Santeri Sahi

NETTIKIUSAAMINEN KYBERRIKOLLISUUDEN MUOTONA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Sahi, Santeri
Nettikiusaaminen osana kyberrikollisuutta
Jyväskylä: Jyväskylän yliopisto, 2021, 37 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Marttiin, Pentti

Nettikiusaaminen on vakava ilmiö, joka on 2000-luvun alusta lähtien vakiinnuttanut asemaansa etenkin lasten ja nuorten keskuudessa. Nettikiusaamisen on todettu aiheuttavan etenkin uhreissa mutta myös kiusaajissa masennusta, itsetunnon laskua, toivottomuutta ja yksinäisyyttä, jotka ovat esiasteita itsetuhoisuudelle. Toistaiseksi nettikiusaamisen tutkimus on tuottanut jokseenkin ristiriitaisia tuloksia, ja keinot ilmiön torjumiseen ovat olleet sen mukaisia.

Myös kyberrikollisuus on yleistynyt ja aiheuttaa vahinkoja etenkin taloudellisesti, mutta myös muilla tavoin, kuten suoraan fyysiseen maailmaan vaikuttamalla. Toisin kuin nettikiusaamisen kohdalla, kyberrikollisuutta on onnistuttu torjumaan melko tehokkaasti jo vuosikymmeniä. Tässä tutkielmassa tarkastelemme nettikiusaamista osana kyberrikollisuutta, tavoitteena pyrkiä selvittämään voidaanko nettikiusaaminen nähdä kyberrikollisuuden muotona ja onko kyberrikollisuuden torjunnan keinoja mahdollista hyödyntää nettikiusaamisen torjunnassa.

Asiasanat: Nettikiusaaminen, kiusaaminen, kyberrikollisuus, rikollisuus, tietoverkot, tietojärjestelmät

ABSTRACT

Sahi, Santeri
Cyberbullying as a form of cybercrime
Jyväskylä: University of Jyväskylä, 2021, 37 pp.
Information Systems, Bachelor's thesis
Supervisor: Marttiin, Pentti

Cyberbullying is a grave phenomenon that has established itself since the beginning of the 21st century, especially among children and youth. Cyberbullying has been found to cause depression, loss of self-esteem, hopelessness, and loneliness, all of which are precursors to self-harm, especially in victims but also in bullies. So far research into cyberbullying has yielded somewhat conflicting results, and the means to combat the phenomenon have been in line with it.

Cybercrime has also become more widespread and causes damage, especially economically, but also in other ways, such as by directly affecting the physical world. Unlike cyberbullying, cybercrime has been tackled quite effectively for decades. In this thesis, we look at cyberbullying as part of cybercrime, with the aim of finding out whether cyberbullying can be seen as a form of cybercrime and whether the means of combating cybercrime can be utilized in the fight against cyberbullying.

Keywords: Cyberbullying, bullying, cybercrime, crime, information networks, information systems

TAULUKOT

SISÄLLYS

1 JOHDANTO

Elämme tietoyhteiskunnassa, jossa datan ja tiedon liikkuvuus on vaivatonta, nopeaa ja kehittyy jatkuvasti entistä tehokkaammaksi. Internet ja tietoverkot yleisesti kannattelevat jokapäiväistä elämäämme ja sekä yhteiskuntamme että henkilökohtaisen elämämme toimintoja. Esimerkiksi lähestulkoon kaikki yhteydenpitomme läheisiimme tapahtuu tietoverkkojen välityksellä ja palvelut, jotka ennen vaativat fyysistä läsnäoloa, kuten pankissa tai jopa terveyspalveluissa asiointi, voidaan toteuttaa täysin etäyhteyksillä, ajasta tai paikasta riippumatta (Ebrand Suomi Oy & Oulun kaupungin sivistys- ja kulttuuripalvelut, 2016).

Siinä missä tiedon vapaa ja nopea liikkuvuus on helpottanut niin kutsutun keskivertokansalaisen elämää, se on luonnollisesti helpottanut myös niiden toimintaa, jotka eivät seuraa lakeja tai moraalisia periaatteita. Jo kauan ennen tietoyhteiskunnan kehittymistä olemassa olleet ongelmat, kuten tässä tutkielmassa käsiteltävät rikollisuus ja kiusaaminen, ovat seuranneet yhteiskunnan kehitystä ja siirtyneet samoin verkkoon ja tehostuneet sen myötä. Esimerkiksi tietoverkkorikollisuuden (kyberrikollisuus) ja sen torjunnasta aiheutuvien kulujen on arvioitu vuonna 2020 aiheuttaneen yli biljoonan dollarin haitan maailmantaloudelle, mikä on noin prosenttiyksikön verran koko maailman bruttokansantuotteesta. Taloudellisten haittojen lisäksi kyberrikollisuus aiheuttaa lukemattomia muita haittoja yrityksille, organisaatioille sekä yksityisille ihmisille. Tällaisia haittoja ovat esimerkiksi mainehaitat sekä fyysiseen maailmaan ulottuvat vaikutukset. (CSIS & McAfee, 2020; Grönroos, 2020; Rautavaara, 2020.)

Kommunikaation siirtyminen lähes kokonaisuudessaan verkkoon, on kiusaamisellekin auennut uusia toteutustapoja. Verkon kautta tapahtuvassa kiusaamisessa (nettikiusaaminen) edellä mainitut muissa yhteyksissä hyväksi mielletyt saavutettavuuden tekijät kääntyvät tarkoitusperiään vastaan ja toimivat haittatekijöinä kiusaamisen uhreille (Willard, 2004). On selvää, että nettikiusaaminen on aito ongelma, josta on vakavia haittoja sen uhriksi joutuneille, mutta aiheen tutkimuksessa on paljon ongelmia esimerkiksi toistettavuuden kanssa, eikä sen tutkimukseen ole juurikaan kehitetty yleisiä viitekehyksiä, jotta se voitaisiin tehokkaammin eritellä perinteisistä kiusaamisen muodoista (Cole, Zelkowitz, Nick, Martin, Roeder, Sinclair-McBride & Spinelli, 2016; Olweus, 2012). Oman roolinsa

nettikiusaamisen ilmiössä esittää myös media, jonka vaikutuksesta ilmiön mittasuhteet ovat vääristyneet niin julkisuudessa, kuin myös joissain tapauksissa tiedeyhteisössäkin. Lisäksi ilmiön laajuutta voi olla vaikea kartoittaa, koska uhriksi joutuneet eivät välttämättä kerro kokemuksistaan kenellekään (Slonje & Smith, 2008).

Molempien edellä mainittujen aiheiden tutkimus on ensisijaisen tärkeää, sillä niillä on suoria vaikutuksia sekä yhteiskunnan toimintaan että yksilöiden hyvinvointiin. Molemmat ilmiöt eivät myöskään näytä merkkejä hidastumisesta, vaan tulevat todennäköisesti olemaan tulevaisuudessa vieläkin suurempia haittatekijöitä yksilöille, yhteiskunnille ja maailmantaloudelle.

Tämä kuvailevana kirjallisuuskatsauksena toteutettu tutkielma pyrkii tarkastelemaan nettikiusaamisen ja kyberrikollisuuden ilmiöitä, syitä niiden syntymiseen sekä niistä aiheutuvia haittoja. Ilmiöitä tarkastellaan ensin toisistaan erillään sisältöluvuissa 2 ja 3, joissa kartoitetaan niiden käsitteistöä ja pyritään luomaan selkeä yleiskuva kustakin aiheesta. Tämän jälkeen sisältöluvussa 4 ilmiötä tarkastellaan yhteisessä kontekstissa pyrkimyksenä tehdä johtopäätelmiä ilmiöiden yhtäläisyyksistä ja eroavaisuuksista. Luvussa käsitellään myös kyberrikollisuuden ja kyberhyökkäysten torjunnan keinoja mahdollisina apuvälineinä nettikiusaamisen torjunnassa.

Tutkielmassa käsitellyn aineiston perusteella luotiin kaksi nettikiusaamista ja kyberrikollisuutta koskevaa tutkimuskysymystä, joihin tutkielma pyrkii vastaamaan. Kysymykset ovat:

- Voidaanko nettikiusaaminen nähdä kyberrikollisuuden muotona?
- Onko kyberrikollisuuden torjuntakeinojen soveltaminen nettikiusaamisen torjuntaan mielekästä?

Kaikki aiheiden kannalta merkittävät käsitteet määritellään tarkemmin luvuissa, joissa kutakin aihetta tarkastellaan.

2 NETTIKIUSAAMINEN

Tässä luvussa pohdimme nettikiusaamista käsitteenä ja ilmiönä. Luokittelemme käsitteen Willardin (2004) tapaan pohjautuen erilaisiin alakategorioihin, jonka lisäksi syvennymme nettikiusaamisen tutkimuksen merkittävimpiin ongelmiin ja lopulta käymme läpi ilmiön todennäköisimpiä haittavaikutuksia sen uhriksi joutuneille.

Nettikiusaamisen käsite on pyritty määrittelemään 2000-luvulta nykypäivään useita kertoja. Määritelmissä on esiintynyt joskus melko suurtakin variaatiota, mutta yleisesti nettikiusaaminen on määritelty kiusaamisen muodoksi, jossa tarkoituksellisesti ja toistuvasti aiheutetaan harmia jollekulle yksilölle tai useammalle henkilölle käyttäen hyväksi elektronisia välineitä, kuten internetiä, älypuhelinta tai tietokonetta (Mannerheimin lastensuojeluliitto, 2017).

2000-luvun lopulla nettikiusaaminen määriteltiin siten, että harmin aiheuttaminen tapahtuisi elektronisen tekstin, kuten sähköpostin tai pikaviestipalveluiden välityksellä (Burgess-Proctor, Patchin & Hinduja, 2009). Useisiin määritelmiin on myös liitetty perinteisen kiusaamisen määritelmästä vallan epätasapaino tekijän ja uhrin välillä (Olweus, 1999). Nettikiusaamisen tapauksessa vallan epätasapainon on ehdotettu muodostuvan esimerkiksi teknologiataitojen eroista tekijän ja uhrin välillä (Smith, 2013) sekä internetin kautta saavutettavasta anonymiteetistä (Vandebosch & Van Cleemput, 2008). Nykyisin käsitteenmäärittelyyn on myös yhdistetty laajempi kirjo erilaisia elektronisen viestinnän muotoja, kuten esimerkiksi suoratoistettu videomateriaali ja modernimmat sosiaalisen median alustat, kuten Instagram, Snapchat ja TikTok (Kumar & Goldstein, 2018).

Tällaiset sosiaalisen median muodot ovat 2010-luvun aikana sekä sen jälkeen kasvattaneet suosiotaan niin maailmanlaajuisesti kuin Suomessakin erityisesti nuorison keskuudessa. Ebrand Suomi Oy:n ja Oulun kaupungin sivistys- ja kulttuuripalveluiden toteuttamasta kyselytutkimuksesta (2016) selvisi, että suomalaisista 13–17-vuotiaista kyselyyn osallistuneista nuorista 61 % käyttivät sosiaalisen median palveluita 3–20 tuntia viikossa. Sosiaalisen median ja sen mahdollistavien laitteiden käytön lisääntyessä on mahdollista, että myös nettikiusaamisen kaltaiset negatiiviset lieveilmiöt yleistyvät.

Nettikiusaaminen on saanut osakseen suurta huomiota perinteisessä mediassa ja myös tieteellisessä yhteisössä 2000-luvun alkupuolelta lähtien (Olweus, 2012). Esimerkiksi jo vuonna 2006 Patchin & Hinduja huomasivat tutkimuksessaan, että 74 % tutkimusaineiston nuorista kertoivat havainneensa kiusaamista internetissä ja 30 % puolestaan kertoivat joutuneensa nettikiusaamisen uhriksi. Ongelman todellinen laajuus ja muoto voivat kuitenkin olla piilossa, sillä nettikiusaamisen uhrit eivät välttämättä kerro uhriksi joutumisestaan kenellekään tai kertovat siitä esimerkiksi vain vertaisilleen, joilla on hyvin vähän keinoja puuttua kiusaamiseen tai auttaa uhria (Slonje & Smith, 2008).

