# Kyberrikollisuuden trendit nyt ja seuraavan kolmen vuoden aikana

Aku Limnell

10/2021

Poliisiammattikorkeakoulun opinnäytetyö / AMK

# TIIVISTELMÄ

**Aku Limnell: Kyberrikollisuuden trendit nyt ja seuraavan kolmen vuoden aikana**

**Opinnäytetyön muoto:** Tutkimuksellinen

**Julkisuusaste:** Julkinen

**Ohjaaja:** Jussi Hakaniemi ja Juha Nuortama

**Tutkinto:** Poliisi (AMK)

---

Tässä opinnäytetyössä käsitellään kyberrikollisuuden nykytilaa ja arvioidaan sen trendejä seuraavan kolmen vuoden aikana. Kyberrikollisuus on ollut kansallisesti ja globaalisti kasvussa usean vuoden ajan. Samanaikaisesti perinteinen rikollisuus on ollut maltillisessa laskusuunnassa. Kyberrikosten todellinen lukumäärä saattaa olla merkittävästi tilastoitua suurempi, koska suurta osaa kyberrikoksista ei ilmoiteta viranomaisille. Kyberrikoksen uhriksi voivat joutua yksittäiset henkilöt, yritykset ja organisaatiot. Kyberrikollisuudella aiheutetaan yhä suurempaa vahinkoa ja haittaa, ja rikollisuudesta on tullut entistä ammattimaisempaa ja järjestäytyneempää. Kyberrikollisuus elää jatkuvassa muutoksessa, ja kyberrikolliset keksivät koko ajan uusia toimintatapoja ja hyödyntävät entistä enemmän teknologiaa toiminnassaan. Kyberrikollisuus on monimuotoista ja arvaamatonta, mikä asettaa viranomaisille haasteita tulevaisuudessa.

Opinnäytetyössä on hyödynnetty laajasti ja monipuolisesti jo tehtyjä tutkimuksia, raportteja, viranomaisasiakirjoja ja uhka-arvioita. Tutkimuksessa käsitellään kyberrikollisuuden kehitystä, opinnäytetyön kannalta keskeisiä käsitteitä, lainsäädäntöä, keskeisiä toimijoita ja aiheuttajia. Työssä tarkastellaan myös kyberrikollisuuden tyypillisimpiä ilmiöitä ja tilannekuvan muodostumista. Varsinaiseen tutkimuskysymykseen eli *”Mitä kyberrikollisuuden trendejä on tällä hetkellä, ja mitä trendejä arvioidaan ilmenevän seuraavan kolmen vuoden aikana”* vastataan ”Nykytilanne” ja ”Tulevaisuuden trendit” -luvuissa.

Aineiston perusteella nykyisiä kyberrikollisuuden trendejä ovat kiristyshaittaohjelmat, virtuaalivaluutan louhintahaittaohjelmat, verkossa tapahtuvat lapsiin kohdistuvat seksuaaliväkivaltarikokset, petosrikokset, maksuvälinepetokset, erilaiset huijaukset, hajautetut palvelunestohyökkäykset, identiteettivarkaudet, tietomurrot sekä esineiden internetiin ja automaatiojärjestelmiin kohdistuvat rikokset. Kyberrikollisuudessa hyödynnetään rikollisten palveluteollisuutta (CaaS), tietojenkalastelua ja käyttäjän manipulointia.

Tutkimuksessa arvioidaan seuraavan kolmen vuoden kyberrikollisuuden trendeiksi kiristyshaittaohjelmat, kryptokaappaukset, verkkopetosrikokset, huijaukset ja automaatiojärjestelmiin ja IoT-laittei-

siin että toimitusketjuihin sekä logistiikkaan kohdistuvat hyökkäykset. Myös kyberaktivismia ja -vakoilua sekä lapsiin kohdistuvaa verkkorikollisuutta voidaan enteillä tuleviksi kyberrikostrendeiksi. Tulevaisuuden kyberrikollisuuden tekomuodoiksi estimoidaan tietojenkalastelua ja käyttäjän manipulointia. Kyberrikollisten arvioidaan tulevaisuudessa hyödyntävän yhä enemmän palveluteollisuutta, erilaisia salaustekniikoita, kryptovaluuttaa ja tekoälyä.

---

**Sivumäärä:** 86

**Tarkastuskuukausi ja vuosi:** Lokakuu 2021

**Avainsanat:** digitalisaatio, esineiden internet, haittaohjelmat, kirjallisuuskatsaukset, kyberrikollisuus, kyberturvallisuus, phishing, tietomurto, tietotekniikkarikokset, tietoverkkorikokset, verkkohyökkäykset

# SAMMANFATTNING

**Aku Limnell: Kyberrikollisuuden trendit nyt ja seuraavan kolmen vuoden aikana**

**Lärdomsprovets form:** Forskning

**Offentlighetsgrad:** Offentlig

**Handledare:** Jussi Hakaniemi och Juha Nuortama

**Examen:** Poliisi (AMK)

---

Detta lärdomsprov behandlar nuvarande och följande tre års cyberbrottslighetstrender. Lärdomsprovet är en litteraturöversikt där redan gjorda undersökningar och rapporter kan nyttjas. Narrativ litteraturöversikt möjliggör att bred och mångsidigt material kan användas i denna undersökning. I lärdomsprovet behandlas cyberbrottslighetens utveckling, centrala begrepp i lärdomsprovet, lagstiftning gällande cyberbrottslighet samt centrala aktörer och upphovsmän. Dessutom behandlas situationsbilden och typiska fenomen. Lärdomsprovet koncentreras på cyberbrottslighetens nuvarande tillstånd samt kommande tre års trender. I tidigare nämnda kapitel svaras det på lärdomsprovets undersökningsfråga, det vill säga hurdana cyberbrottslighetstrender finns det just nu och hurdana det kan utvärderas förekomma i följande tre år.

I dagsläget är bland annat överbelastningsangrepp, skadligt program, utpressningsprogram, kryptokapning, CSE (sexuellt utnyttjande av barn), olika svindlerier, nätfiske och dataintrång populära. Enligt framtidens utvärderingar kan CaaS-industri (tjänster köps eller byts mellan andra aktörer) växas och sakernas internetapparater riktas med olika hot. Leverans- och logistikkedjor kan attackeras. Det bedöms att överbelastningsangrepp, utpressningsprogram, nätfiske, datasäkerhetingrepp och kryptomining förekommer i framtiden på samma sätt som i dagens läge. Cyberbrottslingar kan utnyttja artificiell intelligens i cyberbrottslighet och haktivism kan ökas.

---

**Sidantal:** 86

**Månad och år då granskningen skett:** oktober 2021

**Nyckelord:** cyberbrottslighet, cyberattacker, databrott, dataintrång, datanät, digitalisering, informations- och kommunikationsbrott, litteraturöversikter, nätbrott, nätfiske, sakernas internet

# SISÄLLYS

# 1 JOHDANTO

”Kyberrikollisuus voi pahimmillaan uhata Suomen kansallista turvallisuutta, vaikka rikollisten tavoitteena on ensisijaisesti hankkia rahaa” (Suojelupoliisi, luettu 14.10.2021).

Elämme tiedostamattamme jatkuvasti muuttuvassa kompleksisessa kybermaailmassa. Käytämme päivittäin tietokoneita, älypuhelimia, sosiaalista mediaa ja sähköpostia, mistä syystä kybermaailmasta on tullut osa arkipäiväämme. Teknologia ja digitalisaatio kehittyvät valtavin harppauksin ja muutoksessa on vaikea pysyä mukana. Teknologian kehittymisen ennakointi on vaikeaa, sillä kehitysnopeus vaihtelee aloittain ja se voi olla epätasaista.

Kyberympäristö vaatii kaikilta käyttäjiltä jatkuvaa osaamisen kehittämistä ja ratkaisujen löytämistä, jotta voidaan välttyä ongelmilta ja rikollisuudelta. Kyberturvallisuuden avulla pyritään varautumaan kyberuhkiin ja hallitsemaan niiden aiheuttamia häiriöitä. Datat, bitit, tietoverkot ja tietotekniikka antavat ihmisille uusia mahdollisuuksia, minkä takia etenkin kyberturvallisuuteen tulisi kiinnittää huomiota. Teknologian käyttö kasvaa nopeasti ja tuo mukanaan uusia uhkia. Laajat tietomurrot, huijaukset, kalasteluohjelmat ja kiristyshaittaohjelmat kuuluvat nykypäivän kyberrikollisuuteen.

Kybertoimintaympäristön jatkuva muutostila ja kehitys avaavat myös uusia mahdollisuuksia rikollisille. Tässä tutkimuksessa pyritään kuvaamaan jo tehtyjen tutkimusten ja raporttien avulla kyberrikollisuuden nykytilaa ja arvioimaan sen trendejä seuraavan kolmen vuoden aikana poliisialan kontekstissa.

## 1.1 Kyberrikollisuuden esittely ja tutkimuksen ajankohtaisuus

”Kyberrikollisuus on tieto- ja viestintäjärjestelmiin kohdistuvaa tai niitä hyväksikäyttäen tehtyä rikollisuutta” (CYBERDI 2021, 3). Kyberrikollisuudesta voidaan käyttää myös nimitystä tietotekniikkarikollisuus, ja periaatteessa kaikki rikokset, joissa on käytetty tietotekniikkaa tai tietoverkkoja hyväksi, voivat olla kyberrikollisuutta. Yleisimpiä rikostyyppejä ovat omaisuusrikokset kuten petokset ja maksuvälinepetokset, sekä rahanpesu- ja kiristysrikokset (Sisäministeriö 2021, luettu 28.9.2021). Kyberrikollisuus muuttuu jatkuvasti, ja merkkejä sen järjestäytyneestä toiminnasta on ollut havaittavissa. Kyberrikollisuuden määrä on kasvanut jatkuvasti, ja tekojen vaikutukset muun muassa yrityksille vaihtelevat tapauskohtaisesti vähäisestä kriittiseen (CYBERDI 2021, 3). Kybertoimintaympäristön jatkuva muutos, kansainvälistyminen sekä rikollisten uudet toimintatavat ja -muodot luovat poliisille suuria haasteita tulevaisuudessa. Tuottoisin rikollisuus toimii tietoverkoissa (Sisäministeriö 2017, 5).

Kyberalan ajankohtaisuus näkyy siinä, että kybermaailmasta, -turvallisuudesta ja -rikollisuudesta uutisoidaan yhä enemmän. Myös poliisin viestinnässä kyberrikollisuus on ollut aiempaa enemmän

esillä. Digitalisaation ulottuvuus on tuonut erilaiset palvelut ja mahdollisuudet lähemmäksi jokaista verkonkäyttäjää. Ajankohtaisuus on näkynyt myös Poliisiammattikorkeakoulun kyberalaan liittyvien opinnäytetöiden lukumäärässä, joita on viimeisten vuosien aikana tehty enemmän kuin aiemmin. Poliisiammattikorkeakoulun roolia on nostettu kyberrikostorjuntaosaamisessa muun muassa lisäämällä kyberasioiden opetusta poliisin peruskoulutukseen, tarjoamalla kyberrikostorjuntaan erikoistuville laadukasta erityiskoulutusta, kehittämällä koulutus- ja tutkimusyhteistyötä viranomaisten, yliopistojen ja korkeakoulujen kanssa sekä lisäämällä kyberalan tutkimusta (Sisäministeriö 2017, 6).

Poliisihallinnon lisäresurssit sekä kyberturvallisuuden osaamisen tarpeen kehittäminen, johtaminen, suunnitteleminen ja varautuminen on huomioitu vuoden 2019 Suomen kyberturvallisuusstrategiassa (Turvallisuuskomitea 2019). Poliisissa on panostettu kyberosaamisen lisäämiseen, torjuntaan ja tutkintaan. Kyberrikosten tutkinta on haastavaa muun muassa niiden ilmoittamatta jättämisen, alhaisen kiinnijäämisriskin ja häpeän tunteen pelon takia (CYBERDI 2021, 3) sekä kustannustehokkaan toteutustavan ja alhaisten seurausten takia (Cyberwatch Q1 2021, 10). Useasti tekijät ovat Suomen ulkopuolelta ja heidän jäljittämisensä vie huomattavan paljon aikaa ja resursseja.

Kyberrikollisuus elää jatkuvassa kehityksessä ja muutoksessa. Muutos näkyy siinä, että rikolliset käyttävät ja hyödyntävät toiminnassaan vanhoja ja uusia toimintatapoja. Rikoksentekijät keksivät jatkuvasti kehittyneempiä rikoksentekomuotoja ja hyödyntävät nopeaa kehitystä ja haavoittuneisuuksia. Kyberrikollisuustrendit elävät täten jatkuvassa muutoksessa rinnakkain nopean kehityksen kanssa. Kyberhyökkäyksiä tehdään yhä enemmän, ne ovat yhä monimutkaisempia ja haasteellisia puolustaa. Rikolliset hyödyntävät tekemättömien päivitysten ja muutosten aikaikkunaa. (VNST 2017, 12.)

Yhä suurempi osa poliisin tietoon tulleista rikoksista tehdään tietoverkoissa tai tietojärjestelmissä. Huomion arvoista on se, että kyberrikollisuuden teoista suuri osa ei tule poliisin tietoon, ja rikokset, joista poliisi käynnistää esitutkinnan, jäävät usein selvittämättä tai selviävät vain osittain (Sisäministeriö 2021, luettu 28.9.2021). Tietoverkkorikollisuus ja sen eri tekomuodot ovat jatkuvassa kasvussa (Sisäministeriö 2017, 45), kun perinteinen rikollisuus on maltillisessa laskusuunnassa (Cyberwatch Q1 2021, 3).

Poliisin on varauduttava ja pidettävä riittävän ajankohtaista tilannekuvaa sekä nykytilasta että lähitulevaisuuden kyberrikollisuuden trendeistä poliisin luottamuksen säilyttämiseksi myös kybertoimintaympäristössä. Tämän tutkimuksen aihe on yhteiskunnallisesti ja tieteellisesti merkittävä ja kiinnostava. Tutkimuksessa on tarkoitus käydä läpi kyberrikollisuuden keskeiset käsitteet, toimijat ja tekijäpiiri sekä voimassa oleva kansallinen lainsäädäntö, kyberrikollisuuden ilmiöt ja tilannekuvan muodostaminen. Tutkimuksessa keskitytään kyberrikollisuuden nykytilaan ja seuraavan kolmen vuoden trendeihin.

## 1.2 Tutkimuksesta ja tutkimuksen tavoitteet

Tutkimuksen on tarkoitus olla julkinen, ja sillä tavoitellaan poliiseja, etenkin kyberrikoksia tutkivia poliiseja, ja muita kyberalalla työskenteleviä henkilöjä. Tutkimusta voidaan hyödyntää Poliisiammattikorkeakoulun koulutuksessa ja opetuksessa. Nykyisessä työpaikassani Ahvenanmaan poliisiviranomaisessa ei ole yhtään kyberasioihin perehtynyttä poliisimiestä tai siviilihenkilöä. Tutkimuksen tarkoituksena on kehittää omaa osaamista kyberasioissa.

Tutkimuksen laatiminen kyberrikollisuuden trendeistä edellyttää perehtymistä koko kyberalaan, etenkin kyberrikollisuuteen ja sen aikaisempiin ja nykyisiin ilmiöihin. ”Kyber” sanana luo helposti ennakkoluuloja, ja yleisesti ajatellaan sen sisältävän ammattimaista tietotekniikkaosaamista ja koodaamista sekä erityisasiantuntemusta tietoverkoista. ”Kyber” etuliitteenä on verrattain uusi, ja sen käytön voidaan katsoa alkaneen nykyisessä merkityksessään Yhdysvalloissa 1990-luvulla (Sisäministeriö 2017, 11). Kyber-alkuiset käsitteet ovat paljon muutakin, ja ne ovat osa jokaisen arkipäivää. Nykyään tietoverkot ovat olennainen osa rikollisuuden ja rikostorjunnan toimintaympäristöä, ja yhä suurempi osa poliisille ilmoitettavista rikoksista tapahtuu tietoverkoissa tai tietojärjestelmissä (Sisäministeriö 2021, luettu 28.9.2021).

Kyberrikollisuuden piirteet ovat mielenkiintoisia, koska esille nousee jatkuvasti uusia tapoja, vaikka myös vanhat tavat säilyttävät asemansa osana kyberrikollisuutta. Kyberrikollisuus on jatkuvasti ammattimaisempaa ja kansainvälisempää rikollisuutta. Kyberrikollisuus on kokonaisuutena varsin laaja, joka pitää suuren määrän eri osa-alueita sisällään. Opinnäytetyöprosessi tulee kasvattamaan ja laajentamaan omaa osaamistani ja tietämystäni kyberrikollisuudesta. Tutkimus edellyttää perehtymistä eri viranomaisten ja yksityisten sektorien turvallisuusalan yritysten asiakirjoihin, ja tutkimuksessa on tarkoitus hyödyntää suomenkielisen aineiston lisäksi englannin- ja ruotsinkielisiä aineistoja.

Uskon kyberrikollisuuden vaikutuksen poliisitoimintaan lisääntyvän tulevaisuudessa, mikä erityisesti motivoi minua tutkimuksen tekijänä ja poliisina. Aihe on minusta yhteiskunnallisesti erittäin ajankohtainen ja kiinnostava, mikä luo mielenkiintoisia haasteita ja motivoi ja auttaa tutkimuksen tekemisessä. Tutkimuksen on tarkoitus myös osoittaa minun kykenevän tutkimustyön tekemiseen. Tämän tutkimuksen tavoitteena on tuottaa tietoa kyberrikollisuuden nykytilasta, ja arvioida kyberrikollisuuden trendejä lähitulevaisuudessa.

## 1.3 Tutkimuskysymys

Tämän opinnäytetyön tutkimusmenetelmäksi valittiin kirjallisuuskatsaus, josta tarkemmin seuraavassa luvussa. Kirjallisuuskatsauksessa asetetaan tutkimusongelma, johon pyritään jo tutkittua tietoa keräämällä löytämään vastaus. Tämä edellyttää, että aiheesta on riittävästi tietoa saatavilla.

Ennen tämän tutkimuksen aloittamista suoritettiin esitiedonhakua riittävän aineiston saatavuuden kartoittamiseksi. Voitiin todeta, että aiheesta on riittävästi tietoa saatavilla ja siten tutkimusongelmaan on edellytyksiä vastata. Suunnittelussa selkeytyi itse tutkimusongelma ja sitä kautta tutkimuskysymys. Voidaan sanoa, että suunnitteluvaihetta pitkälti ohjaa tutkimuskysymys.

Tutkimuskysymyksen asettamisella pyritään välttämään mitättömän nollatutkimuksen tuottaminen. Tutkimuskysymys on tarkoitus esittää yhdellä lauseella, mahdollisimman tiiviisti. Tutkimusongelmana on etsiä tietoa, kerätä sitä ja arvioida kyberrikollisuuden trendejä seuraavan kolmen vuoden aikana. Täten tutkimuskysymys voidaan asettaa muotoon: ”*Mitä kyberrikollisuuden trendejä on tällä hetkellä, ja mitä trendejä arvioidaan ilmenevän seuraavan kolmen vuoden aikana?”*

Tutkimuskysymys asettaa lähtökohdat tutkimukselle ja auttaa tutkimusprosessin aikana muun muassa aineiston hankinnassa, käsittelyssä ja analysoinnissa. Tutkimusprosessin lopussa tarkastellaan, onko todella vastattu siihen tutkimuskysymykseen, joka tutkimuksen suunnitteluvaiheessa asetettiin.

# 2 TUTKIMUSMENETELMÄT JA TUTKIMUKSEN RAKENNE

Tutkimusmenetelmän valinta oli aihevalintapäätöksen jälkeen epäselvä, koska pohdintaa käytiin kvalitatiivisen haastattelututkimusmenetelmän ja kirjallisuuskatsaustutkimusmenetelmän välillä. Vallitsevan Covid-19-pandemian ja runsaan aineiston saatavuuden takia päädyttiin kirjallisuuskatsaukseen. Kirjallisuuskatsaus on tutkimusmenetelmänä kvalitatiivisen ja kvantitatiivisen metodin yhdistelmä (Salminen 2011, 4). Tässä luvussa tarkastellaan opinnäytetyön tutkimusmenetelmiä, aihetta ja tutkimuksen rakennetta.

## 2.1 Kirjallisuuskatsaus

Kirjallisuuskatsaus on tieteellinen tutkimusmenetelmä ja metodi, jossa tutkitaan jo tehtyjä tutkimuksia ja jonka avulla voidaan arvioida teoriaa, rakentaa kokonaiskuvaa tietystä asiakokonaisuudesta, tunnistaa ongelmia ja kuvata tietyn teorian kehitystä historiallisesti. Kirjallisuuskatsausta voidaan lähestyä pidättäytymällä omalla tieteenalan alueella ja pyrkimällä antamaan tämän alueen tutkijoiden tuottamasta aineistosta kehityskuva. (Salminen 2011, 1–3.)

Kirjallisuuskatsauksen perustyypeistä yksi on systemaattinen kirjallisuuskatsaus, jossa tietyn aihepiirin aiempien tutkimusten olennaisesta sisällöstä tehdään tiivistelmä. Toinen perustyypeistä on kuvaileva kirjallisuuskatsaus, jota voidaan luonnehtia yleiskatsaukseksi ilman tiukkoja ja tarkkoja sääntöjä. (Salminen 2011, 6 ja 9.)

Tutkimuksen tavoitteena on koostaa tietoa kyberrikollisuuden nykytilasta sekä tehdä arvio seuraavan kolmen vuoden kyberrikollisuustrendeistä. Tarkoituksena on kerätä tutkittavasta aiheesta olevaa tietoa huolellisen suunnittelun sekä edustavan ja luotettavan aineiston valitsemisen avulla. Tiedonkeruun kriteereiksi tässä työssä asetetaan ajankohtaisuus, luotettavuus ja yhteys tutkimusongelmaan. Lisäksi aineistossa hyödynnetään suomen-, ruotsin- ja englanninkielisiä julkaisuja. Tutkimuksessa on tarkoituksena käyttää lähteinä tieteellistä tietoa, oikeustietoa, raportteja, arvioita ja muuta kirjallisuutta. Aineisto koostuu pääosin viranomaisten asiakirjoista.

Systemaattisessa kirjallisuuskatsauksessa tutkimusta tehdään ja analysoidaan jo tehdyn aineiston pohjalta. Systemaattinen kirjallisuuskatsaus on menetelmältään jäykempi kuin kuvaileva kirjallisuuskatsaus. Systemaattisuus edellyttää aineistolta paljon, ja sitä ohjaavat säännöt ovat tiukat. Tutkimuksessa käytettävät aineistot eivät välttämättä täytä kaikkia systemaattisen kirjallisuuskatsauksen sääntöjä, mistä syystä kuvaileva kirjallisuuskatsaus sopii tämän opinnäytetyön tutkimusmenetelmäksi paremmin.

Kuvailevassa kirjallisuuskatsauksessa aineistot voivat olla laajoja ja aineiston valintaa eivät rajoita metodiset säännöt. Tutkittava ilmiö voidaan kuvata laaja-alaisesti, ja tutkimuskysymykset voivat olla väljempiä kuin systemaattisessa katsauksessa. Kuvailevasta katsauksesta voidaan käyttää nimitystä traditionaalinen kirjallisuuskatsaus, joka toimii itsenäisenä metodina, mutta sen katsotaan tarjoavan uusia tutkittavia ilmiöitä systemaattista kirjallisuuskatsausta varten. (Salminen 2011, 6.)

Tutkimuksessa käytettiin aineistoa laajasti, koska kyberala ja tämän tutkimuksen aineiston sisältö elävät jatkuvassa muutoksessa. Ajankohtaisen tutkimustiedon hankkiminen ja kirjaaminen edellyttivät useiden verkkolähteiden käyttöä. Kuvaileva kirjallisuuskatsaus antaa tutkimuksen tekijälle enemmän liikkumavaraa eikä se rajoita tiukoilla säännöillään aineiston valintaa tai laajuutta. Tutkimuksen tutkimuskysymys on melko väljä, joten kuvaileva kirjallisuuskatsaus sopii tässäkin mielessä oikeaksi tutkimusmenetelmäksi. Tässä tutkimuksessa on tarkoituksena käyttää kuvailevaa kirjallisuuskatsausmenetelmää.

Kuvailevasta kirjallisuuskatsauksesta erottuu kaksi orientaatiota, joista toinen on narratiivinen katsaus. Narratiivinen kirjallisuuskatsaus on metodisesti kevyin kirjallisuuskatsauksen muoto, jonka avulla pystytään antamaan laaja kuva käsiteltävästä aiheesta tai kuvailemaan käsiteltävän aiheen historiaa ja kehityskulkua. (Salminen 2011, 6–7.) Narratiivinen kirjallisuuskatsaus mahdollistaa aineiston laajan ja monipuolisen käytön, mikä on edellytyksenä tämän tutkimuksen tekemiselle, koska tutkimuksen aihe elää jatkuvassa muutoksessa ja kehityksessä. Tässä tutkielmassa selvitetään mihin kyberrikollisuustrendeihin poliisin olisi syytä kiinnittää tällä hetkellä huomiota ja minkälaisiin trendeihin tulisi valmistautua lähitulevaisuudessa. Opinnäytetyöllä pyritään luomaan laaja kuva kyberrikollisuudesta, kyberrikollisuuden ilmiöistä ja sen kehityskulusta.

Kirjallisuuskatsaus tarjoaa mahdollisuuden käsitellä ja tiivistää laajoja aineistoja, ja se palvelee tieteenalan tuntemusta (Salminen 2011, 22). Tutkimustuloksia voidaan hyödyntää tieteellisessä jatkotutkimuksessa, poliisin koulutuksessa, kyberrikollisuuden torjunnassa ja tutkinnassa sekä kybertoimintatapojen kehittämisessä ja ennaltaehkäisemisessä. Tutkimuksessa arvioidaan nykytilan lisäksi kyberrikollisuuden lähitulevaisuuden trendejä, jolloin tarkoituksena on kirjallisuustutkimusmenetelmän lisäksi hyödyntää tulevaisuudentutkimusta.

## 2.2 Tulevaisuudentutkimus

Tulevaisuudentutkimuksella tarkoitetaan tieteenalaa, joka perustuu monien tulevaisuuden kehitysmahdollisuuksien tutkimiseen (Kuusi ym. 2013, 331). ”Tulevaisuudentutkimus tuo esille, mikä on mahdollista, mikä on todennäköistä ja mikä on toivottavaa tai ei-toivottavaa” (Turun yliopisto, luettu 25.10.2021). Tässä opinnäytetyössä on tarkoitus hyödyntää tulevaisuudentutkimusta arvioitaessa mahdollisia ja todennäköisiä kyberrikollisuuden trendejä seuraavan kolmen vuoden aikana.

Tulevaisuuden ennakointi on käytännönläheinen osa tulevaisuuden tutkimusta, jolla voidaan arvioida trendien kehityskulkua jollain oletetulla todennäköisyyden asteella määrätyn ajanjakson kuluessa. Kehityskululla eli ennusteella tulkitaan tulevaisuuksientutkimuksessa toimijan sivustakatsojan näkemykseksi kehityskulusta, johon hän ei voi vaikuttaa. Trendillä tarkoitetaan tietyn ajanjakson kuluessa tapahtuvaa tarkasteltavan ilmiön yleistä kehityssuuntaa. (Kuusi ym. 2013, 324 ja 331.)

Opinnäytetyössä on tarkoitus käytännönläheisesti ennakoida tulevia trendejä. Ennakoinnissa on tarkoitus havaita ja hyödyntää kyberrikollisuuden menneisyyden ja nykyisyyden trendejä. Viranomaisten asiakirjoissa on tehty arvioita tulevista kyberrikollisuuden trendeistä, joita on tarkoitus sivustakatsojan roolissa koostaa objektiivisesti, ja siten muodostaa arvio trendien kehityskulusta ja -suunnasta. Trendien tarkastelun ajanjaksoksi on asetettu seuraavat kolme vuotta.

Tulevaisuuden ennakoinnissa voidaan hyödyntää heikkoja signaaleja, joilla tarkoitetaan merkkejä nousevista asioista, joista voi tulevaisuudessa tulla jokin trendi tai ei. Heikkojen signaalien periaatteen mukaan yksi signaali ei vielä kerro mitään, mutta lukuisat samaan suuntaan viittaavat signaalit voivat jo kertoa tulevaisuuden kasvavasta trendistä. (Hiltunen 2013, 296 ja 299.)

Tutkimuksessa on tarkoitus kerätä useista eri viranomaisasiakirjoista näkemyksiä tulevaisuuden näkymistä. Tutkimuksen lopputuloksen kannalta on tärkeää, että onnistutaan keräämään riittävästi heikkoja signaaleja uusista asioista ja ilmiöistä sekä havaitsemaan merkittäviä trendejä nykyisessä kehityksessä. Tarkoituksena on tutkia ja analysoida havaittuja heikkoja signaaleja orastavista uusista ilmiöistä laajasti ja eri lähteistä. Analysoitu aineisto koostetaan lopuksi arvioksi tulevaisuuden kyberrikollisuuden trendeistä.

## 2.3 Aihe ja rajaaminen

Tässä opinnäytetyössä keskitytään kyberrikollisuuteen ja päähuomiona on arvioida kyberrikollisuuden trendejä nyt ja seuraavan kolmen vuoden aikana, tarkemmin ottaen vuosina 2021–2024. Kyberrikollisuuden viitekehyksessä kolme vuotta on pitkä aikaväli, koska kybermaailma elää jatkuvassa muutoksessa ja nopeassa kehityksessä. Teknologia ja digitalisaatio kehittyvät valtavin harppauksin, ja niiden vauhdissa pysyminen aiheuttaa haasteita pidempää aikaväliä arvioitaessa. Tekniikasta, kuten kulutustavaroista, viestintätavoista ja eri pankkipalveluista, tulee yhä älykkäämpää. Kun miettii teknologiaa 10–20 vuotta taaksepäin, on kehitys ollut tähän päivään tultaessa päätä huimaavaa. On lähes mahdotonta sanoa, kuinka paljon teknologia ja digitalisaatio kehittyvät seuraavan 5–10 vuoden aikana. Näistä syistä johtuen tutkimuksessa keskitytään seuraavaan kolmeen vuoteen.

Tavoitteena on luoda lukijalle yleiskuva tämän hetken ja lähitulevaisuuden kyberrikollisuudesta. Kyberrikollisuus on ollut vahvasti julkisuudessa vuosina 2020–2021. Voidaan nostaa esille muun muassa paljon julkisuutta vuonna 2020 kerännyt psykoterapiakeskus Vastaamon laaja tietomurto, eduskuntaan kohdistunut kyberhyökkäys vuonna 2020 ja kybervakoiluoperaatio vuonna 2021. Tulevaisuuden ja kehityksen ymmärtämiseksi on tehtävä katsaus kyberrikollisuuden nykytilasta. Pääpaino on kuitenkin tutkimuksessa vuodessa 2021 ja seuraavassa kolmessa vuodessa. Kyberrikollisuuden lähitulevaisuuden trendeistä voidaan tehdä arvioita ja ennusteita, joita juuri tämän tutkimuksen tuloksen avulla pyritään tuomaan tiivistäen esille.

Katsauksen kirjaaminen nykytilasta ja lähitulevaisuudesta edellyttää kybertoimintaympäristön avaamista. Kybertoimintaympäristö muodostuu monimutkaisista ja -kerroksisista informaatioverkoista, joihin kuuluvat muun muassa kansallisen julkishallinnon ja turvallisuusviranomaisten kommunikaatioverkot ja ohjausjärjestelmät. Nämä informaatioverkot muodostavat internetin välityksellä maailmanlaajuisen verkoston (VNST 2017, 65).

Kyberrikollisuus ja siihen liittyvät seikat muodostavat yhdessä valtavan laajan kokonaisuuden, minkä takia tutkimus on rajattava tarkasti. Tutkimusta lähestytään poliisin viitekehyksestä, joten muiden viranomaisten ja yksityisten toimijoiden näkökulmat jätetään tarkemmin käsittelemättä. Kyberturvallisuus on erittäin laaja aihekokonaisuus, joten tässä työssä sitä lähestytään lähinnä kyberrikollisuuden kontekstissa. Kyberrikollisuuden keskeisiä toimijoita poliisissa ovat Keskusrikospoliisin kyberrikostorjuntaan keskittynyt kyberrikostorjuntakeskus ja paikallispoliisit eli poliisilaitokset, joita tarkastellaan tässä tutkimuksessa kyberrikollisuuden viitekehyksessä. Kyberrikostorjunnan kyvykkyyteen, koulutuksiin, laitteistoihin tai ohjelmistoihin ei ole syytä mennä sen tarkemmin. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus laatii yksityisen sektorin ohella tilanneraportteja kyberrikollisuudesta ja sen tilasta. Poliisin ulkopuolisista toimijoista Kyberturvallisuuskeskus on yksi

keskeisimmistä kyberrikosviranomaista, jotka tekevät yhteistyötä poliisin kanssa. Tutkimuksessa käydään läpi myös Europolin vuosittainen tilannekuvaraportti kyberrikollisuuden osalta, mikä edellyttää Europolin European Cybercrime Centren (EC3) toiminnan kuvaamista.

Kyberrikollisuuteen liittyvät keskeisesti tietoverkot ja digitalisaatio, joita tutkimuksessa on osittain tarkasteltava kokonaisuuden ymmärtämiseksi. Opinnäytetyössä avataan keskeistä kyberrikollisuuden tekijäpiiriä, kuten kybervandaaleita, kybervakoilijoita, -sotilaita ja -terroristeja. Kyberrikollisuusalaa pidetään kompleksisena ja vaikeana, mistä syystä tässä opinnäytetyössä avataan muutamia keskeisiä ilmiöitä ja peruskäsitteitä. Aihe on kokonaisuudessaan laaja, mikä edellyttää rajaamisen ainoastaan keskeisiin peruskäsitteisiin. Käsitteiden ja ilmiöiden avaamisen tarkoituksena on helpottaa lukijaa ymmärtämään opinnäytetyötä. Täten lukijalle pyritään hahmottamaan, mistä kyberrikollisuudesta on kyse ja millaisia yleispiirteitä siihen liittyy.

Raja rikollisuuden ja kyberrikollisuuden välillä ei ole täysin selvä, minkä takia tutkimuksessa on syytä keskittyä myös soveltuvin osin lainsäädäntöön. Kyberrikokselle ei ole erillistä määritelmää rikoslaissa, mutta monet kyberrikoksiksi mielletyt teot löytyvät rikoslain 38 luvusta (CYBERDI 2021, 5). Liikenne- ja viestintäministeriö on vuonna 2020 asettanut työryhmän, jonka tehtävänä on kartoittaa yhteiskunnan toiminnan kannalta keskeisten toimialojen tietoturvaa ja tietosuojaa koskevan lainsäädännön muutostarpeita (Liikenne ja viestintäministeriö 9.11.2020, luettu 14.10.2021). Lisäksi kyberrikollisuuden viitekehyksessä on olemassa runsaasti kansainvälistä lainsäädäntöä.

### 2.4 Rakenne

Tutkimuksen ensimmäinen luku koostuu johdannosta, jossa tuodaan esille tutkimuksen ajankohtaisuus, tutkimuksen tausta ja tarkoitus. Luvussa käsitellään tutkimuksen tavoitetta, tutkimuskysymystä ja -ongelmaa sekä esitellään lyhyesti kyberrikollisuus.

Toisessa luvussa tarkastellaan valittua tutkimusmenetelmää eli kirjallisuuskatsausta sekä tulevaisuudentutkimusta. Lisäksi luvussa tarkastellaan opinnäytetyön aihetta, rajaamista ja rakennetta.

Kolmas luku pitää sisällään lyhyen kybermaailman kehityskulun tarkastelun sekä tutkimuksen keskeiset käsitteet. Käsitteiden merkityksen voidaan katsoa olevan suuri, koska tutkimus rakentuu niiden ympärille ja ne määrittelevät osittain aineiston hankinnan. Käsitteistä voidaan mainita muun muassa kyberrikollisuus, -turvallisuus, -uhkat ja -toimintaympäristö. Luvussa käsitellään niukasti kyberrikollisuuteen liittyvää lainsäädäntöä ja tietoverkkorikoksia. Kyberrikollisuuden ja tavallisten fyysisten rikosten välinen raja ei aina ole yksiselitteinen. Lisäksi luvussa paneudutaan keskeiseen kyberrikollisuuden tekijäpiiriin eli rikollisiin ja keskeisiin toimijoihin eli kyberrikollisuuden torjujiin. Tekijäpiiriin kuuluvat muun muassa kybervandaalit, -terroristit ja -sotilaat. Toimijoista tarkastellaan lähemmin muun muassa Keskusrikospoliisin kyberrikostorjuntakeskusta.

Neljännessä luvussa käsitellään kyberrikollisuuteen liittyviä keskeisiä ilmiöitä. Luvussa pyritään selventämään, että kyberrikollisuuden kohteena voi olla yksityinen henkilö, yritys tai organisaatio. Yleisimpiä ilmiöitä ovat muun muassa haittaohjelmat, palvelunestohyökkäykset, hakkerointi ja tietojenkalastelu. Luvussa myös tarkastellaan kyberrikollisuuden tilannekuvaa - lähinnä selvennetään, miten tilannekuva muodostetaan, ketkä muodostavat tilannekuvaraportteja tai -arvioita ja millaisia arvioita tilannekuvaraporttien pohjalta voidaan tehdä.

Viidennessä luvussa tarkastellaan kyberrikollisuuden nykytilaa. Luvussa tarkastellaan vuosien 2018–2021 kyberrikollisuuden ilmiöitä ja trendejä. Luvussa tuodaan esille millaisia tapoja tai keinoja kyberrikolliset ovat käyttäneet viime vuosina.

Kuudennessa luvussa käsitellään lähivuosien kyberrikollisuuden trendejä. Viidennessä ja kuudennessa luvussa vastataan varsinaiseen tutkimusongelmaan eli mitä kyberrikollisuuden trendejä on nyt, ja mitä trendejä arvioidaan olevan seuraavan kolmen vuoden aikana.

Seitsemännessä luvussa tehdään yhteenveto kyberrikollisuuden trendeistä vuonna 2021 ja arvioiduista trendeistä vuosina 2022–2024. Luvussa esitellään tiivistetysti kerättyä aineistoa ja analysointia sekä niiden vaikutusta kyberrikostorjuntaan.

Viimeisessä luvussa on lyhyttä pohdintaa ja tuodaan esille tutkimukseen kohdistuva kriittisyys.

