

Sini Keto

DIGIHUIJAUSTEN VAIKUTUS PANKKIEN RISKIENHALLINTAAN

Johtamisen ja talouden tiedekunta
Pro gradu -tutkielma
Toukokuu 2025

TIIVISTELMÄ

Sini Keto: Digihuijausten vaikutus pankkien riskienhallintaan

Ohjaaja: Timo Rintamäki

Pro gradu -tutkielma

Tampereen yliopisto

Kauppätieteiden tutkinto-ohjelma, Vakuutustiede

Toukokuu 2025

Digitalisaatio on muuttanut merkittävästi rahoitusala, mutta samalla lisännyt kyberrikollisuuden riskejä. Digitaalisilla huijauksilla on pankkien asiakkaisiin sekä taloudellisia että psykologisia vaikutuksia, ja ne voivat aiheuttaa myös pankeille mainehaittaa ja taloudellisia menetyksiä. Vuonna 2023 pankit estivät Suomessa yli 32 miljoonan euron arvosta huijausmaksuja, mutta digihuijausten määrä jatkaa kasvuaan.

Tutkielmassa tarkastellaan digihuijausten vaikutuksia suomalaisten pankkien riskienhallintaan. Sen tavoitteena on selvittää, millainen ilmiö ovat pankkien asiakkaisiin kohdistuvat digihuijaukset ja millaisia riskejä nämä huijaukset aiheuttavat sekä pankeille itselleen että niiden asiakkaille. Lisäksi tutkitaan, miten digihuijaukset vaikuttavat pankkien riskienhallintaan ja millaisia mahdollisuuksia kehittyvä teknologia tuo digihuijauksista aiheutuvien riskien hallintaan. Tutkielman teoriaosuus jakautuu kahteen pääosaan: ensimmäinen käsittelee digihuijauksia osana kyberrikollisuutta, ja toinen syventyy pankkien riskienhallintaprosessiin, erityisesti digihuijauksiin liittyvän riskienhallinnan näkökulmasta.

Tutkimus on suoritettu kvalitatiivisin menetelmin, ja sen empiirinen aineisto on kerätty puolistrukturoiduilla teemahaastatteluilta haastatteleamalla kolmea pankin asiantuntijaa ja yhtä toimialajärjestön edustajaa. Haastatteluiden avulla kerätty aineisto on analysoitu teoriaohjaavan sisällönanalyysin avulla.

Tutkimuksen tulokset osoittavat, että yleisimpiä huijausmuotoja ovat sijoitus-, rakkaus-, valepoliisi- ja dokumenttihuijaukset sekä tietojen kalastelu. Digihuijaukset ovat monimuotoinen ja jatkuvasti kehittyvä ilmiö, jossa hyödynnetään sosiaalisen manipuloinnin keinoja sekä kehittyvää teknologiaa. Digihuijausten torjumiseksi pankkien on ylläpidettävä dynaamista riskienhallintaprosessia ja kehitettävä kontrollejaan. Asiakkaan tuntemiseen liittyvät toimet, tietoisuuden lisääminen ilmiöstä, maksujen monitorointi ja kehittyvän teknologian hyödyntäminen ovat avainasemassa digihuijausten ennaltaehkäisyssä ja havaitsemisessa. Pankkien riskienhallintatoimien vaikutukset ovat kuitenkin rajallisia, sillä myös asiakkaan toiminta on merkittävässä roolissa, etenkin huijausten ennaltaehkäisyssä.

Avainsanat: Digihuijaukset, kyberrikollisuus, kyberriski, operatiivinen riski, sosiaalinen manipulointi, tekoäly

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

Tekoälyn käyttö tutkielmassa

Opinnäytteessäni on käytetty tekoälysovelluksia:

Ei

Kyllä

Opinnäytteessäni käytetyt tekoälytyökalut ja niiden käyttötarkoitukset on kuvailtu alla:

Tekoälytyökalun nimi (ja versio): ChatGPT (GPT-4)

Käyttötarkoitus ja osiot, joissa tekoälyä käytettiin: Tekoälyä hyödynnettiin tutkimus- ja kirjoitusprosessin aikana työkaluna tekstin johdonmukaisuuden ja selkeyden parantamiseksi kaikissa tutkielman osissa. Mitään ajatuksia tai tekstiä ei kopioitu suoraan tekoälyn tuottamasta sisällöstä, vaan kaikki ideat analysoitiin itse. Tekoälyä käytettiin myös apuna englanninkielisten artikkeleiden kääntämisessä johdannossa ja teorialuvuissa (luvut 1–3), mutta suomennokset tarkistettiin ja lopullinen teksti muotoiltiin itse.

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien tekoälyllä tuotetut osat, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

SISÄLLYSLUETTELO

1 JOHDANTO	1
1.1 Aihealueen esittely ja merkitys	1
1.2 Aikaisemmat tutkimukset ja keskeiset käsitteet.....	3
1.3 Tutkimuskysymykset ja -tavoitteet sekä keskeiset rajaukset	5
1.4 Tieteenfilosofiset lähtökohdat	7
1.5 Tutkimusmenetelmät ja -aineisto	8
1.6 Tutkimuksen rakenne	10
1.7 Teoreettinen viitekehys	10
2 DIGIHUIJAUKSET KYBERRIKOLLISUUDEN ILMIÖNÄ.....	12
2.1 Kyberrikollisuus.....	12
2.2 Digihuijausten määrittely	13
2.3 Digihuijaukset osana rikollisuutta.....	15
2.4 Digihuijausten eri muodot.....	18
2.4.1 Digihuijaukset pankkisektorilla	19
2.4.2 Sosiaalinen manipulointi.....	20
2.4.3 Sijoitushuijaus	20
2.4.4 Valepoliisihuijaus.....	21
2.4.5 Tietojenkalastelu ja sen eri muodot.....	21
2.4.6 Dokumenttihuijaus	22
2.4.7 Rakkaushuijaus	22
2.4.8 Verkkokauppa- ja kaupankäyntialustahuijaukset.....	23
2.5 Digihuijaukset ilmiönä.....	23
3 PANKKIEN RISKIENHALLINTA DIGIHUIJAUSTAPAUKSISSA	25
3.1 Pankkeihin kohdistuva regulaatio digihuijaustapauksissa	25
3.2 Riskienhallintaprosessi ja standardeja.....	28
3.3 Kokonaisvaltainen riskienhallinta ERM	31
3.4 Pankkien operatiivisten riskien hallinta	33
3.5 Kyberriski operatiivisena riskinä	39
3.6 Pankkien kyberturvallisuus	40
3.7 Pankkien riskienhallinta digihuijaustapauksissa	43
4 ASiantuntijahaastattelut.....	51
4.1 Tutkimusaineiston kuvaus ja käsittely	51
4.2 Pankkien asiakkaisiin kohdistuvat digihuijaukset.....	52

4.2.1 Tyypillisimmät pankkien asiakkaisiin kohdistuvat digihuijaukset	52
4.2.2 Trendit pankkien asiakkaisiin kohdistuvissa digihuijauksissa	57
4.3 Pankkien asiakkaisiin kohdistuvien digihuijausten riskit	59
4.3.1 Digihuijausten aiheuttamat riskit pankeille.....	59
4.3.2 Digihuijauksien aiheuttamat riskit pankkien asiakkaille.....	61
4.4 Pankkien digihuijauksiin liittyvät riskienhallintakäytännöt.....	62
4.4.1 Pankkien riskienhallintakeinot digihuijaustapauksissa	62
4.4.2 Digihuijauksiin liittyvät kontrollit ja turvatoimet	64
4.4.3 Asiakaskokemuksen säilyttäminen digihuijaustapauksissa	67
4.4.4 Käytännön haasteet digihuijauksista aiheutuvien riskien hallinnassa.....	68
4.4.5 Riskienhallintakäytäntöjen kehittäminen ja teknologian hyödyntäminen	71
5 YHTEENVETO JA JOHTOPÄÄTÖKSET	74
5.1 Tutkimuskysymyksiin vastaaminen ja johtopäätökset.....	74
5.2 Tutkielman arviointi.....	81
5.3 Lopuksi.....	83
LÄHDELUETTELO	85
Kirjallisuuslähteet	85
Muut painetut lähteet.....	86
Internet-lähteet	86
LIITTEET	91
Liite 1: teemahaastattelun kysymysrunko	91

1 JOHDANTO

1.1 Aihealueen esittely ja merkitys

Rahoituksen digitalisoituminen on hyödyttänyt taloutta ja rahoitusvakautta. Tehokkuus keskeisten pankkipalveluiden tarjoamisessa sekä rahoituksellinen osallisuus ovat parantuneet, jakelukanavat ovat laajentuneet, käyttöliittymät ovat kehittyneet, transaktioiden läpinäkyvyys on parantunut ja kriiseihin reagoidaan nopeammin. Samalla teknologian kehitys on kuitenkin lisännyt myös pankkisektorin riskejä. Esimerkiksi digitaalisten huijausten määrä on kasvanut merkittävästi viime vuosina, sillä rikolliset hyödyntävät digitalisaatiota tehdäkseen verkkohuijauksia suuremmassa mittakaavassa ja laajuudessa kuin aiemmin. (BCBS, 2023.) Vuonna 2023 suomalaisilta pyrittiin huijaamaan yhteensä 76,9 miljoonaa euroa, kasvun ollessa edellisvuodesta 65 prosenttia (Palmgren, 2024a). Huijarit hyödyntävät ajankohtaisia sosiaalipoliittisia trendejä ja kansainvälisiä kriisejä. Europol on arvioinut raportissaan COVID-19-pandemian myötä kiihtyneen digitalisoitumisen ja erilaisiin online-palveluihin siirtymisen johtaneen yleisesti petosrikollisuuden voimakkaaseen kasvuun. Toinen ajankohtainen huijareiden hyödyntämä tilanne on Venäjän hyökkäyssota Ukrainaan, mitä huijarit ovat käyttäneet esittäytymällä Ukrainan tukijoina esimerkiksi perustamalla valeverkkosivustoja ja lähettämällä väärennettyjä sähköposteja. (Europol, 2023.)

Rahanpesulain mukaan pankit ovat selonottovelvollisia, eli havaitessaan tavanomaisesta poikkeavan tai epäilyttävän liiketoimen, tulee niiden selvittää sen tarkoitus (Rahanpesulaki 3:4 §). Vuonna 2023 pankit onnistuivat estämään huijausmaksuja ja palauttamaan asiakkaidensa varoja yhteensä 32,7 miljoonaa euroa, mikä merkitsi 132 prosentin kasvua edellisvuoteen verrattuna. (Palmgren, 2024a.) Pankkien merkitys asiakkaidensa varojen turvaamisessa on siten erittäin suuri. Verkkopankkihuijauksissa pankki saattaa joutua vastaamaan asiakkaan menetyksistä, mikäli asiakkaan ei katsota toimineen tahallisesti tai törkeän huolimattomasti (Riku, 2022). Täten pankkien asiakkaisiin kohdistuviin digihuijauksiin liittyvien riskienhallintakeinojen kehittäminen ennaltaehkäisee myös pankeille itselleen aiheutuvia taloudellisia tappioita.

Pankeilla on Rahanpesulakiin perustuva velvollisuus tehdä ilmoitus epäilyttävästä liiketoimesta rahanpesun selvittelykeskukselle (Rahanpesulaki 4:1.1 §).

Valtiovarainministeriön (2023) Kansallisen rahanpesun ja terrorismin rahoittamisen riskiarvion osittaispäivityksen mukaan vuoden 2023 ensimmäisellä puoliskolla rahanpesun selvittelykeskus teki eniten tietojen luovutuksia liittyen petosrikoksiin. Tyypillisiä petosmuotoja ovat rakkaus-, sijoitus- ja verkkopankkihuijaukset, jotka lukeutuvat myös rahanpesun esirikoksiksi eli taloudellista hyötyä tuottaviksi rikoksiksi. Rahanpesun estämisen näkökulmasta esirikosten tunnistaminen ja ennaltaehkäiseminen on tärkeässä roolissa.

Uusia huijausmuotoja syntyy jatkuvasti lisää teknologian kehittyessä. Yleisin niistä on tietojen, esimerkiksi verkkopankkitunnusten kalastelu (Finanssivalvonta, 2024). Tietojen kalastelua eli phishingiä toteutetaan luotettavien tahojen, kuten viranomaisten ja pankkien nimissä. Tällöin huijarit tavoittelevat taloudellista hyötyä pyytämällä tilitietoja, tunnuksia ja muita salassa pidettäviä tietoja esimerkiksi sähköpostilla tai puhelimesta (Poliisi.fi, 2024).

Pankkien asiakkaille suurimmat rahalliset tappiot vuonna 2023 aiheutuivat sijoitushuijauksista, joiden kasvu edellisvuodesta oli jopa 91 prosenttia. Tällaiset huijaukset saattavat jatkua vuosia ja aiheuttaa näin ollen pitkäaikaisen taloudellisen ahdingon huijauksen kohteelle. (Palmgren, 2024a.) Europolin (2023) mukaan suurin osa EU-alueella tapahtuvista sijoitushuijauksista liittyy kryptovaluuttoihin. Valtionvarainministeriön (2023) Kansallisen rahanpesun ja terrorismin rahoittamisen riskiarvion osittaispäivityksen mukaan virtuaalivaluuttoihin liittyy merkittävä rahanpesun riski muun muassa niiden tarjoaman anonymiteetin myötä, minkä seurauksena digihuijausten ennaltaehkäisyn tärkeys kuluttajien suojelemiseksi ja rikollisen toiminnan estämiseksi korostuu entisestään.

Taloudellisten tappioiden lisäksi huijauksilla on ei-taloudellisia, kansantaloudellisia ja yhteiskunnallisia vaikutuksia. Huijauksen kohteeksi joutunut henkilö voi kokea taloudellisten menetysten lisäksi muun muassa fyysisen ja psyykkisen terveyden ongelmia, psykologisia ongelmia kuten stressiä, vihaa sekä ihmissuhteiden ja itsetunnon huonontumista (Button, Lewis & Tapley, 2014). Huijauksilla on myös laajempia vaikutuksia yksilöllisten seurausten kertautuessa. Huijauksilla on kansantaloudellisia vaikutuksia, sillä ne lisäävät transaktiokustannuksia huijauksille alttiissa liiketoiminnassa, minkä lisäksi ne kuluttavat viranomaisten resursseja. Lisäksi huijaukset

saattavat lisätä kuluttajien riskinkaihtajuutta. (Tuorila, 2018.) Euroopan komission teettämän kyselytutkimuksen mukaan 62 prosenttia kuluttajista, jotka eivät olleet tehneet ostoksia kansainvälisessä verkkokaupassa, katsoi huijatuksi tulemisen pelon olevan este ostosten tekemiselle (European Commission, 2011). Tämän lisäksi verkkopetokset ja -huijaukset hallitsevat kyberrikollisuuden toimialaa. Jos niitä ei hillitä, ne tulevat kehittymään yhä monimutkaisemmiksi ja muodostavat suuremman uhan, kun yhä useammat järjestäytyneet rikollisryhmät osallistuvat tähän laittomaan toimintaan ja hyödyntävät uusia teknologioita, kuten generatiivista tekoälyä. (FATF, 2023.)

1.2 Aikaisemmat tutkimukset ja keskeiset käsitteet

Tutkielma keskittyy suomalaisten pankkien asiakkaisiin kohtaamiin digihuijausten aiheuttamiin riskeihin sekä pankkien riskienhallintakeinojen ja -strategioiden tutkimiseen digihuijaustapauksissa. Digihuijaukset ovat melko tuore ja vasta kehittyvässä oleva ilmiö, jota tämän tutkielman on tarkoitus kartoittaa Suomen pankkisektorin näkökulmasta. Vastaavaa tutkimusta ei ole tehty Suomessa, mutta kansainvälisesti vastaavia etenkin petostentorjunnan teknologiaratkaisuihin keskittyviä tutkimuksia löytyy useita.

Kanu (2023) on tutkinut pro gradu -tutkielmassaan ”Pankkien asiakkaisiin kohdistuvat verkkohuijaukset: Pankin ja asiakkaan välinen vastuunjako sekä riskienhallintakeinot” pankkien asiakkaisiin kohdistuvien huijauksien tyyppejä, vastuunjakoa huijaustapauksissa pankin ja asiakkaan välillä sekä pankkien riskienhallintakeinoja asiakkaisiin kohdistuvissa huijauksissa. Tutkielmassa on yleisluontoisesti käsitelty pankkien riskienhallintakeinoja huijaustapauksissa, mutta ei niiden kehitystä. Lainopillinen näkökulma on myös Piiran (2022) pro gradu -tutkielmassa ”Verkkoavusteisen petoksen sääntely ja torjunta talousrikosoikeudellisesta näkökulmasta”, jossa on selvitetty verkkoavusteisten talousrikosten sääntelyn haasteita erityisesti petosrikosten näkökulmasta.

Kansainvälisesti muun muassa Hoffmann ja Birnbrich (2012) ovat käsitelleet tutkielmassaan petosten ennaltaehkäisyn vaikutusta pankin ja asiakkaan väliseen suhteeseen. Domenig, Rossi, Vanini & Zvizdic (2023) käsitelivät tutkielmassaan koneoppimismallien hyödyntämistä digihuijausten aiheuttamien riskien hallinnassa.

Vastaavia koneoppimisen tuomiin mahdollisuuksiin keskittyviä tutkielmia on julkaistu useita. Cao, Chen, Li, Ou & Wei (2013) ovat tutkineet kehittyneiden algoritmien ja datan louhintatekniikoiden vaikutusta petosten havaitsemisessa ja väärin hälytysten määrän vähentämisessä sähköisissä transaktioissa.

Tutkielmassa tarkastellaan useita keskeisiä käsitteitä, jotka liittyvät digihuijauksiin ja pankkien riskienhallintaan. Nämä käsitteet muodostavat perustan ilmiön ymmärtämiselle ja lisäävät tutkielman selkeyttä. Keskeisiin käsitteisiin sisältyvät digihuijaus, sosiaalinen manipulointi, kyberriski, kyberrikollisuus, operatiivinen riski ja riskienhallinta.

Digihuijaus (engl. digital fraud) on laaja-alainen ja kehittyvä ilmiö, jolle ei ole olemassa yhtä vakiintunutta määritelmää. The Association of Certified Fraud Examiners (2024) määrittelee kiteytettynä huijauksen harhaanjohtamiseksi hyötymistarkoituksessa. Digihuijaus voi täyttää useiden eri rikosnimikkeiden tunnusmerkit (Tuorila, 2018) ja niitä esiintyy useissa muodoissa, kuten sijoitushuijauksina, valepoliisihuijauksina, tietojenkalasteluna ja dokumenttihuijauksina. Laajempänä terminä *kyberrikollisuus* kattaa kaikki rikokset, joissa tietotekniikkaa tai -verkkoja käytetään rikollisiin tarkoituksiin. Kyberrikollisuus on kansainvälistä, anonyymia ja jatkuvasti kehittyvää toimintaa, ja sen muotoja ovat muun muassa petokset, kiristysrikokset ja rahanpesu. (Sisäministeriö, 2024.)

Sosiaalinen manipulointi tarkoittaa ihmisten psykologisten heikkouksien hyväksikäyttöä rikollisessa tarkoituksessa, kuten huijauksissa, joissa uhri saadaan paljastamaan arkaluontoisia tietoja tai suorittamaan maksutapahtumia huijarille (F-Secure, 2024a; Euroopan parlamentti, 2022). Kyseessä on suunniteltu rikollinen teko, jossa hyödynnetään ihmisten psykologisia heikkouksia, kuten hyväuskoisuutta, kiireen tunnetta tai pelkoa (F-Secure, 2024a).

Kyberriski määritellään kyberhyökkäysten todennäköisyyden ja vaikutuksen yhdistelmäksi. Kyberriski kohdistuu tieto- ja teknologiavaroihin ja voi vaikuttaa järjestelmien luottamuksellisuuteen, saatavuuteen ja eheyteen (FSB, 2023; Cebula & Young, 2010). Kyberriskit luokitellaan operatiivisiksi riskeiksi, koska ne aiheuttavat tappioita puutteellisten järjestelmien tai ulkoisten tapahtumien seurauksena (Cebula &

Young, 2010). *Operatiivinen riski* tarkoittaa tappioita, jotka johtuvat puutteellisista sisäisistä prosesseista, ihmisistä tai järjestelmistä, tai ulkoisista tapahtumista (Hull, 2018).

Tekoäly voidaan määritellä konepohjaiseksi järjestelmäksi, joka voi ihmisen määrittelemänä tehdä ennusteita, suosituksia tai päätöksiä, jotka vaikuttavat todellisiin tai virtuaalisiin ympäristöihin vaihtelevilla autonomian tasoilla (OECD, 2019).

Riskienhallinta on organisoitu prosessi, jonka tavoitteena on tunnistaa, arvioida ja hallita riskejä systemaattisesti. Riskienhallintaa voidaan toteuttaa useiden standardien pohjalta, kuten ISO 31000 tai COSO ERM -viitekehyksellä. Riskienhallintaan kuuluu muun muassa riskin tunnistaminen, arviointi, kontrollointi, seuranta ja raportointi. (Hopkin, 2018; Moeller, 2011.)

1.3 Tutkimuskysymykset ja -tavoitteet sekä keskeiset rajaukset

Tämän tutkielman tavoitteena on muodostaa käsitys siitä, millaisia riskejä pankkien asiakkaisiin kohdistuvat digihuijaukset aiheuttavat sekä pankeille itselleen että niiden asiakkaille. Tämän lisäksi tarkoituksena on selvittää, miten digihuijaukset vaikuttavat pankkien riskienhallintaan ja mitä riskienhallinnallisia toimenpiteitä pankit voivat toteuttaa niihin itseensä sekä asiakkaisiin kohdistuvien riskien minimoimiseksi. Tutkimus toteutetaan pankkien näkökulmasta ja tarkoituksena on tutkia niiden suorittamia toimenpiteitä asiakkaiden varojen turvaamiseksi, sillä pankeilla on korostuneen tärkeä rooli petosrikosten torjunnassa, etenkin kun huomioidaan niiden torjumien huijausmaksujen kokonaismäärä ja merkitys.

Tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- 1. Millainen ilmiö on pankkien asiakkaisiin kohdistuvat digihuijaukset?*
- 2. Millaisia pankeihin ja niiden asiakkaisiin kohdistuvia riskejä digihuijaukset aiheuttavat?*
- 3. Miten pankit ovat sopeuttaneet riskienhallintakäytäntöjään digihuijausten lisääntymisen myötä?*

3.1. Mitä mahdollisuuksia kehittyvä teknologia tuo digihuijauksista aiheutuvien riskien hallintaan?

Ensimmäisen tutkimuskysymyksen avulla pyritään määrittelemään, millainen ilmiö digihuijaus on pankkien näkökulmasta. Tarkoituksena on selvittää, millaisia erityispiirteitä pankkien asiakkaisiin kohdistuvissa digihuijauksissa on, ja millaisia toimintamalleja huijareilla on kyseisissä tapauksissa. Lisäksi selvitetään, miten digihuijaukset ovat kehittyneet ja millaisia ovat niihin liittyvät viimeaikaiset trendit.

Toisen tutkimuskysymyksen avulla on tarkoitus selvittää, millaisia pankkeihin ja niiden toimintaan kohdistuvia digihuijauksiin liitännäisiä riskejä pankit ovat havainneet. Tarkoituksena on huomioida etenkin pankkien asiakkaisiin kohdistuvien digihuijausten vaikutukset pankkien riskiasemaan. Toisaalta on tarkoitus myös selvittää, miten digihuijaukset vaikuttavat pankkien asiakkaisiin ja heidän asemaansa. Tämän lisäksi tutkitaan mahdollisia syitä tunnistetuille riskeille sekä seurauksia riskien realisoituessa.

Kolmannen tutkimuskysymyksen tavoitteena on tutkia, miten digihuijaukset ovat vaikuttaneet pankkien riskienhallintakäytäntöihin ja kontroleihin, etenkin huijausten lisääntyttyä. Lisäksi selvitetään digihuijauksiin liittyvän riskienhallinnan haasteita ja sen mahdollisia kehityskohtia. Alakysymyksen avulla on tarkoitus selvittää uuden teknologian, kuten tekoälyn, tuomia mahdollisuuksia liittyen digihuijausten aiheuttamien riskien hallintaan ja näiden ratkaisujen käyttöastetta.

Digihuijaukset ovat maailmanlaajuinen ilmiö, mutta tutkielman kohteeksi on rajattu suomalaiset pankit, jotta voidaan kartoittaa Suomen lainsäädännön piirissä olevien pankkien toimintaa digihuijaustapauksissa. Tutkielman kohteeksi on rajattu vain henkilöasiakkaisiin kohdistuvat huijaustapaukset, eikä tarkoitus ole tutkia yritys-, yhdistys- tai järjestöasiakkaita, sillä niihin kohdistuvissa huijauksissa on omat erityispiirteet ja käytännöt. Näin ollen tutkimuksen kohteena ei myöskään ole pankkien henkilökuntaan kohdistuvat huijaukset, sillä niiden keinot ja tavoitteet eroavat kuluttajiin kohdistuvista huijauksista. Tutkimuksen kohteena ei ole huijarit, joten tutkielmassa ei tarkemmin eritellä toteutetaanko huijaukset yksittäisen henkilön vai yrityksen toimesta.

1.4 Tieteenfilosofiset lähtökohdat

Termi tutkimusfilosofia viittaa uskomusten ja oletusten kokonaisuuteen, joka ohjaa tiedon hankintaa ja kehittymistä tieteellisessä tutkimuksessa. Se rakentuu useista eri oletusalueista, kuten ontologisista, epistemologisista ja aksiologisista oletuksista. Nämä oletukset määrittelevät, kuinka tutkija suhtautuu tutkimuksensa kohteeseen, mitä hän pitää tiedon lähteenä ja kuinka hänen omat arvonsa vaikuttavat tutkimusprosessiin. (Saunders, Lewis & Thornhill, 2019.) Tämä tutkielma, joka käsittelee digihuijausten vaikutusta pankkien riskienhallintaan, hyödyntää pragmatismia tutkimusfilosofiana, koska se korostaa käytännön merkitystä tiedon hankinnassa ja ongelmanratkaisussa.

Ontologiset oletukset liittyvät siihen, miten tutkija hahmottaa tutkimuksen kohteena olevan todellisuuden. Pragmatismien näkökulmasta todellisuus on monimutkainen ja jatkuvassa muutoksessa oleva kokonaisuus, joka syntyy erilaisten prosessien, kokemusten ja käytäntöjen vuorovaikutuksessa. (Saunders ym., 2019.) Tässä tutkielmassa tämä näkökulma ilmenee pankkien riskienhallintaprosessissa ja digihuijausten vaikutuksessa siihen. Toisaalta myös digihuijaukset ovat jatkuvasti muuttuva ja käytännönläheinen ilmiö. Pragmatismien mukaan tutkimus ei pyri esittämään muuttumattomia ja yleispäteviä totuuksia, vaan keskittyy siihen, kuinka käytännön toiminta ja ongelmanratkaisu voivat parantaa organisaatioiden kykyä hallita riskejä. (Saunders ym., 2019.) Tämän tutkielman kontekstissa tämä tarkoittaa pankkien riskienhallinnan tarkastelua digihuijausten näkökulmasta, painottaen käytännönläheisten toimintatapojen ja strategioiden kehittämistä pankkien valmiuksien parantamiseksi digitaalisten petosten tunnistamisessa, ehkäisyssä ja hallinnassa nopeasti muuttuvassa toimintaympäristössä.

Epistemologiset oletukset puolestaan käsittelevät tiedon luonteen ja lähteiden kysymyksiä. Pragmatismien mukaan tiedon merkitys on sidoksissa sen kykyyn tuottaa käytännön ratkaisuja ja edistää toimintaa. Tutkija siis arvioi tietoa sen sovellettavuuden ja hyödyllisyyden perusteella tietyssä kontekstissa. (Saunders ym., 2019.) Tämä näkökulma on erityisen relevantti tässä tutkielmassa, jossa tutkimuskysymyksenä on digihuijausten vaikutus pankkien riskienhallintaan. Tutkija pyrkii löytämään käytännönläheisiä ja tehokkaita tapoja käsitellä näitä vaikutuksia.

Aksiologiset oletukset liittyvät tutkijan omiin arvoihin ja niiden vaikutukseen tutkimusprosessiin. Pragmatismi tunnustaa, että tutkija on aina osittain subjektiivinen ja arvot ohjaavat hänen tutkimusvalintojaan ja -prosessejaan. Pragmatismi korostaa tutkijan reflektioivaa asennetta, jossa tutkija tiedostaa omat arvonsa ja asenteensa ja pyrkii jatkuvaan itsereflektioon tutkimuksen aikana. Tämä on tärkeää, sillä tutkimuksen objektiivisuus voi vaarantua, jos tutkija ei ole tietoinen siitä, kuinka hänen omat uskomuksensa ja arvot voivat vaikuttaa tutkimustuloksiin. (Saunders ym., 2019.) Tässä tutkielmassa pyritään jatkuvaan itsereflektioon, jotta tutkimuksen lopulliset tulokset eivät vääristy tutkijan omien kokemusten ja asenteiden vaikutuksesta. Tämä on merkityksellistä etenkin, sillä tutkijalla on aikaisempaa kokemusta aiheen parissa työskentelystä. Reflektiivinen asenne mahdollistaa myös sen, että tutkija voi oikeudenmukaisesti käsitellä tutkimuksen kohteena olevia ilmiöitä ja varmistaa, ettei tutkimus ole liian yksipuolinen.

1.5 Tutkimusmenetelmät ja -aineisto

Tutkielma toteutetaan laadullisena eli kvalitatiivisena tutkimuksena. Laadullisessa tutkimuksessa tarkastellaan tyypillisesti osallistujien näkemyksiä ja niiden välisiä suhteita hyödyntäen erilaisia aineistonkeruu- ja analyysimenetelmiä teoreettisen viitekehyksen ja kontribuution tuottamiseen (Saunders ym., 2019). Tutkielman empiirinen aineisto kerätään puolistrukturoiduilla teemahaastatteluilla, joka mahdollistaa keskeisiin teemoihin keskittymisen, mutta antaa haastateltaville mahdollisuuden nostaa esiin haluamiaan asioita (Hirsjärvi & Hurme, 2008). Pragmatismi tutkimusfilosofiana tukee osaltaan puolistrukturoidun teemahaastattelun käyttöä, sillä kyseinen aineistonkeruutapa mahdollistaa keskittymisen käytännön merkitykseen. Haastatteluiden kohteiksi valikoitui asiantuntijoita, joilla on työtehtävänsä puitteissa riittävän laaja näkyvyys digihuijauksiin ilmiönä sekä niistä aiheutuvien riskien hallintaan. Asiantuntijahaastattelut valikoituivat aineistonkeruumenetelmäksi sen vuoksi, ettei riittävää täysin ajankohtaista tietoa digihuijausilmiöstä ole saatavilla pelkästä kirjallisesta materiaalista. Myöskään suomalaisten pankkien riskienhallintakäytännöistä digihuijauksiin liittyen ei olisi tarpeeksi kirjallista tietoa saatavilla.

Kvalitatiivinen tutkimus voi lähestyä teorian kehittymistä deduktiivisesti, jolloin olemassa olevaa teoriaa käytetään lähtökohtana ja tutkija kehittää teoreettisen

viitekehyksen, jonka avulla tulkitsee myöhemmin empiriaa. Induktiivisessa lähestymistavassa puolestaan aloitetaan empiirisistä havainnoista, joiden avulla rakennetaan uutta tai vahvistetaan aiempaa teoriaa. Abduktiivinen lähestymistapa puolestaan yhdistää molempia näistä, jolloin se alkaa yleensä tutkijan yllättävistä havainnoista, joita tämä pyrkii selittämään luomalla uusia teorioita tai sovittamalla olemassa oleviin teorioihin. (Saunders ym., 2019.) Tämä tutkielma noudattaa abduktiivista lähestymistapaa, sillä tutkielmassa on vahva riskienhallinnan teoriapohja, mutta toisaalta uudehkoa teoriaa digihuijauksista pyritään vahvistamaan tutkielman avulla.

Laadullisen tutkimuksen aineistoa, eli tämän tutkielman tapauksessa haastattelumateriaalia, voidaan analysoida käyttämällä esimerkiksi sisällönanalyysiä, joka mahdollistaa systemaattisen ja objektiivisen analyysin. Teorialähtöisessä sisällönanalyysissä aineiston analyysiä ohjaa jokin valmis teoria tai malli. Aineistolähtöisessä sisällönanalyysissä tutkimusaineistosta on pyrkimys luoda teoreettinen kokonaisuus, mutta aikaisemmillä tiedoilla tutkittavasta ilmiöstä ei ole vaikutusta analyysin toteuttamiseen tai sen lopputulokseen. Kolmas sisällönanalyysin muoto on teoriaohjaava sisällönanalyysi, jota käytetään tässä tutkielmassa menetelmänä haastatteluaineiston analysoinnissa. Teoriaohjaavassa sisällönanalyysissä aineisto analysoidaan aineistolähtöisen sisällönanalyysin tavoin aineiston ehdoilla, mutta abstrahoinnissa empiirinen aineisto liitetään teoreettisiin käsitteisiin. Teoriaohjaavassa sisällönanalyysissä tulee näin ollen esiin päättelyn abduktiivisuus. (Tuomi & Sarajärvi, 2018). Näin voidaan huomioida teorian soveltaminen ilman, että haastatteluissa nousseet uudet näkökulmat jäävät huomiotta, sillä tarkoituksena on muodostaa kokonaisvaltainen sekä ajankohtainen näkemys digihuijausten vaikutuksesta pankkien ja niiden asiakkaiden riskiasemaan sekä riskienhallintakeinoista digihuijausten lisääntyvässä toimintaympäristössä. Abduktiivinen lähestymistapa ja teoriaohjaava sisällönanalyysi tukevat tutkielman pragmatistista näkökulmaa, sillä ne mahdollistavat sekä aineiston että teorian hyödyntämisen analyysissä, ja auttavat siten ilmiön kokonaisvaltaista ymmärtämistä.

