HAMK
Hämeen ammatti-
korkeakoulu

Pankin maksuliikenteen turvaaminen poikkeustilanteessa

Ammattikorkeakoulututkinnon opinnäytetyö

Liiketalouden koulutus, tradenomi

Kevät 2025

Tiina Tirkkonen

HAMK
Hämeen ammatti-
korkeakoulu

Tiivistelmä

Koulutus	Liiketalouden koulutus	
Tekijä	Tiina Tirkkonen	Vuosi 2025
Työn nimi	Pankin maksuliikenteen turvaaminen poikkeustilanteessa	
Ohjaaja	Risto Järvinen	

Tämän opinnäytetyön tavoitteena oli tutkia pankin maksuliikenteen toimivuutta ja turvallisuutta mahdollisessa poikkeustilanteessa sekä sitä, miten pankissa varaudutaan mahdollisiin häiriötilanteisiin. Opinnäytetyö käsittelee pankin maksuliikennettä osana kriittistä infrastruktuuria sekä maksamisen turvallisuutta. Lisäksi työssä perehdytään maksamisen mahdollistavaan infrastruktuuriin sekä erilaisiin varautumistoimenpiteisiin ja sääntelyyn, joiden avulla maksamista turvataan.

Tutkimus on toteutettu kvalitatiivisena eli laadullisena tutkimuksena. Tutkimusmenetelmänä hyödynnettiin puolistrukturoitua teemahaastattelua. Teemahaastatteluun osallistui pankin asiantuntijoita, joilla on vahva asiantuntemus maksuliikenteestä ja siihen liittyvästä varautumisesta. Tutkimuksen tavoitteena oli selvittää pankissa työskentelevien asiantuntijoiden kokemuksia ja näkemyksiä pankin maksuliikenteen turvallisuudesta ja näiden kokemuksien ja näkemyksien kautta selvittää onko pankin maksuliikenne turvattu häiriö- tai poikkeustilanteessa ja millaista varautumistyötä pankeissa on tehty maksuliikenteen turvallisuuden varmistamiseksi.

Tutkimuksen tulokset osoittivat, että pankin maksuliikenteen turvallisuus on hyvällä tasolla. Vaikka turvallisuusympäristö on muuttunut ja pankkeihin on kohdistunut voimakkaita palvelunestohyökkäyksiä, ollaan pankissa luottavaisia sen suhteen, että maksuliikenteen turvallisuus on varmistettu mahdollisessa häiriö- ja poikkeustilanteessa. Toimintaympäristöä ovat muuttaneet myös maksamisen reaaliaikaistuminen sekä kansainvälistyminen. Pankissa on tehty ja tehdään edelleen jatkuvaa työtä maksuliikenteen turvallisuuden ja häiriöttömyyden eteen. Useat eri toimintamallit ja varajärjestelyt varmistavat maksamisen häiriöttömyyttä.

Johtopäätöksissä todetaan asiantuntijoiden haastatteluiden osoittaneen, että keskiössä ovat yhteistyö, järjestelmät, prosessit sekä työtä tekevät ihmiset. On monen tekijän yhteispelin summa, että yhteiskunnan toimintakyvyn kannalta elintärkeä pankin maksamisen infrastruktuuri on turvattu mahdollisessa häiriö- ja poikkeustilanteessa. Tutkimuksen lopputuloksena syntyi selkeä kuva siitä, millainen on pankin maksuliikenteen tämänhetkinen turvallisuusympäristö, mitkä ovat sen haasteet, millä tavalla pankit ovat varautuneet sekä millaisia toimia turvallisuuden varmistamiseksi tehdään.

Avainsanat	Maksuliikenne, kyberturvallisuus, kriittinen infrastruktuuri, huoltovarmuus ja jatkuvuudenhallinta.
Sivut	54 sivua ja liitteitä 2 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Abstract

DP Degree Programme in Business Administration
Author Tiina Tirkkonen
Year 2025
Subject Securing the bank's payment traffic in an exceptional situation
Supervisors Risto Järvinen

The aim of this thesis was to study the functionality and security of a bank's payment transactions in a possible exceptional situation and how the bank prepares for possible payment transaction disruptions. The thesis deals with the payment traffic of banks as part of a critical infrastructure as well as the security of payment. In addition, the work explores the infrastructure that enables payment, as well as various contingency measures and regulations that are used to secure bank’s payment traffic.

The research has been carried out as qualitative research. A semi-structured theme interview was used as a research method. The theme interview was conducted by experts from the bank, who have strong expertise in payment transactions and related preparedness. The aim of the study was to find out the experiences and views of experts working at the bank on the security of the bank's payment transactions and, through these experiences and views, to find out whether the bank's payment transactions have been secured in a disruption or exceptional situation and what kind of contingency work has been done at the banks to ensure the security of the payment transactions.

The results of the study showed that the bank's payment security is at a good level. Although the security environment has changed and banks have been subject to strong denial-of-service attacks, the bank is confident that the security of payment transactions has been secured in the event of a disruption and emergency. The operating environment has also been changed by real-time payment and internationalisation. The bank has done and continues to do continuous work to ensure that payment transactions are safe and undisturbed. A number of different operating models and back-up arrangements ensure that payment is undisturbed.

The conclusions state that interviews with experts have shown that cooperation, systems, processes, and working people are at the core. It is the sum of many factors that a bank's payment infrastructure, vital to society's ability to function, is secured in the event of a disruption and emergency. The end result of the study was a clear picture of the current security environment of the bank's payment transactions, what are the challenges, how banks are prepared, and what measures are being taken to ensure security.

Keywords Payment transactions, cybersecurity, critical infrastructure, security of supply and continuity management.
Pages 54 pages and appendices 2 pages

Sisällys

Kuvat

Liitteet

1 Johdanto

Maksaminen on talouden perusta ja yksi järjestäytyneen yhteiskunnan peruspilareista. Rahoitusmarkkinoiden vakaa ja häiriötön toiminta on edellytys yhteiskunnan toimivuudelle. Maksaminen on oleellinen, miltei kaikkiin finanssipalveluihin linkittyvä osa. Kaikki rahaliikenne kulkee pankin järjestelmien kautta. (Snellman, 2017; Rehn, 2021)

Geopoliittisen epävarmuuden myötä rahoitusjärjestelmän infrastruktuuriin kohdistuva uhka sekä operatiiviset riskit ovat kasvaneet. Venäjän hyökkäyssota Ukrainaan ja voimakkaasti muuttunut turvallisuusympäristö ovat lisänneet entisestään tarvetta suojata kriittistä infrastruktuuria ja vahvistaa sen häiriönsietokykyä. Viimevuosina olemme nähneet myös Euroopassa kriittiseen infrastruktuuriin kohdistuvia tahallisia vahingontekoja ja lähiaikoina on uutisoitu useaan otteeseen pankkeihin kohdistuneista palvelunestohyökkäyksistä. Pankit ylläpitävät yhteiskunnan kannalta kriittistä infrastruktuuria ja palveluja. Pohjoismaisiin pankkeihin kohdistuneet häiriötilanteet ovatkin herättäneet keskustelua yhteiskunnan häiriönsietokyvystä. Maksaminen on peruspankkipalvelu ja yksi yhteiskunnan kriittisistä toiminnoista. Rahoitusmarkkinoiden vakaa ja häiriötön toiminta on edellytys yhteiskunnan toimivuudelle. Ilman toimivaa maksujenvälityksen järjestelmää yhteiskuntamme seisahtuisi nopeasti. (Suomen Pankki, n.d.-h; Weuro, 2024)

Opinnäytetyön aiheeksi valikoitui pankin maksuliikenteen turvallisuus. Aihe on ajankohtainen ja lähtöisin omasta mielenkiinnostani, mikä on herännyt työni sekä muuttuneen maailmantilanteen myötä. Työssä esiintyvät keskeiset käsitteet ovat maksuliikenne, kyberturvallisuus, kriittinen infrastruktuuri, huoltovarmuus ja jatkuvuudenhallinta. Työllä ei ole toimeksiantajaa. Tämän opinnäytetyön tarkoituksena on tutkia pankin maksuliikenteen turvallisuutta. Opinnäytetyön tavoitteena on selvittää vastaukset tutkimuskysymyksiin:

- Onko pankin maksuliikenne turvattu poikkeustilanteessa?
- Millaisin keinoin pankki varmistaa maksuliikenteen toimivuuden poikkeustilanteessa?

Tässä opinnäytetyössä maksuliikenteen poikkeustilanteella tarkoitetaan tilannetta, jossa joudutaan ottamaan käyttöön varajärjestelyjä pankin maksuliikenteen turvaamiseksi ja toteuttamiseksi. Tai tilannetta, jossa pankki on voimakkaiden kyberhyökkäysten kohteena.

Opinnäytetyö on toteutettu laadullisena tutkimustyönä ja aineisto kerätty teemahaastattelujen avulla. Teemahaastatteluiden avulla pyrittiin selvittämään pankin asiantuntijoiden näkemyksiä ja kokemuksia aiheesta. Työ koostuu tietoperustasta sekä tutkimusosuudesta. Tietoperustassa käsitellään pankin maksuliikennettä osana kriittistä infrastruktuuria ja maksamisen mahdollistavia järjestelmiä. Lisäksi maksamisen turvallisuutta, sitä sääntelevää lainsäädäntöä ja varautumistoimenpiteitä. Tutkimusosuudessa pureudutaan asiantuntijoiden haastatteluihin ja tutkimuksen tuloksiin.

Lähdeaineistona on hyödynnetty muun muassa lainsäädäntöä, viranomaisten julkaisuja, strategioita, verkkosivuja, uutisia, artikkeleita sekä tutkimuksellisessa osuudessa pankin asiantuntijoiden haastatteluita.

2 Pankin maksuliikenne

Maksaminen on peruspankkipalvelu ja yksi yhteiskunnan kriittisistä toiminnoista. Maksamisella tarkoitetaan yksinkertaistettuna rahan siirtämistä eri osapuolten välillä ja se mahdollistaa lähes kaiken taloudellisen toiminnan. Maksuliikenne kattaa kaiken yrityksen saapuvan ja lähtevän rahaliikenteen. Kotimaassa suurin osa maksuliikenteestä tapahtuu sähköisesti ja valtaosa maksuista on sähköisiä tilisiirtoja tai korttimaksuja. Maksaminen ja sen toimivuus on keskeinen tekijä kaikessa taloudellisessa toiminnassa vaikuttaen edelleen kaikkiin taloudellisiin toimijoihin. Maksuliikenne voi sisältää erilaisia rahansiirtotapoja, kuten tilisiirtoja, suoraveloituksia, luottokortti- ja pankkikorttimaksuja sekä mobiili- ja verkkomaksuja. Sen tavoitteena on mahdollistaa nopeat, turvalliset ja tehokkaat rahansiirrot osapuolelta toiselle kotimaassa ja kansainvälisesti. Pankeilla sekä muilla rahoituslaitoksilla on keskeinen rooli maksuliikenteen toteuttamisessa. Pankki mahdollistaa henkilöasiakkaiden sekä yritysasiakkaiden maksuliikenteen toteutumisen ja maksujen välittäminen maksajalta saajalle on keskeinen osa pankkitoimintaa. Pankit vastaavat rahansiirtojen käsittelystä, välittämisestä ja selvityksestä. Samoin ne huolehtivat sujuvista, turvallisista ja tehokkaista maksupalveluista. Suomessa maksamisen palvelut perustuvat pankkien, keskuspankin sekä yksityisten toimijoiden järjestelmiin. Maksut siirtyvät pankista toiseen näiden maksujärjestelmien avulla. Ilman luotettavia ja toimivia maksujärjestelmiä talous seisahtuisi hyvin nopeasti. (Procountor, n.d.; Suomen Pankki, n.d.-c)

Raha liikkuu osapuolten välillä pankkitililtä toiselle pankkien välisen infrastruktuurin avulla. Tilisiirto veloitetaan maksavan asiakkaan tililtä ja välitetään maksujenvälitysjärjestelmän kautta saajan pankkiin, jossa se hyvitetään maksunsaajan tilille. Suomessa käytössä olevien maksupalveluiden tulee perustua infrastruktuureihin, jotka ovat yhteensopivia eurooppalaisten maksujärjestelmien ja standardien kanssa. Maksujärjestelmät toimivat kanavana mahdollistaen rahan liikkumisen. Suomalainen maksuliikenne pohjautuu tilisiirtoihin ja korteilla maksamiseen. (Suomen Pankki, n.d.-c)

Euroalue kattaa kaikki euron käyttöönottaneet maat ja Euroopan Keskuspankki eli EKP on euroalueen maiden yhteinen keskuspankki. EKP ja euromaiden omat keskuspankit muodostavat eurojärjestelmän. Myös niiden EU-alueen jäsenmaiden keskuspankit, jotka eivät ole ottaneet käyttöön euroa, ovat mukana Euroopan keskuspankkijärjestelmässä. Eurojärjestelmän tehtäviin lukeutuu muun muassa maksujärjestelmien moitteettoman toiminnan edistäminen sekä rahoitusjärjestelmän vakauden turvaaminen. Euroalueella maksut siirtyvät osapuolten välillä mittavan järjestelmän kautta. Euroopan Keskuspankin rooli on hoitaa osaa tästä järjestelmästä sekä valvoa muiden sen osien toimintaa. EKP tarkkailee rahoitusjärjestelmän häiriönsietokykyä EU- ja euroalueella sekä pyrkii havaitsemaan haavoittuvuuksia, jotta niihin voidaan reagoida ajoissa. (Suomen Pankki, n.d.-a; Euroopan keskuspankki, 2024-a)

Rahapolitiikan toteuttamisesta Suomessa vastaa Valtion omistama Suomen Pankki, joka toimii Suomen keskuspankkina. Suomen Pankki on jäsenenä Euroopan Keskuspankin valvomassa Euroopan keskuspankkijärjestelmässä. Suomessa sijaitsevat luottolaitokset pitävät keskuspankkitilejään Suomen Pankissa ja voivat osallistua rahaoperaatioihin Suomen Pankin välityksellä. Voidakseen toimia rahapolitiikan operaatioiden vastapuolina pankkien tulee olla vähimmäisvarantovelvollisia, rahoitusvalvonnan alaisia sekä rahoitusasemaltaan vakaita yhtiöitä. Maksujärjestelmien yleisvalvojana Suomessa toimii Suomen Pankki. Sen tehtävä on varmistaa, että maksaminen säilyy luotettavana ja turvallisena nyt ja tulevaisuudessa. (Suomen Pankki, 2019; Kemppainen, 2017)

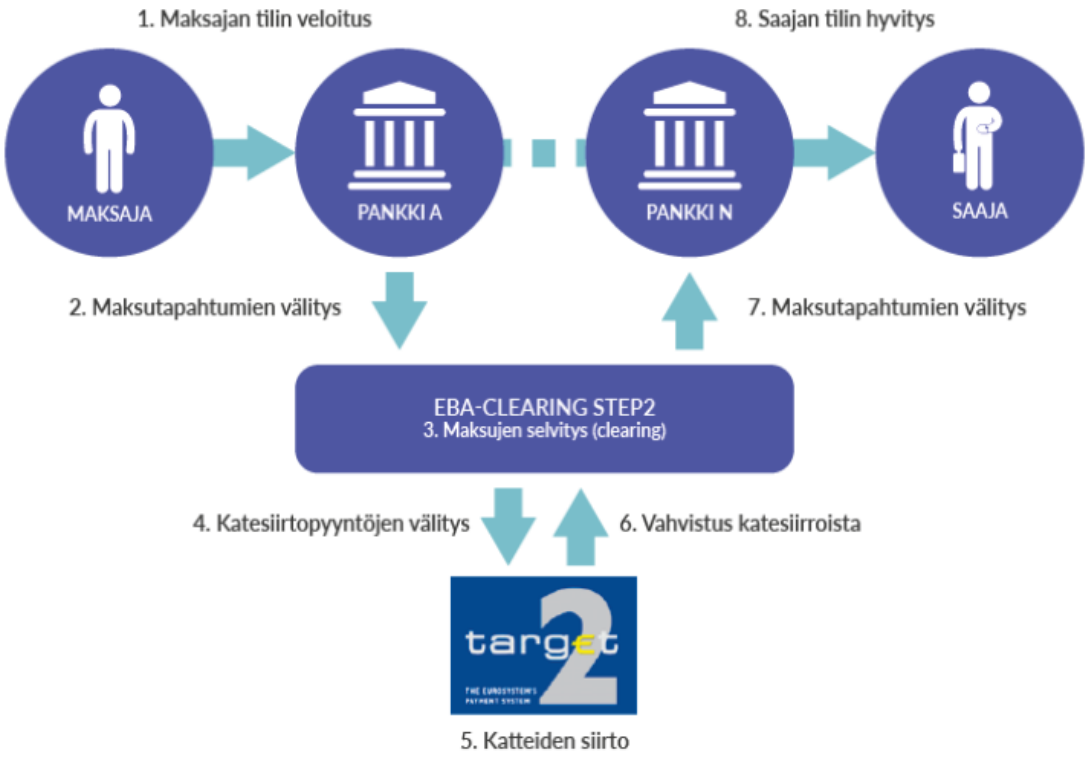
Jokaisen Euroalueen luottolaitoksen on talletettava tietty määrä varoistaan kansallisiin keskuspankkeihin Euroalueella. Pankit pitävät varoja keskuspankissa täyttääkseen vähimmäisvarantovelvoitteensa, hoitaakseen pankkien välisiä maksuja ja tallettaakseen varansa turvallisesti. Pankkien vähimmäisvarantovelvoitteet asetetaan yleensä 6-7 viikoksi kerrallaan eli pitoajanjaksolle. Kyseessä on määrätty prosenttiosuus pankin asiakastalletuksista ja muista eristä. Se lasketaan taseen määrästä ennen pitoajanjakson alkua. Lakisääteinen talletussuojajärjestelmä turvaa tallettajan tilillä olevia varoja ja

talletussuojakorvaus on enintään 100 000 euroa tallettajan yhdessä pankissa olevista talletuksista. Talletussuojajärjestelmät on yhdenmukaistettu Euroopan unionin jäsenmaissa. Talletussuojadirektiivi ja kansalliset lainsäädännöt varmistavat sen, että talletuspankeissa olevat talletukset kuuluvat EU-alueella aina jonkin talletussuojajärjestelmän piiriin. Suomessa talletussuojajärjestelmästä vastaa Rahoitusvakausvirasto. Euroalueen pankkeja koskevan vähimmäisvarantovelvoitteen ja talletussuojajärjestelmän avulla pyritään turvaamaan pankin ja asiakkaan taloudellista riskiä mahdollisessa poikkeavassa tilanteessa. (Rahoitusvakausvirasto, n.d.-b; Tötterman, 2019)

Euromaksut Euroopassa maksetaan pääsääntöisesti SEPA-maksuina. Yhteinen euromaksualue SEPA on lyhenne sanoista Single Euro Payments Area. Maksut kotimaahan ja muihin SEPA-maihin välitetään SEPA-tilisiirtoina maksajalta saajalle. Yhteisen euromaksualueen eli SEPA-alueen tavoitteena on, että maksut toiseen euromaahan välittyvät samoin ehdoin, yhtä helposti, turvallisesti ja tehokkaasti kuin kotimaan sisällä. SEPA-tilisiirto on eurooppalaisen tilisiirtostandardin mukainen tilisiirto. Se on perillä yleensä viimeistään seuraavana arkipäivänä. SEPA-pikasiirto puolestaan mahdollistaa rahan siirtämisen vastaanottajan tilille vuoden jokaisena päivänä kellon ympäri ja varat siirtyvät maksajalta saajalle kymmenessä sekunnissa. Maksaminen nopeutuu entisestään koko euromaksualueella, kun yhä useammat pankit ottavat käyttöön SEPA-pikasiirron korvaamaan SEPA-tilisiirron. Tällä hetkellä suurimmat pankit Suomessa ja koko SEPA-alueella vastaanottavat pikasiirtoja. Pikasiirron myötä maksamiseen liittyvä mahdollinen viive häviää. (EKP, 2020; OP, n.d.)

Maksajan omasta pankistaan saajalle tekemä maksu siirtyy saajan pankille usean välietapin ja järjestelmän kautta. Kuvassa 1 nähdään SEPA-maksun välittymisen vaiheet.

Kuva 1 SEPA-maksun välittyminen (Suomen Pankki, n.d.-b)



Kuvassa 1 nähdään, miten SEPA-tilisiirrot kulkevat pankkien välillä eurooppalaisen selvityksen eli EBA Clearingin välityksellä. SEPA-tilisiirrot kulkevat SWIFT-verkossa ja maksujen katteensiirto tapahtuu TARGET2-järjestelmässä. Maksun perille kirjautumiseksi tarvitaankin useaa järjestelmää ja maksun matka on monivaiheinen. Maksujen välittyminen on ottanut valtavia harppauksia eteenpäin ja muutamien vuosien takainen viive maksujen välittymisessä on jäänyt historiaan uuden ketterämmän teknologian kehittymisen myötä. (Finanssiala, 2023)

2.1 Maksamisen järjestelmät

Maksamisen infrastruktuuri eli maksamiseen liittyvät maksujärjestelmät ovat ne järjestelyt ja järjestelmät, joita käytetään maksujen välittämiseen maksajan ja saajan välillä. Arvopaperi infrastruktuureilla eli selvitysjärjestelmillä tarkoitetaan taas niitä järjestelyä ja järjestelmiä, joita käytetään arvopapereiden, johdannaisten sekä muiden talouden transaktioiden määrittämiseen, toteuttamiseen ja tallentamiseen. Nämä rahoitusjärjestelmän infrastruktuurit pitävät huolen siitä, että raha siirtyy osapuolelta toiselle. Kun kaikki toimii moitteettomasti tämä jää huomaamattomana talouden taustalle. Jos puolestaan ilmenee

ongelmia, yhteiskunnan arki mutkistuu nopeasti. (Suomen Pankki, n.d.-a; Snellman, 2017)

Suomen pankkisektori oli pääosin kotimainen 1990-luvulle asti. Kotimainen finanssisektori, tavat maksaa ja Suomessa käytössä olevat maksujärjestelmät ovat kansainvälistyneet ja hajaantuneet teknologisen kehityksen seurauksena. Taustalla toimivat maksamisen mahdollistavat järjestelmät ovat muuttuneet kotimaisista kansainvälisiksi ja Suomessa tarjottavia palveluita tuotetaan laajasti ulkomailta ja ulkomailla sijaitsevilla tietojärjestelmillä. (Terho & Wathén, 2023)

Pankeilla on käytössään useita kriittisiä järjestelmiä, joiden avulla maksuliikennettä ja likviditeetinhallintaa eli kassanhallintaa toteutetaan. Tutustutaan seuraavaksi kotimaisten pankkien käyttämiin tärkeimpiin maksunvälitykseen liittyviin järjestelmiin, joiden avulla mahdollistetaan maksuliikenteen toteutuminen eri osapuolten välillä.

EBA Clearingin ylläpitämä yhteiseurooppalainen STEP2-järjestelmä on merkittävin vähittäismaksamiseen liittyvä maksujärjestelmä Suomen kannalta. Pankkien välisessä maksuliikenteessä tilisiirrot välitetään tyypillisesti STEP2-järjestelmässä ja se on tarkoitettu yhtenäisen euroalueen eli SEPA-alueen tilisiirroille. Suomessa toimivat pankit välittävät sen kautta tilisiirtoja ja suoraveloituksia kotimaan lisäksi koko euroalueelle. Euromaksualueeseen siirtymisen yhteydessä vuonna 2008 suomalaiset pankit siirsivät myös kotimaiset pankkien väliset sisäiset tilisiirrot tähän ulkomailla sijaitsevaan järjestelmään. Järjestelmän pääjärjestelmä sekä varajärjestelmät ovat Suomen ulkopuolella. (HE 104/2022)

TARGET2 eli T2 on eurojärjestelmän ylläpitämä Euroopan laajuinen automatisoitu reaaliaikainen bruttomaksujärjestelmä, jossa liikkuu pankkien likviditeetti. T2-järjestelmässä sen osapuolina toimivat pankit voivat suorittaa euromääräisiä maksuja reaaliajassa keskuspankeissa olevien tilien välillä. T2-järjestelmässä liikkuvia euroja kutsutaan keskuspankkirahaksi. Euromaksuissa kate sekä maksu tulevat eurooppalaisesta keskuspankkijärjestelmästä, eli T2-järjestelmästä. Useiden muiden maksujärjestelmien, kuten esimerkiksi STEP2, POPS ja EURO1 selvityksen jälkeen tapahtuvat katteensiirrot toteutetaan T2-järjestelmässä pankkien tileiltä. T2 koostuu eurojärjestelmän keskuspankkien osajärjestelmistä ja Suomessa on T2-Suomen Pankki -osajärjestelmä. Sen tekninen infrastruktuuri sijaitsee Suomen rajojen ulkopuolella. Muita suomalaisten pankkien käyttämiä maksujärjestelmiä ovat TIPS, POPS, EURO1, RT1 ja CLS. TIPS eli Target Instant Payment Settlement on eurojärjestelmän ylläpitämä Euroopan laajuinen

reaaliaikainen maksupalvelu. Siellä katteet liikkuvat kellon ympäri keskuspankkirahassa muutamissa sekunneissa vuoden jokaisena päivänä. (HE 104/2022; Suomen Pankki, n.d.-b)

Eurooppalainen pikamaksujen selvitysalusta TIPS otettiin käyttöön vuonna 2018. TIPS ei mahdollista selvitystä valuuttojen välillä, mutta suunnitelmat sen toteuttamiseksi ovat olemassa. Vuoden 2025 alusta kaikilla pankeilla tulee olla valmius vastaanottaa pikamaksuja ja myöhemmin vuoden aikana myös valmius lähettää niitä. EU:n uuden pikamaksuasetuksen myötä euromaiden pankkien on siirryttävä tarjoamaan nopeampia tilisiirtoja vuoden 2025 lokakuuhun mennessä. Asetuksen myötä varojen pitää liikkua pankkien ja euromaiden välillä kymmenessä sekunnissa riippumatta sijainnista tai kellonajasta. Suomessa kaikki pankit pystyvät vastaanottamaan näitä maksuja jo nyt, mutta vain osa lähettää niitä. Tämän uudistuksen myötä maksujen välitys tehostuu merkittävästi. (Kavander, 2024; Ripatti, 2024)

POPS-järjestelmä eli pankkien väliset onlinepikasiirrot ja sekit on lähes ajantasainen pankkien online-pikasiirtojärjestelmä, jossa välitetään kotimaisten pankkien välisiä pikasiirtoja ja sekkimaksuja. Se on puhtaasti kotimainen ja lähes ajantasainen järjestelmä, jossa pankit lähettävät maksutiedot suoraan toisilleen ja pankkien järjestelmät keskustelevat keskenään tietojen välittämiseksi. POPS-pikasiirtoja välitetään pankkipäivinä ja ne välitetään tunnin kuluessa maksajalta saajalle. EURO1 on EBA Clearingin ylläpitämä suurten maksujen järjestelmä, jonka kautta välitetään niin kotimaisia kuin rajat ylittäviä euromääräisiä maksuja. Ne voivat olla asiakasmaksuja tai pankkien välisiä tapahtumia. EURO1-nettojärjestelmässä välitettävien maksujen katteet siirretään kerran päivässä iltapäivisin T2-bruttojärjestelmässä. RT1 on EBA Clearingin ylläpitämä SEPA-pikasiirtoja välittävä järjestelmä. CLS eli Continuous Linked Settlement on maksu vastaan maksua periaatteella toimiva kansainvälinen valuuttakaupan nettojärjestelmä. Sitä operoi CLS Bank.

