TURUN YLIOPISTO
Kauppakorkeakoulu

# Epäsymmetrinen informaatio ja markkinahäiriöt kyber-vakuutusmarkkinoilla


Taloustiede, Taloustieteen laitos

Kandidaatin tutkielma

Laatija:

Henni Harinen

Ohjaaja:

FM, VTM Kristian Martiskainen



6.5.2026

Turku

Opiskelijan lausunto tekoälyn käytöstä tähän tutkielmaan liittyen:

☐ **En ole käyttänyt tekoälyä hyödyntäviä työkaluja** tätä tutkielmaa kirjoittaessani.

☒ **Olen käyttänyt tekoälyä hyödyntäviä työkaluja** tätä tutkielmaa kirjoittaessani. Tämä käyttö on dokumentoitu tutkielman liitteessä. Vakuutan, että tekoälyä käytettiin yliopiston ohjeistuksen mukaisella tavalla.

Kandidaatintutkielma

**Oppiaine**: Taloustiede
**Tekijä**: Henni Harinen
**Otsikko**: Epäsymmetrinen informaatio ja markkinahäiriöt kybervakuutusmarkkinoilla
**Ohjaaja**: FM, VTM Kristian Martiskainen
**Sivumäärä**: 34 sivua + liitteet 1 sivu
**Päivämäärä**: 6.5.2026

## Tiivistelmä

Tutkielma tarkastelee kybervakuutusmarkkinoiden toimivuutta tilanteissa, joissa vakuutuksenottajien ja vakuutusyhtiöiden välinen epäsymmetrinen informaatio aiheuttaa kannustinongelmia ja markkinahäiriöitä. Kyberriskien erityispiirteet kuten vahva keskinäisriippuvuus, voimakkaat ulkoisvaikutukset, datan niukkuus ja uhkien nopea kehittyminen tekevät riskien arvioinnista poikkeuksellisen haastavaa ja heikentävät perinteisten vakuutusmallien soveltuvuutta. Tutkimusongelmana on selvittää, miten epäsymmetrinen informaatio ilmenee kybervakuutuksissa ja millä tavoin ne vaikuttavat riskien hinnoitteluun sekä yritysten tietoturvainvestointeihin.

Tutkielma on toteutettu kuvailevana kirjallisuuskatsauksena, jossa yhdistetään klassisia teoreettisia malleja ja ajankohtaista tutkimuskirjallisuutta. Tarkastelun kohteena ovat etenkin kaksi keskeistä päämies-agentti-ongelmaa: haitallinen valikoituminen ja moraalikato. Tutkielman teoreettinen viitekehys pohjautuukin pitkälti Akerloafin (1970) ja Rothschildin & Stiglitzin (1976) malleihin epäsymmetrisestä informaatiosta. Markkinoiden vuorovaikutusta havainnollistetaan lisäksi yksinkertaisen bayesilaisen peliteoreettisen mallin avulla. Empiirinen aineisto koostuu kansainvälisestä tutkimuskirjallisuudesta, jossa tarkastellaan kybervakuutusmarkkinoita eri toimintaympäristöissä. Esimerkkitapauksina hyödynnetään Malesian, Ruotsin ja Yhdysvaltojen markkinoita. Tutkielma osoittaa, kuinka markkinahäiriöt saavat eri muotoja markkinoiden kypsyysasteen mukaan, mutta ne liittyvät pohjimmiltaan tiedon epätasaiseen jakautumiseen osapuolten välillä.

Tulosten perusteella haitallista valikoitumista esiintyy kybervakuutusmarkkinoilla, mutta empiirinen näyttö ei yksiselitteisesti tue perinteistä teoriaa, jonka mukaan heikoimmin suojautuneet hakeutuisivat vakuutuksen piiriin. Tutkimuksessa löytyi näyttöä myös päinvastaisesta ilmiöstä, jossa kaikkein riskialttiimmat toimijat jäivät vakuutusmarkkinoiden ulkopuolelle. Moraalikadon osalta havainnot poikkeavat yhdenmukaisesti teorian ennustuksista. Vakuutuksen ottaminen ei empiiristen tutkimusten mukaan johtanut tietoturvatoimien laiminlyöntiin, vaan suojautuminen säilyi ennallaan tai jopa parani. Tätä saattaa selittää esimerkiksi vakuutusehtoihin kuuluvat turvallisuusvaatimukset tai kyberriskien vaikeasti ennakoitava luonne.

Johtopäätöksenä todetaan, että kybervakuutusmarkkinoiden keskeinen ongelma on epävarmuus, joka ilmenee riskin määrittelyn epäselvyytenä ja molemminpuolisena tiedon epätasapainona. Vakuutusyhtiöillä on rajallinen tieto asiakkaiden todellisesta riskitasosta, ja yritykset arvioivat omia haavoittuvuuksiaan usein puutteellisesti. Tämä heikentää hinnoittelun tarkkuutta ja rajoittaa vakuutusten kattavuutta erityisesti tilanteissa, joissa riskit ovat vahvasti keskinäisriippuvaisia. Tutkimuskirjallisuus korostaakin tarvetta paremmalle datalle ja yhtenäisemmille arviointikäytännöille. Koska empiirinen tutkimus epäsymmetrisen informaation vaikutuksista on vielä hajanaista, tarvitaan jatkotutkimusta erityisesti myös markkinoiden tasapainon ja kannustinrakenteiden kehittämisestä.

**Avainsanat:** kybervakuutus, epäsymmetrinen informaatio, moraalikato, haitallinen valikoituminen, kyberriskit, markkinahäiriö

# SISÄLLYS

# 1 Johdanto

Kyberriskit ovat nousseet viime vuosina yhdeksi yritysmaailman suurimmaksi uhkatekijäksi. Maailman talousfoorumin (World Economic Forum 2026, 3) mukaan taustalla vaikuttavat erityisesti kolme toisiinsa liittyvää muutosta. Näitä ovat nopea teknologinen kehitys, geopoliittiset epävakaudet sekä digitaalisten riippuvuuksien monimutkaistuminen. Koronaviruspandemia kiihdytti siirtymää perinteisestä lähityöstä kohti joustavampaa etätyötä, mikä on vahvistanut näiden tekijöiden vaikutusta. Hajautetut työympäristöt ovat tehneet yrityksistä haavoittuvampia, ja siksi kyberturvallisuudella on yhä tärkeämpi merkitys yritysten strategisessa riskienhallinnassa (Tsohou ym. 2023).

Kyberriskien taloudellinen merkitys on huomattava. Abrardi ym. (2025) arvioivat, että globaalit kybervahinkojen kustannukset voivat nousta vuosittain jopa 200 miljardiin dollariin. Suorien taloudellisten menetysten lisäksi yritykset kärsivät myös epäsuorista vaikutuksista kuten mainehaitoista ja asiakasluottamuksen heikkenemisestä. Samanaikaisesti kyberturvallisuusmarkkinat kasvavat nopeasti. Cybersecurity Venturesin (2025) ennusteiden mukaan alan maailmanlaajuisten kyberturvallisuustuotteiden ja -palvelujen menojen odotetaan vuonna 2026 nousevan 522 miljardiin. Vuoteen 2031 mennessä kokonaismenojen ennustetaan ylittävän biljoonan dollarin rajan. Näiden arvioiden valossa on selvää, että kyberriskien hallinta on keskeinen edellytys myös yritysten taloudelliselle toimintakyvylle.

Vaikka kyberturvallisuusmarkkinat kasvavat nopeasti, ala kohtaa silti monia haasteita, jotka heikentävät markkinoiden toimivuutta. Kyberhyökkäysten ennalta-arvaamattomuus on tehnyt niistä merkittävän taloudellisen ja toiminnallisen uhan kaikilla toimialoilla. Viime vuosien tapahtumat ovat osoittaneet, että kyberhyökkäykset voivat ilmaantua äkillisesti ja aiheuttaa laajoja häiriöitä myös tilanteissa, joissa yritykset eivät ole suoran hyökkäyksen kohteena. Konkreettinen esimerkki tällaisesta tilanteesta on vuoden 2017 NotPetya-hyökkäys, jossa yhden ukrainalaisen ohjelmistotoimittajan kaapattu haitallinen päivitys levisi automaattisesti käyttäjille ja pysäytti globaalisti useiden suuryritysten toiminnan (Yle 2017). Vastaavia tapauksia on nähty myös viime vuosina. Esimerkiksi vuonna 2025 italialaisen Plus Service -toimittajan tietomurto lamautti useiden liikennöitsijöiden lipunmyynnin kahdeksi päiväksi, vaikka hyökkäys ei kohdistunut suoraan näihin yrityksiin (ENISA 2025).

Kyberhyökkäysten luonne myös muuttuu jatkuvasti. Tekoälyn hyödyntäminen hyökkäyksissä on lisännyt uhkien kehittyneisyyttä ja tehostanut hyökkäystapoja (Abrardi ym. 2025). World Economic Forumin (2026) tuoreen raportin mukaan 87 prosenttia organisaatioista on havainnut tekoälyyn

liittyvien haavoittuvuuksien lisääntyneen. Nämä havainnot korostavat, että kyberturvallisuuden haasteet eivät rajoitu yksittäisiin teknisiin ongelmiin, vaan heijastuvat laajemmin markkinoiden toimintaan ja riskienhallinnan rakenteisiin. Viimeaikaiset teknologiset mullistukset sekä digitaalisten laitteiden ja palveluiden yleistyminen ovat nostaneet esiin huolta kyberturvallisuudesta. Aiheen ymmärtäminen on siis erityisen tärkeää ja ajankohtaista, sillä nykytalous nojaa yhä vahvemmin teknologiaan ja kyberriskit yleistyvät entisestään. Uutta tutkimustietoa kaivataan siis kyberturvallisuuden vahvistamiseksi.

Tutkielman tavoitteena on analysoida, miten epäsymmetrinen informaatio ja sen aiheuttamat kannustinongelmat vaikuttavat kybervakuutusmarkkinoiden tehokkuuteen. Erityisen tarkastelun kohteena on se, millä tavoin vakuutuksenottajien ja vakuutusyhtiöiden välinen tiedon epätasapaino vääristää riskien hinnoittelua sekä vaikuttaa yritysten kannustimiin investoida tietoturvaan. Näin ollen tutkimus kytkeytyy suoraan kysymykseen siitä, missä määrin kybervakuutusmarkkinat kykenevät tuottamaan tehokkaita lopputuloksia tilanteessa, jossa riskit ovat vaikeasti havaittavia ja vahvasti keskinäisriippuvaisia.

Tutkielma toteutetaan kuvailevana kirjallisuuskatsauksena. Teoreettinen viitekehys rakentuu kahden keskeisen päämies–agentti-ongelman, haitallisen valikoitumisen ja moraalikadon, ympärille. Näiden ilmiöiden avulla pyritään selittämään kybervakuutusmarkkinoiden jatkuvaa kamppailua epävarmuuden ja tehottomuuden kanssa, ja perustelemaan miksi perinteiset vakuutusmallit eivät aina sovellu kyberriskien erityispiirteisiin. Markkinoiden tehottomuuksia havainnollistetaan lisäksi yksinkertaisella peliteoreettisella mallilla, bayesilaisella epäsymmetrisen informaation pelillä. Teoriaosuus pohjautuu erityisesti Akerloafin (1970) sekä Rothschildin ja Stiglitzin (1976) klassisiin malleihin, joita sovelletaan kybervakuutusten kontekstiin. Teorian esittelyssä hyödynnetään etenkin Nicholsonin ja Snyderin (2008) mikrotaloustieteen oppikirjaa. Tutkielmassa tarkasteltu empiirinen tutkimuskirjallisuus tarkastelee, miten nämä teoreettiset ongelmat ilmenevät käytännössä ja millaisia ratkaisuja markkinoilla on kehitetty markkinahäiriöiden ja kannustinongelmien lieventämiseksi.

# 2 Kybervakuutus taloudellisena markkinana

## 2.1 Kyberriskien erityispiirteet

Kyberriskeillä viitataan vaaratilanteisiin, jotka kohdistuvat usein esimerkiksi tietoverkkoihin, digitaalisiin palveluihin tai laitteiden haavoittuvuuksiin. Tällaiset riskit voivat johtaa muun muassa tiedon vääristymiseen tai sen joutumiseen vääriin käsiin (Strupczewski 2021, 1–2). Euroopan unionin kyberturvallisuusviraston (ENISA 2025) tuore uhkakuvakatsaus osoittaa, että digitaalisten heikkouksien hyväksikäyttö on nopeutunut ja hyökkäystaktiikat ovat kehittyneet entistä vaikeammin havaittaviksi. Raportin mukaan kyberuhkien seuraukset ulottuvat yhä laajemmin taloudellisiin ja yhteiskunnallisiin rakenteisiin, mikä korostaa tarvetta huolelliselle ja ennakoivalle riskienhallinnalle.

Kyberriskit eroavat monista muista vakuutettavista riskeistä useiden niille ominaisten piirteiden vuoksi. Ensinnäkin niille on tyypillistä voimakas korreloituneisuus. Yritykset hyödyntävät laajasti samoja ohjelmistoja ja pilvipalveluja, minkä seurauksena yhden haavoittuvuuden hyväksikäyttö voi vaikuttaa samanaikaisesti moniin toimijoihin. Tämä keskinäisriippuvuus voi syntyä esimerkiksi yritysten toimiessa samalla toimialalla (Böhme ym. 2019, 179; 181). Awiszus ym. (2023) huomauttavat, että kyberriskejä ei myöskään voida rajata maantieteellisesti samalla tavoin kuin esimerkiksi luonnonkatastrofeihin liittyviä riskejä. Yhteinen digitaalinen haavoittuvuus voi altistaa miljoonia käyttäjiä samanaikaiselle hyökkäykselle, mikä tekee riskien hajauttamisesta poikkeuksellisen haastavaa.