1.6 Tutkimuksen rakenne

Tutkielma koostuu viidestä pääluvusta. Ensimmäisessä luvussa, eli johdannossa, on esitelty tutkielman aihe ja sen merkitys, aikaisempia tutkimuksia aihealueesta sekä keskeiset tavoitteet ja rajaukset. Tämän lisäksi johdannossa on kuvattu tutkielman tieteenfilosofiset lähtökohdat ja teoreettinen viitekehys.

Tutkielman toinen luku käsittelee taustateoriaa eli digihuijauksia kyberrikollisuuden ilmiönä muodostaen tutkielman ensimmäisen teoriaosuuden. Luvussa käsitellään digihuijauksia laajempänä yhteiskunnallisena ilmiönä, mutta perehdytään myös erilaisiin yleisempiin huijausmuotoihin.

Tutkielman kolmas luku eli toinen teoriaosuus käsittelee pankkien riskienhallintaa asiakkaisiin kohdistuvissa digihuijaustapauksissa. Luvussa esitellään aiheeseen liittyvää lainsäädäntöä, riskienhallintastandardeja ja -prosesseja sekä tarkempia digihuijauksiin liittyviä riskienhallintakeinoja ja -kontrolleja. Näiden lisäksi luvussa käsitellään yleisemmin pankkien kyberturvallisuutta ja digihuijauksia kyberriskinä, jotta digihuijauksista ja niiden riskienhallinnasta voidaan muodostaa kokonaisvaltaisempi käsitys.

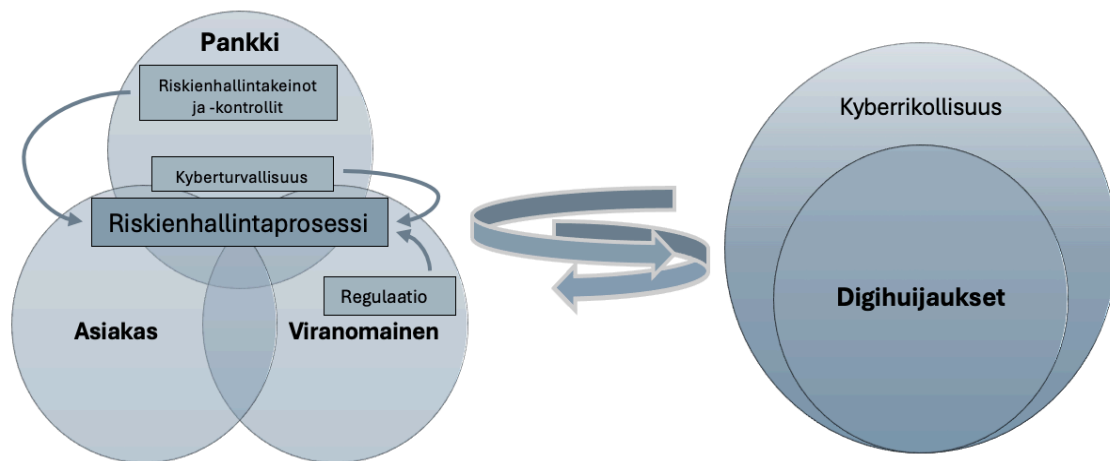
Tutkielman empiriaosuus koostuu neljännessä luvusta, jossa esitellään asiantuntijahaastattelujen avulla kerätty empirinen aineisto ja sen analyysi. Tutkielman viidennessä luvussa pyritään vastaamaan tutkimuskysymyksiin ja esitetään analyysin avulla saadut johtopäätökset sekä mahdollisia jatkotutkimusmahdollisuuksia.

1.7 Teoreettinen viitekehys

Kuviossa 1 on esitetty tutkielman teoreettinen viitekehys. Digihuijaukset ovat kyberrikollisuuteen kuuluva ilmiö, ja ne voivat tapauskohtaisesti täyttää muun muassa petoksen tunnusmerkit (Sisäministeriö, 2024). Pankit pyrkivät ennaltaehkäisemään ja torjumaan ilmiötä riskienhallintaprosessinsa avulla, johon vaikuttavat käytettävissä olevat riskienhallintakeinot ja -kontrollit, regulaatio ja sen muutokset sekä kyberturvallisuuden taso. Samalla, kun pankit lisäävät tietokonejärjestelmien ja internetin käyttöä, syntyy uusia mahdollisuuksia kyberpetoksille, mikä korostaa tarpeen kehittää

riskinhallintakäytäntöjä. (Hull, 2018.) Kyberturvallisuuden taso on osaltaan seurausta enimmäkseen pankin, mutta myös asiakkaan ja viranomaisen toiminnasta. Regulaatio ja sen muutokset ovat pääsääntöisesti viranomaisen vastuulla, mutta vaikuttavat laajalti pankkien toimintaan.

Pankkien, asiakkaiden ja viranomaisen toimilla on päinvastoin vaikutusta digihuijausten kehittymiseen, sillä huijarit pyrkivät hyödyntämään pankkien ja muiden toimijoiden toiminnassa esiintyviä haavoittuvuuksia. Tämän lisäksi huijarit hyödyntävät pankkien tavoin yhä kasvavissa määrin kehittyvää teknologiaa. (FATF, 2023.)



Kuvio 1 Teoreettinen viitekehys

Keskeisintä digihuijausten estämisessä on pankkien riskienhallintaprosessin toimivuus, sillä se auttaa ennaltaehkäisemään ja torjumaan pankkien asiakkaisiin kohdistuvia digihuijauksia, ja tapahtuneissa huijauksissa siitä voi olla hyötyä huijattujen varojen palauttamisessa asiakkaalle. Lisäksi tehokkaan riskienhallinnan avulla hallitaan muita pankkiin ja sen asiakkaisiin kohdistuvia digihuijausten aiheuttamia riskejä.

2 DIGIHUIJAUKSET KYBERRIKOLLISUUDEN ILMIÖNÄ

2.1 Kyberrikollisuus

Kyberrikollisuus eli tietotekniikkarikollisuus, viittaa rikoksiin, jotka kohdistuvat tietotekniikkaan tai tietoverkkoihin, tai rikoksiin, joissa hyödynnetään näitä teknologioita (Sisäministeriö, 2024). Yhteiskunnan digitaalinen kehitys on merkittävästi lisännyt kyberavusteisten talous- ja rahanpesurikosten esiintyvyyttä. Tietotekniikan hyödyntäminen mahdollistaa rikollisille rahavirtojen hämärtämisen ja tarjoaa mahdollisuuden nopeampiin ja suurempiin voittoihin. Lisäksi kyberulottuvuus laajentaa järjestäytyneen rikollisuuden kohteita mahdollistaen useiden uhrien hyväksikäytön. (Europol, 2023.) Tyypillistä kyberrikoksille on kansainvälisyys, sillä verkkoympäristö ei aseta rajoitteita rikollisten ja uhrien fyysiselle sijainnille. Yleisimpiä kyberrikollisuuden rikostyyppejä ovat omaisuusrikokset, etenkin petokset ja maksuvälinepetokset, mutta myös rahanpesu ja kiristysrikokset. (Sisäministeriö, 2024.) Seuraavaksi esitellään tarkemmin joitain rikoslain määrittelemiä kriminalisoituja tekoja, jotka voivat lukeutua kyberrikoksiksi tai kytkeä niihin muutoin.

Petos määritellään rikoslain mukaan teoksi, jolla hankitaan itselle tai toiselle oikeudetonta taloudellista hyötyä tai jolla vahingoitetaan, erehdytetään tai hyväksi käytetään erehdystä saaden toisen tekemään tai jättämään tekemättä jotakin aiheuttaen taloudellista vahinkoa. Kiinni jääneelle voi rangaistuksena olla sakko tai enintään kaksi vuotta vankeutta. (Rikoslaki 36:1§.)

Maksuvälinepetos luokitellaan puolestaan teoksi, jonka avulla hankitaan itselle tai toiselle oikeudetonta taloudellista hyötyä esimerkiksi käyttäen maksuvälinettä ilman sen laillisen haltijan lupaa tai syöttämällä maksuvälineeseen liittyvää dataa saaden aikaan rahan arvon vääristymisen ja aiheuttaen siten taloudellista vahinkoa (Rikoslaki 37:8§).

Rahanpesulla tarkoitetaan muun muassa rikoksella hankitun omaisuuden tai sen tuottaman hyödyn ottamista vastaan, välittämistä ja hallussa pitämistä tarkoituksena hankkia itselle tai toiselle hyötyä tai häivyttää omaisuuden laiton alkuperä. (Rikoslaki

32:6§). Rahanpesuun kytkeytyy rahamuulit, jotka ovat rekrytoitu rikollisten avuksi rahanpesuun usein tietämättöminä laittomista toimista. He siirtävät laittomia varoja tilien välillä, usein eri maissa, toisten puolesta käyttäen henkilökohtaisia ja/tai yritystilejä. (Europol, 2023.)

Kiristysrikos tarkoittaa toisen pakottamista luopumaan taloudellisesta edusta, johon rikoksentekijällä tai sillä, jonka puolesta hän toimii, ei ole laillista oikeutta (Rikoslaki 31:3§).

Kyberrikoksiin voi liittyä myös identiteettivarkaus. Sillä tarkoitetaan rikosta, jossa käytetään oikeudettomasti toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa erehdyttäen kolmatta osapuolta ja siten aiheuttaen taloudellista vahinkoa (Rikoslaki 38:9 a §).

Huomioitavaa on, etteivät kaikki yllä luetellut rikokset ole aina kyberrikoksia, elleivät ne tapahdu digitaalisessa ympäristössä tai hyödynnä tietoteknisiä keinoja.

2.2 Digihuijausten määrittely

Digitaalisten huijausten, eli digihuijausten, käsitteelle ei ole olemassa yksiselitteistä ja kaikenkattavaa määritelmää, vaan tulkintoja ja määritelmiä on useita, mikä osoittaa ilmiön moniulotteisuutta. Yhtenäinen tekijä digihuijauksille on kuitenkin niiden esiintyminen verkko- ja digitaalisessa ympäristössä, jossa huijaukset saavat erilaisia ilmenemismuotoja. Tässä tutkielmassa digihuijaukset asemoidaan osaksi kyberrikollisuuden laajaa kenttää, ja niitä tarkastellaan erityisesti pankkisektorin ja riskienhallinnan näkökulmasta. ACFD (The Association of Certified Fraud Examiners) (2024) mukaan huijaus perustuu harhaanjohtamiseen hyötymistarkoituksessa ja petokseen taas syyllistyy, kun valehtelee riistääkseen henkilöltä tai organisaatiolta rahaa tai omaisuutta. Digihuijaus voi siten täyttää yhden tai useamman rikoksen tunnusmerkin johtuen sen tekotavasta. Kyse voi olla muun muassa petoksesta, maksuvälinepetoksesta, tietomurrosta, markkinointirikoksesta ja joskus kyseessä ei ole lainkaan kriminalisoitu teko (Tuorila, 2018). Suomen viranomaisista Kuluttajaviranomaisten määritelmissä painottuu kuluttajalainsäädäntö ja poliisin määritelmissä rikoslainsäädäntö. Kuluttajien

keskuudessa näkemys ulottuu usein lainsäädännön ulkopuolelle, esimerkiksi tilanteisiin, joissa kuluttaja ei saa olettamaansa tuotetta tai palvelua. (Tuorila, 2018.) Johdonmukaisuuden vuoksi tässä tutkielmassa käytetään yleisesti termiä *digihuijaus*, silloin kun huijauksen rangaistavuus ei ole selkeä tai oleellinen tekijä.

Digitaalinen huijaus liittyy muihin käsitteisiin, kuten operatiivisiin riskeihin (sisältäen kyberriskit ja sosiaalisen manipuloinnin) ja operatiiviseen resilienssiin, mutta käsitteissä on sekä yhtymäkohtia että eroja. (BCBS, 2023). Digihuijaukset aiheuttavat pääosin pankin asiakkaiden menetyksiä eli eivät suoranaisesti kuulu operatiivisen riskin määritelmään, mutta voivat lopulta aiheuttaa operatiivisia tappioita myös pankille. Kyberriski taas kattaa laajemman joukon tapahtumia, jotka voivat vaikuttaa pankkiin ja/tai sen asiakkaisiin, mutta sisältää myös digihuijausten aiheuttamat riskit. Digihuijauksia kyberriskinä ja operatiivisena riskinä käsitellään myöhemmin tutkielmassa. Operatiivinen resilienssi tarkoittaa pankin kykyä ylläpitää toimintaansa häiriötilanteissa ja digihuijausten kontekstissa se tarkoittaa pankin kykyä kestää asiakkaisiinsa kohdistuvia petollisia toimia ja jatkaa kriittisten toimintojen tarjoamista. (BIS, 2023).

Digitaalisilla huijauksilla on omia erityispiirteitä, jotka erottavat ne laajemmista petollisista toimista. Luonteensa vuoksi digihuijaukset toteutetaan etänä ja/tai virtuaalisesti. Toiseksi ne perustuvat petokseen ja/tai väärentämiseen tavoitteen saavuttamiseksi, eli pankin tai asiakkaan kyvyttömyyteen erottaa huijari oikeasta vastapuolesta. Pankkijärjestelmän kontekstissa korostuu tekijänä ulkoinen osapuoli, toimeenpano digitaalisten keinojen kuten sähköpostin kautta sekä pankkivarojen tai asiakkaan tunnistetietojen havittelu. Lisäksi digihuijaukset kohdistuvat pankin asiakkaisiin liittyviin tietojärjestelmiin, kuten tilinhallintajärjestelmiin, korttien käsittelyjärjestelmiin ja pankkisovelluksiin. Toisaalta vaikka digihuijaus kohdistuu pankin asiakkaisiin, pankeilla voi olla epäsuora tai tahaton rooli petosten mahdollistamisessa esimerkiksi mahdollistamalla petolliset maksutapahtumat. Digihuijaukset liittyvät poikkisektoraaalisen luonteensa vuoksi useisiin muihin ilmiöihin, kuten kuluttajansuojaan, markkinoiden eheyteen, rahanpesun torjuntaan ja terrorismin rahoittamisen vastaisiin toimiin sekä rahoitusvakauteen. (BCBS, 2023.)

2.3 Digihuijaukset osana rikollisuutta

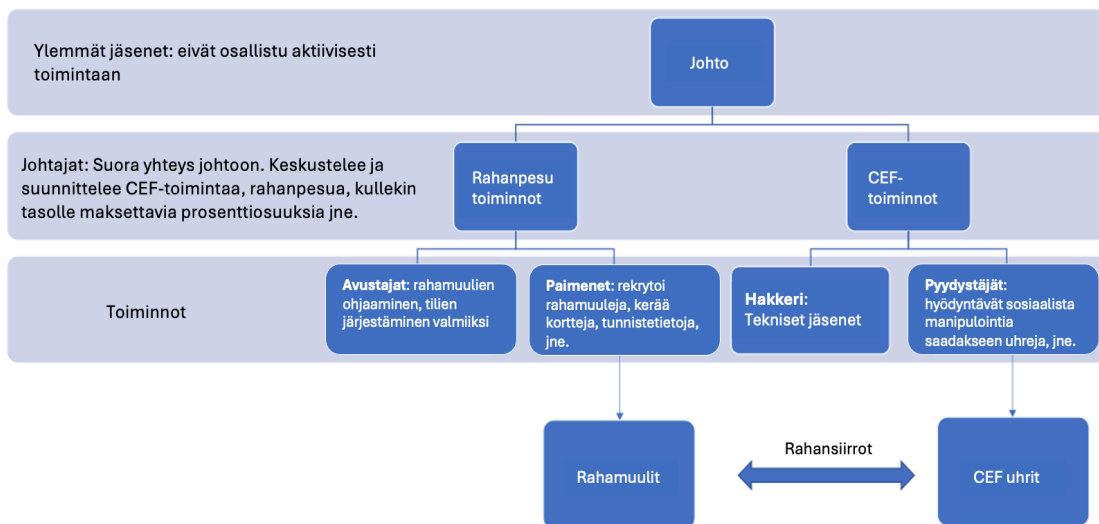
Kyberavusteinen petos (CEF) on kasvava valtioiden rajat ylittävä järjestäytyneen rikollisuuden muoto, johon myös osa digihuijauksista kuuluu. CEF-rikollissyndikaatit ovat usein organisoituja erillisiin alaryhmiin, joilla on erityisiä osaamisalueita, kuten rahanpesu. Toiminnan tutkinnasta tekee monimutkaista alaryhmien hajautettu rakenne eri lainkäyttöalueilla. CEF-syndikaateilla on havaittu olevan yhteyksiä myös muihin rikollisuuden muotoihin, erityisesti ihmiskauppaan ja pakkotyöhön CEF-puhelinkeskuksissa. Uhrit houkuteltaan väärennetyillä työpaikkailmoituksilla online-keskuksiin ja pakotetaan tekemään kyberavusteisia petoksia teollisessa mittakaavassa, mikä antaa CEF-syndikaateille mahdollisuuden laajentaa verkkouhrien maantieteellistä monimuotoisuutta ihmiskaupan uhrien kielitaidon ja kulttuurisen tietämyksen avulla. (FATF, 2023.)

Kyberavusteisilla petoksilla on myös yhteyksiä joukkotuhoukseiden leviämisen rahoitukseen, ja kyberrikollisuus on merkittävä laittoman tulon lähde Korean demokraattiselle kansantasavallalle. Laittomat kybertoimet sisältävät kerätyn henkilötiedon myynnin sekä hakkerointi- ja phishing-työkalujen ja -palvelujen tarjoamisen, joita muut rikolliset voivat käyttää kyberavusteisten petosten tekemiseen. Lisäksi tavallisia ovat CEF-toiminnan toteuttamiseen liittyvät tai sen edellyttämät kyberrikokset, kuten henkilökohtaisen tiedon hankkimiseen tähtäävä hakkerointi, rikollisten ohjelmistojen kehittäminen ja myynti sekä asiakirjaväärennökset. (FATF, 2023.)

Useimmissa valtioissa ei ole havaittu merkittäviä todisteita terroristirahoitustoiminnasta, joka liittyisi kyberavusteisiin petoksiin. Kuitenkin on joitakin havaintoja, joissa terroristitoiminnan ja -rahoituksen elementtejä on liitetty CEF-rikollisiin toimijoihin. (FATF, 2023.)

Rahanpesutapaukset Suomessa liittyvät yleensä petoksiin, varkauksiin, huumausainerikoksiin, verorikoksiin tai muihin talousrikoksiin (IMF, 2023). Huijaukseen saattaa liittyä rahanpesurikos, mikäli sen kohdetta pyydetään välittämään esirikoksella hankittuja varoja eteenpäin. Toisaalta huijaus saattaa toimia esirikoksena, jonka avulla hankittujen varojen alkuperä pyritään myöhemmin häivyttämään

rahanpesulla. CEF-toimintaan liittyvässä rahanpesussa on mukana rahanpesuryhmiä ja ammattimaisia avustajia. Rahanpesuverkostot käyttävät yleensä välikäsiä eli muuleja (money mules), jotka voivat olla tietoisesti tai tietämättään mukana varojen pesussa. Muuleille voidaan tarjota kannustimia tai palkkioita rikollisten varojen käsittelystä. Rahanpesussa voidaan hyödyntää myös bulvaaniyrityksiä tai laillisia liiketoimintayksiköitä, kuten maksu- ja rahalähetyspalveluntarjoajia sekä virtuaalivaluuttapalveluiden tarjoajia (VASPs). Piilottaakseen rikoshyötyjen taloudellisen jäljen rikolliset käyttävät erilaisia rahanpesutekniikoita, kuten käteisrahan käyttöä tai kauppapohjaista rahanpesua. (FATF, 2023.) CEF:n rikollisrakennetta ja rahanpesuverkoston monimutkaisuutta havainnollistetaan kuviossa 2.



Kuvio 2 Esimerkki CEF:n rikollisrakenteesta, mukailen FATF (2023)

Digitalisaation myötä kehittynyt teknologia on mahdollistanut CEF-rikollisille toiminnan laajentamisen, kasvattamisen ja nopeuttamisen. CEF-syndikaatit hyödyntävät teknologian kehitystä nopeuttaakseen rikosten tuottojen pesua. Rikolliset hyödyntävät sosiaalista mediaa ja viestintäalustoja rekrytoidakseen välikäsiä kansainvälisesti suurissa määrissä. Rikolliset myös hyödyntävät nopeasti haavoittuvuuksia, joita ilmenee uusien digitaalisten rahoituslaitosten ja tuotteiden sekä muiden sektorien, kuten verkkokaupan, sosiaalisen median ja suoratoistoalustojen kautta. Rikosten tuotot voidaan pestä nopeasti tiliverkoston kautta ja rikosten tapahtumapaikka onkin usein eri kuin rahanpesun tapahtumapaikka. Yhä useammin rikolliset voivat varastaa henkilöllisyyksiä eri tekniikoilla ja teknologisilla työkaluilla, kuten phishing-hyökkäyksillä,

henkilöllisyyksien ostamisella tai huijaamalla uhrin luovuttamaan henkilöllisyytensä vapaaehtoisesti. Rikolliset perustavat ja hallitsevat näitä tilejä suoraan varastetuilla tai väärillä henkilöllisyyksillä. Tämä tekee rahanpesutoiminnan jäljittämisestä vaikeampaa, koska tilien haltijat eivät välttämättä ole edes tietoisia osallisuudestaan. (FATF, 2023).

CEF-syndikaatit käyttävät teknologian hyödyntämisen lisäksi myös muita tekniikoita välttääkseen kiinnijäämistä, kuten pieniä siirtoja useisiin eri tileihin (smurfing); siirtoja eri rahoituslaitosten, rahansiirto- ja maksupalveluntarjoajien tileillä; ja varojen muuntamista muihin rahoitusvaroihin, kuten virtuaalivaluuttoihin tai prepaid-kortteihin. Tämä voi pidentää aikaa, joka tarvitaan viranomaisten pääsyyn tarvittaviin rahoitustietoihin eri sektorien ja laitosten välillä, jotta laittomat varat voidaan jäljittää, turvata ja lopulta palauttaa. (FATF, 2023). Kryptopalveluntarjoajilla ei ole aina riittäviä asiakkaan tuntemismenettelyjä (Europol, 2024), mitä CEF-syndikaatit käyttävät hyväkseen. Värätyt rahamuulit saattavat myös sallia tilien käytön vain tietyllä, rajallisella ajanjaksolla. Rajallinen aika, yhdessä laillisten rekisteröintimenettelyjen kanssa, tekee prosessista suhteellisen vaikeasti seurattavan. (FATF, 2023).

Digitaalisilla huijauksilla on yhteyksiä myös harmaaseen talouteen, jolla tarkoitetaan organisaation sellaista toimintaa, josta aiheutuvia lakisääteisiä velvoitteita laiminlyödään verojen, lakisääteisten eläke-, tapaturma- tai työttömyysvakuutusmaksujen taikka tullien perimien maksujen suorittamisen välttämiseksi tai perusteettoman palautuksen saamiseksi (Laki Harmaan talouden selvitysyksiköstä 3§). Tietyillä huijaustavoilla, kuten henkilötietojen kalastelu, on yhteys talousrikoksiin, sillä huijari voi käyttää saamiaan tietojaan rahanpesuun tai muihin talousrikoksiin. Tämän lisäksi huijauksella saatuja rahoja voidaan käyttää muun rikollisen aktiviteetin, kuten huumausainekaupan rahoittamiseen. Kuluttajien huijaamiseen keskittyvät yritykset laiminlyövät usein myös muut velvoitteensa, kuten verojen maksun. (Tuorila, 2018.)

Suomalaiset viranomaiset ovat tunnistaneet terrorismin rahoittamiseen ja rahanpesuun liittyen korkeariskiseksi rahavirrat Yhdistyneeseen kuningaskuntaan, Saksaan ja Irlantiin. Osa näihin maihin liittyvistä transaktioista tunnistettiin laittomiksi, esimerkiksi verkkohuijauksiin liittyen. (IMF, 2023.) Huomattava osa petosrikoksella hankituista varoista pestään usein muualla Euroopassa finanssialan toimijoiden kautta. Vuonna 2023

tehdyn selvityksen perusteella petostransaktiot liikkuvat etenkin Liettuaan, Saksaan, Italiaan, Ranskaan ja Espanjaan rekisteröityjen finanssialan toimijoiden tileille. (Keskusrikospoliisi, 2024.)

Digi- ja väestötietoviraston (2023) Digiturvabarometrin 20 prosenttia täysi-ikäisistä suomalaisista on joutunut internetissä petoksen tai muun rikoksen kohteeksi, mutta vain puolet heistä on tehnyt asiasta rikosilmoituksen poliisille. Näin ollen digihuijaukset ovat osa piilorikollisuutta, joten niiden kokonaismäärään ja siten myös vaikutusten täysimääräinen arviointi on haastavaa. Tämä tieto kuitenkin kasvattaa ilmiön merkittävyyttä ja laajuutta entisestään.

2.4 Digihuijausten eri muodot

Vuonna 2023 yleisimmät suomalaisiin kohdistuvat digihuijaukset olivat euromääräisesti merkittävimmiksi arvioituna sijoitus- ja valepoliisihuijaukset, tietojen kalastelu sekä dokumentti- ja rakkaushuijaukset. Lisäksi toimitusjohtajahuijaukset olivat huomattavia. (Palmgren, 2024a.) Näiden lisäksi palveluiden sähköistymisen myötä syntyy jatkuvasti uusia huijausmuotoja, kuten vuonna 2023 yleistynyt turvatilipetos (Finanssiala, 2023). Lisäksi petostapauksissa ja etenkin petosvarojen pesutoiminnassa on yleistynyt erilaisiin FinTech-yrityksiin kytkeytyvien virtuaalisten IBAN:ien käyttö (Keskusrikospoliisi, 2024). Koneoppimista, tekoälyä ja deepfake-teknologiaa voidaan hyödyntää lähes kaikenlaisissa huijauksissa (Europol, 2023). Koneoppimisalgoritmien avulla huijari voi luoda syvävääreännöksen avulla jonkun ääntä tai videota, jota voidaan käyttää kyseisen henkilön matkimiseen puhelimesta tai biometrisissä tunnistautumisjärjestelmissä. Syvävääreännöksiä voidaan myös käyttää yhdessä sosiaalisen manipuloinnin tekniikoiden kanssa huijaamaan uhrit luovuttamaan tilitunnuksensa. Syvävääreännösteknologia on vielä suhteellisen uusi, mutta se voi aiheuttaa merkittäviä riskejä tulevaisuudessa. (FATF, 2023.)

Uhrina ei välttämättä onnistuta huijaamaan yhdellä huijausmuodolla, joten huijarit voivat käyttää useita tekniikoita päästäkseen tavoitteeseensa, joka on usein rahansiirron saaminen. Tämän lisäksi huijarit saattavat siirtyä muihin huijaustyyppisiin, jos alkuperäinen huijaus uhkaa epäonnistua. Esimerkiksi tietojenkalastelun tai sosiaalisen

median huijauksen uhria voidaan alkaa huijata sijoitushuijauksen keinoin, jos luottamus uhriin on saatu jo rakennettua aiemmalla huijausmuodolla. (FATF, 2023.)

2.4.1 Digihuijaukset pankkisektorilla

Pankkisektorilla asiakkaisiin kohdistuvat huijaukset voidaan jakaa neljään kategoriaan, joista ensimmäinen on digitaalinen petos, joka liittyy verkkopankkimaksuvälineisiin ja jossa on tarkemmin kyse valtuuttamattomista maksutapahtumista. Katteoria kohdistuu esimerkiksi kortteihin, pankkisiirtoihin, suoraveloituksiin ja sähköiseen rahaan. Asiakkaiden maksutietojen tai verkkopankkitilille murtautuminen sisältyvät näihin valtuuttamattomiin maksutapahtumiin. Esimerkkejä tällaisista huijauksista ovat asiakkaan maksukorttien tietojen varastaminen sosiaalisen manipuloinnin keinoin tai asentamalla haitallisia skriptejä verkkokauppoihin. Lisäksi tilin kaappaamiseen (Account Takeover, ATO) ja automaattisiin siirtosysteemeihin (Automatic Transfer Systems, ATS) liittyvät petokset kuuluvat tähän kategoriaan. Toinen kategoria liittyy myös verkkopankkimaksuvälineisiin, tarkemmin maksajan manipulointiin maksutapahtuman suorittamiseksi. Tähän liittyvät petolliset tapahtumat, joissa huijari pyrkii manipuloimaan asiakasta maksutapahtuman suorittamiseksi tai antamaan hyvässä uskossa maksupalveluntarjoajalle ohjeet tehdä siirto maksutilille, joka kuuluu huijarille. Tällainen huijaus voi tapahtua esimerkiksi pankin identiteetin väärentämisen tai sosiaalisen manipuloinnin avulla. Kolmas kategoria sisältää pankkien asiakkaiden muihin pankkituotteisiin liittyvät digihuijaukset. Tähän kuuluu esimerkiksi asiakkaiden manipulointi tarkoituksena saada heidät investoimaan väärennettyihin sijoitustuotteisiin tai ottamaan väärennettyjä luottoja. Neljäs eli viimeinen kategoria kohdistuu pankkiin itseensä asiakkaiden tietojen tai pankkien järjestelmien väärinkäytön kautta. Se voi tarkoittaa esimerkiksi pankkitilien avaamista tai luottokorttien hakemista varastetulla tai valeidentiteetillä, sekä näiden tilien tai korttien käyttöä rahanpesussa. (BCBS, 2023). Tutkielman rajausten takia emme käsittele tähän neljänteen kategoriaan liittyviä digihuijauksia enempää vaan seuraavaksi perehdymme erilaisiin pankkien asiakkaita koskeviin huijauksiin.

2.4.2 Sosiaalinen manipulointi

Euroopan unionin kyberturvallisuusviraston ENISAN julkaiseman raportin mukaan yksi yleisimmistä turvallisuusuhista vuosina 2022–2030 on sosiaalinen manipulointi (social engineering), joka tarkoittaa tietojen tai palvelujen hankkimista inhimillisiä virheitä hyödyntämällä. (Euroopan parlamentti, 2022.) Tarkemmin termi viittaa erilaisiin tekniikoihin, joilla hyökkäyksen uhreja pyritään huijaamaan heidän rahojensa, henkilökohtaisen tiedon, käyttäjätunnusten ja muun omaisuuden varastamiseksi. (F-Secure, 2024a.) Näitä tekniikoita hyödynnetään kaikissa tässä tutkielmassa esitetyissä huijausmuodoissa, mutta vain osa sosiaalisesta manipuloinnista toimii työkaluna digitaalisten huijausten toteuttamiseen, sillä sitä hyödynnetään myös laajemmin petoksissa, jotka eroavat digihuijausten määritelmästä (BCBS, 2023).

Tietojen ja rahojen varastamisen lisäksi uhrin tunteita voidaan hyödyntää maksusuoritusten tai tilien hallinnan saamiseksi tai muiden taloudellisten toimien, kuten lainahakemusten tekemiseksi tai rikostuottojen vastaanottamiseen tarkoitettujen tilien avaamiseksi (FATF, 2023). Huijari väittää usein olevansa luotettava taho, kuten työnantaja tai jokin valtiollinen toimija. Sosiaalinen manipulointi on etukäteen tarkkaan suunniteltua rikollista toimintaa, jossa käytetään hyväksi ihmisten hyväntahtoisuutta, ja voidaan vedota kiireeseen tai käyttää uhkailua tai kiristämistä keinoina saada uhri toimimaan rikollisen tahdon mukaan. Näin ollen ilmiö pohjautuu käyttäytymisen ja psykologian ymmärtämiseen (F-Secure, 2024a.)

2.4.3 Sijoitushuijaus

Sijoitushuijauksissa huijarit voivat lähestyä muun muassa puhelimitse tai viestien välityksellä tarjoten tekaistuja uutisia huipputuottavista sijoituskohteista, kuten osakkeista, kryptovaluutoista tai joukkolainoista. Huijarit saattavat pyrkiä asentamaan huijauksen kohteen tietokoneelle etähallintaohjelman tai luoda valesivustoja, joilla näkyy väärennettyä tietoa sijoitusten tuotoista. (Kuluttajaliitto, 2024a.)

Asiakas ymmärtää yleensä tulleen huijatuksi vasta nostaessaan rahoja pois sijoituksesta, jolloin häneltä saatetaan vaatia maksua varojen nostamiseksi, eli esimerkiksi prosenttiosuutta kuvitteellisesta tuotosta. Tällöin huijauksen uhri saattaa tulla

huijatuksi jopa useaan kertaan. Huijarit saattavat myös jopa vuosien jälkeen ottaa asiakkaaseen yhteyttä esimerkiksi viranomaisen tai asianajotoimiston nimissä ja tarjota palvelua huijattujen varojen takaisinsaamiseksi. Osan sijoitushuijausten uhreista on myös itse löytänyt tällaisia palveluntarjoajia ja tullut uudelleen huijatuksi. (FINE, 2024.)

