esimerkiksi

---

[228] Lohse – Meriniemi – Honkanen 2019, s. 76.
[229] Lohse – Viitanen 2019, s. 71.
[230] Lohse –Viitanen 2019, s. 247.
[231] Virtanen – Salmi ym. 2011, s. 3.
[232] Virtanen – Salmi ym. 2011, s. 6–7.

tilanteessa, jossa terroritekoa pidettäisiin Suomeen kohdistettuna aseellisena hyökkäyksenä tai suuronnettomuutena. Tällaisessa tapauksessa valmiuslaki tulisi sovellettavaksi.[233] Hallituksen esityksessä (3/2008 vp) on terrorismiin liittyvä valmiuslain käyttöönotto kirjattu samoin perustein. Aiemmin on todettu, että lainsäädännön lähtökohtana on ollut se, että terroritekoon varaudutaan normaaliolojen lainsäädännön toimivaltuuksin.[234]

Tällä hetkellä voimassa oleva valmiuslaki (2011/1552) ei vastaa nykypäivän uhkakuvia ja turvallisuusvaatimuksia. Valtioneuvosto on ilmoittanut, että valmiuslain kokonaisuudistus on käynnistetty loppuvuodesta 2021. Uudistuksen tarkoituksena on päivittää nykyinen vuonna 2012 voimaan tullut valmiuslaki vastaamaan nykypäivää[235]. Uudessa valmiuslaissa tullaan säätämään mm. hybridivaikuttamisesta, joka liittyy oleellisesti myös kybervaikuttamiseen. Hybridivaikuttamiseen liittyvä lakiuudistus tullaan todennäköisesti toteuttamaan erillisenä nopeutettuna menettelynä. Valmiuslain uudistusta on osittain todennäköisesti vauhdittanut valmiuslain soveltamiseen liittyneet ongelmat koronapandemian aikana.

Kriisitilanteissa aika on hyvin rajallista, eikä harkittua säädösvalmistelua tai lainsäädännön vaikutusten analyysia ole mahdollista toteuttaa ja tästä syystä valmiuslainsäädännön tulee olla hyvin ennakkopainotteista. Vastatakseen tarkoitusta kriisilainsäädännön tule olla huolella suunniteltu ja nopeasti viranomaisten käytettävissä, jolloin valmistelutyöt tulee ajoittaa normaalioloihin.[236] Kyberterrorismiin liittyvä hyökkäys voi mahdollisesti olla hyvinkin välitön ja nopeasti muuttuva, jolloin valmiuslailta vaaditaan ajantasaisuutta ja sovellettavuutta.

6.2.3 Pakotejärjestelmä

Euroopan unioniin ja sen jäsenvaltioihin on kohdistettu pahantahtoista kybertoimintaa viime vuosina ja joka tulee lisääntymään. Tästä syystä on ollut tarve tehostaa ennaltaehkäiseviä toimia

---

[233] Komiteanmietintö 2005:2, s. 45.
[234] Virtanen – Salmi ym. 2011, s. 62.
[235] Valtioneuvosto, Valmiuslain uudistaminen käynnistyy 8.12.2021, [https://valtioneuvosto.fi/-//1410853/valmiuslain-uudistaminen-kaynnistyy]
[236] Virtanen – Salmi ym. 2011, s. 9.

ja reagointivalmiutta. Neuvosto on hyväksynyt 19.6.2017 kyberdiplomatian välineistön (Joint EU Diplomatic Response to Malicious Cyber Activities), jolla pyritään estämään vihamielisen kybertoiminnan vahingot unionissa. Välineistöön kuuluu yhteisen ulko- ja turvallisuuspolitiikan alaan kuuluvia toimia ja rajoittavia toimenpiteitä kuten pakotteita.[237]