Kyberriskeihin liittyy lisäksi merkittäviä ulkoisvaikutuksia, jotka voivat olla sekä negatiivisia että positiivisia. Yhden organisaation toiminnalla on sivuvaikutuksia, jotka vaikuttavat muiden kantamaan riskiin. Negatiiviset ulkoisvaikutukset syntyvät, kun yhden toimijan heikko tietoturva lisää muiden altistumista. Kunreutherin ja Healin (2003) interdependent security -malli havainnollistaa tätä vertaamalla kyberturvallisuutta kerrostalon paloturvallisuuteen. Yksittäisen asunnon tulipaloriski riippuu myös naapureiden suojautumistoimista. Tällaisessa ympäristössä syntyy kannustinongelma, jossa yrityksen investointihalukkuus riippuu siitä, miten se odottaa muiden toimijoiden käyttäytyvän. Jos muut laiminlyövät tietoturvaa, myös oma motivaatio investoida voi heikentyä. Positiiviset ulkoisvaikutukset taas syntyvät, kun yhden toimijan tekemät tietoturvatoimet hyödyttävät myös muita. Tämä voi kuitenkin johtaa niin kutsuttuun vapaamatkustajan ongelmaan (engl. free-rider problem), jolloin yritykset pyrkivät hyötymään muiden tekemistä suojatoimista ilman omia investointeja (Varian 2004).

Shetty ym. (2010) osoittavat, että verkon käyttäjät ovat edelleen riippuvaisia toistensa tietoturvasta, vaikka heillä olisi vakuutus. Kun käyttäjät alkavat pitää verkon turvallisuutta itsestäänselvyytenä, he eivät huomioi sitä, että heidän omat heikot suojauksensa voivat vahingoittaa myös muita. Koska vakuutus ei ota näitä ulkoisvaikutuksia huomioon, se voi jopa heikentää yleistä tietoturvaa.

Böhme ym. (2019, 176–181) tuovat esille erityispiirteenä datan niukkuuden. Toisin kuin monista perinteisistä vakuutettavista riskeistä, kybervahingoista on saatavilla vain rajallisesti vertailukelpoista ja kattavaa tietoa. Kaikkia kybertapahtumia ei raportoida ja yhtenäisiä kirjaamiskäytäntöjä ei ole riittävästi. Lisäksi Böhme ym. (2019) nostavat esiin ongelmaa pahentavana piirteenä kyberriskien jatkuvasti muuttuvan ja kehittyvän luonteen. Kyberuhkien jatkuva kehittyminen tekee historiallisesta datasta vain rajallisesti käyttökelpoista tulevien riskien ennustamiseen. Kuru ja Bayraktar (2017, 335) korostavat juuri kyberuhkien satunnaisuutta ja riippumattomuutta yritysten omista toimista. Yritysten on pakko siis tehdä päätöksiä tilanteessa, jossa hyökkäyksen todennäköisyys ja vaikutukset ovat vain osittain tiedossa. Yksittäinen organisaatio ei voi täysin hallita altistumistaan, vaikka sen omat suojaukset olisivat kunnossa. Nämä piirteet tekevät heidän mukaansa riskien arvioinnista poikkeuksellisen haastavaa ja erottavat kyberriskit monista perinteisistä vakuutettavista riskeistä, joissa vahingon todennäköisyys ja vaikutukset ovat paremmin mallinnettavissa.

Kuru ja Bayraktar (2017, 329–331) korostavat lisäksi, että kyberriskien vaikea ennustettavuus yhdistettynä datan niukkuuteen ja yritysten välisiin suuriin eroihin tietoturvatasossa lisäävät vakuutusmarkkinoiden epävarmuutta. Kun vakuutusyhtiöillä ei ole kattavaa tai vertailukelpoista tietoa riskien toteutumisesta, hinnoittelu muuttuu pakostakin epätarkaksi. Tämä johtaa käytännössä siihen, että vakuutusyhtiöt pyrkivät suojaamaan itseään rajoittamalla vakuutusturvan laajuutta ja pitämällä vakuutusrajat matalina. Perinteinen vakuutustoiminta perustuu oletukseen, että riskit ovat toisistaan riippumattomia, hinnoiteltavissa ja hajautettavissa laajan vakuutuskannan kesken. Kyberriskien luonne poikkeaa siis olennaisesti tästä oletuksesta, mikä tekee niistä vaikeasti vakuutettavia perinteisin menetelmin.

## 2.2 Kybervakuutus osana riskienhallintaa

Kybervakuutus eli tietoturvavakuutus on riskienhallintakeino, jonka tarkoituksena on suojata yrityksiä kyberhyökkäysten aiheuttamilta taloudellisilta menetyksiltä. Tällöin verkon käyttäjän riski siirretään vakuutusyhtiölle vakuutusmaksua vastaan (Pal ym. 2014). Kyberhyökkäykset voivat johtua esimerkiksi tietoturvaloukkauksista, järjestelmävioista, tietomurroista tai inhimillisistä virheistä (Tsohou 2023, 740). Vakuutuksen keskeinen tehtävä on mahdollistaa odotettavissa olevan tappion siirtäminen vakuutusyhtiölle, mikä hajauttaa taloudellista riskiä ja lisää liiketoiminnan vakautta

(Gordon ym. 2003, 81). Kybervakuutus kattaa myös joitakin sellaisia aineettomia vahinkoja, joita perinteiset vakuutukset eivät yleensä huomioi. Sen sijaan esimerkiksi valtiolliset kyberoperaatiot ja tietoturvan tahallisen laiminlyönnin seuraukset rajataan usein vakuutusturvan ulkopuolelle. Tsohou ym. (2023) nostavat esille, että kybervakuutusten kattavuuteen liittyy kuitenkin edelleen useita epäselvyyksiä, jotka vaikuttavat vakuutusten käyttökelpoisuuteen riskienhallinnan välineenä. Esimerkiksi se, missä määrin ei-tahalliset virheet tai muut ei-vahingolliset tapahtumat kuuluvat vakuutuksen piiriin.

Kybervakuutustuotteet kattavat tyypillisesti kahdenlaisia riskejä. Ensimmäisen osapuolen riskit kohdistuvat suoraan vakuutettuun, esimerkiksi tietokoneeseen levinneen kiristyshaittaohjelman kautta. Kolmannen osapuolen riskitilanteessa taas korvausvastuu on vakuutuksenottajalla silloin, kun toiselle aiheutuu haittaa suoraan tai epäsuorasti, esimerkiksi asiakastietojen levitessä ulkopuolisille kyseisen yrityksen kautta (Gordon ym. 2003, 83). Volkova ym. (2021) tutkimuksen mukaan yritykset pitävät tietovuotoihin liittyvää vastuuvakuutusta tärkeimpänä osa-alueena, mikä kertoo kolmannen osapuolen riskien korostumisesta. Tämä on linjassa kansainvälisten havaintojen kanssa, joiden mukaan tietomurroista aiheutuvat korvausvaatimukset ovat usein kaikkein kalleimpia.

Perinteisesti vakuutus on nähty sellaisena turvana, joka aktivoituu vasta vahingon tapahduttua. Franke ja Orlando (2025) kuitenkin huomauttavat, että kyberriskien keskinäisriippuvuus ja tilastollisen tiedon niukkuus ovat ohjanneet vakuutusyhtiöitä omaksumaan aiempaa ennakoivamman lähestymistavan. Vakuutusyhtiöt pyrkivät lisäpalveluillaan aktiivisesti edistämään asiakkaidensa tietoturvakäytäntöjä, ja siten samalla parantamaan omaa riskiprofiiliaan. Ennakoiva riskienhallinta voi käytännössä tarkoittaa esimerkiksi tiettyjen turvallisuusvaatimusten sisällyttämistä vakuutusehtoihin tai vakuutusyhtiön tarjoamia tietoturvakoulutuksia ja teknisiä tukipalveluja (Woods ja Simpson 2017, 12). Sopimussuunnittelulla onkin erinomainen mahdollisuus ennaltaehkäistä markkinoiden tehottomuutta. Pal ja Golubchik (2011) toteavat vakuutusmaksujen ja käyttäjien tietoturvainvestointien olevan tiiviisti yhteydessä toisiinsa. Hinnoittelu vaikuttaa siis investointien tasoon, ja investointien taso puolestaan vaikuttaa vakuutusmaksuun. Tämä monimutkaistaa sopimussuunnittelua luonnostaan ja korostaa tarvetta keinoille, jotka ohjaavat vakuutuksenottajia kohti parempia tietoturvakäytäntöjä.

## 2.3 Markkinoiden haasteet – epävarmuus ja markkinahäiriöt

Markkinahäiriöillä tarkoitetaan tilanteita, joissa kilpailulliset markkinat eivät tuota yhteiskunnan kannalta tehokasta lopputulosta. Kybervakuutusmarkkinoilla näitä häiriöitä aiheuttavat erityisesti kannustimien vääristyminen, ulkoisvaikutukset, toimijoiden väliset koordinaatio-ongelmat sekä

tiedon epätasapaino, joka heikentää sekä kysyntää että tarjontaa. Näiden yhteisvaikutuksena yritykset investoivat usein liian vähän kyberturvallisuuteen (Kopp ym. 2017, 17).

Markkinan kehitystä ovat hidastaneet useat toisiinsa kytkeytyvät tekijät. Kybervakuutusten kysyntä oli pitkään vähäistä, sillä yritykset eivät 1990- ja 2000-luvuilla vielä hahmottaneet kyberriskien taloudellista merkitystä tai niiden mahdollisia seurauksia liiketoiminnalle. Varhaisina vuosina korvausvaatimuksia syntyi myös hyvin vähän, mikä loi vakuutusyhtiöille ja asiakkaille harhaanjohtavan käsityksen siitä, että kybervahingot olisivat harvinaisia ja vaikutuksiltaan rajallisia (Böhme ym. 2019, 165). Vakuutusyhtiöitä huolestutti lisäksi mahdollisuus laajoista, useita toimijoita samanaikaisesti vahingoittavista tapahtumista, joita kutsuttiin kyberhurrikaaneiksi (engl. cyber hurricane). Kyberhurrikaani käsitteenä liittyy pitkälti kyberriskien korreloivaan luonteeseen. Yksi haavoittuvuus voi laukaista vähitellen kasvavia tappioita, jotka pahimmillaan horjuttavat koko vakuutuskantaa (Böhme ym. 2019, 166–167). Tämä epävarmuus vaikeutti hinnoittelua ja vähensi vakuutusyhtiöiden halukkuutta tarjota uusia vakuutuksia.

Kybervakuutusmarkkinoilla esiintyy edelleen selvä epätasapaino kysynnän ja tarjonnan välillä. Kysyntä on kasvanut nopeasti, mutta vakuutuskapasiteetti ei ole kasvanut samassa tahdissa (Tsohou ym. 2023, 744). Monet organisaatiot suhtautuvat yhä varovaisesti vakuutuksiin ja suosivat riskien välttämistä riskin siirtämisen sijaan. Arviolta 35 prosenttia yrityksistä kokee nykyisten kybervakuutustensa kattavuuden tai korvausprosessin puutteelliseksi (Tsohou ym. 2023, 744). Luottamus tuotteeseen heikentyy, mikä voi hidastaa kysynnän kasvua. Kybervakuutusten luotettavuuteen liittyvät haasteet heijastuvat myös kansainvälisesti. Joissakin tapauksissa vakuutukset eivät ole korvanneet vahinkoja asiakkaiden odottamalla tavalla, mikä on heikentänyt luottamusta koko tuotekategoriaan. Kun vakuutusten maine kärsii, yritykset suhtautuvat varovaisemmin vakuutusten hankintaan, mikä osaltaan hidastaa markkinoiden kasvua myös maissa, joissa vastaavia kiistoja ei ole esiintynyt (Volkova ym. 2021, 71).

Kysynnän vähäisyyttä selittävät myös tiedolliset ongelmat. Esimerkiksi pk-yrityksissä uskotaan usein virheellisesti, ettei oma organisaatio ole kyberrikollisten kiinnostuksen kohteena. Davis (2025) raportoi, että jopa 82 prosenttia alle 500 työntekijän yrityksistä toimii ilman kybervakuutusta. Myös tietoisuus vakuutustuotteista on puutteellista. Britannian tiede-, innovaatio- ja teknologiaministeriön tutkimuksen mukaan 38 prosenttia yrityksistä ei ollut lainkaan tietoinen kybervakuutuksista, ja 28 prosentilla ei ollut tarpeeksi tietoa muodostaakseen mielipidettä niiden tarpeellisuudesta (Lister 2025).

