KYBERRIKOKSET

Kirjaaminen ja alkutoimet tietotekniikkarikoksissa

Ari Anttila

5/2018

POLIISIAMMATTIKORKEAKOULUN OPINNÄYTETYÖ / AMK

Tiivistelmä

<table>
<tr><td>Tekijä

Ari Anttila</td><td colspan="3">Tutkinto/kurssi ja opinnäytetyö/nimike

Poliisi (AMK)/AMK20161</td></tr>
<tr><td>Julkaisun nimi

Kyberrikokset
-Kirjaaminen ja alkutoimet tietotekniikkarikoksissa</td><td colspan="3">Julkisuusaste

Osittain salassa pidettävä

Liite 1 ja liite 2 salassa pidettäviä</td></tr>
<tr><td>Ohjaajat ja opintoaine/opetustiimi

Satu Rantaeskola, yliopettaja, VT
Lauri Haapaniemi, ylikomisario</td><td colspan="3">Opinnäytetyön muoto

Toiminnallinen opinnäytetyö</td></tr>
<tr><td colspan="4">Tiivistelmä

Kyberrikollisuuden ilmiöt ja sen tutkinnassa sovellettava lainsäädäntö ovat ajankohtaisia tutkimuskohteita. Kyberrikollisuuden tilannekuvaraportteja laaditaan yksityisen sektorin tietoturva-alan toimijoiden ja turvallisuusviranomaisten toimesta. Kansainvälisten tilannekuvaraporttien vertailu on keskeisessä asemassa Suomen kyberrikollisuuden tilannekuvan muodostamisessa.

Kyberrikoksia koskevat rikosilmoitukset kirjataan Poliisiasiain tietojärjestelmään. Kyberrikoksia koskevien rikosilmoitusten kirjaamisessa tulee noudattaa käytäntöjä, joilla pitkäkestoinen ja vaativa rikostutkinta voidaan turvata. Kirjausohjeen tavoitteena on tehostaa ja yhdenmukaistaa tietotekniikkarikoksia koskevien rikosilmoitusten kirjaamisessa käytettyjä menetelmiä.

Opinnäytetyön produktina valmistui ohje tietotekniikkarikosten kirjaamisesta ja alkutoimista. Ohjeen sisältö on laadittu yhteistyössä Keskusrikospoliisin kyberkeskuksen rikostutkijoiden kanssa. Kirjausohjeen rakenteen suunnittelussa huomioitiin sen käytettävyys, selkeys ja tiivis asiasisältö. Kirjausohje on kenen tahansa rikosilmoituksia kirjaavan henkilön käytettävissä.</td></tr>
<tr><td>Sivumäärä

42 + Liite 1 ja Liite 2</td><td>Tarkastuskuukausi ja vuosi

Toukokuu 2018</td><td colspan="2">Opinnäytetyökoodi (OPS)

Amk2016ONT</td></tr>
<tr><td colspan="4">Avainsanat

Kyberrikollisuus, tietotekniikkarikokset, PATJA, ohjeet, kirjaaminen</td></tr>
</table>

SISÄLLYS

1 JOHDANTO

Tietokoneet ja tietoverkot tuovat kyberrikostutkintaan erityispiirteitä, jotka tulee huomioida rikosilmoituksen kirjaamisen ja alkutoimien yhteydessä. Kyberrikosten kirjaamisessa noudatetaan kuitenkin yleisiltä osin samoja käytäntöjä, kuin muissakin rikostyypeissä. Poliisille säädettyjä tehtäviä (Poliisilaki 1:1) koskevien tietojen kirjaamisesta poliisiasiain tietojärjestelmään (PATJA) on ohjeistettu valtakunnallisesti Poliisihallituksen sisäisellä ohjeella. PATJA-ohjeen tavoitteena on yhdenmukaistaa poliisimiesten tekemien kirjausten yhdenmukaisuutta, laatua ja ajantasaisuutta. Nämä ovat poliisin tutkintatoimien oikeellisuuden ja asianosaisten sekä poliisin oman oikeusturvan kannalta tärkeitä tekijöitä. Yhdenmukaiset, laadukkaat ja ajantasaiset kirjaukset rakentavat myös luotettavan pohjan poliisin sarjoittamis- ja analyysitoiminnalle sekä julkiselle tilastotoiminnalle. Rikosilmoituksen vastaanottamisen yhteydessä tehdyt alkutoimet varmistavat laadukkaan esitutkinnan, jossa esitutkintaprosessin eri vaiheissa työskentelevien henkilöiden työpanos voidaan kohdistaa tehokkaasti ja tarkoituksen mukaisesti. Opinnäytetyössä käsitellään poliisin teknisiä ja taktisia menetelmiä. Tästä johtuen opinnäytetyö on osittain salassa pidettävä.

Opinnäytetyön yleisessä osassa käsitellään kyberrikoksia ja sen ilmiöitä. Tietoturva-alalla toimivat yritykset ja kyberturvallisuudesta vastaavat viranomaiset ylläpitävät kyberympäristöstä tilannekuvaa seuraamalla kyberrikosten kehitystä. Opinnäytetyössä käsitellyt kyberrikokset, niihin liittyvät ilmiöt ja tilannekuvaraportit luovat perustan kyberrikollisuuden ymmärtämiselle.

1.1 Työn tavoitteet

Opinnäytetyöni on toiminnallinen kehitystyö, jossa laaditaan PATJA-kirjausohjeen menettelyjä noudattava ohje kyber- eli tietotekniikkarikosten kirjaamiseksi poliisiasian tietojärjestelmään. Kirjausohje koskee vain rikosilmoituksia eikä sen ole tarkoitus esittää uusia tai PATJA-ohjeesta poikkeavia menetelmiä. Nykyisessä Poliisihallituksen PATJA-ohjeessa kyberrikoksista käytetään termiä tietotekniikkarikos. PATJA-tietojärjestelmässä valittavissa olevien rikosten luokittelukoodistossa käytetään myös termiä tietotekniikkarikos. Selkeyden vuoksi opinnäytetyön produktina syntyneessä kirjausohjeessa käytetään termin kyberrikos sijasta termiä tietotekniikkarikos. Kirjausohjeen nimeksi tulee ”Tietotekniikkarikosten kirjaaminen ja alkutoimet”.

Tavoitteena on kirjausohjeessa listattujen toimintatapojen ja kirjauskäytäntöjen voidaan noudattaa mahdollisimman laajasti poliisin tietojärjestelmissä tapahtuvien muutostenkin jälkeen.

1.2 Kirjausohjeen suunnittelu

Marraskuussa 2017 lähestyin sähköpostitse Keskusrikospoliisin kyberkeskuksen ylikomisario Tero Muurmania mahdollisista opinnäytetyöaiheista, jotka liittyvät kyberrikollisuuteen. Tavoittelin sellaista opinnäytetyöaihetta, jossa käsiteltäisiin kyberkeskuksen päivittäisissä työtehtävissä näkyviä asioita ja ilmiöitä. Sähköpostitse käydyn keskustelun jälkeen aiheeksi valikoitui ohje, jonka sisältö olisi kyberrikosten kirjaaminen ja kyberrikostutkinnan alkutoimet. Kirjausohjeen ensimmäinen versio muotoutui Keskusrikospoliisin tutkijoiden kanssa sähköpostitse käytyjen keskustelujen ja heille tekemieni kyselyjen perusteella. Ensimmäistä versiota kehitettiin sähköpostin välityksellä tehtyjen palautekierrosten kautta. Viimeisin versio hyväksyttiin 9.3.2018.

Kirjausohjeen sisältöön vaikutti Keskusrikospoliisin tutkijoiden kokemukset niistä asioista, jotka ovat esitutkinnan laadun ja yhdenmukaistamisen kannalta kaikkein keskeisimpiä. Keskeisimmiksi koettuja asioita kartoitin kysymyksillä:

1. Mitkä ovat tällä hetkellä yleisimmät puutteet rikosilmoitusten kirjaamisessa?
2. Mitä luokittelutietoja tietotekniikkarikostutkinnassa tulisi käyttää?
3. Mikä on kirjausohjeen kohderyhmä?
4. Mitä muita asioista tietotekniikkarikoksen kirjaamisessa tulisi huomioida?
5. Millainen kirjausohjeen ulkoasun tulisi olla?

Kirjausohjeen ulkoasun suunnittelussa tärkeimmäksi koettiin selkeys ja tiivis asiasisältö. Tarkoituksena oli tuottaa käyttökelpoinen apuväline, johon ei välttämättä tarvitse perehtyä etukäteen, vaan siihen voisi nojata rikosilmoituksen kirjaamisen hetkellä. Tavoitteena oli tuottaa yhden sivun mittainen kirjausohje. Osana opinnäytetyötä laadittiin myös tietotekniikkarikosten kirjaamista ja alkutoimien tekemistä auttava tukimateriaali. Tukimateriaalia käyttämällä rikosilmoituksen kirjaaja saa apua asianmukaisen rikosnimikkeen valintaan ja lisätietoa kirjausohjeesta löytyvistä asioista.

2 KYBERRIKOKSET

Suomen rikoslaissa ei tunneta käsitettä kyberrikos, vaan se on johdettu englannin kielen sanoista ”Cyber crime”. Kyberrikos käsittää useita eri rikosnimikkeitä. Kyberrikokset määritellään tyypillisesti tietotekniikka- tai tietoverkkorikoksiksi eli sellaiseksi rikokseksi, jonka tekovälineenä on tietotekninen laite, tietoverkko tai sovellus. Tietotekninen laite, tietoverkko tai sovellus voi myös olla kyberrikoksen kohteena. Kyberrikoksiksi kutsutaan myös sellaisia perinteisiä rikoksia, joiden teossa tietotekniikkaa on käytetty apuvälineenä. Tietoteknisellä laitteella tarkoitetaan lähestulkoon kaikissa tapauksissa tietokonetta ja tietoverkolla tarkoitetaan internetiä. Sovelluksella tarkoitetaan mitä tahansa hyökkäyksen kohteena olevaa tai rikoksen tekemistä varten luotua tietokoneohjelmaa. Näihin käsitteisiin pureudutaan tässä työssä tarkemmin kyberrikollisuuden ilmiöiden ymmärtämisen helpottamiseksi.

Rikostutkinnan kannalta haastavaa on kyberrikollisuuteen keskeisesti liittyvät anonymiteetti ja kansainvälisyys. Tietoverkkojen välityksellä rikolliset voivat toimia maantieteellisistä etäisyyksistä ja valtioiden rajoista piittaamatta. Tietoverkoissa tehdyissä rikoksissa varmuutta varsinaisesta tekijästäkään ei välttämättä tiedetä (Näsi & Tanskanen, 2017). Myös alkujaan laillisiin tarkoituksiin kehitettyjen salaustekniikoita ja tietoliikenneteknologioita hyödynnetään kyberrikollisten parissa.

Suomessa kansallisen kyberturvallisuusstrategian laatiminen käynnistettiin vuonna 2011 osana yhteiskunnan turvallisuusstrategian toimeenpanoa. Poliisilla on keskeinen rooli 2013 julkaistussa kansallisessa kyberturvallisuusstrategiassa, se on kirjattu seuraavalla tavalla:

> Kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten esitutkintaviranomaisena toimii poliisi. Poliisi kokoaa analysoidun ja korkealaatuisen tilannekuvan kyberrikollisuudesta ja jakaa sen osaksi - - yhdistettyä tilannekuvaa. Poliisi toimii tiiviissä yhteistyössä Kyberturvallisuuskeskuksen kanssa. Huolehditaan, että poliisilla on riittävät toimivaltuudet, resurssit sekä osaava ja motivoitunut henkilöstö, joka hoitaa kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten ennaltaehkäisemisen, taktisen esitutkinnan sekä digitaalisen todistusaineiston käsittelyn ja analysoinnin. Jatketaan ja syvennetään kansainvälistä operatiivista yhteistyötä ja tiedonvaihtoa EU:n ja muiden maiden lainvalvontaviranomaisten ja vastaavien toimijoiden kuten Europolin kanssa. (Suomen kyberturvallisuusstrategia, 24.1.2013.)

Suomessa kyberrikoksia tutkitaan alueperiaatteen mukaan poliisilaitoksilla. Osana kansallista kyberturvallisuusstrategiaa Keskusrikospoliisiin perustettiin vuonna 2015 kyberturvallisuuskeskus, joka tunnetaan nykyisin nimellä kyberkeskus. Kyberkeskuksen vastuulle

kuuluu vakavimpien tietoverkkorikosten tutkinta, tietoverkkorikollisuuden tilannekuvan ylläpito, internet- ja verkkotiedustelu, tietotekninen tutkinta, esitutkintaan liittyvät asiantuntijapalvelut poliisille ja muille viranomaisille. Nämä käsittävät muun muassa niin kutsuttuja hakkerijuttuja, palvelunestohyökkäyksiä ja muita vakavia sekä kansainvälisiä tietojärjestelmiin kohdistuvia rikoksia. Lisäksi kyberkeskus tarjoaa poliisihallinnolle IT-forensiikkaa ja tietoverkkoihin liittyvää tiedonhankintaa koskevia asiantuntijapalveluita (Piiroinen, 22.1.2016). Kyberkeskus ylläpitää kyberrikollisuuden tilannekuvaa seuraamalla ajankohtaisia ilmiöitä ja teknologian kehitystä (Poliisi, 2017). Suomen poliisi tutkii myös ulkomailta Suomeen kohdistuvat hyökkäykset.

2.1 Rikoksentekijät ja rikoksen kohteet

Onnistunut kyberrikos voi tuottaa rikollisille miljoonien tai jopa miljardien eurojen rikoshyödyn tai aiheuttaa kohteelle hyvin merkittäviä vahinkoja. Suuret tuotot kiinnostavat järjestäytynyttä rikollisuutta ja ammattimaistavat kyberrikollisten toimintaa. Kyberrikokset kohdistuvat yksittäisiin kansalaisiin, yhteisöihin, yrityksiin ja julkishallintoon. Rikoksen uhriksi voi joutua luonnollinen henkilö tai oikeushenkilö siinä missä perinteisen rikoksen tapauksessakin. Kyberrikokseen voi myös syyllistyä mikä tahansa edellä mainituista tahoista. Kyberrikoksen taustalla voi olla taloudellisen hyödyn lisäksi ideologiset syyt, valtiollinen toiminta, sodankäynti, terrorismi tai ilkivalta. Yksittäisen kyberrikoksen motiivit vaikuttavat vaihtelevan rikostyypin mukaan. Palvelunestohyökkäysten suurin motiivi oli Europolin raportin mukaan kiristys (Europol 2017, 27.9.2017). Kiristystä tehdään yleensä taloudellisen hyödyn vuoksi ja sen kohteena ovat yleensä keskikokoiset sekä suuret organisaatiot. Kiristys oli motiivina kolmanneksessa palvelunestohyökkäyksiä. Puolet jäljelle jäävistä tapauksista tehtiin ilkivallan ja poliittisten tai ideologisten syiden vuoksi. Euroopassa tapahtuvista tietomurroista 73 % tehdään taloudellisen hyödyn vuoksi (Europol, 27.9.2017).

Vuosi 2017 osoitti, että valtiot ovat aktiivisia toimijoita kyberrikollisuuden saralla. Yhdysvallat syyttivät WannaCry-hyökkäyksestä Pohjois-Koreaa (CNN, 20.12.2017). Maailmalla havaittujen suuren kokoluokan keskitettyjen hyökkäysten on arvioitu olevan valtiollisten toimijoiden voimannäyttöjä ja oman kyberkyvyn testaamista (Lakimiesuutiset, 1.12.2017). Suuren osan tämän hetken vaarallisimmista haittaohjelmista väitetään olevan peräisin valtiotason toimijoiden kyberohjelmista. Ajankohtaisimpana esimerkkinä Eternal Blue -

haittaohjelma, jonka alkuperä vaikuttaa olevan Yhdysvaltain kansallinen turvallisuusvirasto NSA (Microsoft, 14.5.2017).

