

Aada Rouhiainen

**KYBERSOTA JA -RIKOLLISUUS
VAKUUTUSKELPOISUUDEN
NÄKÖKULMASTA**

Johtamisen ja talouden tiedekunta

Kandidaatintutkielma

Marraskuu 2024

Ohjaaja: Jarna Pasanen

TIIVISTELMÄ

Aada Rouhiainen: Kybersota ja -rikollisuus vakuutuskelpoisuuden näkökulmasta

Kandidaatintutkielma

Tampereen yliopisto

Kauppätieteiden tutkinto-ohjelma

Marraskuu 2024

Kyberrikollisuus on uudehko yrityksiä uhkaava rikollisuuden muoto, joka on lisääntynyt digitaalisen datan ja pinta-alan kasvettua merkittävästi viime vuosina. Kyberriskejä voidaan hallita monin tavoin, ja yksi suojausvaihtoehto on kybervakuutus. Tässä kandidaatintutkielmassa perehdytään kyberrikollisuuteen ja kybersotaan sekä näiden vakuutuskelpoisuuteen. Tutkimus on kvalitatiivinen tutkimus, joka jaetaan teoreettiseen ja empiiriseen osuuteen. Teoriaosuus koostuu kahdesta pääluvusta, joista ensimmäisessä syvennytään vakuutusyhtiöiden riskienhallintaan ja vakuutuskelpoisuuteen osana tätä. Jälkimmäisessä teorialuvussa perehdytään kyberrikollisuuteen ja kybersotaan ilmiöinä sekä näiden vakuuttamiseen.

Tutkielman varsinaisena tavoitteena on kartoittaa, millaisia eroavaisuuksia kyberrikollisuuden ja kybersodan vakuutuskelpoisuudessa on, ja mitkä tekijät näihin eroihin vaikuttavat. Tutkielmassa on kolme tutkimuskysymystä: 1. Mitkä tekijät vaikuttavat kyberrikollisuuden eri muotojen vakuutuskelpoisuuteen? 2. Miten kyberrikollisuus ja kybersota eroavat toisistaan vakuutuskelpoisuuden suhteen? 3. Miten muutokset kyberrikollisuuden ja kybersodan luonteessa sekä toisaalta vakuutusten underwritingissa vaikuttavat tulevaisuudessa niiden vakuutuskelpoisuuteen?

Tutkielman empiirinen osuus on kvalitatiivinen ja aineistona käytetään kolmea kybervakuuttamisen asiantuntijan antamaa teemahaastattelua. Haastattelut ovat malliltaan puolistrukturoituja, mikä mahdollistaa joustavan ja suhteellisen vapaan keskustelun aihealueiden ympärillä. Tutkimusaineistoa analysoitiin aineistolähtöisen sisällönanalyysin avulla.

Tutkimuksen tuloksena voidaan todeta vakuutuskelpoisuuden riippuvan monista seikoista, kuten kyberhyökkäyksen motiiveista, toteutustavasta, sekä vakuutusyhtiöiden riskienvalinnasta. Kybersodan ulosrajaaminen vakuutusturvasta johtuu puolestaan osaltaan käytännöstä olla vakuuttamatta sistemivahinkoja, mutta myös käytännön haasteista liittyen kriittiseen infrastruktuuriin sekä vahinkojen holtittomaan leviämiseen. Tulevaisuudessa kyberrikollisuuden voidaan nähdä jatkavan kehittymistään toimialana ja kybervakuutuksen puolestaan kasvattavan vastaavasti markkinaosuuttaan. Kehittyvä toimiala luo uusia haasteita kybervakuutukselle, mikä todennäköisesti pakottaa sen reagoimaan muutoksiin ja sopeutumaan vakuutustuotteena.

Avainsanat: Kybervakuutus, kyberrikollisuus, kybersota, vakuutuskelpoisuus

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

TEKOÄLYN KÄYTTÖ OPINNÄYTTEESSÄ

Opinnäytteessäni on käytetty tekoälysovelluksia:

- Ei
 Kyllä

Ilmoitukseni mukaan olen käyttänyt opinnäytteessäni tutkielmaprosessin aikana seuraavia tekoälysovelluksia:

Tekoälysovellusten nimet ja versiot:

Käyttötarkoitus:

Osiot, joissa tekoälyä on käytetty:

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien osat, joissa on hyödynnetty tekoälyä, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

SISÄLLYSLUETTELO

1 JOHDANTO	5
1.1 Aihealueen esittely	5
1.2 Tutkielman tavoite, tutkimuskysymykset ja rajaukset	5
1.3 Keskeiset käsitteet	7
1.4 Tutkimusmenetelmät ja aineisto	9
1.5 Tutkielman teoreettinen viitekehys ja rakenne	9
2 VAKUUTUSKELPOISUUS JA VAKUUTUSYHTIÖN RISKIENHALLINTA	12
2.1 Vakuutuksen ominaisuudet	12
2.2 Riskien vakuutuskelpoisuus	14
2.3 Vakuutusyrityksen riskienhallinta	16
2.4 Vastuunvalinta	18
3 KYBERRIKOLLISUUS JA VAKUUTTAMINEN	20
3.1 Kyberrikollisuuden lajit ja määritelmät	20
3.2 Kybersota verrattuna kyberrikollisuuteen	21
3.3 Kyberriskien hallinta	24
3.5 Kybersota ja vakuuttaminen	27
4 KYBERVAKUUTTAMINEN NYT JA TULEVAISUUDESSA	28
4.1 Aineiston kerääminen ja analyysi	28
4.2 Kyberrikollisuus ja sen vakuutuskelpoisuus	29
4.3 Kybersota ja sen vakuuttaminen	33
4.4 Kybervakuuttaminen tulevaisuudessa	36
5 YHTEENVETO JA JOHTOPÄÄTÖKSET	41
5.1 Tulosten yhteenveto	41
5.2 Tutkielman arviointi ja jatkotutkimus	44
LÄHTEET	46
LIITTEET	50

1 JOHDANTO

1.1 Aihealueen esittely

Digitaalisen datan ja pinta-alan kasvaessa kasvaa myös hyökkäysten määrä sitä kohtaan. Kyberrikollisuus, joka tullaan määrittelemään käsitteenä tarkemmin myöhemmin tutkimuksessa, on kohtalaisen uusi rikollisuuden muoto, joka uhkaa toimialoja ja yrityksiä uudella tavalla. Kyberrikollisuuden seuraamukset yritykselle voivat olla pahimmillaan tuhoisat ja voivat aiheuttaa pahimmillaan yritykselle äärimmäisen toiminnan keskeytymisriskin ja mainehaitan.

Kyberrikollisuus antaa uuden väylän myös konflikteihin ja sotatilanteisiin; kybersota ja kyberterrorismi ovat nyky maailmassa ja tulevaisuudessa kasvavissa määrin uhkaavia sodankäynnin muotoja, joihin yritykset ja valtiot joutuvat varautumaan. Tämä tutkielma tulee käsittelemään kyberrikollisuuden vakuutuskelpoisuutta, sekä rajanvetoa kyberrikollisuuden ja kybersodan välillä vakuutuskelpoisuuden puolesta.

Tutkielman aihe on ajankohtainen ja relevantti. Kybervakuutus on kohtalaisen tuore ja kasvava vakuutuslaji, joka vasta muotoutuu vastaamaan yritysten tarpeisiin kyberrikollisuutta vastaan. Tällä hetkellä suurin osa vakuutusyhtiöistä tarjoaa jonkinlaisen kybervakuutuksen, mutta eri yhtiöiden kybervakuutusten vertailun jälkeen näiden voidaan todeta olevan pääpiirteittäin sisällöltään samanlaisia. Monia kyberriskejä voidaan vakuuttaa ja kybervakuutukset tarjoavat yrityksille työkaluja esimerkiksi vahinkojen minimoimiseen ja korjaamiseen, sekä korvausta taloudellisista menetyksistä ja tilanteen korjaamisesta aiheutuneista kustannuksista. Tietyt kyberriskit, näistä merkittävimpänä kybersota, ovat kuitenkin rajattu pääsääntöisesti kaikkien vakuutusten ulkopuolelle. Tässä tutkielmassa syvennyttään erilaisten kyberriskien ominaisuuksiin ja eroavaisuuksiin, jotka vaikuttavat niiden vakuutuskelpoisuuteen.

1.2 Tutkielman tavoite, tutkimuskysymykset ja rajaukset

Tutkimuksen tavoitteena on tutkia millaisia eroja kyberrikollisuuden ja kybersodan vakuutuskelpoisuudessa on ja mitkä tekijät näihin eroihin vaikuttavat.

Tutkimuskysymykset ovat seuraavat:

1. Mitkä tekijät vaikuttavat kyberrikollisuuden eri muotojen vakuutuskelpoisuuteen?
2. Miten kyberrikollisuus ja kybersota eroavat toisistaan vakuutuskelpoisuuden suhteen?
3. Miten muutokset kyberrikollisuuden ja kybersodan luonteessa sekä toisaalta vakuutusten ”underwritingissa” vaikuttavat tulevaisuudessa niiden vakuutuskelpoisuuteen?

Tutkielmassa tarkastellaan siis kybersotaa ja kyberrikollisuutta, sekä perehdytään näiden ominaispiirteisiin. Tämä sovitetaan vakuutuskelpoisuuden näkökulmaan pohtien sitä, mitkä tekijät tekevät millaisestakin kyberrikollisuuden muodosta vakuutuskelpoisen tai -kelvottoman. Keskeisiksi käsitteiksi nousee siis kybersodan, -rikollisuuden ja -vakuuttamisen lisäksi myös vastuunvalinta, jota vakuutusyhtiöt harjoittavat päätöksiä tehdessään.

Tutkielman aiheeseen otetaan mukaan myös tulevaisuuspohdintaa. Kyberrikollisuus on jatkuvasti kehittyvä rikollisuuden muoto ja vaikka sen käytöstä sotatoimissa on puhuttu jo pitkään, jatkuvassa kehityksessä oleva laitteisto ja teknologia mahdollistaa sen tulevaisuudessa mahdollisesti uusilla tavoilla. Tutkielmassa pohditaan, miten kybersota ja -rikollisuus voivat mahdollisesti tulevaisuudessa muuttua ja millainen vaikutus tällä mahdollisesti on vakuutusmarkkinoihin. Vaikka nykytilanteessa kybersota on rajattu lähestulkoon täysin vakuutusturvan ulkopuolelle ja muuta kyberrikollisuutta voidaan tietyillä edellytyksillä vakuuttaa, pyrkii tämä tutkielma spekuloidaan voiko tilanne muuttua tulevaisuudessa vakuutuskelpoisuuden näkökulmasta.

Tutkielmassa tullaan tarkastelemaan syvällisemmin kyberriskeistä kyberrikollisuutta ja -sotaa. Kyberriskit tullaan määrittelemään tutkielmassa, mutta tutkielman aihe on rajattu erityisesti kyberrikollisuuden ja kybersodan vakuutuskelpoisuuteen. Tutkielma on rajattu käsittelemään kyberrikollisuuden osalta lähinnä yrityksien, organisaatioiden ja valtiollisten toimijoiden kohtaamaa kyberrikollisuutta. Kyberrikollisuus on laaja käsite, joka koskettaa myös yksilöitä ja luonnollisia henkilöitä. Tässä tutkielmassa jätetään

kuitenkin laajemmasta tarkastelusta pois yksilöiden kohtaamat kyberriskit ja –rikollisuus. Tutkielmassa ei ole tehty maantieteellisiä rajoja johtuen myöhemmin esille tulevasta kyberriskien globaalista ja valtion rajoja tuntemattomasta luonteesta. Tutkielmassa tarkastellaan siis yritysten, organisaatioiden ja valtioiden kohtaamia kyberriskejä globaalilla tasolla, eikä rajautuen tietyn maan kenttään.

1.3 Keskeiset käsitteet

Tutkielman kannalta keskeisiä avainkäsitteitä ovat esimerkiksi kyberrikollisuus, kybersota, kyberhyökkäykset, vakuutuskelpoisuus, sekä kybervakuutus. Olennaista muiden käsitteiden ymmärtämiseksi on selventää, mitä tarkoittaa käsite kyberavaruus, josta johdetaan etuliite ”kyber” tutkielmassa käsiteltäviin aihepiireihin. *Kyber* voidaan liittää lähestulkoon mihin vain toimintaan, joka tapahtuu kybertoimintaympäristössä. Kybertoimintaympäristöllä tarkoitetaan ihmisen luomaa rinnakkaistodellisuutta, joka maailmanlaajuisesti yhdistää informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta toisiinsa ihmisiä ja laitteita valtioiden rajojen yli (Ulkoministeriö, viitattu 2023). Käytännössä kyber siis viittaa digitaaliseen toimintaympäristöön, joka toimii esimerkiksi puhelinten, tietokoneiden ja muiden laitteiden kesken tietoverkossa. Jo Ulkoministeriön määritelmä kertoo, miksi kybertoimintaympäristö on monimutkainen alusta, mitä tulee rikollisuuteen tai sodankäyntiin; se ei tunne valtioiden rajoja, jolloin sen kautta harjoitettu toiminta voidaan tehdä mistä tahansa ja kohdistaa minne vain.

Kyberriskillä tarkoitetaan useasta lähteestä muodostuvaa uhkaa, joka kohdistuu yrityksen tai toimijan tieto-omaisuuteen tai teknologiaan. Kyberriski voidaan määritellä useilla tavoilla; suppeat määritelmät nimeävät kyberriskit riskeiksi, jotka seuraavat haitallisia sähköisiä tapahtumia, jotka aiheuttavat toiminnan keskeytymistä ja taloudellisia menetyksiä (Biener, Eling, Wirfs, 2014).

Kyberhyökkäys on vihamielinen toimi, joka toteutetaan tietokoneella tai niihin liittyvillä verkoilla tai systeemeillä, ja sen tarkoitus on häiritä ja/tai tuhota vastapuolen kriittisiä kybersysteemeitä, varoja, tai toimia (Hathaway 2012, 824).

Kyberrikollisuus on laaja käsite, joka on vaikea määritellä universaalisti yhtenevällä tavalla. Äskeiseen määritelmään pohjustaen kyberrikollisuus on rikollisuutta, joka toteutetaan kybertoimintaympäristössä tai sitä hyödyntäen. Yleisesti ottaen kyberrikoksen voidaan ajatella olevan laitton teko, joka on toteutettu käyttämällä digitaalisia tai tietokonepohjaisia keinoja. Sen voidaan ajatella myös olevan mikä tahansa rikos, joka on toteutettu käyttämällä tietokonetta tai internetiä. (Hathaway 2012, 833–834.)

Muita olennaisia käsitteitä tutkielmaan liittyen on *kybersota*. Kybersota on jälleen termi, jolle löytyy lukuisia eri määritelmiä. Impervan määritelmän mukaan kybersota on kyberhyökkäys tai sarja hyökkäyksiä, jotka kohdistuvat spesifisti maata kohtaan. Niillä on potentiaalia tuottaa suurta vahinkoa hallitukselle ja siviilien infrastruktuurille, sekä häiritä tärkeitä systeemeitä ja pahimmillaan aiheuttaa jopa hengenmenetyksiä (Imperva A, ei pvm.). Richard A. Clarke on antanut kybersodalle melko laajalti käytetyn määritelmän; kybersota on kansallisvaltion harjoittamia toimia, joilla tunkeudutaan toisen valtion tietokoneille ja tietoverkkoihin tarkoituksena aiheuttaa vahinkoa tai häiriötä. Tämä määritelmä kybersodalle on muutoin kelpo, mutta se sulkee ulkopuolelle eivalttiolliset toimijat, jotka voivat myös harjoittaa kybersotaa (Hathaway 2012, 823).