2.4.4 Valepoliisihuijaus

Valepoliisihuijauksen tavoitteena on hankkia uhrien verkkopankkitunnuksia tai maksukorttien tietoja. Valepoliisi lähestyy uhreja usein soittamalla ja esittäytyy poliisiksi pyrkien siten voittamaan uhrinsa luottamuksen. Tämän jälkeen hän varoittaa rikoksesta, jonka kohteeksi uhri on vaarassa joutua, tai tarjoutuu auttamaan tapahtuneen rikoksen selvittämisessä. Valepoliisi voi myös kertoa, että uhrin varat ovat vaarassa ja siirrettävän vuoksi poliisille turvaan. Huijauksissa voidaan käyttää pelottelua tai kiireeseen vetoamista. (OP, 2024.)

2.4.5 Tietojenkalastelu ja sen eri muodot

Tietojen kalastelussa (phishing) uhri huijataan paljastamaan arkaluontoisia tietoja, kuten henkilötietoja, pankkitietoja tai tilin kirjautumistunnuksia. (FATF, 2023.) Tavoitteena voi myös olla saada uhri avaamaan vaarallisia asiakirjoja, tiedostoja tai sähköposteja tai vierailemaan haitallisilla verkkosivustoilla. (Euroopan parlamentti, 2022.) Tietojen kalastelun kohteelle luvataan usein palkintoja tai esitetään tekaistuja maksuja. Yleensä tarkoituksena on saada kohde klikkaamaan linkkiä tai maksamaan pienehkö summa. (Kilpailu- ja kuluttajavirasto, 2024.) Kalastelu voi myös johtaa tilausansaan, jossa erehdytetään tekemään pitkäkestoinen tilaussopimus, jonka perusteella veloitetaan tiliä tai lähetetään laskuja (Kilpailu- ja kuluttajavirasto, 2024).

Tekstiviestihuijaus (smishing) on yleisin kalastelun muoto, ja sen jälkeen seuraavat muut variantit, kuten vishing eli puhelimitse toteutettava kalastelu ja quishing, joka puolestaan viittaa QR-koodin avulla tapahtuvaan tietojen kalasteluun. (Europol, 2024). Rikollinen käyttää näiden tekniikoiden avulla saatuja tietoja uhrien tilien tyhjentämiseen, uusien maksutilien avaamiseen tai vilpillisiin maksutapahtumiin. (FATF, 2023.)

Tietojen kalastelun uusi muoto on turvatilipetos, jossa aluksi uhreille lähetetään houkuttelevia tekstiviestejä, jotka ohjaavat kalastelusivuille, joilla pyritään hankkimaan uhrin verkkopankkitunnukset. Tämän jälkeen huijarit esiintyvät pankin edustajina ja soittavat uhreille kehottaen siirtämään rahat ”turvatilille” varmuuden vuoksi. (Finanssiala, 2023.)

Tietojenkalasteluhyökkäyksiä tehdään usein eri yritysten ja organisaatioiden nimissä. Check Point Research havaitsi vuoden 2023 viimeisellä neljänneksellä seuraavien yritysten nimien esiintyvän kalasteluhuijauksissa: Microsoft (33 %), Amazon (9 %), Google (8 %), Apple (4 %) ja Wells Fargo (3 %). IBM vahvisti vastaavat havainnot. Vuonna 2023 yleisimmin huijauksissa väärinkäytetyt yritykset olivat Google, Telegram, Microsoft, Visa ja Apple. (ENISA, 2024.)

Phishing as a Service -markkinat kasvavat nopeasti EU-alueella tarjoten tuotteita, palveluja ja uhreista kerättyjä tietoja, mikä mahdollistaa yhä useamman rikollisryhmän osallistumisen verkkopetostoimintaan, riippumatta heidän teknisestä asiantuntemuksestaan. Palveluntarjoajilta voi ostaa kalastelusivuston mille tahansa pankille tai postitoimipaikalle, ja nämä sivustot saattavat jopa olla yhteydessä toisiinsa. (Europol, 2024.)

2.4.6 Dokumenttihuijaus

Dokumenttihuijauksissa uhrille lähetetään sähköpostitse tai sosiaalisen median kanavissa virallisen näköinen kirje tai viesti, jossa pyydetään yleensä apua perintö- tai muiden varojen siirtämiseksi maiden välillä. Huijari lupaa huomattavan suuren palkkion avusta, mutta ennen varojen siirtoa uhria pyydetään usein toimittamaan tietoja itsestään tai maksamaan tietty rahasumma kirjeen lähettäjälle eräänlaisena takuumaksuna. Kyseinen maksu voi perustua esimerkiksi valuutanvaihtoon, asianajopalkkion maksamiseen tai rahan kotiuttamiseen. (Finanssivalvonta, 2024.)

2.4.7 Rakkaushuijaus

Rakkaushuijauksessa huijari käyttää hyväkseen toisen ihmisen tunteita ja luottamusta rahallisen hyödyn tai muun edun saamisessa. Seuranhakualustat, sosiaalinen media ja

keskustelufoorumit toimivat merkittävinä alustoina rakkaushuijausten toteutumiseksi. Huijarit pyrkivät manipuloimaan huijauksen kohteen tunteita ja luottamusta. (Finanssivalvonta, 2024.)

"Pig butchering" -huijaus yhdistää romanssihuijauksen ja sijoitushuijauksen. Tässä huijausmuodossa rikolliset luovat luottamussuhteen uhriin ja vakuuttavat hänet sijoittamaan säästönsä petollisille kryptovaluuttakauppapaikoille. Huijaus tapahtuu ajan myötä ja aiheuttaa suuria rahallisia menetyksiä. Petoksen paljastuttua rikolliset usein ottavat yhteyttä uhreihin esiintyen lakimiehinä tai lainvalvontaviranomaisina ja tarjoavat apua varojen palauttamiseen maksua vastaan. (FATF, 2023.)

2.4.8 Verkkokauppa- ja kaupankäyntialustahuijaukset

Verkkokauppa- ja kaupankäyntialustahuijauksissa uhrit houkutellessaan tekaistujen mainosten tai neuvonantajien avulla sijoittamaan väärennetyille kaupankäynti- tai sijoituspalveluille (FATF, 2023). Toisaalta myös luotettavilla kaupankäyntialustoilla, kuten Tori.fi- ja Facebookin Marketplace-palvelussa tapahtuu huijauksia. Tyypillisesti huijari esiintyy tuotteen ostajana ja ottaa yhteyttä myyjään ehdottaen maksun suorittamista ja tuotteen toimitusta esimerkiksi Postin tai muun kuriiripalvelun kautta. Myyjälle lähetetään linkki, joka ohjaa luotettavalta näyttävälle kalastelusivustolle, jolle uhrin on tarkoitus syöttää verkkopankki- ja korttitiedot maksun vastaanottamista varten. Kyseessä on kuitenkin huijaus ja uhrin tiedot päätyvät rikollisille. Nykyisin lisääntyvässä määrin myös majoitus- ja matkapalveluntarjoajien sivustoilla tapahtuu huijauksia, joissa varauksen tehnyt asiakas saa myöhemmin majoituspalvelun nimissä huijausviestin, jossa ilmoitetaan varausmaksun tai varauksen epäonnistuneen. Tämän jälkeen asiakas huijataan linkin kautta huijaussivustolle syöttämään korttitietonsa. (FINE, 2024.)

2.5 Digihuijaukset ilmiönä

Yhteenvedon voidaan todeta digihuijausten olevan osa laajempaa kyberrikollisuuden kenttää, jonka keskiössä on tietotekniikan ja digitaalisten ympäristöjen hyödyntäminen petollisiin tarkoituksiin. Teknologinen kehitys, yhteiskunnan digitalisaatio ja verkkoympäristön kansainvälisyys ovat vaikuttaneet digihuijausten määrän kasvuun mahdollistaen huijausten tehokkaan ja monivaiheisen toteutuksen.

Digihuijauksia ei voida yksiselitteisesti määritellä yhden rikosnimikkeen alle, vaan ne voivat täyttää useiden eri rikostyyppien, kuten petoksen, maksuvälinepetoksen, identiteettivarkauden tai rahanpesun tunnusmerkit. Digihuijauksilla on kytköksiä järjestäytyneeseen rikollisuuteen ja niiden taustalla voi olla kansainvälisiä rikollisverkostoja, ihmiskauppaa tai taloudellista hyväksikäyttöä. Rikolliset hyödyntävät teknologisia keinoja, kuten tekoälyä, Phishing as a Service-palveluja ja rahanpesutekniikoita, jotka vaikeuttavat rikollisten jäljittämistä.

Digihuijausmuotoja on useita, ja niihin lukeutuvat muun muassa sijoitus-, rakkaus-, dokumentti- ja valepoliisihuijaukset sekä erilaiset tietojenkalastelun muodot. Huijauksissa korostuu yhä useammin sosiaalisen manipuloinnin keinot, kun huijarit hyväksikäyttävät ihmisten psykologisia heikkouksia.

Huijauksen kohteeksi joutuminen on yhä yleisempää, sillä jopa viidesosa suomalaisista aikuisista on joutunut verkossa tapahtuneen rikoksen kohteeksi, mutta vain osa ilmoittaa tapahtuneesta viranomaisille. Tämän vuoksi ilmiön todellinen laajuus ja sen taloudelliset ja yhteiskunnalliset vaikutukset ovat osittain tuntemattomia, mutta selvästi kasvavia.

3 PANKKIEN RISKIENHALLINTA DIGIHUIJAUSTAPAUKSISSA

3.1 Pankkeihin kohdistuva regulaatio digihuijaustapauksissa

Digitaaliset huijaukset ovat osa kansainvälisen finanssisektorin kasvavaa uhkakenttää, ja niihin liittyy sääntelyä niin kansallisella kuin kansainvälisellä tasolla. EU:ssa digitalisaatio on johtanut maksupalveluiden turvallisuuden parantamiseen, ja Basel-säännökset korostavat pankkien velvollisuutta raportoida sisäisistä ja ulkoisista petoksista. Tämä sääntelykehys toimii perustana digihuijauksiin liittyvän riskienhallinnan rakenteelle, ja se kytkeytyy tiiviisti myöhemmin tutkielmassa tarkemmin käsiteltävään kokonaisvaltaiseen riskienhallintaan (ERM), joka asettaa strategiset raamit myös digihuijausten hallintaan.

Digitaalisten vähittäismaksujärjestelmien kehitys ja verkkokaupan kasvu ovat edistäneet innovatiivisia verkkomaksumenetelmiä luoden tarpeen parantaa myös turvallisuutta etenkin etätransaktioihin liittyen. Euroopan Unionissa vähittäismaksujen digitalisaatioon on liittynyt tehokkuutta, turvallisuutta ja läpinäkyvyyttä parantavia sääntelytoimenpiteitä, kuten digitaalisten petosten raportointi maksupalveluntarjoajilta. Sekä Basel II- että III-standardit edellyttävät pankkien keräävän tietoja kaikista sisäisistä ja ulkoisista petoksista johtuvista tappioista, mutta eivät erityisesti digitaalisten petosten osalta. (BCBS, 2023.)

Keskuspankin sääntelijät vaativat, että pankit pitävät pääomaa hallitakseen kohtaamiaan riskejä. Vuonna 1988 kehitettiin kansainväliset standardit tämän pääoman määrittämiseksi. Nykyisin pääomaa vaaditaan kolmen riskityypin hallintaan: luottoriskiin, markkinariskiin ja operatiiviseen riskiin. (Hull, 2018.) Vuonna 2017 lopullisesti julkaistuun ja myöhemmin täydennettyyn Basel III -säännökseen kuuluva Basel-viitekehys kuvaa, miten lasketaan riskipainotetut varat (RWA) luottoriskille, markkinariskille ja operatiiviselle riskille (BIS, 2024). Digihuijaukset kuuluvat näistä operatiivisiin riskeihin, jotka Baselin pankkivalvontakomitean määritelmän mukaan johtuvat riittämättömistä tai epäonnistuneista sisäisistä prosesseista, ihmisistä ja järjestelmistä tai ulkoisista tapahtumista (Hull, 2018).

Baselin pankkivalvontakomitean mukaan: ”Uusi standardoitu lähestymistapa operatiiviselle riskille määrittää pankin operatiivisen riskin pääomavaatimukset kahden komponentin perusteella: (i) pankin tulon mittari; ja (ii) pankin historiallisten tappioiden mittari. Konseptuaalisesti se olettaa: (i) että operatiivinen riski kasvaa kiihtyvällä tahdilla pankin tulojen kasvaessa; ja (ii) että pankit, jotka ovat aiemmin kokeneet suurempia operatiivisen riskin tappioita, todennäköisesti kokevat operatiivisen riskin tappioita myös tulevaisuudessa” (BCBS, 2017). Basel III mukaan operatiivisen riskin pääomavaatimukset määräytyvät liiketoimintanäyttäjäkomponentin (BIC) ja sisäisen tappioiden yhdistelmän (ILM) tulona. BIC riippuu pankin koosta ja monimutkaisuudesta, ja ILM perustuu pankin sisäiseen tappiohistoriaan. (Girling, 2022.) Operatiivisen riskin kvantifiointi on yleensä haastavaa, sillä usein tappiohistoriaa ei ole aina saatavilla, ja joitain riskejä ei voida helposti mitata. (Hopkin, 2018.)

Hyvän operatiivisen riskienhallinnan periaatteet (PSMOR) pyrkivät edistämään operatiivisen riskienhallinnan tehokkuutta, joka mahdollistaa pankeille paremman ymmärryksen ja hallinnan riskiprofilistaan mukaan lukien digihuijauksiin liittyvät riskit. Operatiivisen resilienssin periaatteet (POR) puolestaan tähtäävät pankkien kyvyn vahvistamiseen kestää operatiivisen riskin aiheuttamia tapahtumia, jotka voivat aiheuttaa merkittäviä operatiivisia häiriöitä tai laajamittaisia keskeytyksiä rahoitusmarkkinoilla. Digihuijausten kontekstissa operatiivinen resilienssi tarkoittaa pankin kykyä kestää asiakkaitaan koskevia huijauksia ja jatkaa kriittisten toimintojen tarjoamista. Tehokas operatiivinen riskienhallintajärjestelmä ja operatiivisen resilienssin korkea taso vähentävät yhdessä operatiivisten riskitapahtumien esiintyvyyttä ja vaikutusta. (BCBS, 2023.) Baselin ydinperiaatteiden (BCP) mukaan valvojien tulisi varmistaa, että pankeilla on riittävät politiikat ja prosessit, jotta ne voivat estää ja havaita rikollista toimintaa sekä raportoida epäilyttävistä toimista. (BCBS, 2023.)

Vuonna 2023 komitea julkaisi *Riskienhallintaperiaatteet sähköisessä pankkitoiminnassa* auttaakseen pankeja laajentamaan sen hetkisiä riskienvalvontakäytäntöjään kattamaan myös sähköistä pankkitoimintaansa. Näistä neljästätoista periaatteesta kolme on erityisen merkityksellisiä digihuijausten kannalta. Ensinäkin pankkien tulisi toteuttaa asianmukaisia toimenpiteitä asiakkaidensa henkilöllisyyden ja valtuutuksen todentamiseksi, kun ne tekevät liiketoimia internetissä. Mikäli pankki epäonnistuu

asiakkaidensa riittävässä todentamisessa, se voi johtaa valtuuttamattomien henkilöiden pääsyyn sähköisiin pankkitileihin, mikä voi lopulta aiheuttaa taloudellisia tappioita ja mainevahinkoja pankille petoksen, luottamuksellisten tietojen paljastumisen tai tahattomasti rikolliseen toimintaan osallistumisen kautta (Periaate 4). Pankkien tulisi myös varmistaa, että sähköisissä pankkijärjestelmissä, tietokannoissa ja sovelluksissa on asianmukaiset tehtävien erottelua edistävät toimenpiteet, jotta petosriski operatiivisissa prosesseissa ja järjestelmissä pienenee (Periaate 6). Kolmanneksi pankkien tulisi varmistaa, että sähköisen pankkitoiminnan tapahtumien, tietojen ja informaation eheys on suojattu, sillä sähköisen pankkitoiminnan luonteen vuoksi ohjelmointivirheiden tai petostapahtumien havaitseminen varhaisessa vaiheessa saattaa olla haastavaa (Periaate 8). (BCBS, 2023.)

Kansallisena sääntelynä puolestaan vuonna 2010 voimaan tullut Maksupalvelulaki (290/2010) sääntelee maksujenvälitystä perustuen EU:n maksupalveludirektiivin III ja IV osan säännöksiin. Vuonna 2018 toisen maksupalveludirektiivin eli PSD2 myötä maksupalvelulakia muutettiin monilta osin. Sen myötä pankeille tuli velvollisuus avata ulkopuolisille palveluntarjoajille maksutilidata sekä mahdollisuus maksutoimeksiantopalvelujen tarjoamiseen asiakkaan suostumuksella. Ulkoisia palveluntarjoajia voivat olla maksutoimeksiantopalveluiden tai tilitietopalvelujen tarjoajat. Lisäksi PSD2-direktiivi asetti maksupalvelujen käyttäjälle aiempaa vahvemmat tunnistamisvaatimukset ja muutti väärinkäytöstilanteiden vastuunjaon maksupalvelun käyttäjän hyväksi. (Wuolijoki, 2023.) Uuden suunnitteilla olevan maksupalveludirektiivin PSD3 tarkoituksena on muun muassa parantaa kuluttajansuojaa ja tehostaa pankkien petostentorjuntaa entisestään. (Nordea, 2024.)

Maksulaitoslain 19a ja 19b pykälien mukaan maksupalveluntarjoajilla tulee olla riittävät riskienhallintamenettelyt maksupalvelujen operatiivisten ja turvallisuusriskien hallintaan sekä poikkeamien ja petosten seurantaan ja raportointiin. Niiden tulee toimittaa Finanssivalvonnalle tilastotietoja maksuvälineisiin liittyvistä petoksista. Tietoturvallisuuden osalta pankkien tulee muun muassa varmistaa, ettei ulkopuolisilla tahoilla ole pääsyä asiakkaan maksuvälinettä koskeviin henkilökohtaisiin turvatunnuksiin (Maksupalvelulaki 53§:3).

Pankkien kasvavaa vastuuta ehkäistä petoksia vahvistaa suunniteltu maksupalveluasetus, josta Euroopan komissio on 28.6.2023 antanut ehdotuksen (Deloitte, 2024; Oikeusministeriö, 2023). Asetuksen tarkoitus olisi muun muassa laajentaa edelleen maksupalvelun tarjoajien korvausvastuuta koskemaan esimerkiksi spoofing-tapauksia eli tilanteita, joissa hyökkääjä väärentää henkilöllisyytensä tai huijaa uhria valheellisella tiedolla verkossa (Deloitte, 2024; F-Secure, 2024b).

Euroopan neuvosto hyväksyi alkuvuodesta 2024 pikamaksuasetuksen, jonka myötä tulevaisuudessa raha siirtyy tilien välillä kymmenessä sekunnissa mihin vuorokaudenaikaan tahansa myös toiseen EU-maahan. Toisaalta asetus vaatii pikamaksupalveluiden tarjoajien tarkistavan, että maksunsaajan IBAN-tilinumero ja nimi täsmäävät, mikä varoittaa maksajaa mahdollisista virheistä tai petoksista. (Eurooppa-neuvosto, 2024.) Samaa vaatii myös maksupalveluasetus, joka edellyttää lisäksi asiakkaiden tiedottamista petosriskeistä (Deloitte, 2024).

Edellä mainitut sääntelyn asettamat velvoitteet pankeille ennaltaehkäisevät asiakkaiden pankkitunnusten ja maksuvälineiden väärinkäyttöä. Niiden rajallisuuden vuoksi on kuitenkin tärkeää huomioida myös muut riskienhallinnalliset toimenpiteet sekä lainsäädännön jatkuva kehittäminen. Finanssivalvonta on ehdottanut turvallisuuden parantamiseksi muun muassa käyttäjälähtöisiä turvarajoituksia, aiemmasta maksuhistoriasta poikkeavien maksujen pysäyttämisen tehostamista ja eri huijaustavoista tiedottamista. Suositukset heijastelevat ja ennakoivat EU-tason muutoksia. (Deloitte, 2024.)

Sääntely asettaa pankeille velvoitteita petosrikosten ennaltaehkäisyyn, mutta toisaalta luo myös raamit niihin liittyvään riskienhallintaan. Seuraavat alaluvut käsittelevät riskienhallintaprosessia alkaen ylätasolta tarkentuen kyberriskeistä digihuijauksiin liittyvään riskienhallintaan sivuten samalla lainsäädännöllisiä seikkoja.

3.2 Riskienhallintaprosessi ja standardit

Organisaatiot kohtaavat hyvin laajasta erilaisia riskejä, jotka voivat vaikuttaa niiden toiminnan lopputulokseen. Riskillä on monta määritelmää, mutta yleisesti sillä viitataan jonkin lopputuloksen tai seurauksen mahdollisuuteen tai epävarmuuteen. Riskin

realisoiduttua sen seuraukset voivat olla joko positiivisia tai negatiivisia. (Frase & Simkins, 2010.) Riskit voivat estää yrityksen mission tai tavoitteiden saavuttamisen (hazard risks), vahvistaa tavoitetta (opportunity risks) tai luoda epävarmuutta lopputuloksista (control risks). Compliance-riskit liittyvät puolestaan sääntöjen ja organisaatiolle asetettujen pakollisten velvoitteiden noudattamiseen. (Hopkin, 2018.) Riskin lisäksi toinen keskeinen käsite on riskille altistuminen, joka tarkoittaa sitä, miten altis organisaatio on riskille tai riskisalkulle. Tämä riippuu riskitapahtuman todennäköisyydestä ja mahdollisesta vaikutuksesta. Aiemmin mainittujen vaikutusten lisäksi realisoituneilla riskeillä voi olla vaikutuksia myös yrityksen maineeseen. (Frase & Simkins, 2010.)

Riskitapahtuman vahinkopotentiaali ja todennäköisyys voidaan jaotella epävarmaan, matalaan ja korkeaan. Näin riskejä voidaan luokitella eri luokkiin, joiden perusteella voidaan valita sopivin lähestymistapa riskienhallintaan. Tällaisia ovat muun muassa riskiin perustuva, ennaltaehkäisevä ja diskursiivinen. Näin voidaan edelleen valita sopiva toimintastrategia, johon kuuluu riskiin perustuvassa lähestymistavassa muun muassa riskin katastrofipotentiaalin vähentäminen ja resilienssin lisääminen. Ennaltaehkäisevässä lähestymistavassa puolestaan korostuu varovaisuusperiaatteiden noudattaminen ja riskin vähentäminen. Diskursiivinen lähestymistapa painottaa sen sijaan tietoisuuden lisäämistä, varautumishallintaa ja korvaavien ratkaisuiden etsimistä. (Klinke & Renn, 2001.)

Riskienhallinnan on tarjottava integroitu lähestymistapa eri riskityyppien arvioimiseen, hallintaan ja seurantaan. Riskienhallinta voidaan määritellä organisaation sisällä tapahtuvien toimintojen kokonaisuutena, jonka tarkoituksena on saavuttaa mahdollisimman suotuiset tulokset ja vähentää näiden tulosten vaihtelua tai epävakautta. Riskienhallintaprosessin avulla voidaan parantaa organisaation ydintoimintojen hallintaa varmistamalla, että keskeiset riippuvuudet analysoidaan, seurataan ja tarkastellaan. (Hopkin, 2018.) Riskienhallintaa voidaan toteuttaa myös erilaisten standardien avulla ja siten riskienhallintaprosessi voidaan kuvata eri tavoin. Riskienhallintaprosessiin kuuluu yleisesti riskien tunnistaminen ja arviointi, riskien vertailu kriteereihin nähden, merkittäviin riskeihin reagointi, kontrollien resurssien varmistaminen, reagointi ja tapahtumien suunnittelu, riskisuorituskyvyn raportointi sekä riskienhallintajärjestelmän tarkastelu. (Hopkin, 2018.) Riskienhallintastandardi määrittelee lähtökohdan riskien

onnistuneelle hallinnalle, mukaan lukien riskienhallintaprosessin kuvauksen sekä suositellun viitekehyksen, joka tukee tätä prosessia. Hopkinin (2018) mukaan menestyksekkään riskienhallintakehyksen keskeisiä komponentteja ovat viestintä- ja raportointirakenne (arkkitehtuuri), organisaation asettama yleinen riskienhallintastrategia (strategia) ja vakiintuneet ohjeet ja menettelyt (protokollat).

Riskienhallintastandardeista tunnettuja ovat muun muassa ISO 31000 ja COSO ERM-viitekehys (Hopkin, 2018), joista jälkimmäinen esitellään tarkemmin tutkielman seuraavassa luvussa. Kansainvälisen standardointijärjestön luomassa ISO 3100 standardissa korostuu riskien tunnistaminen, arviointi, käsittely ja seuranta (ISO, 2018). Sen mukaan tärkeää on riskienhallinnan integroiminen strategiseen ja operatiiviseen johtamisjärjestelmään (Hopkin, 2018). Vastaavasti Moellerin (2011) mukaan riskienhallinta tulisi nähdä nelivaiheisena prosessina: (1) riskien tunnistaminen, (2) tunnistettujen riskien määrällinen tai laadullinen arviointi, (3) riskien priorisointi ja vasteiden suunnittelu, ja (4) riskien seuranta. Hänen mukaansa menetelmästä riippumatta on aina tarpeen tunnistaa ja ymmärtää yritykseen kohdistuvat erilaiset riskit, arvioida niitä kustannusten, vaikutusten ja todennäköisyyden perusteella, kehittää vastetoimia riskin toteutuessa sekä luoda dokumentointimenettelyjä kuvaamaan tapahtunutta ja jatkossa tarvittavia korjaavia toimia.

Riskienhallintaprosessia voidaan tarkastella kysymysten avulla, mikä mahdollistaa niiden tekijöiden tunnistamisen, joiden tulisi sujua suunnitelmien mukaisesti, sekä niihin liittyvien epäonnistumisten, syiden ja seurausten analysoinnin. Tällöin on myös tärkeää arvioida tapahtuman todennäköisyyttä, kehittää tehokkaita kontrollimekanismeja, selvittää vaihtoehtoisia lähestymistapoja sekä arvioida tapahtuman vaikutuksia. (Jaradat, Magpili & Pinto, 2015.) Toinen tapa on tunnistaa riskejä menneisyyden tapahtumien perusteella. Riskirekisteriin voidaan tallentaa esimerkiksi riskitapahtuman kuvaus, syyt, seuraukset, riskienhallintastrategian tehokkuus ja riskin esiintymistiheys. (Jaradat ym., 2015.) Aina historiallista dataa ei ole saatavilla, esimerkiksi silloin, kun on kyseessä uusi järjestelmä tai merkittävä järjestelmämuutos. Tällöin vertailuanalyysistä voi olla hyötyä, sillä se mahdollistaa toisten samanlaisten järjestelmien ja niiden riskitapahtumien tarkkailun. (Jaradat ym., 2015.)

Tunnistettujen riskien käsittelyyn on neljä eri vaihtoehtoa: riskin välttäminen, vähentäminen, jakaminen esimerkiksi vakuuttamalla ja hyväksyminen (Moeller, 2011). Riskin käsittelytapojen lisäksi riskien haitallisten seurausten vähentämiseen on olemassa kontroleja, jotka voidaan kuvata ennaltaehkäisevinä, korjaavina, ohjaavina ja havainnoivina (Hopkin, 2018). Kontrolli voidaan määritellä toimenpiteenä, joka ylläpitää ja/tai muuttaa riskiä. Ne sisältävät, mutta eivät rajoitu, mihin tahansa prosessiin, politiikkaan, laitteeseen, käytäntöön tai muihin olosuhteisiin, jotka ylläpitävät ja/tai muuttavat riskiä. (ISO, 2018.) Ennaltaehkäisevät kontrollit on suunniteltu rajoittamaan ei-toivottujen haittatapahtumien mahdollisuutta. Korjaavat kontrollit on suunniteltu korjaamaan ei-toivottuja olosuhteita ja vähentämään hyväksymättömiä riskialtistuksia. Näiden avulla riskiä käsitellään siten, että sen todennäköisyys vähenee ja/tai vaikutus vähenee huomattavasti. Ohjaavat kontrollit on puolestaan suunniteltu varmistamaan, että tietty lopputulos saavutetaan ja ne voivat myös liittyä toimiin, jotka on vahinkotilanteessa suoritettava vahinkojen rajoittamiseksi. Havainnoivat kontrollit on suunniteltu tunnistamaan tilanteet, joissa ei-toivottu lopputulos on tapahtunut varmistaen, että olosuhteet eivät huonone entisestään. (Hopkin, 2018.)

3.3 Kokonaisvaltainen riskienhallinta ERM

Yrityksen kokonaisriskiprofiili riippuu markkina-, luotto- ja operatiivisten riskien lisäksi myös muista riskiluokista sekä strategisista ja maineeseen liittyvistä riskeistä ja kaikkien näiden välisistä suhteista. Riskien kompleksisuuden ja monimutkaisten yhteyksien vuoksi osa yrityksistä hyödyntää kokonaisvaltaista riskienhallintaa (ERM), jonka osana voidaan hallita myös operatiivisia riskejä. (Girling, 2020.) Sen avulla voidaan saada laajempi näkemys riskeistä ja tunnistaa mahdolliset haitalliset tapahtumat sekä niiden kokonaisvaikutukset. Kokonaisaltistus haitalliselle tapahtumalle voi olla suurempi tai pienempi kuin tulos, joka saadaan arvioimalla kutakin riskityyppiä erikseen. (Hull, 2018.)

COSO (2023) määrittelee yrityksen kokonaisvaltaisen riskienhallinnan (ERM) seuraavasti: ”Kulttuuri, kyvykkyydet ja käytännöt, jotka yhdistyvät strategian asettamiseen ja sen toteuttamiseen, ja joita organisaatiot hyödyntävät hallitakseen riskejä arvon luomiseksi, säilyttämiseksi ja toteuttamiseksi”. Alkuperäinen COSO ERM-kuutio julkaistiin vuonna 2004 ja sen mukaan yritysten riskienhallinta on monisuuntainen, iteratiivinen prosessi, jossa lähes mikä tahansa komponentti voi vaikuttaa ja vaikuttaakin

kaikkiin muihin komponentteihin. (Hopkin, 2018.) Myöhemmin kuutiomuodosta on luovuttu ja COSO ERM -viitekehys rakentuu viidestä toisiin liittyvästä osasta, jotka ovat: hallinto ja kulttuuri, strategian ja tavoitteiden asettaminen, suorituskyky, arviointi ja tarkistus sekä tiedonvälitys, viestintä ja raportointi (COSO, 2023).

ERM painottaa ylhäältä alas -lähestymistapaa, jolloin johdon ja hallituksen vastuu esimerkiksi erilaisten riskiskenaarioiden todennäköisyyksien ja vaikutusten arvioinnista suhteessa yrityksen riskistrategiaan kasvaa. (Fraser & Simkins, 2010.) Kyseisessä lähestymistavassa määritellään organisaation kokonaisriskin sietokyky, jota käytetään riskirajojen määrittämiseen eri organisaation osille. Päinvastoin alhaalta ylös -lähestymistavassa keskitytään liiketoimintayksiköiden kantamien riskien arviointiin ja niiden yhdistämiseen. Käytännössä rahoituslaitoksen on kuitenkin hyödynnettävä näitä molempia lähestymistapoja määrittääkseen kokonaisriskin sietokykynsä ja arvioidakseen, ovatko liiketoimintayksiköiden ottamat riskit linjassa tämän riskin sietokyvyn kanssa. (Hull, 2018.)

Kokonaisvaltaisen riskienhallinnan tavoitteena on lisätä todennäköisyyttä siitä, että organisaatio saavuttaa tavoitteensa hallitsemalla riskit sidosryhmien riskinsietokyvyn rajoissa samalla luoden arvoa sidosryhmille. ERM täytyy huomioida myös organisaation oma riskinsietokyky, joka tarkoittaa riskiä, jonka ottamisen organisaatio katsoo olevan sille sopivaa tai vältettävää. Riskiensietokykyä määriteltessä organisaation tulee pohtia sen suhtautumista riskeihin, tavoitteitaan, riskienhallintansa tasoa ja kustannuksia sekä tappionsietoa. (Fraser & Simkins, 2010.) Rahoituslaitoksen riskinsietokyvyn yksi ulottuvuus liittyy todennäköiseen tappioon, jonka se on valmis kestämään pahimmassa skenaariossa. Tämä voidaan ilmaista koko yritystä koskevana Value at Risk (VaR) tai odotetun tappion mittarina (Hull, 2018). Riskinsietokykynsä selvittämällä organisaatio saa selville myös hyväksyttävän riskialtistuksen määrän ja laadun. Lisäksi organisaatio voi vertailla todellisia riskialtistuksiaan sallittuihin altistuksiin ja arvioida hallitseeko se tiettyä riskiä sopivissa määrin. (Fraser & Simkins, 2010.) Kun riskirajat on asetettu, on tärkeää myös seurata liiketoimintayksiköiden tekemiä päätöksiä sen varmistamiseksi, että rajoja noudatetaan. Yksi riskinsietokyvyn tärkeä osa on keskittymäriski, johon riskinsietokyvyn tulisi suoraan tai epäsuorasti vaikuttaa. (Hull, 2018.) Riskinsietokyky tulisi määritellä organisaation laatimassa politiikassa, jotta odotukset eri riskilähteiden tai -kategorioiden hallinnasta olisivat virallisia. (Fraser & Simkins, 2010.)

