Haaga-Helia
ammattikorkeakoulu Oy

Kyberrikollisuuden esiintyminen Suomessa

Iina Savela

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2020

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Iina Savela

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Kyberrikollisuuden esiintyminen Suomessa

Sivu- ja liitesivumäärä
43

Kyberrikollisuus on kasvava ilmiö, joka vaikuttaa niin yritysten kuin yksityishenkilöidenkin elämään internetissä. Kyber- tai verkkorikollisuutta on kahta tyyppiä: tietoverkkoihin kohdistuvaa ja niiden avulla tehtävää. Kyberrikos ei ole terminä rikoslain mukainen, mutta se on vakiintunut yleiseen käyttöön niin viranomaisten kuin mediankin keskuudessa.

Tässä tutkimuksellisessa opinnäytetyössä käsitellään Suomessa esiintyviä kyberrikostyyppejä sekä viranomaisten keinoja torjua ja tutkia verkkorikollisuutta. Tutkimus on tarkoitettu verkkorikollisuudesta ja tietoturvasta kiinnostuneille henkilöille sekä poliisiksi opiskeleville tai aiheen parissa työskenteleville. Työn tarkoitus on kattaa perusteet ja tarjota tietoa selkeällä ja yleiskielisellä tavalla. Opinnäytetyön lähteinä on käytetty pääasiassa vuodesta 2015 eteenpäin julkaistua materiaalia, sillä aihe on varsin ajankohtainen ja osa rikosnimikkeistä on kirjattu lakiin vasta vuonna 2015.

Työn avulla voidaan tutustua erilaisiin tapoihin, joilla verkkorikollisuus voi näkyä tavallisessa arjessa. Opinnäytetyön tavoitteena on tuottaa tutkimus, jonka lukijalla ei tarvitse olla ymmärrystä tietotekniikasta. Toinen päätavoite on lisätä tietoa kyberrikollisuudesta ja -turvallisuudesta sekä muistuttaa, että jokaisen tulee huolehtia omasta tietoturvastaan.

Myös Suomessa on nähtävissä paljon kyberrikollisuutta ja sen esiintyminen on ollut viime vuosina kasvussa. Verkkorikollisuus ylittää usein maarajat, mikä vaikeuttaa sen tutkimista. Kaikki verkkorikosten uhrit eivät myöskään häpeän tai muun syyn vuoksi tee rikosilmoitusta poliisille, minkä vuoksi kyberrikollisuudesta puhutaan usein piilorikollisuutena.

Suomessa on erilaisia viranomaistahoja, jotka tutkivat ja ennaltaehkäisevät verkkorikollisuutta sekä tiedottavat siitä kansalaisille ja yrityksille. Keskusrikospoliisiin perustettu Kyberrikostorjuntakeskus ja Traficomin Kyberturvallisuuskeskus ovat hyviä esimerkkejä siitä, kuinka valtiotasollakin on varauduttu verkkorikollisuuden kasvuun.

Opinnäytetyön tuloksena on havaittu, että yksilön vastuu on entistä suurempi toimittaessa kyberrikollisuutta vastaan. Yksityishenkilöt ja yrityksen työntekijät ovat tärkeässä roolissa rikoksien ehkäisemisessä ja yleisen tietoturvan ylläpitämisessä. Yritysten tulee myös jatkuvasti tavoitella parempaa tietoturvaa ja pitää huolta siitä, että niin yrityksen oma data kuin potentiaalinen asiakasdata pysyy tallessa ja varmistettuna.

Asiasanat
Kyberrikollisuus, tieto- ja viestintärikokset, tietoverkkorikokset, tietotekniikkarikokset, tietoturva

Sisällys

1 Johdanto

Kyberrikollisuus on viime vuosien aikana noussut ajankohtaiseksi huolenaiheeksi. Internetin räjähdysmäinen kasvu 2000-luvulla ja sen yleistyminen ympäri maailman ovat tuoneet tiedon yhä useamman ulottuville. Ihmisten yhdistäminen sijainnista riippumatta on yksi sosiaalisen aikakautemme perustekijöistä. Valtavaan määrään tietoa sisältyy kuitenkin väistämättä myös haitallista materiaalia, jolla on monenlaisia vaikutuksia esimerkiksi nykyaikaiseen työskentelyyn ja yksityisyyteen. Tiedon saatavuudella ja sijainnista riippumattomalla kommunikoinnilla on kääntöpuolensa, sillä kaikki tämä ulottuu myös rikollismaailmaan. Perinteiset fyysisessä ympäristössä tapahtuvat rikokset, kuten ryöstöt, asuntomurrot ja pahoinpitelyt ovat saaneet rinnalleen uudenlaisen ilmiön, joka tapahtuu verkossa tai sen avustuksella. Pankkihuijaukset, tunnuksien kalastelu sekä verkkoviha tai kunnianloukkaukset internetissä ovat ottaneet paikkansa virtuaalisen maailman vastineina näille rikoksille. Lähes jokaiselle perinteiselle rikokselle voidaan löytää vastinpari kybermaailmasta, sillä verkon käyttö on vain uudenlaisen työkalun omaksumista – myös rikollisille.

Kyberrikosten yleistyminen ei kuitenkaan tarkoita sitä, että kaikki netissä tapahtuva olisi vaarallista. Samanlainen varovaisuus ja maalaisjärjen käyttö, mikä pätee muuhunkin elämään fyysisessä maailmassa, on hyödyllistä muistaa myös verkossa. Aidon näköisiä verkkopankin kirjautumissivuja on käytetty tunnusten kalastelutarkoituksissa jo vuosikausia. Sosiaalisessa mediassa sekä suoraan sähköpostitse tapahtuvat verkkohuijaukset on helppo kohdistaa useaan henkilöön yhtä aikaa, jolloin huijauksen onnistumisen todennäköisyys kasvaa. Oma käyttäytyminen internetissä on hyvä tiedostaa, ja jokaisen verkossa liikkujan on suotavaa pohtia, onko henkilökohtainen tietoturva ajan tasalla ja kriittinen ajattelu mukana päivittäisessä toiminnassa. Netin käyttö on kuitenkin käytännössä välttämätöntä tänä päivänä, ja järkevän toiminnan avulla se pysyy hyödyllisen lisäksi myös turvallisena.

Kyberrikollisuus koskettaa niin yksityishenkilöitä kuin yrityksiä ja organisaatioitakin. Verkossa tapahtuneen rikoksen uhrin voi joskus olla hankalaa ilmoittaa tapahtuneesta poliisille. Monet saattavat kokea, että rikos on aiheutunut omasta tyhmyydestä tai huolimattomuudesta, jolloin kynnys rikosilmoituksen tekemiselle kasvaa. Häpeän tunteen vuoksi poliisille ilmoitetaan vain osa verkossa tapahtuneista rikoksista. Tämän vuoksi verkkorikollisuus on niin kutsuttua piilorikollisuutta. (Keskusrikospoliisi 2018a.) Kyberrikoksissa hyödynnetään usein ihmisten luottamusta toisiin, jolloin uhri voi jopa kokea olevansa osittain syyllinen tapahtuneeseen. Tällainen stigma liittyy läheisesti erityisesti esimerkiksi rakkaushuijauksiin, joissa henkilöiltä huijataan pahimmassa tapauksessa suuria summia rahaa

oletetun rakkauden vuoksi. Häpeä voi liittyä myös onnistuneisiin pankkitunnusten kalasteluyrityksiin, jolloin uhrin tili on voitu tyhjentää hyvin nopeasti. Näiden rikosten henkilökohtaisuus ja yksityisyys voivat turhaan aiheuttaa uhreille häpeän tunteita, jolloin rikosilmoitus jää tekemättä.

Kyberrikollisuudesta puhuminen on tehokas keino lisätä tietoisuutta ja mahdollisesti siten vähentää uhriksi joutumisen riskiä. Tiedon jakaminen voi lisätä varovaisuutta ihmisten suhtautumisessa ja ylläpitää keskustelua internetin käytöstä. Mitä enemmän tietoa on saatavilla, sitä helpompi sitä on myös löytää ja hyödyntää omiin tarpeisiin. Tämän opinnäytetyön tavoitteena on koota Suomessa esiintyvästä kyberrikollisuudesta kokonaiskuva sekä poistaa faktojen myötä väärinkäsityksiä ja mahdollista pelkoa internetin käyttämisestä. Tarkoituksena on kasvattaa ymmärrystä internetiä ja sen erilaisia puolia kohtaan, sillä tutumpaa ympäristöä on helpompi lähestyä järkevästi ja objektiivisesti. Opinnäytetyö kokoaa tietoa selkeästi ja sellaisessa muodossa, että lukijan ei tarvitse tuntea IT-alaa tai kybermaailmaa.

Opinnäytetyön kohteena on suomalainen kyberrikollisuus, sillä kotimaan tapahtumat kiinnostavat luonnollisesti enemmän kuin ulkomailla sattuneet rikokset. Tutkimuksessa käytetään vain julkisesti saatavilla olevaa materiaalia asian arkaluonteisuuden ja osittaisen salassa pidettävyyden vuoksi. Tämä rajaa tiedonkeruuta hieman, mutta suomalaiset viranomaiset ovat viime vuosien aikana tuottaneet eri näkökulmista useita laajoja katsauksia ja tutkielmia kyberrikollisuuden muodoista ja sen torjunnasta. Uutisointi aiheesta lisääntyy jatkuvasti, ja verkkorikoksista on annettu myös joitakin tuomioita. Varsinaista aikarajausta opinnäytetyöllä ei ole, mutta materiaali koostuu pääasiassa vuonna 2015 ja sitä myöhemmin julkaistusta aineistosta, sillä kyberrikollisuus on aiheena varsin tuore. Opinnäytetyössä ei käsitellä kaikkia olemassa olevia kyberrikoksia, sillä erilaisia rikostyyppejä on melko runsas määrä. Opinnäytetyössä keskitytään muutamaan mielenkiintoisimpaan ja yleisimpään rikostyyppiin, jotka ovat myös olleet eniten esillä aineistoa tutkittaessa.

Opinnäytetyössä kokemusperäistä tietoa ovat tarjonneet kaksi haastateltavaa, jotka ovat tuoneet esille hyvin erilaiset näkökulmansa. Keskusrikospoliisin rikoskomisarion näkemykset kyberrikollisuudesta ja sen tutkinnasta avaavat mielenkiintoisen näkymän poliisin tämän hetken haasteisiin. Toisen näkökulman tarjoavat tor-palvelimen ylläpitäjän mielipiteet sananvapaudesta ja ihmisen oikeudesta yksityisyyteen. IT-alalla työskentelevä haastateltava tuo tärkeän ja pohdintaa herättävän näkökulman kiistanalaisen tor-verkon tarpeellisuudesta. Molempiin haastatteluihin varauduttiin erityyppisin kysymyksin, sillä rikoskomi-

sarion haastattelu käsitteli kyberrikollisuutta laajemmin. Tor-verkosta oli puolestaan tavoitteena saada aikaiseksi haastateltavan omiin kokemuksiin ja tietoon perustuva keskustelu ainoastaan tor-verkkoon ja sen käyttöön liittyen.

Opinnäytetyön johdantoa seuraa katsaus erilaisiin kyberrikostyyppeihin, jotka edustavat yleisintä joukkoa kyberrikollisuuden kirjavassa maailmassa. Tässä osiossa käsitellään tarkemmin, minkälaisia kyberrikoksia yleensä on olemassa ja millaisia piirteitä kuhunkin liittyy. Tämä kappale luo yleiskäsityksen valittuihin kyberrikoksiin, jotka usein ovat moderneja versioita perinteisistä, fyysisessä maailmassa tapahtuvista rikoksista. Käsiteltäviä aiheita ovat esimerkiksi kryptorahat ja niihin liittyvät huijaukset, verkkohuijaukset kuten kalasteluyritykset sekä Tor-verkko ja sen mahdollistama anonyymi rikollisuus kaikkien ulottuvilla.

Seuraavassa osiossa tarkastellaan Suomessa esiintyviä kyberrikoksia edellisen osion pohjalta. Tässä luvussa tutkitaan, millaisia julkaisuja esimerkiksi poliisi ja Poliisiammattikorkeakoulu ovat tuottaneet kyberrikollisuuteen liittyen ja millaista uutisointia aiheesta on kirjoitettu. Osio käsittelee myös kyberrikosten selvittämisen onnistumista verrattuna perinteisiin rikoksiin. Luvussa tutkitaan myös hieman tilastoja, vaikka kyberrikollisuudesta onkin saatavilla hyvin vähän Tilastokeskuksen tai poliisin itsensä tarjoamaa numeerista dataa. Lopuksi pohditaan tor-verkon käyttöä sekä tarpeellisuutta Suomessa haastattelun pohjalta.

Neljäs luku käsittelee kyberrikollisuuden torjuntaa Suomessa. Tässä osiossa paneudutaan muun muassa Keskusrikospoliisiin perustetun Kyberrikostorjuntakeskuksen toimintaan rikoskomisarion haastattelun avulla ja tarkastellaan, millainen kyberturvallisuusstrategia Suomessa on luotu. Neljännessä luvussa käsitellään myös Poliisiammattikorkeakoulun kyberopetusta ja pohditaan, millaiselta kyberrikollisuuden tulevaisuus näyttää.

Lopuksi pohditaan sitä, miltä kyberrikollisuus Suomessa kokonaisuutena näyttää ja miltä se tuntuu kansalaisen näkökulmasta. Tässä luvussa kootaan yhteen kaikki tutkimuksen aikana selvinnyt ja mietitään, millaisia vaikutuksia kyberrikollisuuden yleistymisellä voi olla esimerkiksi yritysten toiminnalle ja yleisesti internetissä liikkumiselle.

2 Kyberrikostyyppejä

Kyberrikos on käsitteenä yhä hieman epämääräinen. Suomen laki ei tunne termiä kyberrikos tai verkkorikos, vaan tämä käsite avautuu rikoslain (39/1889) 38 luvussa erillisiksi pykäliksi, kuten identiteettivarkaus ja tietojärjestelmän häirintä. Kummatkin näistä sekä muutama muu pykälä on lisätty rikoslakiin vasta vuonna 2015, mikä kertoo aiheen tuoreudesta. Lisäksi rikoslain 35 luvussa on säädetty rangaistus datavahingonteolle, joka tarkoittaa esimerkiksi tietovälineelle tallennetun tiedon hävittämistä, muuttamista tai vahingoittamista. Joitakin muita internetiin liittyviä rikoksia löytyy rikoslain muista luvuista, eikä kaikkia ole sisällytetty yhden luvun alle.

Tässä opinnäytetyössä käytetään pääasiassa termejä kyberrikos ja kyberrikollisuus, mutta toiston välttämiseksi myös termejä verkkorikos ja verkkorikollisuus, sillä nämä ovat toistensa synonyymit. Tekstissä käytetään ainoastaan yleistajuista kieltä, joka ei vaadi IT-alan osaamista tai ymmärrystä. Opinnäytetyön tarkoitus on tuottaa tietoa mahdollisimman laajalle yleisölle, jonka arkea kyberturvallisuus ja -rikollisuuskin saattaa koskettaa. Tämän vuoksi erillistä sanastoa ei ole koottu.

2.1 Kyberrikoksen määritelmä

Vuonna 2018 Turvallisuuskomitea, Huoltovarmuuskeskus ja Sanastokeskus TSK ry julkaisivat Kyberturvallisuuden sanaston, joka pyrkii täyttämään aiheeseen liittyvien määritelmien puutetta. Kyseinen sanasto sisältää runsaasti kyberturvallisuuteen sekä -rikollisuuteen liittyvää terminologiaa, joka helpottaa aiheen käsittelyä viranomaisten taholta. Varsinaista sanaa ”kyberrikos” ei kuitenkaan mainita sanastossa lainkaan, mikä kertoo mahdollisesti siitä, että alan ammattilaisetkaan eivät ole varmoja siitä, kuinka tätä kattotermiä tulisi käyttää. Kyberrikos on sanana hieman ympäripyöreä ja kattaa paljon alakäsitteitä, mutta se on vakiintunut myös viranomaiskäytössä yleisesti käytetyksi termiksi.

Kyberturvallisuuden sanastossa viitataan kyberrikos-termin kohdalla kyberrikollisuuteen ei tietoverkkorikollisuuteen, joka on määritelty seuraavasti: ”…rikollisuus, joka muodostuu viestintäverkkoja ja tietojärjestelmiä hyödyntäen tehdyistä sekä niihin kohdistuvista rikoksista” (Sanastokeskus TSK ry 2018, 26). Kyberrikollisuuden merkitys on siis kaksitahoinen. Verkkoja hyödyntäen tehdyt rikokset tarkoittavat esimerkiksi tietojenkalasteluviestejä tai muita internethuijauksia, ja tietoverkkoihin kohdistuvat rikokset sisältävät esimerkiksi palvelunestohyökkäykset, joilla pyritään estämään jonkin verkkopalvelun käyttö kokonaan. Näiden kahden erilaisen rikostyypin alle mahtuu monenlaisia eri hyötymistarkoituksessa

tehtyjä rikoksia. Kevyimmillään palvelunestohyökkäys voidaan toteuttaa parin kokeilunhaluisen harrastelijan toimesta. Tällöin ei usein ymmärretä teon vakavuutta, seuraamuksia ja mahdollista rikosoikeudellista vastuuta, joka tekoon liittyy. Toisessa ääripäässä ovat esimerkiksi pyramidihuijauksina toimivat, organisoidut kryptorahahuijaukset, joissa ihmisille kaupitellaan olematonta valuuttaa taloudellisen rikoshyödyn saamiseksi.

