Hakkerikategoriat kirjallisuudessa

Sanna Santapukki

5/2021

Poliisiammattikorkeakoulun opinnäytetyö / AMK

TIIVISTELMÄ

Sanna Santapukki: Hakkerikategoriat kirjallisuudessa
Opinnäytetyön muoto: tutkimuksellinen
Julkisuusaste: Julkinen
Ohjaaja: Jani Peltola & Hanna Uusitalo
Tutkinto: Poliisi (AMK)

Tietoverkkorikokset jaetaan tietojärjestelmiä ja viestintäverkkoja hyödyntäen tehtyihin rikoksiin sekä rikoksiin, joiden kohteena on tietoverkot ja -järjestelmät. Tietoverkkorikollisuus, joka tunnetaan myös nimellä kyberrikollisuus, on teknologian kehityksen myötä muuttuva ja ajankohtainen rikollisuuden ala, jonka määrä on poliisin tilastojen mukaan jatkuvasti kasvussa. Erityisesti tietoverkkoihin kohdistuvien rikosten tutkinta vaatii tutkijalta perehtyneisyyttä ja ymmärrystä aiheeseen.

Median ja viihdeteollisuuden myötä ihmiset yhdistävät tietoverkkoihin kohdistuvat rikokset usein hakkereihin. Arkikielessä hakkeri termi on vakiintunut kuvaamaan luvatta tietojärjestelmiin tunkeutuvaa henkilöä. Hakkerin määritelmä ei ole kuitenkaan yksiselitteinen, sillä kaikki hakkerointi ei ole rikollista toimintaa.

Tässä opinnäytetyössä tarkastellaan millaisiin kategorioihin hakkereita kirjallisuudessa ja tutkimuksissa jaotellaan. Hakkereita jaotellaan heidän tarkoitusperiensä mukaan erilaisiin ylä- ja alakategorioihin. Opinnäytetyön alussa tutustutaan tietoverkkorikollisuuden ja hakkeroinnin määritelmään tiivistetysti.

Sivumäärä: 17 sivua
Tarkastuskuukausi ja vuosi: Toukokuu 2021
Avainsanat: tietoverkkorikollisuus, kyberrikollisuus, hakkerointi, kirjallisuuskatsaus

SISÄLLYS

1 JOHDANTO

Tietoverkkorikollisuus on ilmiönä erittäin ajankohtainen ja jatkuvasti muuttuva ala. Tätä opinnäytetyötä tehdessä aihe nousi valtakunnallisesti mediassa keskustelun aiheeksi psykoterapiakeskus Vastaamon tietomurron myötä. Psykoterapiakeskus Vastaamon potilastietoihin kohdistui kaksi tietomurtoa vuosien 2018–2019 aikana. Tekijä pääsi käsiksi arviolta 36000 potilaan tietoihin ja julkaisi niitä Tor-verkossa. Tietomurrot tulivat julki lokakuussa 2020. Tietomurto oli kansainvälisestikin poikkeuksellinen, sillä sen vaikutukset koskettivat yrityksen lisäksi useaa yksittäistä henkilöä, ja tietomurron kohteena oli erittäin arkaluontoinen materiaali. (Ralston 2020).

Tietoverkkorikollisuus ei ole ilmiönä uusi. Arkikielessä hakkeri yhdistetään usein luvatta tietojärjestelmiin tunkeutuviin henkilöihin, vaikka sana alun perin kuvasi tietotekniikasta kiinnostunutta henkilöä (Haasio 2013, 99). Vastaamon tietomurron uutisoinnin yhteydessä monet tietoverkkorikollisuuteen ja hakkerointiin liitettävät käsitteet tulivat ihmisten tietoon, mutta termit ja käsitteet saattoivat olla monille vieraita. Esimerkiksi poliisin apuna tapausta tutkivat aktiivisesti valkohattuhakkerit.

Diginatiivilla tarkoitetaan sukupolvea, joka ei ole kokenut aikaa ennen internettiä. Nuoret ovat nykyään taitavia teknisten laitteiden käyttäjiä ja ovat tottuneet viettämään aikaa internetissä. Internetissä toimiviin lapsiin ja nuoriin kuitenkin lukeutuu myös niitä nuoria, jotka voivat aiheuttaa tietoverkoissa yhteiskunnallisia ongelmia ja tietoverkkorikoksia.

Keskusrikospoliisi käynnisti 1.4.2020 Cybercrime Exit- nimisen hankkeen, jota rahoittaa Euroopan unionin sisäisen turvallisuuden rahasto. Hankkeen tavoitteena on nuorten verkkorikollisten rikoskierteen katkaisu ja hankkeen kohteena ovat 15–25-vuotiaat nuoret, jotka ovat tehneet tietoverkkorikoksen tai potentiaalisesti tulevaisuudessa hyödyntävät tietoteknistä osaamistaan rikolliseen toimintaan. Hankkeessa pyritään muun muassa auttamaan nuoria tunnistamaan rikollinen toiminta ja tuomaan esille valkohattuhakkereiden toiminnalle rajoja. (Poliisi 2021).

Tietoverkkorikollisuudessa on tekijä voi jäädä helposti etäiseksi ja ”kasvottomaksi”. Tapaus herätti kuitenkin itsessäni mielenkiintoa kysymykseen millaisia ovat ihmiset tällaisten tekojen takana ja mitä hakkereista tiedetään. Keskustelin opinnäytetyöni kanssa monien kollegoideni ja ystävieni kanssa. Olen käynyt paljon keskusteluja opinnäytetyöni aiheen valinnasta. Vaikka ihmiset eivät tienneet aiheesta paljoa, se herätti monessa kiinnostusta riippumatta siitä, työskentelivätkö he poliisina vai eivät. Opinnäytetyön kirjoittamisen aikana havaitsin itsekin miten paljon erilaista tietoa aihe kattaa ja miten paljon siinä on omaksuttavaa.

Hakkereita jaotellaan erilaisiin kategorioihin useimmiten heidän tarkoitusperiensä perusteella. Tässä opinnäytetyössä tarkastellaan hakkereiden jaottelua eri kategorioihin kirjallisuudessa ja ver-

taillaan jaotteluja keskenään. Opinnäytetyön alussa käsitellään tiivistetysti yleisiä käsitteitä ja perusteita tietoverkkorikollisuudesta ja hakkeroinnista, jotta aiheeseen perehtymättömän lukijan on helpompi ymmärtää myöhemmissä luvissa käsiteltävien jaotteluiden perusteita.