# 3 KYBERRIKOLLISUUS

Kyberrikollisuuden ensivaiheiden voidaan katsoa sijoittuvan 1940-luvun lopulta 1960-luvun loppuun. Ajanjaksoa voidaan pitää tietokonerikollisuuden syntyhetkenä. Omaa kyberlainsäädäntöä ei vielä ollut, ja rikokset tehtiin lähinnä fyysisesti vahingoittamalla tietokoneita. Seuraavan vaiheen voidaan katsoa sijoittuvan 1970-luvulta 1980-luvun lopulle, jolloin tietokonerikokset kehittyivät ja lainsäädäntöön alettiin kiinnittää huomiota. (Peltomäki & Norppa 2015, 38.)

Kybervandalismin ja hakkeroinnin voidaan katsoa alkaneen 1986, kun pakistanilaisveljekset kehittivät tietokoneviruksen nimeltä Brain (Lehto 2021, 49). Kolmannen vaiheen voidaan sanoa käynnistyneen 1990-luvulla, jolloin internetin käyttö yleistyi, mikä mahdollisti entistä monipuolisempien rikosten tekemisen. Tällöin alettiin kiinnittää huomiota tietotekniikkarikosten lainsäädäntöön. (Peltomäki & Norppa 2015, 38.)

Aiemmin kyberrikollisuudella ei siis ollut laeissa omia rikosnimikkeitä eikä ollut merkitystä sillä, miten rikos tehtiin tai kohdistuiko se tietojärjestelmiin. Suomen rikoslain (39/1889) 38 luku muodostettiin nimellä ”Tieto- ja viestintärikoksista” vuonna 1995. Internetin käyttö laajeni voimakkaasti 1990-

luvulla ja yhteiskunnan sektorit tulivat riippuvaisiksi sähköisestä tiedonkäsittelystä, viestintäverkoista ja näitä toimintoja tukevasta infrastruktuurista. (Sisäministeriö 2017, 11.)

Vuonna 2000 ilmestyivät ensimmäiset ammattilaisten haittaohjelmat (Lehto 2021, 49). 2000-luvulla tietokonerikollisuus jatkoi kasvuaan, ja rahaa tekevät haittaohjelmat ilmestyivät vuosina 2002–2004. Interpolin mukaan vuonna 2012 amerikkalaispankeista ryöstettiin 900 miljoonaa dollaria perinteisillä menetelmillä ja kyberrikoksilla 12 miljardia dollaria. Vuonna 2013 kyberrikollisuudessa liikkui Interpolin mukaan enemmän rahaa kuin huumekaupassa. Britanniassa yli 90 prosenttia suurista yrityksistä joutui vuonna 2012 kyberrikollisten hyökkäyksen kohteeksi. (Peltomäki & Norppa 2015, 40.)

Myös Suomessa havaittiin kybertoimintaympäristön aiheuttamat riskit ja uhat. Suomen vuoden 2013 kyberturvallisuusstrategiassa tavoiteltiin, että Suomi olisi vuonna 2016 maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa (Turvallisuuskomitea 2013, 3). Kyberrikollisuus on kansallinen ja kansainvälinen haaste. Kyberrikollisuuden kasvu on nostattanut huolen kybermaailmassa liikkumisen turvallisuudesta. Kybertoimintaympäristössä liikkumisen voidaan katsoa perustuvan luottamukseen. Yksittäiset kansalaiset, yritykset, organisaatiot ja valtiot luottavat siihen, että kaikkia laitteita voidaan käyttää turvallisesti ja bittien maailmassa voidaan liikkua ilman, että meihin kohdistetaan rikollista toimintaa. Kybermaailman varjopuolena voidaan pitää siellä esiintyvää rikollista toimintaa, joka on kompleksista. Usein rikollinen teko huomataan vasta hyökkäyksen jälkeen, mikä tekee esimerkiksi rikoksen tutkinnasta haastavampaa. Täten kyberosaamiseen ja -koulutukseen tulisi kiinnittää huomiota − etenkin kyberhygieniaan, jonka puuttuessa yksikin työntekijä voi aiheuttaa mittavat vahingot työnantajalleen.

Kyberrikollisuus on vuosien saatossa muuttunut myös entistä ammattimaisemmaksi ja järjestäytyneemmäksi. Rikolliset hyödyntävät uusia ja vanhoja toimintatapoja sekä ovat useasti kansallisia ja kansainvälisiä lainsäätäjiä edellä. Rikollisuuden voidaan katsoa olevan monimuotoista ja moniulotteista, ja rikoksentekijät käyttävät entistä enemmän hyväkseen erilaisia salausmenetelmiä ja anonymisointia, mikä vaikeuttaa rikosten torjuntaa ja selvittämistä. Rikoksia voidaan tehdä esimerkiksi paikasta riippumatta, niitä voidaan ajoittaa ja hyökkäyksiä voidaan tehdä useita samanaikaisesti. Kyberrikollisuuden nopeaan kehitykseen voi myös vaikuttaa alhainen kiinnijäämisriski ja rikoksista saatava hyöty.

Kyberrikollisuudella tarkoitetaan rikollisuutta, joka muodostuu viestintäverkkoja ja tietojärjestelmiä hyödyntäen tehdyistä sekä niihin kohdistuvista rikoksista (Turvallisuuskomitea 2018, 26). Kyberrikollisuus vaikuttaa kaikkiin tietoverkkojen ja tietotekniikan käyttäjiin. Kyberrikollisuuden kohteiksi

voivat joutua yksittäiset henkilöt, valtiot, puolustusvoimat, laitokset ja yritykset. On kuitenkin huomioitava, että kaikki tietoverkkojen häiriötilat eivät ole välttämättä rikollisuutta, vaan kyseessä voi olla järjestelmäbugi tai jokin muu ulkoinen aiheuttaja, kuten sääilmiö.

Rikoslaissa käytetään termejä ”tietoverkkorikollisuus” ja ”tietotekniikkarikos”, jotka tulevat englanninkielisestä sanasta *cybercrime*. Nykyään termi ”kyberrikollisuus” on yleistynyt, ja tietoverkkorikollisuudesta puhuttaessa puhutaan kyberrikollisuudesta. (Sisäministeriö 2017, 10.)

Kyberrikollisuus elää jatkuvassa muutoksessa, ja merkkejä sen järjestäytyneestä toiminnasta on ollut havaittavissa (CYBERDI 2021, 3). Kyberrikollisuuden määrä jatkaa kasvuaan, eikä tietoverkkorikollisuus katoa mihinkään. Kyberrikollisuus on yksi suurimmista haasteista, joita yhteiskunnat kohtaavat seuraavan kahden vuosikymmenen aikana. On arvioitu, mikäli kyberrikolliset jatkavat toimintaansa nykyisellä vauhdilla, vuoteen 2025 mennessä maailmanlaajuiset kyberrikollisuuden kustannukset nousevat 10,5 biljoonaan dollariin. Kyberrikollisia on erittäin vaikeaa saada kiinni, ja useissa maissa kyberrikollisuus ei ole välttämättä kriminalisoitua. (Cyber Security Intelligence 2021, luettu 14.10.2021.)

Kyberrikolliset hyödyntävät erilaisia menetelmiä, kuten haittaohjelmia, palvelunestohyökkäyksiä, hakkerointia, tietojenkalastelua ja kybervakoilua. Lisäksi kyberrikollisuudessa hyödynnetään pimeitä verkkoja, erilaisia salausmenetelmiä ja anonymiteettiä. Pimeällä verkolla tarkoitetaan verkkoa, jossa sijaitsee joukko piilotettuja internet-sivustoja ja jonne pääsee ainoastaan erityisellä, siihen tarkoitetulla verkkoselaimella (Mitä syvä ja pimeä verkko ovat? Luettu 16.10.2021).

Kyberrikollisuus voi myös kohdistua yhteiskunnan elintärkeisiin toimintoihin. Näillä tarkoitetaan sellaista toimintoa, joka on välttämätön yhteiskunnan toimivuuden kannalta, kuten johtaminen, kansainvälinen toiminta ja EU-toiminta, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus. (Turvallisuuskomitea 2018, 13.)

### 3.1 Keskeiset käsitteet

Kybermaailmaan liittyvä käsitteistö mielletään helposti vaikeaksi ja monimutkaiseksi. Seuraavaksi on tarkoituksena avata lukijalle, mitä tarkoitetaan tämän opinnäytetyön keskeisillä käsitteillä. Keskeisimpiä käsitteitä on tarkoitus avata laajemmin, kun taas muut käsitteet ja termit pyritään avaamaan niiden esiintyessä tekstissä ensimmäistä kertaa. Osa käsitteistä saattaa olla yleisesti tunnettuja tai entuudestaan tuttuja. Käsitteiden avaamisella pyritään helpottamaan ja auttamaan lukijaa opinnäytetyön tarkastelussa.

**Digitalisaatio.** Lähtökohtaisesti voidaan ajatella, että eletään kahdessa eri maailmassa – fyysisessä ja digitaalisessa. Fyysinen maailma koostuu atomeista ja konkretiasta, kun taas digitaalinen

maailma biteistä ja keinotekoisuudesta. Teknologian nopean kehityksen myötä ovat fyysinen ja digitaalinen maailma nivoutuneet toisiinsa. Jokaisen voidaan katsoa olevan riippuvainen digitalisaatiosta. Esimerkiksi rahojen säilyttäminen pankkitilillä sekä uutisten, sosiaalisen median ja sähköpostien selaaminen älypuhelimella vaativat digitalisaatiota. Yhteiskunnan pyörittäminen, kuten elintarvikkeiden-, sähkön- ja vedenjakelu, edellyttää digitaalisessa toimintaympäristössä toimimista.

Digitalisaatio on digitaalisen tietotekniikan yleistymistä arkielämässä. Tietotekniikalla voidaan taas tarkoittaa teknologiaa, jonka kehitys on nopeaa ja jatkuvaa, mikä edellyttää kaikilta kybertoimintaympäristön käyttäjiltä valppautta ja kybertaitoja. Käyttäjän on huolehdittava omasta osaamisestaan ja turvallisuustekijöistään, jotta tietoverkossa liikkuminen voidaan toteuttaa mahdollisimman turvallisesti. Uusien teknologioiden vuoksi on lainsäädännön, kyberkyvykkyyden ja -torjunnan oltava ajantasaista sekä osaamisen riittävän korkealla tasolla, jotta kyberrikollisuuden vaatimuksiin voidaan vastata.

Kyberrikolliset voivat digitalisaation ansiosta toimia verkossa nopeasti ja valtioiden rajat ylittäen. Myös todistusaineisto digitalisoituu, minkä takia sitä on entistä helpompi kätkeä tai tuhota. (Sisäministeriö 2017, 20.) Organisaatioiden riskinhallinta ei välttämättä pysy digitalisaation vauhdissa ja riskit arvioidaan tai ymmärretään väärin, mikä saattaa aiheuttaa heikon lopputuloksen organisaatiolle tai koko yhteiskunnalle. Digitaalinen yhteiskunta tarvitsee jatkuvasti enemmän ammattilaisia, kuten tietoturva- ja tietosuojaosaajia. (Tietoturvan vuosi 2020, 36.)

**Tietoverkot.** Tietoverkolla tarkoitetaan tietokoneiden ja niiden välisten tiedonsiirtoyhteyksien sekä näiden molempien avulla tarjottavien palvelujen yhdistelmää (Sanastokeskus TSK: *tietoverkko*). Tietoverkkoympäristö käsittää käsittämättömän määrän verkkosivuja, tietokantoja ja palvelimia. Tavallinen käytössä oleva niin kutsuttu näkyvä internet on ainoastaan pieni osa kokonaisuutta, ja joidenkin tilastojen mukaan näkyvät verkkosivustot ja tiedot muodostavat noin viiden prosentin koko internetistä. (Mitä syvä ja pimeä verkko ovat? Luettu 16.10.2021.)

Syvä verkko (englanniksi Deep Web) käsittää noin 90 prosenttia kaikista verkkosivustoista ja siihen kuuluu myös osa, jota kutsutaan pimeäksi verkoksi (englanniksi Dark Web). Usein syvää ja pimeää verkkoa käytetään toistensa synonyymeinä, mutta iso osa syvästä verkosta on täysin laillista ja turvallista käyttää. Pimeällä verkolla tarkoitetaan sivustoja, joita ei ole indeksoitu ja joihin pääsee ainoastaan erityisillä verkkoselaimilla. Pimeä verkko on näkyvää verkkoa pienempi ja erittäin hyvin kätketty syvän verkon osa, jota käyttävät vain harvat kakista internetin käyttäjistä. Pimeässä verkossa voidaan ostaa laittomia tuotteita ja palveluita, mutta myös lailliset tahot voivat hyödyntää verkkoa. (Mitä syvä ja pimeä verkko ovat? Luettu 16.10.2021.)

Avoimessa verkossa liikkuessa kaikista toimistamme jää jälkiä ja tekeminen voidaan jäljittää, koska yksittäisellä tietokoneella oleva IP-osoite (internetin protokollaosoite) on aina yksilöllinen. Tor-verkkoselainta (The Onion Routing, Tor) käyttämällä IP-osoitetta ei saada välttämättä selvillä ja siten verkkosivuvierailut, verkkosisältöjulkaisut, pikaviestinnät ja muut viestinnät voidaan salata. Tor-reitityksellä viestit kulkevat reitittimeltä reitittimelle sattuman varaisesti, mikä perustuu siihen, että ympäri maailmaa tuhannet vapaaehtoiset ylläpitävät reitittimiä, jotka ovat salatussa yhteydessä keskenään. Esimerkiksi viestin alkuperäinen olinpaikka ja käyttäjän henkilöllisyys saadaan tämän avulla piilotettua. Palveluntarjoaja ei kykene havaitsemaan Tor-verkon käyttäjää, koska anonymiteetti säilytetään käyttämällä salattua eli kryptattua VPN-yhteyttä (virtual private network, VPN). Tor-selaimella päästään käyttämään pimeitä verkkoja, joiden sivustojen muodostamaa kokonaisuutta kutsutaan usein Darknetiksi tai Dark Webiksi, missä liikkuu runsaasti laitonta sisältöä ja ovat siten rikollisten suosiossa. (Haasio 2017, 11–14.)

Kyberrikollisuus on suurta Darknetissä, jossa laittomien tuotteiden ja palveluiden lisäksi levitetään lapsiin kohdistunutta väkivaltamateriaalia ja terroristitoimintaa (Senker 2017, 11). Pimeä verkko lisää käyttäjän yksityisyyttä ja siksi sitä käytetään paljon rikollisiin tarkoituksiin, kuten aseiden, huumausaineiden ja petosten myyntiin. Kyberrikostorjuntakeskus pitää huolestuttavana sitä, että yhä nuoremmat ja henkilöt, joilla ei ole aikaisempaa rikostaustaa, ovat osallistuneet huumekauppaan tietoverkoissa. Yleisesti luullaan, että anonyymeillä alustoilla ei voida jäädä kiinni. Lisäksi rikosten realiteetit verkkoympäristössä katoavat. (Ostaisitko huumeita alle 18-vuotiaalta? Luettu 17.10.2021.)

**Tietoturva.** Tietoturvalla tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Tiedon on oltava käytettävissä haluttuna aikana, sen on oltava luottamuksellista eikä sivullisilla saa olla pääsyä siihen. Tietoturvan järjestelyjä voivat olla esimerkiksi kulunvalvonta, asiakirjojen turvallinen säilytys ja hävitys sekä virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. (Turvallisuuskomitea 2018, 15.)

**Tietoturvahäiriö.** Tietoturvahäiriö voi olla yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka mahdollisesti vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti. Tietoturvan yhteydessä puhutaan usein haavoittuvuudesta, eli alttiudesta tietoturvaan kohdistuville uhkille. Haavoittuvuus voi olla minkälainen heikkous tahansa, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Ihmisen toiminnassa, prosesseissa ja tietojärjestelmissä voi esiintyä heikkouksia. Tietoturvaloukkauksella tarkoitetaan oikeudetonta puuttumista tietoon tai tietojärjestelmään. (Turvallisuuskomitea 2018, 15 ja 17.)

**Kyber.** Kyber-sanan merkityssisältö liittyy yleensä digitaalisessa muodossa olevan informaation käsittelyyn, kuten tietotekniikkaan, digitaaliseen viestintään (tietoverkot), tietojärjestelmiin tai tietokonejärjestelmiin (Turvallisuuskomitea 2018, 21). Kyber-etuliite on korvannut aiemmat tieto- ja tietoverkkoetuliitteet, ja sillä on pyritty myös kuvaamaan toimintaympäristön muutosta globaalimmaksi ja modernimmaksi, joista yhteiskunnat ovat voimakkaasti keskinäisriippuvaisia (Sisäministeriö 2017, 11). Etuliitteen voidaan katsoa saavan merkityksensä silloin, kun siihen lisätään loppuosa, esimerkiksi kyberrikollisuus, kyberrikos tai kyberhyökkäys. Kyber-alkuisten käsitteiden käyttö alkoi Yhdysvalloissa nykyisessä merkityksessään 1990-luvun lopussa ja Suomessa kansallisen kyberstrategian laatimisen alkaessa vuonna 2011 (Sisäministeriö 2017, 11).

**Kybertoimintaympäristö.** Kybertoimintaympäristö muodostuu yhdestä tai useammasta sähköisessä muodossa olevan datan tai informaation käsittelyyn tarkoitetusta tietojärjestelmästä. Kyberturvallisuus on tila, jossa kybertoimintaympäristöstä yhteiskunnan elintärkeille toiminnoille tai muille kybertoimintaympäristöstä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallinnassa. (Valtioneuvoston puolustusselonteko 2021, 59.) Kybertoimintaympäristöön kuuluvat elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla sekä datan ja informaation käsittelyyn liittyvät fyysiset rakenteet. Kybertoimintaympäristön esimerkkejä ovat tietojärjestelmiin perustuva ydinvoimalan ohjausjärjestelmä, elintarvikkeiden kuljetus- ja logistiikkajärjestelmä, liikenteen ohjausjärjestelmät sekä pankki- ja maksujärjestelmät. (Turvallisuuskomitea 2018, 20.)

Kyberympäristö on olennainen osa rikollisuuden ja rikostorjunnan toimintaympäristöä. Kyberrikollisuudesta on tullut hyvin kattava rikollisuuden osa-alue, jonka vaikutukset kohdistuvat yksityisiin kansalaisiin, liiketoimintaan ja valtioihin. Rikollisille kyberympäristö on fyysistä ympäristöä edullisempi ja houkuttelevampi paikka toteuttaa rikoksia. (Sisäministeriö 2017, 7.) Ominaisia piirteitä kybertoimintaympäristölle ovat ilmiöläheisyys, kompleksisuus, kiihtyvä muutosnopeus ja osittain ennalta-arvaamattomuus (VNSTK 2018, 30).

**Kyberturvallisuus.** Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristö on luotettava ja turvattu (Turvallisuuskomitea 2018, 22). Kyberturvallisuus on jatkuvassa koetuksessa nopean toimintaympäristön muutoksen ja digitalisaation kehittymisen takia. Kyberturvallisuutta on jatkuvasti ylläpidettävä ja kehitettävä, koska kyberturvallisuusuhat ja kyberrikollisuus muuttuvat jatkuvasti. Kyberturvallisuuden toimivuuteen ja kybertoimintaympäristössä turvalliseen liikkumiseen tarvitaan jokaista käyttäjää, organisaatiota, yritystä ja valtiota. Digitaalinen toimintaympäristö on luonut ja luo jatkuvasti kyberturvallisuudelle uusia haasteita, joihin on kyettävä vastaamaan. Kyberturvallisuudella huolehditaan yhteiskunnan elintärkeistä toiminnoista ja jokaisen käyttäjän turvallisesta tietoverkkojen käytöstä. Suomessa yksi keskeinen kyberturvallisuustoimija on Liikenne- ja

viestintävirasto Traficomin Kyberturvallisuuskeskus, joka kyberturvallisuusstrategian linjausten mukaisesti palvelee viranomaisia, elinkeinoelämää ja muita toimijoita kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi. (Sisäministeriö 2018, 27.)

Kyberturvallisuus on välttämätöntä yhteiskunnan toimivuuden, elintärkeiden toimintojen ja kriittisen infrastruktuurin ylläpitämiseksi. Yrityksestä ja toimialasta riippumatta on tärkeää, että yrityksessä on tunnistettu kyberturvallisuus osana riskienhallintaa ja siitä huolehditaan koko organisaation tasolla (CYBERDI 2021, 35).

**Kyberuhka.** Kyberuhalla tarkoitetaan mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon (Turvallisuuskomitea 2018, 25). Kyberuhat voidaan jakaa viiteen ryhmään: kybervandalismiin, kyberrikollisuuteen, kybervakoiluun, kyberterrorismiin ja kyberoperaatioihin. Kyberhäiriötilanteella tarkoitetaan toteutunutta uhkaa, joka haittaa organisaation tai järjestelmän toimintaa (Turvallisuuskomitea 2018, 28). Kyberuhka tai -häiriö voi olla aiheutettu tahallisesti, tai kyseessä voi olla tahaton tapahtuma, kuten ohjelmistovirhe tai sään aiheuttama häiriö tai katkos.

**Esineiden internet.** Erilaiset älylaitteet ovat tulleet osaksi arkipäivää esimerkiksi viihdepalvelujen ja kotiteknologioiden kautta. Verkkoon liitettyjä laitteita on tuotettu teolliseen käyttöön ja kotikäyttöön, esimerkiksi älylaitteina. Erilaisia laitteita ja palveluita voidaan käyttää internetin kautta, mikä voi aiheuttaa kuluttajalle riskejä ja uhkia. Laitteisiin voidaan kohdistaa hyökkäyksiä, ja sitä kautta niihin voidaan aiheuttaa vahinkoa. Laitteissa itsessään voi myös olla haavoittuvuuksia tai puutteita.

Esineiden internetillä (englanniksi *Internet of things, IoT*) tarkoitetaan laitteiden ja muiden esineiden kytkemistä internetiin, jotta niitä voitaisiin ohjata ja jotta ne voisivat olla vuorovaikutuksessa keskenään (IATE: *IoT*). Tietoteknologia on sulautunut arkisiin esineisiin, kuten kodin laitteisiin, jolloin niitä pystyy internetin yli seuraamaan ja ohjaamaan tietokoneella, puhelimella tai muilla laitteilla (Sisäministeriö 2017, 5). Jokainen internetiin yhdistetty laite kerää tietoa, minkä takia laite ja verkko on suojattava. IoT kasvaa valtavaa vauhtia, ja valmistajat joutuvat kiireessä tuomaan laitteita markkinoille ilman, että IoT-tietoturvaseikkoihin ehditään kiinnittämään riittävästi huomiota. Suuri määrä uusia laitteita aiheuttaa tilanteen, jossa vanhoja laitteita ei enää tueta ohjelmakorjauksilla. Tilaisuuden voi käyttää hyväksi pahantahtoinen hakkeri. (Miksi kotiverkon IoT-tietoturva on tärkeä asia? Luettu 3.10.2021.)

Tietoturvapuutteita sisältävät laitteet voidaan esimerkiksi valjastaa bottiverkkoihin palvelunestohyökkäyksiä tehostamaan (Tietoturvan vuosi 2019, 31). Tietoverkkorikosten määrä on kasvussa ja tulee kasvamaan edelleen merkittävästi, koska tuottoisin rikollisuus toimii kybermaailmassa, mikä taas muuttaa erilaisten vahingontekorikosten toteutusmenetelmiä esineiden internetissä (Sisäministeriö 2017, 5).

**IoT-bottiverkko.** Bottiverkolla (englanniksi *botnet*) tarkoitetaan kaapatuista tietokoneista muodostunutta verkkoa, jota sen haltija käyttää huomaamattomasti haitallisiin ja laittomiin tarkoituksiin (Sanastokeskus TSK: *Bottiverkko*). IoT-laitteeseen voidaan asentaa IoT-botnet eli ohjelmistorobotti, joka etsii muita haavoittuvia laitteita tarkoituksenaan tehdä niistä itsensä kaltaisia ”zombeja”. Bottinettiä hallitsee niin sanottu botmaster, joka ohjeistaa ja antaa käskyjä saastuneille laitteille sekä esimerkiksi käynnistää palvelunestohyökkäyksen valitsemaansa kohteeseen. Bottinetit ovat rakenteeltaan keskitettyjä tai hajautettuja, eli niillä on joko yksi tai useampi komentokeskus. (Lehto 2021, 17.) Kyberrikollinen voi siis käyttää laitteita botteina, joiden laskentakapasiteettia käytetään esimerkiksi klikkauspetokseen, salasanan hakkerointiin, roskapostin lähettämiseen tai kryptovaluutan louhintaan (Miksi kotiverkon IoT-tietoturva on tärkeä asia? Luettu 3.10.2021).

### 3.2 Lainsäädäntö

Kybertoimintaympäristön kompleksisuus ja jatkuva muutostila aiheuttavat haasteita myös lainsäädännölle. Kyberrikollisten voidaan katsoa olevan jatkuvasti lainsäädäntöä askeleen edelle. Tämä johtuu siitä, että rikolliset keksivät jatkuvasti uusi tapoja ja menetelmiä, kun taas lainsäätäminen on työlästä ja hidasta. Toisin sanoen voidaan sanoa, että kyberrikolliset liikkuvat kyberrikollisuuden torjuntaa, tutkintaa ja lainsäätäjää nopeammin, koska rangaistavuuden astuessa voimaan toimivat rikolliset jo uudella tavalla. Tästä syystä nopea tekninen kehitys ja teknologian kehitys on otettava huomioon rikosoikeudellisessa sääntelyssä.

Kyber- ja verkkorikollisuudessa on suuria kansallisia eroja, ja viranomaisyhteistyö etenkin Euroopan unionin ulkopuolella on haastavaa. Kyberrikolliset voivat tästä syystä toimia heikon lainsäädännön maassa ja hakea sieltä käsin kohteensa jostain toisesta maasta. Keskeisenä haasteena voidaan pitää sitä, että kyberrikokselle ei ole selkeää määritelmää, edes viranomaistasolla. Lain säätäminen voi olla vaikeaa, koska kansainvälistä yhteisymmärrystä on vaikea löytää ja varsinaista yhteistä näkemystä eri toimijoiden välillä ei ole olemassa.

Yhdistyneet kansakunnat (YK) 1990-luvulla tunnisti tietotekniikan väärinkäytökset valtioiden rajat ylittäväksi rikollisuudeksi (Lehto 2021, 90). Kyberrikollisuutta koskevia yleissopimuksia, puitepäätöksiä ja direktiivejä on laadittu useita Euroopan unionin toimesta, mutta nämä eivät sido useimpia niistä maista, joista kyberrikollisuutta tehdään. Euroopan neuvoston voidaan katsoa saaneen aikaan konkreettisen sopimuksen erilaisista suosituksista, jotka ovat toimineet ohjeena kansallisia rikoslakeja uudistettaessa (Convention on Cybercrime). Suomen rikoslain 38 luku muutettiin yleissopimusta vastaavaksi vuonna 2007, ja tärkeimpinä uudistuksina voidaan pitää tietojärjestelmän häirintää ja törkeää tietomurtoa koskevia säännöksiä. (Peltomäki & Norppa 2015, 71–72.) Euroopan komissio määrittelee kyber- ja tietoverkkorikollisuuden rikoksiksi, jotka tehdään sähköisiä vies-

tintäverkkoja ja tietojärjestelmiä hyödyntäen tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin. Internetiä rikollisuus hyödyntää jakelukanavana, kommunikaatiovälineenä ja rikoksentekovälineenä. (Lehto 2021, 51.)

Vuonna 2014 tulivat Suomessa voimaan poliisilain (872/2010) ja pakkokeinolain (806/2010) kokonaisuudistukset. Uudistuksissa pyrittiin ottamaan huomioon myös tekninen kehitys, ja lainsäädännössä pyrittiin tekniikkaneutraaliin lainsäädäntöön, jotta lainsäädäntöä ei teknisen kehityksen takia tarvitse lyhyin väliajoin muuttaa. Säännösten avulla pyritään vastaamaan toimintaympäristön muutoksiin. (Sisäministeriö 2017, 40.)

Keskeinen lainsäädäntöön vaikuttava asiakirja on myös Euroopan unionin verkko- ja tietoturvadirektiivi (2016/1148/EU) eli niin sanottu NIS-direktiivi tietoturvavelvollisuuksista ja häiriöraportoinnista. Euroopan unionin yleinen tietosuoja-asetus (2016/679/EU, GDPR) määrittelee henkilötietojen käsittelyä Euroopan unionin alueella. Laki sähköisen viestinnän palvelusta (917/2015) säätelee sähköisen viestinnän palveluiden laatua, tietoturvaa ja viestinnän luottamuksellisuutta. Tietosuojalaissa (1050/2018) säädetään henkilötietojen käsittelystä.

Tietoturvaloukkauksella (englanniksi *security breach*) tarkoitetaan oikeudetonta puuttumista tietoon tai tietojärjestelmiin. Tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palvelunestohyökkäys ja tietojen varastaminen. (Sanastokeskus TSK: *tietoturvaloukkaus*.)

Yleisesti voidaan todeta, että kyberrikokset ovat erilaisia ja monimuotoisia. Tyypillisesti kyberrikoksia tehdään ulkomailta ja rikollinen on uhrille tuntematon. (CYBERDI 2021, 17.) Kybertoimintaympäristössä tapahtuvat muutokset ovat nopeita ja vaikeasti ennakoitavissa, mikä asettaa lainsäätämiselle haasteita.

**Kansalliset kyberrikokset.** Rikos on teko tai laiminlyönti, joka on laissa määritelty rangaistavaksi. Rangaistavuuden edellytyksenä on se, että tekijä on syyllistynyt rikokseen tahallaan tai tuottamuksellisesti ja hän on ollut rikoksen tekohetkellä syyntakeinen. (Peltomäki & Norppa 2015, 34.) Kyberrikoksesta ei ole vakiintunutta määritelmää, ja määritelmissä on korostettu teknologiaa tekovälineenä, kohteena tai ympäristönä. Kyberrikoksesta käytetään myös termiä tietoverkkorikos. (Sisäministeriö 2017, 10.)

Tietotekniikka on otettu Suomen rikoslainsäädännössä huomioon kahdella tavalla. Tietotekniikan väärinkäytösten ollessa samantyyppisiä kuin perinteisten rikosten, tarkastellaan näitä koskevia säännöksiä. Kun tietotekniikka on tuonut mukanaan uudenlaista käyttäytymistä, on uusia tietotekniikkaan liittyviä tunnusmerkistöjä säädetty. Hajanaisia säännöksiä on myös tekijänoikeuslaissa,

aluevalvontalaissa, valmiuslaissa, puolustuslaissa ja puolustusvoimista annetussa laissa sekä viestintämarkkinalaissa ja sähköisen viestinnän tietosuojalaissa. Suomen rikoslaissa rangaistaviksi säädetyt teot on jaoteltu siten, että katsotaan, kohdistuvatko ne tietotekniikkaan vai hyödynnetäänkö rikosta tehtäessä tietotekniikkaa. Pääsääntönä voidaan pitää sitä, että mikä on kiellettyä tietoverkkojen ulkopuolella, on kiellettyä myös tietoverkoissa. (Peltomäki & Norppa 2015, 77–80.) Kyberrikokset ovatkin siten perinteisesti jaettu tietoverkkorikosympäristöön kohdistuviin rikoksiin eli niin sanottuihin puhtaisiin tietoverkkorikoksiin ja tietoverkkoympäristöä hyväksikäyttäen tehtyihin rikoksiin. Rikosten kohdistuessa kyberympäristöön on kyse sellaisista rikosten tekomuodoista, joita esiintyy ainoastaan tietoverkoissa tai tietojärjestelmissä ja joissa rikos kohdistuu tietoverkkoon, tietojärjestelmään tai siinä olevaan dataan. (Sisäministeriö 2017, 10.)

Tietoverkkoympäristöihin kohdistuvassa tietoverkkosidonnaisessa rikollisuudessa (englanniksi *cyber-dependent crime*) ja sitä hyväksikäyttävässä tietoverkkoavusteisessa rikollisuudessa (englanniksi *cyber-enabled crime*) on erityistä se, että yksittäinen tekijä kykenee teknologiaa hyödyntämällä tekoihin, jotka voivat vaikuttaa useisiin eri valtioihin ja miljooniin ihmisiin. (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021.)

Seuraavissa osioissa tarkastellaan Suomen lainsäädäntöä kyberrikollisuuden näkökulmasta. Niin sanotut kyberrikokset määritellään rikoslain 38 luvussa ”Tieto- ja viestintärikoksista”. Luvussa 36 käsitellään petosrikoksia ja luvussa 37 maksuvälinepetoksia. Rikokset jaetaan tietoverkkoihin tai tietojärjestelmiin kohdistuviin rikoksiin ja digitaalista toimintaympäristöä hyödyntäen tehtäviin rikoksiin.

**Tietoverkkoihin tai tietojärjestelmiin kohdistuvat rikokset.** Tietotekniikkarikoksen voidaan katsoa olevan tietoteknisessä ympäristössä tapahtuva rikos, jonka rikoksen tekovälineenä tai teon kohteena on tieto- tai tiedonsiirtojärjestelmä laitteineen. Määritelmillä viitataan tietokoneisiin, dataan ja informaatioon sekä myös tietoverkkomaailmaan. (Jounio 2011, 11.)

Kyberrikosten voidaan katsoa olevan määritelty Suomen rikoslain 38 luvussa. Luku käsittelee tieto- ja viestintärikoksia. Luvun mukaan rikoksiksi on määritelty salassapitorikos (RL 38:1), viestintäsalaisuuden loukkaus (RL 38:3), tietoliikenteen häirintä (RL 38:5), tietojärjestelmän häirintä (RL 38:7a), tietomurrot (RL 38:8), suojauksen purkujärjestelmärikos (RL 38:8b), tietosuojarikos (RL 38:9) ja identiteettivarkaus (RL 38:9a). Tietotekniikkaan kohdistuvissa rikoksissa uhreina ovat usein yritykset, organisaatiot ja valtiot silloin, kun aiheutetaan haittaa tietojärjestelmille tai ohjelmille. Yksityishenkilöt voivat myös olla tietotekniikkarikosten uhreja esimerkiksi silloin, kun sähköpostiin lähetetään haittaohjelmia. (Rikoksentorjunta: Kyberrikokset, luettu 5.10.2021.)

Identiteettivarkaudessa voidaan anastaa ja käyttää henkilötietoja väärin ja henkilökohtaisia tietoja voidaan myydä verkossa eteenpäin. Myös salasanat, fyysiset osoitteet, pankkitilinumerot ja sosiaaliturvatunnukset leviävät jatkuvasti pimeässä verkossa. Rikolliset voivat muun muassa vahingoittaa luottotietoja, tehdä talousrikoksia ja murtaa muita verkkotilejä. (Mitä syvä ja pimeä verkko ovat? Luettu 16.10.2021.) Muita tyypillisiä tietoverkkoihin tai tietojärjestelmiin kohdistuvia rikoksen tekomuotoja tai ilmiöitä ovat haittaohjelmat, tietojärjestelmähyökkäykset ja vakoilu. Näistä enemmän seuraavissa luvuissa.

**Digitaalista toimintaympäristöä hyödyntäen tehdyt rikokset.** Tietoverkkoja hyödyntäen tehtyjä rikoksia ovat muun muassa petos- ja maksuvälinepetos sekä muut rikokset, joissa tietoverkkoa käytetään välineenä rikoksen tekemiselle. Vuonna 2019 tilastoitiin 28 653 petosrikosta ja 6296 maksuvälinepetosta. Petosrikosten määrä on lisääntynyt voimakkaasti 2000-luvulla ja vuonna 2019 viisi prosenttia väestöstä ilmoitti joutuneensa huijatuksi ostaessaan tavaraa tai palvelua. (Helsingin yliopisto 2020, 6.)

Petosrikoksessa tekijä tavoittelee itselleen taloudellista hyötyä uhria erehdyttämällä, ja usein petoksen seurauksena on taloudellinen vahinko uhrille. Petosrikos on nykypäivänä monimuotoinen, ja petosten tekeminen on siirtynyt tietoverkkoihin. Esimerkiksi internet ja sähköposti ovat helpottaneet rikollisia tavoittamaan suuria ihmismääriä lähes olemattomin kustannuksin. (Poliisi: *petosrikokset*, luettu 5.10.2021.)

Maksuvälinepetoksesta tuomitaan se, joka hankkii itselleen tai toiselle oikeudetonta taloudellista hyötyä käyttäen maksuvälinettä ilman sen laillisen haltijan lupaa, ylittää lupaan perustuvan oikeutensa tai muuten ilman laillista oikeutta käyttää väärää tai väärennettyä maksuvälinettä tai maksuvälineeseen liittyvää dataa syöttämällä, muuttamalla, tuhoamalla, vahingoittamalla, siirtämällä tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaa rahan tai rahan arvon siirron lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa (RL 37:8). Maksuvälinepetoksella tarkoitetaan pankki-, maksu- tai luottokortin tai näihin rinnastettavan maksuvälineen käyttöä ilman laillista oikeutta tai sen muunlaista väärinkäyttöä. Maksuvälinepetoksesta voidaan rangaista myös sovitun enimmäisluottorajan tai tilin katteen ylittämisestä.

Tietoverkkoja hyödyntäviä rikoksia voivat olla rikokset, joissa tietoverkkoa käytetään välineenä rikoksen tekemiselle, kuten esimerkiksi rahanpesu ja piratismi (Jounio 2011, 11). Rikoksen täyttäessä tietotekniikkarikoksen tunnusmerkit on kyseessä tieto- ja viestintärikos, vaikka se nimikkeeltään voi viitata muuhun. Tieto- ja viestintärikoksia voivat olla luvaton käyttö (RL 28:7–9), yrityssalaisuuden rikkominen ja yrityssalaisuuden väärinkäyttö (RL 30:4–6), väärennös (RL 33:1–3) ja vahingonteko (RL 35:1 2–3 mom.) sekä vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a) ja tietoverkkovälineen hallussapito (RL 34:9b). (Jounio 2011, 60.) Erityisesti omaisuusrikokset, kiristys (RL

31:3), tietojenkalastelu, nettihäirintä ja kiusaaminen sekä erilaiset kunnianloukkausrikokset (RL 24:9) ja kiihottaminen kansanryhmää vastaan (RL 11:10) voivat olla tietokoneavusteisia rikoksia. Poliittista ja uskonnollista aktivismia on entistä enemmän kybermaailmassa, ja muun muassa sosiaalisesta mediasta on tullut mielipide- ja asennevaikuttamisen foorumi.

Kyberrikosten tunnusmerkistöistä voidaan havaita, että tietojärjestelmiin kohdistuvia rikoksia voidaan toteuttaa useilla eri tavoilla (Pajunen 2020, 65).