2.1 Nettikiusaamisen muotoja

Willard (2004) on jäsentänyt opettajille suunnatussa nettikiusaamisen ja kyberuhkailun torjuntaan tarkoitetussa oppaassaan ilmiön alakategorioihin. Alkuperäisessä tekstissä kategorioita on kahdeksan, mutta tässä tutkielmassa Berania & Litä (2007) mukaillen, *huijaaminen* on jätetty pois, sillä sen on määritelmältään hyvin lähellä *imitointi* -kategoriaa. Jäljelle jäävät seitsemän kategoriaa ovat:

- **”Fleimaaminen”** (flaming). ”Liekkien ruokkimista”. Elektronisen viestinnän kautta käydyt riidat, jotka sisältävät vihaista ja alatyylistä kielenkäyttöä.
- **Häirintä** (harassment). Ilkeiden ja loukkaavien viestien jatkuva lähettäminen jollekulle henkilölle.
- **Mustamaalaus** (denigration, ”dissing”). Henkilön mainetta vahingoittavien juorujen levittäminen internetissä.
- **Imitointi** (impersonation). Jonakin henkilönä esiintyminen ja tämän identiteetillä sellaisen materiaalin levittäminen, joka asettaa henkilön vaaraan, ongelmiin tai vahingoittaa tämän mainetta.
- **Paljastaminen** (outing). Henkilön salaisuuksien tai tätä nolaavan tiedon vuotaminen ulkopuolisille internetiä käyttäen.
- **Syrjiminen** (exclusion). Tahallisesti ja julmasti jonkun jättäminen ulos jostakin verkon kautta toimivasta ryhmästä.
- **Kybervainoaminen** (cyberstalking). Jatkuvaa, äärimmäisen voimakasta häirintää ja mustamaalausta, johon liittyy uhkailua ja joka aiheuttaa merkittävää pelkoa kohteena olevalle henkilölle.

Useat edellä mainituista nettikiusaamisen muodoista täyttävät suoraan rikoslaissa (1889/39) esimerkiksi sellaisten rikosnimikkeiden määritelmät, kuten kunnianloukkaus (24 luku 9 §), yksityiselämää loukkaavan tiedon levittäminen (24 luku 8 §), laiton uhkaus (25 luku 7 §) sekä vainoaminen (25 luku 7 a §). Nettikiusaamisen suhdetta perinteiseen rikollisuuteen sekä kyberrikollisuuteen käsitellään lisää tämän tutkielman neljännessä luvussa.

2.2 Nettikiusaamisen tutkimuksen ongelmia

Osa nettikiusaamisesta tehdystä tutkimuksesta on kyseenalaistanut narratiivia, jota esimerkiksi mediassa, mutta myös tiedeyhteisössä on tuotu julki nettikiusaamiseen liittyen. Tämän käsityksen mukaan nettikiusaaminen olisi lasten ja nuorten keskuudessa hyvinkin laajalle levittäytynyttä sekä esiintyvyydeltään jatkuvassa kasvussa oleva ilmiö. Lisäksi nettikiusaamisen on ehdotettu myös luoneen paljon uusia kiusaajia ja kiusattuja, jotka eivät aiemmin ole olleet kytköksissä kyseiseen toimintaan. (Olweus, 2012.)

Artikkelissaan *Cyberbullying: An overrated phenomenon?* (2012) Olweus esittää väitteen siitä, että aihetta on tutkittu niin kutsutusti tyhjiössä, eli ilman perinteistä kiusaamista kontekstina sen taustalla, jolloin nettikiusaaminen on voinut näyttää ilmiönä yleisemmältä kuin mitä se tosiasiassa on. Olweuksen esittelemissä tuloksissa nettikiusaamista esiintyi lähinnä niissä yhteyksissä, joissa esiintyi myös perinteistä kiusaamista.

Olweus kritisoi artikkelissaan (2012) myös sitä, että aihetta tutkineet tahot eivät ole olleet psykologian tieteenalalta. Vaikkakin psykologian tutkimuksen ammattilaisilla on luonnollisesti usein paras tietämys alansa ilmiöistä, monitieteellisen lähestymistavan on kuitenkin yleisesti todettu tuovan aiheeseen kuin aiheeseen uusia näkökulmia sekä sen myötä laaja-alaisuutta ja uutta tietoa.

Osassa aiheesta tehdystä tutkimuksesta on kuitenkin saatu myös edellisistä eriäviä havaintoja. Esimerkiksi Bonanno ja Hymel (2013) havaitsivat masennusoireiden ja itsetuhoisen ajattelun olevan selvästi yhteydessä nettikiusaamisen uhriksi joutumiseen, vahvistaen näin käsitystä siitä, että nettikiusaaminen on oma, uniikki ilmiönsä eikä vain osa perinteistä kiusaamista, vaikka ilmiöt ovatkin tulosten mukaan läheisesti kytköksissä. Lisää vastaavanlaista näyttöä aiheesta ovat tarjonneet Perren, Dooley, Shaw ja Cross (2010), jotka löysivät myös yhteyden masennusoireiden esiintymisen ja nettikiusaamisen uhriksi joutumisen välillä vielä senkin jälkeen, kun perinteisen kiusaamisen vaikutukset oli kontrolloitu aineiston analyysissä. Perrenin ym. (2010) Tuloksista kävi lisäksi ilmi yhteyden pysyvän samankaltaisena riippumatta siitä, mistä maasta aineisto oli kerätty, viitaten ilmiön mahdollisesti olevan riippumaton kulttuurisista vaikutteista.

Aiheen tutkimustulokset ovat myös joissakin tapauksissa olleet epäselviä, tai selkeää korrelaatiota nettikiusaamisen ja mahdollisten haittavaikutuksia lisäävän vaikutuksen välillä ei ole havaittu. Eräässä pitkittäistutkimuksessa (Cole ym., 2016) nettikiusaamisen uhriksi joutumisen havaittiin aiheuttavan masennusoireita ja negatiivisia itsetuntemuksia uhreissa, mutta nettikiusaamisesta johtuva lisäys jäi melko pieneksi. Toisissa pitkittäistutkimuksissa (Machmutow, Perren, Sticca & Alsaker, 2012; Salmivalli, Sainio & Hodges, 2013) nettikiusaamisen uhriksi joutumisen ei ole havaittu juurikaan lisäävän vaikutusta uhreihin perinteisen kiusaamisen muotojen lisäksi, jotka näissäkin tapauksissa kulkevat käsi kädessä nettikiusaamisen kanssa.

Päätelmänä edellä mainituista aineistoista sekä niiden tuloksista voitaisiinkin sanoa nettikiusaamisen tutkimuksen olevan tähän mennessä vielä jokseenkin

puutteellista tai ainakin vailla laajemmin hyväksyttyä viitekehystä. Tällaisen viitekehyksen kehittäminen, tai vastaavasti jonkin olemassa olevan soveltaminen, voisi auttaa ja selkeyttää uusien tutkimustulosten tulkinnassa. Ongelmat nettikiusaamisen tutkimuksessa voivat johtua myös siitä, että aihe on vielä melko tuore ja riittävän tarkan aineiston vähäisyydestä johtuen parhaat käytännöt sen tutkimukseen eivät ole vielä ehtineet muotoutua.

2.3 Nettikiusaamisen vaikutukset uhreihin

Nettikiusaamisella voi olla vakavia vaikutuksia sen uhriksi joutuneiden hyvinvointiin. Nettikiusaaminen ollessa läheisesti kytköksissä perinteisiin kiusaamisen muotoihin, myös sen aiheuttamat vaikutukset uhreissa saattavat olla osittain samankaltaisia.

Vertaisten häirinnän ja kiusaamisen perinteisillä keinoilla on todettu aiheuttavan sekä uhreissa että kiusaajissa masennusta, itsetunnon laskua, toivottomuutta ja yksinäisyyttä, jotka kaikki ovat esiasteita itsetuhoiselle ajattelulle sekä käytökselle (Langhinrichsen-Rohling & Lamis, 2008; Kaltiala-Heino, Rimpelä, Marttunen, Rimpelä & Rantanen, 1999). Lisäksi osa tutkimuksesta viittaa nettikiusaamisen altistavan valmiiksi vaikeassa elämäntilanteessa olevia itsetuhoisuudelle, vaikka ei yksinään suoraan lisäisikään itsemurhia.

Olweus (2012) havaitsi, että yleisesti nettikiusatuilla lapsilla tai nuorilla oli sen mukaisesti huonompi itsetunto, kuin niillä, joita ei ollut kiusattu. Beran ja Li (2007) puolestaan havaitsivat lasten, joita kiusattiin netissä tai sekä netissä että koulussa suoriutuvan heikommin koulutyössään. Heikommin suoriutuminen ilmeni muun muassa poissaoloina, keskittymiskyvyn puutteena ja alhaisempina arvosanoina. Vähäisempiä tuloksia oli saatu siitä, että myös netissä muita kiusanneilla lapsilla oli vaikeuksia suoriutua koulutyössään. Lisäksi nettikiusaamisen uhrien todettiin todennäköisesti kiusaavan muita samoilla keinoilla. Syyksi tälle ehdotettiin oman kiusaamisen kostamista muille sekä vertaisten puolustamista kiusaamisen keinoin. (Beran & Li, 2007.)

Nettikiusaamisen uhriksi joutuminen on yhdistetty myös yksinäisyyteen. Yksinäisyyden yleisyys johtunee kiusattujen aiemmista huonoista kokemuksista vertaistensa kanssa, jotka voivat toistuessaan johtaa siihen, että uhrit etääntyvät entisestään ja näin kokevat itsensä entistä yksinäisemmiksi. (Şahin, 2012.) Uhrit eivät esimerkiksi välttämättä enää tahdo hyödyntää sosiaalista mediaa tai muita informaatioteknologiaa käyttäviä viestintäalustoja, jos niiden kautta tapahtuu nettikiusaamista. Tällaiset alustat ovat olleet jatkuvassa kasvussa niiden syntyhetkistä lähtien (Perrin, 2015), mikä lisää huoleen siitä, että nettikiusaamisen uhrien internet-palveluiden käyttö rajoittuu kiusaamisen vuoksi. Sen lisäksi, että internetin käyttö on tärkeä osa nyky-yhteiskuntaa niin kommunikaation kuin esimerkiksi peruspalveluidenkin kannalta, mahdollisuus internetin käyttöön on myös julistettu ihmisoikeudeksi (United Nations, 2016).

3 KYBERRIKOLLISUUS

Tässä luvussa tarkastelemme kyberrikollisuuden käsitettä ja pohdimme kyberrikollisia ja näiden tyypillisimpiä motiiveja, kyberrikollisuuden aiheuttamia ongelmia, sen torjunnan keinoja ja sivuamme sitä, miten kyberrikollisuuden käsite sijoittuu suhteessa perinteisiin rikollisuuden muotoihin.

Rikoksen määritelmä on yksinkertaisimmillaan teko tai laiminlyönti, jonka jokin valtio on lainsäädännöllään määrännyt kielletyksi ja rangaistavaksi (Felson, 2006; Oikeusministeriö, 2021). Kyberrikoksen eli tietoverkkorikoksen käsitteelle puolestaan ei ole vakiintunutta määritelmää, mutta se määritellään useimmiten teknologian käytön kautta, korostaen sitä joko tekovälineenä, kohteena tai ympäristönä (Gordon & Ford, 2006). Esimerkiksi poliisi määrittelee kyberrikoksen luokittelemalla ne tietoverkkoihin tai tietojärjestelmiin suoraan kohdistuviin eli tietoverkkosidonnaisiin rikoksiin ja rikoksiin, jotka hyödyntävät tietoverkkoympäristöä välineenä eli tietoverkkoavusteisiin rikoksiin (Poliisi, 2020). Tietoverkkoympäristöihin suoraan kohdistuvia rikoksia ovat esimerkiksi palvelunestohyökkäykset, joissa järjestelmän toimintaa tahallisesti hidastetaan tai kokonaan estetään. Tietoverkkoympäristöä hyväksi käyttäviin rikoksiin puolestaan lukeutuvat kaikki sellaiset rikokset, jotka ovat toteutettu tietoverkkoympäristöä hyödyntäen. (Sisäministeriö, 2017.) Henkilöitä, jotka tekevät rikoksia teknologian väärinkäytön kautta tai yleisesti vievät informaatioteknologiaa ja sen välineitä äärimmäisyyksiin, kutsutaan usein yläkäsitteellä hakkerit (Kilger, Arkin & Stutzman, 2004).

Kyberrikollisuus on myös usein vahvasti globalisoitunutta, sillä verkkoa hyödynnettäessä fyysisiä rajoja ei tarvitse ylittää, eikä rikosten tekijöiden tai uhrien sijainnilla ole juuri merkitystä (SM, 2020). Rikollisten on lisäksi mahdollista kokoontua fyysisestä sijainnistaan riippumatta erilaisilla verkon foorumeilla ja kauppapaikoilla, joihin tavanomaisilla selaimilla tai hakukoneilla ei ole pääsyä. Näin ollen kyberrikollisuuden voidaankin sanoa teollistuneen; ammattimaisesti toimivien rikollisten verkkopalveluiden avulla rikolliset voivat ostaa osia tai kokonaisuuksia, joita tarvitsevat rikosten toteuttamiseen, mutta joita eivät itse pysty tuottamaan. (SM, 2017.)

3.1 Motiivit kyberrikollisuudessa

Kyberturvallisuudella tarkoitetaan lähtökohtaisesti sellaista toimintaa, jossa pyritään suojaamaan tietoteknisiä laitteita, järjestelmiä ja verkkoja tietoteknisin keinoin suoritetuilta hyökkäyksiltä. Tällaiset hyökkäykset ovat lähtökohtaisesti tietoverkkorikollisuutta, eli kyberrikollisuutta. (Craigen, Diakun-Thibault & Purse, 2014.)