2 OPINNÄYTETYÖN TOTEUTUS

2.1 Opinnäytetyön tavoitteet ja tarkoitus

Tämän opinnäytetyön tavoitteena on luoda lukijalleen ymmärrystä hakkeroinnista ja avata hakkeritermin monitulkintaisuutta. Hakkeri ei ole terminä yksinkertainen, sillä sitä käytetään monessa eri merkityksessä. Opinnäytetyön tavoitteena on tutkia, minkälaisiin erilaisiin kategorioihin kirjallisuudessa hakkereita jaotellaan ja mihin jaottelu perustuu. Yksi opinnäytetyön tarkoitus on osoittaa lukijalle, ettei hakkerointi tarkoita ainoastaan rikollista toimintaa.

Opinnäytetyötä on helppo käyttää materiaalina tietoverkkorikollisuuteen ja hakkerointiin tutustumiseen. Työn tarkoituksena on auttaa lukijaa ymmärtämään tutkimusten avulla, keitä hakkerit ovat ja millaisia eroja heidän välillänsä on. Opinnäytetyössä vertaillaan miten eri kirjoittajat ovat heidät jakaneet kategorioihin. Opinnäytetyö tutustuttaa lukijan moniin eri hakkereiden yhteydessä puhuttaviin termeihin.

Koska tietoverkkorikollisuus voi olla lukijalle ylipäätään tuntematon ala, olen sisällyttänyt opinnäytetyöhön yhden luvun, jossa käsittelen tietoverkkorikollisuutta ja hakkerointia yleisesti. Aihe on hyvin laaja, joten olen rajannut käsittämään ainoastaan peruskäsitteet, jotka voivat auttaa ymmärtämään muita opinnäytetyön lukuja paremmin. Luvun tarkoituksena on auttaa lukijaa hahmottamaan minkälaisesta ilmiöstä tietoverkkorikollisuudesta on kyse ja millaisia yleisiä piirteitä tietoverkkorikollisuuteen liittyy. Luvussa käsitellään myös tietoverkkorikollisuuden tilannetta Suomessa. Avaan luvussa lukijalle myös hakkeroinnin määritelmää, tekomuotoja ja kirjallisuudessa esiin nostettuja yleisimpiä motiiveja hakkeroinnille.

Kirjallisuudessa hakkereiden jaottelussa esiintyy jonkun verran päällekkäisyyttä. Käsittelen kirjallisuudessa esiintyviin hakkereiden tarkoitusperiin perustuvia karkeampia jaotteluja opinnäytetyön luvussa neljä. Näitä jaotteluja ovat hakkeri ja krakkeri ja musta-, valko- ja harmaahattuhakkerit. Syvemmälle menevää kategorisointia käsitellään luvussa viisi. Olen jakanut luvut käsittelemään yläkategorioita ja alakategorioita selventämään lukijalle jaottelua ja termejä. Luvussa kuusi käsittelen hakkerikategorioita, joiden sijoittelu vaihteli eniten kirjoittajien mukaan ja tutkimuksia, joiden jaotteluperuste oli muu kuin hakkerin tarkoitusperät.

2.2 Tutkimusmenetelmä

Opinnäytetyön kirjoittamisen tavoitteena on palvella opiskelijan oppimista ja asiantuntijuuteen kehittymistä. Opinnäytetyön tarkoituksena on parantaa opiskelijan tiedonhakutaitoja, tiedon soveltamista, oman työn arviointi ja suullisen ja kirjallisen viestinnän taitoja. (Haikansalo ja Korander 2019). Opinnäytetyö toteutettiin kirjallisuuskatsauksena, jossa kootaan tiivistetysti, miten hakkeri määritellään ja mitä tekomuotoja ja motiiveja hakkeroinnille on esitetty kirjallisuudessa. Lisäksi kirjallisuusanalyysissa tarkastellaan mihin erilaisiin ryhmiin hakkereita jaotellaan ja millä perusteella jaottelu tapahtuu. Kirjallisuuskatsauksen tavoitteena on arvioida jo tehtyä tutkimusta ja tehdä uutta tutkimusta jo tehdyn tutkimuksen pohjalta (Salminen 2011).

Opinnäytetyön aiheen tarkentuessa oli selvää, että tutkimuksellinen opinnäytetyö ja kirjallisuuskatsaus toteuttaa työn tavoitteet parhaiten. Kirjallisuudessa hakkereita jaoteltiin usealla eri tavalla ja tiedon kerääminen haastattelujen kautta olisi voinut antaa kategorioista suppeamman ja pelkistetymmän kuvan. Kirjallisuuskatsaus tarjosi mahdollisuuden tarkastella aihetta mahdollisimman objektiivisesti.

Opinnäytetyön alussa keräsin yleisesti tietoverkkorikollisuutta koskevaa kirjallisuutta. Näiden kirjojen lähteiden ja viittausten kautta löysin erityisesti hakkerointia ja hakkereita koskevaa kirjallisuutta. Lisäksi sain Keskusrikospoliisin kybertorjuntakeskuksen ennalta estävän Cybercrime Exit- projektin päälliköltä tärkeitä vinkkejä aihetta käsittelevistä kirjoista ja sähköisistä lähteistä.

Sähköisinä lähteitä opinnäytetyössä on käytetty viranomaisten ylläpitämiä nettisivuja ja uutisartikkeleita nostamaan esille aiheen ajankohtaisuutta. Lisäksi olen hakenut internetistä aihetta käsitteleviä artikkeleita, jotka laajentavat näkökulmaa kirjoissa esillä olleisiin jaotteluperusteisiin.

Merkittävä hakkereiden kategorioita tutkinut kirjallinen lähde oli Paul Chiesan, Stefania Duccin ja Silvio Ciappin *Profiling Hackers: The Science of Criminal Profiling as Applied to Criminal Profiling as Applied to the World of Hacking*. Tutkimuksessa hakkereiden jaottelua vietiin syvemmälle ja monissa aihetta sivuavissa kirjoissa viitattiin tähän teokseen. Kirja käsitteli hakkereita monesta eri näkökulmasta.

Aihetta käsittelevästä kirjallisuudesta suuri osa on kirjoitettu englanniksi ja tutkimukset on toteutettu ulkomailla. Aiheesta kirjoitettua kirjallisuutta ei ole käännetty suomeksi juuri ollenkaan. Osalle käyttämistäni käsitteistä ei löydy vakiintunutta suomenkielistä käännöstä, joten olen joko itse suomentanut termin tai valinnut mielestäni osuvimman käytössä olleen suomennoksen. Selkeyden vuoksi olen kuitenkin lisännyt joidenkin suomenkielisten termien perään suluissa niiden englanninkielisen vastineen. Alakategorioiden nimiä en lähtenyt kääntämään, vaan säilytin ne selkeyden vuoksi alkuperäisinä.