Kyberrikoksia tehtailevien amatööri- ja ammattilaisrikollisten lisäksi kybermaailmassa esiintyy valkohattuhakkereita sekä niin kutsuttuja haktivisteja. Valkohattuhakkerit ovat tietoturva-alan ammattilaisia, jotka pyrkivät paljastamaan yritysten tietoturvapuutteita ja -uhkia laillisin keinoin. Haktivistit puolestaan haluavat levittää mielipidettään tai puolustaa sananvapautta sekä internetin demokratiaa usein laittominkin keinoin. Heitä ei motivoi raha vaan oman käden oikeuden toteuttaminen ja korruptiota vastaan taisteleminen (Stammeier & Jokelainen 2017). Tällaisia aatteisiin perustuvia ryhmittymiä on maailmalla useita, mutta yksi tunnetuimmista on Anonymous, joka nimensä mukaisesti pysyttelee nimettömänä ja sen jäsenet esiintyvät videoilla kasvot peitettyinä.

Kyberrikollisuuden olennainen elementti on anonyymiys, joka mahdollistaa jopa täydellisen etääntymisen rikoksen uhrista. Verkon yli tehtävät rikokset ylittävät usein kansalliset rajat, mikä osaltaan hankaloittaa tai vähintään hidastaa tutkintaa. Tämä on yksi hyvin tyypillinen verkkorikollisuuden ominaisuus, jonka avulla se myös eroaa perinteisestä rikollisuudesta. Internetin tarjoama kasvottomuus ja nimettömyys myös suojaa osaltaan rikollisia, sillä uhri ei välttämättä edes tiedä, milloin ja miten rikos on tapahtunut. (Aaltonen, Suonpää, Kivivuori, Danielsson & Näsi 2018, 403-404.)

Kyberrikosten monimuotoisuus on lähes yhtä kirjavaa kuin perinteistenkin rikosten. Kuten mainittu, lähes kaikille rikoksille löytyy kybermaailmasta moderni vastine. Monet rikolliset ovat saattaneet siirtyä verkkoon huomattuaan sen tarjoaman suojan olevan oiva apuväline rikosten piilottelussa. Toisaalta tämä on osaamattomalle rikolliselle valheellinen ajatustapa, sillä avoimessa internetissä kaikesta jää jälki ja monet ammattilaisetkaan eivät osaa piilottaa liikkumistaan netissä. Seuraavissa osioissa esitellään yleisimpiä verkkorikostyyppejä, joita nähdään myös Suomessa.

2.2 Kiristyshaittaohjelmat

Kiristyshaittaohjelma (englanniksi ransomware) on Kyberturvallisuuden sanastossa määritelty haittaohjelmaksi, joka salaa tai muuttaa päätelaitteella olevia tietoja. Kiristys liittyy kyseiseen haittaohjelmatyyppiin siten, että yleensä haittaohjelma lukitsee käyttäjän tiedostot ja vaatii sen jälkeen laitteen ruudulla esitetyssä vaatimuksessa rahallista korvausta eli lunnaita (Sanastokeskus TSK ry 2018, 32). Lunnasvaatimus esitetään yleensä jonkinlaisena

kryptovaluuttana, useimmiten bitcoineina. Summa voi vaihdella parista sadasta jopa tuhansiin euroihin (Albrecht 2017). Lunnaiden maksun jälkeen haittaohjelman tekijät lupaavat lähettää salauksenpurkuavaimen, jolla tiedostot saadaan taas käyttöön. Lunnaiden maksaminen rikollisille ei kuitenkaan aina takaa sitä, että salausavain lähetettäisiin ja tiedostot vapautettaisiin, eivätkä viranomaiset missään tilanteissa suosittele rikollisille maksamista. Lunnaiden maksaminen myös tukee ja rahoittaa rikollista toimintaa, ja Keskusrikospoliisin rikosylikomisario Timo Piiroisen mukaan maksamalla lunnaat uhri osoittaakin, että rikollisten toimintatapa on kannattavaa ja toimivaa. (Keskusrikospoliisi 2017a.)

Tyypillinen tapa saada tartunta kiristyshaittaohjelmasta on avata saastunut sähköpostin liitetiedosto tai ladata jokin ohjelma, joka sisältää kyseisen haittaohjelman. Myös epämääräistä linkkiä klikkaamalla voi joutua uhriksi. (Keskusrikospoliisi 2017a.) Ensimmäiset haittaohjelmat nähtiin vuonna 2010, ja tällaiset ohjelmat ovat sen jälkeen kasvaneet räjähdysmäisesti. Vuonna 2016 ilmestyi 193 uutta kiristyshaittaohjelmatyyppiä, ja jokaisesta niistä esiintyi useita muunnelmia. Tämä kiristysmenetelmä on kasvattanut suosiotaan ja menestystään sen vuoksi, että verrattuna muihin verkkohuijauksiin kiristyshaittaohjelman avulla uhri on kerralla ansassa. Tiedostot on jo lukittu ja uhrilla ei ole muuta vaihtoehtoa kuin maksaa tai menettää tiedostonsa, ellei varmuuskopiointia ole suoritettu asianmukaisesti. Lisäksi bitcoinien käyttö lunnaiden maksussa mahdollistaa sen, että pankit eivät voi valvoa tai keskeyttää rahansiirtoja, vaan raha liikkuu suoraan uhrin ja kaappaajan välillä ilman välikäsiä. Bitcoinien käyttäminen on toisaalta myös hankalaa, sillä se ei ole yhtä yksinkertaista kuin verkkopankissa asiointi. Bitcoinit vaativat hieman teknistä osaamista eikä moni ole kuullutkaan kyseisestä valuutasta ennen kuin kiristyshaittaohjelma iskee omalle koneelle. (Albrecht 2017.)

Kiristyshaittaohjelmien torjunnassa avaintekijöitä ovat säännöllinen varmuuskopiointi ja henkilökohtaisen tietoturvan sekä päätelaitteen päivitysten pitäminen ajan tasalla. Jos kiristyshaittaohjelma pääsee iskemään esimerkiksi tietokoneeseen, varmuuskopiot kaikista tiedostoista on tehty säännöllisesti ja tärkeimmät tiedostot on kopioitu myös pilvipalveluun reaaliaikaisesti, kiristyshaittaohjelman vaikutukset jäävät pieniksi. Tällöin koko tietokone voidaan tyhjentää ja asentaa uudelleen, ja tiedostot voidaan palauttaa varmuuskopioista. Varmuuskopioiden ylläpitäminen on kuitenkin ollut jo vuosikausia suositeltavaa kaikille tietokoneiden käyttäjille, mutta siitä huolimatta niistä huolehtiminen jää monelta tekemättä. Yleinen ajatus on, ettei oma kovalevy koskaan hajoa, eikä itse koskaan tule langenneeksi esimerkiksi kiristyshaittaohjelmiin. Sen vuoksi varmuuskopioista palauttaminen ei aina ole mahdollista, vaan haittaohjelmien uhrit ovat joutunut turvautumaan lunnaiden maksuun.

Kiristyshaittaohjelmien muuttuessa vähitellen yleiseksi rikollisuuden muodoksi, eri lainvalvontaviranomaiset ja tietoturvayhtiöt ovat alkaneet taistella yhdessä näitä rikollisia vastaan. Tämän myötä on syntynyt lainvalvontaviranomaisten ja tietoturvayhtiöiden yhteishanke No More Ransom, jonka tarkoituksena on auttaa kiristyksen uhreja saamaan tiedostonsa takaisin ilman lunnaiden maksua. Hankkeen verkkosivuilla myös jaetaan tietoa ja valistetaan käyttäjiä näiden haittaohjelmien toiminnasta ja tartuntojen ennaltaehkäisystä. Sivustolla tarjotaan myös tietoturvayhtiöiden laatimia purkutyökaluja, joiden avulla tiettyjä kiristyshaittaohjelmien asettamia salauksia voidaan purkaa maksamatta lunnaita. Näitä työkaluja on tarjolla jo yli sataan eri haittaohjelmaan, ja määrä kasvaa jatkuvasti, kun uusiin haittaohjelmiin luodaan purkutyökaluja. (No More Ransom 2019.)

2.3 Internetpiratismi vertaisverkoissa ja piratismikirjeet

Erityisesti 2000-luvun alkupuolta väritti internetpiratismi, joka kukoisti erilaisten vertaisverkkojen avulla. Vertaisverkko (englanniksi peer-to-peer tai p2p) on useista tietokoneista muodostunut ”yhteisö”, jonka välillä voidaan esimerkiksi jakaa tiedostoja. Vertaisverkon toiminta ja tehokkuus tiedostonsiirrossa perustuu siihen, että tiedoston lataaja/haltija myös jakaa kyseistä tiedostoa muille vertaisverkko-ohjelman käyttäjille. Vertaisverkko-ohjelmien käyttö itsessään ei ole laitonta, mutta esimerkiksi tekijänoikeudella suojattujen elokuvien, televisiosarjojen ja musiikin laiton jakaminen yleistyi vuosituhannen alussa. (Tekijänoikeuden tiedotus- ja valvontakeskus 2019.) Tätä kutsutaan internetpiratismiksi ja se on rikoslaissa mainittu tekijänoikeusrikoksena, josta on säädetty rangaistukseksi sakkoja tai enintään kaksi vuotta vankeutta.

Tiedostonjakoprotokollia vertaisverkossa on useita, yleisimpinä voidaan mainita BitTorrent ja DirectConnect. BitTorrent-protokollassa tiedoston lataaja (englanniksi leecher) toimii samanaikaisesti jakajana (seeder), jolloin tiedoston osat kulkevat nopeasti käyttäjien välillä. DirectConnect- eli DC-protokollassa taas käyttäjä luo tietokoneelleen erityisen jakokansion, jonka sisältö on nähtävissä ja ladattavissa kaikille samaa vertaisverkko-ohjelmaa käyttäville. DC-protokollaa käyttävät ohjelmat (esimerkiksi DC++) olivat yleisempiä suomalaisten käytössä ennen BitTorrent-ohjelmien yleistymistä. (Tekijänoikeuden tiedotus- ja valvontakeskus 2019.)

Tiedostonjako vertaisverkoissa ei kuitenkaan enää nykyään ole niin yleistä kuin aikaisemmin. Edulliset suoratoistopalvelut, kuten Spotify ja Netflix, ovat muuttaneet audiovisuaalisen median kuluttamisen todella helpoksi ja halvaksi. Moni maksaa mielellään kohtuullista kuukausimaksua siitä, että saa useilla eri laitteilla reaaliaikaisesti pääsyn valtavaan kirjas-

toon, joka myös muuttuu ja päivittyy jatkuvasti. Vertaisverkoista ladattaessa on aina nähtävä erikseen se vaiva, että lataa tiedostot koneelleen. Tämä vie hitaammalla nettiyhteydellä ja isojen tiedostojen kohdalla myös jonkin verran aikaa. On myös aina mahdollista, että tiedoston sisältö ei vastaakaan kuvausta. Suoratoistopalvelut poistavat laittomuusongelman ja niiden avulla voidaan varmistaa, että sisältö on laadukasta ja vastaa sitä, mitä on luvattu.

Piratismikirjeet, joita kutsutaan myös nimillä kiristyskirje tai tekijänoikeuskirje, liittyvät mielenkiintoisella tavalla tekijänoikeuksia rikkovaan laittomaan tiedostojen lataukseen. Piratismikirjeiden lähetys yksityishenkilöille on melko uusi, viime vuosina yleistynyt ja sittemmin jo hieman hiipunut taktiikka. Siinä tekijänoikeuksia hallinnoiva yritys, esim. elokuvayhtiö, vaatii rahaa henkilöltä, joka on oletettavasti ladannut jotain laittomasti. Usein lähettäjänä on ulkomaalainen yritys, joka käyttää suomalaista lakitoimistoa välikätenä lähettäessään kirjeitä. Ulkomaalaisista tekijänoikeusrekistereistä sekä tiedostonjako-ohjelmien lokitiedostoista saadaan IP-osoitteita, joilla pyritään yksilöimään käyttäjä. Tämän jälkeen lakitoimisto esittää nämä IP-osoitteet todisteina markkinaoikeudelle, joka joissain tapauksissa määrää operaattoreita luovuttamaan IP-osoitteisiin liittyvät henkilötiedot. Piratismikirjeissä lakitoimisto kehottaa sopimaan tekijänoikeusrikkomuksen rahallisesti, ennen kuin tekijänoikeuksia hallinnoiva yhtiö vie asian oikeuteen. (Piraattipuolue 2017.)

Piratismikirjeitä on Suomessa lähettänyt muutama lakitoimisto, joista kaksi on jo lopettanut toimintansa. Kolmas yritys on puolestaan lopettanut kirjeiden lähettämisen, kun aluehallintovirasto alkoi tutkia sen toimintaa. (Pehkonen 2019.) Julkisuudessa näiden kirjeiden lähettämisestä on käyty runsasta keskustelua. On pohdittu, onko lakitoimistojen toiminta moraalisesti oikein, sillä todisteina esitetyt aineistot eivät aina pidä paikkaansa. Esimerkiksi avoimia verkkoja voi käyttää kuka vain, eikä tällöin tekijänoikeusrikkomuksesta syytetty välttämättä ole itse syyllistynyt tiedostojen laittomaan jakamiseen. Suomessakin on ollut tapauksia, joissa vastaaja on kyennyt todistamaan syyttömyytensä, mutta prosessit ovat pitkiä ja uuvuttavia yksityishenkilöille, joilla ei välttämättä ole osaamista esittää todisteita syytöksiä vastaan.

2.4 Palvelunestohyökkäykset

Palvelunestohyökkäys on Kyberturvallisuuden sanaston (2018, 31) mukaan tietoturvahyökkäys, jolla pyritään ylikuormittamaan ja lamaannuttamaan jokin palvelu tai tietojärjestelmä. Usein tämäntyyppiset hyökkäykset tehdään useita koneista koostetuista bottiverkoista, sillä yhdestä IP-osoitteesta tuleva jatkuva, kuormittava liikenne on yleensä estetty palomuuriasetuksilla. Tällaista hyökkäystä kutsutaan usein termillä DDos (distributed

denial of service attack, hajautettu palvelunestohyökkäys). Palvelunestohyökkäykset kohdistuvat verkkosivuihin tai usein esimerkiksi viranomaisten tai muun julkishallinnon verkkopalveluihin ja -järjestelmiin. Tällaisella hyökkäyksellä voi olla vakaviakin seurauksia, ja useimmiten ne aiheuttavat kiusallisia ja joskus jopa useita päiviä kestäviä katkoksia palveluihin. Palvelunestohyökkäys ei kuitenkaan itsessään vaaranna tietoturvaa tai saata palveluissa ja palvelimilla sijaitsevia tietoja vääriin käsiin (Kyberturvallisuuskeskus 2016, 3).

Palvelunestohyökkäysten motiivina toimii usein jokin aate tai yleinen erimielisyys sivuston ylläpitäjätahon kanssa, mutta myös pelkästä vihaisuudesta tai näyttämisen halustakin tehtaillaan palvelunestohyökkäyksiä (Kyberturvallisuuskeskus 2016, 3). Tämän vuoksi tämä rikostyyppi onkin usein tyypillinen nuorille aikuisille, jotka haluavat näyttää, että heillä on kuviteltua valtaa. Myös kiristäminen palvelunestohyökkäyksillä on yleistynyt. DDoS-hyökkäysten tekeminen on nykyään halpaa eikä vaadi tekijältä juuri teknistä osaamistakaan. Hyökkäyksiä on käytetty myös hämäyksenä viemään huomiota pois jostain vakavammasta päähyökkäyksestä. Poliittiset motiivit näkyvät myös järjestäytyneempien rikollisten tehtailemissa palvelunestohyökkäyksissä, kun pyritään esimerkiksi estämään äänestäminen vaaleissa. (Kyberturvallisuuskeskus 2016, 3.)

Palvelunestohyökkäyksessä usein käytettyihin bottiverkkoihin voi joutua välikappaleeksi jopa tavallisen yksityishenkilön reititin tai tietokone. Oletussalasanat tai heikot salasanat ovat rikolliselle helppo tapa murtautua laitteelle, asentaa siihen haittaohjelma ja hyödyntää sen kapasiteettia bottiverkon muodostamisessa. Myös päivitysten pitäminen ajan tasalla on tärkeää, jottei laitteessa olevia heikkouksia voida hyödyntää murtautumisessa. (Kyberturvallisuuskeskus 2016, 7–8.)

2.5 Nettipetokset

Nettipetokset kätkevät alleen useita erilaisia rikostyyppejä laajalta alueelta. Terminä nettipetos ei ole rikoslain mukainen, vaan internetissä tapahtuvia petoksia käsitellään petoksina, lievinä petoksina sekä törkeinä petoksina rikoslain 36 luvun mukaan. Internetin anonyymiys ja helppous ovat lisänneet petosten siirtymistä verkkoon, ja esimerkiksi vuosien 2015 ja 2016 välillä poliisin tietoon tulleiden nettipetosten määrä kasvoi yli 2 700 kappaleella (Poliisi 2016).