### 3.3 Keskeiset toimijat ja kyberturvallisuusstrategia

Tässä alaluvussa on tarkoitus avata keskeisiä kybertoimijoita Suomessa. Kybertoiminnan ympärillä toimii useita eri viranomaisia, joille kaikille on määritelty omat tehtävänsä ja vastuualueensa. Kyberrikollisuuden osalta keskeinen toimija on poliisi, jonka tehtäviin kuuluu rikosten selvittäminen, syyteharkintaan saattaminen, ennalta estäminen ja paljastaminen. Vihjetietoa kyberrikoksista voi myös lähettää poliisille, esimerkiksi epäilyttävästä materiaalista verkossa voi ilmoittaa poliisin Nettivinkin kautta (CYBERDI 2021, 36).

Keskusrikospoliisin (KRP) yhteydessä toimivassa kyberrikostorjuntakeskuksessa ja paikallispoliisissa tutkitaan kyberrikoksia. Kyberrikostorjuntakeskuksessa keskitytään vakavien, kansainvälisten tai paljon erityisresursseja vaativien rikosten tutkintaan. (CYBERDI 2021, 36.)

Seuraavaksi esitellään tämän opinnäytetyön näkökulmasta keskeiset kyberrikollisuuden toimijat, ja tarkastellaan Suomen kyberturvallisuusstrategiaa.

**Keskusrikospoliisin kyberrikostorjuntakeskus.** Keskusrikospoliisin (KRP) tehtävänä on torjua ja tutkia kansainvälistä, järjestäytynyttä, ammattimaista ja muuta vakavaa rikollisuutta, tuottaa asiantuntijapalveluita, kehittää rikostorjuntaa ja rikostutkintamenetelmiä (Laki poliisihallinnosta 14.2.1992/110, 9 §). KRP:ssä toimii kyberrikostorjuntaan keskittynyt kyberrikos(torjunta)keskus, jonka tehtäviin kuuluvat vakavimpien tietoverkkorikosten tutkinta, rikosperusteinen internet- ja verkkotiedustelu, erityisosaamista vaativa tietotekninen tutkinta, tietoverkkorikollisuuden ylläpito sekä esitutkintaan liittyvät asiantuntijapalvelut poliisille ja muille viranomaisille. (Jämsén 2019, 3.)

Kyberrikostorjuntakeskus perustettiin vuonna 2015, ja sen perustamisella pyrittiin varmistamaan tietoverkkorikosten torjuntakyky ja poliisihallinnon toimintakyky kybertoimintaympäristössä tapahtuvissa vaativissa poliisitoiminnallisissa tilanteissa sekä törkeiden rikosten estämisessä, paljastamisessa ja selvittämisessä. Keskuksen tehtäviin kuuluu kaksi toisistaan poikkeavaa tehtäväkokonaisuutta. Ensinnäkin keskus vastaa tietoverkkorikostorjunnasta, esimerkiksi palvelunestohyökkäyksistä ja muista vakavista ja kansainvälisistä tietojärjestelmiin kohdistuvista rikoksista. Toiseksi muiden poliisiyksiköiden kanssa kyberrikostorjuntakeskus tekee yhteistyötä tietoverkoissa tapahtuvan

lasten seksuaalisen hyväksikäytön ja maksukorttirikollisuuden torjunnassa. Tehtäväalueet ovat samat, joista Europolin European Cyber Crime Center vastaa. Kyberrikostorjuntakeskuksen tehtäviin kuuluu myös tarjota poliisihallinnolle kybertoimintaympäristön palveluja, kuten tehtäviä, jotka sisältyvät tietoverkkoihin ja tietoteknisiin laitteisiin. Edellä mainituista keskeisimpiä tehtäviä ovat digitaaliforensiikka ja tietoverkkoihin liittyvä tiedon hankinta. Digitaaliforensiikalla tarkoitetaan digitaalisen todistusaineiston käsittelyä ja analysointia. (Sisäministeriö 2017, 26.)

Kyberrikostorjunta tekee yhteistyötä Viestintäviraston Kyberturvallisuuskeskuksen kanssa ja seuraa tietoverkoissa tapahtuvaa rikollisuutta sekä tiedottaa aktiivisesti seurantaan liittyvistä ajankohtaisista uhkista. Edellä mainittuihin tehtäviin osallistuu koko poliisi. Kybertorjuntakeskuksen tehtävänä luoda tilannekuvaa ajankohtaisesta kyberrikollisuudesta. Tilannekuva perustuu muun muassa rikosilmoituksiin, kyberalan kansainväliseen raportointiin, yhteistyöhön Europolin ja Interpolin kanssa. (VNST 2018, 50.)

**Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus.** Liikenne- ja viestintäviraston Kyberturvallisuuskeskus ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä sekä ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Keskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta, ja keskus toimii julkisesti säännellyn satelliittipalvelun vastuuviranomaisena. (Laki Liikenne- ja viestintävirastosta 935/2018, 3 §.) Liikenne- ja viestintäministeriön voidaan sanoa koordinoivan kyberturvallisuutta Suomessa. Kyberturvallisuuskeskuksen tehtävänä on myös viestiä tietoturvallisuusuhkista sekä auttaa tietoturvaloukkauksen selvittämisessä, tutkimisessa ja toimenpiteiden koordinoinnissa (CYBERDI 2021, 36).

Kyberturvallisuuskeskuksen tarkoitus on palvella viranomaisia, elinkeinoelämää ja muita toimijoita kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi. Kyberturvallisuuskeskus on tärkeä yhteistyökumppani poliisille tietoverkkorikosten ja kybertilannekuvan ylläpitämisessä. (Sisäministeriö 2017, 27.) Kyberturvallisuuskeskus julkaisee ohjeita ja käytänteitä organisaatioille kyberturvallisuuden arvioimiseksi ja kehittämiseksi sekä kyberturvallisuusuhkilta suojautumiseksi. Keskus vastaanottaa myös ilmoituksia kyberturvallisuusuhkista sekä varautuu uhkiin ennakolta. (CYBERDI 2021, 36.)

Suomen hallitus antoi syyskuun lopussa 2021 eduskunnalle lakiesityksen, jolla Kyberturvallisuuskeskus nimettäisiin Suomen kansalliseksi kyberturvallisuuden koordinointikeskukseksi EU:n laajuiseen koordinointikeskusten verkostoon. Tavoitteena on syventää julkisen sektorin, yksityisen sektorin ja tutkimusmaailman välistä yhteistyötä kyberturvallisuuden alalla. (Valtioneuvosto 30.9.2021, luettu 12.10.2021.)

**Puolustusvoimien johtamisjärjestelmäkeskus.** Puolustusvoimien johtamisjärjestelmäkeskuksen (PVJJK) tehtäviin kuulu puolustusvoimien tietoteknisten palveluiden järjestäminen, ylläpitäminen ja

kyberpuolustus. Keskukseen kuuluu kyberosasto, joka ylläpitää puolustusvoimien kyberturvallisuuden tilannekuvaa, suojaa puolustusvoimien tietoverkkoja ja -palveluita sekä kehittää kyberpuolustusta. (Turvallisuuskomitea 2018, 36.) Puolustusvoimat vastaa Suomen sotilaallisesta kyberpuolustuksesta osana kansallista kyberturvallisuutta. Puolustusjärjestelmän kybertilannekuvan parantaminen sekä kyberuhkien estäminen ja torjuminen edellyttävät tiedonvaihdon, toimivaltuuksien ja kansallisten yhteistyörakenteiden kehittämistä viranomaisten välillä. (Valtioneuvoston puolustusselonteko 2021, 25.)

**Suojelupoliisi.** Suojelupoliisin tehtävänä on hankkia tietoa kansallisen turvallisuuden suojaamiseksi sekä havaita, estää ja paljastaa sellaisia toimintoja, hankkeita ja rikoksia, jotka voivat uhata valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Suojelupoliisin on myös ylläpidettävä ja kehitettävä yleistä valmiutta yhteiskunnan turvallisuutta uhkaavan toiminnan havaitsemiseksi ja estämiseksi. (Laki poliisin hallinnosta, 10 §.) Suojelupoliisin tehtäviin siis kuuluvat kaikkein vakavimpien kansallisen turvallisuuden uhkien, kuten valtiollisen vakoilun ja terrorismin, ennalta-ehkäisy ja torjunta (CYBERDI 2021, 36) sekä laittoman tiedustelutoiminnan ja valtion turvallisuutta vaarantavien ääriliikkeiden toiminnan estäminen. Suojelupoliisi tutkii myös tietoverkoissa tapahtuneita vakoilurikoksia ja tekee ennalta estävää turvallisuustyötä kyberuhkien torjunnassa lisäämällä uhkia koskevaa tietoisuutta viranomaisissa ja yksityisen sektorin organisaatioissa. Haittaohjelmahyökkäyksiä suojelupoliisi selvittää yhteistyössä muiden viranomaisten ja tarvittaessa yksityisen sektorin kanssa. (Sisäministeriö 2017, 26.)

**Poliisiammattikorkeakoulu.** Poliisiammattikorkeakoulu vastaa poliisialaan liittyvästä tutkinto- ja täydennyskoulutuksesta sekä tutkimus- ja kehitystoiminnasta (Sisäministeriö 2017, 26). Poliisiammattikorkeakoulu osallistui esimerkiksi CYBERDI-hankkeeseen, jossa yhteistyössä muun muassa Jyväskylän ammattikorkeakoulun kanssa kehitettiin opas yrityksille kyberrikostutkinnan kulusta.

**Europol.** Europol eli Euroopan unionin lainvalvontayhteistyövirasto, jonka tehtävänä on parantaa Euroopan turvallisuutta ja avustaa lainvalvontaviranomaisia EU-maissa. Europol on lainvalvontaoperaatioiden toteutuksen tukija, lainvalvontaviranomaisten tietojenvaihtokeskus rikosasioissa ja lainvalvonnan asiantuntijakeskus. Europol myös laatii tasaisin aikavälein pitkän aikavälin selvityksiä rikollisuudesta ja terrorismista kansallisia viranomaisia varten. (Euroopan unioni: *Europol*, luettu 2.10.2021.)

Europol on lainvalvonnasta vastaava Euroopan unionin erillisvirasto, jonka tehtävänä on tukea EU:n jäsenvaltioita kaikentyyppisen kansainvälisen rikollisuuden ehkäisemisessä ja torjunnassa sekä tukea lainvalvontaviranomaisia vaihtamalla ja analysoimalla rikostiedustelutietoja. (Europol katsaus 2011, 7.) Europol julkaisee vuosittain esimerkiksi vakavan ja järjestäytyneen rikollisuuden

uhka-arvion SOCTAn (EU Serious and Organised Crime Threat Assesment) sekä internetiä hyödyntävää järjestäytynyttä rikollisuutta koskevan uhka-arvion IOCTAn (Internet Organised Crime Treat Assesment) (Europol 2011, 16 ja 48).

Europolin kyberrikollisuuskeskus, European Cyber Crime Center (EC3), on poliisin kannalta keskeinen toimija. Se perustettiin Alankomaihin, ja Suomen poliisi lähetti sinne kansallisen asiantuntijan. Suomi osallistuu aktiivisesti ja täysimääräisesti yhteistyöhön Europolin kanssa sen mandaatin ja yhteistyömahdollisuuksien puitteissa. EC3 tekee myös tiivistä yhteistyötä Joint Cybercrime Action Task Forcen (J-CAT) kanssa, jossa toimii eri maiden yhdyshenkilöitä myös Euroopan ulkopuolelta. (Sisäministeriö 2017, 28.)

**Kansainväliset toimijat.** Suomalaiset kybertoimijat tekevät myös yhteistyötä kansainvälisten toimijoiden kanssa. Kyberrikollisuus on usein kansainvälistä, mistä syystä viranomaisten on tehtävä kansainvälistä yhteistyötä rikollisuuden paljastamiseksi, torjumiseksi ja tutkimiseksi. Voidaan sanoa, että kansainvälisistä foorumeista merkittävimpiä ovat Pohjoismaat, Euroopan unioni, YK (Yhdistyneet kansakunnat), Euroopan turvallisuus- ja yhteistyöjärjestö (Etyj), Eurooppa-neuvosto, Taloudellisen yhteistyön ja kehityksen järjestö (*OECD*) ja NATO. Näissä käsitellään kybertoimintaympäristöön liittyviä kysymyksiä. Suomelle keskeisimpiä toimijoita ovat EU ja NATO, joiden kanssa vaihdetaan muun muassa tilannetietoa ja kehitetään kyberpuolustusta. Pohjoismaisella yhteistyöllä pyritään edistämään kyberturvallisuutta, ja Eurooppa-neuvoston tietoverkkorikollisuutta koskeva yleissopimus on kaiken kyberrikollisuuden torjunnan kehittämisen perusta. Etyjin kanssa on pyritty kehittämään luottamusta lisääviä toimia kyberkonfliktien edistämiseksi avoimuudella, yhteistyöllä ja vakaudella. OECD:n kanssa pyritään kehittämään tai harmonisoimaan jäsenmaiden politiikkaa eri talous- ja yhteiskuntaelämän sektoreilla. (Turvallisuuskomitea 2021, 29–30.)

**Yksityiset toimijat.** Yksityisillä toimijoilla on viranomaisten ohella merkittävä rooli kyberrikollisuuden torjunnassa. Useat organisaatiot ovat ulkoistaneet tietoturvansa rakentamisen, laitekannan ja ylläpidon kaupallisille palveluntarjoajille. Organisaatiot ostavat tarvitsemansa palvelut, kuten sähköpostijärjestelmän, tallennus- ja työtilat, sisäiset ja ulkoiset verkkosivut sekä käyttämänsä sovellukset, yksityisiltä palveluntarjoajilta. (CYBERDI 2021, 37.)

Organisaatioiden tasolla yhteistyö toimii finanssisektorin kanssa, mutta kehitettävää on poliisin ja elinkeinoelämän tietoverkkorikollisuuden torjumisessa, yhteistyössä ja tiedonvaihdossa. On olemassa useita tietoturva-alan yrityksiä, kuten SOC-toimijoita (*Security operation center*), joihin voi olla yhteydessä esimerkiksi poikkeamahallintatilanteissa. Näillä tietoturva-alan yrityksillä on erittäin hyvä tilannekuva suomalaisiin yrityksiin kohdistuvista uhkista. (Sisäministeriö 2017, 27.) Palveluntarjoajilta voi myös hankkia esimerkiksi tietoturvaratkaisuja, järjestelmien haavoittuvuuksien kartoittamista, haittaohjelma-analyysia, kybertoimintaympäristöjen auditointia sekä tietoturvapoikkeamien

reaaliaikaista havaitsemista ja ratkaisua. Suomessa on myös vapaaehtoistoimijoita, jotka auttavat organisaatioita myös akuuteissa tietoturvaloukkauksissa. (CYBERDI 2021, 37.)

**Kyberturvallisuusstrategia.** Kyberuhkiin ja -rikollisuuteen pyritään vastaamaan mahdollisimman tehokkaasti. Valtiovallan keskeisimpiä tehtäviä on huolehtia yhteiskunnan turvallisuudesta, ja siitä, että yhteiskunnan elintärkeät toiminnot pystytään turvaamaan kaikissa tilanteissa. Suomen kyberturvallisuusstrategiassa 2013 kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. (Turvallisuuskomitea 2013, 1–2.) Vuoden 2019 kyberturvallisuusstrategiassa asetetaan keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi. Vuoden 2019 strategia nojautuu vuoden 2013 yleisiin periaatteisiin. (Turvallisuuskomitea 2019, 4.)

Suomen kansallisen kyberturvallisuusstrategian kolme strategista linjausta ovat kansainvälinen yhteistyö, kyberturvallisuuden johtamisen, suunnittelun ja varautumisen parempi koordinaatio sekä kyberturvallisuuden osaamisen kehittäminen (Turvallisuuskomitea 2019, 5–9). Viranomaisten välistä yhteistyötä on kehitettävä kyberpuolustuksen, strategisen viestinnän ja informaatiopuolustuksen alalla, ja kansainvälinen yhteistyö on keskeistä Suomen kyberturvallisuudelle ja kyberpuolustukselle. (Valtioneuvoston puolustusselonteko 2021, 8 ja 26.)

Vuoden 2013 strategian tavoitteena oli vastata kyberuhkiin, vahvistaa yhteiskunnan kokonaisturvallisuutta ja varmistaa kybertoimintaympäristön toimivuus kaikissa olosuhteissa (Turvallisuuskomitea 2013, 2, 7 ja 22). Vuoden 2013 strategiassa esitetään kymmenen tavoitetta, joita toteuttamalla Suomi kykenee kansallisesti hallitsemaan kybertoimintaympäristön tahallisia ja tahattomia haittavaikutuksia sekä vastaamaan kyberuhkiin ja toipumaan niistä.

Yksi kansallinen haaste on kyberosaamisen riittämättömyys, niin asiantuntijatasolla kuin yksittäisen käyttäjän tasolla. Ammatillisen osaamisen edistämiseksi tarvitaan panostuksia tutkintoon johtavaan koulutukseen sekä muunto- ja täydennyskoulutukseen kyberturvaosaajien määrän kasvattamiseksi julkiselle ja yksityiselle sektorille. Lisäksi kansalaisten kyberturvallisuustaitoihin on panostettava ja esimerkiksi digiturvaviikkoa, kansallista tietoturvapäivää ja kyberturvallisuuskoulutusta on kehitettävä. (Liikenne- ja viestintäministeriö 2021, 11–13.) Suomella on oltava riittävä osaaminen ja tekninen kyvykkyys huolehtia kyberturvallisuudesta, ja niitä on jatkuvasti ylläpidettävä. Lisäksi lainsäädännöstä ja sen ajankohtaisuudesta on pidettävä huolta.

Kyberturvallisuuden kehittämisohjelman (Liikenne- ja viestintäministeriö 2021, 18) mukaan Suomessa käynnistetään selvitystyö, jossa arvioidaan viranomaisten toimintaedellytykset kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa, ottaen huomioon

kansallisen ja kansainvälisen uhkaympäristön jatkuvan kehittymisen. (Liikenne- ja viestintäministeriö 2021, 18.)

### 3.4 Keskeinen tekijäpiiri ja motiivi

Kyberrikollisuuden voidaan katsoa olevan erityistä sen ominaispiirteiden takia. Kyberrikollisuudessa yksi tekijä voi saada valtavaa tuhoa tai häiriötä aikaiseksi. Voidaan sanoa, että yksi tai muutama tekijä voi vähäisillä resursseilla vaikeuttaa miljoonien ihmisten tai lukuisten valtioiden toimintaa samanaikaisesti. Fyysisessä maailmassa vastaavanlainen toiminta saattaisi olla haastavampaa. Yksittäinen rikollinen voi hyökätä kybermaailmassa lukuisia kertoja löytääkseen esimerkiksi aukon yrityksen tietoturvasta tai vahingoittaakseen valtion kriittistä infrastruktuuria. Kyberrikollisuudessa voidaan myös hyödyntää aikaa esimerkiksi ajoittamalla hyökkäykset. Kyberrikollisuudessa niin sanotulla perinteisellä tapahtumapaikalla ei ole merkitystä, koska rikos voidaan tehdä pitkienkin etäisyyksien päästä. Edellä mainitut ominaispiirteet asettavat omat haasteensa rikostutkinnalle ja rikollisen identifioinnille.

Yleisesti voidaan sanoa, että kyberrikokset kohdistuvat tavallisiin kansalaisiin, yhteisöihin, yrityksiin ja julkishallintoon. Täten rikoksen uhri voi olla luonnollinen henkilö tai oikeushenkilö kuten fyysisissä rikoksissa. Tietotekniikkarikosten uhreiksi joutuvat todennäköisemmin ne, jotka käyttävät internetiä eniten ja monipuolisimmin. Riskitekijöiksi voidaan katsoa ikä ja sukupuoli, kun vaikutetaan tapaan, miten internetiä käytetään (Pajunen 2020, 25 ja 33).

Kyberrikollisuus on monimutkaista johtuen useista eri syistä. Syitä voivat olla erilaiset tekijät, motiivit, kohteet ja lainkäyttöalueet. Kompleksisuus vaikeuttaa tietojen keräämistä ja tuloksien vertailua, koska esimerkiksi havaintojen rekisteröinnin laatu saattaa olla erilaista. (IOCTA 2020, 10.) Myös uhrin kokemuksella on vaikutusta ilmoitusaktiivisuuteen. Uhri voi tuntea häpeää ja jättää tästä syystä ilmoittamatta rikoksesta (Viestintävirasto 2016, 10). Edellä mainitut syyt asettavat haasteet täsmällisen tiedon hankinnalle ja kyberrikollisuuden mittaamiselle.

Kyberrikollisia voivat olla tavalliset kuluttajat, ammattirikolliset, aktivistit ja valtioiden edustajat (Peltomäki & Norppa 2015, 55). Kyberrikollisesta voidaan käyttää useita eri nimityksiä, kuten tietotekniikkarikollinen tai hakkeri. Kyberrikollisuuden taustalla voi myös olla valtiollinen toiminta, sodankäynti, terrorismi tai ilkivalta. Henkilö voi myös tietämättömyyttään tai vahingossa syyllistyä lainvastaiseen tekoon, mutta ammattirikollisuus vaatii ammattitaitoa ja -osaamista sekä koulutusta.

Esimerkiksi datavahingonteko- ja tietomurtorikokset ovat sellaisia rikoksia, joiden toteuttaminen ei pakosti vaadi erityistä tietoteknistä osaamista, mutta tietojärjestelmän häirintä, törkeä tietojärjestelmän häirintä ja törkeä tietomurto lähtökohtaisesti velvoittavat tekijältä jonkinasteista erityistä tietoteknistä taitoa. (Pajunen 2020, 71.)

Tietoverkkorikollisuus on yhä enemmän kansainvälistä, järjestäytynyttä rikollisuutta tai valtiojohtoista toimintaa. Suuri osa tietoverkkorikollisuudesta on entistä ammattimaisempaa ja joissakin maailman alueilla verkkorikollisuus saattaa olla monen ihmisen pääelinkeino. Ammattimaisilla ja järjestäytyneillä kyberrikollisilla on kyky ja mahdollisuus kehittää rikoksentekomenetelmiä kaikkialla maailmassa. (Jämsén 2020, luettu 5.10.2021.) Kyberrikolliset valitsevat usein uhrinsa hyöty-kustannusanalyysin perusteella, jolloin omat resurssit minimoidaan ja saadut tulot maksimoidaan. Kyberrikolliset hyödyntävät erilaisia foorumeja ja muun muassa myyvät toimintaansa palveluna. (Maanpuolustuskorkeakoulu 2019, 32.) Seuraavaksi tarkastelleen tämän opinnäytetyön näkökulmasta keskeisiä aiheuttajia ja motiiveja.

**Kybervandaalit.** Kybervandalismilla tarkoitetaan hakkerin tai hakkeriryhmän tekemää ilkivaltaa, jolla tekijä pyrkii aiheuttamaan vahinkoa tai hankkimaan mainetta. Hakkerilla tarkoitetaan henkilöä, joka tunkeutuu tai vaikuttaa tietoverkkoon, tietojärjestelmään tai niiden sisältämään tietoon ja käyttää ohjelmaa, palvelua tai muuta resurssia. Hakkerit voidaan jakaa valkohattuhakkereihin (englanniksi *white hat*) ja mustahattuhakkereihin (englanniksi *black hat*). (Turvallisuuskomitea 2018, 26.) Hakkerien tarkoitusperien ymmärtämiseksi ne jaetaan eri tyyppeihin eli erivärisiin hattuihin.

Valkohattuhakkerin tunkeutuminen saattaa olla luvallista. Esimerkiksi yritys voi palkata hakkerin etsimään tietoverkostaan tai -järjestelmästään tietoturva-aukkoja tai haavoittuvuuksia. (Turvallisuuskomitea 2018, 26.) Valkohattuhakkerit käyttävät taitojaan auttaakseen organisaatioita suojautumaan vaarallisilta hakkereilta ja siten parantamaan yrityksen tietoturvaa. Valkohattujen yhteydessä puhutaan usein eettisistä hakkereista, jotka voivat olla läpäisytestaajia, jotka keskittyvät erityisesti järjestelmien heikkouksien löytämiseen ja riskien arviointiin. Valkohatut käyttävät samoja hakkerointimenetelmiä kuin mustahatutkin, mutta valkohatuilla on järjestelmän omistajan lupa ja sitä kautta prosessi on myös laillinen. Valkohattujen ja mustahattujen suurin ero on motiivi. (Mustahattu-, valkohattu- ja harmaahattuhakkerien määritelmä ja selitys, luettu 5.10.2021.)

Mustahattuhakkeri, toisin sanoen vihamielinen hakkeri, saattaa tuhota tietojärjestelmästä tietoja tai käyttää järjestelmää omiin tarkoituksiinsa (Turvallisuuskomitea 2018, 26). Mustahatut ovat rikollisia, jotka tunkeutuvat tietokoneverkkoihin hyväksikäyttääkseen niitä. Mustahatut saattavat päästää verkkoihin haittaohjelmia, jotka tuhoavat tiedostoja, pitävät tietokoneita panttivankeina tai varastavat salasanoja, luottokorttinumeroita ja muita henkilötietoja. Mustahatut havittelevat usein taloudellista hyötyä tai kostoa tai haluavat aiheuttaa tuhoa. Johtavat mustahatut ovat yleensä taitavia hakkereita, jotka työskentelevät monimutkaisissa rikollisjärjestöissä. (Mustahattu-, valkohattu- ja harmaahattuhakkerien määritelmä ja selitys, luettu 5.10.2021.)

Lisäksi on olemassa harmaahattuhakkereita, jotka toimivat valko- ja mustahattujen välimaastossa ja soveltavat niiden menetelmiä. Harmaahattuhakkerit etsivät usein järjestelmän heikkouksia ilman

omistajan lupaa tai tietämystä ja ongelman löydettyään raportoivat niistä omistajalle ja pyytävät korvausta vian korjaamisesta. Harmaahattujen motiivina voidaan pitää taitojen näyttämistä, julkisuuden saavuttamista ja arvostuksen tavoittelua. (Mustahattu-, valkohattu- ja harmaahattuhakkerien määritelmä ja selitys, luettu 5.10.2021.)

Tutkimustulosten perusteella hakkerit ovat yleisesti teknisesti lahjakkaita, sosiaalisesti syrjäytyneitä nuoria miehiä, joiden motiiveina ovat muun muassa uteliaisuus, näyttämisen halu ja maineen kasvattaminen. Vain pienellä osalla motiivina raha, ja motiiveihin vaikuttivat hakkerien tietoteknisen osaamisen taso. (Pajunen 2020, 25 ja 76.)

**Kyberaktivisti.** Kyberaktivismilla tarkoitetaan yksittäisen henkilön tai ryhmän kybertoimintaympäristössä harjoittamaa tavoitteellista tai aatteellista toimintaa, jolla voidaan tavoitella huomiota tai muutosta johonkin asiaan. (Turvallisuuskomitea 2018, 25.) Kyberaktivistit voivat käyttää myös rikollisia keinoja, ja laittoman kyberaktivismin muoto on haktivismi, jolla voidaan tarkoittaa esimerkiksi yhteiskunnallisia liikkeitä, jotka ottavat haltuunsa ja käyttöönsä tietoverkkojen mahdollisuuksia edistäessään omia tavoitteitaan (Lehto 2021, 49).

**Kybervakoilijat.** Kybervakoiluissa hyödynnetään tietoverkkoja, niihin liitettyjä laitteita ja ohjelmistoja. Kybervakoilu voi kohdistua valtioihin, kansalaisiin, yrityksiin tai organisaatioihin ja siinä voidaan käyttää hyväksi esimerkiksi kohdistettuja haittaohjelmahyökkäyksiä. Kybervakoilu on kansallisen lainsäädännön mukaan lainvastaista toimintaa. (Turvallisuuskomitea 2018, 26.) Kybervakoilussa voidaan hankkia salaisia tietoja, kuten sensitiivisiä, yksityisoikeudellisia tai turvaluokiteltuja tietoja. Tietoja voidaan hankkia poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi käyttäen laittomia menetelmiä internetissä, verkoissa, ohjelmistoissa tai tietokoneissa. (Lehto 2021, 59.)

Suomessa kybertiedustelu ja -vakoilu voi kohdistua teknologian osaamiseen tai vientivalvonnan alaisiin tuotteisiin. Vuonna 2020 havaittiin intensiivisiä valtiollisia kybervakoiluyrityksiä, jotka kohdistuivat Suomen ulko- ja turvallisuuspoliittisen päätöksenteon valmisteluun. (SUPO 2020 vuosikirja, Vakoilun painopiste verkkoon.)

**Kyberterroristit ja -sotilaat.** Kyberterrorismilla tarkoitetaan terroristista toimintaa, jossa hyökätään tietojärjestelmien kautta kansalaisia, liike-elämää, yhteiskunnan elintärkeintä toimintoja tai kriittistä infrastruktuuria tai muuta kohdetta vastaan (Turvallisuuskomitea 2018, 27). Kyberterroristit käyttävät terroritekojen välineenä kyberympäristöä. Terroristit hyödyntävät uusinta teknologiaa esimerkiksi propagandan levittämiseen ja uusien jäsenten rekrytointiin. Tulevaisuudessa uhkana voidaan pitää kyberkeinojen yhdistämistä perinteiseen terrorismiin. Esimerkiksi pommi-iskujen vaikutuksia voitaisiin pahentaa suuntaamalla samanaikaisesti palvelunestohyökkäys terveydenhuollon tai viranomaisen tietojärjestelmiin. (Maanpuolustuskorkeakoulu 2019, 32–33.)

**Valtiolliset toimijat.** Kybertoimintaympäristössä vaikuttavat aktiivisesti valtiolliset ja ei-valtiolliset toimijat (Valtioneuvoston puolustusselonteko 2021, 21). Valtiolliset toimijat voivat hyödyntää kybertoimintaympäristöä osana tiedustelua ja sodankäyntiä. Valtiollisia toimijoita voivat olla viralliset toimijat ja erilaiset järjestäytyneet ryhmittymät, joilla on jonkinlainen yhteys virallisiin toimijoihin. Tiedustelupalvelut ovat kehittäneet erilaisia kybertiedustelumenetelmiä. Kybervakoilulla pyritään keräämään tietojärjestelmistä käytännössä kaikkea tietoa. Älylaitteiden yleistymisen johdosta on kybervakoilulla saatavan tiedon määrä lisääntynyt ja laitteet ovat olleet kybervakoilun suosiossa. Kybervakoilumenetelmät ovat muihin menetelmiin verrattuna edullisia, ja riski on pieni. (Maanpuolustuskorkeakoulu 2019, 33.)

**Järjestäytynyt rikollisuus.** Suomalainen järjestäytynyt rikollisuus on pääsääntöisesti kotimaista, ja poliisien tietojen mukaan järjestäytyneen rikollisuuden ryhmien määrä on lisääntynyt viimeisten 10 vuoden aikana. Keskusrikospoliisin arvion mukaan Suomessa on noin 90 järjestäytynyttä rikollisryhmää ja niissä jäseniä noin 900–1000. Nykyään myös järjestäytynyt rikollisuus hyödyntää tietoverkkoja rikosten tekemisessä. Tietoverkkoja hyödynnetään petosrikoksien tekemisessä, rahanpesussa ja lasten seksuaalisessa hyväksikäytössä. Lisäksi rikosten tekemisissä käytetään hyväksi haittaohjelmia ja kalasteluhuijauksia. (Sisäministeriö: *Järjestäytynyt rikollisuus*, luettu 6.10.2021.)

Kyberrikokset ovat usein kansainvälisiä, ja verkossa tapahtuvat rikokset ovat useasti kansalliset rajat ylittäviä. Täten rikosten tekijöiden tai kohteiden sijainnilla ja etäisyydellä ei ole periaatteessa merkitystä. (Sisäministeriö: *kyberrikollisuus*, luettu 6.10.2021.) Myös Euroopan kansalaisille, yrityksille ja instituutioille sekä Euroopan taloudelle järjestäytynyt rikollisuus on merkittävä uhka. Rikollisen liiketoiminnan aloilla vuonna 2019 rikollisten tulot olivat 139 miljardia euroa. Järjestäytynyttä rikollisuutta esiintyy kaikissa EU-maissa, ja kyberrikollisuus on yksi yleisimmistä rikoksista Euroopassa. (Eurooppa neuvosto: *Järjestäytyneen rikollisuuden torjunta EU:ssa,* luettu 6.10.2021.)

Teknologian käytöstä on tullut keskeinen piirre vakavalle ja järjestäytyneelle rikollisuudelle vuonna 2021. Rikolliset käyttävät yhä enemmän salattua viestintää keskinäiseen verkostointiinsa sekä sosiaalista mediaa ja pikaviestipalveluita suuremman yleisön tavoittamiseksi ja laittomien tavaroiden tai väärän tiedon levittämiseksi. Kyberympäristö ja verkkokaupat tarjoavat rikollisille asiantuntemusta ja kehittyneitä työkaluja rikollisen toiminnan mahdollistamiseksi. (SOCTA 2021, 11.)

Euroopan unionin neuvoston mukaan vuosien 2022–2025 järjestäytyneen rikollisuuden prioriteetteihin lukeutuvat myös kyberhyökkäykset, verkkopetokset ja -huijaukset sekä lasten hyväksikäyttö verkossa. (EMPACT 2021, 6–8.)

**Motiivi.** Tutkimustulosten perusteella hakkereiden motiivina voivat olla näyttämisen halu, uteliaisuus, maineen kasvattaminen ja sosiaalisen hyväksynnän saaminen (Pajunen 2020, 25). Lisäksi

kyberrikollisten motiivina voidaan usein pitää taloudellisen hyödyn tavoittelua. Kyberrikosten tekeminen voi olla kustannustehokkaampaa kuin muun rikollisuuden, ja kyberrikollisten kiinnijäämisriski ja seurausvaikutukset voivat olla matalampia kuin fyysisissä rikoksissa. Tämä lisää kyberrikollisuuden houkuttelevuutta. (Cyberwatch Q1 2020, 10.)

Järjestäytyneen rikollisuuden lisäksi kyberrikoksia tekevät yksityishenkilöt, joiden motiivina on usein tietotekniikkaan liittyvien taitojen testaaminen sekä riitautuminen kohteena olevan henkilön tai organisaation kanssa (Cyberwatch Q1 2021, 10). Kyberrikollisen motiivit voivat myös liittyä sosiaalisiin syihin, seksuaalisuuteen tai jopa sairauteen (Peltomäki & Norppa 2015, 55). Joskus vakavakin teko voi olla ajattelemattoman ja kokeilunhaluisen tekijän aikaansaannos, mutta usein kyse on taloudelliseen hyötyyn tähtäävästä ammattimaisesta tai puoliammattimaisesta rikollisuudesta (CYBERDI 2021, 7).

Eurooppalaisten viranomaisten mukaan vuonna 2018 palvelunestohyökkäysten ensisijaisena motiivina oli kiristys. Muita motiiveja olivat ideologisuus ja poliittisuus, mutta kaikissa hyökkäyksissä ei välttämättä ollut ilmeistä motiivia, vaan tarkoituksena oli aiheuttaa pahaa. Yleisimpiä kohteita olivat rahoituslaitokset ja julkinen sektori, kuten poliisi- ja paikallishallinnot. Lisäksi kohteina olivat matkatoimistot ja verkkopelaamiseen liittyvät palvelut. (IOCTA 2019, 22.) Rikollisen pyrkimyksenä saattaa myös olla vahingoittamistarkoitus esimerkiksi kilpailevaa yritystä kohtaan, tai hän saattaa muutoin tavoitella kilpailuetua muihin nähden. On myös mahdollista, että toiminta on valtiollista vakoilua tai kyse on muusta valtioon kohdistuvasta vaikuttamispyrkimyksestä. Uhri voi myös olla satunnainen kohde, mutta rikolliset etsivät usein verkosta automaattityökalujen avulla haavoittuvia järjestelmiä ja valitsevat löydösten joukosta kiinnostavimmat kohteet. (CYBERDI 2021, 7.)

Kuitenkin Euroopassa tietomurroista 73 prosenttia tehdään taloudellisen hyödyn takia (IOCTA 2017, 28). Palvelunestohyökkäyksissä voi taustalla olla uskonnollinen syy (Peltomäki & Norppa 2015, 102) sekä haittaohjelmahyökkäyksissä voiton tavoitteleminen ja maineen rakentaminen hakkeriyhteisöissä (SOCTA 2021, 41).

Suomessa on havaittu, että kyberrikollisten joukossa on yhä enemmän nuoria ja alaikäisiä. Esimerkiksi huumausainerikoksiin mukaan lähteneitä nuoria on motivoinut nopeat voitot sekä ajatus siitä, että anonyymeja alustoja käytettäessä ei voida jäädä viranomaisille kiinni. Nuoret eivät välttämättä ymmärrä kyberrikosten realiteetteja tai tilanteen vakavuutta. Suomen poliisi on vuonna 2021 käynnistänyt tietoverkkorikollisuuden varhaiseen puuttumiseen keskittyvän Cybercrime Exit -hankkeen. (Ostaisitko huumeita alle 18-vuotiaalta? Luettu 17.10.2021.)

# 4 KYBERRIKOLLISUUDEN ILMIÖT JA TILANNEKUVA

Suurin osa nykytoiminnoista, yritysten ja yhteiskunnan palveluista sekä asioiden hoitamisesta, on siirtynyt kybermaailmaan. Ihmiset hoitavat entistä enemmän asioitaan verkossa sen helppouden ja käytännöllisyyden takia. Yrityksille palveluiden tuottaminen verkossa on kustannustehokasta ja nopeaa. Jopa yhteiskunnan kriittiset toiminnot sijaitsevat verkossa. Kyberympäristön merkitys on kasvanut ja kasvaa edelleen kaikilla osa-alueilla. Digitalisaatio luo mahdollisuuksia, mutta myös lisää kyberrikollisuutta. Kyberrikollisuudella voidaan aiheuttaa suurta haittaa ja sen vaikutukset voivat koskettaa useita valtioita ja ihmisiä samanaikaisesti. Kyberturvallisuudella tavoitellaan sitä, että kybertoimintaympäristössä voisi toimia suojassa vaaroilta. Kyberturvallisuudella pyritään hallitsemaan riskejä ja rikoksia, mutta väistämättä turvallisuus välillä vaarantuu rikollisen tai muun toiminnan johdosta.

Kyberrikollisuus kasvaa jatkuvasti rikollisuuden kokonaiskentässä, ja sen määrä on kasvanut vuosina 2014–2020 noin 70 prosenttia. Muu rikollisuus globaalisesti on ollut maltillisessa laskusuunnassa. Suomessa rekisteröitiin vuonna 2019 noin 1300 kyberrikollisuustapausta. Kyberrikollisuus on tavoittanut järjestäytyneen rikollisuuden, ja kyberrikoksia käytetään usein rikollisorganisaatioiden varainhankintaan ja muun toiminnan rahoittamiseen. (Cyberwatch Q1 2021, 10.) Kyberrikoksia kirjattiin vuonna 2020 hieman alle 1820 kappaletta. Vuoden 2021 lokakuuhun mennessä tietomurtoja poliisin tietojärjestelmään oli kirjattu 1080, joka oli vain noin 50 vähemmän kuin koko edeltävänä vuonna. Törkeiden tekomuotojen osuus on ollut kasvussa vuonna 2021. (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021.) Kyberrikollisuutta itsessään voidaan pitää ilmiönä, mutta seuraavaksi käsitellään kyberrikollisuuden sisällä ilmeneviä ilmiöitä ja kyberrikollisuuden tilannekuvan muodostamista.