Tyypillistä kyberrikoksen tekijää on vaikea määritellä ja rikosten taustalta on löytynyt yllättäviä tekijöitä ja organisaatioita. Esimerkiksi Mirai-haittaohjelman ennätyksellisen suurten vaikutusten pelättiin alkujaan olevan jonkin valtiotason toimijan harjoittelua Yhdysvaltain edellisten presidentinvaalien sekoittamiseksi. Todellisuudessa Mirai oli saanut alkunsa kolmen yliopisto-opiskelijan kehittämästä haittaohjelmasta, jonka tarkoitus oli horjuttaa suositun verkkopeli Minecraftin palvelimia. Minecraft on yli 122 miljoonan rekisteröityneen käyttäjän pelaama verkkopeli. Minecraft-verkkopeliä varten perustettu palvelin voi tuottaa huippusesonkeina omistajalleen yli 80 000 euroa kuukaudessa (Graff, 13.12.2017), mikä tekee kilpailevien palvelinten häirinnän taloudellisesti houkuttelevaksi. Kyseisen haittaohjelman ohjelmakoodin julkaisu vapaaseen käyttöön oli syy myöhemmin nähdyille hyökkäyksille, joiden taustalla oli jo eri tekijät.

Toinen esimerkki viime aikojen suurten kyberrikosten taustalta löytyvistä tahoista on palvelunestohyökkäyksiä tilauspalveluna myynyt rikollisryhmä vDOS. Rikollisryhmä oli toiminnassa neljä vuotta ja teki siinä ajassa yli 150 000 palvelunestohyökkäystä. Rikollisryhmän taustalta löytyi kaksi israelilaista miestä, jotka käyttivät liiketoiminnan teknisessä toteutuksessa hyväkseen 19-vuotiaan, teknisesti hyvin lahjakkaan autistisen miehen taitoja (Krebs, 20.10.2017).

Opinnäytetyön kirjoittamisen hetkellä etsityimmän kyberrikollisen sanotaan olevan kansainvälisesti etsintäkuulutettu Venäjän kansalainen Evgeniy M. Bogachev. Bogachev rakensi tietokonevirushaittaohjelman avulla botnetin, jonka arvioidaan anastaneen yli sata miljoonaa euroa ympäri maailmaa sijaitsevilta ihmisiltä ja organisaatioilta. (FBI, 2018).

2.2 Yksityishenkilöt rikosten kohteena

Kyberrikosten uhrien määrä ja vaikutukset ovat vaikeasti mitattavissa osittain myös siksi, että osan niistä arvioidaan jäävän kokonaan havaitsematta. Jos rikos havaitaan, siitä ei välttämättä ilmoiteta saman tapaan kuin perinteisestä rikoksesta. Esimerkiksi vuoden 2017 aikana maailmalla levinneen kiristyshaittaohjelma WannaCryn uhreiksi Suomessa joutuneista yli 200 kyberkeskuksen tietoon tulleesta uhrista vain yksi teki rikosilmoituksen (Telia, 7.11.2017). Vaikka tietotekniikka kuuluu jo hyvin kiinteästi ihmisten jokapäiväiseen

elämään, se koetaan silti usein vielä muusta elämästä irrallisena, rikosoikeudellisten seuraamuksien ulkopuolisena todellisuutena. Tämä ajattelutapa saattaa osaltaan myös madaltaa kynnystä rikokseen ryhtymiseksi, mikä pahentaa jo valmiiksi vaikeaa lähtötilannetta kyberrikosten tekemisen helppouden ja selvittämisen sekä vahinkojen korjaamisen vaikeuden suhteen.

Tietoturvan vuosi 2016-raportissa listattiin suurimmat yksityishenkilöön kohdistuvat kyberuhat. Yksityishenkilöön kohdistuvista uhkista suurin ovat huijaukset ja -tilausansat. Seuraavaksi suurimmaksi uhaksi arvioidaan kiristyshaittaohjelmien leviäminen älylaitteisiin ja verkkoon kytkettävien laitteiden yleistyminen kotitalouksissa. Yksityisyyden heikkeneminen sosiaalisessa mediassa ja heikkojen salasanojen käyttö luo seuraavaksi suurimman uhan yksityishenkilöille. (Viestintävirasto, 31.1.2017.)

2.3 Oikeushenkilöt rikoksen kohteena

Suomalaisten organisaatioiden kyky havainnoida kyberuhkia tai tunnistaa joutuminen vakavan tietoturvaloukkauksen uhriksi on edelleen yksi tämän hetken tärkeimmistä tietoturvailmiöistä. Poliisin kannalta ongelmallista asiassa on se, että organisaatiot eivät kerää oman kyberturvallisuuden kehittämisen lisäksi mahdollisen rikostutkinnan kannalta keskeisiä lokitietoja tietojärjestelmistään (Viestintävirasto, 17.1.2017).

Kaupalliset yritykset ja muut organisaatiot saattavat jättää kyberrikokset ilmoittamatta esimerkiksi siitä syystä, että rikoksen uhriksi joutumisen voidaan katsoa olevan haitaksi organisaation maineelle ja luotettavuudelle. Kulttuuri kyberturvallisuusasioita koskien on kuitenkin muuttumassa yritysmaailmassa, mikä helpottaa myös poliisia ajankohtaisten kyberilmiöiden seurannassa. Maersk-yhtiöt tiedottivat heinäkuussa 2017 (Palmer, 16.8.2017) joutuneensa NotPetya-haittaohjelmahyökkäyksen uhriksi. NotPetya-haittaohjelma ilmestyi vain viikkoja WannaCry-haittaohjelman jälkeen ja tiedostojen salaamisen sijasta NotPetya tuhosi saastuttamansa tietokoneen tiedostot. Haittaohjelma aiheutti Maersk-yhtiölle heidän oman arvionsa mukaan 200 – 300 miljoonan euron vahingot. Yhdysvaltain tiedustelupalvelu CIA kertoi tammikuussa 2018 selvittäneensä, että NotPetya-haittaohjelman taustalla on Venäjän armeijan hakkerit (Nakashima, 12.1.2018).

2.4 Tietotekniikan kehityksen haasteet lainsäädännölle

Tietotekniikan nopean kehityksen mukana kehittyvä kyberrikollisuus asettaa rikostutkinnan lisäksi haasteita myös lainsäädännölle. Raja tavanomaisen rikoksen ja kyberrikoksen välillä voi olla vaikeasti erotettavissa ja tulkinnasta tekee haastavaa myös se, että tietotekniikan osuus monissa fyysisen maailman asioissa ja esineissä kasvaa koko ajan. Tämän kehityksen myötä alkaa hämärtyä myös raja siitä, että kohdistuuko rikos tietotekniikkaan vai johonkin muuhun asiaan ja missä suhteessa. Esimerkiksi arvokasta tietoa eli dataa sisältävän tietokoneen turmeleminen fyysistä voimaa käyttämällä voidaan tulkita vahingontekorikokseksi (RL 35:1), mutta saman tiedon tuhoaminen tietoteknistä tai tietojenkäsittelyllistä menetelmää käyttämällä rikosnimike muuttuu datavahingonteoksi (RL 35:3a). Datavahingonteko voidaan luokitella kyberrikokseksi. Näiden rikosnimikkeiden rangaistusasteikko on eri vaikka rikoksella aiheutettu vahinko voi olla sama.

Tieto- ja viestintärikoksista säätävät lait ovat syntyneet ja kehittyneet 1990-luvun alussa Suomen digitalisoituessa kovaa vauhtia. Siihen saakka tieto- ja viestintärikoksia koskevaa käsitteistöä oli löydettävissä vain silloisesta teletoimintalaista (183/1987) ja radiolaista (517/1988). Tietokoneet, matkapuhelimet ja internet alkoivat yleistyä ja tieto alkoi siirtyä paperiarkistoista tietoverkkoihin sekä digitaalisille tallennusvälineille. Tieto alettiin kokea yhteiskunnan kannalta yhä tärkeämmäksi resurssiksi ja tärkeäksi tehokkuustekijäksi. Tämä loi lainsäädännön kannalta tilanteen, jossa tiedon käsittelyyn ja tietoverkoissa toimimiselle ei ollut olemassa säätelyä ja teknologian nopean kehityksen koettiin pitävän alan eettisen normiston eräänlaisessa käymistilassa, jossa oikean ja väärän raja on häilyvä. Muun muassa näistä lähtökohdista säädetyn tieto- ja viestintärikoksia koskevan lain tarkoituksena on antaa selkeitä normeja tietoalan käyttäytymisen perustaksi ja siten olla osaltaan myös luomassa alan eettisiä periaatteita. Lisäksi, teknisten turvaratkaisujen ollessa ensisijaisia suojautumiskeinoja, tulee lainsäädännön taata tiedon tallennuksen, käsittelyn ja siirron luotettavuus, tietoon liittyvät taloudelliset arvot on kyettävä suojaamaan ja kansalaisten yksityisyys on kyettävä suojaamaan tekniikan aiheuttamilta vaaroilta. (HE 94/1993.)

Kyberrikokset eivät välttämättä ole uudenlaisia rikoksia, jotka ovat syntyneet tietotekniikan kehityksen yhteydessä, mutta tietotekniikan käyttö on jokaisessa kyberrikoksessa olennaisessa asemassa. Tällä hetkellä yleisiä tietokone- tai tietoverkkoavusteisia rikoksia ovat internetin välityksellä tehdyt petosrikokset (RL 36:1). Tällaisissa rikoksissa erehdyttäminen tapahtuu perinteiseen tapaan, mutta verkkosivuston, sähköpostin tai muun tieto-

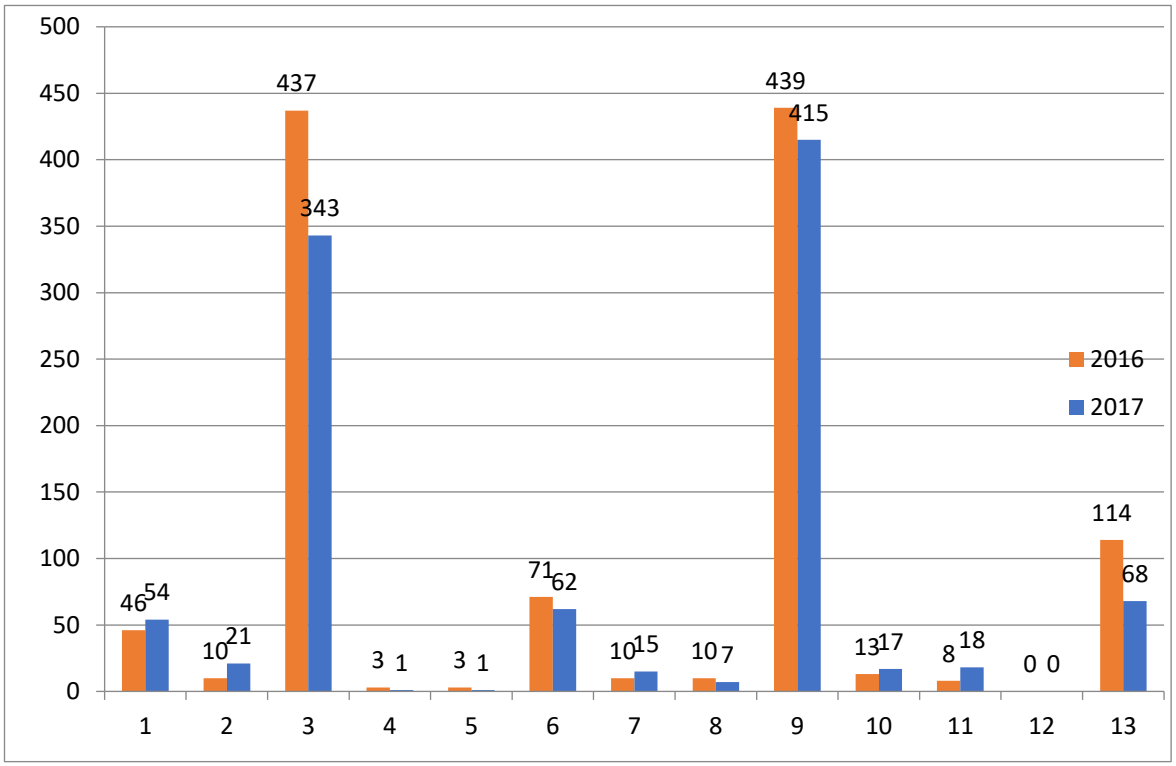
teknisen sovelluksen välityksellä. Internetin mahdollistama anonymiteetti tekee tällaisesta toiminnasta rikollisille turvallista ja vaivatonta kasvotusten tehtäviin petoksiin verrattuna.

Ajoneuvot ja kodinkoneet ovat olleet jo pitkään osa internetiä. Terveydenhuoltolaitteiden, ja yhteiskunnan kriittisen infrastruktuurin alettua myös liittyä yhä suuremmilta osin osaksi internetiä, kasvaa myös riski joutua henkeen ja terveyteen kohdistuvan kyberrikoksen uhriksi. Kyberrikoksen kohdistuessa kriittiseen infrastruktuuriin, kuten energianjakeluun, tai terveydenhuoltolaitteisiin, voivat sen vaikutukset heijastua ihmisten henkeen ja terveyteen. Kaikkia rikoslaissa säädettyjä rikoksia ei nykyisellä teknologian tasolla ole voitu tehdä tietokoneavusteisesti tai tietoverkon välityksellä. Teoriassa mikä tahansa rikos on mahdollista toteuttaa siten, että se voidaan luokitella kyberrikokseksi.

Enemmän tietoteknisiä kuin perinteisiin tekotapoihin liittyviä elementtejä sisältäviä rikosnimikkeitä löytyy tieto- ja viestintärikoksia käsittelevästä rikoslain 38 luvusta. Osa rikoslain luvun 38 tunnusmerkistöistä voi käytännössä toteutua vain tietoteknisessä ympäristössä. Näitä ovat esimerkiksi tietomurto, tietojärjestelmän häirintä ja datavahingonteko. Jokainen näillä rikosnimikkeillä kirjattu rikosilmoitus luokitellaan kyberrikokseksi. Rikoslain 38 lukua on uudistettu viimeksi 2015 voimaan tulleella lakimuutoksella (HE 232/2014). Lakimuutoksella saatettiin Suomen lainsäädäntö vastaamaan Euroopan parlamentin ja neuvoston direktiiviä 2013/40/EU. Direktiivin voimaantulon myötä toteutettiin jäsenvaltioiden lainsäädännön yhdenmukaistaminen sekä ajanmukaistaminen.

Yksi direktiivin syntymisen taustalla oleva tekijä oli myös jäsenvaltioiden kansallisten viranomaisten ja asiantuntijaorganisaatioiden sekä Euroopan unionin tasolla toimivien tahojen välisen yhteistyön kehittäminen. Euroopassa merkittäviä asiantuntijaorganisaatioita ja viranomaisia ovat Eurojust, Europol ja sen kyberturvallisuuskeskus European Cyber Crime Centre ”EC3:n” sekä Europen Network and Information Security Agency ”ENISA”.

Tieto- ja viestintärikosten (RL 38) lukumäärissä ei ole tapahtunut suurta muutosta vuosia 2016 ja 2017 vertailemalla. Identiteettivarkaus (RL 38:9a) on ylivoimaisesti yleisin tieto- ja viestintärikos. Identiteettivarkaus on jätetty diagrammista pois sen suhteettoman suuren osuuden vuoksi, niiden määrä on lähes kymmenkertainen seuraavaksi yleisimpiin rikosnimikkeisiin verrattuna. Identiteettivarkauksia tehtiin vuoden 2016 aikana 3 760 ja 2017 aikana 3 565.