Kyberpakotejärjestelmällä voidaan mahdollistaa matkustusrajoituksia, varojen jäädytyksen kohdentamista henkilöihin tai yhteisöihin, jotka ovat vastuussa kyberhyökkäyksistä tai niiden edistämisestä. Pakotejärjestelmää ei ole maantieteellisesti rajattu eikä poliittiseen kontekstiin pakotettu, vaan rajoitteita voidaan asettaa riippumattomasti. Pakotejärjestelmän ensimmäinen pakotelistaus on tehty 2/2020, jossa Suomi on mukana. Listausehdotus kattaa usean maan kansalaisia ja yhteisöjä, joilla katsotaan olevan kykyjä vahingolliseen kybertoimintaan. Kyberpakotejärjestelmän pakotteet eivät ole suunnattu mitään tiettyä valtiota vastaan, vaan toimenpiteet kohdistuvat laittomuuksiin syyllistyneisiin henkilöihin tai yhteisöihin.[238]

Suomi tukee valmisteltuja listauksia ja katsoo tämän vahvistavan ennaltaehkäisevän kyberpelotteen ylläpitämistä. Tällaiset rajoittavat toimenpiteet ovat tehokas keino osoittaa konkreettisesti ja poliittisesti, että vihamielisellä kybertoiminnalla on seurauksia. Lisäksi pakotteiden tarkka kohdentaminen vähentää pakotteista mahdollisesti sivullisille aiheutuvia negatiivisia vaikutuksia.[239]

6.3 Rikoslain 34 a lukuun liittyvät muutosehdotukset

6.3.1 Kybervakoilu terroristisessa tarkoituksessa

Maailma käy tällä hetkellä globaalisti kyberasevarustelun kilpajuoksua, jonka odotetaan kiihtyvän merkittävästi tulevina vuosina. Valtiot resursoivat tällä hetkellä erilaisien kyberkyvykkyyksien kehittämiseen kuten esimerkiksi puolustukseen, tiedusteluun ja hyökkäykseen. Valtioiden välinen vakoilu on lisääntynyt ja siirtynyt kyberympäristöön. Suomessa vakoilun kohteeksi joutuvat mm.

---

[237] Ulkoministeriö, Perusmuistio UM2020-00783, s. 2.
[238] Ulkoministeriö, Perusmuistio UM2020-00783, s. 2.
[239] Ulkoministeriö, Perusmuistio UM2020-00783, s. 1.

valtionhallinto, poliittinen päätöksenteko ja teknologiayritykset. Kybervakoilu on vakava uhka suomalaiselle yhteiskunnalle sekä sen sisältämälle tietopääomalle. Vakoilun kiinnostuksen kohteet terroristisesta näkökulmasta liittyvät ulko- ja turvallisuuspolitiikkaan ja niiden sisältämiin salaisiin tietoihin. Kybervakoilua on mahdollista toteuttaa Suomen rajojen ulkopuolelta ja houkuttimena siinä on hyvin pieni kiinnijäämisen riski. Kehittyneimmät valtiot pystyvätkin hyödyntämään kybervakoilun erilaisia muotoja siten, ettei niitä kyetä aina edes havaitsemaan.[240]

Sisäministeriö on tietoverkkorikollisuuden torjuntaa koskevassa selvityksessä vuonna 2017 todennut havainnointikyvyn olevan Suomessa puutteellista[241]. Tätä lausuntoa tukee myös tapaus vuodelta 2013, jolloin Suomeen kohdistettiin verkkovakoilua, jonka tosiasiassa paljasti Ruotsi.[242] Voidaan nähdä, että havainnointikyky on ollut heikkoa jo vuonna 2013 ja edelleen vuoden 2017 sisäministeriön selvityksessä todetaan sen olevan puutteellista. Uusinta tietoverkkorikollisuuden torjuntaa koskevaa selvitystä ei ole vielä laadittu, mutta toivottavaa sisäisen tuvallisuuden kannalta on, että havaittuun puutteellisuuteen on kyetty vastaamaan.