## 4.1 Ilmiöt

Kyberrikollisuus on monimuotoista ja vaikeasti ymmärrettävää. Lähes jokainen kyberympäristön käyttäjä on kohdannut kyberrikollisuutta ja sen eri ilmiöitä, kuten esimerkiksi tietojenkalastelua tai haittaohjelmia. Aikaisemmin opinnäytetyössä on käsitelty tietoverkkorikoksia, mutta kyberrikollisuudessa on erilaisia muotoja, toteutustapoja, menetelmiä ja ilmiöitä, joita seuraavaksi tarkastellaan lähemmin.

Tarkasteluun on otettu muutamia, ehkä yleisimpiä, kyberrikollisuusilmiöitä. Tarkoitus on myös käsitellä sitä, millä tavalla kyberrikollisuus vaikuttaa yksittäisiin kansalaisiin, yrityksiin ja organisaatioihin ja mitä tyypillisiä ilmiöitä niihin kohdistuu.

**Yksittäinen kansalainen, yritys ja organisaatio.** Kyberrikollisuus ja sen ilmiöt aiheuttavat haittaa sekä organisaatioille, yrityksille että yksittäisille henkilöille. Helposti mielletään, että kyberrikollisuus

koskee suuria ja yhteiskunnallisia yrityksiä, mutta itse asiassa yksittäisen kansalaisen kyberturvallisuustaidot ja -toimet ovat merkittävässä asemassa kyberturvallisuuden näkökulmasta. Tästä syystä kansalaisen kybertaitoihin ja pelisääntöihin olisi kiinnitettävä erityistä huomiota. Kyberrikollisuuden kohdistuessa yrityksiin ja organisaatioihin voi haitta olla samanlaista kuin yksityishenkilöihin kohdistuessa, mutta myös erilaisia haittatekijöitä ilmaantuu.

Suomessa kyberrikollisuus on varteenotettava riski toimialasta ja koosta riippumatta. Yksittäisten tekojen vaikutukset yrityksille vaihtelevat tapauksen mukaan vähäisestä kriittiseen. Kyberrikoksen uhriksi voi joutua mikä tahansa organisaatio. (CYBERDI 2021, 3 ja 10.) Kyberrikollisuutta voidaan kohdistaa yrityksiin ja organisaatioihin, koska ne ovat entistä riippuvaisempia digitaalisista palveluista ja järjestelmistä. Yrityksiä voidaan vahingoittaa monin eri tavoin, ja aiheutetulla vahingolla voi olla suuria vaikutuksia muun muassa yrityksen toimintaan, maineeseen ja talouteen. Operatiiviseen toimintaan kyberrikollisuus voi liittyä siten, että esimerkiksi sähköpostipalvelut tai ohjelmistot kaatuvat ja siten yrityksen toiminta hidastuu tai lamaantuu pahimmassa tapauksessa kokonaan. Kyberriskit voivat myös kohdistua arkaluontoiseen ja salassa pidettävään materiaaliin sekä oikeudellisiin seikkoihin. Kyberrikollisen päästessä käsiksi yrityksen arkaluontoisiin ja salassa pidettäviin materiaaleihin, voi rikollinen kiristää materiaalilla yritystä tai jopa levittää tietoa julkisesti. Tämä voi mahdollisesti heikentää yrityksen mainetta ja luotettavuutta, ja materiaalin leviäminen tai joutuminen vääriin käsiin voi johtaa kumppaneiden esittämiin vaatimuksiin tai muihin lakisääteisiin vaatimuksiin. Pahimmassa tapauksessa kyberrikollinen voi vaarantaa asiakkaan tai työntekijän turvallisuuden, esimerkiksi tunkeutumalla sairaalan laitteisiin tai tuotannon koneisiin.

Kyberrikollinen voi kalastella yritysten ja organisaatioiden työntekijöiltä tietoja, kuten käyttäjätunnuksia, salasanoja, yhteystietoja tai muita organisaatiolle arvokkaita tietoja. Rikolliset voivat pyrkiä saatujen tietojen pohjalta luomaan valelaskuja tai paljastamaan yrityssalaisuuksia. Valelaskuilla aiheutetaan taloudellista haittaa, ja yrityssalaisuuksien paljastaminen voi aiheuttaa yritykselle oikeudellista vahinkoa. Myös erilaisten huijausten takia yritys voi menettää muita varoja, ja huijauksilla yritykseen voidaan kohdistaa vakoilua ja yrityksen palvelut voivat pettää.

Suomessa kyberturvallisuuden osaamiseen on kiinnitetty erityistä huomiota. Kansalaisten on osattava käyttää digitaalisen tietoyhteiskunnan tuottamia palveluita turvallisesti ja tunnistettava eri laitteisiin, tuotteisiin ja palveluihin liittyvät riskit. Myös suomalainen elinkeinoelämä, kyberturvateollisuus ja viranomaiset ovat havainneet kyberturvaosaajien riittämättömyyden. Kyberturvaosaamisen riittävyys on edellytys alan yritysten kasvulle, kansainvälistymiselle ja uusille innovaatioille. (Liikenne- ja viestintäministeriö 2021, 11.)

Yksityisiltä henkilöiltä voidaan huijata käyttäjätunnuksia, salasanoja tai muita arvokkaita tietoja, kuten pankkitunnuksia tai maksukorttitietoja. Seurauksena voi olla omiin laitteisiin kohdistuneet hyökkäykset, laitteen lukitsemiset ja taloudelliset menetykset. Myös henkilötietoja voivat rikolliset hyödyntää omassa rikollisessa toiminnassaan. Esimerkiksi haittaohjelmien avulla voidaan yksittäiseltä käyttäjältä vaatia lunnaita laitteen lukitsemisen purkamiseksi. Kyberturvallisuus tulisikin nähdä luonnollisena osana jokaisen organisaation ja yksilöiden yhteiskuntavastuuta (Kyberturvallisuuden kehittämisohjelma 2021, 8).

**Haittaohjelmat ja kiristyshaittaohjelmat**. Ohjelma, joka tarkoituksellisesti aiheuttaa koneen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa, kutsutaan haittaohjelmaksi (englanniksi *malware*). Haittaohjelmia voivat olla esimerkiksi virukset, madot ja troijalaiset. (Sanastokeskus TSK: *haittaohjelma.)*

Kiristyshaittaohjelmalla (englanniksi *ransomware*) tarkoitetaan haittaohjelmaa, joka salaa tai manipuloi laitteella olevia tietoja ja tavallisesti vaatii käyttäjältä lunnaita salauksen purkamiseksi. Kiristyshaittaohjelma voi tulla laitteeseen esimerkiksi sähköpostin liitetiedoston kautta siten, että kun käyttäjä avaa liitetiedoston, haittaohjelma latautuu laitteeseen. Tämän jälkeen haittaohjelma voi esimerkiksi muuntaa joitakin tiedostoja salakirjoitettuun muotoon. Ilman salauksenpurkuavainta tietoja ei voi enää avata. Lisäksi ohjelma voi uhata levittää tai paljastaa luottamuksellista tietoa. (Turvallisuuskomitea 2018, 32.) Haittaohjelmalla voidaan tietokoneeseen tartuttaa virus, mato tai troijalainen, jolloin tietojärjestelmä tekee ei-toivottuja toimia tietokoneessa, esimerkiksi vakoilee tai lähettää tietoa tietylle komentopalvelimelle (Sisäministeriö 2017, 10).

Haittaohjelmat voivat myös levitä haittaohjelmilla saastutettujen verkkosivustojen tai haavoittuvien palvelimien kautta. Maailmalla on yleistynyt ilmiö, jota kutsutaan nimellä *Big Game Hunting*, missä rikollinen valitsee kohteikseen erityisen houkuttelevia ja rahakkaita organisaatioita. Hyökkäyksessä rikollinen tunkeutuu organisaation järjestelmiin ja levittäytyy sen verkkoon ja lopuksi käynnistää salatun kiristyshaittaohjelman, joka hidastaa ja haittaa organisaation toimintaa tai lamauttaa sen lähes kokonaan. Lopuksi organisaatiolta kiristetään, esimerkiksi rahaa salauksen purkamiseksi. (Traficom 2020, 7.) Kiristyshaittaohjelmat voivat toimia eri tavoin ja erityyppisesti sekä näyttää erilaisilta. Kiristyshaittaohjelmalla voidaan tuhota arvokasta tietoa tai julkaista arkaluonteisia tietoja.

Haittaohjelmia on myös pimeässä verkossa, ja niitä jaetaan usein erilaisissa portaaleissa, ja siten rikolliset saavat työkaluja kyberhyökkäyksiinsä. Haittaohjelmia voidaan myös tartuttaa pimeässä verkossa, jossa vallalla ei ole samanlaisia yhteiskuntasopimuksia kuin avoimessa verkossa. Pimeässä verkossa käyttäjät voivat altistua haittaohjelmille, kuten näppäilyn tallentimille, botti-verkkohaittaohjelmille ja kiristysohjelmille. Kyberrikollisten hyväksikäytön estämiseksi on olemassa haittaohjelmien torjuntaohjelmia ja virustorjuntaa. (Mitä syvä ja pimeä verkko ovat? Luettu 16.10.2021)

On myös olemassa Rootkit-haittaohjelma, joka on suunniteltu siten, että se antaa kyberrikollisille kohdelaitteeseen pääsyn ja kyvyn hallita sitä. Rootkitit vahingoittavat pääsääntöisesti ohjelmistoa ja käyttöjärjestelmää, mutta voivat myös tartuttaa tietokoneen laitteiston ja laiteohjelmiston. Rootkitin päästyä laittomasti tietokoneeseen voi kyberrikollinen sen avulla varastaa esimerkiksi henkilö- ja muita tietoja sekä asentaa haittaohjelman tai käyttää tietokonetta osana bottiverkkoa levittääkseen roskaposteja ja osallistuakseen palvelunestohyökkäykseen. (Mikä rootkit on – määritelmä ja selitys, luettu 5.10.2021.)

**Palvelunestohyökkäys.** DoS (englanniksi *Denial of Service*) on palvelunestohyökkäys, jolla tarkoitetaan mitä tahansa keinoa, jolla estetään tietojenkäsittelypalvelun käyttö siihen oikeutetuilta henkilöiltä. DDos (englanniksi *Distributed Denial of Service*) eli hajautettu palvelunestohyökkäys tarkoittaa useasta lähteestä tulevaa verkkoliikennettä, joka ylikuormittaessaan kohteen aiheuttaa palvelunestotilan. (Lehto 2021, 39.)

Tietoverkkohyökkäyksellä pyritään kuormittamaan ja siten lamaannuttamaan jokin palvelu tai tietojärjestelmä. Hyökkäyksellä voidaan esimerkiksi lamaannuttaa sähköposti suurella määrällä sähköpostiviestejä taikka palvelin tai reititin suurella määrällä palvelupyyntöjä. Palvelunestohyökkäyksen tullessa yhdestä IP-osoitteesta voi se olla suhteellisen helppoa havaita ja torjua esimerkiksi palomuurin avulla. Tästä syystä palvelunestohyökkäys on yleensä hajautettu eli se toteutetaan useista eri lähteistä. (Turvallisuuskomitea 2018, 31.) Hyökkäykset kestävät yleensä niin kauan, kuin niillä on vaikutusta kohteen toimintaan ja useimmiten ne loppuvat silloin, kun ne saadaan torjuttua ja palvelun toiminta saadaan palautettua entiselleen. Palvelunestohyökkäyksiä tehdään Suomessa tuhansittain joka vuosi. Palveluksenestohyökkäystoiminta on usein kansainvälistä ja pitkälti automatisoitua, ja sillä pyritään saamaan rahaa nopeasti. (Kyberturvallisuus ja yrityksen hallituksen vastuu 2021, 8.)

Palvelunestohyökkäys ei ole murtautumista palveluun eikä se vaikuta tietojen luottamuksellisuuteen tai eheyteen. Suurin osa palvelunestohyökkäyksistä tehdään jonkin aatteen tai erimielisyyden vuoksi, ja tällaista toimintaa kutsutaan haktivismiksi. Palvelunestohyökkäyksiä tehdään myös kiristämistarkoituksessa. Hajautetun hyökkäyksen tekeminen on edullista eikä se vaadi tilaajaltaan erityisiä teknisiä taitoja. Kiristyshyökkäyksillä tavoitellaan taloudellista hyötyä. (Viestintäviraston ohje 2016, 3.)

**Hakkerointi.** Tietoverkkoon tai tietojärjestelmään voidaan tunkeutua luvatta hakkeroinnin avulla, ja siten rikollinen voi esimerkiksi tuhota tietojärjestelmässä olevia tietoja tai käyttää järjestelmää omiin tarkoituksiinsa (Sisäministeriö 2017, 10). Erilaisia hakkeroijia ja heidän tarkoitusperiänsä on käsitelty tarkemmin opinnäytetyön luvussa 3.4. Yleisesti hakkerointi mielletään siten, että rikollinen on

hakkeroinut jonkin laitteen tai palvelun, ja käyttäjä on joutunut esimerkiksi tietovuodon uhriksi. Rikollinen on saattanut tunkeutumalla saada käyttäjästä henkilökohtaisia ja yksityisiä tietoja, kuten henkilötietoja ja salasanoja. Rikollinen saattaa käyttää ja hyödyntää tietoja eri tavoin, kuten levittämällä tietoja pimeässä verkossa muille rikollisille tai kiristämällä käyttäjää eri tavoin.

Hakkerit voivat murtautua tietokoneeseen, laitteeseen tai järjestelmään muun muassa kokeilemalla eri salasanoja ja hyödyntämällä bluetooth-yhteyttä tai langatonta WI-FI-verkkoa. Salasanojen murtaminen on ollut kyberrikollisten yksi suosituimpia tapoja päästä sisään kohteena olevaan tietojärjestelmään, ja tutkimusten mukaan noin puolet tietojärjestelmiin tunkeutumisista on tehty selvittämällä jonkun käyttäjän salasana (Cyberwatch 2021 Q1, 3).

**Tietojenkalastelu.** Tietojenkalastelun (englanniksi *phishing*) avulla yritetään vaikuttaa käyttäjään ja saada henkilö antamaan sähköpostin tai verkkosivun välityksellä luottamuksellista tietoa. Tietojenkalastelusta voi olla kyse, kun pyydetään pankin nimissä sähköpostitse luottokortin numeroa ja tunnuslukua tai kun pyydetään tietoja sähköpostitse tai tekstiviestitse tekeytymällä tutuksi henkilöksi tai organisaatioksi. Viesteissä voidaan käyttää organisaatioiden ulkoasua, esimerkiksi logoa. Rikollinen on myös voinut murtaa jonkun toisen käyttäjän tilin kokonaan, jolloin viestit voivat tulla suoraan tutulta henkilöltä. (Pienyritysten kyberturvallisuusopas 228/2020, 4.)

Kohdennettu tietojenkalastelu (englanniksi *spear phishing*) on kyseessä silloin, kun tiettyyn henkilöön tai tietyn organisaation henkilöstöön kohdistetaan verkkourkintaa esimerkiksi lähettämällä sähköposti, joka näyttäisi tulevan pankilta, työtoverilta tai esimieheltä. Tällöin henkilö ei välttämättä osaa olla varovainen ja lähettää luottamuksellista tietoa rikolliselle. (Pienyritysten kyberturvallisuusopas 228/2020, 4.)

Tietojenkalastelussa voidaan hyödyntää käyttäjän manipulointia. Käyttäjälle voidaan esimerkiksi soittaa (englanniksi *vishing*) ja pyytää tietoja tekeytymällä kollegaksi tai organisaation edustajaksi. Tietoja voidaan pyytää myös tekstiviestillä (englanniksi *smishing*). (Tapoja välttyä käyttäjän manipuloinnilta, 24.9.2021.) Tietoja voidaan kalastella sähköpostien, puheluiden ja tekstiviestien lisäksi sosiaalisessa mediassa ja internetsivustoilla. Noin kolmanneksessa kiristyshaittaohjelmien levittämistapauksissa on käytetty hyväksi käyttäjiltä selville saatuja salasanoja. (Cyberwatch Q1 2021, 3.)

Viime vuosina erityisen yleistä tietojenkalastelu on ollut suomalaisten suosimassa Microsoft Office 365 -ympäristössä, jossa uhreiksi on joutunut useita satoja organisaatioita. Aiheutettujen vahinkojen määrä on kasvanut useisiin miljooniin euroihin. (Kyberturvallisuus ja yrityksen hallituksen vastuu 2021, 6.) Tietojenkalastelun voidaan katsoa olevan osa toimitusjohtajahuijauksia (CEO) ja sähköpostihuijauksia (BEC). CEO- ja BEC-huijauksista enemmän tämän opinnäytetyön luvussa 5.5.

**Kybervakoilu.** Kybervakoilussa hyödynnetään tietoverkkoja ja niihin liitettyjä laitteita ja ohjelmistoja, ja se voi kohdistua valtioihin, yksityisiin kansalaisiin, yrityksiin tai muihin organisaatioihin. Kybervakoilu on kansallisen lainsäädännön mukaan pääsääntöisesti lainvastaista toimintaa. (Turvallisuuskomitea 2018, 26) Kybervakoilu on pitkäkestoista toimintaa, ja sillä luodaan edellytyksiä erilaisille hybridioperaatioille. Kybervakoilun avulla pyritään täydentämään muita tiedonhankinnan ja vakoilun keinoja. Kybervakoilua pyritään tekemään mahdollisimman salassa, se on usein vaikeasti havaittavissa ja sen toimijoiden jäljittäminen on vaikeaa. (Cyberwatch 7.7.2021, luettu 16.10.2021.)

Kyberympäristössä tapahtuu vakoilua ja luvatonta tiedustelutoimintaa. Esimerkiksi vieraan valtion tiedustelupalvelut voivat yrittää muun muassa haittaohjelmien avulla murtautua tietojärjestelmiin ja päästä käsiksi luottamukselliseen ja salaiseen tietoon, jolla voi olla merkitystä näiden omien kansallisten etujen ajamisessa. Oikeudettomassa tiedonhankinnassa voi olla kohteena poliittinen, sotilaallinen, taloudellinen tai tieteellis-tekninen tieto, ja siksi vakoilulla aiheutetut vahingot voivat olla Suomen kansalliselle turvallisuudelle korvaamattomia. (Sisäministeriö 2017, 16.) Turvallisuusympäristön muutos on vakiinnuttanut hybridivaikuttamisen, jonka keinovalikoimaan katsotaan kuuluvan muun muassa poliittisia, diplomaattisia, taloudellisia ja sotilaallisia keinoja sekä informaatio- ja kybervaikuttamista. (Valtioneuvoston puolustusselonteko 2021, 17.)

### 4.2 Tilannekuva

Tilannekuva on tarpeen perusteella valittu, yksittäisistä tiedoista koottu esitys tilanteesta tai suorituskyvystä, mikä antaa perusteet tilannetietoisuudelle. Vastaavasti tilanneymmärrys on päättäjien ja heitä avustavien henkilöiden ymmärrys tapahtuneista asioista, niihin vaikuttaneista olosuhteista, eri osapuolien tavoitteista ja tapahtumien mahdollisista kehitysvaihtoehdoista, joita kaikkia tarvitaan päätösten tekemiseksi tietystä asiasta tai asiakokonaisuudesta. (VNST 2018, 38–39.)

Kyberrikollisuuden tilannekuvaa pyritään muodostamaan ja ylläpitämään mahdollisimman laajasti. Suomessa keskeisiä tilannekuvan muodostajia tämän opinnäytetyön näkökulmasta ovat Keskusrikospoliisin kyberrikostorjuntakeskus ja Traficomin Kyberturvallisuuskeskus. Edellä mainittujen viranomaisten julkaisuja ja ennen kaikkea raportteja, arvioita ja tilannekuvia pyritään hyödyntämään tässä opinnäytetyössä. Kansainvälisiä keskeisiä tilannekuvia muodostavat Europolin European Cybercrime Centre ja Euroopan unionin neuvosto.

Vuonna 2015 Poliisihallituksen asettamassa poliisin kybertyöryhmässä ja sen alaisissa alatyöryhmissä arvioitiin tietoverkkorikollisuuden nykytilaa ja sen kehittämistä. Työssä on pyritty tuottamaan poliisin kokonaisvaltainen kybersuunnitelma, ja poliisihallitus on järjestänyt keskustelutilaisuuden tietoverkkorikollisuuden lainsäädäntötarpeista. Tietoverkkorikollisuuden tilannekuvaa koskevassa selvityksessä kartoitettiin tietoverkkorikollisuuden tilannekuvatyön nykytilaa ja luotiin pohja poliisin

tietoverkkorikollisuuden tilannekuvatyön kehittämiselle. Toteutukseen osallistuivat Poliisiammattikorkeakoulu, poliisin kyberrikostorjuntakeskus, Viestintäviraston Kyberturvallisuuskeskus ja Tampereen yliopiston johtamiskorkeakoulu. (Sisäministeriö 2017, 30.)

Suomen kyberturvallisuusstrategian tavoitteena on parantaa eri toimijoiden tilannetietoisuutta tarjoamalla niille ajantasaista, koottua ja analysoitua tietoa haavoittuvuuksista, häiriöistä ja niiden vaikutuksista. Tietojohtoisen poliisitoimintajohtamismallin mukaan päätöksenteko perustuu rikostiedustelutietoon ja analyysitietoon ja oikea ja ajantasainen tilannetietoisuus on edellytys tietojohtoiselle poliisitoiminnalle. Poliisin tilannekuvan on oltava osa Kyberturvallisuuskeskuksen kybertilannekuvaa. Kyberrikostorjuntakeskus vastaa tilannekuvan laatimisesta tietoverkkorikollisuuden osalta. (Sisäministeriö 2017, 38.)

Suomessa muut viranomaiset ovat myös laatineet aineistoa kyberturvallisuudesta. Hyödynnettävistä aineistosta keskeisimpiä kyberrikollisuuden viitekehyksessä ovat Suomen kyberturvallisuusstrategia 2013 ja 2019, Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020, valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja *Suomen kyberturvallisuuden nykytilasta*, tavoitetilasta ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi kuin myös Tietoverkkorikollisuuden tilannekuva 2016 ja Kyberturvallisuuden strateginen johtaminen (2018). Yksityisistä toimijoista erilaisia tilannekuvia ja raportteja muodostavat muun muassa Cyberwatch Finland, F-Secure, Microsoft ja Kaspersky. Tämän opinnäytetyön kannalta keskeisiä Euroopan tilannekuvia ja uhka-arvioita laatii Europol.

Tilannekuvien ja raporttien avulla voidaan havaita ja tunnistaa uhkia ja rikollisuutta. On tärkeää, että kyberuhat kyetään havaitsemaan ajoissa, ja kyberympäristön muutoksia on seurattava reaaliajassa (Valtioneuvoston puolustusselonteko 2021, 33). Viranomaisilla on oltava riittävät toimintaedellytykset kyberrikollisuuden torjuntaan, ja siinä korostuvat ajantasainen kybertilannekuva ja uhkatiedustelu, joiden avulla voidaan ehkäistä ennakolta havaittuja uhkatekijöitä (Cyberwatch Q1 2021, 4).

**SOCTA.** Europolin laatii *vakavaa ja järjestäytynyttä rikollisuutta koskevan uhka-arvion* eli SOCTAn (englanniksi *Serious and Organised Crime Threat Assesment, SOCTA*) niiden tietojen pohjalta, joita saadaan jäsenvaltioiden lainvalvontaviranomaisilta, Europolin omista tietokannoista, muilta EU:n virastoilta, kuten Frontexilta, Eurojustilta ja EMCDDA:lta, EU:n ulkopuolisilta Europolin kumppanimailta ja yksityisiltä kumppaneilta sekä avoimista lähteistä. SOCTA sisältää analyysin vakavan ja järjestäytyneen rikollisuuden EU:lle aiheuttamista nykyisistä ja tulevista uhkista sekä suosituksia rikostorjunnan prioriteeteiksi. (Eurooppa-neuvosto 2018, 3–4.)

SOCTA-arvion prioriteetteja tutkii sisäisen turvallisuuden operatiivisen yhteistyön pysyvä komitea (COSI), joka tarkastelun pohjalta hyväksyy EU:n rikostorjunnan prioriteetit toimintapoliittista sykliä

varten ottaen huomioon jäsenvaltioiden, eri virastojen ja komission esittämät kommentit sekä muut asiaa koskevat arviot ja toimintalinjaukset. Näiden perusteella laaditaan seuraaville neljälle vuodelle strateginen suunnitelma MASP, jonka COSI hyväksyy. (Eurooppa-neuvosto 2018, 3–4.)

Kyberrikollisuus ja erityisesti tietojärjestelmiin kohdistuneet hyökkäykset, lapsiin kohdistuvat seksuaalirikokset ja muihin maksuvälineisiin kuin käteiseen rahaan kohdistuneet rikokset olivat EU:n rikostorjunnan prioriteetteja vuosina 2018–2021. (Eurooppa-neuvosto 2018, 5.)

**IOCTA.** Europolin EC3 julkaisee vuosittain IOCTA-tilannekuvaraportin (englanniksi *Internet Organised Crime Threat Assesment, IOCTA*). Europolin IOCTA-raportti on strateginen väline, joka korostaa dynaamisia ja muuttuvia uhkia tietoverkkorikollisuudessa. Raportin tarkoitus on tarjota arviointeja uusista haasteista ja tietoverkkorikollisuuden alan keskeisestä kehityksestä. Raportin koonti tapahtuu yhdessä Euroopan lainvalvontaviranomaisten ja yksityisten toimijoiden kanssa, ja sen tarkoitus on auttaa jäsenvaltioiden toimintojen priorisoinnissa ja kohdentaa resurssit oikealla tavalla kyberrikollisuuden torjumiseksi. (IOCTA 2020, 4.)

**Muut tilannekuvat ja raportit.** Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus laatii vuosittain uhkaraportin, joka kantaa nimeä *Tietoturvan vuosi, Kyberturvallisuuskeskuksen vuosikatsaus*. Lisäksi Kyberturvallisuuskeskus laatii ohjeita, oppaita, varoituksia ja ajankohtaisia julkaisuja häiriöistä ja haavoittuvuuksista sekä kuukausittain *Kybersään*, joka kertoo edellisen kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. (Kyberturvallisuuskeskus: *tilannekuva*, luettu 4.10.2021.)

Edellä mainittujen tilannekuvaraporttien ja uhka-arvioiden lisäksi muodostavat myös F-Secure, Kaspersky ja Cyberwatch Finland aineistoa. F-Secure laatii muun muassa raportteja ja muuta aineistoa, kuten tiedotteita ja uutisia, ajankohtaisista kyberuhkista ja -häiriöistä. Kaspersky laatii ajantasaisia dokumentteja, tutkimuksia, kyberturvallisuusvinkkejä, uhka-analyyseja ja tilastotietoa kyberuhista. Cyberwatch Finland laatii muun muassa osavuosikatsauksia digi- ja kyberturvasta sekä artikkeleita ja uutisia ajankohtaisista kyberasioista.

# 5 NYKYTILANNE

Kyberrikosten tekeminen on huomattavasti kustannustehokkaampaa ja kiinnijäämisriski, sekä seurausvaikutukset ovat usein matalampia kuin fyysisissä rikoksissa, mikä lisää kyberrikollisuuden houkuttelevuutta (Cyberwatch Q1 2021, 10). Tietoverkkorikoksen esitutkinta käynnistyy poliisin saatua tiedon epäillystä rikoksesta, ja joissain tapauksissa kyse voi olla asianomistajarikoksesta,

jonka esitutkinta edellyttää asianomistajan tekemää rangaistusvaatimusta. Rikosilmoitusten tekemisen voidaan katsoa olevan toivottavaa ja yhteiskunnallisesti merkityksellistä, koska ilmoitusten tekeminen tuottaa viranomaisille tietoa ajankohtaisista kyberrikoksista ja -ilmiöistä. Suomessa jätetään ilmoittamatta kyberrikoksista erinäisistä syistä, esimerkiksi koska punnittaan ilmoittamisen hyötyjä ja haittoja liiketoiminnan kannalta (CYBERDI 2021, 10). Ilmoitusten tekemättä jättäminen vaikeuttaa viranomaisten tilannekuvan muodostamista (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021).

Vuonna 2019 kyberrikollisten hyökkäykset kasvoivat huomattavasti aikaisempiin vuosiin verrattuna ja erityisesti IoT-laitteet saivat tartuntoja bottiverkkojen ja Eternal Blue -haavoittuvuuksien kautta. Vuoden 2019 kyberhyökkäysten kokonaissaldo oli 5,7 miljardia, vuonna 2018 hieman yli miljardi ja vuonna 2017 hyökkäyksiä todettiin 792 miljoonaa. (F-Secure 2019, 2–3.) Viime vuosien yleisimpiä kyberrikollisuuden muotoja ovat olleet tietojärjestelmien toiminnan häirintä haittaohjelman tai käytettävyyshyökkäyksen avulla sekä tietomurrot. Yhdysvalloissa on ollut valloilla kiristyshaittaohjelmahyökkäykset. Kansainvälinen kyberrikollisuus on uhannut yksityistä ja julkista sektoria, ja kyberrikollisuusorganisaatiot ovat kehittäneet omia liiketoimintamallejaan ja haastaneet viralliset tahot sekä resursseissa että osaamisessa. Rikolliset myyvät osaamistaan ja erilaisia työkaluja toisilleen. Kansalliset kyberhyökkäykset ovat paljastaneet kriittisiä elementtejä valtion huoltovarmuudesta ja ovat täten nousseet yhteiskunnan turvallisuuden uhkaksi. Rikollisten käyttäminen osana poliittisia keinoja on yleistynyt, ja kyberrikollisuuden vaikutus globaaliin politiikkaan on kasvanut. (Cyberwatch 7.7.2021, luettu 16.10.2021.)

Etätyön määrä kasvoi huomattavasti pandemian aikana, mikä lisäsi muun muassa palvelunestohyökkäyksiä organisaation sisäisiin palveluihin, kuten Skypeen ja VPN-ratkaisuihin. Myös koulujärjestelmiin kohdistettiin hyökkäyksiä. (Tietoturvan vuosi 2020, 7–8.) Etätyössä saatetaan käyttää työasioiden hoitamiseen oman kodin verkkoa, joka ei välttämättä ole samalla tavalla suojattu kuin työpaikan verkko. Esimerkiksi erilaiset salausjärjestelmät, tunnistautumiset ja työympäristö lisäävät väärinkäytösten riskiä. Lisäksi lukuisia sovelluksia, kuten Teams, Skype ja Zoom, otettiin käyttöön nopealla aikataululla. Muun muassa kokouksia käytiin virtuaalisesti, ja kokouksissa käsiteltyjä asioita saattoi päätyä hakkereiden tietoisuuteen. Etätyöskentely asetti selkeitä haasteita kyberturvallisuudelle.

**Euroopan trendit.** Euroopassa vuonna 2020 suurimpia kybertrendejä olivat käyttäjän manipulointi, palvelunestohyökkäykset, kiristysohjelmat ja erilaiset haittaohjelmat. Myös havaittiin, että kyberrikollisuus oli tunkeutunut lähes kaikille rikosaloille. Käyttäjän manipulointimenetelmässä kyberrikolliset hyödynsivät tietojenkalastelua muiden verkkorikollisten kanssa, esimerkiksi vaihtamalla tietoja, vääriä henkilöllisyyksiä ja järjestelmiä keskenään. Havaittavissa oli, että muiden kuin käteismaksupetosrikosten määrä kasvoi ja keskittyi tietojenkalasteluun ja käyttäjän manipulointiin. Rikollisten

palveluteollisuuden (CaaS) yhteisön saatavilla olevien tietojen ansiosta pystyivät rikolliset helpommin tehdä kohdennettuja kyberrikoksia. Tämä on suuri syy sille, minkä takia petosrikoksia pidetään edelleen suurena kyberuhkana. (IOCTA 2020, 6.)

CaaS (englanniksi *Crime-as-a-Service*) tarkoittaa rikollisten palveluteollisuutta, liiketoimintaa, joka toimii rikollisten yrittäjien virtuaalisena alamaailman markkinapaikkana. Palveluteollisuus helpottaa rikollista toimintaa muun muassa tietojenkalastelussa, koska erilaisten menetelmien ja tiedonvaihdon ansiosta ovat jopa kokemattomat rikolliset onnistuneet toteuttamaan tietojenkalastelukampanjoita. Palveluteollisuuden ansiosta rikolliset voivat vaihtaa salatusti tietoja, tiedostoja ja antaa neuvoja erilaisilla markkinapaikoilla. (IOCTA 2020, 16–17.) Rikolliset siis hyödyntävät verkkofoorumeita ja internetissä toimivia laittomiin tarkoituksiin suunnattuja Darknettejä ja tavanomaisten hakukoneiden tavoittamattomissa olevia Deepwebbejä ja muita foorumeita. Palveluteollisuutta käyttävät hyväksi myös järjestäytyneen rikollisuuden ryhmät, mikä on myös muuttanut niiden aikaisempia rakenteita. Maailmanlaajuinen kyberympäristö tarjoaa jopa ääriryhmien välisen tiedonvaihdon, verkostoitumisen, ja terroristisen materiaalin levittämisen. Alamaailman verkkofoorumeilla on tarjolla jopa rahansiirto- ja pesupalveluita, ja rikolliset hyödyntävät virtuaalivaluuttoja anonyymiin maksamiseen ja rahanpesun välineenä. Yksittäiset tilaajat ja välittäjät hyödyntävät verkkofoorumeita huumaus-, doping- ja lääkeainehankinnoissa. (Sisäministeriö 2017, 5 ja 12.)

Covid-19-pandemia aktivoi rikollisia hyödyntämään yhteiskunnan kaikkein heikoimmassa asemassa olevia. Kyberrikolliset onnistuivat muuttamaan tietoverkkorikollisuuden muotoja pandemiaan sopiviksi. Rikolliset käyttivät kriisiaikaa hyväksi muun muassa käyttäjän manipuloinnissa, palvelunestohyökkäyksissä ja lapsiin kohdistuvien seksuaalirikosmateriaalien jakamiskiristysohjelmissa. Pandemian aika lisäsi erilaisia tietoturvaongelmia ihmisten tehdessä etätöitä tai opiskelijoiden opiskellessa etänä. Etäopiskelu lisäsi lapsiin kohdistuvia seksuaalirikoksia ja hyväksikäyttöä. Verkossa tapahtuvan CSAM-hyväksikäytön (lapsiin kohdistuva seksuaaliväkivaltamateriaali) ja niin sanotun suoratoistorikollisuuden määrä jatkoi kasvuaan edellisvuosiin verrattuna. (IOCTA 2020, 6.)

Kyberrikollisuuden uhka on kasvanut viime vuosina raportoitujen hyökkäysten määrän ja kehittymisen osalta. Kyberrikoksia on todennäköisesti raportoitu merkittävästi vähemmän kuin, niitä on todellisuudessa tapahtunut. Esimerkiksi erilaiset petosjärjestelmät hyödyntävät digitalisaation aikakautta ja kohdistuvat yksityishenkilöihin, yrityksiin ja julkisen sektorin organisaatioihin. (SOCTA 2021, 12.)

**Suomen trendit.** Kyberrikollisuus on Suomessa jatkanut vuosittain kasvuaan, kun taas perinteinen rikollisuus on maltillisessa laskusuunnassa. Kyberrikollisten tekotavat ovat kehittyneet, ja rikollisiin tekoihin paneudutaan entistä tarkemmin ja yksityiskohtaisemmin. (Tietoturvan vuosi 2018, 8.)

Suomessa suurin osa kyberrikollisuudesta on tietomurtoja ja vain pieni osa tapauksista on tietojärjestelmien tai -verkkojen häirintätapauksia. Tämä erottaa Suomen globaaleista trendeistä. Suomalaisista tietomurroista suurin osa kohdistuu yksityishenkilöihin tai yrityksen työntekijöiden henkilökohtaisiin sähköposti- tai verkkopalvelutileihin. (Cyberwatch Q1 2021, 10.) Suomessa yksityisiin henkilöihin kohdistetaan erilaisia huijauksia ja tietojenkalastelua, ja niissä hyödynnetään usein käyttäjän manipulointia.

Keskusrikospoliisin Christian Jämsén (2019) on eurooppalaisten trendien lisäksi määritellyt suomalaisia kyberrikollisuuden trendejä, jotka kohdistuvat yksityishenkilöihin. Näitä ovat rakkaushuijaukset, identiteettivarkaudet ja tilausansat. (Jämsén 2019, 4.) Ajankohtaisia ja yleisiä trendejä ovat myös robottipuhelut, maksuvälinepetokset sekä erilaiset verkkokiristykset sekä kiristyshaittaohjelmat.

Robottipuhelussa on kyse puhelusta, joka soitetaan automaattisesti puhelinnumerot valitsevalla ohjelmistolla miljoonille ihmisille päivittäin. Automaattisissa puheluissa voidaan toistaa ennalta äänitettyjä viestejä. (Mitä robottipuhelut ovat ja kuinka lopetat ne? Luettu 7.10.2021.)

Yritykset ja organisaatiot ovat entistä riippuvaisempia digitaalisista palveluista ja järjestelmistä, ja niihin kohdistuu entistä enemmän kyberuhkia. Yritykset ja organisaatiot eivät välttämättä ole aina varautuneet riittävällä tasolla kyberuhkiin, tai ymmärrystä uhkista ja vaaroista ei ole. Viime vuosina yritykset ja organisaatiot ovat kehittäneet kyberturvallisuuttaan, etenkin suurissa yrityksissä, mutta pienissä yrityksissä uhkia ei ole välttämättä tunnistettu. Yritykset ja organisaatiot ovat otollisia kohteita. Niihin voidaan kohdistaa suuria taloudellisia vaatimuksia ja niiden toimintaan voidaan vaikuttaa eri tavoin. Haitat ja kustannukset voivat olla suuria, minkä takia kyberosaamiseen tulisi kiinnittää huomiota, ja tietoturvasta huolehtia esimerkiksi tietoturvapalveluiden ja -tuotteiden avulla. Suomalaisiin yrityksiin ja organisaatioihin kohdistuu erilaisia kyberrikollisuuden ilmiöitä.