Pienillä ja kehittyvillä markkinoilla kybervakuutusten tarjontaa rajoittaa usein se, että alan asiantuntijoita on vähän ja osaaminen keskittyy harvoille toimijoille. Tämä hidastaa tuotteiden kehittämistä ja voi johtaa siihen, että vakuutusyhtiöt joutuvat turvautumaan ulkopuoliseen asiantuntija-apuun, mikä taas lisää kustannuksia ja tekee markkinoiden kasvusta hitaampaa. Tällainen tilanne on nähtävissä esimerkiksi Latviassa, jossa markkinoiden rajallinen koko ja osaajapula ovat konkreettisesti hidastaneet kybervakuutusten kehittymistä. Lisäksi kyberriskit vaihtelevat huomattavasti eri toimialojen ja yritysten välillä, minkä vuoksi vakuutussopimukset joudutaan räätälöimään tapauskohtaisesti. Tämä lisää vakuutusyhtiöiden työmäärää ja hidastaa tuotteiden laajamittaista käyttöönottoa. Samalla riskien arviointia vaikeuttaa se, että yritykset eivät aina halua kertoa aiemmista kybervahingoista mainehaittojen pelossa. Kun vahinkotietoa ei jaeta avoimesti, vakuutusyhtiöiden on vaikeampi muodostaa luotettavia riskimalleja ja hinnoitella vakuutuksia oikein (Volkova ym. 2021, 69–71).

Julkisen sektorin rooli korostuu erityisesti markkinoiden alkuvaiheessa. Ilman selkeää kansallista kyberturvallisuusstrategiaa ja valtion tukea vakuutusyhtiöiden riskit pysyvät suurina, mikä voi hidastaa uusien tuotteiden kehittelyä ja markkinoiden vakiintumista (Volkova ym. 2021, 71). Suuret kybervahingot ovat myös kiristäneet markkinoita ja nostaneet hintoja. Viime vuosina markkinat ovat kuitenkin siirtyneet pehmeämpään vaiheeseen. Hinnat ovat laskeneet ja kilpailu lisääntynyt (Lockton 2026). Hintojen vaihtelu heikentää yritysten kykyä suunnitella pitkäaikaisia investointeja kyberturvallisuuteen ja kuvastaa markkinoilla vallitsevaa tiedon epätasapainoa. Vakuutusyhtiöt joutuvat toimimaan puutteellisella tiedolla asiakkaiden riskeistä eivätkä pysty valvomaan vakuutettujen käyttäytymistä, mikä voi johtaa hinnoittelun ja todellisten riskien eriytymiseen. Päästäänkin yhteen kybervakuutusmarkkinoiden keskeisimmistä haasteista, epäsymmetriseen informaatioon, jonka vaikutuksia tarkastellaan seuraavaksi.

# 3 Epäsymmetrisen informaation teoria

## 3.1 Päämies-agentti-ongelma

Epäsymmetrinen informaatio luo markkinoille tilanteita, joissa osapuolten päätöksenteko perustuu epätasapainoiseen tietoon, mikä tekee vuorovaikutuksesta monimutkaista. Tätä asetelmaa kuvataan päämies–agentti-ongelmalla (engl. principal–agent problem), jossa päämies laatii sopimuksen ja agentti hyväksyy sen toimien sopimusehtojen mukaisesti. Agentilla on tyypillisesti hallussaan yksityistä tietoa, ja se toimii omien etujensa mukaisesti, minkä vuoksi osapuolten tavoitteet voivat olla keskenään ristiriidassa. Lisäksi päämiehen mahdollisuudet valvoa agentin toimintaa ovat rajalliset, mikä syventää tiedon epätasapainoa ja vaikeuttaa tehokkaiden sopimusten muodostamista (Nicholson & Snyder 2008, 628).

Jensenin ja Mecklingin (1976, 307–309) mukaan tällaiset ristiriidat ovat väistämätön osa kaikkia sopimussuhteita. Heidän mukaansa agentti ei voi koskaan täysin toimia päämiehen etujen mukaisesti, koska hän kantaa vain osan omien valintojensa seurauksista. Tämä johtaa tilanteeseen, jossa päämiehen on käytettävä resursseja agentin toiminnan seuraamiseen ja rajoittamiseen, ja agentin on puolestaan signaloitava luotettavuuttaan. Koska täydellinen valvonta on joko liian kallista tai teknisesti mahdotonta, hyvinvointitappiota jää aina jonkin verran jäljelle. Näitä valvontaan kuluvia kokonaiskustannuksia kutsutaan agenttikustannuksiksi. Ne syntyvät aina, kun päätösvaltaa siirretään agentille ja joudutaan hyväksymään tehottomuutta, jota ei voida poistaa ilman kohtuuttomia kustannuksia. Lopputulos on yhteiskunnan kannalta tehoton eikä markkinat eivät saavuta optimaalista tasoa.

Vakuutusmarkkinoilla vakuutusyhtiö toimii päämiehenä ja vakuutuksenottaja agenttina. Vakuutusyhtiö kantaa taloudellisen riskin ja vakuutuksenottaja vastaa omista suojatoimistaan. Koska vakuutusyhtiö ei käytännössä pysty seuraamaan vakuutetun toimintaa reaaliajassa, markkinoille syntyy väistämättä tiedon epätasapainoa. Päämies-agentti-teoria jaetaan kahteen keskeiseen malliin: piilotetun tiedon malliin (engl. hidden information), joka tunnetaan haitallisen valikoitumisen ilmiönä, sekä piilotetun toiminnan malliin (engl. hidden action), joka kuvaa moraalikatoa (Nicholson & Snyder 2008, 629). Jensenin ja Mecklingin näkökulmasta nämä ovat juuri niitä tekijöitä, jotka synnyttävät agenttikustannuksia ja heikentävät sopimusten tehokkuutta. Nämä kaksi ilmiötä muodostavat keskeisimmät kybervakuutusmarkkinoiden informaatio-ongelmat, jotka ovat tutkielmassa täten keskiössä.

## 3.2 Haitallinen valikoituminen

Haitallisella valikoitumisella (engl. adverse selection) tarkoitetaan piilotetusta tiedosta johtuvaa markkinahäiriötä, jossa epäsymmetrinen informaatio estää markkinoita saavuttamasta tehokasta lopputulosta. Ilmiö syntyy, kun toisella osapuolella on kaupankäynnissä enemmän tietoa hyödykkeen tai riskin laadusta kuin toisella (Friberg 2025, 266–267). Akerloafin (1970) klassinen käytettyjen autojen eli ”sitruunojen” esimerkki havainnollistaa käsitettä. Kun ostajat eivät pysty erottamaan korkealaatuisia autoja heikkolaatuisista, he tarjoavat keskimääräisiin odotuksiin perustuvaa hintaa, mikä ajaa korkealaatuisten tuotteiden myyjät pois markkinoilta. Hyvien autojen myyjät pitävät tätä hintaa liian alhaisena ja vetäytyvät markkinoilta, jolloin tarjonta koostuu lopulta vain huonolaatuisista autoista. Tämän seurauksena molempia osapuolia hyödyttävät kaupat jäävät toteutumatta puutteellisen tiedon takia.

Vakuutussektorilla haitallinen valikoituminen ilmenee tilanteissa, joissa vakuutuksenottajilla on vakuutusyhtiöitä parempi käsitys omasta riskitasostaan. Vakuutusyhtiöt vastaavat tiedon epäsymmetriaan hinnoittelemalla vakuutukset keskimääräiseen riskiin perustuen. Tämä hinnoittelu houkuttelee erityisesti korkean riskin asiakkaita, mutta on liian kallis matalan riskin asiakkaille. Vakuutettujen riskiprofiilin heikentyessä vakuutusyhtiöiden on korotettava vakuutusmaksuja, mikä taas voi pahentaa haitallista valikoitumista (Friberg 2025, 269). Tämä voi johtaa niin kutsuttuun vakuutusmarkkinoiden kuolemankierteeseen (engl. insurance death spiral), jossa yhä useampi matalan riskin toimija jättäytyy pois vakuutusmarkkinoilta ja markkinat voivat lopulta jopa romahtaa (Akerlof 1970, 490; Nicholson & Snyder 2008, 658).

Rothschildin ja Stiglitzin (1976) mallissa käsitellään informaatio-ongelmaa kilpailullisilla vakuutusmarkkinoilla, joilla on kahdenlaisia kuluttajia. Kuluttajat jakautuvat matalan riskin kuluttajiin, joiden tappion todennäköisyys on $\pi_L$ ja korkean riskin kuluttajiin, joiden tappion todennäköisyys on $\pi_H$, missä $\pi_H > \pi_L$. Merkitään korkean riskin yksilöiden muodostamaa osuutta $\lambda$. Kuluttajat tuntevat oman tyyppinsä, mutta vakuutusyhtiöt joutuvat toimimaan odotusarvon mukaan ja hinnoittelemaan vakuutukset keskimääräisen riskin $\bar{\pi}$ perusteella:

$$\bar{\pi} = \lambda\pi_H + (1 - \lambda)\pi_L.$$

Malli olettaa molempien kuluttajatyyppien riskinkarttajia eli välttävän riskiä ja arvostavan turvallisuutta. Lisäksi kuluttajilla on sama hyötyfunktio $U(W)$. Vakuutuksenantajat taas ovat riskineutraaleja ja toimivat kilpailevilla markkinoilla, minkä vuoksi odotettu voitto tasapainotilanteessa on nolla (Rothschild & Stiglitz 1976, 634). Toisin sanoen kilpailu painaa hinnan niin alas, että

vakuutusyhtiöt kattavat vain korvaukset ja muut kulut, mutta eivät tee taloudellista ylijäämää. Kuluttajan saama odotettu hyöty määräytyy tällöin varallisuuksien perusteella:

$$EU = (1 - \pi)U(W_1) + \pi U(W_2),$$

missä $W_1$ on varallisuus, jos vahinkoa ei tapahdu. Varallisuus lasketaan silloin alkuperäisvarallisuuden $W_0$ ja vakuutusmaksun $p$ erotuksena. $W_2$ on kuluttajan varallisuus vahinkotilanteissa, jolloin alkuperäisestä varallisuudesta $W_0$ vähennetään vakuutusmaksu $p$ ja vahingon suuruus $l$, minkä jälkeen siihen lisätään saatu korvausmaksu $x$. (Nicholson & Snyder 2008; 638, 651, 654) Koska vakuutussopimus koostuu vakuutusmaksusta $p$ ja vakuutusturvasta $x$, vakuuttajan odotettu voitto lasketaan:

$$EV = p - \pi x.$$

Jos vakuutusyhtiö pystyisi havaitsemaan vakuutettujen riskityypit, saavutettaisiin niin kutsuttu paras ratkaisu (engl. first-best), jossa korkean riskin toimijoille tarjottaisiin täysi vakuutus hinnalla $p_H = \pi_H l$ ja matalan riskin toimijoille hinnalla $p_L = \pi_L l$. Toisin sanoen, vakuutusyhtiö hinnoittelisi maksut siten, ettei mikään ryhmä jää voitolle vakuutuksen myötä (Nicholson & Snyder 2008, 650). Käytännössä tämä ei kuitenkaan ole mahdollista, koska vakuutusyhtiöt eivät pysty erottamaan riskityyppejä toisistaan. Tämän vuoksi markkinoilla toteutuu toiseksi paras ratkaisu (engl. second-best), jossa sopimusvalikoima suunnitellaan niin, että matalan riskin asiakkaat hyväksyvät osittaisen vakuutuksen kuten omavastuun, osoittaakseen oman riskityyppinsä ja saadakseen alhaisemman vakuutusmaksun (Rothschild & Stiglitz 1976, 637–638). Omavastuu toimii ikään kuin karsimisvälineenä, sillä korkean riskin asiakkaat arvostavat kattavaa turvaa eivätkä siten ole valmiita hyväksymään omavastuuta vastineeksi alemmasta hinnasta (Rothschild & Stiglitz 1976, 637–638).

Kybervakuutuksen yhteydessä Rothschildin ja Stiglitzin mallin oletus vakuutuksenottajan tiedollisesta etulyöntiasemasta ei kuitenkaan ole yksiselitteinen. Yrityksellä on yleensä parempi käsitys omista järjestelmistään ja toimintatavoistaan, mutta kyberturvallisuuden erityispiirteet heikentävät tätä oletusta. Joskus on epävarmaa, tunnistavatko esimerkiksi pk-yritykset itse käyttävänsä vanhentuneita järjestelmiä tai toimivansa tavalla, joka altistaa ne kyberuhille. Henkivakuutukseen verrattuna, jossa yksilö tuntee omat elintapansa, kyberriskissä vakuutuksenottajan tiedollinen etumatka voi olla huomattavasti vähäisempi. Yritykset voivat myös yliarvioida oman turvallisuustasonsa, mikä johtaa tilanteeseen, jossa ne eivät edes pyri hyödyntämään mahdollista tiedollista etuaan, koska niillä ei ole realistista käsitystä omista haavoittuvuuksistaan (Nieuwesteeg ym. 2018, 18).

Nieuwesteeg ym. (2018, 21) tuovat esille vähemmälle huomiolle jääneen kannustinongelman, käänteisen haitallisen valikoitumisen (engl. reverse adverse selection/inverse adverse selection). Tässä asetelmassa tiedon epäsymmetria toimii vakuutusyhtiön eduksi. Vakuutusyhtiöillä on käytössään tilastollista dataa vahingoista ja pieniä yrityksiä paremmat valmiudet ymmärtämään kyberriskien teknistä toimintaa. Tällainen epäsymmetria voi johtaa strategiseen toimintaan, jossa vakuutusyhtiöt tietoisesti ylläpitävät Akerlofin (1970) kuvaamia ”sitruunoiden markkinoita”. Vakuutusehdot voidaan laatia monimutkaisiksi, jolloin asiantuntematon yritys ei kykene vertailemaan tuotteita tai arvioimaan, mitä turvaa se tosiasiassa tarvitsee. Tämä antaa vakuutusyhtiöille mahdollisuuden hyödyntää tiedollista ylivoimaansa ja tarjota heikompilaatuisia tuotteita korkeampaan hintaan. Se ylläpitää markkinoiden tehottomuutta ja heikentää niiden kykyä ohjata yrityksiä parempaan tietoturvaan. Käänteisen haitallisen valikoitumisen ehkäiseminen edellyttääkin läpinäkyvyyttä. Markkinoiden on mahdollista lähestyä yhteiskunnallisesti toivottua tasapainoa vain silloin, kun vakuutusehdot ja rajoitukset ovat selkeitä ja yksiselitteisiä.