Kyberturvallisuudessa on keskitytty usein teknisiin haavoittuvaisuuksiin ja niiltä suojautumiseen (Holt & Kilger, 2012). Vaikkakin nykyisin ymmärretään myös kyberturvallisuuden koostuvan muistakin tekijöistä kuin teknologian suojaamisesta, niin kutsutut inhimilliset tekijät voivat silti jäädä vähemmälle huomiolle (Conteh & Schmick, 2016). Etenkin kyberrikollisten ja muiden turvallisuuden aukkoja hyväkseen käyttävien motiivit kyseiseen toimintaan ovat tärkeitä ymmärtää sekä rikollisuuden ennaltaehkäisemiseksi että jo tapahtuneiden tapausten ratkaisemiseksi.

Motiivit kyberrikollisuudessa ovat pitkälti yhteneväisiä perinteisen rikollisuuden ja perinteisten rikollisten motiivien kanssa, sillä rikosten perimmäiset tarkoitukset ja päämäärät ovat hyvin samankaltaisia, vaikka rikokset suoritettaisiinkin hyvin erilaisin tavoin. Kuitenkin, koska rikollisuuden toimintaympäristönä toimii kyberavaruus, tietyt motiivit voivat painottua toisia enemmän. Esimerkiksi tietoverkkojen ja -järjestelmien kautta tapahtuvan rikollisuuden näennäisen anonymiteetin ja etenkin rikollisuuden teollistumisen myötä saavutettavan helppouden voidaan olettaa houkuttelevan hyvinkin erilaisin tavoin motivoituneita ihmisiä suorittamaan rikoksia juuri tietoverkkojen ja tietotekniikan kautta.

Kilger ja kumppanit (2004) jakavat kyberrikollisuuden motiivit valtiollisesta tiedustelusta peräisin olevaa MICE (Money, Ideology, Compromise, Ego) -lyhennettä (Levchenko, 1988) mukaillen kuuteen osaan. Nämä kuusi motiivia ovat raha (money), viihde (entertainment), itseriittoisuus (ego), aatteellisuus (cause), sisäänpääsy yhteisöön (entrance to social group) sekä sosiaalisen statuksen tavoittelu (status), joista tutkijat ovat johtaneet lyhenteen MEECES. Holt ja Kilger (2012) valitsevat artikkelissaan edellä mainittuihin pohjaten merkittävimmiksi kyberrikollisten motiiveiksi viihteen, sosiaalisen statuksen tavoittelun, pääsyn sosiaaliseen ryhmään sekä taloudelliset motiivit. Melko samanlaiseen päätelmään pääsevät myös Hald ja Pedersen (2012), jotka nostavat yhtä lailla esiin taloudellisen motivaation, mutta sen lisäksi myös koston, uteliaisuuden ja pahamaineisuuden, joista kaksi viimeisintä ovat suoraan verrattavissa Holtin ja Kilgerin (2012) viihteellisiin motiiveihin ja sosiaalisen statuksen tavoitteluun.

Todellisuudessa motiivit kuitenkin esiintyvät harvoin kyseisellä tavalla selkeinä ja erillisinä kokonaisuuksina, kuten ne ovat tieteellisessä tutkimuksessa esitetty, vaan sekoittuvat toisiinsa (Kilger, 2011). Erityyppiset rikolliset voivat esimerkiksi jakaa samat ensisijaiset motiivit, vaikka tekojen varsinaiset päämäärät olisivat täysin erilaiset (Holt & Kilger, 2012).

Mahdollisesti yleisimmin kyberrikollisia motivoi kyberrikoksen suorittamiseen taloudelliset motiivit. Taloudellisella hyödyllä motivoitujen kyberrikosten yleisyys johtunee internetin laajentumisesta sekä rahaliikenteen ja henkilökohtaisten tietojen liikkumisesta sen kautta yhä suuremmissa määrin (Neufeld, 2010; Franklin, Perrig, Paxson & Savage, 2007; Hyppönen, 2011). Tämän tyyppisessä rikollisuudessa rikollinen suorittaa rikollisen tekonsa vain saavuttaakseen rahallista hyötyä joko suoraan rikoksesta tai epäsuorasti sen seurauksena. Esimerkkinä suorasta hyödystä toimivat etenkin 2010-luvulta lähtien yleistyneet ransomware-hyökkäykset, joissa saastuneen tietokoneen tiedostot salataan ja käyttäjältä kiristetään lunnaita salauksen purkavaa avainta vastaan (F-Secure, 2021). Epäsuorasti kyberrikollisuudesta voi hyötyä esimerkiksi kauppaamalla varastettua dataa verkossa. Taloudellisia motiiveja voidaan myös jakaa edelleen alaluokkiin esimerkiksi sen perusteella, että motivoiko tekijää rikokseen pakottava rahantarve, kuten köyhyydestä selviytyminen, vaiko pelkkä ahneus (Braithwaite, 1993). On myös mahdollista, että motivaatio muuttuu tarpeesta ahneudeksi rikosten aikana sen jälkeen, kun pakottava rahantarve on täytetty (Hutchings, 2013).

Eräs pitkäikäisimmistä motivaattoreista teknologian hyväksikäytössä ja hakkeroinnissa ovat viihteelliset motiivit, jotka ovat olleet läsnä yhtä pitkään kuin itse informaatioteknologiakin (Kilger ym., 2004). Tietotekniikan väärinkäyttö huvin vuoksi otti ensimmäiset askeleensa jo 1900-luvun puolivälissä, jolloin kohteena olivat suurtietokoneet ja päänvaivan aiheuttaminen niitä operoineille työntekijöille. Vaikkakin viihteellisesti motivoitunut teknologian väärinkäyttö on sekoittunut taloudellisiin motiiveihin esimerkiksi 70- ja 80-luvuilla yleisöpuhelinten kaukopuheluiden aktivoinnissa maksutta käyttöön, ovat viihteelliset motiivit epäilemättä tuottaneet kohteilleen vähiten seuraamuksia (Holt & Kilger, 2012).

Tämänkaltainen viihteellisesti motivoitunut toiminta, vaikka onkin usein samanaikaisesti rikollista, ei pyri yleensä olemaan tuhoisaa vaan suorastaan leikkimielistä. Viihde motiivina hakkeritoiminnassa ja kyberrikollisuudessa on pitänyt suosionsa kautta aikojen erilaisin tavoin orientoituneiden tekijöiden keskuudessa, eikä ole syytä olettaa sen häviävän lähitulevaisuudessa. Kyseinen motiivi vastaa kuitenkin lopulta vain pienestä osasta hakkeriyhteisöjen ja kyberrikollisten tekemisten motivaatiosta. (Kilger ym., 2004.)

Motiiveista itseriittoisuuden eli egon kohentaminen ja sosiaalisen statuksen tavoittelu liittyvät melko läheisesti toisiinsa ja niihin sisältyvät piirteet ovatkin siksi joissakin tapauksissa luokiteltu täysin jommankumman alle (Holt & Kilger, 2012). Motiiveja on kuitenkin syytä tarkastella myös erillään, sillä niiden voidaan nähdä eroavan toisistaan etenkin sosiologisesta näkökulmasta; motivoituminen itseriittoisuuden kautta viittaa melko yksiselitteisesti henkilön omaan ajatusmaailmaan, kun puolestaan statuksen tavoittelu on sosiaalinen ilmiö, jossa yksilö pyrkii meriittiensä perusteella nousemaan jossakin hierarkiassa korkeammalle (Holt, 2007; Kilger ym., 2004).

Itseriittoisuuden kautta motivoituminen pohjautuu positiiviseen vahvistamiseen, joka puolestaan liittyy vahvasti välineelliseen ehdollistumiseen.

Tämänkaltainen psykologinen palkinto esimerkiksi tietoteknisten turvajärjestelyjen ohi livahtamisesta tai mistä tahansa muusta tapahtumasta, jossa käyttäjä saa teknologian toimimaan haluamallaan tavalla, voi olla motivaatioista kaikista vahvin ja peittää alleen monet muut rajoitteet, joita yksilö saattaa tuntea. (Kilger ym., 2004; Martela & Jarenko, 2014.)

Sosiaalisen statuksen tavoittelu puolestaan nousee tärkeäksi motivaattoriksi siksi, että hakkerien ja kyberrikollisten yhteisöt ovat usein vahvoja meritokratioita, joissa yksilön status määräytyy tämän taitotason ja saavutusten perusteella. Koska näiden yhteisöjen kommunikaatio tapahtuu lähestulkoon yksinomaan verkon kautta ja monesti yksinkertaisessa muodossa, kuten tekstipohjaisesti, voi statuksen kommunikointi toisille olla hankalaa. Tämä voi puolestaan johtaa jäsenten tai ryhmien välisiin konflikteihin siitä, kuka tai ketkä ovat hierarkiassa korkeammalla. Konfliktit saattavat jäädä pelkkään alatyyliseen kommentointiin, mutta joissakin tapauksissa se saattaa muuntua kilpailuksi, jotka puolestaan voivat vuotaa julkisten verkkojen ja järjestelmien puolelle ja aiheuttaa niille vahinkoa. Esimerkiksi 90-luvun alussa hakkeriryhmä *Masters of Deception* erosi erimielisyyksien vuoksi emoryhmästään nimeltä *Legion of Doom* ja tästä seuranneessa ”jengisodassa” muun muassa varasti luottotietoja, murtautui yksityisille tietokoneille ja järjesteli uudelleen puhelinlinjoja. Aiheen ympärille kokoontuvat konferenssit kuten yhdysvaltalainen *DEF CON* voivat lieventää sekä vähentää tämänkaltaista kilpailua tarjotessaan turvallisen ja suljetun ympäristön hyökkäysten harjoitteluun. (Holt & Kilger, 2012; Kilger ym., 2004; Slatalla & Quittner, 1995.)

Sosiaaliseen statukseen motivaationa kytkeytyy läheisesti myös sisäänpääsy yhteisöön. Edellä mainitusti, hakkeri- ja kyberrikollisyhteisöt ovat vahvoja meritokratioita ja yhteisöön pääsy vaatiikin yksilöltä tiettyä taitotasoa. Lupaus tämänkaltaiseen ryhmään rekrytoinnista voi toimia vahvana motivaattorina etenkin aloittelijoille, jotka eivät vielä ole yhteisön vaatimalla taitotasolla ja haluavatkin juuri sisäänpääsyn varjolla harjoittaa ja testata omia taitojaan. (Kilger ym., 2004.)

Vahvan sosiaalisen ulottuvuuden sisältää myös aatteellinen eli ideologinen motiivi kyberrikollisuuteen, josta eräänä tuoreimpana esimerkkinä voidaan mainita ISIS-terroristijärjestön noin 2010-luvun puolesta välistä alkanut kybervaikuttaminen. Näillä keinoilla järjestö pyrki vaikuttamaan julkiseen mielipiteeseen itsestään muiden muassa siksi, että onnistuisi rekrytoimaan uusia jäseniä sekä vähentämään vastarintaa toiminta-alueillaan. (Awan, 2017.) Internetin laajentumisen myötä eri toimijoiden on helpompi tuoda esiin poliittisia, nationalistisia tai, kuten aiemmassa esimerkissä, uskonnollisia aatteita ja uskomuksiaan, sekä hankkia niille seuraajia Holt & Kilger, 2012). Tärkeänä esimerkkinä poliittisten aatteiden motivoimasta kybervaikuttamisesta ja -rikollisuudesta toimii vuoden 2016 Yhdysvaltojen presidentinvaalit, joiden lopputulokseen Venäjä pyrki, ja mitä ilmeisimmin onnistuikin vaikuttamaan kyberavaruuden kautta (Office of the Director of National Intelligence, 2017).

3.2 Kyberrikollisten luokittelu

Useissa tapauksissa, varsinkin mediassa, termiä *hakkeri* käytetään synonyyminä kyberrikolliselle. Esimerkiksi Oxfordin yliopiston Lexico-sanakirjapalvelu (2021) kuvailee hakkeria henkilöksi, joka käyttää tietokoneita päästäkseen luvatta käsiksi dataan. Määritelmää tarkennetaan kuitenkin yleisesti etenkin tieteellisessä tutkimuksessa siten, että hakkeri voi tunkeutua järjestelmiin sekä luvattomasti aiheuttaakseen haittaa että täysin luvallisesti järjestelmänvalvojan luvalla (Holt & Kilger, 2012; Schell & Dodge, 2002).

