Joonas Lahtinen

KYBERRIKOLLISEN PROFILOINTI OSANA KYBERRI-KOSTEN SELVITTÄMISTÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Lahtinen, Joonas
Kyberrikollisen profilointi osana kyberrikosten selvittämistä
Jyväskylä: Jyväskylän yliopisto, 2022, 25 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Clements, Kati

Kyberrikollisuus aiheuttaa nykypäivän yhteiskunnassa valtavia rahallisia vahinkoja. Kyberrikollisuudelle ei ole yksiselitteistä määritelmää, mutta sillä voidaan tarkoittaa esimerkiksi tietokoneita ja/tai tietoverkkoja hyödyntävää rikollisuutta. Yksi keino kyberrikosten selvittämiseksi on profilointi, eli joukko psykologisia metodeja, joilla pyritään rikollisen kokonaisvaltaiseen ymmärtämiseen. Profilointia suorittavat yleensä viranomaiset osana rikostutkintaa. Tämän kirjallisuuskatsauksen tavoitteena oli hahmottaa yleiskuva siitä, miten kyberrikollisen profiloinnilla voidaan selvittää kyberrikoksia. Löydettyjen tulosten mukaan kyberrikollisen profilointi auttaa erityisesti rajaamaan rikoksen potentiaalisten epäiltyjen määrää ja siten ohjaamaan rikostutkintaa oikeaan suuntaan.

Asiasanat: kyberrikollinen, kyberrikollisen profilointi, kyberrikollisuus, profilointi.

ABSTRACT

Lahtinen, Joonas
The role of cybercriminal profiling in solving cybercrime
Jyväskylä: University of Jyväskylä, 2022, 25 pp.
Information Systems, Bachelor's Thesis
Supervisor: Clements, Kati

Cybercrime is a constant cause of enormous economic damage. While cybercrime has no unequivocal definition, it can be described as "crime involving computers and/or data networks". Cybercriminal profiling is a part of solving cybercrime: it is a cluster of psychological methods with the objective of gaining a comprehensive understanding of a cybercriminal. Cybercriminal profiling is usually performed by governmental authorities. The main goal of this literature review was to reach an overview on how cybercriminal profiling can be used to assist in solving cybercrime. The results show that cybercriminal profiling can specifically help with reducing the suspect pool and thus keeping the overall investigation on the right track.

Keywords: cybercriminal, cybercriminal profiling, cybercrime, profiling.

TAULUKOT

SISÄLLYS

1 JOHDANTO

Erityisesti hyvinvointivaltioissa elämän kaikki osa-alueet, mukaan lukien henkilökohtainen viestintä, talousjärjestelmät ja kriittisen infrastruktuurin ylläpito, ovat riippuvaisia internetistä (Andress & Winterfeld, 2013). Vuonna 2021 jo noin 60 % kaikista maailman ihmisistä oli internetin käyttäjiä (Kemp, 2021). Näin ollen fyysisen maailman rinnalla toimii kyberavaruus: ympäristö, jossa tietokoneet ovat vuorovaikutuksessa toisiinsa tietoliikenneverkkojen avulla (Giansanti, 2021). Leukfeldt ja Holt (2019) toteavat, että perinteisen rikollisuuden rinnalle on kehittynyt kyberrikollisuus. Sillä voidaan tarkoittaa esimerkiksi tietokoneita ja/tai tietoverkkoja hyödyntävää rikollisuutta. (Leukfeldt & Holt, 2019) Kyberrikollisuuden aiheuttamia vahinkoja ei voi arvioida yksiselitteisesti, mutta rahallisesti vuosittaiset vahingot voivat nousta jopa yhteen triljoonaan Yhdysvaltain dollariin (Sviatun ym., 2021).

Yksi keino kyberrikosten selvittämiseksi on profilointi. Se on joukko metodeja, joilla pyritään kyberrikollisen kokonaisvaltaiseen ymmärtämiseen (R. Leukfeldt & Holt, 2019). Tavallisesti profilointia suorittavat viranomaiset osana kyberrikosten tutkintaa, mutta joissakin tapauksissa sitä tekevät yksityiset tutkijat (Edwards, 2019). Vaikka profilointimetodit ovat samankaltaisia ympäri maailman, esimerkiksi rikosten tunnusmerkistöt ja lainsäädännöt valtioiden välillä eroavat merkittävästi (Phillips ym., 2022). Kyberrikollisen profiloinnista on vain vähän Suomessa tehtyjä tai suomenkielisiä tutkimuksia. Tämän kirjallisuuskatsauksen tarkoitus on muodostaa suomenkielinen yleiskuva kyberrikollisen profiloinnista. Ensisijainen tavoite on löytää vastauksia tutkimuskysymykseen:

> ”Miten kyberrikollisen profiloinnilla voidaan selvittää kyberrikoksia?”

Lähteitä etsittiin JYKDOK-, Google Scholar -, IEEE Xplore - ja Scopus-tietokannoista. Lähteinä pyrittiin käyttämään mahdollisuuksien mukaan laadukkaita, viimeaikaisia, vertaisarvioituja tieteellisiä artikkeleita. Hakusanoina käytettiin pääasiassa seuraavia sanoja:

- ”cybercriminal” (tai ”cyber-offender”)

- ”cybercrime” (tai ”cyber crime”)
- ”profiling”
- ja näiden yhdistelmiä.

Tutkielma koostuu viidestä luvusta. Toisessa eli johdannon jälkeisessä luvussa käsitellään kyberrikollisuutta. Kolmas luku koskee kyberrikollisen profilointia. Neljännessä luvussa analysoidaan kahta esimerkkitapausta ja tiivistetään tutkielman tulokset helposti luettavaan muotoon. Lopuksi viidentenä lukuna esitetään yhteenveto.

2 KYBERRIKOLLISUUS

Yar ja Steinmetz (2019) kertovat, että sana kyber esiintyy tavallisesti yhdyssanan määriteosana. Tyypillisissä konteksteissaan se liittyy digitaalisessa muodossa olevan informaation käsittelyyn. (Yar & Steinmetz, 2019.) Fyysisen maailman rinnalle on kehittynyt kyberavaruus: ympäristö, jossa tietokoneet ovat vuorovaikutuksessa toisiinsa tietoliikenneverkkojen avulla (Giansanti, 2021). Kyberturvallisuus tarkoittaa tapoja, joilla puolustetaan tietokoneita, mobiililaitteita, palvelimia, verkkoja, tietojärjestelmiä ja dataa haitallisilta hyökkäyksiltä (Yar & Steinmetz, 2019). Turvallisuuskomitean (2018) mukaan kyberturvallisuudella tarkoitetaan ”tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Kybertoimintaympäristön häiriintyminen aiheutuu usein toteutuneesta tietoturvauhkasta. Tietoturva viittaa tiedon saatavuuteen, eheyteen ja luottamuksellisuuteen. Siten se on kyberturvallisuuden alakäsite. (Turvallisuuskomitea, 2018.) Kyberrikollinen (engl. cybercriminal, cyber-offender) on kyberrikokseen syyllistynyt henkilö (Bada & Nurse, 2021). Tarkempaa yksittäistä määritelmää on vaikea antaa, koska kyberrikollisten joukko on niin monipuolinen (Bada & Nurse, 2021).