Swift eli Society for Worldwide Interbank Financial Telecommunication on maailmanlaajuinen pankkien välinen tietoverkko, joka mahdollistaa rahasiirtojen ja muiden finanssitoimialan kannalta tärkeiden tietojen välittämisen. Sen kautta tapahtuu pankkien välinen viestiliikenne ja se onkin rahoitusmarkkinoiden merkittävin sanomavälityspalvelun tarjoaja. Maksusanomat pankkien välillä välitetään Swift-verkossa pankilta toiselle. Ne antavat tiedon siitä kuka maksaa ja kenelle. Samoin maksun selitteen ja summan. Maksusanomien välitys tapahtuu yksilöivien BIC-koodien avulla standardoiduin sanomin turvallisen tietoliikenneyhteyden välityksellä. Pankkien lisäksi tietoverkossa on esimerkiksi

keskuspankit sekä maksujen- ja arvopapereiden selvitysjärjestelmät. Varsinainen raha eli pankkien väliset katteensiirrot tapahtuvat ja kirjataan puolestaan eri pankkien keskuspankkitilien välillä tai kirjeenvaihtajapankkijärjestelmässä liikepankkien keskinäisten tilien välillä. Swiftin operatiivinen toiminta tapahtuu Suomen rajojen ulkopuolella. Sen kautta muodostetaan yhteys keskeisiin maksuliikenteen infrastruktuureihin, kuten T2- ja STEP2-järjestelmiin. (HE 104/2022; Suomen Pankki, n.d.-a)

Suomen kannalta kriittiset ja keskeiset rahoituslaitosten maksamisen mahdollistavat järjestelmät sijaitsevat ulkomailla. Euromääräisten maksujen katteensiirto näissä kaikissa edellä mainituissa järjestelmissä tapahtuu T2-järjestelmässä. Maksujen ja katteiden välitys eri pankkien välillä toteutetaan useiden eri järjestelmien avulla, joiden välillä vallitsee keskinäisiä kansainvälisiä riippuvuuksia. Maksujenvälitykseen liittyy pitkiä toimitusketjuja ja riippuvuus suhteita. Maksaminen osapuolelta toiselle toimii nopeasti lähes reaaliajassa.

Päivittäin tekemiemme maksujen katteet pankkien välillä selvitetään T2-järjestelmässä olevilla keskuspankkitileillä. Pelkästään Suomen Pankin omat maksujärjestelmäosapuolet lähettivät T2-järjestelmässä maksuja 49 mrd. euron edestä joka päivä vuonna 2022. Järjestelmää käyttää maksujenvälitykseen yli 1 700 pankkia. Jos mukaan luetaan sivuliikkeet tytäryhtiöineen, T2-järjestelmän välityksellä tavoittaa yli 55 000 pankkia eri puolilla maailmaa. Swiftin suojattuja viestipalveluita käyttää yli 11 000 rahoituslaitosta yli 200 maassa ympäri maailmaa. Se on ensisijainen rahoituslaitosten välinen viestintäkanava. (EKP, 2016; Peltoniemi & Ripatti, 2023; Swift, n.d.)

2.2 Kyberturvallisuus

Kyberturvallisuus on monimutkainen kokonaisuus, jonka avulla pyritään turvaamaan yhteiskunnan tai organisaation kriittiset ja tärkeät toiminnot. Se on kyberriskienhallintaa ja yksi kansallisen turvallisuuden osa-alueista. Kyberturvallisuuden merkitys huoltovarmuudelle lisääntyy, sillä yhteiskunnan kriittiset yritykset kuten pankit digitalisoivat keskeisiä toimintojaan. Verkkoyhteyden, erilaisten digitaalisten ympäristöjen sekä järjestelmien toiminta on välttämätöntä yritysten ja koko yhteiskunnan toiminnalle. Suomalainen yhteiskunta on lähes täysin digitalisoitunut. (Huoltovarmuuskeskus, 2020, s. 7; Suomi.fi, 2024-d)

Kun puhutaan kyberturvallisuudesta, tarkoitetaan kaikkia niitä toimia, joilla pyritään edistämään digitalisoituneen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta.

Niitä toimenpiteitä, joiden avulla suojataan tietokoneet, viestintä- ja tietojärjestelmät sekä muut sähköiset järjestelmät. Samoin niissä tallennettavat, käsiteltävät tai siirrettävät tiedot. Lisäksi niiden käyttäjät, hyödyntäjät ja muuten asianosaiset henkilöt kyberuhilta. Kyberturvallisuus liittyy tapoihin, joiden avulla pyritään suojaamaan tietojärjestelmiä, verkkoja ja tietoja varkauksilta, vahingoilta, luvattomalta pääsyltä tai miltä tahansa muulta verkkohyökkäykseltä. Kyberturvallisuus pitää sisällään teknologioita, prosesseja ja käytäntöjä, jotka on suunniteltu varmistamaan sähköinen turvallisuus. Kyberturvallisuus on elintärkeä osa suomalaista kokonaisturvallisuuden mallia. Yhteiskunnan perusrakenteiden ja palvelujen, kuten esimerkiksi tieto- ja viestintäverkkojen ja niihin liittyvän infrastruktuurin pitää toimia kaikissa olosuhteissa. (Valtioneuvosto, 2024-b, s.10; Techopedia, n.d.)

Kyberriskillä tarkoitetaan yleensä organisaation tietojärjestelmiin kohdistuvaa haitallisen tapahtuman uhkaa. Potentiaalisia vaaroja, riskitekijöitä tai hyökkäyksiä, jotka voivat kohdistua esimerkiksi tietojärjestelmiin. Usein ne ovat seurausta rikollisesta toiminnasta, esimerkiksi palvelunestohyökkäyksestä. Hyökkääjät saattavat yrittää murtautua yksityiseen tai organisaation tietokoneeseen taloudellisen hyödyn saamiseksi sekä vahingon ja häiriön aiheuttamiseksi. Kyberhyökkäys voi vaikuttaa arjen sujuvuuteen ja sen seurauksena esimerkiksi verkkoyhteydet voivat katketa tai pankin palvelut voivat olla poissa käytöstä. Häiriön tai hyökkäyksen aikana organisaation digitaaliset palvelut tai järjestelmät eivät toimi normaalisti. Kyberhyökkäyksellä tarkoitetaan vahingontekoa tai häirintää. Se voi kohdistua muun muassa järjestelmiin, tietoverkkoihin, laitteisiin tai digitaalisesti tallennettuihin tietoihin tai kyse voi olla tietojenkalastelusta. (Grym, 2017; Suomi.fi, 2024-c)

Palvelunestohyökkäyksessä verkkopalvelun toimintaa pyritään hidastamaan tai estämään. Tietomurrossa järjestelmiin tallennettuja tietoja varastetaan. Hyökkääjä voi hyökätä tietojärjestelmiin ja häiritä esimerkiksi pankin maksuliikennettä. Kyberrikollisten hyökkäyksien ja kohteiden kirjo on laaja. Ne voivat olla muun muassa palvelunestohyökkäyksiä, kiristyshaittaohjelmia, tuhoavia ohjelmia ja kriittiseen infrastruktuuriin kohdistuvia hyökkäyksiä. Motiiveja voi olla erilaisia. Kyseessä voi olla esimerkiksi sähköinen pankkiryöstö. Turvallisuusuhat ovat aina läsnä, kun rahaa siirretään verkossa. Hyökkääjä voi pyrkiä hyötymään hyökkäyksen vaikutuksista myös välillisesti. Kyse voi olla tiedustelusta, häirinnästä, sabotaasista tai tuhoamisesta. Motiivina voi olla kiusanteko ja mielenilmaus tai kansainvälinen kyberrikollisuus ja valtiollinen vaikuttaminen. (Suomi.fi, 2024-c; Terho & Wathén, 2023)

Kyberhyökkäys voi aiheuttaa haittaa yksittäiselle pankille, mutta myös koko finanssialalle. Tietotekniikkaa on digitalisoituneessa yhteiskunnassamme kaikkialla ja kyberriskit

realisoituvat käytännössä ohjelmistojen kautta. Vakavia uhkia ovat kyberhyökkäykset kriittiseen infrastruktuuriin ja yhteiskunnallisen vakauden horjuttaminen kybervaikuttamisen keinoin. Kybervaikuttaminen on yksi hybridivaikuttamisen keinoista. Valtiollisille kyberuhille on tyypillistä hankkia tietoa laittomilla keinoilla valtionhallinnon päätöksenteosta sekä valtion ja yhteiskunnan kannalta kriittisistä haavoittuvuuksista. Pyrkimyksenä voi myös olla päätöksenteon ja yhteiskunnan toimintakyvyn laajempi häiritseminen, heikentäminen ja lamauttaminen. Poikkeusoloissa kyberhyökkäykset ovat osa sodankäynnin keinovalikoimaa. Finanssialan toiminnot, palvelut sekä tiedot ovat lähes täysin sähköisiä ja niiden suojaaminen kyberuhilta on keskeistä tämän kriittisen infrastruktuurin toiminnan varmistamiseksi. (Sisäministeriö, n.d.; Suomen Pankki, n.d.-g)

Kyberhyökkäykset saattavat tulla kalliiksi yritykselle ja pahimmillaan uhata koko rahoitusjärjestelmän vakautta. Kyberhyökkäykset eivät ole uhka vain yksittäisille instituutioille, vaan kyberriskit ovat luonteeltaan globaaleja. Koska rahoitusalalla on paljon keskinäisiä kytköksiä, ne voivat myös uhata koko rahoitusekosysteemin vakautta. Rahoitusalan toimijat muodostavat keskenään pitkiä toimitusketjuja ja kansainvälisiä riippuvuussuhteita. Vakava häiriötilanne vaikuttaa usein moneen toimialaan. Kyberhyökkäysten torjuntaan tarvitaan pankkien ja viranomaisten yhteistyötä. (Euroopan Keskuspankki, n.d.)

2.3 Huoltovarmuus ja jatkuvuudenhallinta

Huoltovarmuudella tarkoitetaan varautumista mahdollisiin kriiseihin ja häiriötilanteisiin. Lisäksi jatkuvuudenhallintaa turvaamalla elintärkeät toiminnot, joiden avulla yhteiskunta ja elinkeinoelämä toimivat ja ihmiset voivat elää arkeaan turvallisesti. Perinteisesti huoltovarmuudella on tarkoitettu materiaalien saannin varmuutta. Nykyään sen painopiste on entistä vahvemmin kriittisen infrastruktuurin toimintakyvyn varmistamisessa. Huoltovarmuuden perustana on toimivat markkinat ja kilpailukykyinen talous. Erilaisten häiriötilanteiden ja poikkeusolojen varalle tarvitaan huoltovarmuustyötä, minkä avulla varaudutaan ylläpitämään erilaiset kriittiset yhteiskunnan toiminnot mahdollisimman normaaleina näissä tilanteissa. Huoltovarmuutta Suomessa varmistetaan yhteistyössä julkisen, yksityisen ja kolmannen sektorin kanssa.

Kansainvälistyminen, verkostotalous sekä teknologinen kehitys voivat aikaansaada uudenlaisia riskitekijöitä. Sen vuoksi huoltovarmuuden keinoja kehitetään jatkuvasti. Perinteisen materiaalisen varautumisen lisäksi ja sen rinnalle on noussut kriittistä tuotantoa

ja järjestelmiä ylläpitävien organisaatioiden ja verkostojen toiminnan jatkuvuuden varmistaminen eli jatkuvuudenhallinta. Keskeisenä tavoitteena on turvata kriittisten infrastruktuurien, tuotannon ja palvelun toimivuus niin, että väestön, talouselämän sekä maanpuolustuksen välttämättömimmät perustarpeet pystytään täyttämään missä olosuhteissa tahansa. Huoltovarmuustyön tavoite on, että vakavat häiriötilanteet ja poikkeusolot voidaan hoitaa kansallisin toimenpitein. Huoltovarmuustoiminta edellyttää laajaa kansainvälistä yhteistyötä, sillä kansainväliset keskinäisriippuvuudet ja globaalit arvoketjut ovat yhä merkittävämpiä. (Huoltovarmuuskeskus, 2024-b)

Jatkuvuudenhallinta on kokonaisvaltainen prosessi. Se pyrkii varmistamaan organisaation kyvyn toipua ja jatkaa toimintaansa mahdollisimman tehokkaasti erilaisten odottamattomien häiriöiden sattuessa. Se on tärkeä osa riskienhallintaa ja auttaa varautumaan erilaisiin uhkiin ja varmistamaan, että organisaatio voi jatkaa toimintaansa vaikeissakin tilanteissa. Jatkuvuudenhallinta on organisaation ydintoimintojen turvaamista ennalta määriteltyjen mallien mukaan. Hyvin suunnitellun varautumisen avulla turvataan palveluiden ja yhteiskunnan toiminta erilaisissa häiriötilanteissa. Jatkuvuudenhallinta edellyttää, että organisaatio tai yhteiskunta tunnistaa toiminnan mahdollistavat kriittiset tekijät, jonka jälkeen turvallisuuden toimenpiteet voidaan kohdentaa oikeisiin kohteisiin. On tärkeää etukäteen tunnistaa, mistä palveluista toiminta on riippuvaista. Jatkuvuudenhallinnan tavoitteena on ennaltaehkäistä häiriötilanteet ja varmistaa mahdollisimman häiriötön toiminta erilaisissa tilanteissa ja poikkeusoloissa. Sen avulla pyritään välttämään toiminnan keskeytyksistä aiheutuvia negatiivisia vaikutuksia ennaltaehkäisemällä häiriöt ja rajoittamalla mahdollisten häiriöiden vaikutuksia lyhentämällä niiden kestoa. (Suomi.fi, 2024-a; Suomi.fi, 2024-b)

2.4 Pankit osana kriittistä infrastruktuuria

Kriittisellä infrastruktuurilla tarkoitetaan perusrakenteita, palveluja sekä niihin liittyviä toimintoja, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi. Näitä ovat esimerkiksi sähköverkko, vesi- ja jätehuolto, liikenneväylät sekä tieto- ja rahaliikenteen turvatut yhteydet. Kriittinen infrastruktuuri pitää yhteiskunnan rattaat pyörimässä ja on huoltovarmuuden perusta. Se sisältää niin fyysisiä laitoksia ja rakenteita kuin digitaalisia toimintoja ja palveluja. Kriittinen infrastruktuuri voidaan kiteyttää yhteiskunnan perusrakenteiksi ja järjestelmiksi, joita ilman yhteiskunnan elintärkeät toiminnot häiriintyvät vakavasti. Yritys voi olla kriittinen myös sen vuoksi, että se tuottaa muille kriittisille palveluille tai toiminnoille toimivuuden kannalta keskeisiä tukipalveluita ja

on siten itse kriittinen osa toimitusketjua. Suurin osa kriittisestä infrastruktuurista on yksityisen sektorin omistuksessa. (Huoltovarmuuskeskus, 2023-a; Huoltovarmuuskeskus, 2024-b; Valtioneuvosto, 2022-b, s. 45)

Maksaminen on talouden perusta ja yksi järjestäytyneen yhteiskunnan peruspilareista. Rahoitusjärjestelmän ja maksuliikenteen kansallinen varautuminen on tärkeä osa koko kansakunnan kokonaisturvallisuutta. Rahoitusmarkkinoiden vakaa ja häiriötön toiminta on edellytys yhteiskunnan toimivuudelle. Maksaminen on oleellinen, miltei kaikkiin finanssipalveluihin linkittyvä osa. Kaikki rahaliikenne kulkee pankin järjestelmien kautta. Jos pankin maksuliikenne pysähtyy, seisahtuu hyvin äkkiä koko Suomi. Rahoitusjärjestelmän infrastruktuuri pitää huolen siitä, että raha siirtyy henkilöltä tai yritykseltä toiselle. (Rehn, 2021; Snellman, 2017)

Pankin rooli yhteiskunnassa on olla osana kriittistä infrastruktuuria. Keskuspankit ovat osapuolia maksujärjestelmissä ja maksupalveluiden toimivuuden varmistaminen on osa huoltovarmuutta. Suomen Pankin strategiassa luotettavista maksu- ja selvitysjärjestelmistä huolehtiminen on keskeinen osa palveluja suomalaisille. Turvalliset ja tehokkaat järjestelmät ovat edellytyksenä sille, että rahaliikenne toimii luotettavasti yhteiskunnassa. Maksujärjestelmien ja maksupalveluntarjoajien tulee varautua riittävästi häiriöihin ja uhkiin, jotka kohdistuvat niiden tarjoamaan palveluun. Palveluissa olevien häiriöiden leviäminen maksujärjestelmien kautta muihin toimijoihin on pyrittävä estämään. Toimintavarmuuden ja palautumiskyvyn jatkuva kehittäminen on ensiarvoisen tärkeää. (Suomen Pankki, n.d.-c; Rehn, 2021)

Maksujärjestelmät eli rahoitusmarkkinoiden infrastruktuuri toimii parhaimmillaan sujuvasti ja taustalla ilman, että loppukäyttäjät kiinnittävät siihen mitään huomiota. Jos rahat myöhästyvät tai eivät tule perille se aiheuttaa haittaa sekä rahan lähettäjälle että vastaanottajalle. Pahimmillaan maksujärjestelmien toimimattomuus voi vaarantaa rahoitusmarkkinoiden vakauden, sillä yksittäiset rahoitusalan toimijat muodostavat yhdessä laajemman kokonaisuuden. Yksittäinen toimija voi käyttää useita maksu- ja selvitysjärjestelmiä ja toiminta voi olla hajautettua useisiin eri maihin. Jos tällaisella laajasti verkottuneella toimijalla olisi vakavia ongelmia, ne realisoituisivat nopeasti myös monissa muissa maissa ja järjestelmissä aiheuttaen ongelmia ja kerrannaisvaikutuksia useille tahoille. (Laine, 2018; Peltoniemi & Ripatti, 2023)

3 Maksamisen turvallisuus

Kun tarkastellaan yleistä turvallisuustilannetta Suomessa ja Euroopassa, se on vakavampi ja vaikeammin ennakoitavissa kuin kertaakaan kylmän sodan jälkeen. Venäjän hyökättyä Ukrainaan helmikuussa 2022 turvallisuusympäristössä tapahtui perustavanlaatuinen muutos. Jännitteiden lisääntyminen heikentää myös Itämeren alueen turvallisuustilannetta ja sen ennakoitavuutta. Lisääntyvä maailmanlaajuinen keskinäinen riippuvuus, kehittyvä teknologia ja valtionrajat ylittävät uudet uhat ovat muokanneet toimintaympäristöä 2000-luvulla (Valtioneuvosto, 2022-b, ss. 7–8)

Huoltovarmuuden kannalta yksi keskeinen yhteiskunnan taloudellista toimintakykyä vaarantava uhka on sähköisten tieto- ja viestintäjärjestelmien häiriintyminen. Se on erittäin häiriöherkkä monenlaisille uhille sekä riskeille. Erilaiset kyberhyökkäykset, haittaohjelmat, palvelunestohyökkäykset ja muut verkkoterrorismin muodot lisääntyvät entisestään ja niillä voi olla vakavia vaikutuksia. Venäjän hyökkäyssota Ukrainassa sekä Suomen Nato-jäsenyysprosessi nostivat Suomen kriittiseen infrastruktuuriin kohdistuvaa uhkaa niin fyysisessä kuin kyberympäristössä. Suomeen kohdistuu vuosittain noin 10 000 kyberhyökkäystä. (Suomen huoltovarmuusdata oy, n.d.; Terho & Wathén, 2023)

Pankkien palveluiden ja toimintojen digitalisoituminen sekä geopoliittisten jännitteiden voimistuminen ovat vaikuttaneet merkittävästi kyberhäiriöiden lisääntymiseen. Geopoliittiset jännitteet ovat kasvattaneet valtioihin sidoksissa olevien ryhmien hyökkäysten riskiä. Lisääntyvät kyberuhat ja riippuvuus yhteisistä ulkopuolisista palveluntarjoajista asettavat pankeille merkittäviä haasteita. EKP: n valvomien yhteisöjen ilmoittamien merkittävien kyberhäiriöiden määrä lisääntyi voimakkaasti vuonna 2023 ja pysyi samalla tasolla vuoden 2024 ensimmäisenä kolmena neljänneksenä. Geopoliittiset riskit saattavat vaarantaa pankkien kyvyn selviytyä operatiivisista häiriöistä varsinkin, jos ne johtavat tietotekniikka- ja kyberturvallisuusriskien kasvuun. EKP:n pankkivalvonnan strategiassa huomattavina haavoittuvuustekijöinä nousi esiin tietotekniikan ulkoistaminen ja tietoturvaa sekä kyberriskejä koskevat operatiivisen häiriösietokyvyn puutteet. Ulkoistamisen voimakas keskittyminen tietyille palveluntarjoajille voi pahentaa häiriöiden leviämisen riskiä ja lisätä kyberhäiriöiden vaikutuksia koko rahoitusjärjestelmään. (Euroopan Keskuspankki, 2024-b)

Yhteiskunnan normaalia toimintaa ja ihmisten arkea voi uhata rikkomalla ja häiritsemällä kriittistä infrastruktuuria, mutta sen lisäksi myös vaikuttamalla ihmisten mieliin ja luottamukseen. Rahoitussektorin toiminta perustuu luottamukseen, minkä vuoksi nämä

uhat on otettava vakavasti. Rahoitusalan toiminnan välttämätön edellytys on, että luottamus sen toimintaan ja erityisesti maksamiseen voidaan säilyttää. (Rehn, 2021)

Geopoliittisen epävarmuuden myötä rahoitusjärjestelmän infrastruktuuriin kohdistuva uhka sekä operatiiviset riskit ovat kasvaneet. Suojelupoliisi varoitti suomalaisia organisaatioita kyberuhkista pian Venäjän hyökättyä Ukrainaan. Sen myötä uhka kriittistä infrastruktuuria kohtaan on noussut. Rahoitusmarkkinoiden vakaa ja häiriötön toiminta on edellytys yhteiskunnan toimivuudelle. Rahoitusmarkkinoiden yhteiskunnan kannalta kriittisten palveluiden tulee olla käytettävissä myös vakavissa kriisitilanteissa. Pohjoismaisiin pankkeihin kohdistuneet häiriötilanteet ovat herättäneet keskustelua yhteiskunnan häiriönsietokyvystä. Vaatii määrätietoisia toimenpiteitä niin pankeilta, viranomaisilta kuin pankkien asiakkailtakin, kun varaudutaan pankkipalveluiden häiriöihin. Pankit ylläpitävät yhteiskunnan kannalta kriittistä infrastruktuuria ja palveluja. Niihin kohdistuvat vakavat hyökkäykset tarjoavat tehokkaan vaikutuskanavan sellaisille toimijoille, joiden tavoitteena on yhteiskunnan horjuttaminen tai jopa lamaannuttaminen. Tehokas tapa rampauttaa yhteiskunnan toimintaa olisi suunnata vakava kyberisku keskeiseen rahoitusjärjestelmän infrastruktuuriin. (Suomen Pankki, n.d.-h; Weuro, 2024)

Nordea joutui syksyllä 2024 useiden ja laajojen palvelunestohyökkäysten kohteeksi. Yhtiö tiedotti syyskuussa, että palvelunestohyökkäykset voivat aiheuttaa hitautta palveluissa ja palvelunestohyökkäykset ovat lisääntyneet pohjoismaissa viimeisten viikkojen aikana. Nordean häiriöiden myötä eduskunnan pankkivaltuusto pyysi selvityksen näistä verkkopankkiongelmista, sillä kyse on arjen huoltovarmuudesta ja perusinfrasta. Kuultaviksi pyydettiin sekä viranomaisia että teknisistä ongelmista kärsineen Nordean edustaja. Kuultaviksi pyydettiin edustajat Valtiovarainministeriöstä, Suomen Pankista, Finanssivalvonnasta, Rahoitusvakausvirastosta, Kyberturvallisuuskeskuksesta, Suojelupoliisista ja Nordeasta. (Nordea, 2024; YLE, 2024)

Nordeaan kuukauden ajan kohdistuneet palvelunestohyökkäykset olivat voimaltaan ja kestoltaan ennennäkemättömiä. Niiden tarkoituksena näytti olevan yhteiskunnan horjuttaminen ja luottamuksen heikentäminen. Aiemmat hyökkäykset ovat olleet kestoltaan vain muutamia päiviä ja nykyisten voima oli 15 kertainen. Ensimmäisen vuosipuoliskon aikana Nordeaan kohdistui 20 palvelunestohyökkäystä ja nyt niitä oli 360. Hyökkäyksen kohteena on tulkittu olevan yhteiskunnan kriittinen infrastruktuuri ja Nordeaa on käytetty välineenä. Nordean arvion mukaan he torjuivat 90 prosenttia hyökkäyksistä niin, että niistä ei aiheutunut näkyvää vaikutusta asiakkaille. Ennennäkemättömäksi hyökkäykset tekivät niiden kesto, voima, hyökkäysten lähdesuunta sekä tuntemattomaksi jäänyt motiivi.