Kuvio 1. Rikoslain 38 luvun rikosten määrät vuosina 2016 ja 2017, (Polstat 2018)

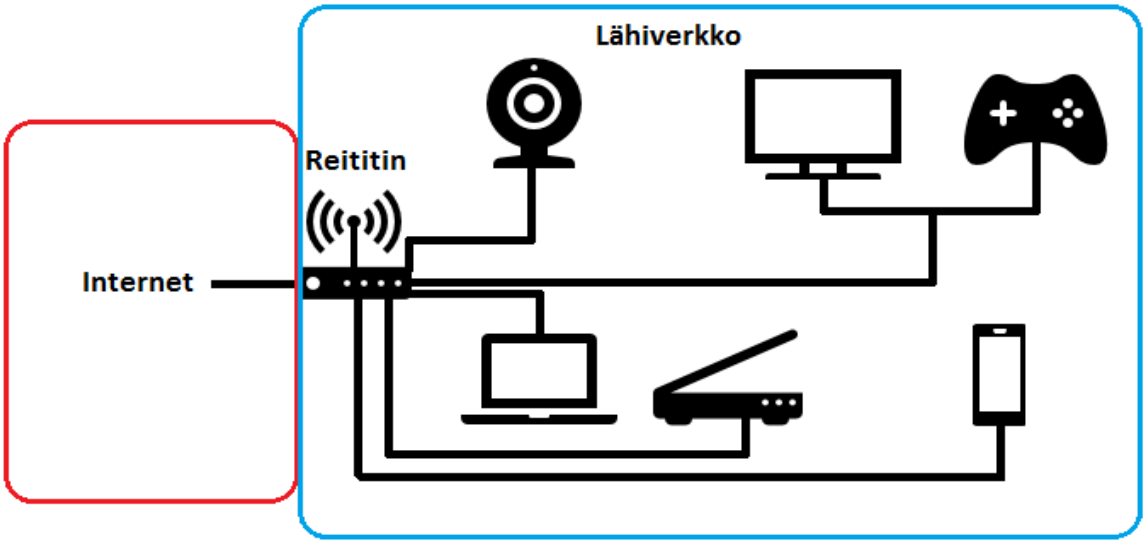
- 1 SALASSAPITORIKOS
- 2 SALASSAPITORIKKOMUS
- 3 VIESTINTÄSALAISUUDEN LOUKKAUS
- 4 VIESTINTÄSALAISUUDEN LOUKKAUKSEN YRITYS
- 5 TÖRKEÄ VIESTINTÄSALAISUUDEN LOUKKAUS
- 6 TIETOLIIKENTEEN HÄIRINTÄ
- 7 TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ
- 8 LIEVÄ TIETOLIIKENTEEN HÄIRINTÄ
- 9 TIETOMURTO
- 10 TIETOMURRON YRITYS
- 11 TÖRKEÄ TIETOMURTO
- 12 SUOJAUKSEN PURKUJÄRJESTELMÄRIKOS
- 13 HENKILÖREKISTERIRIKOS

2.5 Tietoverkot kyberrikollisuuden mahdollistajina

Tietoverkot ovat tietoteknisten laitteiden tiedonvaihtokanava. Tietoverkoissa tietokoneet, matkapuhelimet ja kodin älylaitteet voivat muodostaa toisiinsa verkkoyhteyden ja vaihtaa tietoa laitteen ohjelmistokoodin automatisoimana tai laitetta käyttävän ihmisen toimesta. Laitteiden välistä tietoliikenneyhteyttä on mahdollista käyttää myös rikolliseen tarkoitukseen eri menetelmiä käyttäen. Näitä menetelmiä käsitellään tässä työssä tarkemmin.

2.5.1 Tietoverkot

Tietoverkkoja käsitellään tässä työssä jakamalla ne karkeasti ottaen kahteen tyyppiin: julkiseen verkkoon eli internetiin ja yksityisiin verkkoihin eli lähiverkkoihin. Lähiverkkoja kutsutaan myös sisäverkoiksi. Lähiverkot ovat nimensä mukaan maantieteellisesti suppean alueen kattavia tietoverkkoja. Lähiverkkoja ovat kotien ja yritysten lähiverkot, joissa verkkoon kytketyt laitteet sijaitsevat yleensä korkeintaan kymmenien metrien etäisyydellä toisistaan. Lähiverkoista kuten kotiverkoista muodostetaan yleensä yhteys internetiin teleoperaattorilta hankitun reititinlaitteen kautta. Lähiverkon yksittäinen laite kuten tietokone voi olla reitittimeen yhteydessä langattomasti tai kiinteällä kaapeliyhteydellä. Reititin välittää kodin lähiverkkoon kytkettyjen verkkolaitteiden lähettämän tietoliikenteen internetiin ja internetistä saapuvan verkkoliikenteen asianmukaiselle verkkolaitteelle.



Kuvio 8. Internet ja kodin verkkolaitteet

2.5.2 Anonyymit tietoverkot

Kyberrikollisuudessa keskeisesti vaikuttava verkko on niin kutsuttu ”Darknet” tai toiselta nimeltään ”Deep web”. Darknetillä tarkoitetaan Googlen ja muiden tämän hetken yleisimpien internet-hakukoneiden sisältöindeksoinnin ulkopuolelle jäävää osaa internetistä. Nämä verkkosivustot ovat siis sellaisia, että niitä ei voi löytää yleisiä hakukoneita käyttämällä. Darknet on heikosti tunnettu termi, vaikka kaikista tietoverkkojen tietosisällöstä vain 4 % on niin kutsuttua julkista eli hakukoneiden näkemää verkkoa ja loput 96 % Darknetiksi luokiteltavaa sisältöä.

Anonyymit tietoverkot perustuvat nykyisin suurelta osin Yhdysvaltain laivaston kehittämään tietoliikenteen TOR-reititysteknologiaan (The Onion Router), jossa tietoliikenne salataan monikerroksisella menetelmällä. Nykyisin TOR-verkko on avoin, vapaaehtoisten ylläpitämä tietoverkko. TOR-verkon käyttäjän tietoliikenne on salattu ja reititetty tavalla, joka tekee verkkoliikenteen analyysista vaikeaa tai mahdotonta. (TOR, 2018.)

TOR-verkko mahdollistaa muun muassa toimittajien, poliittisten aktivistien ja sisällön sensurointia harjoittavien valtioiden asukkaiden anonyymin viestinnän. TOR-verkko mahdollistaa myös verkkosisällön lukemisen ilman riskiä tietoliikenteen joutumista kolmannen osapuolen tarkastelun kohteeksi. TOR-verkkoa voidaan hyödyntää melkein mihin tahansa sellaiseen toimintaan, jossa käyttäjä halutaan pitää salassa. TOR-verkossa käytettävä reititysprotokolla mahdollistaa myös niin kutsuttujen piilopalveluiden ("hidden service") julkaisemisen siten, että niiden fyysinen sijainti pysyy piilossa muilta TOR-verkon käyttäjiltä. Tällaiset palvelut voivat olla esimerkiksi verkkosivustoja. Tämä mahdollisuus kiinnostaa myös kyberrikollisia ja TOR-verkossa toimii tällä hetkellä hyvin suuri määrä laitonta sisältöä jakavia verkkosivuja. Europolin mukaan laittoman materiaalin kaupankäynti yleisesti on siirtymässä tietoverkkoihin ja TOR-verkko on yksi tämän hetken laittoman kaupankäynnin mahdollistava tekijöistä. Darknet toimii muun muassa laittoman asekaupan, ihmiskaupan, laittoman maahanmuuton ja väärennettyjen asiakirjojen kauppa-alustana.

Kyberrikosten tekemiseen soveltuvien tietokoneohjelmien ja työkalusovellusten myynti Darknetissä vaikuttaa kasvavan (Europol, 27.9.2017). Vuonna 2016 TOR-verkkoa käytti päivittäin noin kaksi miljoonaa ihmistä ja 95 % TOR-verkon läpi kulkevasta liikenteestä meni julkiseen internetiin ja loput 5 % Darknetiin. TOR-verkon käyttöön on saatavilla selainohjelmistoja, jotka on määritelty valmiiksi käyttämään TOR-verkkoa tietoliikenteen käsittelyssä. Tämä mahdollistaa TOR-verkossa toimimisen ilman teknistä osaamista.

2.5.3 Kryptovaluutat anonyymeissä tietoverkoissa

Yleisin kryptovaluutta on Bitcoin ja muun muassa viime vuosien kiristyshaittaohjelmat ovat vaatineet rikoksen uhreilta Bitcoineja vastineeksi tietojen palauttamisesta. Bitcoin on pankeista ja valtioista irrallinen valuutta, jota ei ole sidottu henkilötietoihin ja tästä syystä se on myös rikollisten markkinoilla käytetty valuutta. Rikollisten kaupankäynti Bitcoineilla mahdollistaa anonymiteetin samoja reititys- ja salaustekniikoita käyttäen kuin mikä tahansa muukin tiedonsiirto. Anonyymin viesti- ja maksuliikenteen tultua mahdolliseksi, alkaa rikollinen toiminta siirtyä yhä enenemissä määrin Darknetin puolelle. TOR-verkossa käydään kauppaa pääasiassa digitaalisessa muodossa olevalla rahalla.

3 KYBERRIKOLLISUUDEN ILMIÖISTÄ

Kyberrikollisuuden ilmiöillä tarkoitetaan tässä työssä niitä teknologioita ja rikostyyppejä, joiden katsotaan synnyttävän tämän hetken suurimmat rikosvahingot ja uhkakuvat. Kyberrikollisuuden ilmiöt muuttuvat nopeasti tietotekniikan kehityksen mukana ja yksittäisissä kyberrikoksissa voi yhdistyä useita kyberrikollisuuden ilmiöitä.

Tietotekniikan nopeasta kehityksestä johtuen osa kyberrikollisuuden ilmiöistä on havaittavissa vain lyhyen ajan. Niiden katoamiseen voivat vaikuttaa tiettyjen laitteiden poistuminen markkinoilta tai ohjelmistohaavoittuvuuden korjaaminen. Osa kyberrikollisuuden ilmiöistä on pitkäkestoisia johtuen internetiin kytkettävien laitteiden kasvavasta määrästä ja niiden heikosta tietoturvasta. Myös internetin palveluita käyttävien ihmisten heikko tietoturvaosaaminen mahdollistaa joidenkin kyberrikollisuuden ilmiöiden olemassaolon.

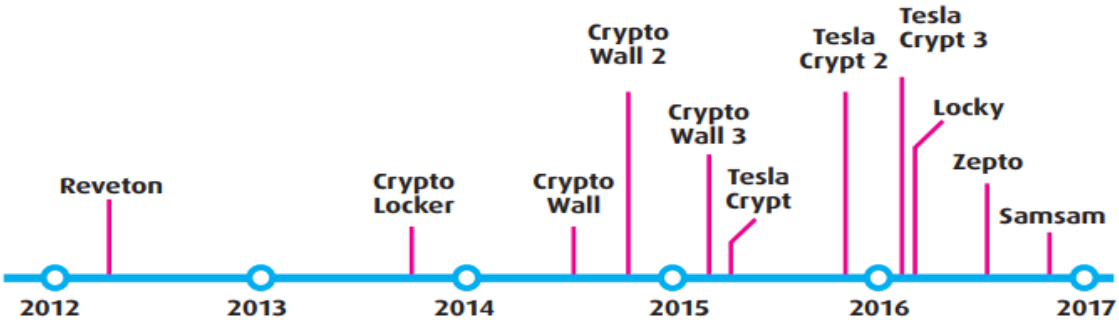
3.1 Haittaohjelmat

Haittaohjelmiksi luokitellaan tietokonevirukset, madot, troijalaiset ja muut yleisesti tunnetut haittaohjelmatyypit. Haittaohjelma on yleisen määritelmän mukaan käyttäjälle vahingollinen sovellus, joka tunkeutuu laitteelle ilman käyttäjän lupaa tai tietämystä. Haittaohjelmia levitetään esimerkiksi sähköpostin saastuneen liitetiedoston tai käyttöjärjestelmän tietoturvahaavoittuvuuden kautta. Haittaohjelman tarkoitus voi olla tietojärjestelmän vahingoittaminen, tietojen anastaminen tai kohdelaitteen valjastaminen rikollista käyttötarkoitusta varten. (Kotimikro, 11.5.2015.) Haittaohjelmat leviävät yllä mainittuja menetelmiä käyttäen ja sen lisäksi niitä kehitetään nykyisin tiettyihin käyttötarkoituksiin. Haittaohjelman kehittäminen on haittaohjelman määritelmän mukaisen tietokonesovelluksen ohjelmointia.

Madoksi luokiteltava haittaohjelma on tietokoneohjelma, joka leviää automaattisesti tietokoneelta toiselle tietoturvahaavoittuvuuksia hyödyntämällä. Tällä tavalla toimiva haittaohjelma käyttää jokaista kaappaamaansa tietokonetta uusien tietokoneiden kaappaamiseen, mikä mahdollistaa laajojen tietokoneverkostojen luomisen hyvin lyhyessä ajassa. Näitä laittomiin tarkoituksiin kaapattuja tietokoneiden verkkoja kutsutaan botneteiksi, joita käsitellään tässä työssä tarkemmin. Haittaohjelmat ovat siis usein apuväline, jota hyödynnetään jonkin kyberrikokseksi luokiteltavan teon toteutuksessa.

Tällä hetkellä yksi näkyvimmistä haittaohjelmien tarkoituksista on saastuneen tietokoneen muokkaaminen käyttökelvottomaan tilaan. Käyttökelvottomaan tilaan muokatun tietokoneen ruudulle ilmestyy tyypillisesti viesti, jossa luvataan palauttaa tietokoneen normaali toiminta viestissä ilmoitettua rahasummaa vastaan. Maksuja vaaditaan yleensä virtuaalivaluutan muodossa. Virtuaalivaluutoista kerrotaan tämän työn myöhemmissä luvuissa tarkemmin.

Haittaohjelmista ylivoimaisesti suurimman vahingon aiheuttivat vuosien 2016 ja 2017 aikana niin kutsutut ”Ransomwaret” eli kiristyshaittaohjelmat. Uusimmat kiristyshaittaohjelmat toimivat tyypillisesti siten, että ne lähetetään esimerkiksi sähköpostiviestin liitetiedostona tai haittaohjelmaan osoittavan linkin kohteeksi valitun organisaation henkilöstölle. Linkin tai liitetiedoston avaamisen jälkeen haittaohjelma leviää automaattisesti uusiin kohteisiin ja alkaa salata kohdelaitteiden kiintolevyjen sisältöä siten, että käyttäjä ei enää pääse käsiksi koneen tiedostoihin ilman salauksen purkamista. Haittaohjelma ilmoittaa tiedostot salanneen järjestelmän käyttäjälle maksuehdoista, jotka suorittamalla salauksen saa purettua ja tiedostot palautettua takaisin käyttöön. Tyypillisesti pyydetty maksu on noin 300-500 euroa per salattu laite. Mikäli käyttäjä ei maksa, tiedostot menetetään pysyvästi. Tästä toimintamallista tulee nimitys kiristyshaittaohjelma. Mitään takeita rikollisten antamalle lupaukselle ei tietystikään ole. Kiristyshaittaohjelmia on nähty aika ajoin kuluvan vuosikymmenen aikana, mutta viime vuosina ne ovat yleistyneet.



