Verkkorikollisuuden muodot 2020-luvulla

Sami Tiainen

11/2021

Poliisiammattikorkeakoulun opinnäytetyö / AMK

TIIVISTELMÄ

Sami Tiainen: Verkkorikollisuuden muodot 2020-luvulla
Opinnäytetyön muoto: Tutkimuksellinen
Julkisuusaste: Julkinen
Ohjaaja: Ossi Kaario, Kari Koppanen
Tutkinto: Poliisi (AMK)

Verkkorikollisuuden historia on muihin rikostyyppeihin verrattuna melko lyhyt. Teknologian nopea kehittyminen on muodostanut monenlaisia uusia rikollisuuden ilmiöitä sekä muuttanut perinteisempien rikosten toteuttamistapoja. Verkkorikollisuus lisääntyy nopeasti, monimuotoistuu sekä asettaa uudenlaisia haasteita myös poliisin näkökulmasta.

Verkkorikollisuuden jatkuvan muutoksen sekä siihen sisältyvien uhkakuvien vuoksi ilmiön tulevaisuuden ennakoiminen on rikostorjunnan sekä tilannekuvan muodostamisen kannalta erittäin tärkeää. Verkkorikollisuuden suurina tulevaisuuden trendeinä ovat kansainvälistyminen, järjestäytyminen sekä mahdollisesti tekoälyn hyödyntäminen rikollisissa tarkoituksissa.

Tämä tutkimuksellinen opinnäytetyö käsittelee verkkorikollisuutta rikollisuuden muotona 2020-luvulla. Opinnäytetyö jakautuu kolmeen pääosaan, joista ensimmäisessä esitellään verkkorikollisuuden käytännön ilmenemismuotoja. Toinen pääkappale käsittelee ilmiön nykyistä tilannekuvaa. Viimeisessä kappaleessa käsitellään verkkorikollisuuden kehittymistä tulevaisuudentutkimukseen ja alan asiantuntijoiden näkemyksiin pohjautuen.

Opinnäytetyön tavoitteena on käsitellä verkkorikollisuutta helposti lähestyttävän oppaan kaltaisesti. Tarkoituksena ei ole syventyä teknisiin yksityiskohtiin, eikä verkkorikollisuuden marginaali-ilmiöihin vaan työn keskeisenä ajatuksena on nimenomaan ytimekkään kokonaiskuvan muodostaminen.

Sivumäärä: 35
Tarkastuskuukausi ja vuosi: 11/2021
Avainsanat: Kyberrikos, Verkkorikos, Verkkorikollisuus, Internet, Tekoäly

SISÄLLYS

1 JOHDANTO

Internetin käytön valtava lisääntyminen on vaikuttanut monin tavoin ihmisten elämään. Länsimainen tietoyhteiskunta pohjautuu nykyään hyvin vahvasti internetin monipuoliseen hyödyntämiseen. Internetin käytöllä kokonaisuudessaan on kiistattomia ja positiivisia vaikutuksia. Sujuvien internet-yhteyksien avulla ihmiset voivat esimerkiksi olla yhteydessä toisiinsa, ostaa mitä tahansa, mistä tahansa ja milloin tahansa.

Internetin käytön valtava lisääntyminen ei kuitenkaan ole tuonut pelkästään positiivisia vaikutuksia mukanaan vaan myös uhkakuvia. Siellä missä on ihmisiä, on myös rikollisia, eikä internet ei ole asian suhteen poikkeus. Internetin avulla rikollisetkin voivat viestiä keskenään, verkostoitua, suunnitella ja toteuttaa rikoksia tavoilla, jotka ennen eivät olleet mahdollisia.

Tämän opinnäytetyön tarkoituksena on toimia yleisluontoisena oppaana internetissä tapahtuvaan rikolliseen toimintaan. Työn tausta-ajatuksena on ollut ajatus oppaasta, joka toisi ymmärrettävästi esiin kyberrikollisuuden ilmiönä siitäkin huolimatta, että aihepiiri käsitteineen ei olisi ennestään tuttu.

Opinnäytetyö jakautuu kolmeen pääosaan. Ensimmäinen osa on verkkorikollisuuden käytännön ilmenemismuotoja käsittelevä kappale. Toinen verkkorikollisuuden nykytilaa käsittelevä ja viimeinen verkkorikollisuuden tulevaisuutta käsittelevä kappale.

Erityisesti poliisin toimintaan liittyen aihepiirin ympärillä on salassa pidettävää tietoa. Tämän työn tarkoituksena on olla kokonaan julkinen ja tämän vuoksi työ on koostettu yksinomaan julkisista lähteistä, jotta lopputulos olisi täysin julkinen.

1.1 Opinnäytetyön tutkimuskysymys

Tämän opinnäytetyön tutkimuskysymyksenä on tarkastella sitä, minkälainen verkkorikollisuuden kokonaiskuva tällä hetkellä on ja mikä se tulee todennäköisesti olemaan tulevaisuudessa. Tarkoituksena on vastata kahteen pääkysymykseen;

1. Mitä rikoksia verkossa tällä hetkellä tapahtuu?
2. Miten verkkorikollisuuden voidaan ennakoida kehittyvän tulevaisuudessa?

Ensimmäisen kysymyksen osalta tarkoituksena on käsitellä kattavasti verkkorikollisuuden tärkeimpiä ja keskeisimpiä ilmenemismuotoja. Tarkastelun ulkopuolelle jätetään myöhemmin kerrotuin perustein useita verkkorikollisuuden ilmiöitä, jotka eivät eri syistä ole tarpeellisia tarkastella osana kokonaiskuvaa. Tarkoituksena ei ole syventyä yhteen tiettyyn rikostyyppiin erityisen syvällisesti vaan muodostaa kokonaiskuva siitä, mitä rikoksia verkossa tapahtuu. Tarkoitus on huomioida myös se, miten tämä globaali ilmiö näkyy nimenomaan Suomessa.

Verkkorikollisuuden kehittymisen ennakointi on toinen tutkimuskysymys. Kysymykseen liittyen tarkastellaan sitä, millä tavoin verkkorikollisuuden voidaan ennustaa ilmenevän tulevaisuudessa. Näkökulma on tarkoituksellisesti osittain globaali johtuen ilmiön globaalista luonteesta. Tulevaisuuden ennakointi pohjautuu aiheesta löytyvään kirjallisuuteen ja alan asiantuntijoiden näkemyksiin.

Verkkorikollisuus on lopulta melko uusi ja nopeasti kehittyvä ilmiö, joten aiheeseen liittyvää koottua tietoa ei ole saatavilla yhtä laajasti kuin perinteisemmistä rikostyypeistä. Myös tämän takia aihetta yleisestä näkökulmasta käsittelevä opinnäytetyö on perusteltu ja tarpeellinen.

1.2 Opinnäytetyön metodologia

Opinnäytetyö on tutkimuksellinen, tarkemmin määriteltynä kuvaileva kirjallisuuskatsaus. Kuvaileva kirjallisuuskatsaus on kirjallisuuskatsaus, jossa ei ole tarkkaa metodologista säännöstöä. Se myös sallii vapaamman tutkimuskysymysten valinnan. Näennäisestä metodologisesta vapaudesta huolimatta kuvailevassa kirjallisuuskatsauksessa pystytään kuvaamaan tarkastelun kohteena olevaa ilmiötä laajasti ja systemaattisesti. (Salminen, 2011, s. 6)

2 VERKKORIKOLLISUUS ILMIÖNÄ

2.1 Internetin käytön lisääntyminen

Internet itsessään on moniin keksintöihin verrattuna melko tuore keksintö, joka vain vähän aikaa sitten ei vaikuttanut maailmaan millään tavalla. Siinä missä keskivertaisessa suomalaisessa kodissa oli 1990-luvulla keskimäärin yksi laite, joka hyödynsi internet-yhteyttä, oli kodeissa vuonna 2015 jo noin 10 laitetta, jotka hyödyntävät Internetiä toimiakseen (Peltomäki, 2015, s. 16-17). Aikaisemmin internet ei tuottanut keskimääräiselle käyttäjälleen suurta hyötyä, mutta vain muutamassa vuosikymmenessä tilanne on muuttunut siten, että internetiä hyödynnetään lähes jokaisella elämän osa-alueella lisääntyvästi aina ruokaostoksista elämänkumppanin löytämiseen. Suuri osa rahallisista transaktioista kulkee sähköisesti internetin välityksellä ja kuka tahansa voi olla helposti yhteydessä mihin päin maailmaa tahansa. On vaikea keksiä montaa elämän osa-aluetta, johon internet ei jollain tavalla liittyisi tänä päivänä.

Alkuvuonna 2021 globaalista maailman väestöstä 59,5 % (4,66 miljardia ihmistä) käyttää internetiä (Statista.com, 2021.) Cybersecurity Ventures ennustaa, että 90% maailman väestöstä tulee olemaan internetin käyttäjiä vuoteen 2030 mennessä. Tämä tarkoittaisi sitä, että mikäli maailmassa tulee olemaan ennusteiden mukaisesti väestöä 8,5 miljardia ihmistä, heistä internetin käyttäjiä olisi 7,5 miljardia. (Cybersecurity Ventures, 2021)

2.2 Internet ja rikokset

Internet tarjoaa rikoksen tekijöille uusia tapoja tehdä rikoksia. Mediasta voi lukea lähes päivittäin esimerkiksi pankkien tiedotteita asiakkailleen, joissa kehotetaan olemaan varovaisia, etteivät he tule huijatuksi pankin sivua jäljittelevillä huijaussivustoilla. Internetissä tapahtuu paljon huijauksia erilaisilla myyntipalstoilla, ihmisistä levitetään perättömiä tietoja sosiaalisessa mediassa ja ihmiset myyvät huumeita ja muuta laitonta tavaraa internetissä. Luetteloa voisi jatkaa loputtomiin. Tässä opinnäytetyössä huomiota kiinnitetään eniten niihin rikollisuuden muotoihin, jotka kaikista verkkorikollisuuden muodoista ovat yleisimpiä.

2.2.1 Verkkorikollisuuden määritelmästä

Verkkorikollisuuden määrittely ei ole aivan yksiselitteistä. Ovatko verkkorikollisuutta vain ne rikokset, joita tehdään suoranaisesti tietoverkoissa tietoverkkoja tai sen osia itseään kohtaan vai onko verkkorikollisuutta myös se, kun tietoverkkoja käytetään hyväksi rikoksen tekemisessä. Onko se verkkorikollisuutta, jos henkilö ostaa verkosta huumeita, jotka kuitenkin toimitetaan henkilölle paikan päällä?

Poliisin näkökulmasta termi verkkorikollisuus (myös *kyberrikollisuus*) voidaan jakaa kahteen osa-alueeseen. Ensimmäisessä osa-alueessa ovat rikokset, jotka kohdistuvat tietoverkkoympäristöön sinänsä. Toisessa kategoriassa ovat rikokset, joissa tehdään rikoksia siten, että rikosten tekemisessä hyödynnetään tietoverkkoja. Tietoverkkoympäristöön sinänsä kohdistuvat rikokset eroavat tietoverkkoja hyödyntäen tehdyistä pääosaltaan siten, että ensimmäisen kategorian teot tapahtuvat tietoverkon itsensä sisällä ja tietoverkkoa itseään vastaan. Rikollinen teko voi kohdistua esimerkiksi johonkin tietoverkon osaan, esimerkiksi tietokantajärjestelmään tai palvelimeen. Toisessa kategoriassa eli tietoverkkoja hyödyntämällä tehdyissä rikoksissa skaala on huomattavasti laajempi ja se kattaa kaikki rikokset, joiden tekemisessä tietoverkkoja voidaan käyttää hyväksi. (Sisäministeriö, 2017, s. 10 - 11)

Tässä opinnäytetyössä puhutaan niin tietoverkon sisäisistä, kuin sen avullakin tehdyistä rikoksista, sillä opinnäytetyön tutkimuskysymyksenä on antaa yleiskuva siihen, mikä internetin rooli on rikollisuudessa tämän päivän toimintaympäristössä. Tämän päivän verkkorikollisuus sisältää kumpiakin verkkorikostyyppejä, joten pelkästään toiseen keskittyminen ei palvelisi kokonaiskuvan muodostamista.