Tämän kappaleen alaluvuissa käsitellään petoksen määritelmän alle kuuluvia rikoksia: identiteettivarkauksia, tietojenkalastelua, sijoitus- ja toimitusjohtajahuijauksia sekä niin kutsuttuja rakkaushuijauksia. Ihmisten hyväuskoisuutta käytetään helposti hyväksi monenlai-

sissa huijausyrityksissä, joista valitettavan moni myös onnistuu. Näiden torjunnassa ennaltaehkäisevä tiedonjakaminen ja valistus ovat ensisijaisen tärkeässä asemassa. Verkossa tapahtuvat petokset ovat joskus tökeröitä ja niiden havaitseminen on helppoa, mutta vuosien mittaan rikolliset ovat oppineet myös luomaan erittäin aidonnäköisiä huijaussivustoja. He osaavat myös esiintyä taitavasti viranomaisina tai esimerkiksi pankkina, jonka edustajana he vaativat uhrilta tunnuksia verkkopalveluun.

2.5.1 Identiteettivarkaudet

Rikoslain (39/1889) 38 luvun 9a pykälän mukaan identiteettivarkaudesta voidaan tuomita, jos henkilö käyttää luvatta toisen henkilötietoja erehdyttääkseen kolmatta osapuolta. Identiteettivarkaudessa on siis kyse toisena henkilönä esiintymisestä, millä pyritään saamaan esimerkiksi taloudellista hyötyä. Kyseinen rikos on asianomistajarikos, eli poliisi tutkii sitä vain, jos uhri tekee rikosilmoituksen. Lisäksi teon on pitänyt aiheuttaa taloudellista vahinkoa tai muuta vähäistä suurempaa haittaa, esimerkiksi asian selvittelykuluja tai netissä tehtyjen tilausten perumista. Usein identiteettivarkauksia tutkitaan osana petosta, jolloin tekijä voidaan tuomita molemmista. Identiteettivarkaudelle on tyypillistä, että rikoksessa käytetyt henkilötiedot tai esimerkiksi pankkitunnukset saadaan hankittua ensin jollain keinolla, ja niillä hankitaan esimerkiksi tavaroita netistä toisen henkilön laskuun. (Poliisi 2018.)

Toisena ihmisenä esiintyminen esimerkiksi sosiaalisessa mediassa, eli valeprofiilin luominen, voidaan myös tuomita identiteettivarkaudeksi. Tällaisen tilin poistaminen vaatii uhrilta usein aikaa ja vaivaa, mikä täyttää identiteettivarkauden vähäistä suuremman haitan määritelmän. Identiteettivarkaus on lisätty rikoslakiin vasta vuonna 2015, joten oikeuden päätöksiä tästä rikoksesta on vielä vähän. Sen vuoksi esimerkiksi verkkokaupassa toisen ihmisen nimissä tehdyt tilaukset on usein tutkittu sekä petoksina että identiteettivarkauksina, koska petoksessa uhrina on verkkokauppa, mutta identiteettivarkaudessa uhriksi joutuu henkilö, jonka tietoja ostossa on käytetty. (Trejtnar 2019, 38–39). Identiteettivarkaudet voivat olla hyvin kiusallisia ja pitkäänkin haittaa aiheuttavia, jos kyseessä on esimerkiksi laajalle levinnyt valeprofiilien tehtailu tai muuten internetissä esiintyminen toisena ihmisenä. Monelle olisi varmasti epämiellyttävää, jos omissa nimissä jaettaisiin verkossa mielipiteitä sensitiivisissä asioissa tai joku tilaisi verkkokaupoista jatkuvasti tavaraa omilla henkilötiedoilla. Myös rahalliset vaikutukset saattavat olla merkittäviä, jos tilanteessa on saatu haltuun myös pankkitunnukset tai luottokortin tiedot.

2.5.2 Tietojenkalastelu

Tietojenkalastelua eli verkkourkintaa (englanniksi phishing) on esiintynyt maailmanlaajuisesti 1990-luvun puolivälistä asti. Silloin kyseessä oli Yhdysvalloissa tapahtuvaa tunnusten kalastelua väärennetyillä järjestelmänvalvojien käyttäjätunnuksilla. Kalastelijat esiintyivät amerikkalaisen internetoperaattori AOL:n työntekijöinä ja lähettivät käyttäjille sähköpostiviestejä, joissa pyydettiin vahvistamaan laskutustiedot. Monet menivät lankaan ja kertoivat kalastelijoille luottokorttinsa tiedot, jolloin tekijät pystyivät aiheuttamaan suuriakin taloudellisia vahinkoja. (Knowbe4 2019.) Tietojenkalastelu on psykologiasta voimansa ammentava rikos, jossa vedotaan ihmisten luottamukseen ja haluun tehdä yhteistyötä virallisen tahon kanssa. Mitään varsinaisia haittaohjelmia ei asenneta käyttäjien koneelle, kaikki tapahtuu vapaaehtoisuuden varassa henkilön syöttäessä tietonsa esimerkiksi kalastelijoiden muokkaamille sivustoille.

Tekotavat eivät tähän päivään mennessä ole muuttuneet kovinkaan radikaalisti, vaan kehitystä on lähinnä tapahtunut hienovaraisuudessa, laadussa ja uskottavuudessa. Tietojenkalasteluun liittyy edelleen usein sähköpostitse tai tekstiviestitse lähetetty urkintaviesti, jossa esiinnytään jonain auktoriteettina tai organisaation edustajana, esimerkiksi poliisina tai internetoperaattorin työntekijänä. Monet viranomaiset ja yritykset joutuvat jatkuvasti muistuttamaan asiakkaitaan henkilökohtaisesti tai esimerkiksi sosiaalisessa mediassa, että he eivät koskaan kysy asiakkaansa pankkitunnuksia tai käyttäjätunnuksia palveluihin.

Tietojenkalastelu alkaa yleensä rikollisen osalta phishing kitin hankkimisella. Tällainen äärimmäisen halpa aputyökalu sisältää usein tuhansia tai kymmeniä tuhansia sähköpostiosoitteita, verkkosivun luomistyökalun sekä mahdollisesti jopa viestipohjat kalasteluviestille. Työkalu asennetaan ensin hakkeroidulle palvelimelle. Käyttäjän syöttäessä hakkeroituun palveluun tunnuksensa ja salasanansa, phishing kit tarkistaa tietojen oikeellisuuden syöttämällä ne kohdepalveluun ja lähettää toimivat tunnukset hyökkääjälle. (Kirves 2007; Ragan 2018.)

Rikolliset osaavat naamioida vilpilliset yrityksensä taidokkaasti, mutta lähes aina on löydettävissä jokin pieni yksityiskohta, josta erottaa aidon ja väärennöksen. Suosittu esimerkki on sähköposti, joka sisältää linkin väärennettyyn kirjautumissivustoon. Itse viestin sisältö saattaa olla äidinkielenään suomea puhuvalle helppo havaita väärennökseksi, sillä kielioppi- tai kirjoitusvirheitä esiintyy usein liikaa. Viestin linkkiä klikkaamalla käyttäjä päätyy joskus tekaistulle verkkosivustolle, joka sekin näyttää tökeröltä tai jotkin sanavalinnat tuntuvat erikoisilta. Kriittisyyttä tulisi aina käyttää, vaikka viestin lähettäjänä olisikin tutun

näköinen osoite tai henkilö, sillä sähköpostiosoitteiden lähettäjäkenttiä pystytään väärentämään. Vastaanottajan tulee jättää viesti huomioimatta, jos se herättää epäilyksiä. Jos epämääräisiä sähköpostiviestejä näkyy usein työpaikalla, siitä on hyvä tiedottaa myös IT-osastoa, joka osaa tehdä tarvittavat toimenpiteet esimerkiksi roskapostisuodatuksen parantamisen ja tiedotuksen osalta.

2.5.3 Toimitusjohtaja- ja sijoitushuijaukset

Vuoden 2019 aikana niin kutsutut toimitusjohtajahuijaukset yleistyivät Suomessa. Toimitusjohtajahuijauksessa rikollinen tekeytyy kohdeorganisaation johtavassa asemassa olevaksi henkilöksi, esimerkiksi toimitusjohtajaksi. Hän pyytää sähköpostitse alaistaan maksamaan laskun, joka ei kuitenkaan ole aito vaan rikollisten tekaisema. Väärennetyn laskun ja identiteetin turvin pyritään uskottelemaan uhrille, että maksu tulee todellakin suorittaa. Laskun maksaja ei välttämättä varmista asiaa esimerkiksi puhelimitse, vaan luottaa esihenkilöön ja maksaa väärennetyn laskun, jolloin rahat siirtyvät rikollisten tilille. Elokuun 2019 loppuun mennessä tällaisista petoksista oli tehty jo 196 rikosilmoitusta, kun koko vuoden 2018 aikana ilmoituksia tehtiin 170 ja vuonna 2017 sata kappaletta. (Poliisihallitus 2019.) Tämä kertoo melkoisesta kasvupyrähdyksestä kahden vuoden aikana. Toimitusjohtajapetokset kohdistuvat niin yrityksiin kuin yhdistyksiinkin, ja niillä saattaa olla tuhoisia vaikutuksia esimerkiksi pienempien yhdistysten talouteen.

Sijoitushuijaukset kohdistuvat yksityishenkilöihin, ja usein viimeaikaisissa huijauksissa on kehotettu sijoittamaan olemattomiin virtuaalivaluuttoihin. Huijauksen kohde on saanut puhelun ulkomaisesta numerosta, jonka aikana soittaja on kysellyt uhrin varallisuudesta ja sijoitustottumuksista. Sen jälkeen uhrille on esitetty sijoitusmahdollisuus ulkomaisessa yhtiössä suurella tuotto-odotuksella ja häntä on pyydetty siirtämään pääoma ulkomaiselle pankkitilille tai virtuaalivaluutan vaihtopalveluun. Usein huijari on soittanut lähipäivinä uudelleen ja pyytänyt sijoittamaan lisää tai maksamaan joitakin lisämaksuja. Joissakin tapauksissa uhria on myös pyydetty asentamaan tietokoneelleen etäkäyttöohjelma, jonka avulla hänen rahaliikennettään on pystytty tarkkailemaan ja uhrin puolesta on tehty jopa maksuja. (Keskusrikospoliisi 2019.) Tällainen etäkäytön salliminen mahdollistaa koko tietokoneen kontrolloinnin ja voi aiheuttaa suuriakin haittoja sekä taloudellisesti että henkilökohtaisesti.

2.5.4 Rakkaushuijaukset

Rakkaushuijaukset ovat mahdollisesti eniten häpeää aiheuttavia rikoksia, kun tarkastellaan yksityishenkilöihin kohdistuvaa verkkorikollisuutta. Rakkaushuijaukset ovat yleensä pidemmällä aikajaksolla tapahtuvia verkkorikoksia, joissa kohdehenkilö yritetään saada

tuntemaan myötätuntoa, empatiaa ja jopa rakkautta huijaria kohtaan. Uhreihin otetaan yhteyttä usein sosiaalisessa mediassa, jossa on helppo tekeytyä toiseksi henkilöksi. Huijarit käyttävät psykologiaa taitavasti hyväkseen ja onnistuvat luomaan esimerkiksi tekaistujen kuvien avulla illuusion, jossa he ovat luotettavia ihmisiä vakaassa sekä arvostetussa työsuhteessa, eikä rahasta varsinaisesti ole puutetta (Rikosuhripäivystys 2019a). Suhteen syvennyttyä uhrille aletaan kertoa tarinoita sairaasta perheenjäsenestä tai matkustuskulujen kattamisesta kohteen luokse. Tarinoita keksitään usein lisää uhrin langettua ensimmäiseen, ja huijari esittää, että maksetut summat eivät olekaan riittäviä sairaalakulujen tai lentolippujen maksamiseksi tai jokin viranomainen pyytää käsittelymaksuja rahansiirrosta. Huijauksen paljastuttua uhri voi kokea häpeää ja epäonnistumisen tunnetta, sillä monesti tämäntyyppisissä petoksissa keskustelut ovat hyvinkin henkilökohtaisia. Uhrille tulee tunne siitä, että heidän välilleen on todella syntynyt syvä suhde, vaikka toista ei olisi vielä tavannutkaan.

Rakkauspetoksien takana on sekä yksityishenkilöitä että kansainvälisiä, ammattimaisia rikollisliigoja (Liukkonen 2018, 30). Suomessakaan ei ole vältytty tällaisilta huijauksilta, ja pankit ovat tiedottaneet asiakkaitaan olemaan varovaisia ja kriittisiä tuntemattomien henkilöiden rahanpyyntöjen suhteen. Pankit myös tarkkailevat asiakkaidensa poikkeuksellisia rahansiirtoja ja voivat olla yhteydessä asiakkaaseen, jos he havaitsevat jotain epäilyttävää. Rakkauspetokset ovat hyvin psykologisia rikoksia ja niiden ennaltaehkäisyssä laaja tiedottaminen on äärimmäisen tärkeässä asemassa. Myös pankkien toiminta rahansiirtojen keskeyttämiseksi on kriittistä. Rikosuhripäivystys, poliisi ja pankit tekevät yhteistyötä näiden rikosten estämiseksi varhaisessa vaiheessa, sillä vaikka vastuu omasta rahankäytöstä ja kriittisesti käyttäytymisestä verkossa on aina henkilöllä itsellään, järkisyitä on näissä rakastumisen kemiaa hyväksi käyttävissä rikoksissa hankala löytää. Suomalaisille ominaista luottamusta käytetään tämäntyyppisissä rikoksissa herkästi hyväksi usein taloudellisesti kohtalokkaalla tavalla, sillä Nordean petosten torjuntayksikön mukaan uhri menettää rakkauspetoksissa keskimäärin 10 000–15 000 euroa (Liukkonen 2018, 30).

2.6 Tor-verkko

Tor-verkko on näkökulmasta ja käyttäjän omista intresseistä riippuen joko kyseenalainen tai käytännöllinen verkko, joka toimii ikään kuin tavallisen internetin pimeällä puolella. Näitä darkwebiä eli ”pimeää verkkoa” selaavia ohjelmistoja on muitakin, mutta tor lienee niistä kaikista suosituin. Tässä opinnäytetyössä tor-verkolla tarkoitetaan yksinkertaisuuden vuoksi pimeän verkon sisältöä ja sen selaamista tor-ohjelmistolla. Tor-verkon perimmäinen tarkoitus on tarjota käyttäjilleen anonyymiyttä sekä palveluita, joita julkisessa inter-

netissä ei välttämättä ole saatavilla. Tor-verkon puolestapuhujat painottavat sananvapauden ja näkymättömyyden etuja, ja tor ei missään nimessä ole synonyymi rikollisuuden pelikentälle eikä sen käyttäminen ole rikos. Tor-verkon anonymiteetti kuitenkin takaa myös rikollisille ja esimerkiksi huumeiden ostajille helpohkon tavan toimia niin, että oma henkilöllisyys tai sijainti ei selviä muille käyttäjille. Tämä aiheuttaa osaltaan Tor-verkon kyseenalaisen maineen. Toinen syy tor-verkon käyttämiselle on henkilön sijainti sellaisessa valtiossa, jossa hallinto rajoittaa internetin käyttöä tai sananvapautta. Tällöin tiedonhaku tai omien mielipiteiden jakaminen internetissä halutaan piilottaa, sillä niiden julkituomisella on joissain maissa vakaviakin seurauksia. Jotkut myös haluavat vastustaa esimerkiksi Googlen ja Facebookin kautta tapahtuvaa seurantaa, jota tor-verkossa ei tapahdu lainkaan. (Krogerus 2019.)

Tor-verkossa esiintyvä rikollisuus on kuitenkin jokseenkin yleistä, ja poliisi on sulkenut sieltä esimerkiksi suositun Sipulikanava-sivuston, jossa käytiin muun muassa huumekauppaa kaupungeittain järjestellyissä keskusteluketjuissa (Laakso 2017). Vuonna 2018 Keskusrikospoliisi (2018b) kertoi myös Subutex-tablettien kauppaamisesta tor-verkon kautta. Tämän rikoksen yhteydessä löytyi lisäksi räjähteitä sekä vaarallisia ampuma-aseita, ja kahta tekijää epäiltiin myös törkeistä petoksista, jotka olivat tapahtuneet internetissä. Tor-verkossa on myös julkaistu useita uhkauksia esimerkiksi kouluampumisista tai kauppakeskuksia kohtaan. 1.5.2019 espoolaiseen kauppakeskus Isoon Omenaan kohdistui uhkaus, josta Länsi-Uudenmaan poliisi kertoi Twitter-tilillään. Asiaa kerrottiin tutkittavan laittomana uhkauksena. (Poliisi 2019.) Poliisi tiedottaa tällaisista uhkauksista sosiaalisessa mediassa kohtuullisen usein, mistä voi päätellä, että uhkauksia tosiaan tehdään esimerkiksi tor-verkossa jonkin verran. Kaikkia uhkauksia ei välttämättä edes kerrota julkisuuteen. Isoon Omenaan kohdistuva uhkaus oli poikinut paljon vinkkejä yleisöltä, joten tor-verkossa myös tartutaan näihin uhkauksiin ja niistä ilmoitetaan herkästi poliisille.

Tor-verkkoon suhtautuminen vaihtelee huomattavasti eri ihmisten välillä. Suurimmalle osalle suomalaisista tor-verkko on täysin tuntematon käsite, mutta joillekin termi voi olla tuttu viime vuosina yleistyneen uutisoinnin vuoksi. Tor-verkosta kirjoitetut uutiset ja artikkelit kertovat käytännössä aina huume- tai asekaupoista, lapsen seksuaaliseen hyväksikäyttöön liittyvän materiaalin levittämisestä tai laittomista uhkauksista. Viranomaisnäkökulmasta tor-verkko on haastava osa internetiä, sillä sen kontrollointi on todella paljon hankalampaa kuin julkisen internetin. Viranomaisten suorittama jäljittäminen on mutkikkaampaa kuin yleisesti internetissä, mutta se on kuitenkin mahdollista (Leponen 8.10.2019).