Rahoituslaitoksen riskikulttuuri liittyy siihen, miten päätöksiä tehdään. Tavoitteena on tehdä päätökset kurinalaisesti, punniten tarkasti mahdollisia lopputuloksia ja arvioida riskejä suhteessa odotettuihin hyötyihin. Tämä ei kuitenkaan tarkoita riskien välttämistä kokonaan vaan niiden huomioimista suhteessa mahdollisiin hyötyihin ja organisaation riskinottohaluun (risk appetite). (Hull, 2018.) Riskinottohalu voidaan määritellä tasoksi ja riskityypeiksi, joita yritys on valmis ottamaan ennalta päätetysti ja riskinkantokyvyn puitteissa saavuttaakseen strategiset tavoitteensa ja liiketoimintasuunnitelmansa. Riskinkantokyky puolestaan viittaa yrityksen kykyyn sietää riskiä. (Girling, 2022.) Riskikulttuurin keskeinen elementti on varmistaa, että keskipitkän ja pitkän aikavälin riskit otetaan huomioon arvioitaessa mahdollisuuksia, jotka tarjoavat lyhyen aikavälin voittoja (Hull, 2018).

Rahoituslaitoksen nykyisen toiminnan ja mahdollisten strategisten sijoitusten merkittävien riskien tunnistaminen on tärkeä osa kokonaisvaltaista riskienhallintaa. Organisaation riskinottohalukkuus tulisi määritellä ylimmältä tasolta ja hallituksen tulisi hyväksyä se. Tämän jälkeen tulee varmistaa, että eri liiketoimintayksiköiden riskienhallinta on yhdenmukaista koko organisaation riskinottohalukkuuden viitekehyksen kanssa ja että otetut riskit pysyvät riskinottohalukkuuden mukaisina. Riskienhallinnassa voi olla joskus tarve luopua tietyistä toiminnoista, jakaa riskiä esimerkiksi vakuuttamalla, ottaa käyttöön toimenpiteitä riskien vaikutuksen vähentämiseksi tai hyväksyä riskejä osana organisaation riskinottohalukkuutta (Hull, 2018.) Lisäksi tunnistettuihin riskeihin tulisia kohdentaa resursseja, mikä edellyttää kattavan liiketoimintakehyksen kehittämistä, käyttöönottoa ja jatkuvaa parantamista. Tarkoituksena on yhdistää organisaation tärkeä data, asiantuntemus, kokemus ja saatavilla oleva tieto koko yrityksenlaajuiseksi prosessiksi. (Fraser & Simkins, 2010.)

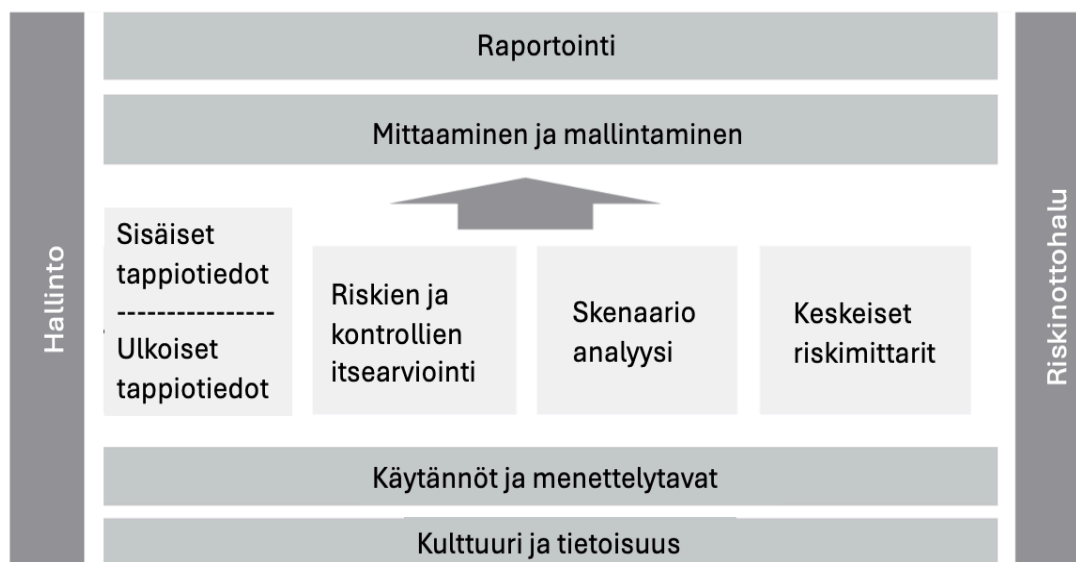
3.4 Pankkien operatiivisten riskien hallinta

Baselin pankkivalvontakomitean määritelmän mukaan digihuijaukset kuuluvat operatiivisiin riskeihin, ja niillä voi olla useita syitä (Hull, 2018). Operatiivinen riski edellyttää tappion eli taloudellisen menetyksen olemassaoloa, joten on oletettava, että tappiota saattaa syntyä (Girling, 2022). Operatiiviset riskit voidaan jakaa korkean frekvenssin matalan vakavuuden riskeihin ja matalan frekvenssin korkean vakavuuden

riskeihin, joista aiemmin mainitut on helpompi määrittää. (Hull, 2018). Digihuijaukset kuuluvat volyyminsa vuoksi korkean frekvenssin ja matalan vakavuuden riskeihin, mutta joissain tapauksissa niillä voi olla myös mittavia seurauksia. Tarkemmin digihuijaukset kuuluvat Baselin pankkivalvontakomitean määritelmän mukaan ulkoisten petosten riskiluokkaan, johon kuuluvat kolmannen osapuolen tekemät teot, joilla on tarkoitus huijata, väärinkäyttää omaisuutta tai kiertää lakia. (Hull, 2018.) Digihuijaukset voidaan luokitella kuuluviksi myös kyberriskeihin, jotka ovat operatiivisia riskejä. Tarkemmin ne voidaan luokitella aiheutuviksi ihmisten toimesta ja edelleen alakategoriana on tahallisuus. (Cebula & Young, 2010.)

Operatiivisen riskin hallintakehyksen tulisi sisältää operatiivisen riskin tunnistamiseen, mittaamiseen ja seurantaan, raportointiin, kontrollointiin ja riskien vähentämiseen liittyvät kehykset (Hopkin, 2018). Operatiivinen riski on noussut erityiseksi haasteeksi finanssilaitoksissa, sillä se on olennainen osa liiketoimintaa ja finanssilaitosten on mitattava ja kvantifioitava kohtaamansa operatiivisen riskin taso pääomavaatimusten täyttämiseksi (Hopkin, 2018; Hull, 2018). Operatiivisessa riskissä onkin kaksi osittain päällekkäistä puolta: operatiivinen riskienhallinta ja operatiivisen riskin mittaaminen (Girling, 2022).

Määrällisen lähestymistavan lisäksi onnistunut operatiivisen riskin hallintaohjelma sisältää myös laadulliset lähestymistavat varmistukseksi, että operatiivinen riski mitataan asianmukaisesti ja hallitaan tehokkaasti (Girling, 2022). Basel III toisen pilarin suosituksen mukaan pankin sisäisen pääoman riittävyyden arviointiprosessin (ICAAP) periaatteen 1 mukaan pankilla tulee olla integroitu lähestymistapa riskien- ja pääomanhallintaan, mihin kuuluu riskitason ja -halukkuuden arviointi sekä pääoman määrän ja laadun varmistaminen pankin riskiprofiilin mukaisiksi (BIS, 2019). Osa pankeista käyttää riskienhallinnassaan apuna riskienhallintastandardeja, kuten ISO 31000, IRM-standardi ja COSO ERM -standardi (Hopkin, 2018). Girlingin (2023) mukaan yleisesti kaksi elementtiä eli hallinto sekä kulttuuri ja tietoisuus ohjaavat operatiivisen riskin kehyksen suunnittelua. Kuviossa 3 on esitetty operatiivisten riskienhallinnan viitekehys, jossa nämä elementit ovat.



Kuvio 3 Operatiivisten riskien viitekehys, mukailten Girling (2022)

Hallinto määrittelee operatiivisen riskin toiminnon päällikön, kehystä hallitsevan tiimin roolit ja vastuut, riskienhallinnan päätöksenteosta vastaavat komiteat, liiketoimintalinjojen operatiivisen riskin johtajat sekä työntekijät, jotka voivat kohdata operatiivisia riskejä. Asianmukainen hallintorakenne tehostaa operatiivisen riskin hallintaa ja hyvä hallinto varmistaa läpinäkyvän riskienhallinnan jokaisella operatiivisen riskin osa-alueella. Kulttuurin ja riskitietoisuuden kehittäminen ovat tärkeitä, sillä riskien käsittely on pitkälti kiinni asenteista ja taidoista. (Girling, 2022.)

Kehyksen seuraava perustavanlaatuisen elementti on käytännöt ja menettelytavat. Hyvin laadittu politiikkakehys antaa liiketoimintalinjoille lisää joustavuutta, kun ohjeet on ilmaistu yksiselitteisesti. Lisäksi hyvin laaditut käytännöt ja menettelytavat lisäävät pankin autonomiaa, koska ne kasvattavat merkittävästi alan sääntelijöiden luottamusta. (Girling, 2022.)

Kun kehyksen perustavanlaatuiset elementit ovat kunnossa, tarvitaan tehokkaan operatiivisen riskin kehyksen luomiseksi seuraavat päätehtävät: tappiotietojen keruu, riskin ja kontrollin itsearviointi, skenaarioanalyysi ja keskeiset riski-indikaattorit. Tappiotyypit voidaan jakaa sisäisiin, jotka tapahtuvat yrityksen sisällä sekä ulkoisiin, jotka tapahtuvat yrityksen ulkopuolella. Basel III vaatii yritystä laatimaan pääomamallinsa sisäisestä tappioprofiilistaan. Jotta laadukkaita tappiotietoja saadaan, tulee niiden keruun olla tehokasta. Siihen vaikuttaa aiemmin luotu asianmukainen

hallinto sekä kulttuurin ja tietoisuuden rakentaminen. Ulkoiset tappiotiedot eli data samalla liiketoimintasektorilla tapahtuneista tappioista on merkittävässä roolissa, kun pyritään ymmärtämään yrityksen kohtaamaa operatiivista riskiä. Nämä ulkoiset tiedot auttavat informoimaan riskin ja kontrollin itsearviointia sekä skenaarioanalyysiä ja ovat usein tärkeä osa tehokasta raportointia. (Girling, 2022.)

Operatiivisen riskinhallinnan neljästä päätehtävästä toinen on riskin ja kontrollin itsearviointi RCSA (Risk Control and Self-Assessment) (Girling, 2022). Siinä liiketoimintayksiköiden johtajia pyydetään tunnistamaan omat operatiiviset riskinsä esimerkiksi kyselylomakkeen tai arviointikorttien avulla (Hull, 2018). RCSA avulla tunnistetaan ja arvioidaan riskejä ja niiden kontrolleja, tavoitteena hallita ja vähentää hyväksymättömiä riskejä. Tappiotiedot liittyvät jälkikäteen tapahtuvaan analysointiin, kun taas riskin ja kontrollin itsearviointi liittyy ennakoivaan analysointiin. RCSA käsittelee proaktiivisesti sitä, että operatiivisen riskin kehityksen tulisi tunnistaa, arvioida, hallita ja vähentää riskiä. (Girling, 2022.)

Pankkivalvojat ovat tunnistaneet seitsemän erilaista operatiivisen riskin tyyppiä ja kahdeksan eri liiketoiminta-alueetta. Kehittyneimmät pankit pyrkivät määrittämään riskit kullekin 56 riskityypin ja liiketoiminta-alueen yhdistelmälle. Kun operatiivisia riskejä mitataan tai pyritään ymmärtämään erilaisten ohjelmien avulla, kehitetään samalla usein myös keskeisiä riski-indikaattoreita (Key Risk Indicators, KRIs). Tärkeimpien indikaattoreiden avulla seurataan organisaation operatiivisten riskien tasoa ja ne ovat ennakoivia sekä toimivat varhaisina varoitusjärjestelminä. (Hull, 2018.) Keskeinen riski-indikaattori ennustaa, että riski on muuttumassa ja mahdollistaa siten ennakoivan puuttumisen. Eskaloinnin tarpeesta puolestaan kertoo riskirajojen ja -määrien indikaattoreille asettamien kynnyksarvojen ylittyminen. Mittarit puolestaan tarjoavat seurantatoiminnon koko kehityksen yli, sillä niitä voidaan liittää tappiotietoihin, riskeihin tai kontrolliin ja ne voivat tarjota hyödyllistä tietoa skenaarioanalyysiin. Tappiotiedot, RCSA ja keskeiset riski-indikaattorit tarjoavat kaikki tapoja riskitasojen seurantaan. (Girling, 2022.)

Girlingin (2022) mukaan kehityksen viimeinen osa on skenaarioanalyysi, joka etsii vain harvinaisia, katastrofaalisia riskejä toisin kuin RCSA. Skenaarioanalyysin tavoitteena on tunnistaa mahdollisesti kohtalokkaita tai yritykselle vakavia tuhoa aiheuttavia riskejä.

Näitä tunnistetaan pohtimalla hallintakeinojen vakavaa epäonnistumista sekä arvioimalla riskien yhdistelmiä. Basel III pääomamallin yksinkertaistaminen poisti aiemmin Basel II vaatiman skenaarioanalyysin laskennasta, joten nykyisin skenaarioanalyysi on käytössä vain riskienhallintatyökaluna. (Girling, 2022).

Aiemmin käsitellyt mittaaminen ja mallintaminen ovat myös tärkeitä elementtejä operatiivisen riskin kehyksessä. Kaikki nämä elementit vaikuttavat operatiiviseen riskiraportointiin, joka mahdollistaa tappiotiedoista, RCSA-ohjelmasta, skenaarioanalyyseista, mittareista ja pääoman mallintamisesta kerätyn datan hyödyntämisen tehokkaasti. Raportoinnin avulla voidaan tuottaa arvokasta riskianalyysia ja lisätä riskien läpinäkyvyyttä, mikä johtaa parempiin liiketoimintapäätöksiin. (Girling, 2022.)

Riskinottohalun määrittelemisen toimii kehyksen yhdistävänä tekijänä, sillä se antaa kontekstin tunnistetuille ja arvioituille riskeille sekä varmistaa operatiivisen riskin asianmukaisen eskaloinnin ja hallinnoinnin. Alkuperäisissä Basel II -asiakirjoissa ei kuitenkaan annettu juuri ohjeistusta operatiiviseen riskinottohaluun liittyen, mutta nyt sääntelijät ovat antaneet lisäohjeistusta, jossa korostetaan hallituksen, ylimmän johdon ja liiketoimintayksiköiden roolia riskinottohalun määrittelyssä ja hallinnassa. Tämä ohjeistus on osoittautunut hyödylliseksi, ja yritykset ovat alkaneet edistyä tässä kehyksen osa-alueessa, vaikka käytännöt vaihtelevatkin laajasti. Basel II sääntelyn toisen pilarin mukaan operatiivisen riskin kehyksen tulisi kattaa pankin riskinottohalu ja toleranssi operatiiviselle riskille, kuten riskinhallintaa koskevissa politiikoissa on määritelty. (Girling, 2022.)

Operatiivisen riskin hallinta perustuu määriteltyyn riskinottohaluun, joka kehittyy yleensä operatiivisen riskiohjelman myötä. Kun operatiivisia riskitapahtumia koskevaa tietoa kerätään, johto voi arvioida, onko tietty tappiotaso hyväksyttävä. Riskien itsearviointien yhteydessä osallistujat kertovat, kokevatko he riskit suuriksi ja vaativatko ne vähentämistoimenpiteitä vai ovatko riskit hyväksyttävällä tasolla. Skenaariotyöpajoissa määritellään pahimmat mahdolliset tapahtumat ja arvioidaan lisätoimien tarvetta. Samoin keskeisiä riskimittareita suunnitellaan ja kerätään siten, että niille määritellään kynnsarvot, jotka heijastavat hyväksyttävää riskitasoa. Näin ollen

operatiivisen riskin kehys itsessään tukee riskinottohalun kehitystä ja tarkentumista. (Girling, 2022.)

Operatiivisen riskin hallinnan olennainen osa on ennaltaehkäisy, johon on useita keinoja. Eräs tapa on tunnistaa päätösten ja tappioiden välillä syy-seuraussuhteita, joita voidaan havaita esimerkiksi tilastollisen analyysin perustella. (Hull, 2018). Operatiivista riskiä voidaan hallita myös kouluttamalla työntekijöitä sähköposteihin ja puheluihin vastaamisessa, sillä esimerkiksi oikeustapaukset, joissa väitetään rahoituslaitoksen toimineen epäasiallisesti tai laittomasti, ovat merkittävä operatiivisen riskin lähde. (Hull, 2018.) Tähän liittyen finanssilaitoksen sisäisen tarkastuksen on tärkeää varmistaa, että käytännön toimintatavat ja prosessit itsessään ovat tehokkaita operatiivisen riskin vähentämiseksi. (Hopkin, 2018.) Tärkeää on lisäksi päättää, missä määrin operatiivista riskiä vakuutetaan. Pankki joutuu aina kuitenkin kantamaan osan riskistä itse, sillä useimmat vakuutukset sisältävät esimerkiksi omavastuita ja vakuutuskattoja. Vakuutusmaksujen kehitys riippuu todennäköisesti myös korvausvaatimuksista ja muista indikaattoreista, jotka osoittavat, kuinka hyvin operatiiviset riskit on hallittu. (Hull, 2018.)

On yleisesti hyväksyttyä, että operatiivisiin riskeihin liittyvät kysymykset tulisi sisällyttää rahoituslaitoksen johtamiseen (Hopkin, 2018). Minkä tahansa operatiivisen riskiohjelman menestyksen kannalta on avainasemassa ylimmän johdon tuki. Baselin pankkivalvontakomitea on tästä tietoinen ja suosittelee, että pankin hallitus osallistuu riskienhallintaohjelman hyväksyntään ja tarkistaa sen säännöllisesti. (Hull, 2018.)

Liiketoimintayksiköiden tulisi pyrkiä tekemään oikeat laskelmat ja määrittämään optimaalinen operatiivisen riskin taso, joka maksimoi pääoman tuoton. Operatiivisen riskien pääomien allokoinnilla voidaan kannustaa liiketoimintayksiköitä parantamaan riskien hallintaansa. Yksikön pääoman tuotto kasvaa, mikäli se on ryhtynyt toimenpiteisiin jonkin riskin esiintymistiheyden ja vakavuuden vähentämiseksi, jolloin sille kohdistetaan vähemmän pääomaa. Kuitenkaan aina operatiivisen riskin vähentäminen ei ole optimaalista, mikäli kustannukset ylittävät pienentyneen pääoman tuottaman hyödyn. (Hull, 2018.)

3.5 Kyberriski operatiivisena riskinä

Kyberriski tarkoittaa kyberhyökkäysten todennäköisyyden ja niiden vaikutuksen yhdistelmää (FSB, 2023). Termi "kyber" liittyy elektronisiin viestintäverkkoihin ja virtuaalitodellisuuteen. Näistä virtuaalitodellisuus korostaa aineetonta luonnetta, mikä tekee tappioiden arvioinnista haastavaa. Toiseksi verkot liittyvät läheisesti termiin kyberavaruus, jota käytetään usein internetin synonyyminä. Vaikka internet saattaa olla kyberuhkien pääasiallinen lähde, kyberavaruus kuvaa jokaista verkkoa, joka yhdistää IT-järjestelmiä, kuten LAN. (Eling & Schnell, 2016.) Kyberriskit voidaan määritellä operatiivisiksi riskeiksi, jotka kohdistuvat tieto- ja teknologiavaroihin ja joilla on vaikutuksia tiedon ja tietojärjestelmien luottamuksellisuuteen, saatavuuteen ja eheyteen. (Cebula & Young, 2010.) Kokonaisuudessaan operatiivinen riski kattaa tappiot, joita pankki kärsii puutteellisten tai epäonnistuneiden sisäisten prosessien, ihmisten tai järjestelmien vuoksi tai ulkoisten tapahtumien seurauksena, ja myös kyberriskit voidaan kategorisoida näihin neljään luokkaan niiden syyn mukaan (BCBS, 2021; Cebula & Young, 2010.) Tämän lisäksi ne voidaan luokitella toiminnan rikollisuuden mukaan, hyökkäyksen tyyppin ja lähteen mukaan. (Cebula & Young, 2010.)

ENISA on arvioinut vuoden 2024 merkittävimpien kyberuhkien olevan kiristys- ja haittaohjelmat, sosiaalinen manipulointi, dataan kohdistuvat uhat, palvelunestohyökkäykset, tiedon manipulointi ja häirintä sekä toimitusketjuhyökkäykset. Uusia tunnistettuja trendejä ovat esimerkiksi kyberrikollisuuden tekoälytyökalut, joita hyödynnetään huijausviestien kirjoittamisessa sekä kiristysohjelmat. (ENISA, 2024.)

Kyberrikollisuusekosysteemi on yhä teollistuneempi ja tarjoaa teknisesti taitamattomille rikollisille keinoja käyttää kybertyökaluja ilman teknistä asiantuntemusta, sillä esimerkiksi pimeän verkon markkinapaikoilla voi ostaa ja myydä maksukorttien tietoja ja verkkopankkitunnuksia. Petosten ja iskujen toteuttamiseen käytettävät tekniikat ovat yhä kehittyneempiä, sillä haitallisten koodien avulla voidaan ohittaa kaksivaiheinen todennus tai muut turvatoimet. (BCBS, 2023.)

3.6 Pankkien kyberturvallisuus

Rahoituslaitoksiin kohdistuva kyberriski johtuu useista tekijöistä, kuten kehittyvästä teknologiasta, joka voi aiheuttaa uusia tai kasvavia haavoittuvuuksia; rahoituslaitosten ja ulkopuolisten osapuolten, kuten pilvipalvelujen ja FinTech-palveluntarjoajien, välisistä yhteyksistä; kyberrikollisten määrätietoisista pyrkimyksistä löytää uusia keinoja tietojärjestelmien vaarantamiseen; sekä rahoituslaitosten houkuttelevuudesta kohteena kyberrikollisille, jotka tavoittelevat laitonta taloudellista hyötyä. (FSB, 2018.) Transaktiomäärien massiivinen kasvu sekä kyberrikollisuuden ja hakkerointihyökkäysten lisääntyminen ovat myös lisänneet pankkien kyberriskiä entisestään (Hasham ym., 2019). Tehokkaan kyberturvallisuusarkkitehtuurin kehittämiseksi on olennaista ymmärtää nykyinen uhkataso yksityiskohtaisesti, mukaan lukien tiettyjen uhkatoimijoiden tyypit ja heidän motivaationsa sekä yleiset taktiikat. Uhkien tuntemus on tärkeää paitsi puolustuksen rakentamiseksi myös riittävän rahoituksen perustelemiseksi puolustusratkaisuille. Syvälinen ymmärrys vaikuttavista kyberuhkista tulee jakaa liiketoimintajohdolle resurssipäätösten tukemiseksi. (Bayuk & Rohmeyer, 2018.)

Kyberuhkat rahoitusorganisaatioille ovat monimutkaisia, monimuotoisia ja mahdollisesti vakavia, ja niiden syvälinen analysointi on välttämätöntä organisaation kyberturvallisuuspolitiikan, toimintasuunnitelmien ja lopulta strategioiden perustaksi. Uhkatiedustelu ja uhkamallinnus ovat olennaisia keinoja kyberuhkien kartoittamisessa. Uhkatiedustelu tarkoittaa tietojen keräämistä ajankohtaisista kyberuhkista ja -toimista ja sen lähteitä on runsaasti saavilla niin kutsutuista avoimen lähdekoodin tietolähteistä (OSINT), joita ovat esimerkiksi julkaistut tutkimusraportit, uutiset, verkkosivut, blogit ja videot. Haasteena on kuitenkin valtava tietomäärä, sillä nykyisenä ”big data” -aikakautena avointen lähteiden seurantaan vaadittava resurssimäärä on kasvanut merkittävästi. Sosiaalisen median tietojen kasvanut määrä on luonut sosiaalisen median tiedusteluksi (SOCMINT) kutsuttavan OSINT-lajin. Sen avulla voidaan löytää viestejä, jotka sisältävät kontekstuaalisia ja kuvailevia tietoja, jotka rikastavat uhkatietojen perustaa. Valtavan tietomäärän hallitsemiseksi on kehitetty menetelmiä ja työkaluja avoimen lähdekoodin tiedon suodattamiseen ja jalostamiseen, kuten palveluita, jotka seulovat suuren määrän potentiaalista uhkatietoa ja esittelevät organisaatiolle sen kannalta tärkeimmät havainnot. Uhkamallinnus on hyvin tarkka riskienarviointimalli ja se alkaa organisaation arvokkaimpien tietojärjestelmien ja -resurssien eli omaisuuserien

kartoittamisesta. Tämän jälkeen tulee määritellä resurssien ominaisuudet, maantieteellinen sijainti sekä sijainti laitteiden ja säilytystilojen osalta. Kartoituksen jälkeen organisaation tulisi järjestää työpajoja erilaisten hyökkäysvektorien tunnistamiseksi ja analysoimiseksi. Hyökkäysvektorien eli hyökkääjän mahdollisten reittien tunnistamisessa voidaan hyödyntää uhkatiedustelun avulla kerättyjä tietoja. Tämän jälkeen uhkamallinnuksen tietoja voidaan hyödyntää sovittamalla riskin lieventämistoimia tunnistettuihin vektoreihin. (Bayuk & Rohmeyer, 2018.)

Rahoitusjärjestelmän arkkitehtuurin kaikilla osa-alueilla esiintyy riskejä. Järjestelmien välinen yhteensopivuus ja liitettävyys tuo mukanaan uusia haavoittuvuuksia, jotka voivat johtaa laajamittaisiin vaikutuksiin erityisesti niissä organisaatioissa, jotka ovat tiiviisti kytketyneet toisiinsa. (Bayuk & Rohmeyer, 2018.) Haavoittuvuudella tarkoitetaan resurssissa tai kontrollissa olevaa heikkoutta, alttiutta tai virhettä, jonka yksi tai useampi uhka voi hyödyntää (FSB, 2023). Haavoittuvuusarviointi on lähtökohta järjestelmän ja sen teknisten, prosessiin liittyvien ja inhimillisten ulottuvuuksien heikkouksien laadun ja laajuuden selvittämiseksi (Bayuk & Rohmeyer, 2018). Sillä tarkoitetaan tietojärjestelmän, sen hallintakeinojen ja prosessien systemaattista tarkastelua, jonka tarkoituksena on arvioida turvallisuustoimenpiteiden riittävyyttä, tunnistaa turvallisuuspuutteita sekä tarjota tietoa, jonka avulla voidaan ennustaa ehdotettujen turvallisuustoimenpiteiden tehokkuutta, ja varmistaa kyseisten toimenpiteiden riittävyys toteutuksen jälkeen (FSB, 2023). Kunkin yksittäisen haavoittuvuusarvioinnin tulisi heijastaa arvioitavan järjestelmän erityisluonnetta, joten huomioon tulisi ottaa muun muassa käyttöön otetun teknologian suhteellinen kehittyneisyys, prosessi-innovaatioiden aste ja uusien teknologisten kehysten tuki. (Bayuk & Rohmeyer, 2018.)

Tunnistettujen haavoittuvuuksien avulla voidaan tunnistaa riskejä, joihin voidaan liittää kontroleja. On olemassa tietoturvakontroleja, jotka on suunniteltu havaitsemaan, kun ennaltaehkäisevät kontrollit epäonnistuvat, ja/tai palauttamaan ennaltaehkäisevistä kyberturvallisuuskontroleista tapahtuneet rikkomukset. On kuitenkin tärkeää ymmärtää, että havaitsemis- ja palautusmekanismit eivät ole ensimmäiset kontrollit, jotka rikotaan kyberhyökkäyksessä. Jotta tällaiset kontrollit voidaan ottaa käyttöön, ennaltaehkäisevässä kontrollissa on jo tapahtunut rikkomus. Tämän vuoksi kyberhyökkäysten välitön tunnistaminen ja korjaaminen on tärkeää. Täten teknologiainfrastruktuurissa tulee olla kyberturvallisuuskontrolliympäristö, joka on

sisäistetty tai ulkoistettu, suunniteltu tai syntynyt tilanteen myötä. Jos ympäristö on suunniteltu, tiedetään tai voidaan tietää, kuinka hyvin tiedot ovat suojattuja kyberuhilta. Ero tunnetun ja tiedettävän välillä on se, että tunnettu tarkoittaa jo toteutettuja mittauksia tietotekniikkakontrolliympäristön ominaisuuksista, jotka on perustettu suunnitelman pohjalta. Jos taas ympäristö ei ole suunniteltu, tiedon suojaustaso ei ole oikeasti tiedettävissä, ja on hyvin todennäköistä, että tiedot ovat äärimmäisen haavoittuvia. Haavoittuvuuksia voidaan arvioida esimerkiksi skenaarioanalyysin avulla. (Bayuk & Rohmeyer, 2018.)

Yksi keskeinen kyberriskien hallinnan periaate on, että kyberriski ei ole pelkästään IT-osaston vastuulla, vaan se vaatii osastojen välistä, laajaa yhteistyötä. Lisäksi institutionaalinen sitoutuminen on erittäin tärkeää. Yrityksillä, joilla on tietoturvaajohtaja tai vastaava rooli, on keskimäärin pienemmät kustannukset tietomurron sattuessa. (Bayuk & Rohmeyer, 2018.)

Uusi uhkakuvaympäristö johtaa tilanteeseen, jossa hakkerit kehittävät entistä älykkäämpiä ja kehittyneempiä haittaohjelmia ja hyökkäystekniikoita. Näin ollen tietoturva-ammattilaisten on luotava uusia tietoturvaparametreja kehittämällä perinteisiä suojautumistapoja ja -arkkitehtuureja. Näiden uusien paradigmaattisten suojamenetelmien tulee tarjota luotettavampia keinoja määrittellä ja valvoa ihmisen identiteettiä. (Awad, Traoré & Woungang, 2017.) Pankit, jotka alkavat mukauttaa toimintaansa talousrikollisuuden muuttuviin piirteisiin, kohtaavat kyberrikkomusten ja useimpien talousrikosten välisten yhteyksien syvenemisen. Aiemmin suurin osa petoksista on ollut transaktiopohjaisia, ja rikolliset ovat hyödyntäneet valvontajärjestelmien heikkouksia, jolloin pankit ovat torjuneet tällaisia petoksia suhteellisen suoraviivaisilla, kanavakohtaisilla ja yksittäisiin seikkoihin kohdistuvilla valvontakeinoilla. Viime aikoina identiteettipohjaiset petokset ovat kuitenkin yleistyneet, kun petostentekijät kehittävät sovelluksia hyödyntääkseen luonnollisia tai synteettisiä tietoja. Kyberhyökkäykset ovat entistä laajempia, mikä heikentää henkilötietojen ja tietoturvan arvoa. Asiakkaat ovat yhä enemmän pankkiin yhteydessä yksinomaan digitaalisten kanavien kautta, joten digitaalinen luottamus on nopeasti noussut merkittäväksi asiakaskokemuksen erilaistavaksi tekijäksi. Turvallinen ja tehokas digitaalinen käyttöliittymä voi täten vaikuttaa positiivisesti pankkien liikevaihtoon. (Hasham, Joshi & Mikkelsen, 2019.) Koska digitaalinen identiteetti on keskeinen

kaikessa laitteilla tapahtuvassa toiminnassa, on olennaista varmistaa sen eheys ja aitous. Haitallisten toimintojen lisääntyvän automaation vuoksi on myös tärkeää määrittellä luotettavia tunnisteita ja malleja, jotka paljastavat automaattiset, haitalliset toimet ja botit. Samalla on tärkeää erottaa ihmisen suorittamat toimet robottiohjatusta automaatiosta. (Awad, Traoré & Woungang, 2017.) Pankit tarjoavat asiakkailleen nykyisin monivaiheista tunnistautumista, jonka käyttöönotto hankaloittaa merkittävästi rikollisten tietojenkalastelumahdollisuuksia. Monivaiheinen tunnistautuminen (Multi-factor Authentication, MFA) tarkoittaa henkilön identiteetin varmistamista useampaa eri tunnistautumistapaa käyttämällä. Kaksivaiheinen tunnistautuminen (2FA) on yleisin monivaiheisen tunnistautumisen muoto. Monivaiheisen tunnistautumisen avulla rikollinen ei pääse kirjautumaan pankkitilille ilman lisätunnistetta, vaikka olisi saanut haltuunsa käyttäjätunnuksen ja salasanan. (Kyberturvallisuuskeskus, 2024.)