Hakkerit voidaan jakaa toiminnan luvallisuuden tai luvattomuuden sekä eettisyyden perusteella kolmeen yleisesti tunnistettuun ryhmään:

- **Mustahatut** (Black hats). Vallan, suuttumuksen tai vihan motivoimia hakkereita, jotka murtautuvat verkkoihin luvatta ja saattavat varastaa tai tuhota sieltä löytämäänsä dataa (Sabillon, Cavaller, Cano & Serra-Ruiz, 2016).
- **Harmaahatut** (Grey hats). Harmaahatut sijoittuvat eettisesti musta- ja valkohattujen välimaastoon. Tämänlaiset hakkerit voivat esimerkiksi työskennellä rikosvastuun rajalla itsenäisesti löytääkseen turvallisuuspuutteita ja haavoittuvuuksia tai olla konsultteina työskenteleviä entisiä mustahattuja. (Sabillon ym., 2016; Kirsch, 2014.)
- **Valkohatut** (White hats). Turvallisuusasiantuntijoina tai muuten lain mukaan ja eettisesti työskenteleviä hakkereita, jotka pyrkivät löytämään mahdolliset haavoittuvuudet ennen vahingollisesti toimivia tekijöitä. (Sabillon ym., 2016.)

Siinä missä hattujen värin mukaan lajittelu antaa melko tarkan yleiskuvan, se on kuitenkin hyvin suurpiirteinen tapa luokitella hakkereita. Tällä tavoin ryhmiin jakaminen antaa jokseenkin yksinkertaistetun kuvan luokiteltujen toiminnasta, jonka lisäksi luokittelu on melko jäykkä, eikä jätä paljonkaan liikkumavaraa. Toisaalta tämänkaltainen luokittelu on helpottaa tarkastelua etiikan näkökulmasta.

Tehokkaampi ja tarkempi tapa luokitella etenkin juuri kyberrikollisia, on tarkastella toimijoiden motiiveja sekä päämääriä. Hyppönen (2011) jakaa verkossa tapahtuvat hyökkäykset ja niiden tekijät kolmeen ryhmään päämäärien avulla. Nämä ryhmät ovat rikolliset, haktivistit ja valtiot, joista ensimmäiseen Hyppönen luokittelee kaikki ne toimijat, jotka suorittavat rikoksia verkossa ja yleisimmin motiivinaan ainoastaan taloudellinen hyöty. Haktivisteihin puolestaan kuuluvat sellaiset tekijät, joiden motiivien taustalla on jokin tietty ideologia tai mielipide, jonka puolesta he tahtovat protestoida. Viimeiseen ryhmään kuuluvat valtiot, jotka pyrkivät vaikuttamaan muihin valtioihin, niiden kansalaisiin tai jopa omiin kansalaisiinsa tai hankkimaan näiltä tietoa.

Rieb, Gurschler ja Lechner (2017) lisäävät Hyppösen (2011) luokitteluun rikollisten sekä valtioiden lisäksi kaksi uutta kategoriaa; niin kutsutut *script kiddiet* sekä työntekijät (employees). *Script kiddiet* ovat useimmiten nuoria ja taidoiltaan

heikompia toimijoita, jotka usein käyttävät hyökkäyksissään muiden tuottamia työkaluja. Tällaisia toimijoita motivoi usein vain uteliaisuus tai pahamaineisuus syvällisempien motiivien sijasta. Työntekijät -kategoriaan kuuluvat organisaatioiden sisäpiiriläiset, joita motivoi usein negatiivisten työperäisten kokemusten aiheuttama kostonhimo tai taloudellinen hyöty. Työntekijöistä tekee varteenotettavan kyberrikollisten ryhmän heidän käyttöoikeutensa työnantajansa IT-infrastruktuuriin sekä fyysisesti että digitaalisesti.

BAE Systems (2021) puolestaan ei jaottele toimijoita selkeärajaisesti esimerkiksi pelkästään rikollisiin, vaan tarkastelee toimijoita heidän roolinsa mukaan kyberrikollisuuden toimintaketjuissa. BAE Systemsin kategoriat ovat aktivisti (the activist), nuoriso (the getaway), sisäpiiriläinen (the insider), muuli (the mule), valtiollinen toimija (the nation state actor) ja ammattilainen (the professional). Verrattaessa Hyppösen (2011) luokitteluun, lähimpänä rikolliset -kategoriaa edellisistä ovat nuoriso, muuli sekä ammattilainen. Nuoriso -kategoria on myös hyvin lähellä Riebin ym. (2017) *script kiddietä*, joskin BAE Systems lisää kuvaukseen varsinaisen rikosvastuun välttämisen matalan iän vuoksi. Nuoret toimivat kokeneempien rikollisten kuten ammattilaisten tai muulien asettamina välikäsinä tai harhautuksina. Ammattilaiset suorittavat rikoksensa esimerkiksi laillisilta vaikuttavaa kulissia käyttäen ja pahimmat riskit itse välttäen. Muulit ovat usein rahanpesijöitä, jotka muuttavat varastetut varat ”puhtaiksi” ja ovatkin siksi usein suurimmassa riskissä jäädä kiinni.

BAE Systemsin kategorioista aktivistit sekä valtiolliset toimijat ovat hyvin yhteneväisiä Hyppösen (2011) vastaavien kanssa. Sisäpiiriläinen -kategoria puolestaan vastaa Riebin ja kumppaneiden (2017) työntekijät -kategoriaa, joskin BAE Systems lisää määritelmään vaihtoehtoisia motivaatioita, kuten esimerkiksi kiristyksen kohteena olemisen.

Taulukko 1 toimii yhteenvetona alaluvussa käsitellyille Hyppösen (2011), Riebin ym. (2017) ja BAE Systemsin (2021) kyberrikollisten luokitteluille, toimintatavoille sekä näiden motiiveille rikosten suorittamiseen.

Taulukko 1 Kyberrikollisten luokittelu, motiivit ja toimintatavat

Hyppönen (2011)	Rieb ym. (2017)	BAE Systems (2021)	Motiivi	Toiminta
Rikolliset	Kyberrikolliset	Ammattilainen	Taloudellinen	Ammattimainen
	Työntekijät	Sisäpiiriläinen	Kosto, taloudellinen	Kiristyksen uhri, huolimattomuus, tahallisuus
	"Script kiddiet"	Muuli	Taloudellinen	Jälkien peittely, välinpitämättömyys
		Nuoriso	Uteliaisuus, maine, taloudellinen	Valmiiden työkalujen käyttö, manipulointi
Haktivistit	Haktivistit	Aktivisti	Ideologinen	Ideologian edistäminen, vastustajien häirintä
Valtiot	Valtiot	Valtiollinen toimija	Taloudellinen, ideologinen	Valtion edun ajaminen

3.3 Kyberrikollisuuden aiheuttamia haittoja

Näkyvin ja ehkä myös merkittävin kyberrikollisuuden aiheuttama ongelma on taloudellisen hyödyn menettäminen. Kyberrikokset voivat aiheuttaa taloudellisia menetyksiä suoraan rikoksen seurauksena, esimerkiksi kaupan pysähtymisenä, korjauskustannuksina ja datan palautuksen kustannuksina tai välillisesti esimerkiksi maine- ja brändihaittana yritykselle, jolloin asiakaskunnan mielikuva yrityksestä muuttuu hyökkäyksen seurauksena siten, että he eivät enää tahdo kuluttaa yrityksen tuotteita tai palveluita (Center for Strategic and International Studies & McAfee, 2018; Smith, Jones, Johnson & Smith, 2019). CSIS ja McAfee (2018; 2020) arvioivat taloudellisten haittojen olleen vuonna 2018 noin 600 miljardia dollaria (USD) eli noin 0,8 % maailman bruttokansantuotteesta ja vuoden 2020 haittojen olleen noin 945 miljardia dollaria eli jo noin prosentin maailman bruttokansantuotteesta. Lisäksi kyberturvallisuuteen on panostettu vuonna 2020 noin 145 miljardilla dollarilla, joten kyberrikollisuuden kokonaishaitta maailmantaloudelle on ollut noin biljoonan dollarin luokkaa (CSIS & McAfee, 2020).

Joidenkin haittojen kohdalla tarkkaa rahallista summaa ei voida määrittää. Tällaisia haittoja ovat esimerkiksi edellä mainitut maine- ja brändihaitat, heikompi tuottavuus, verkon käytön vähentäminen tai rajoittaminen riskeistä johtuen ja kyberturvaan investointi, jota ei olisi välttämättä tarvittu turvallisemmassa ympäristössä. (CSIS & McAfee, 2020.)

Mainehaitat voivat edellä mainitusti vaikuttaa asiakkaiden halukkuuteen kuluttaa yrityksen tuotteita tai palveluita ja julkisesti median käsittelemät kyberturvallisuuspuutteet voivat esimerkiksi laskea yrityksen osakkeen arvoa (CSIS & McAfee, 2018; Smith ym., 2019). Tästä johtuen, murron kohteeksi johtuneet yritykset saattavat yrittää peitellä tapahtunutta välttääkseen suuremmat taloudelliset haitat. Esimerkkeinä vastaavista tapauksista toimivat yhdysvaltalainen Uber, jonka tietoturvajohtaja yritti todistetusti peitellä tietomurtoa (Khosrowshahi, 2017; Chappell, 2018) ja suomalainen Psykoterapiakeskus Vastaamo, jonka aiempaa toimitusjohtajaa syytetään tietomurtotapauksen peittelystä (Hämäläinen, 2021).

Kuten Vastaamon tapauksessa, joissakin tapauksissa kyberrikollisuuden haittavaikutukset eivät rajoitu ainoastaan niin kutsuttuun kyberavaruuteen vaan vuotavat myös fyysisen maailman puolelle. Esimerkiksi juuri mainitun Vastaamo-tapauksen yhteydessä tietomurron kohteena olivat psykoterapiakeskuksen potilastiedot eli jo valmiiksi mahdollisesti haavoittuvaisessa tilassa olevat henkilöt, jotka ovat tietovuodon jälkeen ilmoittaneet mielenterveysoireittensa pahentuneen. (Grönroos, 2020; Rantavaara, 2020.)

Terveydenhuollon alalla on lähivuosina ollut muitakin tapauksia, joissa kyberhyökkäys on vaikuttanut fyysisen maailman toimintoihin ulottuen jopa itse hoitotyöhön. Esimerkiksi WannaCry -kiristyshaittaohjelma on häirinnyt vuodesta 2017 nykypäivään terveydenhuollon toimijoita maailmanlaajuisesti. WannaCry on tullut tunnetuksi tehokkaasta levittäytymisestään ja se onkin levinnyt etenkin terveydenhuollon ja teollisuuden alojen toimijoiden keskuudessa aiheuttaen niin pysähdyksiä tuotannossa kuin potilaiden vastaanottamisen keskeytyksiä (Seri, 2019; Riggi, 2020). Vuonna 2020 eräs toinen kiristyshaittaohjelma pakotti saksalaisen sairaalan sulkemaan potilasvastaanottonsa, jonka seurauksena yksi sairaalaan kuljetettavana oleva potilas jouduttiin siirtämään toiseen sairaalaan, minkä seurauksena potilas kuoli ambulanssiin. Tapauksen spekuloitiin olevan ensimmäinen kerta, kun kyberrikos on aiheuttanut kuoleman, mutta lopulta syytettä ei saatu nostettua. (Reuters, 2020; Ralston, 2020.) Kuitenkin, jos kyseiset haittaohjelmat jatkavat yleistymistään aiemmalla vauhdillaan, voivat tämänkaltaiset tapaukset yleistyä tulevaisuudessa.

Hengen ja terveyden lisäksi kyberrikollisuuden aiheuttamista fyysisen maailman haitoista voidaan mainita esimerkiksi vahingot teollisuudelle. Useimmissa tapauksissa haitat ovat tulleet tuotannon hidastumisesta tai pysähtymisestä (Seri, 2019) esimerkiksi juuri kiristyshaittaohjelmien vuoksi, mutta joissakin tapauksissa kyberhyökkäys on jopa tuhonnut laitteistoa. Näin toimi Stuxnet, joka tuhosi uraanin jalostamiseen käytettyjä sentrifugeja Iranissa ja oli ensimmäinen tunnettu haittaohjelma, joka pystyi tuottamaan vahinkoa laitteistolle. (Langner, 2011) Stuxnetin jälkeen esimerkiksi Industroyer -haittaohjelma on tehnyt

vahinkoa sähköjärjestelmille ja sen on epäilty pystyvän myös vahingoittamaan muuta kriittistä infrastruktuuria (Cherepanov & Lipovsky, 2017).

3.4 Kyberrikollisuuden mahdollistavat haavoittuvuudet sekä niiden torjunta ja ehkäisy

Suureen osaan tietojärjestelmätieteen tutkimusalalle ja sitä sivuaville aloille tehdystä tutkimuksesta on vakiinnuttanut asemansa käsitys siitä, että informaatioteknologian väärinkäyttö on väistämätöntä. Ajatusmallin mukaan kyberhyökkäyksiä ja kyberrikollisuutta ei voida kokonaan pysäyttää, vain parhaimmillaankin torjua asettamalla toiminnan tielle mahdollisimman hankalia esteitä. (Neufeld, 2010.) Tämänkaltaisen ajattelun ympärille perustuu pitkälti myös koko kyberturvallisuuden tieteenala (Craigen, Diakun-Thibault & Purse, 2014). Jotta kyberturvallisuutta voidaan kehittää ja mahdollinen vihamielinen toiminta torjua, on tarkasteltava heikkouksia ja riskejä järjestelmissä tai organisaatioissa (Cebula, Popeck & Young, 2014).