Leukfeldtin ja Holtin (2019) mukaan informaatioteknologian väärinkäytöstä kirjoitettiin ensimmäisen kerran 1970-luvulla. Tuolloin aloitettiin käyttämään termiä ”rikollisuus tietokonetta käyttäen” (engl. crime by computer). Tosin tuohon aikaan tietokoneet eivät olleet niinkään rikosvälineitä, vaan rikosten kohteita. Vuosikymmenien kuluessa on syntynyt lukuisia samankaltaisia termejä, kuten tietokonerikollisuus, e-rikollisuus ja internetrikollisuus. Kyberrikollisuus on kuitenkin ylivoimaisesti eniten käytetty termi muihin verrattuna. Tarkkoja syitä juuri kyseisen termin vakiintumiseen ei tunneta. (Leukfeldt & Holt, 2019.)

Kyberrikollisuudella (engl. cybercrime) voidaan tarkoittaa esimerkiksi ”1. laajaa joukkoa laittomia rikoksia tai muuten haitallisena pidettyä toimintaa, jota yksityiset henkilöt tai ryhmät toteuttavat kohteenaan tietokoneet, tietokoneavusteiset laitteet, muut laitteet tai informaatioteknologiaverkot… ja 2. perinteisiä rikoksia tai muita tekoja, jotka kohdistetaan henkilöihin hyödyntäen internetiä tai teknologiaa” (Donalds & Osei-Bryson, 2019). Tutkija Wall (2001) tiivistää asian lyhyemmäksi: kyberrikollisuus on ”haitallista toimintaa, joka liittyy jollakin lailla tietokoneisiin”. Toisaalta määritelmän liiallinen yksinkertaistaminen voi herättää kysymyksiä, kuten että minkä tyyppisiä rikoksia määritelmään halutaan sisällyttää (Leukfeldt & Holt, 2019).

Yhtenäistä, tarkkaa määritelmää kyberrikollisuudelle ei ole olemassa, mikä aiheuttaa hämmennystä sekä loppukäyttäjissä että tutkijoissa (Sarwar, 2016). Myös maantieteelliset erot ovat oleellisia: rikosten määritelmät voivat olla huomattavan erilaisia, kun tarkastellaan eri valtioiden lainsäädäntöä (Phillips ym., 2022). On kuitenkin muistettava, että tärkein asia ei ole määritelmän tarkkuus, vaan se, mitä me teemme kyberrikollisuuden suhteen (Leukfeldt & Holt, 2019).

2.1 Kyberrikokset

Leukfeldtin ja Holtin (2019) mukaan tieteellisessä kirjallisuudessa kyberrikoksista käytetään yleensä kaksi- tai kolmeosaista mallia. Kaksiosaisen mallin eniten käytetyn version mukaan kyberrikoksia on kahta tyyppiä: kyberavustettuja ja kyberriippuvaisia. Kyberavustetut rikokset ovat sellaisia laittomia tekoja, joita on tehty jo ennen tietokoneaikaa ja joita teknologian käyttö nykypäivänä helpottaa. Niiden joukkoon kuuluvat muun muassa huumausaineiden salakuljetus ja internetissä välityksellä tapahtuva häirintä. Kyberriippuvaiset rikokset edellyttävät digitaalisen maailman käyttöä ja sellaisia ovat esimerkiksi haktivismi tai tietokoneen näytölle syötettävä lunnasvaatimus. Mielenkiintoisesti myös lainsäätäjät käyttävät laajasti kaksiosaista mallia. (Leukfeldt & Holt, 2019.)

Kolmiosaisissa malleissa on joko jaettu kaksiosainen malli kolmeen osaan, tai kahden osan rinnalle on kehitetty kolmas osa (Phillips ym., 2022). Wall (2007) kuului tutkijoihin, jotka ensimmäisen kerran esittivät kolmiosaisen mallin:

- ”Rikokset tietokonetta vastaan”, kuten hakkerointi
- ”Rikokset tietokonetta käyttäen”, kuten piratismi.
- ”Rikokset tietokoneessa”, kuten laiton pornografia. (Wall, 2007.)

Kolmiosainen malli on laajasti käytetty myös valtiollisissa ja muissa vastaavissa toimijoissa. Euroopan komissio otti vuonna 2013 käyttöön edellä mainitun mallin, mutta eri tavoin ilmaistuna:

- ”Rikokset tietokoneisiin tai tietojärjestelmiin, kuten haittaohjelmat”
- ”Perinteiset rikokset, kuten petos, väärennys, identiteettivarkaus”.
- ”Sisältörikokset, kuten laittoman pornografian levitys”. (Euroopan komissio, ei pvm.)

Yksi ansaintakeino kyberrikollisille on varastetun tiedon myyminen pimeillä markkinoilla (Smith ym., 2018). Tosin O’Kane ym. (2018) huomauttaa varastettu tieto ei ole enää nykypäivänä niin arvokasta kuin aiemmin. Sen sijaan haittaohjelmien suosio on lisääntynyt. Esimerkiksi kiristyshaittaohjelmia voi ostaa helppokäyttöisinä palveluina (engl. ransomware as a service, RaaS), jolloin niiden käyttö rikostarkoitukseen ei vaadi välttämättä erityistä teknistä osaamista. (O’Kane ym., 2018.) Mandiant (2020) listaa raportissaan haittaohjelmia, jotka oli havaittu vuoden 2019 aikana. Jopa 41 % haittaohjelmista oli täysin uusia eli niitä ei oltu havaittu koskaan aiemmin ennen vuotta 2019. (Mandiant, 2020.) Tällaiset luvut havainnollistavat alan nopeaa muutosta ja kehitystä.

Finklea (2015) toteaa, että internetin julkisin ja helpoiten löydettävissä osa, avoin verkko (engl. surface web), muodostaa vain noin 5 % koko internetistä. Noin 90 % on syvää verkkoa (engl. deep web), jonka sisältämä tieto ei ole indeksoitua, kuten monet tietokannat ja intraverkot, joten tavalliset hakukoneet eivät löydä niitä. Toisin kuin joskus mediassa annetaan ymmärtää, suurin osa syvästä

verkosta ei liity millään tavalla rikolliseen toimintaan. Syvän verkon pieni osa on pimeä verkko (engl. dark web), jonne pääsy vaatii erityisen, anonymisoivan internetselaimen. Pimeän verkon tarkkaa kokoa tai osuutta syvästä verkosta ei tunneta. Arviolta 57 % internetin rikollisesta toiminnasta tapahtuu pimeässä verkossa. (Finklea, 2015; Nazah ym., 2020.)