### 3.3 Moraalikato

Moraalikato (engl. moral hazard) on yksi päämies–agentti-teorian keskeisimmistä piilotetun toiminnan ilmiöistä, jonka seurauksena markkinoilla voi syntyä taloudellista tehottomuutta. Nicholson ja Snyder (2008, 638) kuvaavat moraalikatoa tilanteena, jossa vakuutusturva vaikuttaa yksilön varotoimiin ja muuttaa tappion todennäköisyyttä tai suuruutta. Agentin käyttäytyminen voi muuttua sopimuksen solmimisen jälkeen, kun taloudellisesta riskistä osa siirtyy päämiehelle (Friberg 2025, 266). Vakuutusturva saattaa siis heikentää agentin kannustimia toimia varovaisesti (Holmström 1979; Nicholson & Snyder 2008, 638). Vakuutusyhtiön on liian kallista valvoa täydellisesti vakuutetun käyttäytymistä, minkä vuoksi vakuutettu pystyy harjoittamaan näitä piilotettuja toimia (Nieuwesteeg ym. 2018, 22).

Moraalikato voidaan jakaa kahteen erilliseen muotoon. Ex-ante-moraalikato ilmenee ennen vahingon syntymistä. Vakuutettu voi tällöin laiminlyödä ennaltaehkäiseviä tietoturvavelvoitteitaan, koska ei itse kanna täyttä taloudellista vastuuta mahdollisista vahingoista. Zhang ja Zhu (2019, 11) kutsuvat tätä ilmiötä riskikompensaatioksi (engl. risk compensation). Kybervakuutusmarkkinoilla tämä voi näkyä esimerkiksi siinä, että yritys jättää tekemättä kriittisiä tietoturvapäivityksiä. Ex-post-moraalikato puolestaan tapahtuu vahingon jälkeen, ennen kuin vakuutusyhtiö maksaa korvauksen. Jos yritys tietää kustannusten korvattavan, se ei välttämättä tee parastaan minimoidakseen vahingon laajuutta tai nopeuttaakseen tappiosta toipumista (Zhang & Zhu 2019).

Nicholson ja Snyder (2008, 638) tarkastelevat tilannetta, jossa vakuutusyhtiö voisi ideaalitapauksessa valvoa vakuutetun varotoimenpiteitä $e$ täydellisesti. Tällöin vakuutusyhtiö voisi asettaa $e$:n ja sopimusehdot $x$ ja $p$ maksimoidakseen odotetun voittonsa sillä osallistumisrajoitteella, että yksilö hyväksyy sopimuksen:

$$(1-\pi)U(W_1) + \pi U(W_2) \geq \overline{U},$$

missä $\overline{U}$ on suurin hyöty, jonka yksilö voi saavuttaa ilman vakuutusta. Vakuutusyhtiö korottaa vakuutusmaksua, kunnes rajoituksen molemmat puolet ovat yhtä suuret. Tämä optimointiongelma voidaan ratkaista Lagrangen funktiota käyttäen:

$$\mathcal{L} = p - \pi x + \lambda(1-\pi)U(W_1) + \pi U(W_2) - \overline{U}.$$

Ensimmäisen asteen ehdot johtavat ratkaisuun, jossa optimaalinen vakuutusturva on täysi korvaus eli $x = l$. Nicholson ja Snyder (2008, 639) selittävät optimointiongelman avulla, että optimaalisessa tilanteessa suojaavan toimenpiteen yhteiskunnallinen rajahyöty vastaa sen rajakustannusta $\frac{\partial \pi}{\partial e} l = 1$. Rationaalisesti toimiva eli hyötyään maksimoiva henkilö panostaa riskin vähentämiseen siihen asti, että lisävarotoimien rajahyöty vastaa niiden rajakustannusta (Nicholson & Snyder 2008, 638).

Käytännössä vakuutusyhtiö ei voi kuitenkaan valvoa suojatoimenpidettä $e$, jolloin sitä ei voida sisällyttää suoraan sopimuksessa. Tällöin kyseessä on toiseksi paras ratkaisu, jossa sopimukseen lisätään kannustimien yhteensopivuusrajoite. Rajoite varmistaa, että agentti valitsee itselleen parhaan mahdollisen suojatoimitason. Toisin kuin ensimmäisen parhaan ratkaisun tapauksessa, toiseksi paras sopimus ei yleensä sisällä täyttä vakuutusturvaa $x = l$. Osoitetaan osittaisen vakuutusturvan kannattavuus matemaattisesti mallintamalla. Täydessä vakuutuksessa varallisuustasot olisivat $W_1 = W_2$, jolloin agentin odotettu hyöty olisi:

$$U(W_0 - e - p).$$

Odotettu hyöty voidaan maksimoida valitsemalla mahdollisimman pieni suojatoimenpiteen taso eli $e = 0$. Tämä osoittaa, että kannustimien ja vakuutusturvan välinen suhde on moraalikadon ydinongelma. Vakuuttajan on löydettävä tasapaino riskille altistamisen ja vakuutusturvan välillä. Liian kattava vakuutus heikentää varotoimia, kun taas liian rajoitettu vakuutus vähentää vakuutuksenottajan halukkuutta maksaa vakuutusmaksuja (Nicholson & Snyder 2008, 639–640).

## 3.4 Bayesilainen epäsymmetrisen informaation peli

Perinteinen haitallisen valikoitumisen ja moraalikadon analyysi keskittyy kahdenväliseen suhteeseen vakuutusyhtiön ja vakuutuksenottajan välillä. Kyberympäristössä tilanne on kuitenkin olennaisesti monimutkaisempi, sillä yritykset toimivat verkottuneessa ympäristössä, jossa päätökset ovat keskinäisriippuvaisia. Peliteoria tarjoaa välineen kuvata tätä strategista vuorovaikutusta sekä sitä, miten epäsymmetrinen informaatio vaikuttaa vakuutusmarkkinoiden dynamiikkaan (Do ym. 2017).

Peliä, jossa ainakin yksi pelaaja ei tunne toisen pelaajan aiempia siirtoja, kutsutaan epätäydellisen tiedon peliksi. Bayesilaisissa epäsymmetrisen informaation peleissä (engl. Bayesian games of incomplete information) pelaajilla on puutteellista tietoa toistensa strategioista ja voitoista, minkä vuoksi he määrittävät muille pelaajille “tyypin” pelin alussa. Vakuutusmarkkinoilla pelaajan ”tyyppi” voi tarkoittaa esimerkiksi todellista riskitasoa tai kykyä ehkäistä tappioita (Nicholson & Snyder 2008, 269). Tyyppien käyttöönotto mahdollistaa sen, että yksityinen tieto voidaan sisällyttää suoraan pelin strategiseen rakenteeseen sen sijaan, että sitä käsiteltäisiin ulkoisena haittana. Bayesilaiset pelit tarjoavat jäsennellyn tavan kuvata, miten yritykset mukauttavat investointistrategioitaan ympäristöissä, joissa tietoturvaan liittyvät ulkoisvaikutukset ovat merkittäviä. (Roy ym. 2010, 2).

Kahden pelaajan pelissä pelaaja 1 kuuluu johonkin tyyppijoukkoon $t \in T = \{t_1, \dots, t_k\}$ todennäköisyydellä Pr ( $t_k$), ja hän valitsee strategiansa oman tyyppinsä perusteella. Pelaaja 2 ei havaitse pelaajan 1 tyyppiä, vaan muodostaa uskomuksia pelaajan 1 tyypistä havaittujen valintojen perusteella ja valitsee strategiansa näiden odotusten pohjalta (Nicholson & Snyder 2008, 269). Nash-tasapaino (engl. Nash equilibrium) tarkoittaa strategiaprofiilia, jossa kenenkään pelaajan ei kannata vaihtaa strategiaansa, kunhan kaikki muut pelaajat noudattavat määrättyä strategiaa (Roy ym. 2010, 3). Tätä käsitettä voidaan soveltaa myös vakuutusmarkkinoihin, joissa vallitsee tiedon epäsymmetria. Tasapainossa jokaisen tyypin on valittava sopimus, joka maksimoi hänen hyötynsä ottaen huomioon riskitason ja vakuutusyhtiön asettamat ehdot. Samalla vakuutusyhtiön on valittava strategia, joka maksimoi oman odotetun voittonsa sen perusteella, millaisia uskomuksia sillä on vakuutettujen riskityyppien jakaumasta (Nicholson & Snyder 2008, 269–270).

Tarkastellaan nyt kahden yrityksen A ja B investointipeliä. Molemmat yritykset tuntevat oman tietoturvatasonsa, mutta eivät toisen. Yritykset voivat joko investoida tietoturvaan tai jättää investoimatta. Investointi tuottaa korkean tietoturvan (K), ja investoinnin laiminlyönti matalan tietoturvan (M). Taulukossa 1 on listattu pelin mahdolliset tulokset:

**Taulukko 1**

Yksinkertainen kahden yrityksen investointipeli

| | Yritys B investoi | Yritys B ei investoi |
|---|---|---|
| Yritys A investoi | (K, K) | (K, M) |
| Yritys A ei investoi | (M, K) | (M, M) |

Täydellisen informaation tilanteessa yritykset voisivat koordinoida toimintansa ja päätyä molempia hyödyttävään ratkaisuun, jossa molemmat investoivat. Epäsymmetrinen informaatio muuttaa kuitenkin pelin luonnetta merkittävästi. Huomataan sama ilmiö, jonka Nagurney ja Nagurney (2015) nostavat esille. Epävarmuus toisen investointipäätöksestä luo kannustimia vapaamatkustamiseen. Yritys, joka uskoo muiden investoivan, voi jättää itse investoimatta ja silti hyötyä muiden toimista (Varian 2004). Taulukon 1 investointipeli osoittaa, että epävarmuus saattaa johtaa epäsymmetrisiin lopputuloksiin, joissa vain toinen kantaa investoinnista kertyvät kustannukset. Molemmat pelaajat kuitenkin hyötyvät keskimääräisen investointitason noustessa, koska markkinat reagoivat vain keskiarvoon. Jos molemmat pelaavat varman päälle ja jättävät investoimatta, lopputuloksena on matala tietoturva ja kaikkien kannalta heikompi tilanne.

Bayesilaisten pelien soveltuvuutta kybervakuutusmarkkinoille havainnollistaa Panda ym. (2019), jotka mallintavat bayesilaisen auditointipelin vakuutusyhtiön ja vakuutuksenottajan välillä. Mallissan vakuutuksenottaja päättää esimerkiksi hakeeko hän ilmoittamaansa tietoturvatasoon perustuvaa vakuutusmaksualennusta vai ei, ja vakuutusyhtiö päättää suorittaako se auditoinnin mahdollisen vahingon jälkeen. Jos auditointi paljastaa, ettei vakuutuksenottaja ole ollut rehellinen tietoturvastaan, vakuutusyhtiö voi kieltäytyä korvauksesta (Panda ym. 2019, 4–6). Pelin ratkaisu perustuu täydelliseen bayesilaiseen tasapainoon (engl. perfect Bayesian equilibrium), jossa kummankaan osapuolen ei kannata muuttaa strategiaansa, ja vakuutusyhtiön uskomukset vakuutuksenottajan riskitasosta ovat yhteensopivia havaittujen valintojen kanssa. Panda ym. (2019) osoittavat, että juuri nämä ennakkouskomukset määrittävät vakuutusyhtiön optimaalisen strategian. Kun riskitasoa koskeva ennakkokäsitys ylittää tietyn kynnysarvon, auditoinnin tekemättä jättäminen on rationaalista. Tutkimuksen mukaan peliteoreettiset menetelmät tarjoavat tehokkaamman päätöksentekopohjan kybervakuutusmarkkinoilla kuin intuitioon perustuvat arviot (Panda ym. 2019, 9–12).

# 4 Käytännön havainnot kybervakuutusmarkkinoista

## 4.1 Epäsymmetrisen informaation ilmeneminen

Kybervakuutusmarkkinoilla toimijoilla on usein eritasoista tietoa riskeistä, ja tämä epätasapaino heijastuu markkinoiden toimintaan teorian ennustamalla tavalla, mutta ilmiölle löytyy myös käytännön näyttöä. Vaikka empiirinen tutkimus kybervakuutuksista ja etenkin niihin liittyvästä epäsymmetrisestä informaatiosta, on vielä rajallista, olemassa oleva aineisto tarjoaa jo selkeitä viitteitä siitä, miten kannustinongelmat ja tiedon epätasainen jakautuminen muovaavat markkinoiden toimintaa.