Kyberturvallisuuden käsitteeseen liittyvät vahvasti ihmiset joko kohteina tai välineinä turvallisuusrikkomuksissa tai rikoksissa, kun taas esimerkiksi tietoturvallisuuden käsitteessä ihmisen rooli on vain lähinnä olla osana turvallisuusprosessia (Von Solms & Van Niekerk, 2013). Ihmisten roolin tunnistaminen kyberturvallisuudessa ja kyberrikollisuuden torjunnassa onkin ensisijaisen tärkeää, sillä riippumatta siitä, kuinka teknisesti turvallinen jokin järjestelmä tai verkko on, inhimillinen tekijä tuo silti aina mukanaan haavoittuvuuden (Cebula ym., 2014; Conteh & Schmick, 2016.). Henkilöiden kautta tehtyjä eli käyttäjää manipuloiden (social engineering) tehtyjä kyberhyökkäyksiä voivat olla esimerkiksi tietojenkalastelu (phishing) ja seuraaminen (tailgating), joista ensimmäinen tapahtuu todennäköisesti kokonaan verkossa esimerkiksi aidolta vaikuttavien verkkosivujen tai sähköpostien kautta, siinä missä jälkimmäinen voidaan suorittaa esimerkiksi seuraamalla kohdehenkilöä tilaan, johon hyökkääjällä ei ole pääsyä. (Conteh & Schmick, 2016.)

Tämänkaltainen kyberrikollisuus on kasvanut tasaisesti etenkin siksi, että se tarjoaa melko vahvan anonymiteetin ja pienen riskin suhteessa mahdolliseen hyötyyn. Organisaatiotasolla ongelmaa on mahdollista torjua parhaiten monitasoisella puolustusstrategialla, joka sisältää hyvän turvallisuuspolitiikan, työntekijöiden koulutusta, turvallisuussäännösten valvontaa, teknisiä turvakeinoja sekä fyysistä kulunvalvontaa tietoturvaherkkiin tiloihin. Yhdistelemällä näitä ennaltaehkäiseviä toimia, on mahdollista rakentaa toimiva monitasoinen puolustus kyberhyökkäyksiä ja kyberrikoksia vastaan. (Conteh & Schmick, 2016.)

Vaikka käyttäjän manipuloinnilla tapahtuvat hyökkäykset ovat selvästi yleistyneet, hyökkäysten ja rikosten suorittaminen hyödyntämällä teknologisia haavoittuvuuksia on myös edelleen yleistä. Teknologisilla haavoittuvuuksilla tarkoitetaan laite-, ohjelmisto- ja järjestelmätason ongelmallista tai arvaamatonta toimintaa, kuten esimerkiksi laitekapasiteetin loppumista, ohjelmiston syntaksi-

tai logiikkavirheitä ja järjestelmien epäsopivuutta valittuun tehtävään. (Cebula ym., 2014.) Tämän tyyppiset haavoittuvuudet johtuvat useimmiten heikosta laitteiston, ohjelmiston tai järjestelmän suunnittelusta tai vaatimusmäärittelystä (Elahi, Yu & Zannone, 2010).

Teknologisia haavoittuvuuksia on mahdollista korjata ja siten torjua kyberhyökkäyksiltä esimerkiksi päivittämällä ohjelmistot ajantasaisiin ja paikattuihin versioihin. Ohjelmisto- ja järjestelmätason heikkouksia voidaan myös ehkäistä esimerkiksi rajoittamalla järjestelmänvalvojaoikeuksia ja kenelle niitä myönnetään, vaikkakin järjestelmänvalvojiin liittyvät heikkoudet ja haavoittuvuudet voidaan myös nähdä käyttäjiin liittyvinä heikkouksina. Myös salasanat ja niiden turvallisuus voidaan nähdä teknologisena haavoittuvuutena, vaikkakin niihin liittyy lähes aina myös inhimillisiä tekijöitä. (Chowdhury, 2016.)

Laitteiston haavoittuvuudet puolestaan voivat usein olla hankalampia ja hitaampia korjata, sillä yleisimmin korjaus vaatii kokonaisten fyysisten laitteiden vaihtamista uusiin, jotka eivät ole haavoittuvaisia tai saastuneita. Kuitenkin joissakin tapauksissa, kuten keskussuorittimissa vuonna 2018 havaitun Spectre -haavoittuvuuden kanssa, kaikkien laitteiden korvaaminen ei ole mahdollista, joko käytännön tai taloudellisista syistä johtuen (Kocher, Horn, Fogh, Genkin, Gruss, Haas, Hamburg, Lipp, Mangard, Prescher, Schwarz & Yarom, 2018). Ratkaisuna laitetason koodin kääntäjä ohjattiin toimimaan eri tavoin, jolloin suorittimien kokonaissuorituskyky laski noin 2–14 % (Linton, 2018; Hachman, 2018).

Edellä mainittujen lisäksi eräs merkittävä kategoria haavoittuvuuksia käsitellessä ovat sisäisten prosessien häiriöt. Sisäisiä prosesseja ovat esimerkiksi organisaatioiden toiminnot, roolit ja vastuut, suorituskyvyn mittarit sekä koulutus. Sisäisten prosessien korjaaminen voi usein olla erityisen haastavaa, koska niiden perustana toimii organisaation kulttuuri ja totutut toimintatavat, joista voi olla hankala päästä tehokkaasti eroon. Esimerkiksi huono irtisanomis- tai lomautuspolitiikka voi aiheuttaa entisissä työntekijöissä kostonhaluisuutta, joka voi ilmetä tahallisena prosessien häirintänä tai tuhoamisena (Neufeld, 2010). Näin voi toimia ja motivoitua aiemmin mainittu kyberrikollistyyppi *sisäpiiriläinen* (insider).

Merkittävänä käytännön esimerkkinä sisäisten prosessien hajoamisesta voidaan käyttää Nokian strategian epäonnistumiseen älypuhelinaikakauden alkuvuosina, joka johti lopulta yrityksen matkapuhelinliiketoiminnan lopettamiseen. 1990-luvulla Nokia tunnettiin laajalti innovatiivisena ja melko ketteränä yhtiönä, joka vastasi tehokkaasti muuttuviin markkinaolosuhteisiin esimerkiksi innovoimalla ja kasvattamalla uusia liiketoimintoja. Kuitenkin 2010-luvun vaihteessa Nokia oli jo niin suuri yhtiö, että pienempien liiketoimintojen avulla tulosvajeenpaikkaaminen ei enää onnistunut, jonka vuoksi ainoaksi ansaintakeinoksi jäivät matkapuhelinliiketoiminnot, mitkä puolestaan olivat selvästi markkinoita ja kilpailijoita jäljessä. Nokian kykenemättömyys reagoida muuttuneeseen organisaatiorakenteeseen sekä siihen yhdistettyyn muuttuneeseen markkinatilanteeseen aiheutti lopulta matkapuhelintoimintojen lopettamisen. (Rooij, 2015.)

4 NETTIKIUSAAMINEN KYBERRIKOLLISUUDEN MUOTONA

Tässä luvussa tarkastelemme edellisissä luvuissa esiteltyjä nettikiusaamista ja kyberrikollisuutta yhteisessä kontekstissa ja pyrimme tekemään johtopäätelmiä niiden yhtäläisyyksistä ja eroavaisuuksista. Luvussa pohditaan nettikiusaamista kyberrikollisuuden muotona verraten ilmiötä perinteiseen kiusaamiseen ja sen sijoittumiseen perinteiseen rikollisuuteen ja lakiin nähden.

Luvussa käsitellään myös kyberturvallisuuden tieteenalalla saatua informaatiota kyberrikollisuuden ja kyberhyökkäysten torjunnasta, joita pyritään soveltamaan apukeinona ja viitekehyksenä nettikiusaamisen torjunnalle.

4.1 Voiko nettikiusaaminen olla kyberrikos?

Tutkielman toisessa luvussa sivuttiin nettikiusaamisen muotojen yhteydessä rikoslain määritelmiä eräistä rikosnimikkeistä, jotka kiusaaminen mahdollisesti täyttää. Näitä rikosnimikkeitä ovat esimerkiksi rikoslain (1889/39) 24 luvusta viestintärauhan rikkominen (1 a §), kunnianloukkaus (9 §) ja yksityiselämää loukkaavan tiedon levittäminen (8 §) sekä 25 luvusta laiton uhkaus (7 §) ja vainoaminen (7 a §).

Viestintärauhan rikkomisen tunnusmerkit täyttyvät Willardin (2004) nettikiusaamisen muodoista esimerkiksi ”fleimaamisessa”, häirinnässä sekä kybervainoamisessa, näiden pitäen sisällään loukkaavan sisällön lisäksi toiminta on jatkuvaa, määrätietoista ja tapahtuu elektronisten viestintäkanavien kautta. Luonnollisesti kybervainoaminen voidaan liittää myös rikosnimikkeeseen vainoaminen, vaikkakin muutkin jatkuvasti tapahtuvat nettikiusaamisen muodot voivat saada vainoamisen tunnusmerkistön täyttäviä piirteitä. Yksityiselämää loukkaavan tiedon levittäminen puolestaan on lähimpänä mustamaalausta sekä paljastamista. Laiton uhkaus ei välttämättä suoraan vastaa mitään mainituista nettikiusaamisen muodoista, mutta voi esiintyä lähes jokaisen yhteydessä. Kunnianloukkaus puolestaan on rikosnimike, joka melko varmasti esiintyy useissa

nettikiusaamistapauksissa, riippumatta mihin kategoriaan kiusaaminen kuuluu. Mahdollisia muita rikosnimikkeitä voivat olla esimerkiksi pakottaminen, salakuuntelu tai -katselu ja vahingonteko, mutta tutkielman rajauksen vuoksi tässä tapauksessa havainnollistamiseen käytetään lähinnä edellä mainittuja. (Lahtinen, 2019.) Lisäksi nettikiusaamisen on katsottu aiheuttavan yksinäisyyttä, joka voi johtua eristäytymisestä negatiivisten kokemusten vuoksi, mikä puolestaan voi haitata yksilön internetin vapaata käyttöä. Tällöin nettikiusaaminen voidaan nähdä jopa ihmisoikeusloukkauksena (United Nations, 2016).

Rikosnimikkeiden sopivuuden lisäksi kiusaamisesta ja sen seurauksista on nostettu useita syytteitä. Suomessa vastaavista tapauksista on myös annettu tuomioita ja tapauksia on käsitelty korkeimmillaan hovioikeudessa (Helsingin hovioikeus, 2016). Rikosnimikkeinä on käytetty esimerkiksi kunnianloukkausta, mutta jopa pahoinpitelyä ja seurauksina ovat tyypillisesti olleet sakot ja korvaukset (Nieminen, 2019; Ahonen, 2020).

Useissa kiusaamistapauksissa teko on suoritettu kyberavaruudessa käyttäen avuksi tietoverkkoja ja verkon palveluita tai pelkästään tietoverkkojen kautta, jolloin näitä tapauksia voidaan pitää joko kokonaan tai ainakin osittain nettikiusaamisena (Tenhunen, 2016; Nieminen, 2019). Itse kiusaamisen pääpiirteet ovat kuitenkin hyvin samankaltaisia perinteisen kiusaamisen kanssa, jonka vuoksi näidenkin tapausten tekijöitä voidaan pitää yhtä lailla rikosvastuullisina. Tällöin rikoksena pidettävää toimintaa harjoitetaan teknologian tai tietoverkkojen avulla tietoverkoissa ja -järjestelmissä, mikä puolestaan täyttää yleisimmät kyberrikollisuuden määritelmät (Poliisi, 2021; Gordon & Ford, 2006). Tällä yksinkertaistetulla käsitteenmäärittely- ja päättelyketjulla voitaisiinkin siis sanoa nettikiusaamisen olevan jonkinasteinen kyberrikos.

Nettikiusaamisen kuulumista tähän rikollisuuden kategoriaan on syytä tarkastella myös rikoksen tekijän motivaation kannalta. Edellisessä luvussa tarkastelluista Kilgerin ja kumppaneiden (2004) määrittelemästä kuudesta kyberrikollisten motiivista nettikiusaamiseen pätevät ainakin neljä; viihde, itseriittoisuus, sisäänpääsy yhteisöön sekä sosiaalinen status. Wilton ja Campbell (2011) löysivät tutkimuksessaan merkkejä viihteeseen ja itseriittoisuuteen liittyvistä motiiveista, kuten *huomion saamisesta muilta* ja *jonkin haluamisesta joltakulta toiselta*. Varjas, Talley, Meyers, Parris ja Cutts (2010) puolestaan havaitsivat tutkimuksessaan kiusaamisen motivaatioksi muiden muassa *hyväksynnän hakemisen* sekä *uuden persoonan kokeilemisen*, jotka voidaan nähdä muotoina ryhmään tai yhteisöön sisäänpääsyn tavoittelulle ja oman sosiaalisen statuksen nostattamiselle.