Alla olevien kappaleiden tarkoitus on tuoda esiin sekä viimeisen muutaman vuoden aikaiset että nykyiset kyberrikostrendit. Kappaleissa on tarkoitus myös selittää trendejä, mikäli niitä ei ole vielä tähän mennessä opinnäytetyössä avattu. On kuitenkin huomioitava, että Euroopassa ja Suomessa yksityisiin henkilöihin ja organisaatioihin kohdistuvat trendit ovat osittain samankaltaisia.

### 5.1 Kiristyshaittaohjelmat

Kiristyshaittaohjelma salaa tai manipuloi laitteella olevia tietoja ja tyypillisesti vaatii käyttäjältä lunnaita salauksen purkamisesta. Esimerkiksi tietokoneeseen voi tulla kiristyshaittaohjelma sähköpostin liitetiedostona, kun käyttäjän avatessa tiedoston, latautuu haittaohjelma koneelle, minkä jälkeen ohjelma voi muuntaa tiedostoja salakirjoitettuun muotoon. Tällöin tiedostoja ei voida avata ilman oikeaa salauksenpurkuavainta. Haittaohjelman levittäjä lupaa toimittaa avaimen lunnaita vastaan.

(Turvallisuuskomitea 2018, 32.) Kiristystroijalaisten käyttämiin hyökkäysvektoreihin (hyökkäysväline) sisältyvät etätyöpöytäprotokolla, tietojenkalastelusähköpostit ja ohjelmiston haavoittuvuudet. Yksityishenkilöt ja yritykset voivat joutua kiristysohjelman hyökkäyksen uhriksi. Kiristysohjelmatyypeistä suosituimpia ovat lukitseva ja salaava kiristysohjelma, jossa lukitseva kiristysohjelma estää tietokoneen perustoiminnot ja salaavan tavoitteena on salata tärkeät tiedot häiritsemättä tietokoneen perustoimintoja. (Kiristysohjelmien tunnistaminen, luettu 4.10.2021.)

Vuonna 2018 tyypillisiä yksityishenkilöihin kohdistuvia verkkokiristyksiä olivat tappouhkaus- ja pornokiristys. Tappouhkauskiristyksessä huijari väittää olevansa palkkamurhaaja, jonka tulisi tappaa uhrinsa, mutta huijari voi jättää teon tekemättä, mikäli uhri maksaa kovat lunnaat. Pornokiristyksessä huijari väittää murtaneensa kohteensa tietokoneen ja asentaneensa siihen vakoiluohjelman, joka on tallentanut uhrin katsomassa esimerkiksi aikuisviihdettä. Huijari ei julkaise arkaluonteista tallennetta, jos kohde maksaa lunnaat. (Tietoturvan vuosi 2019, 29.)

Vuonna 2019 suurin osa honeypot-verkostoista löytyneistä haittaohjelmista oli erilaisia Mirai-versioita (F-Secure 2019, 7). Hunajapurkki (englanniksi *honeypot*) toimii ansana hakkereille, jossa tietojärjestelmä toimii syöttinä kyberrikollisille (Mitä hunajapurkilla tarkoitetaan? Luettu 4.10.2021). Kiristysohjelmien lähettämä roskapostin määrä väheni vuoden aikana, mutta itse kiristyshaittaohjelmat tarkensivat kohdistustaan ja vaikuttivat kohteisiinsa vahvemmin. Haitta oli suurempaa, ja suuryrityksiltä vaadittiin satojen tuhansien dollareiden lunnasvaatimuksia. (F-Secure 2019, 7.)

Vuonna 2019 Big game hunting -ilmiössä edistyneet rikollisryhmät saalistivat kohteikseen yrityksiä tai organisaatioita, joiden toimintaa laajalle levinnyt kiristyshaittaohjelmatapaus haittasi merkittävästi. Rikollisryhmät olivat erikoistuneet kyberrikollisuuden eri osa-alueisiin siten, että yksi ryhmä keskittyi haittaohjelmien laajaan levittämiseen, toinen ryhmä keräsi haittaohjelman avulla tietoja, ja kolmas osti pääsyn sopiviin kohteisiin ja asensi kiristyshaittaohjelman, joka salasi kohteen koko tietoverkon palvelimet, verkkolevyt ja tärkeimmät työasemat. (Tietoturvan vuosi 2019, 21.) Kohteen toiminta täten lamautui ja tietojen vapauttamiseksi vaadittiin suuria lunnaita, esimerkiksi kymmeniä miljoonia euroja. Vuonna 2020 esiintyi ilmiö, missä kohdetta kiristettiin myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimusten tehostamiseksi. (Kybersää 2020, 6.)

Tyypillisiä yrityksiin kohdistuvia kiristyksiä olivat myös roskaposti- ja palvelunestokiristykset. Roskapostikiristyksessä rikollinen uhkasi pilata yrityksen maineen aloittamalla valtavan roskapostikampanjan yrityksen nimissä, ellei lunnaita makseta. Palvelunestokiristyksessä rikollinen uhkasi kaataa yrityksen tietoverkon suurella liikennetulvalla, mikäli yritys ei maksa vaadittuja lunnaita. Uhkauksiin voi liittyä myös pieni palvelunestohyökkäyksen näyte, jollaisia kyberrikolliset toteuttavat ilmaiseksi. (Tietoturvan vuosi 2019, 29.)

Ylipäätänsä vuonna 2020 kiristyshyökkäykset kasvoivat maailmalla. Suomessa organisaatioita kiristettiin palvelunestohyökkäyksillä, mutta useimmiten kiristysviestit olivat aiheettomia eikä hyökkäyksiä kiristyksistä huolimatta toteutettu. Tyypillisesti vaadittu rahasumma oli pieni ja kiristysviestin lähettäjät vaihtelivat. (Tietoturvan vuosi 2020, 8.) Vuoden 2020 kiristyshaittaohjelmaryhmistä 40 prosenttia käytti kiristyshyökkäyksissä tietojen varastamista ja salaamista. Organisaatioilta estettiin pääsy omiin järjestelmiin, ja lukitsemisen lisäksi organisaatioilta anastettiin dataa ja tietoja. Organisaatioiden kieltäydyttyä maksamasta lunnaita uhkasivat rikolliset vuotaa anastettuja tietoja. (F-Secure 2020, 7.) Myös suomalaiseen kriittisen infrastruktuurin järjestelmään kohdistettiin kiristyshaittaohjelmahyökkäys toukokuussa 2020 (Tietoturvan vuosi 2020, 38).

Arvioidaan, että vuoden 2021 loppuun mennessä kiristysohjelmat hyökkäävät yrityksiä kohtaan joka 11. sekunti aiheuttaen jopa 20 miljardin dollarin vahingot. Kiristysohjelmahyökkäykset ovat organisaatioiden, asiakkaiden ja työntekijöiden ongelma. Ne kaikki kärsivät niiden aiheuttamista vahingoista. (Vuoden 2020 tunnetuimmat kiristysohjelmahyökkäykset, 4.10.2021.) Tutkimusten mukaan kolmannes ransomware-hyökkäyksistä tehdään heikkojen salasanojen avulla (Cyberwatch Q1 2021, 7).

### 5.2 Kryptovaluutta ja louhintahaittaohjelmat

Kryptovaluutta on kryptografiaan perustuva verkkoraha, joka ei ole sidoksissa keskuspankkeihin tai valtioihin. Tämä on yksi syy sille, miksi rikolliset suosivat kryptovaluuttaa. Kryptovaluuttaa ei lasketa pankeista liikkeelle perinteisen rahan tavoin, vaan tietokoneet tuottavat kryptovaluuttaa ratkaistessaan erittäin haastavia algoritmeja. (Haasio 2017, 6.) Kryptovaluuttaa voidaan hankkia tai ostaa louhimalla (englanniksi *mining*) eli käyttämällä tietokoneen laskentatehoa valuuttasiirtojen käsittelyyn ja verkon toiminnan turvaamiseen. Kryptovaluuttojen olemassaolo perustuu kryptovaluuttaohjelmia ajavien tietokoneiden vertaisverkossa ylläpitämään laskentatehoon. (Traficom 228/2020, 18.) Tällä hetkellä on olemassa satoja erilaisia kryptovaluuttoja, mutta ehkä tunnetuimpana kryptovaluuttana voidaan pitää Bitcoinia. 29.10.2021 bitcoineja oli kierrossa noin 18,8 miljoonaa, ja niitä louhitaan 21 miljoonaan asti (Coinmarketcap, luettu 29.10.2021).

Kryptovaluutat käyttävät toimiakseen lohkoketjua (englanniksi *blockchain*), jota päivitetään säännöllisesti tiedoilla kaikista transaktioista, jotka tapahtuivat edellisen päivityksen jälkeen. Transaktioiden sarja yhdistetään lohkoksi monimutkaisten matemaattisten prosessien avulla. Kryptovaluutat luottavat yksityishenkilöiden tietojenkäsittelytehoon uusien lohkojen tuottamiseksi ja siten palkitsevat tietojenkäsittelytehoa tuottavia henkilöitä (louhijoita). (Mitä on kryptokaappaus? Luettu 4.10.2021.) Louhinnan tuloksena markkinoille lasketaan kryptovaluuttoja ja lohkoissa muodostuu uutta valuuttaa, mikä päätyy louhintapalkkion muodossa louhijalle. Useimmiten tämän jälkeen varat

siirtyvät louhijalta markkinoille kaupankäynnin kohteeksi. Itse louhinnassa käytetään suurta laskentatehoa, minkä takia muun muassa sähkönkulutus on kallista ja hidasta. Louhinnassa itsessään ei ole mitään laitonta, mutta liiketoiminta ei välttämättä ole laillisesti kannattavaa.

Kryptovaluutan louhinta(salaus)haittaohjelman (englanniksi *cryptomining*) avulla louhintaliiketoiminta voidaan ulkoistaa ulkopuolisille niin sanottuna hyötykuormana. Haittaohjelma käyttää tartunnan saaneiden koneiden tehoa siten, että louhinta vie uhrin osan prosessitehosta. Louhintahaittaohjelmaa levittämällä rikolliselle ei synny louhinnasta kuluja, jos hyötykuorma siirretään ulkopuolisille. Haittaohjelma voi siten aiheuttaa merkittävää häiriötä, vaikka sillä ei välttämättä ole suurta vaikutusta uhreihin. (IOCTA 2018, 8, 19 ja 29.) Kryptokaappauksen (englanniksi *cryptojacking*) eli toiminnan, jossa käyttäjien laitteita käytetään salaa ja luvattomasti kryptovaluutan louhintaan (Interpol 2020, 1), katsottiin olevan riski Euroopan kyberturvallisuudessa (IOCTA 2019, 54). Kryptokaappaus on kyberrikos, jossa rikolliset käyttävät tietokoneita, älypuhelimia, tabletteja ja palvelimia kryptovaluutan louhintaan. Kyberrikollinen hakkeroi laitteen ja asentaa kryptokaappausohjelmiston, joka toimii taustalla louhien kryptovaluuttaa ja varastaen kryptovaluuttalompakkoja. Uhrit eivät välttämättä havaitse ohjelmistoa tai eivät ymmärrä laitteen suorituskyvyn hidastuessa, että kyseessä saattaa olla kryptokaappausohjelma. (Mitä on kryptokaappaus? Luettu 4.10.2021.)

Kryptolouhintahaittaohjelmat olivat selkeästi esillä Europolin vuoden 2018 ja 2019 IOCTA-uhka-arvioissa, mutta ei enää vuoden 2020 arviossa. Kryptolouhintahaittaohjelmia ja niiden aiheuttamia vahinkoja on vaikea tutkia ja mitata, koska käyttäjät eivät välttämättä edes tiedä tulleensa uhriksi. (IOCTA 2018, 19.) Vuonna 2020 ohjelmien aktiivisuuden arvioitiin saavuttaneen huippunsa vuonna 2018 ja havaittavissa oli, että se väheni vuonna 2019. Kohteille aiheutuneet vahingot olivat edelleen melko pieniä, ja havaittavissa oli, että väärinkäytöksistä raportoitiin harvoin viranomaisille. (IOCTA 2019, 54.)

Vuonna 2018 suomalaiseen terveydenhuollon tietojärjestelmiin onnistuttiin asentamaan haittaohjelma (IOCTA 2018, 19), jossa tietojärjestelmiin vaikutti virtuaalivaluuttaa louhiva ja itsestään leviävä WannaMine-haittaohjelma (Tietoturvan vuosi 2018, 11). Samana vuonna varoiteltiin virtuaalivaluutan louhintahaittaohjelmista IoT-laitteissa (Kybersää kesäkuu 2018, 22). Rikolliset hankkivat tulojaan louhimalla virtuaalivaluuttaa kohteiden tietokoneen resursseilla. Louhintaa onnistuttiin tekemään verkkosivuilla vierailevan käyttäjän selaimessa, joten haittaohjelmatartuntaa ei edes tarvittu uhrin koneelle. (Tietoturvan vuosi 2018, 11 ja 46.) Vuonna 2020 tehtiin Suomessa ensimmäisiä automatisoituja hyökkäyksiä, joissa hyökkääjä asensi louhintahaittaohjelman kaikkiin hallinnan piirissä oleviin palvelimiin (Kybersää kesäkuu 2020, 7).

Yleisesti ottaen kryptovaluutat ja niiden kasvu on yhä kasvava huolenaihe, koska yhteistä sääntelyjärjestelmää ei ole olemassa ja valuutat tarjoavat nimettömyyttä. Kryptovaluutat ovat edelleen rikollisille tärkeä keino maksaa rikollisista palveluista ja tuotteista. Kryptovaluuttojen hajauttaminen ja puolinimettömyys tekevät niistä edelleen houkuttelevia rikollisille liiketoimille. Kyberrikolliset käyttävät yleisesti kryptovaluuttoja, ja niitä käytetään maksuvälineenä korruptoituneille virkamiehille sekä uusissa rahanpesutekniikoissa. (SOCTA 2021, 26, 29 ja 32.) Yleisesti voidaan todeta, että kryptovaluuttojen luotettavuuteen liittyy edelleen riskejä. Alati kasvava kryptovaluutta-ala, kryptovaluuttaliikenne ja valuutan käyttö tuovat haasteita viranomaisille rahaliikenteen valvomiseen.

### 5.3 Palvelunestohyökkäykset

Aikaisemmin luvussa 4.1 todettiin, että hajautetussa palvelunestohyökkäyksessä lähetetään kohteeseen tietoliikennettä useista lähteistä samanaikaisesti ja täten ylikuormitetaan kohde ja aiheutetaan sille palvelunestotila.

Kiristysohjelmahyökkäyksissä haittaohjelma salaa uhrin datan ja tiedostot, ja täten ne poikkeavat kiristyskampanjoista, joissa käytetään hajautettua palvelunestohyökkäystä. Palvelunestohyökkäyksessä vaikutetaan uhreihin liikenteen määrällä ja toiminta luvataan lopettaa maksua vastaan. (Vuoden 2020 tunnetuimmat kiristysohjelmahyökkäykset, luettu 4.10.2021.)

Vuonna 2017 palvelunestohyökkäykset olivat yksi yleisimmistä kyberrikoksista Euroopassa ja sitä pidettiin taloussektorilla yhtenä suurimmista uhkista. Palvelunestohyökkäykset lisääntyivät, koska niitä pystyivät toteuttamaan myös osaamattomammat kyberrikolliset. (IOCTA 2018, 24–25.) Esimerkiksi Ruotsissa vuonna 2017 palvelunestohyökkäyksellä pysäytettiin koko junaliikenne tunneiksi kuormittamalla Trafikverketin järjestelmää (ComputerSweden 2017, luettu 6.10.2021). Vuonna 2018 hajautettuja palvelunestohyökkäyksiä pidettiin yhtenä keskeisenä kyberrikollisuuden uhkana. Edellisiin vuosiin verrattuna kiristyselementti osana hyökkäyksiä ja etenkin niiden motiivina vahvistui. Myös hyökkäyksissä havaittiin ideologisia ja poliittisia piirteitä. Kohteina olivat yleisimmin rahoitusalan instituutiot ja julkisen sektorin toimijat, kuten poliisi ja paikallishallinnot. (IOCTA 2019, 6 ja 22.)

Vuonna 2019 hajautettuja palvelunestohyökkäyksiä pidettiin edelleen yhtenä suurimpana kyberrikollisuuden trendinä. Yksityisen sektorin ja jäsenvaltioiden toimijat havaitsivat hajautetuissa palvelunestohyökkäyksissä uusia ilmiöitä. Hyökkäykset kasvoivat massiivisesti, yksinkertaisten hyökkäysten määrä kasvoi, hyökkäyksiä kohdennettiin entistä tarkemmin ja ne olivat osiltaan automatisoituja. Hyökkäykset kohdennettiin aikaisempaa tarkemmin tiettyjä toimialoja ja tietojärjestelmiä kohtaan, ja arvioiden mukaan automatisoidut hyökkäykset kasvoivat todennäköisesti palveluteollisuuden takia. Palveluteollisuuden ansiosta kyberrikolliset voivat ostaa automatisoituja työkaluja ja käyttää niitä omiin tarkoituksiinsa. Tämä tekee hyökkäyksestä edullisempaa ja helpompaa. Myös

vanhat toimintatavat olivat edelleen käytössä uusien ohella. Hyökkäyksiä kohdistettiin telekommunikaatio- ja teknologiayrityksiä kohtaan entistä enemmän. Hyökkäyksiä kohdistettiin myös IoT-laitteisiin ja etenkin laitteisiin, joissa suojaukset olivat heikkoja ja päivitykset vanhentuneita. (IOCTA 2020, 24 ja 32–33.)

Palvelunestohyökkäykset ovat olleet pitkään tunnettu ja jatkuva uhka, niin myös vuonna 2020, jolloin kyberrikolliset kohdistivat aiempaa enemmän hyökkäyksiä pienempiin organisaatioihin. Pienemmillä organisaatioilla voi olla alhaisemmat turvallisuuskyvykkyydet, ja tästä syystä ne voivat olla potentiaalisia kohteita. Hyökkäyksiä kuitenkin edelleen toteutettiin julkisia laitoksia ja kriittisiä infrastruktuureja kohtaan. Kyberrikolliset ajastivat jatkuvia hyökkäyksiä, ja hyökkäysten lopettamiseksi oli kohteen maksettava vastineeksi lunnaita. (SOCTA 2021, 41.)

Palvelunestohyökkäyksiin on varauduttu viime vuosina paremmin, mutta niitä käytetään nykyään myös kiristyshaittaohjelmahyökkäyksen lunnasvaatimusten tehostamiseksi ja etenkin syksyllä 2020 kiristyshyökkäykset maailmalla lisääntyivät. Esimerkiksi yritys voi saada hyökkäyksen ensivaiheessa alalla tunnetun rikollisryhmän tai yksittäisen toimijan nimissä lähetetyn sähköpostin, jossa vastaanottajalta kiristetään yleensä bitcoineja, jotta hyökkäystä ei toteutettaisi. Rikollinen voi tehostaa uhkausviestiään lyhyillä, mutta voimakkailla palvelunestohyökkäyksillä, joilla yritetään pakottaa kohde maksamaan rahat isompien hyökkäysten välttämiseksi. (Tietoturvan vuosi 2020, 7–8.)

Vuonna 2017 Ahvenanmaalla havaittiin palvelunestohyökkäysten sarja, jota voidaan pitää poikkeuksellisena sen keston, volyymin ja kohteiden runsauden takia (Tietoturvan vuosi 2017, 14). Vuonna 2018 tilastojen mukaan 75 prosenttia kaikista Suomessa tapahtuvista palvelunestohyökkäyksistä kesti alle 15 minuuttia. Suomessa nähdyt palvelunestohyökkäykset olivat volyymeiltaan noin 1–10 Gbit/s (gigabittiä sekunnissa). Hyökkäyksiä, joiden voima oli yli 10 Gbit/s, nähtiin useita viikoittain, ja vuoden suurin hyökkäys oli voimaltaan noin 90 Gbit/s - se kesti useita tunteja. Valtion palveluiden toimintaa heikennettiin suomi.fi-tunnistuspalveluun tehdyillä hyökkäyksillä. Hyökkäyksen toteutuksessa käytettiin erilaisia tekniikoita, joista yleisimmät olivat reflektiohyökkäys ja murretuilta päätelaitteilta lähetetty verkkoliikenne. (Tietoturvan vuosi 2018, 17.)

Palvelunestohyökkäysten motiivina on usein häirintä, rahallisen hyödyn tavoittelu sekä halu ja kiinnostus kokeilla hyökkäyksen vaikutuksia. Määrällisesti katsottuna palvelunestohyökkäykset ovat yleisiä, mutta vuonna 2019 hyökkäyksistä noin 80 prosenttia kesti alle 15 minuuttia. Hyökkäysten kohteet vaihtelevat, mutta viime vuosina oppilasjärjestelmä Wilma on korostunut palvelunestohyökkäyksissä. Vuonna 2019 eduskuntavaalien aikaan tehtiin yksi palvelunestohyökkäys, jota KRP tutkii epäiltynä törkeänä tietoliikenteen häirintänä. Myös Suomessa todettiin, että palvelunestohyökkäysten tekeminen on teknisesti helpompaa kuin aikaisemmin ja että palveluna ostamalla hyökkäys

ei vaadi tekijältä omaa teknistä osaamista. Hyökkäyksistä 69 prosenttia oli volyymiltaan yli 1 Gbit/s ja 12 prosenttia yli 10 Gbit/s. (Tietoturvan vuosi 2019, 16 ja 46.)

### 5.4 Rakkaushuijaus ja tilausansat

Rakkaushuijauksesta tai nettihuijauksesta on kyse silloin, kun rikollinen etsii uhrejaan esimerkiksi seuranhakupalveluista. Rikollinen voi myös lähestyä kohdetta sosiaalisen median tai sähköpostin kautta. (Europol EC3 ym. 2021, Deittihuijaus.) Kyseessä voi olla esimerkiksi tapaus, jossa uhriin otetaan yhteyttä väärennetyllä profiililla seuranhakupalvelun kautta. Yhteydenpidossa rikollinen pyrkii muodostamaan luotettavan ja syvän suhteen. Tyypillisesti huijari on kehittänyt tarinan, jossa on jonkinlainen uhka tai ongelma, joka taas ratkeaa uhrin lainatessa rahaa rikolliselle. (Viestintävirasto 2017, 4.) Huijarit voivat pyytää uhrilta maksuja ja kerätä henkilökohtaisia tietoja, esimerkiksi pankkitilitietoja ja luottokorttinumeroita (SOCTA 2021, 61).

Niin sanotuilla nigerialaishuijauksilla tai -kirjeillä tarkoitetaan huijausta, joka perustuu uhrin hyväuskoisuuden väärinkäyttöön. Kyseessä voi olla rakkaus- tai petoshuijaus, jossa uskotellaan, että rahaa siirtämällä saadaan esimerkiksi lottovoitto tai suuri perintö (Viestintävirasto 2017, 5). Tyypillisesti huijarille maksetaan pieniä maksuja, esimerkiksi tulleihin, välityspalkkioihin ja rahansiirtokuluihin. Ensimmäisen maksusuoritteen jälkeen tulee uusi rahapyyntö ja sitten seuraava, aina niin pitkään kuin maksujen maksamista jatketaan. Huijaukset ovat pääsääntöisesti kohdistettu suurelle määrälle ihmisiä, joista pieni osa lankeaa huijaukseen. Huijaukset ovat ammattimaista ja kansainvälistä rikollisuutta. Summat ovat pääsääntöisesti pieniä, vaikka Suomessakin on ollut tapauksia, joissa tavalliset kansalaiset ovat maksaneet rikollisille kymmeniätuhansia euroja. (Turvallisuuskomitea, Kodin kyberopas 2017, 53.) Uhrille voidaan uskotella, että esimerkiksi perinnön voi lunastaa antamalla pankkitiedot tai siirtämällä tietyn rahasumman perinnön käsittelystä aiheutuvia kuluja varten. Summaa tai perintöä ei koskaan kuitenkaan tule. Yleisimmin huijauksissa uhria lähestytään sähköpostilla, tekstiviestillä tai postilla. (Näin meitä huijataan 2017, 5.)

Tilausansalla tarkoitetaan huijausta, jossa kuluttajaa erehdytetään tilaamaan jotain mitä hän ei ymmärrä tilaavansa. Tilausansoissa voidaan tarjota ensin ilmaista tai erittäin halpaa kokeilueräätä jotain tuotetta, mikä saattaa johtaa pidempään ja kalliimpaan tilaukseen. Tilausansaan voi joutua tilaamalla jotain tai osallistumalla johonkin kilpailuun tai kyselyyn verkossa. Välillä tilauksen peruminen saattaa olla hankalaa. (Sanastokeskus TSK: *tilausansa.)*

Tilausansasta voi olla kyse myös silloin, kun käyttäjälle luvataan esimerkiksi uusi älypuhelin tai muu houkutteleva tuote eurolla. Tällöin taustalla saattaa olla luottokortti- tai pankkitietojen kalasteluyritys ja/tai tilausansa. Tilausansassa voidaan yrittää saada kuluttaja tilaamaan mainoksen tai viestin pohjalta jotain, mitä kuluttaja ei ole ymmärtänyt tilaavansa. Erehdyttäminen voi olla tahatonta tai tahallista. (Viestintävirasto 2017, 6.)

Tilausansaan voi myös joutua mainoksen, huijauksen, someviestinnän, tekstiviestin, nettihaun tai ketjukirjeen kautta. Ansan verukkeena voi olla aikaisemmin mainittujen lisäksi arvonta tai saapumisilmoitus. Ansassa uhri voi tietämättään osallistua johonkin kuukausimaksulliseen palveluun, josta on mainittu sivuston pienellä painetussa tekstissä. Siten luottokorttitiedot voivat jäädä rikolliselle ja uhrin tililtä tapahtuu joka kuukausi säännöllinen veloitus. (Tietoturvan vuosi 2018, 28.)

### 5.5 Toimitusjohtajahuijaus ja BEC-huijaus

Tietojenkalastelun voidaan katsoa olevan osa CEO- ja BEC-huijauksia. Tietojenkalastelulla rikollinen pyrkii saamaan haltuunsa esimerkiksi tietojenkalasteluviestillä (sähköpostilla) käyttäjätunnuksia, pankkitunnuksia tai salasanoja tai muita käyttäjälle tai organisaatiolle arvokkaita tietoja, kuten maksukorttitietoja. (Europol EC3 ym. 2021, Tietojenkalasteluviestit.)

Toimitusjohtajahuijauksessa (englanniksi CEO *fraud*) sekä ”yrityksen sähköposti vaarantunut” -huijauksessa (englanniksi *business email compromise*, *BEC*) yrityksen raha- tai maksuliikenteestä vastaava työntekijä huijataan maksamaan valelasku tai tekemään muu siirto yrityksen varoista esimerkiksi siten, että huijari soittaa tai lähettää sähköpostia työntekijälle toimitusjohtajaksi esiintyneenä. Huijari pyytää kiireellistä maksusuoritusta, ja samalla työntekijää pyydetään ohittamaan tavanomaiset valtuuskäytännöt. (Europol EC3 ym. 2020, BEC-huijaus.) Huijari tyypillisesti vetoaa kiireeseen ja luottamuksellisuuteen sekä väittää, ettei pysty viestimään. (Tietoturvan vuosi 2019, 28).

Vuonna 2018 BEC-huijausta ei enää pidetty uutena ilmiönä. Rikolliset olivat kehittäneet menetelmiään ja keksineet uusia toimintatapoja BEC-tekniikkaa hyödyntäen. BEC-huijauksissa hyödynnettiin käyttäjän manipulointia, ja niissä esiinnyttiin esimerkiksi yrityksen työntekijänä, toimitusjohtajana tai muuna toimihenkilönä. Käyttäjän manipuloinnin avulla rikolliset onnistuivat huijaamaan työntekijöitä ja johtajia. Kohteet olivat usein yrityksiä, joilla oli siirtoyhteyksiä ulkomaisten toimittajien kanssa. Kyberrikolliset hyödynsivät huijauksissaan yrityksen tapaa tehdä liiketoimintaa. Käyttäjän manipuloinnin lisäksi BEC-huijauksissa hyödynnettiin myös teknisiä toimenpiteitä, kuten haittaohjelmia ja tunkeutumista verkkoon. BEC-huijausten katsottiin olevan osa laajempaa kyberturvallisuuden verkkohuijauskampanjaa. (IOCTA 2019, 40.)

Vuonna 2019 hyödynnettiin käyttäjän manipulointia osana sähköposteihin pääsyä ja pankkisiirtoja. Samana vuonna BEC-huijaukset aiheuttivat valtavia menetyksiä ja toimeentulon häiriöitä eri liiketoimille. CEO-huijauksissa korostuivat valelaskujen tehtailu sekä rikollisen esiintyminen toimitusjohtajana tai muuna yrityksen työntekijänä. Näiden toimintatapojen avulla kohteet suorittivat rahasiirtoja rikollisten tileille. Huijaukset olivat myös entistä kohdennetuimpia, ja niissä hyödynnettiin muun muassa useita eri kieliä ja niiden oikeellisuutta, paikallisia yhteyksiä ja jopa tekoälyn avulla toimitusjoh-

tajan ääntä. Rikokset kohdistuivat eri järjestöihin ja yrityksiin, mutta havaittavissa oli niiden keskittyminen entistä pienempiin yrityksiin. Vuonna 2020 BEC-huijauksia pidettiin yhtenä suurimmista ja kasvavimmista uhkista viranomaisille ja yksityiselle sektorille. (IOCTA 2020, 47.)

Suomessa toimitusjohtajahuijauksiksi kutsutaan sellaisia huijauksia, joissa organisaation maksuliikenteestä vastaavaa henkilöä lähestytään johtajaksi tekeytyen ja pyydetään suorittamaan kiireellisesti jokin maksu ulkomaalaiselle tilille. Rikollinen vetoaa luottamuksellisuuteen ja väittää olevansa hankalassa tilanteessa, minkä takia toiminnan on tapahduttava nopeasti. Yritysten lisäksi toimitusjohtajahuijauksien kohteiksi voivat joutua urheiluseurat, kirjastot, sairaalat ja seurakunnat. (Tietoturvan vuosi 2019, 28.)

Tyypillisiä huijauksia olivat myös palkanmaksu- ja lahjakorttihuijaukset. Palkanmaksuhuijauksessa rikollinen esiintyi johtajana ja pyysi organisaation palkanlaskijaa muuttamaan palkkatilin huijarin tiliksi. Lahjakorttihuijauksessa rikollinen esiintyi johtajana ja pyysi järjestelmään nopeasti lahjakortteja, joiden koodit huijari pystyi muuttamaan rahaksi muualla. (Tietoturvan vuosi 2019, 29.)

Vuonna 2019 esiintyi teknisen tuen huijauksia, jossa huijari kertoi koneessa olevan ongelma, esimerkiksi haittaohjelma. Myös laskutuspetokset olivat edelleen yleisiä ja aiheuttivat tuntuvia taloudellisia menetyksiä organisaatioille. Eräs kansainvälinen rikollisryhmä esiintyi Finanssivalvonnan ja lakitoimistojen nimissä ja siten yritti päästä käsiksi suurten yrityskauppojen varainsiirtoihin. Laskutuspetoksien osalta havaittiin, että teot huomattiin usein vasta viikkoja vahingon jälkeen ja täten rahojen palauttaminen oli merkittävästi vaikeampaa. (Tietoturvan vuosi 2020, 14.)

### 5.6 Petokset ja maksuvälinepetokset

Huijausviesteistä kärsivät päivittäin yksityisten henkilöiden lisäksi organisaatiot. Huijausviesteillä pyritään viemään tietoja ja rahaa. Viestit voivat olla ilmiselviä tai taitavasti tehtyjä, kohdennettuja ja täysin uskottavia. (Tietoturvan vuosi 2019, 5.) Tyypillistä petosrikollisuutta vuonna 2018 olivat perinteiset huijaukset kotimaisilla kauppapaikoilla, sähköpostihuijaukset ja nigerialaiskirjeet (Tietoturvan vuosi 2018, 8).

Yleisesti petosrikoksissa tekijä tavoittelee itselleen taloudellista hyötyä kohdetta erehdyttämällä. Uhrille petoksesta seuraa usein taloudellista vahinkoa. Petosten tekeminen on siirtynyt entistä enemmän tietoverkkoihin, koska sähköpostin ja internetin avulla rikolliset tavoittavat suuria ihmismääriä helposti ja lähes olemattomin kustannuksin. Huijauksille tyypillistä on, että uhria houkutellaan antamaan rahaa, henkilötietoja tai luottokorttitietoja. Uhri harvoin saa mitään vastineeksi, tai tilaama tuote ei vastaa luvattua. (Poliisi: *petosrikokset*, luettu 5.10.2021.) Tämän luvun aikaisemmissa kappaleissa on käsitelty erilaisia huijauksia. Näissä voi usein olla kyse petosrikoksesta.

Vuonna 2018 huijauksissa korostuivat kiristyshuijaukset ja toimitusjohtajahuijaukset ja arvioissa korostettiin huijausmäärien kasvaneen. Huijausviestejä lähetettiin sähköpostien lisäksi entistä enemmän tekstiviesteillä. Tekstiviestien linkit johtivat muun muassa tilausansoihin. (Tietoturvan vuosi 2018, 7.) Vuonna 2019 rikolliset keskittyivät toimitusjohtajahuijauksiin ja muihin laskutuspetoksiin. Myös Suomessa puhelin-, laskutus- ja tekstiviestihuijaukset olivat yleisiä. (Tietoturvan vuosi 2020, 14.) Huijarit hyödyntävät petosrikoksissa käyttäjän manipulointia eli psykologisia keinoja ja tietojenkalastelua.

Vuonna 2019 tilastoitiin 6 296 maksuvälinepetosta ja 28 653 muuta petosrikosta. Petosrikosten määrä on lisääntynyt selvästi 2000-luvulla. (Rikollisuustilanne 2019, 95.) Vuoden 2021 kahden ensimmäisen neljänneksen aikana kävi ilmi 2 500 maksuvälinepetosta. Se on 900 tapausta eli 26,4 prosenttia vähemmän kuin edellisvuonna. (Tilastokeskus 2021, 2.) Vuonna 2020 nettipetoksia koskevia rikosilmoituksia kirjattiin noin 20 600 kappaletta (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021).

*Muihin maksuvälineisiin kuin käteisrahaan* viitattaessa käytetään lyhennettä *CNP* (englanniksi *Card-not-present*). Euroopan unioni tehosti vuonna 2019 maksukortteihin (luottokortit, verkko-ostokset jne.) liittyvien petosten torjuntaa sääntöjä tiukentamalla ja nykyaikaistamalla. Tavoitteena on torjua CNP-petoksia ja väärennöksiä, joita pidettiin uhkana turvallisuudelle, koska ne ovat muun muassa tulonlähde järjestäytyneelle rikollisuudelle. (Euroopan unionin neuvosto 2019, luettu 7.10.2021.)

Vuonna 2013 maksukortteihin liittyvillä petoksilla saatu rikoshyöty oli arviolta 1,44 miljardia euroa (Euroopan unionin neuvosto 2019, luettu 7.10.2021). Vuonna 2018 CNP-petokset hallitsivat maksupetoksia, ja internetin yleistyessä yhä enemmän maksuja suoritettiin (IOCTA 2018, 43). Vuonna 2019 todettiin sähköisen kaupan lisääntyneen ja etenkin fyysisten tavaroiden ostamisessa esiintyi CNP-petoksia. CNP-petoksia hyödynnettiin myös muissa rikollisuuden muodoissa, esimerkiksi ihmiskaupassa. Lisäksi CaaS-markkinoilla, Darkwebeissä, myytiin luottokorttitietoja ja anastettuja luottokortteja. (IOCTA 2019, 36–37.)

Vuonna 2019 CNP-petosten lukumäärä kasvoi ja e-skimmauksesta tuli uusi tekotapa. SIM-kortin vaihto (SIM Swap) -petos yleistyi. Kyseessä on huijaus, jossa esimerkiksi vaihdetaan kohteen liittymä rikollisen nimiin tai puhelinnumero saadaan siirrettyä rikollisen SIM-kortille. Liittymää hallitsemalla voidaan kaapata kohteen sovelluksia, salasanoja sekä pankki- tai sähköpostitilejä. (IOCTA 2020, 43–44.) Rikolliset saattavat myös pystyä kloonaamaan SIM-kortteja (Senker 2017, 30).

Myös sähköinen skimmaus (englanniksi *e-skimming*) lisääntyi edellisvuosiin verrattuna. Samanlaista menetelmää käytetään myös tekstiviestien (englanniksi *SMishing*) avulla, jolloin kohteelle lä-

hetetään esimerkiksi luotettavalta lähettäjältä tekstiviesti, jossa pyydetään käyttäjätunnuksia, salasanoja tai tunnuslukuja. SMishing-huijaukset kohdistuivat tyypillisesti rahoitusinstituutioihin ja heidän asiakkaisiinsa. Esimerkiksi pankin nimissä pyydetään kohdetta kirjautumaan nettitunnuksilla verkkosivulle ja siten rikollinen saa tiedot käyttöönsä (englanniksi *bank smishing, SMS*). Molemmissa huijauksissa käytettiin hyväksi myös käyttäjän manipulointia, jonka avulla rikollinen sai tietoja käyttöönsä. (IOCTA 2020, 43–45.)

### 5.7 Tietojenkalastelu

Kalasteluviestit sisältävät usein linkin esimerkiksi väärennetylle, pankkisivun näköiselle nettisivulle, jossa käyttäjältä pyritään saamaan pankkitietoja ja henkilökohtaisia tietoja (Europol EC3 ym 2020, huijaussivustot). Tietojenkalastusta kohdennetaan yksityishenkilöihin, yrityksiin ja organisaatioihin.

Vuoden 2017 ilmiönä voidaan pitää Microsoft Office 365 -sähköpostipalveluun kohdistunutta tietojen kalastelua. Käytössä oleva Office-pilvipalvelualusta yhtenäisti eri organisaatioiden sähköpostipalvelut, mikä helpotti tietojenkalastelua, koska sama huijausviesti voitiin kohdistaa samaa palvelua käyttäviin organisaatioihin. Tietoja kalasteltiin myös aiemmin tutuin keinoin, kuten sähköpostien ja tekstiviestien välityksellä. Yleisesti havaittiin, että rikollisiin tekoihin paneuduttiin entistä tarkemmin ja yksityiskohtaisemmin kuin aikaisemmin. Office 365 -kalastelua voidaan pitää myös tietomurtona, koska murron jälkeen varsinainen petoskuvio suunnitellaan sähköpostista tai muusta alustan palvelusta saadun tiedon perusteella. (Tietoturvan vuosi 2018, 7–8.)