Kuvio 2: Kiristysohjelmat vuosina 2012 – 2017 (Viestintävirasto 2017)

Viestintäviraston aikajanalta eri kiristyshaittaohjelmien esiintymisien voidaan nähdä tihentyneen vuosien kuluessa, mutta toistaiseksi kaikkien aikojen suurimmat vahingot aiheuttanut kiristyshaittaohjelma WannaCry nousi esille vasta kuvion aikajanan päättymisen jälkeen, 12.5.2017. WannaCryn arvioidaan salanneen yli 300 000 tietokoneen tiedostot yli 150 eri maassa. Taloudellisten vahinkojen arvioidaan olevan miljardien eurojen luokkaa. Iso-Britanniassa 40 eri terveyskeskuksen tietokoneiden tiedostot salattiin haittaohjelman toimesta eikä hoitohenkilöstö päässyt tiedostoihinsa käsiksi (Erickson, 12.5.2017). Wan-

naCry-kiristyshaittaohjelman ohjelmakoodi perustuu Yhdysvaltain kansalliselta turvallisuusvirasto NSA:lta varastettuun Eternal Blue -haittaohjelmaan, joka hyödyntää Windows XP -käyttöjärjestelmän haavoittuvuutta (Smith, 14.5.2017).

Kuva 1. WannaCry-kiristyshaittaohjelman viesti Windows 8 -käyttäjälle. (kuva Wikipedia, 2017)

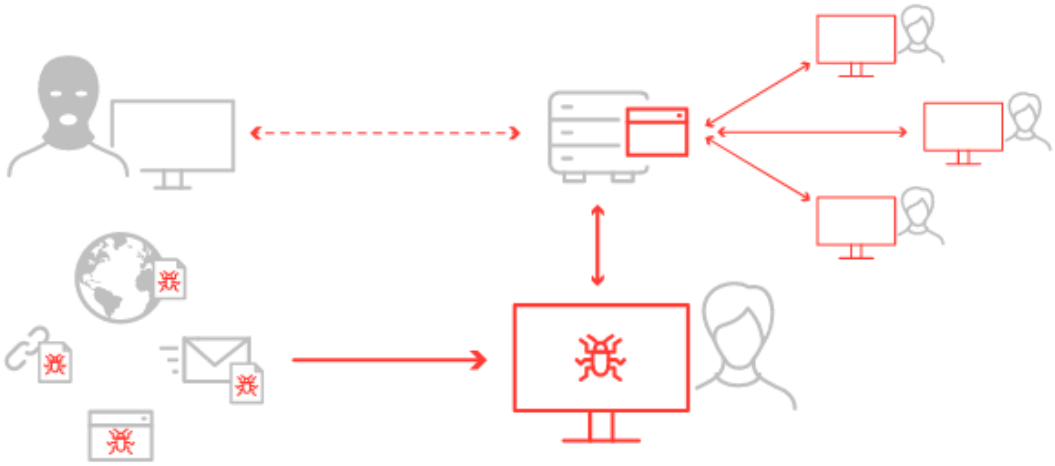
Vuonna 2016 kiristyshaittaohjelmien aiheuttamien vahinkojen ennalta estämiseksi ja vahinkojen korjaamiseksi käynnistettiin No more Ransom! -kampanja Hollannin poliisin, Europolin ja yksityisten tietoturva-alan yritysten toimesta. Kampanjan verkkosivustolla jaetaan tietoa ja sovellustyökaluja, joilla kiristyshaittaohjelman salaamat tiedot voi yrittää avata. Nyt sivuston asiaa ajaa yli 100 kansainvälistä kumppania poliisista ja yksityiseltä sektorilta. Sivun on arvioitu estävän yli kahdeksan miljoonan euron rikoshyödyn työkaluilla avattujen tietojen määrän perusteella. Sivu on olemassa myös suomen kielellä.

3.2 Botnetit

Botneteista puhutaan useiden eri haittaohjelmien yhteydessä ja ne ovat merkittävä tekijä tämän päivän kyberrikollisuudessa. Botnet on yleensä haittaohjelman tai haavoittuvuuden avulla rikolliseen tarkoitukseen kaapattu tietoteknisten laitteiden joukko. Rikoksentekijä hallinnoi tai vuokraa kaapattujen koneiden joukkoa rikollista käyttötarkoitusta varten. Botnetiin kaapattu laite on käytännössä aina kytketty internetiin ja sen internet-yhteys onkin usein ominaisuus, jonka rikollinen haluaa valjastaa käyttöönsä. Internet-yhteyttä voidaan käyttää esimerkiksi haitallisen verkkoliikenteen lähettämiseksi rikoksen kohteeseen. Botneteihin liitettyjen laitteiden määrä voi vaihdella sadoista laitteista miljooniin laitteisiin.

Botnetit kasvavat usein haittaohjelmaan ohjelmoitua automatiikkaa käyttäen siten, että jokainen kaapattu laite etsii verkosta lisää kaapattavia laitteita. Botnetit voivat kasvaa hyvin lyhyellä aikavälillä hyvin suuriksi. Botneteja käytetään käytännössä aina rikollisiin tarkoituksiin kuten roskapostien lähettämiseen tai yleisimmin palvelunestohyökkäyksiin. Tyypillinen botnetin laite on viime vuosiin saakka ollut tavallinen tietokone, mutta vuosien 2016 ja 2017 aikana muun muassa internet-reitittimiä, turvakameroita, televisioita ja muita kodin elektroniikkalaitteita on kaapattu osaksi botneteja. (Viestintävirasto, 18.10.2016.)

Botnet saa alkunsa tyypillisesti siten, että rikollinen luo haittaohjelman, joka leviää joko sähköpostin liitetiedostona tai tietoturvahaavoittuvuuden omaavaan laitteeseen. Haittaohjelma ottaa saastuneelta koneelta yhteyden ohjaus- ja hallintapalvelimeen (C&C server), josta haittaohjelma lataa itselleen toimintatapaohjeita. Botnetin taustalla oleva taho lähettää sovelluskäyttöliittymän avulla botnetiin liittyneille laitteille komentopalvelimen välityksellä ohjeita. Ohjeet voivat sisältää esimerkiksi palvelunestohyökkäyksessä käytettävää menetelmää tai haittaohjelman leviämiseen liittyviä mekanismeja. Nykyisin botneteja voi vuokrata hetkellistä käyttötarkoitusta varten, mikä mahdollistaa edistyneiden kyberhyökkäysten tekemisen ilman syvällistä ymmärrystä tietotekniikasta. Alla olevassa F-Securen kuvassa esitetään tyypillinen botnet, jossa rikollisen hallinnoiman botnetin hallintapalvelin on yhteydessä tyypillisin levitysmenetelmin kaapattuihin koneisiin.



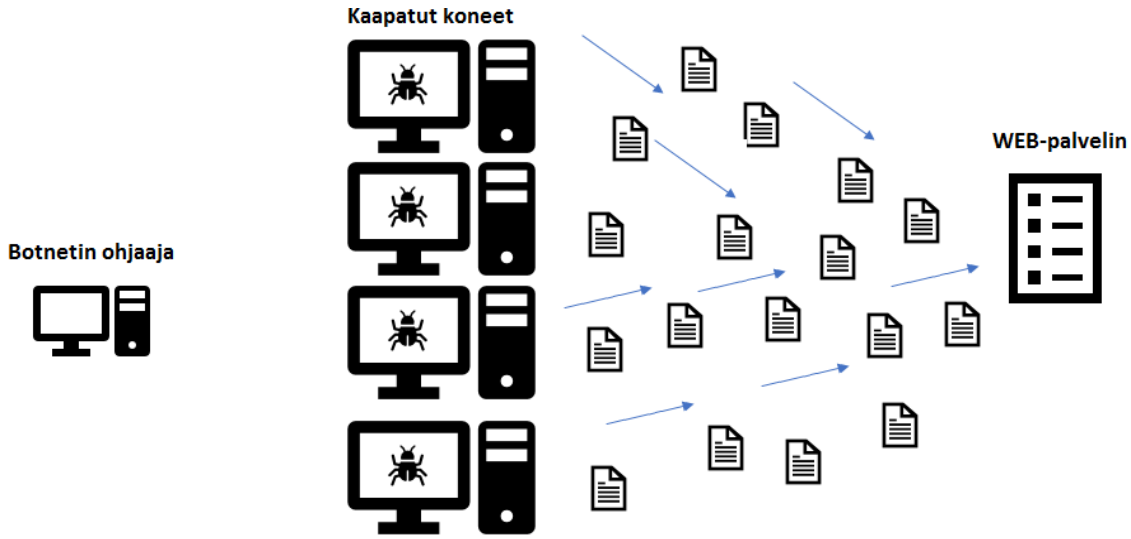
Kuvio 3. Botnetin toimintaperiaate. (kuva: F-Secure 2017)

3.3 Palvelunestohyökkäykset tietojärjestelmän häirinnän välineenä

Tietojärjestelmän toimintaan kohdistuvalla hyökkäyksellä eli tietojärjestelmän häirinnällä pyritään yleensä häiritsemään yksittäisen tietoteknisen palvelun toimintaa. Palvelu voi olla esimerkiksi verkkokauppaa harjoittavan yrityksen verkkosivusto. Tällä hetkellä yleisin keino häiritä tietojärjestelmiä ovat niin kutsutut palvelunestohyökkäykset.

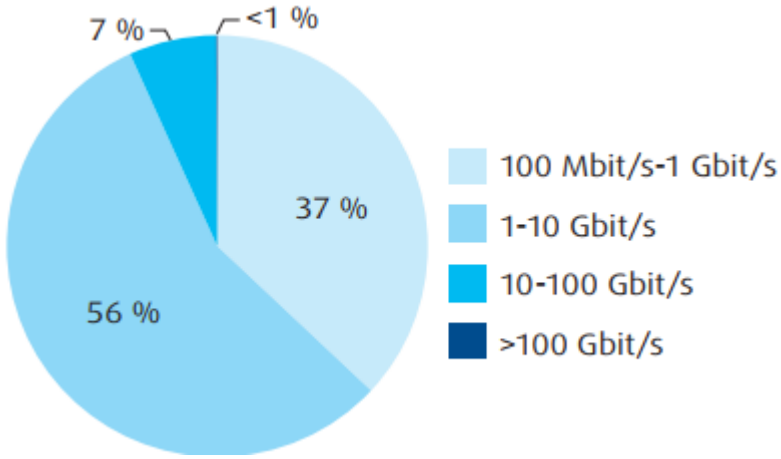
Verkossa sijaitsevan palvelun taustalla oleva palvelinkone pystyy käsittelemään käyttäjien lähettämiä palvelupyyntöjä eli viestiliikennettä vain rajallisen määrän kerrallaan. Määrä on riippuvainen palvelinkoneen fyysisistä laiteresursseista ja siinä käytettävistä sovelluksista. Suorituskyky muodostuu yleisesti ottaen prosessorin laskentatehosta, keskusmuistin tallennusominaisuuksista, internet-yhteyden tiedonsiirtokapasiteetista tai tietojärjestelmän ohjelmakoodin sisäisistä rajoituksista. Palvelunestohyökkäys perustuu palvelinkoneen suorituskyvyn ylikuormittamiseen. Ylikuormitus voidaan aiheuttaa lähettämällä palvelimelle palvelupyyntöjä niin paljon, että sen normaali toiminta häiriintyy. Ylikuormittunut palvelin ei pysty vastaamaan oikeisiin palvelupyyntöihin ollenkaan tai ajallaan, mikä häiritsee joko osittain tai kokonaan tietojärjestelmän suunniteltua käyttötarkoitusta. (McDovel, 6.2.2013). Esimerkiksi verkkosivustolla liiketoimintaa harjoittavan yrityksen toiminnan kannalta tällainen tilanne synnyttää hyvin nopeasti suuria taloudellisia vahinkoja. Ensimmäiset palvelunestohyökkäykset eli DOS (Denial of Service)-hyökkäykset tai hajautetut palvelunestohyökkäykset DDOS (Distributed Denial of Service)-hyökkäykset nähtiin jo 1990-luvulla, mutta viimeisten vuosien aikana ne ovat nousseet yhdeksi kyberrikosmaailman suurimmaksi uhkatekijäksi.

Palvelunestohyökkäykset voidaan jakaa kahteen kategoriaan, DOS-hyökkäys käyttää yhtä internet-yhteyttä ja DDOS-hyökkäys useita internet-yhteyksiä. DOS-hyökkäykseen kohteeksi valitulle palvelulle lähetetään ohjelmistohaavoittuvuutta hyödyntävää tietoliikennettä tai palvelinkoneen suoritin- ja muistiresursseja rasittavia palvelupyyntöjä. DDOS-hyökkäys on periaatteeltaan samanlainen kuin DOS-hyökkäys, mutta sen hajautettu luonne ja usean kaapatun laitteen yhdistetty voima tekevät siitä kohdejärjestelmälle vaikeammin torjuttavan. Hajautetussa hyökkäyksessä hyökkäyksen lähteillä ei välttämättä ole mitään yhdistävää tunnistetietoa tai tekijää, jonka perusteella hyökkäyksen voisi torjua kokonaan.



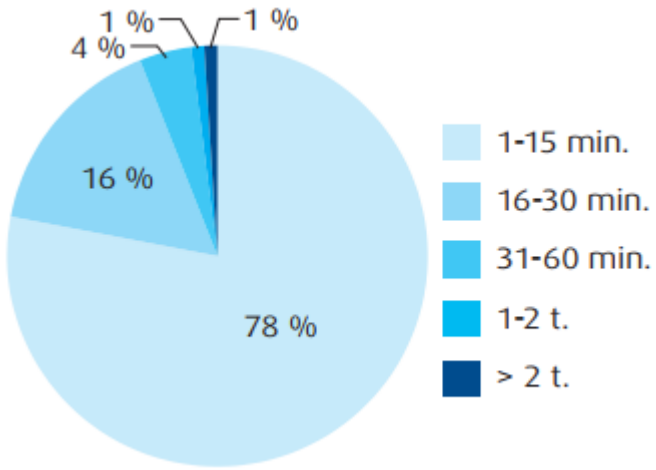
Kuvio 4. Hajautettu palvelunestohyökkäys.

DDOS-hyökkäykset ovat nousseet erityisesti viimeisen vuoden aikana pinnalle, kun Mirai-nimisestä haittaohjelmasta tehtiin ensimmäiset havainnot elokuussa 2016. Mirai-haittaohjelmaa käsitellään seuraavassa luvussa tarkemmin. Suomessa sijaitseviin palveluihin kohdistui vuonna 2016 muutamia erittäin suureksi luokiteltavia, voimakkuudeltaan yli 100 gigabittiä sekunnissa, palvelunestohyökkäyksiä. Vuonna 2016 Suomessa koettiin noin 500 palvelunestohyökkäystä joka kuukausi, voimakkuudeltaan ne olivat keskimäärin noin yksi gigabitti sekunnissa.



Kuvio 5. Palvelunestohyökkäysten voimakkuus (bit/s). (Viestintävirasto 2017)

Tyypillinen vuoden 2016 aikana havaittu palvelunestohyökkäys kesti Suomessa noin 15 minuuttia eli ne olivat kestoltaan hyvin lyhyitä. Palvelunestohyökkäyksen kesto vaikuttaa merkittävästi sen aiheuttamaan haittaan. Mitä pidempi hyökkäys, sitä kauemmin kohteena oleva palvelu on mahdollisesti kokonaan pois käytöstä. Toisinaan palvelunestohyökkäyksiä tehdään siten, että ne ovat lyhytkestoisia, mutta niitä tehdään useita kertoja vuorokaudessa. Oikein ajoitettuna tällainen menetelmä voi olla kohteelle hyvin haitallinen.



