Marko Meretvuo

YRITYSVAKOILU:

TILANNEKUVA, MENETELMÄT JA ESTÄMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Meretvuo, Marko
Yritysvakoilu: tilannekuva, menetelmät ja estäminen
Jyväskylä: Jyväskylän yliopisto, 2021, 73 s.
Turvallisuus ja strateginen analyysi, pro gradu -tutkielma
Ohjaaja(t): Kari, Martti

Yritysvakoilu on yleinen ilmiö ja siitä aiheutuu huomattavia tappioita sekä yksittäisille yrityksille että kansantalouksille. Sitä toteuttavat toiset yritykset, rikolliset hakkeriryhmät ja valtiolliset tiedustelupalvelut. Ilmiönä se on kasvanut entisestään kylmän sodan päättymisen jälkeen, eikä mikään viittaa siihen, että se olisi tulevaisuudessa vähenemässä. Osana globaalia maailmantaloutta myös suomalaiset yritykset ovat alttiita yritysvakoilulle.

Yritysvakoilun estäminen käytännön tasolla kuuluu paitsi viranomaistoiminnan piirin, myös yritysten turvallisuustoimintojen vastuulle. Laittoman tiedonhankinnan keinot ja niiltä suojautuminen eivät kuitenkaan ole olleet juurikaan esillä yritysturvallisuutta, riskienhallintaa tai turvallisuusjohtamista koskevassa keskustelussa, tutkimuksessa tai kirjallisuudessa. Lisäksi vastatiedustelun ja yritysturvallisuuden rajapinta on epäselvä. Tämä johtuu pääasiassa siitä, että vastatiedustelu on käsitteenä sisällöltään tuntematon yritysturvallisuuden kontekstissa, ja se samaistetaan helposti vain valtiollisen turvallisuuden piiriin kuuluvaksi asiaksi.

Yritysvakoilua ilmiönä on tutkittu Suomessa hyvin vähän. Tämän tutkimuksen tarkoituksena oli selvittää yritysvakoilussa käytettäviä menetelmiä ja vastamenetelmiä, sekä ilmiön tämänhetkistä tilannekuvaa Suomessa. Tutkimus toteutettiin teemahaastatteluja hyödyntäen, ja haastateltavina oli kymmenen asiantuntijaa viranomaisorganisaatioista, edunvalvontajärjestöistä ja yksityisistä yrityksistä. Ilmiötä lähestyttiin haastateltavien subjektiivisten käsitysten vertailun kautta, ja käytetty tutkimusmenetelmä oli fenomenografinen.

Tutkimuksen perusteella yritysvakoilussa käytettävät menetelmät ja vastamenetelmät pystyttiin luokittelemaan perinteistä tiedustelulajijaottelua mielekkäämmällä tavalla, ja lisäksi saatiin arvokasta tietoa yritysvakoilun tämänhetkisestä tilanteesta sekä niistä ongelmakohdista, joita varautumiseen yleisellä tasolla liittyy.

Asiasanat: yritysvakoilu, teollisuusvakoilu, vastatiedustelu, liikesalaisuus, yritysturvallisuus

ABSTRACT

Meretvuo, Marko
Corporate Espionage: Situation Picture, Methods and Prevention
Jyväskylä: University of Jyväskylä, 2021, 73 pp.
Security and Strategic Analysis, Master's Thesis
Supervisor(s): Kari, Martti

Corporate espionage is a common phenomenon, causing significant losses for individual companies and national economies. It is implemented by rival companies, criminal hackers and national intelligence agencies. Corporate espionage has increased since cold war and all signs indicate further increasing. As a part of global economy, Finnish companies are also exposed to corporate espionage.

Preventing corporate espionage is a responsibility of authorities and corporate security. Illegal ways of acquiring information and preventing it are nevertheless rarely a subject in literature and study of corporate security and risk management. In addition, a line between corporate security and counterintelligence is ambiguous. This is caused by the fact that counterintelligence is unfamiliar subject in corporate security and is usually identified with national security authorities.

Corporate espionage is a rarely studied subject in Finland. The purpose of this thesis was to sort out methods and counter methods of corporate espionage and clarify the situation of the phenomenon in Finland. Ten specialists from police, advocacy organizations and private companies were interviewed for the thesis. Phenomenon was approached by comparing the views of the specialists and the research method was phenomenography.

As a result, the methods and counter methods of corporate espionage were assorted in a new way. In addition, new knowledge was acquired of the overall situation and problem areas regarding the subject of corporate espionage.

Keywords: corporate espionage, industrial espionage, counterintelligence, trade secret, corporate security

KUVIOT JA TAULUKOT

KUVIO 1 Käsitekartta……..…..21
KUVIO 2 Yritysvakoilun kolme ulottuvuutta…….…..…39
KUVIO 3 Matriisi tarkistuslistan tuloksille…….…..62

TAULUKKO 1 Erilaisia yritysvakoilun menetelmiä……40
TAULUKKO 2 Yritysvakoilun riskin todennäköisyyden arvioiminen…….61

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT JA TAULUKOT

1 JOHDANTO 7

2 TUTKIMUSONGELMA JA TEOREETTINEN VIITEKEHYS 9
2.1 Teoreettinen viitekehys 10
2.1.1 Tiedustelu ja vakoilu 11
2.1.2 Vastatiedustelu ja vastavakoilu 12
2.1.3 Yritysturvallisuus, tietopääoma ja liikesalaisuus 14
2.2 Yritysvakoilu ennen ja nyt 15
2.2.1 Teollisuus- ja talousvakoilun historiaa Suomessa 16
2.2.2 Yritysvakoilun tilanne nykypäivänä 17
2.3 Aiempi tutkimus 18

3 YRITYSVAKOILU JA VASTAAVAT KÄSITTEET 21
3.1 Yrityksiin kohdistuva laiton tiedonhankinta 22
3.2 Yritysten suorittama liiketoimintatiedustelu 23
3.3 Taloudellinen tiedustelu ja talousvakoilu 25

4 TUTKIMUKSEN TOTEUTTAMINEN 27
4.1 Tutkimusmenetelmä 27
4.2 Tutkimusaineiston hankkiminen 29
4.3 Aineiston analyysi 30
4.4 Tutkimuksen tulokset 31

5 YRITYSVAKOILUN TILANNEKUVA SUOMESSA 33
5.1 Yhteiskunnan tuki yrityksille 35
5.2 Varautumiseen liittyvät ongelmat 36

6 YRITYSVAKOILUN MENETELMÄT JA VASTAMENETELMÄT 39
6.1 Menetelmät fyysisessä tilassa 41
6.2 Menetelmät sosiaalisessa tilassa 43
6.3 Menetelmät kybertilassa 46
6.4 Yhdistetyt menetelmät 48
6.5 Yritysvakoiluun varautuminen 48
6.5.1 Vastamenetelmät fyysisessä tilassa 49
6.5.2 Vastamenetelmät sosiaalisessa tilassa 51
6.5.3 Vastamenetelmät kybertilassa 53
6.5.4 Muita vastamenetelmiä 55

6.6 Vastatiedustelullinen näkökulma.....56

7 POHDINTA 59
7.1 Riskin arvioiminen 60
7.2 Lisätutkimuksen aiheita.....63

LÄHTEET……...65

LIITE 1: HAASTATTELUKYSYMYSTEN MALLIRUNKO……..……..74

LIITE 2: KONTROLLITOIMIEN TARKISTUSLISTA……..75

1 JOHDANTO

Yrityksiin kohdistuva tiedonhankinta on yleinen ilmiö. Silloin, kun tiedonhankinta tapahtuu laittomin tai kyseenalaisin keinoin, kutsutaan sitä yleensä vakoiluksi. Sitä toteuttavat esimerkiksi kilpailijat, vieraiden valtioiden tiedustelupalvelut sekä rikolliset tahot, kuten kybervakoilua harjoittavat hakkeriryhmät. Ne saattavat toimia itsenäisesti, myyden varastamiaan tietoja kohdeyrityksen kilpailijoille, tai ne voivat toimia suoraan valtiollisen tiedustelupalvelun ohjauksessa. Varastettu tieto voi kulkea hakkeriryhmältä tiedustelupalvelulle ja sen kautta edelleen kyseisen valtion yrityksille. Raja hakkereiden, kyberrikollisten ja valtiollisten tiedustelupalveluiden välillä onkin nykyisin häilyvä (Cyberwatch & EK, 2018, s. 9). Yritysten itsensä harjoittama laiton tai kyseenalainen tiedonhankinta tapahtuu yleensä hyödyntämällä asiaan erikoistuneita konsulttiyrityksiä, joiden työntekijät ovat työskennelleet aiemmin valtiollisissa tiedustelupalveluissa (Holmström, 2010, s. 20). Yritysvakoilu on siten yleistä ja sitä toteutetaan järjestelmällisesti kaikkialla maailmassa. Myös Suomeen kohdistuu jatkuvasti vakoilua, jonka kohteena on yritysten keskeinen tuotekehitystieto, ja jonka päätyminen ulkomaisiin käsiin rapauttaa suomalaisten yritysten ja sitä kautta koko maamme kilpailukykyä kansainvälisillä markkinoilla (Supo, 2019, s. 2).

Fink (2003) esittää, että yritysvakoilun kohteeksi saattaa joutua käytännössä mikä tahansa yritys. Hänen mukaansa teoreettisesti katsottuna ainoa asia, joka yritysvakoilun syntymiseen ilmiönä tarvitaan, on liiketoiminta, jolla on yksikin kilpailija. Liiketoimintaan nimittäin kuuluu, että yritys pyrkii pitämään liikesalaisuudet salassa kilpailijoiltaan. Liikesalaisuus on yrityksen tietopääomaa, jolla on taloudellinen tai muu olennainen arvo. Käytännössä liikesalaisuuksia voivat olla tuotekehitystiedot tai valmistuskaavat, valmistusprosessiin liittyvät menetelmät, hinnoittelu- tai asiakastiedot sekä erilaiset markkinointi- ja laajenemissuunnitelmat. Kun toinen yritys tai muu taho pyrkii saamaan tällaisen tiedon haltuunsa laittomia keinoja käyttäen, on se yritysvakoilua, josta englanniksi käytetään useimmiten termiä *corporate espionage*. (Fink, 2003.) Tietoa saatetaan pyrkiä tavoittelemaan järjestelmällisesti myös sellaisilla keinoilla, jotka eivät ole laittomia. Tällöin puhutaan liiketoimintatiedustelusta. Käsitteitä

koskevassa luvussa selvitetään tarkemmin yritysvakoilun ja sitä lähellä olevien termien sisältöä.

Käytännössä yrityksillä on toisiinsa verrattuna hyvin erilainen riski joutua yritysvakoilun kohteeksi. Erityisen riskialttiit toimialat tulevat ajoittain esille julkisessa keskustelussa, ja ne vaihtuvat vuosien kuluessa ja teknologisen kehityksen edetessä. Yleisesti ottaen voidaan sanoa, että kullakin hetkellä innovaatiovaiheessa oleva teknologia on erityisen altista yritysvakoilulle. Tällaisen tuotekehitys- tai tutkimustiedon haltuun saaminen pitää sisällään mahdollisuuden suurimmalle taloudelliselle voitolle, kun yritys pystyy lanseeraamaan markkinoille tuotteen, jonka kehittämiseen liittyvä kustannustaakka on jäänyt toisen yrityksen maksettavaksi (Johnson, 2007, s. 165). Kuitenkin yrityksillä on muitakin syitä joutua yritysvakoilun kohteeksi. Nykyisin yhteiskuntien kriittinen infrastruktuuri on hyvin pitkälle yksityisten yritysten hallussa, ja tällaisiin yrityksiin kohdistuva vakoilu ei välttämättä pidä sisällään lainkaan taloudellisen hyödyntavoittelun motiivia. Sen sijaan vakoilun tarkoituksena voi olla selvittää esimerkiksi sähkö- tai tiedonsiirtoverkoista, finanssijärjestelmästä, elintarvikkeiden logistiikkaketjuista tai lääkkeiden valmistus- ja tukkutoiminnasta haavoittuvuuksia, joita voitaisiin hyödyntää mahdollisen sotilaallisen kriisin yhteydessä. Myöskään sotilas- ja kaksoiskäyttöteknologiaan liittyvän tuotetiedon tavoittelun motiivina ei välttämättä ole taloudellisen hyödyn saavuttaminen, vaan esimerkiksi asejärjestelmien ominaisuuksien tunteminen. Koska motiivista riippumatta kaikissa mainituissa tilanteissa kohteena on yrityksen hallussa oleva tieto, käsitellään niihin kohdistuvaa laitonta tiedonhankintaa tässä tutkielmassa yritysvakoilun nimikkeen alla.