Vuonna 2018 Kyberturvallisuuskeskus varoitti suomalaisia yrityksiä useasti tietojenkalastelusta. Sähköpostitunnuksia ja -viestejä anastettiin runsaasti, ja kalastelu kohdistui organisaatioiden johtoon ja maksuliikenteestä vastaaviin henkilöihin. Käyttäjätunnuksia ja salasanoja kalasteltiin sähköpostitse ja huijaussivujen avulla, ja anastetuilla tunnuksilla kirjauduttiin yritysten Office 365 -sähköpostitileille. Sitä kautta rikollinen pyrki seuraamaan yritysten sähköpostiliikennettä, organisaatioiden liikesalaisuuksia tai maksuliikennettä sekä kalastelemaan muiden työntekijöiden tai yhteistyökumppanien tunnuksia. (Kybersää kesäkuu 2018, 2.)

Vuonna 2018 Office 365 -tietomurrot tehtiin myös pääasiassa kalastelluilla tunnuksilla. Käyttäjätunnuksia ja salasanoja kalasteltiin huijausviestein, jotka ohjasivat vastaanottajan erilaisille tietojenkalasteluun tarkoitetuille verkkosivuille. Syötetyt salasanat ja pankkitunnukset päätyivät kalastelun ansiosta rikollisille tietomurtotarkoituksiin. Trendin oletettiin jatkuvan myös tulevana vuonna. (Tietoturvan vuosi 2019, 26.)

Vuonna 2019 rikolliset hyödynsivät televerkkoja miljoonien teknisen tuen huijauspuheluiden tekemisessä. Myös niin kutsuttuja hälytys-puheluita tehtiin noin miljoona. Tietoja kalasteltiin myös tekeyty-

mällä organisaation johtajaksi ja lähettämällä hänen nimissään viestejä organisaation taloushenkilöstölle. Myös tekstiviestien linkkien kautta tapahtuva tietojenkalastelu jatkoi yhtenä tekotapana. (Tietoturvan vuosi 2020, 14.)

Vuonna 2020 tehtailtiin laskutuspetoksia- ja huijauksia, jotka aiheuttivat tuntuvia taloudellisia menetyksiä organisaatioille. Esimerkiksi kansainvälinen rikollisryhmä esiintyi Finanssivalvonnan ja lakitoimistojen nimissä päästääkseen käsiksi suurten yrityskauppojen varainsiirtoihin. Laskutuspetoksissa rikollinen tekeytyi tavallisimmin organisaation johtajaksi ja lähetti tämän nimissä viestejä organisaation taloushenkilölle. Rikoshyöty voi olla satojatuhansia euroja, ja laskutuspetokset huomataan usein vasta viikkoja vahingon jälkeen, mikä vaikeuttaa rahojen palauttamista. (Tietoturvan vuosi 2020, 14.)

### 5.8 Käyttäjän manipulointi

Käyttäjän manipulointi (englanniksi *social engineering*) on toimintaa, jossa tavoitteena on hankkia luottamuksellista tietoa tekeytymällä tiedon käyttöön oikeutetuksi ja käyttämällä hyväksi tiedon käyttöön oikeutettuja henkilöitä. Toiminta voi kohdistua yhteen tai useisiin henkilöihin, ja sillä usein pyritään selvittämään käyttäjän salasana. (Turvallisuuskomitea 2018, 19.) Kalasteluhyökkäykset ovat yksi yleinen käyttäjän manipuloinnin muoto (Lehto 2021, 40), ja siinä uhriin voi kohdistua kiristystä tai uhkailua (IOCTA 2019, 51). Suurimman osan kyberrikoksista mahdollistaa inhimillisen tekijän hyödyntäminen tietoturvallisuuden heikkoutena, mikä voi johtua ihmisten huonosta tietoturvatietoisuudesta ja -osaamisesta (IOCTA 2020, 15–16).

Hyökkääjä pyrkii siis saamaan ihmisen luottamuksen esimerkiksi henkilön heikkouksia hyväksikäyttäen. Esimerkiksi IT-tuen edustajaksi tekeytyvä rikollinen pyrkii saamaan työntekijältä käyttäjätunnuksia ja salasanoja. Käyttäjän manipuloinnin voidaan sanoa olevan petoksen avulla tapahtuvaa ihmisen manipulointia, jossa tavoitteena on saada ihminen antamaan pääsy tietoverkkoon tai luovuttamaan tietoja tai dataa. (Tapoja välttyä käyttäjän manipuloinnilta, luettu 24.9.2021.) Rikolliset ovat tulleet entistä aggressiivisemmiksi ja voivat ottaa suoraan yhteyttä uhreihinsa. Tekotapana on usein kiristys, esimerkiksi kohdistettuja palvelunestohyökkäyksiä tai kiristysohjelmia käyttäen. Uhreina ovat olleet yksityishenkilöt, joiden varallisuustasoa on kyetty selvittämään, sekä yritykset, jotka ovat olleet kiristyshaittaohjelmien kohteena. (Sisäministeriö 2017, 13.)

Käyttäjän manipulointitapoja ovat houkuttelu, peitetarina, tietojenkalastelu, erilaiset lähestymistavat sekä roskapostin lähettäminen yhteyshenkilölle ja sähköpostin hakkerointi (Tapoja välttyä käyttäjän manipuloinnilta, 24.9.2021). Vuonna 2018 käyttäjän manipulointia hyödynnettiin entistä enemmän ja sitä hyödynnettiin etenkin tietojenkalastelussa sähköpostien, puhelimien ja viestien keinoin. Käyttäjän manipulointia hyödynnettiin myös tilien kaappaamisessa, henkilöllisyyksien anastamisessa,

laittomien maksujen aloittamisessa sekä rahan siirtämisessä ja henkilötietojen jakamisessa. (IOCTA 2018, 8.)

Vuonna 2019 havaittiin, että käyttäjän manipulointia hyödynnettiin BEC- ja CEO-huijauksissa. Käyttäjän manipulointia ja etenkin tietojenkalastelua pidettiin merkittävänä monialaisena kyberuhkana. (IOCTA 2019, 51.) Vuonna 2020 käyttäjän manipulointi osoittautui entistä kokonaisvaltaisemmaksi ja siinä hyödynnettiin osaamista, järjestelmiä, haavoittuvuuksia ja vääriä henkilöllisyyksiä ja rikolliset toimivat entistä enemmän yhteistyössä CaaS-yhteisöissä. Käyttäjän manipulointia pidettiin yhtenä suurimmista uhkista, joilla helpotetaan erityyppisten kyberrikosten tekemistä. Tietojenkalastelu ja käyttäjän manipulointi oli tullut entistä hienostuneempaa. (IOCTA 2020, 6–8 ja 15.)

### 5.9 Identiteettivarkaus ja tietomurrot

Rikoslain 38 luvun 9a §:n mukaan identiteettivarkaudesta tuomitaan se, joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee.

Identiteettivarkaudesta on kyse, kun esiinnytään toisen henkilöllisyydellä. Rikollinen käyttää itselleen kuulumattomia henkilötietoja, tunnistautumistietoja tai muuta vastaavaa yksilöivää tietoa, kuten nimeä, osoitetietoja, henkilötunnusta, puhelinnumeroa tai pankkitunnuksia. (Neuvoja identiteettivarkauden tai tietovuodon uhrille, luettu 7.10.2021.)

Ihmisten henkilötietoja on yhä enemmän verkkomaailmassa, esimerkiksi valtion ja yritysten järjestelmissä. Rikollisen päästessä esimerkiksi yrityksen järjestelmään voi hän saada henkilötietoja käsiinsä ja käyttää niitä rikolliseen tarkoitukseen. Rikollinen on voinut myös saada haltuunsa anastetun luottokortin ja soittaa pankkiin sulkeakseen kortin sekä pyytää pankkia lähettämään uusi pankkikortti tai pankkitunnukset uuteen osoitteeseen. Kortin tai tunnukset saatuaan voi rikollinen esiintyä verkossa toisen henkilötiedoilla pankkivarmistuksia hyväksikäyttäen. Rikolliset voivat myös myydä tietojaan pimeässä verkossa muille rikollisille. (Senker 2017, 36–38.)

Identiteettivarkaudesta voi olla kyse, kun toisen ihmisen nimissä tehdään verkkokauppatilauksia. Rikolliset voivat saada identiteettivarkauteen tarvittavia henkilötietoja esimerkiksi verkkotietovuodon tai tietojenkalastelun avulla. Henkilötietoja on myös kerätty teknisen tuen huijauspuheluissa. (Neuvoja identiteettivarkauden tai tietovuodon uhrille, luettu 7.10.2021.) Identiteettivarkaudella voidaan myös ottaa lainoja tai avata luottokortteja uhrin nimissä, mikä voi vahingoittaa uhrin luottotietoja ja taloutta. Rikolliset voivat jopa tonkia roskakoreja löytääkseen laskuja tai muita papereita, joista ilmenee henkilötietoja. Identiteettivarkauden uhriksi voi joutua myös tietojenkalastelun ja haittaohjelmien kautta. (Kuinka turvallisia sähköiset rahansiirrot ovat? Luettu 7.10.2021.)

Vuonna 2020 identiteettivarkauksia koskevia rikosilmoituksia kirjattiin yli 4400 kappaletta (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021).

Vuosina 2018–2021 Office 365 -tietomurrot ovat erottuneet selkeästi. Office 365 -tietomurtoja tehtiin ja tehdään edelleen pääasiassa kalastelluilla tunnuksilla, ja murroilla pyritään pääsemään käsiksi luottamukselliseen materiaaliin, tekemään laskutuspetoksia haltuun saaduilla tiedoilla tai tekemään uusia tietomurtoja haltuun saatujen tunnuksien avulla. (Tietoturvan vuosi 2019, 24 & Tietoturvan vuosi 2020, 12.)

Suomen ensimmäinen suuren luokan tietomurto oli vuonna 2019 Psykoterapiakeskus Vastaamon tietomurtoloukkaus. Tietomurtoa seurasivat kiristysviestit, joissa Vastaamoa ja sen asiakkaita vaadittiin maksamaan lunnaita, jos he halusivat välttää potilastietojensa vuotamisen internetiin muiden saataville. Poliisille on kirjattu yli 25 000 rikosilmoitusta tapauksesta. Useat organisaatiot ja viranomaiset ovat olleet tukemassa ja auttamassa tietomurron uhreja. (Tietoturvan vuosi 2020, 12–13.)

Vuoden 2020 syyskuussa Suomen eduskuntaan kohdistui kyberhyökkäys, jossa muutamia sähköpostitilejä vaarantui. Keskusrikospoliisi tutkii tapausta epäiltynä törkeänä tietomurtona ja vakoiluna. (Tietoturvan vuosi 2020, 9.)

### 5.10 Esineiden internet ja automaatiojärjestelmät

Vuonna 2019 havaittiin Suomessa paljon avoinna olevia ja haavoittuvia IoT-laitteita. Laitteiden tietoturvan tason pääteltiin olevan heikolla tasolla. Laitteiden tietoturvapuutteiden takia pystyttiin ne valjastamaan bottiverkkoihin palvelunestohyökkäyksiä tehostamaan. IoT-laitteet kasvattivat Mirai-bottiverkkoa erityisen runsaasti vuonna 2019. (Tietoturvan vuosi 2019, 31.)

Vuonna 2020 todettiin, että IoT-laitteiden tietoturvallisuusvaatimuksiin ja -sertifioinnin tarpeeseen oli puututtu, vaikkakin älylaitteissa oli vielä runsaasti tietoturvapuutteita. Rikollisille houkutteleva kohde oli verkossa suojaamaton laite, jonka pystyi valjastamaan esimerkiksi palvelunestohyökkäyksiin tai joka voi tarjota pääsyn yrityksen verkkoon. (Tietoturvan vuosi 2020, 15.)

Automaatiojärjestelmillä ohjataan ja monitoroidaan monenlaisia kokonaisuuksia. Käytön tekeminen mahdollisimman helpoksi, saatetaan laitteisiin tai järjestelmiin päästä etänä ja mistä ja milloin tahansa. Helppokäyttöisyys voi aiheuttaa tilanteen, jossa rikolliset pääsevät käsiksi laitteisiin mistä tahansa. Tärkeimpiin järjestelmiin voi rikollinen päästä murrettujen laitteiden kautta. (Traficom 5/2021, 2.)

Suomessa vuonna 2015 lappeenrantalaisen kerrostalon lämmitysjärjestelmä kaatui palvelunestohyökkäyksen seurauksena (Cyberwatch Q1 2021, 9). Vuonna 2020 infrastruktuurin automaatiojär-

jestelmiin kohdennettiin iskuja. Esimerkiksi Israelin vesijärjestelmää vastaan hyökättiin. Israel onnistui estämään hyökkäyksen, mutta se olisi voinut vahingoittaa väestöä merkittävällä tavalla. Isku oli tiettävästi ensimmäinen kerta, kun IoT- ja automaatiojärjestelmien avulla yritettiin aiheuttaa fyysistä vahinkoa kansalaisille. Suomalaisessa kartoituksessa selvisi, että kotimaisista verkoista löydettiin noin 1 000 suojaamatonta automaatiojärjestelmää. (Tietoturvan vuosi 2020, 15.)

### 5.11 Lapsiin kohdistuvat seksuaalirikokset

Verkossa tapahtuvia lapsiin kohdistuvia seksuaalirikoksia (englanniksi *child sexual exploitation online, CSE*) voidaan pitää yhtenä huolestuttavimpana kyberrikoksen tekomuotona. Internetin tulon jälkeen on verkkoulottuvuus antanut rikoksentekijöille mahdollisuuden olla vuorovaikutuksessa keskenään verkossa ja hankkia lapsiin kohdistuvaa seksuaaliväkivaltamateriaalia (englanniksi *child sexual exploitation material, CSEM tai sexual abuse material, CSAM*) sellaisissa määrin, mitä se ei ennen olisi ollut mahdollista. Yhä nuoremmilla lapsilla on pääsy internetyhteyttä käyttäviin laitteisiin ja sosiaaliseen mediaan, jonka avulla rikoksentekijät voivat tavoittaa lapset kybermaailmassa helpommin. Tästä syystä alaikäisiin kohdistuva seksuaalinen pakottaminen ja kiristäminen on lisääntynyt. Suoratoistona (englanniksi *live streaming*) tapahtuva lapsiin kohdistuva seksuaalirikos on erityisen kompleksinen rikos tutkia. Tutkinnan näkökulmasta haasteita lisää jatkuva teknologian käytön kehittyminen ja helpottuminen sekä rikostentekijöiden käyttämät anonymisoinnit ja erilaiset salaukset. Esimerkiksi suoratoistolla itse tuotettu materiaali on lisääntynyt huomattavasti. (IOCTA 2018, 30–33.)

Laittoman materiaalin poistaminen verkosta on hidasta ja vaatii Suomessa aina poliisin pyynnön asiasta. Poliisi ei kuitenkaan pysty velvoittamaan palveluntarjoajia poistamaan materiaalia. Suomessa CSEM-materiaalin vihjeiden esiselvityksestä kansallisesti vastaa Keskusrikospoliisin kyberrikostorjuntakeskuksen CSE-tiimi. Poliisihallituksen, Poliisiammattikorkeakoulun sekä Terveyden ja hyvinvoinnin laitoksen Barnahus-hankkeen tarkoituksena on kehittää viranomaisille ja erityisesti poliisille kansallista koulutusta verkossa ja digitaalisessa mediassa tapahtuvasta lapsiin kohdistuvasta seksuaaliväkivallasta. (Väkivallaton lapsuus 2021, 96.)

Kyberympäristön laajetessa ovat hyväksikäyttömahdollisuudet lisääntyneet. Potentiaalisia uhreja lähestytään internetin keskustelupalstoilla, koska käyttäjämäärät palstoilla ovat suuret. Verkossa tapahtuva ahdistelu on monimuotoista ja joissakin muodoissaan hyvin yleistä. (Sisäministeriö 2017, 18.) Rikolliset ovat taitavia hankkimaan tietoja ja keskustelemaan lapsien kanssa esimerkiksi keskustelupalstoilla (Senker 2017, 26).

Pilvipalveluiden käytön lisääntyminen on yleistänyt lapsiin kohdistuvan seksuaalirikosaineiston levittämistä. Uhrit ovat olleet vuosi vuodelta yhä nuorempia, ja maailmanlaajuisesti noin 80 prosenttia

uhreista on alle kymmenenvuotiaita. Aineistossa on myös todettu yhä äärimmäisempää ja sadistisempaa hyväksikäyttöä. Euroopassa lapsiin kohdistuvien seksuaalirikosaineiston suosimissa Darknet-foorumeissa lapsiin kohdistuvaa seksuaalirikosaineistoa voidaan katsoa ja levittää hyvin riskittömästi. (Sisäministeriö 2017, 18.)

Verkossa tapahtuvat lapsiin kohdistuvat seksuaalirikokset ja niihin liittyvät toimet ovat lisääntyneet jatkuvasti viime vuosina. Viranomaisten tietoon tulleiden tapausten lukumäärää voidaan pitää aliraportoituna. Koska kaikista tapauksista ei ilmoiteta viranomaisille, uhrit jäävät usein tunnistamattomiksi ja väärinkäyttäjät havaitsematta. Lapsiin kohdistuvat seksuaalirikokset ovat traumaattisia, ja uhreille koituu usein pitkäaikaista ja vakavaa vahinkoa niin fyysisesti kuin myös henkisesti, mikä voi johtaa itsensä vahingoittamiseen ja pahimmassa tapauksessa itsemurhaan. Lapsiin kohdistunut seksuaalinen hyväksikäyttö kohdistuu yhteiskunnan haavoittuvimpiin jäseniin. (SOCTA 2021, 12 ja 41.)

Lapsiin kohdistuvaa seksuaaliväkivaltamateriaalia on helppo käyttää kaikentyyppisillä laitteilla. Rikollisten salausvälineiden laajamittainen väärinkäyttö on pienentänyt riskiä havaita rikoksentekijöitä. Tästä syystä rikolliset luottavat yhä enemmän anonymisointipalveluihin, kuten virtuaalisiin yksityisverkkoihin (VPN) ja välityspalvelimiin. (SOCTA 2021, 41.) Lapsiin kohdistuvaa seksuaaliväkivaltamateriaalia on tyypillisesti tuotettu uhrin kotona ja useimmiten lapsen luottamuspiiriin kuuluvien henkilöiden toimesta (Australian Institute of Family Studies 2015, 11). Suoratoistoa pidetään keskeisenä uhkana, ja sen väärinkäytösten määrä on jatkuvasti lisääntynyt viime vuosien ajan (SOCTA, 42).

# 6 TULEVAISUUDEN TRENDIT

Kybervuoden 2020 voidaan sanoa olleen poikkeuksellinen COVID-19-pandemian takia. Pandemian aikana etätöiden määrä Suomessa oli valtavassa kasvussa, mikä on asettanut haasteita myös kyberturvallisuudelle ja -torjunnalle. Koko kyberala on viime vuosina kasvanut nopeasti, ja muutosvauhti on huimaa. Kyberalan työpaikkojen määrä on lisääntynyt ja osaamisesta kilpaillaan entistä enemmän. Suomi on asettanut oman tavoitteensa ollakseen kansainvälisesti kyberturvallisuuden kärkiosaajien joukossa (Suomen kyberturvallisuusstrategia 2019, 4).

Edellisessä luvussa on tuotu esille viime vuosien ja vuoden 2021 kyberrikollisuuden trendejä, jotka ovat asettaneet haasteita kyberrikollisuuden torjunnalle. Torjunnan lisäksi haasteet ovat kohdistuneet yksittäisiin kansalaisiin, yrityksiin ja organisaatioihin. Jatkuva ja nopea muutos aiheuttaa sen, että reaaliaikaisen tilannekuvan ylläpitäminen on vaikeaa. Palvelut siirtyvät tietoverkkoihin ja sähköistyvät, mistä syystä kyberturvallisuutta on kehitettävä jatkuvasti digitalisaation vauhdin mukana

pysymiseksi. Teknologian kehitys on johtanut siihen, että elämme jatkuvasti nopeasti muuttuvassa kompleksisessa maailmassa. Kompleksisuus edellyttää erilaisia ajattelutapoja ja lähestymiskulmia, koska maailmasta on tullut vaikeammin ennustettava (McChrystal 2015, 146).

Kyberrikollisten uudet ja vanhat toimintatavat asettavat haasteita viranomaistoiminnalle ja yksityiselle toiminnalle. Kyberrikollisuuden kasvu ja kehitys luovat haasteita ajankohtaiselle lainsäädännölle sekä tilannekuvan muodostamiselle. Uusien ilmiöiden tunnistaminen on vaikeaa, ja usein vahinkoa aiheutetaan uhrin tai viranomaisen tietämättä. Ilmiöitä tunnistetaan viiveellä, ja rikosilmoitusten tekemisen alhainen aktiivisuus vaikeuttaa viranomaisten kyberrikollistorjuntatoimenpiteitä. Yhteiskunnan ja talouden nopeasti kehittyvä digitalisaatio luo jatkuvasti uusia mahdollisuuksia kyberrikollisille (SOCTA 2021, 12).

Suomi osallistuu EU:n puitteissa kyberrikollisuuden torjuntaan oikeus- ja lainvalvontaviranomaisten kansainvälisellä yhteistyöllä sekä kansainvälisen oikeuden ja sopimusten kehittämiseen. Kyberrikollisuuden torjunnan mahdollistavaa lainsäädäntöä kehitetään siten, että lainsäädäntö mahdollistaa tehokkaan kyberrikosten ennalta estämisen ja tutkinnan. (Suomen kyberturvallisuusstrategia 2019, 5 ja 7.)

EU pyrkii omassa kyberturvallisuusstrategiassaan suojelemaan EU-kansalaisia ja yrityksiä kyberuhkilta sekä edistämään turvallisia tietojärjestelmiä ja suojelemaan maailmanlaajuista, avointa, vapaata ja turvallista kybertoimintaympäristöä. Strategian kolmeksi pääosa-alueeksi on määritelty seuraavat. Ensimmäisenä on häiriönsietokyvyn parantaminen ja teknologinen riippumattomuus ja johtajuus. Toisena on operatiivisten valmiuksien kehittäminen uhkien ehkäisemiseksi ja torjumiseksi ja niihin vastaamiseksi. Kolmanneksi pyritään lisäämään yhteistyötä maailmanlaajuisen ja avoimen kybertoimintaympäristön edistämiseksi. (Euroopan unionin neuvosto 2020, 5.)

Euroopan unionin neuvosto hyväksyi toukokuussa 2021 päätelmät, joissa vahvistettiin EU:n vuosien 2022–2025 prioriteetit Euroopan monialaisen rikosuhkien torjuntafoorumin (EMPACT) kautta tapahtuvassa vakavan ja järjestäytyneen rikollisuuden torjunnassa. Europolin esittämän uhka-arvion perusteella jäsenmaat määrittivät rikostorjunnan prioriteetteja, joista voidaan mainita tässä yhteydessä kyberhyökkäykset sekä verkossa tapahtuva ihmiskauppa, lasten seksuaalirikokset, petosrikokset ja talousrikokset. (Euroopan unionin neuvosto 2021a, luettu 9.10.2021.)

Kyberrikollisuutta esiintyy yhä enemmän ja edistyneemmissä muodoissa kaikkialla Euroopassa. Kasvun odotetaan jatkuvan myös tulevaisuudessa, koska esineiden internetiin liitettyjä laitteita odotetaan olevan 22,3 miljardia eri puolilla maailmaa vuoteen 2024 mennessä. (Euroopan unionin neuvosto 2021c, luettu 5.10.2021.) Rikollisten määrän kasvaessa myös kynnys tehdä kyberrikoksia madaltuu. Kyberrikospalveluiden kysyntä kasvaa, osaaminen lisääntyy ja kyberrikollisuus globalisoituu. (Peltomäki & Norppa 2015, 118–119.)

Perinteinen rikollisuus on globaalisti ollut maltillisessa laskusuunnassa, kun taas kyberrikollisuus on kasvussa. Kyberrikollisuuden määrä on kasvanut vuosina 2014–2020 noin 70 prosenttia. Vuonna 2019 Suomessa rekisteröitiin noin 1 300 kyberrikollisuustapausta, kun taas vuoden 2020 alustavat arviot ennustavat 1 500:aa tapausta. (Cyberwatch Q1 2021, 10.) Kyberrikollisten kohteet tulevat jatkossa olemaan entistä tarkemmin valittuja, ja rikollisten käyttämät menetelmät tulevat kehittymään (Cyberwatch 9.8.2021, luettu 04.10.2021).

Euroopassa kriittisiä kohteita kohtaan tehdyt merkittävät kyberhyökkäykset ovat vuonna 2020 kaksinkertaistuneet. Osasyynä voidaan pitää sitä, että pandemian aikana ihmiset olivat enemmän kotona ja verkossa. Myös terveydenhuoltoverkostoja vastaan tehtyjen hyökkäysten määrä kasvoi 47 prosenttia. (Walsh 2021, luettu 9.10.2021.)

Digitalisaatio, esineiden internet ja koko kybermaailma ovat ajaneet käyttäjät tilaan, jossa lyhyt kestoisetkin hidastumiset tai palvelimien kaatumiset saavat ihmisissä aikaan hermostuneisuutta ja kärsimättömyyttä. Ihmiset ovat nykyään yhä enemmän riippuvaisia kybermaailmasta ja sen tarjoamista palveluista. Digitalisaation myötä on kyberrikollisuus kasvussa, ja se on luonteeltaan entistä vahingollisempaa ja kohdennetumpaa.

Etätöitä ja -opiskelua tehdään entistä enemmän. Kotiolosuhteissa käyttäjällä ei ole välttämättä samanlaisia suojaustoimia kuin työpaikalla tai koulussa olisi eikä teknistä apua välttämättä ole heti saatavilla. Etätyöskentely ja -opiskelu edellyttävät myös työnantajalta toimenpiteitä riittävän tietoturvan takaamiseksi. Työympäristö voi mahdollistaa esimerkiksi vakoilun, eikä valelaskuhuijauksessa voi etätöissä kysyä naapurihuoneesta laskun oikeellisuudesta. Myös laitteiden kytkeminen langattomiin verkkoihin voi mahdollistaa haavoittuvuuksia ja pääsyn yrityksen tiedostoihin. Kyberrikollisuuden vaikutukset kasvavat ja voivat olla merkittäviä yksityishenkilöille, yrityksille ja organisaatioille. Kyberrikollisuus voi vaikuttaa talouteen, tuottoon, maineeseen, lailliseen luotettavuuteen ja moneen muuhun seikkaan.

CaaS-palvelumarkkinoiden kasvu on tuonut rikoksentekotavat ja -välineet laajemman käyttäjäjoukon ulottuville (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021). Palveluteollisuus on luonut rikollisille otollisen paikan käydä kauppaa ja vaihtaa ajatuksia toisten kyberrikollisten kanssa. Markkinoiden avulla voidaan myös tehdä toisen puolesta rikoksia, tiedonhankintaa tai vakoilua. Palveluita sijaitsee pimeän verkon markkinoilla, ja siellä voidaan myydä muun muassa palvelunestohyökkäyksiä, hakkerointipalveluita, kiristyshaittaohjelmia, botteja ja muita työkaluja. Esimerkiksi Darknetissä rikollinen voi käydä kauppaa suojatussa ja anonyymissa verkossa, mikä taas tekee viranomaisten työstä haastavampaa sen jäljittäessä rikollisia. Lisäksi markkinapaikoilla tehdään kauppaa kryptovaluutalla, mikä mahdollistaa anonyymin maksamisen.

Niin kuin edellisvuosina on nähty, voivat kyberrikolliset esimerkiksi myydä oman pääsynsä verkkoon toiselle rikolliselle sen sijaan, että hän itse hyödyntäisi pääsynsä. Palveluteollisuus on tehnyt tiettyjen kyberrikosten tekemisen tietoteknisesti osaamattomille helpoksi. Markkinapaikoilta on helppoa ostaa erilaisia palveluita ja työkaluja oman kyberrikoshyökkäyksen toteuttamiseksi. Markkinapaikkojen avulla voi rikollinen myydä pääsynsä johonkin järjestelmään tai verkkoon esimerkiksi motivoituneelle tekijälle. Toisaalta on myös mahdollista, että seuraavan vaiheen tai vaiheiden toteuttajalla on parempaa osaamista kuin alkuperäisellä. Täten palveluteollisuus antaa otollisen foorumin kyberrikollistoiminnalle. Kasvussa ovat olleet erityisesti tilauksesta kehitettävät kiristyshaittaohjelmat, joita muut rikolliset voivat hankkia juuri haluttuun kohteeseen räätälöitynä (Cyberwatch Q1 2021, 10).

Kybermaailman ja -rikollisuuden kehitys on äärimmäisen nopeaa, minkä takia kyberrikosten ennustaminen pitkällä aikavälillä oikein on mahdotonta. Globalisoituneessa maailmassa lähitulevaisuuden ennustaminen on haastavaa, koska kyberrikollisuuden uudet muodot muuttuvat nopeasti. Uusia ja vanhoja toimintatapoja yhdistelemällä rikolliset keksivät jatkuvasti uusia tapoja, joiden avulla he onnistuvat ohittamaan turvajärjestelyt tai huijaamaan ihmisiä. Kybermaailman kompleksisuus ja nopea muutosvauhti vaikuttavat siihen, että seuraavan kolmen vuoden kyberrikollisuuden trendeistä voidaan tehdä vain varovaisia arvioita heikkojen signaalien avulla.

Keskusrikospoliisin kyberrikostorjuntakeskus arvioi 2021, että tietoverkkorikollisuuden isot trendit muuttuvat hitaasti, mutta nopeaa muutosta on kuitenkin tapahtunut tekotapojen yksityiskohtien kehittämisessä, uusien teknologioiden hyödyntämisessä sekä toiminnan muuttumisessa yhä järjestäytyneemmäksi. (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021.) Suomea voidaan pitää suhteellisen vauraana maana, mikä tekee siitä myös suositun rikollisten kohteen (Rauhamaa 2021, 6).

### 6.1 Haittaohjelmat ja kiristyshaittaohjelmat

”Nykytilanne”-luvussa voitiin havaita, että haittaohjelmat ja kiristyshaittaohjelmat ovat tällä hetkellä suurimpia kyberrikollisuuden trendejä. Kiristyshaittaohjelmilla vaaditaan käyttäjältä lunnaita, kuten kryptovaluuttaa, salausten purkamiseksi. Havaittavissa on, että hyökkäykset kestävät entistä pidempää ja että kyberrikollisilla on käytössään uusia menetelmiä ja tekniikoita. Haittaohjelmien voidaan katsoa olleen ennen yleisempiä ja laajempia, esimerkiksi spämmäystä, kun nykyään ne ovat entistä harkitumpia ja valikoidumpia. Ammattimaiset kyberrikolliset ovat ottaneet ennen hyökkäystä selvää uhristaan sekä tietävät millä tavalla ja ketä lähestyä. Lisäksi kyberrikolliset tietävät, mihin tietoon hyökkäys kohdistetaan ja mikä tieto on kriittistä esimerkiksi yritykselle. Tieto voi olla erittäin arkaluonteista ja levitessään aiheuttaa suurtakin mainehaittaa. Tämän ansiosta rikolliset voivat asettaa entistä suurempia lunnasvaatimuksia.

Erilaiset haitta- ja kiristyshaittaohjelmat ovat olleet kasvussa viimeisten vuosien aikana eikä hidastumisen merkkejä ole näkyvissä. Voidaan olettaa trendin jatkuvan samansuuntaisesti, vaikkakin ohjelmissa tullaan näkemään muutoksia. Kyberrikolliset ovat jo nyt siirtyneet niin sanottuun kaksinkertaiseen kiristyshaittaohjelmaan, jossa anastettuja tietoja käytetään vipuvaikutuksena, jotta yritys maksaisi lunnaat tietojen julkaisematta jättämiseksi. Rikolliset myös ovat tiedostaneet, että heidän alkaessa suodattamaan tai julkaisemaan tietoja eivät he ole enää piilossa kyseisessä verkossa. Kiristyshaittaohjelmissa on hyödynnetty uusia salausmenetelmiä, ja lunnaita vaaditaan yhä enemmän kryptovaluutoissa kiinnijäämisriskin minimoimiseksi.

Haittaohjelmat voivat olla erittäin vakava uhka turvallisuudelle ja terveydelle. Esimerkiksi vuonna 2020 haittaohjelma aiheutti ensimmäisen kuolemantapauksen saksalaisessa sairaalassa, koska haittaohjelman takia sairaalan järjestelmät oli suljettu ja sairaala ei kyennyt hoitamaan menehtynyttä potilasta. (Cimpanu 2020, luettu 5.10.2021). Haittaohjelmia voidaan siis kohdistaa sairaalan järjestelmiin ja hoitokoneisiin, minkä takia potilaiden ja työntekijöiden terveys tai henki voi olla vaarassa. Vastaavaa menetelmää voidaan käyttää kaikkien alojen toiminnassa ja sen vaarantamisessa. Yritykset eivät ole välttämättä edelleenkään varautuneet riittävillä toimenpiteillä haittaohjelmahyökkäyksiin. Myös riittävässä torjunnassa saattaa olla puutteita.

Haittaohjelmia myydään yhä enemmän palveluteollisuudessa, ja sen voidaan katsoa olevan entistä ammattimaisempaa ja järjestäytyneempää rikollistoimintaa. Haittaohjelmien palveluteollisuutta voidaan kutsua MaaSiksi (englanniksi *Malware-as-a-service,* MaaS) (IOCTA 2020, 31). Käytännössä kuka tahansa voi suorittaa haittaohjelmahyökkäyksen ostamalla markkinapaikalta valmiin ohjelman. Uusien menetelmien kehittämiseksi palveluteollisuutta voidaan pitää oivana paikkana.

Matkapuhelimeen kohdistuneet haittaohjelmat ovat olleet viime vuosina yksi kyberuhka. Niitä kohdennetaan, ja niistä on tullut entistä uskottavampia. Matkapuhelimien ja niiden ominaisuuksien lisääntyminen aiheuttaa myös haavoittuvuuksia haittaohjelmille. Matkapuhelimilla liikutaan yhä enemmän verkossa, mikä mahdollistaa vahingoittavien tiedostojen tai linkkien lataamisen.

Kiristyshaittaohjelmahyökkäyksissä voidaan hyödyntää kaikkia kolmea menetelmää. Ensinnäkin hyökkäyksellä voidaan sulkea koko laite ilman tietojen tuhoamista. Toiseksi laite tai osa sen tiedostoista voidaan lukita, jolloin laitetta voidaan osittain käyttää esimerkiksi lunnasvaateiden maksamiseksi. Kolmanneksi rikolliset voivat hyödyntää molempia menetelmiä samanaikaisesti. Hybridimenetelmässä käyttäjä ei pysty käyttämään konetta eikä pääsemään tiedostoihinsa käsiksi. Näiden lisäksi hyökkäyksissä voidaan käyttää hyväksi käyttäjän manipulointia. Esimerkiksi laitteen näyttö voidaan lukita ilmoituksella, jossa kerrotaan, että poliisi on ottanut koneen haltuun tai koneesta löytyy arkaluontoista pornograafista materiaalia, tai jossa muutoin väitetään käyttäjän osallistuneen

laittomaan toimintaan. Hyökkäyksissä voidaan uhata levittää myös kolmannen osapuolen tietoja, jolloin yrityksen lisäksi myös asiakkaan tiedot voivat olla vaarassa.

Brittiläisen turvallisuusyritys Sophosin kyselyn perusteella todettiin, että ransomware-hyökkäysten maksut ovat kaksinkertaistuneet vuonna 2020 edellisvuoteen verrattuna. Maksut sisältävät muun muassa vakuutusmaksut, liiketoiminnan menetykset, korjauskulut ja mahdolliset ransomware-maksut. (Walsh 2021, luettu 9.10.2021.) Lisäksi kiristyshaittaohjelmien kokonaiskustannusten arvioidaan kohoavan vuonna 2021 ja kyberrikollisuuden kokonaisvahinkojen kuuteen biljoonaan dollariin (Blackfog: The state of Ransomware in 2021, luettu 9.10.2021).

Haittaohjelmat ja kiristyshaittaohjelmat on tunnustettu kyberrikollisuuden keskeiseksi uhaksi usean vuoden ajan. Hyökkäysten määrä ja ammattimaisuus on lisääntynyt. Julkisia laitoksia ja suuria yrityksiä kohtaan tehtyjen hyökkäysten määrä on kasvanut, mutta myös pienempiin, heikompien turvallisuusstandardien organisaatioihin on kohdistettu entistä enemmän hyökkäyksiä. Vaarassa ovat myös julkiset laitokset ja kriittinen infrastruktuuri (SOCTA 2021, 41) mukaan lukien terveydenhuolto, kansanterveys, informaatioteknologia, finanssipalvelut ja energia-alat (Microsoft 2021, 8).

Vuonna 2020 toimialoista kohteina olivat eniten vähittäiskauppa (13 prosenttia hyökkäyksistä), finanssipalvelu (12 prosenttia), valmistava teollisuus (12 prosenttia), julkishallinto (11 prosenttia) ja terveydenhuolto (9 prosenttia) (Microsoft 2021, 18).

### 6.2 Automaatiojärjestelmät ja esineiden internet

Automaatiojärjestelmiä käytetään yhä enemmän kriittisen infrastruktuurin toimintaan ja valvontaan, ja järjestelmiä liitetään yhä useammin internetiin, mikä saattaa altistaa ne samoille kyberuhkille kuin muutkin IT-järjestelmät. Kyberrikollisten näkökulmasta automaatiojärjestelmät ovat houkuttelevia kohteita, koska niissä on usein huono suojaus ja korkea vaikutuspotentiaali. Teollisuuden järjestelmien toimintaa ja kykyä palautua normaaliin toimintaan testataan valtiollisten toimijoiden taholta. (Cyberwatch Q1 2021, 8.)

Tulevaisuudessa automaatiojärjestelmiin kohdistetaan entistä kohdennetumpia, monimutkaisempia ja paremmin valmisteltuja hyökkäyksiä. Kyberrikolliset ovat yhä enemmän kiinnostuneita automaatiojärjestelmistä. Arvioidaan, että kiristyshaittaohjelmahyökkäykset automaatiojärjestelmiä kohtaan tulevat lisääntymään tulevaisuudessa. Automaatiojärjestelmiä voidaankin pitää yhtenä houkuttelevimmista kyberhyökkäyskohteista. (Cyberwatch Q1 2021, 8–9.)

Yhtenä kasvavana tulevaisuuden kyberriskinä voidaan pitää sähköisten ja IoT-laitteiden nopeaa vanhentumista sekä järjestelmien ja ohjelmien päivittämisen vanhentumista. Voidaan puhua niin sanotusta haavoittuvuusteollisuudesta, jolla tarkoitetaan sitä, että valmistajilta ei välttämättä tule

päivytyksiä ostamisen jälkeen (Peltomäki & Norppa 2015, 118) tai päivitykset lopetetaan tietyn ajan jälkeen. Liikenne, energia, terveys, televiestintä, rahoitus, turvallisuus, avaruus ja puolustus ovat erittäin riippuvaisia verkosta ja tietojärjestelmistä ja ne liittyvät yhä enemmän toisiinsa. Haitallinen kohdistaminen kriittiseen infrastruktuuriin on suuri maailmalaajuinen riski (The EU's Cybersecurity Strategy for the digital decade 2020, 1–2).