Ning (2025) tarkastelee haitallista valikoitumista Yhdysvaltain kybervakuutusmarkkinoilla yhdistämällä yritysten vakuutusostotiedot, ulkoiset kyberturvallisuuspisteytykset ja vakuutusta hakevien yritysten itsearviointikyselyt. Haitallinen valikoituminen ilmenee tutkimuksessa kolmella tavalla. Ensinnäkin yritykset, joilla on matalammat turvallisuuspisteet ja tuoreita kyberongelmia, ostavat todennäköisemmin vakuutuksen. Toiseksi vakuutusyhtiöt eivät hinnoittele vakuutusmaksuja näiden riskisignaalien perusteella, vaan käyttävät seulonnassaan itsearviointikyselyä, joka on heikommin yhteydessä todellisiin kybertapahtumiin. Tämän seurauksena vakuutuskantaan valikoituu riskialttiimpia yrityksiä ilman, että vakuutusmaksut heijastavat kohonnutta riskitasoa. Kolmanneksi Ning hyödyntää vuoden 2017 verouudistusta ulkoisena hintashokkina ja osoittaa difference-in-differences-menetelmällä, että hinnannousun myötä matalamman riskin vakuutuksenottajat poistuivat markkinoilta ja keskimääräiset korvauskustannukset nousivat kuten haitallisen valikoitumisen teoria ennustaa. Riskinhallinta siirtyy näin hinnasta enemmin kattavuuden rajoittamiseen, ja vakuutusyhtiöt asettavat tiukempia korvauskattoja etenkin suurille asiakkaille.

Näyttö haitallisesta valikoitumisesta on kuitenkin ristiriitaista. Branley-Bell ym. (2021) tarjoavat vasta-argumentin Ningin tuloksille hyödyntämällä laajaa käyttäytymiskokeiden aineistoa. Heidän tutkimuksensa perustuu 4 800 osallistujan laboratoriokokeeseen, jossa mitattiin yksilöiden riskiasenteita sekä halukkuutta investoida tietoturvatoimiin ja hankkia kybervakuutusta. Osallistujille annettiin mahdollisuus valita eritasoisia tietoturvatoimia ja vakuutusturvaa, jolloin valintoja voitiin tarkastella ilman todellisten vakuutusmarkkinoiden hinnoittelun tai sopimusehtojen vaikutusta. Tulokset osoittavat, että riskihakuiset yksilöt olivat vähemmän halukkaita sekä investoimaan edistyneisiin tietoturvatoimiin että ostamaan kattavaa kybervakuutusta. Tämä viittaa siihen, että juuri kaikkein riskialttiimmat toimijat voivat jäädä vakuutusmarkkinoiden ulkopuolelle. Haitallista

valikoitumista ei siis huomata ainakaan yksilötason käyttäytymisessä. Havainto haastaa perinteisen teoreettisen oletuksen, jonka mukaan markkinoille valikoituisi erityisesti korkean riskin asiakkaita.

Moraalikadon osalta empiirinen näyttö on yllättävän yhtenäistä ja poikkeaa selvästi teoreettisista ennusteista. Gómez ym. (2025) tutkivat ilmiötä laajassa verkkopohjaisessa talouskokeessa, johon osallistui 4 800 henkilöä neljästä Euroopan maasta. Kokeessa osallistujat saivat valita eritasoisia tietoturvatoimia ja vakuutusturvaa, minkä jälkeen heidän todellista käyttäytymistään mitattiin erillisessä verkkotehtävässä. Tulokset osoittavat, ettei vakuutuksen hankkiminen lisännyt riskinottoa. Vakuutetut eivät toimineet huolimattomammin, vaan heidän tietoturvakäytäntönsä pysyivät ennallaan tai jopa paranivat. Samoja havaintoja raportoitiin Branley-Bell ym. (2021) tutkimuksessa. Heidän kokeensa perusteella vakuutuksen hankkiminen ei ollut yhteydessä riskialttiimpaan toimintaan, vaan vakuutetut tekivät nimenomaan keskimäärin vahvempia kyberturvavalintoja. Molemmat tutkimukset viittaavat siihen, että vakuutuksen ottaminen ei automaattisesti johda moraalikatoon, vaan yksilöt voivat jopa lisätä suojautumistaan vakuutusturvan rinnalla.

Myös Ning (2025) tutki muuttuuko yritysten kyberriskikäyttäytyminen vakuutuksen hankkimisen jälkeen. Menetelmänä hän käytti porrastettua difference-in-differences-mallia sekä yritysten yhteen sovittamista taustamuuttujien perusteella. Vakuutuksen ostaneet yritykset ja vertailuryhmän yritykset yhdistettiin liikevaihdon, henkilöstömäärän, omistusrakenteen, toimialan ja sijaintiosavaltion perusteella vuotta ennen vakuutuksen hankintaa. Difference-in-differences-analyysi hyödynsi vakuutuksen oston ajoituksen vaihtelua eri yritysten välillä. Ningin tulokset eivät myöskään tue moraalikadon esiintymistä. Vakuutuksen hankkiminen ei johtanut turvallisuuspisteiden laskuun, kyberhyökkäysten todennäköisyyden kasvuun eikä muuttanut yritysten käyttäytymistä.

Näiden empiiristen tutkimusten lisäksi alan toimijoiden näkemykset poikkeavat akateemisesta oletuksesta, jonka mukaan moraalikato olisi yksi merkittävimmistä kyberriskien vakuutettavuuden esteistä. Kurun ja Bayraktarin (2017) toteuttama asiantuntijakysely osoittaa, että käytännön toimijat eivät pidä moraalikatoa keskeisenä ongelmana. Likert-asteikolla (1–5) moraalikato sai kyselyssä keskiarvon noin 3,0, mikä oli yksi alhaisimmista arvioista. Samalle tasolle sijoittui rajallinen vakuutuskapasiteetti, joka näkyy korkeina omavastuina ja matalina korvausrajoina. Sen sijaan mallinnuksen ja hinnoittelun epävarmuus koettiin huomattavasti suuremmiksi haasteiksi.

Moraalikato ei siis näyttäydy kybervakuutusmarkkinoilla perinteisen teorian ennustamalla tavalla. Yksi mahdollinen selitys tälle on se, että vakuutussopimuksiin sisältyvät turvallisuusvaatimukset rajoittavat yritysten tietoista riskikäyttäytymistä. Lisäksi kyberhyökkäysten ulkoinen ja vaikeasti ennakoitava luonne vähentää mahdollisuuksia tahalliseen riskinottoon. Hyökkäykset kohdistuvat

yrityksiin usein niiden omasta toiminnasta riippumatta. Eli varovainen toiminta ei aina takaa sitä, ettei joudu hyökkäyksen kohteeksi.

## 4.2 Markkinahäiriöiden ehkäisy

Kybervakuutusmarkkinoiden sääntelyä koskevassa kirjallisuudessa käydään edelleen aktiivista keskustelua siitä, kumpi lähestymistapa ehkäisee markkinahäiriöitä tehokkaammin ennakkosääntely (ex ante) vai jälkikäteisvastuu (ex post). Ennakkosääntely pyrkii estämään hyökkäykset jo ennen vahinkoa, kun taas jälkikäteisvastuu nojaa siihen, että oikeudelliset seuraamukset kannustavat yrityksiä investoimaan tietoturvaan. Molemmilla lähestymistavoilla on kuitenkin rakenteellisia rajoitteita. Sääntely voi hidastaa innovaatiota, ja jälkikäteinen vastuun kohdentaminen on usein vaikeaa monimutkaisissa kyberympäristöissä (Kopp ym. 2017, 17). Keskustelu ei siis koske vain sääntelyn määrää, vaan sitä, miten epävarmuutta voidaan hallita ilman, että markkinoiden toiminta kärsii.

Ennakkosääntelyn puolesta puhuu erityisesti se, että yritykset eivät aina ota huomioon kyberhäiriöiden kaikkia yhteiskunnallisia kustannuksia omiin päätöksiinsä. Kopp ym. (2017, 9–12) osoittavat, että verkottuneilla aloilla kybertapahtumat voivat aiheuttaa systeemisiä ulkoisvaikutuksia, mikä johtaa ali-investointeihin. Tässä tilanteessa epäsymmetrisen informaation lieventäminen nousee keskeiseksi tavoitteeksi. Yksi tehokkaimmista mekanismeista on signalointi. Paremmin informoitu osapuoli lähettää uskottavan merkin omasta riskitasostaan. Kybervakuutusmarkkinoilla tämä voi tarkoittaa auditointeja tai sertifikaatteja, joita heikosti suojatut yritykset eivät ole valmiita hankkimaan. Uskottavat signaalit voivat siten vähentää haitallista valikoitumista ja parantaa vakuutusyhtiöiden riskinarviointia ilman raskasta sääntelyä (Friberg 2025, 272–274).

Khalilin ym. (2017) tutkimus osoittaa, että vakuutusyhtiöiden suorittama ennakkotarkastus (engl. pre-screening) voi ehkäistä moraalikatoa. Kun vakuutusmaksut sidotaan havaittuun tietoturvatasoon, yrityksillä on kannustin ylläpitää korkeampaa suojaustasoa myös vakuutuksen saamisen jälkeen. Ennakkotarkastus voi lisäksi parantaa koko verkon turvallisuutta verrattuna tilanteeseen, jossa vakuutusta ei ole tai jossa tarkastusta ei hyödynnetä. Markkinahäiriöiden lieventämisen kannalta keskeistä on myös riskinarvioinnin tarkkuus. Kuru ja Bayraktar (2017) korostavat, että vakuutusten hinnoittelu tulisi sitoa todelliseen riskitasoon, jolloin vakuutus toimii osana laajempaa tietoturvainvestointia. Tällöin vakuutus ei ainoastaan siirrä riskiä, vaan myös vahvistaa koko verkoston turvallisuutta ja tuottaa positiivisia hyvinvointivaikutuksia.

Jälkikäteiset mekanismit toimivat puolestaan vain silloin, kun vastuu on sekä ennakoitavissa että todistettavissa. Hui ym. (2024) osoittavat, että kybervakuutus muuntaa oikeudelliset riskit

mitattaviksi vakuutusmaksuiksi ja sisältää ehtoja, jotka ohjaavat asiakkaita ennaltaehkäiseviin toimiin. Korvaus maksetaan vain, jos asiakas täyttää tietyt tietoturvavaatimukset, mikä tekee vakuutuksesta myös valvontaa täydentävän kannustinjärjestelmän. Näin jälkikäteinen korvausmekanismi toimii samalla moraalikatoa hillitsevänä keinona (Hui ym. 2024, 3–5). Arce ym. (2024) kuvaavat menetelmän, jossa vakuuttajat hoitavat vahinkojen jälkihoidon keskitetysti asiantuntijapoolien avulla. Poolit koostuvat etukäteen valituista neuvonantajista, ja vahingon sattuessa vakuutettu ohjataan suoraan näiden palveluiden piiriin. Järjestely siirtää osan käytännön vastuusta vakuuttajalle, joka koordinoi jälkihoitoa ja varmistaa, että toimet etenevät nopeasti ja selkeästi (Arce ym. 2024, 2–5).

Viimeaikainen tutkimus viittaa myös siihen, että vahvemmat kansalliset kyberturvallisuusjärjestelyt voivat vahvistaa sijoittajien luottamusta. Bosen ym. (2025) analyysi 45 930 yritys–vuosihavainnosta 60 maasta osoittaa, että maissa, joissa kansalliset kyberturvallisuusjärjestelyt ovat vahvoja, yritykset saavat keskimäärin korkeampia arvostuksia. Vaikutus korostuu erityisesti korkean kyberriskin ympäristöissä ja on riippumaton siitä, millaisista kyberuhista on kyse (Bose ym. 2025, 2–4). Markkinahäiriöitä voidaan siis lieventää myös makrotason toimilla, jotka vähentävät epävarmuutta sijoittajien ja vakuuttajien näkökulmasta.

## 4.3 Maakohtaiset tutkimustulokset

Kyberriskien jakautuminen on globaalisti epätasaista. Biener ym. (2014) mukaan 51,9 prosenttia kaikista kyberturvallisuusongelmista kohdistuu Pohjois-Amerikkaan, kun Euroopan osuus on 23,2 prosenttia ja Aasian osuus 18,1 prosenttia. Alueellinen jakautuminen ei kuitenkaan suoraan selitä tappioiden suuruutta. Pohjois-Amerikan yritykset nimittäin kokevat eniten kyberriskitapauksia, mutta niiden keskimääräiset vahingot ovat pienempiä kuin Euroopassa tai Aasiassa. Taustalla vaikuttaa Pohjois-Amerikan käytössä olevat laajemmat ja kehittyneemmät kyberturvallisuuskäytännöt. Globaali epätasapaino toimii luontevana lähtökohtana yksittäisten maiden kybervakuutusmarkkinoiden kehityksen tarkastelulle. Tarkastelu etenee kehittyvistä ja vielä muotoutuvista Malesian markkinoista pieniin mutta edistyneisiin Ruotsin markkinoihin ja viimeiseksi suuriin ja kypsiin Yhdysvaltojen markkinoihin.

### 4.3.1 Malesia

Kybervakuutus on Kaakkois-Aasiassa edelleen suhteellisen uusi ilmiö, ja sen käyttöönottoon liittyy huomattavaa epävarmuutta myös Malesiassa (Abdul Rahman ym. 2022, 46). Vaikka kybervakuutusten käyttö on kasvanut teollisuusmaissa, niitä aliarvostetaan edelleen merkittävästi kehittyvissä

talouksissa. Malesia muodostaa tässä suhteessa kiinnostavan poikkeuksen. Maa oli vuonna 2020 kymmenen eniten kyberturvallisuuteen sitoutuneen valtion joukossa, mutta kybervakuutusten käyttöaste on silti erittäin alhainen (Abdul Hamid 2022, 1). Malesiaan keskittyvät empiiriset tutkimukset tarjoavatkin kattavan kuvan siitä, miten markkinahäiriöt ilmenevät maassa, jonka kybervakuutusmarkkinat ovat vasta muotoutumassa.