Vieraan valtion tiedustelupalveluiden tavoite on päästä käsiksi luottamukselliseen ja salaiseen tietoon, joka hyödyttää omien kansallisten etujen ajamista. Tietoon pyritään tyypillisesti pääsemään käsiksi haittaohjelmien kautta murtautumalla tietojärjestelmiin.[243] Kybervakoilua voidaan toteuttaa sisäpiirin toimijoita hyödyntämällä sekä henkilö- ja signaalitiedustelulla. Tiedustelutoiminnan torjuminen on osoittautunut monella tapaa vaikeaksi, sillä ulkomaiset toimijat suojaavat toimintaansa käyttämällä lainkäytöllisiä koskemattomuuden mahdollistavia diplomaattisia peitteitä. Vieraan valtion tiedustelun toiminnasta voidaan hankkia tietoa PolL 5a:3:n 2 kohdan ja TtStL 3 §:n 2 kohdan nojalla, jotka mahdollistavat tiedustelun toiminnasta, toimijoista ja tiedonhankintakeinoista tai -kohteista.[244]

---

[240] Limnèll – Iloniemi 2018, s. 172.
[241] Sisäministeriö 2017, s. 16.
[242] Yle Uutiset., 1.11.2013 HS: Vinkki verkkovakoilusta tuli Ruotsista. [https://yle.fi/uutiset/3-6914048]
[243] Sisäminiteriö 2017, s. 16.
[244] Lohse – Meriniemi – Honkanen 2019, s. 34–35.

Vakoilusta säädetään erikseen rikoslain 12 luvun 5 §:ssä. Lisäksi vakoilu on sisällytetty rikoslain 34 a luvun 4 §:ään terroristiryhmän toimintaan osallistumiseen; ”joka edistääkseen terroristiryhmän 1, 1 a tai 2 §:ssä tarkoitettua rikollista toimintaa taikka tietoisena siitä, että hänen toimintansa edistää sitä, –– 3) hankkii tai yrittää hankkia tiedon, jonka tuleminen terroristiryhmän tietoon on omiaan aiheuttamaan vakavaa vahinkoa maalle tai kansainväliselle järjestölle, taikka välittää, luovuttaa tai ilmaisee terroristiryhmälle sellaisen tiedon, on tuomittava –– terroristiryhmän toimintaan osallistumisesta.”

Säännös kattaa tietojärjestelmiin liittyvän kriminalisoinnin, josta säädetään RL 34a:1.1,4 kohdassa. Rikoslain 34 a luvun 4 §:ssä kuitenkin puhutaan ryhmästä, joten arvioitavaksi tulee, onko yksittäisen henkilön toteuttama vakoilu rangaistavaa kyseisen lainkohdan nojalla? Rikoslain 34 a luvun 6 §:n 2 momentissa säädetään terroristiryhmän määritelmästä, jossa ”terroristiryhmällä tarkoitetaan vähintään kolmen henkilön muodostamaa tietyn ajan koossa pysyvää rakenteeltaan jäsentynyttä yhteenliittymää, joka toimii yhteistuumin ––”.

Säännös voidaan jäsentää viiteen eri osatekijään eli henkilömäärään, pysyvyyteen, jäsentyneisyyteen, yhteistuumaisuuteen ja terrorismirikoksen tekemistarkoitukseen. Näiden tulee olla kaikkien käsillä, jotta voidaan puhua legaalimääritelmän täyttävästä terroristiryhmästä.[245] Terroristiryhmän määritelmä ja kriteerien täyttyminen aiheuttaa tulkintaongelmia uusien toimintamuotojen kehittyessä. Kybervakoilu on yksi tällainen uusi terrorismin muoto, joka ei täytä edellä mainittuja lain edellyttämiä kriteereitä, mikäli vakoilua harjoitetaan yksin tai kaksin. Tällöin henkilömäärä ei täytä terroristiryhmän henkilömäärän edellytystä, joka voidaan nähdä ehdottomana vaatimuksena. Kahden henkilön toiminta voi olla rangaistavaa muissa rikoslain säännöksissä, kuten rikoskumppanuutena (RL 5:3) tai avunantona (RL 5:6).[246] Lisäksi hallituksen esityksestä käy ilmi, että ollakseen rangaistavaa terroristiryhmän toimintaan osallistumisena teon pitäisi olla tehty nimenomaan terroristiryhmän hyödyttämiseksi. Täten valtion tai järjestön vahingoittaminen tai pelkästään uteliaisuus ei kata rangaistavuutta.[247]

---

[245] Lohse 2012, s. 76.
[246] Härkönen 2006, s. 223.
[247] HE 188/2002 vp, s. 53.