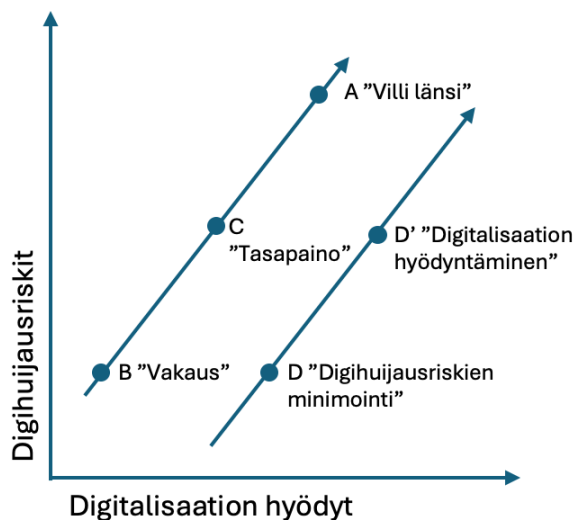
3.7 Pankkien riskienhallinta digihuijaustapauksissa

Digihuijaukset voivat sisältyä muun muassa operatiivisiin riskeihin, teknologiariskeihin sekä rahanpesu- ja terrorisminrahoitusriskeihin. (BCBS, 2023). Huijausten vaikutukset eivät rajoitu pelkästään rahallisiin tappioihin, vaan rikokset voivat aiheuttaa myös vakavia sosiaalisia ja taloudellisia seurauksia. (FATF, 2023). Täten niiden riskienhallintamalli voi poiketa eri pankeissa, mutta pääosin riskienhallinnan prosessit ja kontrollit pohjautuvat sääntelyyn sekä kyberriskien hallintaan, joka on osa kokonaisvaltaista riskienhallintaa (ERM). Näiden lisäksi aiemmin käsitelty operatiivinen riskienhallinta antaa keinoja myös digihuijausten hallintaan. Kyberriskien hallinnalla on toisinaan kuitenkin omia erityispiirteitä. Vaikka pankeilla onkin kehittyneet järjestelmät suojautua kyberhyökkäyksiltä, on hyökkäysten luonne ja monimuotoisuus jatkuvassa muutoksessa. (Hull, 2018.) Etenkin digihuijausten määrän ja tappioiden merkittävyyden kvantifioiminen on haastavaa johtuen tietojen haasteista sekä valtioiden sisällä että niiden välillä. Näihin haasteisiin kuuluvat tiedon puutteet, yhdenmukaisten ja vertailukelpoisten määritelmien puute sekä erot siinä, miten tietoja kerätään eri viranomaisten ja oikeudenkäyttöalueiden kesken. (BCBS, 2023.)

Digihuijauksiin liittyvässä riskienhallinnassa keskeistä on se, miten hyödyntää teknologisten pankkikehitysten etuja samalla kun tunnistetaan, seurataan, hallitaan ja vähennetään digihuijausten riskejä asianmukaisesti suunnitelluilla ja toteutetuilla

valvontakäytännöillä. Maksimaalinen pyrkimys yhä suurempaan digitalisaation voi tuottaa suurempia hyötyjä verkkopankkipalveluissa, mutta toisaalta se voi tapahtua digitaalisten petosriskien kustannuksilla. Toinen ääripää eli paluu analogiseen pankkijärjestelmään ainakin vähentäisi merkittävästä digitaalisten petosten riskejä mutta lopputulos tapahtuisi digitaalisen pankkitoiminnan hyötyjen menettämisen kustannuksella. Tasapainon löytäminen digihuijausriskien vähentämisessä ja digitalisaation sopivan tason löytämisessä voi edellyttää: (i) teknologian parempaa hyödyntämistä valvontatoimien nopeuden ja tehokkuuden lisäämiseksi; (ii) pankkien asiakkaiden tietoisuuden lisäämistä digitaalista petosta kohtaan; (iii) teknologian parempaa hyödyntämistä digitaalisten pankkipalveluiden turvallisuuden parantamiseksi; (iv) suurten tietoaaineistojen, tekoälyn käyttöä regtech- ja suptech-innovaatioissa; (v) tietojen ja tiedustelutiedon jakamisen parantamista asiaankuuluvien sidosryhmien kesken. (BCBS, 2023).

Kuvion 4 vasemmanpuoleinen osoittava viiva edustaa nykyistä maailmantilaa. Viivan siirtyessä oikealle digitalisaation hyödyt voidaan saavuttaa pienemmillä digihuijausriskien tasoilla, mikä on useiden toimijoiden tavoitteena. (BCBS, 2023).



Kuvio 4 Finanssialan digitalisaation hyödyt ja petosriskit, mukaillen BSBS (2023)

Keskeistä on myös digitaalisten petosten pankkijärjestelmille ja pankeille aiheuttamien riskien hallinta. Digihuijaukset voivat aiheuttaa pankille taloudellisia tappioita, jotka pankit itse kärsivät esimerkiksi siirrettyään tietämättään varoja petollisille osapuolille tai

joiden vuoksi niiden on palautettava asiakkailleen varoja esimerkiksi korvattuaan asiakkailleen niiden kärsimiä tappioita. Äärimmäisissä tapauksissa tällaiset tappiot voivat vähentää pankkien pääomaresursseja ja iskuvaimennuskykyä, mikä voi vaikuttaa muihin pankkeihin tai markkinatoimijoihin. (BCBS, 2023.) Maksupalvelulain 63 §:n mukaista pankin velvollisuutta korvata menetetyt varat asiakkaalleen sovelletaan kuitenkin ainoastaan, mikäli kyseinen maksutapahtuma on oikeudeton, eli tehty ilman asiakkaan suostumusta. Mikäli asiakas on itse vahvistanut eli hyväksynyt maksun, ei kyse ole maksuvälineen oikeudettomasta käytöstä eikä pankki ole korvausvastuussa, vaikka asiakas olisi vahvistanut maksun harhaan johdettuna ja tultuaan huijatuksi. (FINE, 2024.) Kuluttajariitalautakunnan (2019) mukaan kuluttajan vastuu verkkopankkitunnusten väärinkäytöksistä on suuri, sillä pankilla ei ole vastuu korvata vahinkoja lainkaan, mikäli kuluttaja on ollut törkeän huolimaton. Tunnukset mahdollistavat tilillä olevien varojen ja luottojen käyttämisen, maksukortin nostorajan muuttamisen ja pikaluottojen hakemisen. Kuluttaja saattaa menetettyjen varojen lisäksi joutua vastaamaan kokonaan uusista luotoista. Maksupalvelulain mukaan 7 luvun 62 pykälän mukaan kuluttajan maksettavaksi tulee 50 euroa, mikäli tapahtunut oikeudeton maksuvälineen käyttö on johtunut sen huolimattomasta säilytyksestä tai mikäli kuluttaja on laiminlyönyt velvollisuutensa ilmoittaa palveluntarjoajalle maksuvälineen katoamisesta tai oikeudettomasta joutumisesta toisen haltuun. Oikeudettomasta käytöstä maksuvälineen haltijan tulee vastata täysin itse, mikäli hän on toiminut törkeän huolimattomasti tai tahallisesti. Mikäli huijari on nostanut luoton siten, etteivät varat ole kulkeneet pankkitilin kautta, tulee maksupalvelulain sijaan sovellettavaksi tunnistuslaki, jossa ei ole lainkaan kuluttajan vastuurajoitusta ja kuluttaja voi joutua vastaamaan luoton täydestä määrästä, vaikka hänen huolimattomuutensa ei olisi ollut törkeää. (Kuluttajariitalautakunta, 2019.)

Taloudellisten tappioiden lisäksi digihuijaukset voivat aiheuttaa pankeille ja valvojille mainehaittaa, joka johtuu korkean profiilin digihuijaustapauksista esimerkiksi laajan lehdistönäkyvyyden vuoksi. Tämä voi johtaa laajempaan luottamuksen menetykseen pankkien eheyttä ja kestävyyttä kohtaa, mikä voisi ääritapauksessa johtaa esimerkiksi massiivisiin pankkitalletusten nostamisiin. (BCBS, 2023.) Tämän lisäksi mainehaittaa saattaa lisätä se, että huijauksia toteutetaan myös pankkien nimissä, mikä saattaa heikentää asiakkaiden luottamusta ja vähentää halukkuutta käyttää pankin palveluita, vaikka se ei olisikaan vastuussa huijauksista.

Pankkien asiakkaisiin kohdistuvien digihuijausten riskienhallinnassa on siis keskeistä digihuijausten ennaltaehkäisy ja toisaalta myös pankkiin kohdistuvien riskien minimoiminen. Nykyaikainen pankkitoiminta edellyttää nopeampia päätöksiä riskien suhteen, kuten reaaliaikaisia maksuja, ja pankkien on löydettävä tasapaino petosten hallinnan ja valtuutettujen tapahtumien välittömän käsittelyn välillä. Talousrikollisuuden ja petosriskien kasvavat kustannukset ovat myös ylittäneet odotukset, ja niitä on nostanut useiden tekijöiden yhteisvaikutus. Pankit, jotka keskittyvät tiiviisti vastuiden ja tehokkuuskustannusten vähentämiseen, jättävät huomiotta tappioita esimerkiksi asiakaskokemuksessa, liikevaihdossa, maineessa ja jopa sääntelyn noudattamisessa. (Hasham ym., 2019.)

Julkisen ja yksityisen sektorin kokemukset osoittavat, että petosten ja rahanpesun torjunnan prosessit täydentävät toisiaan. Tämä sisältää teknologian hyödyntämisen, joka auttaa käyttäjiä hylkäämään automaattisesti huijauksia, yhteistyön yksityisen sektorin kanssa tulevaisuuden huijauskehitysten torjumiseksi, tiliturvallisuusominaisuuksien, valvontatoimien ja sääntöjen luomisen sekä varoitusviestien lisäämisen virustorjuntaohjelmissa mahdollisten phishing-sivustojen varalta. Tämän lisäksi rahoituslaitosten käyttöön ottama reaaliaikainen tapahtumien seuranta, jossa käytetään kehittyneitä ohjelmistoja ja algoritmeja tapahtumien valvontaan ja joka tunnistaa ja estää huijaukset tai laittomat toimet reaaliajassa, on hyödyllinen CEF havaitsemisessa ja estämisessä. Lisäämällä epänormaalien tilinhaltijatietojen ja tapahtumien reaaliaikaista seuranta, rahoituslaitokset voivat nopeasti tunnistaa, tutkia ja raportoida poikkeavat tai epäilyttävät toimet. (FATF, 2023.)

Johtavat rahoituslaitokset pyrkivät yhdistämään talousrikoksiin, petoksiin ja kyberrikollisuuteen liittyvät toimenpiteet, jolloin sekä etulinjan että taustatoimintojen prosesseja suunnataan tähän suuntaan. Tämän integraation aloittamiseen kuuluu kaikkien riskienhallintaan liittyvien toimien täsmällinen määrittely eli talousrikosten, petosten ja kybertoimintojen riskien tunnistaminen ja roolien sekä vastuiden selkiyttäminen puolustuksen eri tasoilla. Ensimmäiseen puolustuslinjaan kuuluu liiketoiminta ja yritystoiminnot, toinen sisältää riskienhallinnan liittyen talousrikoksiin, petoksiin ja kybertoimintoihin. Näin varmistetaan kattavuus ja selkeä vastuunjako samalla, kun päällekkäisyyksiä poistetaan. Petostentorjunnan ja kyberturvallisuuden toimintojen

integroiminen on tulevaisuudessa välttämätöntä, sillä rikokset ovat jo kytköksissä toisiinsa. (Hasham ym., 2019.)

Kaikkiin talousrikoksiin liittyviin riskeihin liittyy kolme vastatoimen kategoriaa: Asiakkaan tunnistaminen ja autentikointi, tapahtumien ja käyttäytymisen poikkeamien seuranta ja havaitseminen sekä riskien ja ongelmien lieventämiseen tähtäävä reagointi. Näitä toimia ja niiden tietolähteitä ja prosesseja voidaan käyttää petoksiin, kyberrikkomuksiin ja muihin talousrikoksiin. Tietojen yhdistäminen analytiikkaan parantaa merkittävästi näkyvyyttä ja mahdollistaa syvemmän ymmärryksen, mikä puolestaan tehostaa havaitsemista ja ehkäisyä. (Hasham ym., 2019.)

Eräs tapa ennaltaehkäistä petosriskejä on strateginen näkökulma, jonka tarkoituksena on ennustaa riskejä pelkän reagoinnin sijaan, ja voi täten merkittävästi parantaa pankin ja asiakkaiden turvallisuutta. Ennakointiin tarvitaan pankkien asiakas- ja sisäisten toimintojen sekä prosessien uudelleenmuotoilua, joka perustuu jatkuvaan arviointiin petosten, talousrikosten ja kyberuhkien todellisista tapauksista. Näistä muodostetaan näkemys asiakaspolun mukaan ja valvontakäytännöt suunnitellaan kokonaisvaltaisesti prosessien ympärille. Toinen tapa petosten ennaltaehkäisyyn on muodostaa kattava käsitys siitä, miten rikolliset todellisesti käyttäytyvät. Pankkien parantaessa turvallisuutta yhdellä sektorilla rikollisuus siirtyy toiselle osa-alueelle, joten petosten torjuntakeinojen on siilomaisen lähestymistavan sijaan keskityttävä kokonaisuuteen. Suunnittelemalla valvontakäytännöt tämän periaatteen mukaan, pankkien on tuotava yhteen eri alojen asiantuntemusta, mikä parantaa tehokkuutta ja vaikuttavuutta. (Hasham ym., 2019.)

Integroitu lähestymistapa petosriskien hallintaan voi johtaa myös optimaaliseen asiakaskokemukseen, jonka avulla voidaan muokata asiakaskäyttäytymistä ja parantaa liiketoimintatuloksia. Tavoitteena on petoksiin liittyvien valvontatoimenpiteiden segmentointi asiakaskokemuksen ja tarpeiden mukaan sekä automaation ja digitalisaation hyödyntäminen asiakaspolun parantamiseksi. (Hasham ym., 2019.) Asiakaslähtöinen ulottuvuus petostentorjunnassa nousee esille myös pankin viestiessä asiakkailleen, esimerkiksi selvityspyyntöjen muodossa. Pankeilla on lakiin perustuva velvollisuus tuntea asiakkaansa ja tämän liiketoimet sekä täten oikeus kysyä tarvittaessa asiakkaan tilille tulevien varojen alkuperästä ja käyttötarkoituksesta. Kirjallisen selvityksen lisäksi pankki voi vaatia dokumentteja, kuten kauppakirjoja. (Finanssivalvonta, 2020.) Tämä

saattaa aiheuttaa asiakkaille ylimääräistä vaivaa ja täten he saattavat kokea saaneensa huonoa kohtelua.

Digitaalisesta luottamuksesta on tulossa pankkien kilpailuetu ja sitä voidaan vahvistaa nimenomaan yhtenäisellä riskienhallinnalla, joka kattaa petokset, talousrikokset ja kyberuhat. Asiakkaat arvostavat etenkin turvallisuutta, läpinäkyvyyttä ja palvelun sujuvuutta, mutta myös esimerkiksi vaivaton tunnistautuminen ja riitojen nopea ratkaisu ovat välttämättömiä tekijöitä digitaalisen luottamuksen rakentamisessa. (Hasham ym., 2019.)

Digihuijausten riskienhallinnan parantamiseen liittyy useita aloitteita, joiden keskiössä on usein useiden sidosryhmien yhteistyö. Näihin aloitteisiin kuuluvat muun muassa julkisen tietoisuuden lisääminen, ohjeet/lausunnot valvontatoimenpiteistä ja turvallisuusprotokollista, pankkien digitaalisen petoksen riskienhallintakäytäntöjen valvonta, yhteistyö useiden viranomaisten kanssa petostoimintojen havaitsemiseksi ja reagoimiseksi sekä rajat ylittävä yhteistyö. (BCBS, 2023.) FATF (2023) nostaa raporttinsa perusteella tärkeimmiksi keinoiksi huijausten ja niihin liittyvän rahanpesun torjumisessa kansallisen yhteistyön parantamisen, monenkeskisen yhteistyön tukemisen ja tehokkaampien havaitsemis- ja ennaltaehkäisykäytäntöjen vahvistamisen.

Asiakkaiden ja työntekijöiden jatkuva koulutus on välttämätöntä, jotta pankin tiedot ja järjestelmät voidaan pitää turvassa ja organisaation kyberturvallisuus voidaan varmistaa. (Hull, 2018.) Yhä useammin digihuijaukset liittyvät reaaliaikaisiin maksuihin, joita uhri ei voi peruuttaa. (BCBS, 2023.) Asiakas on aina vastuussa maksutietojen oikeellisuudesta, eikä tililtä lähtenytä maksua ole mahdollista palauttaa takaisin tai tilille kirjautunutta maksua palauttaa sen lähettäjälle ilman kyseisen tilin omistajan lupaa tai viranomaistoimia. Useissa tapauksissa rahat on myös ehditty siirtää toisen pankin tilille, nostaa käteiseksi tai muuntaa virtuaalivaluutoiksi. Näin ollen pankkien on erittäin tärkeää keskeyttää epäilyttävät transaktiot heti, sillä tililtä lähteneet maksut on haastavaa saada palautettua. (Deloitte, 2023.) Pankit voivat toteuttaa koulutuskampanjoita yhdessä muiden organisaatioiden tai viranomaisten kanssa antamalla varoituksia tai suosituksia lisätäkseen kuluttajien tietoisuutta riskeistä ja uusista petostekniikoista, sekä kannustamalla kuluttajia suojaamaan henkilökohtaisia tietojaan, kuten luottokorttitietoja ja salasanoja. Toisaalta pankit voivat kouluttaa henkilöstöään lisätäkseen tietoisuutta

asiakkaidensa varojen suojelemiseksi sekä petosten havaitsemiseksi ja ilmoittamiseksi. Pankit voivat myös lisätä asiakkailleen keinoja ilmoittaa huijauksista eri kanavien kuten mobiilisovellusten tai verkkosivustojen kautta sekä mahdollisuuksia asettaa esimerkiksi alarajoja korkeampiriskisille tilisiirroille. (BCBS, 2023.) Huijarit hyödyntävät muun muassa exploit kit -paketteja, jotka automaatiota hyödyntäen mahdollistavat haittakoodien asentamisen etänä tietokoneelle sekä siten koneen hallinnan etänä. Tartunta tapahtuu, kun uhri vierailee huijareiden hallitseamalla sivustolla tai klikkaa linkkejä sivulle, jolle exploit kit on asennettu. Laitteen etähallinta antaa huijarille mahdollisuuden vakoilla uhrin toimintoja ja varastaa yksityisiä tietoja, kuten luottotietoja tai sosiaaliturvatunnuksia, joita voidaan käyttää uhrin kiristykseen tai maineen tahraamiseen. (Awad, 2017.) Tällaisia tapauksia voidaan ennaltaehkäistä asiakkaiden kouluttamisella sekä viestinnällä ja lisäksi pankit voivat vähentää linkkejä omissa viesteissään.

3.8 Teknologiset riskienhallintatyökalut digihuijaustapauksissa

Väärinkäytösten torjunnan pohjana voidaan pitää asiakkaan käyttäytymiseen perustuvia ja automaattisia päätöksiä tekeviä älykkäitä järjestelmiä yhdistettynä asiantuntijoiden substanssiosaamiseen (Deloitte, 2023). Teknologia voi tukea digihuijausten torjuntaa muun muassa digitaalisten henkilöllisyysasiakirjojen ja digitaalisten allekirjoitusten käytön avulla, sillä osa digihuijauksista liittyy viestien muokkaamiseen tai luomiseen niin, että ne vaikuttavat tulevan henkilöltä, jotka hallitsevat tilejä tai henkilöltä, joilla on oikeus tehdä maksuja. (BCBS, 2023).

Asiakkaan tunnistamisen prosessi (KYC, know your customer) on lakisääteinen ja pankin sekä asiakkaiden turvallisuuden kannalta hyvin merkittävä. Aiheesta on tehty paljon tutkimuksia ja kehitystöitä liittyen esimerkiksi kosketusbiometrian ja laitteen pienliikkeiden avulla tunnistautumiseen, silmien iiriksen tunnistamiseen ja sormenjäljen sekä salasanan avulla tunnistautumiseen. (Awad, 2017.) Integroimalla erillisten toimintojen dataa sekä sisäisistä että ulkoisista lähteistä pankit voivat parantaa asiakkaidensa tunnistusprosessia. Asiakastietojen yhdistäminen, joka syntyy talousrikosten, petosten ja kyberuhkien hallintaan keskittyvien ryhmien tiiviimmistä yhteistyöstä, lisää merkittävästi pankin analytiikka- ja tunnistuskykyä. Esimerkiksi reaaliaikainen riskipisteytys tehostaa petosten torjuntaa (Hasham ym., 2019.)

Tekoälypohjaiset työkalut voivat käyttää laajasti dataa useista eri lähteistä ja eri kielillä parantaakseen KYC-prosessia sekä tunnistaa asiakkaiden äidinkielet analysoimalla kirjallisia viestejä, havaita muokattuja digitaalisia kuvia ja kerätä asiakkaiden mobiililaitteiden sijaintitietoja rahanpesuriskin arvioimiseen. (Pavlidis, 2023.)

Tekoälyn avulla maksutapahtumien seuranta petosten havaitsemiseksi voidaan myös toteuttaa entistä tehokkaammin. Käyttäytymisanalytiikan avulla seuraamalla asiakkaiden tapahtumia asiakkaista voidaan luoda profiileja, jolloin epäilyttävä tapahtuma voidaan tunnistaa lähes välittömästi. (Pavlidis, 2023.) Tekoälyn ja koneoppimisen avulla voidaan hyödyntää yhdistettyjä tietolähteitä, jolloin analytiikan ennakoivuus voi parantua. (Hasham ym., 2019.) Tilastolliset prosessit ja ennustavat mallit voivat myös arvioida tapahtuman vilpillisyyttä tai sen liitoksia rahanpesuun ilman subjektiivista ihmisen tekemää analyysia. (Pavlidis, 2023.)

Vilpillisiin maksutapahtumiin ja rahanpesun torjuntaan liittyvät hälytykset kuluttavat yhä enemmän henkilöstöresursseja, mitä voidaan helpottaa digitaalisten työkalujen avulla. Tekoälypohjaisia työkaluja voidaan hyödyntää myös laajemmin riskienhallinnassa edistäen dynaamisempaa riskiperusteista lähestymistapaa tukemalla perinteistä riskianalyysia ja tunnistamalla nousevia riskejä, jotka eivät kuulu jo tunnettuun profiiliin ja typologioihin. (Pavlidis, 2023.)

4 ASIANTUNTIJAHAASTATTELUT

4.1 Tutkimusaineiston kuvaus ja käsittely

Tutkimuksen tieteenfilosofia lähtökohtia käsiteltiin tarkemmin johdantokappaleen alaluvussa 1.4. Kuten johdannossa mainittiin, tutkimuksen empiirinen aineisto kerättiin puolistrukturoitujen teemahaastatteluiden avulla. Syksyllä 2024 kolmen eri pankin sekä yhden toimialajärjestön edustajalle lähetettiin sähköpostitse haastattelupyyntö, jossa kerrottiin taustatietoja haastattelijasta sekä taustoitettiin tutkimusta. Haastattelukysymysrunko lähetettiin haastateltaville etukäteen, jotta heidän oli helpompi valmistautua haastatteluun. Toimialajärjestön edustajaa pyydettiin vastaamaan yleisellä tasolla pankkeihin kohdistuviin haastattelukysymyksiin. Haastattelurunko on liitteenä. Kaksi haastatteluista toteutettiin etänä Microsoft Teams- verkkotapaamisohjelman avulla ja yksi kasvotusten. Nämä kolme haastattelua nauhoitettiin puhelimen sanelinsovelluksella ja litteroitiin välittömästi haastatteluiden jälkeen. Haastattelut kestivät noin 1–1,5 tuntia ja ne toteutettiin yksilöhaastatteluina eli paikalla oli haastattelijan lisäksi yksi haastateltava kerrallaan. Haastattelurungon kysymysten lisäksi haastateltaville esitettiin tarkentavia lisäkysymyksiä. Neljäs haastateltavista antoi vastaukset sähköpostitse.

Haastateltavat vastasivat kysymyksiin mahdollisimman kattavasti kuitenkin pankkisalaisuuden puitteissa ja välttämällä liikesalaisuuksien paljastamisen. Haastatteluissa kartoitettiin myös jokaisen haastateltavan urataustaa ja kokemusta tutkielman läpinäkyvyyden ja luotettavuuden lisäämiseksi. Puolet haastateltavista toivoi vastausten anonymisointia, joten tutkielman johdonmukaisuuden ja tietosuojan toteutumisen vuoksi loputkin vastaukset anonymisoitiin.

Asiantuntija A on työskennellyt kolme vuotta pankin väärinkäytöksiin liittyvien riskienhallintaprosessien kehittämisen, väärinkäytösuhkien tunnistamisen ja niihin liittyvien hallintakeinojen määrittelyn parissa. Tämän lisäksi hänen työtehtäviinsä kuuluu väärinkäytösriskien valvonta, väärinkäytösriskeihin liittyvien trendien, sääntelyvelvoitteiden ja tappioiden seuraaminen sekä raportointi.

Asiantuntija B on työskennellyt helmikuusta 2024 lähtien talousrikollisuuden torjunnan asiantuntijana. Hänen työtehtäviinsä kuuluu petos- ja huijaustapausten ennaltaehkäisy

sekä käsittely operatiivisella tasolla. Konkreettisesti työ pitää sisällään yhteydenpitoa asiakasrajapintaan, prosessikehitystä, tapausten käsittelyä ja tulkintaa sekä aktiivista kommunikointia ja näkemysten antoa kehitysmielessä.

Asiantuntija C työskentelee pankissa väärinkäytösten hallinnan yksikössä viestintävastaavana, jona on toiminut noin vuoden verran. Hän on osa operatiivista tutkintatiimiä, jossa oli alun perin tutkijana vuodesta 2020 alkaen. Nykyisin hän keskittyy työtehtävissään viestimiseen ja hänen työnsä tärkeimmät osa-alueet ovat akuutti viestintä eli esimerkiksi turvallisuustiedotteiden kirjoittaminen asiakkaille sekä fraud awareness, joka tarkoittaa tietoisuuden kasvattamista petostentorjunnasta pankin sisäisesti ja ulkoisesti mediassa sekä erilaisissa tilaisuuksissa.

Asiantuntija D työskentelee suomalaisen toimialajärjestön varautumisesta ja rikostorjunnasta vastaavana johtajana, jona hän on toiminut viiden vuoden ajan. Hän työskentelee pankkien ja vakuutusyhtiöiden varautumiseen sekä rikostorjuntaan liittyvissä tehtävissä, joihin liittyy rikostorjunnan toimenpiteet sekä lainsäädännön kehittymisen ja maailman tilanteen seuraaminen.

Haastatteluiden avulla kerätty aineisto analysointiin käyttämällä teoriaohjaavaa sisällönanalyysia, jonka käyttöä on perusteltu tarkemmin johdannossa. Aluksi haastatteluiden perusteella kerätty aineisto redusointiin eli pelkistettiin auki kirjoittamalla haastattelut. Tämän jälkeen aineisto klusteroitiin eli ryhmiteltiin etsien samankaltaisuuksia ja lopuksi suoritettiin abstrahointi eli teoreettisten käsitteiden luominen. Erona aineistolähtöiseen sisällönanalyysiin abstrahoinnissa empiirinen aineisto liitettiin valmiiksi tuotuna ilmiöstä tiedettyihin käsitteisiin. (Tuomi & Sarajärvi, 2018.) Sekä digihuijauksia että niiden riskienhallintaa käsittelevässä aineistossa oli havaittavissa paljon samankaltaisuuksia ja yhtymäkohtia tutkielman teoriaosuuteen. Näin ollen luokkien muodostamisessa pystyttiin hyödyntämään teoreettisen taustan käsitteitä.

4.2 Pankkien asiakkaisiin kohdistuvat digihuijaukset

4.2.1 Tyypillisimmät pankkien asiakkaisiin kohdistuvat digihuijaukset

Haastatteluiden perusteella pankkien asiakkaisiin kohdistuvat digihuijaukset ovat hyvin moniulotteinen, laaja ja jatkuvassa muutoksessa oleva ilmiö. Asiantuntija D viittasi

digihuijausten luokittelusta poliisin termein tietoverkkoavusteisiksi rikoksiksi, jolla tarkoitetaan, että uhria lähestytään jonkin digitaalisen kanavan kautta.

Asiakkaisiin kohdistuvat digihuijaukset voidaan pääsääntöisesti jakaa kahteen kategoriaan. Ensimmäinen näistä on maksajan manipulointiin perustuva huijaus, jossa huijari yrittää saada manipuloinnin keinoin asiakkaan itse tekemään tilisiirto ja vahvistamaan tapahtuma. Maksajan manipulointiin perustuvista huijauksista voidaan käyttää myös nimeä tunnehuijaus. Toiseen kategoriaan kuuluvat huijaukset, jossa huijari pyrkii saamaan asiakkaalta haltuun tämän pankkitunnukset ja voi täten tehdä maksuja vapaammin. Molempiin näistä kategoriasta kuuluu useita erilaisia huijausmuotoja. Asiantuntija C viittaakin tyypillisimpiin huijausmuotoihin liittyen tutkielman teoriaosuudessa esiteltyyn Finanssiala ry:n tilastoon, jonka mukaan volyymiltaan merkittävimpiä huijausmuotoja ovat sijoitus- ja valepoliisihuijaukset, tietojen kalastelu sekä dokumentti- ja rakkaushuijaukset.

Haastateltavien mukaan sijoitushuijaukset perustuvat maksajan manipulointiin, jolloin asiakkaalle uskotellaan tämän sijoittavan rahaa oikealle sijoitusalustalle, joka onkin huijaussivusto. Asiakas saattaa itse löytää kyseisen sivuston osoitettuaan algoritmeille kiinnostusta sijoitustuotteita kohtaan tai suoraan hakukoneen avulla. Toisaalta sosiaalisessa mediassa asiakkaalle saatetaan kohdistaa mainontaa sijoituksiin liittyvistä huijaussivustoista tai asiakas saattaa antaa yhteystietonsa lomakkeelle, jonka kautta huijari ottaa suoraan yhteyttä sijoituksista kiinnostuneeseen henkilöön. Erilaisten kanavien lisäksi sijoituskohteita on lukuisia, kuten kulta, lomakohteet ja kryptovaluutat.

Sijoitushuijausten lisäksi rakkaushuijaukset perustuvat manipulointiin ja tunteisiin vetoamiseen. Sosiaalisen median hyödyntäminen sijoitushuijauksissa on haastatteluiden perusteella lisääntynyt. Myös dokumenttihuijauksissa on tarkoituksena saada uhri tekemään rahansiirto esimerkiksi perintöön liittyen. Uhri voi jopa olla siinä uskossa, että on adoptoimassa lasta ulkomailta, jolloin hän tekee rahansiirtoja väärennettyihin dokumentteihin pohjautuen. Vuoden 2024 alkupuoliskolla dokumentti- ja rakkaushuijauksiin menetetty summa laski 42,4 prosenttia verrattuna edellisvuoden vastaavaan aikaan (Palmgren, 2024b). Asiantuntija C uskoo tämän johtuvan ihmisten valvetuneisuuden lisääntymisestä, mutta ei sinänsä usko kyseisten huijausmuotojen vähentyneen. Toisaalta hän nostaa esiin, että huijaukset voivat kategorisoitua eri tavoin niiden piirteiden mukaan. Yhä tyypillisempää on, että romanttisessa mielessä alkanut

keskustelu voi hyvin nopeasti muuttua sijoitusneuvonnaksi, sillä huijarit saavat näin isomman hyödyn nopeammin verrattuna esimerkiksi rahansiirtojen hankkimiseksi lentolippuja varten. Tällainen huijaus voi esimerkiksi tilastoitua sijoitushuijauksena.

Volyymiltaan merkittävimmät taloudelliset menetykset aiheutuvat perinteisissä kalastelukampanjoissa, joita toteutetaan eri toimijoiden nimissä yrittäen saada asiakas antamaan pankkitunnukset huijaussivustolle, jota kautta huijari saa ne haltuunsa. Haastatteluiden perusteella tietoja kalastellaan kaikkien mahdollisten kanavien kautta, eli tekstiviesteillä, sähköposteilla, puhelimitse ja sosiaalisen median kautta.

Toinen yleistynyt huijaustapa pankkitunnusten hankkimiseksi on verkon kauppapaikoilla tapahtuvat huijaukset, jotka tilastoituvat tietojenkalastelu -kategoriaan. Näissä huijauksen kohteena on nimenomaan tuotteiden myyjät. Kolme haastateltavista nostaa esiin uusimpana Vinted-sovelluksen ja lisäksi huijausten mainittiin jatkuneen jo pidempään esimerkiksi Tori.fi-alustalla ja Facebookin Marketplace-alustalla. Kyseisissä huijauksissa hyödynnetään uhrin osaamattomuutta siitä, mitä maksutapahtuma vaatii ja millaiset markkinapaikan toimintamallit tosiasiallisesti ovat, eli myyjää huijataan antamaan luottokorttinsa numero tai pankkitunnukset huijarille vastaanottaakseen maksun tuotteestaan tai vaihtoehtoisesti huijari kertoo maksaneensa tuotteen postin ennakkopalvelussa ja lunastaakseen rahat myyjän tulee jättää tietonsa linkin kautta.