2.3 Rajauksia

Verkkorikollisuus itsessään on hyvin laaja ilmiö. Sabillon kollegoineen on listannut erittäin kattavasti erilaisia verkkorikollisuuden ilmenemismuotoja. Heidän julkaisussaan International Journal of Computer Networks and Communications Securityssä on listattu peräti 89 erilaista verkkorikollisuuden ilmenemismuotoa. (Sabillion et al, 2016)

Tämän opinnäytetyön tarkoituksena on siis antaa yleinen kuva verkkorikollisuudesta ilmiönä ja on selvää, ettei esimerkiksi kaikkia edellä mainittuja 89:ää ilmenemismuotoa ole mielekästä käsitellä. Tämän takia olen nähnyt järkeväksi rajata tarkastelun ulkopuolelle sellaiset verkkorikollisuuden ilmiöt, joissa rajanveto toiminnan rikollisuuden ja laillisuuden välillä on epäselvä, vaikka toiminnalla olisikin rikolliset motiivit. Ulkopuolelle on jätetty myös sellaiset tietoverkoissa tai niitä hyödyntäen tehdyt teot, jotka edustavat tämän hetken verkkorikollisuuden kontekstissa lähinnä marginaali-ilmiöitä.

Sivuan kuitenkin verkkorikollisuuden tulevaisuutta koskevassa kappaleessa joitakin verkkorikollisuuden kontekstissa tämän hetken marginaali-ilmiöihin kuuluvia ilmiöitä, kuten esimerkiksi tekoälyn käyttöä verkkorikoksissa. Näin siksi, että osa marginaali-ilmiöistä, kuten juuri tekoäly, voi potentiaalisesti olla osa verkkorikollisuuden tulevaisuuden isompaa kokonaiskuvaa. Osa nyt marginaali-ilmiöin tasolla olevista ilmiöistä voi myös tulevaisuudessa olla jopa niin sanottuja *mustia joutsenia* verkkorikollisuuden kontekstissa.

Nassim Taleb kuvaa mustan joutsenen käsitettä siten, että pitkään ihmiset uskoivat, että joutsenet ovat ainoastaan valkoisia ja näin musta joutsen oli metafora mahdottomasta. Lopulta joku löysi Australian

seudulta mustan joutsenen ja mahdottomasta tuli totta. Musta joutsen on siis tapahtuma, jonka todennäköisyys on todella pieni, mutta tapahtuessaan tapahtuma aiheuttaa suuria vaikutuksia. Tällainen musta joutsen oli esimerkiksi syyskuun 11. päivän iskut. Jokin verkkorikollisuuden nyanssi voikin tulevaisuudessa näytellä jopa korostuneen suurta roolia ja muuttaa rikollisuuden kokonaiskuvaa. (Taleb, 2007)

Opinnäytetyössä tarkastelun ulkopuolelle on jätetty myös paljon sellaisia rikollisuuden muotoja, jotka eivät suoranaisesti kohdistu vaikutukseltaan yksityishenkilöihin tai yrityksiin. Ulkopuolelle on siis jätetty esimerkiksi verkon välityksellä tehty vakoilu ja hybridivaikuttaminen, vaikka näissä on kyse rikollisista ilmiöistä, joiden tarkoituksena voi olla aiheuttaa vakavaa haittaa suomalaiselle yhteiskunnalle ja siten lopulta myös yksilölle. Lisäksi tarkastelun ulkopuolelle on jätetty sellaisia verkkorikollisuuden ilmenemismuotoja, joiden selittäminen vaatisi myös ilmiön taustalla vaikuttavan teknologian syvällistä avaamista lukijalle.

Aihepiirin laajuuden sekä tutkimuskysymysten takia tämän opinnäytetyön ei ole tarkoitus ottaa myöskään kantaa rikosten käytännön tutkintaan. Rikosten käytännön tutkintaan liittyy usein myös salassa pidettäviä tietoja, jotka eivät kuulu julkiselle foorumille. Opinnäytetyössä ei oteta kantaa rikosten ennaltaehkäisyyn.

3 VERKKORIKOLLISUUDEN KÄYTÄNNÖN ILMENEMISMUODOT

Verkkorikollisuuden ilmenemismuotoja on olemassa todella monia. Olen valinnut tähän kappaleeseen tarkempaan tarkasteluun kaikista oleellisimpia verkkorikollisuuden muotoja. Oleellisimmiksi on nähty yleiset, sekä yksilölle vaikutuksiltaan merkittävät muodot. Esimerkeiksi on valittu niin verkkoja hyödyntämällä tehtyjä rikoksia, kuin itse järjestelmiin kohdistuvia rikoksia.

3.1 Petos- ja huijaus-tyyppiset rikokset

Petosrikokset edustavat Suomen näkökulmasta verkkorikollisuuden valtavirtaa ja ovat erittäin yleisiä. Petos- ja huijausrikosten alle mahtuu monenlaisia ilmiöitä. Rikosuhripäivystyksen mukaan petosrikosten määrä on 2000-luvulle tultaessa lähestulkoon noussut kaksinkertaiseksi. Voimakkaan kasvun syyksi esitetään nimenomaan internetissä asioimisen lisääntymistä ja sitä, että entistä suurempi osa kaupankäynnistä on siirtynyt verkkoon. Myötävaikuttavana tekijänä perustellaan, että internet ja uudet teknologiat mahdollistava anonymiteetin sekä kokonaan väärien profiilien luomisen. Internetissä tapahtuvat petokset voivat olla erittäin laajoja ja uhreja voi olla jopa satoja. Uhrin näkökulmasta teot

tuottavat suoraa taloudellista haittaa, eivätkä internetpetokset tunne maantieteellisiä rajoja, joten tällaisia rikoksia voi olla joskus erittäin vaikea selvittää. (Rikosuhripäivystys d, 2019)

Rikosuhripäivystyksen mukaan vuonna 2017 jopa 60 % kaikista petosrikoksista tapahtui internetissä. Toisaalta vaikka äsken mainittiin petosrikollisuuden kasvaneen voimakkaasti 2000-luvulle tultaessa, Poliisihallitus tiedotti esimerkiksi 2017, että petosrikokset ovat kääntyneet hetkellisesti laskuun. Syyksi arvioidaan nettipetosten tutkintaan panostamista ja kansalaisten valistamista asiasta. Samaan aikaan todetaan nettipetosten olevan vaikeita siitä näkökulmasta, että nettipetoksen uhri ei välttämättä aina huomaa edes olevansa rikoksen uhri. Ja vaikka hän huomaisi, saattaa huijatuksi tulemisen aikaansaama häpeä estää uhria ilmoittamasta rikoksesta. Nettipetoksien todellinen määrä on piilorikollisuuden takia siis todellisuudessa paljon suurempi kuin mitä poliisin tietoon tulee. (Rikosuhripäivystys b, 2017)

3.1.1 Petosrikosten lainsäädäntö

Petosrikos on säädetty Suomessa rangaistavaksi Rikoslain 36 luvussa 1 §:ssä. Petoksen keskeinen sisältö Rikoslaissa on seuraava:

”Joka, hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä, on tuomittava petoksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.” – Rikoslaki (39/1889) 36:1 §

Petoksesta on olemassa myös kvalifioitu (törkeä)-, sekä lievä tekomuoto.

3.1.2 Romanssihuijaukset

Eräs erityinen sekä yleinen itsenäinen internetissä esiintyvä petosmuoto ovat niin sanotut romanssihuijaukset.

Yleensä romanssihuijauksen tekijät hyödyntävät henkilöitä, jotka etsivät seuraa internetin avulla. Romanssihuijaus tapahtuu yleensä siten, että henkilöä lähestytään internetissä, yleensä sosiaalisessa mediassa. Huijauksen tekijä ei välttämättä asu Suomessa. Syystä tai toisesta huijari ei voi tulla Suomeen tapaamaan uutta tuttavuuttaan. Huijari alkaa kuitenkin pian pyytää erilaisista syistä rahaa uhriltaan. Pyyntöjä lähettää rahaa tulee hyvin usein uudelleen ja uudelleen. Tyypillisesti pyynnöissä vedotaan erilaisiin akuutteihin syihin kuten terveydenhuollollisiin kuluihin. Leimallista romanssihuijauksille

on se, että ihmisten voi olla joskus hyvin vaikea tunnistaa kuka on tosissaan ja kuka huijaa. Romanssihuijausten takana voi olla järjestäytynyttä rikollisuutta ja ei ole tavatonta, että tekijät ovat sosiaalisesti erittäin taitavia. (Rikosuhripäivystys c, 2019)

Tyypillinen romanssihuijauksen uhri on 45 - 74-vuotias nainen. Jopa 90 % uhreista on nimenomaan naisia. Tyypillisiä paikkoja romanssihuijauksen alkupaikaksi ovat erilaiset sosiaalisen median alustat, kuten Facebook (50% tapauksista) sekä treffisivustot. (Rikosuhripäivystys c, 2019)

Yhdysvaltain liittovaltion poliisin FBI:n mukaan tyypillinen romanssihuijari pyrkii aikaansaamaan suhteen uhriin hyvin nopeasti. Tämä voi tapahtua esimerkiksi siten, että huijari kosii uhria hyvin nopeasti ja pyrkii luomaan luottamusta nopeassa tahdissa. (FBI a, 2019)

Keskusrikospoliisin rikoskomisario Lauri Salo on kommentoinut Aamulehdelle rakkaushuijauksia. Keskusrikospoliisin mukaan rakkaushuijaukset jäävät pääsääntöisesti selvittämättä. Syynä tähän on se, että romanssihuijauksissa tekijä jättää itsestään tietoja hyvin vähän. Lisäksi tekijä saattaa hyvinkin olla sellaisesta maasta, jossa ei edes ole käytössä esimerkiksi kaikista henkilöistä tehtyä väestötietojärjestelmää tai viranomaistoiminnan tehokkuus on hyvin kyseenalainen. (Härkönen, 2018)

Tarkkoja tilastotietoja nimenomaan Suomalaisiin uhreihin kohdistuneista romanssihuijauksista ei ole saatavilla. Samassa Aamulehden artikkelissa kuitenkin kerrotaan, että Suomesta lähetetään ulkomaille romanssihuijauksissa vuositasolla jopa miljoonia euroja. (Härkönen, 2018)

3.1.3 Verkkourkinta eli phising (tietojenkalastelu)

Verkkourkinta, tietojenkalastelu eli phising on ilmiö, jota käytetään usein muiden rikosten tekemisen apuna. Urkinnassa rikoksen tekijä pyrkii saamaan haltuunsa uhrin henkilötietoja. Yleinen tapa toteuttaa verkkourkintaa on tehdä toiselta internet-sivulta näyttävä sivu. Tämä sivu ei kuitenkaan tee samaa toiminnallisuutta kuin alkuperäinen sivu. Sen sijaan sivuston tarkoitus on usein kerätä henkilötietoja uhrilta. Tietojenkalastelu eroaa esimerkiksi tietomurrosta siltä osin, että joutuakseen kalastelun uhriksi, on uhrin itse avattava urkkija lähettämä linkki sivustolle tai liitetiedosto. (F-Secure a, 2021)

Tietojenkalastelu on myös Suomessa erittäin yleistä. Kyberturvallisuuskeskus julkaisi 2018 yleisen varoituksen kaikille koskien Microsoftin Office 365-järjestelmän nimissä tehtyjä tietojenkalastuksia. 2018 ilmeni, että verkkorikosten tehtailijat olivat onnistuneet kalastamaan eri yrityksien henkilöstöjen käyttäjätunnuksia ja salasanoja. Nämä salasanat oli annettu työntekijöiden toimesta, kun he olivat tie-

tämättään joutuneet tietojenkalastelun uhreiksi. Näillä käyttäjätunnuksilla ja sähköposteilla kirjauduttiin myöhemmin työntekijöiden Office 365-tileille. Käyttäjätilejä käytettiin muun muassa uusien kalasteluyritysten tekoon. (Kyberturvallisuuskeskus a, 2018)

Tietojenkalastelu voi kohdistua esimerkiksi myös nimenomaan tietyn organisaation henkilökuntaan tai jäseniin. Tämän vuoden syyskuussa Oulun yliopiston opiskelijoille ja henkilökunnalle tuli seuraava viesti, jonka myös itsekin sain: ”Hi [käyttäjätunnus], This is to notify that your [sähköpostiosoite] Password has expired and Outlook access can be suspended. Proceed below for revalidation. Thank you, Student Microsoft Corporation”. Tekstin alla oli linkki sivustolle. Kalevan mukaan jopa 900 Oulun yliopiston käyttäjätunnuksen haltijaa antoi salasanansa linkin kautta (Kaleva, 2021). Epäselväksi jäi mihin tunnuksia oli tarkoitus käyttää.