Tämän tutkielman tarkoituksena on selvittää yritysvakoilussa käytettäviä keinoja, jotta sitä voitaisiin yhä paremmin estää. Lisäksi tavoitteena on selvittää yritysvakoilun tämänhetkistä tilannekuvaa Suomessa. Kokonaisuutena tutkimuksen tavoite on siten edesauttaa aiheeseen liittyvää riskienhallintaa. Tutkielma etenee siten, että seuraavassa luvussa esitetään tutkimusongelma, teoreettinen viitekehys keskeisine käsitteineen, katsaus aiheen historiaan sekä aiheeseen liittyvä aiempi tutkimus. Sitä seuraavassa luvussa täsmennetään tutkimuksen viitekehystä ja teoreettista taustaa käsitteiden esittelyn kautta. Sen jälkeen esitellään tutkimuksessa käytetty tutkimusmenetelmä sekä tutkimuksen eteneminen ja analyysiprosessi. Tutkimuksen tulosten tulkinta on jaettu kahteen osaan: yritysvakoilun tilannekuvaan sekä yritysvakoilun menetelmiin ja vastamenetelmiin. Lopuksi pohditaan ratkaisuita tutkimuksessa esille nousseisiin ongelmakohtiin sekä esitetään joitakin jatkotutkimuksen aiheita. Lähdeluettelo on rakennettu siten, että kirjat, artikkelit, raportit ja uutislähteet sisältyvät kaikki varsinaisiin lähteisiin, minkä jälkeen löytyvät erikseen tutkimuksen yhteydessä tehtyjen haastattelujen lähdetiedot.

2 Tutkimusongelma ja teoreettinen viitekehys

Yritysvakoilu muodostaa merkittävän uhkan sekä yksittäisille yrityksille että kansantaloudelle. Keskuskauppakamarin ja Helsingin seudun kauppakamarin vuosina 2005, 2008, 2012 ja 2017 tekemissä tutkimuksissa yritysvakoilun kohteeksi on epäillyt joutuneensa 8–10 % suomalaisyrityksistä (Silen, haastattelu, 10.2.2020). Vuoden 2020 tutkimuksessa luku oli noussut jo 17 prosenttiin (Helsingin seudun kauppakamari, 2020). Siitä huolimatta aihetta on tutkittu Suomessa tieteellisesti hyvin vähän. Tämän tutkielman tarkoituksena on selvittää

- millä keinoilla yritysvakoilua harjoitetaan ja miten sitä voisi yhä paremmin estää.

Yritysvakoilun keinot ja estäminen ovat sidoksissa toisiinsa. On nimittäin loogisesti pääteltävissä, että tehokas yritysvakoilun torjunta edellyttää siinä käytettävien menetelmien tuntemista käytännössä. Tutkielman tarkoituksena on kerätä yhteen ja luokitella nämä keinot järjestelmällisellä ja ymmärrettävällä tavalla. Yritysvakoilun ehkäisemistä on tarkoitus lähestyä paitsi yritysturvallisuuden, myös vastatiedustelun näkökulmasta. Erityisesti tutkielman teoriaosuudessa tutkitaan yritysturvallisuuden ja vastatiedustelun välistä rajapintaa, sillä vastatiedustelun päätehtävä on estää tietoa päätymästä vastapuolen haltuun. Erona yritysturvallisuuteen, vastatiedustelu sisältää passiivisen turvaamisen lisäksi erilaisia aktiivisia vastatoimia, joita käytännössä usein käytetään myös yritysvakoilun estämisessä. Siitä huolimatta vastatiedustelun menetelmiä osana yrityksissä tapahtuvaa yritysvakoilun torjuntaa ei ole tarkemmin tutkittu ja analysoitu, vaan vastatiedustelu käsitteen tasolla mielletään helposti kuuluvaksi vain valtiollisen turvallisuuden tai sotilaallisen toiminnan piiriin.

Tutkimuksen täydentävänä kysymyksenä on tarkoitus selvittää

- mikä on yritysvakoilun tämänhetkinen tilannekuva Suomessa.

Tällä kysymyksellä pyritään ennen kaikkea hahmottamaan aiheen tutkimisen relevanttiutta. Lisäksi kysymyksellä pyritään löytämään tietoa varautumiseen liittyvistä ongelmakohdista. Koska tutkimuskysymyksiin on vaikea saada vastauksia julkisista lähdeaineistoista, on aihetta tutkittava empiirisesti aiheeseen perehtyneiden asiantuntijoiden kautta. Tämä toteutettiin teemahaastatteluja käyttäen, ja kerättyä aineistoa lähestyttiin fenomenografisen tutkimusmenetelmän lähtökohdista.

Koska laittoman tiedonhankinnan riskiä yksittäisen yrityksen kohdalla on vaikea arvioida, hahmotellaan tutkielman yhteydessä yksinkertaista menetelmää, jota voitaisiin hyödyntää varautumiseen käytettävien resurssien sovittamiseksi riskiä vastaavaksi. Riskienhallinnan ja tietoturvan ISO-standardit eivät ole yleisluonteisuutensa vuoksi tarkoituksenmukaisia välineitä yritysvakoilun kontekstissa (Rajamäki, haastattelu 2.4.2020), eikä yritysvakoilua juurikaan käsitellä riskienhallintaa koskevassa kirjallisuudessa. Kuitenkin on selvää, että varautumiseen käytettävät resurssit voidaan optimoida vain, jos riskin todennäköisyys ja vakavuus ovat selvillä. Jotta tutkimuksen tulokset palvelisivat paremmin yrityksiä ja yhteiskuntaa, muodostetaan riskin arvioimiseen liittyvän menetelmän lisäksi työn liitteeksi yritysvakoilun torjunnan tarkistuslista, jota organisaatiot voivat hyödyntää käytännön varautumisessa.

Kokonaisuutena tutkimuksen tavoite on parantaa yritysvakoiluun liittyvää riskienhallintaa, ja se voisi siten olla hyödyksi esimerkiksi yritysturvallisuuteen liittyvässä koulutuksessa. Henkilökohtaisten tiedonantojen perusteella näyttää siltä, että esimerkiksi Laurea-ammattikorkeakoulun turvallisuuden ja riskienhallinnan koulutusohjelmissa ei juurikaan käsitellä yritysvakoilua, ei alemman eikä ylemmän ammattikorkeakoulututkinnon yhteydessä. Sen sijaan Aalto PRO -yliopiston järjestämässä turvallisuusjohdon koulutusohjelmassa aihealue on enemmän esillä (Ahonen, haastattelu 10.2.2020). Yritysvakoilua koskevan riskitietoisuuden lisääntymisen yhteiskunnassa voidaan myös katsoa olevan osa tutkielman päämääriä varsinaisen tutkimusprosessin ulkopuolella. Kyberturvallisuusalan edunvalvontaorganisaatio FISC nostikin tutkielman uutisaiheeksi 6.8.2020, minkä lisäksi tutkimuksen tekijä pääsi kirjoittamaan aiheesta Turvallisuus ja Riskienhallinta –aikakausjulkaisun lokakuussa 2020 ilmestyneeseen numeroon. Aiheesta uutisoi lisäksi Taloussanomat 25.11.2020.

2.1 Teoreettinen viitekehys

Tutkimuksen aiheen asettamiseksi oikeaan viitekehykseen, tulee ensin käsitellä tiedustelun ja vakoilun, vastatiedustelun ja vastavakoilun sekä yritysturvallisuuden, tietopääoman ja liikesalaisuuden määritelmiä. Nämä aihealueet ovat sisällöltään oleellisesti kytkeytyneitä tutkimuskysymykseen, joten niiden käsittely on välttämätöntä perusymmärryksen luomiseksi käsiteltävästä aiheesta. Tämän jälkeen luodaan yleiskuva yritysvakoilun historiasta Suomessa ja ny-

kypäivän tilanteesta maailmalla. Tutkimuksen tarkoituksena ei kuitenkaan ole esittää kattavaa historiaa aiheesta, eikä käsitellä yritysvakoilun yleisyyttä maailmanlaajuisena ilmiönä. Lisäksi tunnettujen vakoilutapausten case-tyyppisten esimerkkien esittelyt rajautuvat ulos tämän tutkielman viitekehyksestä.

Seuraavan pääluvun käsitteiden vertailuun on terminologian selventämiseksi sisällytetty myös laillisin keinoin tapahtuvan tiedonhankinnan käsitteitä. Sinänsä näiden keinojen tarkempi selvittäminen ei kuulu tämän tutkielman piiriin. On totta, että yrityksiin kohdistuvaan tiedonhankintaan varautuessa tulisi huomioida myös laillisesti esimerkiksi avoimia lähteitä hyödyntävä tiedustelutoiminta. Kuitenkin liikesalaisuus käsitteenä rajautuu sellaisen tiedon ulkopuolelle, joka voisi olla julkisesti saatavilla esimerkiksi yhtiön vuosikertomuksessa tai internetsivuilla. Täten lain rajoissa tapahtuva liiketoiminta-, asiakas- ja kilpailijatiedustelu on aihealue, jota ei tämän tutkimuksen viitekehyksessä käsitellä.

2.1.1 Tiedustelu ja vakoilu

Tiedustelun käsitteen taustalla voidaan nähdä epistemologinen kysymys siitä, mikä on totuus ja miten sen voi tietää. Juuri tämä kysymys sai Yhdysvaltain keskustiedustelupalvelu CIA:ssa työskennelleen Richards Heuerin kehittämään tiedusteluanalyysin menetelmiä (Heuer, 1999). Kuitenkin Lowenthal (2011) esittää, että tiedustelussa ei voi olla kysymys totuudesta vaan korkeintaan likimain tarkasta todellisuudesta, sillä totuus absoluuttisena määreenä on jotakin, johon tiedustelun kautta harvoin päästään. Nykyaikaisen tiedustelututkimuksen piirissä tiedustelun katsotaan olevan sekä prosessi tiedon hankkimiseksi, tämän prosessin seurauksena syntyvä tuote, että palvelu joka tätä prosessia toteuttaa. Sen tavoite on tuottaa tietoa päätöksenteon tueksi. Usein tiedusteluprosessi esitetään ympyränä, joka alkaa toimeksiantajan ohjauksesta ja etenee keräyksen ja käsittelyn kautta jakeluksi toimeksiantajille, jotka voivat antaa kerätystä tiedosta palautetta ja mahdollisesti uuden tiedustelukysymyksen. Tämän prosessin myötä olemassa oleva raakadata saa merkityksiä muuttuen informaatioksi, ja edelleen analyysin kautta tiedoksi. Lopulta tämän tiedon on tarkoitus konkretisoitua viisautena päätöksenteossa. (Lohse & Viitanen, 2019, s. 95–124.)