3 YLEISTÄ TIETOVERKKORIKOKSISTA JA HAKKEROINNISTA

Luvun tarkoituksena on auttaa lukijaa ymmärtämään tietoverkkorikollisuuden ja hakkeroinnin määritelmiä. Luvussa avataan hakkeroinnin menetelmiä ja motiiveja. Hakkerointi saattaa muodostaa negatiivisen mielikuvan, on tärkeää huomioida, ettei kaikki hakkerointi ole rikollista toimintaa.

3.1 Tietoverkkorikokset

Tietoverkkorikokset jaetaan tietojärjestelmiä ja viestintäverkkoja hyödyntäen tehtyihin rikoksiin sekä rikoksiin, joiden kohteena on tietoverkot ja -järjestelmät. Tietojärjestelmiä ja viestintäverkkoja hyödyntäen tehdyt rikokset ovat esimerkiksi nettipetokset ja sähköpostitse leviävät huijauskirjeet. Esimerkkinä rikoksista, joiden kohteena ovat tietoverkot ja järjestelmät ovat tietomurrot. (Haasio 2013, 13). Tietoverkkorikollisuudesta käytetään myös termiä kyberrikollisuus.

Edellä mainitun lisäksi suurin osa tietoverkkorikoksista voidaan jakaa omaisuuteen kohdistuviin rikoksiin ja henkilöihin kohdistuviin rikoksiin (Kirwan ja Power 2013, 3). Toisinaan tietoverkkorikokset jaotellaan lisäksi valtiota vastaan kohdistuviin rikoksiin (Haasio 2013, 13).

Viimeisen kymmenen vuoden aikana kyberrikollisuus on muuttunut ”jostakin keskusteltavasta” vakavaksi ongelmaksi (Chiesa ym. 2009, 15). Tietoverkkorikollisuuden suunta on muuttumassa koko ajan ammattimaisemmaksi. Järjestäytyneillä rikoksentekijöillä on mahdollisuus kehittää rikoksentekomenetelmiä hienovaraisemmaksi ja hyödyntää uutta teknologiaa. Erityistä tietoverkkorikollisuudesta tekee se, että yksittäisen tekijän on teoillaan mahdollista vaikuttaa useisiin eri valtioihin ja miljooniin ihmisiin. (Jämsén 2020).

Tietoverkkoympäristöön kohdistuvia rikosnimikkeitä rekisteröitiin vuonna 2019 poliisin tietojärjestelmiin reilut 1300 kappaletta. Vuoden 2020 aikana rekisteröityjen rikosten määräksi ennustettiin 1400 kappaletta. Vuosittainen vaihtelu on suhteellisesti pientä, mutta kasvu on ollut selkeää viimeisen parin vuoden aikana. Suomen maantieteellisesti syrjäisestä sijainnista ja oudosta kielestä huolimatta Suomi on suhteellisen vauraana maana suosittu kohde rikollisille. (Jämsén 2020).

Suomen rikoslainsäädännössä rangaistavaksi säädetyt tietoverkkorikokset on jaoteltu sen mukaan kohdistuvatko rikokset tietotekniikkaan vai hyödynnetäänkö tietotekniikkaa rikoksen tekemiseen. Pääsääntö on, että mikä on kiellettyä tietoverkkojen ulkopuolella, on kielletty myös tietoverkoissa. Joidenkin rikosten tunnusmerkistöä on täydennetty tai muutettu niin, että se kattaa myös perinteisiä rikoksia muistuttavat tietoverkkorikokset. Tällaisia ovat esimerkiksi luvaton käyttö ja petos. (Peltomäki ja Norppa 2015, 77–80).

Tietotekniikan kehittyminen ja uudenlaisen käyttäytymisen myötä Rikoslain kokonaisuudistuksessa vahvistettiin Rikoslain 38 luku tieto- ja viestintärikoksista.

3.2 Hakkerointi

Hakkerointi on yksi tietoverkkorikollisuuden tunnetuimpia muotoja. Tietoverkkorikoksena hakkerointi vaatii rikostutkijalta laajaa osaamista tietokoneista ja tietoverkoista tai vähintään alan asiantuntijan apua niiden ymmärtämisen kanssa. Tämän vuoksi hakkerointeja tutkii pääasiassa siihen erikoistuneet tutkijat. (Moore 2011, 8).

Tietoverkkorikoksista puhuttaessa hakkerointi-termi käsittää useampia toiminnan muotoja, joissa sekaannutaan tietojärjestelmien ja tietoverkkojen asianmukaiseen toimintaan. Monet oikeusjärjestelmät eivät kuitenkaan käytä hakkerointi termiä sen monitulkinnaisuuden vuoksi. Kriminalisoidut hakkereiden toiminnot on listattu yksityiskohtaisemmin. (Europol 2016).

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (2001) listaa hakkerointiin liitettävät kriminalisoidut teot:

- 2 artikla Luvaton tunkeutuminen
  ”Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen tahallisen tietojärjestelmään tai sen osaan tunkeutumisen kansallisen lainsäädäntönsä mukaisesti rangaistavaksi teoksi. Sopimuspuoli voi asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty turvajärjestelyt murtamalla, tarkoituksin päästä käsiksi dataan, tai muuta epärehellistä tarkoitusta varten, tai että se liittyy sellaiseen tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään.”

- 3 artikla Viestintäsalaisuuden loukkaaminen
  ”Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman teknisin keinoin tapahtuvan tiedon hankkimisen tietojärjestelmän sisäisestä tai tietojärjestelmien välisestä luottamuksellisesta datan siirrosta, sekä tällaista dataa sisältävästä tietojärjestelmästä lähtevästä sähkömagneettisesta säteilystä. Sopimuspuoli voi asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty epärehellisin tarkoituksin, tai että se liittyy sellaiseen tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään.”

- 4 artikla Datan vahingoittaminen
  ”1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman datan vahingoittamisen, tuhoamisen, turmelemisen, muuttamisen tai poistamisen.
  2. Sopimuspuoli voi tehdä varauman, jonka mukaan rangaistavuuden edellytyksenä on, että 1 kappaleessa tarkoitettu teko aiheuttaa huomattavaa vahinkoa.”

- 5 artikla Tietojärjestelmän häirintä
  ”Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman tietojärjestelmän toiminnan vakavan estämisen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla.”