2.2 Kyberrikostyyppejä

On mahdotonta tehdä tarkkaa listaa kyberrikostyypeistä, kun otetaan huomioon alan laajuus ja erimielisyydet siitä, mikä ylipäätään on kyberrikos (Phillips ym., 2022). Clough'n (2015) mukaan yleisimpien kyberrikosten tyyppeihin kuuluvat seuraavat:

Kiristyshaittaohjelma (engl. ransomware) nimensä mukaisesti lukitsee tiedostoja ja uhkaa avata ne vasta, kun uhri on maksanut lunnaat (Clough, 2015). Kiristyshaittaohjelmat ovat rikollisille ”erittäin palkitsevia” muun muassa siksi, koska niitä voi käyttää hyvin pitkälle automatisoituneesti (O’Kane ym., 2018). Yar ja Steinmetz (2019) korostavat, että kiristyshaittaohjelma on haittaohjelmien tyypeistä ”kaikista tuhoisin”.

Tietokonevirus (engl. computer virus) on haittaohjelma, joka saastuttaa tietokoneiden tiedostoja tai ohjelmia (Clough, 2015). Tästä aiheutuva haitta voi olla esimerkiksi halutun viestin näyttäminen ponnahdusikkunassa tai tiettyjen tiedostojen poistaminen. Virukset leviävät tietokoneesta toiseen tekemällä kopioita itsestään. (Clough, 2015.)

Mato (engl. worm) on myös haittaohjelma (Clough, 2015). Toisin kuin virus, mato voi levitä tietokoneesta toiseen ilman minkään tiedoston tai ohjelman saastuttamista. Leviäminen voi olla esimerkiksi tietokoneen RAM-muistin kautta. (Clough, 2015.)

Troijalainen (engl. Trojan horse), on ohjelma, joka tyypillisesti näyttää tavalliselta, mutta samanaikaisesti toimii taustalla aiheuttaen haittaa esimerkiksi asentamalla tietokoneviruksia tai matoja (Clough, 2015).

Hakkerointi tarkoittaa luvatonta tunkeutumista tietokoneisiin. Sillä tavoitellaan esimerkiksi tietokoneeseen tallennetun tiedon muokkaamista, varastamista tai tuhoamista. (Clough, 2015.)

Palvelunestohyökkäyksessä (engl. denial of service, DoS) luodaan kohdetietokoneeseen tai -palvelimeen niin suuri määrä pyyntöjä, että kohde ei pysty toimimaan normaalisti (Clough, 2015). Tosin nykypäivänä on tavallista, että hyökkäys toteutetaan samanaikaisesti useasta eri lähteestä. Silloin kyseessä on hajautettu palvelunestohyökkäys (engl. distributed denial of service, DDoS). Lähdetietokoneet voivat olla saastutettuja tavallisten käyttäjien tietokoneita, jotka toimivat osana hyökkäystä ilman, että käyttäjä välttämättä huomaa asiaa. Silloin kyseessä on niin kutsuttu bottiverkko. (Clough, 2015.)

Identiteettivarkaudessa (engl. identity theft) hankitaan toisten henkilöiden nimiä, henkilötunnuksia tai muita tunnistetietoja (Clough, 2015). Näitä hyväksi käyttäen suoritetaan esimerkiksi petoksia. (Clough, 2015.)

Roskaposti (engl. spam) on postia, jolla pyritään esimerkiksi huijaamaan tai saastuttamaan vastaanottajan tietokone haittaohjelmalla (Clough, 2015). Tavallisille käyttäjille tunnetuin roskapostin levitysmuoto lienee sähköposti (Phillips ym., 2022). Roskapostia voidaan tehostaa esimerkiksi homografihyökkäyksellä. Siinä sähköpostin lähettäjäosoitteesta, kuten ”tim@apple.com”, vähintään yksi merkki on vaihdettu toiseksi, mutta visuaalisesti identtiseksi merkiksi. Tosin sähköpostisovelluksissa ja internetselaimissa on nykyisin tehokkaat suojaukset homografihyökkäyksiä vastaan. (Quinkert ym., 2019.)

Tietojenkalastelua (engl. phishing) voidaan suorittaa monin tavoin (Clough, 2015). Yksi tapa on käyttäjien houkuttelu verkkosivustoille, jotka ovat tarkasti tehtyjä, mutta väärennettyjä kopioita tunnetuista verkkosivustoista. Käyttäjien toivotaan antavan luottokorttinumeroitaan tai muuta arvokasta tietoa. (Clough, 2015.) Huijausverkkosivun osoitteeseen voi olla piilotettu edellä mainittu homografihyökkäys (Quinkert ym., 2019). Tosin nykyisin myös internetselaimet informoivat tehokkaasti käyttäjää havaitessaan väärennetyltä vaikuttavan verkkoosoitteen. (Quinkert ym., 2019.)

2.3 Motiivit

Jokaisen rikoksen takana on yksi tai useampi motiivi (Warikoo, 2014). Toisaalta, jos rikoksella ei ole selvää kohdetta, vaan rikos on suunnittelematon teko tai vahinko, sillä ei välttämättä ole selvää motiiviakaan. Kyberrikollisuuden tutkiminen esimerkiksi sosiaalipsykologian näkökulmasta auttaa ymmärtämään tehtyjen rikosten motiiveja (Thackray ym., 2016). Edwardsin ym. (2022) listauksen mukaan kyberrikollisuuden yleisimpiä motiiveja ovat:

- taloudellinen hyöty
- kosto
- vallanhimo
- uteliaisuus
- tyydytys tietoturvan murtamisesta
- matala rangaistuksi tulemisen riski
- kyberrikollisuuden moraalisesti oikeutetuksi kokeminen. (Edwards ym., 2022.)

Jotta rikoksen voidaan todeta tapahtuneen, vaaditaan monessa tuomioistuimessa näyttöä siitä, että jokainen rikoskolmion kolmesta osasta on ollut läsnä: motiivi, mahdollisuus ja kohde (Leukfeldt & Holt, 2019). Siksi rikosten motiivien ymmärtäminen ja tutkiminen on tärkeää (Leukfeldt & Holt, 2019).

Leukfeldt ja Holt (2019) huomauttavat, että kyberrikollisuuden motiiveihin keskittyvä tieteellinen tutkimus on osittain ongelmallista. Suuri osa tutkimuksista perustuu vastaajien täyttämiin itsearviointilomakkeisiin. Ottaen huomioon aiheen arkaluontoisuuden, osa vastaajista saattaa liioitella tai vähätellä tekojaan.

Toinen haaste on ammattimaisten kyberrikollisten saavuttaminen: vastaajilla on usein suhteellisen vähän kokemusta kyberrikosten tekemisestä. (Leukfeldt & Holt, 2019.)

2.4 Uhrit

Usein kyberrikolliset valitsevat uhrinsa strategisesti ja etsivät näistä heikkoja kohtia (Smith ym., 2011). Uhriksi voi joutua lähes kuka tahansa: yksityishenkilöt, julkisen sektorin toimijat, yritykset, valtiot… (Smith ym., 2011). O'Kane ym. (2018) muistuttaa samasta vaarasta: uhrit eivät rajoitu mihinkään pieneen joukkoon kuten pankkeihin, vaan internet mahdollistaa tavallisten käyttäjienkin helpon tavoittamisen (O'Kane ym., 2018). Internetin käyttäjämäärän lisääntyessä kasvaa myös internetiin tallennetun henkilökohtaisen tiedon määrä, ja tuo tieto on mahdollisesti rikollisille arvokasta (Smith ym., 2018).