Abdul Rahman ym. (2022) toteuttivat laadullisen tutkimuksen kymmenen eri toimialan asiantuntijahaastattelujen pohjalta. Haastateltavat edustivat muun muassa IT-, televiestintä-, valmistus- ja pankkialaa. Tulosten mukaan vain 30 prosenttia organisaatioista oli ottanut käyttöön kybervakuutuksen, ja 40 prosenttia vastaajista ei tiennyt, oliko heidän organisaatiollaan vakuutusta lainkaan (Abdul Rahman ym. 2022, 48–49). Tietoisuus vakuutustuotteista on siis edelleen rajallista, mikä heikentää markkinoiden kykyä toimia tehokkaasti. Kybervakuutusta ei myöskään nähdä luontevana osana organisaatioiden riskienhallintaa tai vaatimustenmukaisuutta. Esimerkiksi henkilötietojen käsittelyä säätelevä PDPA-laki ja finanssisektorin riskienhallintaa ohjaava RMiT-laki tunnetaan usein vain yleisellä tasolla, mikä vaikeuttaa vakuutuksen kytkemistä osaksi niiden noudattamista. Vakuutus jää ikään kuin irralliseksi ratkaisuksi, eikä markkinoille muodostu luotettavia signaaleja organisaatioiden kyberturvallisuuden tasosta (Abdul Hamid ym. 2025, 77–78). Organisaatiot eivät aina tiedä, mitä vakuutuksen saaminen heiltä käytännössä edellyttää. Silloin vakuutusta hankitaan sattumanvaraisesti tai ulkoisten paineiden vuoksi, sen sijaan, että päätös perustuisi systemaattiseen riskien arviointiin (Abdul Hamid ym. 2025, 79).

Abdul Hamid ym. (2022) tunnistivat hybrideduktiivisen ja induktiivisen analyysin avulla kaksitoista keskeistä estettä kybervakuutusten käyttöönotolle. Merkittävimmiksi nousivat vakuutusten standardoinnin puute, historiallisen datan niukkuus, alhainen tietoisuus ja korkeat kustannukset. Standardoinnin puute oli erityisen ongelmallinen, sillä vakuutuksenottajien ja vakuutusyhtiöiden välillä ei ollut yhteistä käsitystä siitä, mitä kybervahinkoihin liittyviä tappioita vakuutukset tosiasiassa kattavat. Lisäksi luotettavan korvaus- ja vahinkodatan puute vaikeutti vakuutusyhtiöiden kyberriskin tarkkaa hinnoittelua. Abdul Rahman ym. (2022, 49) mukaan hinnoittelun epävarmuus rajoittaa markkinoille osallistumista, ja vain suuret yritykset kykenevät maksamaan korkeita vakuutusmaksuja. Tämä voi syrjäyttää pienemmät yritykset markkinoilta, vaikka juuri ne ovat usein heikoimmin varautuneita kattamaan kybervahinkoja ilman vakuutussuojaa. Raju ym. (2024) tulokset ovat linjassa aikaisempien tutkimusten tunnistamien markkinaesteiden kanssa. Heidän 30 puolistrukturoidun haastattelun aineistonsa perusteella esiin nousivat erityisesti epäselvä vakuutusturva, kyberuhkien nopeasti kehittyvä luonne, riittämättömän historiallisen datan aiheuttama epävarmuus sekä läpinäkyvän sääntelyn puute.

Myös konkreettisten esimerkkien ja oikeuskäytäntöjen puute lisää epävarmuutta. Malesiassa ei ole juurikaan kybervakuutuksia koskevia oikeustapauksia, mikä vaikeuttaa korvausvaatimusten ennakointia (Abdul Rahman ym. 2022). Abdul Hamid ym. (2022) kytkevät nämä havainnot suoraan haitallisen valikoitumisen ja moraalikadon teoreettisiin käsitteisiin. Standardoinnin ja datan puute vaikeuttaa organisaatioiden riskitasojen erottamista, mikä lisää haitallisen valikoitumisen riskiä. Samalla monilta organisaatioilta puuttuu kypsä riskienarviointiprosessi, mikä tekee niistä vakuutusyhtiöille vaikeasti arvioitavia. Moraalikadon riski kasvaa, kun vakuutuksenottajat eivät ymmärrä vakuutusehtoja tai eivät koe velvollisuutta ylläpitää riittävää kyberturvallisuutta. (Abdul Hamid ym. 2025, 81–82).

Tutkimuksissa tunnistettiin kuitenkin myös tekijöitä, jotka voivat lieventää markkinahäiriöitä. Raju ym. (2024) korostavat Malesian suunnitelmia uudesta kyberturvallisuuslainsäädännöstä, joka voisi lisätä markkinoiden läpinäkyvyyttä ja vähentää epävarmuutta. Pelkkä laki ei kuitenkaan riitä, jos organisaatioilla ei ole tarvittavia käytännön valmiuksia sen noudattamiseen. Haastatellut asiantuntijat huomauttivat, että esimerkiksi henkilötietojen suojaa koskevien sääntöjen tai finanssialan riskienhallintaohjeiden noudattaminen voi toimia merkkinä siitä, että organisaatio on kypsä ja luotettava. Hallintamallit ovat tärkeitä, sillä ne vähentävät tiedon epätasapainoa ja auttavat luomaan yhteisen ymmärryksen vakuutusyhtiöiden ja asiakkaiden välille (Abdul Hamid ym. 2025, 83–84). Malesian kybervakuutusmarkkinoita vääristävät rakenteelliset haasteet ovat siis merkittäviä, mutta kohdennetuilla toimilla markkinoiden on mahdollista parantaa toimivuutta ja edistää vakuutusten käyttöönottoa.

### 4.3.2 Ruotsi

Skandinaviassa kybervakuutusten käyttöönotto on edennyt hitaasti. Ruotsissa kybervakuutuksen hankkineiden yritysten osuus on noussut vain yhden prosenttiyksikön, ja maa on ollut alueen heikoin, sillä vain 57 prosenttia yrityksistä on hankkinut kybervakuutuksen (Kurmaiev ym. 2020, 70). Ruotsin kybervakuutusmarkkinoille on ominaista pieni mutta erittäin keskittynyt joukko vakuutusyhtiöitä, jälleenvakuuttajia ja välittäjiä. Ruotsin vakuutusalan toimialajärjestö (SFM) raportoi, että kybervakuutusten osuus vakuutusmaksuista oli noin 800 miljoonaa kruunua vuonna 2021, mikä osoittaa markkinan kasvua mutta myös sen varhaista kehitysvaihetta. Vaikka kybervakuutuksia tarjotaan jo aktiivisesti, epävarmuus ja nopeasti muuttuva uhkaympäristö rajoittavat edelleen markkinoiden laajentumista ja vahvistavat markkinahäiriöitä.

Franken (2017) laadullinen haastattelututkimus, johon osallistui kymmenen vakuutusyhtiötä, kaksi jälleenvakuuttajaa ja kolme välittäjää osoittaa, että Ruotsissa markkinaratkaisut keskittyvät

tarjonnan rajoittamiseen. Vakuutusyhtiöt asettavat asiakkaille tiukkoja tietoturvavaatimuksia ja kieltäytyvät vakuuttamasta yrityksiä, joiden kyberturvallisuustaso on liian heikko. Vakuutusten kattavuus ja vaatimustaso vaihtelevat yhtiöittäin, mikä lisää epäselvyyttä ja jättää monet yritykset vakuutuskelpoisuuden ulkopuolelle puutteellisen kyberturvallisuuden vuoksi. Ruotsi edustaakin pientä mutta nopeasti kehittyvää markkinaa, jossa tekninen osaaminen ja digitalisaatio voivat luoda edellytyksiä yhä kehittyneemmille vakuutusratkaisuille (Franke 2017; SFM 2023).

Pienten ja keskisuurten yritysten näkökulmaa tarkastelevat Carlsson ja von Post (2025), joiden yhdeksän yritysedustajan haastatteluihin perustuvat tulokset tukevat Franken (2017) havaintoja markkinoiden rakenteellisista haasteista. Keskeisiksi esteiksi nousivat korkea hinta, luottamusongelmat ja epäselvät vakuutusehdot. Useat haastatelluista kokivat, että vakuutusyhtiöt pyrkivät välttämään korvausten maksamista ehtojen hienosäädöillä. Erään vastaajan mukaan moni yritys vetäytyy vakuutuksen hankinnasta, kun sopimusehdoista paljastuu tilanteita, joissa vakuutus ei korvaakaan vahinkoja. Tämä epäluottamus voidaan kytkeä suoraan käänteisen haitallisen valikoitumisen teoriaan. Vakuutusyhtiö voi tehdä sopimusehdoista niin monimutkaisia, ettei yritys kykene vertailemaan tuotteita tai arvioimaan, mitä turvaa se todella tarvitsee (Nieuwesteeg ym. 2018, 21, 29). Lisäksi osa vastaajista uskoi virheellisesti, ettei pieni yritys ole kiinnostava kohde hyökkääjille, ja vakuutuksen hinta koettiin usein liian korkeaksi suhteessa koettuun hyötyyn.

Markkinoiden toimivuutta hankaloittavat myös yritysten puutteelliset turvallisuuskäytännöt ja riskikäsitykset. Franken ja Wernbergin (2020) kyselytutkimus ruotsalaisista teollisuusyrityksistä osoittaa, että yritysten turvallisuuskäytäntöjen kypsyystaso ja riskikäsitykset ovat usein ristiriidassa todellisen altistumisen kanssa. Vaikka 79 prosenttia yrityksistä pitää digitalisaatiota tulevaisuuden kilpailukyvyn kannalta erittäin tärkeänä, vain 25 prosenttia priorisoi kyberturvallisuusinvestointeja samalla tasolla. Tämä kuilu digitalisaation ja turvallisuuspanostusten välillä luo markkinoille negatiivisia ulkoisvaikutuksia. Yritykset hyötyvät toistensa suojauksista, mutta eivät investoi riittävästi omiin turvallisuuskäytäntöihinsä. Lisäksi 61 prosenttia yrityksistä on vahvasti riippuvaisia ulkoisten toimittajien IT-järjestelmistä, mutta vain 21 prosenttia asettaa näille toimittajille kyberturvallisuusvaatimuksia. (Franke & Wernberg 2020).

Markkinahäiriöiden lieventämiseksi Franke (2017) sekä Carlsson ja von Post (2025) nimeävät useita käytännön keinoja, kuten yksityiskohtaiset riskinarvioinnit, auditoinnit ja jatkuvan seurannan. Carlsson ja von Post (2025) ehdottavat lisäksi porrastettuja vakuutustuotteita ja selkeämpää tukea vahinkotilanteissa luottamuksen vahvistamiseksi. Haastatellut yritykset toivoivat erityisesti oikeudellista ja teknistä tukea vahingon sattuessa sekä mahdollisuutta räätälöidä vakuutusturva yrityksen

koon ja tarpeiden mukaan. Nämä havainnot osoittavat, että tarjonta- ja kysyntäpuolella on kehitettävää, jotta epäsymmetrisen informaation aiheuttamia ongelmia voidaan vähentää.

Ruotsin markkinat ovat siis pienet mutta nopeasti kasvavat. Kybervakuutuksia hankkivat pääasiassa suuret yritykset sekä ne pienemmät toimijat, joilla on liiketoimintaa Yhdysvalloissa, missä vakuutusta pidetään käytännössä välttämättömänä. Korvausvaatimusten määrä on Ruotsissa edelleen hyvin pieni, ja useimmat vakuutusyhtiöt käsittelevät vuosittain vain muutamia tapauksia. Tämän vuoksi hinnoittelu perustuu pitkälti asiantuntija-arvioihin eikä historialliseen dataan. Vaikka joillakin vakuutusyhtiöillä on vuosikymmenten aineistoa Yhdysvalloista, sen soveltaminen Ruotsin markkinoille on rajallista (Franke 2017, 136–137), mikä ylläpitää epävarmuutta ja vahvistaa markkinahäiriöitä.

### 4.3.3 Yhdysvallat

Pohjois-Amerikka on pitkään ollut maailman suurin kybervakuutusmarkkina, ja arvioiden mukaan lähes puolet koko kyberturvallisuusalan kasvusta vuoteen 2030 mennessä syntyy Yhdysvalloissa. Yhdysvallat ja Iso-Britannia ovatkin muovanneet kybervakuuttamisen toimintatapoja jo yli kahden vuosikymmenen ajan. Yhdysvaltojen erityispiirteenä onkin sen markkinoiden varhainen syntyminen. Ensimmäiset kybervakuutustuotteet lanseerattiin jo 1990-luvun lopulla, ja myöhemmät lainsäädännölliset uudistukset, kuten osavaltioiden tietomurtolainsäädäntö, loivat vahvan kysyntäpohjan vakuutuksille. Yhdysvallat toimii edelleen suuntaa näyttävänä valtiona, ja sen markkinatrendit heijastuvat laajasti myös muiden alueiden kehitykseen (American Academy of Actuaries 2025).

Markkinoiden rakenteellisia piirteitä tarkastelevat Cole ja Fier (2021), jotka hyödyntävät monimuuttujaista regressiokehystä analysoidessaan vakuutusyhtiöiden osallistumista NAIC-järjestön datan perusteella. Tulokset osoittavat, että markkinat ovat erittäin keskittyneet ja että yrityskohtaiset ominaisuudet kuten koko, liiketoimintajakauma, jälleenvakuutuksen käyttö ja organisaatiorakenne vaikuttavat merkittävästi sekä kyberturvan tarjoamispäätökseen että tarjotun vakuutusturvan määrään (Cole & Fier 2021, 240). Tämä korostaa sitä, että markkinoille osallistuminen ei ole tasapuolista, vaan riippuu vahvasti vakuuttajien omista resursseista.