Myös OP ja S-Pankki olivat palvelunestohyökkäysten kohteena maaliskuussa 2025. Hyökkäykset kohdistuivat molempiin pankkeihin saman päivän aikana ja niiden seurauksena verkkopalveluissa esiintyi häiriöitä ja joitain palveluja oli hetkellisesti poissa käytössä. (Kavander, A, 2025; Raeste, 2024)

Huoltovarmuuskeskus kehottikin kriittisen infrastruktuurin yrityksiä nostamaan varautumistasoa muuttuneen turvallisuusympäristön vuoksi. Huoltovarmuuskeskuskeskuksen toimitusjohtaja Janne Känkänen totesi, että huoltovarmuuden kannalta tilanne on vakaa ja palvelut toimivat normaalisti. Kriittiseen infrastruktuuriimme kohdistuneet tahalliset teot ovat kuitenkin otettava vakavasti. Pankkeihin kohdistuneiden palvelunestohyökkäysten lisäksi kriittiseen infrastruktuuriin on kohdistunut viime vuosina useita vakavia vahingontekoja. Kriittisen infrastruktuurin geopoliittinen toimintaympäristö on erittäin epävakaa. (Euroopan komissio, 2023; Huoltovarmuuskeskus, 2023-b)

Vuonna 2022 Venäjältä Saksaan kaasua kuljettavissa Nord Stream 1 ja 2 putkilinjoissa havaittiin vuoto Itämeren alueella. On käytännössä mahdotonta, että molemmat putket vahingoittuisivat vahingossa saman päivän aikana. Syyksi epäillään sabotaasia. Marraskuussa 2024 kaksi Itämeren pohjassa kulkevaa tietoliikennekaapelia vaurioitui. Ruotsin ja Liettuan välinen merikaapeli vaurioitui sunnuntaiaamuna ja Suomen sekä Saksan välinen merikaapeli vaurioitui päivä tämän jälkeen maanantaiaamuna. Kaapeli katkesi ja vian seurauksena kaapelissa kulkevat tietoliikenneyhteydet olivat poikki. (Kejo, 2022; Nissilä & Korhonen, 2024)

Joulukuussa 2024 vedenalaista infrastruktuuria vaurioitui, kun Eagle S raakaöljytankkerin epäillään aiheuttaneen ankkurillaan kaapelirikkoja Suomen ja Viron välisen EstLink 2 sähkökaapeliin merenpohjassa. Suomenlahdella tapahtuneen sähkökaapelivaurion seurauksena Eduskunnan puolustusvaliokunta keskeytti joulutaukonsa. Viranomaiset varautuvat hybridivaikuttamiseen ja kertoivat seuraansa tilannetta tarkasti. Latvian ja Ruotsin välinen meressä sijaitseva tietoliikennekaapeli vaurioitui Itämerellä sunnuntaiaamuna tammikuun lopulla 2025. Laivayhtiön edustaja kommentoi sään olleen erittäin huono ja miehistö huomasi sunnuntaiaamuna toisen ankkurin raahautuneen pohjassa. Kaapelivaurioita onkin sattunut viime aikoina useita, ja keskusteluun on noussut kysymys siitä, voiko tankkerialus roikottaa ankkuriaan merenpohjassa kymmeniä kilometrejä vahingossa? (Isokoski, 2024; Liski, 2025)

Huoltovarmuuskeskus julkaisee kuukausittain katsauksen Suomen huoltovarmuuden yleistilanteesta. Syyskuun tiedotteessa ilmeni, että finanssialalla tietojärjestelmissä sekä maksujärjestelmissä on esiintynyt yksittäisiä häiriöitä, mutta häiriöt eivät ole vaikuttaneet huoltovarmuuteen. Myös lokakuun tiedotteessa kerrottiin, että pankkipalveluihin on kohdistunut kyberhyökkäyksiä, jotka ovat aiheuttaneet hetkellisiä palveluhäiriöitä. Nämä häiriöt ovat vaikuttaneet henkilöasiakkaisiin, mutta huoltovarmuuden näkökulmasta häiriöt ovat olleet lieviä. Katsaukset julkaistiin Nordeaan kohdistuneiden häiriöiden jälkeen. (Huoltovarmuuskeskus, 2024-c; Huoltovarmuuskeskus, 2024-d)

Pankit ovat voimakkaiden kyberhyökkäysten kohteena päivittäin ja hyökkäysten määrä lisääntyy jatkuvasti. Samoin hyökkäykset yhteiskunnan kriittisiin toimintoihin ovat arkipäiväistyneet. On olemassa viitteitä siitä, että viimeaikaisten vahingontekojen taustalla on valtiollinen toimija. Sabotaasin yleistymisestä huolimatta niistä vain pienellä osalla on ollut vaikutusta digitaalisiin palveluihin aiheuttaen hitautta tai lyhyitä katkoja. Vuonna 2024 tehty kyberuhkien sietokyvyn stressitesti kertoi, että pankkien käytännöt kyberhyökkäyksiä vastaan ja siihen miten niissä toimitaan ja niistä palaudutaan ovat yleensä erittäin hyviä. Esiin nousi myös osa-alueita, joissa pankeilla on parantamisen varaa. Niitä olivat muun muassa jatkuvuutta koskevat järjestelyt, tietoturvapoikkeamien hallinnan suunnittelu, varmuuskopioinnin tietoturva ja ulkoisten palveluntarjoajien hallinta. Valvojat seuraavat edelleen niitä puutteita, jotka koskevat pankkien kykyä palautua niihin kohdistuneesta kyberhyökkäyksestä. (Ahosniemi, 2024; Euroopan Keskuspankki, 2024-b)

Geopolitiikka, erilaiset kyberuhat ja hybridivaikuttaminen ovat läsnä ja todellisuutta. Erilaiset uudet ja vahvistuneet uhat edellyttävät, että huoltovarmuuden turvaamisen ja varautumisen tasoa vahvistetaan. Tämän tarpeen lähtökohtana on Suomen muuttunut turvallisuusympäristö, joka heijastuu huoltovarmuustoimintaan. Suomeen kohdistuneet palvelunestohyökkäykset ovat lisääntyneet 122 prosenttia vuoden 2024 alusta (Kärkkäinen, 2025).

3.1 Lainsäädäntö ja viranomaiset

Kyberuhat ovat lisääntyneet huomattavasti ja ne ovat rahoitussektorinkin tekemien riskiarvioiden keskiössä. Finanssialan kybervarautuminen on huoltovarmuusorganisaatiossa toteutetun selvityksen mukaan hyvällä tasolla. On kuitenkin fakta, että uhat muuttuvat ja esimerkiksi valtiollisilla toimijoilla sekä niihin sidoksissa olevilla rikollisryhmillä on käytössään laajoja resursseja, viimeisintätekniikkaa sekä yhä enemmän

tekoälyyn ja oppiviin järjestelmiin perustuvaa suorituskykyä. On paljon keinoja, joiden avulla rahoitusalalla varaudutaan edellä mainittuihin uhkiin ja olemassa olevaa keinovalikoimaa kehitetään jatkuvasti. Kyberturvallisuutta, kansallista varautumista ja maksuliikenteen huoltovarmuutta ohjaavat useat lait ja säädökset. Sääntely ja varautumisvelvoitteet ovat viime vuosina lisääntyneet ja lisääntyvät entisestään. Rahoitusalan varautumisvaatimusten laajenemisen perusteena on, että rahoitussektorin tarjoamat peruspalvelut ovat yhteiskunnan toiminnalle välttämättömiä kaikissa olosuhteissa. Finanssiala palveluineen on yhteiskuntamme elintärkeitä toimintoja ja siksi houkutteleva kohde hyökkäyksille, jotka tapahtuvat tietoverkkojen kautta. Alan tietojärjestelmät pitävät sisällään valtavan määrän tietoa kaikista Suomalaisista. Suomen rahoitusala on integroitunut tiiviisti pohjoismaiseen, eurooppalaiseen ja globaaliin markkinaan. Varautuminen hybridiuhkiin onkin tehtävä koko Euroopan laajuisesti. (Finanssiala, 2025; Heikkinen, 2023)

Finanssialan yrityksiltä edellytetään varautumista normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. Varautumisvelvollisuudesta on säädetty finanssialan yrityksiä koskevassa lainsäädännössä, muun muassa luottolaitoslaissa ja maksulaitoslaissa. Keskeistä varautumisessa on kriittisten maksamisen järjestelmien toiminnan varmistaminen ja turvaaminen. Tärkeimpiä ohjaavia lakeja ovat Valmiuslaki 1552/2011, Laki huoltovarmuuden turvaamisesta 1390/1992, Laki huoltovarmuuden turvaamisesta rahoitusalalla 666/2022, Laki luottolaitostoiminnasta 610/2014, Laki luottolaitosten ja sijoituspalveluyritysten kriisinratkaisusta 1194/2014, Laki rahoitusvakausviranomaisesta 1195/2014, Maksulaitoslaki 297/2010, Laki Suomen Pankista 214/1998 sekä näiden lisäksi lukuisat Finanssivalvonnan ohjeet ja Euroopan unionin oikeus. Tietoliikenneyhteyksien suojaamista koskevat vaatimukset asetetaan laissa sähköisen viestinnän palveluista 917/2014, joka on myöhemmin täydentynyt. Ja maksamista ohjaa Maksupalvelulaki 290/2010. (Finanssivalvonta, 2020-a; HE 104/2022, luku 2.2)

Viranomaisten rooli varautumisessa on säännellä ja valvoa sen toteutumista. Sen lisäksi keskuspankit ovat osapuolia tärkeissä maksujärjestelmissä. Omalla toiminnallaan Suomen Pankki voi tukea yksityisen sektorin varautumista. Euroopan Unioni pyrkii erilaisin keinoin parantamaan kyberuhkien sietokykyä, torjumaan kyberrikollisuutta sekä edistämään kyberdiplomatiaa ja puolustusta. Lainsäädäntöä edistetään myös Suomessa. EKP eli Euroopan keskuspankki pyrkii parantamaan jatkuvasti järjestelmiensä tietoturvaa. Se tekee yhteistyötä Euroopan keskuspankkien kanssa pyrkimyksenä vahvistaa Euroopan keskuspankkijärjestelmän ja sen tietojen turvaamista. Se edistää kyberturvallisuutta koko rahoitussektorilla. EKP:n toimenpiteitä kyberturvallisuuden parantamiseksi on kehittää

erilaisia strategioita kyberhyökkäyksiä ja kriisitilanteita varten. Se tekee yhteistyötä muun muassa Euroopan parlamentin, EU:n neuvoston ja komission sekä muiden kansainvälisten organisaatioiden ja rahoituslaitosten kanssa. Pankkivalvojan roolissa EKP edellyttää euroalueen suurimpien pankkien raportoivan välittömästi merkittävistä kyberturvallisuuspoikkeamista. (Euroopan Keskuspankki, 2018)

Maksujärjestelmien yleisvalvojana Suomessa toimii Suomen Pankki. Maksujärjestelmien luotettavuus ja tehokkuus riippuu kaikkien maksamisen ketjuun osallistuvien osapuolten sujuvasta yhteistoiminnasta. Suomen Pankin organisoima Maksuneuvosto on kansallinen yhteistyöelin vähittäismaksamisen kehittämiseksi ja se toimii euromaksualueen vähittäismaksuneuvoston vastaparina. Maksuneuvosto selvittää ja arvioi toimintaympäristön muutoksia, menossa olevia maksamiseen liittyviä hankkeita sekä sääntelyn vaikutuksia. Suomen Pankin koordinoiman maksufoorumin tavoitteena on edistää suomalaisten toimijoiden yhteistyötä ja yhteisten näkemysten muodostumista maksamisen kehittämiseksi. Maksufoorumi kokoaa yhteen maksupalveluiden käyttäjät, tuottajat sekä viranomaiset. Tapahtuma on järjestetty vuodesta 2007 lähtien. (Suomen Pankki, n.d.-e; Suomen Pankki, n.d.-d)

Varautumistyötä tehdään kansainvälisesti, yhteistyössä eri tahojen kesken sekä yhdessä viranomaisten kanssa. Suomessa Valtioneuvosto asettaa yleiset tavoitteet huoltovarmuudelle. Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos. Sen tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta. Huoltovarmuuskeskus toimii tiiviissä yhteistyössä eri alan yritysten, viranomaisten ja julkisen sektorin kanssa varmistaen, että Suomen selkäranka pitää tilanteessa kuin tilanteessa. (Huoltovarmuuskeskus, 2020, s. 4)

Suomessa huoltovarmuus on organisoitu yhteistyöverkostoksi ja sen yhteydessä toimii eri toimialojen yhteistyöverkostoja, joita kutsutaan pooleiksi. Niiden tehtävänä on oman toimialansa huoltovarmuuden ja jatkuvuudenhallinnan kehittäminen, siihen liittyvä neuvonta ja oman toimialan tilannekuvan muodostaminen. Finanssialan sektori ohjaa ja koordinoi alan varautumista yhdessä Huoltovarmuuskeskuksen kanssa. Lisäksi se määrittelee tavoitteet jokaiselle alansa poolille. Finanssialan sektori ja poolit turvaavat toimintaedellytyksiä ja edistävät sekä tukevat alan varautumista poikkeusoloihin. Finanssialan sektori muun muassa kehittää maksujärjestelmiä ja ylläpitää niiden toimintakykyä, kuten pankkien välistä maksuliikennettä. Rahoitusalan pooli vastaa rahoituksen ja maksuliikenteen sekä rahahuollon varautumisesta, alan toimintaedellytysten yleisestä turvaamisesta sekä kansainvälisen yhteistyön koordinoinnista yhdessä alan

toimijoiden ja viranomaisten kanssa. Finanssialan poolin on varmistettava, että tiedonkulkujärjestelmät ovat ajan tasalla ja tarvittaessa kommunikointi on mahdollista nopeasti. Kaikki finanssialan toimijat ovat raportointivelvollisia, jos jotain poikkeavaa tapahtuu. Yhteen pankkiin kohdistuvat ongelmat ja uhat eivät kosketa vain kyseistä pankkia, vaan vaikutukset voivat ulottua koko alalle. Ukrainan tilanteen takia kyberturvallisuuskeskus osallistuu finanssialan sektorin kokouksiin. Siihen liittyen Digitaalinen turvallisuus 2030 on Huoltovarmuuskeskuksen uusi ohjelmakokonaisuus, jonka avulla parannetaan yhteiskunnan sietokykyä kyberhäiriöitä vastaan myös finanssialalla. (Filpus, 2023; Huoltovarmuuskeskus, 2024; Huoltovarmuuskeskus, n.d.-b)

Finanssivalvonta on rahoitus- ja vakuutusvalvontaviranomainen, jonka valvottavia tahoja muun muassa pankit ovat. Pankkivaltuusto puolestaan valvoo Suomen Pankin ja Finanssivalvonnan toimintaa. Maksamisen kyberturvallisuuden näkökulmasta tärkeitä tahoja ovat Kyberturvallisuuskeskus ja Suomen kyberosaamiskeskus. Kyberturvallisuuskeskus on liikenne ja viestintäministeriön Traficomin alaisuudessa toimiva tietoturvaviranomainen. Se tuottaa kyberturvallisuuden tilannekuvaa ja toimii yhteistyössä eri toimijoiden kanssa. Sen tehtäviin kuuluu turvata yhteiskunnan elintärkeitä toimintoja kyberturvallisuusuhilta. Kyberturvallisuuskeskus myös tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyydensuojan toteutumista sähköisessä viestinnässä. Suomen kyberosaamiskeskuksen FICEC:in tehtäviä on kyberturvallisosaamisen kehittäminen, kyberturvallisuustutkimuksen edistäminen ja kansallisen kyberturvallisuuskyvykkyyden ja teollisuuden kyberresilienssin vahvistaminen. Tämä Jyväskylän yliopiston ja ammattikorkeakoulun yhteistyöverkosto edistää Suomen kansallisen kyberturvallisuuden kasvattamista. (Jyväskylän yliopisto, n.d.; Valtiovarainministeriö, n.d.-a)

Rahoitusvakausvirasto osallistuu rahoitusjärjestelmän toiminnan turvaamiseen erilaisissa häiriö- ja kriisitilanteissa. Päämääränään turvata yhteiskunnan toiminnan kannalta välttämättömien rahoitusmarkkinapalvelujen jatkuvuus kaikissa olosuhteissa. Virasto vastaa pankkien kriisinratkaisusta ja talletussuojasta Suomessa. Se myös ylläpitää vakavia häiriötilanteita varten päivittäismaksamisen varajärjestelmää yhdessä Suomen Pankin kanssa. Rahoitusvakausvirasto toimii osana Valtiovarainministeriön asettamaa Rahoitusmarkkinoiden häiriöhallinnan yhteistyöryhmää ja osana EU:n yhteistä kriisinratkaisumekanismia. Valtiovarainministeriö on asettanut rahoitusmarkkinoiden häiriöhallinnan yhteistyöryhmän kehittämään toimintavalmiutta ja varautumistyötä. Yhteistyöryhmä aloitti toimintansa maaliskuussa 2024. Ryhmään kuuluu eri viranomaisia sekä varautumisvelvollisiksi määriteltyjä toimijoita. Häiriöhallinnan yhteistyöryhmän

päätavoite on tukea yksityisiä yrityksiä ja viranomaisia rahoitusmarkkinoiden varautumiseen ja poikkeusolojen toimintavalmiuden kehittämiseen tarvittavassa tietojen vaihdossa sekä suunnittelussa. Yhteistyöryhmä suunnittelee ja yhteensovittaa toimenpiteitä vakavien häiriötilanteiden ja poikkeusolojen tueksi. Se hankkii ja toimittaa tarpeellista tietoa viranomaisten tueksi ja välittää tietoa toimijoille, jotka voivat vähentää häiriötilanteiden haittavaikutuksia yhteiskunnalle. (Laki eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla 666/2022, § 8; Rahoitusvakausvirasto, 2024; Rahoitusvakausvirasto, 2025-a)

3.2 Uudet asetukset ja direktiivit

Rahoitusala on sitoutunut poikkeusolojen varautumistoimiin yhteistyössä viranomaisten ja muiden elinkeinoelämän sektoreiden kanssa. Rahoituslaitosten on varmistettava, että heidän järjestelmänsä ovat turvallisia ja suojattuja erilaisilta tietoturvaan liittyviltä uhilta, kuten hakkeroinnilta ja tietomurroilta. Erilaiset tietoverkkorikollisuuden muodot ovat monimutkaistuneet. Kyberhyökkäykset ovat muuttuneet rohkeammiksi ja niissä hyödynnetään kriittisen infrastruktuurin haavoittuvuuksia. Turvallisuusuhat ovat läsnä aina kun rahaa siirretään verkossa. Maksuliikenteen häiriöttömyys on ensiarvoisen tärkeää ja maksujen tulisi välittyä myös ongelmatilanteissa ja kriisiaikoina. Yhteiskunnassamme on totuttu siihen, että maksaminen on nopeaa ja helppoa. Pankkien on varmistettava myös asiakastietojen turvallisuus ja yksityisyys sekä estettävä mahdolliset kyberhyökkäykset. (Samlink, 2024; Snellman, 2017)

Kriisinkestävyyttä ja varautumista on pyritty kehittämään entisestään. Olemassa olevan lainsäädännön ja sääntelyn tueksi on luotu uusia asetuksia ja direktiivejä, joiden avulla pyritään vastaamaan muuttuneeseen toimintaympäristöön. Euroopan Unioni on laajentanut sääntelyä finanssisektorin kyberriskien kestävyyteen liittyen. Euroopan komissio julkaisi Euroopan turvallisuusunionistrategian vuonna 2020. Siinä linjattiin, että kriittisten toimijoiden fyysistä ja digitaalista kriisinkestävyyttä on edistettävä kokonaisvaltaisesti. EU-maiden tulee yhdenmukaisin menettelyin määrittää ja tunnistaa yhteiskuntien toimintakyvyn kannalta kriittiset toimijat ja parantaa niiden kriisinsietokykyä. Näin parannetaan myös EU:n ja sen jäsenmaiden varautumista laaja-alaiseen vaikuttamiseen, kuten hybridiuhkiin. Tätä tavoitetta tukemaan luotiin uusi lakihanke. Uusi CER-direktiivi toteutetaan sektoreilla, jotka on määritetty kriittisten toimijoiden häiriönsietokyvystä annettavan Euroopan parlamentin ja neuvoston direktiivissä. Sen soveltamisala koskee yhtätoista sektoria muun muassa pankit ja finanssimarkkinat. (Valtioneuvosto, 2022-a)

Lokakuussa 2024 astuikin voimaan kaksi keskeistä EU-direktiiviä. Ne ovat CER ja NIS2. Resilienssidirektiivi CER korostaa liiketoiminnan jatkuvuuden suunnittelua sekä kykyä palautua häiriötilanteista mahdollisimman nopeasti. NIS2-direktiivi puolestaan painottaa tietoturvan hallintaan ja raportointivelvoitteisiin, eli direktiiviä soveltavien toimijoiden toimenpiteiden kyberturvallisuuden parantamiseksi on oltava kunnossa. (Luoma, 2024)

CER-direktiivillä (Critical Entities Resilience) parannetaan EU:n sisämarkkinoiden kriittisten palveluiden häiriönsietokykyä ja toimintavarmuutta. Direktiivi pyrkii vahvistamaan kriittisten toimijoiden ja toimintojen häiriönsietokykyä ja tehostamaan viranomaisten välistä koordinaatiota ja yhteistyötä EU:ssa, sen jäsenvaltioiden välillä sekä jäsenvaltioiden sisällä. Huoltovarmuudella, CER-direktiivillä ja siinä kuvatulla häiriönsietokyvyllä on yksi yhteinen tavoite ja se on yhteiskunnan elintärkeitä toimintoja ylläpitävien palvelujen ja infrastruktuurin mahdollisimman häiriötön toiminta. (Hakala, 2024; Huoltovarmuuskeskus, n.d.-a; Valtioneuvosto, 2024-c)

NIS2-direktiivi EU2022/2555 on Euroopan unionin kyberturvallisuusdirektiivi. Sen tavoitteena on vahvistaa sekä EU:n yhteistä, että jäsenvaltioiden kansallista kyberturvallisuuden tasoa tiettyjen kriittisten sektoreiden osalta. Pankkitoimiala on yksi erittäin kriittisistä toimialoista. Direktiivin tarkoituksena on pyrkiä kasvattamaan kyberhyökkäysten sietokykyä ja varmistaa korkea kyberturvallisuustaso Euroopan unionissa. Direktiivin myötä yhteiskunnan kriittisille sektoreille asetetaan kyberturvallisuutta vahvistavia riskienhallintavelvoitteita sekä merkittäviä poikkeamia koskevia raportointivelvoitteita. Direktiivi määrittää vähimmäistoimenpiteet kyberturvallisuusriskien hallitsemiseksi. NIS2 on Suomessa integroitu valmisteilla olevaan kyberturvallisuuslakiin. (Kyberturvallisuuskeskus, n.d.)

Digital Oparational Resilience Act DORA on Euroopan parlamentin ja neuvoston asetus 2022/2554 finanssialan digitaalisesta häiriönsietokyvystä. Se on tullut voimaan 17.1.2023 ja sovellettavaksi 17.1.2025. Sen pyrkimyksenä on parantaa finanssialan kykyä sietää tietojärjestelmien vikoja ja häiriöitä, eli hallita rahoitusmarkkinoilla ilmeneviä digitaalisia riskejä. Asetus tuo mukanaan johdonmukaisen valvontamallin ja varmistaa, että tietoturvaan ja digitaaliseen häiriönsietokykyyn liittyvät käytännöt ovat yhdenmukaiset koko EU:n alueella. Osana asetusta on vaatimus uhkaperusteisesta tietoturvatestauksesta. Asetus kattaa lähes kaikki Finanssivalvonnan valvomat toimijat. Asetus mahdollistaa valvottavien välisen vapaaehtoisen kyberuhkia koskevan tietojenvaihdon ja kyberuhista ilmoittamisen valvojalle. Kuten nykyiset ICT-häiriöilmoitukset, myös asetuksen edellyttämät häiriöilmoitukset tehdään Finanssivalvonnalle. Erona aiempaan on se, että asetuksen

myötä ilmoitetaan myös vuosittain ICT-häiriöiden aiheuttamat kustannukset. DORA-asetuksen viisi tärkeintä osa-aluetta ovat ICT-riskienhallinta, ICT-palveluihin liittyvät häiriötilanteet, digitaalisen häiriönsietokyvyn testaus, kolmansien osapuolien tarjoamiin ICT-palveluihin liittyvien riskien hallinta sekä tietojenvaihto. Asetus koskee yli 22 000 rahoitusalan toimijaa ja ICT-alan palveluntarjoajaa EU-alueella. DORA velvoittaa tekemään säännöllisiä uhkaperusteisia tietoturvatestauksia ja Suomessa DORA koskee yli 400 Finanssivalvonnan valvomaa toimijaa. Pankki- ja rahoitusalan toimijoiden lisäksi se velvoittaa alan yritysten alihankkijoita ja myös heidän tulee noudattaa sen vaatimuksia. (Finanssivalvonta, 2024-a; PWC, n.d.)

Uuden kyberturvallisuuteen liittyvän sääntelyn taustalla on Euroopan jäsenvaltioiden yhteinen tavoite nostaa tietoturvan perustasoa ja yhdenmukaistaa käytäntöjä. Uudet EU-direktiivit ja DORA parantavat kriittisen infrastruktuurin ja yritysten turvallisuutta. Ne tuovat mukanaan uusia velvoitteita sekä samalla selkeät säännöt ja toimintalinjat. Uudet säädökset kriittisten tietoinfrastruktuurien turvaamiseksi asettavat korkeampia turvallisuusstandardeja organisaatioille useilla eri aloilla ja auttavat varmistamaan sen, että alan toimijat pystyvät tunnistamaan, estämään ja torjumaan erilaisia digitaalisia uhkia entistä paremmin.