Asiantuntija C nostaa esiin myös arpajashuijaukset, jotka tapahtuvat pääasiassa Facebookissa siten, että huijarit kaappaavat sosiaalisen median tilin ja lähettävät tämän kavereille viestin liittyen arpajaisvoiton jakoon pyytäen tavallisesti aluksi kaverin puhelinnumeron ja sen saatuaan jakavat linkin, jonka kautta uhria neuvotaan jättämään tilitietonsa voiton lunastamiseksi.

Asiantuntija B mainitsee pienen osan huijauksista kuuluvan myös muihin huijaustyyppeihin, kuten muulitilihuijauksiin. Huijausmuotoja on siis hyvin laaja skaala ja ongelmallista onkin haastatteluiden perustella se, että asiakkaat joutuvat huijatuksi kohdatessaan itseään koskevia tai hyvin kohdennettuja huijauksia. Näin ollen, vaikka uhri tunnistaisi sijoitushuijauksen, voi hän joutua vaikkapa rakkaushuijauksen uhriksi.

Merkittävin teknologian kehityksen tuoma muutos digihuijauksiin on haastateltavien mukaan huijausten muuttuminen yhä kompleksisemmiksi ja monipolvisemmiksi. Pankit

ovat viime vuosien aikana lisänneet teknisiä ratkaisuja huijausten tunnistamiseksi ja ehkäisemiseksi, minkä vuoksi onnistuneet huijaukset vaativat huijareilta yhä enemmän perehtyneisyyttä esimerkiksi asiakaspolkuun ja kehittyneempiä teknisiä ratkaisuja.

Haastatteluissa kuitenkin ilmeni, että varsinaisesti huijausmuodot eivät ole juurikaan kehittyneet ja tarinat ovat pääosin ennallaan, mutta huijauksissa käytettävät tekniset menetelmät ovat muuttuneet. Tämä on osaltaan johtanut siihen, että tietyt rikollisjoukot osaavat toteuttaa teknisesti vaativat elementit ja pystyvät esimerkiksi luomaan uskottavan näköisiä huijaussivustoja sekä hallitsevat paljon ihmisten dataa, minkä takia he myyvät huijauksia palveluna pienemmille rikollisryhmille ja asiantuntija D:n mukaan myös henkilöille, jotka eivät ole diginatiiveja. Huijauspalveluiden myynti tunnetaan nimellä Fraud as a Service. Tämä näkyy asiantuntija C:n mukaan huijaukampanjoina, joilla on selkeä aikajänne ja joiden viestejä on vain hieman muutettu aiemmista vastaavista kampanjoista. Teknologian kehitys on siten johtanut siihen, että huijaukset ovat muuttuneet ammattimaisemmaksi rikollisuudeksi ja toiminta keskittyy yhä enemmän tietyille tekijöille.

Asiantuntija A, C ja D mainitsevat rikollisten ja rikollisryhmittymien kasvavan siirtymisen huumausainerikoksista digihuijausten pariin niiden vaivattomuuden, tuottavuuden ja pienemmän kiinnijäämisriksin vuoksi. Tämän lisäksi huumausainerikosten tuomiot ovat huomattavasti pidempiä, kuin petoksista, sillä törkeän petoksen maksimirangaistus on neljä vuotta vankeutta. Digihuijaukset on myös helpompaa toteuttaa paikasta riippumatta verkossa, joten maantieteellinen sijainti ei ole este niiden toteutukselle verrattuna huumausainerikoksiin. Näin ollen haastateltavien mukaan verkkorikollisuuden avulla saaduilla varoilla rahoitetaan rikollista toimintaa samoin, kuin aiemmin on tehty huumausainerikoksilla saaduilla rahoilla. Asiantuntija A viittaa tutkielman teoriassa esiteltyyn Rahanpesun selvittelykeskuksen tilastoon petosrikosten lisääntymisestä rahanpesun esirikoksina.

Asiantuntija D:n mukaan maksamisen digitalisoituminen ja kansainvälistyminen sekä kryptovaluuttojen keksiminen ovat edesauttaneet sitä, että rikolliset saavat varoja siirrettyä laillisen ja viranomaisvalvotun pankkiverkoston ulkopuolelle. Kryptovaluuttahuijaukset ovat tuottoisia, koska kryptovaluuttojen toimintaperiaate on osalle kuluttajista hyvin epäselvä, jolloin huijarit voivat luvata isoja tuottoja tietämättömälle kuluttajalle. Asiantuntija B:n mukaan kryptovaluuttahuijauksiin liittyen

väärennetyt ICO:t (Initial Coin Offerings) ja pyramidihuijaukset, ovat yleistyneet. ICO on rahoituksenkeräyskeino, jossa sijoittaja osallistuu tarjoamalla tavallista valuuttaa tai kryptovaluuttaa rahoituksen hakijalle, jolta sijoittajaa saa vastineeksi tokeneita eli uuden kryptovaluutan yksiköitä (Finanssivalvonta, 2017).

Digihuijauksia tehostavana ja lisäävänä tekijänä nousi esiin myös sosiaalinen media, sillä erilaisilla sosiaalisen median alustoilla voidaan mainostaa huijauksia suurelle ihmismäärälle. Haastatteluissa ilmeni, että huijauksia tapahtuu hyvin laajasti kaikenlaisilla sosiaalisen median kanavilla. Esiin nousi muun muassa Facebook, Vinted, Tori.fi, Tinder ja jopa uskonnollinen seuranhakupalvelu Valo. Toisekseen teknologian kehityksen myötä sähköposteja ja tekstiviestejä voidaan lähettää automatisoidusti uhreille.

Asiantuntija C ja B mainitsevat teknologisenä riskinä haittaohjelmien hyödyntämisen huijauksissa. Ne ovat kuitenkin teknisesti haastavia toteuttaa, eivätkä ole välttämättä yhtä tehokkaita muihin huijausmuotoihin verrattuna, joten ne eivät ole Suomessa ainakaan vielä merkittävä ongelma.

Tekoäly on puolestaan muuttanut huijauksia haastatteluiden perusteella etenkin kahdella tavalla. Ensinäkin sen avulla huijausten kieliasut ovat parantuneet eli niissä käytetty teksti on aiempaa selvempää ja sujuvampaa. Tämän seurauksena huijarit pystyvät toteuttamaan huijauksia entistä kansainvälisemmin eikä heiltä vaadita välttämättä lainkaan kohdemaan kielitaitoa. Asiantuntija C nostaa esiin, että aiemmin vaikea kieli oli suomalaisia suojaava tekijä, mutta tekoälyn myötä näin ei enää ole. Toiseksi huijauksissa hyödynnetään yhä enemmän tekoälyn avulla luotuja kuvia ja videoita. Deepfake -teknologian avulla voidaan esimerkiksi luoda videoita julkisuuden henkilöistä tai uhrien läheisistä. Asiantuntija B:n mukaan kyseisen teknologian käytön lisääntyminen on huolestuttavaa:

”Deepfake-uutiset ovat erityisen vaarallisia, koska ne hyödyntävät väärennetyjä videoita ja ääniä levittääkseen valheellista tietoa, joka näyttää tulevan luotettavista lähteistä, kuten uutiskanavilta tai tunnetuilta henkilöiltä. Tämä tekee niiden erottamisesta todellisista uutisista erittäin vaikeaa, mikä voi johtaa laajamittaiseen harhaanjohtamiseen ja luottamuksen heikkenemiseen mediassa.” (Asiantuntija B)

Haastatteluiden perusteella etenkin sijoitushuijauksissa kyseinen deepfake-teknologia on suosittua, sillä sen avulla voidaan luoda uskottavia, mutta väärennettyjä esityksiä ja lupauksia, jotka houkuttelevat sijoittajia. Tekoälyn avulla voidaan myös luoda valeprofiileja esimerkiksi seuranhakualustoille, jolloin tekoälyn avulla luodut kuvat eivät löydy käänteisellä kuvahauulla ja huijausten todentaminen vaikeutuu entisestään. Suomessa deepfake-teknologian hyödyntämiseen liittyvät huijaukset ovat haastateltavien mukaan kuitenkin toistaiseksi vähäisiä, mutta niiden uskotaan lisääntyvän merkittävästi lähivuosina.

4.2.2 Trendit pankkien asiakkaisiin kohdistuvissa digihuijauksissa

Digihuijauksiin liittyviä trendejä ovat vuoden 2024 aikana olleet haastateltavien mukaan etenkin sosiaalinen manipulointi, tietojen kalastelun eri muodot ja kaupankäyntialustahuijaukset. Etenkin Vinded -alustalla tapahtuneet huijaukset ovat kasvaneet huomattavasti.

Sosiaalinen manipulointi ilmenee muun muassa siten, että tekstiviestin lisäksi huijausten kohteille myös soitetaan huijareiden toimesta, jolloin huijareiden on helpompaa vedota näiden tunteisiin. Asiantuntija C:n mukaan näin huijauksen sosiaalisen manipuloinnin aspekti ja siten uskottavuus lisääntyy.

Tietojen kalastelu on ollut toinen selkeästi kasvava trendi haastateltavien mukaan. Uutena tietojen kalastelun muotona on haastatteluiden perusteella lisääntynyt turvatilihuijaukset. Niissä huijarit soittavat asiakkaille esiintyen esimerkiksi pankin edustajina ja kertovat havainneensa asiakkaan tilillä epäilyttäviä tapahtumia, minkä vuoksi tämän tulisi siirtää rahat turvaan turvatilille eli tosiasiallisesti huijarille.

Haastatteluissa ilmeni, että huijausmuodot vaihtelevat kausittain ja vanhoja huijausmuotoja otetaan jonkin ajan kuluttua uudelleen käyttöön eli trendit niin sanotusti kiertävät. Varsinaisissa huijaustarinoissa on vähemmän vaihtelevuutta, mutta sen sijaan huijaustavat vaihtelevat. Kuitenkin ajoittain huijarit myös muuttavat tarinoitaan, kuten viime aikoina on ollut nähtävissä esimerkiksi sijoitus- ja rakkaushuijausten suhteen. Ihmiset ovat yhä valveutuneempia sen suhteen, etteivät lähetä rahaa tuntemattomille, joten huijarit ovat muuttaneet lähestymistapaansa siten, että pyrkivät seuranhakualustoilla lähestymään uhria luoden tähän yhteyden, jonka jälkeen suosittelevat tälle

sijoituskohdetta, jonka avulla saavat tältä huijattua rahaa. Näin uhri ei joudu lähettämään suoraan tuntemattomalle henkilölle rahaa, vaan usko tehneensä kannattavan sijoituksen itse. Ilmiö tunnetaan nimellä ”pig butchering”, joka esiteltiin myös tutkielman toisessa teorialuvussa.

Huijausmuotojen kausivaihtelut näkyvät siten, että huijarit pyrkivät hyödyntämään yhteiskunnassa tapahtuvat muutokset. Haastatteluissa nousi esiin muun muassa alennusviikko Black Week, jonka aikana huijarit pyrkivät valeverkkosivujen avulla hankkimaan rahaa kyseisellä hetkellä suosituimmilla tuotteilla. Joulun aikaan puolestaan postin nimissä toteutettavat huijaukset voivat lisääntyä, veronpalautusten tapahtuessa verottajan nimissä tapahtuvat huijaukset ja influenssarokotusaikaan puolestaan terveyspalveluidentarjoajien nimissä toteutettavat huijaukset. Lainsäädännölliset muutokset koskien pankkeja voivat myös lisätä pankkien nimissä tapahtuvia huijauskampanjoita.

Asiantuntija C nostaa esille merkittävän rahamuulien käytön lisääntymisen digihuijauksiin liittyen. Alkurikoksen varojen alkuperän häivyttämisessä voidaan käyttää jopa kymmentä rahamuulia. Näin ollen kyse on huijareiden harjoittamasta todennäköisyyksien hallinnasta, mikä on johtunut pankkien lisäämistä kontroleista, joiden avulla muulitapausten tunnistaminen on helpottunut. Asiantuntija C tuo esiin myös, että rahamuulit saattavat toimia huijattuina kyseiseen toimintaan vain esimerkiksi yhden tilisiirron ajan, mutta joskus rahamuulitoiminta voi olla ammattimaisempaa.

Kahdessa haastatteluista nousi esiin Traficomien luoma mahdollisuus suojata Sender ID -tunnus. Nykyisin tekstiviestejä kansalaisille lähettävä taho voi suojata tunnuksen, jolloin mikään muu taho ei voi käyttää samaa alfanumeerista lähettäjätunnustetta lähettäessään tekstiviestejä suomalaisiin liittymänumeroihin (Traficom, 2024). Huijarit pyrkivät haastateltavien mukaan kloonaamaan tunnuksia hyvin samankaltaiseksi kuin suojatut tunnukset, esimerkiksi hyödyntämällä pisteitä tai kirjoittamalla numeron yksi ison i-kirjaimen sijaan, jolloin vastaanottaja voi erehtyä luulemaan lähettäjätunnusta oikeaksi.

Deepfake-huijaukset mainitaan haastatteluissa myös viimeaikaisena trendinä. Suomessa tällaiset ovat vielä haastateltavien mukaan melko harvinaisia, mutta esimerkiksi USA:ssa on haastatteluiden perusteella pinnalla nopeasti etenevä eritoten nuoriin kohdistuva rakkauskiristyshuijaus sextortion, jossa tekoälyllä luoduilla profiileilla lähestytään uhreja

romanttisessa mielessä, jonka jälkeen uhrilta pyritään saamaan intiimejä kuvia, joiden avulla uhria voidaan kiristää. Haastatteluiden perusteella on vielä epävarmaa, rantautuuko tämänkaltainen trendi tulevaisuudessa myös Suomeen.

4.3 Pankkien asiakkaisiin kohdistuvien digihuijausten riskit

4.3.1 Digihuijausten aiheuttamat riskit pankeille

Pankkien asiakkaisiin kohdistuvien digihuijausten aiheuttamat riskit pankeille voidaan haastatteluiden mukaan jakaa pääsääntöisesti kahteen kategoriaan. Taloudellinen riski syntyy korvausvastuun myötä ja kustannukset voivat olla merkittäviä, erityisesti kun otetaan huomioon, että asiakas on saattanut menettää useamman vuoden säästöt tai jopa eläkesäästöt. Taloudellinen riski liittyy myös digihuijausten mahdollisesti aiheuttamiin luottotappioihin. Haastateltavat korostavat, että korvausvastuun selvittäminen on aina tapauskohtaista ja pankin osalta se on sidonnainen prosessien ja kontrollien toimivuuteen. Maineriski esiintyy etenkin, jos huijaustapauksista syntyy oikeudenkäyntejä tai muita kiistoja, joita puidaan mediassa.

Näiden lisäksi pankille voi aiheutua oikeudellinen riski, mikäli se ei esimerkiksi pysty suojaamaan asiakkaidensa tietoja ja varoja riittävässä määrin johtaen sakkoihin tai muihin seuraamuksiin. Asiantuntija D nostaa esiin myös digihuijausten aiheuttamat yhteiskunnalliset riskit. Huijareille menetetyt rahat ovat pois kansantaloudesta ja sen sijaan rikollisten hallussa, jolloin niitä voidaan pahimmillaan hyödyntää rikollisuuden rahoittamiseen. Huijaukset voivat myös johtaa uhrien velkaantumiseen, jolla voi olla yhteiskunnallisia vaikutuksia. Digihuijaukset saattavat heikentää myös kuluttajien luottamusta digitaaliseen ostamiseen, mikä voi aiheuttaa verkkokaupoille vakaviakin taloudellisia seurauksia.

Mahdollisena operatiivisena riskinä tai jonkin muun riskin seurauksena haastateltavat nostavat esiin haasteet toimivien pankkipalveluiden tuottamisessa eli pankkien ydintehtävässä. Palveluiden tulisi olla mahdollisimman nopeita ja helppokäyttöisiä, jolloin asiakasprosessi olisi mahdollisimman sujuva ja palvelut vastaisivat teknologian kehittyviä vaatimuksia. Toisaalta pankkipalveluiden tulisi huijausten ennaltaehkäisemiseksi olla mahdollisimman turvallisia ja turvallisuuskontrollien tulisi toimia tehokkaasti, jotta rikolliset eivät pysty hyödyntämään järjestelmien heikkouksia

tai kiertämään turvatoimia. Mainehaitan aiheuttama ilmapiiri on yhä enemmän johtanut edellä mainittuun vaatimukseen asiakkaiden toimesta, mutta toisaalta turvallisuuskontrollien lisääminen voi vaikuttaa palveluiden käytettävyyteen ja nopeuteen negatiivisesti. Vaatimukset eriyvät asiakasryhmien välillä, jolloin pankkien on löydettävä näiden kahden tavoitteen välillä tasapaino, jolla voidaan myös osaltaan ennaltaehkäistä mainehaittaa.

Muita vakaviakin seurauksia pankeille voivat olla sääntelyseuraamukset ja operatiiviset häiriöt. Näiden lisäksi eräs seuraus pankkien kannalta on se, että riskien konkretisoituessa pankit pyrkivät oppimaan tapahtuneesta ja parantamaan toimintaansa, jolloin muun muassa riskienhallintastrategiat ja kontrollit voivat parantua.

Huijauksia toteutetaan julkisten organisaatioiden lisäksi myös pankkien nimissä. Haastateltavien mukaan tämä ja muiden huijausten lisääntyminen ei ole ainakaan huomattavasti vaikuttanut asiakkaiden luottamukseen pankkeja tai pankkipalveluita kohtaan, vaan pikemminkin asiakkaiden epäluuloisuuden kasvamiseen. Tämän vuoksi asiakkaat haluavat yhä enemmän vaikuttaa omien palveluidensa ja oman turvallisuutensa räätälöintiin. Toisaalta osa haastateltavista tuo esiin, että heidän havaintojensa mukaan joissain asiakassegmenteissä on ollut havaittavissa epäluottamusta suomalaisten pankkien toimintaa kohtaan, mikä on näkynyt varallisuuden siirroissa kryptovaluuttoihin ja ulkomaalaisiin pankkeihin. Tämä on heidän mukaansa ollut todennäköisesti seurausta huijausten lisääntymisestä ja uutisoinnista, vaikka itsessään pankin toiminnassa ei ole olisikaan tapahtunut muutoksia. Asiakkaat saattavat kokea, ettei pankki pysty suojaamaan heidän tietojaan tai varojaan. Vaatimukset huijausmaksujen estämisestä ovat näissä asiakasryhmissä todella korkeat, vaikka todellisuudessa huijausmaksut ovat hyvin pieni osa kaikesta tililiikenteestä, jossa on myös hyvin paljon tavallisia ulkomaanmaksuja. Toisaalta tapahtuneet tietomurrot ja huijaustapausten korvausvastuun selvittäminen ovat voineet vaikuttaa yksittäisiin asiakkaisiin tai asiakasryhmiin, ja julkisuuteen päätyessään nämä voivat vahingoittaa pankin mainetta ja brändiä sekä sen kykyä toimia markkinoilla. Estääkseen tällaisia tapauksia pankkien on investoitava jatkuvasti uusiin tietoturvaratkaisuihin ja koulutettava henkilökuntaansa sekä asiakkaitaan, mikä voi lisätä operatiivisia kustannuksia.

Asiantuntija A:n mukaan pankkien nimissä toteutettavat huijaukset eivät ole enää vastaavanlainen trendi kuin muutamia vuosia sitten, sillä huijausmuodot, jossa

tunnistautumistapana voi käyttää mitä tahansa pankkia, ovat tehokkaampia. Jos huijaus tapahtuu yhden pankin nimissä, vain kyseisen pankin asiakkaat kuuluvat huijauksen kohderyhmään. Lisäksi asiakkaita on pyritty kouluttamaan tarkistamaan verkkoselaimen URL-osoite, jonka avulla huijaussivustot voi tunnistaa.

4.3.2 Digihuijauksien aiheuttamat riskit pankkien asiakkaille

Pankkien asiakkaisiin kohdistuvien digihuijausten aiheuttamat riskit asiakkaille voidaan myös jakaa pääsääntöisesti kahteen kategoriaan, jotka nousivat haastatteluissa esiin. Merkittävin riski asiakkaalle on taloudellinen riski, jonka seurauksena on varojen ja pahimmillaan merkittävien säästöjen menettäminen. Asiakkaat saattavat kohdata vaikeuksia menetettyjen varojen palauttamisessa oikeusteitse, sillä huijareita ei aina pystytä identifioimaan, ja/tai heitä ei saada rikosoikeudelliseen vastuuseen teoistaan. Omien varojensa menettämisen lisäksi asiakas saattaa korvausvastuuseen huijarin hakemista lainoista, jotka voivat olla jopa hyvin korkeakorkoisia. Menetettyjen varojen ja lainojen takaisinmaksu voi vaikuttaa uhrin taloudelliseen tilanteeseen hyvin pitkään.

Toisena riskinä haastateltavat nostivat esiin asiakkaan yksityisyydensuojaan liittyvän riskin eli asiakkaan tiedot voivat vaarantua, jonka seurauksena hän voi esimerkiksi menettää henkilötietonsa. Asiakkaan menetettyä tunnistusvälineensä huijarille, voi siitä seurata muutakin haittaa, mutta yleensä vaikutukset ovat joko taloudellisia tai henkilötietoihin liittyviä.

Digihuijausten aiheuttamat teknologiset riskit puolestaan aiheutuvat, kun rikolliset hyödyntävät kehittyvää teknologiaa löytääkseen uusia keinoja huijata. Nämä voivat sisältää muun muassa haittaohjelmia, tietojenkalastelua ja muita teknisiä hyökkäyksiä.

Tämän lisäksi huijaukset voivat yleisesti olla uhreille hyvin traaginen kokemus, joka saattaa vaikuttaa myös läheisten hyvinvointiin. Riskien seurauksena voi pahimmassa tapauksessa olla huijauksen uhrin henkisen tasapainon järkkäminen.

Syynä digihuijauksen uhriksi joutumiseksi haastateltavat mainitsevat asiakkaiden tietämättömyyden tietoturvasta tai esimerkiksi sijoituskohteistaan. Toinen merkittävä syy on huijausten psykologinen aspekti, sillä rikolliset manipuloivat uhreja järjestelmällisesti, jolloin uhri saattaa uskoa toimivansa täysin oikein tai laillisesti. Tämän lisäksi asiakkaan

käyttämien laitteiden, kuten tietokoneen suojauksissa voi esiintyä puutteita, jotka mahdollistavat huijauksen tapahtumisen.

4.4 Pankkien digihuijauksiin liittyvät riskienhallintakäytännöt

4.4.1 Pankkien riskienhallintakeinot digihuijauksissa

Digihuijauksiin liittyvä riskienhallinta tapahtuu pankin organisaatorakenteen mukaan pääosin operatiivisessa tiimissä, reklamaatiokäsittelyssä ja kehityspuolella. Pankeilla on useita riskienhallintakeinoja asiakkaisiin kohdistuvien digihuijauksen torjumiseksi ja hallitsemiseksi. Haastateltavien mukaan pankit hallitsevat samanaikaisesti riskiä siitä, ettei asiakas tule huijatuksi ja toisaalta sitä, ettei pankki joudu korvausvastuuseen. Tärkeimpänä tavoitteena on estää varojen ja tietojen päätyminen rikollisille. Asiantuntija A:n mukaan kehitystöiden kannattavuuden laskeminen lähtee kuitenkin pankin tuloksesta ja siihen vaikuttamisesta. Digihuijauksiin liittyvä riskienhallinta on näin ollen osa strategista päätöksentekoa ja kokonaisvaltaista riskienhallintaa. Haastatteluiden perusteella digihuijauksia käsitellään operatiivisena riskinä.

Asiantuntija D:n mukaan: ”*Asiakas on puolustuslinja numero yksi*”, jolla hän viittaa siihen, että asiakas on merkittävässä roolissa siinä, päätyykö tämän verkkopankkitunnukset tai rahat rikollisille, sillä asiakas yleensä hyväksyy maksutapahtumat tai uuden laitteen käyttöönoton. Näin ollen pankin asiakkaalle antama vahva sähköinen tunniste ja sen ohjeiden mukainen käyttö on merkittävässä roolissa digihuijauksissa. Asiakkaan vahvistaessa tapahtumia verkkopankkitunnuksillaan, pankin voi olla haastavaa erottaa, onko kyseessä oikeasti asiakas vai huijari. Näin ollen asiakkaan on erittäin tärkeää tietää, mitä on tekemässä ja on siten merkittävässä asemassa riskienhallinnallisesti.

Yhdeksi tärkeimmäksi pankin riskienhallintakeinoksi haastateltavat nimeävät asiakkaan tuntemisen, johon kuuluu asiakkuuden avaamisen yhteydessä sekä asiakkuuden ylläpidossa tehtävät asiakkaan tuntemiseen liittyvät toimet. Ajantasaiset asiakastiedot ovat erittäin tärkeitä digihuijauksen ennaltaehkäisyssä ja havaitsemisessa, jotta pankit voivat tunnistaa asiakkaan normaalista poikkeavaa toimintaa. Asiakkaan tunteminen on sidoksissa asiakkuuden hallintaan, johon liittyy asiakkuuden avaamisen jälkeen

säännöllisesti toteutettava asiakkuuden riskillisyyden tarkastus ja siihen liittyvät tarvittavat toimenpiteet.

Kouluttaminen ja viestintä ovat myös tärkeä pankkien riskienhallintakeino huijauksien ennaltaehkäisyyn liittyen. Pankit järjestävät koulutuksia ja tiedotuskampanjoita asiakkailleen sekä henkilökunnalleen kertoakseen digihuijausten tunnistamisesta ja välttämisestä. Näin ne voivat estää asiakkaitaan joutumasta huijausten uhreiksi ja toisaalta vähentää korvausvastuutaan toteutettuaan regulaation asettaman tiedotusvelvollisuutensa. Viestintä on kuitenkin hyvin yleistä eikä erikseen kohdennettua. Ajantasaisten tiedotusten ja koulutusten lisäksi pankit määrittelevät poliitikoissa, periaatteissaan ja ohjeissaan henkilökunnalleen toimintaperiaatteita digihuijauksiin liittyen.

Kolmas merkittävä riskienhallintakeino jo tapahtuneissa huijauksissa on maksujen monitorointi, jonka tavoitteena on pysäyttää huijarille liikkuvat varat ja palauttaa ne asiakkaalle. Haastatteluissa ilmeni, että pankeilla on kehittyneitä järjestelmiä ja tietoturvaohjelmistoja, joiden avulla voidaan tunnistaa poikkeavat kortti- ja tilitapahtumat, minkä seurauksena asiakkaaseen voidaan olla yhteydessä tapahtuman asianmukaisuuden varmistamiseksi.

Asiantuntija B nostaa esille myös selkeiden ilmoituskanavien luomisen, joiden kautta työntekijät ja asiakkaat voivat raportoida epäilyttävistä toimista, minkä avulla voidaan estää esimerkiksi mahdollinen lisävahinko.

Teknologisista ratkaisuista myös palomuurit ja virustorjuntaohjelmat mainittiin haastatteluissa tärkeinä työkaluina huijausten torjumiseksi. Niiden lisäksi arkaluontoisten tietojen suojaaminen vahvoilla salauksilla ja pääsyn rajoittaminen vain tarpeellisille henkilöille on olennaista. Säännölliset tietoturva-auditoinnit ja haavoittuvuustarkastukset auttavat tunnistamaan ja korjaamaan mahdolliset heikkoudet ennen kuin ne voidaan hyödyntää.

Useassa haastattelussa nousi esiin myös pankkien tekemä tiivis yhteistyö viranomaisten ja muiden finanssialan toimijoiden kanssa huijausten torjumiseksi, tutkinnassa avustamiseksi, uusimpien huijausmenetelmien sekä parhaiden käytäntöjen jakamiseksi. Asiantuntija A:n mukaan pankit tekevät keskinäistä yhteistyötä regulaation

mahdollistamissa rajoissa eli jakavat tietoa yleisistä ilmiöistä yhteistyöfoorumeissa. Tämä lisäksi hän mainitsee yhteistyön poliisin, teleoperaattoreiden ja Kyberturvallisuuskeskuksen kanssa.

Pankit tekevät asiakkaisiin kohdistuvaa turvallisuuden hallintaa myös pyrkiessään saamaan asiakas ymmärtämään, että tätä on huijattu. Pankkien riskienhallintakeinot ovat rajalliset, etenkin kun asiakas toimii huijareiden manipuloimana. Tunnehuijaukset ovat sen suhteen haasteellisia, että asiakas haluaa tietoisesti lähettää rahaa tietämättä kuitenkaan lähettävänsä niitä huijarille. Haastatteluissa ilmeni, että on myös tapauksia, joissa asiakas tietää lähettävänsä rahaa rikollisille mutta toimii niin silti saadakseen näiltä jatkuvia yhteydenottoja. Näin ollen asiantuntija D korostaa, että pankkien riskienhallintakeinot ovat rajallisia, sillä Suomessa täysi-ikäinen ja -valtainen henkilö saa käyttää varojaan haluamallaan tavalla. Pankkien tulee estää varojen liikkuminen rahanpesun estämisen ja terrorismin rahoituksen torjuntaan liittyen, mikäli on tiedossa, että vastapuolena on rikollinen. Huijausmaksuissa tämä on kuitenkin harvoin tiedossa etukäteen.

Kuten yllä on todettu, pankit tekevät huijausten elinkaaren näkökulmasta aktiivisia riskienhallinnallisia toimenpiteitä, jotka sisältävät ennaltaehkäisyn, kuten asiakkaiden ohjeistamisen verkkopankin turvalliseen käyttöön, sekä jälkikäteiset toimet, kuten maksujen monitoroinnin, petosten selvittämisen rahavirtojen jäljittämiseksi ja varojen siirtymisen estämiseksi, sekä asiakkaiden tukemisen palautusprosessien ja vahingonkorvausmenettelyjen yhteydessä.

4.4.2 Digihuijauksiin liittyvät kontrollit ja turvatoimet

Pankkien korvausvastuun muodostumista pyritään ennaltaehkäisemään toimivien kontrollien laatimisella, kuten hälytysten ja asiakkaiden varoittamisen avulla. Kortti- ja tilimaksamisessa pankeilla on käytössä hieman erilaisia riskienhallintakeinoja ja -kontrolleja.

Haastatteluiden perusteella verkkopankkitunnukset ovat tärkein kontrolli. Ne luovutetaan asiakkaalle todennetusti. Asiakkaiden tilien ja varojen suojaamiseksi pankeilla on käytössä kaksivaiheinen tunnistautuminen, jossa käyttäjältä vaaditaan toinen vahvistusvaihe, kuten tekstiviestikoodi. Tämän lisäksi mobiilisovelluksen tai

verkkopankin tapahtumien vahvistamiseksi voidaan lähettää asiakkaille vahvistusviestejä esimerkiksi verkkopankin käyttöönoton tai maksutapahtumien yhteydessä. Verkkopankin asennus ja käyttöönottoprosessi sisältää useita monivaiheisia toimenpiteitä, jotka on suunniteltu estämään kalastelurytykset ja muut tietoturvaohauhat. Uuden tunnistusvälineen käyttöönotossa voidaan myös vaatia lisävahvistuksia. Esimerkiksi asiantuntija B:n mukaan vahvistussovelluksen käyttöönottoon on tehty parannuksia, jotta varmistetaan, että asiakas ottaa sovelluksen käyttöön itse. Tämä saavutetaan informatiivisilla aktivointivaroitusviesteillä, jotka ohjaavat asiakasta prosessin läpi ja varmistavat, että hän ymmärtää kaikki vaiheet.

Lähettäessään vahvistusviestejä maksun tai tapahtuman kontekstiedon avulla pankki hallitsee riskiä korvausvastuuseen joutumisesta ja pyrkii estämään huijauksen tapahtumisen. Asiantuntija D:n mukaan korvausvastuun selvittämisessä otetaan huomioon, olisiko asiakkaan täytynyt ymmärtää vahvistusviestistä, mitä hän oli tekemässä. Näin ollen kontrollina maksujen vahvistusviestit ovat sekä asiakkaan, että pankin edun mukaisia.

Asiakkaan tuntemiseen liittyvät kontrollit liittyvät toimenpiteisiin, joilla varmistetaan asiakkaalle tyypillinen toiminta, eli esimerkiksi tämän tyypillinen rahaliikenne ja sen erityispiirteet esimerkiksi ulkomaanmaksuineen. Lisäksi siihen liittyy muun muassa poliittisesti vaikutusvaltaisten asiakkaiden tunnistaminen, sillä pankit ovat rahanpesusäädösten perusteella velvollisia tuntemaan asiakkaansa (KYC). Mikäli asiakastietoja ei saada päivitettyä, voidaan asiakkaan palveluita rajoittaa, kunnes tiedot saadaan päivitettyä. Asiakkuuden hallintaan liittyviä kontrolleja ovat puolestaan esimerkiksi korkean rahanpesuriskin asiakkuuksien tunnistaminen ja siihen liittyvät kontrollit, joiden avulla asiakkuutta voidaan seurata väärinkäytösten ennaltaehkäisemiseksi.