Kuvio 6. Palvelunestohyökkäysten ajallinen kesto. (Viestintävirasto 2017)

Kuten kyberrikosten tapauksessa usein on, palvelunestohyökkäyksen tekeminen on hyvin helppoa verrattuna sen aiheuttamiin kustannuksiin. Palvelunestohyökkäyksiä on myyty rikollisten keskuudessa laittomana palveluna siten, että asiakas voi maksua vastaan tilata palvelunestohyökkäyksen valitsemaansa kohteeseen. Palvelunestohyökkäyksillä ei pyritä vahingoittamaan tai tuhoamaan kohteen tietoa eikä menetelmällä pysyvää vahinkoa pystykään aiheuttamaan. Palvelunestohyökkäyksen välilliset vaikutukset esimerkiksi yrityksen mainetta tai menetettyä myyntiaikaa koskien voivat kuitenkin olla merkittävät (Viestintävi-

rasto, 2017). Suomessa palvelunestohyökkäyksen kohteeksi on viime aikoina joutunut muun muassa Kelan Kanta-palvelut (Sundqvist, 27.9.2017).

Tietojärjestelmän häirintä ja tietoliikenteen häirintä ovat tekotavoiltaan saman kaltaisia rikostyyppejä, mutta palvelunestohyökkäyksen tapauksessa on kyse tietojärjestelmän häirinnästä. Tietoliikenteen häirintä kohdistuu tele- tai radioviestintään (RL 38:5). Tietoverkkojen tapauksessa tämä voitaisiin tulkita esimerkiksi tietoverkkojen välistä viestiliikennettä välittäväksi reititinlaitteeksi tai yksityisen lähiverkon viestilaitteiden välisen tietoliikenteen häirintää. Tietoliikenteen häirintää on myös internetin keskustelupalstoille lähetyt viestit, joiden tarkoituksena on häiritä keskustelupalstan tavallista toimintaa.

3.3.1 Mirai-haittaohjelma palvelunestohyökkäysten taustalla

Miraissa yhdistyy useita kyberrikollisuuden ilmiöitä. Mirai on madoksi luokiteltava haittaohjelma, joka kaappaa verkkoon kytkettyjä laitteita osaksi botnetiä. Mirai-haittaohjelma rakensi teknisen toteutustapansa johdosta poikkeuksellisen suuren botnetin. Mirai etsii tietokoneiden sijasta internetistä IoT-laitteita (Internet of Things). IoT-laitteilla tarkoitetaan internetiin kytkettyjä älylaitteita kuten valvontakameroita, kotiverkkojen reititinlaitteita ja muita kotitalouksista löytyviä verkkolaitteita. Mirai-haittaohjelma on kehitetty toimimaan siten, että se etsii internetistä verkkolaitteita ja kokeilee kirjautua niiden tietojärjestelmään laitevalmistajien yleisimmin käyttämillä oletuskäyttäjätunnuksilla ja -salasanoilla. Useimmat verkkolaitteet käyttävät samanlaisia käyttäjätunnuksen ja salasanan yhdistelmiä kuten ”admin/admin” tai ”root/root” (Viestintävirasto, 18.10.2016). Mikäli Mirain löytämä verkkolaite hyväksyy sen kokeilemat käyttäjätunnukset, pääsee haittaohjelma tekemään muutoksia tietojärjestelmään ja kaappaamaan sen osaksi botnetiä. Karkeasti ottaen tätä menetelmää käyttäen Mirai saastutti satoja tuhansia laitteita ympäri maailman (Viestintävirasto, 18.10.2016). Suomessa saastuneita laitteita arvioidaan olleen marraskuussa 2016 yli 16 000 (Viestintävirasto, 29.11.2016). Mirain varsinainen tarkoitus oli käyttää kaapattuja verkkolaitteita palvelunestohyökkäysten toteuttamiseksi. Mirain avulla toteutetut palvelunestohyökkäykset olivat sen kaappaamien laitteiden suuren määrän johdosta erityisen haitallisia.

Mirai nousi ensimmäisen kerran esille tietotekniikka-alan toimittaja Brian Krebsin sivuston jouduttua yhden kaikkien aikojen suurimman DDOS-hyökkäyksen kohteeksi (Krebs, 16.9.2016). Hyökkäyksessä lähetetty datamäärä ylitti 620 gigabittiä sekunnissa, minkä

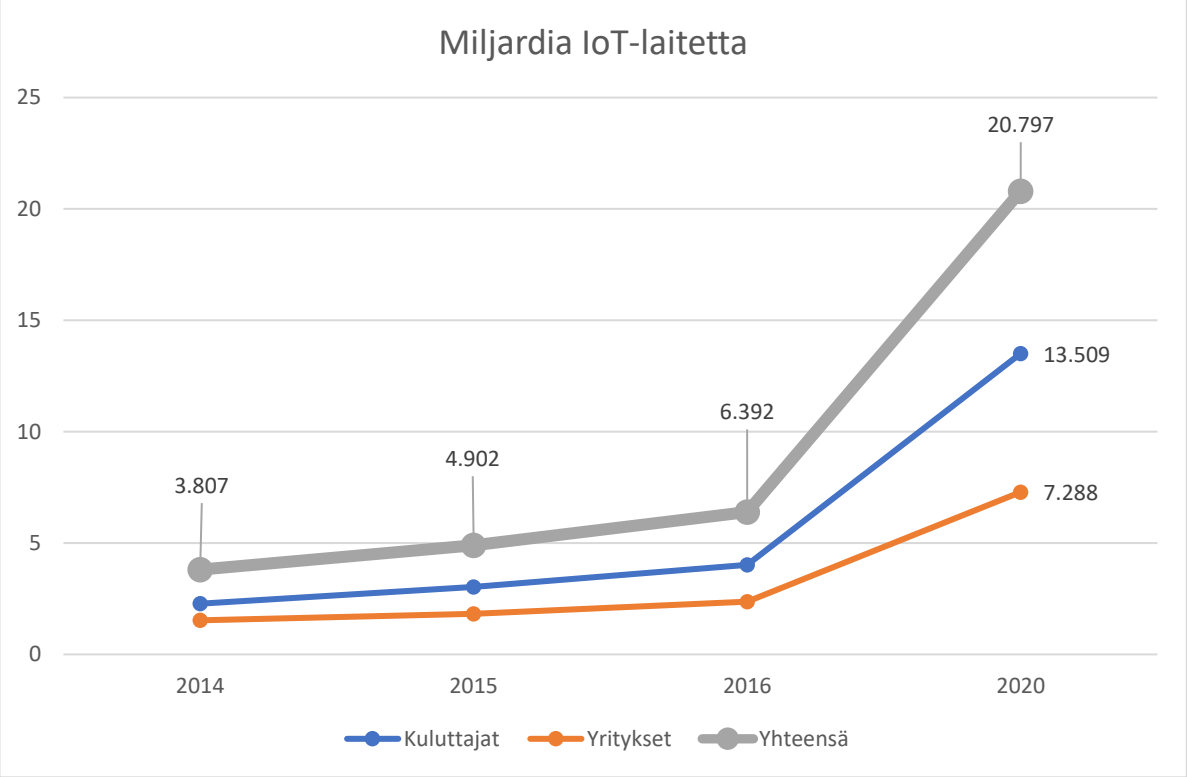
katsotaan ylittävän moninkertaisesti tyypillisen verkkosivuston lamauttavan tietoliikenteen määrän. Suomessa ei ole koettu yhtään yli 100 gigabittiä sekunnissa voimakkuuden palvelunestohyökkäystä. Seuraava havainto Miraista oli ranskalaisen tietotekniikkapalveluita tarjoavan yhtiö OVH:n kohdistuva hyökkäys, joka yhden terabitin eli 1 000 gigabittiä sekunnissa tietoliikennemäärällään oli kaikkien aikojen suurin DDOS-hyökkäys (Symantec, 27.10.2016). Internetin nimipalveluita eli käyttäjän ja palveluntarjoajan, esimerkiksi asiakkaan ja Amazon-verkkokaupan välisiä tietoliikenneyhteyksiä ohjaavan, Dyn-yrityksen palvelu joutui Mirai-hyökkäyksen kohteeksi. Hyökkäys aiheutti maailmanlaajuisia häiriöitä internetissä ja monet suurimmat internet-palvelut kärsivät vaikutuksista.

3.3.2 ”Asioiden internet” palvelunestohyökkäysten alustana

Perinteisten verkkolaitteiden kuten tietokoneiden ja älypuhelinten ulkopuolisiksi laitteiksi miellettävien koneiden kytkeytymistä internetiin kutsutaan ”IoT”:ksi eli ”Asioiden internetiksi” tai ”Esineiden internetiksi”. Termi on johdettu englannin kielen termistä ”Internet of Things”. Nykyisin internetiin yhteydessä voi tietokoneen ja matkapuhelimen lisäksi olla yhteydessä myös kodinkone, viihde-elektroniikkalaite tai vaikka henkilöauto, joka on varustettu verkko-ominaisuuksilla. Useat tietotekniikka-alan ammattilaiset näkevät IoT:n yhtenä historiamme suurimpana teknisenä ilmiönä. IoT:sta puhutaan usein eräänlaisena vallankumouksena, joka synnyttää uusien mahdollisuuksien lisäksi myös suuren määrän aivan uudenlaisia uhkia. IoT on suuren laitemääränsä vuoksi jo nykyisessä kehitysvaiheessaan osoittanut mahdollistavansa rikollisiin tarkoituksiin valjastettaessa aivan uudenlaisen suuruusluokan alustan esimerkiksi palvelunestohyökkäyksille.

IoT-laitteen verkko-ominaisuudet mahdollistavat sen kytkeytymisen internetiin esimerkiksi laitevalmistajan palvelimelta haettavan ohjelmistopäivityksen noutamista varten. Laitevalmistajat pyrkivät myös tuotekehityksen ja tuotetiedon hallinnan vuoksi keräämään tietoa asiakkaiden käytössä olevista laitteista, joten verkko-ominaisuuksien lisääminen melkein jokaiseen tuotteeseen on houkuttelevaa. Verkko-omaisuudet ja kotitietokoneisiin verrattuna heikot tietoturvaominaisuudet mahdollistavat laitteen joutumisen rikoksen kohteeksi tai se voidaan kaapata rikoksen tekovälineeksi. Kiinalaiset tutkijat osoittivat jo vuoden 2016 lopussa, että he pystyvät murtautumaan ja hallitsemaan etäyhteyden kautta Teslan Model S -henkilöauton jarruja, peilejä ja joitakin muita ominaisuuksia (Peterson, 20.9.2016).

Teknologian globaalia kehitystä seuraava kansainvälinen ICT-alan tutkimus- ja konsultointiyritys Gartner ennusti 2015 lokakuussa, että IoT-laitteiden määrä tulisi kasvamaan 30 % 2016 mennessä (Gartner, 10.11.2015). Ennuste piti paikkansa ja IoT-laitteiden määrä ylitti 6,4 miljardin laitteen rajan vuonna 2016 (Gartner, 10.11.2015). Gartner ennusti vuonna 2016 IoT-laitteiden määrän kasvavan vuoden loppuun mennessä 31 % edellisestä vuodesta. Laitteiden määrä oli vuoden lopussa 8.31 miljardia, mikä vastasi ennustetta (Gartner, 7.2.2017). Samaa trendiä seuraamalla vuoden 2020 ennuste on yli 20 miljardia laitetta, mikä luo aivan uudenlaisia uhkakuvia IoT-laitteiden haavoittuvuuksia hyödyntäville haittaohjelmille ja botneteille. IoT:tä pidetään uhkakuvien lisäksi myös yhtenä tulevaisuuden tärkeimmistä kilpailutekijöistä, mikä kiihdyttää osaltaan IoT-laitteiden määrän kasvua maailmalla.



Kuvio 9. IoT-laitteiden määrän kehitys ja ennuste

Tällä hetkellä tietoturva-alalla on löydetty merkkejä IoT-laitteita Mirain tapaan valjastavan haittaohjelma Reaperin toiminnasta. Toistaiseksi hyökkäyksiä ei vielä ole esiintynyt (Viestintävirasto, 1.11.2017).

3.4 Tietomurrot keskitettyjen hyökkäysten välineenä

Tietomurto käsittää kaikki sellaiset teot, joissa tietoteknisin menetelmin hankitaan luvattomasti pääsy tietojärjestelmään (RL 38:8). Käytännössä tämä voi tarkoittaa esimerkiksi

sitä, että rikollinen hankkii sähköpostin liitetiedostona lähetettyä haittaohjelmaa käyttämällä rikoksen kohteen käyttäjätunnukset. Toiselle henkilölle kuuluvia käyttäjätunnuksia käyttämällä rikollinen kirjautuu kohteena olevaan tietojärjestelmään. Keskitetty hyökkäys on käytännössä tietomurto, mutta se toteutetaan systemaattisella ja pitkäjänteisellä toimintamallillaan. Keskitetyllä hyökkäyksellä on selvä tavoite ja sen kohdeorganisaatio on tarkkaan valittu. Keskitetyn hyökkäyksen toteutuksessa voidaan hyödyntää haittaohjelmia tai useita eri tietoteknisiä hyökkäysmenetelmiä, joita on käsitelty tämän opinnäytetyön aiemmissa luvuissa.

Valittuun organisaatioon kohdistetut hyökkäysmenetelmät valitaan sen heikkouksien mukaan. Heikkoudet voivat liittyä henkilöstön heikkoon kykyyn tunnistaa sosiaalista manipulointia tai teknisen järjestelmän haavoittuvuuteen. Keskitetyssä hyökkäyksessä kohdeorganisaatiosta voidaan kerätä tietoa kuukausien tai jopa vuosien ajan ennen kuin rikoksessa edetään varsinaiseen tietomurtoon. Tietomurron jälkeen kohdeorganisaation suojauksia ja toimintatapoja kartoitetaan sisältä päin eri tietojärjestelmiin murtautumiseksi ja rinnakkaisten hyökkäystapojen suunnittelemiseksi (Symantec). Keskitetyt hyökkäykset ovat hyvin edistyneitä ja pitkäkestoisia rikosoperaatioita. Voidaan myös arvioida, onko niiden taustalla valtiollisia toimijoita vai ovatko ne yksittäisten toimijoiden tekemiä

Viestintäviraston laatimassa kuviossa esitetään tyypillisen keskitetyn hyökkäyksen vaiheet rikoksen valmisteluvaiheesta siihen saakka, kunnes rikoksen kohde tekee rikosilmoituksen. Kuviossa esitetyn keskitetyn hyökkäyksen tarkoituksena on verkkovakoilu, jolla tarkoitetaan tässä tapauksessa arkaluontoisen tiedon luvatonta käyttöä. Rikoksen valmistelusta rikosilmoituksen syntymiseen voi kestää jopa yhdeksän kuukautta. Suuressa osassa tapauksista tietomurto jää rikoksen kohteeksi joutuneelta organisaatiolta kokonaan havaitsematta.

Kuvio 7. Verkkovakoilun anatomia. (Viestintävirasto 2017)

Tietomurtojen motiivit voivat vaihdella, mutta yleisimmin niiden ajatellaan olevan taloudelliset. Esimerkiksi pääsy yrityksen tuotekehitystietoihin voi olla rikollisten markkinoilla arvokasta kauppatavaraa. Yrityssalaisuuden rikkomisesta ja väärinkäytöstä säädetään erikseen elinkeinorikoksia käsittelevässä rikoslain 30 luvussa. Tietomurtojen taustalla voivat olla myös poliittiset motiivit (Limnéll, 4.6.2016).