3.3 Varautumisharjoittelu

Suojaamalla tietoja ja järjestelmiä kyberhyökkäyksiltä ja tietomurroilta, voidaan estää merkittävät taloudelliset ja maineelliset vahingot. Pankkeihin kohdistuvat kyberiskut ovat hyvinkin tavallisia ja finanssialan suurin uhka. Ne ovat lisääntyneet entisestään Ukrainan sodan myötä. Ala on varautunut hyvin häiriötilanteisiin ja selviytymiskykyä harjoitellaan säännöllisesti muun muassa finanssialan toimintaharjoituksissa. EU on tehnyt toimenpiteitä parantaakseen kriittisen infrastruktuurin suojaamista, joiden avulla voidaan välttyä keskeisten palvelujen häiriöiltä tai lieventää niiden vaikutuksia. (Harjuniemi, 2022)

Euroopan keskuspankki julkaisi 2018 TIBER EU-toimintamallin kehittämään kyberturvallisuutta finanssialalla. Se on tarkoitettu sovellettavaksi kansallisesti. Toimintamallin tavoitteena on tehdä havaintoja finanssialan infrastruktuurin ja toimijoiden suojaamiseksi kohdennetuilta kyberhyökkäyksiltä. Suomen Pankki on tuonut finanssisektorin käyttöön todellisia uhkaskenaarioita ja hyökkäysmenetelmiä simuloivan eurooppalaisen TIBER-testausmallin ja julkaisi ensimmäisen vapaaehtoisen TIBER FI-soveltamisohjeen 2020. Malli on yhteensopiva muiden valtioiden TIBER-sovellutusten

kanssa mahdollistaen rajat ylittävän yhteistyön, kun toiminnot ovat hajautuneet useiden maiden alueelle. Suomen Pankki ohjeistaa, avustaa ja valvoo TIBER-FI-mallin mukaisesti ne testit, joita Finanssivalvonta edellyttää valvottaviltaan. Finanssialalla on toteutettu viimevuosina useita testausprojekteja. Uhkaperusteinen TIBER-FI hyökkäysharjoitus on osana pankin tietoturvallisuuden testaamista. Toimintamallin tavoitteena on tuottaa havaintoja finanssialan infrastruktuurin ja toimijoiden suojaamiseksi kohdennetuilta kyberhyökkäyksiltä. TIBER-FI-testaus kohdistuu erityisesti kriittisiin finanssialan toimintoihin. Se on kehikko ja toimintamalli näiden toimintojen toimintavarmuuden varmistamiseksi kohdennettujen kyberhyökkäysten varalta. (Suomen Pankki, n.d.-g)

Rahoitusalan varautumista on harjoiteltu viime vuosina useaan otteeseen. Syyskuussa 2024 järjestettyyn Pohjoismaiden ja Baltian kriisisimulaatioharjoitukseen osallistui lähes 450 henkilöä, kun Pohjoismaiden ja Baltian maiden rahoitusvakaudesta vastaavat viranomaiset testasivat valmiuttaan kuvitteellisessa kriisitilanteessa harjoittelemalla kolmeen Pohjoismaissa ja Baltiassa toimivaan pankkiin kohdistuvan simuloidun finanssikriisin hallintaa. Harjoituksessa testattiin viranomaisten välistä viestintää, tiedonjakoa ja yhteistyötä kriisinhallintatilanteessa aikapaineen ja korkean epävarmuuden alla. Harjoituksessa kuvitteelliset pankit etenivät kolmen vaiheen läpi. Vaiheet olivat normaalista liiketoiminnasta elvytykseen mukaan lukien likviditeetin palauttamistoimenpiteet, elvytyksestä kriisinratkaisuun ja kriisinhallintaviranomaisten hallinnan alaisuuteen sekä kriisinratkaisun jälkeen uudelleenjärjesteltynä paluu markkinoille. Harjoituksen opit jaetaan ja otetaan osaksi nykyisiin kriisinhallintatoimenpiteisiin. (Finanssivalvonta, 2024-b)

Jyväskylän ammattikorkeakoulun Jamk ja Huoltovarmuuskeskuksen järjestämään kyberharjoitukseen joulukuussa 2024 osallistui yli kaksikymmentä finanssialan organisaatiota. Harjoituksen avulla pilotoitiin alan yhteistä kyberharjoittelua ja harjoitusympäristöä. Harjoituksessa alan palveluihin liittyvien järjestelmien toimintaa pyrittiin estämään erilaisilla laajoilla kyberhyökkäyksillä. Harjoittelun ansiosta toimiminen aidossa kriisissä on nopeampaa, sujuvampaa ja tehokkaampaa. Myös tiedonvaihto organisaatioiden välillä paranee. (Huoltovarmuuskeskus, 2024-a)

Suomi harjoitteli rahoitusalan varautumista myös Yhdysvaltojen ja lähialueen kumppanimaiden kanssa Northern Bastion-harjoituksessa elokuussa 2023. Kyseessä on Valtiovarainministeriön järjestämä rahoitusalan varautumisharjoitus, jonka tarkoituksena on parantaa kriisinkestävyyttä Itämeren alueella. Kansainvälistä Northern Bastion-harjoitusta isännöi Euroopan hybridiuhkien torjunnan osaamiskeskus. Osallistujamaat perehtyivät

toistensa toimintatapoihin sekä prosesseihin ja kehittivät niitä. Tarkastelussa oli varautuminen siihen, että kyberhyökkäys ja fyysisen infrastruktuurin vaurio häiritsisivät yhtäaikaisesti rahoitusalan digitaalisia toimintoja. (Valtioneuvosto, 2023)

FATO on finanssialan toimintaharjoitus, joka testaa rahoitusalan ja viranomaisten yhteistyötä kriisitilanteessa. Harjoitus toteutettiin edellisen kerran vuonna 2021 ja se osoitti, että finanssialan varautuminen on hyvällä tasolla. Harjoitukseen osallistui suomalaiset pankit ja rahoitusalan viranomaiset. Siinä testattiin rahoitusalan ja viranomaisten välistä yhteistyötä kriisitilanteessa. Harjoitukseen otti osaa Huoltovarmuusorganisaation Rahoitusalan poolin jäsenet eli Valtiovarainministeriö, Suomen Pankki, Finanssivalvonta, Rahoitusvakausvirasto ja huoltovarmuuskriittiset rahoituslaitokset, eli käytännössä kaikki suomalaiset pankit. Yhteensä osallistuneita organisaatioita oli 22. Ideoita harjoiteltaviin tilanteisiin on hankittu laajasti esimerkiksi Kyberturvallisuuskeskukselta ja Euroopan hybridiuhkien torjunnan osaamiskeskukselta. Finanssitoimiala oli vahvasti mukana myös TIETO24-harjoituksessa, joka järjestettiin lokakuussa 2024. Harjoituksessa oli noin 500 osallistujaa ja siinä harjoiteltiin yhteiskunnan poikkeustilannetta varten. (Huoltovarmuuskeskus, 2022-a; Virolainen, 2024)

Kyberympäristölle on ominaista sen huima muutosnopeus ja siihen reagointi vaatii aktiivista työtä. Suomessa digitaalinen turvallisuus ja jatkuvuudenhallinta on osa suomalaista kokonaisturvallisuutta ja huoltovarmuutta. Näitä kehitetään jatkuvasti monipuolisella yritysten ja kansallisen tason varautumisella, pitämällä yllä ajantasaista tilannekuvaa ja aktiivisesti harjoittelemalla. Turvallisuuden ylläpitämiseksi tehdään laajaa yhteistyötä kansainvälisesti ja kotimaassa rahoitusalantoimijoiden, muiden sektorien sekä viranomaisten välillä. Uudistuva sääntely asettaa myös varautumisharjoitellulle aiemmasta poikkeavia uusia velvoitteita.

3.4 Varautumistoimenpiteet

Viranomaiset ja pankkisektori ovat kehittäneet pitkään varautumista erilaisiin häiriötilanteisiin, mutta Euroopan turvallisuuspoliittisen tilanteen nopea muutos on kiihdyttänyt tarvetta nyt toteutettaville ratkaisuille. Kehittyvä ja uudistuva sääntely sekä varautumisharjoitukset erilaisia uhkatilanteita vastaan ovat tärkeässä asemassa poikkeustilanteisiin varautumisessa. Varajärjestelyksi päivittäismaksamisen tukemiseksi on luotu huoltovarmuustilijärjestelmä. (Valtiovarainministeriö, n.d.-b)

Finanssialan sektori käynnisti viranomaisten kanssa yhteistyössä hankkeen vähittäismaksamisen varmistamisesta kaikissa oloissa ja lainsäädäntöä on sen myötä uudistettu. Hallitus antoi kesällä 2022 eduskunnalle esityksen laiksi eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla. Eduskunta hyväksyi lakiesityksen 7.7.2022. Esityksessä ehdotettiin perustettavaksi huoltovarmuustilijärjestelmä ja pankkien välisen maksamisen varajärjestelmä. Huoltovarmuustilijärjestelmä on tarkoitettu otettavan käyttöön tarvittaessa normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa Valtioneuvoston päätöksellä. Järjestelmä on rakennettu yhteistyössä Suomen Pankin kanssa ja suomalaisten pankkien kesken. Sen tarkoituksena on turvata yhteiskunnan toiminnan kannalta välttämätön kotimainen maksuliikenne tilanteessa, jossa yksi tai useampia pankkeja ei pysty osallistumaan normaaleihin maksunvälityksen prosesseihin. Huoltovarmuustilijärjestelmä voitaisiin ottaa käyttöön esimerkiksi silloin, jos yhteyttä T-2 järjestelmään ei ole. Se voidaan ottaa käyttöön yhdessä tai useammassa pankissa. Pankkien on huolehdittava siitä, että huoltovarmuustilillä on tarpeeksi rahaa, jotta pankki voi vastata maksuliikennevelvoitteestaan mahdollisessa poikkeustilanteessa. (Laki eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla 666/2022)

Keskeisiä rahoitusmarkkinapalveluja tarjoaville yrityksille on asetettu varautumisvelvollisuus, jolla toimijat varautuvat vakaviin häiriötilanteisiin ja poikkeusoloihin. Rahoitusvakausviraston ylläpitämä huoltovarmuustilijärjestelmä pitää sisällään huoltovarmuustilipalvelun ja korttimaksamisen huoltovarmuustilipalvelun. Huoltovarmuustilijärjestelmän avulla turvataan pankkien asiakkaille mahdollisuus tehdä eurotilisiirtoja omalta pankkitililtään, vastaanottaa maksuja tililleen sekä maksaa debit-korteilla ja nostaa käteistä. Suomen Pankki puolestaan vastaa päivittäismaksamisen varajärjestelyihin kuuluvan pankkien välisen maksuliikenteen turvaamisesta. (Rahoitusvakausvirasto, n.d.-a)

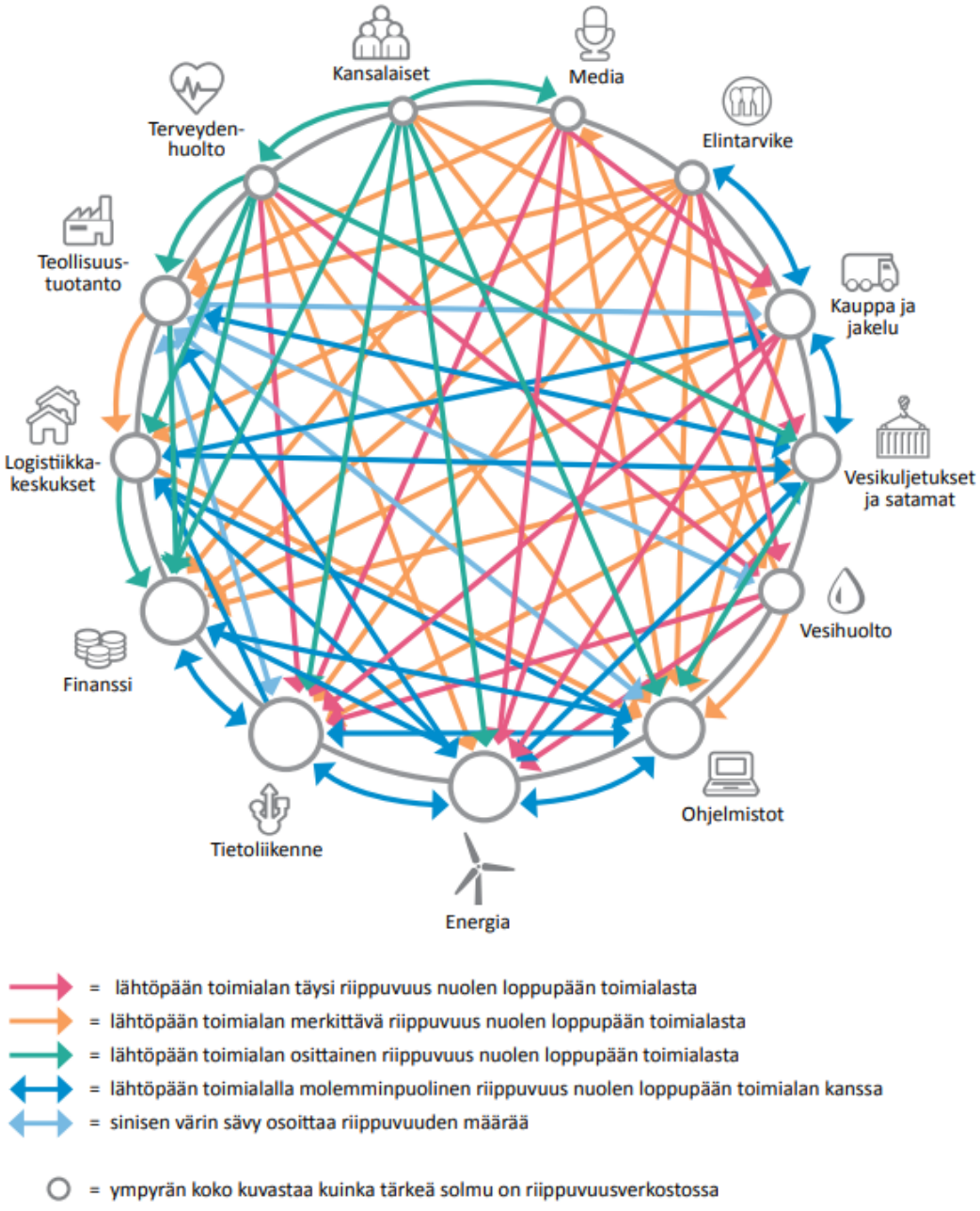
Varajärjestelyt on luotu sen varalta, jos yhteiskunnan vakavissa häiriötilanteissa tai poikkeusoloissa ei voida käyttää normaaleja maksamisen järjestelmiä. Käytännössä tämä tarkoittaa sitä, että jos jonkin pankin järjestelmät tai tietoliikenneyhteydet ovat kyberhyökkäyksen vuoksi pitemmän aikaa poikki ja pankki on toimintakyvytön, saadaan maksuliikenne sujumaan varajärjestelyjen avulla. On ensiarvoisen tärkeää varmistaa maksuliikenteen ja korttimaksamisen toimivuus myös silloin, jos tietoliikenneyhteydet muihin maihin ovat poikki. Kriisinsietokyky ja riskienhallinta ovat tärkeässä roolissa, kun puhutaan häiriönsietokyvystä ja sen varmistamisesta. Kansalliseen varautumiseen liittyen finanssisektorilla tarvitaan kattavat varajärjestelyt, jotka voidaan ylläpitää ja ottaa käyttöön kotimaisin voimin. Niiden on katettava koko maksamisen ketju. Päivittäisessä käytössä

olevat tutut vaihtoehtoiset maksujärjestelmät ovat varautumisen kannalta parempi ratkaisu kuin unohduksissa ja pölyttymässä säilytettävät varajärjestelmät. Monimutkaiset arvoketjut vaikeuttavat osaltaan varajärjestelyjen luomista. (Finanssivalvonta, 2020-b; Rehn, 2021)

Merikaapeleihin kohdistuneet häiriöt ovat herättäneet huolta myös tietoliikenneyhteyksien toimivuudesta. Suomalaisten teleyritysten kansainväliset yhteydet perustuvatkin useiden merikaapeleiden kautta kulkeviin yhteyksiin. Nämä merenpohjassa kulkevat yhteydet ovat erittäin tärkeä osa Suomen viestintäverkkojen infrastruktuuria. Kansainvälisiä tietoliikenneyhteyksiä suojataan monin tavoin. Tärkeät yhteydet ovat rakennettu niin, että ne eivät ole yhden kaapelin varassa ja yksittäinen vikatilanne ei pysäytä koko Suomen tietoliikennettä. Tarvitaan häiriö useassa kaapelissa samanaikaisesti, että tietoliikenneyhteydet saadaan kokonaan poikki. Yksittäiset häiriöt merikaapeleissa voivat aiheuttaa lähinnä hetkellisiä katkoksia tai hitautta yhteyksiin dataliikenteessä. Kriittiset yhteydet on varmistettu usean eri järjestelyn kautta ja Suomessa on varauduttu merenalaisen infrastruktuurin vaurioitumiseen erilaisin huoltovarmuustoimin. Valtioneuvosto on asettanut tavoitteet digitaalisen yhteiskunnan huoltovarmuudelle. Tärkein tavoite on varmistaa digitaalisen yhteiskunnan kriittisten toimijoiden välttämättömien verkkojen palveluiden toimivuus, häiriönsietokyky ja palautumiskyky. Yksi painopiste on kansainvälisten tietoliikenneyhteyksien varmentaminen osana huoltovarmuustoimintaa. (Huoltovarmuuskeskus, 2023-a; Huoltovarmuuskeskus, 2022-b)

Finanssialan yritykset ovat erittäin merkittävä tekijä eri alojen muodostamassa verkostossa, jotka ovat riippuvaisia toisistaan.

Kuva 2 Toimialariippuvuudet (Huoltovarmuuskeskus, 2020, s. 16)



Kuvasta 2 nähdään, kuinka yhteiskunnan elintärkeiden toimintojen turvaaminen ja huoltovarmuus muodostuvat riippuvuussuhteista rakentuvien ketjujen kautta. Eri sektorien välillä on vahva kytkös ja yhden kriittisen sektorin häiriö heijastuu nopeasti muihin. Huoltovarmuuskeskuksen tekemässä selvityksessä finanssiala on kolmen kriittisimmän alan joukossa, kun tarkastellaan sitä, miten tärkeässä asemassa kyseinen ala on tässä eri alojen muodostamassa toimialojen keskinäisessä riippuvuusverkostossa. Varsinaiset uhat toteutuvat lopulta yksittäisten toimijoiden ja niiden käyttämien yksilöllisten järjestelmien

välityksellä. Kun mietitään riskienhallintaa, verkoston häiriöihin voi varautua esimerkiksi kahdella tyypillisellä tavalla. Parantamalla toimialan kyberturvallisuutta häiriösietoisemmaksi vaihtoehtoisten yhteyksien ja varajärjestelmien avulla. Tai ottamalla käyttöön vaihtoehtoisia toimintatapoja mahdollisen häiriön aiheuttamien vaikutusten ajaksi. (Huoltovarmuuskeskus, 2020, s. 15–17)

Finanssiala on saanut parhaat pisteet Huoltovarmuuskeskuksen kyberturvallisuusselvityksessä. Vuonna 2024 tehty kyberuhkien sietokyvyn stressitestissä nousi esiin myös ne osa-alueet, joissa pankeilla on vielä parantamisen varaa ja valvojat seuraavat edelleen niitä puutteita, jotka koskevat pankkien kykyä palautua niihin kohdistuneesta kyberhyökkäyksestä. Valtioneuvosto on hyväksynyt uudistetun kyberturvallisuusstrategian vuosille 2024–35. Se vastaa toimintaympäristön muutokseen ja vie kyberturvallisuuden paremmin osaksi kokonaisturvallisuuden mallia. Muuttuneen toimintaympäristön takia uutena kokonaisuutena mukana strategiassa ovat reagointi ja vastatoimet. Kyberturvallisuusstrategian uudistamisessa on otettu huomioon muun muassa kyberturvallisuusdirektiivin NIS2 vaatimukset. (Euroopan Keskuspankki, 2024-b; Valtioneuvosto, 2024-a)

Vuonna 2025 Finanssivalvonnan painopisteet liittyvät edellisten vuosien tapaan epävakaan toimintaympäristön operatiivisiin ja taloudellisiin riskeihin. Tämän vuoden painopisteet ovat valvottavien hallinnon luotettavuus ja toimintaympäristön epävarmuuksiin vastaaminen. Geopoliittinen tilanne, toimintaympäristön muutokset ja entisestään lisääntyvä sääntely korostavat valvottavien riskienhallinnan valvontaan. Vuoden 2025 painotettavien hallittavien riskien joukossa ovat mukana muun muassa operatiivinen ja taloudellisen varautuminen sekä IT- ja kyberriskit. (Finanssivalvonta, 2025)

Varautuminen riskeihin edellyttää IT-alan osaamista, rahoitusalan osaamista sekä koko toimialan ja viranomaisten välistä yhteistyötä. Maksuliikenteen kansallinen varautuminen tiivistyy kansakunnan kokonaisturvallisuuteen. Finanssialan toimijat investoivat huomattavasti tietojärjestelmien ja palveluiden kyberturvallisuuden suunnitteluun, toteuttamiseen ja seurantaan. Keskuspankin asettamat järjestelmien kehityksen tavoitteet keskittyvät järjestelmien luotettavaan toimintaan ja tehokkuuteen. Myös järjestelmien huoltovarmuus ja resilienssin vahvistaminen ja niihin liittyvät eri vaihtoehdot ovat nousseet kolmanneksi pääteemaksi. Kyberuhat ovat rahoitussektorinkin riskiarvioiden keskiössä. (Suomen Pankki, n.d.-g)

Valtioneuvosto on hyväksynyt 16.1.2025 päivitetyn Yhteiskunnan turvallisuusstrategian. Venäjän hyökkäyssota Ukrainassa ja laaja-alainen vaikuttaminen korostavat jokaisen hallinnonalan vastuuta varautua valtiolliseen vihamieliseen vaikuttamiseen. Uusi strategia painottaa juuri kriisinkestävyyden vahvistamista, yhteiskunnan kysyä vastata häiriötilanteisiin sekä myös yksilöiden roolia turvallisuuden lisäämiseksi. Muuttuneen turvallisuusympäristön takia pankkisektorille on luotu ratkaisuja huoltovarmuuden ja maksuliikenteen toimivuuden varmistamiseksi erittäin vakavien häiriötilanteiden ja poikkeusolojen varalle. (Rahoitusvakausvirasto, 2025-a)

Rahoitusvakausvirasto tekee kriisinratkaisusuunnittelutyötä sen suorassa toimivallassa olevien pankkien kanssa. Sen avulla varaudutaan mahdollisiin eteen tuleviin kriisitilanteisiin ja niiden hoitoon. Ensiarvoisen tärkeää on pankkien kriisinratkaisuvalmiuksien edistäminen niin, että toiminta voidaan kriisitilanteessa vakauttaa ja organisoida hallitusti. Vuonna 2025 rahoitusvakausvirasto painottaa kriisinratkaisuvalmiuksien testausta. (Rahoitusvakausvirasto, 2025-b)

Pankit kohtaavat uusia haasteita kriittisten järjestelmien turvaamisessa ja uusien sääntelyvaatimusten täyttämisessä. Hyökkäykset ovat entistä rohkeampia ja niissä hyödynnetään kriittisen infrastruktuurin haavoittuvuuksia. Uhat muuttuvat ja valtiollisilla toimijoilla ja niihin sidoksissa olevilla rikollisryhmillä on käytössään laajoja resursseja, viimeisintä tekniikkaa ja entistä enemmän tekoälyyn ja oppiviin järjestelmiin perustuvaa suorituskykyä. On luotava pesunkestävät riskienhallintakäytännöt, joiden avulla varmistetaan, että rahoitusalan toimijat voivat kestää vakavatkin häiriöt sekä toipua niistä. Riskienhallinnan näkökulmasta on ensiarvoisen tärkeää tunnistaa etukäteen, mistä palveluista toiminta on riippuvaista. (Samlink, 2024)

Juuri kyky sopeutua häiriöihin ja turvata toiminnan jatkuvuus häiriöistä huolimatta määrittää kriittisen tuotannon ja palveluiden kriisinsietokyvyn. Huoltovarmuus rakentuu pitkälti kriittisillä sektoreilla toimivien yritysten kyvystä reagoida poikkeusoloihin, sietää kriisi- ja häiriötilanteita sekä palautua niistä nopeasti. (Valtioneuvosto, 2022-b, s. 7)

4 Tutkimusmenetelmät

Tämän opinnäytetyön tutkimus on laadullinen eli kvalitatiivinen tutkimus, jossa aiheistonkeruumenetelmänä on hyödynnetty puolistrukturoitua teemahaastattelua. Opinnäytetyön tavoitteena on löytää vastaukset seuraaviin kysymyksiin:

- Onko pankin maksuliikenne turvattu poikkeustilanteessa?
- Millaisin keinoin pankki varmistaa maksuliikenteen toimivuuden poikkeustilanteessa?