3.2 Palvelunestohyökkäykset

Palvelunestohyökkäyksellä tarkoitetaan sitä, että joku estää verkkosivuston käytön. Käytännössä tämä estetään siten, että hyökkääjä kohdistaa niin suuren määrän verkkoliikennettä internet-palveluun, että palvelu ei kestä tällaista määrää (Poliisi a, 2020.) Valtavasti lisääntynyt tietoliikenne ylittää lopulta internet-palvelun fyysisten resurssien (palvelimet) kantokyvyn, jonka johdosta ihmiset eivät enää pääse sivustolle. Suomalaisen tietoturvayhtiö F-Securen mukaan yleisimmin palvelunestohyökkäyksiä kohdistetaan nimenomaan verkkosivustoihin. Palvelunestohyökkäyksessä on tietoliikenteen estämisen lisäksi mahdollista joissakin tapauksissa aiheuttaa myös suoraa aineellista fyysistä tuhoa palvelimia ylläpitäville laitteille. (F-Secure b, 2021)

Suomen Rikoslaki käsittelee 38 luvun 5 §:ssä tietoliikenteen häirintää:

” Joka puuttumalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkivaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää tai häiritsee postiliikennettä taikka tele- tai radioviestintää, on tuomittava tietoliikenteen häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. ” - Rikoslaki 38:5 §

Suomessa on ollut melko usein palvelunestohyökkäyksiä, jotka ovat kohdistuneet niin pienempiin kuin suurempiinkin palveluihin. Hyökkäykset ovat saattaneet kohdistua jopa viranomaisiin. Helsingin Sanomat uutisoi 23.8.2019, että palvelunestohyökkäyksen seurauksena usean eri viranomaisen verkkopalvelut kärsivät palvelunestohyökkäyksen seurauksena. Hyökkäyksen kohteena oli Poliisi, Verohallinto,

Rajavartiolaitos sekä Hätäkeskuslaitos. Myös viranomaisten tarjoama Suomi.fi-palvelu kärsi toiminta-häiriöistä. Tässä tapauksessa häiriö toistui toisenkin kerran. Primääritilanteessa ei voitu esittää arviota hyökkäyksen tekijästä tai hänen motiiveistaan. (Helsingin Sanomat, 2019)

Palvelunestohyökkäys ei vaadi tekijältään suuria resursseja eikä välttämättä suurtakaan ymmärrystä. Tämä on nähty siinä, että jopa lapset ovat tehneet Suomessa palvelunestohyökkäyksiä. Suomessa lapset ovat esimerkiksi tehneet palvelunestohyökkäyksiä Wilma-oppimisalustaa vastaan. (Linnake, 2020)

Tietoturvayhtiö Kaspersky tutki artikkelissaan palvelunestohyökkäysten hintaa hyökkäyksen tekijälle. Artikkelista voidaan ensinnäkin päätellä, että hyökkäyksen tekijän ei tarvitse tietää käytännön tason teknologiasta mitään toteuttaakseen hyökkäyksen. Hän voi yksinkertaisesti ostaa verkon pimeiltä markkinoilta palvelunestohyökkäyksen esimerkiksi viiden Yhdysvaltain dollarin hinnalla. Toteuttaja toteuttaa maksua vastaan hyökkäyksen teknisen toteutuksen, eikä ostajan tarvitse ymmärtää tekniikasta mitään. Esimerkissä todetaan, että tällaisella hinnalla voi ostaa 5 minuutin hyökkäyksen suureen verkkokauppaan. Hyökkäysten toteuttajat myyvät jopa kuukausihintaisia paketteja, joiden mukana tulee ympärivuorokautinen asiakaspalvelu. (Makrushin, 2017)

Tekijän motiivina hyökkäyksessä voi olla lähes mikä tahansa. Kyberturvallisuuskeskuksen mukaan yleisimpiä motiiveja ovat kuitenkin erimielisyydet sekä aatteelliset syyt. Palvelunestohyökkäys voi siis näin ollen olla mielenosoituksellisen luonteista toimintaa. Näiden motiivien lisäksi palvelunestohyökkäyksellä voidaan myös kiristää rahaa kohteelta. Jos kohde ei maksa, uhataan kohdistaa palvelunestohyökkäys, jonka käytännön uhkaa on kohteen hyvin vaikea arvioida. Kyberturvallisuuskeskus kertoo, että kohteilta saatetaan kiristää rahaa ilman, että maksamatta jättämisestä koituu minkäänlaisia seurauksia. Kohteen on siis mahdotonta arvioida onko uhka hyökkäyksestä realistinen. (Kyberturvallisuuskeskus b, 2016)

Useiden lähteiden mukaan on mahdollista, että palvelunestohyökkäyksen motiivit eivät ole pelkästään palveluiden käytön estämisessä tai ilkivallassa. On mahdollista, että myös palvelujen tietoturva muilta osin vaarantuu hyökkäysten yhteydessä. Tämä voi tapahtua esimerkiksi siten, että todellisuudessa palvelunestohyökkäys on vain sumuverho, jonka takana toteutetaan toisenlainen kyberhyökkäys samalla kun päähuomio on palvelunestohyökkäyksessä. (Kyberturvallisuuskeskus b, 2016)

Ottaen huomioon aiemmin todetun palvelunestohyökkäyksen toteuttamisen suhteellisen halvan hinnan, aiheuttaa hyökkäys yleensä valtavasti suuremmat vahingot suhteessa sen tekemisestä aiheutuneeseen kustannukseen. Yrityksille taloudelliset riskit palvelunestohyökkäyksen toteutuessa voivat olla suuret. Vakuutusyhtiö IF kertoo verkkosivuillaan korvanneensa esimerkiksi suomalaiselle pienehkölle

askartelutarvikkeita myyvälle liikkeelle 4500 euroa palvelunestohyökkäyksen estettyä liikkeen myynnin kokonaan hetkeksi. (IF, 2021)

Suuremmille yrityksille hyökkäyksillä on luonnollisesti paljon suurempi vaikutus. Esimerkiksi vuonna 2013 ja 2015 Osuuspankkiin kohdistui palvelunestohyökkäys. Osuuspankki esitti käräjäoikeudessa kahta vastaajaa kohtaan 455 000 euron vahingonkorvausvaatimuksen. (Nykänen, 2017)

Palvelunestohyökkäysten arvioitu kokonaiskustannus suomalaiselle yhteiskunnalle jää epäselväksi sillä aiheesta ei löydy luotettavaa analyysia. Selvää kuitenkin on edellisten esimerkkien kautta, että palvelunestohyökkäykset aiheuttavat toistuvasti taloudellisia vahinkoja etenkin yrityksille, eivätkä vahingot ole useinkaan pieniä.

3.3 Tietomurrot

Kybertuvallisuuskeskuksen mukaan tietomurrot ovat Suomessa yleisiä. Kyberturvallisuuskeskuksen tilannekeskus käsitteli manuaalisesti vuonna 2019 yhteensä noin 4500 tietoturvaloukkausta. Käsitellyistä loukkauksista 604 käsitteli nimenomaan tietomurtoja. Tietomurrot ovat kyberturvallisuuskeskuksen mukaan kohdistuneet Suomessa niin yksittäisiin henkilöihin kuin kuntiin ja yrityksiinkin. (Kyberturvallisuuskeskus c, 2019)

Suomen Rikoslain 38 luvun 8 § käsittelee tietomurtoja. Tietomurron tunnusmerkistö pääpiirteissään on seuraavanlainen:

”joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. … .” - Rikoslaki 38:8§

Tietomurron käsite on siis melko hyvin avattu jo Rikoslain tunnusmerkistössä. Tietomurron pääsisältö on siis järjestelmään pääsy tai sen yritys. Vakuutusyhtiö IF:n mukaan tietomurto käytännössä tarkoittaa sitä, että henkilö yleensä murtaa jonkin tietojärjestelmän suojauksen. Tyypillisin tapa tietomurron tekemiseen on se, että käytetään käyttäjätunnusta, joka ei kuulu tietomurron tekijälle. (IF, 2021)
Myös poliisin mukaan yleisin tietomurron toteutustapa on nimenomaan käyttäjätunnuksen oikeudeton käyttö (Poliisi b, 2020.) Tietomurto on verkkorikoksena luonteeltaan tietoverkkoon itseensä kohdistunut rikos.

Kyberturvallisuuskeskuksen mukaan tietomurtojen motiiveja on useita. Usein motiivina on tekijän halu päästä käsiksi materiaaliin, joka ei ole julkista. Tietomurtojen avulla voidaan kohdistaa yrityksiin ja yhteisöihin laskutuspetoksia [yrityksen laskutukseen lähetetään väärä lasku, jolle ei ole perustetta] perustuen tietomurrossa käsiin saatuun tietoon. Motiivina tietomurrolle voi myös olla se, että tekijä haluaa saada murron avulla erilaisia käyttäjätunnuksia haltuunsa. Käyttäjätunnusten avulla tekijä tekee jälleen uusia tietomurtoja eri järjestelmiin (Kyberturvallisuuskeskus, 2019)

3.3.1 Case Vastaamo sekä kiristykset verkossa

Tietomurtojen kohteet saattavat valikoitua joskus pelkästään sillä perusteella, että erilaisten järjestelmien joukosta seulotaan heikoiten suojattuja järjestelmiä (Kyberturvallisuuskeskus, 2019.) Eräs esimerkki tällaisesta heikosti suojatusta, tietomurrolle alttiista järjestelmästä sekä tietomurtojen potentiaalista on vastikään paljastunut, erittäin korkean profiilin rikostapaus, psykoterapiakeskus Vastaamon valtava tietomurto.

Lokakuussa 2020 mediassa alkoi näkyä uutisia, joiden mukaan psykoterapiakeskus Vastaamo on joutunut massiivisen tietomurron kohteeksi. Helsingin sanomat uutisoi, että tietomurto oli kohdistunut Vastaamon asiakkaiden eli psykoterapiassa käyneiden potilaiden potilastietoihin. Tietomurrossa vuotaneet potilasasiakirjat sisälsivät hyvin henkilökohtaista nimen tasolle yksilöitävää tietoa potilaista. Alkutilanteessa tulleiden tietojen mukaan tietoja hyödynnettiin siten, että niiden avulla kiristettiin Vastaamoa maksamaan 450 000 euroa lunnaista Bitcoineissa. Mikäli vaatimukseen ei suostuttaisi, uhkasi kiristyksen tekijä julkaista sadan Vastaamon asiakkaan tiedot internetissä päivittäin. (Huhtanen, 2020)

Vastaamon tapaus herätti mielenkiintoa laajasti myös ulkomailla asti. Wired-lehti uutisoi 2020 joulukuussa, että Vastaamon potilasasiakirjat jopa 33 000 asiakkaasta olivat ehkä päätyneet tietomurtajalle jo 2018 marraskuussa. Syyksi arvioitiin se, että Vastaamon tietoturva ei ollut ajan tasalla. (Wired, 2020)

Ylen mukaan Vastaamon järjestelmiin murtauduttiin uudestaan 2019. Myöhemmin lokakuussa 2020 tekijä alkoi julkaista potilastietoja internetin foorumeilla. Saman kuukauden aikana tekijä alkoi kiristää myös erikseen tietomurron uhreja. (Hämäläinen et al., 2020)

Keskusrikospoliisi piti 27.10.2021 Vastaamon rikostapauksen tilanteesta tiedotustilaisuuden. Keskusrikospoliisi luonnehti tapausta poikkeukselliseksi ja kertoi asianomistajia olevan 22 000 luokkaa. Rikoskomisario Marko Leponen kommentoi tiedotustilaisuudessa, että poliisi on edistynyt jutun tutkinnassa ja kertoi, että yksi merkittävä tutkintalinja johtaa ulkomaille. Leposen mukaan linja ei mene Eurooppaan vaan sen ulkopuolelle. Jutun tutkinnassa on tehty yhteistyötä ulkomaisten viranomaisten kanssa. Leponen kertoi tilaisuudessa myös, että tekijän varmistaminen on mahdollista vasta kun henkilö on saatu konkreettisesti kiinni, sillä verkkoympäristö tarjoaa mahdollisuuden esiintyä toisena henkilönä tai anonyymisti. Leponen antoi tilaisuudessa ymmärtää, ettei ole varmaa ovatko tietomurron tekijä ja kiristyksien tekijä yksi ja sama henkilö. (Keskusrikospoliisi, 2021)

Vastaamon tapauksesta on nähtävissä tärkeitä verkkorikollisuuteen liittyviä näkökulmia. Ensimmäinen näkökulma on se, että vaikka verkkorikollisuudesta puhuttaessa eritelläänkin paljon sitä, mistä rikoksesta milloinkin puhutaan, todellinen rikollisuus ei tunne yksittäisten tekomuotojen rajoja. Lisäksi rikollisuudessa yhdistyvät usein tietoverkkoon itseensä kohdistetut rikokset ja reaalimaailmassa tehdyt rikokset. Vastaamon tapauksessa tekijä murtautui ensin järjestelmään ja vasta paljon myöhemmin teki varsinaisia reaalimaailmaan kohdistuvia rikoksia, kuten kiristyksiä. Myöskin teon motiivit vaikuttavat varsin selkeiltä. Motiivina vaikuttaa vahvasti tähän asti ilmenneiden seikkojen perusteella olleen taloudellinen hyöty. Vastaamon tapauksesta voidaan myös nähdä, ettei verkkorikollisuus tunne valtion rajoja, mikäli tekijä lopulta on ulkomailta. Kiristysrikos verkkorikoksen keinoin toteutettuna on tietoverkkoja hyödyntäen tehtyä rikollisuutta vaikka kiristystilanteeseen pääseminen voi edellyttääkin tietoverkkoa itseään kohtaan tehtyjä laittomia tekoja.

