Niklas Viitanen

KYBERRIKOSTUTKINTAAN VAIKUTTAVAT TIETOJÄRJESTELMIEN OMINAISUUDET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Viitanen, Niklas
Kyberrikostutkintaan vaikuttavat tietojärjestelmien ominaisuudet
Jyväskylä: Jyväskylän yliopisto, 2020, 42 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Halttunen, Veikko

Tässä kirjallisuuskatsauksessa käsitellään kyberrikollisuutta ja kyberrikosten tutkimista. Kyberrikollisuus on kasvava uhka yhteiskunnassa ja siksi kyberrikollisuuden ja kyberrikostutkinnan tarkastelu onkin tärkeää. Kyberavaruudessa on paljon erilaisia tapoja tehdä suorasti tai epäsuorasti rikoksia. Erilaiset haittaohjelmat ovat yksi yleisimmistä arjessa kohdattavista kyberuhista, mutta kyberrikoksissa käytetään myös monia muita välineitä ja tapoja, joita esimerkiksi hakkerit hyödyntävät. Yksi kyberrikostutkinnan tehtävistä on selvittää rikoksen tekijä, ja siksi tässä tutkielmassa keskitytään tarkastelemaan, ketkä tekevät kyberrikoksia ja mihin tarkoituksiin. Lisäksi tutkielmassa avataan hakkerien motiiveja. Yksi merkittävistä havainnoista kirjallisuuskatsauksessa on kyberrikollisuuden luokittelu, jossa esitettiin tarkemmat kategoriat kuin yksinkertaisemmassa kaksijakoisessa jaottelussa. Kyberrikollisuus on muodostunut suhteellisen isoksi liiketoiminnaksi, ja sen aiheuttamat vahingot ovat nousseet merkittävästi viime vuosina. Vaikka kyberrikollisuutta esiintyy maailmanlaajuisesti, silti esimerkiksi mantereiden välisiä eroja löytyy, joiden syitä kirjallisuuskatsaus tarkastelee. Kirjallisuuskatsauksessa kyberrikostutkintaa lähestytään enemmän kyberrikostutkinnan suorittamisen näkökulmasta ja pyritään avaamaan kyberrikostutkinnan prosessia. Prosessimalleja on kehitetty aktiivisesti vuosituhannen alusta, mutta mikään tarkastelluista malleista ei ole vielä noussut ylitse muiden. Prosessimallien tarkastelussa näkyy selkeästi läpileikkaus erilaisista tarpeista ja aikakausista, joiden pohjalta mallit ovat muodostettu. Tietojärjestelmien suunnittelu- ja toteutusvaiheessa kuuluisi ottaa huomioon kyberrikostutkintaan kuuluvia ominaisuksia, joilla voidaan edesauttaa kyberrikostutkinnan eri vaiheita. Käytännön toteutukset eivät kuitenkaan ole niin yksinkertaisesti toteutettavissa ja erilaisilla kyberrikostutkintaa hyödyttävillä ratkaisuilla on myös omat haasteensa. Lisäksi kyberrikolliset pystyvät kehittämään vastatoimia kyberrikostutkintaa hyödyttäville ominaisuuksille, mikä aiheuttaa kehittämisen näkökulmasta ongelmia.

Asiasanat: tietojärjestelmät, kyberrikollisuus, kyberrikostutkinta, digitaalinen tutkinta

ABSTRACT

Viitanen, Niklas
Properties of information systems affecting cybercrime investigation
Jyväskylä: University of Jyväskylä, 2020, 42 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Halttunen, Veikko

This bachelor's thesis addresses cybercrime and cyber forensics. Cybercrime is a growing threat to society and that is why it is important to look at cybercrime and cybercrime investigation. In cyberspace, there are many ways to commit crimes, either directly or indirectly. Various types of malware are one of the most common cyber threats in everyday life, but cybercrime also takes advantage of many other tools and methods that are exploited by hackers, for example. One of the objectives of a cybercrime investigation is to find out the perpetrator of the crime. Therefore, this study inspects who commits cybercrimes, for what purposes, and explains some of the motives of hackers. A significant finding in the literature review was the categorization of cybercrimes, which presented more specific categories for cybercrime than the easier two-part classification. Cybercrime has become a relatively large business and the damage it causes has increased significantly in recent years. All in all, cybercrime is a global threat. For example, there are differences between continents, the causes of which are examined in this thesis. The study takes a more cybercrime investigation approach from the perspective of conducting a cybercrime investigation and seeks to examine the cybercrime investigation process. Process models have been actively developed since the turn of the millennium, but none of the models examined have yet risen above the others. An examination of process models clearly shows a cross-section of the different needs and eras on the basis of which the models are formed. The design and implementation of information systems should consider the execution of cybercrime investigation and what factors can contribute to it being more effective. However, practical implementations are not so simple to implement and various solutions that benefit cybercrime investigation also have their own challenges. In addition, cybercriminals are able to develop countermeasures to features that benefit cybercrime investigation, which poses problems from a development perspective.

Keywords: information systems, cybercrime, cybercrime investigation, digital forensics

KUVIOT

SISÄLLYS

1 JOHDANTO

Kyber- ja tietoturvallisuuden merkitys on kasvanut tällä vuosituhannella digitalisaation myötä. Erilaisten kyberhyökkäyksien uhat näkyvät jokapäiväisessä elämässä erilaisina kyberturvallisuuteen liittyvinä toimina, kuten salasanan vaihtokehotuksina ja älylaitteiden automaattipäivityksinä. Kyberrikollisuudesta aiheutuvien kustannusten on arvioitu nousevan vuoteen 2021 mennessä 6 biljoonaan dollariin (Morgan, 2017). Kyberrikollisuuden yleistyminen rikosmuotona on vaikuttanut luonnollisesti myös viranomaisten tehtäviin. Kyberrikollisuuden torjunnan parissa työskenteleminen onkin yleistynyt poliisien tehtävissä huomattavasti. Kyberrikostutkinnan perimmäisenä tarkoituksena voidaan pitää pyrkimystä vähentää kyberrikollisuutta. Ottaen huomioon kyberrikosten toteutuessa aiheutuvat korkeat kustannukset, on kyberrikoksia, mutta myös niiden tutkintaa, tärkeää tarkastella talouden kannalta (Hyman, 2013). Tietojärjestelmien rooli kyberrikoksissa on ilmeisen selvä niiden ollessa ainakin osaksi alustana kyberrikollisuudelle ja sen kohteille. Tämän takia on tärkeää, ettei kyberrikoksen tutkintaa jätetä tietojärjestelmissä huomiotta, ja ajatella kyberrikostutkinnan tekevän tehtävänsä järjestelmän ominaisuuksista huolimatta. Yhä enemmän tietojärjestelmissä täytyisi integroida mahdollisuuksia kyberrikostutkinnalle, mikä auttaa pitkällä aikavälillä niin järjestelmän käyttäjiä kuin lyhyellä aikavälillä kyberrikoksen tutkijoita. (Park, Cho & Kwon, 2009.) Yhä useammin nykyään tietojärjestelmien kehityksessä pyritään saamaan järjestelmä nopeasti käyttöön, mikä johtaa helposti siihen, että kyberrikostutkintaa helpottavat ominaisuudet kärsivät.

Tämä kandidaatintutkielma suoritetaan kirjallisuuskatsauksena. Kirjallisuuskatsauksen tarkoituksena on selvittää kyberrikosten ja kyberrikostutkinnan nykytilaa, sekä tarkastella kyberrikostutkinnan prosessia tietojärjestelmien näkökulmasta. Tutkielman tutkimuskysymykset ovat:

- Millainen on kyberrikosten tutkinnan prosessi?
- Mitkä tekijät tietojärjestelmissä vaikuttavat kyberrikostutkintaan?

Tutkielmassa on käytetty paljon englanninkielistä termistöä, sillä kaikille kyberturvallisuuteen, kyberrikollisuuteen tai kyberrikostutkintaan liittyvillä sanoilla tai malleilla ei ole virallisia suomenkielisiä vastineita tai suomennosten tarkoitus ei vastaa tutkielman tarpeita. Englanninkielistä käsitteistöä pyritään tutkielmassa suomentamaan tai selittämään auki.

Tutkielman rakenne etenee kyberrikollisuudesta kyberrikostutkintaan, jonka jälkeen käsitellään kyberrikostutkintaa tietojärjestelmien näkökulmasta. Toisessa luvussa aluksi määritellään kyberrikollisuuteen liittyviä käsitteitä, josta edetään erilaisiin kyberrikollisuuden muotoihin ja esitellään mallikyberrikollisuuden kategorisointiin. Toisen luvun lopussa käsitellään kyberrikosten yleisyyttä ja aiheuttamia vahinkoja. Kolmannessa luvussa tarkastellaan kyberrikostutkintaa. Luvun alussa määritellään kyberrikostutkintaa, jonka jälkeen käsitellään erilaisia kyberrikostutkinnan prosessimalleja ja vertaillaan niitä. Neljännessä luvussa käydään läpi, mitkä ominaisuudet vaikuttavat tietojärjestelmissä kyberrikostutkintaan. Lopuksi neljännessä luvussa käsitellään, mitä haasteita ratkaisuista huolimatta tietojärjestelmien kyberrikostutkinnassa kohdataan.

Lähteiden hankintaa käytin pääasiassa Googlen Scholar -hakukonetta, Jyväskylän yliopiston kirjastopalveluita ja IEEE:n hakupalveluita. Esimerkiksi hakukriteereillä ”digital forensics” OR ”cyber forensics” vuosilta 1970–2021, löytyi Google Scholarista noin 90000 osumaa. Vastaavasti samoilla hakusanoilla IEEE:n hakukone antoi noin 4221 osumaa. Jyväskylän yliopiston JYKDOK-palvelu antoi vastaavilla hakusanoilla osumiksi noin 170 kirjaa. Aineistoa ei ole siis valtavaa määrää, koska kyberrikollisuutta ja kyberrikostutkintaa koskevaa tieteellistä tutkimusta ei ole tehty vielä pitkään. Lisäksi tutkielmassa pyritään välttämään lakiteksteihin viittaamista paitsi, jos halutaan nostaa esille eri lainsäädäntöjen näkemyksiä asiasta. Lähteinä kirjallisuuskatsauksessa on käytetty relevantteja kirjoja, julkaisuja ja konferenssipapereita. Lisäksi ei-tieteellisiä julkaisuja on käytetty muun muassa esimerkkitapausten, kansainvälisten tilanneraporttien ja tilastojen esittelystä. Julkaisufoorumin mukaan lähteistä eniten oli toista eli johtavaa tasoa. Toiseksi eniten oli kolmannen tason eli korkeimman tason lähteitä. Käytettyjä lähteitä on yhteensä 79.

2 KYBERRIKOLLISUUS

Tässä luvussa käydään läpi kyberrikollisuuden eri osa-alueita ja taustoja. Ensimmäisenä kohdassa 2.1 määritellään kyberrikollisuuteen liittyviä tärkeimpiä käsitteitä, taustoja ja historiaa. Kohta 2.2 käsittelee kyberrikollisuuden erilaisia muotoja ja niiden eroja. Alaluvussa 2.3 käsitellään kyberrikollisuuden yleisyyttä, sekä millaista vahinkoa kyberrikokset voivat aiheuttaa. Nämä aihealueet luovat pohjaa tutkimuksen seuraaville luvuille ja antavat käsityksen tutkimuksen alueesta.

2.1 Käsitteiden määrittely ja historia

Kyberturvallisuus ja kyberrikollisuus kehittyvät jatkuvasti. On siis luonnollista, että kyberturvallisuuteen liittyviä uusia käsitteitä syntyy koko ajan lisää. Lisäksi jo olemassa olevat käsitteet saattavat muotoutua uudelleen. Kyberturvallisuuden jatkuvan muutoksen takia kaikkia tämänhetkisiä käsitteitäkään ei pystytä yksiselitteisesti määrittelemään, mikä luo haasteita aiheen tutkimiselle. Seuraavaksi käydään läpi tällä hetkellä tärkeimpiä kyberturvallisuuden käsitteitä. Seuraavat alaluvut tulevat mahdollistamaan tutkimukseni kannalta relevantin ymmärryksen kyberturvallisuuden tämän hetken keskeisistä käsitteistä

Kyberrikollisuus toteutetaan kyberavaruuden kautta ja monet kyberrikokset tapahtuvat pääosin siellä. Tästä syystä on tärkeää määritellä kyberavaruus. **Kyberavaruus** termiä käytti ensimmäisenä William Gibson vuonna 1982 (Fourkas, 2004). Hän tarkoitti termillä tietokoneen luomaa virtuaalista todellisuutta, joka oli vielä kaukana siitä, mitä kyberavaruudella nykyään tarkoitetaan. Vuonna 2009 Yhdysvaltojen puolustusministeriö jakoi kyberavaruuden kolmeen tasoon: fyysiseen, syntaktiseen sekä semanttiseen tasoon. Fyysinen taso tarkoittaa kaikkia fyysisen maailman rakenteita, kuten tietokoneita, mastoja ja palvelimia. Syntaktinen taso kattaa esimerkiksi ohjausjärjestelmät, verkkoprotokollat sekä vastaavat hallintajärjestelmät. (Libicki, 2009.) Semanttiseen tasoon kuuluu käyttäjien informaatio, ohjelmistot sekä toimintojen ohjaus.

Ensimmäisiä luotuja mallinnuksia kyberavaruudesta oli malli, johon kuuluu seitsemän tasoa. Sen pohjalta soveltaen on esitetty viisitasoinen malli, joka

toimii sopivana välimuotona tämän katsauksen tarpeisiin. (Libicki, 2009.) Kyseisessä viisitasoisessa mallissa on lisättynä vielä kaksi päällimmäistä kerrosta: palvelukerros ja kognitiivinen kerros. Palvelukerros sisältää erilaiset julkiset ja kaupalliset palvelut. Kognitiivinen kerros muodostuu käyttäjän tilannekuvasta ja ymmärryksestä. (Libicki, 2009.) Nämä tasot toimivat käsitteen määrittelyssä, mutta tasojen painotus ja merkitys saattaa muuttua riippuen tulkitsijasta. Esimerkiksi tietotekniikan tutkijat saattavat antaa enemmän painoarvoa synteettiselle tasolle omassa tulkinnassaan. (Van Puyvelde & Brantly, 2019.) Kyberavaruus tämän tutkimuksen kontekstissa määritellään fyysiseksi ja virtuaaliseksi tilaksi, jonka eri kerrokset ovat vuorovaikutuksessa toistensa kanssa, täten muodostaen kyberavaruuden. Tässä kyberavaruudessa pystytään liikuttamaan dataa, ja avaruuteen voidaan päästä käsiksi eri tasoilta (Folsom, 2007).