Edellä mainituin perustein vakoilu terroristisessa tarkoituksessa vaatisi rikoslain 34 a lukuun oman säännöksensä, sillä tällä hetkellä vakoilu terroristisessa tarkoituksessa on rangaistavaa vain terroristiryhmässä. Täten yhden tai kahden henkilön harjoittama vakoilu tai kybervakoilu ei ole rangaistavaa rikoslain 34 a luvun mukaan, vaan sovellettavaksi tulee RL 12:5 tai RL 12:6. Kybervakoilu ja luvaton tiedustelutoiminta on yhä kasvava uhka Suomen sisäiselle turvallisuudelle, joten rikoslain 34 a luvun päivitys tältä osin olisi edellä selvitetyn perusteella aiheellista.

Todettakoon vielä, että valtiollinen kybervakoilu voi olla yhteiskuntaa vakavasti haavoittavaa ja Suomi kiinnostaa tällä hetkellä erityisesti Kiinaa ja Venäjää. Ongelmallista ilmiössä on kuitenkin se, että vaikka valtion organisoima kybervakoilu täyttää useamman rikoksen tunnusmerkistön, teon selvittäminen rikosoikeudellisessa kontekstissa edellyttää valtiolta oikeusapua. Mikäli vakoilua toteutetaan sijaintivaltion lukuun, oikeusapua ei ole saatavissa.[248]

Käytännössä tällaisissa tilanteissa voidaan nähdä, että kybervakoilussa on teon rangaistavuuden sijaan kyse ennemminkin kyvykkyydestä suojautua ja torjua kybervakoilua. Alussa mainittu sisäministeriön selvitys Suomen puutteellisesta havainnointikyvystä kybervakoilussa lisää huolta, sillä vakoilulla voidaan aiheuttaa kansalliselle turvallisuudelle korvaamatonta vahinkoa, eikä tekijöitä kaikissa tapauksissa voida saattaa vastuuseen. Toisaalta taas vakoilulla mahdollisesti aiheutettu tuho on moninkertaista siihen nähden, vaikka jotain lainsäädännöllisesti rangaistaisiinkin. Kybervakoilulla saavutettu tieto voi nimittäin pahimmassa tapauksessa lamauttaa ja haavoittaa vakavasti Suomen kriittistä infrastruktuuria.

6.3.2 Kybervaikuttaminen terroristisessa tarkoituksessa

Kybervaikuttamista on aiemmassa kappaleessa käsitelty esimerkkitapausten nojalla ja vaikuttamisen voidaan katsoa olevan tutkimuksen mukaan uusi uhka Suomelle. Vaikuttaminen on kui-

[248] Sisäministeriö 2017, s. 16.

tenkin lainsäädännöllisesti määrittelemätön, mutta eduskunnassa käsitteillä oleva hybridivaikuttamiseen liittyvä lainsäädäntö todennäköisesti tulee antamaan hybridivaikuttamisen osalta määritelmän, joka selittää osin myös kybervaikuttamista. Tällä hetkellä on sanottu, että vaikuttamisessa vaikuttaja pyrkii päämääriensä edistämiseksi käyttämään erilaisia keinoja kussakin tilanteessa[249].

Kuten on todettu, terrorismi on jatkuvasti kehittyvä ja muovautuva ilmiö, joka käyttää hyödykseen teknologian kehitystä. Täten kybervaikuttamista terroristisessa tarkoituksessa varmasti tullaan vielä näkemään, ja jotta tällainen vaikuttaminen saataisiin rangaistusten piiriin, tulisi se saattaa myös lainsäädäntöön. Joidenkin tutkimusten mukaan terveydenhuoltoalaan tullaan kohdistamaan digitaalisen vaikuttamisen muotoja, sillä terveydenhuollossa on arvokkaita potilastietoja, joita voidaan hyödyntää mm. poliittisessa vaikuttamisessa. Lisäksi terveydenhuollon kautta voidaan tehdä tietomanipulaatiota, joka horjuttaa kansalaisten luottamusta valtioon. Terveydenhuoltoalalla uhkana voidaan tietomanipulaation osalta mainita veriryhmätietojen ja laboratoriotulosten manipulaatio, jolloin tuloksiin ei voida luottaa.[250]