- 6 artikla Laitteiden väärinkäyttö
  ”1. Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen kansallisen lainsäädäntönsä mukaisesti rangaistaviksi seuraavat tahalliset ja oikeudettomat teot:
  a) seuraavien tuottaminen, myynti, hankkiminen, tuonti, levittäminen tai muu saataville asettaminen:
  i) väline, mukaan luettuna tietokoneohjelma, joka on suunniteltu tai muutettu ensisijaisesti tämän yleissopimuksen 2–5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemistä varten;
  ii) tietojärjestelmän salasana, pääsykoodi tai muu vastaava tieto, joka mahdollistaa pääsyn tietojärjestelmään tai sen osaan,
  tarkoituksin, että sitä käytetään tämän yleissopimuksen 2–5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemiseen.
  b) tämän kappaleen a kohdan i tai ii alakohdassa tarkoitetun tuotteen hallussapito, tarkoituksin käyttää sitä 2–5 artiklan mukaisesti rangaistaviksi säädettyjen rikosten tekemiseen. Sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, että tekijän hallussa on useita tällaisia tuotteita. –”

Hakkerit käyttävät useita eri metodeja saavuttaakseen tavoitteensa. Hakkerit voivat käyttää erilaisia tarkoitusta luotuja työkaluja ja tekniikoita tai hankkia esimerkiksi järjestelmän käyttäjätunnukset ja salasanan käyttäjältä epärehellisin keinoin. Tällainen toiminta ei vaadi välttämättä hakkerilta erityistä osaamista tietokoneiden kanssa. (Kirwan ja Power 2013, 62).

Motiiveja hakkeroinnille on tutkittu jonkun verran, mutta useimmat tutkimukset ovat teoreettisia. Empiiristä tutkimusta aiheesta on suhteessa tehty vähän. Tutkimuksissa on esitetty useita erilaisia motiiveja hakkeroinnille ja samanaikaisesti yhdellä hakkerilla voi olla useita motiiveja. Motiivit rikollisin tarkoituksin hakkeroivien ja laillisesti hakkeroivien kesken eivät välttämättä eroa merkittävästi keskenään. (Kirwan ja Power 2013, 65).

Ensiaskeleet hakkerointiin otetaan usein uteliaisuudesta ja tiedonhalusta. Myöhemmin harrastuksesta voi kehittyä hakkerille intohimo ja ammatti. Hakkerointia voidaan kuvata eräänlaisena kasvuprosessina ja itsensä kehittämisessä. Hakkerit haluavat ymmärtää miten tietokoneet toimivat ja testata niiden rajoja. (Chiesa ym. 2009, 144–145).

Osa nuorista hakkereista haluaa kuulua johonkin, minkä takia he saattavat liittyä hakkeriryhmään. Osa hakkereista kuitenkin haluaa toimia yksin, sillä he tuntevat olonsa niin turvallisemmaksi (Chiesa ym. 2009, 163). Hakkeroimalla nuoret voivat hakea tunnustusta ja mainetta teoistaan ja osoittaa olevansa fiksuja.

Rikollisin tarkoitusperin hakkeroivat hakevat usein jännitystä tai haluavat kostaa jollekin kuka on tehnyt väärin heitä kohtaan (Chiesa ym. 2009, 48). Muita tutkimuksissa esiin nousseita motiiveja hakkeroinnille on vallantunne, tylsyys ja taloudelliset syyt (Kirwan ja Power 2013, 65). Yleisesti ottaen taloudellisen hyödyn tavoittelu vaikuttaa olevan suurin motiivi verkon kautta tehdyissä rikoksissa (Jämsén 2020).

4 HAKKEREIDEN YLÄKATEGORIAT

Luku käsittelee hakkereiden jaottelua eri kategorioihin heidän tarkoitusperiensä perusteella. Ensimmäinen jaottelu erottelee hakkerit ja krakkerit toisistaan. Jälkimmäinen jaottelu musta- valko- ja harmaahattuhakkereihin antaa enemmän soveltamisalaa kategorisoinnille.

4.1 Hakkeri ja krakkeri

Alun perin termillä hakkeri tarkoitettiin henkilöä, joka oli melkein riippuvuuteen asti kiinnostunut tietotekniikasta. 1980-luvulla termi muutti merkitystään, sillä se yhdistettiin tietoverkoissa tapahtuvaan laittomaan toimintaan. Arkikielessä termi on vakiintunut kuvaamaan luvatta tietojärjestelmiin murtautuvaa henkilöä. (Haasio 2013, 99).

Ensimmäiset hakkeroinnin ikävät seuraukset tulivat esiin jo 1960-luvulla. Tuolloin alkuperäiset lakia noudattavat hakkerit halusivat erottautua rikollisista hakkereista. Luvatta tietojärjestelmiin tunkeutuvista hakkereista alettiin käyttää termiä krakkeri. Yrityksistä huolimatta krakkeri termi ei kuitenkaan vakiintunut valtaväestön ja median käyttöön.

Vaikka termi hakkeri on saanut nykypäivänä negatiivisen sävyn, kaikki hakkerit eivät kuitenkaan ole rikollisia. Yksi kirjallisuudessa esitetty määritelmä hakkerille on ”henkilö, jolla on suuri mielenkiinto tietokoneisiin ja teknologiaan ja joka tätä tietoa hyödyntäen pääsee käyttämään toisen henkilön tietokonejärjestelmää luvallisesti tai ilman lupaa” (Taylor ym. 2019, 78).

Hakkereista käytetään kirjallisuudessa myös ilmaisua kokeilijat. Heillä ei ole välttämättä poliittista tai rahallista motiivia, vaan he haluavat kokeilla taitojaan ja testata järjestelmien heikkouksia. (Peltomäki ja Norppa 2015, 56).

Krakkerilla tarkoitetaan henkilöä, joka tunkeutuu luvatta tietojärjestelmiin joko haitta- tai rikollistarkoituksessa (Peltomäki ym. 2015, 56). Erona hakkerin ja krakkerin välillä on krakkerin toiminnan tarkoitusperässä. Krakkerin tarkoitus on vahingoittaa tai tuhota dataa.

Rajanveto hakkerin ja krakkerin välille ei ole helppoa. Jaottelu hakkereihin ja krakkereihin ei esiinny kaikissa kirjoissa, vaan monet aiheesta kirjoitetut kirjat käyttävät molemmista ryhmistä puhuttaessa termiä hakkeri. Chiesa ym. (2009) jaottelevat krakkerit alakategorioihin ja kuvaavat heitä väkivaltaisiksi hakkereiksi.

4.2 Hatut

Toinen kirjallisuudessa paljon esiintyvä jaottelu hakkereiden tarkoitusperien mukaan jakaa hakkerit musta-, valko- ja harmaahattuhakkereihin. Osassa kirjallisuudessa esiintyy ainoastaan kahtiajako musta- ja valkohattuhakkereihin. Kyseinen jaottelu on ollut esillä myös mediassa ja voi sen kautta olla tutumpi ihmisille.

4.2.1 Mustahattuhakkerit

Mustahattuhakkereiden tarkoituksena on vahingoittaa tietojärjestelmiä tai toimia muutoin rikollisissa aikeissa (Haasio 2013, 100). Kuten aiemmin mainituilla krakkereilla, mustahattuhakkereiden tunkeutuvat luvatta tietojärjestelmiin nimenomaan rikollisissa tarkoituksissa. Löydettyään tietojärjestelmistä heikkouksia he eivät tarjoa apua niiden korjaamiseen (Kirwan ja Power 2013, 54).