Tiedustelutietoa kerätään erilaisten keräyslajien kautta, jotka voidaan jakaa henkilötiedusteluun, signaalitiedusteluun, paikka- ja olosuhdetiedusteluun, mittaus- ja tunnusmerkkitiedusteluun sekä avointen lähteiden tiedusteluun (Clark & Lowenthal, 2016, s. 1–3). Tämä ja muut vastaavat jaottelut toimivat hyvin, kun tutkitaan valtioiden harjoittamaa tiedustelua kokonaisuutena, mutta liiketoimintatiedustelun ja yritysvakoilun käsitepiiriin ne sopivat huonosti. Yritystoimintaan liittyvää tiedonhankintaa suoritetaan pääasiassa tietoverkkojen välityksellä, taloudellisia sopimuksia hyödyntämällä, lähietäisyydeltä havainnoimalla ja tallentamalla, tai kyselemällä ja kuuntelemalla henkilöitä, joilta tietoa halutaan saada. On tosin olemassa tapauksia, joissa esimerkiksi lentoko-

neesta tapahtuvaa ilmakuvausta on hyödynnetty yritysvakoilussa. Tällaista tapahtui tiedusteluyhtiö Diligencen toimesta, ja tavoitteena oli lämpökameroiden avulla selvittää energiayhtiö Enronille, milloin kilpailevien yhtiöiden voimalaitokset olivat huollon takia pois käytöstä (Javers, 2011). Yleisesti ottaen liiketoimintaan liittyvän tiedonhankinnan voidaan kuitenkin katsoa poikkeavan käytännöiltään valtioiden poliittisesta ja sotilaallisesta tiedustelusta siinä määrin, että edellä mainittua keräyslajien jaottelua ei sen yhteydessä ole järkevää käyttää.

Tyypillisesti vakoilua voidaan pitää tiedonhankintana, joka ylittää laillisuuden rajat. Dikotomia laillisen tiedustelun ja laittoman vakoilun välillä on kuitenkin kyseenalainen, sillä toisen tiedustelu on usein toiselle vakoilua. Esimerkiksi taloudellisen tiedon hankkiminen toisen valtion yrityksistä saattaa nimenomaisesti olla kirjattu lakiin maan tiedustelupalvelun tehtäväksi. Lisäksi on huomioitava, että tiedustelun ja vakoilun määritelmät eivät ole yksiselitteisiä, vaan lähdekirjallisuudessa käytetään usein vakoilua terminä kuvaamaan salaista ja epämääräistä mutta ei välttämättä laitonta toimintaa. Vastaavasti tiedustelun käsite sisältää monessa yhteydessä moraalisesti kyseenalaisia konnotaatioita, vaikka itse toimet eivät olisi laittomia. Näin on usein puhuttaessa esimerkiksi liiketoimintatiedusteluun liittyen käänteissuunnittelusta, kilpailijatiedustelusta tai osaamisen siirtämisestä kilpailijalta rekrytoimalla. Tässä tutkielmassa käytetään vakoilua terminä kuvaamaan sellaisia tiedonhankinnan menetelmiä, jotka ovat ristiriidassa Suomen lainsäädännön kanssa. Vastaavasti tiedustelua terminä käytetään toimista, joiden osalta tällaista ristiriitaa ei ole.

2.1.2 Vastatiedustelu ja vastavakoilu

Vastatiedustelua on tutkittu akateemisella tasolla vasta hyvin vähän, eikä sille käsitteenä ole olemassa yksiselitteistä ja yleisesti käytössä olevaa määritelmää. Ehrman (2009) esittelee artikkelissaan useita käsitteelle annettuja määritelmiä. Näitä ovat mm. seuraavat:

- Vastatiedustelu tarkoittaa tiedon keräämistä ja erilaisia toimenpiteitä vakoilun ja tiedustelun sekä erilaisten hyökkäysten estämiseksi.

- Vastatiedustelu on tiedustelua, joka keskittyy vastustajan harjoittamaan tiedustelutoimintaan, pyrkien tuntemaan sen ja hyödyntämään sen heikkouksia.

- Vastatiedustelu tarkoittaa vieraiden valtioiden tiedustelupalveluiden aiheuttaman uhkan tunnistamista ja torjumista. (Ehrman, 2009, s. 7.)

Nämä määritelmät etenevät laajemmasta suppeampaan: laajimmillaan vastatiedustelu tarkoittaa mitä tahansa toimenpiteitä oman toiminnan suojaa-

miseksi, suppeimmillaan se on tiedustelupalvelujen toimintaa toisiaan vastaan. Van Cleave (2013, s. 1–2) määrittelee vastatiedustelun pyrkivän vastaamaan kysymyksiin siitä, mitä vastustaja tietää meistä, olemmeko pystyneet pitämään salaisuutemme ja keihin voimme luottaa. Hänen mukaansa se tarkoittaa käytännössä mm. vastustajan vakoojien löytämistä ja neutralisoimista sekä omien tiedusteluoperaatioiden turvaamista. Tässä tutkielmassa vastatiedustelusta puhutaan sen laajassa määritelmässä, jonka mukaan siinä on kyse sekä tiedosta että turvaamisesta. Koska esimerkiksi terrori-iskun suorittaminen jotakin kohdetta vastaan edellyttää yleensä tietoa kyseisestä kohteesta, voidaan tämän tiedon saamisen estämistä tai vaikeuttamista pitää vastatiedusteluna. Käsitteenä se on siten hyvin lähellä, mutta ei identtinen turvallisuuden kanssa. Vastatiedustelun suojaama tieto voi olla mitä tahansa hyödynnettävissä olevaa tietoa, ei ainoastaan esimerkiksi valtionsalaisuuksia tai liikesalaisuuksia.

Van Cleaven mukaan vastatiedustelu sisältää käsitteellisesti turvallisuustoiminnan, tarkoittaen passiivista suojaamista, mutta sen lisäksi aktiivisina toimina uhkan tunnistamisen, arvioinnin, neutralisoimisen sekä tarvittaessa hyväksikäytön harhauttavaa tietoa antamalla. Mikään määrä pelkkiä passiivisia suojaustoimia ei riitä antamaan turvaa kohdistetulta tiedonhankinnalta, joten vastatiedustelu pyrkii etsimään ja kohtaamaan uhkan suoraan (Van Cleave, 2007, s. 2). Prunckun (2012) on kehittänyt vastatiedustelun teoreettisen mallin, joka sisältää neljänlaisia toimenpiteitä: suojaukseen, havaitsemiseen, harhauttamiseen ja neutralisoimiseen liittyviä. Näistä suojaus ja havaitseminen ovat lähtökohtaisesti defensiivisiä ja harhauttaminen ja neutralisoiminen offensiivisia toimenpiteitä. Vastatiedustelun ja vastavakoilun Prunckun määrittelee eroavan juuri siinä, että vastavakoilu voidaan käsitteenä samaistaa offensiivisiin toimenpiteisiin, jotka kohdistuvat vastapuolen vakoilijoihin. Vastavakoiluun kuuluu monimutkaisia operaatioita, joissa omat toimijat saatetaan henkilökohtaiseen kontaktiin vastapuolen tiedusteluorganisaation kanssa. Tällaiset operaatiot voivat sisältää soluttautumista vastapuolen organisaatioon sekä harhauttavan tiedon "syöttämistä" vastapuolen tiedonhankintaprosessin häiritsemiseksi ja omien tietovuotojen paljastamiseksi. Tiedustelun nelikenttämallissa, joka sisältää vakoilun, havainnoinnin, analyysin ja salaiset operaatiot, vastatiedustelu sijoittuu keskelle, mahdollistaen näiden muiden häiriöttömän toiminnan. (Prunckun, 2012, s. 18–24.)

Yritysten vastatiedustelun voidaan määritellä tarkoittavan omien liiketoimintaprosessien valvontaa ja analysoimista, jotta kilpailevia yrityksiä hyödyttävät haavoittuvuudet voitaisiin havaita. Käytännössä tämä toiminta voi sisältää myös väärän tai puutteellisen tiedon päästämistä yritysvakoilua harjoittavan tahon saataville. (Carlisle, 2005, 172–173.) Myös yritysten osalta vastatiedustelu käsitteenä tulee siten erottaa pelkästään suojaavista kontrollitoimista, vaikka määritelmästä riippuen myös ne voidaan sisällyttää vastatiedustelun käsitteen alle.

2.1.3 Yritysturvallisuus, tietopääoma ja liikesalaisuus

Yritysturvallisuus, tai laajemmin kutsuttuna organisaatioturvallisuus, on osa yrityksen kokonaisvaltaista riskienhallintaa, ja sen tulisi olla osa yrityksen johtamista ja päivittäisiä rutiineja. Leppäsen (2006) mukaan yritysturvallisuus koostuu kaikista niistä toimenpiteistä, joiden avulla turvallisuusriskejä hallitaan. Se ei ole itsenäinen yksikkö tai tukitoiminto, vaan kaikkien niiden toimenpiteiden kokonaisuus, joilla häiriötön liiketoiminta pyritään varmistamaan. Operatiivisen turvallisuustoiminnan näkökulmasta yritysturvallisuus voidaan Leppäsen mukaan jakaa osa-alueisiin, jotka ovat henkilöturvallisuus, työturvallisuus, palo- ja pelastustoiminta, rikostorjunta, tietoturvallisuus, valmiussuunnittelu, ympäristöturvallisuus, ulkomaantoimintojen turvallisuus, tuotannon ja toiminnan turvallisuus sekä toimitilaturvallisuus. Turvallisuusjohtaminen on osa riskienhallintaa, joka laajempana kokonaisuutena sisältää turvallisuusriskien lisäksi mm. strategisten ja taloudellisten riskien hallinnan. Kyse ei siten ole vain yksittäisten riskien ennaltaehkäisystä, vaan kokonaisuudesta, jolla varmistetaan yrityksen strategisten tavoitteiden saavuttaminen. (Leppänen, 2006, s. 58–59, 203.)

Tietopääoma on organisaation arvokkainta omaisuutta. Leppäsen mukaan suojattava tieto voi olla muokkaamatonta raakatietoa eli dataa, merkitystä antavaa tietoa eli informaatiota, varsinaista hyödynnettävissä olevaa tietoa, tai osaamista eli tietoa, jonka avulla luodaan lisäarvoa. Tietomäärä yrityksessä on siten niin suuri, että kaikki tieto ei voi olla suojattava kohde. Yrityksen tulisikin tietoturvallisuusluokituksen avulla määritellä toiminnan kannalta kriittinen tieto, joka pyritään suojaamaan. Tietoriskit jaetaan johtamiseen, toimitiloihin, tietojärjestelmiin, henkilöstön toimintaan ja liikesuhteisiin liittyviin riskeihin. Tätä kokonaisuutta hallitaan tietoturvapolitiikan ja tietoturvakäytäntöjen avulla, jotka sisältävät käytännön toimia tietojärjestelmien suojaamisesta toimitilojen turvallisuusvyöhykkeisiin, murtosuojaukseen ja paloturvallisuuteen asti. (Leppänen, 2006, s. 66–69, 103–105.)

Avainasemassa tietoriskien hallinnassa on kuitenkin henkilöstö, joka tulisi perehdyttää, kouluttaa ja ohjeistaa tietoturvaperiaatteiden noudattamiseen ja tietoriskien tunnistamiseen. Tietoturvallisuudella pyritään tiedon käytettävyyden, eheyden ja luottamuksellisuuden varmistamiseen. Yksinkertaistettuna tämä tarkoittaa, että kukaan ei näe hänelle kuulumatonta tietoa, ja että kukaan tai mikään tapahtuma ei pysty muuttamaan tai hävittämään tietoa asiattomasti. Leppänen jakaa tietoturvallisuuden edelleen hallinnolliseen tietoturvallisuuteen, tietoaineistoturvallisuuteen, fyysiseen tietoturvallisuuteen, tietoliikenneturvallisuuteen, laitteisto- ja ohjelmistoturvallisuuteen sekä käyttöturvallisuuteen. Tieto tulee suojata koko sen elinkaaren ajan, tiedon syntymisestä käsittelyyn, siirtämiseen, varastointiin ja hävittämiseen asti. (Leppänen, 2006, s. 260–305.)