Tällainen menettely voidaan nähdä toteutettavan myös terroristisessa tarkoituksessa, sillä toiminta lisää yhteiskunnassa pelkoa ja terveystietojen manipulaatiolla voidaan menettää pahimmassa tapauksessa myös ihmishenkiä, mikäli terveystietojen luotettavuus kärsii ja sitä myötä hoidettavan potilaan tilanne hämärtyy. Lisäksi kybervaikuttamisella voidaan horjuttaa sisäistä turvallisuutta, jolloin epävarmuus lisää turvattomuuden tunnetta[251]. Haltuun saaduilla potilastiedoilla voidaan kiristää yhteiskuntamme keskeisiä toimijoita, jolloin kiristystä käytetään vaikuttamisen keinona. Kybervaikuttaminen on laaja käsite, joka kattaa monenlaisia eri tekomuotoja, joissa teknologiaa voidaan hyödyntää. Tästä syystä kybervaikuttamisesta on mahdotonta tehdä tyhjentävää esitystä, sillä ilmiössä vain mielikuvitus on rajana. Tästä syystä lainsäädäntöön tulisi saada vaikuttamisen määritelmä, jolloin se olisi sovellettavissa tulevaisuuden uhkissa.

---

[249] Sisäministeriö 2022, s. 11.
[250] Limnéll – Iloniemi 2018, s. 196.
[251] Limnéll – Iloniemi 2019, s. 207.

7 JOHTOPÄÄTÖKSET

Tämän tutkimuksen tavoitteena oli selvittää, voidaanko rikoslain 34 a lukua soveltaa kyberterrorismiin liittyvissä rikoksissa. Sovellettavuuden arviointi toteutettiin kyberhyökkäyksen, kybervaikuttaminen, värväyksen ja julkisen kehottamisen osalta. Toisena tutkimuksen tavoitteena oli selvittää rikoslain 34 a luvun kattavuus kyberterrorismiin liittyvän rikollisuuden osalta. Kyberterrorismi on varsin uusi, jäsentymätön ja määrittelemätön ilmiö, johon kohdistuu suhteellisen vähäinen määrä oikeudellista tutkimusta. Terrorismilla on olemassa paljon poliittista kosketuspintaa, sillä terrorismirikoksia rinnastetaan toisinaan myös poliittisiin rikoksiin[252]. Tämän tutkimuksen aikana Venäjä ja Ukraina ovat käyneet sotaa, joten sota on osaltaan nostanut esiin useita keinoja kyberhyökkäysten osalta.

Kyberterrorismilla ei ole olemassa lainsäädännöllisesti yksiselitteistä määritelmää, mutta kyberterrorismilla ei kuitenkaan tarkoiteta mitä tahansa tietoteknologiapohjaista toimintaa hallintoa tai muuta auktoriteettia vastaan. Kyberterrorismia voidaan määritellä terrorismin kautta, jolloin tarkasteltavaksi tulee millä ehdoin teot voidaan katsoa terroristiseksi ja mitkä tavat käyttää teknologiaa täyttävät nämä kriteerit.[253] Tutkielmasta voidaan huomata, että kyberterrorismi ei samalla tavalla sisällä väkivallan määritelmää kuten tavallinen terrorismi eikä toiminnan taustalla välttämättä toimi jihadistinen ideologia, vaan iskuja voidaan toteuttaa erilaisin tavoittein. Voidaan sanoa, että kyberterrorismi on aiemmin totuttuun terrorismiin nähden täysin uudenlainen ilmiö, jota voidaan kuvata terrorismin ja kyberavaruuden yhteenliittymänä. Tutkimuksessa selvitetyn perusteella kyberterrorismista ei voida tehdä vain yhtä määritelmää, sillä ilmiöllä on olemassa terrorismin kaltainen kameleonttimattimainen luonne.