Suomen rikoslaki määrittelee kiristyksen 31 luvun 3 §:ssä, jonka mukaan kiristyksessä uhkauksella (joku muu uhkaus kuin ryöstössä) ”pakottaa toisen luopumaan taloudellisesta edusta.”. Kiristäjällä ei saa lain mukaan olla laillista taloudelliseen etuun. Kiristyksestä on olemassa törkeä eli kvalifioitu tekomuoto. (Rikoslaki 31:3§)

Kiristysrikokset ovat poliisin mukaan kasvussa. Lisäksi näihin liittyy usein digitaalista todistusaineistoa. Yhdistettynä verkon käytön lisääntymiseen on järkevää ajatella kiristysrikosten siirtyvän enenevässä määrin verkkoon. (Poliisi a, 2021)

3.4 Haittaohjelmat

Haittaohjelmat ovat ohjelmistoja, joita käytetään muun muassa tietojärjestelmän vahingoittamiseen. Haittaohjelmat voivat pyrkiä myös hyödyntämään laitteistoa johonkin tarkoitukseen vahingoittamisen lisäksi. Haittaohjelmia voidaan käyttää myös tietojenkalastelussa. Haittaohjelma käsitteenä kattaa

kaikki edellä mainitut ohjelmien muodot. Haittaohjelmia yhdistää se, että niiden tarkoitusperä on käyttäjän kannalta haitallinen. (McAfee, 2021)

Eräs esimerkki tällaisesta on se, että poliisi varoitti internetsivuillaan tämän vuoden kesäkuussa haittaohjelmasta nimeltä FluBot, joka kohdistui Android-laitteisiin. Haittaohjelman sai laitteelleen siten, että sattui saamaan tekstiviestin, jossa oli olevinaan postipaketin seurantalinkki. Linkin kautta uhria neuvottiin lataamaan Googlen sovelluskaupasta ohjelmiston, joka todellisuudessa oli haittaohjelma. Kun käyttäjä latasi sovelluksen, joka todellisuudessa sisälsi FluBotin, sai FluBot laajat käyttöoikeudet laitteeseen. Oikeuksien avulla rikolliset onnistuivat kalastelemaan verkkopankkitunnuksia ja siirtämään rahaa (Poliisi d, 2021). Saksalaisen teleoperaattori Telekomin mukaan FluBotin tartuntoja oli enimmillään jopa yli 2500 tartuntaa päivässä ja syyskuun 2021 lopussa tartuntoja oli edelleen 500 – 1000, joten kyse ei ollut täysin marginaalisesta haittaohjelmasta (Barabosch, 2021).

Tyypillisesti haittaohjelmien tekijät ovat ammattimaisia, vaikka historiallisesti haittaohjelmat saattoivatkin olla myös harrastelijoiden tekemiä. Haittaohjelmien pyrkimyksenä on usein saada tehtyä rahaa tavalla tai toisella. Jo vuoden 2010 tasolla arvioitiin, että haittaohjelmilla onnistuttiin keräämään 100 miljardia rikoshyötyä vuosittain. Ohjelmistot ovat yleensä luonteeltaan viruksia, niin sanottuja troijan hevosia ja vakoiluohjelmia. Näitä ohjelmistoja kaupataan eri sivustoilla internetissä. Tätä nykyä haittaohjelmistoja voi ostaa suoraan palvelunomaisesti halpaankin hintaan. Tähän malware as a service-tyyppiseen pakettiin kuuluu yleensä myös päivityksien julkaiseminen ohjelmistoon, jotta se voi entistä paremmin välttää laitteistojen viruksentorjunnan. (Brenner, 2010, s. 63 - 64)

Voidaan todeta edellisten esimerkkien avulla, että haittaohjelmistojen laatu on parantunut selkeästi. Niistä on tullut myös aina vain parempia välttämään haittaohjelmistojen torjumiseen tarkoitettuja tietoturvaohjelmia. Tulevaisuuden kannalta on selvä uhkakuva mikäli haittaohjelmistot kehittyvät entisestään ja kehittyvät nopeammin kuin niiden torjuntaan käytettävät keinot. Myös malware as a service-tyyppisen toiminnan lisääntyminen on selkeä tulevaisuuden uhkakuva.

3.5 Deep web, darkweb ja verkon laittomat markkinat

Verkkorikollisuutta käsittelevissä artikkeleissa ei usein voi olla törmäämättä niin sanottuun deep webiin sekä darknetiin. Internetissä on olemassa sivustoja, joita perinteiset hakukoneet eivät löydä eivätkä voi löytää. Darknet taas tarkoittaa deep webin osa-aluetta, jossa tietokoneet yksilöivät IP-osoitteet ovat salattuja. Dark webiin pääseminen voi edellyttää erityistä ohjelmistoa normaalin selaimen sijaan (Grannan, 2021). Tällainen ohjelmisto on esim Tor-selain. Darknetin tai Deepwebin käyttö ei ole itsessään laitonta.

Deep webissä sekä darknetissä toimii useita laittomien tuotteiden myyntipaikkoja. Eräs tällaisista oli DarkMarket. DarkMarket oli maailman suurin tiedetty laittomien tuotteiden markkinapaikka, joka useiden maiden yhteisoperaatiossa onnistuttiin sulkemaan tänä vuonna. DarkMarketissa oli jopa yli puoli miljoonaa käyttäjää ja 2400 myyjää. Yli 320 000 myyntitapahtumaa ehdittiin tehdä DarkMarketin olemassaolon aikana. Euromääräisesti arvioituna DarkMarketissa ehdittiin myydä 140 miljoonan euron edestä tuotteita. Tuotteet itsessään olivat huumeita, väärää rahaa, väärennettyjä pankkikorttitietoja, anonymisoituja SIM-kortteja sekä haittaohjelmistoja. (Europol, 2021)

Darknetin myötävaikutuksella voidaan tehdä mitä tahansa rikoksia. Sen myötävaikutuksella on syntynyt myös Suomen rikoshistorian kannalta ennennäkemätön internetistä tilattu palkkamurha. Vuonnna 2019 Tor-verkon Torilaudalle jätettiin ilmoitus, joka näytti tarjoavan palkkamurhapalveluita. Ilmoituksen jättänyt Mustakolmio-nimimerkillä toiminut henkilö korosti viestissään, ettei kyse ole vitsistä. Mustakolmio kertoi palvelun hinnaksi kommenttiketjussa noin 4000 – 9000 euroa. Ei mennyt kauan, kun joku tilasi palvelun oikeasti ja Mustakolmio toteutti palkkamurhan tilauksesta. Murhan seurauksena kuoli palvelun 20-vuotiaan tilaajan isä. (Kemppinen, 2020)

Ennen DarkMarketia, vuodesta 2013 vuoteen 2019 darknetissä toimi Silkkitieksi kutsuttu myyntipaikka, jossa myytiin valtava määrä huumeita. Tulli takavarikoi Silkkitien palvelimen yhteistoimin Ranskan viranomaisten kanssa. Silkkitiessä myytiin huumeiden lisäksi myös aseita ja doping-aineita. Silkkitien liikevaihdon arvioitiin olleen jopa 50 miljoonan euron luokassa. Silkkitien arvioitiin yhdessä muiden verkkokauppojen kanssa lisänneen merkittävästi Suomeen virranneiden huumausaineiden määrää. Tullin epäiltyinä Silkkitiehen liittyen oli jopa 30 myyjää. Tutkintojen yhteydessä takavarikoitiin Bitcoinia suunnilleen 20 miljoonan euron arvosta. Itse laittomat tuotteet vaihtoivat postitse omistajaa. Silkkitien myynti kohdistui hyvin voimakkaasti nimenomaan Suomeen. Silkkitien toimintalogiikka oli se, että palveluun voitiin lisätä myyjiä, jotka myivät tuotteita ja Silkkitien ylläpitäjä ylläpiti markkinapaikkaa. (Tulli, 2020)

3.6 Seksuaalirikokset

Internet on mahdollistanut seksuaalirikollisille täysin uudenlaisen pelikentän, jossa mahdollisuudet kaikenlaisille seksuaalirikoksille ovat paljon aiempaa suuremmat. Seksuaalirikokset internetissä voivat olla joko fyysiseen kontaktiin johtavia tai sitten rikoksia, jotka tapahtuvat ilman fyysistä kontaktia. Internet on myös mahdollistanut seksuaalirikosten kaikista järkyttävimpien sisältöjen jakamisen anonyymisti rikollisten kesken. Seksuaalirikokset verkkorikosten muotona muodostavat melko laajan kokonaisuuden, jonka vuoksi ilmiöstä on käsitelty vain joitakin esimerkkejä. Vaikuttaa siltä, että hyvin usein verkossa tapahtuneissa seksuaalirikoksissa uhreina ovat nimenomaan kaikista heikoimmassa asemassa olevat eli alaikäiset.

Englantilainen lastensuojelun hyväksi toimiva järjestö National Society for the Prevention of Cruelty to Children kertoo sivuillaan, että Englannissa lapsiin kohdistuneista seksuaalirikoksista 16 % oli jonkinlainen kontaktipinta internetiin ja arvioi, että ilmiössä on mukana piilorikollisuutta, jonka takia ongelma on todellisuudessa luultavasti suurempi. (NSPCC, 2019)

Samaa eurooppalaista trendiä edustaa myös Suomi. Pelastakaa Lapset-järjestön mukaan merkittävässä osassa lapsiin kohdistuneissa hyväksikäyttörikoksissa on liityntä internetiin. Tutkimus on vanha, mutta vuonna 2011 poliisi ja Pelastakaa Lapset Ry suorittivat kyselyn, joka koski nuorten kokemaa seksuaalista häirintää ja hyväksikäyttöä internetissä. Kyselyn tulokset osoittavat kiistattomasti seksuaalirikosten olevan erittäin yleinen verkkorikollisuuden muoto, jota ei voi jättää huomiotta. Kyselyyn vastanneista nuorista, alle 16-vuotiaista jopa 33 % vastaajista kertoi saaneensa seksuaalissävytteisiä valokuvia tai videoita vanhemmilta ihmisiltä. 24 % vastaajista oli käynyt seksuaalisen sävyn omaavia keskusteluja vanhemman ihmisen kanssa. Viidennes vastaajista kertoi, että oli ollut seksuaalisävyteisessä nettikamerayhteydessä itseään selkeästi vanhemman henkilön kanssa. 8 % vastaajista oli tavannut henkilön, joka oli ehdottanut seksiä nuorelle internetissä. 3 % vastaajista oli lopulta harrastanut seksiä internet-keskusteluiden pohjalta tapaamansa aikuisen kanssa. (Pelastakaa Lapset, 2013)

Tilastokeskuksen mukaan seksuaalinen hyväksikäyttö on muuttanut tänä päivänä muotoaan siksi, että etenkin internetyhteydellä varustetut älypuhelimet mahdollistavat hyväksikäyttäjille uudenlaisia mahdollisuuksia. (Ellonen et al., 2019)

Eräs seksuaalisen hyväksikäytön muoto, joka tapahtuu nimenomaan verkon avulla on niin sanottu alastonkuvilla kiristäminen eli sextortion. Alastonkuvakiristyksessä tekijä tyypillisesti esiintyy uhrin ikäisenä henkilönä, joka on kiinnostunut solmimaan suhdetta uhrin kanssa tai muulla tavalla haluaa tuoda lapsen/nuoren elämään jotakin hyödyllistä. Pian tekijä pyrkii erilaisia vaikuttamiskeinoja hyödyntäen saamaan lapsen/nuoren tuottamaan seksuaalista kuvasisältöä tekijälle. Hyvin pian tekijä alkaa vaatia lisää sisältöä ja tehostaa vaatimustaan uhkaamalla julkaista aiemmin lähetettyjä kuvia. Vaatimuksia voidaan tehostaa myös väkivallan uhalla. Tyypillisesti uhri häpeää ja pelkää tilannetta ja tämä estää heitä ilmoittamasta asiasta eteenpäin. Yhdysvaltain liittovaltion poliisin mukaan tällaiset rikokset ovat lisääntyneet valtavasti. (FBI b, 2021)

Sextortion-tyyppisen kiristyksen todellisista lukumääristä esimerkiksi Suomessa on vaikea saada kunnollista kuvaa sillä aiheesta ei ole saatavilla selkeää tilastotietoa. Yhdysvaltalainen Brookings-tutkimusinstituutio tutki 2016 sextortion-tyyppisiä rikoksia 78 tapauksen pohjalta. Osa tapauksista oli varsin laajoja sisältäen enemmän kuin 100 uhria. Yhteensä löydettyjä uhreja oli 1397, todellisuudessa heitä saattoi olla tuhansia enemmän. Tutkimuksessa selvisi, että 71 % tapauksista uhri oli alaikäinen.