Keskitetyt hyökkäykset ovat olleet pinnalla erityisesti vuoden 2016 Yhdysvaltain presidentinvaalien jälkeen. Yhdysvaltain sen hetkinen hallinto, liittovaltion poliisi FBI:n ja kansallisten tiedustelupalvelun syyttivät Venäjää Yhdysvaltain vaalituloksen manipuloinnista (Hirschfeld Davis, Sanger, 15.12.2017). Guccifer niminen internet-persoona, jonka Yhdysvallat väitti olevan Venäjän tiedustelupalvelun luoma hahmo, julkaisi vaalien alla kymmeniä tuhansia sivuja Yhdysvaltain demokraattisen puolueen asiakirjoja ja kirjeenvaihtoa. Julkaistu materiaali oli hankittu Yhdysvaltain demokraattisen puolueen palvelimille murtautumalla. Tutkijoiden mukaan murtautujilla oli ennen materiaalin julkaisua ollut vuoden ajan pääsy tietoihin ilman asianomistajan tietoa. (Hirschfeld Davis, 6.1.2017.) Rikollisten toimintatapa sisälsi keskitetyn hyökkäyksen piirteitä.

3.5 Tietokoneavusteiset petokset

Tietokoneavusteisesti tehdyistä rikoksista petos (RL 36:1) on hyvin yleinen. Petos käsittää perinteiseen erehdyttämiseen perustuvan tekotavan ja tietototekniikkaa hyödyntävän, datan manipulointiin perustuvan tekotavan. Vaikka toinen tekotapa onkin sisällöltään kokonaan tietotekniikka käsittelevä, perinteiseen erehdyttämiseen perustuva tekotapa on silti yleisempi kyberrikoksena kirjattava petosrikos. Perinteiseen erehdyttämiseen liittyvä tekotapa voi olla esimerkiksi verkossa toimivan osto- ja myyntipalstalla tapahtuva huijaus, jossa myyjä ei koskaan toimita maksun suorittaneelle ostajalle luvattua tuotetta.

Suurimmat tietokoneavusteiset petokset koskevat vuoden 2016 jälkeen niin kutsuttuja toimitusjohtajahuijauksia. Toimitusjohtajahuijauksissa rikolliset tekeytyvät eri yritysten toimitusjohtajiksi väärentämällä sähköpostiosoitteensa yrityksen toimitusjohtajan sähköpostiosoitteeksi. Väärennettyä sähköpostiosoitetta käyttämällä rikolliset pyytävät yrityksen henkilöstöä tekemään tilisiirtoja haluamilleen tileille. Aidon näköinen sähköpostiosoite riittää monessa tapauksessa, mutta joissakin tapauksissa rikolliset soittavat vielä perään esiintyen esimerkiksi lakimiehinä ja painostivat tilisiirron pikaisessa tekemisessä. Toisena petostyyppinä esiin nousevat valepoliisirikokset, jotka usein tapahtuivat matkapuhelinverkossa, ja muun muassa suomalaisten teleoperaattoreiden nimissä lähetetyt valelaskut.

3.6 Tietokoneavusteiset seksuaalirikokset

Yksi tämän hetken nousevista seksuaalirikosilmiöstä kyberrikosten maailmassa on niin kutsuttu SCE (Sexual Coersion and Extortion of Minors). Tässä rikosilmiössä lapsi houkutellaan tekemään seksuaalisia tekoja, jotka tallennetaan videolle. Tämän jälkeen lasta aletaan kiristää videomateriaalin julkaisemisella. Seksuaalirikokset ovat petosten tapaan yksi tietokoneavusteisesti tehtävien rikosten laji, joka on yleistynyt tietoverkoissa. Rikos tehdään yleisimpiä sosiaalisen median sovelluksia käyttäen esimerkiksi siten, että rikollinen tekeytyy joko julkisuuden henkilöksi, kohteen kanssa saman ikäiseksi henkilöksi tai muutoin lasta kiinnostavaksi henkilöksi. Rikollinen suostuttelee lapsen tai nuoren henkilön seksuaalisiin tekoihin ja tallentaa ne videoyhteyden välityksellä. Tämän jälkeen lasta aletaan kiristää materiaalin julkaisemisella internetissä tai sen lähettämisellä kohteen perheenjäsenille ja ystäville. Rikollinen voi kiristää lapselta rahaa, mutta yleensä rikolliset pyrkivät saamaan lisää CSEM- eli lapsen seksuaalisen hyväksikäytön materiaalia (Child Sexual

Explotation Material). Rikollisten haltuun saamat CSEM:t on mahdollista myydä tai levittää eteenpäin.

Europolin IOCTA 2017 -raportin mukaan pienempi osa SCE-toiminnasta perustuu rahan kiristämiseen, mutta se osa on osoittanut järjestäytyneen rikollisuuden piirteitä. Kiristysoperaatioita on tehty muun muassa puhelinmyynnissä käytettäviä keskuksia vastaavista tiloista, joissa työskentelee useita rikoksentekijöitä yhtä aikaa. Varsinaisen CSEM:n eli lasten seksuaalista hyväksikäyttöä esittävän kuva- ja videomateriaalin suuri määrä on haaste rikostutkinnalle. Tavallisen SCEM-tapauksen sanotaan sisältävän 1-3 teratavua tutkittavaa dataa, mikä tarkoittaa 1-10 miljoonaa kuvaa ja tuhansia tunteja videomateriaalia. Suurimmissa tapauksissa datan määrän kerrotaan olevan jopa 100 teratavua, joka tarkoittaa yli 100 miljoonaa kuvaa ja tuhansia tunteja videomateriaalia. Tällaisen massan läpi käyminen on käytännössä mahdotonta. Tällä hetkellä apua asiaan toivotaan materiaalin analysointia automatisoivia teknisiä ratkaisuja toteuttavilta yrityksiltä.

Kokonaisuutena CSEM-ilmiö ei Europolin keräämien tietojen perusteella vaikuta kasvaneen, mutta ilmiössä on havaittavissa ammattimaistumisen ja järjestäytyneen rikollisuuden piirteitä. Euroopassa havaittu CaaS (Crime-as-a-Service) eli "rikos palveluna"-liiketoimintamalli leviää myös CSEM-materiaalin pariin. CSEM-as-a-Service-mallissa palveluntarjoaja tuottaa kysynnän mukaan asiakkaan toiveen mukaista materiaalia. Europol käynnisti vuonna 2017 ”Stop Child Abuse – Trace an object” -kampanjan CSEM-rikollisuuden torjumiseksi. Kampanjan ajatus on julkaista CSEM:sta kuten valokuvista tai videoista leikattujen esineiden julkistaminen verkkosivustolla. Mikäli joku sivulla vierailija tunnistaa kuvissa näkyvän esineen, voidaan CSEM-materiaalin alkuperä yrittää selvittää. (Europol, 27.9.2017.)

3.7 Kyberrikollisuuden ilmiöt tilannekuvan perustana

Kyberrikollisuuden ilmiöiden kehitystä seuraamalla voidaan muodostaa tilannekuva omasta toimintaympäristöstä. Kyberrikollisuuden ilmiöt heijastuvat usein eri sektorin toimijoille eri tavoilla. Kattavan tilannekuvan muodostamisessa tulisi hyödyntää usean eri sektorin ilmiöseurantaa.

Tilannekuvaraporteista käy ilmi, että monet kyberrikollisuuden ilmiöt kehittyvät ajan kuluessa. Kyberrikollisuuden tulevaisuuteen voi varautua jatkuvalla tilannekuvan rakentamisella ja ilmiöseurannalla.

4 KYBERRIKOLLISUUDEN TILANNEKUVA JA TULEVAISUUS

Kyberrikollisuuteen liittyvät ilmiöt ovat kansainvälisiä ja usein ne havaitaan samaan aikaan useassa eri maassa. Yksittäisen kyberrikoksen kohteena voi olla useita ihmisiä useasta eri maasta. Yksittäisen kyberrikoksen tekijät voivat myös sijaita useassa eri maassa. Kyberrikollisuuden tilannekuvaa muodostetaan ja ylläpidetään sekä Suomessa että muualla maailmassa. Europol perusti vuonna 2013 eurooppalaisen kyberrikoskeskuksen European Cybercrime Centre, EC3:n, jonka tarkoituksena on vahvistaa EU:n valmiutta kyberrikollisuuden torjunnassa. EC3 on julkaissut perustamisestaan lähtien vuosittaisen ”IOCTA:n”, Internet Organised Crime Threat Assessment -tilannekuvaraportin (Europol, 27.9.2017). Raportin on tarkoitus auttaa jäsenvaltioita toimintojen priorisoinnissa ja resurssien kohdentamisessa kyberrikollisuuden vastaisessa toiminnassa.

Suomessa poliisi tekee yhteistyötä viestintäviraston kyberturvallisuuskeskuksen kanssa kyberrikollisuuden tilannekuvan muodostamisessa (Poliisi, 2017). Viestintävirasto julkaisi vuoden 2017 tammikuussa 10 tietoturvanäkymää vuodelle 2017 ja suurin osa niistä on jossain määrin jatkuvia uhkia. Viestintävirasto julkaisi myös vuoden 2017 alussa kattavasti ajankohtaisia kyberilmiöitä käsittelevän Tietoturvan vuosi 2016 -raportin. Myös useat yksityisellä sektorilla toimivat tietoturva-alan yritykset julkaisevat omat vuosittaiset tilannekuvaraporttinsa. Suomalainen tietoturva-alan yritys F-Secure julkaisi elokuussa 2017 Attack Landscape H1 2017 -raporttinsa (F-Secure, 9.8.2017), jossa esitetyt luvut perustuvat heidän asettamiinsa mittalaitteisiin ympäri internetiä.

4.1 Europolin tilannekuvaraportti

Europol käsitteli vuosittaisessa tilannekuvaraportissaan tämän hetkisiä rikosilmiöitä ja lainsäädännöllisiä haasteita kyberrikollisuutta koskien. Raportti ei muodosta tilannekuvaa yksittäisten jäsenvaltioiden tilanteesta, se käsitelle Euroopan Unionia kokonaisuutena. Rikostyypeistä Euroopassa esiin nousivat niin kutsutut ”Social engineering” eli sosiaaliseen manipulointiin perustuvat rikokset. Suomessa tällaiseen menetelmään perustuvia rikoksia ovat olleet niin kutsutut toimitusjohtajahuijaukset. Lisäksi pinnalla ovat olleet Card-Not-

Present, "CNP-rikokset", jotka ovat käytännössä varastettujen luottokorttitietojen käyttöä maksuvälineenä verkkokaupoissa. Lapsiin kohdistuvat seksuaalirikokset verkossa ja haittaohjelmien leviäminen nousevat myös suurina ilmiöinä esille. (Europol, 27.9.2017.)

Yksi raportin keskeinen ilmiö on kriittiseen infrastruktuuriin eli yhteiskunnalle tärkeisiin toimintoihin kohdistuvat hyökkäykset. Kriittiseen infrastruktuuriin kohdistuvien hyökkäysten kasvu on vakava ongelma ja vuonna 2016 Suomessa koettiin ilmiön vaikutukset, vaikka hyökkäyksen kohde olikin muualla. Hyökkäyksessä käytettiin ympäri maailmaa laittomasti hallintaan otettuja verkkolaitteita. Verkkolaitteet olivat kiinteistö- ja teollisuusautomaatiolaitteita, joilla lähetettiin hyökkäykseen kohteeseen haitallista verkkoliikennettä. Kyseessä ei ollut Mirai, vaikka hyökkäys perustui samaan menetelmään. Hallintaan otettujen laitteiden mukana oli Lappeenrannassa sijaitsevien asuinkiinteistöjen sähköjärjestelmien ohjaukseen käytettäviä kiinteistöautomaatiolaitteita, jotka ylikuormittuivat alhaisen laitetehonsa vuoksi. Henkilövahinkoja ei syntynyt, mutta tapaus muistutti etenkin vaativien sääolosuhteiden alueiden riskeistä ja kyberhyökkäysten potentiaalista. (Europol, 27.9.2017.)

Raportin mukaan kyberrikollisuus jatkaa edelleen kasvuaan ja kehitystään. Käytännössä kaikki raportissa selvitetyt kyberrikostyypit ovat kasvaneet edellisestä vuodesta. Europolin raportin mukaan on havaittu, että useiden sektoreiden toimijoiden yhteistyössä koordinoitu, tietojohtoinen ja mukautumiskykyinen lähestymistapa voi johtaa hyviin tuloksiin kyberrikosten vaikutusten minimoimisessa. Kansainvälisen poliisiyhteistyön lisäksi toimivan kyberrikostorjunnan yhtenä keskeisenä edellytyksenä pidetään yhteistyötä yksityisen sektorin toimijoiden kanssa. Tällä hetkellä yhteistyö toimii ja sen tulokset ovat olleet hyviä. Globaalin kyberhyökkäyksen tapauksessa toimiva ja kansainvälinen yhteistyöverkosto julkisen ja yksityisen sektorin toimijoiden kesken on välttämättömyys. (Europol, 27.9.2017.)

4.2 Viestintäviraston tilannekuvaraportit

Viestintäviraston 10 tietoturvanäkymää vuodelle 2017 -raportissa pohditaan vuoden 2016 tapahtumien pohjalta seuraavan vuoden mahdollisia tapahtumia (Viestintävirasto, 27.1.2017). Kaikki kymmenen tietoturvanäkymää vaikuttavat pitäneen jossain määrin paikkansa. (Viestintävirasto, 31.1.2017.)

Ensimmäisenä asiana Viestintävirasto listaa teknologian kehityksen synnyttämät haasteet. Teknologian kehitys luo kiihtyvällä tahdilla uusia tuotteita, palveluita ja toimintamalleja. Kyberrikollisuus kehittyy samassa tahdissa ja tämä synnyttää uhkia, joita vastaan ei osata puolustautua eikä niitä välttämättä kyetä edes tunnistamaan. Tietoverkkojen häiriöt ovat osoittaneet, että yhteiskunnan talous, turvallisuus ja toiminta yleisesti ovat riippuvaisia tietoverkoista. Tietoverkkoihin ja -järjestelmiin kohdistuvien hyökkäysten vaikutukset voivat heijastua ja ketjuuntua tavalla, jota ei ole osattu ennakoida eikä niitä vastaan ole rakennettu asianmukaisia teknisiä ratkaisuja. Yhteen organisaatioon kohdistuva isku voi vaikuttaa ennakoimattomiin paikkoihin, kuten Lappeenrannan tapaus osoitti. Molempia edellä mainittuja uhkia koskee Viestintäviraston näkemys suomalaisten organisaatioiden kyvystä tunnistaa omissa järjestelmissä sijaitsevat uhkat. Monet yksityisellä sektorilla toimivat yritykset ja julkishallinnon organisaatiot ovat olleet tietämättään kyberrikosten kohteita. Kaikissa organisaatioissa ei tunneta omia tietojärjestelmiä niin syvällisesti, että kyettäisiin tunnistamaan niihin kohdistuvat uhkakuvat ja suojautumaan niitä vastaan. Myös suunnitelmat onnistuneesta hyökkäyksestä toipumiselle ja sitä seuraavalle rikostutkinnalle ovat usein puutteellisia tai ne puuttuvat kokonaan. Organisaatiossa asianmukaisesti ja omaan tietotekniseen toimintaympäristöön räätälöity tietoturvasuunnitelma voi estää kyberrikoksen kohteeksi joutumisen. Ainakin sellaisen laatimisella voi minimoida vahingot ja nopeuttaa kyberrikoksesta toipumista. (Viestintävirasto, 31.1.2017.)

Viestintäviraston raportissa arvioidaan, että ymmärrys tietoturvan merkityksestä kasvaa. Ymmärryksen parantuessa, alkaa myös kysyntä tietoturvaosaamiselle kasvaa. Ongelmaksi asiassa voi muodostua se, että tietoturvan kysyntä kasvaa tarjontaa nopeammin eli osaavia tarjoajia ei riitä kaikille tarvitsijoille. Samaan aikaan kun tietoturvaan panostetaan, ammattimaistuu myös kyberrikollisuus. Rikosoperaatiot ovat pitkäkestoisempia ja korkeatasoisempia. Kohteen näkökulmasta vahingot ovat siis entistä suurempia ja tutkintaviranomaisen näkökulmasta rikoksen selvittäminen on entistä vaikeampaa. (Viestintävirasto, 31.1.2017.)