Donato (2021) muistuttaa, että rikoksen kohde ei tarkoita samaa kuin rikoksen uhri, vaikka ne ovat joskus samoja. Yrityksen verkkosivua vastaan suoritettavan DDoS-hyökkäyksen kohde voi olla yrityksen hallitus. Jos kyseinen verkkosivusto kaatuu, voidaan rikoksen uhreiksi katsoa yrityksen lisäksi käyttäjät, jotka eivät voi enää käyttää verkkosivustoa. (Donato, 2021.)

Kun vertaillaan kaikkien alojen pörssiyrityksiä, kyberrikosten yleisiä uhreja ovat vähittäiskauppa ja terveydenhuoltoala (Smith ym., 2018). Kyberrikos yritystä vastaan voi aiheuttaa "äärimmäisen korkeat" rahalliset vahingot (Meland ym., 2015). Tietoturvayritys Kaspersky (2021) kertoo, että hajautettu palvelunestohyökkäys voi aiheuttaa jopa 120 tuhannen Yhdysvaltain dollarin kulut pienelle–keskisuurelle yritykselle. Suuryrityksen tapauksessa kulut voivat ylittää kaksi miljoonaa dollaria. (Kaspersky, 2021)

Välittömien kulujen, kuten haittaohjelmien poistamisen tai tietojärjestelmien korjaamisen, lisäksi täytyy muistaa myös mahdolliset asiakkaille maksettavat korvaukset. Tällaisten riskien olemassaolon vuoksi vakuutusyhtiöt ovat aloittaneet erityisten kybervakuutukset myymisen. (Meland ym., 2015) Pidemmällä aikavälillä kyberrikoksia runsaasti kohdannut yritys voi menettää tärkeitä sidosryhmiään, ja pörssiyritysten markkina-arvot voivat laskea (Smith ym., 2011).

2.5 Eroja perinteiseen rikollisuuteen

Yleisesti katsottuna kyberrikokset ovat "merkittävästi haastavampia" havaita ja tuomita kuin perinteiset rikokset, kuten ryöstöt tai murtovarkaudet (Butkovic ym., 2019). Suuressa osassa perinteistä rikollisuutta tekijän täytyy olla tapahtumapaikalla suorittaakseen rikoksensa, mutta kyberrikoksia voi tehdä ilman minkäänlaista fyysistä läsnäoloa (Clough, 2010). Nykyteknologian myötä tekijä voi toimia täysin virtuaalimaailmasta käsin niin, että hänellä ei ole havaittavissa

minkäänlaisia kasvoja tai tunteita (Greco & Greco, 2020). Smith ym. (2018) on samaa mieltä: kyberrikollisuus mahdollistaa helpon piiloutumisen tietokoneen taakse.

Verrattuna perinteisiin rikoksiin, kyberrikokset saattavat tuottaa tekijöilleen huomattavasti enemmän rahallista hyötyä (Leukfeldt & Holt, 2022). Kyberrikoksissa voi saavuttaa vaivattomammin suuren määrän uhreja samanaikaisesti, ja saatu rikoshyöty on usein helpommin muutettavissa rahaksi, jos se ei ole jo rahana (Leukfeldt & Holt, 2022).

Kriminologian keskuudessa on epäselvää, tekevätkö kyberrikolliset säännönmukaisesti tietyntyyppisiä rikoksia (”erikoistuminen”) vai tekevätkö he erityyppisiä rikoksia tilanteista ja olosuhteista riippuen (”mukautuminen”) (Leukfeldt & Holt, 2022). Ensimmäinen tähän kysymykseen vastausta etsivä tutkimus julkaistiin yllättävän myöhään, vuonna 2022 Leukfeldtin ja Holtin toimesta. Tutkimuksessa analysoitiin 37:ää systemaattisesti valikoitua rikollisverkkoa, joiden data oli kerätty viranomaisilta Alankomaista, Saksasta, Iso-Britanniasta ja Yhdysvalloista. Tuloksien mukaan 48 % rikollisverkostoista teki ainoastaan tietyntyyppisiä kyberrikoksia, kun taas 52 % teki useita erityyppisiä kyberrikoksia ja/tai perinteisiä rikoksia. (Leukfeldt & Holt, 2022.)

3 KEINOJA KYBERRIKOLLISEN PROFILOIMISEKSI

Bada ja Nurse (2021) näyttävät, että nopeasti kasvava kyberrikollisuus on synnyttänyt erilaisia vastakeinoja yrityksissä, valtionhallinnoissa ja akateemisessa maailmassa. Valtiot ovat reagoineet rakentamalla säädöksiä sekä lakeja ja vahvistamalla viranomaisten oikeuksia torjua rikoksia. Yrityksissä on priorisoitu turvallisuusperiaatteita, -prosesseja ja -säännöstelyä. Tiedeyhteisöissä on keskitytty yhdistämään tieteenaloja kuten tietotekniikkaa, psykologiaa ja kriminologiaa eli rikollisuuden tutkimusta. Edellä mainitut toimet ovat kriittisiä kokonaiskuvan kannalta, mutta eräs asia on saanut huomattavasti vähemmän huomiota: kyberrikollisen profilointi. (Bada & Nurse, 2021.)

Ennen profiloinnin käsittelyä on oleellista esitellä kyberrikosten tutkinta (engl. cyber forensics). Sammes'n ja Jenkinsonin (2007) mukaan se on prosessi, jossa pyritään tunnistamaan, säilyttämään, analysoimaan ja esittämään digitaalista todistusaineistoa. Toisinaan käytetään synonyymitermiä ”digitaalisten rikosten tutkinta” (engl. digital forensics). Tietokonerikostutkintakin (engl. computer forensics) nähdään tavallisesti synonyymina kyberrikosten tutkinnalle, mutta joissakin lähteissä sillä viitataan ainoastaan tietokoneympäristöön, joka puolestaan on vain yksi osa kyberrikosympäristöä. (Sammes & Jenkinson, 2007.)

3.1 Profilointi

Rikollisen profilointi (engl. criminal profiling), tarkoittaa ”laillisia psykologisia metodeja, joilla määritetään rikollisen käytöstapoja, luonteenpiirteitä, demografisia piirteitä ja joilla ennustetaan rikollisen tulevia tekoja” (Kipane, 2019). Donaton (2021) mukaan se on välttämätön edellytys, jotta puolustajaosapuolet kykenevät tehokkaaseen kyberriskien hallintaan. Vaihtoehtoisia termejä ovat psykologinen profilointi (engl. psychological profiling) ja käyttäytymisprofilointi (engl. behavioural profiling) (Donato, 2021).