Kyberrikollisuus eroaa kyberhyökkäyksestä, jonka määritelmä esitetään myöhemmin, koska rikollisuus perustuu pääosin lakiin ja siten sen termi on helpommin määriteltävissä, mutta määritelmien välisiä eroja silti ilmenee. Kierkegaard (2005) määrittelee kyberrikollisuuden laajasti rikokseksi, joka on mahdollistettu tietokoneteknologian avulla. Kyberrikollisuuden voi karkeasti jakaa kahteen kategoriaan: perinteiset rikokset, joita voidaan tehdä tietokoneita hyväksi käyttäen, ja uudenkaltaisiin rikoksiin. Perinteisillä rikoksilla tarkoitetaan tässä kontekstissa rikoksia, jotka olivat olemassa jo ennen kyberrikollisuutta. Näitä rikoksia ovat esimerkiksi uhkailu, petos, kiristys ja immateriaalioikeuksien varastaminen (Khadam, 2012). Uudenkaltaisilla rikoksilla tarkoitetaan tässä kontekstissa rikoksia, joissa tekijä käyttää tietokonetta suoraan rikoksen tekemiseen. Näihin rikoksiin kuuluu hakkerointi, virusten levittäminen ja palvelunestohyökkäykset. Kyberrikollisuus ei siis käsitä vain tietynlaisia rikoksia vaan sisältää moniulotteisesti rikoksia, joita voidaan suorittaa suoraan tietokoneella tai epäsuorasti sen välityksellä. Tämä on yksi suurimpia haasteita kyberrikollisuuden käsitteelle. Skaalan suuruuden takia pitäisi pyrkiä pitämään johdonmukaisuus rikosten lainsäädännössä ja valvonnassa, jotka tapahtuvat internetissä ja internetin ulkopuolella (Clough 2011).

Kyberrikollisuus ja **kyberhyökkäys** täytyy erottaa toisistaan, koska tämä tutkielma rajautuu vain kyberrikollisuuteen. Vaikka ne ovat osittain päällekkäisiä käsitteitä, löytyy niistä eroavaisuuksia. Kyberhyökkäyksen käsitteellisessä määrityksessä esiintyy eriäväisyyksiä eri lähteissä, joten sen määritelmä ei ole vielä täysin vakiintunut. Clarke ja Knake (2014) määrittelevät kybersodan tahallisiksi kyberhyökkäyksiksi toista valtiota vastaan, joiden tarkoituksena on aiheuttaa vahinkoa tai häiriötä. Tämä määritelmä ei kuitenkaan erota käsitteitä, kuten kyberrikollisuus, kyberhyökkäys, kybertiedustelu tai kybersota. Tämä määritelmä on lisäksi liian kapea, koska se käsittelee vain valtiollisia toimijoita, ja siten ei kata kaikkia muita mahdollisia toimijoita, kuten muut poliittiset toimijat. (Hathaway ym., 2012.) Kyberhyökkäyksessä pyritään tietoverkkojen kautta aiheuttamaan vahinkoa kohteelle tai varastamaan kohteen tietoja. Hathawayn ym. (2012) mukaan kyberhyökkäyksen motiivit sisältävät kyberrikollisuuden, mutta myös sen lisäksi juuri poliittiset tai kansalliset motiivit, mikä erottaa sen normaaleista kyberrikoksista. Shabut, Lwin ja Hossain (2016) esittävät yhden

tärkeimmistä kyberhyökkäysten kanavista olevan ihmisiin kohdistuvat hyökkäystavat, joka on myös totta kyberrikollisuuden kohdalla.

Kyberrikollisuudessa yksi keskeisistä käsitteistä on dark web eli **pimeä verkko**. Pimeän verkon tarkoituksena on mahdollistaa internetin anonyymi käyttö, josta seuraa luonnollisesti myös ongelmia mahdolliseen viranomaisten valvontaan. Tor-verkko on yksi yleisimmistä palveluista pimeän verkon selaamiseen. Tor on lyhenne sanoista The Onion Router, joilla viitataan palvelun sipulinkerrosmaisiin salattuihin kerroksiin. Yhdistäessä internettiin palvelu välittää pyynnön satunnaiseen Tor-verkon koneeseen, joka taas lähettää sen eteenpäin rajatulla määrällä tietoa. (Li, Edin, Gunes, Bebis & Shipley, 2013.) Yhteyspisteet eivät pysty näkemään kaikkea informaatiota, joka kulkee niiden kautta, joten käyttäjää on vaikea, muttei mahdotonta jäljittää (McCoy, Bauer, Grunwald, Kohno & Sicker, 2008). Tor-verkko toimii kyberavaruudessa suosittuna alustana laittomien tuotteiden ja palveluiden kaupankäynnissä sen anonyymiyden takia. Esimerkiksi asekauppaa käydään Tor-verkossa paljon. Yksi tunnettu tapaus, johon liitettiin Tor-verkosta ostettuja aseita, oli Münchenin ampumavälikohtaukset vuonna 2016. (Vice, 2017.)

2.2 Erilaiset kyberrikokset

Eri kyberrikoksilla on erilaiset määritelmät riippuen lainsäädännöstä ja pienetkin tekijät vaikuttavat siihen mikä lasketaan kyberrikokseksi ja mikä ei. Tästä syystä tutkimuksessa on pyritty välttämään suoraan lakiteksteihin viittaamista ja käsitellään yleisellä tasolla konsepteja kyseisistä rikoksista. Kuten aiemmin todettiin, yksi tapa osittaa kyberrikollisuus on karkeasti jakaa se kahteen osa-alueeseen: perinteisiin rikoksiin ja uudenkaltaisiin rikoksiin, jotka tietokoneet ja tietoverkot ovat mahdollistaneet. Tämä on vain helppo esimerkki, miten kyberrikollisuutta voi mallintaa. Seuraavaksi esitetään erilaisia kyberrikollisuuden muotoja, kyberrikosten tekijöitä ja erilaisia tapoja kategorisoida kyberrikoksia.

Hakkerit liitetään usein kyberrikollisuuden tekijöiksi, vaikka tämä ei pidä todellisuudessa paikkaansa. Yksi tapa esittää hakkerit on omistautuneiksi ohjelmoijiksi, jotka haluavat nähdä kuinka pitkälle tietokoneiden suorituksia voi viedä. Hakkerit voidaan jakaa tarkoitusperiensä mukaan eri osiin. Tämän tutkielman tarkoituksiin jaetaan käsite neljään alakäsitteeseen:

- ”Black-hat” -hakkerit eli pahantahtoiset hakkerit
- ”White-hat” -hakkerit eli hyväntahtoiset hakkerit
- Haktivistit eli verkkoaktivistit
- Kyberterroristit

Pahantahtoisilla hakkereilla tarkoitetaan verkkorikollisia, jotka haluavat aiheuttaa vahinkoa tai ansaita rahaa rikollisuudellaan. Hyväntahtoiset hakkerit taas

toimivat mahdollisesti konsultteina tai muuten työskentelevät tietoturva-asiantuntijoina. Valkohattuhakkerit pyrkivät esimerkiksi etsimään heikkouksia yritysten tietoturvajärjestelmistä ja raportoimaan ne heille. (Xu, Hu & Zhang, 2013.) Verkkoaktivistit toimivat pääosin poliittisten motiivien takia. He haluavat nostaa sitä kautta tietoisuutta asioista, joita pyrkivät ajamaan. Kyberterroristeilla tarkoitetaan hakkereita, ketkä yrittävät toimillaan herättää pelkoa ja luoda kaaosta ihmisissä. (Staff, 2013.)

Kyberrikollisuuden yksi yleisimmistä muodoista on immateriaalioikeuksia koskevat rikokset. Tästä yleisenä esimerkkinä tekijänoikeusrikokset. Tekijänoikeus annetaan teoksen tuottajalle, jolloin tekijällä on määritellyn ajan monopoli omaan teokseensa (Clough, 2015). Tänä aikana, jos joku muu kuin oikeuden haltijan tai haltijan luvalla toimiva käyttää tekijänoikeuksiin liittyviä oikeuksia, on kyseessä tekijänoikeusrikos. Vertaisverkoissa (P2P), eli verkoissa, joissa osalliset toimivat niin palvelimina kuin lataajina (Löser, Wolpers, Siberski & Nejd, 2003), jaetaan paljon tekijänoikeudella suojattua materiaalia. Vertaisverkoissa käyttäjät jakavat toisilleen esimerkiksi musiikkia, elokuvia ja ohjelmistoja ilmaiseksi. Yksi kuuluisimmista tapauksista on Napsterin vuosituhannen vaihteesta. Napster oli vertaisverkko-ohjelma, jossa pystyi jakamaan tiedostoja vapaasti. Tätä käytettiin pääosin musiikin jakamiseen laittomasti, jonka seurauksena monet artistit haastoivat Napsterin oikeuteen ja palvelu suljettiin nopeasti sen jälkeen (Ku, 2002).

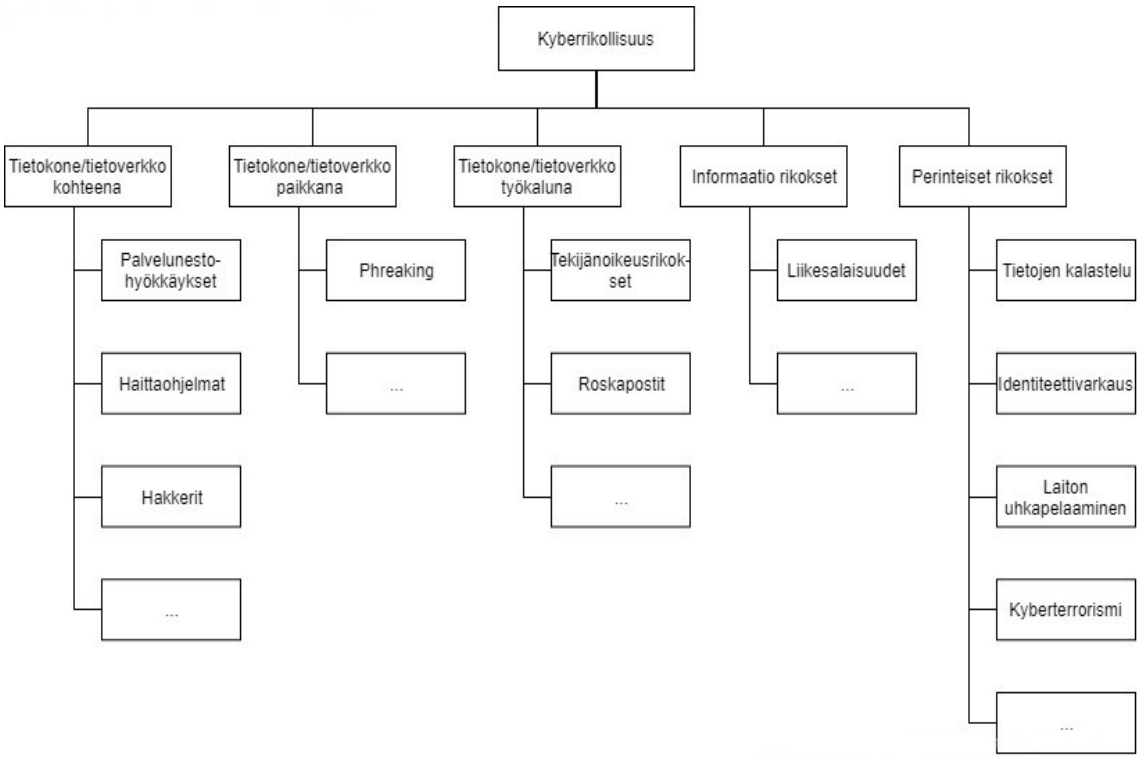
Palvelunestohyökkäykset ovat tunnettuja julkisuudessa niiden haittavaikutusten takia. Palvelunestohyökkäysten päätavoite on ylikuormittaa hyökkäyksen kohde valtavalla määrällä liikennettä, joka johtaa loppujen lopuksi verkon kaatumiseen tai huomattavaan hidastumiseen (Phan, & Park, 2019). Yksi yleinen tapa on lähettää yhdistyspyyntöjä palvelimella niin paljon, ettei oikeille käyttäjille riitä tarpeeksi kapasiteettia. Motiiveja palvelunestohyökkäyksille voi olla useita. Esimerkiksi haktivistit ovat useasti käyttäneet palvelunestohyökkäyksiä omien motiiviensa takia. Lamauttamalla julkisia palveluja voidaan pyrkiä luomaan sekaannusta ja tyytymättömyyttä niiden käyttäjiin (Sarga & Jasek, 2011). Hyökkääjät voivat myös käyttää palvelunestohyökkäystä pystyäkseen kiristämään kohdetta tai aiheuttamaan järjestelmän uudelleenkäynnistyksen, joka saattaa antaa hakkereille tien sisään järjestelmään. Vuoden 2020 alussa Amazon Web Services torjui ennätyssuuren palvelunestohyökkäyksen, jonka liikennemäärä oli parhaillaan 2,3 terabittiä sekunnissa. Edellisen ennätyksen liikennemäärä oli noin 1,7 terabittiä sekunnissa. (The Verge, 2020.)

Haittaohjelma on käsite, joka kattaa yleisesti ohjelmat, joilla pyritään aiheuttamaan vahinkoa yksittäiseen tietokoneeseen, palvelimeen tai verkkoon (Moir, 2009). Haittaohjelmiksi luetaan esimerkiksi seuraavat: virukset, madot, troijalaiset, vakoiluohjelmat ja rootkitit. Yksi yleisimpiä haittaohjelman muotoja ovat kiristyshaittaohjelmat. Kiristyshaittaohjelma lukitsee tietokoneen tai pääsyn sen tiedostoihin ja vaatii niiden avaamisesta lunnaita. Virus on haittaohjelma, jonka tunnusomaisena piirteenä on sen uusiutuminen. Se pyrkii monistumaan ja sen takia siitä on todella vaikea päästä eroon. Viruksesta hyvä esimerkki on WannaCry -virus, josta kerrotaan enemmän luvussa 2.3. Mato on itsestään lisääntyvä haittaohjelma, joka pyrkii leviämään verkossa ja hyödyntämään heikkoja kohtia

tietoturvassa. Troijalaiset saattavat usein vaikuttaa aivan normaaleilta ohjelmilta, mutta niissä on sisäänrakennettuna takaovi. Takaovea hyödyntäen hakkeri pääsee käsiksi tietokoneeseen käyttäjän tietämättä. Vakoiluohjelmistoilla pyritään seuraamaan huomaamatta käyttäjän toimintoja ja lähettämään dataa niistä kolmannelle osapuolelle. Vakoiluohjelmat pyrkivät nauhoittamaan esimerkiksi näppäimistön painalluksia. Rootkit on paketti, jolla hakkeri voi syöttää komentoja tai varastaa tietoja tietokoneelta omistajan tietämättä. (Primiero, Solheim, & Spring, 2019.) Haittaohjelmien ja niiden vastatoimien kehitys on pitkää kädenvääntöä valkohattuhakkerien ja mustahattuhakkerien välillä (Kramer & Bradfield, 2010).

Yrityksiin kohdistuu monenlaisia kyberhyökkäyksiä ja yksi yleisimmistä kohteista yrityksiin kohdistuvassa rikollisuudessa ovat liikesalaisuudet. Liikesalaisuuksien varastaminen on yleistynyt internetin myötä ja voi aiheuttaa paljon vahinkoa kohteena olevalle yritykselle. Liikesalaisuuksilla pyritään luomaan etua kilpailijoihin nähden ja siksi niitä pyritään pitämään salaisina. Samasta syystä kilpailijat tai alalle havittelevat voivat haluta päästä käsiksi näihin salaisuuksiin.

Helpoin kategorisointi, joka kyberrikoksista voidaan tehdä, on jakaa se perinteisiin ja ei-perinteiseen rikollisuuteen, mutta tämä ei ole kovin merkityksellinen jako. Zhang ym. (2012) ovat jakaneet kyberrikollisuuden viiteen kategoriaan, joka on visualisoitu kuviossa 1 (Zhang, Xiao, Ghaboosi, Zhang & Deng, 2012).