Esineiden internet on ollut selvässä kasvussa viime vuosina, ja sitä voidaan pitää yhtenä kyberrikollisuuden trendinä. IoT-laitteista voi rikollinen hankkia salasanoja, käyttäjätunnuksia ja muita tietoja, joita käyttämällä rikollinen voi päästä murtautumaan esimerkiksi yrityksen järjestelmään. Laitteiden lisääntyessä myös riskit ja haavoittuvuudet lisääntyvät. Massiiviset kyberhyökkäykset IoT-ympäristössä voivat johtaa häiriöihin tuotannon ja logistiikan lisäksi myös kuljetuksissa, terveydenhuollossa, koulutuksessa, vähittäiskaupassa ja kotiympäristössä. 4D-tulostuksen kasvu on aiheuttanut tulostuksessa häiriöitä, ja tuotteita voidaan etäyhteydellä esimerkiksi muokata erilaiseksi kuin on tarkoitettu. Tuotteet eivät siten valmistu vaaditulla ja aiotulla tavalla.

Yritykset käyttävät yhä enemmän tekniikkaa IoT-ominaisuuksilla, koska se on edullista, tehokasta ja helppoa. Tästä johtuen yhä useampaan laitteeseen kohdistuu riskejä kyberrikollisuudesta. Uudet laitteet tulevat markkinoille tuotannosta niin nopeasti, että turvallisuuteen ei ehditä kiinnittämään riittävästi huomiota. Myös laitteiden, kuten matkapuhelimen, kautta voidaan päästä käsiksi yksityisiin ja arkaluonteisiin tietoihin, mikä luo riskejä ja uhkia kyberturvallisuudelle. Osana automatisaatiota esineiden internetillä on suuri rooli, koska päivittämättömissä laitteissa piilee uhkia. Erilaiset haavoittuvuudet voivat olla kriittisiä koko yrityksen toiminnalle.

Uusia palveluita ja tekniikkaa tulee niin nopeasti, että haavoittuvuudet kasvavat ja tietoverkkohyökkäyksiä on vaikea hallita (Cybersäkerhet i Sverige 2020, 24). IoT-laitteisiin kohdistuvia hyökkäyksiä on kuitenkin onnistuttu estämään kansainvälisten turvallisuusstandardien avulla (Microsoft 2021, 84). Kyberriski kohdistuu jokaiseen verkkoon kytkettyyn laitteeseen, mikä asettaa korkeat vaatimukset tietoturvalle, jotta kaikkiin riskeihin pystyttään vastaamaan ja rikollisten uusien tekotapojen mukana pysytään. Laitteilta halutaan yhä enemmän helppoutta, nopeutta ja yksinkertaisuutta, mikä taas asettaa haasteita laitteen tietoturvalle.

### 6.3 Toimitusketjuihin ja logistiikkaan kohdistuvat hyökkäykset

Logistiikkaan ja toimitusketjuihin (englanniksi *supply chain*) kohdistuvat hyökkäykset ovat lisääntyneet. Suurin osa yrityksistä ja organisaatioista on osa toimitusketjua, esimerkiksi valmistajan, maahantuojan tai jälleenmyyjän roolissa. Toimitusketjuhyökkäyksessä rikollinen voi tunkeutua toimitusketjun muiden jäsenten verkkoihin ja järjestelmiin ja päästä siten käsiksi usean organisaation tietoihin. (Toimitusketjut uhka yritysten kyberturvalle, luettu 8.10.2021.) Esimerkiksi lisäämällä takaoven

johonkin tuotteeseen voi hyökkääjä onnistua lisäämään haitallista aineistoa tuotteeseen sen valmistajan kautta. Tällaista hyökkäystapaa kutsutaan toimitusketjuhyökkäykseksi. (SolarWinds Orion Platformin takaovi mahdollisti vakoilun ja tietomurtoja, luettu 9.10.2021.)

Vuonna 2018 toimitusketjujen kautta tehdyt tietomurrot korostuivat yrityksiin kohdistuvassa vakoilussa. Toimitusketjuhyökkäyksien havaitsemista pidettiin haastavana. (Tietoturvan vuosi 2018, 15.) Alihankinta- ja toimitusketjuihin liittyvät uhkat konkretisoituivat vuonna 2019, kun useisiin yhdysvaltalaisministeriöihin ja -organisaatioihin tehtiin tietomurtoja, jotka liittyivät SolarWinds-etähallintatuotteisiin. Rikollinen onnistui ujuttamaan omaa koodiaan asiakkaille jaeltuun päivitykseen, ja siten hyökkääjällä oli pääsy kaikkiin haitallisen koodin asentaneisiin organisaatioihin. Myös suomalaisia organisaatioita joutui uhriksi. (Tietoturvan vuosi 2020, 9.)

Hyökkääjät hyödyntävät ohjelmistohaavoittuvuuksia, ja erityisen hankalaksi haavoittuvuuksilta suojautuminen on osoittautunut IoT- ja automaatiomaailmassa, jossa järjestelmien toimitusketjut ja elinkaaret ovat pitkiä ja päivityksen vaatimat tuotannon katkokset hankalia (Haavoittuvuudet hallintaan SBOMmin-varmasti, luettu 8.10.2021). Pandemia aiheutti sen, että lentoliikenne vähentyi. Logistiikkaketjuissa merenkulun asema korostui ja eri arvioiden mukaan niihin kohdistuvien kyberhyökkäysten määrä nelinkertaistui viimeisen vuoden sisällä. Varustamot ovat joutuneet muun muassa verkkohyökkäysten ja kiristyshaittaohjelmien kohteeksi. Varustamot ja satamat ovat kärsineet tuntuvia taloudellisia tappioita kyberhyökkäysten vuoksi. (Cyberwatch Q3 2021, 3 ja 6–7.)

### 6.4 Tietojenkalastelu

Tietojenkalastelua voidaan pitää perinteisenä kyberrikollisuuden trendinä, joka on ollut olemassa pitkään ja jonka tekotavat ovat muovautuneet vuosien aikana. Tietojenkalastelussa hyödynnetään yhä enemmän sosiaalista manipulointia, jonka avulla rikollinen voi esimerkiksi asentaa haittaohjelman tai päästä käsiksi arkaluonteiseen materiaaliin ja levittää sitä.

Vuonna 2021 Suomessa havaittiin aggressiivinen kalastelukampanja, jossa rikolliset pyrkivät saaman pankkitunnuksia haltuunsa. Esimerkiksi OP:n ja Nordean väärennetyissä kirjautumissivuissa kalasteltiin pankkitunnuksia. Sivustoille ohjattiin tekstiviestien ja hakukonetuloksiin ujutettujen linkkien avulla. (Traficom elokuu 2021, luettu 9.10.2021.)

Kyberrikolliset ja etenkin valtiolliset aiheuttajat käyttävät spear phishing -menetelmää, jossa rikolliset ovat selvittäneet etukäteen esimerkiksi tietoja kohteesta, ja tietoja käyttämällä kohdistavat kalastelun juuri kyseiseen kohteeseen. (Cybersäkerhet i Sverige 2020, 16.) Federal Bureau of Investigation (FBI) laati 2020 internet-rikosraportin, jonka mukaan uhrien kantelujen rikostyypeistä yleisin oli tietojenkalastelu (FBI 2020, 19). Tietojenkalastelua pidetään merkittävänä kyberuhkana yrityk-

sille ja yksilöille (Microsoft 2021, 20). Tietojenkalastelu ja käyttäjän manipulointi ovat rikollisen näkökulmasta tehokkaita, halpoja ja kannattavia. Kyberrikolliset kehittävät ja keksivät jatkuvasti uusia tietojenkalastelumenetelmiä huijatakseen ja saadakseen tietoja käyttäjistä. Tietojenkalastelua on vaivatonta ja helppoa toteuttaa myös lähitulevaisuudessa.

### 6.5 Kryptovaluutat ja -kaappaukset

Kryptovaluutta on tullut yhä yleisemmäksi, ja sitä hyödyntävät myös rikolliset. Esimerkiksi lunnasvaatimuksina vaaditaan usein kryptovaluuttaa, koska valuuttaa ja sen liikennettä on vaikea valvoa, seurata ja jäljittää. Myös kryptovaluuttaympäristöön voi kohdistua hyökkäyksiä tai se voi joutua hakkeroiduksi.

Viime vuosina ovat olleet suosittuja kryptokaappaukset, joissa haittaohjelman avulla ohjelmaa, järjestelmää tai laitetta käytetään louhinnassa. Kryptokaappauksen voidaan katsoa olevan tuottoisa markkina, koska louhintaprosessi on yksinkertainen prosessi, jossa rahaa ei tarvitse nostaa tai pestä. Kaappausten suosion voidaan arvioida säilyvän, koska rikollisen kiinnijäämisriski on pieni, toteuttamistapa on yksinkertainen ja onnistuessaan se mahdollistaa tasaisen tulovirran rikolliselle. Kaappauksissa uhri ei edes välttämättä ymmärrä laitteensa tulleen kaapatuksi, minkä takia rikosten tutkiminen on haasteellista ja louhintaa voidaan tehdä pidemmän aikaan ilman, että kaappaus tulee huomatuksi.

Kryptovaluuttojen käyttö ja leviäminen sekä anonymisointitekniikat, kuten salaus, tulevat jatkamaan kasvuaan. Myös sijoituspetoksia on kohdennettu yhä enemmän kryptovaluuttamarkkinoille laatimalla väärennettyjä sivustoja, jotka tarjoavat huijaussijoitusmahdollisuuksia. (SOCTA 2021, 40 ja 60) Myös terroristit käyttävät kryptovaluuttoja hyväkseen rahavaroja siirtäessään välttääkseen tulemasta havaituksi (Senker 2017, 163). Salattujen viestintä- ja maksuratkaisujen avulla voivat myyjät ja ostajat tehdä suojattua kauppaa keskenään (Cybersäkerhet i Sverige 2020, 12).

Voidaan arvioida, että tulevaisuudessa kyberrikolliset hyödyntävät entistä enemmän kryptovaluuttaa anonyymissa kaupanteossa ja maksuliikenteessä. Kryptovaluuttojen arvonmuutokset ja epävakaa markkinatilanne voi vaikuttaa sen suosioon tulevaisuudessa. Energian hinnannousulla voi olla vaikutuksia kryptokaappausten suosioon vastaisuudessa.

### 6.6 Verkkopetokset ja erilaiset huijaukset

Erilaiset huijaukset ovat olleet pitkään kyberrikollisten suosiossa. Nettikauppahuijaukset myynti- ja ostopalstoilla sekä toimitusjohtaja-, rakkaus-, sijoitus-, perintö-, laina-, lotto- ja arvontahuijaukset ovat suosittuja. Lisäksi rikolliset pyrkivät huijaamaan uhrejaan käyttäjän manipulointia hyödyntäen

sekä sähköpostien, tekstiviestien ja puheluiden avulla. Tietoja voidaan kalastella useilla eri menetelmällä, ja siten niitä voidaan käyttää hyväksi erilaisissa huijauksissa. Trendin voidaan arvella jatkuvan vielä pitkään. Huijausten muodot ja ilmiöt tulevat muuttumaan, ja rikolliset tulevat käyttämään erilaisia menetelmiä ja keksintöjä myös tulevaisuudessa.

Microsoftin teettämän mukaan puoleen Suomessa asuviin aikuisiin on kohdennettu viimeisen vuoden aikana teknisen tuen huijauksia, ja näistä kolme prosenttia on menettänyt rahaa huijauksen seurauksena (Microsoft 4.10.2021, luettu 14.10.2021). Suomessa erilaiset ihmisiin kohdistuvat huijaukset yleistyvät, ja tietojenkalastelu- ja pankkihuijaukset ovat kehittyneet ja monipuolistuneet niin kielellisesti kuin teknisesti. Taitavasti kohdennettuja huijauksia voidaan kohdentaa oikea-aikaisesti. Uusina ilmiöinä voidaan pitää Kanta.fi-kirjautumiseen liittyvää pankkitunnuskalastelua ja Kelan nimissä tehtyjä MobilePay-maksupyyntöjä. (Cyberwatch lokakuu 2021, 9.)

Huijaukset ovat edullinen tapa toteuttaa rikoksia. Niitä voidaan kohdistaa suurille määrille samanaikaisesti, ja valitettavan usein joku tai jotkut lankeavat huijauksiin ja maksavat rikollisille. Viime vuosina huijaukset ovat olleet aikaisempia ammattimaisempia ja selkokielisempiä. Nykyiset huijausviestit eivät ole kielelliseltä ulkoasultaan yhtä heikkoja kuin aikaisemmin. Valitettavan usein uhrit ymmärtävät vasta useiden maksusuoritteiden jälkeen tulleensa huijatuksi. Harmittavan usein uhrit myös jättävät rikoksista ilmoittamatta esimerkiksi häpeän tunteen takia.

### 6.7 Kyberaktivismi ja vakoilu

Kyberaktivismilla tarkoitetaan yksittäisen henkilön tai ryhmän kybertoimintaympäristössä harjoittamaa tavoitteellista tai aatteellista toimintaa. Sillä voidaan tavoitella huomiota tai muutosta johonkin asiaan, ja kyberaktivistit voivat käyttää myös luonteeltaan rikollisia keinoja. (Sanastokeskus TSK: *kyberaktivismi*.) Haktivismia voidaan kuvata eräänlaiseksi digitaaliseksi tottelemattomuudeksi, jota toteutetaan tekniikan avulla poliittisen viestin välittämiseksi. Sillä voidaan myös kannustaa muita tekemään hyökkäyksiä tietyn tarkoitusperän johdosta. (Cybersäkerhet i Sverige 2020, 12.) Haktivistit voivat käynnistää verkossa erilaisia kampanjoita esimerkiksi verkossa tapahtuvan valvonnan kasvun estämiseksi tai eläinten oikeuksien puolustamiseksi. Verkossa on myös helppo liittyä aktivistiryhmään. (Senker 2017, 65–66.)

Disinformaatiolla tarkoitetaan väärän tiedon tarkoituksellista käyttöä siten, että sillä pyritään vaikuttamaan yleiseen mielipiteeseen. Nykyisten kuluttaja-alustojen ja kuluttajapalvelujen, kuten sosiaalisen median ja hakukoneiden, avulla voidaan väärää tietoa levittää tehokkaasti ja laajasti. Tämä tarjoaa mahdollisuuden valtiollisille ja riippumattomille toimijoille väärän tiedon levittämiseen. (Microsoft 2021, 110.)

Kyberaktivistit voivat hyödyntää kybermaailmaa niin kansallisesti kuin globaalisti agendansa levittämiseksi ja julkisuuden saamiseksi. Aktivistit voivat ajaa omia tarkoitusperiään ja vahingoittaa esimerkiksi yritysten julkisuutta disinformaation keinoin. Yritykset voivat kärsiä taloudellista vahinkoa ja mainehaittaa. Haktivistit voivat käyttää verkkoa protestikeinona, ja motiivina voi olla esimerkiksi poliittiset syyt. Aktivismia voidaan toteuttaa yksilöinä ja ryhminä.

Valtioiden välinen kybervaikuttaminen on yleistä ja sen motiivina voivat olla esimerkiksi vakoilu, kriittisen infrastruktuurin häirintä tai poliittisen ilmapiirin muokkaaminen. Valtiot voivat vakoilla toisiaan tietoverkoissa, vaikuttaa toisiinsa ja poliittiseen ilmapiiriin sosiaalisen media avulla sekä tehdä kyberhyökkäyksiä toisten valtioiden tietoverkkoja ja kriittistä infrastruktuuria vastaan. Myös Suomea kohtaan on kohdistettu hyökkäyksiä. Kaikki hyökkäykset eivät aina päädy julkisuuteen, mutta esimerkiksi viime vuonna uutisoitiin eduskunnan tietojärjestelmiin ja kansanedustajien sähköposteihin kohdistuneista tapauksista. (Cyberwatch Q3 2021, 10–11.)

Suomeen kohdistuu kansainvälistä verkkovakoilua ja laaja-alaista vaikuttamista, kuten informaatio- ja hybridivaikuttamista (Cyberwatch lokakuu 2021, 6). Valtion toimijat voivat toteuttaa hyökkäyksiä kerätäkseen tietoa, jota voidaan käyttää oman maan ulko- ja turvallisuuspoliittisia etuja ajaessa tai talouden vahvistamiseksi (Cybersäkerhet i Sverige 2020, 8).

Suomen yhteiskunnan turvallisuutta voivat valtiollisten tahojen lisäksi uhata myös kyberrikolliset, jotka voivat kiristyshaittaohjelmilla estää yhteiskunnan kannalta kriittisiä toimijoita, kuten sairaala- tai vesihuoltotoimintaa. Kyberrikollisuus voi uhata Suomen kansallista turvallisuutta, vaikka rikollisen ensisijaisena tavoitteena olisikin hankkia rahaa. (SUPO: kansallisen turvallisuuden katsaus 2021.) Euroopan Unioni ja Saksa syyttivät Venäjää verkkourkinnasta, kun haitallisia kybertoimia havaittiin kohdistetun lukuisiin parlamenttien jäseniin, valtionhallintojen virkamiehiin, poliitikkoihin sekä kansalaisyhteiskunnan jäseniin EU:ssa. Venäjän epäillään pyrkineen vaikuttamaan pitkäkestoisilla operaatioillaan valtioiden vaaleihin. (Cyberwatch lokakuu 2021, 12.)

Kybervakoilu on kasvussa, koska sen toteuttaminen on entistä helpompaa ja tehokkaampaa. Vakoilu on vaikeasti havaittavissa sekä toimijoiden jäljittäminen on vaikeaa ja aikaa vievää. Valtioiden, yritysten ja yksittäisten henkilöiden tulisi muuttaa toimintatapojaan vakoilun estämiseksi. (Cyberwatch 7.7.2021, luettu 12.10.2021.)

Vuonna 2020 valtiolliset kyberhyökkäykset keskittyivät kasvavissa määrin yritysten konesalien palvelimiin sekä toimitusketjun haavoittuvuuksiin. Valtiollisista hyökkäyksistä 79 prosenttia kohdistui organisaatioihin ja 21 prosenttia kuluttajiin. Disinformaation levittämistä voidaan pitää nousevana uhkana. (Microsoft 2021, 52–53 ja 111) Vuoden 2021 aikana kyberhyökkäyksillä on ollut vaikutusta kansalliseen turvallisuuteen. On havaittu, että merkittävien rikosilmiöiden taustalla on useimmiten

järjestäytynyttä rikollisuutta, joskus jopa valtioihin kytkeytyvää toimintaa. (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021.)

### 6.8 Lapsiin kohdistuva rikollisuus

Lapset käyttävät entistä enemmän tietoverkkoa ja verkkoon kytkettyjä laitteita, mikä on kasvattanut rikollisten lapsiin kohdistuvaa seksuaalirikosten määrää. Rikollisten palveluteollisuus on mahdollistanut ja helpottanut laittoman lapsen seksuaalisen hyväksikäyttömateriaalin levittämistä.

Lapsiin kohdistuvat seksuaaliset teot verkossa ovat yleisiä ja kasvussa. Aikuisen lapseen kohdistama seksuaalinen teko on verkkoympäristössä rikos. On tärkeää, että rikoksista ilmoitettaisiin viranomaisille, koska tekijöillä voi olla useita uhreja ja ilmoittamalla voidaan estää rikollisen toiminnan jatkuminen. Verkossa tapahtuvat seksuaalirikokset voivat olla esimerkiksi seksuaalisävytteistä viestittelyä, kuvien tai videoiden lähettämistä tai pyytämistä tai web-kameran välityksellä tapahtuvaa hyväksikäyttöä. (Poliisi: *seksuaalirikokset*, luettu 8.10.2021.)

Yksityisten toimijoiden näkökulmasta haasteena on toiminnan havaitseminen esimerkiksi viestintäpalveluissa. Viranomaisten näkökulmasta tutkiminen ja paljastaminen on haasteellista palveluteollisuuden ja anonymisoinnin takia. Materiaalia levitetään pimeissä verkoissa, ja tekijöiden kiinni saaminen on vaikeaa ja työlästä. Poliisin rajalliset resurssit asettavat haasteita vinkkitietojen läpikäymiseen ja materiaalin poistamiseen. Poliisilla tulisi olla riittävät työkalut ja resurssit lapsiin kohdistuvan rikollisuuden torjumiseksi, kitkemiseksi, tutkimiseksi ja paljastamiseksi.

Viranomaisten lisäksi yksityiset toimijat ovat tarjonneet palveluitaan ja teknologiaansa lasten seksuaalisen hyväksikäytön havaitsemiseksi ja materiaalin poistamiseksi (EU:n neuvosto 2021, luettu 8.10.2021). Verkossa tapahtuva lasten hyväksikäyttö on yksi järjestäytyneen ja vakavan rikollisuuden torjunnan prioriteeteistä 2022–2025 (EMPACT 2021, 6).

Lapsiin kohdistuvan seksuaaliväkivaltamateriaalin levittäminen verkossa on ollut pandemian aikana kasvussa. Pandemian aikana lapset viettivät enemmän aikaa verkossa kuin aikaisemmin. Lapset jakoivat kuvia ja videoita, joita rikolliset hyödynsivät muun muassa kohteidensa valitsemisessa. Rikolliset hyödynsivät myös salattuja keskustelusovelluksia, mikä vaikeutti rikosten selvittämistä ja paljastamista. Myös itse tuotetun suoratoistomateriaalin kasvun katsottiin olevan kasvussa. Rikolliset levittivät materiaalia pimeissä verkoissa salaisten viestien avulla. Hyväksikäytön todettiin olevan entistä kaupallisempaa. (IOCTA 2020, 36–38.)

Vuonna 2020 verkossa tapahtuvia lasten seksuaaliseen hyväksikäyttöön liittyviä rikosilmoituksia kirjattiin Suomessa noin 2000 kappaletta. Poliisi arvioi, että vuonna 2021 määrä kasvaa edellisvuoteen verrattuna. (Tietoverkkorikollisuus poliisin silmin 2020–2021, luettu 17.10.2021.)

### 6.9 Tekoäly

Tekoälyllä (englanniksi *artificial intelligence, AI*) tarkoitetaan koneen kykyä käyttää perinteisesti ihmiseen älyyn liitettyjä taitoja, kuten oppimista, suunnittelemista, päättelyä tai luomista. Tekoälyn ansiosta tekniset järjestelmät voivat havainnoida ympäristöään, käsitellä havaintojaan ja ratkaista ongelmia saavuttaakseen halutun päämäärän. Esimerkiksi tietokone voi ottaa vastaan tietoa, jonka sen omat tunnistimet ovat keränneet, käsitellä sen ja vastata siihen. (Euroopan parlamentti 2021, luettu 9.10.2021.)

Tekoäly pitää sisällään eri tieteiden menetelmiä, jotka yhdessä muodostavat älykkään järjestelmän. Tekoälyn perustana voidaan pitää koneoppimismenetelmiä. (Tarkoma 2017, luettu 9.10.2021.) Koneoppiminen (englanniksi *machine learning*) hyödyntää olemassa olevia käyttäytymismalleja sekä tekee päätöksiä käytettyyn dataan ja päätelmiin perustuen. Syväoppiminen (englanniksi *deep learning*) tekee päätöksiä aiempien mallien mukaisesti, mutta se osaa myös tehdä säätöjä itse ja juuri tämä erottaa sen koneoppimisesta. (Tekoäly ja koneoppiminen kyberturvallisuudessa, luettu 14.10.2021.)

Yhä laajenevissa määrin yhteiskunnan tärkeillä osa-alueilla hyödynnetään tekoälyä. Tekoälyratkaisut mahdollistavat entistä laajemman automatisoinnin ja päätöksenteon tuen, mutta samalla luovat uusi haasteita järjestelmien suojaamiseen ja toiminnan varmistamiseen. Tekoälyteknologia asettaa myös kokonaisturvallisuuden kannalta haasteita. Tekoäly voi olla esimerkiksi haitallista, tekoälyjärjestelmiä vastaan voidaan hyökätä ja tekoäly voi erehtyä. (Tarkoma 2017, luettu 9.10.2021.)

Tekoälyllä voidaan katsoa olevan kahdenlaisia vaikutuksia. Tekoälystä voi olla valtavaa etua yhteiskunnalle, mutta se voi myös aiheuttaa digitaalisia, fyysisiä ja poliittisia uhkia (IOCTA 2020, 18). Viranomaiset ja yksityiset toimijat voivat käyttää tekoälyä rikoksentorjunnassa, mutta myös kyberrikolliset voivat hyödyntää tekoälyä rikollisessa toiminnassaan. Tekoäly mahdollistaa väärinkäytökset tekoälyä vastaan voidaan esimerkiksi harjoitella hyökkäyksiä ja se voidaan opettaa tekemään rikoksia, hankkimaan tietoja uhrista tai löytämään heikkouksia verkoista ja järjestelmistä.

Rikolliset voivat esimerkiksi käyttää hyväkseen tekoälyä helpottaakseen ja parantaakseen hyökkäyksiä sekä maksimoidakseen hyödyn mahdollisimman lyhyessä ajassa. Tekoälyn avulla voidaan myös hyväksikäyttää uusia uhreja ja löytää entistä innovatiivisempia rikosmalleja. Edellä mainittujen seikkojen ansiosta rikollisen kiinnijäämisriski pienenee. Tekoälyä voidaan käyttää myös palveluna (englanniksi *AI-as-a-service*), jonka avulla osaamista ja teknistä asiantuntemusta ei enää tarvita. Tulevaisuuden skenaarioina voidaan pitää muun muassa tekoälyä hyödyntäviä haittaohjelmia, käyttäjän manipulointia, salasanojen arvaamista ja tiedustelua. (IOCTA 2020, 18.) Tekoälyn avulla voidaan myös matkia esimerkiksi toimitusjohtajan ääntä toimitusjohtajahuijauksissa (IOCTA 2020, 47).

Tekoälyä voidaan myös hyödyntää tietojenkalastelussa, jolloin laite oppii täydellisiä huijaustekniikoita. Kyberrikolliset voivat hyödyntää tekoälyä ja koneoppimistekniikoita parantaakseen huijaustekniikoitaan. Yhtenä tapana voidaan käyttää älykkäitä haittaohjelmia tietojen louhintaan käyttäjien tietokoneissa ja puhelimissa. Tietojenkalastelua voi täten hienosäätää hyökkäyksen kohteen verkkotottumusten ja mieltymysten perusteella, kuten sen perusteella, millä sivustoilla käyttäjä on vieraillut ja mistä tehnyt verkko-ostoksia. Älykkäitä tietojenkalasteluja on vaikeampi havaita, koska ne on suunniteltu ainutlaatuisesti näyttämään kohdeyleisön mielestä laillisilta ja vakuuttavilta. (GB Tech, luettu 9.10.2021.)

Tekoäly koneoppimisen tukemana on tehokas lähitulevaisuuden työkalu kyberturvallisuudessa. Ihmisten työpanostus on nykyisin suuri kyberturvallisuudessa, mutta tulevaisuudessa teknologia voi suoriutua tehtävistä ihmisiä paremmin. Tekoäly toimii ilman väsymystä, lyhyellä vastausajalla, tehokkaasti ja ilman inhimillisiä virheitä. Koneoppimisratkaisuja voidaan pitää tehokkaimpina nykyisin voimassa olevien kyberturvallisuuden työkaluina. (Tekoäly ja koneoppiminen kyberturvallisuudessa, luettu 14.10.2021.) Tekoäly voi avata uusia mahdollisuuksia kyberrikollisuudelle.

# 7 YHTEENVETO

Kyberrikollisuus on ollut kasvussa usean vuoden ajan ja se aiheuttaa yhä kasvavissa määrin enemmän vahinkoa, niin taloudellista kuin muuta haittaa. Kyberrikokset ovat yhä yleisimpiä ja ne koskettavat meitä kaikkia. Kyberrikosten kohteina ovat yksityiset henkilöt, yritykset ja organisaatiot. Kyberrikosten todellinen lukumäärä saattaa olla merkittävästi suurempi, koska suurin osa kyberrikoksista jää ilmoittamatta viranomaisille. Kyberrikollisuus on vuosien saatossa muuttunut yhä ammattimaisemmaksi ja järjestyneemmäksi, ja siitä on tullut kansainvälistä rajat ylittävää rikollisuutta. Kyberrikolliset hyödyntävät entistä enemmän ja paremmin teknologiaa rikollisessa toiminnassaan.

Rikollisten markkinapaikkana toimiva palveluteollisuus on kehittynyt perinteisten hierarkkisten rikollisryhmien ja verkostojen rinnalle. Palveluteollisuuden avulla voivat rikolliset vaihtaa salatusti tietoja, tiedostoja, työkaluja, ohjelmistoja, pääsyjä verkkosivustoille tai järjestelmiin sekä käydä kauppaa erilaisista tuotteista. Rikollinen voi esimerkiksi myydä pääsynsä tai haittaohjelmansa toiselle rikolliselle, jolla ei tarvitse edes olla tietoteknistä osaamista kyberrikoksen toteuttamiseksi. Rikolliset hyödyntävät markkinapaikoilla virtuaalivaluuttoja anonyymissa maksamisessa ja rahanpesun välineenä. Palveluteollisuuden kasvua ja kehitystä voidaan pitää tulevaisuuden uhkana kyberrikollisuudessa.

### 7.1 Kyberrikollisuuden trendit vuonna 2021

Euroopan ja Suomen tämänhetkisissä kyberrikollisuuden trendeissä on havaittavissa yhtäläisyyksiä. Euroopassa kyberrikollisuus on tunkeutunut lähes kaikille rikosaloille. Aiemmat trendit ovat säilyttäneet asemansa nykyisten trendien parissa, mutta myös uusia ja erilaisia kyberrikollisuuden muotoja on havaittavissa.

Kiristyshaittaohjelmat ovat muodostuneet selkeäksi trendiksi Euroopassa ja Suomessa. Kiristyshaittaohjelmahyökkäysten määrä on ollut kasvussa maailmanlaajuisesti. Kiristyshaittaohjelmahyökkäyksiä kohdistetaan yhä enemmän yrityksiin. Kiristyshaittaohjelmissa voidaan hyödyntää myös muita rikoksen tekotapoja samanaikaisesti. Kiristyshaittaohjelmat voivat aiheuttaa merkittäviä taloudellisia kustannuksia ja muuta haittaa yrityksille ja organisaatioille. Kiristyshaittaohjelmat voivat aiheuttaa haittaa myös yrityksen asiakkaille ja koko toiminnalle. Rikollinen voi vuotaa yrityksestä saamiaan arkaluontoisia tietoja eteenpäin. Myös suomalaiseen kriittisen infrastruktuurin järjestelmään kohdistettiin kiristyshaittaohjelmahyökkäys.

Kryptovaluutta on kyberrikollisten suosiossa, koska se ei ole sidoksissa keskuspankkeihin tai valtioihin eikä sillä ole olemassa yhteistä sääntelyjärjestelmää. Kryptovaluutat tarjoavat rikollisille nimettömyyttä, ja ne toimivat tärkeänä keinona maksaa rikollisista tuotteista ja palveluista. Valuuttaliikenteen valvonta ja seuraaminen aiheuttaa haasteita viranomaisille. Kryptovaluuttojen louhinta on kallista sen sähkönkulutuksen takia, minkä takia rikolliset hyödyntävät louhinnassa kryptovaluutan louhintahaittaohjelmia. Haittaohjelmat vievät uhrin laitteesta osan prosessitehosta. Kryptokaappausten avulla rikolliset voivat ulkoistaa louhintaliiketoimen ulkopuolisille hyötykuormana. Energian hinnannousulla saattaa olla vaikutuksia kryptokaappausten suosioon lähitulevaisuudessa.

Verkossa tapahtuvat lapsiin kohdistuvat seksuaalirikokset ovat olleet kasvussa viime vuosina. Viranomaisten tietoon tulleiden tapausten määrää pidetään aliraportoituna. Kyberympäristön laajentuminen on kasvattanut hyväksikäyttömahdollisuuksia, koska rikolliset tavoittavat tietoverkkojen kautta lapset helpommin. Live-streamauksen eli suoratoiston kautta tapahtuvaa lapsiin kohdistuvia seksuaaliväkivaltarikoksia pidetään Euroopassa uhkana. Lapsiin kohdistuvaa seksuaaliväkivaltamateriaalia levitetään salaustyökaluja ja anonymisointia hyödyntäen.

Palvelunestohyökkäyksiä pidetään yhtenä keskeisenä kyberrikoksena, ja hyökkäyksistä on tullut yhä hajautetuimpia. Rikolliset hyödyntävät hyökkäyksissä kiristystä, kohdentamista ja automatisointia. Hyökkääjät suosivat palvelunestohyökkäyksissä rikollisten palveluteollisuutta ja pienten yritysten tietoturvapuutteita. Palvelunestohyökkäykset ovat olleet yksi suurimmista kyberrikollisuuden trendeistä vuosien ajan.

Petosrikokset ja erilaiset huijaukset ovat olleet rikollisten suosiossa jo useita vuosia. Petosrikollisuus on monimuotoista ja sen arvioidaan kasvavan tulevaisuudessa. Erilaiset petosrikokset, kuten CEO- ja BEC-huijaukset, ovat säilyttäneet suosionsa. Muihin maksuvälineisiin kuin käteisrahaan liittyvä petosrikollisuus on monimuotoistunut esimerkiksi e-skimmauksen ja SIM Swap -muodossa. Petosrikollisuus on kansallista ja kansainvälistä rikollisuutta, joka on entistä järjestäytyneempää ja ammattimaisempaa. Suomessa erilaiset huijaukset ovat säilyttäneet asemansa osana petosrikollisuutta. Rikolliset hyödyntävät erilaisia huijausmuotoja, kuten tilausansoja, rakkaus- ja pankkihuijauksia sekä toimitusjohtajahuijauksia. Suomessa petosrikoksia toteutetaan tekstiviestien, sähköpostien ja eri verkkomarkkinapaikkojen kautta. Huijausrikoksissa tekijät hyödyntävät tietojenkalastelua ja käyttäjän manipulointia.

Tietojenkalastelua ja käyttäjän manipulointia hyödynnetään yhä enemmän kyberrikoksissa. Tietojenkalastelu on vakiinnuttanut paikkansa kybertrendien joukossa. Käyttäjän manipulointia pidetään yhtenä suurimpana uhkana osana erityyppisten kyberrikosten tekoa.

Yksittäisten kansalaisten henkilötietoja sijaitsee yhä enemmän verkkomaailmassa eri palveluilla ja järjestelmissä. Rikollisten päästessä käsiksi henkilötietoihin voidaan niitä myydä eteenpäin rikollisten markkinoilla. Kolmannet osapuolet voivat henkilötiedot saatuaan käyttää toisen identiteettiä laittomasti. Myös tietomurrot ovat edelleen kyberrikollisten suosiossa. Edellisvuosina esillä ovat olleet erityisesti Microsoft Office 365 -tietomurrot ja psykoterapiakeskus Vastaamon tapaus.

Rikolliset ovat löytäneet IoT-laitteista haavoittuvuuksia. Tekijät ovat hyödyntäneet heikkoja tietoturvia ja päivitysten vanhentumisia rikoksissa. IoT-laitteet voidaan kytkeä eri järjestelmiin ja ohjelmiin, ja niiden avulla voidaan ohjata ja monitoroida monenlaisia kokonaisuuksia. Tämä asettaa haasteita tietoturvalle ja kyberturvallisuudelle.

### 7.2 Kyberrikollisuuden trendit vuosina 2022–2024

Kyberrikollisten yhteisö ja markkinat eli palveluteollisuus on kasvanut ja yleistynyt edellisten vuosien aikana. Palvelumarkkinat ovat luoneet rikollisille otollisen paikan käydä kauppaa tuotteista ja palveluista. Rikolliset hyödyntävät yhä enemmän palveluteollisuutta erilaisten pääsyjen, ohjelmien ja hyökkäyksien kauppaamisessa. Palveluteollisuuden avulla rikoksentekijältä ei edellytetä tietoteknistä osaamista hyökkäyksen toteuttamiseksi. Rikolliset voivat hyödyntää toistensa osaamista virtuaalisessa alamaailmassa esimerkiksi vaihtamalla tietoa ja taitoa keskenään. Kyberrikolliset suosivat teknologian kehitystä rikoksentekomenetelmissään.

Kiristyshaittaohjelmien suosiolle ei näy laskua. Haittaohjelmista on tullut entistä kohdennetuimpia, automaattisia ja niitä tehdään entistä suuremmalla volyymilla. Kiristyshaittaohjelmia kohdennetaan yhä enemmän myös matkapuhelimiin. Haittaohjelmista on tullut uskottavampia ja niissä voidaan

hyödyntää kolmea eri elementtiä: sulkemis-, lukitsemis- ja hybridimenetelmää. Kiristyshaittaohjelmilla vaaditaan suurempia lunnaita ja ne ovat aikaisempaa kohdistetumpia. Globaalisti hyökkäysten määrä on lisääntynyt ja ne ovat muuttuneet ammattimaisimmiksi. Kiristyshaittaohjelmia ovat vakava ja edelleen kasvava ongelma kyberrikollisuudessa (Microsoft 2021, 8 ja 19).

Esineiden internet jatkaa kasvuaan. Laitteiden tietoturvahaavoittuvuudet ja päivityspuutteet mahdollistavat salasanojen, käyttäjätunnusten ja muiden tietojen hankkimisen rikollisin keinoin. IoT-laitteiden avulla voi rikollinen päästä murtautumaan esimerkiksi yrityksen ohjelmiin tai järjestelmiin. Laitteita kytketään yhä enemmän verkkoon, mikä altistaa ne kyberrikollisuuden vaaroille.

Automaatiojärjestelmiä käytetään yhä enemmän kriittisen infrastruktuurin toimintaan ja valvontaan. Järjestelmiä liitetään useammin verkkoon ja sitä kautta niihin kohdistuu kyberriskejä. Automaatiojärjestelmiin arvioidaan kohdistettavan tulevaisuudessa kohdistettuja ja monimutkaisia hyökkäyksiä. Automaatiojärjestelmiä voidaan pitää yhtenä houkuttelevimmista kyberhyökkäyskohteista lähitulevaisuudessa.

Tietojenkalastelua ja käyttäjän manipulointia hyödynnetään tulevaisuudessa yhä enemmän kyberrikollisuudessa. Rikolliset keksivät ja kehittävät jatkuvasti uusia muotoja ja menetelmiä hankkiakseen tietoja henkilöstä, yrityksestä tai organisaatiosta. Tietojenkalastelua voidaan kohdistaa useisiin kohteisiin samanaikaisesti ilman suuria henkilöresursseja tai kustannuksia.