Ainoastaan 12 % tapauksista oli sellaisia, joiden uhrina oli pelkästään aikuisia. Lähes kaikki aikuisuhreista olivat naisia. Joka ikinen 78 tapauksen sextortion-rikoksista syytetyistä oli miehiä. Huomionarvoista oli myös, että monessa tutkitussa tapauksessa oli joku uhri, joka oli rikoksen aiheuttaman tuskan takia tehnyt itsemurhan. Tutkijat nostavat esille myös, että sextortion-tyyppiset rikokset ovat radikaalisti alitutkittuja, mutta vaikuttaa siltä, että ne ovat äärimmäisen yleisiä. (Wittes et al., 2016) Olisi mielekästä päätellä, että samanlaiset lainalaisuudet pätisivät myös Suomessa.

Toinen Suomessakin nuoria uhkaava ilmiö on niin sanottu grooming-ilmiö, jossa internet näyttelee erittäin tärkeää osaa. Grooming ilmiönä jakaa joitakin samankaltaisuuksia aiemmin kuvatun sextortion-ilmiön kanssa. Groomingissa aikuinen alkaa lähestyä lasta viestittelemällä tämän kanssa. Tekijä pyrkii luomaan uhriin luottamuksellisen suhteen. Suhteen luomisen lomassa tekijä alkaa vähitellen tuomaan seksuaalisia elementtejä keskusteluun ja pyrkii arkipäiväistämään seksuaalissävytteisen sisällön keskusteluihin. Grooming-ilmiö saattaa päättyä aiemmin kuvattuun tilanteeseen, jossa lapselta kiristetään aina vain lisää seksuaalista materiaalia. Grooming-ilmiö voi myös realisoitua myöhemmin seksuaalisena väkivaltana lasta kohtaan internetin ulkopuolella. (Pelastakaa Lapset, 2021) Suomessa poliisi on varottanut nuoria useilla internetin alustoilla internetissä tapahtuvasta grooming-ilmiöstä.

Verkkorikollisuuden kontekstissa on jopa hieman yllättävää, että nimenomaan lapset vaikuttavat edellä kuvattujen tilastojen perusteella olevan melko usein verkkorikollisten uhreja. Tämä vaikuttaa erityisen huolestuttavalta signaalilta sillä yhä nuoremmat lapset saavat käyttöönsä laitteita, joilla pääsee monien sovellusten kautta toimimaan verkkoympäristössä. Kun tähän yhdistetään verkkorikollisuuden ennustettu kasvu, on odotettavissa, että lapsiin kohdistuvat verkkorikokset eivät ainakaan olisi vähenemässä ellei valvontaan ja ennaltaehkäisyyn onnistuta panostamaan riittävästi, oikea-aikaisesti sekä riittävässä määrin.

4 ARVIO VERKKORIKOLLISUUDEN NYKYTILANTEESTA

4.1 Tilannekuva

Poliisin näkemyksen mukaan verkkorikollisuuden kentässä on paljon piilorikollisuutta ja arvioidaankin, että ainoastaan pieni osa todellisuudessa tapahtuneista verkkorikoksista lopulta päätyy poliisin tietoon ja järjestelmiin. Poliisi arvioi, että Suomessa tapahtuneiden verkkorikosten rikoshyöty konservatiivisesti arvioiden pyörii satojen miljoonien eurojen tasolla vuosittain. Suomenkin kohdalla kyse on siis erittäin tavanomaisesta rikollisuuden muodosta. Koska piilorikollisuuden osuus on epäselvä, on mahdollista, että rikoshyöty on todellisuudessa paljonkin arviota suurempi ja verkkorikollisuus on siten tiedettyä suurempi ilmiö. (Jämsén, 2020).

Verkkorikollisuutta tapahtuu lähes kaikissa sen muodoissa myös Suomessa. Poliisin mukaan verkkorikollisuuden ilmiöt ovatkin usein luonteeltaan kansainvälisiä ja niihin liittyy järjestäytynyttä rikollisuutta sekä jopa valtiojohtoisuutta (Poliisi c, 2020). On huomionarvoista, että kaikissa esitellyissä verkkorikollisuuden ilmiöissä oli kyse globaaleista ilmiöistä, jotka ovat ulottaneet vaikutuksensa Suomeen. Suomeen kohdistuu tarkastelun perusteella hyvin paljon ulkomailta koordinoitua rikollisuutta kuten esimerkiksi internetpetosten osalta voitiin todeta. Tilannekuvan kannalta on merkittävää, että niin suuri osa rikoksista voi kohdistua Suomeen ulkomailta sen sijaan että Suomeen kohdistunut rikos olisi suomalaisen tekemä.

Verkkorikollisuuden kehitykselle on ominaista huomattava rikostapausten määrällinen kasvu. Määrällisen kasvun lisäksi verkkorikollisuus ilmiönä myös monipuolistuu. Rikollisille tarjoutuu jatkuvasti uudenlaisia alustoja joilla toimia tai löytää uusia uhreja ympäri maailmaa. Vuoden 2019 tasolla pelkästään tietoverkkoihin itseensä kohdistuneita rikoksia tuli poliisin tietoon jo 1300 kappaletta. Vuoden 2020 tason ennustettiin jo 2019 nousevan noin 1400 rikoksen tasolle. Vaikka nettipetoksissa havaittiin jossain välissä laskuakin, ovat nekin lähivuosina jatkamassa poliisin ennusteen mukaan kasvuaan (Jämsén, 2020).

Koronapandemia on vaikuttanut yhteiskuntaan erittäin paljon ja näin on tapahtunut myös verkkorikollisuuden suhteen. Poliisin mukaan verkossa tapahtuneiksi ilmoitettujen rikosten määrä oli ensinnäkin kasvanut pandemian myötä. Kasvun lisäksi myös rikosten muoto muovautui pandemia-aikana vastaamaan paremmin pandemian aiheuttamia toimintaympäristön muuttuneita olosuhteita. Esimerkiksi petosrikollisuuteen pandemia ja rajoitustoimet vaikuttivat lieventävästi silloin kun rajoitustoimet olivat voimakkaimmillaan. Rajoitusten palaaminen normaaliin näyttää poliisin mukaan kuitenkin muuttavan verkkorikollisuuden tilannetta lähemmäs normaalia, joten pandemian vaikutukset vaikuttavat olevan ainakin joidenkin rikostyyppien osalta luonteeltaan väliaikaisia. (Jämsén, 2020)

4.2 Motiivit

Verkkorikosten motiivit näyttävät jakavan osittain samoja motiiveja kuin perinteisetkin rikokset. Sabillonin mukaan verkkorikosten motiivien määritteleminen on erittäin vaikeaa sillä verkkorikokset eivät edusta mitään homogeenista joukkoa, vaan enemmänkin edustettuna saattaa olla suuri joukko erilaisia motiiveja tekojen taustalla. Tyypillisiä motiiveja erilaisten rikosten taustalla voi olla erilaiset motiivit aina uteliaisuudesta poliittiseen aktivismiin. (Sabillon et al, 2016)

Toisin kuin voisi ehkä ajatella, verkkorikollisuudessa vakavia vahinkoja aiheuttava teko ei välttämättä tarvitse taakseen vakaasti harkittuja motiiveja ja kannustimia. Suurissakin verkkorikoksissa taustalla voi olla puhtaasti kokeilunhalu ja teot saatetaan tehdä varsin vähäisen harkinnan perusteella. (Leppänen, 2021)

Onkin mielekästä tarkastella verkkorikollisuuden motiiveja ennen kaikkea erilaisten tekojen ja profiilien kautta. Useimmissa edellä tarkastelluissa rikostyypeissä motiivi liittyi jollakin tavalla rahaan. Esimerkiksi haittaohjelmien teon motiivi liittyy usein siihen, että niiden avulla voidaan saada tietoja, joiden avulla tekijä saavuttaa itselleen taloudellista hyötyä joko suoraan tai välillisesti. Tietojenkalastelussa on tyypillisesti samanlainen päämäärä. Samoin petosrikoksissa motiivi saada rahaa rikollisin keinoin on voimakkaasti korostunut. Näistä eroten esimerkiksi palvelunestohyökkäysten ja tietomurtojen kohdalla on todettu, että motiivina saattaa olla mikä tahansa aina poliittisesta vaikuttamisesta näyttämisenhaluun. Poliisin näkemyksen mukaan päämotiivina suuressa osassa rikoksissa on taloudellisen hyödyn saavuttaminen joko suoraan tai epäsuorasti rikollisen toiminnan avulla. (Jämsen, 2020)

4.3 Kansainvälinen verkkorikollisuus Suomessa

Eräs tärkeä kysymys verkkorikollisuutta arvioitaessa on se, missä määrin verkkorikollisuuden ilmiöt ja muodot ovat sovellettavissa nimenomaan Suomen toimintaympäristöön ja tulevaisuuteen. Kysymys on validi, sillä monissa rikollisuuden ilmiöissä kehitys on aiemmin ollut Suomessa huomattavastikin muuta maailmaa jäljessä. Suomalaisessa rikollisuudessa on myös omat erityispiirteensä. Jälkikäteinen kehitys on ollut nähtävissä esimerkiksi terrorismirikollisuudessa. Maailmalla terrorismi on ollut verrattain yleistä jo vuosia, mutta Suomessa kehitys on ollut huomattavasti hitaampaa. Terroristisen tekojen suunnittelu sekä potentiaalisten terroritekojen tekijöiden määrä on noussut vasta melko hiljattain. Samalla tavalla esimerkiksi järjestäytyneen rikollisuuden ilmiöt ovat tulleet Suomeen jälkijunassa muihin länsimaihin verrattuna. Lopulta kuitenkin kaikki nämä ilmiöt ovat tulleet myös Suomeen. On siksi oletettavaa, että se mitä verkkorikollisuuden kentässä tapahtuu ulkomailla, tapahtuu lähes varmasti jonain päivänä myös Suomessa.

Lisäksi verkkorikollisuuden toimintakenttä on globaali, joten verkkorikoksen tekijän ei tarvitse olla fyysisesti Suomessa. Suomi myös kiinnostaa poliisin mukaan verkkorikoksentekijöitä. Tämä johtuu siitä, että Suomi ja suomalaiset uhrit ovat melko varakkaita globaaleilla standardeilla mitattuna. (Poliisi, 2020)

Vaikka Suomi tuleekin joissakin rikollisuuden ilmiöissä jälkijunassa, on tämä itse asiassa tulevan ennakoinnin näkökulmasta etu. Tällöin aikaa varautua tulevaan voi olla enemmän ja kehityssuunnat maailmalla ovat jo ilmaisseet itsestään enemmän ennen kuin ne rantautuvat täysimittaisena Suomeen.

4.4 Verkkorikosten lainsäädäntötaustasta

Tutkittaessa Suomen Rikoslakia voidaan huomata, että monet verkkorikoksia koskevat tunnusmerkistöt ovat suhteellisen uusia. Lisäksi on huomionarvoista, ettei rikoslaista löydä erikseen suoranaisia verkkorikosten tunnusmerkistöjä. Edellä on mainittu, että verkkorikokset voivat olla joko tietojärjestelmään kohdistuvia tai vaihtoehtoisesti tietojärjestelmiä hyväksi käyttäen tehtyjä. Keskeiset tietoverkkoihin itseensä kohdistuvat rikokset on lueteltu Rikoslaissa (Leppänen, 2021.) Useat muut verkkorikoksiin kuuluvat teot ovat muita Rikoslakirikoksia, joissa verkkoa käytetään hyväksi rikosten tekemisessä.

Seuraavassa listataan tällä hetkellä keskeisiä tietoverkkoihin kohdistuvia rikostyyppejä perustuen Leppäsen tekemään listaukseen:

- Tietomurto (oikeudeton tunkeutuminen tietojärjestelmään - Rikoslaki 38:8§)
- Luvaton käyttö (laitetta käytetään luvatta - Rikoslaki 28:7§)
- Datavahingonteko (datan hävittämistä tai muuttamista tarkoituksena tuottaa vahinkoa - Rikoslaki 35:3§)
- Vaaran aiheuttaminen tietojenkäsittelylle (esimerkiksi verkkorikostyökalujen hankkiminen ja levittäminen tai vahingon aiheuttaminen tietojärjestelmälle - Rikoslaki 34:9§)
- Tietoliikenteen häirintä (tietoliikenteen häirintää oikeudettomasti - Rikoslaki 38:5§)
- Tietojärjestelmän häirintä (tietojärjestelmää itseään häiritään - Rikoslaki 38:7§)

(Leppänen, 2021)

Aiemmin käsiteltyihin rikollisuuden muotoihin pohjautuen voidaan todeta, että tietoverkkoja hyödyntäen tehdyissä rikoksissa tulee usein kyseeseen perinteisemmät rikoslain pykälät. Esimerkiksi petosrikoksissa nimikkeenä petos, huumausainekaupassa huumausainerikokset ja niin edelleen.