Tor-verkko on monille sen käyttäjille muuta kuin rikosten suunnittelua ja toteutusta. Internetissä yksilön yksityisyyden rajat ovat hämärtyneet sosiaalisen median yritysten ja esimerkiksi Googlen myötä. Näillä yrityksillä on runsaasti keinoja seurata tavallista käyttäjää internetissä muun muassa Facebook-liitännäisten ja Google-hakujen myötä. Ihmisten internetkäyttäytymisen tunnistaminen, seuranta ja analysointi tuo lähes rajattomasti ansaintamahdollisuuksia esimerkiksi kohdennetun mainonnan ja tietojen myynnin avulla. Moni verkon käyttäjä ei tiedosta, että jokainen Google-haku ja Facebookiin tallennettu kontakti, julkaisu tai tykkäys tallentuu monimutkaiseksi yhdistelmäksi käyttäjän tietoja. Näitä tietoja yritykset käyttävät algoritmien avulla hyödykseen kohdentaakseen mainontaa paremmin jokaiselle sopivaksi, jotta klikkaukset ja niiden myötä mainostulot kasvaisivat.

Tor-verkko tarjoaa kanavan, jossa käyttäjää ei seurata eikä Google-hakuja tallenneta. Tor-verkon käyttäjä Patric Puola (3.11.2019) kertoo sähköpostihaastattelussa, että hänelle suurimmat syyt käyttää tor-verkkoa ovat nimenomaan yksityisyydensuojan säilyttäminen ja seurannasta aiheutuvat ongelmat. Hyvänä esimerkkinä hän kertoo lentolippujen hintojen nousun. Kun käyttäjä selaa julkisessa internetissä lentolippuja eri sivustoilta, hinnat nousevat sitä mukaa, kuinka usein hän vierailee kyseisellä sivustolla. Verkkosivut käyttävät tämän seurantaan usein evästeitä (englanniksi cookies), joiden poistaminen selaimen historiasta voi joskus auttaa välttämään muutokset lippujen hinnoissa. Jotkut sivustot voivat kuitenkin seurata käyttäjän IP-osoitetta, joka ei välttämättä muutu juuri koskaan. Tällöin lippujen hintojen nousuun ei voi vaikuttaa millään tavalla, vaan käyttäjä on täysin sivustojen seurannan armoilla.

Puola on ylläpitänyt omaa tor-palvelinta vuodesta 2014 asti. Toisena tor-verkon käytön syynä hän mainitsee sosiaalisesti tai yksityisyyden kannalta arkaluonteisten internethakujen tekemisen. Kuten mainittu, Google kerää kaikki haut itselleen ja analysoi niitä kehittääkseen algoritmejaan paremmiksi, mutta myös saadakseen mahdollisimman paljon tietoa käyttäjistä, sillä internetissä tieto on rahaa. Puola mainitsee myös alueellisesti rajattujen sivustojen ja ulkomaisten suoratoistopalvelujen käytön syyksi tor-verkon hyödyntämiselle. VPN-palvelut eli internetyhteyden tunnelointisovellukset ovat toinen ratkaisu maantieteellisten rajoituksien kiertämiseksi, mutta ne ovat käytännössä aina maksullisia ja käyttäjä ei voi olla varma siitä, ylläpitääkö VPN-palveluja tarjoava yritys lokitiedostoja käyttäjien internetin selailusta. (Puola 3.11.2019.)

Yksityisyyteen ja seurantaan liittyvien syiden lisäksi Puola (3.11.2019) kertoo sananvapauden olevan yksi tärkeä kriteeri sille, miksi hän pitää tor-verkkoa tärkeänä. Hänen mukaansa tor-verkko tarjoaa edes yhden paikan, jossa käyttäjän liikkeitä ei jatkuvasti seu-

rata. Puola on myös IT-arkkitehdin työnsä puolesta kiinnostunut tor-verkon teknisestä toiminnasta ja mainitsee, että on kiinnostavaa ylläpitää omaa tor-palvelinta osana suurta maailmanlaajuista verkostoa. Hänen mukaansa tor-verkon ja kyberrikollisuuden välille on mediassa vedetty yhteys liiankin kevyin perustein. Tähän on syynä se, että nykyään internetin käyttäjien klikkauksia kalastellaan mahdollisimman kiinnostavilla otsikoilla, joita tor-verkon rikollisuus tarjoaa. Hän myöntää, että tor-verkossa tapahtuu rikoksia ja se mahdollistaa myös laittomia sekä moraalittomia tekoja. Puola kuitenkin pitää tällaisia tapahtumia osana yhteiskuntaa, sillä myös ennen tor-verkon olemassaoloa on tehty rikoksia. Puolan mielestä yleinen negatiivinen mielipide tor-verkosta ei ole ratkaisu, vaan yhteiskunnan tulisi kiinnittää huomiota rikollisuuden, huumeiden ongelmakäytön ja väkivaltaisen käyttäytymisen ennaltaehkäisyyn ja tunnistamiseen.

2.7 Kryptoraha ja sen lieveilmiöt

Kryptoraha eli kryptovaluutat ovat uudenlainen verkossa maksamisen muoto, jossa valuutta on olemassa ainoastaan digitaalisena. Kryptovaluuttoihin liittyy useita digitaalisia turvatoimia sekä mahdollisuus louhia valuuttaa itselleen tietokoneiden laskentakapasiteettia käyttäen. Bitcoinia pidetään laajalti ensimmäisenä kryptovaluuttana, ja se on edelleen suosituin ja arvokkain virtuaaliraha maailmassa (Reiff 2019). Muita kryptovaluuttoja ovat esimerkiksi ethereum, litecoin ja dogecoin (Reynard 2018). Tässä opinnäytetyössä keskitytään lähinnä bitcoiniin sen suosion vuoksi, mutta myös joitakin muita virtuaalivaluuttoja koskevia rikoksia sivutaan. On myös erittäin tärkeää huomata, että virtuaalivaluutat itsessään eivät ole millään tavalla rikollisia tai laittomia, mutta niitä käytetään usein anonyymiyden vuoksi rahansiirtoihin rikosten yhteydessä.

Keskusrikospoliisi kartoitti kahden hankkeen myötä vuosina 2016–2018 poliisin tietojärjestelmiin kirjattuja rikoksia, joihin liittyi kryptovaluuttoja. Hankkeissa tutkittiin myös virtuaalivaluuttojen käyttöä rahanpesun ja terrorismin rahoituksessa sekä niiden torjuntamahdollisuuksia. Ensimmäisen kerran kryptovaluuttoihin liittyviä rikoksia kirjattiin vuonna 2011, jolloin niitä oli vain 13 kappaletta. Vuonna 2016 kryptovaluuttoihin liittyviä rikoksia kirjattiin 650 kappaletta, ja seuraavana vuonna määrä oli jo 1005. Vuosien 2016 ja 2017 välillä kasvua oli siis 53 prosenttia, mikä oli siihen mennessä suurin kasvuprosentti näiden rikosten osalta. (Keskusrikospoliisi 2018c.) Tutkivasta viranomaisesta riippuen kryptovaluutat liittyvät erityyppisiin rikoksiin. Tullissa kirjatuista rikoksista 86 prosenttia liittyi huumausaineisiin, kun taas poliisin kirjaamista kryptovaluuttarikoksista 36 % oli petosrikoksia ja 22 % huumausainerikoksia (Keskusrikospoliisi 2017b).

Kuten fyysiseen rahaan, kryptovaluuttoihinkin liittyy useita turvallisuustekijöitä, joista keskeinen on lohkoketju (blockchain). Bitcoin-tilit, rahansiirrot ja siirtojen historia ovat julkista tietoa, mutta mitään näistä ei voida yksilöidä tiettyyn henkilöön. Bitcoin-tilit eivät ole sidoksissa henkilötietoihin, vaan lohkoketjuun on kirjattu kaikki tapahtumat ikään kuin kirjanpidoksi. Lohkoketjuista muodostunut tietokanta on hajautettu ympäri maailman, ja sen tietueita on lähes mahdotonta väärentää, sillä se vaatisi enemmän laskentatehoa kuin kaikilla bitcoinin käyttäjillä on yhteensä. Bitcoin ei ole Suomessa virallista rahaa, mutta sillä voi maksaa ostoksia lukemattomissa kansainvälisissä verkkokaupoissa. Syyskuussa 2019 yli 60 suomalaista kivijalkayritystä hyväksyi bitcoinin maksuvälineenä. (Bittiraha 2019; Keronen 2018; Jäntti 2019.)

Erilaiset kryptovaluutat ovat aiheuttaneet rikollisen maksuliikenteen lisäksi myös erinäisiä sijoitushuijauksia. Viime vuosina Suomessakin kyseenalaista kiinnostusta ja sijoitusinnokkuutta aiheuttanut OneCoin-kryptoraha on FBI:n mukaan pelkkä pyramidihuijaus, eikä valuuttaa oikeasti ole olemassa. Kyseisen rahan nimissä on myyty koulutuksia, joiden myötä ostajat ovat saaneet optioita olemattomaan OneCoin-kryptovaluuttaan, eli varsinaista valuutan ostoa yhtiö ei ole tarjonnut. Keskusrikospoliisi tutki vuonna 2015 OneCoinin laillisuutta mutta ei kyennyt selvittämään yhtiön lainmukaisuutta eikä käynnistänyt asiasta esitutkintaa. Keskusrikospoliisi ilmoitti voivansa määritellä laillisuuden vasta sillä hetkellä, kun OneCoinin arvo julkaistaisiin, mitä ei vieläkään ole tehty. (Halminen 2019; Keskusrikospoliisi 2015.) Tällaiset sijoitus- ja pyramidihuijaukset, jotka lupaavat helppoa rahaa ja runsaita tuottoja nopeasti, on paketoitu usein taidokkaasti ja houkuttelevasti. Verkkosivut ovat ammattimaisen oloiset ja koulutuksissa sekä myyntitilaisuuksissa puhujat ovat taitavia ja saavat kuulijat tuntemaan olevansa osa jotain suurempaa. Huijarit käyttävät psykologiaa taitavasti hyväkseen saadakseen ihmiset uskomaan myyntipuheisiin ja osallistumaan näihin olemattomiin yrityksiin.

2.8 Verkkoviha ja nettikiusaaminen

Verkossa tapahtuva vihanlietsonta ja vihapuhe sekä nettikiusaaminen eivät sellaisenaan ole rikoslain mukaisia rikoksia, vaan niiden kohdalla voidaan käyttää erilaisia rikosnimikkeitä tilanteesta riippuen. Joissakin tapauksissa voi kyseessä olla myös useamman rikosnimikkeen täyttyminen yhdellä kertaa. Verkossa tapahtuvan kiusaamisen, häirinnän ja ahdistelun rikosnimikkeinä voi olla esimerkiksi kunnianloukkaus, yksityisten tietojen levittäminen, vainoaminen tai laiton uhkaus. (Hokkanen 2017a.) Vihapuhe on myös poliisin käyttämä kattotermi erilaisille rikoksille, joihin sisältyvät muun muassa kiihottaminen kansanryhmää vastaan ja uskonrauhan rikkominen. Jos rikoksen lähtökohtana on esimerkiksi

kohteen rotu, ihonväri, uskonto tai seksuaalinen suuntautuminen, rikosta voidaan käsitellä myös kunnianloukkauksena tai laittomana uhkauksena. (Hokkanen 2017b.)

Internetissä tapahtuva kiusaaminen koskettaa useimmiten nuoria, ja sillä on hyvin paljon eri muotoja. Tekijät käyttävät myös erilaisia alustoja, kuten nuorten suosimia sosiaalisen median palveluita (esimerkiksi Instagram tai TikTok) tai pikaviestisovelluksia kuten WhatsAppia. Niin julkinen kuin yksityinenkin kiusaaminen on verkossa mahdollista, ja sen jälkiä voi olla hyvin vaikea saada pysyvästi poistettua (Nuortennetti 2019). Nettikiusaamista on esimerkiksi pilkkaviestien lähettäminen, toisen henkilön valokuvien muokkaaminen tai jakaminen luvatta sekä toisen nimellä tai nimimerkillä esiintyminen (Rikosuhripäivystys 2019b).

Verkkovihan levittäjinä tavataan taas enemmän aikuisia tai nuoria aikuisia. Todennäköisimmin tekijä on mies ja tavallista impulsiivisempi, iäkkäistä ihmisistä vihanlietsojia ei juuri löydy (Kaakinen 2018, 61-62). Sosiaaliset suhteet ja niiden vahvuudet fyysisessä maailmassa sekä verkossa vaikuttavat verkkovihan tekijäksi, mutta myös uhriksi päätymisen todennäköisyyteen. Henkilön vahvat sosiaaliset suhteet verkossa, mutta heikot suhteet verkon ulkopuolella korreloivat kasvaneeseen todennäköisyyteen joutua nettivihan uhriksi tai päätyä itse tekijäksi. Käänteisesti nämä seikat puolestaan pienentävät todennäköisyyttä, eli vahva sosiaalinen elämä verkon ulkopuolella auttaa integroitumaan yhteiskuntaan ja välttämään verkkovihaa. (Kaakinen 2018, 64.)

2.9 Lasten seksuaalinen hyväksikäyttö verkossa

Internet mahdollistaa samankaltaisten henkilöiden kanssa verkostoitumisen ympäri maailmaa ja usein ilman minkäänlaisia henkilötietoja. Tämän varjopuolena on mahdollisuus jakaa helposti myös erityisen järkyttävää materiaalia, kuten lasten seksuaaliseen hyväksikäyttöön liittyvää dataa. Lasten seksuaalisuutta loukkaavaa materiaalia kutsutaan CAM-materiaaliksi (engl. child abuse material), ja hyväksikäyttö voi ilmetä siinä eri tavoilla. Keskusrikospoliisin internettiedustelu tekee tiedonhankintaa aiheesta sekä seuraa siihen liittyviä tapauksia. Rikosylikomisario Sari Sarani kertoo Sonja Tanttarin artikkelissa, että yhdysvaltalaisen NCMEC:n kautta Keskusrikospoliisi saa tietoonsa yli tuhat CAM-tapausta vuodessa. Suomessa näitä rikoksia tutkivat sekä paikallispoliisilaitokset että Keskusrikospoliisi. KRP:ssä tutkitaan joitain vakavimpia ja laajimpia juttuja, joissa voi olla myös kytköksiä ulkomaille. (Tanttari 2018.)

Tor-verkko vaikeuttaa lasten seksuaalisten hyväksikäyttöjen tutkintaa, sillä siellä tekijät pysyvät anonyymeina, ja samanhenkiset ihmiset voivat melko vapaasti jakaa laitonta materiaalia ja pitää yllä keskustelua. Tor-verkossa viranomaisten on vaikeampaa jäljittää tekijöitä. Sari Saranin mukaan tällaiset henkilöt jäävät usein kiinni poliisille vasta silloin, kun hyväksikäyttöä on tapahtunut jo pidemmän aikaa. Erilaisia hyväksikäytön muotoja on useita, tekijä voi esimerkiksi vakuutella lapsen lähettämään seksuaalissävytteisiä kuvia tai videoita, ja sen jälkeen kiristää uhria. Viime aikoina CAM-materiaalin levittämisen lisäksi tekotavaksi on ilmestynyt streaming, jossa uhri ja tekijä ovat videoyhteydessä reaaliaikaisesti. Tällöin tekijä voi kontrolloida tilannetta eikä videosta välttämättä jää tallennetta mihinkään. (Tanttari 2018).

2.10 Psykologia kyberrikollisten apuna

Osa kyberrikoksista toteutetaan teknisin apuvälinein eli tietokoneita ja -verkkoja hyväksikäyttäen. Esimerkkejä puhtaasti teknisesti toteutetuista verkkorikoksista ovat tietoverkkoihin murtautuminen ja tor-verkossa tapahtuvat huumausaine- ja ampuma-aserikokset. Merkittävä osa rikoksista vaatii kuitenkin kontaktia ihmiseen, ja myös kyberrikollisuudessa tekijät pyrkivät hyödyntämään psykologisia menetelmiä edukseen, jotta rikosten onnistumisprosentti sekä tuotto-odotukset olisivat mahdollisimman korkeita. Psykologiaa ja ihmiskontakteja hyödyntävät rikokset voidaan jakaa vielä kahteen kategoriaan: niihin, joissa hyödynnetään esim. haittaohjelmia ja niihin, joissa lähestytään suoraan uhria ilman mitään apuvälinesovelluksia.

Kyberrikollisilla on käytössään useita erilaisia psykologisia työkaluja, joiden avulla he pyrkivät saavuttamaan haluamansa lopputuloksen – eli rikoksen onnistumisen. Usein esimerkiksi illuusiota kiireestä käytetään houkuttelemaan uhri lankeamaan hyvään tarjoukseen tai uhkaillaan rangaistuksella, jos kohdehenkilö ei toimi nopeasti. Uhrin ainutlaatuisuuden korostaminen on myös yleistä, jotta hän tuntisi olonsa erityiseksi. Empaattisuuden hyväksikäyttö on tuttua kyberrikollisille, sillä ihmiset ovat valmiita auttamaan tuntemattomiakin varsinkin sen jälkeen, kun tekijä on esimerkiksi luonut kuvitelman aidosta tunnesiteestä tai suhteesta, jollaista tapahtuu erityisesti rakkaushuijauksissa. Häpeän tunteen istuttaminen uhriin on tehokas keino varmistaa, että hän ei puhu asiasta muille tai hae apua viranomaisilta. Rikolliset voivat syyttää kohdettaan esimerkiksi lapsipornon hallussapidosta. Uhri voi jopa maksaa mahdollisesti vaaditut lunnaat rangaistuksen pelossa, vaikka tietäisi olevansa syytön esitettyyn rikokseen. (Albrecht 2018).