Vakuutuskelpoisuus nousee olennaiseksi käsitteeksi tutkielman edetessä. Vakuutuskelpoisuudella tarkoitetaan yksinkertaisuudessaan sitä, onko riski vakuutettavissa ja millä perusteilla. Riskin ollakseen vakuutuskelpoinen sen toteutumisen todennäköisyyden tulee olla riittävästi ennustettavissa, riskin tulee olla edunsaajasta riippumaton, riskin tulee olla ajallisesti stabiili eli säilyä riittävän vakaana ajan yli, ja riskin toteutumisen tulee olla riittävän harvinaista, etenkin suurvahinkojen tapauksessa. (Rantala & Kivisaari, 2014, 78.)

Kybervakuutus on vakuutustuote, jolla varaudutaan kyberriskeihin. Kybervakuutus kattaa yleisimmin kuluja, jotka koituvat liiketoiminnan keskeytymisestä ja tulojen menetyksestä, sekä tietojen palauttamisesta ja korvauskustannuksista. Kybervakuutus suojaa sen ottajaa sekä ulkoisilta, että sisäisiltä kyberriskeiltä. (Lubin, 2019, 59–61.)

1.4 Tutkimusmenetelmät ja aineisto

Tutkielman empiirinen osuus tulee perustumaan kvalitatiiviseen, laadulliseen tutkimukseen, jonka tarkoituksena on tulkita ja ymmärtää tutkimusongelmaa ja aihetta ilman ennakkohypoteesia (Eskola & Suoranta, 1998). Tutkielma pyrkii antamaan laajan käsityksen kyberrikollisuuden ja kybersodan vakuutuskelpoisuudesta, sekä tulevaisuudennäkymistä vakuutuslalla. Laadullisen tutkimuksen aineistona tullaan hyödyntämään kolmea kybervakuuttamisen asiantuntijan antamaa teemahaastattelua. Haastattelut ovat malliltaan puolistrukturoituja, jotta keskustelusta saadaan mahdollisimman vapaata aihealueiden sisällä ja aiheesta saadaan monipuolinen kuva (Hirsjärvi & Hurme, 2022).

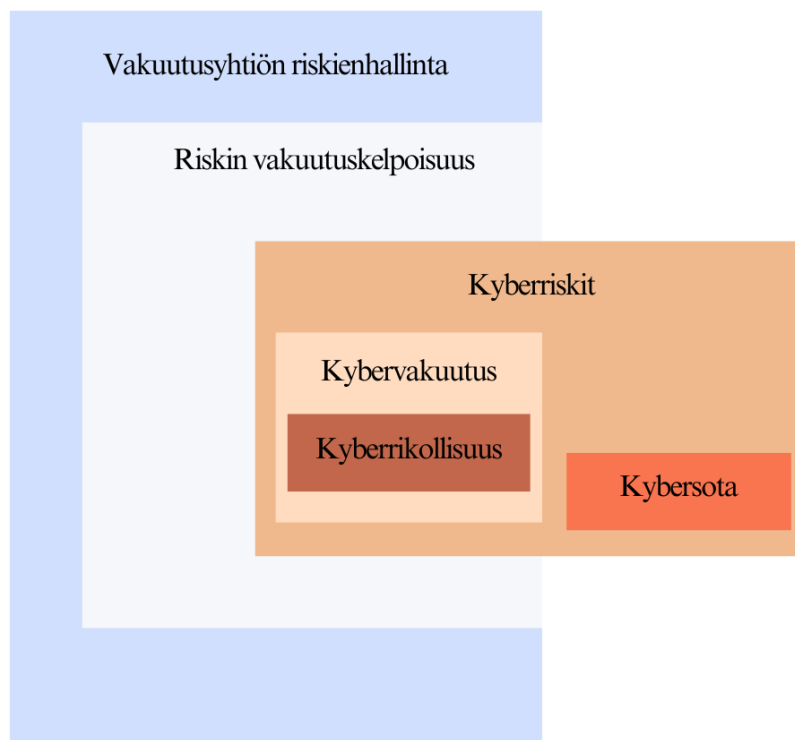
Asiantuntijat haastatellaan yksitellen ja haastattelut toteutetaan videohaastatteluina. Haastattelut nauhoitetaan sekä itse haastattelutilanteen, että litterointiprosessin sujuvoittamiseksi. Haastateltavat pysyvät anonyyminä ja heihin viitataan myöhemmin empirialuvussa nimikkeillä Asiantuntija A, Asiantuntija B ja Asiantuntija C.

Aineiston analyysimenetelmänä käytetään aineistolähtöistä sisällönanalyysiä. Aineistolähtöisessä analyysissä tarkoituksena on luoda tutkimusaineistosta teorettinen kokonaisuus, missä analyysiyksiköt valitaan aineistosta tutkimuksen tarkoituksen mukaisesti (Tuomi & Sarajärvi, 2018). Aineistolähtöinen sisällönanalyysi toteutetaan tämän tutkimuksen tapauksessa haastatteluja analysoidessa ryhmittelemällä ja teemoittelemalla haastattelumateriaalia ja poimimalla aineistosta esille etenkin tutkimuksen tutkimuskysymysten kannalta relevantteja seikkoja.

1.5 Tutkielman teorettinen viitekehys ja rakenne

Tutkielman teorettinen viitekehys on visuaalisesti kuvattu alla kuviossa 1. Kuviossa teorettisen viitekehysten pohjana toimii vakuutusyhtiön riskienhallinta, joka ohjaa pitkälti vakuutusyhtiön päätöksiä ja valintoja siitä, millaisia riskejä vakuutetaan ja millaisia ei. Tästä syystä sisempänä viitekehyksessä on riskin vakuutuskelpoisuus. Se on tärkeä osa vakuutusyhtiön riskienhallintaa, muttei kuitenkaan ainut tapa toteuttaa sitä.

Teoreettisessa viitekehyksessä melko keskiössä on kyberriskit, jotka ovat tämän tutkielman keskeisimpiä aiheita. Kyberriskit kuuluvat osin vakuutuskelpoisuuden sisälle johtuen siitä, että monet kyberriskit ovat vakuutettavissa, mutteivät kuitenkaan kaikki. Kyberriskien sisälle muodostuu viitekehyksessä laatikko kybervakuuttamiselle. Kybervakuutus kuuluu sekä kyberriskien, että vakuutuskelpoisuuden piiriin, sillä luonnollisesti kybervakuutus tulee ajankohtaiseksi vakuutuskelpoisten kyberriskien kohdalla. Kybervakuutuksen sisällä viitekehyksessä on kyberrikollisuus, joka on tutkielmassa keskeinen aihe, sekä lähtökohtaisesti vakuutettavissa kybervakuutuksella. Kyberriskien laatikko ulottuu viitekehyksessä kuitenkin myös vakuutuskelpoisuuden ulkopuolelle, sillä kaikki kyberriskit eivät ole vakuutettavissa. Näihin lukeutuu viitekehyksessä esimerkiksi kybersota, joka on myös tutkielmassa tärkeä käsiteltävä teema.



Kuvio 1. Tutkielman teoreettinen viitekehys

Tutkielma jakautuu viiteen eri lukuun. Ensimmäinen luku on johdanto, jota seuraa kaksi teorialukua, empirialuku, sekä tutkielman yhteenveto. Johdanto esittelee tutkielman aiheen ja tavoitteet, tutkimuskysymykset, sekä muut tutkimuksen kannalta olennaiset seikat, kuten keskeisimmät avainkäsitteet. Ensimmäisessä teorialuvussa käydään läpi

tutkielman taustateoriaa. Taustateorialuku käsittelee riskien vakuutuskelpoisuutta, sekä vakuutusyhtiön riskienhallintaa. Toisessa teorialuvussa, tulkintateorialuvussa, syvennytään kyberrikollisuuteen ja sen vakuuttamiseen ilmiönä, sekä kybersodan piirteisiin.

Empirialuvussa esitellään tutkielman tutkimusaineisto sekä tulokset. Lisäksi luvussa käsitellään aineistossa ilmenneitä seikkoja liittyen etenkin tulkintateorian teemoihin. Lopun yhteenvetoluvussa tiivistetään empirialuvussa käsitellyt asiat ja peilataan näitä tutkimuskysymyksiin sekä pohditaan koko tutkielman yleistä onnistumista ja mahdollisia jatkotutkimusaiheita.

2 VAKUUTUSKELPOISUUS JA VAKUUTUSYHTIÖN RISKIENHALLINTA

2.1 Vakuutuksen ominaisuudet

Vakuutusta määriteltäessä on relevanttia aloittaa määrittelemällä käsite *riski*. Yksinkertaistettuna riskin suomenkielisiä vastineita ovat vahingonvaara, vahingonuhka ja tappionuhka (Rantala & Kivisaari, 2014, 62). Toisen määritelmän mukaan riski on mahdollisuus, että haitallinen tapahtuma toteutuu; se on siis tilanne, jossa on mahdollista, muttei varmaa, että esiintyy ei-toivottu tapahtuma, jolla on haitallisia seurauksia. Siten riskin määritelmään sisältyvät niin todennäköisyys, kuin seurauksetkin. (Suomen Riskienhallintayhdistys, ei pvm.)

Yleiskielessä riskin ja epävarmuuden käsitteet usein sekoittuvat. Riski ja *epävarmuus* on klassisesti määritelty niin, että riski viittaa objektiivisiin todennäköisyyksiin ja epävarmuus subjektiivisiin todennäköisyyksiin, jotka eivät ole mitattavissa (Knight, 1921). Riski, eli puhdas riski, viittaa objektille ei-toivotun tapahtuman mahdollisuuteen. Epävarmuus, eli spekulatiivinen riski, puolestaan on objektille ei-toivottavan tai toivottavan tapahtuman mahdollisuus. Puhdas riski ei siis tämän määritelmän mukaan huomioi positiivisia tapahtumia, toisin kuin epävarmuus eli spekulatiivinen riski. (Koskinen, 2018.)

Riskeihin voi varautua lukuisilla eri tavoilla. Perinteisesti riskienhallintakeinot jaotellaan riskien välttämiseen, pienentämiseen, siirtämiseen vakuuttamalla tai sopimuksella, ja omalla vastuulla pitämiseen. Näistä tavoista yksi ja tämän tutkielman kannalta tärkein on vakuuttaminen. Vakuutus pohjautuu riskin tasaamiseen; vakuutuksenottajat, eli riskin alaiset yksiköt, sopivat riskin tasaamisesta vakuutuksenantajan, eli vakuutuslaitoksen kanssa. Riskin toteutuessa vakuutuksenantaja korvaa riskistä koituneen vahingon vakuutuksenottajalle. Vakuutuksenottaja puolestaan maksaa vakuutuksenantajalle

vakuutusmaksua vastikkeeksi korvauksensaantioikeudesta. Tätä maksua maksetaan huolimatta siitä, toteutuiko riski tai ei. (Rantala & Kivisaari, 2014, 70.)

Vakuuttaminen perustuu ilmiöön, jota kutsutaan *suurten lukujen laiksi*. Yksinkertaistettuna suurten lukujen lain mukaan riski voidaan jakaa suuren ryhmän kesken, jolloin se tasaantuu niin, ettei se vaaranna kenenkään maksukykyä. Suurten lukujen laki muodostuu tekemällä tilastoja riskeistä ja niiden toteutumisesta. (Rantala & Kivisaari, 2014, 69.) Kun tarkkaillaan tilastoituja yksittäistä riskiä, esimerkiksi liikenneonnettomuuksia, voidaan niiden ilmaantuvuudessa huomata suuriakin eroja vuosittain; yhtenä vuonna liikenneonnettomuuksia sattuu huomattavasti enemmän, kuin seuraavana. Kun tarkastellaan tilastoa liikenneonnettomuuksista pidemmällä aikavälillä, huomataan kuitenkin vahinkojen suhteellisen lukumäärän vaihtelevan pitkän aikavälin keskiarvon ympärillä. Suurten lukujen laki mahdollistaa riskien ennustamisen riittävällä tasolla, vaikka lyhyen aikavälin tarkastelussa lukumäärät saattavat heitellä paljonkin.

Vakuutuksia on erilaisia ja erilaisille toimijoille. Karkeasti vakuuttaminen voidaan jakaa yksityisvakuuttamiseen, sekä sosiaalivakuuttamiseen. Sosiaalivakuutus on lakisääteistä, tai lain ohjaamaa vakuuttamista, jonka hoitaminen jakautuu niin yksityisten, kuin julkisten toimijoiden kesken. Yksityisvakuutus puolestaan perustuu sopimukseen vakuutuksenottajan ja vakuutuksenantajan välillä, eikä näiden sopimuksien sisältöä ohjailta laeilla yleisiä määräyksiä ja direktiivejä lukuun ottamatta. Yksityisvakuuttamista hoitavat vain yksityiset vakuutuslaitokset. (Rantala & Kivisaari, 2014, 81.) Tämä tutkielman kannalta relevanttia on tarkastella vain yksityisvakuuttamista. Yksityisvakuuttamiseen sisältyy niin henkilö-, kuin vahinkovakuutus ja niissä vakuutuksenottajana voi olla niin yksityishenkilö, kuin yritys tai muu organisaatio.

Yritys voi ja yrityksen tulee vakuuttaa itsensä erilaisilla vakuutuksilla. Karkeasti jaoteltuna ainut jokaiselle yrittäjälle pakollinen vakuutus on YEL-vakuutus, eli yrittäjän eläkevakuutus. Yritykselle, jolla on työntekijöitä, puolestaan pakollinen on myös TyEL-vakuutus, eli työntekijöiden eläkevakuutus. (Yrittajat.fi, ei pvm.) Liikerytystä kuitenkin uhkaavat lukuisat riskit, jotka voidaan karkeasti jakaa viiteen kategoriaan; omaisuusvahingon vaaraan, keskeytysvahingon vaaraan, vahingonkorvausvastuuseen, liikeriskeihin, sekä henkilövahinkojen vaaraan. (Rantala & Kivisaari, 2014, 64.)

Huomataan siis, että toisin kuin yksityishenkilöllä, suurin osa liikeyritystä uhkaavista riskeistä kohdistuu liiketoiminnan jatkumiseen, kassavirtoihin, sekä omaisuuteen. Tästä poikkeuksena on viimeinen, henkilöriskien kategoria, joka kohdistuu yrityksen henkilöstöön ja johtoon. Myös yritys voi vakuuttaa itsensä suurimman osan edellä mainituista riskeistä varalta.

Huolimatta siitä, että ainut jokaiselle yrittäjälle pakollinen vakuutus on YEL-vakuutus, kohtaavat monet yritykset esimerkiksi toimialasidonnaisia säädöksiä ja ohjeita mitä tulee vakuuttamiseen. Esimerkiksi terveys- ja sairaanhoitoalan yrittäjän tulee ottaa potilasvakuutus, kun taas yrityksen, joka omistaa ajoneuvoja, tulee huolehtia liikennevakuutus ja muut autovakuutuksen lajit kuntoon. (Rantala & Kivisaari, 2014, 441, 455–456.) Lähtökohtaisesti yrityksen tulee kuitenkin pohtia, mitkä riskit se haluaa toiminnassaan kantaa itse, ja mitkä olisi hyvä jakaa vakuuttamalla. Yleisimpiä vapaaehtoisia yritysvaluutusia ovat keskeytysvakuutus, vastuuvakuutus ja oikeusturvavakuutus. Keskeytysvakuutus turvaa vakuutetun yrityksen toiminnan tuloksen toiminnan keskeytyessä osittain tai kokonaan vahingon seurauksena. Tyypillisesti keskeytysvakuutuksesta korvataan käyttöomaisuutta kohdanneita omaisuusvahinkoja. (Rantala & Kivisaari, 2014, 572.) Toiminnan vastuuvakuutus taas korvaa yrityksen toiminnasta aiheutuneet vahingot. Vahinko voi olla henkilö- tai omaisuusvahinko ja se voi olla seurausta niin yrityksen toiminnasta, kuin esimerkiksi virheellisestä tuotteestakin. (If A, ei pvm.) Oikeusturvavakuutus yrityksen tapauksessa korvaa yritystoimintaa koskevista oikeudellisista toimista, kuten riita-, rikos- ja hakemusasioista aiheutuvia kuluja, kuten asianajo-, tai oikeudenkäyntikuluja (Rantala & Kivisaari, 2014, 351).