Suomessa rikokset voivat olla joko asianomistajarikoksia tai virallisen syytteen alaisia rikoksia. Asianomistajarikoksessa on edellytyksenä, että asianomistaja vaatii rikoksen tekijälle rangaistusta. Suomessa esitutkintalaki säätelee asianomistajarikoksen esitutkintaa. Mikäli asianomistaja ei vaadi rangaistusta, rikoksen esitutkinta tyypillisesti päätetään, ellei erittäin tärkeä yleinen etu vaadi sen tutkimista siitä huolimatta. Virallisen syytteen alaisissa rikoksissa rikoksen tutkinta toimitetaan siitä välittämättä, mikä asianomistajan kanta on. Verkkorikollisuuden piirissä on sekä asianomistajarikoksia, että yleisen syytteen alaisia rikoksia. (Leppänen, 2021)

5 VERKKORIKOLLISUUDEN KEHITTYMINEN TULEVAISUUDESSA

5.1 Tieteellinen tulevaisuuden ennakointi

Tässä kappaleessa on tarkoitus pohtia sitä, mihin suuntaan verkkorikollisuus olisi mahdollisesti tulevaisuudessa kehittymässä. Ennakointiin liittyykin aina suuri määrä sattumaa. Tästä huolimatta tulevaisuutta on mielekästä pyrkiä ennakoimaan, vaikka lopputulema tarkkuudeltaan olisikin jotakin parhaan arvauksen ja hyvän ennusteen välimaastosta.

Tulevien kehityssuuntien hahmottamiseksi olen tarkastellut asiantuntijoiden näkemyksiä verkkorikollisuuden tulevaisuuden näkymistä, sekä perehtynyt tulevaisuudentutkimukseen liittyvään kirjallisuuteen ja soveltanut periaatteita verkkorikollisuuden näkökulmasta. Tarkastelen myös sitä, minkälaisin keinoin viranomaisten tulee varautua tulevaan ja mitä mahdollisesti on jo tehty tulevaan varautumisessa.

On eri asia arvioida tulevaisuutta puhtaasti subjektiivisten käsitysten pohjalta, kuin arvioida tulevien tapahtumien todennäköisyyksiä ja potentiaalisia kehityskulkuja tieteellisin keinoin. Tieteellisessä tulevaisuuden arvioinnissa ei siten ole kyse eksaktien arvioiden tekemisestä. Osmo Kuusi on ottanut kantaa tieteelliseen tulevaisuudentutkimukseen Tieteessä Tapahtuu -lehdessä. Osmo Kuusi korostaa, että tieteellisessä tulevaisuudentutkimuksessa etsitään korkeatasoisia argumentteja, jotka liittyvät tulevaisuuteen (Kuusi, 2008).

Toinen tapa tutkia tulevaa tieteellisesti on kiinnittää huomiota niin kutsuttuihin heikkoihin tulevaisuuden merkkeihin/signaaleihin (Kuusi, 2008). Elina Hiltunen on ottanut kantaa siihen, mitä heikot tulevaisuuden merkit ovat. Hiltunen kuvaa, että heikot signaalit ovat tässä hetkessä näkyviä merkkejä, jotka ennakoivat tulevaisuutta. Heikkojen merkkien lisäksi on kiinnitettävä huomiota nouseviin ilmiöihin. Signaaleja ja nousevia ilmiöitä havaitaan niin sanotulla ympäristön skannauksella, joka tarkoittaa sitä, että eri informaatiolähteistä havainnoidaan edellä mainittuja. Hiltunen kuvaa kirjoituksessaan niin sanotun informaation elämänsyklin. Informaation elämänsyklin varhaisvaiheessa tieto on lähinnä pienen piirin informaatiota ennen kuin informaatio siirtyy osaksi yleistä tietoisuutta. Informaation elämänsyklin mukaan varhaisessa vaiheessa tulevaisuutta ennakoivia ilmiöitä voidaan havaita (verkkorikollisuuden kontekstin kautta tulkittuna) ensinnäkin asiantuntijoiden kannanotoista, väitöskirjoista ja alan spesialisoituneista julkaisuista. (Hiltunen, 2008)

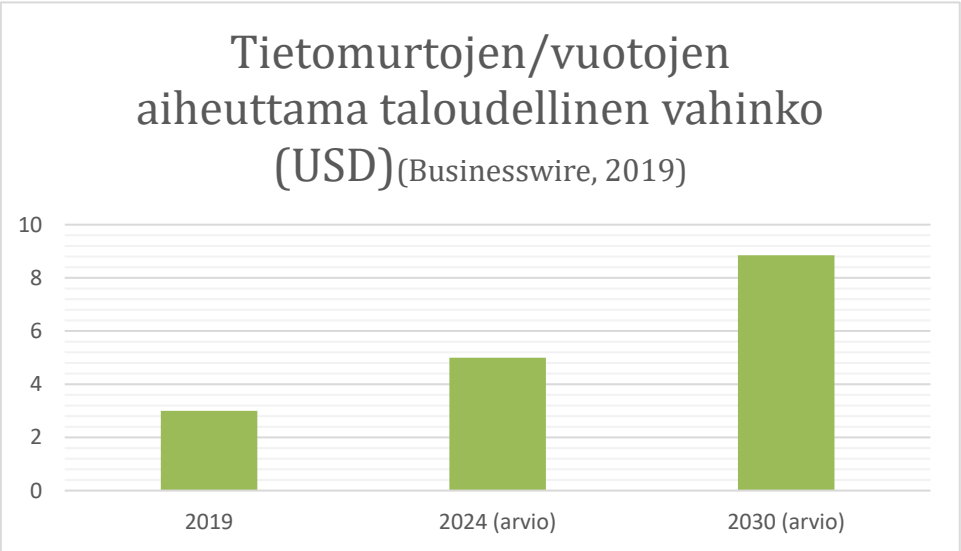
Koska tulevaisuudentutkijoiden näkemysten mukaan asiantuntijoiden näkemykset edustavat oletettavasti sekä korkeatasoisia argumentteja, että toimivat heikkojen signaalien havaitsemisessa hyvänä lähteenä, on syytä ennakoida verkkorikollisuuden tulevaisuudenkuvaa korostuneesti nimenomaan asiantuntijoiden näkemysten kautta. Näistä signaaleista pyrin muodostamaan kokonaiskuvaa tulevasta.

5.2 Verkkorikollisuuden tulevia trendejä

5.2.1 Verkkorikosten määrän ennustetaan kasvavan

Useat verkkorikollisuuteen perehtyneet asiantuntijat sekä toimittajat arvioivat tulevaisuudessa verkkorikosten määrän kasvavan. Yksikään lähdeaineistona käytetyistä asiantuntijanäkemyksistä ei ennakoinut verkkorikollisuuden vähenevän millään osa-alueella, joten määrän kasvusta vallitsee selvä konsensus. Myös taloudellisen vahingon ennustetaan lisääntyvän, eikä tästäkään ollut poikkeavia näkemyksiä asiantuntijoiden kesken.

Juniper Research niminen verkkoympäristöön erikoistunut analyysiyhtiö ennusti vuonna 2019, että verkkorikollisuuden aiheuttamat taloudelliset vahingot jo pelkästään vääriin käsiin päätyneen datan osalta kasvavat noin 11 % vuosivauhdilla. Tämä tarkoittaa, että vuonna 2024 vahingot kasvaisivat viiteen miljardiin Yhdysvaltain dollariin, kun vuoden 2019 taso oli vielä kolmessa miljardissa. Vahinkojen kasvun yksi selittävä tekijä on itse rikollisuuden lisääntymisen lisäksi se, että erilaisten yhtiöiden riippuvuus digitaalisesta ympäristöstä tulee vain kasvamaan. (Businesswire, 2019)



Kuvio 1.1 Mikäli verkkorikoksissa vuotaneiden tietojen aiheuttamien taloudellisten vahinkojen ajatellaan kasvavan ennusteen mukaisella 11 % vuosivauhdilla, on vahinkojen suuruus jo lähes 9 miljardia Yhdysvaltain dollaria vuonna 2030. Tällöin ilmiön aiheuttama vahinko olisi lähes kolminkertaistunut vain kymmenessä vuodessa.

Haittaohjelmien ennustetaan lisääntyvän jatkuvasti. Teknologian nopea kehitys vaatii yrityksiltä ohjelmistojen julkistamista yhä nopeammin ja tässä yhteydessä tietoturva saattaa jäädä puutteelliseksi. Puutteita paikataan tietoturvapaikkauksilla ja päivityksillä, mutta usein liian hitaasti. Haittaohjelmistojen kehittäjät sen sijaan kehittävät ohjelmistojaan jatkuvasti paremmiksi ja itsestään kehittyviksi siten, että ne pystyvät välttämään niitä vastaan tehtyjen tietoturvaohjelmistojen vastatoimet. (Kamat, 2018)

5.2.2 Verkkorikollisuuden tulevaisuutta leimaa järjestäytyminen

Poliisin mukaan verkkorikollisuudessa vallitsevat suuret trendit eivät ole erityisen nopeita muuttumaan. Onkin siis nähtävissä, että nykyisen kaltaiset trendit vaikuttavat vielä pitkälle tulevaisuuteen. Sen sijaan tekotapojen muutos on nopeampaa. Poliisi arvioi erityisesti, että uudet teknologiat muuttavat tekotapoja ja toiminnasta tulee järjestäytyneempää. Tulevaisuudessa onkin odotettavissa, että verkkorikollisuudesta tulee ammattimaisempaa. Poliisi arvioi, että verkkorikollisuuden muodoista erityisesti kiristykset, joko haittaohjelmia hyödyntäen tai ilman niitä, tulevat lisääntymään. Tekotavoista tulee järjestelmällisempiä. (Poliisi, 2020)

Susan W. Brenner arvioikin jo vuonna 2002 järjestäytyneen rikollisuuden korostuvan verkkorikollisuudessa. Brenner ennakoi jopa, että olisi odotettavaa, että internetiin syntyy niin sanottuja kyberrikosma-

fioita ja kyberrikoskartelleja. Toisaalta Brenner korosti myös, että verkkorikollisuuden ei tarvitse ehdottomasti noudattaa reaalimaailman rikollisuuden kehityssuuntia, sillä järjestäytyminen organisaatioiksi voisi osoittautua vähemmän tärkeäksi verkkoympäristön rikollisuudessa. Kartellit ja organisaatiot eivät olisi Brennerin mukaan samoja organisaatioita kuin tosielämän nykyhetken organisaatiot, vaan ne olisivat uusia (Brenner, 2020, s. 7, 24 - 25). Käsittääkseni emme ole nähneet vielä varsinaisia kyberrikosmafioita, mutta vaikuttaa siltä, että Brennerin ennakointi järjestäytymisestä sen sijaan on osunut oikeaan, sillä jo edellä on todettu verkkorikoksiin liittyvän varsin järjestäytyneitä elementtejä.

Sisäministeriö kertoo verkkosivuillaan, että järjestäytynyt rikollisuus on kasvanut siihen liittyvillä ryhmillä mitattuna viimeisen 10 vuoden aikana. Keskusrikospoliisin mukaan Suomessa toimisi jo nyt noin 90 järjestäytynyttä rikollisryhmää. Sisäministeriön mukaan järjestäytyneet ryhmät kansainvälistyvät ja hyödyntävät tietoverkkoja rikoksien tekemisessä erityisesti käyttämällä kiristysohjelmia, tekemällä tietojenkalastelua, petosrikoksia, rahanpesua sekä lapsen seksuaalisia hyväksikäyttöjä. (Sisäministeriö, 2021)

5.2.3 Tekoäly osana tulevaisuuden verkkorikollisuutta

”*Seuraava teknologiavallankumous on hyvää vauhtia lähestymässä, ja sen moottorina toimivat koneoppiminen ja tekoäly. Myös rahan teknologiavallankumous on lähellä. Sitä seuraavat vallankumoukset kuulostavatkin jo tieteiskirjallisuudelta.*” – Mikko Hyppönen, 2021. Internet, s. 271

Kukaan teknologian kehittymistä edes etäisesti seurannut ei ole voinut välttyä tekoälyn ja koneoppimisen käsitteiltä. Useat asiantuntijat ovat viime vuosina tutkineet tekoälyn kehittymistä nimenomaan rikosten apuvälineenä ja alkaneet spekuloida asialla. Tämän takia on järkevää laskea tekoäly yhdeksi merkittäväksi signaaliksi tulevan arvioinnissa. Toteutuessaan tekoälyn uhkakuvat ovat siinä mittaluokassa, ettei aihetta voi jättää kevyen tarkastelun varaan.