4.1 Laadullinen eli kvalitatiivinen tutkimus

Tämä tutkimuspainotteinen opinnäytetyö toteutettiin laadullisena tutkimuksena. Laadullisen tutkimuksen alle mahtuu erilaisia laadullisia tutkimuksia ja niillä on useita ominaispiirteitä. Laadullinen eli kvalitatiivinen tutkimus on yksi tieteellisen tutkimuksen menetelmäsuuntauksista. Siinä pyritään ymmärtämään kokonaisvaltaisesti kohteen laatua, ominaisuuksia ja merkityksiä. Yleisimmät käytetyt aineistonkeruumenetelmät ovat haastattelu, kysely, havainnointi ja erilaisiin dokumentteihin pohjautuva tieto. Menetelmistä voi valita sopivimman tai käyttää useampaa. (Tuomi & Sarajärvi, 2018 s. 83)

Laadullisen tutkimuksen tarkoituksena on ymmärtää tutkittavaa kohdetta, jota tutkimuksessa analysoidaan. Siinä pyritään syventymään myös ilmiöiden taustoihin ja ymmärtämään niitä. Tutkittava kohde rajataan ja lähdetään pureutumaan tutkimusongelmaan. Laadullisessa tutkimuksessa pyritään yleensä ymmärtämään tarkasteltavaa ilmiötä tutkimuksen kohteena olevien henkilöiden näkökulmasta ja saamaan selville tutkimuksen kohteena olevien henkilöiden kokemuksia. Tavoitteena on saada mahdollisimman yksityiskohtaista tietoa tutkimuksen kohteena olevasta ilmiöstä tutkimukseen osallistujien kokemuksien avulla, niitä kuvailemalla ja tulkitsemalla. Tutkimuksen osallistujat valitaan tarkoin parhaan tutkimustuloksen saamiseksi. Tutkimukseen pyritään valitsemaan osallistujiksi henkilöitä, joilla on asiantuntemusta sekä kokemusta tutkimuksen kohteena olevasta ilmiöstä ja jotka voivat tuottaa parhaiten tietoa tästä ilmiöstä. Kyseessä on tarkoituksenmukaisuusotanta. Kun halutaan tietää mitä ihminen ajattelee tai miksi hän toimii, kuten toimii, on parasta kysyä asiaa häneltä. Menetelmänä voi käyttää kyselyä tai haastattelua. Haastattelu onkin hyvä keino saada syvällistä tietoa haastateltavan ajatuksista, kokemuksista ja toiminnasta. (Tuomi & Sarajärvi, 2018, ss. 83–84)

Laadullisessa tutkimuksessa aineiston kokonaislaatu on ratkaiseva tekijä ja tavoitteena on aineiston sisällöllinen laajuus. Kun mietitään tutkimukseen osallistuvien määrää ja aineiston kokoa, voidaan todeta, että usein laadullisissa tutkimuksissa aineiston koko on pieni. Tutkimusresurssit ovat rajalliset ja pienemmän joukon haastattelu ja siitä kerääntyvän aineiston analysointi helpompaa ja vie vähemmän aikaa verrattuna suurempaan haastateltavien määrään. (Tuomi & Sarajärvi, 2018, s. 97–98)

Tutkimuksen luotettavuus on raportoinnin kannalta olennainen seikka. Tutkimuksessa pyritään välttämään virheiden syntymistä ja luotettavuutta onkin tärkeä arvioida huolellisesti eri näkökulmista. Tutkimuksen eettisyys, uskottavuus ja luotettavuus perustuu hyvän tieteellisen käytännön noudattamiselle. Eettisyys koskee myös tutkimuksen laatua ja hyvää tutkimusta ohjaa eettinen sitoutuneisuus. Tutkimuksen riippumattomuudella eli reliabiliteetilla tarkoitetaan toistettavuutta. Sen voi ajatella tarkoittavan sitä, että jos samaa asiaa tutkitaan kahdella eri tutkimuskerralla, saadaan sama tulos. Myös sitä, että kaksi eri tutkijaa päätyvät samaan tulokseen eli yksimielisyyteen, Sekä sitä, että kahdella eri tutkimusmenetelmällä päästään samaan lopputulokseen. Reliaabelius koskee tutkijan toimintaa sekä analyysin luotettavuutta. Tutkimuksen validius tarkoittaa sitä, että on tutkittu sitä mitä on luvattu ja tutkijan on pystyttävä dokumentoimaan ja perustelemaan tekemisensä. Luotettavuuden arviointi tapahtuu koko prosessin ajan aina suunnittelusta tutkimustulosten todennettavuuteen. Tutkimuksen luotettavuuteen liittyen puhutaan lisäksi objektiivisuudesta ja totuudenmukaisuudesta. Objektiivisuudella tarkoitetaan havaintojen luotettavuutta ja puolueettomuutta. Totuudenmukaisuudella taas sitä, että tulokset ovat paikkansapitäviä. (Hirsjärvi & Hurme, 2022, luku 8.2.1; Tuomi & Sarajärvi, 2002, s.131–138; Tuomi & Sarajärvi, 2018, s.149)

Tämän opinnäytetyö toteutetaan laadullisena tutkimuksena ja menetelmäksi valikoitui teemahaastattelu, sillä se palvelee parhaiten tämän tutkimuksen tarpeita ja auttaa saavuttamaan vastaukset tutkimuskysymyksiin. Laadullisen lähestymistavan avulla voidaan selvittää pankin ja siellä työskentelevien asiantuntijoiden näkemys ja kokemus siitä, onko pankin maksuliikenne turvattu mahdollisessa häiriö- tai poikkeustilanteessa. Laadullinen tutkimus mahdollistaa tarkastelun yksilöiden näkemysten, kokemusten sekä tulkintojen kautta. Sen avulla saadaan selvitettyä asiantuntijoiden henkilökohtaisia ajatuksia ja päästään sitä kautta pintaa syvemmälle.

4.2 Teemahaastattelu

Haastattelun avulla voidaan kerätä syvällistä ja yksityiskohtaista tietoa tutkittavasta ilmiöstä. Haastatteluja voidaan toteuttaa eri menetelmillä ja niistä valitaan kuhunkin tutkimukseen sopivin vaihtoehto. Tämän tutkimuksen menetelmäksi valikoitui puolistrukturoitu teemahaastattelu, mikä on yksi laadullisen tutkimuksen aineistonkeruumenetelmistä. Se toteutettiin puolistrukturoitujen kysymysten avulla keskustelunomaisesti ja vapaamuotoisesti. Teemahaastattelu on tiettyihin aiheisiin ja kysymyksiin keskittyvä henkilökohtainen haastattelu. Se on menetelmänä vapaamuotoisempi, kuin strukturoitu haastattelu ja antaa haastateltaville mahdollisuuden tuoda esiin omia ajatuksiaan. Kuitenkin niin, että haastattelija luo kysymyksenasettelun avulla rajauksen haastattelun sisällölle, mutta mahdollistaa lisäksi keskustelun käymisen. Haastattelu voidaan ajatella keskusteluksi, jolla on etukäteen asetettu tavoite ja se etenee etukäteen asetettujen teemojen ympärillä. (Sarajärvi & Tuomi, 2002, s. 73–79)

Menetelmän etuna on joustavuus. Haastattelija voi esimerkiksi pyytää tarkennusta haluamastaan asiasta ja tehdä havaintoja haastateltavan tunteista, eleistä ja ilmeistä. Näiden avulla on mahdollista saada arvokasta lisätietoa tutkittavasta asiasta, vältetään vääriä tulkintoja ja voidaan hyödyntää oheisviestintää. Kun haastateltavilla on mahdollisuus kuvailla omia kokemuksiaan ja näkemyksiään, saadaan arvokasta lisätietoja, mikä voisi toista tutkimusmenetelmää käyttämällä jäädä saamatta. Menetelmässä annetaan tilaa asiantuntijoiden omalle puheelle ja keskeistä on vuorovaikutus ja turvallinen haastattelutilanne. Ymmärrys haastateltavan ja haastattelijan välillä perustuu keskusteluun ja vuoropuheluun. Tutkija voi tarvittaessa tarkentaa kysymyksiä ja syventyä haastateltavan vastauksiin. Haastattelussa on myös mahdollisuus keskustella sen aikana esiin nousseista ajatuksista aiheeseen liittyen, joita haastattelija ei ole ennalta suunnitellut. Haastattelu etenee valittujen teemojen mukaisesti etukäteen suunniteltujen kysymysten pohjalta. Tarvittaessa osa kysymyksistä voidaan jättää kysymättä tai kysymysten esitysjärjestystä voi haastattelutilanteessa muuttaa. (Sarajärvi & Tuomi, 2002, s. 73–79)

Tämän tutkimuksen teemahaastatteluissa tärkeintä oli saada mahdollisimman paljon tietoa siitä, onko pankin maksuliikenne turvattu poikkeustilanteessa ja millaisin keinoin pankki varmistaa maksuliikenteen turvallisuuden poikkeustilanteessa. Teemahaastattelu menetelmänä sopii tähän tutkimukseen, sillä haastateltavat on valikoitu tarkoin ja haastattelu toteutettiin tietoperustan perusteella valittujen keskeisten teemojen ympärillä, joista haastattelijalla on vahva ymmärrys. Haastatteluiden kohteina olivat tarkoin valitut pankin asiantuntijat, joilla on syvä osaaminen ja asiantuntijuus tutkimuksessa käsiteltävistä

teemoista. Valikoidut haastateltavat työskentelevät asiantuntijoina aiheen parissa, mutta tarkastelevat asiaa hieman eri kulmasta. Näin pyrittiin varmistamaan mahdollisimman laaja-alainen näkemys, joka huomioi eri näkökulmat. Tutkimukseen osallistujien joukko on varsin rajattu. Siten varmistetaan mahdollisimman luotettavat ja kattavat tutkimuksen tulokset. Kyseessä on näin ollen tarkoituksenmukainen ja harkinnanvarainen näyte. Haastateltavilla oli vapaus valita, osallistuvatko he tutkimukseen ja halutessaan mahdollisuus kieltäytyä siitä. (Sarajärvi & Tuomi, 2002, s. 73–79)

Teemahaastattelun kysymykset perustuvat työn tietoperustaan ja haastattelukysymykset rakentuvat tietoperustassa esiin nousseiden keskeisten teemojen ympärille. Haastattelukysymykset suunniteltiin huolellisesti ottaen huomioon aiheen arkaluonteisuus. Kysymyksenasettelua tarkennettiin ja kysymyksiä muokattiin vielä saadun palautteen perusteella ja aihetta koskeva salassapitovelvollisuus huomioiden. Haastattelun suunnittelussa oli tärkeää, että valittujen teemojen ja kysymysten avulla saadaan vastattua mahdollisimman kattavasti opinnäytetyön tutkimuskysymyksiin. Kysymykset pyrittiin muotoilemaan mahdollisimman selkeiksi ja ymmärrettäviksi.

Haastateltaville lähetettiin kysymykset etukäteen tiedoksi, jotta he saivat tutustua niihin ja sen myötä annettiin aikaa selvittää mahdollisia vastauksia ennen haastattelua. Haastateltavien kanssa sovittiin ajankohdat haastatteluiden toteuttamiselle ja ennen haastatteluiden aloittamista tutkimukseen osallistuvia muistutettiin vielä tutkimuksen anonymiteetista. Heitä muistutettiin myös siitä, että kaikkiin kysymyksiin ei tarvitse vastata ja informoitiin, että haastattelut nauhoitetaan. Haastattelut toteutettiin Teamsin välityksellä ja ne tallennettiin.

Haastattelussa on kolme teemaa. Ne ovat turvallisuusympäristö, sidosryhmät sekä varautumistoimet ja sääntely. Haastattelun kysymykset rakentuivat näiden teemojen ympärille ja haastattelun runko eteni niiden mukaisesti. Teemahaastattelun kysymykset löytyvät liitteestä 1.

Varsinaisten kysymysten lisäksi haastatteluissa keskusteltiin muistakin esiin nousseista asioista tutkimuksen aiheeseen liittyen ja esitettiin tarkentavia kysymyksiä. Aineistoa on suhteellisen helppo analysoida teemoittain ja myös sen vuoksi tutkimusmenetelmäksi valikoitui teemahaastattelu. Se antoi lisäksi mahdollisuuden selvittää asiantuntijoiden omia kokemuksia, tunteita ja ajatuksia. Menetelmän etu on myös se, että se mahdollistaa joustavuuden. Haastattelutilanteessa voi syventyä haastateltavan esiin nostamiin näkökulmiin ja asioihin, joihin haastattelija ei ole osannut varautua valmiilla kysymyksillä.

Haastatteluiden alussa käytiin vielä läpi, mistä tutkimuksessa on kysymys sekä avattiin työn taustoja, kerrattiin tutkimuskysymykset, joihin työssä pyritään löytämään vastaus ja käytiin läpi haastattelun teemat. Sen jälkeen aloitettiin varsinaiset haastattelut ja ne etenivät ennalta laaditun rungon pohjalta. Haastateltavat saivat kertoa vapaasti omia näkemyksiään sekä kokemuksiaan ja nostaa esiin haluamiaan tärkeiksi kokemiaan asioita. Haastattelut olivat vuorovaikutuksellisia ja keskustelunomaisia.

4.3 Aineiston analysointi

Aineiston analysoinnilla tarkoitetaan sen tiivistämistä ja työstämistä teoreettiseen muotoon. Analysoinnin avulla päästään kiinni varsinaisiin tutkimuksen tuloksiin ja sen myötä niistä voidaan tehdä tulkintoja. Tulkinnalla tarkoitetaan aineistoa analysoidessa esiin nousevien merkitysten selkeyttämistä sekä pohdintaa. Analyysin tarkoitus on tuottaa kerätylle tiedolle lisää informaatioarvoa ja analyysin avulla tutkimusaineisto pyritään tiivistämään. Kuitenkin säilyttäen sen sisältämä olennainen tieto. Avainasemassa on systemaattisuus, avoimuus, tarkistettavuus ja perusteltavuus. Yksi vaihtoehto analysoida tutkimuksen tuloksia on tehdä se teemoittelemalla. Teemoittelusta puhutaan silloin, kun aineistosta poimitaan tutkimuksen kannalta tärkeimmät aiheet ja ne esitetään omina asiakokonaisuuksinaan. Yleensä teemahaastattelun avulla kerätty aineisto on runsas. Se tekee usein analyysivaiheesta mielenkiintoisen mutta haastavan. Tämän tutkimuksen tulokset analysoidaan haastattelun teemojen mukaisesti teemoittelemalla. Haastattelun runko ja teemat valittiin tutkimuksessa käytettävä analysointimenetelmä huomioiden, jotta tulosten purkaminen sujuisi mahdollisimman vaivattomasti ja selkeästi. (Puusa, 2020, luku 7 & 9)

Tutkimusaineiston analyysi piti sisällään monta vaihetta. Ensin tallennetut Teams-haastattelut litteroitiin eli ne purettiin kirjoittamalla auki pian haastatteluiden jälkeen. Tällä tavalla päästiin pureutumaan paremmin kerättyyn tietoon ja muodostamaan siitä kokonaiskuva. Haastattelut olivat vielä tuoreessa muistissa. Jo haastatteluiden aikana päästiin aloittamaan analysointi tekemällä havaintoja esimerkiksi siitä, millaisella tavalla haastateltavat kertoivat näkemyksiään. Kun tutkimuksen aineisto oli litteroitu eli muutettu tutkittavaan muotoon puhtaaksi kirjoitetutuksi tekstiksi, alkoi aineiston varsinainen analysointi. Puhtaaksikirjoitettu teksti luettiin läpi useaan kertaan huolellisesti ja sen myötä siitä onnistuttiin löytämään tutkimuksen kannalta olennaiset asiat. Kun aineistoa oli karsittu ja tutkimuksen kannalta tärkeimmät tulokset olivat selvillä, päästiin tekemään tulkintoja ja päätelmiä peilaten tutkimusongelmaan ja työn tietoperustaan. Lopulliset tutkimuksen tulokset analysoitiin, jaoteltiin ja raportoitiin haastattelun teemojen mukaisesti. Vaikka

teemahaastattelun teemat eivät ole automaattisesti sama asia, kuin teemoittelun teemat, jako haastattelua mukaileviin teemoihin tuntui parhaalta ja selkeimmältä ratkaisulta. Haastattelun runko ja kysymykset laadittiin siten, että niiden avulla saataisiin vastaukset tutkimuskysymyksiin ja ongelmaan. Tulosten esittäminen saman jaottelun mukaisesti auttoi järjestämään aineiston selkeään ja tiiviiseen muotoon. (Puusa, 2020, luku 7 & 9)

Teemahaastattelun tutkimustuloksia kerättäessä ja analysoitaessa huomioitiin luottamuksellisuus ja anonymiteetti. Se säilytettiin läpi prosessin. Tutkimusmateriaalia käsiteltiin aineistonhallintasuunnitelman mukaisesti, joka on liitteessä 2. Lopputuloksena syntyi selkeä ja johdonmukainen raportti.

5 Teemahaastattelun tulokset

Tämän tutkimuksen teemahaastattelut toteutettiin maaliskuussa 2025 ja kukin haastattelu kesti noin tunnin. Haastattelut etenivät sujuvasti ja ennalta laadittua suunnitelmaa mukaillen. Tutkimustulokset käydään läpi teemahaastattelun teemojen mukaisesti.

5.1 Turvallisuusympäristö

Haastatteluiden avulla pyrittiin selvittämään, millainen on pankin tämänhetkinen maksuliikenteen turvallisuusympäristö ja onko siinä tapahtunut muutosta verrattuna aiempaan. Vastauksista ilmeni pankin maksuliikenteen vakauden olevan hyvä eikä suuria pitkäkestoisia häiriöitä ole ollut. Pankkien palvelut ovat toimineet pääsääntöisesti hyvin ja olleet suurimman osan ajasta käytettävissä. Vastaajat totesivat ilmassa olevan epävakautta ja toimintaympäristön muuttuneen varsinkin geopoliittisen tilanteen myötä. Erilaiset vaikuttamisyritykset ovat lisääntyneet esimerkiksi Venäjän hyökkäyssodan jälkeen ja toimintaympäristö on muuttunut haastavammaksi. Haastatteluissa nousi esiin, että yksittäisiin toimijoihin kohdistuu valitettavasti enenevissä määrin erinäköisiä pahantahtoisia toimenpiteitä, enimmäkseen palvelunestohyökkäyksiä. Pankkeihin kohdistuvat kyberuhat ovat uudenlaisia verrattuna aiempaan. Uhat voivat kohdistua yksittäiseen rahoitusalan toimijaan tai maksuliikenteen infraan. Myös erilaiset valtiolliset toimijat saattavat aiheuttaa uhkaa. Asiantuntijat kokivat, että vaikka ilmassa on epävakautta, siihen on pystytty pankkina vastaamaan. Geopolitiikasta aiheutuviin riskeihin sekä ympäristönmuutokseen on pyritty varautumaan monin tavoin.

Keskustelimme fyysiseen infraan kohdistuvista uhista ja niihin varautumisesta. Sekä siitä, millaisia muutoksia turvallisuusympäristössä on tapahtunut. Haastatteluun osallistunut asiantuntija pohti, että se mitä maailmassa tapahtuu, on iso muutos. Muuttuneen maailmantilanteen lisäksi toimintaympäristöä on muuttanut maksuliikenteen nopeutuminen ja sen seurauksena pankkien on kyettävä reagoimaan nopeammin. Kehitystyötä on jouduttu vauhdittamaan ja se aiheuttaa omat riskinsä. Pankkien IT-järjestelmät eivät ole välttämättä niin stabiileja, kuin ne ovat olleet aiemmin ja niitä on kehitetty kireällä aikataululla. Kun mietitään vuosia taaksepäin, toimintaympäristöä on muuttanut osaltaan maksuliikenteen kansainvälistyminen. Maan sisäistä maksuliikennettä ei enää ole vaan Euroopassa maksuliikenne on SEPA-maksuliikennettä.

Haastateltavat nostivat esiin, että maksuliikenteessä mukana olevat rahoituslaitokset ovat vahvasti linkittyneitä toisiinsa. Mukana on useita maksupalvelutoimijoita ja maksujenvälitystä tarjoavia palveluntarjoajia. Nopeutumisen myötä yksittäisen toimijan haasteet ja häiriöt saattavat heijastua esimerkiksi palkkojen ja etuuksien maksamisen viivästyksinä muihin toimijoihin. Yksittäiseen toimijaan kohdistuva isompi häiriö voi vaikuttaa sen kykyyn täyttää siihen kohdistuvat velvoitteet. Varsinaiset häiriön vaikutukset riippuvat tilanteesta, mutta sillä voi olla vaikutuksia maksujenvälitysketjussa tai vähintään kyseinen toimija joutuu kohdistamaan resursseja häiriötilanteen hoitamiseksi.

Kävi ilmi, että merkittävä ja suhteellisen tuore muutos on lisäksi yksittäisten asiakkaiden huijaaminen. Myös operatiivinen riski on aina läsnä, sillä työtä tekevät ihmiset. Yksittäisiä henkilöitä tai pankin työntekijöitä voidaan painostaa tekemään tietynlaisia asioita. Sellainen ei ole ollut esillä mietittäessä vuosia taaksepäin, mutta on nykypäivänä todellinen riski. Haastateltava kuvasi maksamisen muutoksia näin:

> *”Maailma on jatkuvasti muuttuva ja siihen on pystyttävä reagoimaan monella eri tasolla. Tiedostaen samalla miksi pankkina olemme olemassa ja mitä olemme tekemässä. Mitä me pankkina mahdollistetaan yhteiskunnassa ja mikä meidän merkityksemme on yhteiskunnalle. Ja toisaalta myös yksittäiselle ihmiselle. On jatkuvasti pystyttävä reagoimaan muutoksiin ja olemaan askeleen edellä, että kaikki toimii kuten pitää.”*

Haastatteluun osallistunut asiantuntija korosti pankkitoiminnan olevan luottamustoimintaa. Alan toimijat ottavat turvallisuuden vakavasti kaikissa tilanteissa. Kaikki toimijat tekevät jatkuvaa työtä sen eteen, että pankki voi tarjota tehokkaat, toimivat ja turvalliset

maksupalvelut kaikille asiakkailleen. Hän totesi näin olevan pankissa, jossa työskentelee, mutta uskoo samoin olevan kaikissa pankeissa.

5.2 Sidosryhmät

Toinen esiin noussut teema oli sidosryhmät. Haastatteluiden avulla pyrittiin selvittämään millaisia sisäisiä ja ulkoisia sidosryhmiä pankilla on maksuliikenteen turvallisuuden varmistamiseen liittyen ja millaista yhteistyötä sen eteen tehdään. Selvisi, että turvallisuuden sekä palveluiden häiriöttömyyden ja jatkuvuuden eteen tehdään jatkuvaa työtä monin eri tavoin. Se on keskiössä kaikilla toimijoilla. Haastateltava kertoi, että maksuliikenteen turvaamiseksi tehdään laajaa yhteistyötä lähes koko pankin voimin. Ensiarvoisen tärkeää on varmistaa, että järjestelmät toimivat. Ilman niitä pankki on isoissa ongelmissa. Myös yhteistyö viranomaisiin on tiivistä. Heiltä tulee paljon vaateita ja niitä pyritään ratkaisemaan yhdessä. Raportointi viranomaisille sekä maksuliikenteeseen liittyvien riskienhallinta on keskiössä. Maksuliikenteen mahdollistavan likviditeetinhallinnan ja sen riittävyyden näkökulmasta maksamisen turvallisuus on isossa roolissa. Jos häiriön sattuessa likviditeettiä ei saada oikeaan paikkaan oikeaan aikaan, sellaisessa tilanteessa on ensiarvoisen tärkeää yrittää allokoida kokoon saatavat varat sinne, missä niitä sillä hetkellä eniten tarvitaan.

Tärkeimmiksi ulkopuolisiksi sidosryhmiksi asiantuntijat mainitsivat muut pankit, Euroopan keskuspankin sekä Suomen Pankin, joka toimii usein vastapuolena ja yhteistyökumppanina. Näiden lisäksi on useita muita keskusvastapuolia. Esimerkiksi EBA Clearing. Myös Swiftin järjestelmiä käytetään monessa eri maksuliikenteen prosessin osassa ja heidän järjestelmien turvallisuudella on iso merkitys. Esiin nousi myös eri valvojat sekä viranomaiset. Haastateltavat mainitsevat Finanssivalvonnan, Rahoitusvakausviraston sekä Huoltovarmuuskeskuksen olevan isossa roolissa. Kävi ilmi, että Finanssiala on järjestönä sellainen, jossa tehdään tiivistä yhteistyötä pankkien välillä ja pyritään siihen, että kaikki toimii. Merkittävänä yhteistyötaho on lisäksi Kyberturvallisuuskeskus. Kybertuvallisuuskeskus on eri organisaatioiden käytettävissä varsinkin sellaisessa tilanteessa, jos kriittiseen infraan liittyvällä toimijalla on jokin tilanne päällä. He tarjoavat silloin resursseja ja ohjeistusta. Haastateltava kuvasi sidosryhmiä näin:

> *”Jokaisella pankin ulkopuolisella sidosryhmällä on oma kulmansa, jolla asioita lähestytään. Oli kyseessä sitten esimerkiksi viranomaistaho tai valvoja. Jonkun pyrkimys on auttaa, toinen vaatii asioita, kolmas sivistää ja neljäs*

haluaa tehdä yhteistyötä. Kun miettii tarkkaan, taustalla kaikilla on kuitenkin sama päämäärä, jolla pyritään siihen, että kaikki sujuu hyvin ja että kriittinen infrastruktuuri ja kaikki siihen liittyvä toimisi kuten pitää."

Keskustelimme siitä, millaista yhteistyötä konkretian tasolla tehdään. Haastatteluissa selvisi, että käytännön yhteistyö pankin sisällä on sitä, että toimintojen välillä käydään läpi asioita jokaisen näkökulmasta. Eri toiminnoilla on oma roolinsa ja kukin antaa oman asiantuntijuutensa oli kyseessä sitten kehitystyö tai pyrkimys vastata viranomaisen vaateeseen. Pankin sisällä tehdään töitä yhdessä yhteisen päämäärän eteen. Pankin ulkopuolella yhteistyö pitää sisällään kokouksia, koulutuksia ja tiedonjakoa. Lisäksi havaittujen riskien esiintuomista ja niiden analysointia. Olennaisessa osassa on myös erilaisten toimintamallien luominen ja mietitään yhdessä, miten asiat hoidetaan pankkien välillä. Ja mikä toistuu nykyään entistä useammin, niin harjoitellaan erilaisia tilanteita. Sitä miten niistä selvitään ja mitä erilaisia vaihtoehtoja on. Harjoittelua voidaan tehdä pankin sisällä yksittäisen vastapuolen kanssa tai isomman ryhmän kanssa. Haastateltava mainitsee, että nämä ovat tärkeimpiä erimerkkejä siitä millä tavalla käytännössä toimitaan.

5.3 Varautumistoimet ja sääntely

Kolmas teema oli varautumistoimet ja sääntely. Sen avulla pyrittiin selvittämään, millä tavalla sääntely vaikuttaa varautumistyöhön ja minkälaisia varautumistoimia pankit tekevät maksuliikenteen turvallisuuden varmistamiseksi. Keskustelimme aluksi uudistuneen sääntelyn vaikutuksista varautumistyöhön. Haastateltavat korostivat sen lisääntyneen ja tuoneen mukanaan lisätyötä. Pankit ovat uuden äärellä ja uudistunut sääntely on tuonut muun muassa paljon raportointivaateita. Pankin tehtävänä on varmistaa ja tehdä tarvittava työ sen eteen, että valvovien viranomaisten vaateet saadaan täytettyä. Haastateltava toi esiin, että uutta sääntelyä on tullut eri tahoilta suhteellisen lyhyellä aikajänteellä suhteellisen paljon. Hän koki, että operatiivisesta näkökulmasta vaateet eivät ole aina täysin selviä ja ne saattavat tulla toimeenpantavaksi kireällä aikataululla. Joskus saattaa tuntua siltä, ettei uusi sääntely palvele sitä mihin pyritään. Uudistunut sääntely asettaa kaikille markkinatoimijoille tiukkoja ja nopeita vaateita, jotka vaativat järjestelmä- ja prosessikehitystä. Vaaditaan kykyä ja resursseja pysyä kehityksen mukana. Vaateiden kiristyessä pienempi toimija ei pärjää ja pankkien on oltava entistä suurempia.