Yritysturvallisuus on kaikkein tärkein työkalu yrityksen henkisen pääoman suojaamisessa (Holmström, 2010, s. 12). Yritysvakoilu riskinä edellyttää muiden riskien tapaan sen tunnistamista, arvioimista, analysointia ja kontrollitoimista päättämistä. Ensimmäinen askel tietopääomaan kohdistuvien riskien

osalta on kuitenkin liikesalaisuuden piiriin kuuluvan tiedon eksplisiittinen määrittely, jonka vain yritys itse voi tehdä. Esimerkiksi rikoslaki ei määrittele salassapitovelvollisuutta, vaan ainoastaan salassapidon rikkomisesta seuraavan rangaistuksen (Leppänen, 2006, s. 69). EU:n liikesalaisuusdirektiivistä johdettu liikesalaisuuslaki sanoo liikesalaisuudella tarkoitettavan tietoa, joka ei ole yleisesti tunnettua, jolla on taloudellista arvoa, ja jonka laillinen haltija on ryhtynyt kohtuullisiin toimenpiteisiin sen suojaamiseksi (Jääskeläinen, 2018, s. 22).

Sisäministeriön, Viestintäviraston ja Elinkeinoelämän keskusliiton julkaisu ”Yritys – miten olet suojannut tietopääomasi?” (2017, s. 3) antaa esimerkkeinä tällaisista tiedoista tuotekehitystiedot, strategia- ja liiketoimintasuunnitelmat, valmistus- ja tuotantopiirustukset, lähdekoodit, prototyypit, testitulokset, kauppasopimukset, asiakasrekisterit, hinnastot ja henkilöstöä koskevat tiedot. Jääskeläinen (2018, s. 22) jakaa liikesalaisuudet teknisiin ja taloudellisiin yritys-salaisuuksiin, ja luettelee edellä mainittujen lisäksi niihin kuuluvaksi valmistusohjeet, käsikirjat, kemiallisten yhdisteiden koostumukset, käsittely- ja säilöntämenetelmät, talousennusteet, kilpailija-analyysit, markkinointisuunnitelmat, hankintahinnat ja katetiedot. Liikesalaisuus voi olla siten muutakin tietopääomaa, kuin yrityksen ydintoimintoihin liittyvää teknistä tietoa. Oleellista on, että käsitellessään kyseistä tietoa, yrityksen työntekijä tai muu taho tietää käsittelevänsä liikesalaisuudeksi katsottavaa tietoa.

2.2 Yritysvakoilu ennen ja nyt

Liiketoimintaan liittyvää tietoa on pyritty saamaan haltuun varmasti niin kauan, kuin yritystoimintaa on ollut olemassa. Lambergin (2019) mukaan varhaisimmat tiedot yritysvakoilusta löytyvät muinaisesta Kiinasta, jossa silkin valmistusta pidettiin niin merkittävänä salaisuutena, että sen vienti ulkomaille oli kuolemanrangaistuksen uhalla kielletty. 500-luvulla kaksi kristittyä munkkia onnistuivat kuitenkin salakuljettamaan silkkitoukan munia länteen, mistä sai alkunsa Välimeren maiden silkkiteollisuus. Toinen Kiinasta länteen siirtynyt innovaatio oli posliininvalmistuksen taito, jonka britit oppivat 1700-luvulla jesuiitta François Xavier d'Entrecollesin kirjeiden perusteella. Näitä tapauksia voidaan hyvin pitää oman aikansa yritysvakoiluna, sillä innovaatioiden alkuperäinen hyödyntäjä pyrki tietoisesti pitämään niiden valmistustekniikan salaisena. Kaikkea tietotaidon siirtymistä alueelta toiselle ei kuitenkaan voida luokitella näin selkeästi vakoilun nimikkeen alle. Esimerkiksi Suomen menestyksekäs puunjalostusteollisuus syntyi 1800-luvulla osittain ulkomailta hankitun osaamisen kautta. Tämä mallioppiseksi kutsuttava osaamisen siirtyminen on yhä tänäkin päivänä merkittävä tekijä taloudellisen kasvun tuottamisessa, ja kuuluu luonnollisena osana liiketoimintaan. Organisaatiot oppivat sekä tekemällä itse että oppimalla toisilta, ja suurin osa innovaatioista syntyykin jonkinlaisen jäljittelyn kautta. (Lamberg, 2019.)

2.2.1 Teollisuus- ja talousvakoilun historiaa Suomessa

Yrityksiin, tutkimuslaitoksiin ja kansantaloudellisiin toimijoihin kohdistuvasta järjestelmällisestä tiedustelusta ja vakoilusta on Suomessa dokumentoitua historiaa lähinnä kylmän sodan ajalta. Simolan (2009) mukaan vakoilua maassamme harjoittivat tuolloin ennen kaikkea Neuvostoliiton valtiolliset tiedustelupalvelut. KGB:n osalta tieteellis-teknisestä tiedustelusta vastasi ulkomaantiedustelun X-linja, joka toimi sotateollisen komission VPK:n ohjauksessa. Toinen Suomessa tieteellis-teknistä tiedustelua harjoittanut neuvostoliittolainen toimija oli sotilastiedustelu GRU. Vuonna 1977 ilmi tulleessa tapauksessa suomalainen liikemies oli hankkinut GRU:lle sotilasmateriaalia ja kaksoiskäyttötuotteita Britanniasta ja Israelista. Tuotteiden joukossa oli mm. konetuliase, suuntimalaite, sukeltajien painepuku, arktisiin oloihin tarkoitettu kumivene, lääkkeitä ja erikoislakkaa. Vaikka esitutkintakynnys asiassa ylittyi selvästi, päädyttiin asia tuon ajan tapaan unohtaa poliittisista syistä johtuen. (Simola, 2009, s. 71, 103.)

Simolan mukaan vielä 1960-luvulla Suomi ei kuulunut Neuvostoliiton tieteellis-teknisen vakoilun pääkohteisiin, ja kiinnostusta osoitettiin KGB:n taholta lähinnä Suomeen muuttaneisiin ulkomaalaisiin insinööreihin. Yksi heistä oli ranskalainen tutkateknikko ja agentuuriliike Startradingin johtaja Charles Azema, jolta KGB yritti Helsingissä ostaa Photoplot-ilmavalvontalaitetta vuonna 1966. Vuonna 1974 eräs kanadalainen käveli sisään Tehtaankadulla sijainneeseen lähetystöön ja halusi myydä työpaikallaan kehitteillä olevan, laseriin perustuvan ohjustorjunnan salaisuudet Neuvostoliitolle. Vuonna 1976 Suojelupoliisissa arvioitiin, että KGB oli käynnistänyt erityisen kampanjan teknisten tietojen hankkimiseksi suomalaisista yrityksistä ja Teknillisestä korkeakoulusta. Tuolloin maassamme alkoi olla orastavaa elektroniikka- ja tietokonealan osaamista, ja KGB:n arveltiin yrittävän myös ostaa insinööritoimistojen kautta teknologiaa, jota Neuvostoliittoon ei tuolloin ollut vientirajoitusten puitteissa lupa myydä. Useat suomalaisyritykset kuitenkin aloittivat kyseisten tuotteiden myynnin Neuvostoliittoon, minkä pelättiin pahimmassa tapauksessa aiheuttavan Suomen joutumisen länsimaiden kieltolistalle. Merkittävin teollisuusvakoiluun liittyvä tapaus sattui vuonna 1978, kun KGB hankki tietoja Kemiran tietopalvelun päälliköltä, diplomi-insinööri Eila Heliniltä sukupuolisuhdetta hyödyntäen. Tietojen luovutus oli alkanut jo vuonna 1973 ja johti kahden vuoden ja kuuden kuukauden vankeustuomioon. (Simola, 2009, s. 104–108.)

Simolan mukaan 1980-luvulla tieteellis-teknisen tiedustelun painoarvo kasvoi ja vakoilu muuttui suorasukaisemmaksi. Neuvostoliiton kulttuuri- ja tiedekeskus järjesti aktiivisesti Töölössä esitelmiä ja cocktailtilaisuuksia eri tieteenalojen edustajille, ja suomalaistutkijoita kosiskeltiin yhteistyöhön mm. erilaisten stipendien avulla. Hankalin tapaus sattui vuonna 1982, kun Rauma-Repola alkoi suunnitella Neuvostoliiton tiedeakatemian tilauksesta kahta sotilaskäyttöönkin soveltuvaa syvänmeren sukellusalusta. Vaikka Suomi ei ollut

allekirjoittanut teknologian vientiä Neuvostoliittoon rajoittavaa CoCom-sopimusta, oli sitä Teollisuuden keskusliiton piirissä noudatettu vapaaehtoisesti. Muita rikkomuksia tähän käytäntöön liittyen olivat VAX 11/750-tietokoneen ja Tektronix-työaseman vienti Neuvostoliittoon, jonka seurauksena kolme liikemiestä joutui syytteeseen ulkomaankaupan säädösrikkomuksista. (Simola, 2009, s. 109 ja 164.)

Marteliuksen mukaan kylmän sodan jälkeen Venäjän harjoittama teollisuusvakoilu lisääntyi edelleen, sillä maan talouden uudistaminen vaati viimeisimmän länsimaisen teknologian hyödyntämistä. Tieteellis-teknisen kehityksen edistäminen siihen liittyvää tietoa hankkimalla kirjattiin lakiin yhdeksi ulkomaantiedustelu SVR:n tehtäväksi vuonna 1992. Samaa edellytti myös asevoimien uudistaminen, ja sotilastiedustelu GRU:n ehdottomaksi prioriteetiksi asetettiin sotilasasioihin liittyvä talous- ja teollisuusvakoilu. Vuonna 1996 presidentti Jeltsin kritisoi Venäjän tiedustelupalveluita huonosta menestyksestä teollisuusvakoilussa, sillä maan tulevaisuuden sivilisaationa katsottiin riippuvan suoraan teknologisesta kehityksestä, ja lännen taloussalaisuuksien hankkiminen tulisi huomattavasti edullisemmaksi kuin omat taloudelliset ja tekniset innovaatiot. (Martelius, 1999, s. 238–241.)

2.2.2 Yritysvakoilun tilanne nykypäivänä

Kaksinapaisen suurvaltapoliittisen jännitystilan purkautumisesta huolimatta yritysvakoilu ilmiönä on kasvanut merkittävästi kylmän sodan jälkeisenä aikana. Tähän on tunnistettavissa monia syitä. Neuvostoliiton hajoamisen jälkeen alkanut globalisaatio ja Euroopan yhdentyminen ovat yritysvakoilun ohella edesauttaneet terrorismin sekä talous- ja huumerikollisuuden leviämistä (Kupi & Lanne, 2014, s. 11). Tiedon taloudellinen arvo on kasvanut kilpailun kovetessa, kun työvoima, pääoma ja hyödykkeet liikkuvat vapaammin kansallisten rajojen yli, minkä lisäksi sitoutuminen työnantajiin on heikentynyt työsuhteiden luonteen muututtua kohti osa-aikaisuuksia ja vuokratyövoiman käyttöä (Kähkönen, 2015, s. 1–2). Tiedustelupalveluiden henkilökuntaa on vapautunut yksityisille markkinoille, kaksoiskäyttöteknologia on lisääntynyt, ja tutkimuksen ja tuotekehityksen rooli on korostunut, kun Eurooppa ei ole kyennyt kilpailemaan tuotantokustannuksissa Kiinan ja muiden alhaisen kustannustason maiden kanssa (Holmström, 2010, s. 17–21). Suomi osana globaalia taloutta on yhä kiinteämmin osallisena tässä kehityksessä, eikä maallamme voida tässä suhteessa nähdä olevan erityisasemaa syrjäisen maantieteellisen sijainnin tai pienen väkiluvun ansiosta.