2.2 Riskien vakuutuskelpoisuus

Riskeihin ja niiden vakuuttamiseen liittyy olennaisesti vakuutuskelpoisuuden käsite. *Vakuutuskelpoisuus* tarkoittaa yksinkertaisuudessaan sitä, voidaanko riskiä vakuuttaa vai ei. Kaikki riskit eivät ole vakuutuskelpoisia, vaan niiden vakuuttamiselle on tiettyjä edellytyksiä (Rantala & Kivisaari, 2014, s. 77). Jos tarkastellaan vakuutuskelpoisuuden näkökulmasta yksilöä tai organisaatiota, voidaan vakuutuskelpoisuus nähdä vakuutuksenantajan arviona vakuutuksenottajan riskitasosta (Insuranceopedia, 2023).

Riskien vakuutuskelpoisuuden ymmärtämiseksi on tärkeää eritellä riskien ominaisuuksia ja niiden luokittelua; tyypillinen tapa jakaa riskit on erotella *staattiset* ja *dynaamiset riskit*. Staattiset riskit ovat kohtalaisen muuttumattomia ja yleisesti ottaen vakuutuskelpoisia riskejä. Tällaisia ovat esimerkiksi tulipalon vaara, murtovaara ja keskeytysvahinkojen vaara. Dynaamiset riskit puolestaan muuttuvat herkästi suhdanteiden ja olosuhteiden mukaan, mikä tekee niistä vaikeammin ennustettavia. Tällaiset riskit luokitellaan usein liikeriskien alle ja niihin asettuu esimerkiksi menekin ja hintojen vaihtelusta aiheutuva tappionvaara ja kilpailutilanteen muuttumisesta aiheutuvat vaarat. (Rantala & Kivisaari, 2014, 65.)

Seuraavaksi tarkastellaan edellytyksiä, joita riskin vakuutuskelpoisuudella on. Näistä ensimmäisenä tarkastellaan ennustettavuutta. Ollakseen vakuutuskelpoinen, riskin toteutumisen todennäköisyyden on oltava riittävällä tarkkuudella ennustettavissa, jotta vakuutusmaksut voidaan määrätä ennakolta. Tästä syystä esimerkiksi äskettäin esitellyt staattiset riskit ovat usein vakuutuskelpoisia, kun taas dynaamiset riskit vaativat enemmän soveltamista. Ennustettavuus ei ole kuitenkaan ehdoton vakuutuskelpoisuuden ehto; vakuutusyhtiöt voivat ottaa suuriakin riskejä, joiden ennustettavuutta ei voida etukäteen määritellä, jos vakuutusyhtiöt käyttävät omia hinnoittelumenetelmiä ja erilaista riskinottopolitiikkaa spesifin riskin kohdalla. (Rantala & Kivisaari, 2014, 77.)

Toinen edellytys riskin vakuutuskelpoisuudelle on se, että riski on edunsaajasta riippumaton. Tämä tarkoittaa käytännössä sitä, että vakuutuskorvauksen saaja ei voi omalla tahallisella toiminnallaan aiheuttaa vahinkoa, tai vaikuttaa sen määrän suurenemiseen. Vakuutussopimuksissa on vakioehtona se, ettei korvausta suoriteta, mikäli edunsaaja on itse tahallaan aiheuttanut vahingon; yritykset saattaisivat ryhtyä tarpeettoman uhkarohkeisiin liiketoimiin, jos vakuutus vastaisi kaikesta vahingosta ilman rajauksia. (Rantala & Kivisaari, 2014, 78.)

Kolmantena vakuutuskelpoisen riskin tuntomerkkinä on ajallinen stabiliteetti. Jotta vakuutusmaksu voidaan laskea, tulee riskin pysyä ajan myötä melko samansuuruisena. Mikäli on nähtävissä, että riski muuttuu huomattavasti ajan mukana ja esimerkiksi suhdanteista, hintavaihteluista, kilpailutilanteesta tai maailmantilasta riippuen, ei vakuutusmaksua voida laskea ennalta tarkkaan. (Rantala & Kivisaari, 2014, 78.)

Viimeinen keskeinen ehto riskin vakuutuskelpoisuudelle on riskin toteutumisen harvinaisuus. Jos vahinkotapahtuman toteutuminen on hyvin yleistä ja todennäköistä, kasvaa luonnollisesti myös vakuutusmaksu. Tällöin maksu saattaa jopa kasvaa niin suureksi, että se on lähes suoritettavan korvauksen suuruinen, eikä vakuutuksen ottaminen ole enää mielekästä. (Rantala & Kivisaari, 2014, 80.)

2.3 Vakuutusyrityksen riskienhallinta

Vakuutusyritys kohtaa toiminnassaan riskejä aivan kuten muutkin yritykset ja myös vakuutusyhtiön tulee harjoittaa osana toimintaansa tarkkaa riskienhallintaa toimintansa turvaamiseksi. Tässä alaluvussa syvennyttään näihin vakuutuslaitoksien kohtaamiin riskeihin sekä niiden hallintaan.

Vakuutusyrityksen riskit voidaan jakaa karkeasti kahteen luokkaan: toiminnan perusriskeihin ja operatiivisiin riskeihin. Toiminnan perusriskit jakautuvat edelleen alaluokkiin, joita ovat markkina-, henkivakuutus-, sairausvakuutus- ja vahinkovakuutusriski, sekä vastapuoli- tai luottoriski ja aineettomat hyödykkeet -riski. Näiden lisäksi kategorioiden ulkopuolelle jääviä, mutta vakuutusyhtiöitä siitä huolimatta uhkaavia riskejä ovat esimerkiksi erityisen tärkeä liiketoimintariski. (Kivisaari & Kahola, 2017, 51.)

Toiminnan perusriskit tarkoittavat siis vakuutusten myöntämisestä aiheutuneita riskejä (Kivisaari & Kahola, 2017, 50). Esimerkiksi henkivakuutusriski tarkoittaa kuolevuuden toteutumista ennustetusta poiketen, jolloin kuolevuuden kasvu aiheuttaa yritykselle tappioita kuoleman varalta otettujen henkivakuutusten kautta. Vahinkovakuutusriskillä tarkoitetaan vastaavasti odotetut korvaukset ylittävää korvausmenoa. Markkinariski puolestaan tarkoittaa markkinamuuttujien aiheuttamaa riskiä johtuen muutoksista esimerkiksi koroissa, osakkeissa, inflaatiossa tai kiinteistöjen arvossa. (Kivisaari & Kahola, 2017, 51–59.)

Operatiiviset riskit ovat määritelmältään laajin riskiryhmä, joka kohdistuu kaikkiin yrityksiin, myös vakuutusyhtiöihin. Operatiivisella riskillä tarkoitetaan tappion riskiä,

joka aiheutuu riittämättömistä tai luottamuksen pettäneistä sisäisistä prosesseista, henkilöistä tai järjestelmistä, tai ulkoisista tapahtumista (Kivisaari & Kahola, 2017, 63). Operatiivisiin riskeihin kytetään usein myös compliance-riski, joka tarkoittaa oikeudellisiin tai hallinnollisiin seuraamuksiin, tappioihin tai maineen menettämiseen liittyviä riskejä, jotka ovat seurausta siitä, että yhtiö on jättänyt noudattamatta lakeja tai muita hallinnollisia määräyksiä (Sampo Group A, 2023). Operatiivisiin riskeihin sisältyy myös tietojärjestelmiin kohdistuva riski, eli kyberriski (Kivisaari & Kahola, 2017, 65).

Vakuutustoiminta on pitkälle säädeltyä ja vakuutusyhtiöillä on erityisiä vaatimuksia ja säädöksiä toiminnan ylläpitämiseksi. Vakuutustoiminnan ehdottomia vaatimuksia on toiminnan vakavaraisuus, joka varmistaa sen, että korvauksenhakijat ja vakuutuksen ottaneet saavat korvauksensa ja suorituksensa vakuutussopimuksen mukaisesti. Vakuutuslaitoksen maksukyvyttömyys on riski, jonka toteutumisella olisi merkittävät seuraukset niin vakuutuslaitokselle, kuin vakuutuksenottajille, jotka tarvitsevat korvaukset kyseiseltä vakuutuslaitokselta. Vakavaraisuuteen liittyy olennaisesti niin sanotut kolme puolustuslinjaa, jotka turvaavat taustalla vakuutusyhtiön toimintaa ja vakavaraisuutta. Puolustuslinjoista ensimmäinen on yhtiön johdon huolellinen ja oikeellinen toiminta, toinen on tiettyjen keskeisten hallinnollisten toimintojen olemassaolo ja kolmas yhtiön sisäinen valvontajärjestelmä. (Rantala & Kivisaari, 2014, 189.) Puolustuslinjat siis toimivat pohjana vakuutuslaitoksen onnistuneelle toiminnalle ja riskien välttämislle.

Kolmen puolustuslinjan lisäksi vakuutuslaitoksilla on määrälliset vakavaraisuusvaatimukset. Nämä tarkoittavat pääomapuskureita, joita yhtiöillä tulee olla erilaisten riskien varalta. Vaatimukset ovat usein porrastettu niin, että vaatimukset tiukkenevat yhtiön tilanteen mukaan; vakavaraisuuden vaatimusten kevyt alittaminen vaatii kevyitä korjaustoimia, mutta tilanteen heikentyessä korjaustoimet tulevat vaativimmiksi ja pahimmassa tapauksessa vakuutusyhtiö joutuu lopettamaan liiketoimintansa. (Rantala & Kivisaari, 2014, 189.) Vakuutusyhtiöiden vakavaraisuutta ja taloudellista tilaa seurataan tarkoin. Vakuutusyhtiölaissa on määrätty, että vakuutusyhtiön on julkaistava vuosittain hallituksen hyväksymä kertomus yhtiön vakavaraisuudesta ja taloudellisesta tilasta (Vakuutusyhtiölaki 8 a 2 §).

Vakuutusyhtiön riskienhallinta perustuu Solvenssi II:n periaatepohjaiseen sääntelykokonaisuuteen, ORSA:n eli Own Risk and Solvency Assessment (Kivisaari & Kahola, 2017, 227). ORSA on prosessi, joka sisältää kuvan yrityksen vakavaraisuudesta, tarkastelun vakavaraisuusaseman kehittymisestä erilaisten riskien toteutumisen ja johdon mahdolliset päätökset huomioiden, sekä riskienhallinnan ja sen toimivuuden ja riittävyuden suhteessa riskiprofiiliin (Kivisaari & Kahola, 2017, 230–231). ORSA puolestaan rakentuu klassisen yritysten riskienhallintakehikon ERM:n ympärille. ERM määritellään yrityksen hallituksen, muun johdon ja henkilökunnan vetämäksi prosessiksi, jota sovelletaan strategian laadinnassa ja yrityksen koko toiminnassa ja jonka tarkoituksena on havaita tapahtumia, jotka voivat vaikuttaa yritykseen, ja hallita riskiä riskinottohalukkuuden puitteissa (Committee of Sponsoring Organizations of the Treadway Commission, 2004). Riskienhallinnan voidaan siis todeta olevan koko organisaation kattava prosessi, mikä kytkeytyy hyvin yhteen myös vakavaraisuuden kolmeen puolustuslinjaan.

2.4 Vastuunvalinta

Vakuutusyhtiöt harjoittavat toiminnassaan *vastuunvalintaa*, joka voidaan nähdä myös osana vakuutusyritysten riskienhallintaa, erityisesti vahinkovakuutusriskien osalta. Vastuunvalinta tarkoittaa vakuutustoiminnassa vakuutuksenantajan valintaa siitä, mitä riskejä otetaan ja vakuutetaan. Vastuunvalinnalla vakuutusyhtiö pyrkii saavuttamaan mahdollisimman tasapainoisen vakuutusliikkeen. (Sampo Group B, 2023.) Kukin vakuutusyhtiö määrittelee itse liiketoimintansa mukaiset vastuunvalintaperiaatteet, joilla määritellään millaisia riskejä ja millä ehdoilla yhtiö voi vakuuttaa. Vastuunvalintaperiaatteet ovat siis vakuutusyhtiökohtaisia ja niissä voi olla suuriakin eroja eri yhtiöiden välillä. (Finanssiala, 2021.)

Vakuutusliiketoiminta perustuu vakuutuksenantajan ja vakuutuksenottajan väliselle sopimukselle. Vahinkovakuuttaminen on pääsääntöisesti vapaaehtoista vakuutustoimintaa, minkä vuoksi siinä vallitsee sopimusvapaus. Tämä tarkoittaa sitä, että vakuutuksenantaja eli vakuutusyhtiö voi tietyillä perusteilla kieltäytyä myöntämästä vakuutusta ja solmimasta sopimusta vakuutuksenottajan, eli asiakkaan kanssa. Vastuunvalinta tarkoittaa siis käytännössä vakuutusyhtiön näkökulmasta

sopimuskumppaneiden, eli asiakkaiden valintaa. (Pellikka, Peilimö, Puntari & Vaitioma 2020, 77.) Vakuutusyhtiöillä on erilaisia periaatteita mitä tulee vastuunvalinnan harjoittamiseen ja asiakkaiden valitsemiseen. Vakuutusyhtiön tulee kuitenkin aina perustella asiakkaalle vakuutushakemuksen hylkäämispäätös, tai olemassa olleen vakuutussopimuksen irtisanomispäätös (Vakuutussopimuslaki 1994/543, 2:6a).

Hyvän vakuutustavan mukaan vakuutusyhtiön tulee selvittää potentiaalisen asiakkaan vakuutusturvan tarve ammattimaisesti, huolellisesti ja asiantuntevasti, tavoitteena tehdä asiakkaan tarpeiden mukainen vakuutussopimus. Yleisiä periaatteita, joita yhtiön tulee yleisesti noudattaa vastuunvalinnassaan, on useita. Vakuutusyhtiö ei esimerkiksi ilman hyvää syytä saa asettaa erilaisia henkilöryhmiä eriarvoiseen asemaan esimerkiksi sukupuolen, iän, vammaisuuden tai vakaumuksen takia. Tästä huolimatta on olemassa vakuutuskohtaisia hyväksyttäviä syitä kohdella erilaisia ryhmiä perustellusti eri tavalla. Esimerkiksi henkilövakuutuksessa vakuutettavan ikä ja terveydentila vaikuttavat vakuutuksen myöntämiseen ja mahdolliseen vakuutusturvan laajuuteen ja korvausmaksuun. Hinnoitteluun saattaa vaikuttaa myös vakuutettavan pysyvä asuinpaikka, vakuutettava kohde, halutun vakuutusturvan laajuus ja vahinkojen lukumäärä. (Finanssiala, 2021.)

Vakuutusyhtiöllä on tiettyjä rajoituksia koskien myös vakuutuksen irtisanomista. Sen lisäksi, että vakuutusyhtiön täytyy perustella irtisanominen asiakkaalle aiemmin kerrotun mukaisesti, on väliä myös sillä, milloin yhtiö irtisanoo sopimuksen. Vakuutukset myönnetään vakuutuskaudeksi kerrallaan; vakuutuskausi on vuoden mittainen ajanjakso, joka ei kuitenkaan ole välttämättä kalenterivuosi, vaan määräytyy vakuutuskirjan mukaan (If B, ei pvm.). Useat vahinkovakuutukset ovat jatkuvia, eli ne jatkuvat automaattisesti vakuutuskauden kerrallaan, ellei vakuutuksenottaja, tai -antaja irtisano sopimusta. Samoin kuin vakuutusta myönnettäessä, vakuutuksenantajan kieltäytyminen sopimuksen jatkosta voi perustua vakuutusyhtiön vastuunvalintaperiaatteisiin perustuvaan yleiseen, vakuutettavaan riskiin. Tällöinkin vakuutuksen uusiminen tulee perustella asiakkaalle hyvän vakuutustavan mukaisesti. Kesken vakuutuskauden vakuutusyhtiö voi irtisanoa vakuutuksen vain vakuutusmaksun maksamisen laiminlyönnin tai muun vakuutussopimuslain määräämän syyn perusteella. (Finanssiala, 2021.)