KUVIO 1 Kyberrikollisuuden kategorisointimalli

Tässä mallissa on erotettu perinteiset rikokset ja loput kyberrikollisuuden kategoriat erilleen omiksi haaroikseen. Tässä mallissa näkyy kyberrikollisuuden monimuotoisuus paremmin kuin karkeammassa perinteisiin ja ei-perinteisiin rikoksiin jaottelussa, sillä muilla kuin perinteisillä rikoksilla on neljä kategoriaa. ”Tietokone/tietoverkko kohteena” kategoriaan kuuluu palvelunestohyökkäykset, haittaohjelmat, hakkeroinnit ja muut vastaavat rikokset. Tämä kategoria kattaa yleisimmät hyökkäykset, joissa pyritään hyökkäämään tietokoneeseen tai tietoverkkoon estämällä sen toiminta tai saamaan se hyökkääjän hallintaan. Tietokone/tietoverkko paikkana ei ole enää niin ajankohtainen kuin muut näistä kategorioista. Mallissa kategorian pääkyberrikollisuuden muoto on phreaking, joka oli ensimmäisiä kyberrikollisuuden muotoja. Sillä viitataan noin 1960- ja 1970-luvuilla yleistyneeseen toimintaan, jossa vaikutettiin puhelinverkkoyhteyksiin. Pääasiassa phreakingiä tekevät saattoivat soittaa ilmaisia puheluja ja ruuhkauttaa puhelinverkkoja. Vaikka Gold (2011) argumentoi phreakingin uudelleennoususta, ei sen merkitys tai yleisyys ole samalla tasolla muiden rikosten kanssa ja sen takia olisi syytä tutkia pitäisikö se jättää mallista pois.

2.3 Kyberrikollisuuden yleisyys ja vaikutukset

Kyberrikollisuuden määrä on noussut räjähdysmäisesti 2000-luvulla. Kyberrikollisuuden yleisyys vaihtelee maasta riippuen. Rikosten laatu, määrä ja rikosten tyyppi vaihtelevat maakohtaisesti ja myös ajankohtaisesti. Seuraavaksi tutkielmassa käsitellään kyberrikollisuuden yleisyyttä ja sen aiheuttamia vaikutuksia.

2.3.1 Yleisyys Suomessa, Euroopassa ja maailmalla

Suomessa yleisimpiä ilmoitettuja rikoksia ovat keskusrikospoliisin tilastojen mukaan maksuvälinepetokset, identiteettivarkaudet, tietomurrot ja viestintäsalaisuuden loukkaus (Jämsén, 2018). Maksuvälinepetoksia ilmoitettiin vuosina 2010–2018 noin 70 000, joka on selkeästi näistä eniten. Muita kolmea rikostyyppiä ilmoitettiin samana aikana noin 16 000 tapausta. Näistä kolmesta rikoksesta selkeästi eniten tehtiin identiteettivarkauksia, joita ilmoitettiin 10 235 tapausta, joista ylivoimainen enemmistö on tapahtunut vuosina 2016–2018. Tietomurtojen ja viestintäsalaisuuden loukkauksien määrä on pysynyt tasaisesti noin 250 ja 500 välillä joka vuosi.

Euroopassa suurimmat trendit viime vuosina ovat olleet tietokoneisiin tai tietoverkkoihin kohdistuvat hyökkäykset, sekä lisäksi maksuvälinepetokset. Europolin tilannekatsausraportissa (IOCTA) käsitellään Euroopan kyberrikollisuus uhkia ja niiden tilannetta vuosittain. Vuoden 2017 raportista selviää, että haittaohjelmien ja varsinkin kiristyshaittaohjelmien yleisyys on ollut kasvussa (Europol, 2017). Yksi suurimmista syistä tähän on todennäköisesti WannaCry -

kiristyshaittaohjelma, joka oli yksi suurimmista kiristyshaittaohjelmakampanjoista ikinä. Tämän taustalla oli NSA:n kehittämä Eternal Blue -hyökkäys, jota käytettiin kyseisessä haittaohjelmassa ja alettiin käyttää myös muissa haittaohjelmissa ja yleisesti hakkeroinnissa (Mohurle & Patil, 2017). Eternal Blue hyödynsi Windowsin SMB (Server Message Block) protokollan haavoittuvuutta. SMB onkin ollut jo pitkään Windowsin yksi suurimmista tietoturvahaavoittuvuuksista ja tässä tapauksessa se johti hakkereille koodin etäsuorittamismahdollisuuksiin.

Vuoden 2019 tilannekatsausraportissa (IOCTA, 2019) nostetaan paljon samoja asioita esille kuin vuoden 2017, vaikka eroavaisuuksiakin löytyy. Edelleen tietokoneisiin tai tietoverkkoihin kohdistuvia rikoksia pidetään prioriteettina, mutta kiristyshaittaohjelmien merkitystä ei ole tuotu yhtä selvästi esille kuin aiemmin. Myös maksuvälinepetokset on mainittu prioriteetiksi kuten aiemmin, eikä se ole yllätys, sillä maksuvälinepetoksiin liittyy myös usein muuta rikollista toimintaa, kuten ihmiskauppaa. Uutena lisäyksenä on kuitenkin pimeän verkon käyttö rikolliseen toimintaan. Europol (2019) arvioi Tor-ympäristön olevan ainakin vielä toistaiseksi hallitseva sovellus kyseiseen tarkoitukseen sen käyttäjäystävällisyyden, tarjonnan ja vakiintuneen käyttäjäkunnan takia.

Maailmanlaajuisesti Pohjois- ja Etelä-Amerikassa, sekä Euroopassa tehdään määrällisesti vähemmän kyberrikoksia kuin esimerkiksi Aasiassa, mutta vahingot ovat keskimäärin suurempia rikosta kohden. Informaatiorikokset ovat etenkin Amerikoissa yleisempiä ja siksi vahingot saattavat olla suurempia. Rikosten kohteina on usein liikesalaisuuksia, sekä lisäksi Yhdysvalloissa on esiintynyt paljon tietojenkalastelua. Yksi nousevimmista tietojenkalastelun muodoista Yhdysvalloissa on ollut tekstiviestien (engl. smishing) ja tekaistujen internetsivujen (engl. pharming) muodossa (FBI, 2019). Lisäksi maailmanlaajuisesti Crime as a Service (CaaS) palvelut ovat yleistyneet kyberrikollisuudessa. CaaS:llä tarkoitetaan palveluna ostettavaa rikosta. CaaS:n yleistyminen kertoo ennen kaikkea siitä, kuinka organisoitua ja liiketoimintamaista kyberrikollisuudesta on tullut. (Manky, 2018.)

Matalamman elintason maissa, kuten monissa Afrikan maissa yleinen ongelma on laittomasti ladatut ohjelmistot. Esimerkiksi Libyassa lähes 90 % ohjelmistoista on piraattiversioita. Laittomasti ladatut ohjelmistot ovat kyberrikollisuuden näkökulmasta suuri riski. Ensinnäkin ohjelmistojen laiton lataaminen on itsessäänkin jo rikos, mutta laittomat ohjelmistot eivät useimmiten saa kehittäjien päivityksiä. Tämä tekee kyseisistä ohjelmistoista helppoja kohteita hyökkääjille, mikä lisää kyseisissä maissa selkeästi haittaohjelmistojen leviämistä, verrattuna maihin, joissa kyberturvallisuutta ei pidetä ylellisyystuotteena. (Kshetri, 2019)

2.3.2 Kyberrikollisuudesta aiheutuvat vahingot

Kyberrikollisuuden taloudellisia vahinkoja on lähes mahdotonta kokonaisuudessaan arvioida tarkasti, sillä mahdollisia epäsuoria vaikutuksia yrityksiin,

valtioihin ja talouteen on mahdotonta saada merkittäviksi ja todenmukaisiksi tilastoiksi.

European Crime Prevention Network (2016) kuitenkin arvioi teoreettisesti kyberrikollisuuden avulla saadun rikoshyödyn olevan vuonna 2016 noin 350 miljardia euroa maailmanlaajuisesti. Tämä alkaa jo lähestymään globaalin huumekaupan vuosittaista rikoshyötyä. Kyberrikollisuuteen perehtyvä julkaisija Cybersecurity Ventures, arvioi kyberrikollisuudesta aiheutuvien haittojen olleen vuonna 2015 noin 3 biljoonaa dollaria ja arvioi kyseisen luvun nousevan 6 biljoonaan vuoteen 2021 mennessä (Morgan, 2017). Tämä on kuitenkin vain yksi arvio ja esimerkiksi Forbesin arviot ovat maltillisempia. Forbes (2016) arvioi vahinkojen olleen 2015 vielä 500 miljardin luokkaa ja luvun nousevan noin 2 biljoonaan vuoteen 2020 mennessä. Arvioiden varianssi tukeekin hyvin väitettä, että kyberrikollisuuden vahinkoihin tai taloushyötyihin liittyviä lukuja on todella vaikea tarkasti tilastoida tai arvioida. Arvioista kuitenkin voidaan nähdä, että aiheutuvien vahinkojen määrä on noussut viime vuosina ja tulee nousemaan vielä nopeammin.

Havainnollistavana esimerkkinä kyberrikollisuuden taloudellisista vaikutuksista voi toimia aiemmin mainittu WannaCry -virus. Virus todettiin yli 400 000 tietokoneessa ympäri maailmaa ja aiheutti noin 4 miljardin dollarin vahingot pelkästään vuonna 2017 (Varonis, 2020). Keskimäärin yksi onnistunut kiristyshaittaohjelmahyökkäys aiheuttaa yritykselle noin 133 000 dollarin vahingot.

3 KYBERRIKOSTEN TUTKINTA

Tässä luvussa käsitellään kyberrikosten tutkintaa. Kohta 3.1 määrittelee kyberrikosten tutkintaa ja tutkinnan historiaa. Kohdassa 3.2 esitellään malleja kyberrikostutkinnan suorittamiseen ja vertaillaan niitä. Kohta 3.3 käy läpi, mitkä ovat kyberrikostutkinnan haasteita.

3.1 Kyberrikostutkinnan määritelmä ja historia

Kyberrikollisuus aiheuttaa paljon vahinkoa, ei pelkästään suurille yrityksille, vaan nykypäivänä myös pienet ja keskisuuret yritykset (SME) ja yksityishenkilöt ovat yleisiä kohteita. Erityisesti informaatiorikokset, joiden kohteena on SME ovat yleistyneet. Kyberturvallisuuteen erikoistuneen yrityksen Varoniksen (2020) mukaan 43 % tietomurroista kohdistuu pieniin yrityksiin. Vakavatkin kyberrikokset ovat siis lähellä yksittäisten ihmisten arkielämää. Kyberrikosten tutkinnan tavoite loppukädessä on vähentää rikollisuutta, ja sitä kautta vähentää näitä ongelmia, jotka koskettavat lähes jokaista yksilöä nykypäivänä. Seuraavaksi tutkielmassa selvitetään kyberrikostutkinnan määritelmää, tarkoitus sekä käydään läpi kyberrikosten tutkinnan historiaa.

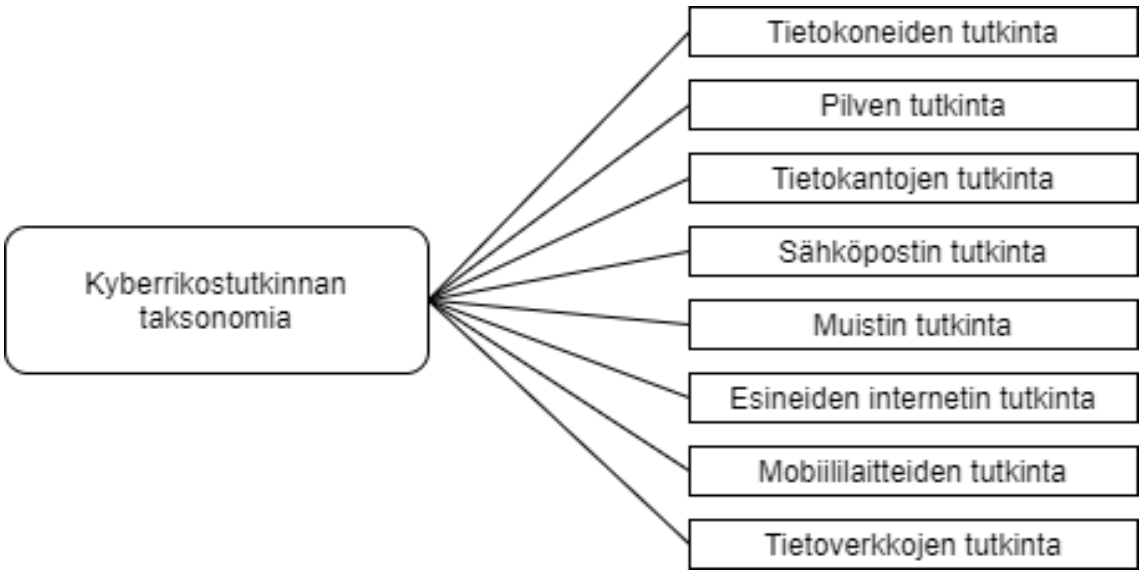
3.1.1 Määritelmä

Kyberrikosten tutkinta eli cyber forensics tai digital forensics on syntynyt viranomaisten tarpeesta tutkia kyberrikoksia. Tämä tarve on syntynyt tietokoneiden ja tietoverkkojen yleistymisen myötä.

Kyberrikosten tutkinnalla tarkoitetaan prosessia, jolla pyritään tunnistamaan, säilyttämään, analysoimaan ja esittämään digitaalista todistusaineistoa (McKemmish, 1999). Palmer (2002) esittää, että tällä prosessilla voidaan pääasiassa kerätä vain dataa, jota analysoimalla voidaan muodostaa johtopäätöksiä.

Tätä väitettä myös tukee perinteisen rikostutkinnan periaate, jonka mukaan todistusaineistoa täytyy tulkita tapahtumien selvittämiseksi (Robertson, Vignaux & Berger, 2016). Casey (2009) esittää yhden kyberrikostutkinnan perusperiaatteista olevan taustalla toimivan teknologian ja metodien ymmärtäminen.

Kyberrikostutkinta kattaa monta osa-aluetta. Esimerkiksi computer forensics termiä käytettiin ennen termejä cyber forensics ja digital forensics. Tänä päivänä kuitenkaan termi computer forensics ei kata kaikkia kyberrikostutkinnan osa-alueita, vaan se tarkoittaa vain tietokoneympäristöä. (Sammes & Jenkinson, 2007.) Termit digital forensics tai cyber forensics koostuvat kahdeksasta alakategoriasta, jotka ovat esitettynä kuviossa 2.



KUVIO 2 Kyberrikostutkinnan taksonomia (Narwal & Goel, 2020, mukaan).

Näistä uusimpia lisäyksiä ovat pilvipalveluiden, IoT -laitteiden sekä puhelimien tutkinta. Kaikissa kahdeksassa käytetään paljon erilaisia työkaluja ja niitä kehitetään koko ajan lisää.