Terrorismirikoksista säädetään rikoslain 34 a luvussa, joka on sisällytetty Suomen rikoslakiin vuonna 2003. Lainsäädäntöä on tämän jälkeen jatkuvasti kehitetty, jotta lainsäädännöllä pystyttäisiin paremmin vastaamaan tämän päivän uhkakuviin. Rikoslain 34 a luvussa on monessa eri

[252] Lohse 2012, s. 68.
[253] Limnell – Majewski – Salminen 2014, s. 130–135.

säännöksessä otettu huomioon tietoverkkorikollisuuteen liittyvät muutokset. Rikoslain 34 a lukua on kritisoitu sen monimutkaisesta kokonaisuudesta johtuen ja lisäksi se sisältää paljon luvun sisäisiä viittauksia sekä viittauksia rikoslain muihin säännöksiin. Lisäksi säännösten taustalla on monia kansainvälisiä asiakirjoja, joita tulee soveltaa sääntelyssä. Rikoslain 34 a lukuun on ehdotettu kokonaisuudistusta, joka todennäköisesti tullaan toteuttamaan jossain vaiheessa.[254] Kaiken tämän lisäksi terrorismilainsäädännössä tulee ottaa huomioon perus- ja ihmisoikeudet, jotta torjuntatoimet eivät perusteetta loukkaisi näitä oikeuksia. Kaiken kaikkiaan voidaan puhua haastavasta kokonaisuudesta, jota rikosten kansainvälisyys ja rajattomuus korostaa.

Tutkielman tutkimuskysymyksenä oli selvittää, voidaanko rikoslain 34 a lukua soveltaa kyberhyökkäyksiä koskeviin rikoksiin. Palvelunestohyökkäyksen voitiin katsoa tulevan sovellettavaksi RL 34a:1.1,4 kohdan nojalla, sillä palvelunestohyökkäyksessä on kyse törkeästä tietojärjestelmän häirinnästä. Rikoslain 34 a luvun sovellettavuus edellyttää tekijältä terroristista tarkoitusta ja teon on pitänyt olla omiaan aiheuttamaan vakavaa vahinkoa. Ongelmallista terroristisen tarkoituksen osalta on soveltaa määritelmää pelon aiheuttamisesta väestön keskuudessa. Hallituksen esityksen mukaan tilannetta arvioidaan tapauskohtaisesti[255], joten käytännössä tämä tarkoittaa sitä, että käytännön sovellettavuus odottaa asiasta ennakkotapausta.

Palvelunestohyökkäysten lisäksi tarkasteltavaksi valikoituivat haittaohjelmat ja haittaohjelmia tarkasteltiin tutkielmassa kyberrikosvälineenä. Rikoslain 34a:4.1,2 kohdassa säädetään terroristiryhmän toiminnan kannalta erittäin tärkeistä välineistä. Tutkielmassa näiden välineiden on katsottu olevan fyysisiä tietojenkäsittelyyn tai -viestittelyyn liittyviä välineitä kuten tietokoneita tai matkapuhelimia. Täten haittaohjelman ei voida katsoa kuuluvan kyseiseen säännökseen, mutta RL 34a:1.1,4 kohta sisältää säännöksen haittaohjelmien käytöstä rikoksen yhteydessä. Säännöksessä ei ole säädetty haittaohjelman hallussapidosta, joten hallussapito ei ole rikoslain 34 a luvun nojalla rangaistavaa.

---

[254] Melander 2015, s. 416–420.
[255] HE 188/2002 vp, s. 59.

Tutkielman tarkoituksena oli myös selvittää rikoslain 34 a luvun sovellettavuus kybervaikuttamista koskevissa rikoksissa. Kybervaikuttamisen osalta voidaan todeta, että siihen liittyy pääsääntöisesti sitä edeltävä teko, joka on laissa kriminalisoitu kuten murtautuminen tietojärjestelmiin, hakkerointi, haittaohjelmien käyttö ja palvelunestohyökkäys. Kybervaikuttamista voidaan pääsääntöisesti harjoittaa näiden tekojen yhteydessä, joka tarkoittaa sitä, että osa teosta on kriminalisoitu. Kybervaikuttamista voidaan toteuttaa myös ilman kriminalisoitua tekoa, jolloin varsinainen vaikuttaminen poliittisine tavoitteineen ei ole rikoslain 34 a luvun nojalla rangaistavaa.