3 KYBERRIKOLLISUUS JA VAKUUTTAMINEN

3.1 Kyberrikollisuuden lajit ja määritelmät

Jo johdantoluvussa käsiteltiin joitakin keskeisiä käsitteitä, joita kyberriskeihin ja kyberaihepiiriin liittyy. Tässä luvussa syvennytään tarkemmin siihen, millaisia eri muotoja ja lajeja kyberrikollisuudesta on ja miten nämä määritellään.

Kyberrikollisuus voidaan tyypillisesti jakaa kahteen kategoriaan; rikoksiin, jotka kohdistuvat tietotekniikkaan ja tietoverkkoihin, sekä rikoksiin, jotka tehdään näitä käyttäen mutta jotka eivät kohdistu itse tietoverkkoon. Tietotekniikkaan ja tietoverkkoihin kohdistuvia rikoksia on esimerkiksi erilaiset tietomurrot, haittaohjelmilla toteutetut tietojen kaappaukset, sekä verkkohyökkäykset, kuten palvelunestohyökkäykset. Tietotekniikkaa hyväksi käyttäen tehtyjä rikoksia on puolestaan erilaiset petokset, tietojenkalastelu, kiristyshaittaohjelmat, rahanpesu, huumausainerikollisuus sekä terrorismiin liittyvät rikokset. (Rikosuhripäivystys, ei pvm.) Huomataan siis, että kyberrikollisuutta on hyvin erilaista ja se voidaan kohdistaa eri tahoille. Tietynlaiset rikokset ovat suuri uhka yrityksille ja organisaatioille, kun taas yksittäiset ihmiset ovat alttiimpia esimerkiksi erilaisille petoksille.

Kyberrikollisuus voidaankin jakaa yleistäen neljään kategoriaan sen perusteella, kehen tai mihin rikos kohdistuu. Kyberrikos voi kohdistua yksilöihin, eli yksittäisiin ihmisiin. Tyypillisimpiä yksilöihin kohdistuvia kyberrikoksia on esimerkiksi niin sanottu ”phishing”, eli suomennettuna verkkourkinta, tietojenkalastelu tai kalastelu. (Cyber Talents, ei pvm.) Kyseessä on rikos, jolla pyritään saamaan luottamuksellisia tietoja henkilöltä esimerkiksi huijaussähköpostien ja viestien avulla, esiintyen jonakin virallisena tahona (Poliisi, ei pvm.). Samankaltaista yksilöön kohdistuvaa rikollisuutta on myös ”spoofing”, eli rikos, jossa hakkerit esiintyvät toisina henkilöinä tai virallisina tahoina ja pyrkivät saamaan joko henkilötietoja, salasanoja tai tilitietoja rikoksen kohteelta. Tavoitteena voi myös olla saada yksilö lataamaan jokin haittaohjelma omalle laitteelleen. (Folger, 2022.) Yleisimmin yksilöön kohdistuvaa rikollisuutta on myös

”spam”, eli turhien tai haitallisten viestien lähettely, sekä erilainen stalkkerointi, eli väijyminen ja henkilön seuraaminen netin välityksellä. (Cyber Talents, ei pvm.)

Toinen kategoria, johon kyberrikollisuus voi kohdistua, on organisaatiot. Luonnollisesti tässä kategoriassa rikoksen kohteena ja uhrina on jokin organisaatio tai yritys. Tässä kategoriassa rikoksen takana on usein tiimi hakkereita ja kyberrikollisia, jotka kohdistavat organisaatioon erilaisia haittaohjelmahyökkäyksiä ja palvelunestohyökkäyksiä. (Cyber Talents, ei pvm.) Kolmas kategoria asettaa kyberrikoksen uhan alle omaisuuden, kuten esimerkiksi luottokorttitiedot, sekä immateriaalioikeuden. Viimeinen ja monella saralla vaarallisin kategoria on yhteiskuntaan kohdistuva kyberrikollisuus. Kyseisestä ryhmästä niin vaarallisen tekee se, että siihen sisältyy esimerkiksi kyberterrorismi ja muut kokonaiseen yhteiskuntaan kohdistuvat kyberrikokset. (Cyber Talents, ei pvm.)

Syvennyttään nyt erityisesti organisaatioita ja yhteiskuntaa uhkaaviin kyberrikoksiin, jotka ovat tämän tutkielman kannalta keskeisimpiä rikosmuotoja. Rikoksen uhrina on erityisen usein yritys tai valtionhallinto, kun kyseessä on tietotekniikkaan kohdistuvat rikokset. Tällöin rikoksella aiheutetaan haittaa tietojärjestelmille tai ohjelmille; esimerkiksi tietoliikenteen häirintä, tietojärjestelmien häirintä ja tietomurrot ovat yritysten tyypillisesti kohtaamia kyberrikoksia. (Rikoksentorjuntaneuvosto, ei pvm.) Yritysten sekä hallintoelinten kohtaama suuri uhka on niin kutsutut DDoS-hyökkäykset, eli Distributed Denial-of-Service -hyökkäykset. Kyseessä on palvelunestohyökkäys, jolla estetään verkkosivuston tarkoitettu käyttö ja niitä voidaan hyödyntää joko yksittäisinä toimina, tai harhautuksena suuremman skaalan kyberhyökkäyksessä. Onnistuneella palvelunestohyökkäyksellä voi olla yritykselle tuhoisat vaikutukset, sillä ne voivat vaikuttaa sähköisiin palveluihin jopa kuukausien ajan ja ne voivat häiritä yrityksen toimintaa vaikuttaen sen talouteen, brändiin, sekä asiakaskuntaan. (Panda Security, 2022.) Palvelunestohyökkäys toteutetaan esimerkiksi kuormittamalla kohdepalvelua tai verkkoliikennettä ylimääräisellä liikkeellä, usein lukuisista eri lähteistä bottiverkolla (Traficom, 2022).

3.2 Kybersota verrattuna kyberrikollisuuteen

Kybersota poikkeaa monin tavoin kyberrikollisuudesta, niin sen tavoitteiden ja pyrkimysten, toteutuksen, kuin vakuutuskelpoisuudenkin puolesta. Kybersodalle ei ole olemassa yksiselitteistä ja universaalia määritelmää. Kybersodankäynnille on saatu johdettua määritelmä, jonka mukaan kybersodankäynti tarkoittaa kyberhyökkäysten käyttöä ja hyödyntämistä sotatarkoituksiin, tai sodan kaltaisilla tarkoituksilla. Kybersota puolestaan seurauksena tästä tarkoittaa sotatilannetta, jossa sotaa käydään vain kybersodankäynnillä ja sen välineillä. Satunnaisesti nämä käsitteet myös sekoittuvat toisiinsa. (Robinson, Jones & Janicke, 2015.)

Kybersota eroaa kyberrikollisuudesta ensinnäkin tavoitteiden ja pyrkimysten osalta. Siinä, missä kyberrikollisuuden taustalla on usein rahallinen motiivi ja sen kohteena on yksittäiset yritykset, on kybersodan tarkoituksena toteuttaa tai tukea sodankäyntiä eri valtioiden välillä. Kybersota voi sisältää hyökkäyksiä taloudelliseen infrastruktuuriin tai julkiseen infrastruktuuriin, kuten patoihin tai elektroniikkaverkkoihin. Hyökkäykset voivat kohdistua myös turvainfrastruktuuriin, kuten liikenteenohjaukseen tai yleisiin varoitussysteemeihin. Hyökkäykset voivat kohdistua myös suoraan armeijan resursseihin tai organisaatioihin. (Fortinet, ei pvm.) Koska kybersodassa hyökkäykset voivat kohdistua tärkeään infrastruktuuriin, sillä on suorat vaikutukset sekä hyökkäyksen kohteeksi joutuneen valtion toimintaan, että sen mahdollisuuksiin puolustautua fyysistä sodankäyntiä vastaan. Kybersodankäyntiä voidaankin käyttää sekä itsenäisenä hyökkäyksenä tarkoituksena esimerkiksi sotkea valtion informaatioliikennettä tai urkkia valtiosalaisuuksia, mutta myös yhdessä fyysisen sodankäynnin kanssa. (Robinson, Jones & Janicke, 2015.)

Toisekseen kybersota eroaa kyberrikollisuudesta toteutuksen osalta. Kybersotaan liitettäviä hyökkäyksiä on erilaisia ja ne voidaan jakaa päätyyppeihin, kuten kyberrikollisuudenkin lajit ja osa lajeista on yhteisiä kyberrikollisuudelle sekä kybersodalle. Kybersodankäynnin toteutustyyppinä ovat vakoilu, sabotaasi, palvelunestohyökkäykset eli DoS-hyökkäykset, elektroniikkaverkon häirintä, propaganda, taloudellinen häirintä, sekä yllätyshyökkäykset (Imperva A, ei pvm.).

Vakoilulla tarkoitetaan tässä yhteydessä toisten valtioiden tarkkailua tarkoituksena varastaa valtiosalaisuuksia tai muuta arkaluontoista tietoa. Tämä voidaan toteuttaa

erilaisilla kybertoimilla; vihollinen voi käyttää esimerkiksi bottiverkkoa. Bottiverkko voidaan ajatella ”zombie armeijana”, sillä se on suuri joukko kaapattuja laitteita, joita voidaan hallita etäältä ja laitteen omistajan tietämättä. (Imperva B, ei pvm.) Myös verkkourkintaa voidaan käyttää apuna; tällöin rikoksen tekijä naamioituu luotettavaksi lähteeksi ja saa kohteen jakamaan arkaluontoista informaatiota tai lataamaan haitallisen ohjelman tietokoneelle (Imperva C, ei pvm.). Näiden toimien tarkoituksena on heikentää tietokonetta tai turvaverkkoja ennen arkaluontoisen tiedon suodattamista (Imperva A, ei pvm.).

Sabotaasi linkittyy jonkin verran vakoiluun, sillä siinäkin keskiössä on arkaluontoisen informaation varastaminen tai tuhoaminen. Hallituksen toimien tulee määritellä mikä tiedosta on arkaluontoista ja tunnistaa riskit, mikäli tämä tieto pääsee vuotamaan. Sabotaasissa suuri uhka valtiolle on myös sisäiset uhat, joita vihollinen voi hyödyntää sabotaasissaan. Tällaisia sisäisiä uhkia on esimerkiksi tyytymättömät tai huolimattomat työntekijät, tai työntekijät, joilla on kytköksiä ja kannusteita toimia hyökkäävän maan puolesta. (Imperva A, ei pvm.)

Jo aiemmassa luvussa käsitellyt palvelunestohyökkäykset, eli DoS-hyökkäykset ovat myös tyypillinen työkalu kybersodankäynnissä. Palvelunestohyökkäykset estävät oikeita käyttäjiä käyttämästä nettisivua kuormittamalla sen valheellisilla palvelupyynnöillä, pakottaen nettisivun käsittelemään ne; tämä johtaa nettisivun kaatumiseen tai toiminnan häiriintymiseen niin, ettei nettisivu toimi toivotulla tavalla. Tämän tyyppinen hyökkäys voi häiritä erilaisia operaatioita ja systeemien toimintaa. (Imperva A, ei pvm.)

Sähkö- ja elektroniikkaverkostoihin hyökkääminen mahdollistaa kriittisten systeemien käytön eston, häiriöt infrastruktuurissa, sekä jopa fyysiset vahingot yksilöille. Sähköverkkojen toimintaan vaikuttaminen häiritsee myös kommunikaatiota, sillä esimerkiksi nettiverkot ja puhelinverkostot on hakkereiden kaadettavissa ja tällöin kohdemaalta viedään tekstiviestien ja muun sähköisen kommunikaation mahdollisuus. (Imperva A, ei pvm.)

Kolmanneksi kybersota eroaa kyberrikollisuudesta sen vakuutuskelpoisuuden suhteen. Yrityksen tai organisaation menetykset ja vahingot, jotka voidaan linkittää tietyn maan

tai hallituksen toimiin, eli tässä yhteydessä kybersotatoimiin, ovat tyypillisesti rajattu ulos vakuutuksen piiristä, sillä riskit ovat niin suuria ja yksittäisten vakuuttajien kapasiteetin ulottumattomissa (The Association of British Insurers A, ei pvm.). Tarkemmin kybersodan vakuuttamiseen liittyvistä seikoista kerrotaan luvussa 3.4.

3.3 Kyberriskien hallinta

Kyberriskit ovat vuoden 2023 tärkein globaali liiketoimintariski (Allianz Global Corporate & Specialty, 2023). Eräs syy, miksi yritykset ja organisaatiot näkevät kyberriskin niin merkittävänä uhkana ympäri maailmaa, liittyy kyberriskien luonteeseen; kyberriski koskee kaikkia ja kaikkialla, eikä sen estämiseksi ole olemassa varmaa tapaa. Kyberriskien riskienhallinta on haastavaa, sillä se vaatii tasapainottelua teknisten ratkaisujen ja henkilöstön koulutuksen välillä (Vornanen, 2020).

National Institute of Standards and Technology, eli NIST suosittelee organisaatioita lähestymään kyberriskien hallintaa jatkuvana ja toistuvana prosessina mieluummin kuin kertaluontoisena tapahtumana. Prosessin jatkuva kehittäminen antaa organisaatiolle mahdollisuuden sisällyttää uutta informaatiota riskienhallintaprosessiin ja vastata uusiin kehityksiin riskimaisemassa ja yrityksen omissa IT-systeemeissä. (IBM, ei pvm.) Kyberriskin riskienhallinta omaa siis samoja piirteitä organisaation muunkin riskienhallinnan kanssa.

Kyberriskien hallinta voidaan jakaa neljään eri vaiheeseen: riskien tunnistamiseen, riskien arvioimiseen, riskien hallintaan ja toimintojen arvioimiseen. Riskien tunnistamisvaiheessa organisaatio arvioi sen toimintaympäristöä tunnistaakseen tämänhetkiset ja potentiaaliset riskit, jotka voivat vaikuttaa liiketoimintaan. Riskien arviointivaiheessa analysoidaan tunnistetut riskit, jotta tiedetään kuinka todennäköisesti ne vaikuttavat organisaatioon ja mikä tämä vaikutus voisi olla. Riskien hallintavaiheessa määritellään menetelmät, toimenpiteet, teknologiat ja muut toimet, jotka voivat auttaa organisaatiota hillitsemään riskejä. Viimeiseksi arviointivaiheessa arvioidaan, kuinka tehokkaita toimenpiteet ovat riskien hillitsemisessä, ja tarpeen mukaan lisätään ja muokataan toimintatapoja. (Imperva D, ei pvm.)

Kyberriskien lähteet voidaan jaotella neljään eri luokkaan: ihmisten toimiin, järjestelmävirheisiin, sisäisten prosessien epäonnistumiseen ja ulkoisiin tapahtumiin. Kyberriski voi syntyä myös useamman tapahtuman yhdistelmänä ja seurauksena. Ihmisten toiminnasta johtuvat kyberriskit voivat olla tahattoman tai tahallisen toiminnan seurausta, kuten myös toimimatta jättämisen seuraus. Tällaiset ihmisten toimet ovat usein organisaation sisäisiä, ja ne voidaan edelleen jakaa erehdyksiin, virheisiin ja laiminlyönteihin. (Cebula & Young, 2010.) Tästä voidaan päätellä kyberriskien hallinnan olevan monimutkainen prosessi, jonka täytyy huomioida kaikki edellä mainitut lähteet kyberriskin syntymiselle. Ihmisen toiminnan vaikutuksen myötä kyberriskin hallinnassa keskiöön nousee henkilöstön ja yksilöiden kouluttaminen.

Keskeinen osa kyberriskien hallintaprosessia on organisaation tietoturva ja sen ylläpitäminen. Kyberriskien hallinnassa ensilinjan prosessi on hankkia kattava ja laadukas valikoima ohjelmistoja, jotka suojaavat organisaation tieto-omaisuutta. Tämä sisältää esimerkiksi vakoilunesto-ohjelmia, ei-toivottujen mainosten tunnistus- ja esto-ohjelmia ja haittaohjelma- ja antivirussuojaa, jotka ovat kaikki hankittu luotettavalta ja hyvämaineiselta tarjoajalta. (Brockett, Golden & Wolman, 2012.)