Mustahattuhakkereiden takia virustorjunnasta ja tietokoneturvallisuudesta on tullut kokoaika business, joka maksaa yrityksille ympäri maailmaa miljoonia dollareita. Mustahattuhakkereita kuvataan ihmisten pelkäämän tietoverkkorikollisen malliesimerkkinä.

4.2.2 Valkohattuhakkerit

Valkohattuhakkerit esiintyvät kirjallisuudessa täysin vastakohtana mustahattuhakkereille. Valkohattuhakkereiden päätavoite on estää laittomat tunkeutumiset tietojärjestelmiin. He julkaisevat turvallisuutta lisäävät ohjelmansa internetissä tai järjestelmiä tuottavien yritysten kautta. (Moore 2011, 24). Mustahattu- ja valkohattuhakkereihin jaottelua voidaan pitää karkeasti jaotteluna ”pahiksiin” ja ”hyviksiin” tai rikolliset tarkoitukset ja ei rikolliset tarkoitukset.

Valkohattuhakkerit voivat murtautua tietojärjestelmiin tuodakseen esiin niissä olevia tietoturva-aukkoja, mutta heidän toiminnallaan ei ole tarkoitus vahingoittaa ketään (Haasio 2013, 100). Vaikka

valkohattuhakkerin tarkoituksena ei olisi vahingoittaa tietojärjestelmää, voi valkohattuhakkeri syyllistyä rikokseen tunkeutumalla luvatta tietojärjestelmään. Luvatta tietojärjestelmiä käyttävät valkohattuhakkerit perustelevat ja oikeuttavat tekonsa sillä, että he varoittavat tietojärjestelmän puutteista ja heikkouksista. (Kirwan ym. 2013, 54).

Kirjallisuudessa valkohattuhakkerit esiintyvät eräänlaisina ”metsästäjinä”. Valkohattuhakkereiden osaaminen on yhtä korkealla tasolla kuin mustahattuhakkereiden, mutta he ovat päättäneet hyödyntää osaamistaan taistellakseen hyvän puolesta. He toimivat yhteistyössä viranomaisten kanssa ja voivat toimia konsultteina viranomaisille ja yrityksille. (Chiesa ym. 2009, 47).

Toisinaan valkohattuhakkerista käytetään myös termiä eettinen hakkeri (ethical hacker). Joidenkin määritelmien mukaan eettisellä hakkerilla tarkoitetaan tietojärjestelmän turvallisuuden kehittämiseen palkattua työntekijää tai konsulttia. Eettisellä hakkerilla on luvallinen pääsy tietojärjestelmään. Tietoturvakonsulttiyritysten laskuun organisaatioiden tietojärjestelmistä etsivistä hakkereista käytetään joskus myös ilmaisua sinihattuhakkerit (blue hat hackers) (Haasio 2013, 100).

Valkohattuhakkereista esiintyy myös varoituksia. Heitä ei pidetä huolenaiheena, mutta he voivat kääntyä musta- tai harmaahattuhakkereiksi. Yleisimpänä syynä tähän pidetään sitä, etteivät ohjelmistojen kehittäjät tai ylläpitäjät kuuntele heitä, kun he varoittavat turvallisuusuhasta tai etteivät he saa tarpeeksi kunnioitusta löydöistään. Valkohattuhakkerit käyttävät haavoittuvuuksien etsimiseen huomattaman määrän aikaa ja vaivaa, mutta siitä huolimatta heidän löytönsä voidaan jättää kokonaan huomioimatta. Tämä voi aiheuttaa hakkerissa suuren määrän raivoa ja kapinahenkeä. Pahimmassa tapauksessa heikkouden löytänyt hakkeri pysyy vaiti löydöstään ja käyttää sitä rikollisiin tarkoituksiin tai vahingoittaa ohjelmiston tuottajan imagoa. (Chiesa ym. 2009, 52).

4.2.3 Harmaahattuhakkerit

Harmaahattuhakkereita kuvaillaan kirjallisuudessa valkohattuhakkereiden ja mustahattuhakkereiden sekoituksena. (Moore 2011, 25). Harmaahattuhakkerit eivät identifioi itseään valkohattuhakkereiden tapaan ”hyviksiin”, mutta ei myöskään mustahattuhakkereiden tapaan ”pahiksiin” (Chiesa ym. 2009, 47). Harmaahattuhakkerit voivat toimia näkyvästi tai olla jakamatta hyvin vähän tietoa itsestään.

Harmaahattuhakkerit toimivat samoin kuin valkohattuhakkerit, mutta heidän löydettyään tietoturva-aukon esimerkiksi yrityksen sivuilla he haluavat löydöstään palkkion sen korjaamisesta (Haasio 2013, 100). Harmaahattuhakkerit voivat toimia ryhmissä, jossa yksi murtautuu tietojärjestelmään laittomasti ja sen jälkeen suosittelee järjestelmänylläpitäjälle ystäväänsä korjaamaan järjestelmän (Moore 2011, 25).

5 ALAKATEGORIAT

Edellisten ylemmän tason jaottelujen lisäksi muutamat tutkijat ovat vieneet jaottelua vielä syvemmälle. Näissä tutkimuksissa ja jaotteluissa on jonkun verran päällekkäisyyksiä. Suurin osa jaottelutavoista perustuu hakkerin kokemukseen, metodeihin ja motiiveihin.

5.1 Script-kiddie

Script-kiddies kategoria esiintyy kirjoissa omana kategorianaan musta-, valko- ja harmaahattuhakkereiden ohella (Moore 2011,25), mutta se esiintyy myös alakategoriana erityisesti mustahattuhakkereille (Chiesa ym. 2009, 48). *Script-kiddie*-hakkereita pidetään usein alimpana hakkerihierarkiassa ja heillä on usein vähän tai ei ollenkaan tietokoneohjelmoinnin taitoja (Moore 2011, 25). He käyttävät rikkomusten tekemiseen muiden kehittämiä työkaluja.

Script-kiddie-hakkeri on useimmiten teini-ikäinen, joka toimii yksin tai ryhmässä. (Chiesa ym. 2009, 53). *Script-kiddie*-hakkereita pidetään vaarallisena, sillä heillä ei ole ymmärrystä siitä, miten ohjelma vaikuttaa tietojärjestelmään hyökkäyksen yhteydessä (Moore 2011, 25).