Rahallisten tai ideologisten motiivien yhteydelle nettikiusaamiseen ei tutkielmaa tehtäessä löytynyt merkittävää tukea. Tosin ainakin yhdessä aineistossa käsiteltiin yhteiskunnallisten päätöksentekijöiden kokemaa kiusaamista ja nettikiusaamista, jolla on todennäköisesti jokin yhteys kiusattujen asemaan yhteiskunnassa ja ideologiaan sen takana. Kiusaajien motiivit ovat kuitenkin todennäköisesti lopulta lähtöisin jostakin muualta, kuin pelkästään suoraan esimerkiksi poliittisesta ideologiasta. (Knuutila, Kosonen, Saresma, Haara & Pöyhtäri, 2019.)

4.2 Kyberrikollisuuden torjunta apukeinona nettikiusaamisen torjunnassa

Jos nettikiusaamisen torjuntaa pyritään tarkastelemaan kyberrikollisuuden torjunnan ja kyberturvallisuuden näkökulmasta, on huomioon otettava Neufeldin (2010) artikkelissaan mainitsema perusperiaate siitä, että informaatioteknologian väärinkäyttöä ei voida koskaan täysin estää, mutta sen tielle tulisi rakentaa mahdollisimman hankalia esteitä. Ajatusmallin siirtäminen nettikiusaamisen kontekstiin on siten ongelmallista, että netti- ja muun tyyppisessä kiusaamisessa toleranssin tulisi luonnollisesti olla nolla ja tavoitteena ilmiön lopettaminen kokonaan (KiVa Koulu, 2021). Neufeldin ajatusta mukaillen kuitenkin olisi ehkä tärkeämpää keskittyä muiden muassa kiusaamisessa käytettäville teknologisille keinoille esteiden rakentamiseen, jotta kiusaaminen vähenisi minimiinsä ja jäljelle jäävän osan seuraukset olisi mahdollista saada hallintaan, vaikka kiusaamisen uhreja olisikin syntynyt.

Mahdollisina teknologisina torjuntakeinoina voidaan ajatella esimerkiksi tehokkaampaa kiusaamisen tai muuten käyttäjäehtoja rikkovan käyttäytymisen ilmiantamista ja läpikäyntiä palveluntarjoajan toimesta. Esimerkiksi Facebook on kertonut lisäävänsä koneoppimisen ja algoritmien käyttöä väärän informaation torjunnassa alustallaan ensinnäkin estääkseen haitallisen informaation leviämistä, mutta myös lievittääkseen ihmismoderaattorien taakkaa tällaisen materiaalin käsittelyssä (Gillespie, 2020; Vincent, 2020). Toistaiseksi moderaattorit tekevät kuitenkin lopulliset päätökset suuresta osasta materiaalista, joten moderaattorien joutuminen tekemisiin haitallisen materiaalin suodattamisessa sosiaalisen median alustoilta on vielä toistaiseksi suuri ongelma.

Lisää ongelmia kuvattuun lähestymistapaan tuo se, että useissa sosiaalisen median palveluissa ja viestintäteknologioissa on mahdollista viestiä yksityisesti, jolloin palveluntarjoajan kajoamisessa käyttäjien viesteihin tai muuhun sisältöön liikutaan lähellä ihmisoikeuksien rajoittamista, vaikka tavoitteena olisi haitallisen sisällön kuten nettikiusaamisen rajoittaminen (United Nations, 2016).

Etenkin sosiaalisen median alustojen kohdalla vastuunkanto haitallisen materiaalin poistamisesta on ollut heikohkoa, ja usein juuri lain määräämän tason saavuttavaa. Torjunnan hyödyt olisivat todennäköisesti suuremmat, jos alustat panostaisivat torjuntaan proaktiivisesti enemmän kuin absoluuttisen minimin, jonka lait ja säädökset vaativat. (Grygiel & Brown, 2019.) Todennäköisesti tehokkain toimintatapa olisi kuitenkin säätää tarkempia alustojen tarjoajien toimintaa koskettavia lakeja.

Kyberrikollisuuden torjunnassa ja kyberturvallisuuden kehittämisessä on vuosikymmenten ajan käytetty toimintatapaa, jossa turvallisuuspuutteista, kuten teknisistä haavoittuvuuksista tai huonoista käytänteistä julkaistaan kriittisimmät tiedot vapaasti käytettäväksi sen jälkeen, kun kuvattu tietoturvapuute on korjattu (Google, 2021; F-Secure, 2021). Tällöin kohteena ollut taho on saanut tietoturvapuutteensa korjattua ajoissa, mutta haavoittuvuuden tunnistamisesta

ovat hyötyneet myös ulkopuoliset, jotka ovat voineet tarkistaa omat järjestelmänsä tai käytänteensä vastaavien uhkien varalta.

Vastaavaa tapaa toimia ehdottaa Olweus (2012), joka suosittelee nettikiusaamisen torjunnan keinona julkaisemaan anonymisoitua tietoa tapahtuneista nettikiusaamistapauksista julkisuuteen. Tällöin kiusaamistapauksen toimintamallit ovat suuremman yleisön tietoisuudessa, jonka vuoksi mahdollisten kiusaajien näkökulmasta kiinnijäämisen riski kasvaa suuresti, millä puolestaan on potentiaalia vähentää kiusaamista yleisellä tasolla. Lisäksi, vaikka tapausten tietojen julkistaminen ei suoraan vähentäisi aktiivista kiusaamista kiusaajien puolelta, kiusaamistapausten jatkuminen voidaan keskeyttää ja mahdollisten uusien tapausten syntymistä rajoittaa, kun varsinaiseen kiusaamiseen johtavat vaiheet ovat yleisesti tunnettuja.

Yhteys kyberrikollisuuden torjuntaan ja ehkäisyyn voidaan nähdä myös nuoruudessa tapahtuneen kiusaamisen yhteydessä vanhemmalla iällä tapahtuvaan rikollisuuteen. Nuorena kiusaamiseen syyllistyneiden henkilöiden on havaittu syyllistyvän rikoksiin merkittävästi enemmän aikuisuudessaan kuin sellaisten, jotka eivät ole kiusanneet nuorena. Rikoksen vähintään kolme kertaa uusineiden kohdalla kiusanneilla todennäköisyys oli noin viisinkertainen verrattuna niihin, jotka eivät olleet kiusanneet nuorena. Väkivaltarikosten kohdalla kiusaajat olivat kuudesta kahdeksaan kertaa todennäköisempiä syyllistymään tämänkaltaiseen rikokseen kuin ne, jotka eivät olleet kiusanneet. (Olweus, 2011.) Samankaltaista päättelyä hyödyntäen kuin kappaleessa 4.1, on mahdollista olettaa, että jos perinteisellä kiusaamisella on rooli esimerkiksi väkivaltarikoksiin syyllistymisessä myöhemmällä iällä, voi jo valmiiksi teknologiaorientoituneella nettikiusaajalla olla kohonnut mahdollisuus syyllistyä teknologian tai verkkojen kautta suoritettaviin rikoksiin, eli kyberrikoksiin.

5 YHTEENVETO

Nettikiusaaminen on saanut osakseen suurta huomiota sekä mediassa että tieteellisessä yhteisössä etenkin 2000-luvun alusta lähtien. Ilmiön kartoittamisen myötä on käynyt ilmi, että nettikiusaaminen on mekanismeiltaan ja esiintyvyydeltään hyvin samankaltaista kuin perinteinenkin kiusaaminen, sillä erotuksella, että nettikiusaaminen tapahtuu aina verkon ja tietoteknisten välineiden kautta.

Nettikiusaamisen määritelmät ovat vaihdelleet tutkijoiden näkemysten sekä aikakausien mukaan, mutta peruspiirteiltään nettikiusaaminen on määritelty kiusaamisen muodoksi, jossa tarkoituksellisesti ja toistuvasti aiheutetaan harmia kohteelle jonkin tietoteknisen välineen kautta (MLL, 2017). Suurimmassa määrin määritelmä on muuttunut siihen lisättyjen tai siitä poistettujen viestintämuotojen myötä (Kumar & Goldstein, 2018; Burgess-Proctor, Patchin & Hinduja, 2009). Määrittelyssä on myös tuotu esiin vallan epätasapainoa uhrin ja tekijän välillä (Olweus, 1999).

Beranin ja Lin (2007) mukaan Willardia (2004) mukaillen nettikiusaaminen on mahdollista luokitella sen esiintymismuotojen mukaisesti seitsemään kategoriaan, joista usea täyttävät suoraan useamman rikoksen tunnusmerkistön. Kategoriat ovat niin kutsuttu fleimaaminen, häirintä, mustamaalaus, imitointi, paljastaminen, syrjiminen sekä kybervainoaminen. Kategorioita vastaavia rikosnimikkeitä ovat esimerkiksi kunnianloukkaus, yksityiselämää loukkaavan tiedon levittäminen, laiton uhkaus sekä vainoaminen (RL 1889/39).

Nettikiusaamisen tutkimuksessa on esiintynyt ristiriitaisia tuloksia läpi koko tutkimusaiheen elinkaaren. Eniten ongelmia on esiintynyt nettikiusaamisen erottamisessa perinteisestä kiusaamisesta, sillä ilmiöt liittyvät hyvin läheisesti toisiinsa ja esiintyvät usein yhdessä (Machmutow ym., 2012; Salmivalli, Sainio & Hodges, 2013; Olweus, 2012). Toisissa tutkimuksissa on saatu viitteitä siitä, että nettikiusaaminen olisi oma ilmiönsä ja aiheuttaisi lisähaittoja perinteisen kiusaamisen lisäksi, kun taas toisissa tutkimuksissa tulokset ovat olleen päinvastaisia tai epäselviä (Bonanno & Hymel, 2013; Perren ym., 2010; Cole ym., 2016)Kritiikkiä osakseen on saanut myös tutkimuksen leviäminen psykologian ulkopuolisille tieteen osa-alueille, vaikkakin monitieteellisyyden uskotaankin toimivan lähinnä hyödyllisenä tekijänä tutkimuksessa (Olweus, 2012). Analysoidun

aineiston perusteella voitaisiinkin päätellä, että nettikiusaamisen tutkimus on vielä joiltakin osin puutteellista ja aiheen tutkimus voisi hyötyä jonkinlaisesta yleisestä viitekehyksestä. Tutkimuksen tulokset voivat myös selkiytyä ajan myötä, sillä nettikiusaamisen tutkimusta on tehty tämän tutkielman kirjoitushetkellä vasta noin kaksi vuosikymmentä.

Nettikiusaamisen on myös huomattu voivat aiheuttaa vakavaa vahinkoa sen uhriksi joutuneiden hyvinvoinnille. Nettikiusatuilla lapsilla tai nuorilla on havaittu olevat huonompi itsetunto, kuin sellaisilla lapsilla tai nuorilla, joita ei ole kiusattu ja he suoriutuvat heikommin koulutyössään (Olweus, 2012; Beran & Li, 2007). Viitteitä on myös saatu siitä, että itse nettikiusaajilla on vaikeuksia suoriutua koulutyöstä. Lisäksi nettikiusatut todennäköisesti kiusaavat muita samoilla keinoilla, kuin heitä on kiusattu, mikä johtunee lähinnä kostonhalusta tai vertaistensa puolustamisesta. (Beran & Li, 2007.) Vakavampia nettikiusaamisen aiheuttamia haittoja ovat muiden muassa yksinäisyys, toivottomuus ja masentuneisuus, jotka ovat esiasteita itsetuhoiselle ajattelulle ja käytökselle (Langhinrichsen-Rohling & Lamis, 2008; Kaltiala-Heino ym., 1999; Şahin, 2012). Yksinäisyyden on myös katsottu johtuvat negatiivisten kokemusten vuoksi eristäytymisestä, joka voi pahimmillaan haitata internetin vapaata käyttöä ja näin häiritä henkilön perusoikeuksia (United Nations, 2016).

Päinvastoin kuin nettikiusaamisen käsitteellä, kyberrikollisuuden käsitteen määrittelyssä on esiintynyt hyvinkin suurta vaihtelua, jonka johdosta yksiselitteisen tarkkaa määritelmää ei ole vakiintunut. Määrittely tehdään kuitenkin useimmiten rikoksessa käytetyn teknologian kautta ja sen perusteella, onko teknologia ollut rikoksessa tekoväline, kohde vai ympäristö (Gordon & Ford, 2006). Määritelmää on jaettu tarkempiin kategorioihin esimerkiksi tietoverkkosidonnaisiin, eli tietoverkkoihin ja -järjestelmiin kohdistuviin rikoksiin sekä tietoverkkoavusteisiin, eli tietoverkkoympäristöjä välineinä hyödyntäviin rikoksiin (Poliisi, 2020). Kyberrikollisuuteen liitetään vahvasti myös globalisoituneisuus ja nykyisin myös niin kutsuttu kyberrikollisuuden teollistuminen (SM, 2017).