3.4 Kyberriskien vakuuttaminen

Kyberriskien vakuutuskelpoisuutta tarkastellessa on olennaista palata vakuutuskelpoisuuden määritelmiin, joita käsiteltiin laajemmin luvussa 2.2. Rantalan ja Kivisaaren mukaan riskin ollakseen vakuutuskelpoinen, sen tulee täyttää tietyt kriteerit; riskin toteutumisen tulee olla riittävän ennustettavaa, vahingon riskin tulee olla edunsaajasta riippumaton, riskin tulee säilyä riittävän stabiilina yli ajan ja vakuutustapahtuman toteutumisen tulee olla riittävän harvinaista. (Rantala & Kivisaari, 2014, 77-80.)

Asetetaan nyt kyberriskit ja näiden ominaisuudet vakuutuskelpoisuuden raameihin. Riskin tulee olla ennustettava sen ollakseen vakuutuskelpoinen, sillä vakuutusmaksut tulee voida määrätä ennalta (Rantala & Kivisaari, 2014, 77). Kyberriskien ennustettavuuteen liittyy haasteita, sillä kyberriskit muuttuvat jatkuvasti kehittyvän teknologian mukana. Kyberriskejä arvioidaan ja kybervakuutusten ehtoja kirjoitetaan jo

tapahtuneiden tapahtumien ja skenaarioiden pohjalta, eikä tulevaisuuden mahdollisia kyberuhkia ole mahdollista nähdä ennalta tässä hetkessä (Munich Re A, 2020). Ajalliseen stabiliteettiin riittyy pitkälti samat haasteet kyberriskien tapauksessa, kuin niiden ennustettavuuteenkin. Kyberriskien ei voida ajatella säilyvän stabiileina ja keskiarvillisesti muuttuvina ajan yli, sillä teknologia ja tämän myötä kyberriskit kehittyvät ja muuttuvat jatkuvasti.

Bienerin, Elingin ja Wirfsin (2014) mukaan suurimmat haasteet kybervakuuttamisessa liittyvätkin juuri vahinkojen satunnaisuuteen, tietojen epäsymmetriaan, sekä riskin mahdolliseen äkilliseen ja suureenkin muutokseen. Kyberriski on kuitenkin haasteistaan huolimatta vakuutuskelppoinen riski.

Kybervakuutuksen markkina-ala osana yritysten vakuutuspoolia on ollut kuluneina vuosina räjähdysmäisessä kasvussa ja sen ennustetaan jatkavan kasvuaan samaan suuntaan. Vuonna 2019 globaali kybervakuutusmarkkina oli suuruudeltaan 5,9 miljardia, kun taas viimeisimmän Munich Re:n raportin mukaan vuonna 2023 vastaava luku oli noin 14 miljardia, lähes kolminkertainen luku. Munich Re:n arvion mukaan vuoteen 2027 mennessä kybervakuutusmarkkina on suuruudeltaan 29 miljardia euroa, mitä perustellaan esimerkiksi kyberhyökkäysten tiheyden ja monimutkaisuuden kasvaessa. (Munich Re B, 2024.)

Kybervakuutuksien ehdot ja tarjoamat turvat ovat melko yhtenevät eri vakuutusyhtiöiden ja vakuutuksentarjoajien kesken. Lähtökohtaisesti kybervakuutus korvaa menetyksiä, jotka seuraavat tietojärjestelmien tai –verkkojen vaurioista. Kybervakuutukset tarjoavat kuitenkin tämän sisällä hyvinkin laajaa turvaa. Jo ennen vahingon tapahtumista, kybervakuutus voi tarjota asiantuntija-apua tietoverkkojen heikkouksien tunnistamisessa, sekä henkilöstön kouluttamisessa, jottei vahinkoa pääsisi tapahtumaan. Vahingon tapahtuessa kybervakuutus puolestaan korvaa tietovuodon käsittelystä seuraavia kuluja, kuten asiakkaiden informoimisesta, sekä lakitoimista johtuvia kuluja. Useimmissa kybervakuutuksissa myös vahingon tapahtuessa tarjotaan asiantuntija-apua järjestelmien arvioimiseksi ja vastaavien tapahtumien välttämiseksi tulevaisuudessa. Useimpiin kybervakuutuksiin liittyy myös usein tärkeimpänä nähty turvapalikka, toiminnan keskeytyksen kulujen korvaaminen. Mikäli kyberhyökkäys keskeyttää yrityksen

toiminnan, vakuutus korvaa keskeytymisen seurauksena menetetyt tuotot, sekä mahdolliset suuremmat kustannukset toiminnan käynnistyttyä uudelleen. (The Association of British Insurers B, ei pvm.)

3.5 Kybersota ja vakuuttaminen

Kybersota on riski, jota vähän, jos ollenkaan vakuutetaan tavanomaisilla vahinkovakuutustuotteilla (Keskinäinen Vakuutusyhtiö LähiTapiola, 2022). Syyt tähän ovat moninaiset ja niiden ymmärtämiseksi tulee palata vakuuttamisen peruseräpäätteisiin.

Vakuutusehdot on luotu normaaliin arkeen, jossa voidaan soveltaa hyväksytyjä lakeja ja viranomaismääräyksiä. Vakuutuksen ajatus on varautua arjen erilaisiin riskeihin, joiden todennäköisyys voidaan riittävällä tasolla arvioida. Vahingon on oltava ennalta-arvaamaton, eli ei tahallaan aiheutettu tai yksittäisen ihmisen päätöksen seurausta. Riskit, jotka tapahtuvat yhtäaikaaisesti laajalle joukolle, kuten esimerkiksi sota, pandemia, tai globaalista ilmastonmuutoksesta johtuvat vahingot, joudutaan rajaamaan vakuutusehtojen ulkopuolelle. Näin myös sota on lähestulkoon kaikissa vahinkovakuutuksissa rajattu vakuutusturvan ulottumattomiin; sen aiheuttamien vahinkojen suuruutta on vaikea tai mahdoton ennakoida ja riskille on vaikea laskea todellista vakuutusmaksua. (Keskinäinen Vakuutusyhtiö LähiTapiola, 2022.)

Lloyd's on maailman suurin jälleenvakuutusmarkkina, joka on vuonna 2022 luonut kybersotarajoitusehdot koskemaan kybervakuutuksia. Koska Lloyd'sin ehdot koskettavat suurinta osaa vakuutustoimijoista jälleenvakuutusketjujen kautta, ovat Lloyd'sin sotarajoitusehdot yleisesti ottaen sovelletut. Lloyd'sin sotarajoitusehto käytännössä määrää, että kybervakuutuksista tulee poislukea kaikki valtion tukemat tai suorittamat kyberhyökkäykset, ellei Lloyd's toisin määrää. Rajoitusehdon tulee esimerkiksi poissulkea sodasta johtuvat menetykset, oli sotaa julistettu tai ei, sekä poissulkea valtion tukemista kyberhyökkäyksistä johtuvat menetykset, mikäli hyökkäys merkittävästi heikentää valtion toimintakykyä, tai valtion turvallisuusresursseja. (Clifford Chance, 2023.) Lloyd'sin sotarajoitusehdon vaikuttaessa niin suureen osaan vakuutuksen tarjoajista, on kybersota lähes pakonkin edessä rajattu ulos kybervakuutuksien piiristä.

4 KYBERVAKUUTTAMINEN NYT JA TULEVAISUUDESSA

4.1 Aineiston kerääminen ja analyysi

Tutkielman empiirisen osuuden aineistonkeruumenetelmänä toimivat laadulliset teemahaastattelut kybervakuuttamisen asiantuntijoiden kanssa. Haastattelut olivat puolistrukturoituja teemahaastatteluja, joissa käytettiin yhtenevää, valmista haastattelurunkoa. Teemahaastatteluissa käydään läpi tiettyjä teemoja ja aiheita, joiden ympärillä keskustellaan avoimesti. Teemahaastattelu mahdollistaa haastattelun tutkijan näkökulmasta ja tuo tutkittavien äänet kuuluviin. (Hirsjärvi & Hurme, 2022.) Haastatteluiden tavoitteena oli saada laaja ymmärrys kybervakuuttamisesta ilmiönä, syventyä keskeisimpiin yritysten kohtaamiin kyberrikollisuuden muotoihin sekä näiden vakuutuskelpoisuuteen, sekä käsitellä kybersotaa ilmiönä.

Empirialuvun haastattelut toteutettiin loka- ja marraskuussa syksyllä 2023. Haastattelut toteutettiin videohaastatteluina Microsoft Teamsin välityksellä ja haastattelut tallennettiin Microsoft Teamsin nauhoitustoimintoa käyttäen analyysiä varten. Haastattelut toteutettiin yksilöhaastatteluina, eli kussakin haastattelutilanteessa oli paikalla tutkija ja haastateltava. Kukin haastattelu litteroitiin tallenteen pohjalta ennen analyysin aloittamista. Litteroinnissa jätettiin huomiotta tutkimuksen kannalta epärelevantit täytesanat ja teksti litteroitiin puhekielimäisenä kunkin haastattelun mukaan.

Haastateltavia käsitellään tässä tutkielmassa nimettöminä ja heihin viitataan Asiantuntijoina kirjaimilla A-C. *Asiantuntija A* työskentelee suomalaisessa vahinkovakuutusyhtiössä cyber underwriterina. Työnkuvassaan hän työskentelee tiiviisti riski-insinöörin kanssa ja underwriterina katsoo kybervakuutusjärjestelyn kokonaiskuvaa, ehtoja ja hinnoittelua.

Asiantuntija B työskentelee cyber underwriterina saksalaisessa vakuutuskonsernissa. Hän tekee töitä myös teknologian varallisuusvastuuvakuutuksien parissa. Tehtävässään hän kertoo arvioivansa kyberriskejä ja kybermarkkinaa, sekä toimivansa meklarien kanssa pyrkien löytämään oikeat riskit oikeaan hintaan.

Asiantuntija C työskentelee cyber underwriterina tanskalaisessa vakuutusasiamiesyhtiössä. Työtehtävässään hän arvioi yritysten kyberriskejä, hinnoittelee heille vakuutusratkaisuja, sekä neuvottelee ehdoista ja vakuutusmaksutasoista meklareiden kanssa. Hän kertoo operoivansa pääsääntöisesti vakuutusmeklareiden kanssa, eikä suorien asiakkuuksien kautta.

Tutkimusaineistoa analysoidaan aineistolähtöisen sisällönanalyysin avulla. Käytännössä aineistoa käsiteltiin vaiheittain ja poimien litteroidusta materiaalista tutkimuskysymyksien kannalta olennaisia lausuntoja. Tutkielman ensimmäinen tutkimuskysymys on “Mitkä tekijät vaikuttavat kyberrikollisuuden eri muotojen vakuutuskelpoisuuteen?”. Toinen tutkimuskysymys on “Miten kybersota ja kyberrikollisuus eroavat toisistaan vakuutuskelpoisuuden suhteen?”. Kolmas tutkimuskysymys asettaa teeman puolestaan tulevaisuusaspektiin, sen ollessa “Miten tulevat muutokset kybersodan ja kyberrikollisuuden luonteessa sekä toisaalta vakuutuksen “underwritingissa” vaikuttavat niiden vakuutuskelpoisuuteen?”

4.2 Kyberrikollisuus ja sen vakuutuskelpoisuus

Haastattelurungon ensimmäisessä kysymyksessä käsiteltiin sitä, millaista kyberrikollisuutta yritykset yleisimmin kohtaavat. Kaikki haastateltavat nostivat yhdeksi yleisimmäksi yritysten kohtaamista hyökkäysmalleista ransomware-hyökkäykset, eli kiristyshaittaohjelmahyökkäykset. Asiantuntija A kuvaa kiristyshaittaohjelmahyökkäyksiä seuraavalla tavalla:

“Siinä se pääjuttu on se, että pyritään halvaannuttamaan sitä firman toimintaa, eli esimerkiksi saadaan jotkut systeemit alas silleen, että se firma ei vaikka voi tuottaa lisää tuotteita.”

Myös asiantuntija C nimeää yleisimmiksi muodoiksi haittaohjelmahyökkäykset, mutta näiden lisäksi myös palvelunestohyökkäykset, sekä erilaiset tietomurrot. Hän kuitenkin tarkentaa näiden olevan yleisimpiä tapauksia, joista syntyy yrityksille häiriöitä ja jotka tulevat vakuutusyhtiöiden tietoon. Yritykset kohtaavat puolestaan jopa päivittäin tietomurtojen yrityksiä, sähköpostihuijauksia, sekä muita toimia, joilla pyritään pääsemään yrityksen tietojärjestelmiin sisään oikeudettomasti ja käynnistämään esimerkiksi haittaohjelmahyökkäys. Tyypillisesti pelkiksi yrityksiksi jäävät hyökkäykset eivät kuitenkaan asiantuntija C:n mukaan tule yleisimmin vakuuttajien käsiteltäväksi, eikä näistä yleensä synny vahinkoja.

Asiantuntijalta A kysyttiin tarkentava kysymys siitä, onko kyberrikollisuuden ilmenemistavoissa vaihtelua tarkastellessa suomalaista yrityskenttää, sekä globaalia markkinaa. Hänen mukaansa suomalaisellakin kentällä kiristyshaittaohjelmahyökkäyksiä tapahtuu. Hän mainitsee myös tyypilliseksi ilmiöksi pienempiin yrityksiin hyökkäämisen, sillä esimerkiksi suurissa globaaleissa konserneissa emoyhtiö on usein suojattu niin hyvin, että sinne hyökkääminen on vaikeaa. Pienempi firma osana tuotantoketjua voi asiantuntija A:n mukaan usein olla heikomman suojaustason takana, jolloin sinne on helpompi hyökätä, mutta sillä voidaan saavuttaa suuret vaikutukset. Hyökkäys tuotantoketjuun voi vaikeuttaa monen yrityksen toimintaa ja samalla antaa vipuvartta hyökkääjälle useamman yrityksen kiristämiseen samanaikaisesti.

Haastattelurungossa seuraavana käsiteltiin sitä, kuinka monelle ensimmäisessä kohdassa mainituista yleisistä rikoslajeista on tarjolla vakuutusturvaa. Asiantuntija C:n mukaan vakuutusturvaa on tarjolla kaikkiin hänen mainitsemiin rikoslajeihin, poislukien laskuhuijaukset, joissa kybervakuutus korvaa selvittelykustannukset ja muut tekniset seikat, mutta itse siirretty rahasumma kuuluu tyypillisesti rikosvakuutuksen piiriin. Asiantuntija C:n mukaan on vaikea keksiä kyberrikollisuuden muotoa, jolle ei lähtökohtaisesti olisi tarjolla vakuutusturvaa.

Asiantuntija A:n mukaan puolestaan kyberrikollisuuden muodot on turvattu enemmänkin sen mukaan, millaisia kustannuksia niistä koituu, kuin spesifiä rikoslajia vastaan. Tässä tapauksessa vakuutuksilla korvataan esimerkiksi haittojen minimointia ja datan palautusta, kiristykseen liittyviä kustannuksia, sekä esimerkiksi tilanteita, joissa

kyberrikollisuuden avulla saadaan otettua varoja suoraan yrityksestä. Asiantuntija A:n mukaan kuitenkin esimerkiksi lunnasmaksujen korvaamisessa on eroja vakuutusyhtiöiden välillä.

Asiantuntija B tarkastelee kyberrikollisuuden vakuutusturvaa kyberrikollisten motiivien kautta. Hänen mukaansa rahan motivoima kyberrikollisuus on oletettavasti yleisin muoto, mutta sen takana voi olla myös esimerkiksi poliittiset motiivit, erilaiset haktivistiryhmät, sekä puhdas kokeilunhalu. Vakuutusturvaa on hänen mukaansa tarjolla eniten rahan motivoimaan kyberrikollisuuteen, sillä suurin osa kybervakuutuksista suuryritysten puolella lähtee kybervahinkojen ja -rikollisten aiheuttamien taloudellisten vahinkojen korvaamisesta.