Suurimmat eroavaisuudet perinteiseen rikostutkintaan rikosten luonteiden ja tapahtumapaikkojen selvien eroavaisuuksien lisäksi, on todisteiden ominaisuuksissa. Kyberrikostutkinnan menetelmillä dataa voidaan kerätä paljon suurempia määriä suhteessa aikaan. Esimerkiksi todistusaineistoa voi olla monta kovalevyllistä tekstiä tai kuvia, jonka käsittelyssä tai keräämisessä menee huomattavasti vähemmän aikaa kuin vastaavien fyysisten todisteiden. Lisäksi digitaalista todistusaineistoa voidaan salata, mikä tekee siitä monimutkaisempaa. Samoja periaatteitakin löytyy esimerkiksi todisteiden käsittelyssä ja dokumentoinnissa (Gayed, Lounis, Bari & Nicolas, 2013). Kyberrikoksisissa ei välttämättä varasteta mitään fyysistä, vaan immateriaalioikeuksia tai bittejä kyberavaruudessa.

Yhteenvetona kyberrikostutkintaan koostuu eri kategorioista ja siihen kuuluu paljon erilaisia ja kohdekohtaisia työkaluja. Kyberrikostutkinnassa pyritään kasaamaan dataa kohteesta ja esittämään se muodossa, jota voidaan käyttää

oikeustoimissa. Nykypäivän kyberrikostutkinnassa ei riitä, että tietää mitä työkalua kuuluu käyttää tai mitä dataa sillä voidaan saada, vaan tutkijan kuuluisi ymmärtää työkalujen toiminta ja periaatteet.

3.1.2 Historia

Koska kyberrikostutkinta on suhteellisen nuori tieteenala ja kehitystä tehdään ennennäkemätöntä vauhtia joka vuosi, ei sillä ole vielä kovinkaan paljoa historiaa. Suhteellisen lyhyt historia antaa kuitenkin hyvän käsityksen kyberrikostutkinnan lähtökuopista ja siitä, kuinka nopeasti internetin ja tietokoneiden yleistymisen seurauksena se alkoi kehittymään. Historian läpikäyminen antaa perspektiiviä tämän päivän kehitykselle.

Ensimmäisen kerran kyberrikostutkinnan tekniikoita käytettiin 1970-luvulla. Yhdysvaltojen armeija ja tiedusteluorganisaatiot pyrkivät suojelemaan omia tietojansa keskustietokoneillaan. Tämä toiminta pidettiin kuitenkin salaisena, eikä sitä ikinä dokumentoitu. (Bayuk, 2010.) Vuonna 1976 Donn Parkerin kirja Crime by Computer oli ensimmäisiä teoksia, jossa esitettiin ajatuksia digitaalisten todistusaineiden käytöstä. Tätä todistusaineistoa voitaisiin sitten käyttää syyttäessä rikoksia, joissa on käytetty tietokoneita. (Pollitt, 2010.) Kuitenkaan tämä ei vielä realisoitunut kovinkaan paljon käytäntöön, sillä viranomaisten oli vaikea käsittää, miten tietokonetta voitaisiin sekä käyttää rikoksen tekemiseen, että sen selvittämiseen.

1980-luvun alkupuoliskolla kyberrikostutkinta alkoi yleistymään. Sen rooli oli enemmänkin tukea perinteistä rikostutkintaa kuin suorittaa omia tutkintoja. Tähän aikaan tietokoneiden käyttö alkoi yleistymään ja kyberrikostutkinnan tarve alkoi hiljalleen kasvaa. Edistyneimmät rikolliset alkoivat pitämään kirjanpitoa ja tallentamaan kuvia ja suunnitelmia tietokoneille. Vaikka kyberrikostutkinnan rooli alkoi 1980-luvulla kasvamaan, ei se vielä saanut tukea suuremmilta rikostutkintaorganisaatioilta, vaan osaaminen oli tutkijoiden oman mielenkiinnon ja opiskelun varassa. (Bayuk, 2010.)

1990-luvulla kyberrikostutkinnan tarve ja tärkeys alkoi nousta niin merkittäväksi, että lainvalvontaorganisaatioiden oli alettava kiinnittämään huomiota tarkemmin kyberrikostutkintaan. Tähän aikaan kyberrikollisuus oli vielä pitkälti perinteistä rikollisuutta, jonka apuna käytettiin tietokoneita ja tietoverkkoja, ja oli vielä nykypäivän standardeihin verrattuna yksinkertaista. Työkaluina toimi lähinnä vaatimattomat komentoriville annettavat ohjelmat. Vuonna 1993 FBI piti ensimmäisen International Conference on Computer Evidence, jossa osallistujia oli 26 eri maasta. Tässä kokouksessa päätettiin kansainvälisen yhteistyön lisäämisestä, joka lopulta johti International Organization on Computer Evidencen (IOCE) muodostumiseen vuonna 1995. Tämän lisäksi 1990-luvulla syntyivät ensimmäiset kyberrikoslaboratoriot. (Pollitt, 2010.)

2000-luvulle tultaessa kyberrikollisuus ja sen riskit alkoivat olemaan suuremman yleisön tiedossa. Kyberrikostutkinnan keinoilla saadut todisteet

alkoivat olla yleisempiä ja siitä syystä tuomarien, asianajajien ja muiden lakia harjoittavien täytyi alkaa katsomaan kyberrikostutkintaa ja sen tuottamaa informaatiota uudessa valossa. Sen takia lakitekniset vaatimukset digitaaliselle todistusaineistolle alkoivat kehittyä ja pyrittiin määrittelemään tarkemmin, mikä on oikeuteen kelpaavaa materiaalia. (Pollitt, 2010.)

Samaan aikaan kyberrikostutkijat alkoivat törmätä ongelmiin kyberrikollisuuden kehittymisen ja yleistymisen kanssa. Moninaisten kyberrikollisuuden muotojen kehittyminen muodostui ongelmaksi sen hetkisille tutkijoille, koska työkalut tai työkoneistot eivät olleet kovin skaalautuvia. Yksi tutkija ei voinut enää tehdä kaikkea vaadittavia tehtäviä tarpeeksi korkealla tasolla. Tämän takia kyberrikostutkintaa alettiin kehittämään ja koulutusta alettiin lisäämään. Tutkijat alkoivat erikoistumaan omille kyberrikostutkinnan aloille, jotka esiteltiin kuviossa 2. Lisäksi skaalautuvampia työkaluja alettiin kehittämään, koska enää yksittäisten tietokoneiden työstäminen kerralla ei riittänyt. (Bayuk, 2010.)

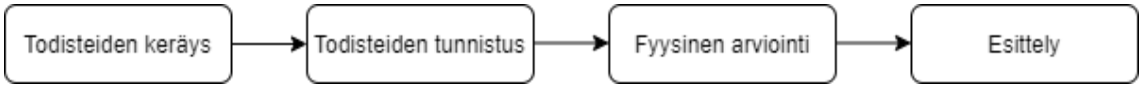
Lähestyttäessä vuotta 2010 kyberrikostutkintaa koulutettiin yhä enemmän ja kyberrikostutkijoilla oli todennäköisemmin akateemista taustaa käytännön koulutuksen lisäksi. Kyberrikostutkinnan urapolkua alettiin arvostamaan enemmän ja alettiin luomaan erilaisia sertifikaatteja. (Pollitt, 2010.)

3.2 Kyberrikostutkinnan prosessin mallit

Minkä tahansa toiminnan ja prosessien optimointi ja selkeyttäminen parantaa sen tuloksia, eikä kyberrikostutkinta ole poikkeus. Kyberrikostutkinnan suorittamiseen on esitetty monia malleja, joita ei ollut montaa varteenotettavaa ennen vuotta 2000. Vasta vuosituhannen vaihteen kyberrikollisuuden nousun aikana alettiin kehittää enemmän prosessimalleja. Tämän alaluvun tarkoituksena on selvittää, mitä erilaisia malleja kyberrikostutkinnan prosessille on esitetty ja vertailla niiden heikkouksia ja vahvuuksia keskenään.

3.2.1 Tietokoneiden tutkinnan prosessi (1984)

Pollitt (1995) esitti ensimmäisen prosessimallin kyberrikostutkinnalle. Se oli neljään vaiheeseen jaettu malli, jonka tarkoituksena oli tarjota kaavio, jota noudattamalla saataisiin käsiteltyä digitaalisia todisteita. Mallilla pyrittiin varmistamaan, että toiminta pysyy luotettavana, sekä kelpaisi oikeuteen. Malli on esitettynä kuviossa 3.



KUVIO 3 Tietokoneiden tutkinnan prosessi (Yusoff, Ismail, Hassan, 2011).

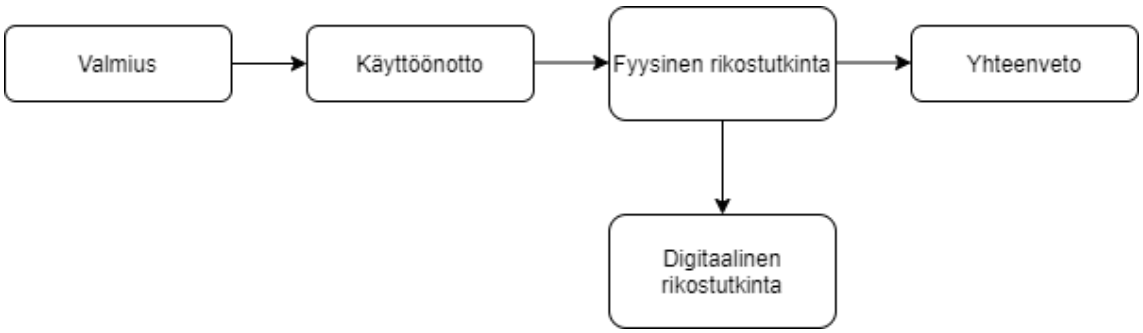
Ensimmäinen vaihe on todisteiden keräämistä. Sillä tarkoitetaan todisteiden hankkimista lain sallimin tavoin, jotta todistusaineisto olisi mahdollisesti esitettävissä oikeudessa. Tässä vaiheessa joudutaan mahdollisesti käyttämään lainkäyttövaltaa tai teknistä osaamista. Tämän vaiheen tuotos on yleensä vain raakaa aineistoa, jonka tarkoitusta tai käytettävyyttä ei vielä tarkoin tiedetä (Pollitt 1995).

Seuraavana vaiheena on todisteiden tunnistaminen. Pollitt (1995) jakoi tämän vaiheen kolmeen osaan. Todisteen täytyy olla määriteltävissä fyysisessä muodossa eli esimerkiksi kovalevy. Lisäksi todisteen täytyy olla määriteltävissä loogisesti eli, missä se sijaitsee kovalevyllä. Viimeiseksi todiste täytyy sijoittaa oikeaan kontekstiin. Esimerkiksi lukemalla aineistoa ohjauskomentoina, jolloin ihminen voi ymmärtää sitä. Todisteiden tunnistamisen tuotoksena raaka-aineistosta on saatu dataa. (Pollitt, 1995.)

Seuraavassa vaiheessa arvioidaan todisteet. Tässä vaiheessa mukaan tulevat lakitekniset seikat. Teknisestä näkökulmasta datasta voidaan jalostaa paljon eri informaatiota, mutta lakitekniset seikat määrittelevät sen, minkälaista informaatiota tarvitaan. Tämän vaiheen tarkoitus on jalostaa datasta informaatiota oikeaan kontekstiin. Viimeisessä vaiheessa tämä informaatio esitellään oikeudessa. (Pollitt, 1995.)

3.2.2 Integroitu digitaalinen tutkintaprosessi (IDIP) (2003)

IDIP on viisivaiheinen prosessimalli, jonka esittivät Brian Carrier ja Eugene Spafford vuonna 2003. He tutkivat 2000-luvun ensimmäisiä malleja ja päättivät niiden pohjalta esittää oman mallinsa. IDIP oli ensimmäisiä tunnettuja malleja, joka otti myös fyysisen rikospaikan huomioon kyberrikostutkinnassa. Yksi malleista, jota Carrier ja Spafford mainitsevat tutkineensa, oli perinteisen rikostutkinnan rikospaikan käsittelyyn tarkoitettu malli, mikä selittää fyysisten todisteiden ja rikospaikan huomioimisen. IDIP:n vaiheet ovat esitettynä kuviossa 4.



KUVIO 4 IDIP (Yusoff, Ismail, Hassan, 2011).

Ensimmäinen vaihe tarkoittaa valmiutta, joka on jaettu kahteen osaan: infrastruktuurin valmius ja operaatiovalmius. Operaatiovalmiudella tarkoitetaan esimerkiksi henkilöstön kouluttamista, työkalujen hankintaa ja laitteiston päivittämistä. Henkilöstön ja kaluston valmius täytyy olla riittävällä tasolla, jotta tutkintaa voidaan suorittaa. Infrastruktuurin valmiudella tarkoitetaan järjestelmiä, joiden avulla saadaan dataa kyberrikostutkintaa varten. Esimerkkinä tästä toimii palvelimien lokien tallennusjärjestelmät. Jotta palvelinlokeja voidaan tutkinnassa hyödyntää, täytyy niiden olla olemassa ja käsiteltävissä. Ensimmäinen vaihe ei ole sidoksissa mihinkään tapahtumaan tai muuhun vaiheeseen, vaan se on käynnissä koko ajan. (Carrie & Spafford, 2003.)

Seuraavassa vaiheessa tutkinnan varsinaiset tapahtumat alkavat, kun jokin tapahtuma, hälytys tai havainto kyberrikoksesta vaatii kyberrikostutkintaa. Tämän vaiheen tarkoituksena on saada valtuutukset rikospaikalle. Tarvittavat valtuudet riippuvat tapauskohtaisesti rikospaikan sijainnista ja paikallisesta lainsäädännöstä. (Carrie & Spafford, 2003.) Tähän vaiheeseen kuuluu lisäksi kyberrikoksen tunnistaminen kohteesta. Esimerkiksi mahdollisesti saastuneesta tietokoneesta etsitään viruksia tai rootkittiä, jotta voidaan varmistua rikoksen tapahtumisesta.

IDIP oli ensimmäisiä malleja, joka erotti fyysisen rikospaikan ja digitaalisen rikospaikan. Koska kyberrikostutkinnan päätarkoituksista on myös tunnistaa rikoksen tekijä, on tärkeää muistaa myös fyysisen rikospaikan tutkinta. Fyysisen rikospaikan tutkinnan tärkeimmät tehtävät kyberrikoksissa ovat auttaa yhdistämään rikoksen tekijä rikokseen, sekä tunnistaa potentiaaliset digitaaliset todisteet. Fyysisen rikospaikan tutkimiseen käytetään tässä mallissa normaaleja rikostutkinnan prosesseja. Fyysisen rikospaikan tutkimisessa pyritään muodostamaan kuva tai hypoteesi, mitä rikospaikalla on tapahtunut.