Useimmiten profilointia toteuttavat viranomaiset, kuten rikostutkijat (Kipane, 2019). Toisinaan toteuttaja on yksityinen tutkija tai muu ei-viranomainen (Edwards, 2019). Rikollisen profiloinnilla on monipuolinen rooli rikostutkimuksessa. Rikospsykologisen profiilin muodostaminen on vain yksi tavoitteista (Donato, 2021). Muita tavoitteita ovat:

- Rajata epäiltyjen määrää
- Avustaa tapausten kytköksien löytämisessä
- Mahdollistaa tutkintaresurssien tehokkaampi käyttö
- Ohjata tutkijoita huomaamattomien todisteiden luo
- Luoda strategioita selvittämättömiin tapauksiin
- Määrittää sovellettavia kuulustelustrategioita
- Suojata potentiaalisia uhreja. (Donato, 2021; Turvey, 2012.)

Profiloitava kohde on yleensä rikollinen, mutta profiloinnilla tutkitaan muitakin käyttökohteita (Donato, 2021). Sen avulla voidaan pyrkiä etsimään henkilöitä, jotka ovat korkeammassa riskissä joutua tiettyjen rikosten uhriksi, tai paikkoja, joissa rikosten tapahtuminen on todennäköisempää (Custers, 2021).

Rikollisen profilointi voidaan jakaa yksinkertaisimmillaan kahteen eri metodiin (Georgiev, 2019). Induktiivisessa profiloinnissa analysoidaan tuomituista rikollisista saatua dataa, josta muodostuu yleistäviä käyttäytymismalleja. Näin voidaan ennustaa henkilön luonteenpiirteitä ja käyttäytymistä tietyntyyppisiin rikoksiin liittyen. Nimensä mukaisesti metodi perustuu induktiiviseen logiikkaan eli yksittäisistä havainnoista rakennetaan yleisiä käsityksiä. (Georgiev, 2019.) Butkovic'n ym. (2019) mukaan eräs esittelemisen arvoinen induktiivinen metodi on maantieteellinen profilointi. Siinä syötetään olemassa olevaa dataa tarkoitukseen erikoistuneeseen ohjelmistoon, joka matemaattisten kaavojen avulla voi auttaa rikollisen sijainnin paikallistamisessa. (Butkovic ym., 2019.)

Deduktiivisessa profiloinnissa analysoidaan rikoksista kerätyn datan muodostamaa kokonaiskuvaa, jonka perusteella rakennetaan oletuksia ja johtopäätöksiä yksittäisistä rikollisista (Georgiev, 2019). Tässä metodissa tutkijan on tärkeää pystyä asettamaan itsensä rikollisen asemaan. (Georgiev, 2019.)

Profiloinnin tuloksena voi muodostua liian yksinkertaistettuja tai merkityksettömiä malleja (Custers, 2021). Butkovic ym. (2019) muistuttaa, että pelkkä profilointi itsessään riittää harvoin rikoksentekijän tunnistukseen. Ensisijaisesti profilointi mahdollistaa potentiaalisten epäiltyjen määrän rajaamisen, mikä omalta osaltaan auttaa käyttämään rajattuja tutkintaresursseja tehokkaammin. Maantieteelliselle profiloinnille ominaisia haasteita ovat rikollisten muuttuva käytös, kyberavaruuden uniikkius verrattuna fyysiseen maailmaan ja todellisen rikospaikan paikantaminen. (Butkovic ym., 2019.)

Taulukossa 1 esitetään Georgiev'n (2019) yksinkertainen malli profilointimenetelmän valitsemiseksi silloin, kun vaihtoehtoina ovat induktiivinen ja deduktiivinen metodi. Taulukkoa tulkitaan seuraavasti:

- Kyberrikollisilta tiedon saaminen on vaikeaa. Kuitenkin yksittäisten kyberrikollisten piirteistä voidaan rakentaa yleiskuva käyttämällä deduktiivista me
- Kyberrikosten uhreilta on helppo saada tietoa. Voidaan käyttää kumpaa tahansa metodia.
- Kyberrikosten tutkijoilta on helppo saada tietoa. Voidaan käyttää kumpaa tahansa metodia. (Georgiev, 2019.)

TAULUKKO 1 Profilointimetodin valinta (Georgiev, 2019 mukaan)

Rooli	**Käyttö ensisijaisena tiedonlähteenä**	**Mahdollisuus käyttää yleiskuvan rakentamiseksi**	**Sovellettava profilointimetodi**
Kyberrikollinen	Vaikeaa	Hyvä	Deduktiivinen
Kyberrikoksen uhri	Helppoa	Erittäin hyvä	Induktiivinen ja deduktiivinen
Kyberrikoksen tutkija	Helppoa	Erittäin hyvä	Induktiivinen ja deduktiivinen

3.2 Tieteellisen tutkimuksen puutteita

Kyberrikollisen profilointiin keskittyvän tieteellisen tutkimuksen määrä kasvaa vakaasti (Leukfeldt & Holt, 2019). Jatkuvasti kehittyvä tutkimus johtaa väistymättä kehittyneempiin ja hyödyllisempiin rikollisentunnistusprosesseihin ja -strategioihin (Nykodym ym., 2005). Vaikka kyberrikosten tutkinta kehittyykin, se on silti ”alkutekijöissään” verrattuna muun tyyppisten rikosten tutkintaan (Donato, 2021). Bada ja Nurse (2021) esittävät neljä osa-aluetta, joissa tarvitaan kriittisesti lisää tutkimusta:

- Yhtenäinen määritelmä. Kyberrikollisen profiloinnille olisi tarpeellista saada nykyistä yhtenäisempi määritelmä. (Bada & Nurse, 2021.)
- Yhtenäisempi lähestymistapa. Kyberrikollisen profiloinnin tutkimukselle täytyy saada nykyistä yhtenäisempi ja systemaattisempi lähestymistapa (Bada & Nurse, 2021.). Silloin tällöin tutkijat ovat esittäneet erilaisia viitekehyksiä ja malleja kyberrikollisen profiloinnille, mutta mitkään niistä eivät ole päätyneet alan standardiksi (Bada & Nurse, 2021; Balogun & Zuva, 2018; Georgiev, 2019; Nykodym ym., 2005).
- Persoonallisuuden piirteet. Tarvittaisiin tutkimuksia muun muassa siitä, miten henkilön persoonallisuuden piirteet vaikuttavat siihen, suuntaako hän tekemään kyberrikoksia (Bada & Nurse, 2021).
- Datan puute. Laajoja datamassoja on liian vähän ja tutkijoiden pääsy niihin on haasteellista. Dataa keräämään tarvitaan erityisesti viranomaisia. (Bada & Nurse, 2021.) Myös Butkovic ym. (2019) pitää data-aineistojen vähyyttä ongelmallisena. Donato (2021) tarkentaa ongelmia: viranomaisilta pyydettävän datan luottamuksellisuus voi estää datan luovuttamisen. Datan liikuttamisen haasteet lisääntyvät entisestään, jos tutkijat ja viranomaiset sijaitsevat keskenään eri valtioissa. (Donato, 2021.)