Yksi kyberrikollisuuden kasvava laji on verkkovakoilu. Verkkovakoilua tehdään esimerkiksi poliittisista tai taloudellisista syistä. Tietoa voidaan hankkia muun muassa poliittisen päätöksenteon tai kaupallisen tuotekehityksen tueksi. Organisaatioiden kyky havaita heihin kohdistuvaa verkkovakoilua on heikko. Haittaohjelmia kohdistetaan tarkoin eri organisaatioihin, mutta tavoiteltava hyöty on kallistumassa tiedon sijasta rahaan. Maksu- ja valuutta-

liikenne on siirtynyt suurilta osin verkkoon ja uusia haittaohjelmia kohdistetaan siihen. (Viestintävirasto, 31.1.2017.)

Vuoden 2016 helmikuussa Bangladeshissa kyberrikolliset saivat pankkien sähköistä rahaliikennettä manipuloimalla haltuunsa 66 miljoonaa euroa. Rikoshyöty olisi voinut ilman rikollisten tekemää inhimillistä virhettä olla yli miljardi euroa (Tivi 25.4.2016). Tapauksen selvittyä myös muualla maailmassa havaittiin, että samaa tietoteknistä haavoittuvuutta on hyödynnetty muuallakin.

Kyberrikolliset kehittävät kiristyshaittaohjelmia toimiala- ja yrityskohtaisesti. Kiristyshaittaohjelma salaa yrityksen päivittäisessä toiminnassa välttämättömien tietojen lisäksi myös yrityksen varmuuskopiot, joiden ajatellaan yleisesti olevan väline toipua haittaohjelman vaikutuksista. Rikolliset asettavat kiristyshaittaohjelman tekemien vahinkojen vaikutusten korjaamiseen tarvittavien keinojen hinnan kohdeorganisaation maksukyvyn mukaan. IoT-laitteiden määrän kasvaessa myös rikollisten tarkoituksiin kaapattujen IoT-laitteiden määrä kasvaa, koska niissä olemassa olevat haavoittuvuudet ovat edelleen olemassa. Rikollisten kaappaamien laitteiden määrä kasvattaa myös palvelunestohyökkäysten tehoa. Teollisuus- tai viihdelaitteiden käyttötarkoituksen vastainen hyödyntäminen rikoksissa voi synnyttää myös uudenlaisia häiriötilanteita niihin kytketyissä järjestelmissä. Erityisen vaarallista tämä on kriittisen infrastruktuurin tapauksessa. Viestintävirasto arvioi myös mobiililaitteiden kasvattavan kiinnostavuutta kyberrikosten alustana. (Viestintävirasto, 31.1.2017.)

4.3 F-Securen tilannekuvaraportti

F-Secure mittaa verkkohyökkäysten määrää niin kutsutulla "Honey pot" -verkolla. Honey pot -verkossa kyberrikollisten houkuttelemiseksi on rakennettu palvelinkoneita, jotka vaikuttavat sisältävän rikollisia kiinnostavaa tietoa. Niiden ainoa käyttötarkoitus on siis toimia houkuttimena. Rikollisten hyökätessä houkutinkoneisiin, kerää F-Secure tietoa hyökkäyksissä käytetyistä tekniikoista, menetelmistä ja hyökkäyksen alkuperästä. F-Securen mittalaitteet havaitsivat verkkohyökkäysten kasvaneen 223 % edellisestä vuodesta. Samoin kuin Interpol arvioi omassa tilannekuvaraportissaan, myös F-Secure arvioi osan kasvusta selittyvän kehittyneillä havaitsemismenetelmillä ja kasvaneella tietoturvaosaamisella. Selvää on kuitenkin se, että kyberrikollisuuden määräkin kasvaa. (F-Secure 2017.)

F-Securen mittausten perusteella kyberhyökkäyksistä 87 % on lähtöisin kymmenestä valtiosta. 44 % tapauksista eli selvästi suurimman osan alkuperä oli Venäjällä, 15 % Yhdysvalloissa ja 7 % Hollannissa. Hyökkäysten alkuperä ei kuitenkaan tarkoita sitä, että hyökkääjät itse olisivat fyysisesti noissa maissa. Hollannin suhteettoman suuri osuus hyökkäysten alkuperänä selittyykin todennäköisimmin sillä, että maan lainsäädäntö sallii niin sanotut ”Bulletproof”-palvelut. (F-Secure 2017.)

Hollantiin sijoitettua Bulletproof-palvelua myyvä palvelu voi markkinoida itseään sanomalla, että muualla Euroopassa kielletty sisältö on luultavasti sallittua Hollannissa. Käytännössä näillä palveluilla tarkoitetaan sitä, että esimerkiksi Hollannista voidaan ostaa laittoman tai lain harmaalla alueella sijaitsevan materiaalin säilyttämistä tai levittämistä varten rakennettu palvelin tai muu tekninen ratkaisu. Sisältöön mahdollisesti käynnistyvää esitutkintaa vaikeutetaan lainsäädännöllisiä hidasteita käyttämällä, muun muassa ylläpitämällä palveluita monikansallisessa ympäristössä. Jotkut palveluntarjoajat auttavat asiakkaitaan tilanteissa, joissa toiminta joutuu tutkinnan kohteeksi tarjoamalla heille lainopillisia neuvoja. (Pindrop)

Suomi ei ole globaalisti katsoen merkittävässä asemassa kyberrikosten tekijänä tai kohteena. Kaikista kyberhyökkäyksistä suurin osa tapahtuu Venäjältä Yhdysvaltoihin ja muistakin maista lähtöisin olevat hyökkäykset kohdistuvat pääasiassa Yhdysvaltoihin. (F-Secure 2017.)

Raportin yhteenvedossa F-Secure vahvistaa Europolin ja viestintäviraston näkemystä siitä, että kyberrikolliset kykenevät mukautumaan nopeasti teknologian kehitykseen ja reagoimaan nopeasti alalla tapahtuviin muutoksiin. Kyberrikollisuuden haasteet nähdään tällä hetkellä suurempana kuin koskaan. (F-Secure 2017.)

4.4 Yhteenveto raporteista

Kyberrikollisuuden suuret ilmiöt ovat pääsääntöisesti rajat ylittäviä ja niitä on usein vaikea tutkia yksittäisen valtion tasolle rajaamalla. Raportteja vertailemalla voi havaita sen, että eri maanosiin ja valtioihin kohdistuu erityyppisiä kyberrikoksia. Samoin eri maanosat ja valtiot ovat erityyppisten kyberrikosten alkuperä. Afrikasta EU:n jäsenvaltioihin kohdistuu pääasiassa petoksia ja sosiaaliseen manipulointiin perustuvia rikoksia kuten tietojen kalastelua. Suomessa tapahtuneista toimitusjohtajahuijauksista osa oli lähtöisin Afrikan maista

ja EU-kansalaisten pankkikorttitietojen väärinkäyttöä on tapahtunut eri Afrikan valtioissa (Europol, 27.9.2017).

Yksityisen sektorin raporteissa Afrikka ei nouse esille, sillä se on vielä verrattain pieni tekijä kyberrikollisuudessa. Tällä hetkellä kolmasosa Afrikan valtioista omaa alle 10 % internet-penetraation, joka on internet-yhteyden omaavien kansalaisten määrää kuvastava termi. Vastaava luku Amerikassa on 88 %, mutta internetin käyttäjistä mantereella asuu vain 8,6 %. Pienestä käyttäjäluvusta huolimatta Pohjois-Amerikan alue on ylivoimaisesti suurin kyberrikosten kohde jokaisen kyberrikostyypin kohdalla. Yhdysvallat on merkittävä tekijä tietotekniikan maailmassa yleisestikin ja siellä sijaitsee muun muassa merkittävä määrä maailman WEB-palveluista. EU-kansalaisten luottokorttien väärinkäytöistä suurin osa tapahtuu Yhdysvalloissa. (Europol, 27.9.2017.)

Euroopan sisältä kohdistuu enemmän kyberuhkia maanosan valtioille kuin muista maanosista yhteensä. Asiaa voi selittää Euroopan valtioiden poliisiviranomaisten tekemä yhteistyö. Euroopan sisäinen yhteistyö on kehittänyt valtioiden kykyä havaita ja tutkia tietoverkoissa tapahtuvaa rikollisuutta. Euroopan alueelta lähtöisin olevien keskitettyjen hyökkäysten katsotaan olevan lähtöisin Itä-Euroopan alueelta, pääasiassa Venäjältä. Eurooppaan kohdistuu Yhdysvaltojen jälkeen eniten taloudellisesti motivoituneita kyberrikoksia. Kehittynyt tekninen infrastruktuuri Euroopassa kiinnostaa kyberrikollisia ja useat botnet-hallintakoneet sijaitsevat tällä hetkellä Euroopassa. Europolin raportissa esitetyn arvion mukaan niistä sijaitsee Hollannissa jopa 24 % (Europol, 27.9.2017). Suomessa suurimmat kyberuhat koskevat tällä hetkellä huijauksia ja kiristyshaittaohjelmia (Viestintävirasto, 31.1.2017). Kiristyshaittaohjelmat aiheuttivat vuosien 2016 ja 2017 aikana suuria vahinkoja yksityishenkilöille ja yrityksille.

Aasiassa sijaitsee yli 50 % internetin käyttäjistä, mutta silti vain suhteettoman pieni osa globaaleista kyberuhista kohdistuu alueelle. Alueen valtioita kuten Kiinaa ja jossain määrin myös Pohjois-Koreaa pidetään monien kohdistettujen hyökkäysten alkuperänä. Suuri osa maailmalla tapahtuneista haittaohjelmien aiheuttamista ongelmista sai alkunsa niin kutsutusta Shadow Brokers -ryhmän julkaisemista hyökkäystyökaluista, jotka ryhmä kertoi anastaneensa Yhdysvaltojen palveluksessa toimivalta Equation Group -kyberalan ryhmältä. Julkaisun seurauksena laitevalmistajat käynnistävät kiireellisen päivityskampanjan työkalujen muodostamaa uhkaa vastaan, mutta vaikutukset olivat suuret siitä huolimatta. Julkais-

tuja työkaluja on käytetty ja niitä tullaan todennäköisesti käyttämään uusien haittaohjelmien kehityksessä.

Ennalta estämisen kannalta keskeisiksi toimenpiteiksi nähdään kyberhyökkäystyökalujen, kiristyshaittaohjelmien ja muiden haittaohjelmien sekä DDOS-sovellusten sekä botnetien kehittäjiin ja tarjoajiin keskittyminen (Europol, 27.9.2017). Merkittäväksi torjuntakeinoksi sosiaaliseen manipulointiin perustuville rikoksen tekotavoille raportti esittää kansalaisten kouluttamista ajankohtaisista kyberrikosilmiöistä. Tällä pystyttäisiin vaikuttamaan muun muassa toimitusjohtajahuijauksiin. EU:n jäsenvaltioiden suositellaan muodostuvan yhteiseurooppalainen valistus- tai koulutusjärjestelmä ajankohtaisten ilmiöiden torjumiseksi. Verkossa tapahtuvan lasten seksuaaliseen hyväksikäyttöön liittyvien rikosten tutkintaa varten EU:n jäsenvaltioiden tulisi varmistaa, että tutkintaviranomaisella on käytettävissä riittävät tutkintatyökalut ja resurssit, joilla tutkinta voidaan tehdä tehokkaasti.

Darknetissä toimivan rikollisuuden kuten rikollisen materiaalin myyntipaikkojen horjuttaminen ja sulkeminen edellyttää globaalilla tasolla koordinoitua yhteistyötä alan toimijoiden kesken. Darknetin rikollisuutta tutkivien viranomaisten tietotaidon ja työkalujen laadun riittävä taso on myös keskeisessä asemassa. Ilman ajantasaista ja syvällistä ymmärrystä Darknetin sen hetkisistä ilmiöistä ja toimintatavoista, ovat rikolliset jatkuvasti viranomaisten tavoittamattomissa. Kyberrikollisuuden kasvavan uhan vuoksi lainsäädäntöä tulisi kehittää siten, että mahdollistaa viranomaisten läsnäolon ja toimimisen tietoverkoissa. Kyberrikollisuuteen vajavaisesti soveltuva lainsäädäntö johtaa jatkuvasti sekä tutkittavien johtolankojen menetykseen että kykyyn asettaa kyberrikoksia syyteharkintaan.

4.5 Kyberrikollisuuden vaikutukset

Kyberrikollisuuden vaikutuksia rahallisina kustannuksina on vaikea mitata sen synnyttämien epäsuorien kustannusten ja vaikeasti havaittavien vaikutusten vuoksi. Siitä syystä asiasta ei ole olemassa kattavaa tilastotietoakaan. Tietotekniikka-alan ammattilaisten keskuudessa vallitsee kuitenkin konsensus siitä, että kyberrikoksilla globaalisti aiheutetut kustannukset olivat maltillisen arvion mukaan vuonna 2015 noin 500 miljardia euroa (Forbes, 17.1.2016) ja korkeimman arvion mukaan noin 2 500 miljardia (2,5 biljoonaa) euroa (Cybersecurity ventures 16.10.2017). Kokonaiskustannus muodostuu useista eri tekijöistä. Näitä ovat datan vahingoittuminen ja tuhoutuminen, organisaation tuottavuuden lasku, immateriaalioikeuksien loukkaukset, henkilö- ja taloustietojen anastukset sekä petokset.

Rikosten kohteeksi joutuneiden organisaatioiden tietojärjestelmien sekä mainevahinkojen korjaukset synnyttävät myös kustannuksia, joiden tarkka määrä voi olla vaikeasti arvioitavissa. Luku sisältää myös teknisen rikostutkinnan kustannukset. Kyberrikollisuuden arvioidaan olevan tällä hetkellä nopeimmin maailmalla kasvava ja kehittyvä rikoslaji myös siitä saadun rikoshyödyn vuoksi.

Eri menetelmiin perustuvia kyberrikoksia kuten palvelunestohyökkäyksiä tarjotaan rikollisten toimesta kutsutulla CaaS (Crime-as-a-Service)-mallilla. CaaS-malli pohjautuu pääasiassa IT-alan liike-elämässä käytettyyn IaaS (Infratructure-as-a-Service), PaaS (Platform-as-a-Service) ja SaaS-palvelumalliin (Software-as-a-Service). Näissä palvelumalleissa asiakas voi vuokrata tarvitsemansa tietoteknisen palvelun käyttöönsä siihen erikoistuneelta toimijalta. Asiakas itse säästyy monimutkaisen teknisen sovelluksen kehitystyöltä ja mahdollisilta lisenssikustannuksilta. CaaS-malli mahdollistaa hyvin tuhovoimaisten ja teknisesti edistyneiden kyberhyökkäysten tekemisen ilman teknistä osaamista. CaaS-malli käsittää useita eri ”as-a-Service”-malleja kuten Hacking-as-a-Service-, Money-Laundering-as-a-Service-, jotka ovat osa kyberrikosten maailmaa. Kaikki kyberrikosten maailman toimijat eivät siis ole varsinaisia hyökkääjiä, osa tekijöistä on tarjoamassa kasvaville markkinoille tekovälineitä. (Europol 2014, 29.9.2014.)

Kyberrikoksilla saadun rikoshyödyn arvioidaan ylittäneen globaalin huumekaupan vuosittaisen rikoshyödyn, jonka on arvioitu olevan 356 – 544 miljardia euroa (Global Financial Integrity, 27.3.2017). Vuosittaisen kehityksen perusteella kyberrikollisuuden kustannusten uskotaan ylittävän viiden biljoonan euron vuosikustannukset vuoteen 2021 mennessä (Cybersecurity ventures, 16.10.2017). Viimeisten vuosien aikana kyberrikollisuutta on kuvattu muun muassa Yhdysvaltain kansallisen turvallisuusvirasto NSA:n ja tietoturva-asiantuntijoiden toimesta historiamme suurimmaksi varainsiirroksi. Tällä tarkoitetaan pääasiassa länsimaihin kohdistuneen verkkovakoilun tuloksena saatuja yrityssalaisuuksia ja sähköistä materiaalia. (CNN, 4.8.2011.), (Zero day, 10.7.2012.)