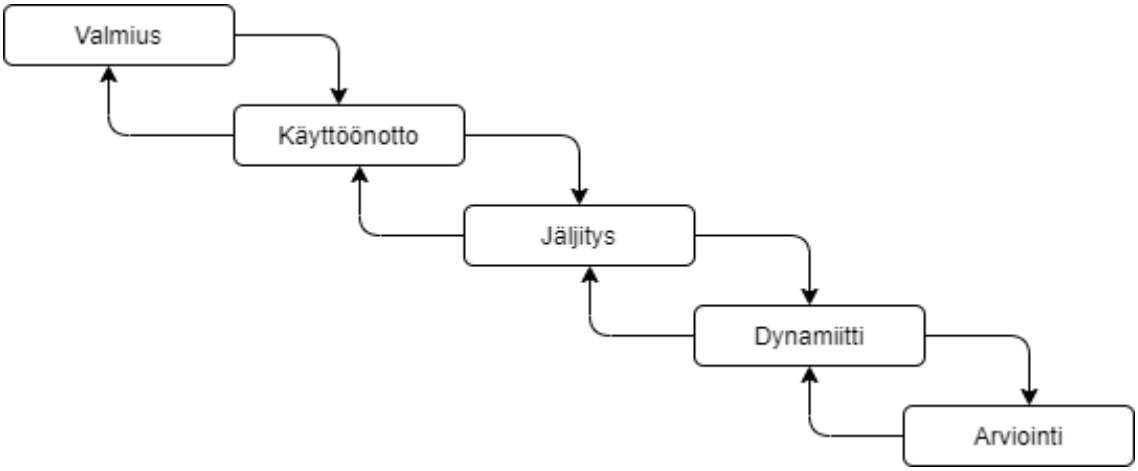
Digitaalisen rikospaikan tutkinta aloitetaan fyysisen rikospaikan tutkinnan jälkeen. Digitaalinen rikospaikka voi olla esimerkiksi palvelin, josta sitten etsitään tietoa kyberrikostutkinnan työkaluilla. Digitaalisen rikospaikan tutkimisen jälkeen muodostetaan hypoteesi, mitä digitaalisella rikospaikalla on tapahtunut, jonka jälkeen johtopäätökset ja molemmat lopputulemat esitellään oikeudessa. (Carrie & Spafford, 2003.)

Viimeisessä eli yhteenveto vaiheessa käydään läpi suoritettu tutkinta ja arvioidaan, kuinka hyvin rikostutkinnassa onnistuttiin. Tässä vaiheessa on tärkeää molempien, fyysisen ja digitaalisen, rikospaikkojen tutkimisvaiheiden erillinen arviointi, sekä miten molemmat vaiheet onnistuivat suhteessa toisiinsa. (Carrie & Spafford, 2003.)

3.2.3 Paranneltu digitaalinen tutkintaprosessi (EDIP) (2004)

EDIP tulee englannin sanoista Enhanced Digital Investigation Process ja se on kehitetty IDIP:n pohjalta sitä parannellen (Baryamureeba & Tushabe, 2004). Siitä johtuu nimen ensimmäinen sana Enhanced eli paranneltu. EDIP on iteratiivinen

malli, joka koostuu viidestä vaiheesta, jotka ovat esitetty kuviossa 5. Ensimmäinen ja viimeinen vaihe ovat sisällöltään samoja kuin IDIP:ssä ja toisella vaiheella on sama nimi, mutta sen sisältö hieman eroaa IDIP:n toisesta vaiheesta.



KUVIO 5 EDIP (Yusoff, Ismail, Hassan, 2011).

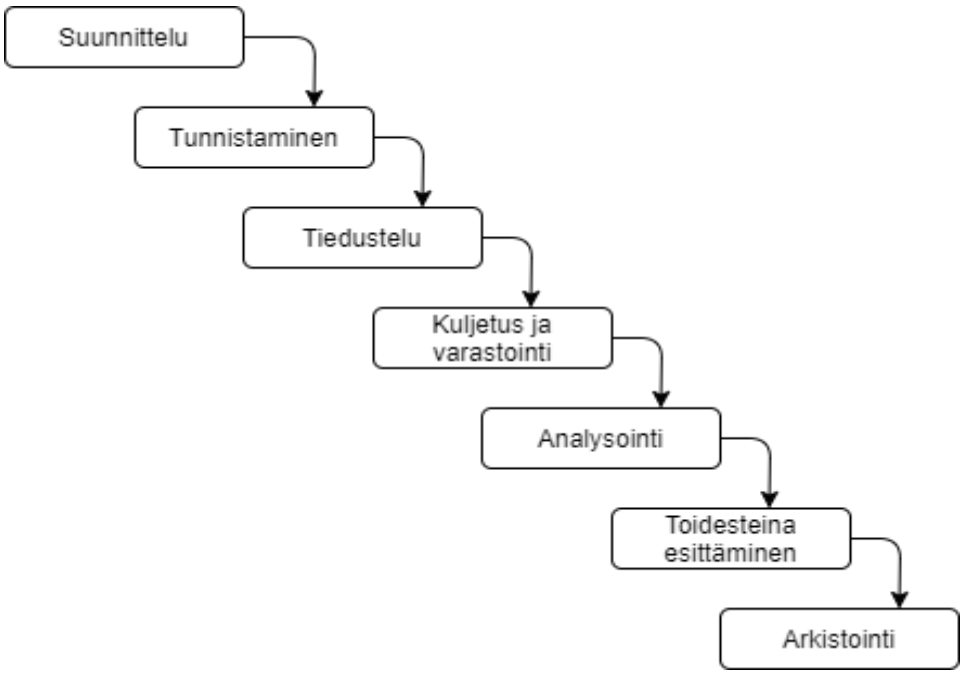
Ensimmäiset erot mallien väliltä löytyvät toisesta vaiheesta. Toisessa vaiheessa tarkoituksena on edelleen saada hälytys tai muu tekijä, joka laukaisee tutkimusprosessin, mutta seuraavaksi tutkitaan fyysistä rikospaikkaa ja paikannetaan mahdolliset todisteet. Se on suurin eroavaisuus IDIP:n toiseen vaiheeseen. Seuraavaksi tutkitaan digitaalista rikospaikkaa ja todennetaan mahdollinen hyökkäys. Kun hyökkäys on todennettu, suoritetaan samat toimenpiteet kuin IDIP:ssä. (Baryamureeba & Tushabe, 2004.)

Seuraavassa vaiheessa pyritään jäljittämään hyökkäyksen käytetty laite esimerkiksi tietokone. Tähän voidaan käyttää erinäisiä kyberrikostutkinnan työkaluja tai palveluita, joilla voidaan yrittää paikantaa laitetta esimerkiksi IP-osoitteen perusteella. Tässä vaiheessa mallin iteratiivisuus nousee esille. Jos mahdollinen laite, jolla rikos on tehty, löydetään, suoritetaan sille rikospaikalle taas toisen vaiheen toimenpiteet. (Baryamureeba & Tushabe, 2004.)

Neljännessä vaiheessa yhdistetään IDIP:n fyysisen ja digitaalisen rikospaikan tutkinnan vaiheet, mutta erona on se, ettei vaiheissa tehdä erikseen hypoteesia, mitä on tapahtunut. EDIP-mallissa tarkoituksena on tehdä hypoteesi siitä, mitä on tapahtunut vasta molempien tutkintojen jälkeen, jotta tuloksena olisi yksi luotettavampi hypoteesi, eikä kaksi erillistä hypoteesia (Baryamureeba & Tushabe, 2004).

3.2.4 Digitaalisen tutkinnan malli perustuen Malesian tutkintaprosessiin (DFMMIP) (2009)

DFMMIP on Malesian kyberavaruuteen liittyvän lain puitteissa tehty seitsemänvaiheinen malli. Sen on esittänyt Sundresan Perumal vuonna 2009. Mallia muodostaessa Perumal on tutkinut aikaisempia kyberrikostutkinnan prosessimalleja mukaan lukien esimerkiksi IDIP ja EDIP mallit. DFMMIP:n vaiheet ovat esitetty kuviossa 6.



KUVIO 6 DFMMIP (Yusoff, Ismail, Hassan, 2011).

DFMMIP:n ensimmäinen vaihe on planning eli suunnittelu. Nimi on hieman harhaanjohtava suoraan suomennettuna, koska tässä vaiheessa suoritetaan tarvittavat lakiin liittyvät toimet rikospaikkaa varten kuten etsintäluvan hankinta. Suunnitteluvaihetta seuraa todisteiden tunnistaminen. Tunnistusvaiheessa pyritään tunnistamaan materiaali, joka saattaa olla tutkinnalle mahdollisesti hyödyllistä. Lisäksi tässä vaiheessa Perumal (2009) nostaa esille ”elossa” olevien laitteiden tutkimisen. Elossa olevalla tarkoitetaan tässä kontekstissa laitetta, jota ei ole vielä sammutettu tai sen tilaa ei ole muuten merkittävästi rikoksen jälkeen. Mallin mukaan ”elävistä” tietokoneista voi saada irti materiaalia, joka ei ole enää saatavilla sen ”kuoltua”, ja siksi tässä vaiheessa arvioidaan, täytyykö tutkittavia laitteita tutkia ennen kuin ne sammutetaan.

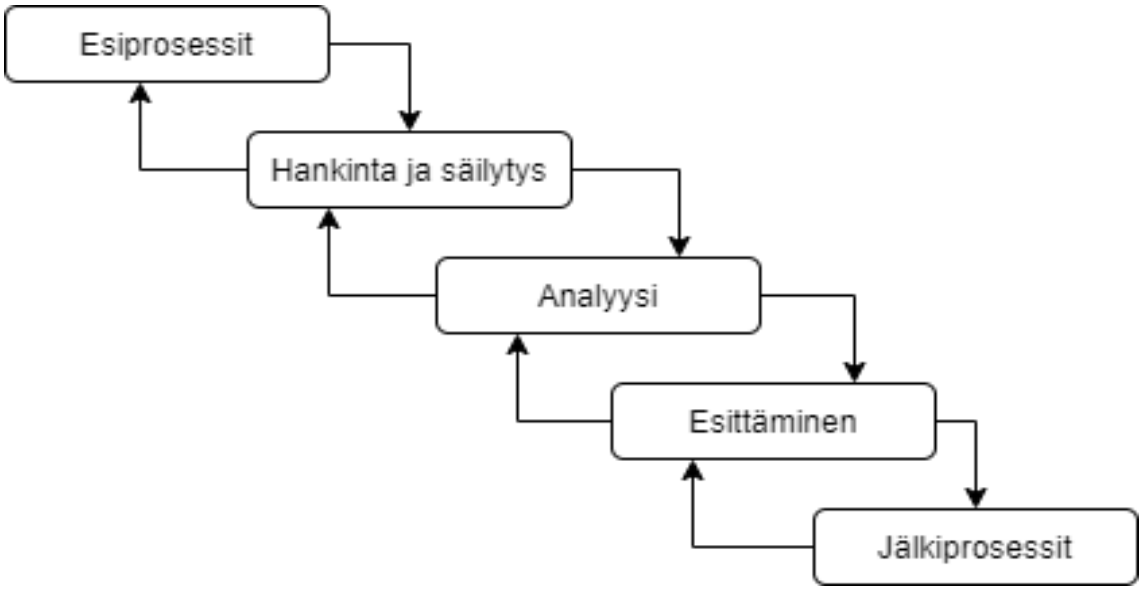
Tiedusteluvaiheessa hankitaan informaatiota rikospaikasta. Tällaista informaatiota on esimerkiksi laitteiden käyttötarkoitukset. Tämä on tärkeää esimerkiksi palvelinten kanssa, sillä informaatio, mihin palvelinta käytetään helpottaa tutkijoiden työtä.

Seuraava vaihe on mahdollisten todisteiden kuljetus viranomaisten haltuun ja niiden säilöntä. Tämän vaiheen epäonnistuminen voi pahimmassa tapauksessa estää ratkaisevien todisteiden esittämisen oikeudessa. Kun todisteet ovat saatu kuljetettua rikospaikalta seuraa analysointivaihe. Analysointivaiheessa analysoidaan kerätyt mahdolliset todisteet käyttäen kyberrikostutkinnan eri työkaluja. (Perumal, 2009.)

Toiseksi viimeisessä vaiheessa kyberrikostutkinnan havainnot esitetään oikeudessa, jossa tutkijoiden täytyy perustella havaintonsa ja esittää oma hypoteesinsa tapahtumien kulusta. Oikeudenkäynnin jälkeen siirrytään viimeiseen vaiheeseen, joka on tutkimuksen tulosten arkistointi. (Perumal, 2009.)

3.2.5 Geneerinen tietokoneiden tutkintaprosessi malli (GCFIM) (2011)

GCFIM on viisivaiheinen malli, jonka esittivät Yusoff, Ismail ja Hassan vuonna 2011. Vuoteen 2011 mennessä kyberrikostutkintaan oli esitetty jo paljon erilaisia suoritusmalleja ja ideana oli koota niistä yksi yleispätevämalli. Sen muodostamisessa tutkittiin yhteensä 14 erilaista kyberrikostutkinnan mallia. Mallin kehittäjät tutkivat eri mallien vaiheita ja vaiheisiin kuuluvia toimia ja koostivat vaiheista, joita esiintyi eniten, omansa, joka on esitettynä kuviossa 7.



KUVIO 7 GCFIM (Yusoff, Ismail, Hassan, 2011).

Useimmissa malleissa on jonkinlainen valmistautumisvaihe ensimmäisenä, joten tämäkin malli esittää sen prosessin ensimmäisenä vaiheena. Yusoff ym. (2011) mukaan tämä prosessi sisältää kaikki valmistelut ennen rikospaikalle siirtymistä, sekä tarvittavien lupien hankkimisen.

Toiseksi vaiheeksi muodostui todisteiden hankinta ja säilöminen. Tässä vaiheessa kaikki tutkimukselle tarpeellinen materiaali kerätään ja valmistellaan seuraavaa vaihetta varten. Seuraava vaihe onkin todisteiden analysointi. Tämä on kyberrikostutkinnan päävaihe, jossa digitaalisista todisteista kerätään informaatiota valmiiksi seuraavaan vaiheeseen. (Yusoff ym., 2011).

Toiseksi viimeinen vaihe on löydösten esittely oikeudessa. Käytännössä tämä vaihe on koko kyberrikostutkinnan tarkoitus. Kaikki muut vaiheet ovat turhia, jos todisteita ei voida esittää oikeudessa. Tässä vaiheessa kaikki havainnot ovat dokumentoitu ja niiden täytyy olla esittävässä ja ymmärrettävässä muodossa.

Viimeinen vaihe on tutkimuksen sulkeminen. Siinä mahdollisesti palautettavat todisteet palautetaan niiden omistajille ja arvioidaan kyberrikostutkinnan onnistuminen kokonaisuutena.

3.2.6 Vertailu

Käydyt mallit tuovat erilaisia näkökulmia kyberrikostutkintaan hyvin esille. Kaikissa malleissa näkyy hyvin aikakausi, jolloin se on kehitetty ja sen aikakauden tarpeet. Esimerkiksi Pollittin vuonna 1984 esittelemä tietokoneiden tutkinnan prosessi on hyvin yksinkertainen verrattuna muihin, koska kyberrikostutkinnan prosessiin tarvittiin edes jonkinlaista standardisointia, sillä muita malleja ei ollut olemassa. Vastaavasti IDIP ja EDIP mallien aikaan ei ollut olemassa tarkkoja prosessimalleja ja kyberrikostutkinnan kasvavan kysynnän takia piti kehittää uusia malleja. Molemmat mallit esittävät hyvin, kuinka paljon erilaisia tehtäviä kyberrikostutkintaan kuuluu. Lisäksi IDIP ja EDIP helpottavat resurssitarpeiden arvioimista, mikä oli tärkeää 2000-luvun alussa, koska kyberrikosten yleistyessä resursseja ei aina ollut riittävästi (Carrier & Spafford 2003).