4 ESIMERKKITAPAUKSET JA TULOKSET

Tässä luvussa käsitellään kahta esimerkkitapausta, joissa on käytetty profilointia kyberrikosten tutkintaan liittyen. Tavoite on rakentaa parempi kokonaiskuva siitä, miten kyberrikollisia profiloidaan ja minkälaisia tuloksia profiloinnilla saadaan selville. Sen jälkeen analysoidaan esimerkkitapauksia ja pyritään tunnistamaan niistä teorioita, joita on esitetty tämän tutkielman edellisissä luvuissa. Lopuksi kootaan tutkielmassa löydetyt tulokset helposti luettavaan muotoon ja yhdistetään ne erääseen viitekehykseen.

4.1 Tapaus 1: Huumausaineiden salakuljetusrikoksia

Ovcharenkon ym. (2020) artikkelissa *Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method* tutkitaan huumausaineiden salakuljetukseen liittyviä rikoksia, jotka oli tehty internetiä hyödyntäen Ukrainassa. Kaikki viisi kirjoittajaa toimivat julkaisuhetkellä yliopistoissa Ukrainassa muun muassa kriminologian ja psykiatrian laitoksilla. Tutkimus perustuu toissijaisiin lähteisiin, lähinnä tutkimuksiin, koska määrällisen datan hankkiminen järjestelmällisesti Ukrainassa on haastavaa. Tutkimuksen tavoitteet olivat seuraavat:

1. Tutkia rikollisia, jotka tekevät internetiä hyödyntäen huumausaineiden salakuljetukseen liittyviä rikoksia.
2. Tutkia tyypillisiä rikostutkimustilanteita, joita syntyy, kun tutkitaan mainittuja rikoksia.
3. Muodostaa tavoitteita 1. ja 2. hyödyntäen kokonaisvaltaisia suosituksia, jotka auttavat taistelemaan mainittuja rikoksia vastaan. (Ovcharenko ym., 2020.)

Ovcharenko ym. (2020) on samaa mieltä yleisen käsityksen kanssa siitä, että kyberrikollisen profilointiin kuuluu neljä peräkkäistä ja toisiinsa sitoutuvaa vaihetta: 1. uhrien tutkinta, 2. rikollisen motivaation tutkinta, 3. rikollisten ominaispiirteiden tunnistaminen ja 4. todistusaineiston tutkinta.

Tuloksien mukaan tyypillinen rikoskokonaisuus on sellainen, jossa henkilö myy huumausaineita internetiä käyttäen, etsii internetistä mahdollisia ostajia, ottaa maksun muuten kuin käteisenä (esimerkiksi kryptovaluuttana), ja antaa erillisen välittäjän viedä huumausaineet paikkaan, jonka GPS-koordinaatit lähetetään ostajalle. (Ovcharenko ym., 2020.)

Mainittuihin rikoksiin syyllistyvien psykologiset piirteet sisältävät tyypillisesti seuraavia: impulsiivisuus, aggressiivisuus, karuus, valehtelu, itsekkyys, vihamielisyys, riskinotto, pelkuruus, taipumus yksinäisyyteen, provokatiivinen käytös, kevytmielisyys, taipumus kontrollointiin, poikkeava käytös ja identiteettikriisi. Henkilöiden tietotekniset taidot ovat keskivertoa paremmalla tasolla.

Tämän tyyppiset kyberrikokset ovat poikkeuksellisia siinä mielessä, että huumausaineet välitetään luonnollisesti reaalielämässä – ei kyberavaruudessa. (Ovcharenko ym., 2020.)

Profiloinnin käyttö apuvälineenä juuri huumausaineiden salakuljetusrikoksissa on ”melko edistyksellistä”, koska rikolliset ovat erilaisten apukeinojen avulla hyvin anonymisoituja, ja koska viiveet rikosten selvittämisessä ovat pitkiä (Ovcharenko ym., 2020).

4.2 Tapaus 2: Pimeä verkko Etelä-Koreassa

Tiedemaailmassa tutkimus pimeän verkon kronologisesta analysoinnista ja perusteellisesta profiloinnista on puutteellista (Lee ym., 2020). Leen ym. (2020) syvällinen tutkimus *Shedding Light on Dark Korea: An In-Depth Analysis Profiling of the Dark Web in Korea* pyrkii vastaamaan tähän puutteeseen analysoimalla 3000:a pimeän verkon sivustoa. Näistä kahdeksan tunnistettiin toimivan Etelä-Korean alueella. Näistä kolme valikoitui tarkempaan profilointiin. Sivustojen nimet ovat HiGH KOREA, Agora ja 666LETOM. Rikolliseen toimintaan viittaava tietoliikenne haettiin aikajaksolta maaliskuu 2017 – elokuu 2018. (Lee ym., 2020.)

Vuorokausitason analysoinnissa havaittiin, että suurin osa huumausaineisiin liittyvästä toiminnasta tapahtui iltapäiväisin aikavälillä 12 – 18. Pornografia-aiheisia hakusanoja käytettiin pääosin öisin. Muu rikollinen toiminta jakautui melko tasaisesti vuorokaudelle. Vuositasolla rikollista aktiivisuutta havaittiin eniten elokuussa, mutta tarkastellun aikajakson lyhyys täytyy ottaa huomioon. (Lee ym., 2020.)

Henkilökohtaisten tietojen vuotojen määrä havaittiin valtavaksi: tarkastelujaksolla tapahtui 893 uniikkia henkilökohtaisten tietojen vuotoa. Tutkijat pystyivät keräämään puhelinnumeroita, sähköpostiosoitteita, Bitcoin-lompakko-osoitteita ja henkilötunnuksia. Tutkijat huomauttavat, että rikollisten on helppo yhdistää näitä pimeän verkon tietoja julkiseen tietoon, jota on saatavilla internetin avoimesta verkosta. Näin rikolliset voivat vähällä vaivalla rakentaa tarkempaa henkilökohtaista tietoa, kuten kokonaisia nimiä, kotiosoitteita ja työpaikkoja. (Lee ym., 2020.)

4.3 Esimerkkitapausten analysointi

Tapaus 1 vaikuttaa sisältävän sekä induktiivista että deduktiivista profilointia. Tapaus perustuu toissijaisiin lähteisiin, koska luotettavan ensisijaisen datan hankkimisen mainitaan olevan haastavaa Ukrainassa. Ongelma ei rajoitu Ukrainaan, vaan on maailmanlaajuinen (Bada & Nurse, 2021). Tapauksessa 1 saatiin luotua profiloinnin avulla kyberrikollisista hyödyllisiä profiileja, joita voinee käyttää tulevien kyberrikosten estämiseksi.

Tapaus 2 näyttää perustuvan deduktiiviseen profilointiin. Koska suora yhteys pimeän verkon rikollisiin on vaikeaa, aloitetaan yleiskuvan keräämisellä, aivan kuten Georgiev'n 2019) suosituksessa. Tapauksessa käytetty data on tutkijoiden hankkimaa ensisijaista dataa. Tapauksessa 2 saatiin kerättyä profiloinnin avulla yllättävän paljon henkilökohtaistakin, jota hyödyntäen viranomaiset voisivat päästä ilmeisesti suhteellisen helposti ainakin joidenkin tiettyjen kyberrikollisten jäljille.