Tietoturva-asiantuntija, F-Securen tutkimusjohtaja Mikko Hyppönen katsoo, että tekoäly kehittyy juuri nyt ennen kaikkea koneoppimisen suuntaan. Tämä tarkoittaa sitä, että tekoälyä hyödyntävää ohjelmaa ei ohjelmoida jokaista potentiaalista skenaariota varten vaan ohjelma oppii itse pääsemään sille asetettuun lopputulokseen eri ympäristöissä yrityksen ja erehdyksen kautta. Koneoppimista voidaan käyttää myös verkkorikollisuudessa. Hyppönen nostaa kirjassaan Internet esille, että tietoturvayhtiöt hyödyntävät koneoppimista jatkuvasti kehittäessään tietoturvaansa. Koneoppimista on myös käytetty useissa suuren mittakaavan verkkohyökkäyksissä. Nämä verkkohyökkäykset ovat onneksi kuitenkin suurimmassa osassa tapauksista olleet viranomaisten tai tutkimusyhteisöjen tekemiä harjoituksia, joiden tarkoitus on ollut parantaa tietoturvaa eikä tehdä rikoksia. Koneoppiminen ei Hyppösen mukaan

ole ainakaan vielä tullut varsinaisesti osaksi rikollisten työkalupakkia. Hyppösen mukaan tämä voi johtua nimenomaan siitä, että älykkäiden ohjelmistojen tekeminen on vielä niin hankalaa. Hyppösen mukaan tekoälyohjelmistojen tekemisen vaikeus edellyttää niin suurta osaamisen tasoa, että tällaisen kompetenssin omaavalle ihmiselle löytyy todennäköisemmin laillisia ansaintakeinoja. Hyppönen kuitenkin jättää lopulta avoimeksi sen mikä tekoälyn osuus verkkorikoksista tulee olemaan. (Hyppönen, 2021, s. 276)

Hyppösen keskeinen argumentti on tekoälyohjelmien teon vaikeus. Tekoälyä hyödyntävien ohjelmien kehittyminen on kuitenkin tehnyt ohjelmien teosta ja käytöstä helpompia ja tämä yksinkertaistuminen vain jatkuu tulevaisuudessa. Voi olla perusteltua ajatella, että ohjelmien tullessa valtavirtaisemmiksi, on ohjelmien avulla myös helpompi organisoida hyökkäyksiä. Tutkijoiden keskuudessa ei vallitse selvää yhteisymmärrystä siitä, mikä voi olla tekoälyä hyödyntävän verkkorikollisuuden tulevaisuus. Crime Science Journal (CSJ) on avoin rikollisuuteen pureutuva verkkolehti. CSJ julkaisi 2020 useiden alan tutkijoiden kirjoittaman tekoälyä hyödyntävää verkkorikollisuutta käsittelevän artikkelin. Artikkelissa todetaan, että tekoälyä hyödynnetään jo nyt paljon suuremmassa mittakaavassa kuin yleisesti ajatellaan. Tekoälyn hyödyntämisen ennustetaan myös entisestään kasvavan. Artikkelissa todetaan, että osa potentiaalisista tekoälyn avulla tehdyistä rikoksista voi tuoda lisäulottuvuuksia tavanomaisiin rikoksiin ja osa rikoksista saattaa olla täysin uusia. (Caldwell et. al, 2020)

Caldwell ja kollegat nostavat artikkelissaan esille, että on tärkeää analysoida tulevaisuuden skenaarioita, jotta uhkiin voidaan varautua. Yhtenä keinona ennakointiin tutkijat ovat tehneet kirjallisuuskatsauksen eri potentiaalisista tekoälyä hyödyntävistä rikollisuuden muodoista. Jotkut artikkelissa esitetyt tekoälyä hyödyntävät skenaariot vaikuttavat tulevan yllättävän lähelle aivan tavallista ihmistä korkealentoisen abstraktion asemesta. Esimerkkeinä uhkakuvista mainitaan itsestään ajavien autojen väärinkäyttö, väärän, mutta oikealta näyttävän sisällön luominen (esimerkiksi niin sanotut todellisen näköiset deepfake-videot, joiden kohde laitetaan tekoälyn avulla tekemään ja sanomaan asioita, joita hän ei ole sanonut), automatisoitu tietojen hankkiminen henkilöstä (urkinta), kuljettajattomien autojen ja kuormaautojen käyttö terroriteoissa sekä koneoppimista hyödyntävät tietomurrot ja kyberhyökkäykset. (Caldwell et al., 2020)

Osassa edellä mainituista skenaarioista tekoäly voi toimia työkaluna rikosten tekemiseen nimenomaan reaalimaailmassa. Tällaisia tapauksia voisivat olla esimerkiksi ihmisten sekä organisaatioiden käyttäytymisen ennakoiminen ja haavoittuvuuksien etsiminen. Deepfake-teknologialla luodulla sisällöllä voitaisiin kiristää ihmisiä videoiden julkaisemisella. Deepfake-videot ovat tutkijoiden mukaan tehokkaita, sillä artikkelin mukaan ihmisillä on voimakas taipumus uskoa näkemäänsä ja kuulemaansa. Henkilöä imitoivat deepfake-videot olivat artikkelin käyttämän eräänlaisen huolestuttavuusasteikon kärkipäässä. Artikkelin mukaan tällaisia videoita vastaan taisteleminen onkin erityisen vaikeaa, vaikka teknologiaa deepfake-sisällön paljastamiseksi onkin kehitetty. (Caldwell et. al, 2020)

Kyberrikollisuuden asiantuntija ja Soulin yliopiston tutkija Doowong Jeongin mukaan jotkut tutkijat ovat varoittaneet siitä, että hakkerit käyttävät jo tällä hetkellä tekoälyä parantaakseen hyökkäystensä tehokkuutta. Tekoälyä käytetään hänen mukaansa nimenomaan parantamaan perinteisten rikosten tehokkuutta. Esimerkkejä tällaisista tietoverkkojen avulla tehdyistä rikoksista on muun muassa petosrikollisuus, kyberterrorismi ja kiristys. Jeongin mukaan tutkijoiden näkemys on, että tekoäly tulee vaikuttamaan nimenomaan laajentamalla nykyisiä rikollisuuden uhkakuvia. Tekoälyn avulla rikollisia operaatioita voidaan helposti skaalata suuremmiksi, koska ihmisen tekemän työn osuutta voidaan pienentää teknologian avulla. Tätä kautta rikolliset voivat kohdentaa rikoksia entistä laajemmalle yleisölle. Tekoälyyn pohjautuvan teknologian yleistyminen rikollisten työkalupakissa tulee muuttamaan sitä, mitkä ovat tyypilliset rikollisuuden uhat myös fyysisessä maailmassa. Jeong nostaa esimerkiksi fyysisistä uhista automaattisesti ajavien autojen käytön vahingoittamistarkoituksessa. (Jeong, 2020)

Itsestään ajavien autojen käyttö terroristisiin tarkoituksiin on myös yksi keskeisistä Caldwellin ja kollegoiden artikkelin esiin nostamista uhkakuvista. Autoja on käytetty terroritarkoituksissa usein. Autoihin voidaan asentaa räjähteitä tai sitten autoilla on ajettu väkijoukkoon surmaten useita ihmisiä lyhyessä ajassa. Tällaisista hyökkäyksistä on useita esimerkkejä lähivuosilta, Nizza ja Berliini vuonna 2016, Lontoo 2017 sekä Barcelona ja New York vuonna 2017. Artikkelin mukaan tekoälyä hyödyntäviä autoja voitaisiin hyödyntää jopa koordinoiduissa, suuren mittaluokan terrori-iskuissa, joissa esimerkiksi useita autoja ajaa eri paikoissa tuhoisasti. (Caldwell et al, 2020)

Jeong nostaa artikkelissaan esille myös tekoälyn kasvun vaikutuksen tulevaisuuden tietoverkkoihin kohdistuvissa rikoksissa. Jeongin mukaan tekoäly mahdollistaa teknologisia mahdollisuuksia, joiden avulla rikolliset voivat toteuttaa aiemmin mahdottomiltakin vaikuttaneita teknologisia toimia. Erityisesti rikollisten pääsy tietojärjestelmiin luvattomasti voi helpottua. Esimerkiksi Jeong nostaa, että eri tutkijoiden mukaan salasanojen murtaminen (arvaamistekniikoita käyttäen) on ollut vaikeaa, sillä murroissa on pitänyt käyttää useita erilaisia ohjelmistoja ja keinoja samaan aikaan. Tekoälyn avulla salasanamurtoihin käytettävät useat ohjelmat voidaan helposti integroida ja tätä kautta tietomurrot helpottuvat. Automaattisia, tekoälyyn perustuvia ohjelmistoja voidaan käyttää erilaisten haavoittuvuuksien löytämiseen aiempaa merkittävästi helpommin. (Jeong, 2020)

Voidaan siis todeta, että tekoälyn ja koneoppimisen roolista tulevaisuuden rikollisuudessa ei vallitse täyttä yksimielisyyttä tutkijoiden keskuudessa. Kuitenkin yhteistä lähes kaikkien tutkijoiden näkemyksissä on se, että tekoälyllä voi melko todennäköisesti olla jonkinlainen rooli tulevaisuuden rikollisuuden kokonaiskuvassa. Kiistanalaista sen sijaan on se, millä käytännön tavoilla ja missä mittakaavassa tekoäly tulee ilmenemään verkkorikollisuudessa. Jeong korostaa artikkelinsa lopussa, että rikostutkijoiden on kasvatettava osaamistaan tekoälystä ja heidän tulee ymmärtää sen toimintamekanismeja ja rikollisia sovellutuksia (Jeong, 2020).

Tekoälyn kautta perinteisiin verkkorikoksiin voitaisiin luoda automaattista älyä. Älyä, jossa ihmisen ei tarvitse seurata ohjelmiston toimintaa sillä ohjelmisto toimii automaattisesti. Stoecklin kertoo SecurityIntelligence-lehdessä, että IBM Research on tehnyt kokeellisia haittaohjelmiston, DeepLockerin. DeepLocker leviää paikasta toiseen ja aktivoituu lopulta kohdatessaan tietyn kohteen. Kohteen se tunnistaa erilaisia tekoälyn sovellutuksia apuna käyttäen. Apuna kohteen tai kohteiden tunnistamisessa voidaan käyttää kasvojentunnistusta sekä äänentunnistusta. Perinteiseen haittaohjelmaan nähden kyseessä on varsin erilainen ohjelmisto, jota verrataankin artikkelissa tarkkuusammuntaan. Tällaista haittaohjelmiston aiheuttamaa infektiota tietojärjestelmälle on erittäin vaikea huomata perinteisin keinoin. Stoecklinin mukaan tällaiset täysin uudet haittaohjelmistot ovat tulossa verkkorikollisuuden kenttään hyvin pian. Hänen mukaansa työkalut tällaiset haittaohjelmiston tekemiseen ovat olemassa eikä olisi ihme, että sellaisia tietämättä jo käytetäänkin. (Stoecklin, 2018)

Tekoälyn vaikutuksien voidaan perustellusti ajatella olevan suuria, mikäli tekoäly tulee osaksi verkkorikollisuutta. Näin siksi, koska tekoäly voi tuoda yhtäältä uusia ulottuvuuksia vanhoihin rikoksiin sekä luoda kokonaan uusia rikollisuuden muotoja. Kovin moni teknologia ei välttämättä voisi samassa mittakaavassa luoda uusia uhkakuvia ja laajentaa entisiä.

5.3 Verkkorikollisuus ja Suomen poliisi

Kuten aiemmin on todettu, verkkorikollisuuden voidaan perustellusti ajatella lisääntyvän ja monimuotoistuvan. Lainsäädäntömme tuntee aiempaa enemmän verkkorikollisuuden muotoja. Tätä kautta myös poliisi joutuu suorittamaan tulevaisuudessa verkkorikosten tutkintaa esitutkintalain velvoittamana. Näkisin erityisen tärkeiksi kysymyksiksi nimenomaan poliisin näkökulmasta sen, onko poliisi valmistautunut siihen, että verkkorikollisuus lisääntyy runsaasti? Onko poliisilla valmiutta tutkia suurta määrää internetissä ja sen avulla tapahtuneita rikoksia? Miten poliisiin saadaan riittävä osaaminen tutkimaan monimutkaisia verkkorikoksia?