Yritysvakoilua valtiollisella tasolla laajamittaisesti harjoittaviksi tahoiksi on toisinaan ajateltu ainoastaan sellaisia maita, jotka ovat teknologisesta kehityksestä jäljessä, omaavat moraalisesti kyseenalaisia kulttuurisia piirteitä, tai joissa on enemmän tai vähemmän autoritaarinen hallinto. Tällaisina maina mainitaan julkisessa keskustelussa usein esimerkiksi Venäjä, Kiina, Iran ja Poh-

jois-Korea. Kuitenkin myös monet länsimaat harjoittavat merkittävää taloudellista tiedustelua ja vakoilua sekä toisia länsimaita että muita valtioita kohtaan, mikä saattaa länsimaiden omassa julkisessa keskustelussa jäädä vähemmälle huomiolle. Ranskassa presidentti Jacques Chirac perusti 1990-luvulla taloudellista ja teknologista tiedustelua koordinoivan hallintoelimen, mikä sai CIA:n syyttämään Ranskaa tiedusteluoperaatioista yhdysvaltalaisia yrityksiä kohtaan (Harris, 1998, s. 3). Ranskalaisten tiedetään esimerkiksi asentaneen vakoilulaitteita Air-France-lentoyhtiön matkustajakoneiden istuimiin (Wimmer, 2015, s. 80). Kaikkein merkittävimpänä tiedustelua harjoittavana tahona voidaan kuitenkin pitää Yhdysvaltoja, jonka mittavat tiedusteluresurssit on Edward Snowdenin paljastuksiin perustuen valjastettu myös laittomaan taloudellisen tiedon hankintaan. Yhdysvaltojen tiedustelupalveluiden on epäilty saavan yksityisiä käyttäjätietoja sellaisilta yhtiöiltä, kuten Google, Microsoft ja Facebook (Lamberg, 2019).

Tällä hetkellä yritysvakoilu näyttäytyy julkisessa keskustelussa useallakin tavalla. Yhdysvaltojen ja Kiinan välinen kauppasota on edelleen kiihdyttänyt vakoilusyytöksiä Kiinaa kohtaan, ja erityisesti Huawein asema 5G-verkkoihin liittyen on kyseenalaistettu juuri vakoilun riskin takia. Uudet teknologian alueet, kuten cleantech, nanomateriaalit ja erityisesti tekoäly, ovat nousseet keskustelussa halutuiksi yritysvakoilun kohteiksi, ja Venäjä on ollut toistuvasti syytettynä tekoälyä koskevan tiedon vakoilusta. Uusimpana käänteenä maailman turvallisuustilanteessa on ollut COVID-19-pandemia, joka on korostanut lääketeollisuuteen liittyvän tuotekehitystiedon roolia yritysvakoilun kohteena. Koronarokotteen lisäksi on todennäköistä, että vakoilua kohdistuu lääketeollisuuden koko valmistus-, logistiikka- ja jakeluverkostoon kaikkine sopimus- ja hinnoittelutietoineen, sillä viruksen uudet aallot pakottavat valtiot tavoittelemaan varastoihinsa monia erilaisia lääkkeitä ja suojavälineitä. Geopoliittisen tilanteen jännittyminen eri puolilla maailmaa ja siihen liittyvä geoekonomisen vaikuttamisen lisääntyminen indikoivat selkeästi yritys- ja talousvakoilun riskin kasvua myös tulevina vuosina.

2.3 Aiempi tutkimus

Tutkielman taustoittamiseksi tuli tehdä kirjallisuuskatsaus koskien yritysvakoilua, yritysturvallisuutta ja vastatiedustelua. Kansainvälisesti yritysvakoilua on tutkittu erityisesti 1990-luvulta alkaen. Merkittäviä tutkijoita ovat olleet mm. Turun yliopistossa vierailevana professorina toiminut Hedieh Nasheri Kentin yliopistosta, taloushistorian professori J.R. Harris Birminghamin yliopistosta sekä rikosoikeuden tohtori Daniel J. Benny Capella yliopistosta. Aihetta onkin lähestytty monien tieteenalojen näkökulmasta: taloustieteen, juridiikan, informaatioteknologian, kriminologian sekä jossain määrin myös tiedustelutut-

kimuksen. Tutkimusten painottuminen ilmiön syihin, seurauksiin, historiaan ja käytännön menetelmiin on vaihdellut näkökulman mukaan.

Suomessa yritysvakoilu on aiheena varsin vähän käsitelty akateemisen tutkimuksen alueella, ja aiheesta on löydettävissä enimmäkseen case-tyyppisiä tutkimusartikkeleita esimerkiksi Poliisiammattikorkeakoulusta. Kybervakoiluun liittyen on viime vuosina kirjoitettu jonkin verran erilaisia opinnäytetöitä, mutta nimenomaan yrityksiin kohdistuva vakoilu ei ole niiden pääaiheena, eikä kybervakoilua aseteta niissä yritysvakoilun viitekehykseen. Yritysvakoiluun liittyvää historiatietoa on löydettävissä Suojelupoliisin vuosikatsauksista sekä kootusti Suojelupoliisin historiikeista. Salassapitosyistä johtuen vuosikatsauksissa yritysvakoilutapauksia ei käsitellä yksilöidysti, minkä lisäksi historiikit päättyvät ajallisesti 1990-luvun alkuvuosiin. Sitä uudempia tietoja yritysvakoilutapauksista on löydettävissä lähinnä uutisartikkeleiden kautta.

Tiedon saatavuutta tutkimuksissa on rajoittanut erityisesti se, että yritykset eivät useinkaan halua kertoa tai tehdä rikosilmoitusta toteutuneista tapauksista mainesyistä johtuen. Siten tieto jää pinnan alle, yritysten johdon ja turvallisuudesta vastaavien tietoon. Yritysvakoilussa käytettävistä menetelmistä ja vastamenetelmistä on kuitenkin kirjoitettu jonkin verran kirjoja. Ne perustuvat sisällöltään alalla pitkään toimineiden turvallisuusasiantuntijoiden omiin kokemuksiin ja havaintoihin, eivätkä ole akateemisesti vertaisarvioituja teoksia. Tutkimusaineistona ne voidaan tässä tutkimuksessa rinnastaa asiantuntijahaastatteluihin. Yritysvakoilun tutkimista ja siitä kirjoittamista on rajoittanut aiheeseen liittyvä salaisuuksien ilmapiiri, sillä myöskään viranomaiset eivät aina ole halukkaita kertomaan vakoilussa käytetyistä menetelmistä tai vastamenetelmien tehokkuudesta. Tämä on ymmärrettävää, sillä niiden tunteminen saattaisi antaa arvokasta tietoa laitonta tiedonhankintaa suunnitteleville. Kuitenkin on perusteltua väittää, että rajoitettu tutkimus aiheesta samalla myös hidastaa ja jopa estää yritysten varautumista yritysvakoilun uhkaan.

Yritysturvallisuudesta löytyy paljon kirjallisuutta ja tutkimustietoa, mutta aihealueena se on varsin laaja ja sisältää mm. työturvallisuuteen ja paloturvallisuuteen liittyviä asioita. Yritysvakoilu näyttäytyy yritysturvallisuutta koskevassa kirjallisuudessa lähinnä tietoturvallisuuteen liittyen. Riskienhallinta vielä laajempana kokonaisuutena ei läpi käydyn kirjallisuuden valossa käsittele yritysvakoilua spesifinä riskinä lainkaan, vaan sen katsotaan implisiittisesti sisältyvän tietopääomaan kohdistuviin riskeihin. Mm. Sandberg (2015, s. 3) pitää yritysvakoilun näkymättömyyttä riskienhallintaa koskevassa tutkimuksessa merkittävänä ongelmana. Yritysturvallisuuden sekä operatiivisten ja vahinkoriskien hallinnan perusoppikirjana voidaan Suomessa pitää turvallisuusjohtamisen asiantuntija Juha Leppäsen vuonna 2006 julkaisemaa Yritysturvallisuus käytännössä -teosta.

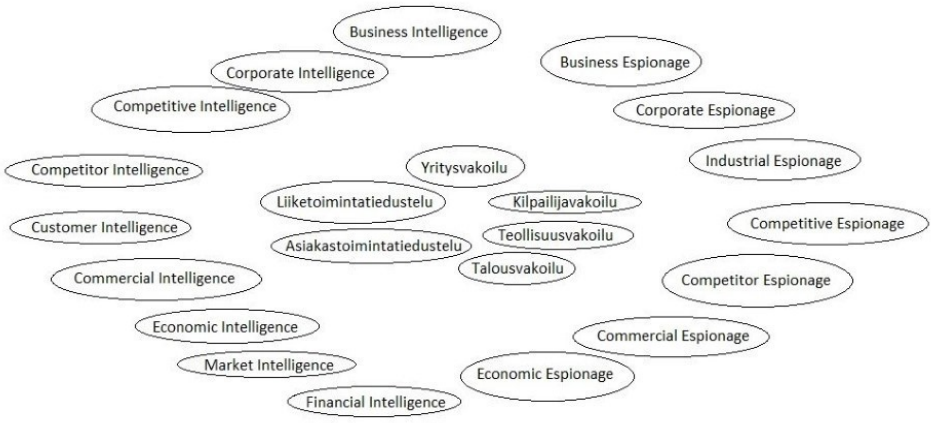
Vastatiedustelu akateemisena tutkimusalueena on uusi jopa tiedustelututkimuksen piirissä, ja siihen liittyvä kirjallisuus on hyvin rajallista. Suurin osa aiheeseen liittyvistä tutkimusartikkeleista käsittelee kylmän sodan aikaista vastavakoilutoimintaa. Käytännössä ainoa vastatiedustelun teoreettista mallia akateemisella tasolla kehittelevä teos on australialaisen Charles Stuart yliopiston

tiedusteluanalytiikan apulaisprofessori Hank Prunckunin kirja Counterintelligence, theory and practice (2012). Teoksessaan Prunckun ei kuitenkaan käsittele vastatiedustelua nimenomaisesti yritysten näkökulmasta. Akateemisena tutkimusalueena yritysvakoilun käsitteleminen vastatiedustelun kontekstissa on siten uutta paitsi Suomessa, myös kansainvälisellä tasolla.

Suomessa samaa tutkimuskysymystä, kuin tämä tutkielma, on aiemmin käsitellyt Juhani Matila pro gradussaan Yritysvakoilu – mitä se on ja miten siltä suojaudutaan? (2011). Väitöskirjojen osalta yritysvakoilua on sivuttu lähinnä oikeustieteen alalla. Aiheen tutkimista hankaloittaa sekin, että yrityksiin ja muihin taloudellisiin toimijoihin kohdistuvan tiedonhankinnan terminologia ei ole yhdenmukaista, vaan akateemisetkin lähteet käyttävät samoja termejä tarkoittamaan eri asioita. Perinpohjaisen käsiteanalyysin tekeminen olisi siten hyödyksi aihealueen tutkimiselle.

3 YRITYSVAKOILU JA VASTAAVAT KÄSITTEET

Yrityksiin liittyvän tiedustelutoiminnan yhteydessä käytetään isoa joukkoa termejä, joiden määrittely ei ole yksiselitteistä. Määritelmiä voidaan muodostaa sen mukaan, onko tiedustelutoiminta laitonta vai laillista, toteuttaako sitä yksityinen yritys vai valtiollinen toimija, ja onko sen kohteena yksittäinen yritys vai laajempi kokonaisuus, kuten jokin tietty markkina-alue tai kansantalous. Termejä määritellään eri yhteyksissä toisistaan eriävillä ja usein keskenään ristiriitaisilla tavoilla. Asiaa hankaloittaa lisäksi se, että aiheesta on kirjoitettu suomeksi hyvin vähän, joten vakiintuneita termejä ei suomen kielellä ole kaikissa tapauksissa löydettävissä lainkaan. Joitakin käännöstermejä, kuten liiketoimintatiedustelu ja asiakastoimintatiedustelu, ollaan vasta lanseeraamassa käyttöön mm. Jyväskylän yliopiston opetussuunnitelmissa, eikä niille löydy juurikaan hakutuloksia internetin hakukoneita käyttämällä (Jyväskylän yliopisto, 2020). Tiedustelun vakiintuminen akateemisen tutkimuksen alueelle edellyttää kuitenkin myös suomenkielisten termien vakiintumista käyttöön sekä niiden täsmällistä ja mielellään toisensa poissulkevaa määrittelyä. Lähdeaineistossa esiintyvät, sekä suomen- että englanninkieliset termit on esitetty kuviossa 1.