Pankeilla on käytössään kehittyneitä järjestelmiä, jotka tunnistavat asiakkaan poikkeavaa maksuliikennettä, hyödyntävät big dataa ja hälyttävät mahdollisista epäilyttävistä tapahtumista. Maksujen monitoroinnissa pyritään tunnistamaan anomalioita ja luomaan riskipisteytyksiä, joiden avulla huijausmaksuja voidaan tunnistaa ja estää siten mahdolliset petokset. Monitoroinnissa maksuja voidaan estää, viivästyttää tai palauttaa maksajalle, mikäli on epäily, että kyseessä on huijausmaksu. Näiden lisäksi asiakkaalta saatetaan varmistaa eri keinoin, haluaako hän varmasti tehdä kyseisen maksun. Maksujen

monitoroinnissa on haastatteluiden perusteella tarkoitus muodostaa tietyillä reunaehdoilla hälytyksiä, joiden joukosta pyritään erottamaan epäilyttävät maksutapahtumat. Maksuihin liittyvät kontrollit voivat liittyä muun muassa niiden suuruuteen, maaviitteisiin, tiheyteen tai viesteihin. Jälkikäteinen kontrolli digihuijauksen tapahtumisen jälkeen on kortin tai tilin sulkeminen, kun asiakas ilmoittaa pankille, että hänen tietonsa ovat päätyneet väärin käsiin. Pankeilla on käytössä ympärivuorokautiset puhelinnumerot, joihin asiakkaat voivat soittaa kyseisissä tapauksissa.

Asiakkaiden turvatoimet, kuten asiakkaiden tilinkäyttövälineiden rajoitteet ovat myös tärkeä osa digihuijauksen riskienhallintaa. Haastatteluiden perustella osa pankeista tarjoaa mahdollisuuden asettaa maksukortteihin sekä euromääräisiä että aluekohtaisia turvarajoja, jolloin korttia ei voi käyttää tietyn summan tai alueen ulkopuolella muuttamatta turvarajoja. Tilisiirtojen osalta on olemassa maantieteellisiä aluerajoituksia (geo-blocking), jotka estävät rahansiirrot tiettyihin maihin, ellei asiakas muuta näitä erikseen verkkopankkinsa kautta. Tämän lisäksi myös tilisiirroille on mahdollista asettaa euromääräisiä rajoitteita, jotka rajoittavat kerralla siirrettävän rahamäärän suuruutta. Asiantuntija B:n mukaan tämä antaa asiakkaalle enemmän hallintaa ja joustavuutta omien turvallisuusasetustensa suhteen, mikä parantaa kokonaisvaltaista turvallisuutta ja käyttökokemusta. Haasteita kuitenkin aiheuttaa se, että saadessaan asiakkaan verkkopankin tai mobiilisovelluksen hallintaansa, huijari voi yleensä muuttaa kyseisiä rajoja.

Haastatteluissa ilmeni vaihtelevuutta sen suhteen, onko kontrolleja lisätty tai päivitetty. Kaikkien haastateltavien mukaan kontrolleja tarkastellaan säännöllisesti, mutta osa haastateltavissa kertoi, että heidän edustamassaan pankissa kontrolleja on lisätty paljonkin, toisten mukaan taas hyvin vähän pelkästään digihuijauksiin liittyen. Useat haastateltavista kuitenkin korostivat, että digihuijauksen ennaltaehkäisy ja tunnistaminen on ”jatkuva kilpajuoksua rikollisten kanssa”, sillä ammattimaiset rikolliset pohtivat jatkuvasti uusia ja tehokkaampia keinoja tehdäkseen onnistuneita huijauksia. Näin ollen pankkien on säännöllisesti päivitettävä järjestelmiään, koulutettava henkilöstöään ja hyödynnettävä uusia teknologioita asiakkaiden turvallisuuden ja pankin maineen suojelemiseksi.

4.4.3 Asiakaskokemuksen säilyttäminen digihuijaustapauksissa

Pankit ovat yhä tietoisempia asiakaskokemuksen merkityksestä myös huijaustapausten yhteydessä. Pankit pyrkivät huomioimaan asiakaskokemuksen säilymisen digihuijausten ennaltaehkäisyssä ja niiden tapahduttua usealla eri tavalla, vaikka keinot ovat hyvin rajalliset. Asiantuntija A toteaa asiakaskokemuksen huomioimisesta seuraavasti:

”Me yritetään huomioida asiakaskokemus siis siten, että vaikutetaan mahdollisimman vähän oikeaan maksamiseen. Ja haitataan sitä mahdollisimman vähän. Me haluamme pysäyttää mahdollisimman paljon huijausmaksuja. Ja tavallaan sen balanssin löytäminen on sitten se, minkä kanssa tässä tasapainotellaan.” (Asiantuntija A)

Kyse on siis tasapainottelusta kahden hyvin erilaisen toimintamallin välillä, sillä riskienhallintatoimenpiteet yleensä vaikeuttavat tai hidastavat jollain tavoin maksamista. Asiantuntija B:n mukaan asiakaskokemusta voidaan kuitenkin parantaa kehittämällä turvallisempia ja käyttäjäystävällisempiä palveluita sekä kehittämällä ennakoivia riskienhallintastrategioita, jotka perustuvat reaaliaikaiseen data-analyysiin ja ennusteisiin.

Asiakaspalvelun laatu on avainasemassa ja pankeilla on huijaustapausten käsittelyyn erikoistuneet henkilöt, jotka auttavat asiakkaita palauttamaan varoja ja suojaamaan tilejä tulevilta hyökkäyksiltä. Asiakkaille tiedotetaan säännöllisesti turvallisuuskäytännöistä ja huijauksilta suojaumisesta. Tiedotteet voivat sisältää tietoa ja varoituksia uusista huijausmenetelmistä sekä ohjeita turvalliseen pankkiasiointiin.

Asiakaskokemusta on haastatteluiden perusteella se, ettei asiakas menetä rahoja huijareille, mikä on siis tavoite. Täten nopea reagointi, kuten tilivarojen välitön jäädyttäminen tai epäilyttävien tapahtumien tutkiminen, on asiantuntija B:n mukaan tärkeää, jotta asiakkaat kokevat olonsa turvalliseksi ja luottavaiseksi. Mikäli varojen menetystä kuitenkin tapahtuu, pyritään varmistamaan, että asiakaspalvelussa on riittävät ohjeet, joilla asiakasta pystytään auttamaan muun muassa ohjaamalla tämä rikosuhripäivystykseen ja luomaan täten mahdollisimman hyvä asiakaskokemus, jotta asiakas saa tarvitsemansa avun. Pankki ei kuitenkaan välttämättä korvaa menetettyjä varoja, mikä tekee asiakaskokemuksen säilymisestä hyvin haastavaa. Etenkin jos asiakas kokee, että pankki olisi voinut vaikuttaa varojen menettämisen ennaltaehkäisyyn, leimaa

tämä usein koko loppua asiakassuhdetta. Mikäli pankki on kuitenkin tehnyt varsinaisen virheen eikä kyse ole niinkään korvausvastuustasiasta, hyvittää pankki asiakkaalle virheensä.

Asiakaskokemus ja siihen vaikuttaminen eroaa haastatteluiden perusteella jonkin verran eri digihuijausmuodoissa. Esimerkiksi pidempiaikaisissa sijoitus- ja rakkaushuijauksissa uhrilta pyydetään usein aluksi pienempi rahasiirto, jotta hän ikään kuin varmistuu esimerkiksi sijoitussivuston luotettavuudesta. Tehdessään seuraavan isomman siirron, asiakas on usein vakuuttunut toimintansa oikeellisuudesta ja saattaa näin ollen reagoida hyvin kielteisesti pankin pysäyttäessä maksun. Kalasteluhuijauksissa puolestaan haastatteluiden perusteella asiakkaiden suhtautuminen pysäytettyihin maksuihin on lähtökohtaisesti positiivinen. Asiakkaan ajattelutapa vaihtelee näin ollen eri huijauksissa, mikä tekee pankkien toiminnasta asiakaskokemuksen säilyttämiseksi yhä haastavampaa.

4.4.4 Käytännön haasteet digihuijauksista aiheutuvien riskien hallinnassa

Yhtenä merkittävämpänä käytännön haasteena asiakkaisiin kohdistuvien digihuijausten riskienhallinnassa haastateltavat nostavat esiin, ettei huijausprosessista ole paljoakaan pankin vaikutuspiirissä. Tämä tarkoittaa sitä, että esimerkiksi sijoitushuijauksessa asiakas on saattanut olla jo pitkään tekemisissä huijarin kanssa ennen kuin asiakas tekee huijaussivustolle maksun, jonka seurauksena huijaus paljastuu pankille, kun asiakas puolestaan on jo pitkään uskonut huijaukseen. Näin ollen pankki näkee vain hyvin pienen osan koko huijauksesta ja asiakkaan rooli puolustuslinjana korostuu. Tunnehuijausten odotetaan haastatteluiden perusteella lisääntyvän tulevaisuudessa, mikä hankaloittaa pankkien riskienhallinnallisia toimia huijausten ehkäisemiseksi, sillä tekniset keinot ovat rajallisia, kun uhri on manipuloitu huijauksen uhriksi. Näin ollen huijausten ennaltaehkäisemiseksi pankkien on jatkuvasti koulutettava asiakkaitaan digihuijauksista, mikä voi olla haastavaa rajallisten resurssien ja oikean kohderyhmän tavoittamisen vuoksi.

Toinen merkittävä haaste on se, että pankkien tulisi pystyä poimimaan suuresta datamassasta yksittäiset poikkeukselliset maksutapahtumat, joita tehdessään asiakas voi kuitenkin olla tunnistautuneena laitteella, jolla normaalistikin asioi. Haastatteluissa nousi lisäksi esiin, että vastatili, jolle huijatut rahat siirretään, on usein toisessa pankissa. Lähtökohtaisesti pankit luottavat siihen, että vastaanottajapankki on tehnyt tarvittavat

KYC-toimenpiteet maksun vastaanottajalle, minkä lisäksi maksupalvelulain mukaan pankin tulee suorittaa viipymättä asiakkaan tekemä maksu, ellei vastaanottaja ole tiedetysti rikollinen taho. Näin ollen merkittävänä nykyhetken ja tulevaisuuden haasteena haastateltavat pitävät tasapainottelua maksamisen helppouden ja nopeuden sekä toisaalta turvallisuuden välillä. Asiantuntija D nostaa esiin myös voimaan tulevan sepapikasiirron, jonka seurauksena rahan tulee olla vastaanottajan tilillä 10 sekunnissa, johon sisältyy myös arvio siitä, onko kyseessä petollinen maksutapahtuma. Täten pankkien riskienhallintaprosessien tulee olla erittäin tehokkaita, jottei petollisia maksuja välity.

Kaksi haastateltavista tuo esiin sosiaalisen median alustojen vastuun. Molemmat heistä nimeävät esimerkkinä Metan, jonka alustoja (esimerkiksi Facebook) huijarit hyödyntävät mainostamisessa. Mikäli pankit ilmoittavat kyseisistä huijausmainoksista tällaiselle toimijalle, ilmoittaa tämä lähtökohtaisesti aina, ettei mainos riko yhteisönormeja. Kyseisillä toimijoilla on kaupalliset intressit, sillä kyseessä on maksettu mainostila, eikä näin ollen huijausmainosten kitkeminen ole yhtä tehokasta, kuin voisi parhaimmassa tapauksessa olla. Asiantuntija D nostaa esiin myös sen, että etenkin merkittävimmiltä IT-yrityksiltä toivottaisiin enemmän muun muassa teknologisten resurssien hyödyntämistä huijaussivustojen ja -mainosten tunnistamisessa, jolloin huijausten ennaltaehkäisy ja torjunta jakautuisi useammalle toimijalle. Operaattoreiden Sender ID-muutos on auttanut huijausten ennaltaehkäisyssä, mutta myös niiltä toivottaisiin aktiivisempia toimia, sillä etenkin SMS-viestien vaikea seulonta ja pikaviestisovellusten salausta ovat merkittäviä tekijöitä huijauksissa, sillä yhdestä puhelinnumerosta voidaan lähettää tuhansittain huijausviestejä.

Sääntelyn noudattaminen ja lainsäädännön muutokset nousevat esiin myös kolmessa haastattelussa. Nykyisinä haasteina kaksi haastateltavista nostaa esiin pankkien keskinäisen sekä muiden organisaatioiden kanssa tapahtuvan tiedonvaihdon huijauksiin liittyen, mitä sääntely ei nykyisellään tue muun muassa tiukkojen pankkialaisuussäännösten ja GDPR:n vuoksi. Haastatteluiden perusteella esimerkiksi tiedonjako huijauksissa käytettävistä tileistä voisi estää niiden laajuutta. Tämän lisäksi regulaatio asettaa tiukkoja vaatimuksia asiakastiedon käyttötarkoituksen määrittelyyn ja kuvaamiseen. Koska digihuijaukset ovat muuttuvia ilmiöitä ja samoja tietoja voitaisiin tarvita useaan eri tarkoitukseen, nostaa asiantuntija A esille byrokraattisen haasteen ja

siten toimintaan vaikuttavan hitauden, joka ilmenee, mikäli tilimaksamisen monitoroinnissa käytettäviä tietoja tarvittaisiin myös korttimaksamisen monitoroinnissa.

Tulevaisuudessa etenkin EU-tasolta odotetaan lisää sääntelyä, johon pankkien tulee sopeutua. Sääntelyviranomaisten odotetaan mahdollisesti asettavan tiukempia vaatimuksia tietoturvalle ja riskienhallinnalle. Asiantuntija D:n mukaan muun muassa UK:ssa on käytännössä lainsäädäntö, joka velvoittaa yhä useammassa tapauksissa korvaamaan uhrille tämän huijauksessa menettämät varat. Tämä on pankille riski osakkeenomistajien suhtautumisen kannalta sekä sen vuoksi, että asiakas saattaa joutua useita kertoja huijauksen uhriksi saatuaan menettämänsä varat takaisin. Kyseinen lainsäädäntö on johtanut asiantuntija D:n mukaan siihen, että pankit ulkomailla pysäyttävät maksuja aiempaa enemmän, mikä hankaloittaa kuluttajien asiointia ja täten heikentää luottamusta maksamiseen. Lisäksi lainsäädäntö saattaa aiheuttaa Fraud friendly nimellä kutsuttavaa ilmiötä, jossa osa ihmisistä tekaisee huijauksia esimerkiksi tuttaviansa kesken saadakseen pankilta korvauksia, vaikkei ole todellisuudessa menettänyt lainkaan varoja. Näin ollen lainsäädännölliset muutokset voivat vaikuttaa huomattavasti pankkien ja asiakkaiden asemaan sekä toimintaan. Vastaavanlaisen sääntelyn odotetaan koskevan myös Suomea, kun PSR (Payment Services Regulation) tulee tulevina vuosina voimaan. Sääntelyssä muun muassa pankkien korvausvastuu tiukentuu siten, että mikäli huijaus on tehty pankin nimissä, tulee sen korvata huijauksessa menetetyt varat. Tämä voi mahdollisesti aiheuttaa asiakkaiden epärehellistä toimintaa korvauksen saamiseksi, mikä voi aiheuttaa asiakkaiden välillä eriarvoisuutta ja lisätä pankkien taloudellisia menetyksiä lisääntyneen korvausvastuun lisäksi.

Tulevaisuuden haasteina haastateltavat nostavat esiin myös huijausten kompleksisuuden lisääntymisen ja siten tarpeen mukautua aiempaa nopeammin. Asiantuntija A:n mukaan huijarit eivät yleensä tee järjestelmiinsä aikaa ottavia muutoksia. Pankit puolestaan eivät voi nopeasti vaihtaa peruspankkijärjestelmän toimittajaa ja yleisesti järjestelmämuutokset vaativat aikaa, minkä vuoksi pankkien haasteena on hitaus reagoimisessa ympäröivän maailman muutoksiin. Asiantuntija B:n mukaan käytännön haaste tietoturvan ylläpidon lisäksi on jatkuva tarve päivittää pankin tietoturvajärjestelmiä.

Haastateltavien mukaan tulevaisuudessa on odotettavissa muutoksia muun muassa asiakkaiden tunnistautumistapoihin esimerkiksi EUID:n myötä. EUID toimii yksiköllisenä tunnisteena, ja antaa käyttäjille täyden hallinnan valita sekä seurata, mitkä

osat heidän identiteetistään, tiedoistaan ja sertifikaateistaan jaetaan kolmansille osapuolille (European Commission, 2024). Toisaalta tunnistautumistavasta riippumatta huijareiden käyttämät sosiaalisen manipuloinnin keinot voivat saada asiakkaan tekemään huijareiden haluamia asioita, jolloin huijarit vain keksivät uuden tavan hyödyntää tunnuksia. Haastatteluiden perusteella esimerkiksi mobiilivarmenteen käytön lisääntyttyä huijarit alkoivat kalastelemaan mobiilivarmenteita saaden täten pääsyn esimerkiksi potilastietoihin ja luottorekisteriin, jonka jälkeen huijarit kiristivät uhrejaan kyseisillä tiedoilla.

Resurssien hallinta nousi myös esiin kolmessa haastattelussa. Pankkien on kohdennettava riittävästi resursseja riskienhallintaan, ja haastatteluiden perusteella digihuijausten ja niiden aiheuttamien hälytysten lisäämänä resursointitarvetta on ollut sekä operatiivisella puolella että kehityspuolella.

4.4.5 Riskienhallintakäytäntöjen kehittäminen ja teknologian hyödyntäminen

Kaikki haastateltavista olivat yhdenmukaista mieltä siitä, että merkittävimmät tulevaisuuden kehityskohteet digihuijausten ennaltaehkäisyssä ovat tietoisuuden lisääminen ja teknologian hyödyntäminen.

Tietoisuutta lisäisi esimerkiksi pankkien ja muiden finanssialan toimijoiden tiiviimpi yhteistyö ja tiedonjako huijauksista. Säännölliset koulutukset ovat keskeisiä niin työntekijöiden kuin asiakkaiden kannalta, jotta huijaukset tunnistetaan ja niihin liittyen osataan oikeat toimintatavat. Teknologiaa voidaan hyödyntää tietoisuuden lisäämisessä käyttämällä sitä koulutusten ja resurssien luomisessa, minkä avulla voidaan auttaa asiakkaita tunnistamaan ja välttämään huijauksia. Asiantuntija D nostaa esille taloustaitojen ohella digihuijauksista opettamisen mahdollisuuden jo peruskoulutusta lähtien. Näin ollen kansalaisosaaminen voisi vähitellen nousta tasolle, jossa yksinkertaisimmat huijaukset eivät enää toimisi. Tärkeää olisi hänen mukaansa koulutus myös kryptovaluutoista, jotta ihmiset osaisivat validoida niihin liittyviä tietoja, joita huijauksissa uhreille kerrotaan.

Haastatteluiden perustella tulevaisuudessa pankit tulevat todennäköisesti hyödyntämään entistä enemmän tekoälyä ja koneoppimista huijausten havaitsemisessa ja estämisessä. Tekoälyratkaisuita voitaisiin haastateltavien mukaan hyödyntää esimerkiksi

monitoroinnin tukena, sillä sen avulla voidaan suodattaa tärkeää tietoa laajasta datamassasta ja verrata eri järjestelmien välisten tietojen yhteneväisyyksiä nopeuttaen epäilyttävien maksutapahtumien eli hälytysten tutkintaa. Lisäksi sen avulla voidaan luoda tarkempia havaintoja kuin ihmiset pystyvät tekemään laajan datamassan käsittelyn avulla, mutta haastateltavat eivät kuitenkaan usko, että tekoäly voisi täysin korvata ihmisten tekemää työtä ja päätöksentekoa digihuijausten ennaltaehkäisyssä ja tutkinnan parissa.

Haastatteluissa kuitenkin ilmeni haasteet liittyen 2024 voimaan tulleeseen tekoälysäädökseen, sillä siinä on tarkasti rajattu, mihin tekoälyä saa käyttää ja rajattu pois automaattinen päätöksenteko sekä profilointi. Tulevaisuudessa osa haastateltavista uskoo kuitenkin sääntelyn muuttuvan mahdollistaen tekoälyn hyödyntämisen muun muassa monitorointimalleissa, jotka tunnistavat asiakkaan käyttäytymisestä eli maksamisen lisäksi asioinnista sen, onko kyseessä oikea asiakas vai huijari.

Nykyisin on saatavilla digitaalisia henkilökohtaisia avustajia, joilla on kyky muistaa aiempia keskusteluita ja joiden kanssa käyttäjä voi käydä keskustelua esimerkiksi korvaan asetettavan laitteen kautta. Asiantuntija D:n mukaan riippuen siitä, miten digitaalista avustajaa koulutetaan, tulevaisuudessa voisi olla mahdollista, että avustaja tunnistaisi saapuvista puhelusta huijauksiin viittaavia elementtejä. Tämä kuitenkin vaatisi sen, että avustajalla olisi käytössä laaja kielimalli, muisti ja paljon dataa, jonka avulla se voisi verrata saapunutta puhelua esimerkiksi väitettyyn poliisin numeroon.

Tekoälyn hyödyntämiseen on kuitenkin sidoksissa myös muutokset asiakkaiden tunnistautumisessa. Haastatteluissa nousi esiin myös data-analytiikan hyödyntäminen digihuijausten ennaltaehkäisyssä ja havaitsemisessa. Sen avulla järjestelmä voi oppia esimerkiksi tunnistamaan asiakkaan sen perusteella, miten tämä pitää puhelinta kädessään. Näin ollen puhelimen päätyessä huijarille hälyttäisi järjestelmä siitä, ettei puhelin ole todennäköisesti sen ihmisen kädessä, joka on aikaisemmin tehnyt maksuja. Toisaalta tunnistautuminen voi tapahtua myös biometriikalla eli esimerkiksi sydämen sykkeellä, sormenjäljellä tai kasvojen avulla, mikä parantaisi Asiantuntija B:n mukaan merkittävästi turvallisuutta.

Haastateltavat toivat kuitenkin esiin, että tulevaisuuden muutokset ovat hyvin riippuvaisia siitä, mitä sääntelyssä hyväksytään, sillä esimerkiksi yksityisyyden suojan lainsäädäntö tuo muutoksiin omat rajoituksensa. Tällä hetkellä tekoälyä hyödynnetään haastatteluiden

perusteella pankeissa digihuijausten tunnistamiseksi ja ennaltaehkäisemiseksi eri tavoin ja määrin. Osa haastateltavista korosti, ettei täysin toimivaa sovellusta kyseisen pankin tarpeeseen ole vielä ollut tarjolla.

Kokonaisvaltainen asiakkuuden tarkastelu on myös yksi mahdollinen tulevaisuuden suuntaus digihuijausten ennaltaehkäisyyn liittyen. Tällä haastatteluissa viitattiin siihen, että mikäli asiakkaalla on epäilyttäviä maksutapahtumia kortilla, tulisi pohtia, täytyykö pankin silti sallia asiakkaan tilimaksaminen, tunnistautuminen tai lainanhaku vai voidaanko näitä rajoittaa. Haasteita kuitenkin tuo se, ettei regulaatio vaadi tällaista tarkastelua, jolloin tahtotila muutokseen täytyy löytyä pankista itsestään.

5 YHTEENVETO JA JOHTOPÄÄTÖKSET

5.1 Tutkimuskysymyksiin vastaaminen ja johtopäätökset

Tutkielman tavoitteena oli vastata kolmeen johdannossa esitettyyn tutkimuskysymykseen. Ensimmäinen tutkimuskysymys pyrki selvittämään, millainen ilmiö on pankkien asiakkaisiin kohdistuvat digihuijaukset. Haastatteluaineiston analyysin perusteella pankkien asiakkaisiin kohdistuvat digihuijaukset ovat laaja, moniulotteinen ja jatkuvasti kehittyvä ilmiö. Digihuijaukset ovat tietoverkkoavusteisia huijauksia, joissa uhreja lähestytään digitaalisten kanavien kautta. Ilmiö on monisyinen ja ihmisten psykologisen heikkouksien hyödyntämisen lisäksi kehittyneen teknologian hyödyntäminen tekee huijauksista yhä vaikeammin torjuttavia. Kuluttajien tietämättömyys ja digitaalinen osaamattomuus altistavat huijauksille. Huijauksissa pyritään vetoamaan uhrin tunteisiin kuten kiireeseen ja tämän lisäksi niissä hyödynnetään ihmisten luottamusta ja tietämättömyyttä esimerkiksi taloudellisista tuotteista, kuten kryptovaluutoista. Suomalaisten pankkien asiakkaisiin kohdistuvat yleisimmät digihuijaukset voidaan jakaa kahteen pääkategoriaan, sekä edelleen alakategorioihin, jotka on esitelty taulukossa 1.

Taulukko 1 Yleisimmät digihuijaukset

Huijausmuoto	Selite	Alakategoriat
Maksajan manipulointiin perustuvat huijaukset (ts. tunnehuijaukset)	Asiakas manipuloimaan tekemään tilisiirto ja vahvistamaan tapahtuma	Sijoitushuijaukset, rakkaushuijaukset, dokumenttihuijaukset, valepoliisihuijaukset, useimmat deepfake-huijaukset
Pankkitunnusten/korttitietojen haltuunottoon perustuvat huijaukset	Huijari pyrkii saamaan pankkitunnukset tai kortin tiedot haltuunsa ja tekemään maksuja vapaasti	Tietojen kalastelu, verkkokauppa- ja kauppapaikkahuijaukset, arpajaishuijaukset

Teorialuvussa esitettyyn Finanssialan huijaustilastoon viitattiin yhdessä haastattelussa ja myös kolmessa muussa haastattelussa kyseiset huijausmuodot nousivat esille, joten taulukko vastaa pitkälti kyseistä tilastoa.

Keskeisiä trendejä digihuijauksiin liittyen ovat sosiaaliseen manipulointiin hyödyntäminen sekä tekoälyn käyttö, joista jälkimmäinen nousi haastattelumateriaalissa vahvemmin esiin, kuin tutkielman teoreettisessa osuudessa. Teknologinen kehitys, kuten deepfake-teknologia mahdollistaa entistä monimutkaisempien ja aidompien huijausten toteutuksen. Lisäksi sosiaalinen manipulointi ja tietojenkalastelun uudet muodot, kuten turvatilihuijaukset ovat lisääntyneet. Toisaalta haastatteluissa ilmeni, että huijauksissa käytettävät tarinat ovat pysyneet melko samankaltaisina pidemmän aikaa. Huijauksissa käytetään laajasti erilaisia viestintäkanavia, kuten sähköpostia, tekstiviestejä, puheluita ja sosiaalista mediaa. Uutena trendinä voidaan pitää kaupankäyntialustoilla tapahtuvia, varsinkin myyjiin kohdennettuja, huijauksia. Etenkin teknologian kehitys ja huijauksista saatavat tuotot ovat johtaneet huijausten muuttumiseen ammattimaiseksi, ja huijauksia toteutetaan organisoituina kampanjoina, sillä Fraud as a Service-ilmio mahdollistaa huijauspalveluiden myymisen pienemmille rikollisryhmille ja muille toimijoille.

Johtopäätöksenä voidaan todeta digihuijausten olevan monitasoinen ja globaalisti kasvava ongelma, joka on osa järjestäytyntä rikollisuutta ja jolla on kytköksiä muihin rikoksiin, kuten rahanpesuun. Etenkin teknologisten työkalujen käyttö yhdistettynä sosiaalisen manipulointiin altistaa varsinkin digitaalisesti osaamattomat kuluttajat huijauksille.

Toisella tutkimuskysymyksellä selvitettiin, millaisia pankkeihin ja niiden asiakkaisiin kohdistuvia riskejä digihuijaukset aiheuttavat. Haastatteluiden perusteella pankit kohtaavat erilaisia taloudellisia, maineeseen liittyviä ja operatiivisia digihuijausten aiheuttamia riskejä. Pankkien riskienhallinnan ja turvallisuusjärjestelmien on jatkuvasti kehityttävä huijauksien monimutkaistumisen ja lisääntymisen myötä. Taloudellinen riski voi realisoitua, mikäli pankki joutuu korvausvastuuseen asiakkaan menettämistä varoista, jotka voivat pahimmillaan olla pitkäaikaisia säästöjä. Haastatteluissa ei kuitenkaan noussut esiin huolia pankkien operatiiviseen resilienssiin liittyen, sillä nykyisen lainsäädännön mukainen digihuijausten aiheuttama korvausvastuu ei vaikuta olevan erityisen suuri tekijä suhteessa pankkien liiketoimintaan. Suomen Pankin tilaston mukaan vuonna 2023 pankit ottivat vastuulleen vain 4 % petollisten tilisiirtojen tappioista, kun

taas asiakkaille jäi vastattavaksi 92 %, mikä johtuu nykyisestä tavasta tulkita lainsäädäntöä yleensä kuluttajan vahingoksi (Kuluttajaliitto, 2024b). Näin ollen voidaan todeta, ettei tämänhetkisen lainsäädännön puitteissa taloudellinen riski ole pankeille yhtä merkittävä kuin asiakkaille.

Maineriskiä pankeille voi puolestaan aiheuttaa huijaustapauksista syntyvä julkisuus, oikeudenkäynnit ja negatiivinen mediahuomio, mikä voi johtaa pankin maineen heikentymiseen. Oikeudellinen riski voi olla aiheutua esimerkiksi korvausvastuun realisoituessa tai pankin virheellisestä reklamaatiokäsittelystä huijaustapauksessa. Tietosuoja- ja turvallisuusvelvoitteiden laiminlyönneistä seurauksena voi olla sakkoja tai muita sääntelyseuraamuksia, jotka aiheuttavat pankille sääntelyriskin. Yhteiskunnallisena riskinä voidaan pitää menetettyjen varojen päätymistä rikollisten haltuun, mikä voi heikentää kansantaloutta ja lisätä rikollisuuden rahoittamista. Toisaalta huijausten myötä myös kuluttajien luottamus esimerkiksi verkkokauppoihin voi heikentyä. Digihuijausten aiheuttamien riskien ennaltaehkäisemiseksi pankkien täytyy tasapainotella palveluiden nopeuden ja turvallisuuden välillä. Asiakkaat vaativat helppokäyttöisiä palveluita, mutta turvallisuustoimenpiteiden lisääminen voi hidastaa prosesseja, mikä voidaan itsessään nähdä myös pankkien maineeseen kohdistuvana riskinä. Pankkien on myös mukautettava palveluitaan asiakassegmenttien vaihtelevien luottamus- ja turvallisuusodotusten mukaisesti.

Digihuijaukset aiheuttavat pankkien asiakkaille eli tämän tutkielman tapauksessa huijausten uhreille hyvin monenlaisia riskejä. Taloudellinen riski on usein niistä merkittävin, sillä suorat rahalliset menetykset ja korvausvastuut huijareiden hakemista lainoista voivat olla merkittäviä. Yksityisyydensuojaan liittyvät riskit voivat aiheutua asiakkaan henkilötietojen ja tunnistusvälineiden väärinkäytöstä, joka voi johtaa pitkäaikaisiin ongelmiin ja epävarmuuteen. Kehittyvät teknologiset hyökkäykset, kuten haittaohjelmat ja tietojenkalastelu lisäävät puolestaan uhkaa asiakkaiden tietoturvalle aiheuttaen teknologisen riskin. Näiden lisäksi huijauksen uhriksi joutuminen voi aiheuttaa vakavia henkisiä seurauksia, kuten taloudellista stressiä ja pahimmassa tapauksessa pitkään jatkunut ahdinko voi aiheuttaa uhrille vakavaa henkisen tasapainon järkkymistä.

Keskeisenä johtopäätöksenä voidaan todeta digihuijausten aiheuttavan suorien taloudellisten tappioiden lisäksi muita riskejä, kuten kuluttajien luottamuksen

heikentymistä. Pankeille digihuijaukset aiheuttavat korvausvastuun lisäksi etenkin maineeseen ja oikeudelliseen asemaan liittyviä riskejä, kuluttajille puolestaan taloudellisia tappioita ja mahdollisesti jopa pitkäkestoisia vaikutuksia henkiseen hyvinvointiin ja yksityisyydensuojan heikkenemistä. Keskeiset digihuijausten aiheuttamat riskit on koottu taulukkoon 1. Yhteiskunnalliset riskit eivät varsinaisesti olleet tutkimuksen kohteena, mutta nousivat kuitenkin haastatteluissa useasti esiin, joten digihuijausilmiön kokonaisvaltaisen ymmärryksen vuoksi ne on nostettu esiin tutkielman empiirisessä osiossa.

Taulukko 2 Digihuijausten aiheuttamat riskit

Osapuoli	Riskit
Pankit	Taloudellinen riski, maineriski, operatiivinen riski, oikeudellinen riski, sääntelyriski
Asiakkaat	Taloudellinen riski, yksityisyydensuojan heikkeneminen, psykologiset vaikutukset
Yhteiskunta	Rikollisuuden rahoitus, kansantalouden heikkeneminen, kuluttajien luottamuksen heikkeneminen verkkokauppoihin ja pankkipalveluihin

Kolmannen tutkimuskysymyksen avulla tutkittiin, miten pankit ovat sopeuttaneet riskienhallintakäytäntöjään digihuijausten lisääntyttyä. Alakysymyksen avulla selvitettiin, millaisia mahdollisuuksia kehittyvä teknologia tuo digihuijauksista aiheutuvien riskien hallintaan. Asiantuntijoiden mukaan digihuijauksiin liittyvä riskienhallinta on monitasoista ja tapahtuu etenkin operatiivisessa tiimissä, reklamaatiokäsittelyssä ja kehitystoiminnassa. Haastatteluiden perusteella pankit ovat tunnistaneet tarpeen kokonaisvaltaiselle riskienhallintastrategialle, joka yhdistää muun muassa teknologiset ratkaisut, asiakkaiden kouluttamisen, yhteistyön ja asiakaskokemuksen ylläpitämisen. Siilomaisen lähestymistavan sijaan riskienhallinta keskittyy digihuijauksiin kokonaisuuteen huomioiden myös niiden kytkökset muihin rikoksiin.