DFMMIP keskittyy seuraaviin ongelmiin, joihin kyberrikostutkinnassa on törmätty 2000-luvun alun jälkeen. Näihin ongelmiin lukeutuu esimerkiksi todisteiden käsittelyketjun eheyden varmistaminen (Du, Le-Khac & Scanlon, 2017). Aikaisemmissa malleissa keskityttiin itse tietokoneiden ja laitteiden tutkimiseen laboratoriossa, eikä mietitty esimerkiksi ”elävien” koneiden tutkimisen mahdollisuuksia (Yusoff ym. 2011). Toisaalta GCFIM taas on yksinkertaistettu malli, mikä viittaa mallien paljouteen. GCFIM tarkoituksena on esittää yleisimmät vaiheet, joita kyberrikostutkinnassa on, jotta saadaan hyvä yleiskäsitys kyseisestä prosessista.

Käytännön kannalta IDIP, EDIP ja DFMMIP määrittelevät vaiheet ja vaiheisiin kuuluvat tehtävät parhaiten ja ovat täten paremmin suoraan sovellettavissa käytäntöön. Lisäksi iteratiivisuus EDIP:ssä ja DFMMIP:ssä on otettava huomioon vertaillessa malleja. Iteratiivisuus EDIP:n tapauksessa lisäsi tutkinnan laadun tasaisuutta ja sitä voitiin soveltaa useampiin rikospaikkoihin (Baryamureeba & Tushabe, 2004).

IDIP:ssä ja EDIP:ssä esitetään tarkasti vaiheet ja niiden tehtävät, mikä helpottaa esimerkiksi resurssitarpeiden arviointia. Kuitenkin tarkka tehtävien kuvaus hidastaa prosessia ja tekee siitä raskaamman, sillä nämä mallit eivät pysty mukautumaan eri rikoksiin ja rikospaikkoihin yhtä hyvin kuin muut käsiteltävät mallit. GCFIM toisaalta on paljon joustavampi malli siinä mielessä, että sitä voidaan soveltaa eri tilanteisiin ja tapauksiin (Satti & Jafari, 2015).

4 TIETOJÄRJESTELMIEN KYBERRIKOSTUTKINTA

Tässä kappaleessa käsitellään kyberrikostutkintaa tietojärjestelmien näkökulmasta. Kohdassa 4.1 käsitellään, mitkä tekijät tietojärjestelmissä vaikuttavat kyberrikostutkintaan, sekä mitä asioita niiden suunnittelussa ja toteuttamisessa olisi tärkeää ottaa huomioon kyberrikostutkinnan kannalta. Kohta 4.2 käsittelee yleisesti tietojärjestelmien kyberrikostutkinnan haasteita sekä erottelee erilaisten järjestelmien ja niiden osien tutkinnan haasteita.

4.1 Kyberrikostutkintaan vaikuttavat tekijät tietojärjestelmissä

Tässä luvussa käsitellään pääosin neljän erityyppisen tietojärjestelmän tai tietojärjestelmän osan kautta niiden kyberrikostutkintaa sekä, mitkä asiat vaikuttavat siihen. Kyseiset järjestelmät tai osat ovat tietokannat ja niiden hallintajärjestelmät, tietoverkot sekä pilvipohjaiset järjestelmät. Tässä esitellyt havainnot eivät ole pelkästään aihekohtaisia, vaan niitä voidaan soveltaa muihinkin tietojärjestelmiin ja niiden eri osien kehittämiseen ja toteuttamiseen.

Tietokantojen hallintajärjestelmät ovat monipuolisia työkaluja, joilla sujuvoitetaan sekä tietokantojen hallintaa että myös muun organisaation liiketoimintaa. Tietokantojen hallintajärjestelmät mahdollistavat suurten tietokantojen käytön, hallinnan, ulosannin ja ne toimivat monien järjestelmien perustuksina. Tietokantojen hallintajärjestelmien yleistyminen on vaatinut niiden suunnittelulta ja toteutukselta enemmän. Tänä päivänä dataa kerätään valtavasti ja tehokkaiden tietokannan hallintajärjestelmien kehittäminen vaatii enemmän resursseja, koska yhä useammin käytetään massiivisia tietokantoja. (Hjertström, Nyström & Sjödin, 2012.) Hallintajärjestelmillä automatisoidaan toimintaa tietokantojen käsittelyssä. Ne passiivisesti tai aktiivisesti käsittelevät tietokantaa.

Passiivisella käsittelyllä tarkoitetaan tässä kontekstissa esimerkiksi tietokannan hallintajärjestelmän yhteistoimintaa muiden järjestelmien kanssa, jolloin tietoa lisätään tai muokataan muiden järjestelmien toiminnan kautta. Aktiivisella käsittelyllä tarkoitetaan tietokannan hallintajärjestelmän kautta tapahtuvaa tietojen lisäämistä, muokkausta tai poistamista. (McCarthy & Dayal, 1989.) Lisäksi tietokantajärjestelmät pystyvät toimimaan erilaisissa tilanteissa riippuen järjestelmästä myös työkaluina esimerkiksi esittäen dataa (Dittrich, Gatziu & Geppert, 1995).

Tärkeimpiä ominaisuuksia tietokantojen hallintajärjestelmissä ovat kyselyjen suoritusteho, erilaisten toiminnallisuuksien kehittämismahdollisuudet, sekä datan eheyden säilyttäminen. Tietokannan hallintajärjestelmää arvioitaessa taas voidaan pääosin tarkastella kolme kriittisintä tekijää: skaalautuvuus, luotettavuus ja verkkomahdollisuudet. (Post & Kagan, 2001.) Kyberrikostutkinnan näkökulmasta kiinnostavin näistä on erityisesti luotettavuus. Luotettavuudella tarkoitetaan järjestelmän luotettavuutta niin käyttöasteen ja käytettävyyden kannalta kuin myös turvallisuuden näkökulmasta (Post & Kagan, 2001). Tietokannan hallintajärjestelmälle on kriittisen tärkeää, ettei tietokannassa oleva data pääse korruptoitumaan, hukkumaan tai ettei tietoja päästä muuttamaan ilman asianmukaisia oikeuksia (Bertino, Catania & Ferrari, 2001). Jos ei-toivotut tahot kuitenkin pääsevät muuttamaan dataa, järjestelmän olisi hyvä olla suunniteltu ja toteutettu tukemaan myös kyseisten tapahtumien tutkintaa.

Tietokantojen ja sitä kautta tietokantojen hallintajärjestelmien kyberrikostutkintaan käytetään suurimmaksi osaksi algoritmeja. Näiden algoritmien tarkoituksena on havaita muutoksia tietokannassa ja vastata erilaisiin tutkimuksen kysymyksiin. Näitä kysymyksiä ovat esimerkiksi ”mitä”, ”missä”, ”milloin” ja ”kuka”. (Pavlou & Snodgrass, 2013.) Tietokannan täytyy olla dokumentoitu oikein ja ajantasaisesti, jotta tiedetään mitä algoritmeja voidaan käyttää ja että algoritmien tuloksia voidaan tulkita oikein. Tästä esimerkkinä, jos algoritmi paikantaa tietokannasta muunnellun datan sijainnin, täytyy dokumentoinnin perusteella kyetä tekemään johtopäätöksiä muuntelun laajuudesta. Tietokantajärjestelmän dokumentointimahdollisuuksien tärkeys korostuukin kyberrikostutkinnassa digitaalisen rikospaikan tilannekuvaa muodostettaessa.

Tärkeä ominaisuus tietokannan hallintajärjestelmälle kyberrikostutkinnan näkökulmasta on, että datan lisääminen on ”vain lisäämistä” (engl. append-only), joka tarkoittaa, että dataa lisätään eikä vanhaa dataa poisteta lisäämisen yhteydessä tai heti sen jälkeen (Pavlou & Snodgrass, 2013). Sen tarkoituksena on mahdollistaa datan vertailu. Vertailun kautta pystytään tunnistamaan datan muutokset ja muutosten kohde. Se miten vanha data säilytettään ei sinänsä ole kriittistä kyberrikostutkinnan kannalta, olettaen että vanhaan dataan päästään jotenkin käsiksi. (Ahn & Snodgrass, 1988.)

Kyberrikostutkinnan kannalta tietokannan lokit ovat tärkeässä asemassa, koska lokien kautta päästään käsiksi tärkeisiin tietoihin kyberrikostutkinnan kannalta. Näitä tietoja ovat esimerkiksi kuka on tehnyt ja mitä on tehty. Tietokannan hallintajärjestelmää kehitettäessä ja toteutettaessa on siis tärkeää varmistaa, että lokit sisältävät tarvittavan määrän informaatiota ja ovat turvallisia.

Tarpeellisia ominaisuuksia lokeille on aikaleimaus ja tunnistusmahdollisuudet. Turvallisuus on lokien kohdalla avainasemassa. Jos hyökkääjä pääsee muuntelemaan lokitietoja hyökkäyksen jälkeen, niiden arvo kyberrikostutkinnalle katoaa. Lisäksi väärennetyt lokitiedot voivat johtaa kyberrikostutkintaa harhaan. Esimerkiksi lokein yksisuuntainen salaus on tehokas keino estää luvaton muokkaaminen. Salauksia pitää valvoa, jotta tiedetään, ettei niitä olla muuteltu. (Pavlou & Snodgrass, 2013.)

Tietokantoja ja tietokannan hallintajärjestelmiä suunniteltaessa ja toteuttaessa on tärkeää huomioida kyberrikostutkinnan näkökulma ja mahdollistaminen. Tärkeimpiä tekijöitä tietokannassa ja sen hallintajärjestelmässä ovat algoritmien mahdollistaminen, dokumentointi, lokitietojen suojeleminen, lokitietojen aikaleimaus sekä vanhojen tietojen säilyttäminen.

Yhä enemmän siirretään dataa, tietokantoja, palveluja ja muita vastaavia objekteja tai mahdollisuuksia pilveen. **Pilvipalvelujen** hyötyjä ovat esimerkiksi niiden skaalautuvuus, jakamismahdollisuudet sekä käytettävyys. Pilvipalveluita käytetään yleisesti kahdella eri tavalla. Yritys voi itse pyörittää omia pilvipalveluitaan hankkimalla itsellensä kyseistä teknologiaa omaan omistukseensa tai toisena vaihtoehtona on vuokrata itsellensä esimerkiksi sovelluksia, tallennustilaa tai laskentatehoa omien tarpeidensa mukaan, mikä on paljon yleisempää. (Tamburri, Miglierina & Di Nitto, 2020.) Pilvipalveluiden yleistymisen myötä myös niihin kohdistuvat hyökkäykset ovat yleistyneet ja siksi kyberrikostutkinnan merkitys pilvessä on noussut.

Pilvessä suoritettavassa kyberrikostutkinnassa on tärkeää analysoida datan kulkua. Datan kulkua käsitellään pääasiallisesti kolmessa vaiheessa. Nämä kolme vaihetta ovat: kun data on asiakkaan laitteilla, siirtymävaiheessa sekä palveluntarjoajan laitteilla. Dataan käsiksi pääsy voi olla hankalaa kaikissa näissä vaiheissa, mutta silti olisi suotuisaa päästä käsiksi kaikkiin tai ainakin loppu ja alkupään dataan. Kyberrikostutkinnan kannalta on tärkeää kyetä todentamaan todisteiden aitous. Se onnistuu parhaiten pääsemällä käsiksi dataan riippumatta siitä, onko se asiakkaan laitteilla, liikkeessä vai palveluntarjoajan hallussa. Pilveä hyödyntävien järjestelmien olisi siis hyvä implementoida ominaisuus, joka pääsee käsiksi dataan jokaisessa vaiheessa. Yksi mahdollinen ratkaisu on luoda järjestelmään dataa käsittelevä moduuli, joka pystyy muuntamaan datan käsiteltävään muotoon kyberrikostutkinnan kannalta ja pääsemään sen liikkumisen jokaisessa vaiheessa. (Zawoad & Hasan, 2016.) Toinen mahdollinen ratkaisu on käyttää asiakkaiden laitteiden varmuuskopioita dataa vertaillessa (Zhu, Hu, Ahn & Yau, 2012). Tämä ei ole välttämättä yhtä tehokas ratkaisu, mutta sillä pystytään tekemään alku- ja loppupisteiden vertailua.

Samoin kuin tietokantojen kohdalla pilveä hyödyntävien järjestelmien kyberrikostutkinnassa lokitiedoilla on todella suuri merkitys. Pilveä hyödyntävissä järjestelmissä eroavaisuus löytyy kuitenkin lokien saatavuudessa. Lisäksi lokien kohdentaminen tiettyyn laitteeseen ja käyttäjään on myös mahdollinen ongelma, jos tietojärjestelmän kehittäjät eivät ota kyberrikostutkinta ystävällisyyttä huomioon järjestelmää suunniteltaessa ja toteutettaessa. Pilveä hyödyntäviä järjestelmiä kehitettäessä on siis tärkeää kehittää mekanismi palveluntarjoajan päähän,

jolla voidaan kohdistaa oikeat lokit vastaamaan asiakkaan päässä kyberrikostutkintaan liittyviä koneita. Lisäksi mekanismin olisi hyvä päästä käsiksi kaikkiin lokeihin, jotta sen kautta saataisiin mahdollisimman hyvä kokonaiskuva. Tämä parantaisi pilveä hyödyntävien järjestelmien tehokkuutta merkittävästi. (Irfan, Abbas, Sun, Sajid & Pasha, 2016.) Lokeista puhuttaessa on huomioitava myös, mitä lokien kuuluisi sisältää. Manral, Somani, Choo, Conti ja Gaur (2019) esittävät, että lokien kuuluisi sisältää tietoa sekä ohjelmistoista että laitteistosta tietoja. Etenkin pilveä hyödyntävissä järjestelmissä tämä on tärkeää, jotta lokeja pystytään kohdistamaan tarkemmin ja tehokkaammin, mikä taas helpottaa digitaalisen rikospaikan tapahtumien selvittämistä. Lokien on tärkeää olla salattuja, koska kuten aiemmin mainittiin, lokit liikkuvat palvelun käyttäjän laitteilta palveluntarjoajalle, jolloin ne ovat alttiita rikoksentekijän vastatoimille. Yksi ehdotettu ratkaisu tähän on lohkoketjuteknologian käyttö, joka varmistaisi lokien turvallisuuden. (Manral, ym., 2019.)

Pilvipalveluita ja pilveä hyödyntäviä järjestelmiä voidaan tutkia kahdella tapaa: ”elossa” ja ”kuolleina”. Tällä tarkoitetaan sitä, onko järjestelmä vielä samassa tilassa kuin hyökkäyksen tapahtuessa eli ”elossa” vai ei. Pilveä hyödyntävissä järjestelmissä tämän merkitys korostuu, koska järjestelmä, joka on vielä elossa on paljon helpompi tutkia kuin etsiä ”kuollut” järjestelmä ja selvittää sen tila. ”Elossa” tutkiminen ei kuitenkaan ole aina mahdollista erinäisistä syistä kuten esimerkiksi, jos hyökkäys havaitaan jälkikäteen. Tästä syystä järjestelmissä olisi tärkeää kyberrikostutkinnan näkökulmasta olla mahdollisuus palauttaa palvelu, muisti tai virtuaalitietokone tiettyyn aikaisempaan tilaan. (Freet, Agrawal, John & Walker, 2015.) Tämä ei ole kuitenkaan käytännössä tehokkaasti toteutettavissa, koska jokaista ajan hetkeä ei voida varmuuskopioida. Yksi mahdollinen ratkaisu on kuitenkin säilyttää esimerkiksi virtuaalisten koneiden aloitus- ja lopetustiloja varmuuskopioituna, jolloin kyseisiä kopioita voitaisiin käyttää vertailua varten kyberrikostutkinnassa.