Haastatteluissa selvisi uudistuneen sääntelyn ja raportointivaateiden tuoneen mukanaan vaateita likviditeettiin liittyen. Sen määrään ja siihen, missä muodossa pankin varojen on

oltava. Esimerkiksi minkä arvoista on pankin tallentama raha Keskuspankkiin tai mihin pankin varat saavat olla sijoitettuna ja minkä arvoisia eri sijoituskohteet ovat. On entistä suurempi merkitys, missä varat ovat sillä ne arvotetaan eri tavalla. Sen perusteella missä varat ovat, muodostetaan erilaisia tunnuslukuja, joiden tulee olla tietyllä tasolla. Esimerkiksi LCR eli Liquidity Coverage Ratio nimistä tunnuslukua raportoidaan viranomaisille. Tunnusluku mittaa pankkien resilienssiä likviditeetin näkökulmasta ja se on velvoittava maksuvalmiusaste, joka mittaa pankin likvidien varojen määrää, mikä on oltava käytettävissä lyhyen aikavälin likviditeettivelvoitteen varmistamiseksi esimerkiksi markkinahäiriön sattuessa (Deutsche Bundesbank, n.d.). Haastateltava alleviivasi, että pankkien on oltava entistä tarkempia siitä, miten varat ovat sijoitettu, mihin instrumentteihin ja miten niitä hyödynnetään.

Sääntelyn etuna on, että se tasalaatuistaa tekemistä. Olemme vahvasti digitaalinen yhteiskunta ja pankin järjestelmissä liikkuu valtava määrä sensitiivistä dataa. On hyvä, että on olemassa tietyt raamit, miten digitaalisia järjestelmiä käytetään ja millä tavalla niissä liikkuvaa tietoa suojataan. Järjestelmien sisältämä sensitiivinen henkilökohtainen data on talletettujen varojen lisäksi todella arvokasta. Uudistuneesta sääntelystä haastateltavat mainitsivat esimerkkeinä Doran, GDPR-asetuksen sekä pikamaksuasetuksen. Pikamaksuasetuksen myötä tänä vuonna pakolliseksi pankeille tulee saapuva ja lähtevä pikasiirto sekä uutena toiminnallisuutena maksunsaajan tarkistus. Sen myötä maksaja näkee, onko maksu menossa oikealle saajalle. Näiden rakentaminen vaatii paljon työtä eikä vielä tiedetä kuinka paljon ne tulevat vaikuttamaan tulevaisuudessa työmäärään, esimerkiksi käsiteltäviin maksunpalautuspyyntöihin.

Keskustelimme tärkeimmistä maksuliikenteen mahdollistavista järjestelmistä. Haastateltavat vahvistivat usean järjestelmän vaikuttavan maksuliikenteen kokonaisuuteen. Järjestelmien osalta perustan muodostaa peruspankkijärjestelmä liitännäisineen. Tärkeimmät ovat Euroopan alueella EBA Clearingin järjestelmät, jotka mahdollistavat SEPA-maksuliikenteen ja Euroopan laajuinen T2-järjestelmä mahdollistaen keskuspankkirahan liikkumisen. Ne muodostavat tukirangan, jonka kautta suurin osa maksuliikenteestä kulkee. Myös Swiftin mahdollistavat yhteydet ja siihen liittyvä sanomaliikenne ovat hyvin kriittisiä. Haastateltava totesi, että jos nämä kaikki toimivat, pankit ovat aika hyvässä tilanteessa. Haastatteluissa nousi esiin, että Swiftiin kohdistuu keskimääräistä enemmän uhkaa heidän ollessa kriittinen toimija koko maksuliikenneprosessissa, mutta he ovat hyvin varautuneita. Haastateltavat totesivat, että maksamisen mahdollistavat järjestelmät ovat toimineet luotettavasti. Haastatteluun osallistunut asiantuntija nosti esiin, että nykypäivänä erittäin isossa roolissa ovat myös

kaikki perus tietoliikenneyhteydet. On huomattu, että niihin voidaan vaikuttaa erilaisin tavoin. Ei tarvitse olla kyberhyökkäys vaan perinteinen vaikuttaminen esimerkiksi ankkurin avulla on mahdollista. Hän korosti, että yhteydet ovat moneen kertaan varmennettu ja Suomi ei ole yhden kaapelin varassa. Haastateltava kuvasi asiaa näin:

> *”On hyvä muistaa ja huomioida, että kun suurin osa meidän kotimaammekin maksuista prosessoidaan Manner-Euroopan puolella, niin yksi kriittinen osa mikä ei ole pelkästään maksuliikenteen kriittinen osa, on kaikki toimivat tietoliikenneyhteydet.”*

Selvisi, että EU:n myötä on jouduttu luopumaan maan sisäisistä maksamisen järjestelmistä. Kolikon toisena puolena on varautumistyö, jota maan sisällä tehdään. Näiden välillä tuleekin löytää kultainen keskitie. Mitään maan sisäistä ei voida kehittää, mutta samalla sitä pitää olla. Haastateltava kokee sen haasteelliseksi. Asiantuntija pohti sen olevan kaksiteräinen miekka, kun rakennetaan laajalle ulottuvia järjestelmiä. Silloin myös häiriö kyseisessä järjestelmässä ulottuu laajalle. Kansallinen ja kansainvälinen maksaminen ovat kehittyneet hyvin paljon. Jos mietitään vuosikymmeniä taaksepäin, yhteiseurooppalainen maksujärjestelmä on tuonut paljon hyvää. Sen myötä rahat liikkuvat nopeasti, turvallisesti, vakaasti ja pääsääntöisesti häiriöttömästi. Lisäksi eri eurooppalaisten maiden välillä samaa vauhtia. Haastateltava näkee, että varajärjestely on hyvä tapa kasvattaa resilienssiä siten, että on vielä kotimaiset järjestelmät, mikäli niille on tarvetta. Yleistä maksamisen kehityskulkua ei tulisi kuitenkaan jarruttaa.

Haastateltavat nostivat esiin vuonna 2022 Valtioneuvoston antaneen lain varajärjestelyistä. Maksupalveluiden tarjoajat ja pankit velvoitettiin rakentamaan varajärjestelmää maksuliikenteelle kriittisen infran näkökulmasta. Viimevuosien aikana varautumistyötä Suomessa on ohjattu kansalliselta tasolta. On olemassa varajärjestelyt, joiden avulla Suomi voisi toimia poikkeustilanteessa huoltovarmuuden vaarantumatta, jos normaalit järjestelmät eivät ole toiminnassa. Järjestelyitä pyritään kehittämään jatkuvasti entistä paremmiksi. Resilienssiä poikkeustilanteessa löytyy ja huoltovarmuustilijärjestelmä on yksi konkreettinen varautumiskeino, jonka avulla lisätään yleistä kriisinsietokykyä. Keino turvata pankin asiakkaiden päivittäismaksaminen mahdollisessa isossa häiriötilanteessa, jonka avulla voidaan tukea ja ylläpitää yhteiskunnan toimintaa laajan ja pitkäkestoisen häiriötilanteen sattuessa. Se on yksi mekanismeista mitä on rakennettu kriittisen maksupalveluinfrastruktuurin toiminnan turvaamiseksi. Haastateltava kuvasi asiaa näin:

> *”Vaatii normaalielämästä poikkeuksellisen tilanteen, mutta mikäli sellainen tulisi ja poikkeuksellinen tilanne koskettaisi yhtä tai useampaa suomalaista pankkia, niin meillä on mahdollisuus aktivoida se. Ei olla tyhjänpäällä.”*

Tietoliikennekaapeleita on useita ja se, että kaikki yhteydet olisivat poikki Manner-Eurooppaan vaatisi monen kaapelin yhtäaikaisen sabotoinnin, mutta sekään ei ole mahdotonta. Tilanne, joissa kansallinen varajärjestelmä saattaisi lunastaa paikkansa, on juuri tilanne, jossa olisi jostakin syystä verkkoyhteydet ulkomaailmaan katki. Silloin ei olisi suurella todennäköisyydellä mahdollisuutta toimia osana yleiseurooppalaisia maksujärjestelmiä. Sellaisessa tilanteessa kartoitettaisiin millaisia vaihtoehtoja olisi, jotta pystytäisiin turvaamaan yhteiskunnan toimintakykyä.

Haastateltava näkee pankkien nostaneen varautumistaan maksuliikenteen turvallisuuteen liittyen. Maksuliikenteen näkyvyys pankin sisällä ja yleisesti yhteiskunnassa on ollut perinteisesti alue, josta moni ei tiedä tai ole kiinnostunut. Kun kaikki toimii, ollaan tyytyväisiä ja siinä vaiheessa, kun ongelmia ilmenee alkaa kiinnostus heräämään. Siihen on tullut vuosien varrella muutos. Maksuliikenteen näkyvyys on kasvanut ja sen myötä siihen panostaminen. Kun on enemmän näkyvyyttä, on enemmän merkitystä.

Selviää, että varautumisen eteen on tehty paljon. Esimerkiksi kehitystä prosessi- ja järjestelmätasolla, myös tietoturvan ja jatkuvuuden näkökulmasta. Lisäksi koulutetaan ja lisätään tietoisuutta sekä tehdään erilaista harjoittelua liittyen poikkeustilanteisiin ja varajärjestelyihin. Merkittävä tekijä on myös yhteistyö viranomaisten, keskusvastapuolien sekä toisten pankkien kanssa. Sen avulla varautumista saadaan nostettua ja tietoisuuden kautta päästään korkeammalle tekemisen tasolle. Nämä ovat isoja elementtejä, joiden avulla saadaan kyberturvallisuutta järjestelmien ja tekijöiden tasolla paremmaksi ja varmistetaan, että kaikki toimii. Olennaista on tiedostaa, milloin on mahdollisuuksia toimia ja milloin ei. Paljon on tehty ja paljon on tehtävää, haastateltava kertoo.

Pankin tulee kyetä toimimaan osana kansallisia varajärjestelmiä ja suunnitelmia. Jatkuvuudenhallinta on tärkeä osa minkä tahansa yrityksen toimintaa. Varsinkin kun puhutaan kriittisestä infrastruktuurista, on asiat oltava mietittynä etukäteen. Pankkeja velvoitetaan ylläpitämään jatkuvuussuunnitelmaa häiriöiden ja poikkeustilanteiden varalle, eli sellainen on ja se on tärkeä osa toimintoa. Sitä ylläpidetään ja päivitetään säännöllisesti sekä arvioidaan maksuliikenteeseen kohdistuvia riskejä. Sen pohjalta laaditaan toiminta- ja toipumissuunnitelmia ja sitä, miten häiriöistä viestitään. Jatkuvuussuunnitteluun kuuluu, että työntekijöillä on oltava tiedossa mitä tehdään, mikäli tilanne osuu päälle. Pankissa on

selkeät toimintaohjeet, miten poikkeavissa tilanteissa menetellään. Kaikkeen ei voi toki luoda ohjetta ja tapauskohtaisesti tarkastellaan mitä välineitä on käytössä ja mitä voidaan erilaisissa skenaarioissa hyödyntää. On usein useamman toiminnon yhteistyötä, että asiat menevät kuten halutaan. Kyse on yhteistä tekemistä, vaikka ydin on maksuliikenteen puolella. Haastateltava alleviivaa, että yksin ei näitä asioita usein tehdä.

On paljon sisäistä, ulkoisten tahojen järjestämää sekä tiettyjen keskusvastapuolien järjestämää harjoittelua, johon pankki osallistuu. Harjoittelu voi pitää sisällään erilaista skenaarioita tai varajärjestelyiden testaamista. Ulkopuolelta annetaan erilaisia harjoituskehikoita ja malleja, joihin esimerkiksi Suomen Pankin TIBER kuuluu osana kokonaisvarautumista. Jotta mikä tahansa organisaatio on varmasti ja tosiallisesti varautunut täytyy olla suunnitelmat, askelmerkit ja ohjeet ja niitä pitää harjoitella. Harjoittelun tahti on tiivistynyt. Haastateltava totesi, että mikä muunkin muutoksen kautta olisi kummallista, jos niin ei tapahtuisi. Varautuminen on jatkuvaa työtä. On pysyttävä riittävällä tasolla ja sääntelyn vaatimuksiin on vastattava kunnolla. Haastateltava kuvasi varautumisharjoittelua näin:

> *”Joku pölyttynyt mappi jossain arkistohuoneen takanurkassa, jonka sisältöä kukaan ei muista ja jos pilliin vihelletään ja se pelikaani menee turbiiniin, saattaa olla pikkaisen ikävämpi tilanne verrattuna siihen, että näitä asioita on jumpattu ja ne ovat tuoreessa muistissa.”*

Syksyllä pankeille pakolliseksi tuleva lähtevä pikasiirto asettaa valvonnan tarpeita ja omanlaiset vaatimukset infrastruktuurille monesta näkökulmasta. Jos mietitään huijaustapauksia tai sitä, miten varmistetaan pankin likviditeetin riittävyys ja mietinnän paikka on myös se, kuinka pienetkin järjestelmäkatkokset näkyvät. Aiemmin suurin osa maksuista on lähtenyt massamaksuina. Lyhytkestoiset katkokset esimerkiksi tietoliikenneyhteyksissä eivät ole välttämättä näkyneet maksujen välityksessä. Maksuja sisältävä tiedosto lähtee, kun se lähtee. Lyhyen katkoksen yli odotetaan ja maksut lähetetään tarvittaessa vasta, kun häiriö on ohi eikä se välttämättä näy kuluttajalle. Nyt kun maksun tulee olla kymmenessä sekunnissa valmis, saattavat lyhyemmätkin häiriöt heijastua tulevaisuudessa enemmän. Eikä puhuta välttämättä pankin tai finanssisektorin häiriöstä, vaan saatetaan puhua esimerkiksi verkkoliikenneinfrastruktuurin häiriöstä. Puhumattakaan siitä, että kehitys menee varmasti eteenpäin. Maksamisen reaaliaikaistuminen ja integroituminen muihinkin kuin pankin perinteisiin palveluihin tulee jatkamaan kasvuaan. Kyllähän tässä varmasti ollaan uuden äärellä myös näiden tukevien infran vaatimusten osalta. Lähtevällä pikasiirrolla on omat vaikutuksensa, joihin pitää

pystyä mukautumaan. Se on yksi merkittävä muutos monen joukossa, haastateltava toteaa. Haastateltava kuvasi maksamisen reaaliaikaistumista näin:

> *”Kun maksaminen on reaaliaikaistunut, kaikki mahdolliset häiriötilanteet ja niiden vaikutukset tuntuvat paljon nopeammin kuin vuosikymmeniä sitten, jolloin maksujen välittyminen oli hitaampaa. Näin ollen reagoinnin nopeus ja odotusarvo minkä yhteiskunta asettaa vaikka nyt tässä tapauksessa pankeille on omalta osaltaan kiristynyt. Jos aiemmin puhuttiin päivän tai kahden viiveestä ja sen kanssa elettiin, niin nyt aletaan olemaan kohta siinä tilanteessa, että tunnin viivekin alkaa tuntua liian pitkältä. Sekin sitten omalta osaltaan ehkä luo tarvetta siihen, että kaikki mahdolliset oli kyse varajärjestelyistä tai jostain poikkeustilamenettelystä tai mistä tahansa, niin se tarve saada ne nopeasti käyttöön on kasvanut.”*

Haastatteluiden myötä selvisi pankkien ottavan turvallisuuden todella vakavasti. Olennainen osa on toimintaympäristön jatkuva seuraaminen ja siihen reagointi. Yksi osa sitä on resurssit. Haastateltava uskoo, että kaikki toimijat pyrkivät varmistamaan, että resurssit tämänkaltaiseen toimintaan ovat riittävät. Suomessa, Euroopan laajuisesti sekä maailmanlaajuisesti on erittäin hyvät ja tehokkaat maksamisen järjestelmät. Niiden häiriöt ovat olleet kohtalaisen pieniä ja aika minkä ne ovat toiminnassa, on prosentuaalisesti korkea. Pankit ovat luottamusalalla. Asiakkaiden tulee voida luottaa siihen, että maksujenvälitys toimii turvallisesti ja niin hyvin kuin mahdollista. Luottamuksen ylläpitämiseksi täytyy tehdä jatkuvaa työtä. Jos se menetetään, menetetään koko liiketoiminta. Menetettyä luottamusta on vaikea saada takaisin ja selviää, että se on kaatanut pankkeja. Usein rikolliset, esimerkiksi kyberrikolliset ottavat ensimmäisen askeleen ja pankkien tulee kyetä pysymään heidän kintereillään. On tärkeä pysyä kehityksen perässä sekä varmistaa, että pankki voi osaltaan tarjota yhden yhteiskunnan kriittisistä toiminnoista, jonka avulla yhteiskunnan toimivuus varmistetaan sekä normaalioloissa, että mahdollisissa poikkeusoloissa.

IT-järjestelmien ja niiden tietoturvan on oltava kunnossa. Samoin työntekijöiden tietoturvan. Jotta voidaan varautua poikkeustilanteisiin, on riskienhallinta tärkeää niin maksuliikenteen sisällä kuin koko pankissa. Esiin nousee myös työntekijöiden koulutus, tiedonvaihto ja yhteistyö niin pankin sisällä kuin muiden toimijoiden kanssa. Pankissa seurataan jatkuvasti ja ajantasaisesti maksuliikennettä sen toteutumisen ja likviditeetin kannalta. Eli tiedetään joka hetki missä ollaan ja mihin ollaan menossa. Se varmistaa kyvykkyyden varautua ja nähdään poikkeuksia, jotka eivät mene kuten pitää. Jatkuvan seurannan avulla poikkeamat

nousevat esiin ja niihin pystytään reagoimaan. Merkittävä osa on ydintyötä tekevillä ihmisillä ja sillä, että heillä on riittävä osaaminen, kyky toimia ja ymmärtää syy-seuraussuhteita. Näiden asioiden kanssa työskentelevien tulee olla keskimääräistä enemmän hereillä siitä, mitä he tekevät ja miten toimivat. Haastateltava vetää yhteen, että sillä että ollaan mahdollisimman hyvin ajan tasalla omasta tilanteesta, päästään hyvin pitkälle. Myös toinen haastateltava vahvistaa, että tärkeimpiä tekijöitä ovat teknologian, prosessien sekä henkilöstön pyhä kolminaisuus. Niiden kaikkien tulee olla kunnossa. Tietoturva ja kyky toimia erilaisissa tilanteissa ovat välttämättömiä taitoja nykymaailmassa. Organisaatioiden on huolehdittava, että osaamisen taso on riittävällä tasolla kaikilla tekijöillä. Haastateltava kuvasi asiaa näin:

> *”Vaikka olisi maailman paras teknologia, mutta prosessit ja varautumissuunnitelmat eivät ole kunnossa, niin se ei auta. Ja toisaalta jos ei panosta meidän henkilöstöömme, että heillä on se osaaminen, halu ja motivaatio niin sekään ei auta. Tai jos meillä ei ole riittävät resurssit. Me tarvitsemme kaikkia kolmea tukipilaria. Niiden päälle pystymme rakentamaan niin vakaan kokonaisuuden että se kestää vähän isommatkin myrskyt.”*

Asiantuntijat ovat luottavaisia sen suhteen, että pankin maksuliikenne on turvattu. Se ei tarkoita, etteikö ongelmia voisi tulla, mutta miten pankissa toimitaan, varaudutaan ja tiedostetaan pankin vastuu, he ovat luottavaisin mielin. Finanssisektorilla Suomessa on tehty todella hyvää työtä varautumisen suhteen. Työ toki jatkuu ja hyvä niin. Haastateltavat näkevät, että asiaan on kiinnitetty riittävästi huomiota itse toimijoiden tasolta sekä valvojien ja lainsäätäjien tasolta. Asia on erittäin hyvällä tavalla seurannassa ja turvallisuus keskiössä.

6 Johtopäätökset

Tässä opinnäytetyössä etsittiin vastausta siihen, onko pankin maksuliikenne turvattu poikkeustilanteessa. Eli tilanteessa, jossa joudutaan ottamaan käyttöön varajärjestelyitä pankin maksuliikenteen turvaamiseksi ja toteuttamiseksi tai tilanteessa, jossa pankki on voimakkaiden kyberhyökkäysten kohteena. Opinnäytetyön tarkoituksena oli selvittää vastaukset seuraaviin tutkimuskysymyksiin:

- Onko pankin maksuliikenne turvattu poikkeustilanteessa?

- Millaisin keinoin pankki varmistaa maksuliikenteen toimivuuden poikkeustilanteessa?

Tämä tutkimus osoittaa maailman ja sen myötä yleisen turvallisuusympäristön muuttuneen merkittävästi. Yhteiskunnassa vallitsee erilaisia jännitteitä ja geopoliittista epävarmuutta eikä jatkuvan epävarmuuden vallitessa ei voi ennustaa mitä huominen tuo tullessaan. Kriittiseen infrastruktuuriin on kohdistunut vaikuttamista ja useat pankit ovat olleet palvelunestohyökkäyksien kohteena. Viholliset käyttävät uudenlaisia hyökkäystekniikoita ja suuntaavat niihin ison määrän resursseja. Hyökkäysten taustalla saattaa olla myös valtiollisia toimijoita. Palvelunestohyökkäysten määrä on lisääntynyt ja niiden voima on kasvanut. Pankkien on kyettävä vastaamaan alati uudistuviin uhkiin ja kehitettävä jatkuvasti uusia keinoja puolustautua. Kyberuhat ovat uudenlaisia verrattuna aiempaan. Kriittisenä toimialana rahoitusala on keskiössä yhteiskunnan toimintakyvyn kannalta. Maailma on kovassa murroksessa ja geopoliittisesti vaikeassa maastossa on pystyttävä navigoimaan. Toimintaympäristön muutos on lisännyt maksamiseen ja pankkeihin kohdistuvia uhkia merkittävästi. Maksaminen on houkuttava kohde hybridivaikuttamiselle. Iskemällä kriittiseen maksamisen infrastruktuuriin saataisiin yhteiskunnan toimintakyky rampautettua. Se haastaa ja asettaa paineita maksamisen järjestelmille ja järjestelyille. Turvallinen maksaminen ei ole enää itsestäänselvyys.

Tutkimuksen tulokset osoittavat pankin maksuliikenteen turvallisuuden olevan hyvällä tasolla eikä pitkäkestoisia häiriöitä ole ollut. Vaikka toimintaympäristö on muuttunut ja pankit ovat olleet palvelunestohyökkäysten kohteena, palvelut ovat toimineet pääsääntöisesti hyvin ja olleet suurimman osan ajasta käytettävissä. Maksamisen mahdollistava infrastruktuuri on toiminut kuten pitää. Pankin maksuliikenne on turvattu mahdollisessa häiriö- tai poikkeustilanteessa useiden toimenpiteiden ja varajärjestelyiden avulla. Voidaan todeta, että resilienssiä poikkeustilanteessa löytyy. Maksuliikenteen turvallisuuden varmistamiseksi on tehty paljon töitä ja se työ jatkuu. Mahdollisiin häiriötilanteisiin on varauduttu ja useat varajärjestelyt turvaavat maksamista mahdollisen häiriön tai poikkeustilanteen sattuessa.

Digitalisoitunut yhteiskunta on yhä riippuvaisempi tietoverkkojen toimintavarmuudesta ja turvallisuudesta. Itämerenalaiset merikaapelit ovat elintärkeitä finanssialalle. Tutkimuksen tulokset osoittivat, että kriittiset tietoliikenneyhteydet ovat varmistettu usean kaapelin avulla. On teoreettisesti mahdollista vaikkakin hyvin epätodennäköistä, että kriittiset kaapelit voivat katketa samanaikaisesti. Tällaisessa tilanteessa huoltovarmuustilijärjestelmä on keino, joka voitaisiin ottaa käyttöön maksamisen mahdollistamiseksi. Yksittäinen toimija ei voi varautua

ja vaikuttaa kaikkeen sillä maksamisen ketjuun kuuluu useita toisiinsa tiiviisti verkottuneita toimijoita ja komponentteja. Vakavien ja laajojen häiriöiden varalle on varajärjestelyt, joiden avulla maksamisen huoltovarmuus saadaan turvattua. Yksittäiset häiriöt merikaapeleissa voivat aiheuttaa lähinnä hetkellisiä katkoksia tai hitautta yhteyksiin dataliikenteessä. Kriittiset yhteydet on varmistettu usean eri järjestelyn kautta ja Suomessa on varauduttu merenalaisen infrastruktuurin vaurioitumiseen erilaisin huoltovarmuustoimin.

Kuten tutkimustulokset osoittivat, pankit ovat luopuneet useista kotimaisista maksujärjestelmistä. Maksuliikenteen kansainvälistymisen ja EU:n myötä on siirrytty kansainvälisiin maksujärjestelmiin. Tutkimusprosessin aikana nousi esiin kysymys siitä kannattaako pankkien luopua kaikista kotimaisista järjestelmistä, sillä niille voisi olla muuttuneessa turvallisuusympäristössä vielä tarvetta. Pitäisikö nykyisten rinnalle rakentaa uusia kotimaisia järjestelmiä? Haastatteluissa selvisi, ettei uusia kotimaisia järjestelmiä voida kehittää. Pankin asiantuntijoiden näkemyksen perusteella voidaan todeta, että yleistä maksamisen kehityssuuntaa ei tulisi jarruttaa, mutta toisella kädellä kotimaisten järjestelmien olemassaolon merkitys vahvistuu epävarmassa toimintaympäristössä. Maksamisen kansainvälistyminen mahdollistaa reaaliaikaisen rahan välittymisen eurooppalaisten maiden välillä samaa vauhtia kuten kotimaassa ja maksamisen viive on poistunut. Kansainvälistyminen on tuonut mukanaan paljon hyvää. Toisaalta taas järjestelmähäiriö toisella puolella maailmaa saattaa realisoitua hyvinkin nopeasti. Tulokset osoittivat, että maksuliikenteen toimintaympäristöä on muuttanut osaltaan maksamisen nopeutuminen. Edellä mainituista seikoista sekä maksamisen kehittymisestä aiheutuu uudenlaisia haasteita, joihin pitää pystyä varautumaan.