Eling ym. (2024) tarkentavat Yhdysvaltojen kybervakuutusmarkkinoiden rakenteellisia ongelmia hyödyntämällä vuoden 2017 BEAT-verouudistusta (engl. Base erosion and anti-abuse tax). Uudistus muutti ulkomaisten tytäryhtiöiden kautta ostetun jälleenvakuutuksen verokohtelua ja teki erityisesti Bermudalla sijaitsevien tytäryhtiöjälleenvakuuttajien käytöstä selvästi kalliimpaa. Koska muutos koski vain niitä vakuutusyhtiöitä, jotka olivat riippuvaisia ulkomaisesta jälleenvakuutuksesta,

osa yhtiöistä kohtasi äkillisen kustannusshokin ja osa ei. Tutkimus hyödyntää tätä eroa luonnollisena koeasetelmana arvioidakseen, miten ulkoisen pääoman kallistuminen vaikuttaa kybervakuutusten tarjontaan. Tulokset osoittavat, että kybervakuutusmarkkinat ovat edelleen hyvin pienet. Vuonna 2022 niiden osuus Yhdysvaltojen koko omaisuus- ja vahinkovakuutusmaksuista oli vain 0,8 %. BEAT-uudistus heikensi ulkomaisen jälleenvakuutuksen saatavuutta ja hidasti kybervakuutusmaksujen kasvua erityisesti niillä vakuuttajilla, joilla altistus uudistukselle oli suurin. Näillä yhtiöillä kasvuvauhti putosi noin 30 prosenttia, mikä viittaa siihen, että kybervakuutusten tarjonta reagoi voimakkaasti ulkoisen pääoman kustannuksiin.

Selittääkseen, miksi ulkoinen jälleenvakuutus on niin kallista, Eling ym. erottelevat kolme keskeistä kustannustekijää: äärimmäisten tappioiden mahdollisuuden, kyberriskin jakauman epävarmuuden ja informaatioepäsymmetrian vakuuttajien ja jälleenvakuuttajien välillä. Kaikki nämä tekijät nostavat ulkoisen pääoman hintaa, mutta erityisesti informaatioepäsymmetria korostuu silloin, kun vakuuttajan kybervakuutusten osuus on suuri ja ulkoisen jälleenvakuutuksen tarve kasvaa. Ulkopuoliset sijoittajat vaativat tällöin korkeampaa riskipreemiota, koska heillä on rajallinen näkyvyys vakuuttajan todelliseen riskiprofiiliin. Näiden tulosten perusteella Yhdysvaltojen kybervakuutusmarkkinoiden keskeinen markkinoiden tehottomuus liittyy pääoman saatavuuteen. Ulkoinen pääoma on kallista ja herkkää sääntelymuutoksille, mikä rajoittaa tarjontaa ja selittää, miksi vakuutusyhtiöt tukeutuvat voimakkaasti sisäisiin pääomamarkkinoihin kyberriskin rahoittamisessa.

Nurse ym. (2020) tarkastelevat riskinarviointikäytäntöjä analysoimalla yhdysvaltalaisten vakuuttajien ja kyberturvallisuusammattilaisten näkemyksiä. Heidän havaintonsa osoittavat, että vakuuttajat tukeutuvat vahvasti itse täytettyihin arviointilomakkeisiin ja ulkoisiin tietoturvatarkastuksiin. Nämä menetelmät tarjoavat kuitenkin vain rajallisen ja usein puutteellisen kuvan yrityksen todellisesta tietoturvatasosta. Läpinäkymättömyys lisää riskiä haitalliselle valikoitumiselle. Matalan riskin yritykset eivät pysty uskottavasti osoittamaan parempaa turvallisuuttaan, kun taas korkean riskin yrityksillä ei ole kannustimia tuoda esiin omia haavoittuvuuksiaan.

Johansmeyer (2024) tarkastelee Yhdysvaltojen kybervakuutusmarkkinoiden rakenteellisia ongelmia sekamenetelmätutkimuksella, joka yhdistää markkinadataa ja syvähaastatteluja. Haastatteluihin osallistui yksitoista suurten ja keskisuurten vakuutusyhtiöiden johtajaa, jotka edustavat noin 42 prosenttia maailman kybervakuutusmaksuista. Tulokset osoittavat, että markkinoita vaivaa pysyvä pääomapula. Vakuutusyhtiöt siirtävät yhä noin puolet kyberriskeistään jälleenvakuuttajille, mutta markkinoille ei tule riittävästi uutta pääomaa. Sijoittajat suhtautuvat varovaisesti, koska systeemiset kyberriskit ovat vaikeita mallintaa ja voivat pahimmillaan aiheuttaa erittäin suuria tappioita. Vaikka

vakuutussidonnaisten arvopaperien määrä on kasvanut noin 800 miljoonaan dollariin, tämä vastaa vain pientä osaa siitä kapasiteetista, jota markkinoiden vakaaseen toimintaan tarvittaisiin. Haastatteluista tuli ilmi myös koordinaatio-ongelma. Osa alan johtajista pitää kyberriskiä vakuutettavana, osa ei, mikä taas heikentää markkinoiden kykyä houkutella pääomaa. Näiden rakenteellisten häiriöiden vuoksi kybervakuutusmarkkinat eivät tällaisenaan pysty täyttämään niitä odotuksia, joita Yhdysvaltain kyberturvallisuusstrategia asettaa niille.

## 4.4 Johtopäätökset

Kybervakuutusmarkkinoiden kokonaisuutta leimaa ennen kaikkea epävarmuuden hallinnan ongelmat. Tutkimuksissa korostuu, että markkinoiden tehottomuus liittyy siihen, ettei riskille ole muodostunut yhteistä ja vakiintunutta käsitteellistä perustaa (Abdul Hamid ym. 2022). Vakuuttajat, asiakkaat ja sääntelijät tarkastelevat samaa ilmiötä eri näkökulmista, mikä hajottaa ymmärrystä ja vaikuttaa suoraan markkinoiden toimintaan. Riskin mittaaminen on epävakaata, ja epäsymmetrinen informaatio näkyy jo siinä, miten riski ylipäätään hahmotetaan (Friberg 2025). Tällaisessa tilanteessa vakuuttajat turvautuvat varovaisiin ratkaisuihin, jotka vaikuttavat suoraan vakuutusten tarjontaan ja ehtoihin.

Varovaisuus puolestaan ilmenee rajoituksina ja epäselvyyksinä, jotka lisäävät asiakkaiden epäröintiä (Abdul Hamid ym. 2022; Carlsson & von Post 2025). Näin muodostuu kierre, jossa epävarmuus lisää varovaisuutta, varovaisuus lisää epäselvyyttä ja epäselvyys syventää markkinahäiriöitä. Tällaisessa ympäristössä myös haitallinen valikoituminen ja moraalikato poikkeavat osittain teorian ennusteista, sillä niiden muotoutuminen riippuu enemmän riskin tulkinnasta kuin tietoisista valinnoista (Branley-Bell ym. 2021; Gómez ym. 2025). Markkinahäiriöt eivät siis synny vain tiedon puutteesta, vaan myös siitä, että osapuolet ymmärtävät riskin eri tavoin.

Maakohtaiset erot havainnollistavat, miten markkinahäiriöt saavat erilaisia muotoja riippuen markkinoiden kypsyydestä ja siitä, millaisia ratkaisuja epävarmuuden hallintaan on kehitetty. Malesiassa keskeinen haaste on tiedon puute, mikä näkyy muun muassa matalana kysyntänä ja epäselvinä vakuutusehtoina (Abdul Rahman ym. 2022; Raju ym. 2024). Ruotsissa ongelmat liittyvät enemmän riskin tulkinnan eroihin vakuuttajien ja yritysten välillä, mikä johtaa tiukkoihin vaatimuksiin, rajattuun vakuutuskelpoisuuteen ja epäluottamukseen sopimusehtoja kohtaan (Franke 2017; Carlsson & von Post 2025). Yhdysvalloissa markkinahäiriöt korostuvat erityisesti silloin, kun riskit ovat laajoja ja keskinäisriippuvaisia, eikä käytettävissä oleva tieto riitä mallintamaan äärimmäisiä tai systeemisiä uhkia (Johansmeyer 2024).

# 5 Yhteenveto

Tutkielmassa tarkasteltiin, miten epäsymmetrinen informaatio ja siitä johtuvat kannustinongelmat muokkaavat kybervakuutusmarkkinoiden toimintaa. Analyysi osoittaa, että markkinoiden tehottomuus syntyy ennen kaikkea kyberriskien erityispiirteiden ja vakuutusyhtiöiden sekä vakuutuksenottajien välisten tietoaukkojen yhteisvaikutuksesta. Kyberriskit ovat vahvasti korreloivia, vaikeasti mitattavia ja jatkuvasti muuttuvia, minkä vuoksi historiallinen data ei tarjoa luotettavaa pohjaa riskien arvioinnille. Lisäksi riskit ovat keskinäisriippuvaisia. Yhden yrityksen tietoturvavalinnat vaikuttavat muiden altistukseen, mikä rikkoo perinteisten vakuutusmallien oletuksen riskien riippumattomuudesta ja hajautettavuudesta. Poikkeama näkyy suoraan siinä, miten haitallinen valikoituminen ja moraalikato ilmenevät kybervakuutusmarkkinoilla verrattuna klassisiin vakuutusteoreettisiin malleihin.

Teoreettinen viitekehys (Rothschild & Stiglitz 1976; Akerlof 1970; Nicholson & Snyder 2008; Friberg 2025) vahvistaa, että vakuutusyhtiöt eivät pysty havaitsemaan asiakkaiden todellista riskiprofiilia eivätkä valvomaan näiden tietoturvatoimia. Tämä informaation epäsymmetria pakottaa markkinat toiseksi parhaaseen tasapainoon, jossa vakuutusturva on tarkoituksellisesti epätäydellinen. Esimerkiksi omavastuut ja turvallisuusvaatimukset toimivat välineinä, joilla vakuutusyhtiöt pyrkivät hillitsemään kannustinongelmia tilanteessa, jossa riskin tarkka hinnoittelu ei ole mahdollista. Kyberriskien kohdalla epäsymmetrinen informaatio on kuitenkin kaksisuuntaista. Yrityksillä itsellään ei usein ole realistista käsitystä omista haavoittuvuuksistaan, mikä heikentää niiden kykyä arvioida vakuutustarpeitaan ja altistaa ne monimutkaisten vakuutusehtojen tulkintariskeille.

Empiirinen näyttö osoittaa, että haitallista valikoitumista esiintyy kybervakuutusmarkkinoilla, mutta sen muodot vaihtelevat. Yhdysvalloissa heikomman turvallisuustason yritykset hankkivat vakuutuksen todennäköisemmin, mutta vakuutusmaksut eivät heijasta havaittavia riskisignaaleja, mikä johtaa riskialttiimpien asiakkaiden kasautumiseen markkinoille (Ning 2025). Vakuutusyhtiöt reagoivat tähän rajoittamalla vakuutusturvaa hinnankorotusten sijaan, mikä puolestaan karkottaa matalamman riskin asiakkaat ja vahvistaa klassista haitallisen valikoitumisen dynamiikkaa. Toisaalta Branley-Bell ym. (2021) tutkimuksen mukaan kaikkein riskihakuisimmat toimijat voivat myös vältellä vakuutuksia, mikä viittaa valikoitumisen mahdolliseen käänteiseen muotoon ja korostaa kyberriskien erityispiirteiden merkitystä.

Moraalikadon osalta empiirinen näyttö poikkeaa selvästi teorian ennustuksista. Piilotetun toiminnan malli olettaa, että riskin siirtäminen vakuutusyhtiölle vähentää kannustimia investoida tietoturvaan.

Kokeelliset tutkimukset ja yritystason analyysit eivät kuitenkaan tue tätä oletusta (Gómez ym. 2025; Branley-Bell 2021). Vakuutuksen hankkiminen näyttää pikemminkin liittyvän ennallaan pysyviin tai parantuneisiin tietoturvakäytäntöihin. Tätä saattaa selittää se, että kybervakuutukset sisältävät yhä useammin ennakoivia ehtoja, kuten turvallisuusvaatimuksia ja jatkuvaa valvontaa. Nämä rajoittavat piilotetun toiminnan mahdollisuuksia ja ylläpitävät kannustimia investoida tietoturvaan.

Kokonaisuutena epäsymmetrinen informaatio ja siitä seuraavat kannustinongelmat heikentävät kybervakuutusmarkkinoiden tehokkuutta sekä teoriassa että osittain käytännössä. Kyberriskien vaikea havaittavuus, datan niukkuus ja vahva keskinäisriippuvuus estävät markkinoita muodostamasta yhteistä käsitystä todellisesta riskitasosta. Vakuutusyhtiöt hinnoittelevat tuotteensa puutteellisen tiedon varassa, ja yritykset puolestaan saattavat yliarvioida oman turvallisuustasonsa. Tämä molemminpuolinen epävarmuus estää täydellisen riskinsiirron ja johtaa markkinoihin, joissa tasapaino jää rajoittuneeksi. Se näkyy muun muassa korkeina omavastuina ja tiukkoina korvausrajoina sekä erityisesti pienten sekä keskisuurten yritysten alivakuuttamisena. Haitallinen valikoituminen heikentää vakuutuskannan laatua, ja moraalikadon riski on olemassa, ellei sopimuksia suunnitella huolellisesti.