Käsitellyn aineiston perusteella kyberrikollisuuden motiivit ovat pitkälti yhteneväisiä perinteisen rikollisuuden kanssa, mutta myös poikkeuksia havaittiin. Tutkielmassa kyberrikollisuuden motiiveja tarkasteltiin pääosin Kilgerin ja muiden (2004) jaottelun mukaisesti, kuuteen pääryhmään, jotka ovat *raha*, *viihde*, *itseriittoisuus*, *aatteellisuus*, *sisäänpääsy yhteisöön* sekä *sosiaalisen statuksen tavoittelu*. Muita aineistosta ilmenneitä motiivien jaotteluita olivat Haldin ja Pedersenin (2012) *taloudellinen motivaatio*, *kosto*, *uteliaisuus* ja *pahamaineisuus*, sekä Holtin ja Kilgerin (2012) ensimmäiseksi mainittuun pohjaava, joka poistaa alkuperäiseen nähden *itseriittoisuuden* ja *aatteellisuuden*. Motiiveista mahdollisesti yleisimpiä olivat taloudelliset motiivit, vaikkakin taloudellisen hyödyn tavoittelu kyberrikollisuudella on huomattavasti nuorempi ilmiö kuin esimerkiksi viihteen tai sosiaalisen statuksen tavoittelun vuoksi niiden suorittaminen (Kilger ym., 2004). Eniten edellisellä vuosikymmenellä yleistynyt motiivi oli todennäköisesti aatteellisuus, joka on ollut ilmeisenä motiivina esimerkiksi ISIS-järjestön harjoittamassa kyberrikollisuudessa sekä Yhdysvaltojen vaalivaikuttamisessa vuonna 2016 (Holt & Kilger, 2012; Office of the Director of National Intelligence, 2017). Toisin kuin

tutkimuksessa, motiivit rikoksiin esiintyvät käytännössä kuitenkin usein sekoittuneena toisiin tai vain yleisesti epäselvinä (Kilger, 2011).

Kyberrikollisten luokittelussa esiin nousi eettisyyden mukaan tehty luokittelu *musta-, harmaa- ja valkohattuhakkereihin*, jossa mustahatut toimivat yksiselitteisen rikollisesti, harmaahatut rikollisuuden rajamailla tai ovat niin sanotusti tapansa parantaneita rikollisia ja valkohatut asiantuntijoina rikollista toimintaa vastaan. Luokittelu on kuitenkin informatiivisempaa, jos se tehdään esimerkiksi motiivien ja päämäärien mukaan, esimerkiksi *rikollisiin*, *haktivisteihin* ja *valtioihin* (Hyppönen, 2011). Tässä luokittelussa rikollisiin kuuluvat kaikki, jotka tekevät rikoksensa vain esimerkiksi taloudellisin motiivein, haktivisteihin ne, jotka tekevät rikoksensa aatteellisin motiivein ja valtioihin luonnollisesti valtiolliset tahot, jotka pyrkivät edistämään oman valtionsa poliittista tai taloudellista etua. Muut käsitellyt luokittelut eivät poikenneet suuresti Hyppösen (2011) määritelmästä, mutta laajensivat etenkin *rikolliset* -luokkaa, eritellen esimerkiksi *ammattirikolliset* ja *työntekijät* (BAE Systems, 2021; Rieb ym., 2017).

Kyberrikollisuuden haittojen havaittiin olevan huomattavia etenkin maailmantalouden näkökulmasta (CSIS & McAfee, 2020; CSIS & McAfee 2018; Smith ym., 2019). Kyberrikollisuuden havaittiin myös pystyvän aiheuttamaan mittavaa haittaa organisaation tai yrityksen maineelle, joka voi välillisesti muuttua taloudelliseksi haitaksi (CSIS & McAfee, 2020). Haitat voivat siirtyä myös fyysiseen maailmaan, kuten aihetta tarkasteltaessa huomattiin käyneen esimerkiksi Psykoterapiakeskus Vastaamon tapauksessa, jossa tietomurron vuoksi Vastaamon aiemmat potilaat tunsivat mielenterveytensä heikenneen (Grönroos, 2020; Rantavaara, 2020). Lisäksi kyberrikollisuus on näkynyt fyysisessä maailmassa teollisuuden alalla, jossa Stuxnet-mato on levinnyt tehokkaasti ja rikkonut tietyntyyppistä laitteistoa muuallakin, kuin sen alkuperäisessä kohteessa (Langner, 2011).

Haitat konkretisoituvat kuitenkin vain. jos kyberhyökkäys saadaan toteutettua, jota varten yleisesti tarvitaan jonkinlainen haavoittuvuus. Katsauksessa pääosallisia haavoittuvuuksia havaittiin olevan käyttäjän manipulointi eli inhimilliset tekijät, teknologiset haavoittuvuudet, jotka pitävät sisällään laitteiston, ohjelmiston ja järjestelmät sekä sisäisten prosessien hajoaminen, jossa esimerkiksi organisaation toimintatavat aiheuttavat turvallisuuteen aukon.

Edellä mainittuja pääaiheita tarkasteltiin viimeisessä sisältöluvussa yhteisessä kontekstissa, tavoitteena vastata asetettuihin tutkimuskysymyksiin. Nettikiusaamisen tarkasteleminen kyberrikoksena havaittiin olevan varsin loogista, ottaen huomioon sen, että nettikiusaamisen muodot täyttävät usean rikosnimikkeen tunnusmerkistön. Esimerkiksi rikosnimikkeen kunnianloukkaus tunnusmerkistö vastaa lähestulkoon jokaisen aiemmin käsiteltyyn nettikiusaamisen kategorian määritelmiä, kun taas laiton uhkaus -rikosnimikkeelle ei suoraan ole vastinetta nettikiusaamisen kategorioista, mutta se voi esiintyä ja on esiintynyt lähes jokaisen yhteydessä. (Helsingin hovioikeus, 2016; Nieminen, 2019; Ahonen, 2020.) Sen lisäksi, että rikosnimikkeet ja nettikiusaamisen kategoriat täsmäävät monessa tapauksessa, nettikiusaamistapauksista on myös nostettu syytteitä ja annettu tuomioita, joka tuo aiheeseen konkreettisia esimerkkejä (Helsingin hovioikeus, 2016; Nieminen, 2019; Ahonen, 2020).

Koska kiusaaminen on rikollista toimintaa ja nettikiusaamistapauksissa se on tapahtunut tietoverkkoja ja tietoteknisiä välineitä avuksi käyttäen, se täyttää myös kyberrikollisuuden määritelmät (Poliisi, 2021; Gordon & Ford, 2006). Myös kyberrikollisuuden motiivien kannalta tarkasteluna, nettikiusaaminen vaikuttaisi sisältävän paljon samankaltaisia tekijöitä, kuin aiemmin kyberrikollisuudeksi mielletyt tapaukset (Wilton & Campbell, 2011; Varjas ym., 2010). Näin ollen analysoidun aineiston perusteella voimme vetää johtopäätelmän siitä, että nettikiusaaminen voidaan nähdä kyberrikollisuuden muotona.

Myös nettikiusaamisen torjuntaa pyrittiin tarkastelemaan kyberrikollisuuden näkökulmasta. Jos perusperiaatteena käytetään oletusta siitä, että informaatioteknologian väärinkäyttöä ei voida täysin estää, vaan vain haitata mahdollisimman tehokkaasti, törmätään eettiseen ongelmaan kaikenlaisen kiusaamisen nollatoleranssista (Neufeld, 2010; KiVa Koulu, 2021). Käytännössä ilmiön hävittäminen kokonaisuudessaan voi olla mahdotonta, joten vaikka täydellisyyttä pidettäisiin tavoitteena, nettikiusaamisen minimointi teknologisin keinoin voisi olla riittävää. Tällöin jäljelle jäävät tapaukset voitaisiin saada hallintaan ja niiden aiheuttamat haitat rajattua.

Mahdollinen teknologinen minimointikeino voisi olla esimerkiksi viestintäpalveluiden tarjoajien asettaminen suurempaan vastuuseen haitallisen sisällön poistamisessa. Vaikkakin nykyiset toimet hyödyntävät paljolti esimerkiksi koneoppimista ja muita teknologisia keinoja, haitallista materiaalia on silti paljon ja sivutuotteena sille altistuvat myös ihmismoderaattorit, koska puhtaasti teknologiset järjestelmät eivät vielä voi tehdä täysin itsenäisiä päätöksiä. (Gillespie, 2020; Vincent, 2020.) Jos palveluntarjoajat eivät onnistu itsenäisesti ja proaktiivisesti paikkaamaan puutteitaan, mahdollinen korjaus tilanteeseen voisi olla tarkempien lakien ja säädösten säätäminen toimintaa ohjaamaan.

Kyberrikollisuuden torjunnassa käytetyllä turvallisuuspuutteiden julkaisulla kohteelle tehtyjen korjausten jälkeen voisi olla potentiaalia myös nettikiusaamisen torjunnassa (Google, 2021; F-Secure, 2021). Vastaavaa tapaa kiusaamisen torjuntana on aiemmin ehdottanut Olweus (2012), joka suosittelee anonymisoitujen tietojen julkaisua kiusaamistapauksista, jotta toimintatavat tulisivat suuremman yleisön tietoisuuteen ja eivät siten jäisi huomaamatta eskaloitumaan. Tällöin, vaikka tietojen julkistaminen ei suoraan vähentäisi aktiivista kiusaamista, tapauksia saattaisi syntyä harvemmin ja ne saataisiin estettyä ennaltaehkäisevästi.

Tutkielman aiheen rajauksen vuoksi siinä ei käsitelty esimerkiksi nettikiusaamista, jossa uhreina ovat aikuiset tai työpaikkakiusaamista tietoverkkojen kautta, joka voisi olla erittäin antoista aihepiiri tulevalle tutkimukselle. Myös kyberrikollisuuden periaatteessa rajattomasta aihepiiristä olisi mahdollista tuottaa tulevaisuudessa uutta tutkimusaineistoa, esimerkiksi liittyen informaatiovaikuttamiseen ja niin kutsuttuihin trolleihin, jotka kytkeytyvät myös nettikiusaamisen aihepiiriin.

Taulukko 2 Tutkielman merkittävin kirjallisuus aihealueittain.

Aihealue	**Lähde**
Nettikiusaamisen muodot	Willard (2004)
Nettikiusaamisen tutkimus	Olweus (2012) Perren (2010) Salmivalli, Sainio & Hodges (2013)
Nettikiusaamisen vaikutukset	Beran & Li (2007) Olweus (2012)
Kyberrikollisuuden määritelmä	Oikeusministeriö (2021) Gordon & Ford (2006) Poliisi (2020)
Kyberrikollisuudessa esiintyvät motiivit	Holt & Kilger (2012) Kilger, Arkin & Stutzman (2004) Conteh & Schmick (2016)
Kyberrikollisuuden luokittelu	Sabillon, Cavaller, Cano & Serra-Ruiz (2016) Hyppönen (2011) Rieb, Gurschler & Lechner (2017) BAE Systems (2021)
Kyberrikollisuuden aiheuttamat haitat	CSIS & McAfee (2020) Reuters (2020) Langner (2011)
Kyberrikollisuus ja kyberturvallisuuden haavoittuvuudet	Neufeld (2010) Cebula, Popeck & Young (2014) Conteh & Schmick (2016)
Nettikiusaamisen tarkasteleminen kyberrikoksena	Rikoslaki (1889/39) Willard (2004) Kilger, Arkin & Stutzman (2004)
Kyberrikollisuuden torjuntakeinot nettikiusaamisen torjunnassa	Neufeld (2010) Gillespie (2020) Olweus (2011)

LÄHTEET

Ahonen, R. (23.3.2020). Kyse on elämästä ja terveydestä. *Ilta-Sanomat*. Haettu osoittesta https://www.iltalehti.fi/tyoelama/a/d41daf4f-2aec-4a69-b7b7-7107f0c6e586

Awan, I. (2017). Cyber-extremism: Isis and the power of social media. Society, 54(2), 138-149.

Beran, T., Li, Q. (2007). The relationship between cyberbullying and school bullying.

Bonanno, R. A., & Hymel, S. (2013). Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying. Journal of youth and adolescence, 42(5), 685-697.

Braithwaite, J. (1993). Crime and the average American.

Burgess-Proctor, A., Patchin, J. W., & Hinduja, S. (2009). Cyberbullying and online harassment: Reconceptualizing the victimization of adolescent girls. Female crime victims: Reality reconsidered, 153-175.

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). A taxonomy of operational cyber security risks version 2. Carnegie-Mellon University. Pittsburgh Pa Software Engineering Inst.

Center for Strategic and International Studies & McAfee. (2018). Economic Impact of Cybercrime—No Slowing Down.

Center for Strategic and International Studies & McAfee. (2020). The Hidden Costs of Cybercrime.