Finanssitoimijoiden varautumista on vauhditettu ja sen myötä on tullut parannuksia esimerkiksi etätyöskentelyssä hyödynnettävään teknologiaan. Tietoturvan merkitys on korostunut entisestään. Kuten tutkimuksen tuloksista ilmeni, on pankkien järjestelmien sisältämä sensitiivinen data pankkiin tallennettujen varojen lisäksi todella arvokasta. Olemme nähneet surullisia esimerkkejä siitä, millaisia seurauksia tietovuodoista voi aiheutua. Pankin asiakkaisiin kohdistuva huijaaminen on lisääntynyt ja se osoittaa, että arkaluontoisia tietoja yritetään väärinkäyttää ja ne ovat arvokkaita rikollisille. Tulokset vahvistivat rahoitusalan toiminnan perustuvan luottamukseen ja jos luottamus särkyy, ollaan hyvin äkkiä ongelmissa. Mahdollisesta pankkiin kohdistuvasta tietovuodosta aiheutuisi vähintäänkin mainehaittaa ja pahimmillaan se voisi asiakkaiden vetäytyessä kaataa koko liiketoiminnan. Perinteisesti on ehkä ajateltu varojen turvallisuuden olevan keskiössä, mutta nyky-yhteiskunnassa sen lisäksi korostuu sensitiivisen datan suojaaminen.

Maksamisessa on totuttu nopeuteen sekä siihen, että maksujenvälittymiseen liittyvät prosessit toimivat häiriöttömästi reaaliajassa. Maksamisen turvallisuutta on nostettu enemmän esille ja sitä kautta herätelty yhteiskuntaa siihen, ettei kaikki välttämättä aina toimi kuten pitää. Tulosten perusteella voidaan todeta, että nykyisessä maailmantilanteessa korostuu hajauttamisen tärkeys. Kuluttajia onkin kehotettu useamman pankin asiakkuuteen, jolloin mahdollisessa häiriötilanteessa yhden pankin ollessa poissa pelistä, on päivittäinen rahaliikenne ja asiointi mahdollista toteuttaa toisen pankin välityksellä. Mahdollisessa häiriötilanteessa tunnistautuminen pankkitunnuksilla ei onnistu ja maksukortit eivät välttämättä toimi. Käteisen rahan merkitystä on korostettu ja suositeltu pitämään maksamisen kotivaraa eli muutaman päivän tarpeita vastaava määrä käteistä rahaa varalla esimerkiksi ruoka- ja lääkeostoksia varten.

Vaikka kohtaisimme kyberhyökkäyksen, sähkökatkon, kaapeleita rikkoutuisi tai yhteiskunta kohtaisi muita yllättäviä häiriöitä, tulee kriittisen maksuliikenteen toteutua ajallaan. Pitkään jatkuessa siihen kohdistuvilla häiriöillä olisi vaikutuksia yritysten kassanhallintaan, laskujen maksuun ja sitä myötä koko yhteiskunnan toimintakykyyn. Palkkojen ja eläkkeiden on oltava käytettävissä ajallaan. Koska rahoituslaitokset ovat vahvasti sidoksissa toisiinsa, yksittäisen toimijan haasteet voivat heijastua nopeasti toisiin toimijoihin. Senkin vuoksi yksittäisen pankin puolustuksen ajantasaisuus on ensiarvoisen tärkeää. Varsinaiset uhat toteutuvat lopulta yksittäisten toimijoiden ja niiden käyttämien yksilöllisten järjestelmien välityksellä. Tutkimuksen tulokset vahvistivat, että turvallisuus otetaan vakavasti ja turvallisuuden, häiriöttömyyden sekä jatkuvuuden eteen tehdään jatkuvaa työtä. Kriittisen infrastruktuurin varautumistyötä säädellään kansalliselta tasolta. Se kertoo, että kyse on merkittävistä asioista ja varautumisen lisääntyessä voidaan päätellä uhkatason kasvaneen.

Kyberturvallisuus on monimuotoinen ja haastava kenttä. Varautuminen ja harjoittelu ovat ensiarvoisen tärkeässä asemassa toimintakyvyn varmistamiseksi häiriön sattuessa. Silloin ei ole aikaa ihmetellä, on oltavat selkeät toimintamallit. Kriisit seuraavat aina toisiaan ja on todennäköistä, että jollain aikavälillä kohtaamme merkittävän hybridi- tai kyberiskun. Varautumistyö, harjoittelu sekä niiden tulokset konkretisoituvat silloin kun jotain tapahtuu ja mitataan se, kuinka valmistautuneita ollaan. Teemahaastattelujen tulokset osoittivat, että harjoittelu ja sen myötä varautuminen on hyvällä tasolla. Harjoittelun tahtia on tiivistetty. Pankissa on selkeät prosessit, toimintamallit, jatkuvuussuunnitelma sekä toipumissuunnitelma häiriötilanteiden varalle. Näitä ylläpidetään ja päivitetään säännöllisesti. Aktiivinen harjoittelu, varajärjestelmien säännöllinen testaaminen sekä yhteistyö pankin sisällä ja yhdessä useiden ulkopuolisten tahojen kanssa vahvistavat ja rakentavat turvallisuutta. Selkeät prosessit ja toimintamallit luovat resilienssiä

poikkeustilanteessa. Keskeisenä avaintekijänä nousi esiin yhteistyön merkitys niin pankin sisällä kuin laajemmin eri toimijoiden kesken sen ulkopuolella. Rahoitusmarkkinoiden vakaa ja häiriötön toiminta on edellytys yhteiskunnan toimivuudelle.

Kuten tutkimuksen tuloksista selvisi, nykytilanne on vauhdittanut monen asian etenemistä. Useita suunnittelun asteella olleita kehitystöitä on polkaistu käyntiin ja viety nopeammin eteenpäin. Konkreettisena esimerkkinä tästä on tämän projektin aikana voimaan astunut uudistunut lainsäädäntö ja sen myötä myös varautumisharjoittelun on vastattava uudistunutta sääntelyä. Uudistuneen sääntelyn tarpeen ovat herättäneet kyberhyökkäykset sekä geopoliittinen tilanne. Kävi ilmi, että viranomaisten vaateilla on työllistävä vaikutus. Voidaan todeta, että kun asiat ovat uusia niiden ratkominenkin on sitä myötä haastavaa, sillä asioita tehdään ensimmäistä kertaa. Lainsäädäntö ohjaa pankkien toimintaa tiukasti ja asettaa velvoitteita esimerkiksi viranomaisraportoinnille. Uudistuvalla ja lisääntyvällä sääntelyllä sekä lainsäädännöllä on pankeissa työllistävä vaikutus. Sen päämääränä on kuitenkin yhtenäiset toimintamallit ja turvallisuuden sekä tietoturvan tason parantaminen. Tavoitteena on yhteiskunnan elintärkeitä toimintoja ylläpitävien palvelujen ja infrastruktuurin mahdollisimman häiriötön toiminta.

Kaapelien rikkoutuminen ja lainsäädännön uudistaminen opinnäytetyötä kirjoittaessa kertoo siitä, että tilanne elää. Tätä vahvisti lisäksi opinnäytetyöprojektin aikana suomalaisiin pankkeihin kohdistuneet useat palvelunestohyökkäykset. Jopa useampaan eri toimijaan saman päivän aikana. On oltava jatkuvasti varuillaan ja ajan hermoilla. Pankkipalveluita tuotetaan sekä käytetään reaaliaikaisesti kellon ympäri päivästä riippumatta. Tämän vuoden aikana kaikille pankeille pakolliseksi tuleva lähtevä pikasiirto sujuvoittaa ja muuttaa maksuliikennettä entistä reaaliaikaisemmaksi. Samaan aikaan myös erilaisiin häiriöihin ja kyberriskeihin varautuminen ja reagointi vaatii entistä enemmän nopeutta. Valvonnan ja reagoinnin on toimittava kellon ympäri.

Tutkimustulosten yhteenvetona voidaan todeta, että pankkienvälinen maksuliikenne on reaaliaikaista ja kansainvälistä. Sen toteuttamiseksi tarvitaan useita maksamisen mahdollistavia kansainvälisiä järjestelmiä ja maksuliikenteen infrastruktuuri on usean järjestelmän muodostama kokonaisuus, jossa jokaisen komponentin on toimittava ja yhden haasteet vaikuttavat toisiin. Eri järjestelmien ja toimijoiden välillä vallitsee vahvoja keskinäisiä ja kansainvälisiä riippuvuussuhteita. Yhden pankin ongelmat heijastuvat hyvin nopeasti muihin toimijoihin sekä muille toimialoille. Pahimmillaan maksujärjestelmien toimimattomuus voi vaarantaa rahoitusmarkkinoiden vakauden, sillä yksittäiset rahoitusalan toimijat muodostavat yhdessä laajemman kokonaisuuden.

Rahoitusjärjestelmän ja maksuliikenteen kansallinen varautuminen on tärkeä osa koko kansakunnan kokonaisturvallisuutta. Varautuminen riskeihin edellyttää IT-alan osaamista, rahoitusalan osaamista sekä koko toimialan ja viranomaisten välistä yhteistyötä. Finanssiala on kolmen kriittisimmän alan joukossa, kun mietitään toimialojen muodostamaa riippuvuusverkostoa. Riskienhallinnan näkökulmasta on ensiarvoisen tärkeää tunnistaa etukäteen, mistä palveluista toiminta on riippuvaista. Tärkeimpiä tekijöitä, joiden avulla pankin maksuliikenteen turvallisuutta varmistetaan ovat riskienhallinta ja ennakkoon tehtävä varautumistyö. Tiivis yhteistyö pankin sisällä ja ulkoisten sidosryhmien kanssa on ensiarvoisen tärkeää. Samoin aktiivinen tiedonvaihto. Kukaan ei voi yksin, yhden toiminnon tai yhden yrityksen voimin varmistaa kriittisen maksamisen infrastruktuurin turvallisuutta. Kyberhyökkäysten torjuntaan tarvitaan pankkien ja viranomaisten yhteistyötä. Harjoittelun avulla vahvistetaan toimintavarmuutta. Pankeissa on tehty paljon työtä varautumisen eteen. Keskiössä pankin maksuliikenteen turvallisuuden varmistamisessa ovat prosessi- ja järjestelmäkehitys sekä tietoturva ja jatkuvuudenhallinta. Tutkimuksen tuloksissa korostui koulutuksen ja tietoisuuden lisäämisen merkitys. Samoin aktiivinen harjoittelu, yhteistyö ja tiedonvaihto sekä toimintaympäristön ja maksuliikenteen aktiivinen ja ajantasainen seuranta. Niputettuna yhteen opinnäytetyö osoittaa, että onnistuneen kokonaisuuden muodostavat teknologia, prosessit sekä henkilöstö. Pankkeihin kohdistuu isot odotukset maksuliikenteen reaaliaikaisuudesta ja häiriöttömyydestä ja näihin odotuksiin on pystyttävä vastaamaan. Turvallisuus otetaan vakavasti ja tutkimusten tulosten perusteella voidaan todeta, että pankin maksuliikenteen turvallisuus on turvattu mahdollisissa häiriö- ja poikkeustilanteissa.

7 Pohdinta

Laadullisen tutkimuksen asetelma on joustava ja tutkimuksen eri vaiheiden välillä voi olla paljon päällekkäisyyttä. Työn eri osiot etenivät, muokkaantuivat ja valmistuivatkin osittain toistensa lomassa. Aluksi painopiste oli vahvasti lähteisiin tutustumisessa, tietoperustassa ja sen koostamisessa. Tämän jälkeen teemahaastattelun haastattelukysymykset tarkentuivat lopulliseen muotoonsa ja painopiste siirtyi tutkimusosuuden työstämiseen, kerätyn aineiston analysointiin ja työn valmiiksi saattamiseen.

Projekti käynnistyi lokakuussa 2024, kun tallensin aihe ehdotuksen sekä laadin opinnäytetyösuunnitelman ja aineistohallintasuunnitelman. Raportin työstäminen alkoi sisällysluettelon hahmottelemisella sekä tutustumalla tietoperustan lähteisiin. Pidimme opinnäytetyöohjauksen lokakuun lopulla 2024 ja sen jälkeen käynnistyi tietoperustan

kirjoittaminen. Määrittelin keskeiset käsitteet ja koostin tietoperustan valitsemieni lähteiden pohjalta. Suunnittelin samalla tutkimusosuutta ja teemahaastattelun kysymyksiä. Pidimme toisen opinnäytetyöohjauksen tammikuun lopulla 2025 ja sen jälkeen siirryin tutkimusosuuden työstämiseen. Sen myötä haastattelukysymykset tarkentuivat lopulliseen muotoonsa valittujen teemojen ympärille. Osallistuin viestintäpajaan ja opinnäytetyön väliseminaariin helmikuun lopussa. Niistä saadun palautteen perusteella työn rakenne ja sisältö muokkaantuivat lopulliseen muotoonsa ja viimeistelin tietoperustan. Sain väliseminaarista ja viestintäpajasta arvokasta palautetta. Koin hyödylliseksi, kun joku katsoi työtä uusin silmin. Palautteen perusteella tekemäni suurimmat muokkaukset koskivat kappalejakoja ja niiden sisältöjä. Tämän jälkeen painopiste siirtyi vahvasti tutkimukselliseen osuuteen. Tutustuin menetelmäkirjallisuuteen, toteutin teemahaastattelut sekä analysoin niiden tulokset. Näiden jälkeen kirjoitin johtopäätökset sekä pohdinnan, viimeistelin työn ja osallistuin loppuseminaariin. Työskentely eteni laatimani suunnitelman pohjalta. Projekti toteutui suunnitellusti ja ajallaan. Tavoitteeni oli saada työ valmiiksi maaliskuun loppuun mennessä. Varasin tarvittaessa huhti- ja toukokuun aikaa, mikäli alkuperäinen aikataulu osoittautuisi liian tiukaksi. Pysyin suunnitelmassa, tosin teemahaastattelut toteutuivat aikataulusta jäljessä ja työ valmistui toukokuun alussa 2025. Eli varatulle lisäajalle oli tarvetta.

Opinnäytetyön aihe on laaja ja rajauksen tekeminen osoittautui hieman haastavaksi. Aiheesta löytyi paljon mielenkiintoista tietoa ja sitä tuli prosessin edetessä lisää. Kaikkea ei voinut sisällyttää mukaan raportille ja näin ollen työ tarkentui ja rajautui lopulliseen muotoonsa. Työn aihe kypsyi opintojen aikana ja mielenkiinto sitä kohtaan heräsi oman työni sekä muuttuneen maailmantilanteen myötä. Opinnäytetyöprosessi on ollut kokonaisuudessaan opettavainen ja mielenkiintoinen kokemus. Se on opettanut suunnitelmallisuutta, aikataulutusta, kokonaisuuksien hallintaa, lähdekriittisyyttä, tiedon etsimistä sekä sen soveltamista. Samoin tavoitteellisen haastattelurungon luomista ja haastattelijana toimimista. Tietoperustan ja teemahaastattelun tulosten tarkastelun myötä lisäksi analysointitaitoja ja syyseuraussuhteiden hahmottamista. Opin projektin edetessä paljon hyödyllistä tietoa myös työhöni liittyen. Aiheeseen perehtyminen on syventänyt osaamistani maksamisen järjestelmistä, niiden keskinäisriippuvuuksista sekä ohjaavasta lainsäädännöstä ja sääntelystä. Samoin valvovista viranomaisista sekä siitä, miten maksujen katteet liikkuvat eri pankkien ja järjestelmien välillä. Projektin myötä ymmärsin entistä paremmin, että pankin maksuliikenteen turvallinen toteutuminen on monisyklinen ja laajasti verkottunut kokonaisuus ja sen vaikutukset ulottuvat koko yhteiskuntaan. Itseäni kiinnostava aihe on pitänyt työstämisen mielekkäänä. Työtä on ollut sen vuoksi mukava tehdä ja mielenkiinto on säilynyt läpi prosessin. Koen, että aihe on ajankohtainen ja elää

jatkuvasti. Esimerkkinä maksuliikenteen turvallisuuden varmistamiseksi astui prosessin aikana voimaan uutta sääntelyä ja pankkeihin kohdistui palvelunestohyökkäyksiä sekä muutamia kaapeleita katkesi Itämerellä.

Teemahaastattelut onnistuivat hyvin. Niiden avulla saatiin arvokasta lisätietoa siitä, millä tavalla pankit varmistavat maksuliikenteen turvallisuuden ja millainen on tämänhetkinen toimintaympäristö pankin ja siellä työskentelevien asiantuntijoiden näkökulmasta. Teemahaastatteluiden avulla kerätyt tutkimustulokset antoivat syvempää ja konkreettisempaa lisätietoa ja tukivat, vahvistivat ja täydensivät työn tietoperustaa. Opinnäytetyössä onnistuttiin vastaamaan tutkimuskysymyksiin.

Tämän opinnäytetyön toteutuksessa on noudatettu hyvää tieteellistä käytäntöä. Siinä on käytetty monipuolisesti luotettavia lähteitä sekä kiinnitetty huomiota lähdekriittisyyteen. Eri lähteistä löydettyjä tietoja on vertailtu keskenään ja tiedot ovat näin vahvistettavissa. Laadullisen tutkimuksen luotettavuus perustuu osaltaan tutkijan rehellisyyteen ja dokumentaation tuleekin olla riittävää ja tehtyjen valintojen perusteltuja. Tutkimuksen tuloksia sekä lähdeaineistoa on pyritty tarkastelemaan objektiivisesti eli puolueettomasti. Tehdyt havainnot ja tutkimustulokset on esitetty totuudenmukaisesti ja irrottamatta alkuperäisestä asianyhteydestään. Raportissa on kuvattu avoimesti tutkimuksen prosessi ja sen eteneminen. Miten tietoperusta ja tutkimus on koostettu ja työ rakentunut. Millaisia lähteitä siihen on käytetty, millä tavalla aineisto on kerätty, miten tutkimus on toteutettu ja tulokset analysoitu. Lähteet on luetteloitu ja haastattelujen litteroinnit säilytetty asianmukaisesti. Haastatteluihin osallistui pieni, mutta tarkoin valittu vastaajajoukko. Pankin maksuliikenteen turvallisuutta koskevat seikat ovat pienen ja rajatun asiantuntijapiirin tiedossa. Heiltä on saatu luotettavaa ja erityistä asiantuntijuutta vaativaa tietoa aiheesta. Haastateltavat olivat alansa ammattilaisia, joilla on vahva tietotaito ja näkemys tutkittavasta ilmiöstä. Haastateltavien valinnassa pyrittiin kiinnittämään huomiota siihen, että saadaan tutkimustietoa eri näkökulmien edustajilta. Teemahaastattelu menetelmänä mahdollisti syvällisemmän näkökulman, kuin esimerkiksi strukturoitu haastattelu tai kysely. Haastatteluiden luotettavuus perustui suunnitelmaan ja sitä mukailevaan toteutukseen. Laadukkuutta on pyritty rakentamaan hyvän haastattelurungon avulla sekä huolellisella perehtymisellä siihen, miten olla hyvä haastattelija. On silti muistettava, että teemahaastattelun tuloksiin liittyy aina tutkijan tulkintaa.

Opinnäytetyön aihevalinnassa on pyritty huomioimaan vastuullisuus ja kestävä kehitys. Vastuullisuus liittyy tapaan toimia ja tehdä päätöksiä. Kestävyys taas on mahdollinen seuraus näistä päätöksistä. Pankkitoimialalla on kyse luottamuksesta, sillä pankit

hallinnoivat ja ovat vastuussa yksityisten ihmisten sekä yritysten varallisuudesta. Sitä myöten pankeilla on kokonaisvastuu merkittävistä rahavirroista ja yhteiskunnan toimintakyvystä. Onkin vastuullinen aihevalinta tutkia, onko pankin maksuliikenne turvattu poikkeustilanteessa ja millaisin keinoin pankki varmistaa maksuliikenteen turvallisuuden poikkeustilanteessa. Näiden ratkaisujen tulee olla kestäviä. Yhteiskunnassa on totuttu siihen, että maksaminen on turvallista, nopeaa ja että se toimii moitteettomasti. Siihen ei ole kiinnitetty juurikaan huomiota. Oli kiinnostava huomata, että maksamiseen kohdistuvat epävarmuustekijät, sitä koskettaneet häiriöt sekä muuttunut maailmatilanne on nostanut aiheen jalansijaa ja maksamisen kokonaisuus on alkanut kiinnostaa. Tässä maailmantilanteessa erilaiset digitaaliset uhat ovat hyvin todennäköisiä.

Prosessin myötä kiinnostavia esiin nousseita jatkotutkimusaiheita olisi selvittää, missä pankin prosesseissa olisi kehitettävää maksuliikenteen turvallisuuteen liittyen ja millä tavalla näitä esiin nousseita haavoittuvuuksia pyritään pankeissa parantamaan. Samoin mielenkiintoinen aihe olisi eri finanssialan toimijoiden välinen maksamisen turvallisuuteen liittyvä yhteistyö ja sen tarkempi tutkiminen. Lisäksi se, miten maksamisen kehittymisen myötä syntyvät uudet haasteet ratkaistaan.

Yksi osa pankkien varautumista ja turvallisuustyötä on, ettei arkaluontoista ja salassa pidettävää tietoa jaeta asiaan kuulumattomille tai puhuta ulospäin tietoja, jotka eivät ole saatavilla julkisesta lähteestä. Tämä vahvistui prosessin aikana ja haastateltavat olivat tarkkoja vastauksissaan. Tutkimuksen tulokset käytiin pankissa läpi, ennen kuin ne julkaistiin. Kaikki tieto minkä viholliset saavat ovat arvokasta. Vaikka yksittäiset palaset tuntuisivat pieniltä, riittävän monta yhdistelemällä muodostuu looginen kokonaisuus. Salassapitovelvollisuus on alalla ensiarvoisen tärkeää ottaa vakavasti.

Maksamisen kehittyminen, reaaliaikaistuminen ja pakolliseksi tuleva lähtevä pikasiirto herättivät ajatuksia siitä, muuttuuko työnteon luonne pankeissa kohti ympärivuorokautista prosessien valvontaa. Kiristyvien vaateiden myötä poikkeamiin on reagoitava ja tiukat velvoitteet täytettävä. Aika näyttää millä tavalla maksamisen kenttä ja siihen liittyvä tekeminen tulevaisuudessa muuttuu. Haastatteluissa nousi esiin resurssien merkitys ja pankit priorisoivat ja resursoivat varautumiseen liittyvää työtä korkealle.

Kulissien takana tapahtuu varmasti paljon ja on hyvä, ettei ulospäin kerrota kaikkea. On huojentavaa tietää, että useat vaihtoehtoiset varajärjestelyt ja toimenpiteet turvaavat maksamisen infrastruktuuria. On monia toimenpiteitä, joita mahdollisissa häiriö- ja poikkeustilanteissa voidaan hyödyntää. Pankkien ja viranomaisten tekemä jatkuva

intensiivinen yhteistyö, kansallisen tason ohjeistus sekä uudistuva sääntely vahvistavat maksamisen turvallisuutta. Tätä aihetta ei ole tutkittu suoranaisesti aiemmin opinnäytetyön muodossa. Työn sisältämiä keskeisiä teemoja kyllä ja niistä löytyy erilaisia tutkimuksia. Tutkimustyötä voidaan pitää onnistuneena, sillä tutkimuskysymyksiin löydettiin vastaus.