4.4 Tulokset yhdistettynä IGCPF-viitekehykseen

Kuten aiemmin tutkielmassa todettiin, kyberrikollisen profiloinnille ei ole vieläkään standardiksi asti muodostuneita viitekehyksiä tai malleja (Bada & Nurse, 2021; Balogun & Zuva, 2018; Georgiev, 2019; Nykodym ym., 2005). Eräs viimeisimmistä tähän tarkoitukseen kehitetyistä viitekehyksistä on Balogunin ja Zuvan (2018) alustavasti esittämä IGCPF-viitekehys (engl. Integrated Generic Cybercriminal Profiling Framework). Sen neljä päävaihetta ovat:

1. Kerätään:
    - Kyberrikoksen tyyppi
    - Rikospaikan luonto
    - Rikospaikan lainkäyttö
    - Rikospaikan auktorisointi
2. Analysoidaan:
    - Todistusaineiston tyypit
    - Tekotapa
    - Rikoksen tarkoitus
    - Järjestäytyneisyyden taso
3. Raportoidaan:
    - Motivaatio
    - Tarkoitusperä
    - Taidot/kokemus
    - Tunnusmerkit
    - Tekotapa
    - Järjestäytyneisyyden taso
4. Kootaan:
    - Väestötiedot
    - Ammatti
    - Mielenkiinnonkohteet
    - Rikoshistoria
    - Kodin/työpaikan sijanti
    - Persoonallisuus. (Balogun & Zuva, 2018.)

Tähän mennessä tutkielmassa on käsitelty olennaisia asioita kyberrikollisuudesta ja kyberrikollisten profiloinnista. Tutkimuskysymyksenä oli *"Miten*

kyberrikollisten profiloinnilla voidaan selvittää kyberrikoksia?". Taulukossa 2 yhdistetään tämän tutkielman olennaisimmat tulokset IGCPF-viitekehyksen neljään vaiheeseen.

TAULUKKO 2 IGCPF-viitekehys (Balogun & Zuva, 2018) ja tulokset

IGCPF: Kyberrikollisen profiloinnin vaiheet (Balogun & Zuva, 2018)	**Keinoja kyberrikosten selvittämiseksi (tämän tutkielman tuloksia)**
1. Keräämisvaihe	Rajataan potentiaalisten epäiltyjen joukkoa (Donato, 2021; Georgiev, 2019). Paikannetaan rikospaikkaa (Butkovic ym., 2019). Huomioidaan rikospaikan lainsäädännön vaikutukset tutkinnan kulkuun (Casey, 2011). Yleensäkin saadaan vietyä tutkintaa oikeaan suuntaan (Leukfeldt & Holt, 2019).
2. Analysointivaihe	Tutkitaan kyberrikollisen mahdollista järjestäytyneisyyttä (Bada & Nurse, 2021). Tutkitaan epäiltyjen kokonaismäärää (Bada & Nurse, 2021).
3. Raportointivaihe	Määritellään epäillyn tietoteknisiä taitotasoja (Nykodym ym., 2005). Tutkitaan kyberrikoksen motiivia (Edwards ym., 2022). Etsitään kytköksiä epäillyn mahdollisesti suorittamiin muihin kyberrikoksiin (Georgiev, 2019).
4. Kokoamisvaihe	Määritellään epäillyn sukupuoli, siviilisääty, asuinpaikka... (Petherick & Turvey, 2012). Yleensäkin hyödynnetään luotua psykologista profiilia kyberrikollisen löytämisessä (Georgiev, 2019).

5 YHTEENVETO

Kyberrikollisuus on valtava kuluerä jo pelkästään rahallisesti – puhumattakaan muista vahingoista. Yksi keino kyberrikollisuuden selvittämiseen on profilointi. Vaikka profiloinnin suorittajat ovat useimmiten viranomaisia, tarvitaan onnistuneeseen profilointiin ja laajemminkin kyberrikollisuuden torjuntaan kaikkia: yrityksiä, valtioita, tutkijoita ja yksityisiä henkilöitä. Profiloinnista on yllättävän vähän joko Suomessa tehtyjä tai suomenkielisiä tutkimuksia. Siten tämän kirjallisuuskatsauksen tavoitteena oli luoda suomenkielinen yleiskuva kyberrikollisen profiloinnista. Lähteitä etsittiin ensisijaisesti JYKDOK-, Google Scholar -, IEEE Xplore – ja Scopus-tietokannoista. Hakusanoina käytettiin englanninkielisiä termejä ”cybercriminal”, ”cybercrime” sekä ”profiling” ja niiden yhdistelmiä. Lähteinä käytettiin mahdollisuuksien mukaan laadukkaita, ajankohtaisia tieteellisiä artikkeleita. Tavoite oli etsiä ja löytää vastauksia tutkimuskysymykseen:

> ”Miten kyberrikollisten profiloinnilla voidaan selvittää kyberrikoksia?”

Löydettyjen tulosten mukaan kyberrikollisen profilointi auttaa erityisesti rajaamaan rikoksen potentiaalisten epäiltyjen määrää ja siten ohjaamaan rikostutkintaa oikeaan suuntaan. Lisäksi profilointi mahdollistaa yksityiskohtaisen psykologisen profiilin luomisen epäillystä. Profiili voi sisältää tietoa esimerkiksi epäillyn persoonallisuuden piirteistä, maantieteellisestä olinpaikasta tai mahdollisista kytköksistä muihin rikollisiin. Tutkielman lopussa yhdistettiin löydetyt tulokset IGCPF-viitekehykseen – nämä vaikuttivat sopivan hyvin yhteen.

Tämä tutkimus on monelta osin rajoittunut. Tällaisenaan aiheesta löytyy niin paljon materiaalia, että sen suodattaminen ja priorisointi on haastavaa. Siksi monen asian käsittely on jäänyt vähäiseksi, esimerkiksi profilointiprosessin tarkempi kulku. Aihe kannattaisi mahdollisesti rajata kapeammaksi. Kapeampi aihe voisi helpottaa myös nykyistä systemaattisempaa lähteiden etsimistä ja hyödyntämistä. Toisaalta tutkielman tavoite olikin yleiskuvan rakentaminen.

Jatkotutkimusaiheina olisi hyödyllistä etsiä keinoja, joilla voitaisiin edistää yritysten ja viranomaisten yhteistyötä kyberrikollisen profiloinnissa. Profiloinnista yleensäkin olisi mielenkiintoista saada enemmän Suomeen keskittyvää tutkimusta niin, että siinä otettaisiin huomioon Suomen lainsäädäntö ja muut olosuhteet.

LÄHTEET

Andress, J. & Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier.