Poliisin strategia vuosille 2020–2024 tuntuu ottaneen vakavasti verkossa tapahtuvaan rikollisuuteen puuttumisen. Poliisin strategiassa korostetaan sitä, että yhteiskunta on muutoksessa ja käynnissä on edelleen teknologinen vallankumous. Kokonaiskuvassa otetaan huomioon digitalisoituminen sekä tekoäly ja kyberuhat. Edellä mainitun kehityksen ennustetaan heijastuvan poliisiin nimenomaan verkossa tapahtuvana ja verkkoja hyödyntävänä rikollisuutena. Strategiassa korostetaan myös yhteistyön merkitystä. Poliisin strategiassa korostuu yhteistyön syventäminen eri yhteistyötahojen kanssa, mikä varmasti on perusteltua myös verkkorikollisuuden suhteen. (Poliisi c, 2020)

Poliisin näkökulmasta tuntuisi tärkeältä huomioida se, miten poliisi saa rekrytoitua riittävästi kyberosaajia osaksi organisaatiota. Usein kyberosaajat ovat varsin haluttuja työntekijöitä eri organisaatioissa. Esimerkiksi sanomalehti Kaleva uutisoi jo 2016, että Suomessa on kyberosaajista ”huutava pula”. Erityisesti pulaa oli tietoturvayrityksissä (Juupaluoma, 2016). Kyberosaajille maksetaan huomattavia summia eri organisaatioissa, joten on oletettavaa, että heidät viedään käsistä tietoturvaosaajiksi yrityksiin, kun heistä on siellä pulaa. Poliisin ja verkkorikollisuuden kontekstissa olisi tärkeää varmistaa myös se, että poliisi houkuttelee työpaikkana kyberosaajien kärkijoukoissa.

LÄHTEET

Barabosch, Thomas, 2021. Telekom. Flubot's Smishing Campaigns under the Microscope. Luettavissa: https://www.telekom.com/en/blog/group/article/flubot-under-the-microscope-636368

Brenner, W. Susan. North Carolina Journal of Law & Technology. Volume 4 Issue 1. Organized Cybercrime – How Cyberspace May Affect the Structure of Criminal Relationships. Luettavissa: https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1044&context=ncjolt

Brenner, W. Susan., 2010. Cybercrime, Criminal Threats From Cyberspace. Praeger.

Businesswire, 2019. Business Losses to Cybercrime Data Breaches to Exceed $5 trillion by 2024. Luettavissa: https://www.businesswire.com/news/home/20190826005013/en/Business-Losses-Cybercrime-Data-Breaches-Exceed-5

Caldwell et al., 2020. Crime Science. AI-enabled future crime. Luettavissa:

https://crimesciencejournal.biomedcentral.com/track/pdf/10.1186/s40163-020-00123-8.pdf

Ellonen et al., 2019. Tilastokeskus. Lapsiin kohdistuvat seksuaalirikosten ilmoitukset kasvussa, uhrikokemukset eivät. Luettavissa:

https://www.stat.fi/tietotrendit/artikkelit/2019/lapsiin-kohdistuneiden-seksuaalirikosten-ilmoitukset-kasvussa-uhrikokemukset-eivat/

Europol, 2021. Darkmarket: World's largest illegal dark web marketplace taken down. Luettavissa: https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

FBI a, 2019. Romance Scams. Luettavissa: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams

FBI b, 2021. Sextortion. An Online Threat to Kids and Teens. Luettavissa: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/sextortion

F-Secure a, 2021. Mitä on tietojenkalastelu. Luettavissa: https://www.f-secure.com/fi/home/articles/what-is-phishing

F-Secure b, 2021. Denial Of Service (DOS). Luettavissa: https://www.f-secure.com/v-descs/articles/denial-of-service.shtml

Grannan, Cydney, 2021. What's the Difference Between the Deep Web and the Dark Web? Luettavissa: https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web

Helsingin Sanomat, 2019. 23.8.2019 lehti. Palvelunestohyökkäys kaatoi poliisin, hätäkeskuksen ja Verohallinnon verkkosivuja. Luettavissa: https://www.hs.fi/paivanlehti/23082019/art-2000006213053.html

Hiltunen, Elina, 2008. Good Sources of Weak Signals: A Global Study of Where Futurists Look For Weak Signals. Luettavissa: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.390.9014&rep=rep1&type=pdf

Huhtanen, Jarmo, 2020. Helsingin-Sanomat 21.10.2020. Potilaiden tietoja vietiin psykoterapiakeskuksen tietomurrossa, yritys kertoo joutuneensa kiristyksen uhriksi. Luettavissa: https://www.hs.fi/kotimaa/art-2000006676407.html

Hyppönen Mikko, 2021. Internet. WSOY.

Hämäläinen et al., 2020. YLE. Yksi heistä on kiristäjä. Luettavissa: https://yle.fi/uutiset/3-11616210

Härkönen, Rebekka, 2018. Aamulehti. Ahneus, myötätunto ja rakkaudennälkä saavat uhrin tarttumaan syöttiin – Nettihuijarien viemiä rahoja on lähes mahdotonta saada takaisin. Luettavissa: https://www.aamulehti.fi/uutiset/art-2000007308859.html

IF b, 2021. Tietomurtoon tarvitaan vain yksi klikkaus. Luettavissa: https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvavakuutus/tietomurto

IF, 2021. Esimerkkejä tietoturvarikoksista. Luettavissa: https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvavakuutus/esimerkkeja-kyberrikollisuudesta

Jeong, Doowon, 2020. Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. Luettavissa: https://www.researchgate.net/publication/346952094_Artificial_Intelligence_Security_Threat_Crime_and_Forensics_Taxonomy_and_Open_Issues

Juupaluoma, Johanna, 2016. Kaleva. Kyberosaajista huutava pula – ”Tarvitsemme parempia koulutusohjelmia”. Luettavissa: https://www.kaleva.fi/kyberosaajista-huutava-pula-tarvitsemme-parempia-k/1744702

Jämsén, Christian, 2020. Poliisi. Tietoverkkorikollisuus poliisin silmin 2019–2020. Luettavissa: https://poliisi.fi/blogi/-/blogs/tietoverkkorikollisuus-poliisin-silmin-2019-2020

Kamat et al. 2018. ResearchGate. Recent Trends in the Era of Cybercrime and the Measures to Control Them. Luettavissa: https://www.researchgate.net/publication/326774451_Recent_Trends_in_the_Era_of_Cybercrime_and_the_Measures_to_Control_Them/link/5b8a32eba6fdcc5f8b75cfae/download

Kemppinen, Ilkka, 2021. YLE. ”Anonyymi murhapalvelu, maksu bitcoineina”. – Kun kaksi suomalaista nuorukaista löysi toisensa netissä, seuraukset olivat kohtalokkaat. Luettavissa. https://yle.fi/uutiset/3-11386629

Keskusrikospoliisi, 2021. YouTube. Keskusrikospoliisin tiedotustilaisuus 27.10.2021. Katsottavissa: https://www.youtube.com/watch?v=igSRFWwqkC0

Kuusi, Osmo, 2008. Tieteessä Tapahtuu 5/2008. Miten tulevaisuutta voi tutkia tieteellisesti? Luettavissa. https://journal.fi/tt/article/download/541/458

Kyberturvallisuuskeskus a, 2018. Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota! Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

Kyberturvallisuuskeskus c, 2019. Traficom. Tietoturvan vuosi 2019. Kyberturvallisuuskeskuksen vuosikatsaus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_tietoturvanvuosi_2019_WEB_sivuittain.pdf

Kyberturvallisuuskeskus, 2016. Viestintävirasto. Ohje 3/2016 Palvelunestohyökkäysten ehkäisy ja torjunta. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta_0.pdf

Leppänen, Anna, 2021. Kyberrikos on poliisiasia. Opas yrityksille kyberrikostutkinnan kulusta. Luettavissa: https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212?t=1616740405258

Linnake, Tuomas, 2020. Ilta-Sanomat. Poliisilta vakava varoitus pilaileville etäkoululaisille: ”Hölmöilyllä voi olla vakavat seuraukset lapsen tulevaisuudelle”. Luettavissa: https://www.is.fi/digitoday/tietoturva/art-2000006460118.html

Makrushin, Denis, 2017. Securelist by Kaspersky. The cost of launching a DDoS attack. Luettavissa: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/

McAfee, 2021. Mikä on haittaohjelma. Luettavissa: https://www.mcafee.com/fi-fi/antivirus/malware.html

NSPCC, 2019. Over 9,000 police-recorder online child sexual abuse offences. Luettavissa: https://www.nspcc.org.uk/about-us/news-opinion/2019/web-exploited-by-child-sex-offenders/

Nykänen, Riikka, 2017. Ilta-Sanomat. Muistatko kun laaja verkkohyökkäys kaatoi OP:n palveluita? Nyt käräjillä siitä syytetään yhtä miestä. Luettavissa: https://www.is.fi/kotimaa/art-2000005410874.html

Pelastakaa Lapset, 2013. Internet ja lasten seksuaalinen hyväksikäyttö. Ota puheeksi. Luettavissa: https://pelastakaalapset.s3.eu-west-1.amazonaws.com/main/2016/02/09160156/Ota-puheeksi.pdf

Pelastakaa Lapset, 2021. Lapsen houkuttelu seksuaalisiin tarkoituksiin (grooming). Luettavissa: https://www.pelastakaalapset.fi/kehittamis-ja-asiantuntijatyo/nettivihje-ja-seksuaalivakivallan-ennalta-ehkaisy/tietoa-lapsiin-kohdistuvasta-seksuaalivakivallasta/lapsen-houkuttelu-seksuaalisiin-tarkoituksiin-grooming/

Poliisi a, 2021. Poliisin tietoon tulleiden rikosten määrä on laskenut, mutta tutkinta-ajat pidentyneet. Luettavissa: https://poliisi.fi/-/poliisin-tietoon-tulleiden-rikosten-maara-on-laskenut-mutta-tutkinta-ajat-pidentyneet

Poliisi b, 2020. Tietomurrot. Luettavissa: https://poliisi.fi/tietomurrot

Poliisi c, 2020. Poliisin strategia 2020–2024: https://poliisi.fi/documents/25235045/28127375/Poliisin-strategia-2020-2024.pdf/712129e3-0110-cdc1-3ef3-8c29052a5763/Poliisin-strategia-2020-2024.pdf?t=1606152509317

Poliisi d, 2021. Poliisi varoittaa kahdesta Suomessa aktiivisesta huijauksesta. Luettavissa: https://poliisi.fi/-/poliisi-varoittaa-kahdesta-suomessa-aktiivisesta-huijauksesta

Poliisi, 2020 a. Palvelunestohyökkäykset. Luettavissa: https://poliisi.fi/palvelunestohyokkays

Rikoslaki (39/1889) / (21.4.1995/578)

Rikosuhripäivystys a, 2019. Rikokset verkossa yleistyvät verkon käytön lisääntyessä. Luettavissa: https://www.riku.fi/rikosuhripaivystys/riku-lehti/riku-lehti-2-2017/rikokset-verkossa-yleistyvat-verkon-kayton-lisaantyessa/

Rikosuhripäivystys b, 2017. RIKU-lehti nro. 2/2017. Luettavissa: https://www.riku.fi/content/uploads/su_file/1883__RIKU_2_2017.pdf

Rikosuhripäivystys c, 2019. Rakkauspetokset ja romanssihuijaukset verkossa. Luettavissa: https://www.riku.fi/erilaisia-rikoksia/rakkauspetokset-verkossa/

Rikosuhripäivystys d, 2019. Petokset. Luettavissa: https://www.riku.fi/erilaisia-rikoksia/petokset/

Sabillon et al., 2016. International Journal of Computer Networks and communications Security. Vol 4, NO 6. Cybercrime and Cybercriminals: A Comprehensive Study. Luettavissa: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/78507/1/p1_4-6.pdf

Salminen, Ari, 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopisto. Luettavissa: https://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Sisäministeriö, 2017. Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf?sequence=1

Sisäministeriö, 2021. Järjestäytynyt rikollisuus vaikuttaa laajasti yhteiskuntaan. Luettavissa: https://intermin.fi/poliisiasiat/jarjestaytynyt-rikollisuus

Stoecklin, Marc, 2018. SecurityIntelligence. DeepLocker: How AI can Power a Stealthy New Breed of Malware. Luettavissa: https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

Taleb, Nassim Nicholas, 2007. Musta joutsen. Erittäin epätodennäköisen vaikutus. Terra Cognita

Tulli, 2020. Tuhansien rikosepäilyjen Silkkitie. Luettavissa: https://tulli.fi/web/tullinvuosi/2019/valvonta/huumausainerikokset/tuhansien-rikosepailyjen-silkkitie

Wired, 2020. 9.12.2020. A dying man, a therapist and the ransom raid that shook the world. https://www.wired.co.uk/article/finland-mental-health-data-breach-vastaamo

Wittes et al., 2016. Brookings. Report. Sextortion: Cybersecurity, teenagers, and remote sexual assault. Luettavissa: https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/