Mustahattu *script-kiddies*-hakkerit voidaan jakaa edelleen pienempiin kategorioihin. Ensimmäinen alakategoria on *basic coders*, jotka ovat matalan tason ohjelmoijia. *Basic coders*-hakkerit eivät pysty muokkaamaan koodia tietoturvaheikkouksia paljastavaa hyökkäystä varten. Toinen alakategoria on *full-blown coders,* jotka käyttävät omaa koodiaan, mikäli se pystyvät siihen. Viimeinen alakategoria on *oops! script kiddies.* Heitä ei pidetä enää varsinaisina mustahattuhakkereina, mutta he ottavat vaikutteita mustahattuhakkereista. *Oops! Script kiddies*-hakkerit tekevät suuria ohjelmointivirheitä. (Chiesa ym. 2009, 48).

Matalamman tason harmaahattuhakkereita, jotka ymmärtävät vain vähän käytössä olevista keinoista tai antavat muiden tehdä päätökset heidän puolestaan, käytetään termiä *sheep* (Chiesa ym. 2009, 51).

Script-kiddie-hakkerin kanssa yhtäläisyyksiä löytyy Rogersin (2000) alakategoriasta *Newbie/tool kit.* Tällä kategorialla kuvataan henkilöä, kenellä on rajalliset tietokone- ja ohjelmointitaidot. Hakkerointi on heille uutta ja he tukeutuvat muiden tekemiin sovelluksiin. (Kirwan ja Power 2013, 56).

”37337 K-rAd iRC #hack 0-day Exploitz” Guy esiintyy kirjallisuudessa omana kategorianaan. Heitä kuvataan script-kiddies-hakkereiden tapaan huolta aiheuttaviksi, sillä he ovat valmiita tekemään mitä tahansa saadakseen nimensä tunnetuksi. He eivät hakkeroi tutkimalla, vaan sitä mitä on jo saatavilla. (Chiesa ym. 2009, 54).

5.2 Skill testers

Skill testers-hakkereita pidetään erityisesti harmaahattuhakkereiden alakategoriana. Hakkerit liikkuvat tietojärjestelmän sisällä käyttäen ”tarkistuslistaa” ja vahingoittaen järjestelmää. Musta- ja harmaahattuhakkereiden välillä skill testers-hakkereiden välillä on ero motiiveissa ja käytössä olevissa metodeissa. (Chiesa ym. 2009, 49–50).

5.3 Wannabe lamer

Wannabe lamer-hakkereita kuvataan huvittavaksi kategoriaksi. Heihin on mahdollista törmätä melkein missä tahansa internetissä, ja he pyytävät julkisesti ja jatkuvasti neuvoa moninaisilla selittelyillä. (Chiesa ym. 2009, 53).

5.4 Cyber-punks

Cyber-punks-hakkereilla on jo hieman paremmat tietokone- ja ohjelmointitaidot. He pystyvät jotenkuten luomaan omia työkaluohjelmia hakkerointiin ja heillä on hieman ymmärrystä järjestelmästä, johon he hyökkäävät. Heidän tarkoitusperänsä ovat pahantahtoisia. (Rogers 2000, viitattu teoksessa Kirwan ja Power 2013, 56).

5.5 Industrial spy

Industrial spy-hakkerin motiivina toimii raha. Heillä on usein paljon kokemusta ja taitoa. Tähän kategoriaan kuuluu esimerkiksi työtehtävien kautta tietoihin käsiksi pääsevät henkilöt. (Chiesa ym. 2009, 56.) Rogers (2000) käyttää kyseisistä hakkereista termiä *internals* (Kirwan ja Power 2013, 56).

5.6 Quiet, paranoid and skilled hacker

Quiet, paranoid and skilled hacker-kategorian hakkereita kuvataan ovelimmiksi hakkereiksi keiden motiivina ei ole raha. Heitä on hyvin vaikea löytää ja he saattavat viettää pitkiä aikoja hakkeroimissaan järjestelmissä tekemättä kuitenkaan mitään epämiellyttävää tai vakavaa. Heitä ei kiinnosta hakkeroinnin tuoma kuuluisuus, vaan he hakkeroivat kartuttaakseen omaa kokemusta. (Chiesa ym. 2009, 55).

6 MUUT HAKKERIKATEGORIAT JA TUTKIMUKSET

Tähän lukuun on koottu muita hakkerikategorioita ja tutkimuksia. Kyseiset kategoriat esiintyvät useammassa eri lähteessä, mutta niiden sijoittelu eri ylä- ja alakategorioiden välillä vaihtelee teoksen mukaan.

6.1 Haktivisti

Haktivistit ovat toimivat samalla tavalla kuin muut hakkerit, mutta tekojen motivaatio erottaa heidät muista hakkereista. Haktivisti hakkeroi levittääkseen poliittista viestiä. Suurimmassa osassa haktiviestien hyökkäyksistä tarkoituksena on päästä käsiksi nettisivujen servereihin ja muokata nettisivujen ulkoasu ja sisältö näyttämään haktivistien omaa viestiä tai poliittista näkemystä. Ekstrenimiset järjestöt hankkivat haktivisteja valtaamaan suosittuja nettisivuja ja muokkaamaan niitä järjestön tarpeiden mukaiseksi. (Moore 2011, 25–26).

Haktivistien toiminta on eräänlaista kansalaisvaikuttamista verkossa. Toiminnan tavoitteena on saada muutosta tai huomiota johonkin tiettyyn asiaan. Esimerkkejä haktivistien toiminnasta on sananvapauden ja ihmisoikeuksien edistäminen. (Haasio 2013, 101). Hakkeriryhmät yhdistetään joskus haktivismiin (Kirwan ja Power 2013, 74).

Peltomäki ja Norppa (2015, 56) luokittelevat haktivistit omaksi kategoriakseen hakkereiden ja krakkereiden rinnalle.

6.2 Kyberterroristi

Kirjallisuudessa kyberterroristit esiintyvät hakkereiden alakategorioissa ja käsite kattaa kaikki ammattirikolliset (Chiesa ym. 2009). Tämän lisäksi kyberterroristit esiintyvät kirjallisuudessa omana kategorianaan aiemmin mainittujen yläkategorioiden rinnalla (Moore 2011, 26).

Kyberterroristi-käsitettä pidetään melko uutena. Sitä käytetään kuvaamaan henkilöä, joka käyttää hakkerointitaitojaan herättääkseen ihmisissä pelkoa. Merkittävä ero muiden hakkereiden ja kyberterroristin välillä on hyökkäysten kohde. Kyberterroristi kohdentaa hyökkäyksensä kriittiseen infrastruktuuriin esimerkiksi ydinvoimaloihin ja vedenpuhdistamoihin. Hyökkäyksissä tunkeudutaan tietojärjestelmiin tai tietoverkkoihin, joilla aiheutetaan vahinkoa tai pahimmassa tapauksessa kuolemia. Internetin kasvun myötä kriittisiä kohteita on helpompi paikantaa ja aiheuttaa kauhua väestössä. (Moore 2011, 26).