Varsinaiselle kybervaikuttamiselle ei ole olemassa lainsäädännössä määritelmää, joten lainsäädäntöä tulisi uudistaa kybervaikuttamista koskevan rikosten osalta ja täten vaikuttamisen määritelmä tulisi saattaa lainsäädäntöön. Eduskunnassa on käsitteillä valmiuslain kokonaisuudistus, joka kattaa myös hybridivaikuttamista koskevan sääntelyn[256]. Todennäköistä ja toivottavaa on, että kyseisen lainsäädännön muutoksen kautta myös kybervaikuttamista koskevat teot määritellään ja kriminalisoidaan lainsäädännön keinoin, sillä kyseessä on tutkielmassakin useasti todettu vakava uhka yhteiskunnalle.

Rikoslain 34 a luvun sovellettavuuden osalta tehtiin myös muita huomioita. Värväyksen osalta säännös RL 34a:4c kattaa internetin kautta toteutettavan värväyksen kyberterrorismirikosten tekemiseen, mutta toisaalta sovellettavaksi tulisi myös terrorismirikoksiin liittyvä julkinen kehottaminen RL 34a:5e. Esimerkkinä tutkielmassa käytettiin Venäjän ja Ukrainan sodassa hakkereiden perustamaa Telegram-viestiryhmää nimeltään IT-Army of Ukraine. Ryhmän tarkoituksena oli toteuttaa kyberhyökkäyksiä Venäjää vastaan. Ongelmallista lain sovellettavuuden osalta oli arvioida, sovelletaanko tapaukseen rikoslain 34 a lukua vai tulisiko rikoslain 11 luvun säännökset sotarikoksista sovellettavaksi. Tapausta analysoitiin rikoslain 34 a luvun nojalla, jonka todettiin tulevan värväyksen ja julkisen kehottamisen osalta sovellettavaksi. Jatkotutkimuskysymyksenä voisi olla, katsotaanko kyberhyökkääjien olevan oikeudellisesti sodan vierastaistelijoita vai onko kyseessä terrorismiin liittyvä teko, mikäli hyökkääjät osallistuvat sotaa käyvien maiden väliseen konfliktiin muualta kuin konfliktialueilta? Mahdolliseen jatkotutkimukseen olisi aiheellista myös

[256] Valtioneuvosto, Valmiuslain uudistaminen käynnistyy 8.12.2021. [https://valtioneuvosto.fi/-//1410853/valmiuslain-uudistaminen-kaynnistyy]

selvittää kyberterrorismin ja kybersodan välinen rajapinta sekä arvioida oikeudellisesti, milloin kybertoimi ylittää tilanteen, jolloin tekoon voidaan vastata aseellisesti.

Toisena tutkimuskysymyksenä oli arvioida Suomen rikoslain 34 a luvun sääntelyn kattavuutta kyberterrorismissa. Tällä hetkellä lainsäädäntö kattaa tyypillisimpiä tietoverkkorikoksia, mutta teknologian ja terrorismin kehityksestä johtuen lainsäädäntöä tulisi jatkuvasti pyrkiä kehittämään siten, että tekoihin voitaisiin vastata lainsäädännöllisesti etupainotteisesti. Toisekseen rikoslain 34 a luku on kokonaisuutena hyvin epäselvä, jonka on todettu vaativan kokonaisuudistuksen säädöksen yksinkertaistamiseksi[257]. Tämänhetkisen monimutkaisen ja hajanaisen sisällön voidaan katsoa tuovan haasteita myös kattavuuden arvioinnin osalta, sillä sääntelyn rikkonaisuudesta johtuen ei voida olla varmoja ovatko teot kriminalisoitu lainsäädännössä ja millä tasolla.