Pilvipohjaisissa ja pilveä hyödyntävissä järjestelmissä voidaan ottaa huomioon digitaalinen kyberrikostutkinta monella tapaa. Lokitietojen turvallinen säilöminen nousee myös pilviratkaisuissa avain asemaan. Lisäksi lokitietoihin on hyvä päästä käsiksi vähintään asiakkaan ja palveluntarjoajan päädyissä ja jos mahdollista, myös siirtymävaiheessa. Pilvipalveluiden erilaisten tilojen varmuuskopiot ja tallentaminen on kyberrikostutkinnan kannalta tärkeää. Tämä antaa vertailukohtia palveluille ja mahdollistaa digitaalisen kyberrikospaikan tilannekuvan muodostamisen.

Tietoverkot ovat olennainen osa tietojärjestelmiä ja ne ovat tärkeitä yksilöille ja organisaatioille. Langattomista yhteyksistä ja suoratoistopalveluista on tullut osa ihmisten arkea. Lisäksi tietoverkot ovat laajalti käytössä yritysmaailmassa esimerkiksi yrityksen sisäisessä kommunikaatiossa. Tietoverkot ovat houkutteleva kohde rikollisuudelle, koska niiden kautta voidaan päästä käsiksi esimerkiksi yksityishenkilön tietoihin tai yritysten järjestelmiin ja tietoihin käsiksi (Bartoli, Medvet, De Lorenzo & Tarlao, 2019). Tietoverkkojen digitaalinen tutkinta koostuu pääosin neljästä vaiheesta. Ensimmäinen vaihe on tunnistaa epätavallinen liikenne verkossa. Tähän liittyy esimerkiksi avointen porttien

skannaamista. Toisessa vaiheessa etsitään varoituksia tai hälytyksiä. Seuraavaksi sessioiden data muutetaan analysoitavaan muotoon ja analysoidaan. Viimeiseksi pakettien data analysoidaan. (Merkle, 2008.)

Tunkeilijan havaitsemisjärjestelmät (engl. Intrusion Detection System (IDS)) ovat tietoverkkojen kyberrikostutkinnan kannalta erittäin tärkeitä. Tunkeilijan havaitsemisjärjestelmän tarkoituksena on valvoa tietoverkkoja ja siihen yhdistettyjä laitteita, jotta voitaisiin huomata verkkoon tunkeutuminen tai haitallinen toiminta (Leite & Girardi, 2017). Tietojärjestelmien kehittämisessä tunkeilijan havaitsemisjärjestelmien sisällyttäminen järjestelmään lisää sen kyberrikostutkinta ystävällisyyttä. Etenkin uuden sukupolven tunkeilijan havaitsemisjärjestelmät, joissa käytetään esimerkiksi tekoälyn syväoppimista tai tiedonlouhintaa ovat tehokkaita ottaen huomioon nykyisten tietoverkkojen koon ja liikenteen määrän. Syväoppimisella tunkeilijan havaitsemisjärjestelmissä voidaan vähentää väärien hälytysten määrää sekä parantaa havaitsemistehokkuutta (Buczak & Guven, 2015). Myös tiedonlouhintaa hyödyntämällä pystytään saamaan tarkempia tuloksia, ja se on lisäksi vielä selkeästi parempi käsittelemään suuri määriä dataa (Pan, Morris & Adhikari, 2015).

Joissain tietoverkoissa käytetään pakettien datan luokittelujärjestelmiä (engl. Payload Attribute System (PAS)). Niiden tarkoituksena on tallentaa verkossa kulkeneen paketin datakuorma ja mahdollistaa niiden vertailu. Tähän on kehitetty erilaisia ratkaisuja, koska kaikkien verkossa kulkeneiden pakettien kopiointi olisi todella epäkäytännöllistä esimerkiksi tallennustilasta johtuvista syistä. Ensimmäisiä ratkaisuja oli käyttää hajautusalgoritmeja, joiden avulla voitiin tunnistaa pakettien dataa, mutta se oli kuitenkin vielä suhteellisen tilaa vievää. Lisäksi hajautusalgoritmien käyttö toi väärien tulosten mahdollisuuden. Bloom-suodattimet lisäsivät kyseisen teknologian tilatehokkuutta, mutta mitä pienempään tilaan tieto saatiin puristettua, sitä enemmän väärien tulosten riski kasvoi. Nykyään on kehitetty parempia ratkaisuja kuten hierarkkinen Bloom-suodatin, joka pystyy tehokkaampaan suorittamiseen pienemmällä virhemarginaalilla. (Wang & Daniels, 2008.)

Tietoverkoissa tunkeilijoiden havaitsemisjärjestelmän käyttö on todella tärkeää digitaalisen kyberrikostutkinnan kannalta. Se antaa kyberrikostutkinnalle mahdollisuuksia toimia nopeammin ja antaa tarvittavia tietoja itse tutkintaan. Toinen tärkeä elementti tietoverkoissa kyberrikostutkinnan näkökulmasta on pakettien datan luokittelujärjestelmät. Niiden avulla pystytään tutkimaan, minkälaista dataa verkossa on liikkunut. Lokitietojen säilyttäminen on tärkeää myös tietoverkkoja suunniteltaessa ja toteuttaessa. Niillä on tietoverkoissa samanlainen tehtävä kuin aiemmin mainituissa tietojärjestelmissä tai niiden osissa.

4.2 Tietojärjestelmien rikostutkinnan haasteet

Kyberrikostutkinta kohtaa uusia haasteita kyberrikollisuuden kehittyessä ja teknologian monimutkaistuessa koko ajan enemmän. Haasteita kohdataan niin tietojärjestelmien ominaisuuksien kuin myös niiden ihmisrajapinnan kanssa. Tämän kohdan tarkoituksena onkin tutkia, minkälaisia haasteita kyberrikostutkinnassa kohdataan. Havaitut ongelmat eivät välttämättä ole järjestelmätyyppi tai osa kohtaisia, vaan niitä voidaan soveltaa muihinkin tietojärjestelmien osa-alueisiin.

Ihmisten kanssa toimittaessa voidaan yleisesti kohdata haasteita johtuen joko tietämättömyydestä tai välinpitämättömyydestä. Esimerkiksi saastuneen tietokoneen omistaja saattaa tuhota todistusaineistoa tai muuten haitata tutkijoiden toimintaa ennen kuin tutkijat pääsevät laitteeseen käsiksi. Lisäksi tutkintaa suorittaessa, jos laitteen omistajan tai vastaavan toimijan kanssa halutaan tehdä yhteistyötä, kannattaa se tehdä tutkinnan ensimmäisten kolmen viikon aikana. Tämä johtuu siitä, että kyseisten toimijoiden mielenkiinto tutkintaan alkaa loppumaan kolmen viikon jälkeen. Tutkijat ovat alkaneet kutsua tätä ilmiötä nimellä ”kultaiset viikot”, joilla viitataan kyseisiin ensimmäisiin kolmeen viikkoon. (Leibolt, 2010.)

Toinen haaste on kyberrikostutkinnan työkalujen kehittäminen. Työkaluihin liittyy kahdenlaisia ongelmia. Toinen niistä on työkalujen riittämätön kehittyminen. Al Fahdin, Clarken ja Furnellin (2013) mukaan useimpien kyberrikostutkijoiden mielestä kyberrikostutkinnan työkalut eivät vastaa täysin heidän tarpeitaan. Haasteita nousee esiin esimerkiksi erilaisten alustojen, kuten pilvipohjaisten järjestelmien yhteensopivuuden kanssa (Manral, ym., 2019). Tämä johtuu osakseen siitä, että työkalujen täytyisi pystyä havaitsemaan pienimmätkin muutokset laitteissa, sillä hakkerit kehittyvät koko ajan omien jälkiensä peittelyssä. Toinen ongelmista on työkalujen skaalautuvuus. Hyökkäykset eivät enää rajoitu vain yhteen laitteeseen tai verkkoon, mikä vuorostaan vaatii työkaluilta enemmän (Roussev, 2011).

Yksi koko ajan kehittyvistä haasteista kyberrikostutkinnassa on digitaalisen rikostutkinnan vastatoimet, joilla tarkoitetaan kyberrikollisten toimia, joilla pyritään vaikeuttamaan tutkinnan toteuttamista (Kessler, 2007). Näitä toimia ovat muun muassa: datan piilottaminen tai salaus, datan, lokien tai vastaavien tiedostojen poistaminen, suorat hyökkäykset digitaalisia työkaluja vastaan ja tekaistujen jälkien jättäminen (Conlan, Baggili & Breitinger, 2016). Yksi esimerkki tästä on digitaalisten todisteiden varmentamisessa käytettävän elektronisen verkon taajuussignaalin muokkaaminen. Kyseisellä signaalilla pyritään varmentamaan digitaalisten todisteiden aitoutta ja tapahtuma-aikaa. Kyseinen signaali on kuitenkin todistetusti pystytty väärentämään aidon näköiseksi, mikä on ongelma kyberrikostutkinnalle. (Chuang, Garg & Wu, 2013.)

Tietokannoissa haasteena on, jos salaus ei ole yksisuuntaista, voi tunkeutuja päästä käsiksi dataan järjestelmän huomaamatta, koska tunkeutuja voi silloin manipuloida salauksia ja peittää omat jälkensä. Lisäksi huono

tietokantajärjestelmän suunnittelu voi tuottaa haasteita järjestelmän kyberrikostutkinnalle. Esimerkiksi, jos tietokannan hallintajärjestelmä poistaa vanhan datan arvoja muutettaessa, algoritmien käyttö rajoittuu huomattavasti, mikä vaikeuttaa tutkintaa entisestään. Itse algoritmeissa on myös omat haasteensa. Riippuen algoritmista ne tasapainottelevat tulosten tehokkuuden ja resurssitarpeen kanssa. ”Yksiväriset algoritmit” (engl. Monochromatic algorithm), joita käytetään korruptoituneen datan paikantamiseksi, ovat nopeampia kuin esimerkiksi a3D algoritmi, mutta ne eivät aina pääse tarpeeksi tarkkoihin tuloksiin. A3D algoritmi taas toisaalta vaatii enemmän laskentatehoa, mutta pääsee tarkempaan lopputulemaan. Laskentatehon määrä on muutenkin noussut ongelmaksi yhä suurempien tietokantojen myötä. (Pavlou & Snodgrass, 2013.) Laskentatehon tarpeeseen voidaan kuitenkin vastata esimerkiksi käyttämällä pilvestä vuokrattavaa laskentatehoa, mutta se ei ole pitkällä aikavälillä kestävä ratkaisu.

Pilvipalveluihin tai pilveä hyödyntäviin järjestelmiin liittyvät rikokset ovat vaikeita käsitellä tapauskohtaisesti, koska pilviteknologia ei välttämättä ole vain yhden henkilön käytettävissä, mikä vaikeuttaa huomattavasti yhtä kyberrikostutkinnan vaihetta eli digitaalisen rikospaikan määrittämistä. Pilviteknologiassa mahdollisesti laitteiden konfiguraatiot ovat erilaisia eri käyttäjillä, mikä myös vaikeuttaa kyberrikostutkinnan työkalujen käyttöä ja digitaalisen rikospaikan tilannekuvan muodostamista. Lisäksi kyseisissä järjestelmissä silkka datan määrä aiheuttaa kyberrikostutkinnalle ongelmia. Paljon käytössä oleva palvelu tai virtuaalinen tietokone saattaa tuottaa valtavia määriä dataa rikostutkintaan, josta suurin osa ei välttämättä liity kyseiseen tutkintaan millään tavalla. Pilvipalveluissa tai pilveä hyödyntävissä järjestelmissä on yleensä lähes mahdotonta saada fyysisiä laitteita tarkasteluun, sillä ne saattavat sijaita ympäri maailmaa. Samasta syystä lakitekniset asiat voivat muodostua ongelmaksi, koska eri maissa on erilaisia lainsäädäntöjä rikostutkinnan osalta. Lisäksi laitteiden on tärkeää saada jatkaa toimintaansa palveluntarjoajan näkökulmasta. (Simou, Kallonatis, Gritzalis & Mouratidis, 2016.) Lisäksi pilveä hyödyntävien järjestelmien data saattaa olla epävakaampaa kuin niissä, jotka eivät hyödynnä pilveä. Esimerkiksi virtuaalisten tietokoneiden muisti ja tilannekuvat ovat vaikeasti käsiteltävissä ja niissä saattaa olla suurempi korruptoitumisen riski. (Manral, ym., 2019.)

Tietoverkkojen kyberrikostutkinnassa tuli vahvasti esille tunkeilijan havaitsemisjärjestelmien tärkeys. Näillä järjestelmillä on myös omat haasteensa. Ensinnäkin useimmat tunkeilijan havaitsemisjärjestelmät ovat automatisoitu niin, että ne tunnistavat pääosin vain jo tunnetut hyökkäykset. Toinen ongelma tunkeilijan havaitsemisjärjestelmissä on niiden ylikuormittaminen. Jos hyökkääjä on tunnistanut heikon tunkeilijan havaitsemisjärjestelmän, hyökkääjä voi käyttää sitä hyväkseen esimerkiksi aiheuttamalla valtavan määrän hälytyksiä. Tämä aiheuttaa sekaannusta ja vähentää järjestelmän antamien hälytysten ja datan merkitsevyyttä. (Werlinger, Hawkey, Muldner, Jaferian & Beznosov, 2008.) Lisäksi oikeiden hälytysten erottelu tahallaan aiheutetuista vaatii paljon resursseja. Tunkeilijan havaitsemisjärjestelmät vaativat myös paljon resursseja. Ne kustantavat suhteellisen paljon ja vaativat henkilöstöä valvomaan ja konfiguroimaan niitä (Werlinger, ym., 2008).

5 YHTEENVETO

Tässä tutkielmassa tarkasteltiin kyberrikollisuutta, sen tutkintaa ja tietojärjestelmien ominaisuuksia, jotka vaikuttavat kyberrikostutkintaan. Tutkielman tarkoituksena oli kartoittaa, kuinka paljon ja minkälaista tutkimusta kyberrikostutkinnasta tietojärjestelmien näkökulmasta on tehty. Tutkielman tutkimuskysymykset olivat:

1. Millainen on kyberrikosten tutkinnan prosessi?
2. Mitkä tekijät tietojärjestelmissä vaikuttavat kyberrikostutkintaan?

Tutkielmassa huomattiin, että kyberrikollisuus on lisääntynyt vuosi vuodelta lähes koko 2000-luvun ja se näkyy yhä enemmän myös yksilöiden arjessa. Erilaiset kyberrikollisuuden muodot, kuten esimerkiksi kiristyshaittaohjelmien käyttö on yleistynyt, ja ne ovat aiheuttaneet yrityksille ongelmia, esimerkiksi tiedon menetykseen ja talouteen liittyen. Erilaisia kyberrikollisuuden muotoja löydettiin paljon. Palvelunestohyökkäykset, haittaohjelmat, immateriaalioikeuksien väärinkäyttö ja liikesalaisuuksien havittelu ovat olleet yleisiä kyberrikollisuuden muotoja. Tutkielmassa löydettiin kyberrikoksille viisiosainen kategorisointi vaihtoehtona yksinkertaisempaan perinteisiin ja ei-perinteisiin kyberrikoksiin jaottelulle. Lisäksi tutkielmassa käytiin läpi erilaisia hakkereita ja todettiin, etteivät kaikki hakkerit tee kyberrikoksia, vaan myös ehkäisevät niitä. Lisäksi kyberrikollisuus aiheuttaa taloudellisesti merkittäviä vahinkoja, jonka takia kyberrikostutkinnan merkitys korostuu entisestään. Tästä löydettiin esimerkkitapaus WannaCry-viruksesta, joka havainnollisti yhtä kyberrikollisuuden tapaa nykypäivänä.