Kuvio 1: Käsitekartta

3.1 Yrityksiin kohdistuva laiton tiedonhankinta

Tämän tutkielman kannalta oleellista on sellainen yrityksiin kohdistuva tiedustelu, joka ei ole laillista, toisin sanoen yritysvakoilu. Englanniksi siitä käytetään termiä *corporate espionage*, minkä lisäksi yrityksiin kohdistuvaa laitonta tiedustelua kuvataan lähdeaineistossa termeillä *competitor espionage, competitive espionage, commercial espionage, industrial espionage, business espionage* ja *economic espionage*. Vastaavasti pääosin lain rajojen puitteissa tapahtuvaa tiedustelua kuvaamaan käytetään tyypillisesti päätettä *intelligence*. Kuitenkin esimerkiksi Harrison ja Andrii käyttävät artikkelissaan sanamuotoa ”laillinen teollisuusvakoilu”, tarkoittaen tiedonhankinnassa käytettäviä keinoja, jotka eivät ole ristiriidassa lainsäädännön kanssa (2017, s. 3). Termien suomentamisen tekee hankalaksi jo se, että sana *intelligence* sisältää erilaisia konnotaatioita asiayhteydestä riippuen, eikä aina viittaa tiedusteluun tuotteena, prosessina tai organisaationa. Vastaavasti päätettä *espionage* ei aina käytetä viittaamaan lakia rikkovaan toimintaan, vaan se voi pitää sisällään ainoastaan viittauksen salaisesta tai kyseenalaisesta toiminnasta.

Tässä tutkielmassa käytetään yritysvakoilua käsitteenä kuvaamaan kaikkea sellaista laitonta tiedonhankintaa, jonka kohteena on yritys. Tämä määrittely noudattelee rikoslakia, jonka 30 luvun 4 pykälän mukaan yritysvakoilulla tarkoitetaan toiselle kuuluvan liikesalaisuuden oikeudetonta hankkimista (Rikoslaki 39/1889). Tutkielman kannalta ei siten ole olennaista se, kuka vakoilua toteuttaa: toinen yritys, rikollisryhmä vai valtiollinen toimija. Olennaista määritelmän kannalta ei ole myöskään vakoilun tarkoitus, joka voi liittyä taloudellisen hyödyn saavuttamiseen, sotilaallisesti tärkeän teknologisen suorituskyvyn selvittämiseen tai kriittisen infrastruktuurin haavoittuvuuksien löytämiseen. Toisinaan yritysvakoilu liitetään terminä kuvaamaan pieniin ja keskisuuriin yrityksiin kohdistuvaa vakoilua, kun taas suuryritysten vakoilutapaukset luokitellaan talousvakoilun alle (Secmeter, 2020). Laittoman tiedonhankinnan menetelmät ja niihin varautuminen noudattelevat kuitenkin samoja periaatteita yrityksen koosta riippumatta. Tästä syystä yritysvakoilun käsitettä ei tässä tutkielmassa määritellä yrityksen koon perusteella.

Lainsäädännössä lähellä yritysvakoilun käsitettä ovat myös yrityssalaisuuden rikkominen ja yrityssalaisuuden väärinkäyttö (Rikoslaki 39/1889, 30 luku 5 ja 6 §). Ensimmäisen tarkoittaa käytännössä, että yrityksessä työskentelevä tai muutoin sen kanssa sopimussuhteessa oleva henkilö ilmaisee hallussaan olevaa tietoa yrityksen ulkopuoliselle taholle. Yritysvakoilusta tämän erottaa se, että tieto on henkilön saatavilla tämän työtehtävän perusteella, eikä sitä tarvitse erikseen hankkia esimerkiksi tietoteknisiä tai fyysisiä suojauksia murtamalla. Yrityssalaisuuden väärinkäytöstä on laissa säädetty, jotta myös se taho, jolle joko laittomasti tai laillisesti saatavilla olevat tiedot on toimitettu, saataisiin vastuuseen, mikäli hän näitä tietoja päättää käyttää taloudellista hyötyä saadakseen. Paljon julkisuutta saaneessa Nokian renkaiden ja Black Donuts Engineering-yhtiön rikostutkinnassa nämä kaikki rikosoikeudelliset termit olivat

esillä, ja hovioikeuden käsittelyssä tehtiin oikeuskäytäntöä muodostavaa rajanvetoa yrityssalaisuuden ja ammattitaidon välillä (Yle uutiset, 2019). Muita Suomessa tällä vuosituhannella esillä olleita, yritysvakoiluun liittyneitä tapauksia ovat olleet mm. Patria-konserniin liittyvä lahjustutkinta 2011–2013, Tietotekniikkayhtiö Promexin tapaus vuodelta 2005 sekä Soneran ja Telian välinen kiista vuosituhannen vaihteessa.

3.2 Yritysten suorittama liiketoimintatiedustelu

Siinä missä yritysvakoilun englanninkielinen termi *corporate espionage* viittaa yleensä laittomaan tiedonhankintaan, käytetään yritysten toteuttamasta laillisesta tiedonhankinnasta, tiedon analysoimisesta ja tiedolla johtamisesta termiä *business intelligence*. Suomennettuna se tarkoittaa vakiintuneen käytännön mukaan liiketoimintatiedon hallintaa. Se on käsitteenä kuitenkin paljon laajempi, kuin erilaisilla menetelmillä tehtävään tiedonhankintaan liittyvä toiminta, eikä useimmissa asiayhteyksissä sisällä lainkaan yrityksen ulkopuolelta suoritettavaa tiedonhankintaa. Liiketoimintatiedon hallinnan voidaan määritellä olevan informaatioprosessi, joka sisältää tietoa tarvitsevien päätöksentekijöiden tekemiä systemaattisia toimenpiteitä kilpailuedun saavuttamiseksi (Kaikkonen, 2017).

Grossmanin (2015) mukaan termiä *business intelligence* käytti ensimmäisen kerran H.P. Luhan vuonna 1958 mutta se vakiintui käyttöön vasta vuonna 1989. Tuolloin Howard Dresner määritteli sen tarkoittavan käsitteitä ja metodeja, joiden avulla parannetaan liiketoimintaan liittyvää päätöksentekoa faktapohjaisia järjestelmiä käyttäen (Grossmann, 2015, s. 1). Liiketoimintatiedon hallinnassa tyypillisesti käytettäviä käytännön keinoja, kuten tiedonlouhintaa, ei sinänsä voidakaan samaistaa tiedustelun käsitteen kanssa. Tästä syystä yritysten toteuttamaa, laillista ja tiedusteluluonteista tiedonhankintaa kuvataan termillä *corporate intelligence*, jonka suomenkieliseksi vastineeksi on muodostumassa liiketoimintatiedustelu. Carlisle (2005) määrittelee sen muodostuvan yrityksen johdon ohjauksesta, tiedon keräämisestä, tiedon oikeellisuuden analysoimisesta sekä tiedon välittämisestä päätöksiä tekeville tahoille. Tämä prosessi muistuttaa klassista tiedusteluympyrää. Hän myös rinnastaa termit *corporate intelligence* ja *competitive intelligence* toisiinsa, mikä viittaa siihen, että tiedon keräämisen toteuttajana on joko yritys itse tai sen lukuun toimiva alihankkija. (Carlisle, 2005, s. 170.) Osana liiketoimintatiedon hallintaa ja asiakkuudenhallintaa voidaan lisäksi nähdä *customer intelligence* eli asiakastoimintatiedustelu, jota voidaan toteuttaa mm. tekstianalytiikan ja markkinatutkimusten keinoin sekä havainnoimalla asiakkaiden liikkumista yrityksen internetsivustolla tai toimipaikassa.

Kilpailullinen tiedustelu tai kilpailijatiedustelu, englanniksi *competitive intelligence* ja *competitor intelligence*, voidaan nähdä osana *business intelligence* -kattotermiä. Suomessa on totuttu aiheeseen liittyen puhumaan kilpailijatiedon hankinnasta tai kilpailija-analyysistä, ja terminä kilpailijatiedustelun käyttäminen on hakukoneiden hakutulosten perusteella harvinaista. Siinä missä asiakas-

toimintatiedustelun tarkoituksena on pyrkiä asiakkaiden tuntemiseen, kohdistuu kilpailijatiedustelun huomio kilpaileviin yrityksiin. Se voidaan määritellä systemaattiseksi ohjelmaksi tiedon keräämiseksi ja analysoimiseksi kilpailijoiden aktiviteeteistä sekä kyseisen markkinan yleisistä kehityssuunnista oman yhtiön tavoitteiden edesauttamiseksi (Kahaner, 1998, s. 13–15). Kilpailijatiedustelu on prosessi, jonka avulla selvitetään kilpailijoiden toimia ja tilannetta, ja jonka tuottamaa tietoa käytetään hyödyksi suunniteltaessa markkinointikampanjoita, tuotantoa, rahoitusta, henkilöstöresursseja ja ylipäätään kaikkea, johon yrityksen kilpailijoilla on suora tai epäsuora vaikutus (West, 2001). Westin mukaan yksityistäminen, sääntelyn purkaminen, globalisaatio, markkinaliberalismi sekä ajoittaiset talouden laskusuhdanteet ovat lisänneet kilpailijatiedustelun merkitystä liiketoiminnassa. Hänen mukaansa tiedustelu kohdistuu sekä yrityksen suoriin että myös epäsuoriin kilpailijoihin, eli niihin, jotka pyrkivät vastaamaan samaan tarpeeseen asiakaskunnassa. Lisäksi tiedustelu voi kohdistua yrityksen omaan hankintaketjuun, tavarantoimittajiin ja muihin yhteistyöyrityksiin, jakeluverkostoon ja mahdollisiin investointikohteisiin. Näiden kaikkien osalta pyritään selvittämään niiden olemassa olevia tai potentiaalisia suhteita yrityksen kilpailijoihin. (West, 2001.)

Jo vuonna 2002 Business Week uutisoi, että Yhdysvaltojen suurista yrityksistä yhdeksälläkymmenellä prosentilla on henkilöstöä, jonka toimenkuvaan kuuluu kilpailijatiedustelu, ja useat näistä yhtiöistä käyttivät sen toteuttamiseen enemmän kuin miljardi dollaria vuodessa (Billand, 2009, s. 2). Tiedustelua voi yrityksessä toteuttaa siihen osoitettu henkilö tai tiimi, mutta usein sitä ostetaan kyseistä palvelua tarjoavilta konsulttiyrityksiltä. Käytännössä tällainen konsulttiyritys lähestyy kilpailijaa esimerkiksi puhelimitse tai sähköpostitse erilaisten kysymysten muodossa. Niin kauan kuin konsultti käyttää omaa ja yrityksensä nimeä, toiminta pysyy yleensä lain asettamien rajojen sisäpuolella, vaikka kohteena oleva yritys ei ymmärtäisi antamiensa tietojen päätyvän kilpailijalle. Yleinen tapa onkin herättää kuva, että ollaan tekemässä jonkinlaista markkinatutkimusta. Mikäli kuitenkin esittäydytään väärällä henkilöllisyydellä tai jonkin muun tahon nimissä, muuttuu tiedustelu kilpailijavakoiluksi ja sitä kautta laittomaksi toiminnaksi. Samoin tapahtuu messuilla tai konferensseissa, joissa on tyypillistä lähestyä kilpailijoita esitteiden ja tuotenäytteiden saamiseksi, ja samalla saadaan mahdollisuus esittää kysymyksiä kilpailijan edustajalle.