Ihminen on usein hyväuskoinen ja altis luottamaan auktoriteetteihin, minkä phishing-viestien yleistyminen ja usein myös onnistuminen osoittaa. Tähän heikkoon kohtaan panostaminen on yrityksille kriittisen tärkeää tämän päivän onnistuneessa tietoturvapolitiikan toteuttamisessa. Koneet ja verkot voidaan aina yrittää suojata parhaiden ja uusimpien mahdollisten teknologioiden mukaisesti, mutta ihmisiä on vaikeampi totuttaa uusiin tapoihin toimia. Valistaminen, koulutukset sekä tietojen tarkistus ja päivittäminen säännöllisesti ovat yksi tietoturvan kulmakiviä. Asiasta tulee tehdä helposti ymmärrettävää ja IT-osastojen tulee tukea käytännön toteutusta esimerkiksi tiedottamalla, että pienimmästäkin epäilyksestä voi ja tulee ilmoittaa tietoturvasta vastaavalle taholle organisaatiossa. Yksityishenkilöiden tapauksessa jokainen on tietysti myös vastuussa omasta toiminnastaan verkossa. Helposti lähestyttävää ja modernisti tarjolla olevaa tietoa tarjoavat esimerkiksi viranomaisten ja järjestöjen uudet kampanjat, kuten Kuluttajaliiton ylläpitämä Huijausinfo-sivusto Facebookissa.

3 Suomessa esiintyvän kyberrikollisuuden eri puolet

3.1 Turvallisuus ja rikosten ratkaiseminen Suomessa

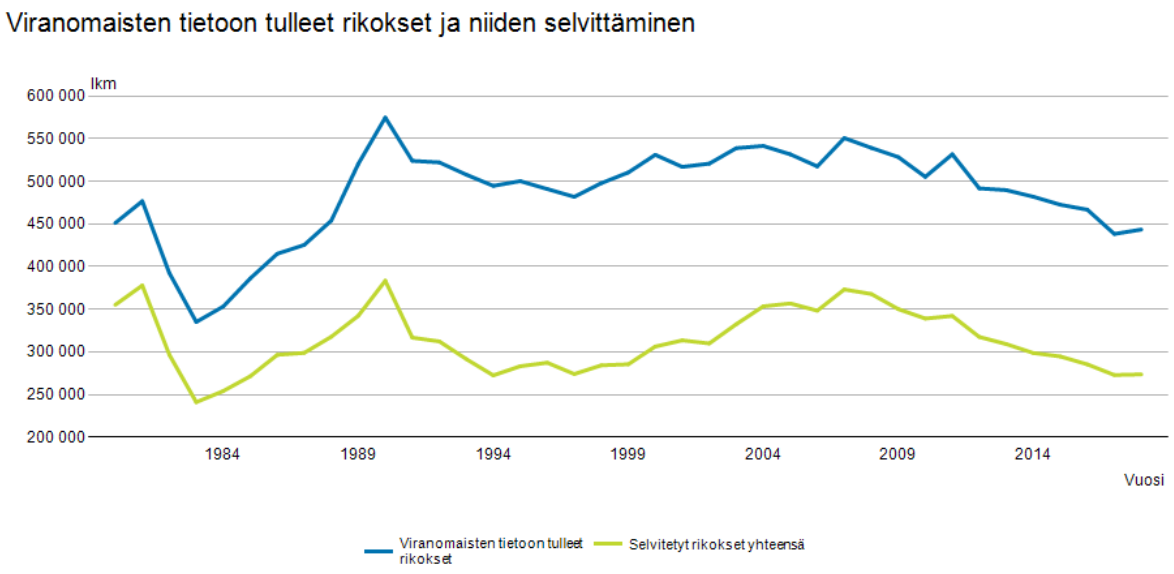
Suomi on monesta näkökulmasta erittäin turvallinen maa. Isoissa kaupunkikeskuksissakin ihmiset kokevat olevansa turvassa yllättäviltä rikoksilta, ja toisiin kansalaisiin luotetaan – joskus jopa liian sokeasti. Ulkomaailman turvallisuudentunne saattaa siirtyä sellaisenaan internetiin, mikä voi altistaa rikoksen uhriksi joutumiselle. Suomi ei ole välttynyt kyberrikollisuuden arkipäiväistymiseltä, sillä esimerkiksi tietojenkalastelua ja toimitusjohtajapetoksia yritetään toteuttaa jatkuvasti. Niin yritysten kuin yksityishenkilöidenkin tulisi suhtautua harkiten kaikkeen internetissä liikkuvaan tietoon. Vähitellen varovaisuudesta tulee rutiinia ja mahdollinen ahdistus tai epäluuloisuus vähenee samassa suhteessa. Tällöin esimerkiksi yleiset ja usein tökeröt kalasteluyritykset eivät enää häiritse internetin käyttöä.

Suomalaisten luottamus poliisiin on aina ollut korkea. Suomalaiset ovat tottuneet siihen, että viranomaisten korruptiota ei juuri ole ja auktoriteettitahoihin voi luottaa kaikessa yhteiskuntaan liittyvissä asioissa. Elinkeinoelämän valtuuskunta EVA on tehnyt vuonna 2018 arvo- ja asennetutkimuksen, jonka osana tutkittiin suomalaisten luottamusta muun muassa erilaisiin viranomaisiin, yrityksiin, mediataloihin, pankkeihin sekä poliittisiin puolueisiin. Kaikista kyselyssä mainituista tahoista poliisiin luotettiin eniten. Vastaajista 86 prosenttia koki melko suurta ja hyvin suurta luottamusta poliisiin. Edellisen kerran asiaa oli tutkittu vuonna 2009, jonka jälkeen luottamus poliisiin on noussut hieman. Poliisiin luotettiin enemmän kuin esimerkiksi oikeuslaitokseen, johon luotti yhteensä 75 prosenttia vastanneista. (Elinkeinoelämän valtuuskunta 2019.)

Korkeasta turvallisuudesta ja luottamuksesta viranomaisiin huolimatta suomalaisilla on myös huolenaiheita, niin perinteiseen turvallisuuteen kuin kyberturvallisuuteenkin liittyen. Euroopan komission vuonna 2017 tekemän tutkimuksen mukaan 47 prosenttia suomalaisista pelkää, että joku käyttää heidän henkilötietojaan väärin esimerkiksi verkkopankkien tai verkkokauppojen palveluita hyödynnettäessä. Verkkomaksut itsessään aiheuttavat huolta 44 prosentissa vastaajista. Tutkimuksen mukaan yhteensä 94 prosenttia suomalaisista on täysin tai lähes sitä mieltä, että riski joutua kyberrikollisuuden uhriksi on kasvamassa. Vain viisi prosenttia ei näe kyberrikollisuuden uhriksi joutumista kasvavana todennäköisyytenä. (Euroopan komissio 2017, 2.) Osuus on onneksi pieni ja kertoo ihmisten valveutuneisuudesta kyberrikollisuuden uhkaa kohtaan.

Perinteisissä rikoksissa Suomen poliisin kyky ratkaista rikoksia on korkea. 2000-luvun alussa rikoksia on tullut vuosittain ilmi noin 500 000–550 000. Tässä tilastossa ei ole

otettu huomioon rikkomuksia, kuten esimerkiksi liikenne- tai ajoneuvorikkomuksia. Alla olevasta kuviosta 1 näkyy, että vuodesta 2010 lähtien rikosten kokonaismäärän trendi on ollut laskeva, ja vuonna 2018 ilmeni hieman alle 450 000 rikosta. Selvitettyjen rikosten määrä suhteessa viranomaisten tietoon tulleiden rikosten määrään on koko 2000-luvun ajan pysynyt melko samana. Esimerkiksi vuonna 2018 ilmeni 443 525 uutta rikosta, joista 273 636 eli noin 61 % selvitettiin.



Lähde: Rikos- ja pakkokeinotilasto, Tilastokeskus

Kuvio 1. Viranomaisten tietoon tulleet rikokset ja selvitettyjen rikosten määrä vuosina 1980-2018 (Tilastokeskus)

Kyberrikollisuuden osalta poliisi kykenee ratkaisemaan jonkun verran vähemmän viranomaisten tietoon tulleita rikoksia. Rikoskomisario Marko Leponen (8.10.2019) Keskusrikospoliisista kertoo, että tilastollisesti noin 90 % verkkorikoksista jää selvittämättä. Todellinen luku on noin 50–60%, sillä monesti poliisi saa selville tekijät, mutta he oleskelevat esimerkiksi toisessa maassa eikä heitä tavoiteta. Tällöin rikos jää tilastojen valossa selvittämättä, vaikka tekijät olisivatkin tiedossa.

Kybermaailma on monella tavalla erilainen kuin fyysinen maailma, vaikka samoja rikoksia nähdäänkin kummassakin ympäristössä. Leponen (8.10.2019) toivookin Keskusrikospoliisin tutkintaan myös tavallisia poliiseja ilman IT-koulutusta. Tällaiset henkilöt hallitsisivat myös poliisin näkökulman verkkorikostutkinnassa. Leposen mukaan verkkorikosten esitutkinta on samanlaista kuin muidenkin rikosten, sillä tapahtui rikos missä tahansa ympäristössä, tekijänä on aina henkilö tai jonkinlainen ryhmittymä, ja poliisin tehtävä on saada tämä kohde kiinni. Kyberrikosten tutkinta ei hänen mukaansa eroa perinteisten rikosten

tutkinnasta, mutta haasteita tuo esimerkiksi tiedon sijainti Suomen ulkopuolella. Usein joudutaan pyytämään virka-apuna tietoa muista maista, jolloin tiedonsaanti voi kestää kauan. Pyydetty tieto ei aina ole selkeässä muodossa, jolloin sen analysointi voi myös viedä poliisin resursseja.

Tekijöiden sijoittuminen eri maihin hankaloittaa verkkorikosten tutkintaa viranomaisten maakohtaisten rajoitusten vuoksi. Tekijöiden lisäksi myös uhrit ja rikokseen liittyvät todisteet voivat sijaita eri puolilla maailmaa, ja ilman viranomaisten järjestelmällistä ja laajamittaista suunnittelutyötä niitä on myös mahdotonta saada yhdistettyä. Tutkintaa hankaloittaa yleisesti myös se, että kyberrikollisuus on luonteeltaan piilorikollisuutta. Uhrit eivät aina tee rikosilmoitusta poliisille, jolloin viranomaisten on hankalampaa pitää yllä kokonaiskuvaa kyberrikoksista. Suurempi tiedon määrä helpottaisi tutkintaa ja lisäisi myös viranomaisten tietämystä Suomessa tapahtuvasta kyberrikollisuudesta. (Poliisiammattikorkeakoulu 2018a, 105-106.)

3.2 Yleisimmät kyberrikokset Suomessa

Niin yksityishenkilöt kuin yrityksetkin Suomessa ovat viime vuosien aikana joutuneet verkkorikollisuuden uhreiksi, ja tietoturvasta puhutaan nykyään monissa medioissa eri tavoin. Marko Leponen (8.10.2019) nostaa selvästi suurimmaksi ja eniten työllistäväksi kyberrikokseksi phishing-hyökkäykset eli tietojenkalastelun. Nämä rikokset koskevat sekä yksityishenkilöitä että yrityksiä, mutta yrityksiin kohdistuvat hyökkäykset ovat rikollisille kannattavampia, sillä yrityksissä liikkuu rahaa. Rikolliset haluavat saada pääsyn organisaation järjestelmiin, jolloin voidaan päästä käsiksi myös arkaluonteiseen tietoon, jota voidaan myydä eteenpäin tai käyttää muuten hyödyksi vilpillisesti. Phishing mahdollistaa myös toimitusjohtajapetokset, jolloin voidaan lähettää esimerkiksi väärennettyjä sähköpostiviestejä toimitusjohtajan tai muun taloudellisista päätöksistä vastaavan henkilön nimissä (englanniksi business email compromise attacks).

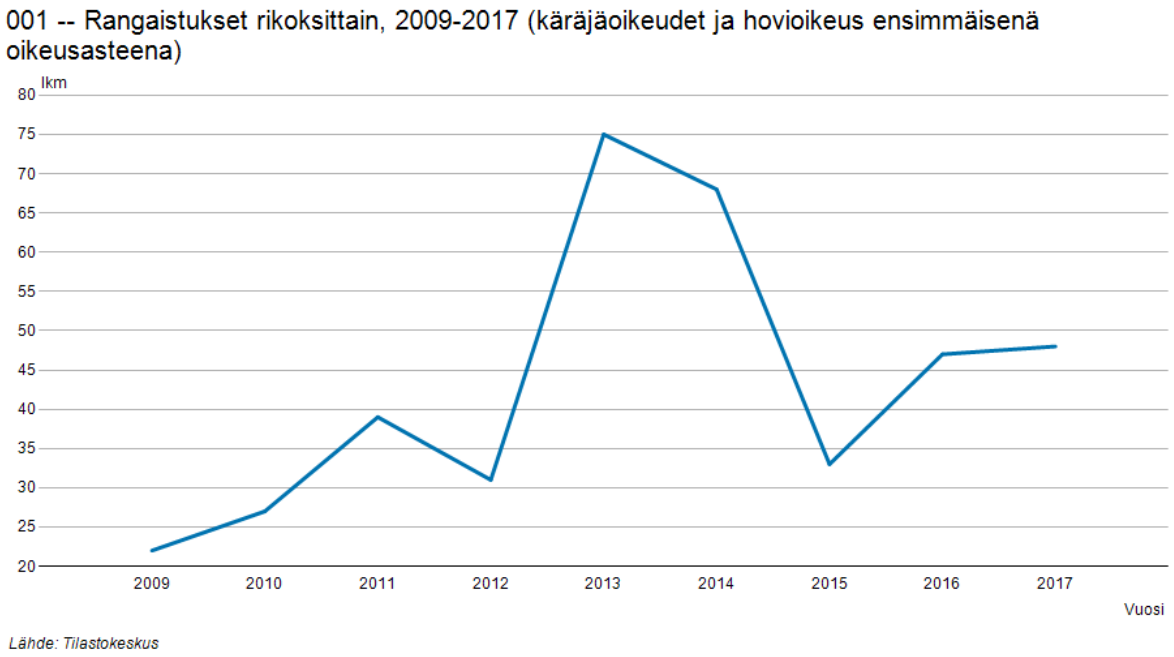
Rikolliset ovat havainneet, että laitteisiin ja tietoverkkoihin murtautuminen on työlästä, kallista ja hidasta, joten phishing-hyökkäysten toteuttaminen helpottaa mahdollista tiedon saantia. Riittävän suurella otannalla tehty tietojenkalasteluhyökkäys todennäköisesti tuottaa tuloksia, sillä joku lankeaa huijauksiin aina. Leponen myös mainitsee, että toivoisi uhrien tekevän phishing-hyökkäyksistä aina rikosilmoituksen, jotta kokonaiskuva olisi luotettavampi ja tutkimuksia saataisiin suoritettua laajemmalla skaalalla. (Leponen 8.10.2019.)

Palvelunestohyökkäykset nousivat haastattelussa toiseksi suureksi kyberrikokseksi Suomessa. Hajautettuja palvelunestohyökkäyksiä eli DDoS-hyökkäyksiä tehdään jatkuvasti,

sillä se on todella halpa hyökkäysmuoto ja siihen löytyy valmiita työkaluja. Myös erityyppisiksi petoksiksi luettavat rikokset ovat siirtyneet suuressa määrin verkkoon, sillä ihmisiltä on verkossa helppo huijata rahaa monilla eri tavoilla. Kasvottomuus auttaa huomattavasti esimerkiksi kaupankäyntiin liittyvien rikosten onnistumisessa. (Leponen 8.10.2019.)

3.3 Tekijät ja tuomiot

Kyberrikosten tekijät ovat yleensä melko nuoria. Vanhemmilla ihmisillä ei välttämättä ole tarvittavia taitoja, joiden avulla voitaisiin toteuttaa rikoksia verkossa. Nuorten henkilöiden kohdalla puhutaan usein diginatiiveista, joille tietoteknisten laitteiden käyttäminen on luonnollista, ja he ovat hyvin nuoresta lähtien tottuneet toimimaan digitaalisessa ympäristössä. Verkkorikoksissa tekijät voivat olla hyvin harjaantuneita ammattilaisia, jotka kehittävät itseään jatkuvasti, tai sitten toisessa ääripäässä amatöörejä, jotka ostavat valmiita työkaluja esimerkiksi tietojenkalastelua tai palvelunestohyökkäystä varten. Vaativien verkkorikosten kohdalla kyseessä on kuitenkin pitkäjänteisyyttä ja ammattitaitoa vaativa projekti, jossa avainasemassa on useiden yritysten ja erehdysten kautta saavutettu onnistuminen (Leponen 8.10.2019).



Kuvio 2. Rangaistukset tieto- ja viestintätekniikkarikoksista vuosina 2009–2017 (Tilastokeskus)

Vuosien 2009–2017 tietoverkkorikoksista annetut tuomiot ovat Suomessa olleet kasvussa. Yllä olevassa kuvassa on esitetty koko maassa kyseisten vuosien välillä annetut rangaistukset käräjä- ja hovioikeuksissa. Rangaistukset kattavat kaikki oikeudessa annetut ran-

gaistusmuodot. Kuvaan on valittu rikoslain 38 luku tieto- ja viestintärikoksista, ja siitä puuttuu datavahingonteko. Vuosien 2012 ja 2013 välillä rangaistukset ovat yli kaksinkertaistuneet, mutta pudonneet sen jälkeen roimasti takaisin normaalille kasvukäyrälle. Kyseisistä kyberrikoksista annetut tuomiot ovat silti määrältään yhä hyvin vähäisiä.