Hakkereiden alakategorioissa esiintyy myös termi *cyber-warrior*, jota ei pidä sekoittaa kyberterroristiin. *Cyber-warrior* harvoin hyökkää kansainvälisiin kohteisiin, vaan he pitävät matalaa profiilia ja heidän kohteenaan voi olla esimerkiksi paikallinen yliopisto. Heidän motiivinsa on raha tai aatteellinen. (Chiesa ym. 2009, 56).

6.3 Knowledge exchange behavior

Aiemmin mainituista hakkereiden tarkoitusperiin perustuvista jaotteluista poiketen *knowledge exchange behavior*- jaottelussa (Zhang, Tsang, Yue ja Chau 2015) hakkerit jaetaan neljään ryhmää sen mukaan, kuinka hakkerit opettavat ja oppivat muilta hakkeriyhteisössä. Ensimmäinen ryhmä on

guru hakkerit (guru hackers), jotka pääasiassa opettavat muille hakkerointia. Toinen ryhmä koostuu kasuaaleista hakkereista (casual hackers), keiden osallistuminen hakkeriyhteisöihin on vähäistä. Kolmas ryhmä on oppivat hakkerit (learning hackers), jotka pääasiassa omaksuvat tietoa muilta ja neljäntenä ryhmänä noviisit hakkerit (novice hackers), ketkä pääasiassa oppivat muilta, mutta myös jakavat tietoaan hakkeroinnista. (Taylor ym. 2019, 101).

Knowledge exchange behavior- jaottelu haastaa muun jaottelun alan kehittyessä ja kuvaa hakkerointia käytöksenä, jossa opitaan muilta.

6.4 Jaottelu motiivien perusteella

Hakkereista esiintyy myös jaottelu neljään eri kategoriaan heidän motiiviensa perusteella. Ensimmäiseen kategoria on *the Funsters*, johon kuuluvat hakkerit hakkeroivat hauskuuden ja jännityksen takia ja ovat harvoin uhaksi. Toinen kategoria on *the Conscience of the Community.* He hakkeroivat paljastaakseen tietoturva-aukkoja. Kolmas Daviesin esittämä kategoria on *the Pink Slip Hackers,* joiden motiivina toimii kosto. Usein koston kohteeksi joutuu entinen työpaikka tai parisuhde. Viimeinen motiiveihin perustuva kategoria on *the Malicious Hackers*, jota Davies kuvaa kaikista harvinaisimmaksi kategoriaksi. *The Malicious Hacker* tavoittelee usein suurempaa vahinkoa ja omaa etuaan esimerkiksi hyötymällä hyökkäyksestä taloudellisesti. (Davies 2004).

7 POHDINTA

7.1 Johtopäätökset

Opinnäytetyön tavoitteena oli tutkia mihin eri kategorioihin hakkereita kirjallisuudessa jaetaan ja millä perusteilla jaottelu tapahtuu. Tutkiessani aihetta huomasin, että kirjallisuudessa esiintyvät jaottelut tapahtuvat pääasiassa hakkereiden tarkoitusperien ja motiivin perusteella. Käyttämässäni lähdemateriaalissa tuli vastaan yksi tutkimus, jossa hakkereiden jaottelu toteutettiin muulla perusteella.

Nostin esiin opinnäytetyössäni kaksi erilaista yläkategoriaa, joihin hakkerit jaetaan. Parissa käyttämässäni kirjassa kyseiset kategoriat olivat ainoat, joihin hakkereita jaoteltiin, parissa kirjassa niiden rinnalle oli nostettu muitakin kategorioita ja yhdessä kirjassa jaottelua jatkettiin vielä pidemmälle alakategorioihin. Hakkereiden jakaminen ainoastaan ”hyviksiin” ja ”pahiksiin” voi antaa hakkerista ja hakkerin aikeista liian pelkistetyn kuvan.

Kirjallisuudessa esiintyvät hakkerikategoriat eivät ole selkeitä. Kaikissa käyttämässäni lähdekirjallisuudessa hakkereita kuitenkin jaoteltiin jonkinlaisiin kategorioihin ja tuotiin ilmi, ettei hakkerin määritelmä ole yksiselitteinen.

Hakkereiden jaottelu eri kategorioihin ei ole mustavalkoista. Kirjallisuudessa esiin nousseet jaottelut olivat monilta osin päällekkäisiä ja sama termi oli määritelty eri tavalla riippuen tutkijasta ja kirjoittajasta. Haastavuutta jaotteluun toi se, että määritelmäeroja esiintyi myös ydintermien välillä ja sama termi saattoi olla määritelty hieman eri tavalla riippuen kirjoittajasta. Esimerkiksi osa kirjoittajista kirjoitti valkohattuhakkereista ja eettisistä hakkereista synonyymina, mutta toisessa teoksessa niiden kerrottiin eroavan toisistaan.

Opinnäytetyö sai minut pohtimaan hakkereiden kategorisoinnin tarpeellisuutta ja hyötyä. Yläkategorioiden kohdalla kirjallisuudesta kävi ilmi, että jaottelulla haluttiin erottaa rikolliset hakkerit laillisesti toimivista hakkereista.

Alakategorioiden kohdalla jäin pohtimaan miksi jaottelua on tarpeen viedä niin pitkälle ja miten jaottelua on mahdollista tehdä. Opinnäytetyötä kirjoittaessa pohdin ketä hakkereiden kategoriat palvelevat ja millaisia hyötyjä sillä saavutetaan.

Kirjallisuudesta kävi ilmi, etteivät hakkerit itse välttämättä osaa sijoittaa itseään mihinkään kategoriaan tai he sijoittavat itsensä eri kategoriaan kuin tutkijat. Olisi mielenkiintoista tietää miten paljon jaottelut eroavat hakkereiden itsensä tekemänä verrattuna tutkijoiden ja ulkopuolisen ihmisen tekemänä.

Jäin pohtimaan hakkereiden näkökulmaa jaotteluun. Kokevatko he, että kategorioita on tarpeeksi tai kokevatko he sopivansa mihinkään kirjallisuudessa mainittuihin kategorioihin. Ulkopuolisen määrittelemä jaottelu voi mahdollisesti tuntua negatiivisessa mielessä lokeroimiselta.

Opinnäytetyötä tehdessä huomasin, että suuri osa saatavilla olevasta aihetta käsittelevästä kirjallisuudesta on kirjoitettu noin kymmenen vuotta sitten. Aiheesta on kuulemma kirjoitettu viime vuosinakin paljon ja olisi mielenkiintoista tietää onko jaotteluihin tullut muutoksia tai uusia näkökulmia.

Aiheena hakkerointi ja sen taustatekijät ovat hyvin mielenkiintoisia. Tietoverkkoihin kohdistuvat rikokset eroavat perinteisestä rikollisuudesta hyvin paljon. On tärkeää, että sen ennalta estävään toimintaan on kiinnitetty huomiota.