Kattavuuden arviointiin on tutkielmassa tarkasteltu myös muun kansallisen lainsäädännön merkitystä kyberterrorismin osalta. Uudella tiedustelulainsäädännöllä voidaan katsoa olevan merkittävää vaikutusta kyberterrorismirikosten torjunnan osalta, sillä tiedustelulla pyritään turvaamaan kansallista turvallisuutta ennakoivasti. Tekoihin pystytään puuttumaan jo niiden valmisteluasteella tai niiden valmistelu pystytään kokonaan torjumaan. Valmiuslain osalta voidaan todeta, että tällä hetkellä laki on vanhanaikainen eikä vastaa nykypäivän turvallisuushaasteita. Tämä on ymmärretty myös valtiotasolla ja laki onkin kokonaisuudistuksen alla. Valmiuslailla on merkitystä kyberterrorismirikosten osalta siinä, että lailla pystytään varautumaan ja toimimaan erilaisin keinoin kriisitilanteissa. Terrorismia voitaisiin valmiuslain näkökulmasta pitää esimerkiksi suuronnettomuutena, joka täyttäisi poikkeusolojen tunnusmerkit.[258] Kyberpakotejärjestelmä sen sijaan mahdollistaa erilaisia keinoja vastata henkilöiden tai yhteisöjen tekemiin iskuihin. Näistä esimerkkeinä voidaan mainita varojen jäädyttämiset.[259]

[257] Melander 2020, s. 1–9.
[258] Komiteanmietintö 2005:2, s. 45.
[259] Ulkoministeriö, Perusmuistio UM2020-00783, s. 2.

Tutkielmassa voidaan lainsäädännön kattavuuden osalta tulla lopputulokseen, että lainsäädäntö on kattavalla tasolla, mutta rikoslain 34 a luvun kokonaistarkastelulle olisi tarvetta. Tutkimuksen perusteella voidaan todeta, että kybervakoilu terroristisessa tarkoituksessa tulisi sisällyttää rikoslain 34 a lukuun samoin kuin kybervaikuttaminen. Molemmissa on kyse vakavasti yhteiskuntaa uhkaavasta ilmiöstä, jossa pieni kiinnijäämisen riski ja rajattomuus houkuttelee tekijöitä kyseisiin tekoihin. Vakoilusta on tällä hetkellä säädetty rikoslain 12 luvun 5 §:ssä ja terroristisesta teosta rikoslain 34 a luvun 4 §:ssä, jossa säädetään terroristiryhmän toimintaan osallistumisesta. Ongelmallista säännöksen osalta on, että teko koskee terroristiryhmässä toteutettua tekoa, joka siten käsittää vähintään kolmen henkilön muodostaman ryhmän (RL 34a:6.2). Täten yhden tai kahden henkilön toteuttama kybervakoilu ei tule sovellettavaksi kyseisen säännöksen nojalla, ja ne jäävät täten vaille rangaistavuutta terroristisen tarkoituksen osalta.

Tulosten osalta voidaan yleisesti todeta, että kyberterrorismi aiheena on erittäin haastava. Aiheen monimuotoisuudesta johtuen tutkimustulokset sovellettavuuden osalta voivat poiketa toisistaan tarkasteluun valittavan näkökulman takia. Mikäli tarkastelu toteutettaisiin esimerkiksi rikosvälineen kannalta tietoverkko-ohjelmiston luonteen ja rakenteen osalta, voitaisiin lain sovellettavuuden osalta saada erilaisia tuloksia. Mielenkiintoista on, milloin tuomioistuimessa ensimmäinen kyberterrorismiin liittyvä kokonaisuus tulee käsiteltäväksi, sillä tällaisella ennakkopäätöksellä tulee olemaan merkitystä lain käytännön sovellettavuuden ja kattavuuden arvioinnin osalta. Tällä hetkellä kyberterrorismiin liittyvää ennakkotapausta ei ole, eikä lain sovellettavuudesta ole olemassa käytännön kokemusta. Kootusti voidaan todeta, että tutkimus kyberterrorismista tutkimuskysymysten osalta osoittautui haasteelliseksi aiheen monimuotoisuuden ja vähäisten oikeustieteellisten tutkimusten osalta.