3.4 Tor-verkon kyseenalainen maine ja käyttö Suomessa

Kuten aikaisemmin on mainittu, tor-verkko ei ole vielä suurimmalle osalle suomalaisista tuttu käsite. Media luo osaltaan tietynlaista, melko kielteistä kuvaa tästä internetin toisesta puolesta. Vaikka tor-verkon käytölle on monia muitakin syitä kuin rikollisen hyödyn tavoittelu tai laittomien tuotteiden hankkiminen, jää jokaiselle pohdittavaksi tor-verkon kokonaiskuva. Se mahdollistaa anonyymin kanssakäymisen niin hyvässä kuin pahassa, ja auttaa ihmisiä salaamaan henkilöllisyytensä esimerkiksi siinä tapauksessa, kun oma valtio kiristää vapaan internetin käytettävyyttä ja estää tiedon hankkimisen ulkomaisilta sivustoilta. Tätä ongelmaa ei kuitenkaan Suomessa ole, sillä täällä tieto on vapaasti käytettävissä, mielipiteiden ilmaisu on jokaisen oikeus ja valtionjohtoa vastaan voi esittää kritiikkiä. Tämän kaiken voi toteuttaa ilman pelkoa työpaikan, kansalaisoikeuksien tai esimerkiksi kasvojen menetyksestä.

Viranomaiset suhtautuvat tor-verkkoon ymmärrettävistä syistä tietyllä varauksella. Rikollinen toiminta tor-verkossa aiheuttaa ylimääräistä työtä ja haasteita henkilöllisyyksien selvittämiseksi ja rikosten ratkaisemiseksi. Esimerkiksi laittomia uhkauksia näkyy Marko Leposen (8.10.2019) mukaan paljon tor-verkossa, mutta myös sosiaalisessa mediassa julkisen internetin puolella. Julkaisualusta riippuu tekijän motiiveista ja siitä, haetaanko julkisuutta vai aiotaanko rikos oikeasti toteuttaa. Julkaisupaikan perusteella ei kuitenkaan voida vetää varmoja johtopäätöksiä siitä, aikooko tekijä toteuttaa uhkauksensa vai hakeeko hän vain huomiota ja näkyvyyttä.

Patric Puola (3.11.2019) kertoo, että hämäriin ja rikollisiin verkkosivustoihin on tor-verkossa vaikea törmätä vahingossa. Sivustojen hakeminen ei onnistu yhtä helposti kuin Googlen avulla julkisessa internetissä, joten käytännössä selaajan täytyy tietää, mihin haluaa päästä. Tämän vuoksi esimerkiksi huume- ja asekauppaa sisältäville sivustoille on hankala päätyä tiedostamattaan. Tällaiset sivustot käyttävät .onion-päätettä verkkosivustonsa osoitteessa. Näitä sivustoja kutsutaan onion serviceiksi, ja niissä on kyse juuri sellaisesta toiminnasta, jota ei laillisesta tai laittomasta syystä haluta näyttää avoimesti tavallisille internetin käyttäjille. Näiden sivustojen käyttäminen tor-selaimen kautta takaa sen, että liikenne ei koskaan lähde tor-verkosta ulos, käyttäjän IP-osoitetta ei tallenneta eikä liikennettä ole yhtä helppoa seurata kuin avoimessa internetissä. Rikolliseen tarkoitukseen

perustettujen onion service -sivustojen lisäksi esimerkiksi Ison-Britannian yleisradioyhtiö BBC on perustanut tor-verkkoon oman onion servicensä, joka on suunnattu käyttäjille, joiden sijaintimaassa BBC:n sisältö on estetty (Porter 2019).

Tor-verkon tarpeellisuudesta, laillisuudesta ja moraalisuudesta voidaan olla montaa mieltä. Viranomaisten, tavallisten käyttäjien, sensuuria pakenevien ja rikollisten mielipiteet eroavat toisistaan huomattavasti. Tavallinen julkisen internetin käyttäjä ei ehkä tarvitse tor-verkkoa mihinkään, vaikka yksityisyyden rajojen hämärtyminen onkin aiheuttanut keskustelua viime vuosien aikana runsaasti. On vaikea sanoa, kuinka paljon jokainen enää omistaa omasta henkilökohtaisesta datastaan ja kuinka paljon siitä tiedosta kulkee kauppatavarana erinäisten internetissä toimivien yritysten kesken. Internetin käytön lopettaminen on kuitenkin nykyään hyvin hankalaa, jos haluaa käyttää yhteiskunnan ja yritysten tarjoamia palveluita. Tor-verkon suosiminen on taas suurimmalle osalle pelottava ja vieras ajatus, vaatii teknisesti jonkin verran osaamista, eikä esimerkiksi nopeutensa puolesta ole verrattavissa julkiseen internetiin.

4 Kyberrikosten torjunta Suomessa

4.1 Lainsäädäntö

Rikoslakiin lisättiin vuonna 2015 muutamia pykäliä koskien verkkorikollisuutta, esimerkiksi identiteettivarkaus, tietojärjestelmän häirintä ja viestintäsalaisuuden loukkaus (rikoslaki 39/1889). Nämä lisäykset ovat tulleet melko myöhään ottaen huomioon internetin yleistymisen jo 2000-luvun alkupuolella. Suomen ensimmäisenä nettipoliisina tunnettu Marko Forss ja Itä-Suomen yliopiston lainsäädäntötutkimuksen ja empiirisen oikeustutkimuksen professori Anssi Keinänen julkaisivat vuonna 2017 artikkelin, jossa käsiteltiin internetin ja sosiaalisen median esiintymistä lakiesityksissä. Tutkimuksessa tarkasteltiin vuosina 2009-2016 tehtyjä lakiesityksiä, joita tehtiin yhteensä 111 kappaletta. Näistä lakiesityksestä vain 20 liittyi internetiin tai sosiaaliseen mediaan, ja yleisesti internet mainittiin esityksissä vain muutamalla lauseella. Tutkimuksessa mainitaan, että lainvalmistelijoita tulisi kouluttaa huomioimaan internet ja sosiaalinen media paremmin uusien säädösten valmistelussa. Kotimainen lainsäädäntö ei tekijöiden mukaan riitä vastaamaan kaikkiin nykyisen yhteiskunnan haasteisiin. Tutkijoiden mukaan suuressa osassa netti- ja somerikoksia tekijä selviää ilman rangaistusta, jos hän asuu eri maassa kuin asianomistaja eli uhri. Forssin ja Keinäsen mukaan olisi tärkeää pohtia myös sitä, kuinka kansallisella tasolla voidaan puuttua globaaleihin ongelmiin. (Forss & Keinänen 2017, 1, 6, 10, 24)

Keskusrikospoliisin rikoskomisario Marko Leponen kertoo, että Suomen lain rikosnimikkeet ovat tänä päivänä riittävät ja niitä on määritelty tarpeeksi. Lainsäädännön haasteena on se, että rikos- ja pakkokeinolaki on tehty fyysiseen maailmaan, eikä kyberulottuvuudesta ole tiedetty niiden säätämisen aikaan mitään. Verkkoympäristöön kohdistuva lainsäädäntö pakkokeinojen eli esim. tele- tai datakuuntelun osalta ei ole yhtenevä perinteisen rikosten ja verkkorikosten välillä. Poliisilla on jo työkaluja esimerkiksi edellä mainittujen pakkokeinojen osalta, mutta verkkorikosten tutkinnassa niitä ei voida käyttää, vaikka ne olisivat erittäin hyödyllisiä ja merkittäviä apukeinoja rikosten selvittämiseksi. (Leponen 8.10.2019.)

4.2 Kyberrikostorjuntakeskus

Kyberrikostorjuntakeskus on Keskusrikospoliisissa toimiva, vuonna 2015 perustettu kybertorjunnan yksikkö, joka tutkii vakavia tietoverkkorikoksia sekä kansainvälistä kyberrikollisuutta. Keskuksen tehtäviin kuuluvat myös internettiedustelu, tietotekninen tutkinta sekä tietoverkkorikollisuuden tilannekuvan ylläpitäminen ja päivittäminen yhdessä muiden viranomaisten kanssa. (Poliisi.) Kyberrikostorjuntakeskus myös tukee paikallispoliisilaitoksia

niiden tietoteknisessä tutkinnassa. Kyberrikostorjuntakeskus toimii Keskusrikospoliisin sisällä matriisiorganisaationa, eli siihen kuuluu henkilöitä useista eri Keskusrikospoliisin sisäisistä yksiköistä. Yhteensä työntekijöitä on noin 80, kun otetaan huomioon kaikki verkkorikosten tutkintaan liittyvät henkilöt. Nämä henkilöt työskentelevät Keskusrikospoliisin eri osastoilla, kuten rikosteknisessä laboratoriossa, internettiedustelussa ja verkkorikostorjunnassa. Vain 7 henkilöä keskittyy tällä hetkellä pelkästään kyberrikosten esitutkintaan. Keskusrikospoliisissa verkkorikosten parissa työskentelevät henkilöt tulevat hyvin eri taustoista. Osa on yhdistänyt poliisin koulutuksen IT-alan tutkintoon tai työkokemukseen, heidän tehtäviinsä kuuluvat poliisin esitutkinta verkkorikosten parissa. Osalla ei ole poliisin koulutusta, vaan he ovat Keskusrikospoliisissa siviilityöntekijöinä ja tekevät esimerkiksi ICT-forensiikkaa eli laitteiden tutkintaa. Forensiikka auttaa tutkinnassa silloin, kun tarvitaan pääsyä jollain tavalla lukittuun laitteeseen tai kun laitteesta tai muualta saatu data täytyy analysoida tutkinnan käyttöön. (Leponen 8.10.2019.)

Kyberrikostorjuntakeskus tekee tiivistä yhteistyötä eri tahojen kanssa sekä Suomessa että ulkomailla. Suomessa Traficomin Kyberturvallisuuskeskus sekä Suojelupoliisi ovat merkittävimpiä yhteistyökumppaneita. Kansainvälisesti Europol eli EU:n lainvalvontavirasto on tärkeä partneri, jonka kanssa vaihdetaan tietoa. Europol myös tuottaa erilaisia tietopalveluita ja on luotettava sekä laaja toimija EU:ssa. Myös Interpolin eli kansainvälisen rikospoliisijärjestön sekä muiden maailmalla toimivien poliisiviranomaisten kanssa tehdään yhteistyötä. Suomessa osaaminen on keskittynyt Keskusrikospoliisiin, minkä vuoksi ammattitaitoa tarjotaan myös muiden poliisilaitosten käyttöön Suomen sisällä. (Leponen 8.10.2019.)

4.3 Poliisiammattikorkeakoulu

Poliisiammattikorkeakoulu (Polamk) on Suomessa ainut oppilaitos, jossa voi opiskella poliisiksi. Polamkissa järjestetään myös jatko- ja täydennyskoulutusta jo valmistuneille poliiseille, ja nämä koulutukset sisältävät myös mahdollisuuden tutustua kyberrikollisuuteen (Leponen 8.10.2019). Poliisin ammattikorkeakoulutasoisessa tutkinnossa ei ole erikseen määritelty kyberrikollisuuteen liittyviä opintokokonaisuuksia, mutta osana Pakkokeinot ja tiedonhankinta -osajaksoa sivutaan kyberturvallisuusympäristöä ja kyberrikollisuutta (Poliisiammattikorkeakoulu 2018b). Leposen mukaan Poliisiammattikorkeakoulun tarkoituksena on kuitenkin tuottaa monialaosaajia sekä kenttätyöhön että tutkintaan, joten oppilaitoksella on halu kehittää koulutusta myös kyberrikostorjunnan suuntaan.

Poliisiammattikorkeakoulusta valmistuvat tuottavat lopputyönään opinnäytetyön, joita oppilaitos on vuodesta 2015 tallentanut Theseus-hakupalveluun. Poliisiammattikorkeakoulun

opinnäytetöitä löytyi hakusanalla ”kyber” seitsemän kappaletta, joista vain kolme liittyi kyberrikollisuuteen tai sen käsittelyyn poliisin työssä. Yksi näistä kyberrikollisuutta sivuavista lopputöistä on Ari Anttilan vuodelta 2018 oleva opinnäytetyö, jonka otsikkona on ”Kyberrikokset - Kirjaaminen ja alkutoimet tietotekniikkarikoksissa”. Kyseisen työn tarkoituksena oli tuottaa ohjeistus henkilöille, jotka kirjaavat tietotekniikka- eli kyberrikoksia Poliisiasiain tietojärjestelmään. Opinnäytetyö sisältää myös tiedot alkutoimista, joita viranomaisen tulisi kyseisiä rikoksia kirjatessa tehdä. Varsinaiset kirjausohjeet on määrätty salassa pidettäväksi. (Anttila 2018.) On tärkeää, että jatkuvasti yleistyvien verkkorikosten kirjaamisessa noudatettaisiin samoja periaatteita ympäri Suomen. Paikallispoliisilaitoksetkaan eivät tulevaisuudessa välty rikoksilta, jotka on heidän toimialueellaan tehty verkon välityksellä.

4.4 Suomen kyberturvallisuusstrategia

Suomi julkaisi ensimmäisen kyberturvallisuusstrategiansa vuonna 2013. Siinä määriteltiin tavoitteet ja toimenpiteet, jotta myös valtiotasolla voitaisiin vastata kyberympäristöön liittyviin haasteisiin ja uhkiin. Strategian tavoitteena oli luoda turvallinen kybertoimintaympäristö, joka auttaa yrityksiä ja yksityishenkilöitä toimimaan verkossa paremmin ja järkevämmin. Suunniteltujen toimenpiteiden myötä Suomi voisi paremmin hallita kybertoimintaympäristössä esiintyviä haittavaikutuksia sekä toipua niiden mahdollisesti aiheuttamista vahingoista. (Turvallisuuskomitea.)

Ensimmäisen strategian myötä asetettiin myös toimeenpano-ohjelma, joka uusittiin jälleen vuosille 2017–2020. Uudessa toimeenpano-ohjelmassa esitetään kyberturvallisuuden kehittäminen kokonaisuutena, jossa valtio, kunnat ja yritykset luovat toiminnalle kehyksen. Tällöin kansalaisesta tulee asiakas, joka hyödyntää tuotettuja palveluita. Uusi toimeenpano-ohjelma sisältää kolme kokonaisuutta, jotka liittyvät kyberturvallisuuden johtamiseen, yhteiskunnan digitalisoituihin toimintoihin sekä kansalaisten, yritysten ja hallinnon kyberosaamiseen. Näiden osa-alueiden myötä kyberturvallisuusstrategian linjauksia pyritään täyttämään ja kehittämään myös tulevaisuudessa. (Turvallisuuskomitea 2017.)

Mielenkiintoinen poiminta strategian sisältämästä visiosta on se, että Suomen tavoitteena on olla maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa sekä niistä johtuvien häiriötilanteiden hallinnassa (Turvallisuuskomitea 2017). Tämä on erinomainen esimerkki siitä, kuinka tavoitteet voi nostaa korkealle, jolloin niiden saavuttaminen luo positiivista painetta. Laadukkaiden ja tarkasti määriteltyjen tavoitteiden saavuttaminen on helpompaa, vaikka ne vaatisivatkin paljon työtä ja uudistumista. Tässä uusi toimeenpano-ohjelma on suuressa roolissa, sillä sen avulla strategiset linjaukset voidaan pilkkoa pienempiin osiin ja

keskittyä muutaman vuoden sykleissä niihin osa-alueisiin, joihin kulloinkin tarvitsee panostaa.

4.5 Tietoverkkorikollisuuden torjuntasuunnitelma

Sisäministeriö julkaisi vuonna 2017 selvityksen, jossa käsitellään tietoverkkorikollisuuden torjuntaa ja sen kehittämiseksi suunniteltavia toimenpiteitä. Selvitykseen osallistuivat sisäministeriön lisäksi poliisihallituksen asettama työryhmä, Keskusrikospoliisi sekä Suojelupoliisi. Julkaisussa kerrotaan, että suuri osa yhteiskunnan kriittisistä tuotantoprosesseista on automatisoituja ja yhdistetty tietoverkkoihin. Tämä asettaa esimerkiksi sähkönhallintaan, kiinteistöautomaatioon ja järjestelmien etäkäyttöön liittyvät toiminnot alttiiksi kyberhyökkäyksille. Myös terveystoimialaan kohdistuneet iskut ovat yleistyneet ja onnistuessaan esimerkiksi tietomurrot voisivat lamauttaa tai vaarantaa terveysviranomaisten toiminnan tai potilasturvallisuuden. (Sisäministeriö 2017.)

Selvityksessä tunnistetaan myös kybervakoilu olemassa olevaksi uhaksi. Sen havainnointiin liittyvä osaaminen ei Suomessa julkaisun mukaan ole tarpeeksi korkealla tasolla. Vieraan valtion toteuttama kybervakoilu aiheuttaa tutkinnallisia ongelmia sen vuoksi, että vaikka teko täyttäisikin useamman rikoksen tunnusmerkit, sen selvittämiseksi tarvittaisiin virka-apua lähdemaasta. Jos tekijät toimisivat sen maan nimissä, jossa he sijaitsevat, ei kyseiseltä valtiolta todennäköisesti tulisi apua rikoksen tai tekijöiden selvittämiseksi. (Sisäministeriö 2017.)