5 JOHTOPÄÄTÖKSET JA POHDINTA

Opinnäytetyöskentelyni aikana syvennyin kansainvälisten toimijoiden tilannekuvaraportteihin ja Suomen tilastotietoihin kyberrikollisuuden ilmiöitä koskien. Tilannekuvaraporttien pohjalta syntyy käsitys, että kyberrikollisuudessa hyödynnetyt menetelmät monimutkaistuvat ja toiminta ammattimaistuu. Tietoverkot ovat kustannustehokas kanava vaikuttaa ihmisten mielipiteisiin ja niistä onkin tullut yksi hybridivaikuttamisen pääasiallisista välineistä. Tietoverkot ovat helppo ja halpa tapa tehdä tietokoneavusteisia rikoksia kuten petoksia.

Kyberrikollisuuden merkittävät ilmiöt ovat usein kansainvälisiä ja niiden taustalla on järjestäytynyttä rikollisuutta. Kyberrikollisuudessa erityistä on silti se, että yksittäinen tekijäkin kykenee teknologiaa hyödyntämällä tekoihin, jonka vaikutukset voivat heijastua useisiin eri valtioihin. Yhteiskunnan kannalta tärkeistä toiminnoista vastaavaa kriittistä infrastruktuuria kytketään osaksi internetiä, mutta teknisessä toteutuksessa käytettävän laitteiston tietoturvaominaisuudet eivät välttämättä ole riittäviä torjumaan keskitettyä kyberhyökkäystä.

Ammattimaisemmat kyberrikokset voivat olla asiantuntijaryhmien suorittamia operaatioita, joiden suunnittelu- ja toteutusvaiheet voivat olla kestoltaan kuukausien tai jopa vuosien mittaisia. Operaatioiden rahoituksen taustalla voi olla valtiolliset toimijat, jotka testaavat kyberkykyjään. Tällaiset suunnitelmallisesti toteutetut keskitetyt hyökkäykset voivat olla teknisesti niin edistyneitä, että ne voivat jäädä kokonaan havaitsematta alan tietoturvaosaajiltakin. Tämä ilmiö asettaa suuria haasteita niin rikoksen kohteiksi valikoituvien organisaatioiden kuin viranomaistenkin toiminnalle. Yksittäisen valtion poliisin resurssit ovat usein riittämättömät laajojen kyberrikosten tutkimiseksi ja laajat yhteistyöverkostot alkavat olla välttämättömyys.

Euroopassa yhteistyötä tehdään laajasti eri jäsenvaltioiden kesken, mutta toiminnassa on vielä paljon kehittämisen varaa yhtenäisen lainsäädännön ja toimintatapojen luomisen osalta. Kyberrikollisten parissa nämä heikkoudet varmasti tunnistetaan ja niitä osataan hyödyntää rikollisessa toiminnassa.

Opinnäytetyön produktina syntyneessä kirjausohjeessa kyberilmiöt eivät suoranaisesti tule esille, mutta ohjeen toimimalla yksittäisten kyberrikosten tutkintaa voidaan tehostaa. Ym-

märrys kyberrikollisuuden ilmiöistä kuitenkin parantaa poliisin ja kyberrikosten kohteiden kykyä havaita tapahtuneet kyberrikokset. Luokittelutietojen ja yksilöivien tunnisteiden yhdenmukaisilla kirjausmenettelyillä mahdollistetaan myös rikossarjoja paljastava toiminta. Yhdistettäessä rikosilmoituksen kirjausvaiheessa kerätyt tunnistetiedot toimivaan yhteistyö- ja tiedonjakoverkostoon, voi yksittäisen rikosilmoituksen kirjaaminen tuottaa hyvin arvokasta lisätietoa tutkittavana olevaan kokonaisuuteen. Kirjausohjeen periaatteet ovat sellaisia, joita voisi soveltaa minkä tahansa rikostyypin kirjaamisessa rikostyypille ominaisia tunnistetietoja keräämällä. Kirjausohjeen mukaan toimiminen palveleekin siinä mielessä kahdella eri tasolla: esitutkinnan laadun parantumisella kirjauskäytäntöjen kautta ja analyysikelpoisen tiedon tuottamisella.

Kirjausohjeen suunnitteluvaihe oli ammatillisen kasvun kannalta merkittävä prosessi. Prosessin aikana rikosilmoituksen kirjauksen ja alkutoimien merkitys esitutkinnassa kirkastui mielessäni. Ymmärrys luokittelutietojen asianmukaisesta käytön merkityksestä kasvoi samalla, kun käsitys tietotekniikkarikollisuuden ilmiöiden suuresta kokoluokasta alkoi hahmottua. Tietotekniikkarikollisuuden torjunnan täytyy perustua tietojohtoiseen toimintaan, jossa tiedustelu- ja analyysitoiminta ovat tärkeässä roolissa. Jokaisen rikosilmoituksia kirjaavan henkilön tulisi omalta osaltaan tuottaa laadukasta tietoa analyysitoiminnan tueksi.

Rikostutkijoilta saadun palautteen perusteella kirjausohjeeseen on onnistuttu tiivistämään paljon niitä asioita, joita rikosilmoituksen kirjaamisen yhteydessä tulisi huomioida. Monet kirjausohjeen asiat ovat sellaisia, jotka unohtuvat helposti tai niitä ei koeta merkityksselliseksi. Tästä syystä voisikin pohtia, että olisiko rikosilmoituksen kirjaamisen yhdenmukaistamista järkevintä tehdä tietojärjestelmän käyttöliittymää kehittämällä. Olisiko viranomaisten tietojärjestelmissä mahdollista pakottaa käyttäjä kirjaamaan sellaiset asiat, jotka ovat rikostiedustelu- ja analyysitoiminnalle välttämättömiä? Tapauksessa, jossa kirjaaja valitsee rikosnimikkeeksi tietojärjestelmän häirintä, pakottaisi tietojärjestelmä syöttämään tai ainakin arvioimaan luokittelu- ja tunnistetietojen tarpeellisuutta. Tämä ohjaisi rikosilmoituksen kirjaavaa henkilöä selvittämään ilmoittajalta kaikki ne asiat, jotka ovat tulevan esitutkinnan kannalta kaikkein keskeisimpiä.

LÄHTEET

Nettisivustot:

Cyber Security Ventures 2017: Morgan, Steve. Cybercrime Report. Luettavissa: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. Luettu 2.12.2017

Forbes 2016: Morgan, Steve. Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Luettavissa: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#13799853a913. Luettu 5.12.2017

Gartner 2017: van der Meulen, Rob. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Luettavissa: https://www.gartner.com/newsroom/id/3598917. Luettu 15.5.2018

Gartner 2015: van der Meulen, Rob. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. https://www.gartner.com/newsroom/id/3165317. Luettu 15.5.2018

Global financial Integrity 2017: May, Channing. Transnational Crime and the Developing World, By. Luettavissa: http://www.gfintegrity.org/report/transnational-crime-and-the-developing-world/.Luettu 2.1.2018

Helsingin yliopisto 2017: Näsi. Matti; Tanskanen, Maiju. Rikollisuustilanne 2016. Luettavissa: https://helda.helsinki.fi/handle/10138/191756. Luettu 23.05.2018

Kotimikro 2015: Mitä on malware? Luettavissa: http://kotimikro.fi/tietoturva/haittaohjelmat/mita-on-malware. Luettu 10.5.2018

Symantec: Advanced Persistent Threats: A Symantec Perspective. Luettavissa: https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf. Luettu 15.5.2018

Symantec 2016: Mirai: what you need to know about the botnet behind recent major DDoS attacks. Luettavissa: https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks. Luettu 16.1.2018

Tivi 2016: Karkimo, Ari. Ei palomuuria, 10 taalan reititin: näin 80 miljoonan puhallus onnistui. Luettavissa: https://www.tivi.fi/Kaikki_uutiset/ei-palomuuria-10-taalan-reititin-nain-80-miljoonan-puhallus-onnistui-6544545. Luettu 25.4.2018

TorProject: Tor overview. Luettavissa: https://www.torproject.org/about/overview.html.en. Luettu 3.1.2018

US-CERT 2013: Understanding Denial-of-Service Attacks. McDowell, Mindi. Luettavissa: https://www.us-cert.gov/ncas/tips/ST04-015. Luettu 29.12.2017

Wikipedia 2017: Screenshot of a WannaCry ransomware attack on Windows 8. Luettavissa: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#/media/File:Wana_Decrypt0r_screenshot.png. Luettu 3.1.2018

Tilannekuvaraportit:

Europol 2017: IOCTA 2017. Luettavissa: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017. Luettu 10.1.2018

F-Secure 2017: [Report] Cyber Attack Landscape of 2017, So Far. Luettavissa: https://business.f-secure.com/report-cyber-attack-landscape-of-2017-so-far. Luettu: 10.1.2018

F-Secure 2017: BOTNETS. Luettavissa: https://www.f-secure.com/en/web/labs_global/botnets. Luettu 28.12.2017

Viestintävirasto 2017: Tietoturvan vuosi 2016. Luettavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf. Luettu 2.12.2017

Viestintävirasto 2017: 10 tietoturvanäkymää vuodelle 2017. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/01/ttn201701171301.html. Luettu 2.12.2017

Uutiset ja blogit:

CNN 2011: Neild, Barry. Massive cyberspying operation targeted U.S., U.N., others. Luettavissa: http://edition.cnn.com/2011/TECH/web/08/03/cyber.attacks.shady.rat/index.html. Luettu 29.12.2017

CNN 2017: Watkings, Eli. White House officially blames North Korea for massive 'WannaCry' cyberattack. Luettavissa: http://edition.cnn.com/2017/12/18/politics/white-house-tom-bossert-north-korea-wannacry/index.html. Luettu 12.1.2018

Krebs, Brian 2016: KrebsOnSecurity Hit With Record DDoS. Luettavissa: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. Luettu 2.12.2017

Krebs, Brian 2017 Correcting the Record on vDOS Prosecutions. Luettavissa: https://krebsonsecurity.com/2017/11/correcting-the-record-on-vdos-prosecutions/. Luettu 2.12.2017

Lakimiesuutiset 2017: Aukia, Jussi-Pekka. Kyberrikollisuus eli tietojärjestelmiin kohdistuva rikollisuus. Luettavissa: https://lakimiesuutiset.fi/9144-2/. Luettu 5.12.2017

Limnell, Jarno. Tietomurrot Yhdysvalloissa on poliittisesti vaikea asia. https://blogit.iltalehti.fi/jarno-limnell/2016/08/04/tietomurrot-yhdysvalloissa-on-poliittisesti-vaikea-asia/

Microsoft 2017: Smith, Brad. The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. Luettavissa: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/. Luettu 5.12.2017

New York Times 2017: Hirschfeld Davis, Julie. Following the Links From Russian Hackers to the U.S. Election. Luettavissa: https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html. Luettu 5.12.2017

New York Times 2016: Hirschfeld Davis, Julie ja Sangerdec, David. Obama Says U.S. Will Retaliate for Russia's Election Meddling. Luettavissa: https://www.nytimes.com/2016/12/15/us/politics/russia-hack-election-trump-obama.html. Luettu 5.12.2017

Pindrop, Inside the fight against Bulletbroof hosting providers. Luettavissa: https://www.pindrop.com/blog/inside-the-fight-against-bulletproof-hosting-providers/. Luettu 15.5.2018

Piiroinen, Timo 2016: Poliisin kyberkeskukselle lentävä lähtö. http://www.polamk.fi/avauksia/kirjoitukset/1/0/timo_piiroinen_poliisin_kyberkeskukselle_lentava_lahto_43689. Luettu 2.12.2017

Telia 2017: Kärki, Heta. KÄVIKÖ DIGIVARAS KOTONASI VIIME YÖNÄ? Luettavissa: https://www.telia.fi/kauppa/palvelut/tietoturva/artikkeli/kaviko-digivaras-kotonasi-newsroom. Luettu 3.1.2018

Washington Post 2017: Erickson, Amanda. What you need to know about the massive hack that hit the British health-care system and elsewhere. Luettavissa: https://www.washingtonpost.com/news/worldviews/wp/2017/05/12/what-you-need-to-know-about-the-massive-hack-that-hit-britain-and-11-other-countries/?utm_term=.6494ab5303c2. Luettu 13.1.2018

Washington Post 2018: Nakashima, Ellen. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. Luettavissa: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?noredirect=on&utm_term=.40c2af947d0e. Luettu 23.5.2018

Washington Post 2016: Peterson, Andrea. Researchers remotely hack Tesla Model S. Luettavissa: https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s/?utm_term=.8b676513a859. Luettu 9.1.2018

Wired 2017: Graff, Garrett M. How a Dorm Room Minecraft Scam Brought Down the Internet. Luettavissa: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/. Luettu 2.12.2017

YLE 2017: Sundqvist, Vesa. Palvelunestohyökkäys haittaa Kanta-palveluiden toimintaa. Luettavissa: https://yle.fi/uutiset/3-9854962. Luettu 2.12.2017

ZDNET 2012: Protalinski, Emil. NSA: Cybercrime is 'the greatest transfer of wealth in history'. Luettavissa:
http://www.zdnet.com/article/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history/. Luettu 29.12.2017

ZDNET 2017: Palmer, Danny. Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk.
https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/. Luettu 23.05.2018

Viranomaislähteet:

Eur-Lex 2013: EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI 2013/40/EU. Luettavissa:
https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32013L0040&from=EN. Luettu 15.4.2018

Europol 2014: ORGANISED CRIME GROUPS EXPLOITING HIDDEN INTERNET IN ONLINE CRIMINAL SERVICE INDUSTRY. Luettavissa:
https://www.europol.europa.eu/newsroom/news/organised-crime-groups-exploiting-hidden-internet-in-online-criminal-service-industry. Luettu 2.12.2017

FBI 2018: Luettavissa: https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev. Luettu 10.1.2018

HE 94/1993 vp: Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi. Luettavissa:
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_94+1993.pdf.
Luettu 1.12.2017

HE 232/2014 vp, Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi. Luettavissa:
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_232+2014.pdf. Luettu 1.12.2017

Poliisi 2017, Kyberrikollisuus
http://www.poliisi.fi/rikokset/kyberrikollisuus. Luettu 2.2.12.2017

Suomen kyberturvallisuusstrategia. Turvallisuuskomitea 2013: Suomen kyberturvallisuusstrategia ja taustamuistio.
https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf. Luettu 22.05.2018

Viestintävirasto 2017: Reaper-bottiverkko saastuttaa IoT-laitteita. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/11/ttn201711011452.html. Luettu 9.12.2017

Viestintävirasto 2017: Mirai voi hyvin – sinun modeemissasi! Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/08/ttn201708181500.html. Luettu 17.1.2018

Viestintävirasto 2016: Mirai-bottiverkko on ottanut haltuunsa tuhansien suomalaisten modeemeja. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/11/ttn201611291741.html. Luettu 2.12.2017

Viestintävirasto 2016: IoT-bottiverkot etsivät aktiivisesti internetiin kytkettyjä laitteita. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/10/ttn201610181402.html. Luettu 2.12.2017

LIITTEET

Liite 1: Tietotekniikkarikosten kirjaaminen ja alkutoimet -ohje

Liite 2: Tietotekniikkarikosten kirjaaminen ja alkutoimet, tukimateriaali