7.2 Opinnäytetyön arviointi

Tämän opinnäytetyön työstäminen on ollut opettavaista monella tavalla, sillä aihe ei ollut minulle tuttu entuudestaan. Opinnäytetyön aihe ja sisältö muovautui jatkuvasti työstäessä sitä. Perehtyminen hakkerointiin ja hakkereihin opetti minulle valtavasti opinnäytetyön aiheesta ja sen ympäriltä.

En ollut aiemmin tehnyt opinnäytetyötä tai siihen rinnastettavaa kirjallista työtä. Opinnäytetyö opetti minulle tiedonhakua ja kykyä tarkastella lähteitä kriittisesti. Opin lukemaan tutkimuksia ja löytämään niistä oleellisen asian omaa työtäni varten.

Mielestäni kirjallisuuskatsaus oli hyvä tutkimusmenetelmä opinnäytetyön toteuttamista varten. Opinnäytetyön aineisto koostui suurimmaksi osaksi alaa käsittelevästä kirjallisuudesta ja aiemmista tutkimuksista, joten sen lähteitä voidaan pitää luotettavina. Käyttämistäni lähteistä kokosin olennaiset tiedot, joilla vastasin opinnäytetyöni tarkoitukseen selvittää kirjallisuudessa hakkereista esiintyvä jaottelu ja jaottelun perusteet.

Haastavinta opinnäytetyötä tehdessä oli aiheen rajaus. Hakkerointi oli minulle aiheena aivan uusi ja ymmärtääkseni hakkereiden jaottelua minun oli tutustuttava hakkerointiin laajemmin. Halusin tehdä opinnäytetyöstä selkeän ja helposti ymmärrettävän myös sellaiselle lukijalle kenelle aihe on entuudestaan tuntematon. Työstäessäni opinnäytetyötä huomasin, että hakkerointia olisi mahdollista tutkia enemmänkin, mikä toi haasteita opinnäytetyön raameihin.

Aihetta käsittelevää kirjallisuutta oli mielestäni saatavilla tarvittava määrä. Suurempi määrä lähteitä olisi tuonut lisää haasteita muodostaa opinnäytetyöstä johdonmukainen, sillä jokaisessa lähdeteoksessa jaottelu toteutettiin hieman eri tavalla ja osa kirjallisuudessa esiintyneistä määritelmistä termeille oli ristiriidassa keskenään. Opinnäytetyön sisältö jäi kuitenkin niukaksi, sillä kirjallisuudessa esiin nousivat pääasiassa samat termit. Ero kirjojen välillä syntyi näiden termien määritelmissä ja sijoittelussa ylä- ja alakategorioihin.

Useampi käyttämistäni lähteistä oli kirjoitettu jo 2010-luvun alkupuolella. En pidä lähteiden tarjoamaa tietoa vanhentuneena, vaikka tietoverkot ja niiden tarjoamat mahdollisuudet ovat kehittyvät jatkuvasti. Haastetta kirjoittamiseen toi myös englannin kielen taipumattomuus suomeksi. Tietojärjestelmiin liittyvät ilmaisut ovat yleisesti vakiintuneet lainasanoina suomen kieleen.

Opinnäytetyössäni käytin muutamia internetistä löytyviä lähteitä. Lähteet olivat pääasiassa viranomaisten ylläpitämiä nettisivuja. Lisäksi käytin uutista lähteenä tuomaan tietoa ajankohtaisesta ilmiöstä ja poliisin nettisivuja tietoverkkorikollisuuden tilastoihin ja tilanteeseen Suomessa.

Opinnäytetyölläni saavutin tavoitteeni avata lukijalle hakkerin käsitettä ja miten hakkerit eroavat kirjallisuudessa toisistaan. Opinnäytetyöni tarjosi perustietoa hakkeroinnista ja hakkereista sellaiselle lukijalle, joka on kiinnostunut aiheesta.

LÄHTEET

Chiesa, Raoul & Ducci, Stefania & Ciappi, Silvio 2009: Profiling hackers: The Science of Criminal Profiling as Applied to the World of Hacking, Boca Raton, Auerbach

Davies, Bryan 2004: Hacking: The Cyberworld's Oldest Profession is Indispensable R&D, iTnews. Luettavissa: https://www.itnews.com.au/feature/hacking-the-cyberworlds-oldest-profession-is-in-dispensable-rd-61773. Luettu: 17.5.2021.

Euroopan neuvosto 2001: Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus 60/2007. Luettavissa: https://www.finlex.fi/fi/sopimukset/sopsteksti/2007/20070060/20070060. Luettu 27.4.2021.

Haasio, Ari 2013: Netin pimeä puoli, Saarijärvi, Suomalaisen kirjallisuuden seura

Haikansalo, Anu % Korander, Timo 2019, Opinnäytetyöohje: Opinnäytetyön prosessi, toteutus ja arviointi poliisi (AMK) -tutkinnossa

Jämsén, Christian 2020: Tietoverkkorikollisuus poliisin silmin 2019-2020. Blogikirjoitus. Luettavissa: https://poliisi.fi/blogi/-/blogs/tietoverkkorikollisuus-poliisin-silmin-2019-2020. Luettu 12.3.2021.

Kirwan, Grainne & Power, Andrew 2013: Cybercrime: the psychology of online offenders. Cambridge, Cambridge University Press

Keskusrikospoliisisa käynnistyi hanke nuorten vakavaan tietoverkkorikollisuuten puuttumiseksi. Poliisin verkkosivut. Uutinen. Luettavissa: https://poliisi.fi/-/keskusrikospoliisissa-kaynnistyi-hanke-nuorten-vakavaan-tietoverkkorikollisuuteen-puuttumiseksi. Luettu 17.5.2021.

Moore, Robert 2011: Cybercrime: Investigating high-technology computer crime. 2. Painos, Burlington, Anderson

Peltomäki, Juha & Norppa, Kati 2015: Rikos meni verkkoon, Helsinki, Talentum

Ralston, William 2020: A dying man, a therapist and the ransom raid that shook the world, Wired. Luettavissa: https://www.wired.co.uk/article/finland-mental-health-data-breach-vastaamo. Luettu 28.4.2021.

Salminen, Ari 2011: Mikä on kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin, Vaasa, Luettavissa: https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf. Luettu 12.3.2021.

Taylor, Robert W. & Fritsch, Eric J. & Liederbach, John & Saylor, Michael R. & Tafoya, William L. 2019: Cyber crime and cyber terrorism. 4. Painos Hoboken, Pearson

Europol 2016: Youth Pathways into Cybercrime. Luettavissa: https://www.europol.europa.eu/publications-documents/youth-pathways-cybercrime. Luettu 12.3.2021.