Raportissa mainitaan muitakin Suomen toimintakykyä heikentäviä uhkia, ja niiden ennaltaehkäisemiseksi ja verkkorikostorjunnan kehittämiseksi kokonaisuutena esitetään useita toimenpidesuosituksia. Verkkorikostorjunnan kehittämisessä painotetaan yhteistyön tärkeyttä eri kotimaisten sekä kansainvälisten toimijoiden välillä. Myös suomalaiset yliopistot ja korkeakoulut tulee saada kouluttamaan tulevaisuuden osaajia kyberrikostorjunnan osalta. Poliisiammattikorkeakoulun vastuulle annetaan AMK- ja YAMK-tutkintojen kehittäminen kyberrikososaamisen suuntaan ja täydennyskoulutuksien järjestäminen. Myös lainsäädännön kehittämiseksi on selvityksessä mainittu useita toimenpidesuosituksia, joissa mainitaan myös pakkokeinolain muutostarpeiden selvitys, joka nousi esille myös Marko Leposen haastattelussa. (Sisäministeriö 2017.)

4.6 Tietoturva ja käytettävyys

Tietoturva kulkee aina yhdessä käytettävyyden kanssa. Nämä kaksi liittyvät toisiinsa siten, että mahdollisimman tiukan tietoturvan periaatteiden mukaan toimittaessa käytettävyys kärsii aina hieman. Tällöin käyttäjä joutuu usein käymään läpi monta vaihetta ennen kuin

pääsee kirjautumaan esimerkiksi johonkin verkkopalveluun. Nämä periaatteet koskevat niin yrityksiä kuin yksityishenkilöitäkin, mutta yrityksissä tietoturvan ja käytettävyyden rinnakkaiselon mahdollistaminen korostuu vieläkin enemmän. Yritykset joutuvat määrittelemään itselleen tarpeeksi hyvän tietoturvasuunnitelman ja kartoittaa ne riskit, jotka sitä voivat kohdata ja kuinka niihin varaudutaan. Rikollisille yritykset ovat tuottoisampi kohde, sillä yritysten järjestelmät sisältävät huomattavasti enemmän arkaluonteista ja myyntikelpoista tietoa. Kyberrikollisen kannalta parhaassa tapauksessa rikoksen avulla päästään käsiksi jopa suoraan rahavirtoihin. Jos päivittäinen työ tapahtuu pelkästään tietokoneen ääressä, voi tuntua erittäin epämiellyttävältä joutua jatkuvasti keskeyttämään työnteko tietoturvapolitiikan noudattamisen vuoksi. Se on kuitenkin yksi kriittinen osa yrityksen toimintavarmuutta, sillä ihminen on käytännössä aina teknologian heikoin lenkki.

Marko Leponen (8.10.2019) vertaa yritysten tietoturvasta huolehtimista lukittuihin oviin, joihin on avain vain tietyillä työntekijöillä. Järjestelmien tietoturva koetaan usein hankalaksi, mutta kukaan ei kyseenalaista lukittuja ovia ja tiloja, joihin kaikilla työntekijöillä ei ole pääsyä. Yhdellä avaimella myöskään ei pääse kaikkiin tiloihin, ja sama pätee myös tietoturvaan. Yksi ja sama salasana ei riitä kaikkiin järjestelmiin, vaan kokonaisuudesta täytyy muodostua avainnippu, jonka avulla voidaan hallinnoida tietoturvan toteutumista ja henkilöiden pääsyä vain heille tarkoitettuihin järjestelmiin.

4.7 Kyberrikollisuuden tulevaisuus

Kyberrikollisuus on ilmiönä uusi, mutta jatkuvasti kasvava ja arkipäiväistyvä rikollisuuden muoto. Osa siitä ilmenee helposti ohitettavina tietojenkalasteluviesteinä tai epäilyttävinä sähköpostin liitetiedostoina, mutta myös järjestäytynyttä kyberrikollisuutta esiintyy. Asia on vakavasti otettava, mistä kertoo esimerkiksi Keskusrikospoliisiin perustettu Kyberrikostorjuntakeskus ja viranomaisten yleistyvät tiedotuskampanjat.

Marko Leposta (8.10.2019) kyberrikollisuudesta tehtyjen rikosilmoitusten vähäinen määrä jopa turhauttaa, sillä sen tiedetään olevan yleisempää kuin rikosilmoituksista voidaan päätellä. Yhteiskunta ei ole vielä tarpeeksi kehittynyt tunnistamaan verkkorikollisuutta, sillä vanhemmat, suuret ikäluokat joutuvat vasta pakotetusti siirtymään verkkopalveluihin. Heidän osaamistasonsa on huomattavasti alhaisempi kuin nuorten ikäpolvien. Leponen toivoo, että 5–10 vuoden kuluttua ihmisten kyky liikkua digitaalisessa maailmassa olisi kehittynyt huomattavasti sen suhteen, että he osaisivat havaita väärinkäytöksiä helpommin ja nopeammin. Fyysisessä maailmassa tunnistetaan huijaus tänä päivänä melko nopeasti, mutta verkkoympäristö on uusi ja vielä melko tuntematon maailma. Sitä mukaa kun inter-

netin käyttäjien kypsyys asiassa kasvaa, petosten vaikuttavuus vähenee. Verkossa keksitään jatkuvasti uusia palveluita, ja Leposen mukaan tämä altistaa rikollisuudelle ja tuo mukanaan mahdollisuuden kehittää rikoksia yhä hienovaraisemmiksi ja uskottavimmiksi. Leponen korostaa tässäkin käytettävyyden ja tietoturvan tasapainoa, joka on ikuinen ongelma tietoturvan ja palveluiden kehittämisessä. Käyttäjät eivät välttämättä ole valmiita luopumaan palveluiden helppokäyttöisyydestä kritiikittä. Tulevaisuus kuitenkin vaatii jokaiselta mukautumista tietoturvan haasteisiin ja siihen taisteluun, jota kyberrikollisuutta vastaan käydään.

5 Pohdinta

Kyberturvallisuutta ja sen merkitystä ei voi yksikään suomalainen enää sivuuttaa. Internet on arjessamme niin tärkeässä roolissa, että tietoturva on otettava huomioon niin yksityiskuin yrityselämässäkin. Verkkopankissa asiointi yleistyy, verkkokaupat helpottavat ihmisten asiointia ympäri maata ja sosiaalinen media tarjoaa jatkuvasti päivittyvää sisältöä sekä mahdollistaa yhteyden toisiin ihmisiin ympäri maailman. On äärimmäisen tärkeää, että kaikki nämä toteutetaan turvallisesti ja yksityisyydensuojaa kunnioittaen. Jossain määrin olemme joutuneet luopumaan siitä periaatteesta, että omistaisimme omat tietomme täydellisesti. Kieltäytymällä esimerkiksi sosiaalisen median tai Googlen palveluista voi välttyä enimmältä seurannalta ja tietojenkeruulta, mutta samalla luopuu kyseisten palvelujen tarjoamista hyödyistä. Pahinta internetyritysten toiminnassa on se, että tavallinen käyttäjä ei usein tiedä, mitä kaikkea tietoa hänestä kerätään. Rekisteröitymällä johonkin palveluun tulee aina hyväksyneeksi joukon käyttöehtoja, jolloin käyttäjä usein antaa oikeuden kerätä käytön myötä tiettyjä tietoja itsestään sekä tavasta, jolla hän käyttää palvelua.

Viranomaiset tekevät kyberrikollisuuden kartoittamiseksi ja ehkäisemiseksi paljon taustaja kenttätyötä, joka ei näy tavalliselle kansalaiselle mitenkään. Tiedottamisessa Suomen poliisilla on myös tärkeä rooli, sillä tiedon lisääminen on aina hyödyllistä ja auttaa ennaltaehkäisemään myös verkkorikoksia. Viranomaisten toteuttama kansainvälinen yhteistyö auttaa poliisiorganisaatioita maailmanlaajuisesti pysymään tilanteen tasalla ja edistämään rikosten tutkintaa esimerkiksi tiedonvaihdon avulla. Kyberrikosten tutkiminen perinteisiin rikoksiin verrattuna on kuitenkin melko samanlaista, ja poliisilla on käytössään erittäin ammattitaitoisia tutkijoita ja menetelmiä. Poliisiammattikorkeakoululla on myös tärkeä rooli tulevien poliisien kouluttamisessa. Heidän tulee olla ajan tasalla kyberrikollisuuden etenemisestä, vaikka järjestyspoliisin kenttätyössä ei juuri verkkorikollisia tarvitsekaan jahdata. Eri viranomaisten kyberrikostutkinnassa sijaitsevat työpaikat tulevat varmasti lisääntymään seuraavien vuosien aikana, joten näihin uhkiin valmistautuminen on tärkeää jo koulutusvaiheessa.

Aikaisemmin mainittu pakkokeinolainsäädännön kehittäminen nähdään erittäin tärkeänä viranomaisten keskuudessa. Viranomaisille tulisi turvata tarpeeksi kattavat menetelmät, jotta rikoksia voitaisiin ehkäistä sekä tutkia parhaalla mahdollisella tavalla. Viranomaistahot eivät valvo jatkuvasti kansalaisten internetkäyttäytymistä, vaan tietoa hankitaan aina perusteltuihin epäilyihin pohjautuen. Yksityisyys on ollut parina viime vuonna suuri ja tunteita herättävä keskustelunaihe, ja mielipiteitä riittää puolesta sekä vastaan. Onko oikein,

että tor-verkossa voidaan suunnitella vakaviakin rikoksia ja etsiä samanhenkisiä keskustelukumppaneita? Kuinka paljon voimme omistaa omasta tiedostamme, jos jaamme sen julkisesti esimerkiksi sosiaalisessa mediassa? Joudummeko hyväksymään riskin mahdollisesta tietovuodosta aina, kun rekisteröidymme uuteen palveluun? Näitä kysymyksiä jokainen voi pohtia liikkuessaan nykyisellä tavalla toimivassa, mainontaan ja käyttäytymisen seurantaan panostavassa internetissä.

5.1 Tutkimuksen luotettavuus ja jatkokehitysideat

Tutkimuksen aikana on etsitty materiaalia ja taustatietoa pääasiassa viranomaisten raporteista, uutisista ja muista luotettavista lähteistä. Kaikki tieto on julkaistu muutaman viime vuoden aikana, mikä lisää luotettavuusarvoa, sillä tapahtuneista tai materiaalin julkaisusta ei ole ehtinyt kulua useita vuosia. Faktat eivät ole vanhentuneet, vaan olemme päinvastoin vasta kyberrikollisuuden arkipäiväistymisen alkuvaiheissa. Tutkimuksessa käytetty materiaali on julkista, sillä aihe rajoittaa tiedonsaantia esimerkiksi rikosten tutkintaprosessista tai yksittäisten rikosten osalta.

Tutkimusta varten on myös haastateltu kahta kyberrikollisuuden eri tavalla näkevää henkilöä. Rikoskomisarion ja tor-verkon käytön mahdollistavan palvelimen ylläpitäjän näkökulmat eriävät työperäisten syiden vuoksi. Rikoskomisario näkee myös tor-verkossa tapahtuvat rikokset, kun taas tor-verkon käyttäjä pitää sitä alustana, jonka avulla ihmiset voivat säilyttää yksityisyytensä ja käyttää internetiä ilman seurantaa. Tämä muistuttaa hyvin siitä, että kaikki pimeässäkään verkossa ei välttämättä ole pahaa, vaikka sen ympärillä olisikin paljon laitonta. Jokainen päättää itse, mihin asti arvostaa yksilön sananvapautta ja oikeutta pysyä pois viranomaisten näkyvistä.

Suomessa kyberrikollisuudesta on kirjoitettu vielä hyvin vähän virallisia raportteja tai katsauksia. Verkkorikollisuus on aiheena hyvin tuore, mutta materiaalia esimerkiksi rikostilastojen muodossa löytyy jo jonkin verran. Aiheesta tulisi keskustella julkisuudessa jatkuvasti ja yhä enemmän, sillä internet jatkaa kasvukauttaan todennäköisesti loputtomiin. Viranomaisten välinen yhteistyö on ehdottoman tärkeää ja myös erilaisten tietoturvayritysten tulisi osallistua julkiseen keskusteluun. Kyberrikollisuuden tunnistamisesta ja sen ehkäisystä tulee tehdä arkipäiväistä, jotta aihe ei tuottaisi kenellekään aiheetonta pelkoa, mutta siihen suhtauduttaisiin tarvittavalla vakavuudella. Jatkotutkimuksena olisi mielenkiintoista toteuttaa laaja kysely siitä, kuinka ihmiset kokevat kyberrikollisuuden uhan ja miten he itse torjuvat sitä arjessa. EU:n Eurobarometrissä asiaa on tutkittu vuonna 2017,

mutta tutkimus olisi syytä toteuttaa uudelleen ja pyrkiä kasvattamaan vastaajamääriä. Kovin moni ei varmasti tunne voivansa ehkäistä verkkorikollisuutta tai edes tiedä, kuinka se onnistuisi.

Vuoropuhelua haastateltavien välillä voisi jatkaa myös tutkimuksen valmistumisen jälkeen. Tor-verkon käyttäjän ja rikoskomisarion kesken olisi mielenkiintoista luoda keskustelua, jossa tor-verkon käytön tuomat mahdollisuudet ja uhat tuotaisiin ilmi eri näkökulmista. Haastateltaville voisi esittää samoja kysymyksiä ja hankkia mielipiteitä myös laajemmin esimerkiksi julkisen kyselyn avulla. Haastatteluja voisi myös toteuttaa lisää eri tahoilla, esimerkiksi Poliisiammattikorkeakoulun edustajan tai kouluttajan kanssa. Omakohtainen kokemus alalta on aina värikkäämpää ja mielenkiintoisempaa kuin erilaisista virallisista julkaisuista poimitut tiedot. Haastattelujen myötä saadaan myös täsmällistä ja yksityiskohtaista tietoa.

5.2 Oma oppiminen opinnäytetyön aikana

Opinnäytetyöprosessi on ollut yllättävän helppo ja suoraviivainen, eikä missään vaiheessa ole tullut vaikeuksia sen loppuun asti suorittamisessa. Kirjoittaminen on ollut helppoa, vaikka materiaalia onkin loppujen lopuksi ollut hyvin runsaasti ja lähteitä jäi vielä käyttämättä. Työn alkuperäinen rajaus on ollut erittäin onnistunut. Sen avulla työstä on tullut sopivan tiivis, ja se on täyttänyt sille annetut tavoitteet mielestäni erinomaisesti. Lopputuloksena on kattavat perustiedot sekä empiiristä kokemustietoa sisältävä tutkimus, josta on hyötyä alaa opiskeleville tai asiasta kiinnostuneille.

Prosessin aikana aihe on tullut tutuksi, ja se on myös herättänyt pohdintaa siitä, kuinka paljon yksittäinen ihminen voi vaikuttaa kyberrikollisuuden leviämiseen. On myös ollut hienoa huomata, kuinka paljon aihe kiinnostaa ihmisiä yleisesti ja miten tarpeellista kyberrikollisuudesta puhuminen on. Erityisen tärkeää on tuottaa tietoa helposti ymmärrettävässä muodossa, sillä tietotekniset termit eivät välttämättä ole monelle tuttuja eikä tietotekniikka itsessään kiinnosta kaikkia.

Opinnäytetyön tekeminen oli äärimmäisen mielenkiintoista ja mielekästä aiheen ajankohtaisuuden ja henkilökohtaisen kiinnostuksen vuoksi. Aihe valikoituikin alun perin omasta mielenkiinnosta, sillä kyberrikollisuuden tutkiminen on todella mielenkiintoinen tietotekniikan ja poliisitoiminnan yhdistävä osa-alue. Oli hienoa huomata, että aihe suoranaisesti vei mukanaan ja tärkeää lisäsisältöä tuovat haastattelut järjestyivät helposti. Haastateltavat tarjosivat lyhyessä ajassa valtavan tietomäärän, josta oli todella paljon hyötyä opinnäyte-

työn sisällön laajentamisen kannalta. Molemmat myös suhtautuivat kysymyksiin ja opinnäytetyöhön vakavasti ja kiinnostuneesti, mikä oli todella ilahduttavaa. Jatkokysymyksiä haastateltaville olisi voinut esittää runsaasti vielä pitkän ajan päästä, ja keskustelua voisi hyvin jatkaa myös opinnäytetyön julkaisemisen jälkeen. Aiheesta riittää puhuttavaa ja viranomaistyöstä olisi kiinnostavaa tietää lisää, mutta siviilillä on tietysti tähän rajalliset mahdollisuudet.

Ennen opinnäytetyön aloittamista epäluuloisuutta ja huolta aiheutti se, löytyisikö aiheeseen liittyen julkisesti saatavilla olevaa materiaalia. Tämä pelko kumoutui kuitenkin nopeasti, sillä useat eri viranomaiset poliisin lisäksi ovat tuottaneet viime aikoina laajojakin katselmuksia verkkorikollisuuden eri näkökulmista. On äärimmäisen tärkeää, että tietoisuus lisääntyy niin yrityksissä kuin yksityishenkilöidenkin keskuudessa, sillä internet koskettaa tänä päivänä jokaista. Tieto voi tässä tapauksessa lisätä tuskaa ja ihmisten pelkoakin, mutta mitä enemmän aiheesta puhutaan julkisesti, sitä paremmin osataan varautua ja toimia ennaltaehkäisevästi. Jokaisella on velvollisuus ja myös oikeus vaatia parempaa tietoturvaa, käyttäytyä järkevästi internetissä ja huolehtia omalta osaltaan kyberrikollisuuden ehkäisemisestä.