Digihuijauksiin liittyvät riskienhallintakeinot keskittyvät sekä pankin korvausvastuun että huijausten uhrien määrän ja heidän taloudellisten tappioidensa minimoimiseen. Tärkeimpänä tavoitteena on estää varojen ja tietojen päätyminen rikollisille. Tähän

pyritään etenkin asiakkaan toiminnan ohjaamisen kautta, sillä tämä on merkittävässä roolissa verkkopankkitunnusten turvallisen käytön takaamisessa ja huijausten tunnistamisessa. Asiakkaiden kouluttamisen lisäksi pankin henkilöstön kouluttaminen on olennaisessa osassa etenkin uusien huijausmuotojen tunnistamisessa. Ennaltaehkäistäkseen digihuijausten aiheuttamia riskejä ja lisätäkseen omaa sekä muiden tietoisuutta, pankit tekevät yhteistyötä muiden finanssialan toimijoiden ja viranomaisten kanssa muun muassa jakamalla tietoa uusista huijausmenetelmistä ja parhaista käytännöistä.

Pankin eräs merkittävimpiä riskienhallintakeinoja digihuijausten ennaltaehkäisyssä ja tunnistamisessa on asiakkaan tunteminen, joka kattaa asiakastietojen ylläpidon, riskien arvioinnin ja näiden avulla epätyypillisen toiminnan tunnistamisen. Tämän lisäksi pankit käyttävät kehittyneitä järjestelmiä, kuten maksujen monitorointia ja riskipisteytyksiä tunnistaa epäilyttävää toimintaa. Teknologisten kontrollien avulla voidaan tunnistaa anomalioita ja estää epäilyttäviä maksutapahtumia. Huijausten ennaltaehkäisyssä ja torjunnassa käytetään myös tietoturvatyökaluja, kuten vahvaa salausta, palomureja ja säännöllisiä tietoturva-auditointeja. Haastatteluiden perusteella pankkien keskeisimmät riskienhallintakeinot digihuijauksiin liittyen on esitelty taulukossa 3.

Taulukko 3 Pankkien riskienhallintakeinot digihuijaustapauksissa

Riskienhallintakeino	Kuvaus
Asiakkaan rooli puolustuslinjana	Asiakkaan ymmärryksen ja toiminnan merkitys verkkopankkitunnusten ja rahojen suojaamisessa. Vahva sähköinen tunnistautuminen ja sen oikea käyttö ovat keskeisessä roolissa.
Asiakkaan tunteminen (KYC)	Asiakkaan tuntemiseen liittyvät toimet asiakkuuden avaamisessa ja ylläpidossa, minkä avulla voidaan tunnistaa asiakkaan normaalista poikkeavaa toimintaa.
Koulutus ja viestintä	Asiakkaiden ja henkilökunnan koulutus huijausten tunnistamiseksi. Asiakkaiden kouluttaminen verkkopankin turvalliseen käyttöön.
Maksujen monitorointi	Poikkeavien maksutapahtumien tunnistaminen ja varojen palauttaminen.
Ilmoituskanavat	Selkeät kanavat, joiden kautta epäilyttävästä toiminnasta voidaan raportoida.
Teknologiset ratkaisut	Palomuurit, virustorjuntaohjelmat, vahva salaus, pääsyn rajoittaminen ja säännölliset tietoturva-auditoinnit.
Yhteistyö viranomaisten ja toimialan kanssa	Tiedonvaihto huijausmenetelmistä ja parhaista käytännöistä poliisin, teleoperaattoreiden, Kyberturvallisuuskeskuksen ja muiden pankkien kanssa.
Kontrollit	Muun muassa verkkopankkitunnukset, korttien ja/tai tilien sulkeminen, maksutapahtumien kontekstieto.
Asiakkaiden vapaaehtoiset turvatoimet	Geo-blocking, euromääräiset rajat tilisiirroissa/kortin käytössä.

Kehittyvä teknologia tarjoaa pankkien riskienhallintaan uusia ratkaisuja, kuten tekoälyyn perustuvia analyysseja ja automaattisia hälytysjärjestelmiä, jotka tehostavat huijausten tunnistamista ja ennaltaehkäisyä. Tekoäly ja koneoppiminen mahdollistavat suurten tietomäärien analysoinnin, mikä voi helpottaa muun muassa epäilyttävien maksutapahtumien tunnistamisesta. Data-analytiikkaa voidaan puolestaan hyödyntää esimerkiksi asiakkaan maksutapahtumien yhteydessä tapahtuvan käyttäytymisen analysointiin, mikä auttaa reaaliaikaisesti huijausten tunnistamisessa. Turvallisuus voi

parantua myös biometrinen tunnistautumisjärjestelmien avulla, kun tunnistautumisessa hyödynnetään esimerkiksi sydämen sykettä tai kasvojentunnistusta.

Pankit tasapainottelevat riskienhallintatoimenpiteiden ja positiivisen asiakaskokemuksen välillä. Huijausmaksujen nopea tunnistaminen ja käsittely, kuten maksujen jäädyttäminen, on olennaista asiakastyytyväisyyden säilyttämisessä. Asiakaskokemuksen huomioiminen on olennaista etenkin huijausten uhrien tapauksessa, jotta nämä saavat tarvitsemansa avun ja tuen. Toisaalta riskienhallintatoimenpiteet, kuten maksujen pysäyttäminen ja lisäselvityspyynnöt voivat hidastaa normaalia maksamista ja vaikuttaa täten negatiivisesti asiakastyytyväisyyteen sekä palveluiden sujuvuuteen.

Pankkien haasteena digihuijausten riskienhallinnassa on etenkin rajoitettu vaikutusvalta huijausprosesseihin, sillä asiakas on saattanut olla pitkään yhteydessä huijariin pankin havaittua tilanteen. Tämän vuoksi pankin ennaltaehkäisevä ja tiedotuksellinen rooli korostuu. Pankkien riskienhallintakeinot ja tekniset ratkaisut osoittautuvat riittämättömiksi usein myös tunnehuijauksissa, kun uhri on sosiaalisen manipuloinnin seurauksena itse halukas suorittamaan huijareiden pyytämät maksutapahtumat. Poikkeavien maksutapahtumien tunnistamista hankaloittaa puolestaan suuri käsiteltävä datamäärä ja maksujen volyymi, josta huijausmaksut ovat vain hyvin pieni osa. Toisaalta, kuten aiemmin on esitelty, tekoälyn hyödyntäminen voi olla tulevaisuudessa ratkaisu tähän ongelmaan. Pankkien riskienhallintatoimenpiteitä rajoittaa myös sääntely. GDPR ja pankkialaisuussäännöt vaikeuttavat pankkien välistä tiedonvaihtoa huijauksista. Lainsäädäntö asettaa rajoituksia myös teknologian, kuten tekoälyn hyödyntämiselle. Tulevaisuudessa sääntelymuutokset saattavat mahdollistaa laajempia ja tehokkaampia riskienhallintatoimia, mutta toisaalta niiden arvellaan mahdollisesti lisäävät pankkien korvausvelvoitteita. Haastatteluiden perusteella digihuijausten lisääntyttyä myös niiden riskienhallintaan tarvittavat resurssit ovat lisääntyneet johtaen investointitarpeeseen sekä operatiivisella puolella että kehitystoiminnassa.

Johtopäätöksenä voidaan todeta, että asiakas on ”ensimmäinen puolustuslinja” digihuijausten torjunnassa, sillä asiakkaiden vapaus hallita omia varojaan asettaa rajoja pankkien riskienhallinnalle. Pankit sopeuttavat riskienhallintakäytäntöjään vastaamaan huijausten määrän ja monimutkaisuuden kasvua, mikä vaatii jatkuvaa teknologian ja järjestelmien päivittämistä sekä henkilöstön kouluttamista. Tietoisuuden kasvattamisen ja pankkien sekä finanssialan yhteistyön lisäksi teknologisten ratkaisujen kehittäminen

ovat avainasemassa huijausten ennaltaehkäisemiseksi. Digihuijausten vastainen työ on jatkuvaa kilpajuoksua rikollisia vastaan, mikä vaatii pankeilta proaktiivista lähestymistapaa. Riskienhallintaa vaikeuttaa muun muassa lainsäädännön tuomat rajoitukset ja riskienhallintatoimien rajallinen vaikutus asiakkaan roolin vuoksi. Pankkien mahdollinen korvausvastuun kasvaminen yhdistettynä nopeampiin maksutapahtumiin asettaa ne haastavaan asemaan, jossa tehokkaat riskienhallintaprosessit ja toimivat kontrollit ovat välttämättömiä. Toisaalta tulevaisuudessa sääntelymuutokset voivat tukea pankkien laajempia riskienhallintatoimia ja muut ratkaisut, kuten asiakkuuden kokonaisvaltainen tarkastelu voivat parantaa turvallisuutta. Digihuijaukset muodostavat näin ollen jatkuvasti kehittyvän haasteen pankkien riskienhallinnalle, ja teknologian, yhteistyön sekä lainsäädännön kehitys ovat avainasemassa tehokkaiden ratkaisujen löytämisessä.

5.2 Tutkielman arviointi

Tutkielman laatua voidaan arvioida reliabiliteetin kautta, millä viitataan tutkimuksen toistettavuuteen ja johdonmukaisuuteen. Mikäli aiempi tutkimusasetelma voidaan toistaa ja saavuttaa samat tulokset, voidaan tutkimusta pitää luotettavana. Reliabiliteetti voidaan edelleen jakaa sisäiseen ja ulkoiseen reliabiliteettiin, joista ensimmäisellä tarkoitetaan tutkimusprojektin johdonmukaisuutta. (Saunders ym., 2019.) Tämän tutkielman johdonmukaisuus varmistettiin tarkoilla kirjauksilla tutkielman etenemisestä ja seuraavista askeleista. Näin voitiin varmistaa, että tutkielmassa huomioidaan kaikki olennaiset seikat, ja että etenkin aineiston analyysi tapahtui johdonmukaisesti. Ulkoisella reliabiliteetilla puolestaan tarkoitetaan sitä, tuottaisivatko käytetyt aineistonkeruumenetelmät ja analyysiprosessit johdonmukaisia tuloksia, jos ne toistettaisiin tai jos toinen tutkija replikoi ne (Saunders ym., 2019). Tämä varmistettiin kuvaamalla mahdollisimman tarkasti aineiston kerääminen ja analyysiprosessi. Mikäli haastateltaviksi valikoituisi eri asiantuntijat kuin tässä tutkielmassa, voisivat tulokset hieman poiketa. Toisaalta vastaajana oli myös toimialajärjestön edustaja, joka pystyi antamaan kokonaisvaltaisempia vastauksia suomalaisten pankkien toiminnasta ja näkemyksistä, myös sellaisten pankkien osalta, jotka eivät haastatteluihin osallistuneet. Mikäli tutkimuksen suorittaisi eri ajanhetkenä, poikkeaisivat tulokset todennäköisesti hieman, sillä digihuijaukset ja niihin liittyvä riskienhallinta muuttuvat jatkuvasti.

Toinen tutkielman luotettavuuteen liittyvä käsite on validiteetti, jolla viitataan mittareiden tarkoituksenmukaisuuteen, tulosten analyysin tarkkuuteen ja löydösten yleistettävyyteen. Validiteetin käsite voidaan edelleen jakaa sisäiseen ja ulkoiseen. Sisäisellä validiteetilla tarkoitetaan sitä, missä määrin tulosten voidaan katsoa johtuvan tutkimuksen kohteesta eikä tutkimusasetelman puutteista. (Saunders ym., 2019.) Tutkimuksen kohteena oli digihuijausten vaikutus pankkien riskienhallintakäytäntöjen ja -prosesseihin. Muiden tekijöiden vaikutukset pyrittiin poistamaan esittämällä haastateltaville tarkentavia kysymyksiä siitä, mistä syystä ja milloin riskienhallintaan on tehty muutoksia.

Ulkoisella validiteetilla puolestaan viitataan tulosten yleistettävyyteen (Saunders ym., 2019). Tutkimuksen aineisto kerättiin haastatteleamalla kolmea pankin edustajaa sekä yhtä toimialajärjestön edustajaa. Etenkin toimialajärjestön edustajan asiantuntemuksen avulla pystyttiin luomaan kattavampi kuva suomalaisen pankkisektorin digihuijauksista ja niiden riskienhallinnasta. Koska haastatteluiden kohteena ei kuitenkaan ollut kaikkien suomalaisten pankkien edustajia, ei tuloksia voida suoraan pitää kaikkien suomalaisten pankkien ja niiden edustajien näkemyksenä.

Puolistrukturoitu temahaastattelu oli aineistonkeruumenetelmänä sopivan joustava, mikä mahdollisti tarkentavien kysymysten esittämisen ja täten tarkemman ymmärryksen digihuijausilmiöstä sekä siihen liittyvän riskienhallinnasta. Rajallinen haastattelu-aika osoittautui kuitenkin haasteeksi yhdessä haastattelussa, minkä seurauksena kaikkia teemoja ei pystytty käsittelemään yhtä laajasti kuin muissa haastatteluissa. Kaikkiin haastattelukysymyksiin saatiin kuitenkin vastaukset. Haastattelukysymykset olivat relevantteja, sillä niiden avulla tutkimuskysymyksiin saatiin kattavia vastauksia. Eri kysymyksillä tutkimuksen tulokset saattaisivat kuitenkin hieman poiketa nykyisestä. Aineistolähtöisen ja teoriaohjaavan sisällönanalyysin yhdistelmä oli tutkimusasetelman kannalta hyvin tarkoituksenmukainen, sillä analyysissa pystyttiin hyödyntämään teoriataustaa yhdistettynä aineistosta nousseisiin teemoihin. Tutkielman empiriassa ja teoriassa esiintyi paljon yhtäläisyyksiä, ja tutkielman teoreettisia käsitteitä pystyttiin hyödyntämään teoriaohjaavassa analyysissa. Toisaalta etenkin kolmannessa teorialuvussa käsitelty kokonaisvaltainen riskienhallinta ERM jäi hieman irralliseksi empiriaosuudesta, pääosin johtuen haastattelukysymysten asettelusta.

Tutkielmaprosessi oli kestoltaan noin viisi kuukautta, joka oli tutkielman tavoitteiden saavuttamiseksi melko sopiva aika. Haastattelumateriaali kerättiin noin kuukauden aikana, mikä mahdollisti materiaalin huolellisen litteroinnin ja siihen perehtymisen sekä myöhemmin analysoinnin. Tutkielmasta olisi kuitenkin todennäköisesti saatu kattavampi pidemmällä aikajänteellä, joka olisi mahdollistanut esimerkiksi useamman haastattelun pitämisen. Toisaalta haastateltavien hankinta osoittautui muutoinkin melko haastavaksi, sillä pankkisalaisuuteen vedoten useat asiantuntijat kieltäytyivät haastattelusta. Pankkisalaisuus osoittautui haasteeksi myös haastatteluiden aikana, sillä etenkin pankkien kontroleihin haastateltavat eivät voineet ottaa kovin tarkalla tasolla kantaa. Digihuijausilmiötä puolestaan saatiin hyvin kartoitettua ja haastatteluiden avulla siitä kerättiin hyvin ajantasaista tietoa. Neljä haastattelua riitti tutkimusaineiston kylläntymiseen, sillä vastauksissa toistui samat teemat ja piirteet.

Tutkimus oli onnistunut sen suhteen, että esitettyihin tutkimuskysymyksiin saatiin kattavia ja ajantasaisia vastauksia. Tutkielma tarjoaa ajankohtaisen ja kartoittavan näkemyksen suomalaisten pankkien asiakkaisiin kohdistuvista digihuijauksista, niiden erityispiirteistä ja niihin liittyvistä riskienhallintakeinoista.

5.3 Lopuksi

Jatkotutkimusmahdollisuuksia digihuijauksiin liittyvästä riskienhallinnasta on useita, etenkin kun aiempaa tutkimusta Suomessa on tehty hyvin vähän. Digihuijaukset ovat lisäksi verrattain uusi ja jatkuvasti kehittyvä ilmiö, minkä seurauksena mahdollisia tutkimusmahdollisuuksia syntyy jatkuvasti lisää. Mahdollinen tarkastelunäkökulma olisi esimerkiksi tarkempi tutkimus teknologian ja tekoälyn roolista digihuijausten ennaltaehkäisyssä ja tunnistamisessa, missä voitaisiin ottaa huomioon myös tekoälyn tuomat eettiset haasteet.

Asiakkaiden näkökulmasta mielenkiintoista olisi tutkia näiden digihuijauksiin liittyvää riskitietoisuutta eri ikä- ja väestöryhmissä sekä digihuijausten ja niihin liittyvien riskienhallintatoimenpiteiden vaikutusta asiakkaiden käyttäytymiseen ja luottamukseen. Myös digitaalisen kansalaiskasvatuksen ja kuluttajien kouluttamisen roolia digihuijausten ennaltaehkäisyssä voisi tutkia lisää. Eräs jatkotutkimusmahdollisuus olisi vertailla Suomen ja muiden maiden lainsäädännöllisten erojen vaikutusta digihuijausilmiöön ja sen

riskienhallintaan tai vertailla suomalaisten pankkien asiakkaisiin kohdistuvia digihuijauksia ja niiden riskienhallintaa maihin, joissa pankkien riskienhallinta ei ole vielä yhtä kehittyneellä tasolla.

LÄHDELUETTELO

Kirjallisuuslähteet

Awad, A., Traoré, I. & Woungang, I. (2017). *Information Security Practices: Emerging Threats and Perspectives* (1st ed. 2017.). Springer International Publishing.

Bayuk, J. L. & Rohmeyer, P. (2018). *Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions* (1st ed.).

Button, M., Lewis, C., & Tapley, J. (2015). *Fraud Typologies and the Victims of Fraud Literature Review*. National Fraud Authority.

https://pure.port.ac.uk/ws/portalfiles/portal/1926122/NFA_report3_16.12.09.pdf

Cao, L., Chen, J., Li, J., Ou, Y., & Wei, W. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web*.

<https://link.springer.com/article/10.1007/s11280-012-0178-0#Bib1>

Cebula, J. & Young, L. (2010). A taxonomy of operational cyber security risks. Carnegie Mellon.

<https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395>

Domenig, T., Rossi, S., Vanini, P. & Zvizdic, E. (2023). Online payment fraud: from anomaly detection to risk management. *Financial Innovation* 9, 66.

<https://doi.org/10.1186/s40854-023-00470-w>

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5), 474–491.

<https://doi.org/10.1108/JRF-09-2016-0122>

Fraser, J., & Simkins, B. J. (2010). *Enterprise risk management* (1st edition). Wiley.

Girling, P. X. (2022). *Operational Risk Management: A Complete Guide for Banking and Fintech* (Second edition). Wiley.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. In *McKinsey Insights*. McKinsey & Company, Inc.

Hirsjärvi, S. & Hurme, H. (2008). Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Gaudeamus Helsinki University Press.

Hull, J. (2018). *Risk management and financial institutions* (Fifth edition.). Wiley.

Hoffmann, A. O. I., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. *International Journal of Bank Marketing*, 30(5), 390–407.

<https://doi.org/10.1108/02652321211247435>

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, Evaluating and*

Implementing Effective Risk Management. 5. painos.

Jaradat, R. Magpili, L. & Pinto, C. (2015). *Operational risk management* (1st ed.). Momentum Press Engineering.

Klinke, A., & Renn, O. (2001). Precautionary principle and discursive strategies: classifying and managing risks. *Journal of Risk Research*, 4(2)

Moeller, R. R. (2011). COSO enterprise risk management establishing effective governance, risk, and compliance processes (2nd ed.). John Wiley & Sons.

Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*, 26(7), 155–166.

<https://doi.org/10.1108/JMLC-03-2023-0050>

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (Eighth edition.). Pearson.

Tuomi, J. & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi (Uudistettu laitos). Tammi.

Wuolijoki, S. (2023). *Pankkioikeus. II* (3., uudistettu painos.). Alma Talent.

Muut painetut lähteet

Laki Harmaan talouden selvitysyksiköstä 21.12.2010/1207

Laki rahanpesun ja terrorismin rahoittamisen estämisestä, Rahanpesulaki, 28.6.2017/444

Maksulaitoslaki 30.4.2010/297

Maksupalvelulaki (290/2010)

Rikoslaki 19.12.1889/39

Internet-lähteet

ACFD. (2024). Fraud 101: What is fraud? Viitattu 14.10.2024
<https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud>

Basel Committee on Banking Supervision. BCBS. (2017). High level summary of Basel III reforms. Viitattu 11.11.2024
https://www.bis.org/bcbs/publ/d424_hlsummary.pdf

Basel Committee on Banking Supervision. BCBS. (2021). Revisions to the principles for the sound management of operational risk. Viitattu 11.11.2024
<https://www.bis.org/bcbs/publ/d515.pdf>

Basel Committee on Banking Supervision. (2023). Discussion paper. Digital fraud and banking: supervisory and financial stability implications. Viitattu 11.11.2024
<https://www.bis.org/bcbs/publ/d558.pdf>

BIS. (2019). Pillar 2 framework - Executive Summary. Viitattu 20.11.2024
<https://www.bis.org/fsi/fsisummaries/pillar2.htm>

BIS. (2024). Basel III: international regulatory framework for banks. Viitattu 20.11.2024
<https://www.bis.org/bcbs/basel3.htm?m=76>

COSO. (2023). COSO ERM Framework. Viitattu 28.11.2024
https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf

Digi- ja väestötietovirasto. (2023). Tutkimus: Yli puolet digimailman rikoksista jää ilmoittamatta viranomaisille. Viitattu 1.10.2024
<https://dvv.fi/-/digiturvabarometri-yli-puolet-digimailman-rikoksista-jaa-ilmoittamatta-viranomaisille>

Deloitte. (2023). Pankeilla on suuri vastuu digihuijausten torjunnassa. Viitattu 3.10.2024
<https://www2.deloitte.com/fi/fi/blog/finland-blog-homepage/2023/pankeilla-on-suuri-vastuu-digihuijauksien-torjunnassa-.html>

Deloitte. (2024). Väärinkäytösriskit nousussa Suomessa ja Euroopassa. Viitattu 3.11.2024
<https://www2.deloitte.com/fi/fi/pages/risk/articles/vaarinkaytosriskit-nousussa-suomessa-ja-euroopassa.html>

ENISA. (2024). ENISA Threat Landscape 2024. Viitattu 7.11.2024
DOI: 10.2824/0710888

Euroopan parlamentti. (2022). Kyberturvallisuus: nykyiset ja tulevat uhat. Viitattu 15.11.2024
<https://www.europarl.europa.eu/topics/fi/article/20220120STO21428/kyberturvallisuus-nykyiset-ja-tulevat-uhat>

Eurooppa-neuvosto. (2024). Neuvosto hyväksyi pikamaksuasetuksen. Viitattu 4.11.2024
<https://www.consilium.europa.eu/fi/press/press-releases/2024/02/26/council-adopts-regulation-on-instant-payments/>

European Commission. (2011). Consumer attitudes towards cross-border trade and consumer protection. Viitattu 28.9.2024
http://ec.europa.eu/consumers/archive/consumer_research/editions/docs/consumer_euro_barome-ter_2011_en.pdf

European Commission. (2024). European Digital Identity. Viitattu 18.1.2025
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

Europol. (2023). The Other Side of the Coin: An Analysis of Financial and Economic Crime: European Financial and Economic Crime Threat Assessment 2023. Publications Office of the European Union, Luxembourg, 2023. Viitattu 5.10.2024
<https://op.europa.eu/en/publication-detail/-/publication/83f3cef9-5769-11ee-9220-01aa75ed71a1/language-en>

Europol. (2024). Internet organized threat assessment. Viitattu 5.10.2024
<https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf>

FATF. (2023). Illicit Financial Flows from Cyber-Enabled Fraud. Viitattu 3.11.2024
<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf>

FSB. (2023). Cyber Lexicon. Viitattu 3.11.2024
<https://www.fsb.org/uploads/P130423-3.pdf>

Finanssiala. (2023). Turvatilipetokset yleistyneet kesällä – tietojenkalastelu vaivaa suomalaisia. Viitattu 28.10.2024
<https://www.finanssiala.fi/uutiset/turvatilipetokset-yleistyneet-kesalla-tietojenkalastelu-vaivaa-suomalaisia/>

Finanssivalvonta. (2017). Kryptovaluutat ja ICO sijoituskohteina, onko kyse kuplasta? viitattu 18.1.2025
<https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/blogit/2017/kryptovaluutat-ja-ico-initial-coin-offering-sijoituskohteina-onko-kyse-kuplasta/>

Finanssivalvonta. (2020). Asiakkaan tunnistaminen ja tunteminen. Viitattu 1.11.2024
<https://www.finanssivalvonta.fi/kuluttajansuoja/asiakkaan-tunnistaminen-ja-tunteminen/>

Finanssivalvonta. (2024). Huijaukset. Viitattu 12.10.2024
<https://www.finanssivalvonta.fi/kuluttajansuoja/huijaukset/>

FINE. (2024). Huijausten selvittäminen ja ratkaisukäytännöt FINEssä. Viitattu 14.10.2024
<https://www.fine.fi/oppaat/julkaisu/huijausten-selvittaminen-ja-ratkaisukaytannot-finessa.html>

F-Secure. (2024a). Mitä on käyttäjän manipulointi? Viitattu 28.10.2024
<https://www.f-secure.com/fi/articles/what-is-social-engineering>

F-Secure. (2024b). Mitä on spoofing? Viitattu 1.11.2024
<https://www.f-secure.com/fi/articles/spoofing>

IMF. (2023). Nordic-Baltic Technical Assistance Project. Financial Flow Analysis and AML/CFT Supervision. Viitattu 20.10.2024
<https://www.finanssivalvonta.fi/globalassets/fi/tiedotteet-ja-julkaisut/verkkouutiset/2024/imf-nordic-baltic-aml-study-2013-finland-report-julkaistava.pdf>

ISO. (2018). ISO 31000 - Risk Management - Guidelines. Viitattu 20.11.2024
<https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>

Kanu, B. (2024). Pankkien asiakkaisiin kohdistuvat verkkohuijaukset: Pankin ja asiakkaan välinen vastuunjako sekä riskienhallintakeinot. Vaasan yliopisto. Pro gradu-tutkielma. Viitattu 7.10.2024
https://osuva.uwasa.fi/bitstream/handle/10024/16647/Pro%20gradu_Ballu%20Kanu.pdf?sequence=2&isAllowed=y

Keskusrikospoliisi. (2024). Rahanpesun selvittelykeskuksen vuosikertomus 2023. Viitattu 2.9.2024
<https://rahanpesu.fi/documents/25235045/67733116/vuosikertomus-saavutettava.pdf/da6396ec-eb64-814a-3006-89b38baca942/vuosikertomus-saavutettava.pdf?t=1709018951850>

Kilpailu- ja kuluttajavirasto. (2024). Huijaukset. Viitattu 1.11.2024
<https://www.kkv.fi/kuluttaja-asiat/huijaukset/>

Kuluttajaliitto. (2024a). Varo, varmista ja varoita: Nettihuijaukset ja tietojen kalastelu mututavat muotoaan, mutta niiltä on mahdollisuus suojautua. Viitattu 17.11.2024
<https://www.kuluttajaliitto.fi/varo-varmista-varoita/>

Kuluttajaliitto. (2024b). Pankkien otettava lisää vastuuta digihuijauksen korvauksissa. Viitattu 17.1.2025
<https://www.kuluttajaliitto.fi/2024/12/04/pankkien-otettava-lisaa-vastuuta-digihuijauksen-korvauksissa/>

Kuluttajariitalautakunta. (2019). Pankkitunnistamisen riskit kasvaneet. Viitattu 3.11.2024
<https://www.kuluttajariita.fi/fi/index.html>

Kyberturvallisuuskeskus. (2024). Monivaiheinen tunnistautuminen suojaa käyttäjätilejasi. Viitattu 14.10.2024
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi>

Nordea. (2024). What are PSD3 and PSR? Viitattu 28.10.2024
<https://www.nordea.com/en/news/what-are-psd3-and-psr>

OECD. (2019). Recommendation of the council on artificial intelligence. Viitattu 1.11.2024
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

Oikeusministeriö. (2023). Maksupalvelulainsäädännön uudistaminen (EU-valmistelu). OM068:00/2023. Viitattu 4.10.2024
<https://oikeusministerio.fi/hanke?tunnus=OM068:00/2023>

OP. (2024). Valepoliisi. Viitattu 7.10.2024
<https://www.op.fi/turvallinen-asiointi/verkkorikollisuus/valepoliisi>

Palmgren, J. (2024a). Huijareilla oli aktiivinen vuosi 2023 – Pankit saivat estettyä digihuijauksia lähes 33 miljoonan euron edestä. Finanssiala.fi. Viitattu 1.10.2024
<https://www.finanssiala.fi/uutiset/huijareilla-oli-aktiivinen-vuosi-2023-pankit-saivat-estettya-digihuijauksia-lahes-33-miljoonan-euron-edesta/>

Palmgren, J. (2024b). Huijaukset kovassa kasvussa – pankit onnistuivat pysäyttämään yli 18 miljoonaa euroa huijattua rahaa. Finanssiala.fi. Viitattu 23.10.2024
<https://www.finanssiala.fi/uutiset/huijaukset-kovassa-kavussa-pankit-onnistuivat-pysayttamaan-yli-18-miljoonaa-euroa-huijattua-rahaa/>

Piira, M. (2022). Verkkoavusteisen petoksen sääntely ja torjunta talousrikosoikeudellisesta näkökulmasta. Viitattu 28.9.2024
https://lauda.ulapland.fi/bitstream/handle/10024/65190/Piira_Mikko.pdf?sequence=1&isAllowed=y

Poliisi.fi. (2024). Petosrikokset. Viitattu 1.10.2024
<https://poliisi.fi/petosrikokset>

Riku. Rikosuhripäivystys. (2022). Verkkopankkihuijauksen sattuessa pankki saattaa vastata menetyksistä. Viitattu 3.10.2024
<https://www.riku.fi/verkkopankkihuijauksen-sattuessa-pankki-saattaa-vastata-menetyksista/>

Sisäministeriö. (2024). Kyberrikollisuus ylittää rajat tietoverkoissa. Viitattu 25.9.2024.
<https://intermin.fi/poliisiasiat/kyberrikollisuus>

Tuorila, H. (2018). Huijaukset heikentävät yhteiskunnallista hyvinvointia. Viitattu 10.9.2024
<https://urn.fi/URN:NBN:fi-fe2018091735900>

Traficom. (2024). SMS Sender ID -tunnus.
<https://traficom.fi/fi/viestinta/laajakaista-ja-puhelin/sms-sender-id-tunnus>

Valtiovarainministeriö. (2023). Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2023: Osittaispäivitys. Viitattu 2.9.2024
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165433/VM_2023_8.pdf?sequence=1&isAllowed=y

Henkilölähteet

Asiantuntija A. Haastattelu 27.11.2024

Asiantuntija B. Sähköpostivastaus 20.12.2024

Asiantuntija C. Haastattelu 9.12.2024

Asiantuntija D. Haastattelu 28.11.2024

LIITTEET

LIITE 1: TEEMAHAASTattelun kysymysrunko

OSA 1, taustatiedot:

1. Mitä nykyiseen työtehtävääsi kuuluu?
2. Kuinka kauan olet työskennellyt nykyisessä tehtävässä/vastaavissa tehtävissä?

OSA 2, digihuijaukset:

1. Millaisia digihuijauksia pankkien asiakkaisiin kohdistuu?
2. Miten huijaukset ovat muuttuneet tai kehittyneet teknologian kehityksen, kuten tekoälyn myötä?
3. Oletteko tunnistaneeet uusia trendejä digihuijauksiin liittyen? Jos kyllä, millaisia?
4. Millaisia riskejä olette tunnistaneeet digihuijauksiin liittyen?
 - a. Millaisia riskien seurauksia olette tunnistaneeet?
5. Miten digitaaliset huijaukset vaikuttavat pankkien asemaan ja maineeseen?

OSA 3, riskienhallinta digihuijauksissa:

1. Millaisia riskienhallintakeinoja pankeilla on asiakkaisiin kohdistuvissa digihuijauksissa?
 - a. Missä määrin hallitaan riskiä siitä, ettei asiakas joudu huijauksen kohteeksi ja missä määrin sitä, ettei pankki joudu korvausvastuuseen?
2. Mitä keskeisiä kontroleja pankeilla on digihuijauksiin liittyvissä riskeissä?
3. Miten riskienhallintakeinot ja kontrollit ovat muuttuneet huijauksien lisääntyä?
4. Onko asiakkaillanne mahdollisuus lisätä vapaaehtoisia turvatoimia digihuijauksiin liittyen?
5. Millaisia käytännön haasteita pankeilla on digihuijauksiin liittyvässä riskienhallinnassa?
 - a. Miten odotat näiden muuttuvan tulevaisuudessa?
6. Miten pankit huomioivat asiakaskokemuksen säilymisen asiakkaisiin kohdistuvissa huijauksissa?
7. Millaisia mahdollisuuksia kehittyvä teknologia tuo digihuijauksista aiheutuvien riskien hallintaan?
 - a. Oletteko hyödyntäneet tällaisia mahdollisuuksia?
8. Miten riskienhallintaa digihuijauksiin liittyen voitaisiin kehittää?