Haastatteluissa tarkasteltiin seuraavaksi puolestaan sitä, millaisia kyberriskejä ei voi vakuuttaa ja miksi kaikki kyberriskit eivät ole vakuutuskelpoisia. Kaikki haastateltavista nostivat ensimmäisenä vakuutuskelvottomana riskinä esille kybersodan, jota kuitenkin käsiteltiin syvällisemmin vasta myöhemmin haastattelurungossa omana kohtanaan. Asiantuntija C nosti esille infrastruktuurivahingot:

“Mulla tulee ehkä isoimpana mieleen semmoiset infrastruktuurivahingot, eli jos puhutaan että koko maailmanlaajuinen internet on alhaalla, niin toki yksittäisen kybervakuutusratkaisun ei ole tarkoitus tätä kattaa. Ja tätä on hyvin hankala vakuuttaa, enkä usko, että tätä oikeastaan voikaan vakuuttaa, koska kyse on systeemisistä.”

Myös Asiantuntija B korosti aggregaation merkitystä vakuutus päätöksissä, eli sitä onko jokin riski liian suuri otettavaksi vakuutusyhtiön toimesta.

“Toisenlaista akkumulaatiota ja aggregaatiota, mitä ei välttämättä pystytä vakuuttamaan, on esimerkiksi tällaiset isot, massiiviset IT-palveluntarjoajat”

Asiantuntija B nosti esimerkiksi saksalaisen ohjelmistovalmistajan SAP, joka valmistaa toiminnanohjausjärjestelmiä Euroopassa.

“Jos SAP:illa on iso kybervahinko, se voi kenties jollain todennäköisyydellä levitä sitten suureen osaan yrityksiä, jotka käyttää myös SAP-toiminnanohjausjärjestelmiä.”

Asiantuntija B:n näkemykset aggregaatiosta siis kytkeytyvät monin tavoin asiantuntija C:n lausuntoihin infrastruktuuririskeistä, sillä molemmissa tapauksissa vahingot voisivat levitä hallitsemattomasti laajalle eri toimijoihin, eikä yksittäinen vakuutusyhtiö tai kybervakuutus kykenisi enää kantamaan riskiä. Asiantuntija C:n näkemyksen mukaan systeemivahinkojen ja infrastruktuurien ulkopuolella ei kuitenkaan ole kovinkaan montaa riskiä, mitä ei voisi vakuuttaa, vaan kyseeseen tulee tällöin ehdot ja vakuutusmaksut.

“Jos on tosi ison riskin toimialasta kyse ja jonkin sortin poikkeuksellinen turvapalikka, niin sehän on vaan kyse vakuutusmaksusta lopun kaiken, että jos se tarpeeksi korkealle saadaan asetettua niin... Kybervakuutukset, mä näen että se on aika joustava vakuutuslaji. Siinä näkyy paljon että siinä pelataan vakuutusmaksuilla ja omavastuutasoilla vakuutettavuuden kannalta.”

Myös Asiantuntija A nosti vastauksessaan esille niin kutsutut “widespread events”, eli yksittäiset hyökkäykset, jotka voivat aiheuttaa suuren aggregaatoriskin ja vaikuttaa laajalti toimialaan. Näihin liittyy esimerkiksi infrastruktuurin häiriöt, myöhemmin käsiteltävä sota, sekä luonnonkatastrofeista aiheutuvat vahingot, jotka ovat myös asiantuntija A:n mukaan rajattu pois vakuutuksen piiristä. Hänen mukaansa kuitenkin yrityskohtaisella tasolla voidaan esimerkiksi nähdä, että yrityksen tietoturvassa on isoja aukkoja tai se ei ole toivotulla tasolla, ja tämä voi vaikuttaa päätökseen vakuuttamisesta. Toisaalta tämä voi myös synnyttää ratkaisuja, jotka sekä hyödyttävät vakuutettavaa yritystä, että pienentävät vakuutusyhtiön riskiä:

“Sit jos nähdään et se (tietoturva) ei oo riittäväällä tasolla niin me ei vakuuteta sitä, mut siihen voidaan myös löytää sellasia ratkasuja et jos niillä vaikka muuten on melko hyvä systeemi mut vaikka niiden varmuuskopiointi ei oo riittäväällä tasolla, niin me voidaan vaikka kirjottaa silleen et me vakuutetaan ne mut me vaikka alennetaan sitä määrää mitä me vakuutetaan jos se vahinko tapahtuu ransomware-hyökkäyksestä. Et me voidaan ettiä et okei muuten tää on

jees, mut niillä ei oo oikein responsea tähän, niin sitten lasketaan tätä riskiä ja vakuutetaan niitä muuten. Ja sitten siinä vakuutusyhtiö samalla tulee toimineeks vähän sellasena tietoturvakonsulttina, että ohjaa niitä vähän silleen että mitä teidän pitäis kehittää että ootte alan standardien mukana.”

4.3 Kybersota ja sen vakuuttaminen

Aiemmin haastattelurungossa käsiteltiin kyberriskejä, joille ei ole tarjolla vakuutusturvaa ja jotka ovat täten vakuutuskelvottomia. Jokaisessa haastattelussa eri asiantuntijoiden A, B ja C kanssa esille nousi kybersota, mutta sen käsittely jätettiin myöhempään vaiheeseen.

Kuten jo tämän tutkielman teoriaosuudessa todettiin, kybersota on tällä hetkellä rajattu lähes täysin ulos perinteisistä kybervakuutuksista. Haastatteluissa haluttiin kerätä näkökulmia ja syitä tämän ilmiön taustalla. Haastateltavilta kysyttiin kysymys: “Kybersota on käytännössä kokonaan suljettu vakuutusturvan ulkopuolelle. Mitkä ovat merkittävimpiä syitä tämän taustalla?”.

Asiantuntija B kertoi haastattelussaan tapahtumista, jotka nostivat kybersodan ja sotarajoitusehdot merkittävällä tavalla keskusteluun vakutusmaailmassa. Venäläinen kyberhyökkäystiimi Sandworm on hakkerointitiimi, joka toimii Venäjän GRU:n alla, ja jonka erikoisalaa on yritysten tietoverkkojen hakkerointi ja pysäyttäminen yrityksen toiminnan estämiseksi. Vuonna 2014 Krimin valloittamisen jälkeen Venäjä teki Ukrainasta “kyberhyökkäyslaboratorion”, ja Sandworm suoritti useita hyökkäyksiä kriittiseen infrastruktuuriin Ukrainassa. Vuonna 2017 tapahtui yksi historian suurimpia kyberhyökkäyksiä, kun Sandwormin luoma haittaohjelma NotPetya pääsi Ukrainaan hyökkäämisen myötä leviämään hallitsemattomasti ympäri maailmaa, vaikuttaen esimerkiksi logistiikkayhtiö Mærskin, sekä lääketeollisuuden firman Merckin toimintaan huomattavalla tavalla.

Kyseisestä hyökkäysketjusta seurasi suuria vahinkoja kybervakuuttajille, sillä kybervakuutuksissa ei ollut spesifejä sotarajoitusehtoja. Asiantuntija B kuvaa keskustelua, joka seurasi suurta NotPetya-haittaohjelmahyökkäystä:

“Sit alettiin keskustelemaan sen (NotPetya-haittaohjelmahyökkäyksen) jälkeen, että hetkinen, mitäs tää sota on nykyisin? Siihen aikaan, 2018–2020, sotarajoitusehdot taisi olla jostain lähemmäs 100 vuoden takaa ja ne ei ehkä ollut enää niin kovin käyviä sitten enää nykymaailmassa, missä sotaa käydään monissa eri ulottuvuuksissa, kuten kyberulottuvuudessa”

Lloyd’s of London, globaali vakuutusmarkkinapaikka, kehitti uudet sotarajoitusehdot, joissa rajataan pitkälti kybersota ulos kybervakuutuksen piiristä tietyillä erityisehdoilla. Asiantuntija A viittasi jo aiemmin haastattelussa käsiteltyihin systeemiriskeihin perustellessaan kybersodan ulos rajaamista. Vakuutusmaailman standardien mukaan systeemiset riskit, kuten sota ja luonnonkatastrofit, on haluttu sulkea ulkopuolelle, sillä kyseiset riskit eivät liity enää firman profiiliin tai liiketoimintaan, eikä niitä voi ennalta ottaa huomioon.

“Jos sen (vakuutuksen) selittää palikkamatikalla, niin vakuutus... Periaatteessahan kaikki firmat, jotka ei kärsi vahinkoja, maksaa sen firman menetykset, joka kärsii vahingot. Tollaisissa systeemisissä riskeissä on just se ajatus, et kun kaikki yhtäkkiä kärsis vahingot niin sitä ei vaan vakuutusyhtiö pystyis kattamaan.”

Asiantuntija C nosti esille merkittävänä syynä sodan pois rajaamiseen valtiollisten toimijoiden resurssit. Usein valtiollisilla toimijoilla on käytössään huomattavat määrät kyberosaamista, sekä myös kyberrikollisuutta, joilla ne voivat halutessaan suorittaa hyökkäyksiä.

“Jos jokin valtiollinen toimija haluaa päästä käsiksi jonkin yrityksen tietojärjestelmiin, niin se kanssa pääsee. Että valtiollisilla tahoilla on ne resurssit, ja nimenomaan taloudelliset resurssit. --- Niin kyllä se on siitä puhtaasti, että se ei ole kauhean vakuutettava riski siinä tapauksessa.”

Asiantuntija C huomioi haastattelussa myös sen, että kaikissa yritysvakuutuksissa sota on aina ollut rajattuna ulkopuolelle, jolloin se tietyillä tavoilla ei yksinkertaisesti kuulu vakuutustuotteeseen.

Kybersodan poisrajaamista kybervakuutuksen piiristä voidaan siis perustella useilla eri tavoilla ja näin on tehty oletusarvoisesti aina, huolimatta siitä, että tarkemmat sotarajoitusehdot kybervakuutukseen muodostuivat Lloyd'sin sotarajoitusehdon myötä vasta kuluneina vuosina. Asiantuntija B:n kommentit Sandwormista ja NotPetya-haittaohjelmahyökkäyksen leviämisestä muualle maailmaan, vaikka alkuperäisenä kohteena oli Ukraina, nostivat kuitenkin esille olennaisen kysymyksen. Miten kybermaailmassa, jossa ei tunneta valtiollisia rajoja, anonymiteetin säilyttäminen on mahdollista, ja hyökkäykset pääsevät mahdollisesti leviämään holtittomasti myös muihin kuin alkuperäisiin kohteisiin, voidaan tunnistaa tietyn kybertoimen olevan sotatoimi?

Asiantuntija C:ltä kysyttiin, miten kohdellaan niin kutsuttuja harmaan alueen tilanteita, joissa on epäselvää, onko tietty hyökkäys sotatoimi ja osa suurempaa kokonaisuutta, vai yksittäinen hyökkäys. Rajanveto on aikoinaan ollut huomattavasti vaikeampaa, sillä vielä pari vuotta taaksepäin kybervakuutus sopimuksissa luki yksinkertaisesti kaikkien sotaan liittyvien vahinkojen olevan rajattu ulkopuolelle. 1–1,5 vuotta sitten tutkielmassa jo aiemminkin mainittu Lloyd's julkaisi päivityksen markkinoiden kybersotarajoitusehdolle, joka sitoo suurta määrää vakuuttajia. Päivityksen myötä tuli selvennys siihen, ettei sotarajoitusehdon perusteella ulkopuolelle rajaamiseen riitä vain se, että hyökkäys tulee maasta, joka käy sotaa toisen maan kanssa.

“Siinä on oikeastaan pari vahvaa kriteeriä, jotka pitää täytyä, jotta se sotarajoitusehto aktivoituisi. Eli joko sen kyberhyökkäyksen tulisi olla osa ihan fyysistä, kineettistä sodankäyntiä. Tai jos ei tällaista fyysistä sodankäyntiä liity siihen tapaukseen, niin silloin sillä kyseisellä valtiollisen tahon tekemällä kyberhyökkäyksellä tulisi olla merkittävä haitallinen vaikutus sen koko kohdevaltion kriittisen infrastruktuurin toimintaan.”

Asiantuntija C nosti esille merkittävänä pointtina myös attribuutiolausekkeen, joka useissa sotarajoitusehdoissa on. Kyseinen lauseke tarkoittaa sitä, että vakuuttajalla on

todistusvastuu sotatoimen osoittamisesta. Vakuuttajan tulee siis pystyä objektiivisiin todisteisiin vetoamalla todistamaan, että sotarajoitusehto aktivoituu, eikä kybervakuutuksesta korvata tiettyä vahinkoa. Kyseiset päivitykset voidaan nähdä vakuutettujen kannalta hyvinä muutoksina, kuten Asiantuntija C: kin haastattelussaan totesi.

“Tää on ollut aiemmin paljon haastavampi vakuutetuille, kun siellä on vaan lyhyesti mainittu, että sota. Mutta nykyään se on sen sivun mittainen rajoitusehto markkinoilla ja se vaatii kyllä vakuuttajalta paljon ja siltä tapahtumalta paljon, jotta se sotarajoitusehto purisi.”

Asiantuntija A:lta kysyttiin, miten sotatoimi voidaan tunnistaa. Hän kertoi vakuutusyhtiöiden ehtojen omaavan pitkälti samoja elementtejä, näiden perustuessa kyseiseen attribuutiolausekkeeseen. Hän mainitsi tunnistamista hankaloittavan myös oikeuskäytännön vähäisyyden sekä sen, että suurin osa kyseisestä oikeuskäytännöstä asian tiimoilta on Yhdysvalloissa. Hänen mukaansa tilannekohtainen harkinta nousee keskiöön “harmaan alueen” tapauksissa.

“Sehän siinä on vaikea, että siinä missä perinteisessä sodankäynnissä on aika selkeää sanoa, että noi ohjukset tulee tuosta suunnasta, mutta kyberhyökkäyksissä just sen alkuperän selvittäminen on hankalampaa.”

Asiantuntija B totesi todistusvelvollisuuden olevan tällä hetkellä pitkälti vakuutusyhtiön vastuulla, vaikkakin jotkin rajoitusehdot nojaavat esimerkiksi tiettyihin päätöksiin, joita globaalit toimijat, kuten United Nations tai Nato ovat tehneet. Todistaminen ei ole helppoa, eikä aina mahdollista, mutta siihen on asiantuntija B:n mukaan keinoja.

4.4 Kybervakuuttaminen tulevaisuudessa

Haastatteluiden viimeinen osio keskittyi kyberrikollisuuden mahdolliseen tulevaisuuskehitykseen, sekä pohdintaan siitä, voisiko kybersota muuttuvassa maailmantilanteessa ja aiemmin käsitellyt seikat huomioiden mahdollisesti tulla vakuutuskelpoiseksi.

Haastateltavista kaikki olivat yhtä mieltä siitä, että muuttuva kyberympäristö ja kehittyvä teknologia tuovat luomaan uusia haasteita, johon yritykset ja vakuutusyhtiöt joutuvat vastaamaan. Puolestaan siitä, millaisia kyseiset muutokset ja haasteet tulevat olemaan, näkemykset olivat hieman eriäviä. Asiantuntija A korosti tulevaisuuden haasteeksi esimerkiksi tekoälyn, sekä muiden vastaavien työkalujen kehittymisen ja käytön lisääntymisen.

“Sinänsä mulla ei riitä mielikuvitus keksiin, että olisi joku uusi muoto, jolla rikolliset hyökkäis, mut näissä mitä ollaan nyt käyty eli perinteiset tietomurrot ja ransomware niin niissä tekoälyn kehittyminen antaa paljon uusia mahdollisuuksia rikollisille.”