Rikolliset hyödyntävät kryptovaluuttaa lunnasvaatimuksissa, kryptovaluutan louhintahaittaohjelmissa ja rahansiirroissa. Kryptovaluuttaliikennettä on vaikea jäljittää ja valvoa. Kryptovaluutan salauksen ja anonymiteetin ansiosta on rikollisten jäljittäminen haastavampaa. Kryptovaluutta yleistyy ja sitä louhitaan jatkuvasti. Louhinnasta aiheutuvat korkeat kustannukset lisäävät kyberrikollisten houkuttelevuutta hyödyntää kryptokaappauksia tulevaisuudessa. Kryptokaappausten ansiosta rikollisen ei tarvitse ostaa kalliita laitteistoja tai maksaa korkeita sähkölaskuja.

Petosrikokset ja erilaiset huijaukset ovat olleet vuosia kyberrikollisten suosiossa. Rikoksissa ja huijauksissa voidaan hyödyntää tietojenkalastelua ja käyttäjän manipulointia. Rikoksentekomenetelmiä on lukuisia ja niistä on tullut entistä ammattimaisempia, kohdennetuimpia, teknisimpiä ja selkokielisempiä.

Kyberaktivismilla tavoitellaan huomiota tai muutosta joihinkin asioihin, ja niissä voidaan käyttää rikollisia keinoja. Kyberaktivismilla voidaan levittää omaa agendaa tai levittää disinformaatiota. On tiedostettu, että hybridivaikuttaminen on yleistynyt. Valtioilla ja organisaatioille on tällä hetkellä ja tulevaisuudessa suuremmat kyvykkyydet kybervakoiluun. Vakoilun tapahtuessa tietoverkoissa tai tietoteknisiä laitteita hyödyntämällä on hyökkääjän identifiointi vaikeaa ja kiistettävissä. Kasvava

kybervaikuttaminen on yksi tulevaisuuden trendeistä. Kyberrikollisuudella voidaan vaikuttaa Suomen kansalliseen turvallisuuteen ja kriittisiin toimijoihin.

Lapsiin kohdistuvat seksuaalirikokset ovat olleet kasvussa viime vuosina. Rikollisten palveluteollisuus on mahdollistanut lapsiin kohdistuvan seksuaaliväkivaltamateriaalin levittämisen ja kaupallistamisen. Rikollisuudessa hyödynnetään pimeiden markkinoiden lisäksi salaustyökaluja ja salaisia viestivälineitä. Suoratoistopalveluiden hyödyntäminen lapsiin kohdistuvissa seksuaalirikoksissa on ollut kasvussa eikä hidastumista valitettavasti ole näköpiirissä. Lapsia voidaan tietoverkoissa kiristää ja houkutella erilaisiin seksuaalisiin toimiin. Viranomaisten arvion perusteella Suomessa enteillään tietoverkoissa tapahtuvan lasten seksuaalisten hyväksikäyttötapausten määrän nousevan tulevaisuudessa.

Rikolliset voivat tulevaisuudessa hyödyntää tekoälyä rikollisessa toiminnassaan. Tekoälyn avulla tai sen kanssa voidaan harjoitella hyökkäyksiä, tehdä ja kehittää parempia hyökkäyksiä, ja löytää heikkouksia järjestelmistä ja verkoista. Tekoälyä voidaan tulevaisuudessa hyödyntää haittaohjelmissa, tietojenkalastelussa, käyttäjän manipuloinnissa ja tietomurroissa. Tekoäly ja koneoppiminen mahdollistavat tehokkaammat hyökkäykset verrattuna ihmisten tekemiin hyökkäyksiin, koska tekoäly voi hyökätä tehokkaasti ilman väsymistä, suurilla resursseilla, samanaikaisesti ja ilman inhimillisiä virheitä.

### 7.3 Kyberrikollisuuden torjunta

Kyberrikollisuuden torjumiseksi on eri viranomaisten tehtävä tiivistä yhteistyötä kansallisesti ja kansainvälisesti. Torjunnassa tarvitaan myös viranomaisten ja yksityisten toimijoiden välistä yhteistyötä. On varmistettava yhteiset ajantasaiset kyberturvallisuusstrategiat ja lainsäädäntö kyberrikollisuuden torjumiseksi.

Kyberturvallisuudesta huolehtiminen kuuluu kaikille - yksittäisille ihmisille, yrityksille ja organisaatioille. Teknologiariippuvuus ja digitalisaatio koskettavat meitä kaikkia. Tietoturvasta ja kyberhygieniasta on pidettävä huolta sekä kyberrikollisuuteen ja kyberuhkiin on varauduttava. Valtio- ja organisaatiotasolla on huolehdittava turvallisuustarpeista, harjoitella puolustautumista, tehostaa nykyisiä suojauskeinoja, arvioida riskejä, pitää yllä ajankohtaista tilannekuvaa, huolehtia sietokyvystä sekä laatia suunnitelmia ja ohjeita.

Rikollisten palveluteollisuuteen, tekoälyyn ja robotiikkaan hyödyntävään rikollisuuteen on pyrittävä vastaamaan mahdollisimman tehokkaasti tulevaisuudessa. Viranomaisten, etenkin poliisin, on tunnistettava rikostorjunnan tarpeet, ja tehostettava toimintaansa kyberrikollisuutta vastaan. Kyberosaamisesta on huolehdittava muun muassa tutkintoon johtavissa koulutusohjelmissa ja muussa koulutuksessa. Osaamista on kehitettävä ja se on varmistettava. Poliisilla on oltava riittävä kyky

vastata kyberrikollisuuteen, myös tulevaisuudessa. Kyberrikokset ovat vaikeita rikoksia tutkia, koska tekijä saattaa oleskelle toisella puolella maapalloa tai hän osaa piilottaa jälkensä taitavasti.

Kyberrikollisuutta ei kuitenkaan torjuta ainoastaan viranomaistasolla, vaan viranomaisten on tehtävä yhteistyötä yksityisen sektorin kanssa kansallisesti ja kansainvälisesti. Lainsäädännön kehittämiseen ja ajantasaisuuteen on kiinnitettävä huomiota, vaikka kyberrikollisuuden monimuotoisuus ja kompleksisuus asettavatkin kehittämiselle haasteita. Olisi toivottavaa, että jokainen kyberrikoksen uhri ilmoittaisi rikoksesta viranomaisille. Siten saataisiin ajankohtaista tilannekuvaa kyberrikollisuuden ilmiöistä ja pystyttäisiin lähettää selkeä viesti kyberrikollisille, että rikoksia ei hyväksytä.

Jokaisella käyttäjällä on oma vastuunsa kyberrikollisuuden torjunnassa. Tästä syystä on kyberhygieniasta pidettävä huolta ja kybertietoisuutta levitettävä kaikilla tasoilla. Jokainen käyttäjä on saatava mukaan huolehtimaan kyberturvallisuudesta. Kyberrikollisuus elää jatkuvassa muutoksessa ja kyberrikolliset kehittävät jatkuvasti uusia kyberrikosilmiöitä. Kyberrikollisuus on arvaamatonta ja monimuotoista. Digitalisaation kehittyminen luo rikollisille uusia mahdollisuuksia ja vaikeuttaa rikollisuuden ennakointia.

# 8 POHDINTA

Opinnäytetyön aihe oli laaja ja tekijälleen entuudestaan tuntematon. Aihe edellytti asiaan paneutumista ja uuden opettelua. Aiheeseen liittyvää materiaalia oli runsaasti saatavilla suomen, ruotsin ja englannin kielillä, mikä aiheutti myös haasteita aineiston keruulle ja käsittelylle.

Opinnäytetyöprosessi eteni aikataulun mukaisesti, vaikka aihe laajenikin työn aikana. Alkuperäisen suunnitelman mukaan tarkoituksena oli arvioida ainoastaan seuraavan kolmen vuoden trendejä. Nykytilanteen käsittelemisen laajuuden vuoksi oli luonnollista muuttaa tutkimuskysymystä, ja opinnäytetyön aihetta koko työn sisältöä vastaavaksi. Uusien asioiden opettelu vei suunniteltua enemmän aikaa, koska kyberrikollisuus on monimutkainen ja kompleksinen rikollisuuden ala. Aihe oli tekijälle erittäin mielenkiintoinen, mikä vaikeutti muun muassa työn rajaamista. Lisäksi haasteita aiheuttivat oikeiden ja ymmärrettävien suomennusten löytäminen sekä käännöstyö kokonaisuudessaan. Aineistoa käytiin laaja-alaisesti läpi, ja ensisijaisesti työssä pyrittiin käyttämään kansallisia ja kansainvälisiä viranomaislähteitä. Käytetty aineisto oli pääsääntöisesti ajankohtaista, luotettavaa ja edustavaa. Aineisto osoitti aiheen laajuuden ja käsittelyä olisi voitu vieläkin jatkaa. Lähteitä olisi voinut päivittää loputtomiin, ja työn viimeistelyyn panostaa entistä enemmän.

Opinnäytetyössä saavutettiin sille asetetut tavoitteet eli koostaa tietoa kyberrikollisuuden nykytilasta sekä tehdä arvioita seuraavan kolmen vuoden trendeistä. Lisäksi opinnäytetyössä vastattiin

tutkimuskysymykseen valittuja menetelmiä käyttäen. Tutkimusmenetelmien valinnat osoittautuivat oikeiksi ja edesauttoivat työn loppuun saattamisessa. Opinnäytetyön tekijälle tutkimus oli valtava ja hieno oppimisprosessi.

Kyberrikollisuutta ja sen trendejä tulisi arvioida säännöllisesti. Selkeää tilannekuvaa on muodostettava ja päivitettävä jatkuvasti. Kyberrikollisuutta on seurattava riittävän tarkasti, ja seurannan tulisi olla laadukasta. Kyberrikollisuuden tilastointia tulisi käydä läpi toistuvasti. Kyberrikollisuuden ilmiöitä ja trendejä tulisi päivittää tasaisin väliajoin, ja tulevia uhkia arvioida aktiivisesti. Tarvetta jatkotutkimukselle tulevaisuuden kyberrikollisuuden trendien päivittämiseksi olisi esimerkiksi vuoden päästä. Jatkotutkimuksessa voitaisiin tehdä katsaus senhetkisestä nykytilasta ja tulevista kyberrikollisuuden trendeistä. Vastaavanlaista tutkimusta tai opinnäytetyötä ei ole Poliisiammattikorkeakoulussa aiemmin tehty.

Kyberrikollisuus koskettaa meistä jokaista.

# LÄHTEET


Australian Institute of Family Studies 2015: Conceptualising the prevention of child sexual abuse, Antonia Quadara, Vicky Nagy, Daryl Higgins and Natalie Siegel, Australian government. Australia. Luettavissa: https://acuresearchbank.acu.edu.au/download/5bb2f7760724b150faee97eef3bf9afcfd4cb50e87d7fbab4096c71055c5c82c/1704205/OA_Quadara_2015_Conceptu%02alising_the_prevention_of_child_sexual.pdf. Luettu 6.10.2021.

Blackfog: The state of Ransomware in 2021, julkaistu 01.10.2021. Luettavissa: https://www.blackfog.com/the-state-of-ransomware-in-2021/. Luettu 9.10.2021.

Cimpanu, Catalin 2020: First death reported following a ransomware attack on a German hospital, Zeroday, ZDNet. julkaistu 17.9.2020. Luettavissa: https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/. Luettu 5.10.2021.

CoinMarketCap: Today's Cryptocurrency prices by Market Cap. Luettavissa: https://coinmarketcap.com/. Luettu 29.10.2021.

ComputerSweden 2017: Bekräftat: ddos-attack bakom tågförseningar, julkaistu 11.10.2017. Luettavissa: https://computersweden.idg.se/2.2683/1.690504/ddos-bakom-tagforseningar. Luettu 6.10.2021.

CYBERDI 2021: Kyberrikos on poliisiasia – Opas yrityksille kyberrikostutkinnan kulusta. Opetus- ja kulttuuriviraston rahoittama CYBERDI-hanke, julkaistu maaliskuu 2021.

Cyber Security Intelligence 2021: Cyber crime just keeps on growing, julkaistu 27.9.2021. Luettavissa: https://www.cybersecurityintelligence.com/blog/cyber-crime-just-keeps-on-growing-5888.html. Luettu 30.9.2021.

Cybersäkerhet i Sverige 2020: FRA, Försvarsmakten, MSB, Polisen & Säkerhetspolisen: Hot, metoder, brister och beroenden. Luettavissa: https://www.msb.se/contentassets/e25a61193a12414d9840f81c70841be3/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf. Luettu 13.10.2021.

Cyberwatch Q1 2021: Kvartaalikatsaus 2021, Q1 2021, Cyberwatch Finland.

Cyberwatch Q3 2021: Kvartaalikatsaus 2021, Q3 2021, Cyberwatch Finland.

Cyberwatch lokakuu 2021: Lokakuu-kuukausikatsaus 2021, Cyberwatch Finland.

Cyberwatch 7.7.2021: Mitäs me sanottiin? Cyberwatch Finland, julkaistu 7.7.2021. Luettavissa: https://www.cyberwatchfinland.fi/fi/mitas-me-sanottiinkaan/. Luettu 4.10.2021.

Cyberwatch 9.8.2021: Mitäs me sanottiinkaan? Cyberwatch Finland, julkaistu 9.8.2021. Luettavissa: https://www.cyberwatchfinland.fi/fi/mitas-me-sanottiinkaan-v-4/. Luettu 4.10.2021.

FBI 2020: Federal Bureau of Investigation, Internet crime complaint center: Internet Crime report 2020. Luettavissa: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. Luettu 14.10.2021.

F-Secure 2019: Attack landscape H2 2019, F-Secure. Luettavissa: https://blog-assets.f-secure.com/wp-content/uploads/2020/03/04101313/attack-landscape-h22019-final.pdf. Luettu 24.9.2021.

F-Secure 2020: Attack landscape update, Ransomware 2.0, automated recon, supply chain attacks, and other trending threats. Luettavissa: https://blog-assets.f-secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf. Luettu 9.10.2021.

EMPACT 2021, Euroopan unionin neuvosto, EMPACT fighting crime together, Neuvoston päätelmät järjestäytyneen ja vakavan kansainvälisen rikollisuuden torjuntaa koskevien EU:n prioriteettien asettamisesta EMPACTia varten vuosiksi 2022–2025, julkaistu 12.5.2021 Bryssel, Belgia. Luettavissa: https://data.consilium.europa.eu/doc/document/ST-8665-2021-INIT/fi/pdf. Luettu 7.10.2021.

Euroopan parlamentti 2021: Mitä tekoäly on ja mihin sitä käytetään? julkaistu 29.3.2020. Luettavissa: https://www.europarl.europa.eu/news/fi/headlines/society/20200827STO85804/mita-tekoaly-on-ja-mihin-sita-kaytetaan. Luettu 9.10.2021.

Euroopan unionin neuvosto 2021a: Eurooppa-neuvosto, Järjestäytyneen rikollisuuden torjunta: neuvoston 10 prioriteettia seuraavaksi neljäksi vuodeksi, julkaistu 26.5.2021. Luettavissa: https://www.consilium.europa.eu/fi/press/press-releases/2021/05/26/fight-against-organised-crime-council-sets-out-10-priorities-for-the-next-4-years/. Luettu 24.9.2021.

Euroopan unionin neuvosto 2021b: Eurooppa-neuvosto, Järjestäytyneen rikollisuuden vastainen EU:n toimien tuloksia 2020. Luettavissa: https://www.consilium.europa.eu/fi/infographics/results-eu-fight-against-crime-2020/. Luettu 24.9.2021.

Euroopan unionin neuvosto 2021c: Eurooppa-neuvosto, Kyberturvallisuus: miten EU torjuu kyberuhkia? Luettavissa: https://www.consilium.europa.eu/fi/policies/cybersecurity/#. Luettu 5.10.2021.

Euroopan unionin neuvosto 2020: Ehdotus neuvoston päätelmiksi EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle, julkaistu Bryssel, Belgia 9.3.2021. Luettavissa: https://www.consilium.europa.eu/fi/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/. Luettu 28.9.2021.

Euroopan unionin neuvosto 2019: EU tiukensi sääntöjään muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten torjumiseksi, lehdistötiedote, julkaistu 9.4.2019. Luettavissa: https://www.consilium.europa.eu/fi/press/press-releases/2019/04/09/eu-puts-in-place-tighter-rules-to-fight-non-cash-payment-fraud/. Luettu 8.10.2021.

Euroopan unioni: Europol, Euroopan unionin lainvalvontayhteistyövirasto (Europol). Luettavissa: https://europa.eu/european-union/about-eu/agencies/europol_fi. Luettu 2.10.2021.

Euroopan unionin neuvosto: Convention on Cybercrime, European Treaty Series 185, 2001 Budapest, julkaistu 23.11.2001. Luettavissa: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Luettu 8.10.2021.

Eurooppa neuvosto: Järjestäytyneen rikollisuuden torjunta EU:ssa. Luettavissa: https://www.consilium.europa.eu/fi/policies/eu-fight-against-crime/. Luettu 6.10.2021.

Eurooppa-neuvosto 2018: Euroopan unionin neuvosto, EU:n toimintapoliittinen sykli järjestäytyneen ja vakavan kansainvälisen rikollisuuden torjumiseksi. Luettavissa: https://www.consilium.europa.eu/fi/documents-publications/publications/empact/. Luettu 3.10.2021.

EU:n neuvosto 2021: Verkossa tapahtuva lasten hyväksikäytön torjunta – neuvosto valmis neuvottelemaan väliaikaisesta toimenpiteestä, julkaistu 28.10.2020. Luettavissa: https://www.consilium.europa.eu/fi/press/press-releases/2020/10/28/combating-child-abuse-online-council-ready-to-negotiate-a-temporary-measure/. Luettu 8.10.2021.

European Union terminology, IATE. Luettavissa: https://iate.europa.eu/entry/result/2228657/all. Luettu 23.9.2021.

Europol 2011: Europol-katsaus, yleiskertomuksia Europolin toiminnasta, Euroopan poliisivirasto 2011. Luettavissa: https://www.europol.europa.eu%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2Ffi_europolreview.pdf&usg=AOvVaw1Hg86oA4d7_jam0KG8q3oB. Luettu 2.10.2021.

Europol EC3, EBF, Poliisi, Finanssiala, Traficom Authority 2020: BEC-huijaus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/CEO%20fraud_FI_2020.pdf. Luettu 19.9.2021.

Europol EC3, EBF, Poliisi, Finanssiala, Finnish commucations Regulatory Authority 2021: Deittihuijaus. Luettavissa: https://www.europol.europa.eu/sites/default/files/documents/fi_0.pdf. Luettu 19.9.2021.

Europol EC3, EBF, Poliisi, Finanssiala, Finnish commucations Regulatory Authority 2021: Tietojenkalasteluviestit. Luettavissa: https://www.europol.europa.eu/sites/default/files/documents/fi_0.pdf. Luettu 19.9.2021.

Europol EC3, EBF, Poliisi, Finanssiala, Traficom Authority 2020: Huijaussivustot. Luettavissa: https://www.europol.europa.eu%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2Ffi_0.pdf&usg=AOvVaw1mAI6ukmb_az90sEJn9YeC. Luettu 19.9.2021.

EUR-Lex Euroopan unionin verkko- ja tietoturvadirektiivi 2016/1148/EU. Luettavissa: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. Luettu 3.10.2021.

EUR-Lex Euroopan unionin yleinen tietosuoja-asetus 2016/679/EU. Luettavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679. Luettu 4.10.2021.

Europol IOCTA 2017: Internet organised crime threat assesment (IOCTA), Europol, EC3 European Cybercrime Centre. Luettavissa: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017. Luettu 20.9.2021.

Europol IOCTA 2018: Internet organised crime threat assesment (IOCTA), Europol, EC3 European Cybercrime. Luettavissa: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018. Luettu 20.9.2021.

Europol IOCTA 2019: Internet organised crime threat assesment (IOCTA), Europol, EC3 European Cybercrime. Luettavissa: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019. Luettu 20.9.2021.

Europol IOCTA 2020, Internet organised crime threat assesment (IOCTA), Europol, EC3 European Cybercrime. Luettavissa: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020. Luettu 20.9.2021.

F-Secure: Mikä on troijalainen? Luettavissa: https://www.f-secure.com/fi/home/articles/what-is-a-trojan. Luettu 4.10.2021.

GB Tech: Top phishing trends to watch out for this year, julkaistu 23.7.2021. Luettavissa: https://www.gbtech.net/top-phishing-trends-to-watch-out-for-in-2021/. Luettu 9.10.2021.

Haasio, Ari 2017: Verkkorikokset. Avain, Helsinki.

Haavoittuvuudet hallintaan SBOMmin-varmasti. Liikenne- ja viestintäministeriö Traficom Kyberturvallisuuskeskus, julkaistu 09.02.2021. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-hallintaan-sbommin-varmasti. Luettu 8.10.2021.

Hiltunen, Elina 2013: Luku 20: Heikot signaalit. Kuusi, Osmo & Bergman, Timo & Salminen, Hazel 2013: Miten tutkimme tulevaisuuksia? Sastamala, Vammalan kirjapaino.

Interpol 2020, Cryptojacking, Lyon Ranska syyskuu 2020. Luettavissa: https://www.interpol.int/Crimes/Cybercrime/Cryptojacking. Luettu 4.10.2021.

Jounio, Anu 2011: Tieto- ja viestintärikokset rikoslain 38 luvussa. Lapin yliopisto. Oikeustieteiden tiedekunta. Pro gradu -työ. Luettavissa: http://urn.fi/URN:NBN:fi:ula-201110261190. Luettu 4.10.2021.

Jämsén, Christian 2019: Kyberrikollisuuden tilannekuva ja ajankohtaiset ilmiöt 2018. Luettavissa: https://intermin.fi/documents/10623/10333141/4_Christian_J%C3%A4msen_KRP_Kyberrikollisuuden+tilannekuva_JHDTTK_0810_2018.pdf/89ffa9b6-7c12-4a03-bd61-80a72962de1d/4_Christian_J%C3%A4msen_KRP_Kyberrikollisuuden+tilannekuva_JHDTTK_0810_2018.pdf. Luettu 4.10.2021.

Jämsén, Christian 2020: Tietoverkkorikollisuus poliisin silmin 2019-2020, julkaistu 10.12.2020. Luettavissa: https://poliisi.fi/blogi/-/blogs/tietoverkkorikollisuus-poliisin-silmin-2019-2020. Luettu 5.10.2021.

Kiristysohjelmien tunnistaminen – kuinka salaustroijalaiset eroavat toisistaan, Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/threats/ransomware-attacks-and-types. Luettu 04.10.2021.

Kuinka turvallisia sähköiset rahansiirrot ovat? Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/threats/how-safe-are-money-etransfers. Luettu 7.10.2021.

Kuusi, Osmo & Bergman, Timo & Salminen, Hazel 2013: Miten tutkimme tulevaisuuksia? Sastamala, Vammalan kirjapaino.

Kyberturvallisuuskeskus: Tilannekuva. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen. Luettu 4.10.2021.

Laki Liikenne- ja viestintävirastosta 935/2018.

Laki poliisihallinnosta 14.2.1992/110.

Laki sähköisen viestinnän palvelusta 917/2015.

Lehto Martti 2021: Digitaalisen kybermaailman ilmiöitä ja määrittelyjä - Kyber on kaikkialla. Jyväskylän yliopisto informaatioteknologian tiedekunta 2021, julkaistu 6.4.2021. Jyväskylä.

Liikenne- ja viestintävirasto 2020: Työryhmä selvittämään keinoja yhteiskunnan kriittisten toimialojen tietoturvan ja tietosuojan parantamiseksi, julkaistu 09.11.2020. Luettavissa: https://www.lvm.fi/-/tyoryhma-selvittamaan-keinoja-yhteiskunnan-kriittisten-toimialojen-tietoturvan-ja-tietosuojan-parantamiseksi-1241272. Luettu 19.4.2021.

Liikenne- ja viestintäministeriö 2021: Kyberturvallisuuden kehittämisohjelma, Liikenne- ja viestintäministeriön julkaisuja 2021:7. Luettavissa: https://julkaisut.valtioneuvosto.fi/handle/10024/163219. Luettu 3.10.2021.

Maanpuolustuskorkeakoulu 2019: Kyberkäsikirja Puolustusvoimien henkilöstölle. Sotataidon laitos: julkaisusarja 3, työpapereita 12. Toimittanut: Tommi Laari. Tekijät: Laari, Tommi & Flyktman, Jouni, Härmä, Katriina & Timonen, Jussi & Tuovinen, Jussi. Luettavissa: https://urn.fi/URN:ISBN:978-951-25-3120-2. Luettu 5.10.2021.

McChrystal Stanley 2015: Team of teams: New rules of engagement for a complex world. New York Protfolio, Penguin.

Microsoft 4.10.2021: Tutkimus: Puolet Suomen väestöstä joutunut teknisen tuen huijausten kohteeksi viimeisen vuoden aikana, Microsoft News center, julkaistu 4.10.2021. Luettavissa: https://news.microsoft.com/fi-fi/2021/08/04/tech-support-scam-research-2021/. Luettu 14.10.2021.

Microsoft 2021: Digital Defense Report, julkaistu lokakuu 2021. Luettavissa: https://news.microsoft.com/fi-fi/2021/10/07/digital-defence-report-2021/. Luettu 14.10.2021.

Miksi kotiverkon IoT-tietoturva on tärkeä asia? Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/threats/secure-iot-devices-on-your-home-network. Luettu 3.10.2021.

Mitä hunajapurkilla tarkoitetaan? Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/threats/what-is-a-honeypot. Luettu 4.10.2021.

Mitä robottipuhelut ovat ja kuinka lopetat ne? Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/definitions/what-are-robocalls. Luettu 7.10.2021.

Mikä rootkit on – määritelmä ja selitys? Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/definitions/what-is-rootkit. Luettu 5.10.2021.

Mitä syvä ja pimeä verkko ovat? Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/threats/deep-web. Luettu 16.10.2021.

Mustahattu-, valkohattu- ja harmaahattuhakkerien määritelmä ja selitys. Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/definitions/hacker-hat-types. Luettu 5.10.2021.

Neuvoja identiteettivarkauden tai tietovuodon uhrille. Liikenne- ja viestintäministeriö Traficom Kyberturvallisuuskeskus, julkaistu 22.10.2020. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-identiteettivarkauden-tai-tietovuodon-uhrille. Luettu 7.10.2021.

Ostaisitko huumeita alle 18-vuotiaalta? Keskusrikospoliisi kyberrikostorjuntakeskus, julkaistu 12.10.2021. Luettavissa: https://poliisi.fi/blogi/-/blogs/ostaisitko-huumeita-alle-18-vuotiaalta. Luettu 17.10.2021.

Pajunen Iina 2020: Tietojärjestelmiin kohdistuvat rikokset Suomessa. Jyväskylän yliopisto. Informaatioteknologian tiedekunta, 2020. Pro gradu -työ. Luettavissa: http://urn.fi/URN:NBN:fi:jyu-202012157145. Luettu 4.10.2021.

Peltomäki, Juha & Norppa, Kati 2015: Rikos meni verkkoon - Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen, Viro, Alma Talent.

Poliisi: *Petosrikokset*. Luettavissa: https://poliisi.fi/petosrikokset. Luettu 5.10.2021.

Poliisi: *Seksuaalirikokset*. Luettavissa: https://poliisi.fi/seksuaalirikokset. Luettu 8.10.2021.

Rauhamaa, Mikko 2021: Keskusrikospoliisi - Rikostorjunnan haasteet globaalissa verkkoympäristössä. Salo Cyber Talks 2021, kyberrikostorjuntakeskus 2020. https://salo.fi/wp-content/uploads/2021/01/SaloCyberTalks_20210126_Mikko-Rauhamaa.pdf. Luettu 9.10.2021.

Rikollisuustilanne 2019: Helsingin yliopisto, Kriminologian ja oikeuspolitiikan instituutti, Danielsson, Petri. Katsauksia 42/2020. Luettavissa: http://urn.fi/URN:ISBN:978-951-51-0675-9. Luettu 8.10.2021.

Rikoksentorjunta: Kyberrikokset. Luettavissa: https://rikoksentorjunta.fi/kyberrikokset. Luettu 5.10.2021.

Rikoslaki 39/1889.

Saaranen-Kauppinen, Anita & Puusniekka, Anna 2009: Menetelmäopetuksen tietovaranto KvaliMOTV kvalitatiivisten menetelmien verkko-oppikirja. Yhteiskuntatieteellisen tietoarkiston julkaisuja. Tampere 2009.

Salminen, Ari 2011: Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallinto-tieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja, Vaasa 2011.

Sanastokeskus TSK: TEPA-termipankki, Erikoisalojen sanastojen ja sanakirjojen kokoelma. Luettavissa: https://termipankki.fi/tepa/fi/. Luettu 3.10.2021.

Senker 2017: Cybercrime and the darknet – Revealing the hidden underworld of the internet, Cath Senker, 2017, Arcturus.

Sisäministeriö 2017: Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14/2017, Sisäinen turvallisuus. Sisäministeriö Helsinki 2017.

Sisäministeriö 2021: Kyberrikollisuus ylittää rajat tietoverkoissa. Luettavissa: https://intermin.fi/poliisiasiat/kyberrikollisuus. Luettu 28.9.2021.

Sisäministeriö: Järjestäytynyt rikollisuus vaikuttaa laajasti yhteiskuntaan. Luettavissa: https://intermin.fi/poliisiasiat/jarjestaytynyt-rikollisuus. Luettu 6.10.2021.

SOCTA 2021: EU SOCTA 2021, Europol, European Union, Serious and organised crime threat assesment. Luettavissa: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment. Luettu 6.10.2021.

SolarWinds Orion Platformin takaovi mahdollisti vakoilun ja tietomurtoja, Liikenne ja viestintävirasto Traficom Kyberturvallisuuskeskus, julkaistu 18.12.2020. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/solarwinds-orion-platformin-takaovi-mahdollisti-vakoilun-ja-tietomurtoja. Luettu 9.10.2021.

Sosiaali- ja terveysministeriön raportteja ja muistioita 2021:17: Väkivallaton lapsuus 2020–2025 – toimeenpano ja viestintä. Helsinki 2021. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163202/STM_2021_17_rap.pdf. Luettu 20.9.2021.

Suojelupoliisi 27.9.2021: Kansallisen turvallisuuden katsaus: Suomeen kohdistuu jatkuvia kybervakoiluyrityksiä, julkaistu 27.9.2021. Luettavissa: https://supo.fi/-/suomeen-kohdistuu-jatkuvia-kybervakoiluyrityksia. Luettu 14.10.2021

Suojelupoliisi (SUPO): kansallisen turvallisuuden katsaus 2021. Luettavissa: https://supo.fi/kansallisen-turvallisuuden-katsaus. Luettu 12.10.2021.

Suojelupoliisi (SUPO) vuosikirja 2020. Luettavissa: https://supo.fi/-/supon-vuosikirja-2020-terrorismin-uhka-arviossa-nakyy-aarioikeiston-muuttunut-tilannekuva. Luettu 20.9.2021.

Tapoja välttyä käyttäjän manipuloinnilta. Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/threats/how-to-avoid-social-engineering-attacks. Luettu 24.9.2021.

Tarkoma, Sasu 2017: Tekoäly ja kokonaisturvallisuus, Maanpuolustus, Maanpuolustuskurssiyhdistyksen julkaisu, julkaistu 5.12.2017. Luettavissa: https://www.maanpuolustus-lehti.fi/tekoaly-ja-kokonaisturvallisuus/. Luettu 9.10.2021.

Tekoäly ja koneoppiminen kyberturvallisuudessa – kuinka ne muokkaavat tulevaisuutta. Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/definitions/ai-cybersecurity. Luettu 14.10.2021.

Tietosuojalaki 1050/2018.

Tietoturvan vuosi 2018, Liikenne- ja viestintävirasto, Traficom, Kyberturvallisuuskeskus, kyberturvallisuuden vuosikatsaus.

Tietoturvan vuosi 2019, Liikenne- ja viestintävirasto, Traficom, Kyberturvallisuuskeskus, kyberturvallisuuden vuosikatsaus, Traficomin julkaisuja 5/2020.

Tietoturvan vuosi 2020, Liikenne- ja viestintävirasto, Traficom, Kyberturvallisuuskeskus, kyberturvallisuuden vuosikatsaus, Traficomin julkaisuja 13/2021.

Tietoverkkorikollisuus poliisin silmin 2020–2021, Lehtinen Viivi, Keskusrikospoliisi kyberrikostorjuntakeskus, julkaistu 5.10.2021. Luettavissa: https://poliisi.fi/blogi/-/blogs/tietoverkkorikollisuus-poliisin-silmin-2020-2021 Luettu 17.10.2021.

Tilastokeskus 2021: Suomen virallinen tilasto (SVT): Rikos- ja pakkokeinotilasto (verkkojulkaisu). Helsinki: Tilastokeskus. Luettavissa: http://www.stat.fi/til/rpk/2021/02/. Luettu 8.10.2021.

Toimitusketjut uhka yritysten kyberturvalle, BDO Suomi, blogi, julkaistu 27.10.2020. Luettavissa: https://www.bdo.fi/fi-fi/nakemyksia/blogit/asiantuntijat/toimitusketjut-uhka-yritysten-kyberturvalle. Luettu 8.10.2021.

Traficom 2/2020: Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus: Kyberturvallisuus ja yrityksen hallituksen vastuu. Traficomin julkaisuja 2/2020. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf. Luettu 12.10.2021.

Traficom 5/2021: Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus: Suojaamattomia automaatiojärjestelmiä suomalaisessa verkossa, Traficomin julkaisuja 5/2021. Luettavissa:

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Automaatiolaitekartoitus_2020.pdf. Luettu 8.10.2021.

Traficom elokuu 2021: Liikenne- ja viestintäministeriö Traficom Kyberturvallisuuskeskus: Elokuun kybersää oli vaihteleva – Flubotin väistyminen toi aurinkoa epävakaiseen säähän, Kybersää elokuu 2021, julkaistu 16.9.2021. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa_elokuu_2021. Luettu 9.10.2021.

Traficom kesäkuu 2020: Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus: Kybersää kesäkuu 2020. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%20kes%C3%A4kuu%202020.pdf. Luettu 23.9.2021.

Traficom kesäkuu 2018: Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus: Kybersää kesäkuu 2018. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybersaa_2018_06.pdf. Luettu 23.9.2021.

Traficom 228/2020: Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus: Pienyritysten kyberturvallisuusopas, Traficomin julkaisuja 228/2020. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf. Luettu 23.9.2021.

Turun yliopisto: Mitä on tulevaisuuden tutkimus? Anita Rubin: Tulevaisuudentutkimus tiedonalana ja tieteellisenä toimintana. Luettavissa: https://www.utu.fi/fi/yliopisto/turun-kauppakorkeakoulu/tulevaisuuden-tutkimuskeskus/mita-on-tutu. Luettu 25.10.2021.

Turvallisuuskomitea 2013: Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. Luettavissa: https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/. Luettu 22.10.2021.

Turvallisuuskomitea 2017: Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020. Luettavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf. Luettu 12.10.2021.

Turvallisuuskomitea: Kodin kyberopas 2017: Kodin kyberopas, ohjeita digitaaliseen arkeen, Laitinen, Jaana. Luettavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2017/04/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf. Luettu 7.10.2021.

Turvallisuuskomitea 2018: Kyberturvallisuuden sanasto, sanastokeskus TSK 5, Helsinki 2018. Luettavissa: https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/. Luettu 12.10.2021.

Turvallisuuskomitea 2019: Suomen kyberturvallisuusstrategia 2019, Valtioneuvoston periaatepäätös 3.10.2019. Luettavissa: https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/. Luettu 12.10.2021.

Valtioneuvosto 30.9.2021: Kyberturvallisuuskeskuksesta Suomen kansallinen kyberturvallisuuden koordinointikeskus, julkaistu 30.9.2021. Luettavissa: https://valtioneuvosto.fi/-/national-cyber-security-centre-to-be-designated-as-finland-s-national-coordination-centre-for-cyber-security-matters. Luettu 12.10.2021.

Valtioneuvoston selvitys- ja tutkimustoiminta 2016: Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2016 - Tietoverkkorikollisuuden tilannekuva. Leppänen, Anna & Linderborg, Karl & Saarimäki, Jarkko, huhtikuu 2016. Luettavissa: https://vnk.fi/julkaisut/julkaisu?pubid=URN:ISBN:978-952-287-251-7. Luettu 28.9.2020.

Valtioneuvoston selvitys- ja tutkimustoiminta (VNST) 2017: Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Martti Lehto ja Jarno Limnéll, julkaistu helmikuu 2017. Luettavissa: https://julkaisut.valtioneuvosto.fi/handle/10024/160233. Luettu 28.9.2021.

Valtioneuvoston selvitys- ja tutkimustoiminta (VNST) 2018: Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018, Kyberturvallisuuden strateginen johtaminen Suomessa. Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen ja Mirva Salminen, maaliskuu 2018. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf?sequence=1&isAllowed=y. Luettu 4.10.2021.

Valtioneuvoston puolustusselonteko 2021: Valtioneuvoston julkaisuja 2021:78. Valtioneuvosto Helsinki 2021. Luettavissa: https://julkaisut.valtioneuvosto.fi/handle/10024/163405. Luettu 12.10.2021.

Viestintävirasto 2016: Selviytymisopas kiristyshaittaohjelmia vastaan, Kokemuksia kiristyshaittaohjelmista Suomessa ja neuvoja niistä selviytymiseen, Viestintäviraston julkaisu 005/2016. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf. Luettu 4.10.2021.

Viestintävirasto 2017: Näin meitä huijataan! Verkossa yleisesti tavattuja huijausmenetelmiä, kyberturvallisuuskeskus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Nain_meita_huijataan.pdf. Luettu 23.9.2021.

Viestintäviraston ohje 2016: Ohje 3/2016 Palvelunestohyökkäysten ehkäisy ja torjunta, Kyberturvallisuuskeskus. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Ohje_3_2016_Palvelunestohyokkaysten_ehkaisy_ja_torjunta_0.pdf. Luettu 5.10.2021.

Viestintäviraston julkaisu 005/2016: Selviytymisopas kiristyshaittaohjelmia vastaan, kokemuksia kiristyshaittaohjelmista Suomessa ja neuvoja niistä selviytymiseen. Luettavissa: https://www.kyber-turvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teema-kooste_07_2016.pdf. Luettu 20.9.2021.

Vuoden 2020 tunnetuimmat kiristysohjelmahyökkäykset. Kaspersky. Luettavissa: https://www.kaspersky.fi/resource-center/threats/top-ransomware-2020. Luettu 4.10.2021.

Walsh, Nick 2021: Serious cyberattacks in Europe doubled in the past year, new figures reveal, as criminals exploited the pandemic, Nick Paton Walsh, julkaistu 10.6.2021. Luettavissa: https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html. Luettu 9.10.2021.