Toisessa sisältöluvussa tarkasteltiin kyberrikostutkintaa, sen suorittamiseen erilaisia malleja sekä kyberrikostutkinnan haasteita. Kyberrikostutkinnan historiasta tärkein löydös oli 2000-luvun alun kyberrikollisuuden nousu. Kyberrikokset yleistyivät merkittävästi ja sen takia myös kyberrikostutkinnan kysyntä kasvoi. Tämä pakotti kyberrikostutkinnan kehittymään niin lakitoimijoiden puolella kuin tieteellisellä saralla. Yleistymisen myötä alettiin kehittämään erilaisia malleja kyberrikostutkinnan prosessille. Tutkielmassa käsiteltiin viittä erilaista

mallia, joista neljä on 2000-luvulla esiteltyjä. Näiden mallien vertailussa huomattiin mallien ratkaisevan eri ongelmia. Ongelmat ovat osaksi sidonnaisia oman aikansa tarpeisiin, esimerkiksi DFMMIP:n tapauksessa ongelmana oli todisteiden käsittelyketjun eheyden varmistaminen. Kokoavana mallina toimi GCFIM, joka esitti monista eri malleista yleisimmät vaiheet ja loi täten yleispätevää kuvaa kyberrikostutkinnan prosessista. Toinen sisältöluku vastasi tutkielman ensimmäiseen tutkimuskysymykseen.

Kolmannessa sisältöluvussa tutkittiin, mitä asioita kuuluisi ottaa tietojärjestelmien kehittämisessä ja toteutuksessa huomioon kyberrikostutkinnan kannalta. Merkittävin yksittäinen tekijä oli lokitietojen oikea käsittely ja sisältö. Lokitiedoilla pystytään muodostaa kuvaa mahdollisista rikoksista, missä ne ovat tapahtuneet, milloin ne ovat tapahtuneet ja kuka ne on tehnyt. Lisäksi kyseisten tietojen oikea käsittely, salaus ja varmentaminen ovat avainasemassa. Tietojärjestelmien kyberrikostutkinnassa koetaan myös haasteita, ja havaittiin myös ratkaisut, joilla pyritään helpottamaan kyberrikostutkintaa kohtaavat erilaisia haasteita.

Tutkielma auttaa hahmottamaan, mitä tekijöitä olisi hyvä ottaa huomioon tietojärjestelmissä, jotta niiden kyberrikostutkinta olisi tehokkaampaa. Lisäksi tutkielma auttaa ymmärtämään kyberrikostutkinnan prosessia, jonka kautta järjestelmien kehittäjät ja ylläpitäjät voivat kehittää ratkaisuja paremmin omiin järjestelmiinsä. Tutkielma myös käy läpi kyberrikollisuutta ja pyrkii lisäämään tietoisuutta siitä.

Tutkielmassa pyrittiin käyttämään mahdollisimman ajantasaista lähdemateriaalia kohdissa, joissa se oli relevanttia. Kyberrikostutkinnasta ei ole tehty paljoa tieteellistä tutkimusta verrattuna esimerkiksi esineiden internettiin tai vastaaviin aihepiireihin, joten lähdemateriaali oli kuitenkin hieman rajoittunutta. Varsinkin lähteiden, joihin on viitattu useita kertoja, löytäminen tuotti haasteita.

Mahdollisia jatkotutkimusaiheita kyberrikollisuuteen ja sen tutkintaan on useita. Tämän kirjallisuuskatsauksen pohjalta lisää tutkimusta olisi hyvä tehdä esimerkiksi siitä, kuinka paljon kyberrikostutkintaa otetaan huomioon tietojärjestelmiä kehittäessä ja kuinka paljon kyberrikostutkinnan onnistumiseen vaikuttaa tietojärjestelmien kyberrikostutkintaystävällisyys.

LÄHTEET

Ahn, I., & Snodgrass, R. (1988). Partitioned storage for temporal databases. Information Systems, 13(4), 369-391.

Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013, August). Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In 2013 Information Security for South Africa (pp. 1-8). IEEE.

Bartoli, A., Medvet, E., De Lorenzo, A., & Tarlao, F. (2019). Enterprise wi-fi: we need devices that are secure by default. Communications of the ACM, 62(5), 33-35.

Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. Digital Investigation.

Bayuk, J. (2010). Introduciton. Teoksessa Bayuk, J. (toim.), CyberForensics: Understanding Information Security Investigations. Springer Science & Business Media.

Bertino, E., Catania, B., & Ferrari, E. (2001). A nested transaction model for multilevel secure database management systems. ACM Transactions on Information and System Security (TISSEC), 4(4), 321-370.

Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. International Journal of digital evidence, 2(2), 1-20.

Casey, E. (2009). Handbook of digital forensics and investigation. Academic Press.

Chuang, W. H., Garg, R., & Wu, M. (2013). Anti-forensics and countermeasures of electrical network frequency analysis. IEEE transactions on information forensics and security, 8(12), 2073-2088.

Clarke, R. & Knake, R. (2014). Cyber War. Harper Collins Publisher, New York.

Clough, J. (2011). Cybercrime, Commonwealth Law Bulletin, 37:4, 671-680, DOI: 10.1080/03050718.2011.621277

Clough, J. (2015). Principles of Cybercrime. Cambridge University Press.

Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital investigation, 18, S66-S75.

Dittrich, K. R., Gatziu, S., & Geppert, A. (1995, September). The active database management system manifesto: A rulebase of ADBMS features. In International Workshop on Rules in Database Systems (pp. 1-17). Springer, Berlin, Heidelberg.

Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service.

EUCPN (2015). Cybercrime: a theoretical overview of the growing digital threat. EUCPN Theoretical Paper Series, European Crime Prevention Network: Brussels.

Europol. (2017). IOCTA 2017. Haettu osoitteesta https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Europol. (2019). IOCTA 2019. Haettu osoitteesta https://www.europol.europa.eu/iocta-report

Federal Bureau of Investigation (FBI). (2019). 2019 Internet Crime Report. Haettu osoitteesta https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

Folsom, T. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). Tulane Journal of Technology and Intellectual Property 75.

Forbes. (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Haettu osoitteesta https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#56c83fdf3a91

Fourkas, V. (2004). What is cyberspace?. Spatial Development Research Unit, Department of Urban and Regional Planning and Development, Aristotle University of Thessalonica.

Gayed, T. F., Lounis, H., Bari, M., & Nicolas, R. (2013). Cyber forensics: representing and managing tangible chain of custody using the linked data principles. In The international conference on Advanced Cognitive technologies and Application (IARIA 2013) (pp. 87-96).

Gold, S. (2011). The rebirth of phreaking. Network security, 2011(6), 15-17.

Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. California Law Review, 100(4), 817-885. Retrieved June 30, 2020, from www.jstor.org/stable/23249823.

Hjertström, A., Nyström, D., & Sjödin, M. (2012). Data management for component-based embedded real-time systems: The database proxy approach. Journal of Systems and Software, 85(4), 821-834.

Hyman, P. (2013). Cybercrime: it's serious, but exactly how serious?. Communications of the ACM, 56(3), 18-20.

Irfan, M., Abbas, H., Sun, Y., Sajid, A., & Pasha, M. (2016). A framework for cloud forensics evidence collection and analysis using security information and event management. Security and Communication Networks, 9(16), 3790-3807.

Jämsén, C. (2018). Kyberrikollisuuden tilannekuva ja ajankohtaiset ilmiöt. Keskusrikospoliisi, Kyberrikostorjuntakeskus.

Kessler, G. C. (2007). Anti-forensics and the digital investigator.

Kierkegaard, S. (2005). Cracking Down On Cybercrime Global Response: The Cybercrime Convention. Communications of the IIMA: Vol. 5.

Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. Journal in computer virology, 6(2), 105-114.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22:2, 77-81.

Ku, R. S. R. (2002). The creative destruction of copyright: Napster and the new economics of digital technology. The University of Chicago Law Review, 263-324.

Leibolt, G. (2010). Teoksessa Bayuk, J. (toim.), CyberForensics: Understanding Information Security Investigations. Springer Science & Business Media.

Leite, A., & Girardi, R. (2017). A hybrid and learning agent architecture for network intrusion detection. Journal of Systems and Software, 130, 59-80.

Li, B., Erdin, E., Gunes, M. H., Bebis, G., & Shipley, T. (2013). An overview of anonymity technology usage. Computer Communications, 36(12), 1269-1283.

Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND corporation.

Löser, A., Wolpers, M., Siberski, W., & Nejdl, W. (2003). Efficient data store discovery in a scientific P2P network. In Proc. of the WS on Semantic Web Technologies for Searching and Retrieving Scientific Data, CEUR WS (Vol. 83).

Manky, D. (2013). Cybercrime as a service: a very modern business. Computer Fraud & Security, 2013(6), 9-13.

Manral, B., Somani, G., Choo, K. K. R., Conti, M., & Gaur, M. S. (2019). A systematic survey on cloud forensics challenges, solutions, and future directions. ACM Computing Surveys (CSUR), 52(6), 1-38.

McCarthy, D., & Dayal, U. (1989). The architecture of an active database management system. ACM Sigmod Record, 18(2), 215-224.

McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008, July). Shining light in dark places: Understanding the Tor network. In International symposium on privacy enhancing technologies symposium (pp. 63-76). Springer, Berlin, Heidelberg.

McKemmish, R. (1999). What is forensic computing? (pp. 1-6). Canberra: Australian Institute of Criminology.

Merkle, Laurence D. "Automated network forensics." Proceedings of the 10th annual conference companion on Genetic and evolutionary computation. 2008.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5).

Moir, R. (2009). Defining Malware, technet.microsoft.com. Haettu 7/2020

Morgan, S. (2017). Cybercrime report, 2017.

Narwal, B., & Goel, N. (2020). A Walkthrough of Digital Forensics and its Tools.

Palmer, G. L. (2002). Forensic analysis in the digital world. International Journal of Digital Evidence, 1(1), 1-6.

Pan, S., Morris, T., & Adhikari, U. (2015). Developing a hybrid intrusion detection system using data mining for power systems. IEEE Transactions on Smart Grid, 6(6), 3104-3113.t

Park, H., Cho, S., & Kwon, H. C. (2009, January). Cyber forensics ontology for cyber criminal investigation. In International Conference on Forensics in Telecommunications, Information, and Multimedia (pp. 160-165). Springer, Berlin, Heidelberg.

Pavlou, K. E., & Snodgrass, R. T. (2013). Generalizing database forensics. ACM Transactions on Database Systems (TODS), 38(2), 1-43.

Perumal, S. (2009). Digital forensic model based on Malaysian investigation process. International Journal of Computer Science and Network Security, 9(8), 38-44.

Phan, T. V., & Park, M. (2019). Efficient distributed denial-of-service attack defense in SDN-based cloud. IEEE Access, 7, 18701-18714.

Pollitt, M. (1995). Computer Forensics: an Approach to Evidence in Cyberspace (pp 487-491). National Information Systems Security Conference, Baltimore.

Pollitt, M. (2010, January). A history of digital forensics. In IFIP International Conference on Digital Forensics (pp. 3-15). Springer, Berlin, Heidelberg.

Ponec, M., Giura, P., Wein, J., & Brönnimann, H. (2010). New payload attribution methods for network forensic investigations. ACM Transactions on Information and System Security (TISSEC), 13(2), 1-32.

Post, G., & Kagan, A. (2001). Database management systems: design considerations and attribute facilities. Journal of Systems and Software, 56(2), 183-193.

Primiero, G., Solheim, F. J., & Spring, J. M. (2019). On malfunction, mechanisms and malware classification. Philosophy & Technology, 32(2), 339-362.

Robertson, B., Vignaux, G. A., & Berger, C. E. (2016). Interpreting evidence: evaluating forensic science in the courtroom. John Wiley & Sons.

Roussev, V. (2011, May). Building open and scalable digital forensic tools. In 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (pp. 1-6). IEEE.

Sammes, T., & Jenkinson, B. (2007). Forensic computing (pp. 1-6). Springer London.

Sarga, L., & Jasek, R. (2011, July). Distributed Denial of Service Attacks as Threat Vectors to Economic Infrastructure: Motives, Estimated Losses and Defense Against the HTTP/1.1 GET and SYN Floods Nightmares. In European Conference on Cyber Warfare and Security (p. 228). Academic Conferences International Limited.

Satti, R. S., & Jafari, F. (2015). Reviewing existing forensic models to propose a cyber forensic investigation process model for higher educational institutes. International Journal of Computer Network and Information Security, 7(5), 16.

Schjolberg, S. (2008). The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva. Journal of international commercial law and technology.

Schjolberg, S. (2014). The History of Cybercrime. Books on Demand.

Simou, S., Kalloniatis, C., Gritzalis, S., & Mouratidis, H. (2016). A survey on cloud forensics challenges and solutions. Security and Communication Networks, 9(18), 6285-6314.

Staff, C. A. C. M. (2013). Plenty more hacker motivations. Communications of the ACM, 56(7), 8-9.

Tamburri, D. A., Miglierina, M., & Di Nitto, E. (2020). Cloud applications monitoring: An industrial study. Information and Software Technology, 127, 106376.

The Verge. (2020). Amazon says it mitigated the largest DDoS attack ever recorded. Haettu osoitteesta https://www.theverge.com/2020/6/18/21295337/amazon-aws-biggest-ddos-attack-ever-2-3-tbps-shield-github-netscout-arbor

Varonis. (2020). Must-Know Cybersecurity Statistics for 2020. Haettu osoitteesta https://www.varonis.com/blog/cybersecurity-statistics/

Vice. (2017). The Dark Web Gun Trade May Be Bigger Than You Think. Haettu osoitteesta https://www.vice.com/en_us/article/j5qnbg/dark-web-gun-trade-study-rand

Wang, W., & Daniels, T. E. (2008). A graph based approach toward network forensics analysis. ACM Transactions on Information and System Security (TISSEC), 12(1), 1-33.

Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P., & Beznosov, K. (2008, July). The challenges of using an intrusion detection system: is it worth the effort?. In Proceedings of the 4th symposium on Usable privacy and security (pp. 107-118).

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. Communications of the ACM, 56(4), 64-74.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common phases of computer forensics investigation models. International Journal of Computer Science & Information Technology, 3(3), 17-31.

Zawoad, S., & Hasan, R. (2016). Trustworthy digital forensics in the cloud. Computer, 49(3), 78-81.

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cyber crimes. Security and Communication Networks, 5(4), 422-437.

Zhu, Y., Hu, H., Ahn, G. J., & Yau, S. S. (2012). Efficient audit service outsourcing for data integrity in clouds. Journal of Systems and Software, 85(5), 1083-1095.