Asiantuntija B puolestaan kertoi monien tilastojen valossa näyttävän siltä, että kyberrikollisuus toimialana tulee kasvamaan ja raha, mitä kyberrikolliset tulevat saamaa huijauksista ja hakkeroinnista tulee lisääntymään. Kyberrikollisuuden lisääntymisen puolesta puhuu hänen mukaansa esimerkiksi yritysten kasvava digitalisoituminen ja tietoverkkojen yhdistely, sekä erilaiset hakkereiden turvasatamat eri puolilla maailmaa. Hän nostaa esille kyberrikollisuuden ammattimaistumisen, sekä myös asiantuntija A:n mainitseman työkalujen kehittymisen kyberrikollisuuden lisääntymisen puolestapuhujina. Hän korostaa myös, että vaikka indikaatteja kyberrikollisuuden kasvulle on nähtävillä, on vaikea sanoa, tuleeko näin tapahtumaan. Hän pohtii rikollisuuden kasvua jarruttavina tekijöinä olevan esimerkiksi virtuaalivaluuttojen jäljittämisen ja muun teknologian kehittymisen.

Myös Asiantuntija C näkee useita vakuuttajia mietityttäviä seikkoja tulevaisuuden kybermaailmassa. Hän nostaa esille muutoksen hyökkäysten kohteeksi joutuvissa yrityksissä:

“Mä uskon, että se kyberrikollisuus alkaa kohdistumaan yhä enemmän myös yhä pienempiin yrityksiin, että se on tyypillisesti ollut vähän semmoista big game huntingia --- Mutta mitä ollaan jo nähty kuluneen vuoden aikana niin nää hyökkäykset kohdistuu yhä enemmän myös PK-sektoriin.”

Muutosta selittää Asiantuntija C:n mukaan osin haittaohjelmahyökkäyksien hinnan alaspäin tuleminen. Rikollisuuden kehittyessä hyökkäysten toteuttaminen on tullut entistä helpommaksi, sillä sitä pystyy esimerkiksi tilaamaan netistä ja täten ulkoistamaan pitkälti koko tapahtumat. Yhteenvetona hän näkee kyberrikollisuuden kasvavana ja kehittyvänä uhkana tulevaisuudessa.

Kaikilta asiantuntijoilta kysyttiin, miten ja kuinka nopeasti kybervakuutusmarkkinat reagoivat kyberrikollisuuden kehittymiseen tulevaisuudessa. Yleinen konsensus asiantuntijoiden kesken oli, että markkina sopeutuu ja elää tarpeen mukana. Asiantuntija C:n mukaan vakuutusyhtiöt voivat sopeutua parantamalla tarjoamaansa tuotetta siten, että kaikenkokoisille ja eri turvatasojen yrityksille tarjotaan yhä enemmän turvaa. Tällöin vakuuttajat auttavat vakuutettuja myös tarvittaessa parantamaan tietoturvasa tasoa, ja vastaavanlainen näkemys nousi aiemmin haastatteluissa esille myös asiantuntijalta A:lta kohdassa 4.2. Tämä toimisi vastauksena haasteeseen, jossa hyökkäykset kohdistuvat yhä pienempiin yrityksiin. Asiantuntija C korostaa myös sitä, että vakuutusmarkkina sopeutuu lopulta aina tapahtumiin vakuutusmaksun tason ja riskienvalinnan kautta.

Myös asiantuntija A näkee vakuutusmarkkinoiden reagoivan, melko nopeastikin, etenkin yrityspuolella vakuutusten ollessa tyypillisesti vuoden voimassa. Asiantuntija A korosti edelleen yhtenevästi asiantuntija C:n kanssa mahdollisena skenaariona tietoturvakonsulttien sekä muiden teknisten palveluiden, ja vakuutusyhtiöiden lähentymisen. Tämä mahdollistaisi yritysten reaaliaikaisen skannaamisen ja mahdollisten heikkouksien havaitsemisen ennaltaehkäisevästi.

Asiantuntija B puolestaan näkee markkinan kehittyvän hieman jälkijunassa vakuutusyhtiöiden elävän pitkälti historiallisesta datasta. Tämä nähtiin esimerkiksi vuosina 2020–2022 kun kybervakuutuksien hinnat hyppäsivät rajusti ylöspäin. Ransomware-kiristyshaittaohjelmat yleistyivät huomattavasti 2020-luvun taitteessa, eivätkä vakuutusyhtiöt olleet osanneet ennustaa tätä etukäteen johtaen riskien väärin arviointiin. Toisaalta vakuutusmarkkina ei Asiantuntija B:n mielestä voikaan olla kovin proaktiivinen: liiketoimintaa voitaisiin hävitä tilanteessa, jossa muut vakuutusyhtiöt

tarjoaisivat parempaa turvaa, mutta toisaalta myös tilanteessa, jossa syntyy epävarmuutta siihen, mitä vakuutus korvaa, mitä ei, ja millä hinnalla.

Viimeisenä laajana kysymyksenä kytkeytyen kybervakuutuksen kehittämiseen, asiantuntijoilta kysyttiin, näkisivätkö he kybersodan muuttuvan tulevaisuudessa vakuutuskelpoiseksi. Asiantuntija A ei näe, että itse kybersotaa alettaisiin vakuuttamaan, sillä systeemiriskien vakuuttaminen ei yleisesti ottaen kuulu alan käytäntöihin. Hän kuitenkin nosti esille kyberterrorismin, joka on poikkeus yleisiin linjauksiin:

“Yleensä on kirjoitettu silleen, että vakuutuksesta ei korvata vahinkoa, joka aiheutuu sodasta tai terrorismista, mutta tästä poisluetaan kyberterrorismi. Et sitä ei nähdä sellasena systeemisenä riskinä, vaan se sitten katetaan.”

Kyberterrorismia ei nähdä valtionmuotoisena, vaan esimerkiksi jonkin järjestön tai liikkeen toteuttamana toimena. Täten kyberterrorismissa ei tarvitse asiantuntija A:n mukaan olla aspektia, jossa tulisi selvittää onko se peräisin tietystä valtiosta. Asiantuntija A kuitenkin kertoo kyberterrorismin ja kybersodan satunnaisesti limittyvän toisiinsa, mikäli esimerkiksi militanttijärjestö toimisi osana sotaa ja suorittaisi hyökkäyksiä itse järjestönä. Tällöin myös kyberterrorismitoimet voitaisiin liittää sotatoimeksi ja tulisi suorittaa tapauskohtaista harkintaa siinä, korvataanko vahinkoja kybervakuutuksesta vai ei.

Asiantuntija B:n näkemys on hieman eriävä edellä kerrotusta, sillä hän näkee kybersodan mahdollisesti korvattavana riskinä, tai ainakin asiana, jota tulisi tulevaisuudessa miettiä uudelleen. Hänen mielestään tilanteessa, jossa valtion julistamaan sotaan liittyy kybersodan lisäksi fyysinen sota, sen tulisi säilyä poisrajattuna kybervakuutuksesta. Puolestaan tilanteessa, jossa kyseessä on puhtaasti kybersota ilman fyysistä ulottuvuutta, asiantuntija B:n mielestä ei voi sanoa suoraan onko se korvattavissa vai ei, mutta kyseessä on asia, joka voisi kaivata lisäselvyyttä. Asiantuntija B perustelee näkemystään seuraavasti:

“Jotta kybervakuutus pysyy terveenä ja jotta pystytään tarjoamaan kestävästi kybervakuutusta, niin näihin aggregaattiriskeihin on kyllä puututtava myöskin ja kybersota on yks näistä isoista aggregaattiriskeistä.”

Asiantuntija B kuitenkin korostaa, että mikäli kybersotaa alettaisiin korvaamaan, tulisi yritysten ja koko vakuutusketän ymmärtää sen näkyminen myös vakuutusten hinnoissa. Asiantuntija C on näkemykseltään samalla kannalla asiantuntija B:n kanssa ja näkee kybersodan mahdollisesti tulevan vakuutuskelpoiseksi tietyillä rajoituksilla. Asiantuntija C perustelee näkemystään:

“Yrityksethän ostaa myös sotavakuutuksia, omaisuusvakuutusten puolella sodalle on vakuutustuotteet. Niin miksei myös kybersodalle. Jos joku hyvin kriittisen infrastruktuurin toimija, sanotaan joku ydinvoimayhtiö, vaikka Suomessa, kokee sen riskin semmoiseksi, että he haluaisivat vakuuttaa, vakuutusmaksutasosta viis, niin näkisin että se olisi ihan paikallaan.”

Asiantuntija C kertoo, että markkinoille on jo julkistettu vakuutustuote kybersotaa varten. Hän muistelee, että noin vuosi sitten, Beazley-niminen vakuuttaja toi markkinoille stand-alone cyber war –tuotteen, joka herätti paljon keskustelua. Hän ei tiedä onko tuotteelle ollut kysyntää, mutta näkee sen mahdollisuutena ja toisaalta esimerkin todistamana myös mahdollisena.

5 YHTEENVETO JA JOHTOPÄÄTÖKSET

5.1 Tulosten yhteenveto

Tutkimuksen tavoitteena oli kartoittaa, millaisia eroja kyberrikollisuuden ja kybersodan vakuutuskelpoisuudessa on ja mitkä tekijät näihin eroihin vaikuttavat.

Tutkimuskysymykset olivat seuraavat:

1. Mitkä tekijät vaikuttavat kyberrikollisuuden eri muotojen vakuutuskelpoisuuteen?
2. Miten kyberrikollisuus ja kybersota eroavat toisistaan vakuutuskelpoisuuden suhteen?
3. Miten muutokset kyberrikollisuuden ja kybersodan luonteessa sekä toisaalta vakuutuksen “underwritingissa” vaikuttavat tulevaisuudessa niiden vakuutuskelpoisuuteen?

Tutkielman aineistona toimi kolme asiantuntijahaastattelua, joissa käytiin läpi tutkimuskysymysten ympärille rakennettua haastattelurunkoa. Haastattelut olivat muodoltaan puolistrukturoituja teemahaastatteluja, mikä mahdollisti vapaan keskustelun aiheiden ympärillä.

Ensimmäiseen tutkimuskysymykseen saatiin kerättyä vastauksia jo teoriaosuudessa, mutta syvempää tietoa saatiin asiantuntijahaastatteluista. Kyberrikollisuuden vakuutuskelpoisuus perustuu monilta osin vakuutuksen peruseriaatteiden ympärille. Jotta riski olisi vakuutuskelppoinen, sen toteutumisen tulisi olla riittävällä tarkkuudella ennustettavissa, riskin tulisi olla edunsaajasta riippumaton, ja sen tulisi olla ajallisesti stabiili (Rantala & Kivisaari, 2014, 77-78). Asiantuntijahaastatteluiden perusteella suurin osa kyberriskeistä, myös kyberrikollisuudesta, on kuitenkin vakuutettavissa. Tällöin kyseeseen tulee ehtojen, vakuutusmaksun ja omavastuuosuuden säätäminen oikealle tasolle. Kyberrikollisuuteen kytkeytyy vahvasti vakuutettavan yrityksen tietoturva, jonka puutteellisuus voi mahdollistaa erilaisten kyberriskien toteutumisen. Tietoturvan puutteellisuus ei kuitenkaan itsessään ole välttämättä este kyberrikollisuuden vakuuttamiselle. Asiantuntijahaastatteluiden mukaan vakuutusyhtiö voi puutteellisen tietoturvan tilanteessa toimia tietynlaisena tietoturvakonsulttina, ja sulkea vakuutuksen

piiristä pois esimerkiksi puutteelliset sektorit. Täten yritystä voidaan vakuuttaa kyberrikollisuuden varalta puutteista huolimatta. Asiantuntijahaastatteluiden perusteella myös kyberrikollisuuden taustalla oleva motiivi voi vaikuttaa sen vakuutuskelpoisuuteen. Esimerkiksi rahan motivoima kyberrikollisuus on usein vakuutettavissa, sillä monet suuryritysten kybervakuutukset pyrkivät korvaamaan kyberrikollisuuden aiheuttamia taloudellisia vahinkoja.

Asiantuntijahaastatteluista nousi esille muutamia merkittäviä tekijöitä, jotka voivat tehdä kyberriskistä ja erilaisesta kyberrikollisuudesta vakuutuskelvottoman. Esimerkiksi suuren toimialan riskit, infrastruktuuririskit, sekä suuret systeimiriskit eivät ole lähtökohtaisesti vakuutettavissa kybervakuutuksella. Suuren toimialan riskeissä, esimerkiksi suurten IT-palveluntarjoajien tapauksissa, vahingot voisivat potentiaalisesti levitä niin moneen yritykseen ettei vakuutus riittäisi kattamaan tätä. Infrastruktuurivahingoissa nousee myös esille vahinkojen laajuus, mikä tekee niistä vakuutuskelvottomia.

Toiseen kysymykseen saatiin muodostettua vastaus etenkin asiantuntijahaastatteluiden pohjalta. Entuudestaan oli selvää, että kybersota lähtökohtaisesti ei ole vakuutuskelpoista, siinä missä kyberrikollisuus laajalti on. Haastatteluissa oli tavoitteena selvittää syitä tämän taustalla ja täten muodostaa ero kyberrikollisuuden ja kybersodan vakuuttamiseen. Jokaisessa asiantuntijahaastattelussa systeimiriskit ja kybersota nousivat esille vakuutuskelvottomina ilmiöinä heti, kun siirryttiin käsittelemään kyberilmiöitä, joille ei ole tarjolla vakuutusturvaa. Myöhemmin haastatteluissa saatiin kuitenkin kattavaa informaatiota ja syvällisempää pohdintaa siitä, miksi näin on. Systeimiriskit ovat jo luonteeltaan sellaisia, ettei niitä lähtökohtaisesti vakuuteta. Vakuutusyhtiöiden olisi epäkannattavaa vakuuttaa riskejä, joiden toteutuessaan pahimmillaan kokonainen toimiala tai kokonaisen maan infrastruktuuri kärsisi vahingot, sillä korvausmenot nousisivat liian suuriksi yksittäisille vakuuttajille. Toisaalta myös koko vakuutuksen tausta-ajatus siitä, että vahingon välttävät yritykset kustantaisivat vakuutusmaksuillaan vahingon kärsineen yrityksen kulut, ei toteutuisi tilanteessa, jossa vahinko osuu jokaisen vakuutetun kohdalle.

Nykyään kuitenkin yksittäiseltä hyökkäykseltä vaaditaan melko paljon, jotta se voitaisiin luokitella kybersotatoimeksi ja jotta se voitaisiin rajata sotarajoitusehdoilla ulos vakuutuksen piiristä. Attribuutiolausekkeen nojalla todistusvelvollisuus jää suurimmassa osassa tapauksista vakuutusyhtiön kontolle, ja niin kutsutuissa harmaan alueen tapauksissa, joissa ei välttämättä ole selvää, onko kyseessä sotateimi vai ei ja mistä hyökkäys on peräisin, joudutaan soveltamaan hyvinkin tilannekohtaista harkintaa. On siis selkeä periaate, että kybersota on rajattu ulos perinteisestä kybervakuutuksesta ja täten poikkeaa merkittävästi kyberrikollisuudesta vakuutettavuudeltaan. Asia puolestaan ei ole aivan yhtä selkeä enää silloin, kun yksittäisestä tapauksesta tulisi määritellä onko kyseessä kybersotateimi, vai hyökkäys, joka voidaan korvata kybervakuutuksesta.

Viimeiseen kysymykseen, joka pohti kybervakuuttamisen ja kyberrikollisuuden tulevaisuutta ja kehitystä, ei puolestaan saatu yksiselitteistä vastausta, eikä toisaalta näin ollut tarkoituskaan. Tulevaisuutta on mahdotonta ennustaa, mutta etenkin kyberrikollisuuden kaltaisella, nopeasti kehittyvällä alalla on sekä mielenkiintoista, että myös tarpeellista pohtia tulevia ilmiöitä ja näiden vaikutuksia kybervakuuttamiseen markkinana. Haastatteluista saatiin arvokasta materiaalia mahdollisista kyberrikollisuuden ja siten myös kybervakuuttamisen kehitystrendeistä. Monet indikaatit viestivät kyberrikollisuuden kasvavan toimialana tulevaisuudessa ja kehittyvä teknologia, sekä kyberrikollisuuden lisääntyvä ammattimaisuus ja saatavuus luovat uusia haasteita kyberrikollisuuden hillitsemiseen. Toisaalta kehittyvää teknologiaa voidaan hyödyntää myös rikollisuuden jäljittämässä. Ei voida siis suoraan sanoa varmaksi, tuleeko kyberrikollisuus ja sen myötä kybervakuuttaminen kasvamaan lähivuosina, mutta näin voidaan olettaa perustuen viime vuosien kehitykseen, sekä tulevaisuuden ilmiöihin.