Lähteet

Suomen Pankki. (n.d.-b). SEPA-maksun välittyminen *[kuva].* https://www.suomenpankki.fi/fi/raha-ja-maksaminen/maksu--ja-selvitysjarjestelmat/

Huoltovarmuuskeskus. (2020). Toimialariippuvuudet *[kuva].* https://www.huoltovarmuuskeskus.fi/files/bbb790d6eb4a6c776cd32e185104a2d8516bce65/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

Ahosniemi, A. (13.11.2024). *Pankkien osoittelu ei auta – kyberhyökkäysten torjuntaan tarvitaan pankkien ja viranomaisten yhteistyötä.* Finanssiala. https://www.finanssiala.fi/kolumni/pankkien-osoittelu-ei-auta-kyberhyokkaysten-torjuntaan-tarvitaan-pankkien-ja-viranomaisten-yhteistyota/

Deutsche Bundesbank. (n.d.). *Liquidity regulation.* https://www.bundesbank.de/en/tasks/banking-supervision/individual-aspects/liquidity/liquidity-regulation-622878

Euroopan Keskuspankki. (2024-a). *Maksaminen & rahoitusvakaus.* https://www.ecb.europa.eu/paym/html/index.fi.html

Euroopan Keskuspankki. (10.4.2018). *Miksi kyberturvallisuus on tärkeää?* https://www.ecb.europa.eu/ecb-and-you/explainers/tell-me/html/cyber-resilience.fi.html

Euroopan Keskuspankki. (29.6.2016). *Mitä ovat maksujärjestelmät? Entä TARGET2-järjestelmä?* https://www.ecb.europa.eu/ecb-and-you/explainers/tell-me/html/target2.fi.html

Euroopan Keskuspankki. (1.2.2020). *Mitä ovat pikamaksut?* https://www.ecb.europa.eu/ecb-and-you/explainers/tell-me-more/html/instant_payments.fi.html

Euroopan Keskuspankki. (2024-b). *Valvontaprioriteetit vuosille 2025–2027.* https://www.bankingsupervision.europa.eu/framework/priorities/html/ssm.supervisory_priorities202412~6f69ad032f.fi.html

Euroopan Keskuspankki. (n.d.). *What is cyber resilience?* https://www.ecb.europa.eu/paym/cyber-resilience/html/index.fi.html

Euroopan komissio. (7.9.2023). *Kriittinen infrastruktuuri: Komissio ehdottaa suunnitelmaa, jolla tehostetaan reagointia rajat ylittävissä häiriötilanteissa.* Suomen-edustusto. https://finland.representation.ec.europa.eu/uutiset/kriittinen-infrastruktuuri-komissio-ehdottaa-suunnitelmaa-jolla-tehostetaan-reagointia-rajat-2023-09-07_fi

Filpus, L. (4.1.2023). *Finanssialan sektori pitää yhteiskunnan verisuoniston kunnossa.* Varmuuden vuoksi. https://www.varmuudenvuoksi.fi/artikkeli/finanssialan-sektori-pitaa-yhteiskunnan-verisuoniston-kunnossa

Finanssiala. (15.3.2025). *Kyberturvallisuus ja tietosuoja.* https://www.finanssiala.fi/aiheet/kyberturvallisuus-ja-tietosuoja/#/

Finanssiala. (28.8.2023). *Yhtenäinen Euromaksualue SEPA.* https://www.finanssiala.fi/aiheet/yhtenainen-euromaksualue-sepa/#/

Finanssivalvonta. (19.12.2024-a). *Asetus finanssialan digitaalisesta häiriönsietokyvystä.* Valvottavatiedote 88/2024. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2024/asetus-finanssialan-digitaalisesta-hairionsietokyvysta/

Finanssivalvonta. (2.1.2025*). Finanssivalvonnan painopisteenä vuonna 2025 säilyvät valvottavien hallinnon luotettavuus ja toimintaympäristön epävarmuuksiin vastaaminen – tiivistelmät tarkastusten tuloksista verkkosivuille.* Valvottavatiedote 3/2025. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2025/finanssivalvonnan-painopisteena-vuonna-2025-sailyvat-valvottavien-hallinnon-luotettavuus-ja-toimintaympariston-epavarmuuksiin-vastaaminen--tiivistelmat-tarkastusten-tuloksista-verkkosivuille/

Finanssivalvonta. (20.9.2024-b). *Pohjoismaiden ja Baltian kriisisimulaatioharjoitus 2024.* https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/verkkouutiset/2024/pohjoismaiden-ja-baltian-kriisisimulaatioharjoitus-2024/

Finanssivalvonta. (24.8.2020-a). *Varautuminen.* https://www.finanssivalvonta.fi/saantely/varautuminen/

Finanssivalvonta. (7.7.2020-b). *Varautumissuunnitelmat toimitettava Finanssivalvonnalle 31.12.2020 mennessä.* Valvottavatiedote 44/2020. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2020/varautumissuunnitelmat-toimitettava-finanssivalvonnalle-31.12.2020-mennessa/

Grym, A. (28.12.2017). *Kyberriskit huomioitava, jotta rahoitusvakaus säilyy*. Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/blogit/2017/kyberriskit-huomioitava-jotta-rahoitusvakaus-sailyy/

Hakala, J. (23.5.2024). *Yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (CER direktiivi).* Sisäministeriö. https://sisainenturvallisuus.fi/documents/8347581/0/JohannaHakala.pdf/d1f08335-4b39-cc9a-f943-9845c644fce4/JohannaHakala.pdf?t=1717588231940

Hallituksen esitys HE 104/2022 vp. *Hallituksen esitys eduskunnalle laiksi eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla ja siihen liittyviksi laeiksi.* https://www.eduskunta.fi/fi/vaski/hallituksenesitys/sivut/he_104+2022.aspx

Harjuniemi, T. (31.3.2022). *Onko syytä rahahuoliin – miten finanssiala varautuu kriiseihin?* Varmuuden vuoksi. https://www.varmuudenvuoksi.fi/artikkeli/onko-syyta-rahahuoliin-miten-finanssiala-varautuu-kriiseihin

Heikkinen, P. (19.10.2023). *Keskuspankki panostaa maksamisen merkittäviin kehityshankkeisiin.* Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/2023/5/keskuspankki-panostaa-maksamisen-merkittaviin-kehityshankkeisiin/

Hirsjärvi, S. Hurme, H. (2022). Tutkimushaastattelu. Gaudeamus.

Huoltovarmuuskeskus. (2.11.2023-a). *Ajankohtaisia kysymyksiä ja vastauksia kriittisestä infrastruktuurista ja varautumisesta.* https://www.huoltovarmuuskeskus.fi/a/ajankohtaisia-kysymyksia-ja-vastauksia-kriittisesta-infrastruktuurista-ja-varautumisesta

Huoltovarmuuskeskus. (n.d.-a). *CER-direktiivin valmistelu.* https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/kansainvalinen-yhteistyo/cer-direktiivin-valmistelu

Huoltovarmuuskeskus. (16.12.2024-a). *Finanssialan kyberharjoituksessa hyökättiin digitaalisiin palveluihin ja pilotoitiin harjoitusympäristöä.* https://www.huoltovarmuuskeskus.fi/a/finanssialan-kyberharjoituksessa-hyokattiin-digitaalisiin-palveluihin-ja-pilotoitiin-harjoitusymparistoa

Huoltovarmuuskeskus. (9.2.2022-a). *Finanssialan varautuminen hyvällä tolalla.* https://www.huoltovarmuuskeskus.fi/a/finanssialan-varautuminen-hyvalla-tolalla

Huoltovarmuuskeskus. (2024-b). *Huoltovarmuus Suomessa.* https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/huoltovarmuus-suomessa

Huoltovarmuuskeskus. (11.10.2023-b). *HVK on kehottanut kriittisen infrastruktuurin yrityksiä nostamaan varautumistasoa.* https://www.huoltovarmuuskeskus.fi/a/hvk-on-kehottanut-kriittisen-infrastruktuurin-yrityksia-nostamaan-varautumistasoa

Huoltovarmuuskeskus. (26.9.2024-c). *Huoltovarmuuden yleistilannekuva 24.9.2024: Ei merkittäviä muutoksia, epäilyttävä toiminta jatkunut.* https://www.huoltovarmuuskeskus.fi/a/huoltovarmuuden-yleistilannekuva-24-9-2024-ei-merkittavia-muutoksia-epailyttava-toiminta-jatkunut

Huoltovarmuuskeskus. (24.10.2024-d). *Huoltovarmuuden yleistilannekuva 22.10.2024: Tilannekuva vakaa, pankkipalveluihin kohdistettu kyberhyökkäyksiä.* https://www.huoltovarmuuskeskus.fi/a/huoltovarmuuden-yleistilannekuva-22-10-2024-tilannekuva-vakaa-pankkipalveluihin-kohdistettu-kyberhyokkayksia

Huoltovarmuuskeskus. (2020). *Kyberturvallisuuden nykytila eri toimialoilla - kartoituksen keskeiset havainnot.* Huoltovarmuusorganisaatio. https://www.huoltovarmuuskeskus.fi/files/bbb790d6eb4a6c776cd32e185104a2d8516bce65/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

Huoltovarmuuskeskus. (n.d.-b) *Sektori ja poolit.* https://www.huoltovarmuuskeskus.fi/toimialat/finanssiala/sektori-ja-poolit

Huoltovarmuuskeskus. (30.9.2022-b). *Suomen tietoliikenneyhteydet suojattu monin tavoin.* https://www.huoltovarmuuskeskus.fi/a/suomen-tietoliikenneyhteydet-suojattu-monin-tavoin

Isokoski, R. (26.12.2024). *"Pimeän laivaston" tankkeri pysähtyi Suomen edustalle – Tämä siitä tiedetään.* Kauppalehti. https://www-kauppalehti-fi.ezproxy.hamk.fi/uutiset/pimean-laivaston-tankkeri-pysahtyi-suomen-edustalle-tama-siita-tiedetaan/f04a262f-bd7b-4dac-b45f-f28b5a84f5d8

Jyväskylän yliopisto. (n.d.). *Kyberturvallisuuden jatkuva kehittäminen.* https://www.jyu.fi/fi/suomen-kyberosaamiskeskus-ficec

Kavander, A. (4.3.2025). *Myös S-pankkiin tehtiin palvelunestohyökkäys – mobiilipankkiin ei pääse, verkkosivut eivät toimineet hetkeen.* https://yle.fi/a/74-20147429

Kavander, A. (19.12.2024). *Tilisiirron odottelu jää historiaan – ensi vuonna rahat siirtyvät kaverin pankkitilille 10 sekunnissa.* https://yle.fi/a/74-20132578

Kejo, J. (28.9.2022). *Nordstream-kaasuputkien sabotaasi pakottaa Saksan pysymään Venäjä-vastaisessa pakoterintamassa*. UMV-lehti. https://mvlehti.net/2022/09/28/nordstream-kaasuputkien-sabotaasi-pakottaa-saksan-pysymaan-venaja-vastaisessa-pakoterintamassa/

Kemppainen, K. (5.5.2017). *Maksaminen muuttuu reaaliaikaisemmaksi ja huomaamattomammaksi.* Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/2017/2/maksaminen-muuttuu-reaaliaikaisemmaksi-ja-huomaamattomammaksi/

Kyberturvallisuuskeskus. (n.d.). *NIS2 - Euroopan unionin kyberturvallisuusdirektiivi.* Traficom. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

Kärkkäinen, H. (6.3.2025). *Näin Suomeen hyökätään nyt – USA:n piiloon jääneellä päätöksellä saattaa olla pian ikävä vaikutus.* https://www.is.fi/digitoday/tietoturva/art-2000011079554.html

Laine, T. (8.5.2018). *Digitalisaatio haastaa maksujärjestelmien turvallisuuden.* Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/2018/2/digitalisaatio-haastaa-maksujarjestelmien-turvallisuuden/

Laki eräistä huoltovarmuuden turvaamisen järjestelyistä rahoitusalalla 666/2022. https://www.finlex.fi/fi/laki/alkup/2022/20220666

Liski, J. (27.1.2025). *HS selvitti: Merikaapelin vaurioitumisesta epäillyn aluksen omistaa Kiinan valtio.* Helsingin Sanomat. https://www.hs.fi/tutkiva/art-2000010992041.html

Luoma, I. (27.9.2024). *NIS2- ja CER-direktiivit asettavat uusia vaatimuksia kyberturvallisuudelle ja kriittisten toimijoiden toimintavarmuudelle.* CGI. https://www.cgi.com/fi/fi/blogi/tietoturva-ja-kyberturvallisuus/nis2-ja-cer-direktiivit-asettavat-uusia-vaatimuksia

Nissilä, A. & Korhonen, J. (19.11.2024). *Kaikki tapahtui 11 sekunnissa – KRP:llä hyvä kuva merikaapelin tuhoalueen aluksista.* https://www.iltalehti.fi/kotimaa/a/3f72ec78-4f81-47ec-b09a-dec4f9bbe220

Nordea. (23.9.2024). *Palvelunestohyökkäykset voivat aiheuttaa hitautta Nordean digitaalisiin palveluihin kirjautumisessa.* https://www.nordea.com/fi/uutiset/paivitys-palvelunestohyokkaykset-voivat-aiheuttaa-hitautta-nordean-digitaalisiin-palveluihin-kirjautumisessa

OP. (n.d.). *SEPA-maksu.* https://www.op.fi/henkiloasiakkaat/paivittaiset/maksaminen/sepa-maksu

Peltoniemi, T. & Ripatti, K. (15.3.2023). *Rahoitusmarkkinoiden putkiremontti: uusi T2 -maksujärjestelmä otetaan käyttöön 20.3.2023.* Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/2023/artikkelit/rahoitusmarkkinoiden-putkiremontti-uusi-t2-maksujarjestelma-otetaan-kayttoon-20-3-2023/

Procountor. (n.d.). *Maksuliikenne- mitä tarkoittaa maksuliikenne?* https://procountor.fi/taloushallinnon-sanakirja/maksuliikenne/

Puusa, A & Juuti, P. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät.* Gaudeamus Oy.

PWC. (n.d.). *DORA-asetus ja sen vaikutukset yrityksille.* https://www.pwc.fi/fi/palvelut/teknologia-ja-digitaalisuus/kyberturvallisuus-ja-tietosuoja/dora-asetus-ja-sen-vaikutukset-yrityksille.html

Raeste, J-P. (15.10.2024). *Nordea: Verkkohyökkäysten voima ja kesto täysin ennennäkemätön, tarkoitus horjuttaa yhteiskuntaa.* Helsingin Sanomat. https://www.hs.fi/talous/art-2000010761540.html

Rahoitusvakausvirasto. (20.1.2025-a). *Kokonaisturvallisuutta vahvistetaan uudella yhteiskunnan turvallisuusstrategialla.* https://rvv.fi/-/kokonaisturvallisuutta-vahvistetaan-uudella-yhteiskunnan-turvallisuusstrategialla

Rahoitusvakausvirasto. (n.d.-a). *Päivittäismaksaminen vakavissa häiriötilanteissa.* https://rvv.fi/huoltovarmuus

Rahoitusvakausvirasto. (4.3.2025-b). *RVV aloittaa vuoden 2025 kriisinratkaisusuunnittelutyön pankkien kanssa.* https://rvv.fi/-/rvv-aloittaa-vuoden-2025-kriisinratkaisusuunnittelutyon-pankkien-kanssa

Rahoitusvakausvirasto. (n.d-b). *Talletussuoja Suomessa*. https://rvv.fi/talletussuoja

Rahoitusvakausvirasto. (15.3.2024). *Valtiovarainministeriö on asettanut rahoitusmarkkinoiden häiriönhallinnan yhteistyöryhmän*. https://rvv.fi/-/valtiovarainministerio-on-asettanut-rahoitusmarkkinoiden-hairionhallinnan-yhteistyoryhman

Rehn, O. (19.5.2021). *Kriisiherkkyys kasvanut myös maksamisessa – häiriöihin varaudutaan yhteisin toimin.* Suomen Pankki. Maksufoorumi 2021. https://www.suomenpankki.fi/fi/ajankohtaista/puheet-ja-haastattelut/2021/paajohtaja-olli-rehn-kriisiherkkyys-kasvanut-myos-maksamisessa-hairioihin-varaudutaan-yhteisin-toimin/

Ripatti, K. (21.11.2024). *TIPSistä tulossa euroalueen ja Pohjoismaiden johtava maksamisen selvitysalusta.* Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/2024/artikkelit/tipsista-tulossa-euroalueen-ja-pohjoismaiden-johtava-maksamisen-selvitysalusta/

Samlink. (28.10.2024). *The Future of Security and DORA: Preparing for Tomorrow's Threats.* https://samlink.fi/news/the-future-of-security-and-dora/

Snellman, H. (5.5.2017). *Maksamisen sujuttava kaikissa tilanteissa.* Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/2017/2/maksamisen-sujuttava-kaikissa-tilanteissa/

Suomen Huoltovarmuusdata oy. (n.d.). *Huoltovarmuudella turvataan yhteiskunnan toimintakyky häiriötilanteissa.* https://www.suomenhuoltovarmuusdata.fi/huoltovarmuus

Suomen Pankki. (n.d.-a). *EKP ja eurojärjestelmä.* https://www.suomenpankki.fi/fi/suomen-pankki/strategia-ja-tehtavat/eurojarjestelma-ja-ekp/

Suomen Pankki. (14.5.2024). *Geopoliittiset jännitteet ja jähmettyneet kiinteistömarkkinat varjostavat rahoitusvakautta.* Euro ja talous. Vakausarvio. https://www.eurojatalous.fi/fi/2024/2/geopoliittiset-jannitteet-ja-jahmettyneet-kiinteistomarkkinat-varjostavat-rahoitusvakautta/

Suomen Pankki. (n.d.-b). *Maksu- ja selvitysjärjestelmät*. https://www.suomenpankki.fi/fi/raha-ja-maksaminen/maksu--ja-selvitysjarjestelmat/

Suomen Pankki. (n.d.-c). *Maksaminen.* *https://www.suomenpankki.fi/fi/raha-ja-maksaminen/maksaminen*

Suomen Pankki. (n.d.-d). Maksufoorumi. https://www.suomenpankki.fi/fi/raha-ja-maksaminen/maksaminen/maksufoorumi/

Suomen Pankki. (n.d.-e). *Maksuneuvosto.* https://www.suomenpankki.fi/fi/raha-ja-maksaminen/maksaminen/maksuneuvosto/

Suomen Pankki. (n.d.-f). *Päivittäismaksamisen turvaaminen.* https://www.suomenpankki.fi/fi/raha-ja-maksaminen/varautuminen/paivittaismaksamisen-turvaaminen/

Suomen Pankki. (n.d.-g). *TIBER-FI toimintamalli.* https://www.suomenpankki.fi/fi/raha-ja-maksaminen/tiber-fi-toimintamalli/

Suomen Pankki. (26.04.2019). *1.2 Rahapolitiikan toteuttaminen euroalueella ja Suomessa.* Vuosikertomus 2018. https://vuosikertomus.suomenpankki.fi/2018/toimintakertomus/rahapolitiikka/rahapolitiikan-toteuttaminen-euroalueella-ja-suomessa/

Suomen Pankki. (n.d.-h). *Varautuminen.* https://www.suomenpankki.fi/fi/raha-ja-maksaminen/varautuminen/

Suomi.fi. (13.12.2024-a). *Jatkuvuudenhallinta ja varautuminen*. https://kehittajille.suomi.fi/palvelut/digiturva/jatkuvuuden-hallinta-ja-varautuminen

Suomi.fi. (13.12.2024-b). *Kriittisten kohteiden suojaaminen*. https://kehittajille.suomi.fi/palvelut/digiturva/jatkuvuuden-hallinta-ja-varautuminen/kriittisten-kohteiden-suojaaminen

Suomi.fi. (15.11.2024-c). *Kyberhyökkäykset tai -häiriöt.* https://www.suomi.fi/oppaat/varautuminen/miten-varaudun-hairio-ja-kriisitilanteisiin/kyberhyokkaykset-tai-hairiot

Suomi.fi. (28.11.2024-d) *Tietoturva ja kyberturvallisuus.* https://kehittajille.suomi.fi/palvelut/digiturva/tietoturva

Sisäministeriö. (n.d.). *Kyberturvallisuus osana kansallista turvallisuutta.* https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus

STT-YLE. (8.10.2024). *Verkkopankkien käyttökatkoista järjestetään kuuleminen eduskunnassa.* https://yle.fi/a/74-20116728

Swift. (n.d.). *Messaging and Standards.* https://www.swift.com/about-us/discover-swift/messaging-and-standards

Techopedia. (n.d.). *Kyberturvallisuus.* https://www.techopedia.com/fi/kyberturvallisuus

Terho, J. & Wathén, H. (19.10.2023). *Eurojärjestelmän kyberstrategia Suomeen.* Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/2017/2/maksamisen-sujuttava-kaikissa-tilanteissa/

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

Tuomi, J & Sarajärvi, A. (2022). *Laadullinen tutkimus ja sisällönanalyysi.* Tammi.

Tötterman, K. (3.10.2019). *Eurojärjestelmän porrastettu talletuskorkojärjestelmä.* Euro & talous. Suomen Pankki. https://www.eurojatalous.fi/fi/2019/4/eurojarjestelman-porrastettu-talletuskorkojarjestelma/

Valtioneuvosto. (8.12.2022-a). *Kriittisen infrastruktuurin häiriönsietokykyä parannetaan ja yhteiskunnan toimintakyvyn kannalta kriittiset toimijat tunnistetaan.* https://valtioneuvosto.fi/-//1410869/kriittisen-infrastruktuurin-hairionsietokykya-parannetaan-ja-yhteiskunnan-toimintakyvyn-kannalta-kriittiset-toimijat-tunnistetaan-

Valtioneuvosto. (2022-b). *Valtioneuvoston huoltovarmuusselonteko*. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164329/VN_2022_59.pdf

Valtioneuvosto. (10.10.2024-a). *Valtioneuvosto hyväksyi uudistetun kyberturvallisuusstrategian.* https://valtioneuvosto.fi/-/valtioneuvosto-hyvaksyi-uudistetun-kyberturvallisuusstrategian

Valtioneuvosto. (2024-b). *Suomen kyberturvallisuus - strategia 2024–2035*. Valtioneuvoston kanslia. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165860/VNK_2024_11.pdf?sequence=1

Valtioneuvosto. (19.12.2024-c). *Hallitus esittää uutta lakia ohjaamaan yhteiskunnan toimintakyvyn kannalta kriittisen infrastruktuurin suojaamista ja häiriönsietokyvyn parantamista.* https://valtioneuvosto.fi/-/1410869/hallitus-esittaa-uutta-lakia-ohjaamaan-yhteiskunnan-toimintakyvyn-kannalta-kriittisen-infrastruktuurin-suojaamista-ja-hairionsietokyvyn-parantamista

Valtioneuvosto. (1.9.2023). *Suomi harjoitteli rahoitusalan varautumista Yhdysvaltojen ja lähialueen kumppanimaiden kanssa.* https://valtioneuvosto.fi/-/10623/suomi-harjoitteli-rahoitusalan-varautumista-yhdysvaltojen-ja-lahialueen-kumppanimaiden-kanssa

Valtiovarainministeriö. (n.d.-a). *Finanssivalvonta, Euroopan finanssivalvontajärjestelmä ja yhteinen valvontamekanismi.* https://vm.fi/finanssivalvonta-ja-euroopan-finanssi-valvontajarjestelma

Valtiovarainministeriö. (n.d.-b). *Päivittäismaksamisen turvaaminen vakavissa häiriötilanteissa.* https://vm.fi/paivittaismaksamisen-turvaaminen

Virolainen, A. (10.10.2024). *Finanssiala mukana hybridiuhkien torjunnan harjoituksessa.* Finanssiala. https://www.finanssiala.fi/uutiset/finanssiala-mukana-hybridiuhkien-torjunnan-harjoituksessa/

Weuro, J. (9.11.2024). Kotona kannattaa pitää sopiva määrä käteistä muutaman päivän tarpeisiin. *Helsingin Sanomat.* Mielipide. https://www.hs.fi/mielipide/art-2000010814801.html

Liite 1. Teemahaastattelu

Teema 1 Turvallisuusympäristö

Millainen on pankin maksuliikenteen toimintaympäristön vakaus?
Onko pankin maksuliikenteen turvallisuustilanne muuttunut verrattuna aiempaan? Jos on, millä tavalla?
Onko pankin maksuliikenteen turvallisuuteen liittyen havaittu riskejä? Jos on, millaisia?
Mitä haluat sanoa pankin maksuliikenteen turvallisuusympäristöstä?

Teema 2 Sidosryhmät

Ketkä ovat sisäisiä sidosryhmiä, joiden kanssa tehdään yhteistyötä pankin sisällä pankin maksuliikenteen turvallisuuden varmistamiseksi?
Ketkä ovat sidosryhmiä talon ulkopuolella, joiden kanssa tehdään yhteistyötä pankin maksuliikenteen turvallisuuden varmistamiseksi?
Millaista yhteistyötä sen eteen tehdään, että varmistetaan pankin maksuliikenteen turvallisuus ja häiriöttömyys?
Mitä haluat sanoa pankin maksuliikenteen turvallisuuteen liittyvistä sidosryhmistä ja yhteistyöstä?

Teema 3 Varautumistoimet ja sääntely

Onko pankki nostanut varautumistaan maksuliikenteen turvallisuuteen liittyen verrattuna aiempaan? Jos on, millaisin käytännön toimenpitein pankki on nostanut varautumistaan maksuliikenteen turvallisuuteen liittyen?
Millä tavalla pankissa varmistetaan, ettei maksuliikenteen turvallisuus vaarannu tai häiriinny?
Millaisin toimenpitein mahdollisiin maksuliikennettä koskeviin havaittuihin riskeihin on reagoitu ja varauduttu?
Onko pankilla jatkuvuussuunnitelma maksuliikenteen häiriö- ja poikkeustilanteiden varalle? Mitä voit kertoa siitä?
Onko olemassa toimintasuunnitelma ja selkeät toimintaohjeet, kuinka mahdollisessa pankin maksuliikennettä koskevassa häiriö – ja poikkeustilanteessa menetellään? Mitä voit kertoa niistä?
Harjoitellaanko pankissa maksuliikenteen poikkeustilanteiden ja häiriöiden varalle?
Mitä haluat sanoa pankin maksuliikenteen turvallisuuteen liittyvästä varautumisesta?
Mitä haluat sanoa pankin maksuliikenteen turvallisuuteen liittyvästä sääntelystä?

Mitkä ovat mielestäsi tärkeimpiä tekijöitä, joiden avulla varmistetaan pankin maksuliikenteen turvallisuus ja häiriötön toiminta?
Koetko, että pankin maksuliikenne on turvattu häiriön tai poikkeustilanteen sattuessa?

Liite 2. Aineistonhallintasuunnitelma

1 Opinnäytetyön aineiston kuvaus

Aineistonhankinnan menetelmänä käytetään puolistrukturoituja teemahaastatteluja. Teemahaastattelun kohderyhmänä ovat pankin asiantuntijat. Analysoitava aineisto kerätään sähköisesti Teams-haastatteluiden välityksellä ja haastattelut tallennetaan haastateltavien luvalla äänitallenteiksi ja litteroidaan tekstitallenteiksi. Litteroinnin jälkeen haastatteluiden äänitallenteet poistetaan.

2 Aineiston tallennus ja säilytys

Analysoitava ja litteroitu aineisto säilytetään opinnäytetyön tekijän henkilökohtaisella tietokoneella, mikä on salasanalla suojattu. Pääsy aineistoon on vain tekijällä itsellään. Varmuuskopiota säilytetään tekijän toisella henkilökohtaisella tietokoneella, mikä on myös salasanalla suojattu ja pääsy aineistoon on vain tekijällä itsellään. Opinnäytetyön tekijän lisäksi aineistoa käsittelee mahdollisesti myös opinnäytetyön ohjaaja.

3 Henkilötietojen ja arkaluontoisten tietojen säilytys

Opinnäytetyössä ei käsitellä henkilötietoja.

4 Aineiston omistajuus

Opinnäytetyön tekijä omistaa opinnäytetyön aineiston ja tulokset. Tekijänoikeus ja omistusoikeus projektityön tuloksiin ja muuhun aineistoon kuuluu opinnäytetyön tekijälle.

5 Aineiston jatkokäyttö työn valmistumisen jälkeen

Tutkimusaineistoa ei jatkokäytetä opinnäytetyön valmistumisen jälkeen. Opinnäytetyön tekijä säilyttää aineiston tietoturvallisesti vuoden ajan opinnäytetyön hyväksymispäivästä, jotta opinnäytetyön tulokset voidaan tarvittaessa varmistaa ja hävittää tämän jälkeen aineiston tietoturvallisesti.