Toinen tyypillinen tapa kilpailijan tuotteiden valmistusteknologian ja -prosessin selvittämiseksi on käänteissuunnittelu tai takaisinmallinnus, eli tuotteen hankkiminen markkinoilta ja sen purkaminen osiin. Tämäkin toiminta on sinänsä laillista, kunhan tuote on ostettu laillisesti eikä suunnitteluprosessin selvittäminen johda suoraan immateriaalioikeuksien rikkomiseen tuotetta kopioimalla. Kilpailijatiedustelua voidaan toteuttaa myös *mystery shopping* -toiminnalla, eli asioimalla asiakkaana kilpailijan myymälöissä havaintoja ja muistiinpanoja tehden, joskin tätäkin toimintaa voidaan pitää epäeettisenä (Shing & Spence, 2002, s. 1–2).

3.3 Taloudellinen tiedustelu ja talousvakoilu

Taloudellisella tiedustelulla, *economic intelligence*, tarkoitetaan vakiintuneen määritelmän mukaan tiedustelua, jota valtiollinen toimija toteuttaa oman valtionsa talouden ja yritysten tukemiseksi. Trimin mukaan se voidaan jakaa kahteen alakäsitteeseen, mikro- ja makroekonomiseen tiedusteluun, joista ensin mainittu tarkoittaa tiedonhankintaa oman valtion yritysten ulkomaisista kilpailijoista kansainvälisillä markkinoilla, sekä toisaalta oman maan yritysten suojaamista kilpailijavakoilun kohteeksi joutumiselta. Viimeksi mainittu taas tarkoittaa strategista analyysiä toisen valtion taloudellisesta, talouspoliittisesta, sosiaalisesta ja teollisesta tilanteesta. Vastaavasti sanan *intelligence* vaihtaminen sanaan *espionage* siirtää saman käsitteen tarkoittamaan lainvastaista toimintaa eli talousvakoilua. (Trim, 2002, s.8.)

Käsitteiden moniselitteisyyttä kuvaa se, että mm. Trim (2002) liittää Johnsoniin (1996) nojautuen kaupallisen tiedustelun, *commercial intelligence*, taloudellisen tiedustelun kattotermin alle, vaikka useimmiten sitä käytetään synonyyminä yritysten harjoittamalle liiketoimintatiedustelulle. Termiä teollisuusvakoilu, *industrial espionage*, käytetään usein talousvakoilun osa-alueena, tarkoittaen valtiollisten tiedustelupalvelujen kohdistamaa, laitonta tiedonhankintaa merkittäviä taloudellisia panostuksia tutkimukseen ja tuotekehitykseen käyttäviin teollisuusyhtiöihin (Secmeter, 2020). Kuitenkin esimerkiksi Søilen (2016, s. 52) erottelee teollisuusvakoilun talousvakoilusta siten, että ensiksi mainittu ei tapahdu valtiollisen organisaation vaan kilpailevan yrityksen toimesta. Myös Crane (2004) antaa jo artikkelinsa nimessä ymmärtää, että teollisuusvakoilu on yksityisen yrityksen suorittamaa tiedonhankintaa, joka on siirtynyt laittoman toiminnan puolelle. Holmström (2010, s. 21) käyttää artikkelissaan muutoin lähdeaineistossa harvoin esiintyvää termiä *industrial intelligence* rinnakkain teollisuusvakoilun kanssa. Hän tukeutuu käsitteiden määrittelyssä Pourteusiin (1994), jonka mukaan teollisuusvakoilu on yksityisten yritysten suorittamaa laitonta, salaista tai petollisessa tarkoituksessa toteutettavaa taloudellista tiedustelua. Budiono ja Sawitri (2017, s. 31) puolestaan käyttävät termiä *business espionage* riippumatta siitä, onko vakoilua suorittava taho yksityinen henkilö, yritys tai valtiollinen organisaatio.

Termejä *market intelligence* ja *financial intelligence* käytetään liiketoimintatiedon hallinnan eli *business intelligencen* yhteydessä, missä kontekstissa sanan *intelligence* merkityssisältö viittaa enemmän älykkyyteen kuin tiedusteluun. Suomeksi tunnettu termi markkina-analyysi tarkoittaa ymmärrystä markkinoilla toimivista tahoista, hinnoista, asiakkaista sekä nykyisistä ja tulevista trendeistä, sekä kaiken tämän tiedon integroimisesta yrityksen strategiaan esimerkiksi markkinoille penetroitumiseen liittyen. Sen tehtävä on tarjota yrityksen päätöksentekijöille kokonaiskuva yrityksen suoriutumisesta ja mahdollisuuksista suhteessa niihin markkinoihin, joilla se toimii (Prescott & Miller, 2001, s. 195–202). *Financial intelligencen* voidaan laajassa määritelmässä katsoa tarkoittavan talousälyä, eli ymmärrystä taloudellisten toimien, kuten sijoittamisen ja lainan-

oton tuottomahdollisuuksista ja riskeistä. Suppeassa määritelmässä sillä viitataan enemmän tiedustelutoimintaan, kuten varojen siirtoihin, verovilppiin ja rahanpesuun liittyvään talousrikostutkintaan.

Viime aikoina sekä *market intelligence* että *financial intelligence* -termejä on alettu käyttää myös taloudelliseen tiedusteluun viittaavassa kontekstissa. Siinä yhteydessä niiden katsotaan tarkoittavan valtiollisen tiedustelupalvelun tai tutkimuslaitoksen tutkimustoimintaa, joka kohdistuu globaaleiden markkinoiden tiettyihin segmentteihin tai finanssijärjestelmiin, ja jonka tehtävä on seurata ja selvittää geoekonomiseen vaikuttamiseen liittyviä tapahtumia (Alonso-Trabanco, 2020). Nykyisessä geopoliittisessa toimintaympäristössä, jossa geoekonomiaa käytetään yhä enemmän suurvaltapoliittisen vaikuttamisen välineenä, korostuu talouteen, markkinoihin ja finanssijärjestelmiin kohdistuvan tiedustelun merkitys enenevässä määrin.

4 TUTKIMUKSEN TOTEUTTAMINEN

Tässä luvussa käsitellään tutkimuksen toteuttamista. Ensin esitellään käytetty tutkimusmenetelmä ja sen jälkeen kuvataan tutkimusaineiston hankkiminen sekä analyysiprosessi. Lopuksi kuvataan tapa, jolla tulokset syntyivät tutkimusdatasta valittua metodia käyttäen, sekä arvioidaan tutkimuksen validiteettia ja reliabiliteettia. Tutkimus alkoi aiheen valinnan jälkeen aiheeseen perehtymisellä, lähdeaineiston hankkimisella sekä haastateltavien etsimisellä. Lähes kaikki haastateltaviksi kutsutut asiantuntijat halusivat osallistua tutkimukseen. Varsinainen haastatteluosuus toteutettiin pääosin tammi-toukokuun 2020 aikana, minkä lisäksi joitakin täydentäviä haastatteluita tehtiin syksyllä 2020. Vallitsevan COVID-19 –epidemiatilanteen takia kaikki haastattelut toteutettiin sähköpostitse tai etäkokousmenetelmiä käyttäen. Tässä luvussa pohditaan siksi myös sähköpostin käyttämistä teemahaastattelun toteuttamisessa.

4.1 Tutkimusmenetelmä

Tämän tutkimuksen tarkoituksena oli selvittää yritysvakoilussa käytettäviä menetelmiä ja vastamenetelmiä, sekä yritysvakoilun tämänhetkistä tilannekuvaa Suomessa. Tätä varten tuli valita sopiva tutkimusmenetelmä. Käsitteellisesti kvalitatiivinen tutkimusmenetelmä on tutkimussuuntauksen, aineistonkeruumenetelmän ja analyysimenetelmän yhdistelmä. Koska tässä tutkimuksessa tutkimuksen kohteena olevaa ilmiötä lähestytään haastateltavien sitä koskevien käsitysten kautta, valittiin tutkimusmenetelmäksi fenomenografia. Fenomenografisessa tutkimusotteessa päähuomio on kokevan ihmisen ymmärryksessä, kokemuksessa ja tapahtumien kytkemisessä niitä selittäviin yhteyksiin (Heinonen, Keinänen & Paasonen, 2013, s. 38).

Tutkimuskysymysten laajuudesta ja viitekehyksen haastavuudesta johtuen aineistonhankintamenetelmäksi valittiin teemahaastattelu. Sen kautta pyrit-

tiin saavuttamaan tutkimuksessa tavoiteltu ymmärrys aiheesta, josta löytyy hyvin rajallisesti aiempaa tutkimusta. Teemahaastattelu onkin sopiva menetelmä silloin, kun halutaan tietoa vähemmän tunnetuista ilmiöistä. Se antaa haastateltaville tilaa puhua aiheesta asetettua kysymystä laajemmin, ja mahdollistaa tiettyjen kysymysten painottamisen haastateltavasta riippuen. (KvaliMOTV, 2020.) Usein tutkimus- ja aineistonhankintamenetelmän määrittely on teemahaastattelua käytettäessä väljää, ja esim. Heinonen, Keinänen ja Paasonen (2013, s. 37) rinnastavat haastattelut yhdeksi kvalitatiiviseksi tutkimusmenetelmäksi fenomenografian, tapaustutkimuksen ym. rinnalle. Myöskään fenomenografian asemasta tutkimusmenetelmänä ei ole yksimielisyyttä, vaan joissakin lähteissä sitä pidetään ainoastaan aineiston analyysimenetelmänä.

Sekä fenomenografia että teemahaastattelu kuuluvat kvalitatiivisen eli laadullisen tutkimuksen piiriin. Hirsjärven, Remeksen ja Sajavaaran (2016) mukaan laadullinen tutkimus pyrkii kokonaisvaltaiseen, todellisen elämän ilmiöiden kuvaamiseen. Tiedonkeruun instrumentteina ovatkin yleensä ihmiset, ja tutkimus tapahtuu keskusteluiden ja havaintojen kautta. Laadullisen tutkimuksen tarkoitus ei ole testata ennalta määriteltyä hypoteesia, vaan se pyrkiä löytämään uutta ja ennalta odottamatonta tietoa. Haastatteluiden, havainnoinnin ja analyysin kautta pyritään tuomaan ilmi tutkimukseen osallistuvien näkökulmia aiheeseen, mistä johtuen laadullinen tutkimus ei yleensä perustu satunnaisotantaan vaan tarkasti valikoituun tutkimusjoukkoon. Kvalitatiivisessa tutkimuksessa tutkimussuunnitelma saattaa usein muovautua ja muuttua tutkimuksen edetessä, mistä syystä tutkimuksen toteutuksen tulee mahdollistaa tietynasteinen joustavuus. (Hirsjärvi, Remes & Sajavaara, 2016, s. 164.)

Heinosen, Keinäsen ja Paasosen (2013) mukaan haastattelua käytetään tutkimuksessa silloin, kun tarvitaan tietoa henkilöiden kokemuksista, havainnoista ja mielipiteistä. Siinä, kuten muissakin kvalitatiivisissa tutkimusmenetelmissä, käytetään usein avoimia kysymyksiä, joihin saadaan vapaamuotoisia suusanallisia tai kirjallisia vastauksia. Haastattelu on tutkijan ja tutkittavan henkilökohtaista kommunikointia edellyttävää toimintaa, joka voi tapahtua joko täysin vapaamuotoisesti, ennalta suunnitellusti eli strukturoidusta, tai kuten tämän tutkimuksen kohdalla, puolistrukturoidusti. (Heinonen ym., 2013, s. 35–37.) Tässä tutkimuksessa fenomenografisen tutkimusotteen avulla pyritään vastaamaan sekä pää- että apututkimuskysymykseen, mutta varsinkin päätutkimuskysymyksen osalta hyödynnetään myös kirjallista tutkimusaineistoa, joka sisällöltään voidaan rinnastaa asiantuntijahaastatteluihin. Pohdintaa sisältävässä luvussa tutkielma saa myös kehittämishankkeen piirteitä, sillä siinä esitetään käytännön menetelmiä ratkaisuksi tutkimuksessa esille tulleisiin ongelmiin. Nämä menetelmät ovat riskin todennäköisyyden arviointimalli sekä kontrollitoimien laajuutta visuaalisesti havainnollistava matriisikartta.