Kyberrikollisuuden kehittyessä myös kybervakuutuksen tulee kehittyä vakuutustuotteena, jotta sitä pystytään tarjoamaan kestävästi. Eräs mahdollinen, jo nähtävilläkin ollut, kehityssuunta kyberrikollisuudelle on sen leviäminen vain suurista yrityksistä myös pk-sektorin yrityksiin ja tuotantoketjun varrelle. Kybervakuutus voi reagoida tähän laajentamalla turvaansa myös pienemille yrityksille, sekä tekemällä tulevaisuudessa kiinteää yhteistyötä tietoturvakonsulttien ja muiden teknisen osaamisen tarjoajien kanssa. Asiantuntijahaastatteluiden yleinen konsensus oli, että kybervakuutus sopeutuu ja elää tarpeen mukana, ja tästä toisaalta kertoo myös historiadata.

Mielenkiintoista aineistoa haastatteluista saatiin erityisesti kybersodan vakuutettavuuteen liittyen. Nykytilanteessa kybersota on hyvinkin selkeästi rajattu ulos kybervakuutuksesta ja linjattu lähes vakuutuskelvottomaksi. Asiantuntijahaastatteluissa nousi esille tästä huolimatta useampi mielipide ja näkemys, joiden perusteella tulevaisuudessa myös kybersota voitaisiin nähdä vakuutuskelpoisena ja sen vakuuttaminen voisi olla jopa tarpeellista. Haastatteluista kävi ilmi, että kybersodalle jopa on julkaistu oma vakuutustuotteensa, mikä kertoo siitä, että keskustelua ja ajatustyötä kyseisen vakuutustuotteen tarpeesta on käyty, ja mahdollisesti tulevaisuudessa tämä tarve voi myös lisääntyä.

5.2 Tutkielman arviointi ja jatkotutkimus

Tutkielman avulla onnistuttiin keräämään ja kokoamaan yhteen laajalti tietoa ja vastauksia tutkimuskysymyksiin. Laadullisessa tutkimuksessa pyritään tarkastelemaan aineistoa kokonaisuutena ja ymmärtämään tutkittavaa aihetta, sekä tekemään tulkinta tutkittavasta aiheesta (Alasuutari, 2011). Nämä kriteerit täyttyivät tämän tutkielman kohdalla. Tutkittava aihe oli myös hyvinkin ajankohtainen ja mielenkiintoinen, kyberrikollisuuden lisääntyessä ja kybervakuuttamisen ollessa kohtalaisen nopeasti muuttuva vakuutuslaji.

Tutkielman aineistona käytettiin kolmea asiantuntijahaastattelua kybervakuuttamisen asiantuntijoilta. Kolmella haastattelulla saatiin kerättyä kattavasti materiaalia, mutta optimaalisessa tilanteessa haastatteluja olisi toteutettu neljä tai viisi, jotta olisi voitu saavuttaa laajempi skaala näkemyksiä ja aineistoa. Haasteeksi haastateltavien löytämisessä nousi alan tuoreus sekä melko pienet markkinat Suomessa, eikä kandidaatin tutkielman laajuutta ajatellen nähty järkevänä alkaa toteuttamaan haastatteluja tai koko tutkielmaa englanniksi.

Jälkikäteen ajateltuna tutkielman aihetta olisi voinut rajata hieman tarkemmin. Tutkielmaa aloittaessa melko vähäisillä pohjatiedoilla en osannut hahmottaa, kuinka laaja aihe kybervakuuttaminen ja siihen kytkeytyvät vakuutuskelpoisuuden aspektit on. Jo

pelkästä tulevaisuusaspektista olisi riittänyt kerrottavaa tutkielmaan, mutta toisaalta tällöin taustoitusta ja muut aiheen kannalta relevantit asiat olisivat jääneet käsittelemättä.

Kyselylomakkeen laajuus keräsi kiitosta haastateltavilta ja siihen valikoitui aiheeseen valikoituneen rajauksen kannalta relevantteja kysymyksiä. Olisi ollut mielenkiintoista lisätä haastattelurunkoon laajempaan omana kysymyksenään kysymys siitä, miksi kyberterrorismia vakuutetaan, mutta kybersotaa ei, sillä nyt tämä nousi esille haastatteluissa vain lyhyesti. Myös tapauskohtaisesta harkinnasta siinä, millaiset tapaukset luokitellaan kybersotatoimiksi ja millaiset puolestaan ei, olisi voinut olla oma kysymyksensä haastattelurungossa, vaikkakin tätä tuli käsiteltyä nytkin haastatteluissa melko kattavasti.

Jatkotutkimusaiheita voisi esimerkiksi olla kvantitatiivinen tutkimus kyberhyökkäyksiä jakautumisesta erikokoisten yritysten kesken, tai tämän rakenteen muutos kuluneina vuosina. Kyseessä on myös niin nopealla tahdilla muuttuva ala, että jo muutaman vuoden kuluttua voisi olla mielenkiintoista tutkia myös uudelleen, millaisia kyberrikoksia vakuutetaan ja miten kybervakuutuksen korvaavuus ja turvan laajuus on muuttunut. Minua henkilökohtaisesti kiinnostaa myös tapauskohtaiset esimerkit siitä, mitä luetaan kybersotatoimien piiriin ja mitä puolestaan kyberterrorismin toimiin, sekä miksi ja millaisilla rajauksilla jälkimmäisiä vakuutetaan, mutta sotatoimia ei. Uskon, että kyseisestä aiheesta saisi aikaiseksi jonkinlaisen case-tutkimuksen, jossa syvennyttäisiin tarkemmin jonkin hyökkäyksen vakuutusratkaisuihin ja oikeuskäytäntöihin.

LÄHTEET

Kirjallisuus

Alasuutari, P. (2011). *Laadullinen tutkimus 2.0*. Vastapaino.

Allianz Global Corporate & Specialty SE. (2023). *Allianz Risk Barometer 2023*.

Biener, C., Eling, M., & Wirfs, J. H. (2014). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40(1), 131–158. doi: <https://doi.org/10.1057/gpp.2014.19>

Brockett, P., Golden, L. & Wolman, W. Editioija Emblemsvåg, J. (2012). *Risk management for the future: Theory and cases*.

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

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk management – Integrated framework*.

Eskola, J. & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 100(4), 817–885.

Hirsjärvi, S., & Hurme, H. (2022). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Gaudeamus Helsinki University Press.

Pellikka, T., Peilimö, P., Puntari, P. & Vaitomaa, M. (2020). *Omaisuuuden vakuuttaminen*. Helsinki: FINVA.

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

Kivisaari, E. & Kahola, M.-L. (2017). *Vakuutustalous – Vakuutusyritysten riskienhallinta, tilinpäätös ja vakavaraisuus*. Helsinki: FINVA

Knight, F.H. (1921). *Risk, uncertainty and profit*. Boston: Houghton Mifflin Company

Koskinen, L. (2018). *Riskienhallinnan ajankohtaisia teemoja*. Tampere University Press

Lubin, A. (2019). Public policy and the insurability of cyber risk. *5 Journal of Law and Technology at Texas*. doi: <http://dx.doi.org/10.2139/ssrn.3452833>

Rantala, J. & Kivisaari, E. (2014). *Vakuutusoppi* (12. uudistettu painos). Helsinki: FINVA

Robinson, M., Jones, K. & Janicke H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, 49, 70-94

https://www.sciencedirect.com/science/article/pii/S0167404814001692?casa_token=rCgF89k3pfcAAAAA:Ma0Y41j9IUCPi_rL9wu1DNvJI3_c23BNDIKmJPY9LdY1UfF3aoRdh-jEEIx8Ao7Xuuz2-0kVQ

Muut lähteet

Clifford Chance (2023). *Lloyd's cyber war exclusion*

<https://www.cliffordchance.com/insights/resources/blogs/insurance-insights/2023/09/lloyds-cyber-war-exclusion.html>

Cyber Talents (ei pvm.). *What is Cybercrime? Types, examples, and prevention.*

Viitattu 22.10.2023. <https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention>

Finanssiala.fi (päivitetty 2021). *Hyvä vakuutustapa ja vakuutustoiminnan yleiset periaatteet.*

Viitattu 19.10.2023. <https://www.finanssiala.fi/aiheet/hyva-vakuutustapa-ja-vakuutustoiminnan-yleiset-periaatteet/#1>

Folger, J. (päivitetty 2022). *What is spoofing? How scam works and how to protect yourself.*

Viitattu 22.10.2023 <https://www.investopedia.com/terms/s/spoofing.asp>

Fortinet (ei pvm.). *What is cyberwarfare?* Viitattu 23.10.2023.

<https://www.fortinet.com/resources/cyberglossary/cyber-warfare>.

IBM (ei pvm.). *What is cyber risk management?* Viitattu 29.10.2023.

<https://www.ibm.com/topics/cyber-risk-management>

If B (ei pvm.). *Usein kysyttyä: Vahingot ja korvaaminen.* Viitattu 20.10.2023.

<https://www.if.fi/henkiloasiakkaat/asiakaspalvelu/usein-kysyttya/korvausasiat>

If A (ei pvm.). *Toiminnan vastuuvakuutus.* Viitattu 11.10.2023.

<https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/toiminnan-vastuu>

Imperva A (ei pvm.). *What is cyber warfare?* Viitattu 16.9.2023.

<https://www.imperva.com/learn/application-security/cyber-warfare/>

Imperva B (ei pvm.). *Botnet DDoS attacks.* Viitattu 23.10.2023.

<https://www.imperva.com/learn/ddos/botnet-ddos/>

Imperva C (ei pvm.). *Spear phishing.* Viitattu 23.10.2023.

<https://www.imperva.com/learn/application-security/spear-phishing/>

Imperva D (ei pvm.). *What is cybersecurity risk management?* Viitattu 29.10.2023. <https://www.imperva.com/learn/data-security/cybersecurity-risk-management/>

Insuranceopedia (2023). *Insurability*. Viitattu 8.10.2023. <https://www.insuranceopedia.com/definition/2384/insurability>

Keskinäinen Vakuutusyhtiö Lähitapiola (2022). *Tietoa yritysasiakkaille Ukrainan sotatilanteeseen liittyen*. Viitattu 29.10.2023. <https://www.lahitapiola.fi/tietoa-lahitapiolasta/uutishuone/uutiset-ja-tiedotteet/uutiset/uutinen/1509576514151>

Marsh Commercial (2021). *A history of cyber insurance*. Viitattu 29.5.2024. <https://www.marshcommercial.co.uk/articles/history-of-cyber-insurance>

Munich Re. A (2020). *Evaluating cyber risk? Here are some things to consider*. Viitattu 29.5.2024. <https://www.munichre.com/en/insights/cyber/evaluating-cyber-risk.item-b4d3ad995eeead5bfd599073bee97ae.html>

Munich Re. B (2020). *Cyber Insurance – Risks and Trends 2024*. Viitattu 10.6.2024. <https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html>

Panda Security (2022) *DDoS Meaning: What Is a Distributed Denial-of-Service Attack?* Viitattu 23.10.2023. <https://www.pandasecurity.com/en/mediacenter/security/ddos/>

Poliisi (ei pvm.) *Petosrikokset*. Viitattu 22.10.2023. <https://poliisi.fi/petosrikokset>

Rikoksantorjuntaneuvosto (ei pvm.) *Kyberrikokset*. Viitattu 23.10.2023. <https://rikoksantorjunta.fi/kyberrikokset>

Rikosuhripäivystys (ei pvm.) *Kyberrikollisuudella on monta eri muotoa*. Viitattu 20.10.2023. <https://www.riku.fi/erilaisia-rikoksia/nettihuujaus/kyberrikollisuus/>

Sampo Group A (2023). *Operatiiviset riskit*. Viitattu 11.10.2023. <https://www.sampo.com/fi/konserni/riskienhallinta/operatiiviset-riskit/>

Sampo Group B (2023). *Sanasto*. Viitattu 13.10.2023. <https://www.sampo.com/fi/media/sanasto/>

Suomen Riskienhallintayhdistys – PK-RH-riskienhallinta (ei pvm.). *Usein kysytyjä kysymyksiä riskienhallinnasta*. Viitattu 29.9.2023. <https://pk-rh.fi/riskienhallinta/ukk.html>

The Association of British Insurers A (ei pvm.) *Cyber insurance – Common exclusions*. Viitattu 23.10.2023. <https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/common-exclusions-cyber/>

The Association of British Insurers B (ei pvm.) *What does cyber insurance cover?* Viitattu 25.6.2024. <https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/what-does-cyber-insurance-cover/>

Traficom; Kyberturvallisuuskeskus (2022) *Toimintaohje – Palvelunestohyökkäys*. Viitattu 23.10.2023.

<https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/PalvelunestohyökkäysToimintaohje.pdf>

Ulkoministeriö (ei pvm.). *Kyberturvallisuus ja kybertoimintaympäristö*. Viitattu 16.9.2023. <https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto>

Vakuutus.fi (ei pvm.). *Yritysvakuutus*. Viitattu 11.10.2023. <https://www.vakuutus.fi/yritysvakuutus>

Vornanen, N. (2020). *Kyberriskin hallinta on haastavaa*. Viitattu 29.10.2023. <https://howdenfinland.fi/kyberriskin-hallinta-on-haastavaa/>

Yrittäjät (ei pvm.). *Vakuutukset*. Viitattu 11.10.2023. <https://www.yrittajat.fi/tietopankki/turvaa-yrittamiseen/vakuutukset/>

Oikeudelliset lähteet

Vakuutuslakia 28.6.1994/543

Vakuutusyhtiölaki 18.7.2008/521

LIITTEET

Liite 1: Haastattelurunko

Osio 1: Haastateltavan tausta ja nykyinen asema

1. Millaista työkokemusta sinulle on kertynyt vakuutusosalalta?
2. Millaisissa tehtävissä työskentelet tällä hetkellä?
3. Millaiset kytkökset sinulla on kybervakuuttamiseen?

Osio 2: Kyberrikollisuus ja sen vakuutuskelpoisuus

4. Millaista kyberrikollisuutta yritykset yleisimmin kohtaavat?
5. Mitkä ovat keskeisimpiä kyberrikollisuuden muotoja, joille on tarjolla vakuutusturvaa?
6. Millä tavalla kybervakuutukset ovat kustomoitavissa tietyn organisaation tarpeisiin?
7. Millaisia kyberriskejä ei voi vakuuttaa?
8. Miksi kaikki kyberriskit eivät ole vakuutuskelpoisia?
9. Kybersota on suljettu käytännössä kokonaan vakuutusturvan ulkopuolelle. Mitkä ovat merkittävimpiä syitä tämän taustalla?

Osio 3: Kyberriskit, -sota ja -vakuuttaminen tulevaisuudessa

10. Miten uskot kyberriskien ja -rikollisuuden kehittyvän lähitulevaisuudessa?
11. Kuinka nopeasti ja millä tavalla kybervakuutusmarkkinat yleisesti ottaen sopeutuvat edellä kuvattuihin muuttuviin tilanteisiin?
12. Näetkö mahdollisena tai tarpeellisena, että tulevaisuudessa myös kybersota tulisi tietyillä rajoituksilla vakuutuskelpoiseksi, miksi tai miksi et?

Osio 4: Yhteenveto

13. Tuleeko sinulle mieleen muuta olennaista tai tärkeää aiheeseen liittyen?