Markkinoilla kehitetyt ratkaisut kuten ennakkotarkastukset, tietoturvavaatimukset, auditoinnit ja vakuutusyhtiöiden tarjoamat ennakoivat palvelut pyrkivät lieventämään näitä ongelmia vähentämällä tiedon epätasapainoa ja vahvistamalla yritysten kannustimia ylläpitää korkeaa tietoturvatasoa. Johtopäätöksenä voidaan todeta, että kybervakuutusmarkkinoiden toimivuus riippuu pitkälti siitä, kuinka hyvin osapuolet onnistuvat vähentämään informaation epätasapainoa ja hallitsemaan keskinäisriippuvaisia riskejä. Vaikka markkinoilla on kehitetty useita mekanismeja kannustinongelmien lieventämiseksi, niiden vaikutus on rajallinen kyberriskien luonteen pysyessä vaikeasti mallinnettavana ja vahvasti keskinäisriippuvaisena. Jatkotutkimusta tarvitaan erityisesti haitallisen valikoitumisen ja moraalikadon empiirisestä ilmenemisestä, sillä nykyinen tutkimus on vähäistä ja osin ristiriitaista. Lisäksi kyberriskien keskinäisriippuvuuksien mallintamisen ymmärtäminen on välttämätöntä markkinoiden kehittämiseksi kohti tehokkaampaa markkinatilannetta.

## Lähteet


Abdul Hamid, N. H. A. – Mokhtar, M. – Wan Abd Manan, W. K. A. – Hashim, H. (2025) Exploring Critical Success Factors in Compliance-Driven Cyber Insurance within Malaysian Organizations: A COBIT 5 enabler approach. *Environment-Behaviour Proceedings Journal*, 10(SI31), 77–84

Abdul Hamid, N. H. A. – Nor, N. – Hussain, F.M. – Raju, R. – Naseer, H. – Ahmad, A. (2022) Barriers and enablers to adoption of cyber insurance in developing countries: An exploratory study of Malaysian organizations. *Computers & Security*, 122, 102893

Abdul Rahman, N. H. – Raju, R. – Ariffin, S. – Abdul Hamid, N. H. A. (2022) Adoption of cyber insurance in Malaysian organisations. *International Journal of Innovative Computing*, 12(2), 45–51

Abrardi, L. – Comino, S. – Grassini, S. (2025) The Economics of Cyber Risk: A Survey of the Literature. *Journal of Industrial and Business Economics*, 52(1), 1-37

Akerlof, G. A. (1970) The Market for "Lemons": Quality Uncertanty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3), 488-500

American Academy of Actuaries. (2025) *An Overview of the Global Cyber (Re)Insurance Market.* https://actuary.org/wp-content/uploads/2025/08/Toolkit-GlobalCyber-8-25.pdf

Arce, D. G. – Woods, D. – Böhme, R. (2024) Economics of incident response panels in cyber insurance. *Computers & Security,* 140, 103742

Awiszus, K. – Knispel, T. – Penner, I. – Svindland, G. – Voß, A. – Weber, S. (2023) Modeling and Pricing Cyber Insurance. *European Actuarial Journal*, 13, 1–53

Biener, C. – Eling, M. – Wirfs, J. (2014) Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 39(3), 406-437

Bose, S. – Akhtaruzzaman, M. – Zaman, R. – Abbassi, W. (2025) Global cybersecurity, cyber risk and firm value: International evidence. *The International Journal of Accounting*

Branley-Bell, D. – Gómez, Y. – Coventry, L. – Vila, J. – Briggs, P. (2021) Developing and Validating a Behavioural Model of Cyberinsurance Adoption. *Sustainability*, 13(17), 9528.

Böhme, R. – Laube, S. – Riek, M. (2019) A Fundamental Approach to Cyber Risk Analysis, *Variance*, 12(2), 161-185

Carlsson, V. – von Post, M. (2025) Cyber insurance and small to medium sized enterprises in Sweden. Jönköping University, School of Engineering, *Computer Science and Informatics*

Cole, C. – R. Fier, S. G. (2021) An empirical analysis of insurer participation in the US cyber insurance market. *North American Actuarial Journal*, *25*(2), 232-254

Cybersecurity Ventures (2025) *2026 Cybersecurity Market Report*, Cybercrime Magazine. Julkaistu 14.11.2025. https://cybersecurityventures.com/wp-content/uploads/2023/11/Cybersecurity-Market-Report-2026.pdf

Davis, C. (2025) *Cyber insurance gaps exposed as SMBs remain largely unprotected*. Insurance Business America, Julkaistu 24.11.2025. https://www.insurancebusiness-mag.com/us/news/cyber/cyber-insurance-gaps-exposed-as-smbs-remain-largely-unprotected-557661.aspx, viitattu 9.3.2026

Do, C. T. – Tran, N. H. – Hong, C. – Kamhoua, C. A. – Kwiat, K.A. – Blasch, E. – Ren, S. – Pissinou, N. – Iyengar, S. S. (2017) Game Theory for Cyber Security and Privacy. *ACM Computing Surveys (CSUR)*, 50(2), 1-37

Eling, M. – Kartasheva, A. – Ning, D. (2023) The Supply of Cyber Risk Insurance. *Swiss Finance Institute Research Paper,* 23-118

ENISA (2025) *ENISA Threat Landscape 2025. European Union Agency for Cybersecurity*. Julkaistu 1.10.2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Franke, U. (2017) The cyber insurance market in Sweden. *Computers & Security,* 68, 130-144

Franke, U. – Orlando, A. (2025) Independent cyber risk and the role of insurers. *Research in Economics*, 79(3), 101059

Franke, U. – Wernberg, J. (2020) A survey of cyber security in the Swedish manufacturing industry. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1-8

Friberg, R. (2025) *Microeconomics: An open introduction (1st edition)*. Luku 14. Routledge. https://doi.org/10.4324/9781003623854

Gómez, Y – Branley-Bell, D. – Briggs, P. – Vila, J. (2025) Cyberinsurance adoption strategies and security of online behaviour: An experimental study. *Behaviour & Information Technology,* 44(6), 1169–1182

Gordon, L. A. – Loeb, M. P. – Sohail, T. (2003) A Framework for Using Insurance for Cyber-Risk Management, *Communications of the ACM*, 46 (3), 81-85

Heiskanen, H. (2017) *Ukraina kamppailee uuden verkkohyökkäysaallon estämiseksi*. Yle Uutiset. Julkaistu 5.7.2017. Viitattu 3.5.2026. https://yle.fi/a/3-9707875

Holmström, B. (1979) Moral Hazard and Observability. *The Bell Journal of Economics*, 10(1), 74-91

Hui, W. – Hui, K. – Yue, W. T. (2024) Cyber Insurance and Post-Breach Services: A Normative Analysis. *Service Science*, 16(2), 124–141

Jensen, M. C. – Meckling, W. H. (1976) Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360

Johansmeyer, T. (2024) If Cyber Is Uninsurable, the United States Has a Major Strategy Problem. *The Journal of Risk Management and Insurance*, 28(2)

Khalili, M. M. – Naghizadeh, P. – Liu, M. (2017) Designing cyber insurance policies: Mitigating moral hazard through security pre-screening. *In International Conference on Game Theory for Networks*, 63-73, Springer International Publishing

Kopp, E. – Kaffenberger, L. – Wilson, C. (2017) Cyber risk, market failures, and financial stability, IMF Working Paper No. WP/17/185. *International Monetary Fund*.

Kunreuther, H. – Heal, G. (2003) Interdependent Security. *Journal of Risk and Uncertainty*, 26(2-3), 231-249

Kurmaiev, P. – Seliverstova, L. – Bondarenko, O. – Husarevych, N. (2020) Cyber insurance: the current situation and prospects of development. *Amazonia Investiga*, 9(28), 65–72

Kuru, D. – Bayraktar, S. (2017) The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime,* 24(2), 329–346

Laube, S. – Böhme, R. (2016) The economics of mandatory security breach reporting to authorities. Journal of Cybersecurity, 2(1), 29–41

Lister, S. (2025) *Why don't small and medium UK enterprises buy cyber insurance?* Binding Hook, Julkaistu 6.11.2025. https://bindinghook.com/why-dont-small-and-medium-uk-enterprises-buy-cyber-insurance/, Viitattu 9.3.2026

Lockton (2026) *Cyber Insurance Market Update: Rates decline despite rising claims*. Lockton Companies, Julkaistu 06.02.2026. Viitattu 9.3.2026, https://www.global.lockton.com/gb/en/news-insights/cyber-insurance-market-update-rates-decline-despite-rising-claims,

Nagurney, A. – Nagurney, L.S. (2015) A game theory model of cybersecurity investments with information asymmetry. *Netnomics*, 16(1-2), 127-148

Nicholson, W. – Snyder, C. (2008) *Microeconomic theory: Basic principles and extensions* (10th edition), Luvut 8 ja 18, Thomson South-Western

Nieuwesteeg, B. – Visscher, L. – de Waard, B. (2018) The law & economics of cyber insurance contracts: A case study. *European Review of Private Law*, 26, 371–420

Ning, D. (2025) Selection and screening in cyber insurance markets. *SSRN Electronic Journal*

Nurse, J. R. C. – Axon, L. – Erola, A. – Agrafiotis, I. – Goldsmith, M. – Creese, S. (2020) The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment.*

Pal, R. – Golubchik, L. (2011) Pricing and investments in internet security: A cyber-insurance perspective. *arXiv preprint*, https://doi.org/10.48550/arXiv.1103.1552

Pal, R. – Golubchik, L. – Psounis, K. – Hui, P. (2014) Will cyber-insurance improve network security? A market analysis. *IEEE Conference on Computer Communications*, 235-243

Panda, S. – Woods, D.W. – Laszka, A. – Fielder, A. – Panaousis, E. (2019) Post-Incident Audits on Cyber Insurance Discounts, *Computers & Security*, 87, 101593

Raju, R. – Abdul Rahman, N. H. – Sangaran, S. – Ariffin, S. – Syed Yasin, S. N. – Eri, Z. D. (2024) Cyber insurance in Malaysian organisations: An introductory journey. *International Journal of Social Science Research, 12*(1)

Rothschild, M. – Stiglitz, J. E. (1976) Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information. *Quarterly Journal of Economics*, 90(4), 629-649

Roy, S. – Ellis, C. – Shiva, S. – Dasgupta, D. – Shandilya, V. – Wu, C. (2010) A Survey of Game Theory as Applied to Network Security. *Proceedings of the Annual Hawaii International Conference on System Sciences*. 1-10

Shetty, N. – Schwartz, G. – Felegyhazi, M. – Walrand, J. (2010) Competitive cyber-insurance and internet security. *In Economics of information security and privacy*, 229-247. Springer US

Strupczewski, G. (2021) Defining Cyber Risk. *Safety Science*, 135, 105143

Svenska försäkringsförmedlares förening. (2023) *Branschrapport SFM 2023: Cyberrisker, försäkring och försäkringsförmedling – Hur bidrar branschen till ett samhällsviktigt område?* SFM. viitattu: 31.3.2026. https://sfm.se/wp-content/uploads/2024/11/SFM_folder_cyberrapport_231018-1.pdf

Tsohou, A. – Diamantopoulou, V. – Gritzalis, S. – Lambrinoudakis, C. (2023) Cyber insurance: state of the art, trends and future directions. *International Journal of Information Security*, 22, 737-748

Varian, H. R. (2004) System reliability and free riding. *Economics of Information Security*, 1-15

Volkova, T. – Jekabsone, L. – Lavrinovica, Z. – Saba, E. – Saba, M. (2021) The challenges of cybersecurity insurance development: The case of Latvia. *Journal of Business Management*

Woods, D. W. – Simpson, A. C. (2017) Policy Measures and Cyber Insurance: A Framework, *Journal of Cyber Policy*, 2(2), 209-226

World Economic Forum (2026) *Global Cybersecurity Outlook 2026*. Julkaistu 12.1.2026. Viitattu 9.3.2026, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Zhang, R. – Zhu, Q. (2019) FlipIn: A Game-Theoretic Cyber Insurance Framework for Incentive-Compatible Cyber Risk Management of Internet of Things. *IEEE Transactions on Information Forensics and Security*, 2026–2041

# Liitteet

## Liite 1 Selvitys tekoälyn käytöstä

Olen hyödyntänyt tekoälyä tämän tutkielman laatimisen tukena. Alla kuvaan hyödyntämäni työkalut ja niiden roolin työskentelyssäni. Tekoälyn käyttö ja siitä raportoiminen on toteutettu yliopiston ohjeistuksen mukaisesti, ja vastaan itse täysin tutkielman sisällöstä.

Työkalu: Microsoft Copilot

- Käyttövaihe: Suunnitteluvaihe
- Käyttötarkoitus: Tutkielman rakenteen ja kokonaisuuden ideointi.
- Varmistus: Arvioin tekoälyn ehdottamaa rakennetta. Lopullisen ryhmittelyn tein itse.

Työkalu: OpenAI ChatGPT (GPT 5.3-malli)

- Käyttövaihe: Tekstin muokkaaminen
- Käyttötarkoitus: Tekstin selkeyttäminen korjaamalla esimerkiksi oikeinkirjoitusta ja lauseenrakenteita akateemisemmaksi.
- Varmistus: Käyn ehdotukset läpi, ja varmistan ettei alkuperäiset merkitykset ole muuttuneet korjausehdotusten myötä. Vastaan täysin itse lopullisen tekstin sisällöstä ja muotoilusta