Chappell, B. (27.9.2018). Uber Pays $148 Million Over Yearlong Cover-Up Of Data Breach. *National Public Radio*. Haettu osoitteesta https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach

Cherepanov, A., & Lipovsky, R. (2017). Industroyer: Biggest threat to industrial control systems since stuxnet. *WeLiveSecurity, ESET*, *12*.

Chowdhury, A. (2016). Recent cyber security attacks and their mitigation approaches–an overview. In International conference on applications and techniques in information security (pp. 54-65). Springer, Singapore.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).

Ebrand Suomi Oy & Oulun kaupungin sivistys- ja kulttuuripalvelut. (2016). Suomessa asuvien 13-29 -vuotiaiden nuorten sosiaalisen median palveluiden käyttäminen ja läsnäolo. Haettu osoitteesta https://wordpress.ebrand.fi/somejanuoret2016/6-tulevaisuus-ja-trendit/

Elahi, G., Yu, E., & Zannone, N. (2010). A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities. Requirements engineering, 15(1), 41-62.

Felson, M. (2006). Crime and nature. Sage publications.

Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. ACM conference on Computer and communications security (Vol. 10, s. 1315245-1315292).

F-Secure. (24.4.2021). Ransomware on haitta-ohjelmista pahimpia. Haettu osoitteesta https://www.f-secure.com/fi/home/articles/what-is-a-ransomware-attack

F-Secure. (28.4.2021). F-Secure Life, Threats & Research: F-Secure R&D discovers exploitable vulnerability in Apple's macOS Gatekeeper [blogikirjoitus]. Haettu osoitteesta https://blog.f-secure.com/vulnerability-macos-gatekeeper/

Gillespie, T. (2020). Content moderation, AI, and the question of scale. Big Data & Society, 7(2).

Google. (18.5.2021). Google Application Security. Haettu osoitteesta https://www.google.com/about/appsecurity/reward-program/

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13-20.

Grygiel, J., & Brown, N. (2019). Are social media companies motivated to be good corporate citizens? Examination of the connection between corporate social responsibility and social media safety. Telecommunications Policy, 43(5), 445-460.

Grönroos, R. (17.2.2020). Vastaamon tietomurrosta on kuukausia, ja uhrit ovat yhä kuin löysässä hirressä: "Tämä on elinikäistä – tiedot on jo verkossa". *Yle*. Haettu osoitteesta https://yle.fi/uutiset/3-11784431

Hachman, M. (9.1.2018). Microsoft tests show Spectre patches drag down performance on older PCs. *PCWorld.* Haettu osoitteesta https://www.pcworld.com/article/3245742/microsoft-tests-show-spectre-patches-drag-down-performance-on-older-pcs.html

Hald, S. L., & Pedersen, J. M. (2012). An updated taxonomy for characterizing hackers according to their threat properties. 2012 14th International Conference on Advanced Communication Technology (ICACT), 81-86. IEEE.

Helsingin hovioikeuden ratkaisu. 2016:4. Haettu osoitteesta https://oikeus.fi/hovioikeudet/helsinginhovioikeus/fi/index/hovioikeusratkaisut/1460373164827.html

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. Deviant Behavior, 28(2), 171-198.

Holt, T. J., & Kilger, M. (2012). Know your enemy: The social dynamics of hacking. The Honeynet Project, 1-17.

Hutchings, A. (2013). Hacking and fraud: Qualitative analysis of online offending and victimization. Global criminology: Crime and victimization in the globalized era, 93-114.

Hyppönen, M. (2011). Three types of online attack. [video] Haettu osoitteesta https://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack?utm_campaign=tedspread&utm_medium=referral&utm_source=tedcomshare

Hämäläinen, V-P. (22.1.2021). Uudet tiedot: Vastaamon potilaiden tiedot olivat ehkä jopa vuosia suojaamatta netissä – tietoturva-asiantuntija: "Älyvapaata". *Yle*. Haettu osoitteesta https://yle.fi/uutiset/3-11750220

Kaltiala-Heino, R., Rimpelä, M., Marttunen, M., Rimpelä, A., & Rantanen, P. (1999). Bullying, depression, and suicidal ideation in Finnish adolescents: school survey. Bmj, 319(7206), 348-351.

Khosrowshahi, D. (21.11.2017). 2016 Data Security Incident. [lehdistötiedote] Haettu osoitteesta https://www.uber.com/newsroom/2016-data-incident/

Kilger, M. (2011). Social Dynamics and the Future of Technology-Driven Crime. Teoksessa Holt, T. J., & Schell, B. H. (Eds.), Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (s. 205-227). IGI Global. http://doi:10.4018/978-1-61692-805-6.ch011

Kilger, M., Arkin, O., & Stutzman, J. (2004). Profiling. Know your enemy: learning about security threats, 505-556.

Kirsch, C. (2014). The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law. N. Ky. L. Rev., 41, 383.

KiVa Koulu®. (19.5.2021). Mikä KiVa on?. Haettu osoitteesta https://www.kivakoulu.fi/kivaohjelmasta/

Knuutila, A., Kosonen, H., Saresma, T., Haara, P., & Pöyhtäri, R. (2019). Viha vallassa: Vihapuheen vaikutukset yhteiskunnalliseen päätöksentekoon.

Kocher, P., Horn, J., Fogh, A., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M., & Yarom, Y. (2018). Spectre attacks: Exploiting speculative execution. Cornell University.

Kumar, V. L., & Goldstein, M. A. (2018). Cyberbullying and Adolescents.

Lahtinen, E. (2019). Juristi vastaa: Milloin kiusaaminen on rikos?. *RIKU-lehti*, s. 28.

Langhinrichsen-Rohling, J., & Lamis, D. A. (2008). Current suicide proneness and past suicidal behavior in adjudicated adolescents. Suicide and Life-Threatening Behavior, 38(4), 415-426.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51.

Levchenko, S. (1988). On the wrong side: My life in the KGB. Pergamon-Brassey's.

Linton, M. (4.1.2018). More details about mitigations for the CPU Speculative Execution issue [blogikirjoitus]. Haettu osoitteesta https://security.googleblog.com/2018/01/more-details-about-mitigations-for-cpu_4.html

Machmutow, K., Perren, S., Sticca, F., & Alsaker, F. D. (2012). Peer victimisation and depressive symptoms: Can specific coping strategies buffer the negative impact of cybervictimisation?. Emotional and Behavioural Difficulties, 17(3-4), 403-420.

Mannerheimin Lastensuojeluliitto. (2017). Nettikiusaamisen ehkäiseminen. Haettu osoitteesta https://www.mll.fi/ammattilaisille/kouluille-ja-oppilaitoksille/kiusaamisen-ehkaiseminen/nettikiusaamisen_ehkaiseminen

Martela, F., & Jarenko, K. (2014). Sisäinen motivaatio. Tulevaisuuden työssä tuottavuus ja innostus kohtaavat. Eduskunnan tulevaisuusvaliokunnan julkaisu, 3, 2014, 14-15.

Neufeld, D. J. (2010). Understanding cybercrime. 2010 43rd Hawaii International Conference on System Sciences (s. 1-10). IEEE.

Nieminen, J. (1.7.2019). Tapa ittes! Vitun majava! Vedä ittes jojoon! – Riikka vei nettikiusaamisen oikeuteen. *Yle*. Haettu osoitteesta https://yle.fi/aihe/artikkeli/2018/05/03/tapa-ittes-vitun-majava-veda-ittes-jojoon-riikka-vei-nettikiusaamisen-oikeuteen

Office of the Director of National Intelligence. (2017). Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections. Haettu osoitteesta https://www.dni.gov/files/documents/ICA_2017_01.pdf

Oikeusministeriö. (6.4.2021). Rikosoikeus. Haettu osoitteesta https://oikeusministerio.fi/rikosoikeus

Olweus, D. (1999). Sweden. Teoksessa Smith, PK., Morita, Y., Junger-Tas, J., Catalano, R., Slee, P. The Nature of School Bullying. Routledge;1999:7-27.

Olweus, D. (2011). Bullying at school and later criminality: Findings from three Swedish community samples of males. Criminal behaviour and mental health, 21(2), 151-156.

Olweus, D. (2012). Cyberbullying: An overrated phenomenon?. European journal of developmental psychology, 9(5), 520-538.

Oxford University Press. (20.5.2021). Definition of hacker. *Lexico*. Haettu osoitteesta https://www.lexico.com/definition/hacker

Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. Youth violence and juvenile justice, 4(2), 148-169.

Perren, S., Dooley, J., Shaw, T., & Cross, D. (2010). Bullying in school and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents. Child and adolescent psychiatry and mental health, 4(1), 1-10.

Perrin, A. (2015). Social media usage. Pew research center, 125, 52-68.

Poliisi. (6.4.2021). Kyberrikokset. Haettu osoitteesta https://poliisi.fi/kyberrikokset

Ralston, W. (11.11.2020). The untold story of a cyberattack, a hospital and a dying woman. *Wired*. Haettu osoitteesta https://www.wired.co.uk/article/ransomware-hospital-death-germany

Rantavaara, M. (25.10.2020). Vastaamon tietomurron uhrit kertovat turvattomuuden, epäuskon ja suuttumuksen tunteista: ”Tämä on vienyt kaiken energian”. *Helsingin Sanomat*. Haettu osoitteesta https://www.hs.fi/kotimaa/art-2000006699427.html

Reuters. (18.9.2020). Prosecutors open homicide case after hacker attack on German hospital. *Reuters*. Haettu osoitteesta https://www.reuters.com/article/idUSKBN26926X

Rieb, A., Gurschler, T., & Lechner, U. (2017). A gamified approach to explore techniques of neutralization of threat actors in cybercrime. Annual Privacy Forum (pp. 87-103). Springer, Cham.

Riggi, J. (2020). Ransomware Attacks on Hospitals Have Changed. American Hospital Association Center for Health Innovation. Haettu osoitteesta https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

Rikoslaki 1889/39. (1889). Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF) (pp. 1-9). IEEE.

Şahin, M. (2012). The relationship between the cyberbullying/cybervictmization and loneliness among adolescents. Children and Youth Services Review, 34(4), 834-837.

Salmivalli, C., Sainio, M., & Hodges, E. V. (2013). Electronic victimization: Correlates, antecedents, and consequences among elementary and middle school students. Journal of Clinical Child & Adolescent Psychology, 42(4), 442-453.

Schell, B. H., & Dodge, J. L. (2002). The hacking of America: Who's doing it, why, and how. Greenwood Publishing Group Inc..

Seri, B. (2019). Two Years In and WannaCry is Still Unmanageable. Haettu osoitteesta https://www.armis.com/resources/iot-security-blog/wannacry/

Sisäministeriö. (17.9.2020). Kyberrikollisuus. Haettu osoitteesta https://intermin.fi/poliisiasiat/kyberrikollisuus

Sisäministeriö. (2017). Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Haettu osoitteesta http://julkaisut.valtioneuvosto.fi/handle/10024/79866

Slatalla, M., & Quittner, J. (1995). Masters of deception: The gang that ruled cyberspace. HarperCollins Publishers.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying?. Scandinavian journal of psychology, 49(2), 147-154.

Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society.

Smith, P. K., Del Barrio, C., & Tokunaga, R. S. (2013). Definitions of bullying and cyberbullying: How useful are the terms. Principles of cyberbullying research: Definitions, measures, and methodology, 26-40.

Tenhunen, A. (7.6.2016). Nettikiusaamisesta tuomio 15-vuotiaalle tytölle. *Savon Sanomat*. Haettu osoitteesta https://www.savonsanomat.fi/paikalliset/3047271

United Nations General Assembly. 2016. The promotion, protection and enjoyment of human rights on the Internet. Thirty-second session. A/HRC/32/L.20. Haettu osoitteesta https://digitallibrary.un.org/record/845727?ln=en

Van Rooij, A. (2015). Sisyphus in business: Success, failure and the different types of failure. Business History, 57(2), 203-223.

Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. CyberPsychology & Behavior, 11(4), 499-503.

Varjas, K., Talley, J., Meyers, J., Parris, L., & Cutts, H. (2010). High school students' perceptions of motivations for cyberbullying: An exploratory study. Western Journal of Emergency Medicine, 11(3), 269.

Vincent, J. (13.11.2020). Facebook is now using AI to sort content for quicker moderation. The Verge. Haettu osoitteesta https://www.theverge.com/2020/11/13/21562596/facebook-ai-moderation

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Willard, N. (2007). Educator's guide to cyberbullying and cyberthreats. Center for safe and responsible use of the Internet. https://education.ohio.gov/getattachment/Topics/Other-Resources/School-Safety/Safe-and-Supportive-Learning/Anti-Harassment-Intimidation-and-Bullying-Resource/Educator-s-Guide-Cyber-Safety.pdf.aspx

Wilton, C., & Campbell, M. (2011). An exploration of the reasons why adolescents engage in traditional and cyber bullying. Journal of Educational Sciences and Psychology, 1(2), 101-109.