Bada, M. & Nurse, J. R. C. (2021). Profiling the Cybercriminal: A Systematic Review of Research. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–8. https://doi.org/10.1109/CyberSA52016.2021.9478246

Balogun, A. M. & Zuva, T. (2018). Criminal Profiling in Digital Forensics: Assumptions, Challenges and Probable Solution. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 1–7. https://doi.org/10.1109/ICONIC.2018.8601268

Butkovic, A., Mrdovic, S., Uludag, S. & Tanovic, A. (2019). Geographic profiling for serial cybercrime investigation. *Digital Investigation*, *28*, 176–182. https://doi.org/10.1016/j.diin.2018.12.001

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd p.). Academic Press, Inc.

Clough, J. (2010). Principles of Cybercrime. *Principles of Cybercrime*, 1–449. https://doi.org/10.1017/CBO9780511845123

Clough, J. (2015). *Principles of Cybercrime* (2. painos). Cambridge University Press. https://doi.org/10.1017/CBO9781139540803

Custers, B. (2021). Profiling and Predictions: Challenges in Cybercrime Research Datafication. Teoksessa A. Lavorgna & T. J. Holt (toim.), *Researching Cybercrimes* (s. 63–79). Springer International Publishing. https://doi.org/10.1007/978-3-030-74837-1_4

Donalds, C. & Osei-Bryson, K.-M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403–418. https://doi.org/10.1016/j.chb.2018.11.039

Donato, L. M. (2021). *Computer criminal profiling applied to digital investigations*. https://hdl.handle.net/2086/21604

Edwards, G. (2019). *Cybercrime Investigators Handbook*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=5896937

Edwards, M., Williams, E., Peersman, C. & Rashid, A. (2022). *Characterising Cybercriminals: A Review* (arXiv:2202.07419). arXiv. http://arxiv.org/abs/2202.07419

Euroopan komissio. (ei pvm.). *Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace.* Noudettu 18. marraskuuta 2022, osoitteesta https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en

Finklea, K. (2015). Dark Web. *Dark Web*, 18.

Georgiev, V. (2019). Profiling Human Roles in Cybercrime. *Information & Security: An International Journal*, *43*(2), 145–160. https://doi.org/10.11610/isij.4313

Giansanti, D. (2021). Cybersecurity and the Digital-Health : The Challenge of This Millennium. *Healthcare (Basel)*, *9*(1), 62-. https://doi.org/10.3390/healthcare9010062

Greco, F. & Greco, G. (2020). Investigative techniques in the digital age: cybercrime and criminal profiling. *European Journal of Social Sciences Studies*, *5*(3), Article 3. https://doi.org/10.46827/ejsss.v5i3.821

Kaspersky. (2021). *DDoS Breach Costs Rise to over $2M for Enterprises finds Kaspersky Lab Report*. https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report

Kemp, S. (ei pvm.). *Digital 2021: Global Overview Report*. DataReportal – Global Digital Insights. Noudettu 27. marraskuuta 2022, osoitteesta https://datareportal.com/reports/digital-2021-global-overview-report

Kipane, A. (2019). Meaning of profiling of cybercriminals in the security context. *SHS Web of Conferences*, *68*, 01009. https://doi.org/10.1051/shsconf/20196801009

Lee, J., Hong, Y., Kwon, H. & Hur, J. (2020). Shedding Light on Dark Korea: An In-Depth Analysis and Profiling of the Dark Web in Korea. Teoksessa I. You (toim.), *Information Security Applications* (s. 357–369). Springer International Publishing. https://doi.org/10.1007/978-3-030-39303-8_27

Leukfeldt, E. R. & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, *126*, 106979. https://doi.org/10.1016/j.chb.2021.106979

Leukfeldt, R. & Holt, T. J. (2019). *The Human Factor of Cybercrime*. Routledge.

Mandiant. (2020). *Top Trends in Cyber Security | Cyber Attacks Trends | M-Trends*. https://www.mandiant.com/m-trends

Meland, P. H., Tondel, I. A. & Solhaug, B. (2015). Mitigating Risk with Cyberinsurance. *IEEE Security & Privacy*, *13*(6), 38–43. https://doi.org/10.1109/MSP.2015.137

Nazah, S., Huda, S., Abawajy, J. & Hassan, M. M. (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. *IEEE Access*, *8*, 171796–171819. https://doi.org/10.1109/ACCESS.2020.3024198

Nykodym, N., Taylor, R. & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Computer Law & Security Review*, *21*(5), 408–414. https://doi.org/10.1016/j.clsr.2005.07.001

O'Kane, P., Sezer, S. & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*, 321–327. https://doi.org/10.1049/iet-net.2017.0207

Ovcharenko, M. O., Tavolzhanskyi, O. V., Radchenko, T. M., Kulyk, K. D. & Smetanina, N. V. (2020). Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method. *Journal of Advanced Research in Law and Economics*, *11*(4(50)), 1296–1304. https://doi.org/10.14505/jarle.v11.4(50).26

Petherick, W. A. & Turvey, B. E. (2012). Alternative Methods of Criminal Profiling. Teoksessa B. E. Turvey (toim.), *Criminal Profiling* (s. 67–99). Elsevier. https://doi.org/10.1016/B978-0-12-385243-4.00003-4

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S. & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Quinkert, F., Lauinger, T., Robertson, W., Kirda, E. & Holz, T. (2019). It's Not what It Looks Like: Measuring Attacks and Defensive Registrations of Homograph Domains. *2019 IEEE Conference on Communications and Network Security (CNS)*, 259–267. https://doi.org/10.1109/CNS.2019.8802671

Sammes, T. & Jenkinson, B. (2007). *Forensic Computing*. https://doi.org/10.1007/978-1-84628-732-9_1

Sarwar, T. B. (2016). *Analyzing the Challenges of Cybercrime in the Global Context: Need for A Cross–Border Response*. 13.

Smith, K. T., Jones, A., Johnson, L. & Smith, L. M. (2018). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, *17*(1), 42–60. https://doi.org/10.1108/JICES-02-2018-0010

Smith, K. T., Smith, L. M. & Smith, J. L. (2011). Case Studies of Cybercrime and Their Impact on Marketing Activity and Shareholder Value. *Academy of Marketing Studies Journal*, *15*(2), 67–81.

Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O. & Kozych, I. V. (2021). Combating Cybercrime: Economic and Legal Aspects. *WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS*, *18*, 751–762. https://doi.org/10.37394/23207.2021.18.72

Thackray, H., Mcalaney, J., Dogan, H., Taylor, J. & Richardson, C. (1.7.2016). *Social Psychology: An under-used tool in Cybersecurity*. https://doi.org/10.14236/ewic/HCI2016.64

Turvallisuuskomitea. (2018). *Kyberturvallisuuden sanasto – Turvallisuuskomitea*. https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Turvey, B. E. (2012). Chapter 17 - Inferring Offender Characteristics. Teoksessa B. E. Turvey (toim.), *Criminal Profiling (Fourth Edition)* (s. 403–446). Academic Press. https://doi.org/10.1016/B978-0-12-385243-4.00017-4

Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective*, *23*(4–6), 172–178. https://doi.org/10.1080/19393555.2014.931491

Yar, M. & Steinmetz, K. (2019). *Cybercrime and Society*. SAGE Publications Ltd. https://uk.sagepub.com/en-gb/eur/cybercrime-and-society/book260644