5.3 Tärkeimmät havainnot

Kaikista tärkein opinnäytetyön aikana löytynyt tutkimustulos ja havainto on ehdottomasti se, että kyberturvallisuudesta huolehtiminen kuuluu nykyään jokaiselle, oli henkilön rooli mikä hyvänsä. Internetin käyttö on niin yleistä ja se sulautuu jatkuvasti kiinteämmäksi osaksi elämää. Kotona, oppilaitoksissa, työpaikalla, harrastustoiminnassa ja joka ikisessä yhteisössä ja organisaatiossa tulee minimoida riskit, jotta kyberrikollisuus eri muodoissaan ei pääsisi leviämään. Eri viranomais- ja asiantuntijatahojen tulisi säännöllisesti viestiä turvallisesta verkkokäyttäytymisestä erilaisten medioiden kautta, jotta tieto saavuttaisi mahdollisimman monen verkossa liikkuvan. Myös mahdollisista rikostapauksista tulisi välittömästi ilmoittaa poliisille, jotta tutkinta tiedon karttuessa vähitellen helpottuisi.

Yritysten, niin pienten kuin suurtenkin, tulisi ottaa entistä suurempi vastuu ja huolehtia siitä, että niin asiakkaiden kuin omien työntekijöiden tiedot ovat turvassa ja riski väärinkäyttöön on minimoitu. Jokaiselle yritykselle hyvä ohjenuora olisi, että tietoturvaa pyritään aina tekemään paremmin kuin muut. Tällöin tavoitteet ovat korkealla ja niiden saavuttamiseksi tehdään todennäköisesti enemmän työtä kuin silloin, jos tietoturvalle ei ole määritelty mitään strategiaa. Pienissä yrityksissä, joissa tietoturvaan ei resurssien kannalta voida panostaa kovin paljon, olisi tärkeää edes kartoittaa omat IT-laitteet ja -palvelut mahdollisimman turvallisiksi ja ajantasaisiksi. Tarvittaessa mukaan voidaan ottaa ulkopuolista

apua lyhyeksi ajaksi, jotta yritys voi keskittyä omaan osaamiseensa ja toimintaansa. Samalla voidaan saavuttaa sellainen tietoturvan taso, jonka avulla yrityksen data on turvattu, häiriötilanteisiin on varauduttu ja toiminta voi jatkua tulevaisuudessakin ongelmitta.

Kyberturva-alalla on sanonta, jonka mukaan amatöörit hakkeroivat laitteita ja ammattilaiset ihmisiä. Rikolliset ovat vuosien myötä havainneet, että tietoteknisiin laitteisiin pääseminen vaatii työtä ja aikaa, mutta ihmiset saattavat luovuttaa halutun tiedon yhdellä klikkauksella. Tämän vuoksi jokaisen rooli yksityishenkilönä sekä mahdollisesti yrityksen työntekijänä on olla valppaana, huolehtia omalta osaltaan tietoturvasta ja harkita kaksi kertaa, mitä klikkaa. Kyberrikollisuus ei välttämättä kosketa jokaista suomalaista, kuten ei perinteinen rikollisuuskaan. Moni voi ajatella, että omat tiedot eivät ole niin kiinnostavia tai rahallisesti arvokkaita, eivätkä rikolliset siksi haluaisi kohdistaa iskujaan heihin. Tämä on kuitenkin vaarallinen ajattelutapa, sillä jokaisella on hallussaan dataa ja omaisuutta, jonka ei varmasti haluaisi päätyvän vääriin käsiin. Pankki- tai luottokorttien tiedot tai henkilötunnus yhdistettynä osoitetietoihin avaavat mahdollisuuden tilata toisen nimissä esimerkiksi verkkokaupasta tuotteita. Kyberrikollisuuden uhriksi jäämisen minimointi on kuitenkin mahdollista hyvin pienellä vaivalla. Se vaatii verkon käyttäjältä lähinnä kolmen asian yksinkertaisen yhdistelmän: valppautta, vastuullisuutta ja virusturvaohjelmiston. Ihminen on kuitenkin aina teknologiaketjun heikoin lenkki.

Lähteet

Aaltonen, M., Suonpää, K., Kivivuori, J., Danielsson, P. & Näsi, M. 2018. Kriminologia: Rikollisuus ja kontrolli muuttuvassa yhteiskunnassa. Gaudeamus. Helsinki.

Albrecht, M. 2017. Lunnastroijalaisten hyökkäys. Luettavissa: https://www.haaste.om.fi/fi/index/lehtiarkisto/haaste22017/lunnastroijalaistenhyokkays.html. Luettu: 5.9.2019.

Albrecht, M. 2018. Psykologia – kyberrikollisen uusi työkalu. Luettavissa: https://www.haaste.om.fi/fi/index/lehtiarkisto/haaste42018/psykologia-kyberrikollisenuusityokalu.html. Luettu: 13.10.2019.

Anttila, A. 2018. Kyberrikokset – Kirjaaminen ja alkutoimet tietotekniikkarikoksissa. Opinnäytetyö. Poliisiammattikorkeakoulu. Tampere. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/150431/ON_Anttila.pdf?sequence=1&isAllowed=y. Luettu: 3.11.2019.

Bittiraha 2019. Bitcoin-maksupaikat Suomessa. Luettavissa: https://bittiraha.fi/bitcoin-maksupaikat-suomessa/. Luettu: 24.9.2019.

Euroopan komissio 2017. Special eurobarometer 464a. Luettavissa: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79746. Luettu: 20.10.2019.

Forss, M. & Keinänen, A. 2017. Rikoslakia koskeva lainvalmistelu – miten internet ja erityisesti sosiaalinen media huomioitiin vuosina 2009–2016 annetuissa hallituksen esityksissä. Edilex 2017/38. Luettavissa: https://www.edilex.fi/artikkelit/18068. Luettu: 8.12.2019.

Halminen, L. 2019. Yle. Viidelle syytteitä vero-petoksista ja rahanpesusta Pohjanmaalla: Taustalla pyramidi-huijaukseksi arvioitu virtuaali-valuutta. Luettavissa: https://www.hs.fi/teknologia/art-2000006214242.html. Luettu: 24.9.2019.

Hokkanen, T. 2017a. Kiusaaminen on rikos, myös netissä! Luettavissa: https://blogi.poliisi.fi/kiusaaminen-rikos-myos-netissa/. Luettu: 29.9.2019.

Hokkanen, T. 2017b. Vihapuhe, viharikokset ja rikokseen kehottaminen. Luettavissa: https://blogi.poliisi.fi/vihapuhe-viharikokset-ja-rikokseen-kehottaminen/. Luettu: 29.9.2019.

Jäntti, E. 2019. Elisa. Mistä bitcoinissa on kysymys? Luettavissa: https://yksityisille.hub.elisa.fi/mista-bitcoinissa-on-kysymys/. Luettu: 20.9.2019.

Kaakinen, M. 2018. Disconnected Online - A social psychological examination of online hate. Väitöskirja. Tampereen yliopisto. Luettavissa: https://trepo.tuni.fi/bitstream/handle/10024/103681/978-952-03-0767-7.pdf?sequence=1&isAllowed=y. Luettu: 29.9.2019.

Keronen, J. 2018. Kryptovaluuttojen turvallisuus perustuu kryptografiaan. Bittiraha.fi. Luettavissa: https://bittiraha.fi/blog/kryptovaluuttojen-turvallisuus-perustuu-kryptografiaan/. Luettu: 20.9.2019.

Keskusrikospoliisi 2015. KRP on selvittänyt OneCoin-virtuaalirahaa. Luettavissa: https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/krp_on_selvittanyt_onecoin-virtuaalirahaa_41044. Luettu: 24.9.2019.

Keskusrikospoliisi 2017a. Kiristyshaittaohjelmista on tullut maailmanlaajuinen turvallisuusuhka. Luettavissa: https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/kiristyshaittaohjelmista_on_tullut_maailmanlaajuinen_turvallisuusuhka_58230. Luettu: 5.9.2019.

Keskusrikospoliisi 2017b. Keskusrikospoliisi selvittää virtuaalivaluutan roolia terrorismi- ja rahanpesurikoksissa. Luettavissa: https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/keskusrikospoliisi_selvittaa_virtuaalivaluutan_roolia_terrorismi-_ja_rahanpesurikoksissa_59282. Luettu: 24.9.2019.

Keskusrikospoliisi 2018a. Poliisi kehottaa yrityksiä suojautumaan verkkohyökkäyksiltä – tapauksia ollut tavallista enemmän. Luettavissa: https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/poliisi_kehottaa_yrityksia_suojautumaan_verkkohyokkayksilta_tapauksia_ollut_tavallista_enemman_68678. Luettu: 2.9.2019.

Keskusrikospoliisi 2018b. Kaksikon epäillään välittäneen Subutexeja TOR-verkossa – Poliisin ja Tullin esitutkinnassa tuli ilmi useita muita törkeitä rikoksia. Luettavissa: https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/kaksikon_epaillaan_valittaneen_subutexeja_tor-verkossa_poliisin_ja_tullin_esitutkinnassa_tuli_ilmi_useita_muita_torkeita_rikoksia_75271. Luettu: 20.9.2019.

Keskusrikospoliisi 2018c. Virtuaalivaluuttojen käyttö terrorismi- ja rahanpesurikoksissa kasvanut. Luettavissa: https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/virtuaalivaluuttojen_kaytto_terrorismi-_ja_rahanpesurikoksissa_kasvanut_71123. Luettu: 24.9.2019.

Keskusrikospoliisi 2019. Poliisin kyberrikostorjuntakeskus varoittaa sijoitushuijauksista. Luettavissa: https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/poliisin_kyberrikostorjuntakeskus_varoittaa_sijoitushuijauksista_77656?fbclid=IwAR1W_fKHfohb8Mbw2V6uFO5e1KiIkMwmFu2CCObnUM6SK226Vev8jdbwsRg. Luettu: 17.9.2019.

Kirves, A. 2007. Symantec: Pankkien on opastettava asiakkaitaan. Luettavissa: https://www.is.fi/digitoday/tietoturva/art-2000001505792.html. Luettu: 11.9.2019.

Knowbe4 2019. Phishing: History of phishing. Luettavissa: https://www.phishing.org/history-of-phishing. Luettu: 11.9.2019.

Krogerus, M. 2019. Yle. Tor-verkko ei ole pelkästään rikollisten temmellyskenttä: “Anonyymiys on virkistävä kokemus”. Luettavissa: https://yle.fi/uutiset/3-10816305. Luettu: 20.9.2019.

Kyberturvallisuuskeskus 2016. Palvelunestohyökkäysten ehkäisy ja torjunta. Viestintävirasto. Ohje 3/2016. Helsinki. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta.pdf. Luettu: 9.9.2019.

Laakso, A. 2017. Pahamaineisen Tor-verkon osa suljettiin – sivulle ilmestyi Poliisin ja tullin terveiset. Aamulehti. Luettavissa: https://www.aamulehti.fi/a/200502987. Luettu: 19.9.2019.

Leponen, M. 8.10.2019. Rikoskomisario. Keskusrikospoliisi. Haastattelu. Vantaa.

Liukkonen, S. 2018. Rakkauspetoksen uhri tarvitsee myötätuntoa. RIKU-lehti, 2/2018, s. 30-31.

No More Ransom 2019. The No More Ransom Project. Luettavissa: https://www.nomoreransom.org/fi/index.html. Luettu: 5.9.2019.

Nuortennetti 2019. Nettikiusaaminen. Luettavissa: https://www.nuortennetti.fi/netti-ja-media/nettikiusaaminen/. Luettu: 29.9.2019.

Pehkonen, K. 2019. Leffapiraattien kurinpalautus – jälkinäytös: käsikirjoitus. Yle. Luettavissa: https://yle.fi/aihe/artikkeli/2019/01/29/leffapiraattien-kurinpalautus-jalkinaytos-kasikirjoitus. Luettu: 9.9.2019.

Piraattipuolue 2017. Kiristyskirje.fi. Luettavissa: http://www.kiristyskirje.fi/. Luettu: 9.9.2019.

Poliisi. Kyberrikollisuus. Luettavissa: https://www.poliisi.fi/rikokset/kyberrikollisuus. Luettu: 20.10.2019.

Poliisi 2016. Poliisin tilastot: vuosi 2016 nettipetokset. Luettavissa: https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/polisenaxwwwstructure/56209_Poliisin_tilastot_vuosi_2016_nettipetokset.pdf?456f6b9d1372d688. Luettu: 17.9.2019.

Poliisi 2018. Identiteettivarkaudet kasvussa - huolehdi henkilötiedoistasi! Luettavissa: https://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/identiteettivarkaudet_kasvussa_-_huolehdi_henkilotiedoistasi_70618. Luettu: 10.9.2019.

Poliisi 2019. TOR-verkossa 1.5. julkaistu uhkaus kauppakeskusta kohtaan. Luettavissa: https://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/tor-verkossa_1_5_julkaistu_uhkaus_kauppakeskusta_kohtaan_80170. Luettu: 20.9.2019.

Poliisiammattikorkeakoulu 2018a. Poliisin toimintaympäristö. Poliisiammattikorkeakoulun katsaus. Poliisiammattikorkeakoulu. Tampere. Luettavissa: https://www.theseus.fi/bitstream/handle/10024/155638/POLAMK%20Rap%20132_web.pdf?sequence=1&isAllowed=y. Luettu: 17.11.2019.

Poliisiammattikorkeakoulu 2018b. Poliisi (amk) opetussuunnitelma 2018–2020. Opetussuunnitelma. Poliisiammattikorkeakoulu. Tampere. Luettavissa: https://www.polamk.fi/instancedata/prime_product_julkaisu/intermin/embeds/polamkwwwstructure/61107_Poliisi_amk_ops.pdf?8709481261dbd588. Luettu: 3.11.2019.

Poliisihallitus 2019. Yrityksiin ja yhdistyksiin sataa valelaskuja – jopa harrastusseurat rikollisten kohteina. Luettavissa: https://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/yrityk-

siin_ja_yhdistyksiin_sataa_valelaskuja_jopa_harrastusseurat_rikollisten_kohteina_83699?fbclid=IwAR16lo5FiNrA0N5RxUC3UMGDp0EfXKOiXLTuBdY-RIk0lbO56MnB-TZstJg0. Luettu: 17.9.2019.

Porter, J. 2019. BBC News heads to the dark web with new Tor mirror. The Verge. Luettavissa: https://www.theverge.com/2019/10/24/20930085/bbc-news-dark-web-tor-the-onion-browser-secure-censorship. Luettu: 8.12.2019.

Puola, P. 3.11.2019. Sähköposti.

Ragan, S. 2018. What are phishing kits? Web components of phishing attacks explained. Luettavissa: https://www.csoonline.com/article/3290417/csos-guide-to-phishing-and-phishing-kits.html. Luettu: 11.9.2019.

Reiff, N. 2019. Were There Cryptocurrencies Before Bitcoin? Investopedia. Luettavissa: https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/. Luettu: 20.9.2019.

Reynard, C. 2018. The 10 most popular cryptocurrencies in 2018. The Telegraph. Luettavissa: https://www.telegraph.co.uk/technology/digital-money/top-10-popular-cryptocurrencies-2018/. Luettu: 20.9.2019.

Rikoslaki 39/1889.

Rikosuhripäivystys 2019a. Rakkauspetokset verkossa. Luettavissa: https://www.riku.fi/fi/erilaisia+rikoksia/omaisuusrikos/petokset/rakkauspetokset+verkossa/. Luettu: 19.9.2019.

Rikosuhripäivystys 2019b. Turvaohjeita nettiin. Luettavissa: https://www.riku.fi/fi/oppaat+ja+ohjeet/turvaohjeita+nettiin/. Luettu: 29.9.2019.

Sanastokeskus TSK ry 2018. Kyberturvallisuuden sanasto. Luettavissa: http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf. Luettu: 3.9.2019.

Sisäministeriö 2017. Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14/2017. Sisäministeriö. Helsinki. Luettavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf?sequence=1. Luettu: 28.12.2019.

Stammeier, J. & Jokelainen, L. 2017. Anonymous, Assange, Lauri Love – ovatko hakkerit internetin terroristeja vai vapaustaistelijoita? Yle. Luettavissa: https://yle.fi/aihe/artikkeli/2017/10/03/anonymous-assange-lauri-love-ovatko-hakkerit-internetin-terroristeja-vai#anonymous. Luettu: 10.9.2019.

Tanttari, S. 2018. Lasten seksuaalinen hyväksikäyttö netissä saa uusia muotoja. Luettavissa: https://www.haaste.om.fi/fi/index/lehtiarkisto/haaste32018/lastenseksuaalinenhyvaksikayttonetissasaauusiamuotoja.html. Luettu: 13.10.2019.

Tekijänoikeuden tiedotus- ja valvontakeskus 2019. Nettipiratismi. Luettavissa: https://ttvk.fi/piratismi/nettipiratismi. Luettu: 6.9.2019.

Trejtnar, E. 2019. Juristi vastaa: Mikä on identiteettivarkaus ja milloin se tulee rangaistavaksi? RIKU-lehti, 1/2019, s. 38-39.

Turvallisuuskomitea. Suomen kyberturvallisuusstrategia. Luettavissa: https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/. Luettu: 25.12.2019.

Turvallisuuskomitea 2017. Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020. Luettavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf. Luettu: 25.12.2019.