4.2 Tutkimusaineiston hankkiminen

Tutkimusaineiston hankkiminen on tärkeä osa tutkimusta, sillä oikeanlainen aineisto on edellytys tutkimusten tulosten luotettavuuden varmistamiselle (Heinonen ym., 2013, s. 15). Heinosen ym. mukaan kvalitatiivisessa tutkimuksessa tutkimusotanta on harkinnanvarainen verrattuna kvantitatiivisen tutkimuksen satunnaisotantaan. Tämä asettaa erityisiä haasteita tutkimuksen yleistämiseen ja toistettavuuteen liittyen. Harkinnanvarainen otanta onkin yleensä aina mielivaltainen, mikä on syytä huomioida tuloksia tarkasteltaessa. Tutkimuksen toistettavuus ei useinkaan onnistu, mistä syystä liian pitkälle meneviin yleistyksiin tulee aina suhtautua varauksella. (Heinonen ym., 2013, s. 59.) Hirsjärven (2016, s. 164) mukaan laadullisella tutkimuksella ei kuitenkaan edes tule pyrkiä yleispätevyyteen. Yleistämisen sijaan kvalitatiivisessa tutkimuksessa voidaankin puhua tutkimuksen suhteuttamisesta aiempaan tietoon (Alasuutari, 1993).

Haastateltaviksi tutkimukseen valittiin yhteensä kymmenen asiantuntijaa sellaisista organisaatioista, jotka tavalla tai toisella ovat tekemisissä yritysvakoilun kanssa. Nämä organisaatiot ovat Elinkeinoelämän keskusliitto, Suojelupoliisi, Keskusrikospoliisi, Helsingin seudun kauppakamari, Finnish Information Security Cluster, Cyberwatch, F-Secure ja Opsec. Haastattelukysymysten malliruko löytyy liitteestä 1. Potentiaalisia haastateltavia lähestyttiin ensin viestillä, jossa kysyttiin halukkuutta osallistua tutkimukseen. Näitä viestejä lähetettiin kaikkiaan neljätoista, joten neljä asiantuntijaa ei halunnut osallistua, tai peruivat myöhemmin halukkuutensa. Varsinaiset haastattelukysymykset lähetettiin toisessa viestissä, minkä jälkeen asiaan palattiin vielä tarkentavien kysymysten muodossa joko sähköpostitse tai etäkokousmenetelmällä. Joidenkin asiantuntijoiden kohdalla aikaväli ensimmäisestä viestistä tarkentaviin vastauksiin oli neljä kuukautta, minkä tutkimukseen varattu aikaikkuna myös mahdollisti.

Toisin kuin Matilan tutkimuksessa (2011), tässä tutkimuksessa haastateltavia ei pääsääntöisesti ole anonymisoitu, vaan haastateltavien antamat lausunnot osoitetaan lähdeviittausmerkinnöillä. Tällä pyritään nostamaan tutkimuksen uskottavuutta, kun huomioidaan aiheen yhteiskunnallinen merkitys sekä tutkimuksen tulosten mahdollinen hyödyntäminen jatkossa. Ainoastaan yritysvakoilun vastamenetelmiä koskevassa osiossa sekä sosiaalisessa ja fyysisessä tilassa toteutettavien vakoilumenetelmien osalta ei kaikkia haastateltavien antamia tietoja ole voitu turvallisuussyistä johtuen liittää tiedon antajaan. Haastateltavaksi valittujen määrä oli riittävä, sillä vaadittu saturaatiopiste saavutettiin hyvin. Tämä tarkoittaa sitä, että haastatteluissa ei enää tullut esiin uutta tietoa, vaan vastauksissa alkoivat toistua samat asiat.

Oma kysymyksensä tutkimusta arvioitaessa on haastatteluiden toteuttaminen Suomessa vallinneista poikkeusoloista johtuen pääasiassa sähköpostitse. Aihetta on tutkinut mm. Koivula Jyväskylän yliopiston pro gradu –tutkielmassa vuonna 2010. Hän on todennut, että sähköpostilla on teemahaastattelun välineenä sekä etunsa että haittansa. Sähköposti on vähemmän henki-

lökohtainen menetelmä kasvokkain tapahtuvaan keskusteluun verrattuna, eikä mahdollista haastateltavien välittömien reaktioiden arvioimista. Toisaalta sähköposti tarjoaa haastateltaville enemmän aikaa harkita vastauksiaan. Sähköpostilla tapahtuvan haastattelun ei myöskään tarvitse olla muodoltaan strukturoitu, vaan kysymyksiä voidaan esittää eri tavalla ja eri järjestyksessä haastateltavasta riippuen. Vaikka vastavuoroisuus sähköpostitse on vaikeampaa, on sekin mahdollista toteuttaa useita viestejä vaihtamalla. (Koivula, 2010, s. 3–17.) Tässä tutkimuksessa haastatellut henkilöt toimivat sellaisissa asiantuntija- ja johtotehtävissä, että sähköpostitse tapahtuneen haastattelun selväksi eduksi muodostui haastateltavien mahdollisuus paneutua haastattelukysymyksiin haluamanaan ajankohtana.

4.3 Aineiston analyysi

Empiiristä tutkimusta varten hankittua, käsittelemätöntä tietoa kutsutaan tutkimusaineistoksi. Jotta sitä voitaisiin hyödyntää, tulee aineisto analysoida tutkimusmenetelmän edellyttämällä tavalla. Tässä tutkimuksessa haastatteluaineiston analyysi aloitettiin teemoittelemalla vastaukset tutkimuskysymysten mukaisesti. Valitut teemat olivat seuraavat:

1. Yritysvakoilussa käytettävät menetelmät
2. Yritysvakoilun estämiseen liittyvät toimet
3. Yritysvakoilun tilannekuva Suomessa
4. Varautumiseen liittyvät ongelmakohdat

Haastateltavat eivät tutkimuksen puolistrukturoidusta muodosta johtuen vastanneet ainoastaan yhteen kysymykseen kerrallaan, vaan kysymysten alla olevat vastaukset polveilivat aiheesta toiseen. Täten vastauksia eri teemoihin löytyi aineistosta lukuisista eri kohdista. Teemoittelulla kaikki haastatteluaineiston kautta saadut tiedot ryhmiteltiin yllä oleviin ryhmiin. Tämän kautta lähdettiin muodostamaan tutkimuksen tuloksia tutkimusasetelman kontekstissa ja fenomenografista analyysia hyödyntäen. Tutkimusasetelma on tutkimusongelman, -menetelmän ja –aineiston kokonaisuus, ja sen on tarkoitus muodostaa jatkumo johdantoluvussa esitellylle teoreettiselle pohjatyölle (Eskola 1998, s. 80).

Tutkimuksen analyysivaiheessa jouduttiin eettisen ongelmallisuuden osalta pohtimaan samaa asiaa kuin Matila (2011) omassa pro gradu –tutkielmassaan, nimittäin yritysvakoilun menetelmien ja vastamenetelmien esittelyn mahdollista edesauttavaa vaikutusta yritysvakoilua harjoittaville tai sellaista suunnitteleville tahoille. Toisin sanoen pohdittavaksi tuli kysymys, olisiko tutkimuksen

lukemisesta hyötyä henkilölle, joka aikoo toteuttaa yritysvakoilua, ja muodostuisiko tutkimuksen julkisuus siten haitalliseksi yritysten ja yhteiskunnan kannalta? Pohdinnassa päädyttiin siihen, että yritysvakoilua harjoittavat tahot ovat jo nyt perillä siihen käytettävistä menetelmistä ja tuntevat yritysturvallisuuden kontrollitoimia tarpeeksi hyvin niitä kiertääkseen. Sen sijaan menetelmät ja vastamenetelmät ovat usein tuntemattomia laittoman tiedonhankinnan kohteena olevissa yrityksissä, joten tutkimuksen hyödyllisyys yrityksille ylittää teoreettisen ajatuksen eettisestä ongelmallisuudesta.

Tutkimuksen luotettavuuden kannalta pohdittava asia oli se, kuinka rehellisesti ja avoimesti haastatteluihin osallistuneet asiantuntijat pystyivät aiheesta puhumaan. Esimerkiksi viranomaisten osalta oli selvää, että tietoa Suomessa tapahtuvasta yritysvakoilusta pystyttiin antamaan vain rajallisesti ja kohteeksi joutuneita yrityksiä yksilöimättä. Tämä ei kuitenkaan muodostu tutkimuksessa ylitsepääsemättömäksi ongelmaksi, sillä tavoite oli tutkia yritysvakoilua ilmiönä, riippumatta yksittäisestä tekijästä tai teon kohteesta. Luonnollisesti myös muut haastattelututkimuksia yleisesti koskevat ongelmallisuudet tulee huomioida, kun tutkimusta tarkastellaan kriittisesti. Näitä ovat mm. haastateltavien mahdollinen ajan puute paneutua vastauksiin, elite bias, eli haastateltavien korkean asiantuntija-aseman vaikutus lopputuloksiin, tutkijan oma vaikutus mm. kysymyksenasettelun kautta sekä ns. Hawthorne-ilmiö, eli haastateltavien käyttäytymisen muuttuminen tarkkailun kohteena olemisen seurauksena (Mayers & Newman, 2006, 4–5).

4.4 Tutkimuksen tulokset

Fenomenografinen tutkimus ei pitäydy pelkästään tutkimusaineiston kuvailemisessa, vaan päämääränä on antaa erilaisille käsityksille merkityksiä ja rakentaa niistä kategorioita eli merkitysluokkia (Ahonen, 1994). Siinä, missä fenomenologia keskittyy tutkittavan ilmiön subjektiiviseen kokemiseen, painottaa fenomenografia erilaisten näkökulmien ja käsitysten löytämistä. Siitä huolimatta päähuomio tulee pitää tutkimuskysymyksessä, metodin ollessa ainoastaan keino päämäärään pääsemiseen eli tutkimuskysymykseen vastaamiseen. Vaikka fenomenografia lähestyy tutkimusaihetta eri henkilöiden käsitysten kautta, eivät näiden käsitysten syyt tai eroavuudet toisistaan ole tutkimuksen tuloksia, mikäli ne eivät ole tutkimuskysymys.

Tutkimusaineiston keräämisen jälkeen aineistosta etsittiin tutkimuskysymysten näkökulmasta oleellisia käsityksiä. Nämä käsitykset teemoiteltiin tutkimuskysymystä mukaillen edellä kuvaillulla tavalla. Näiden teemojen sisältä oli löydettävissä selvästi toisistaan poikkeavia merkitysyksikköjä, joiden muodostuminen fenomenografiassa tapahtuu intersubjektiivisesti eli haastateltavan antaman vastauksen ja tutkijan tekemän tulkinnan yhdistelmänä (Ahonen, 1994). Kun nämä merkityssisällöt lajiteltiin kategorioiksi ja merkityskategoriat yhdistettiin tutkimuksen taustalla olleeseen teoreettiseen tietoon, alkoivat tut-

kimuksen tulokset hahmottua. Fenomenografisen prosessin mukaisesti nämä kategoriat muodostivat lopulta tutkimuksen tekijän oman teorian tutkittavasta aiheesta.

Käytännössä merkitysyksiköt poimittiin aineiston teemoista taulukoimalla, minkä jälkeen taulukoitu aineisto ryhmiteltiin ylemmän tason kategorioihin. Esimerkkinä teemasta on yritysvakoilussa käytetty menetelmä, jonka sisältä oli löydettävissä merkityssisältöinä erilaisia, spesifejä käytännön menetelmiä, jotka voitiin luokitella kolmen erilaisen merkityskategorian alle.

Eräs tutkimuksen oleellisista löydöksistä oli tutkimuskysymyksessä esitettävien, yritysvakoilussa käytettävien keinojen ryhmittely uudella tavalla. Yritysvakoilun keinovalikoima voidaan näin lajitella vaihtoehtoisella, asiayhteyteen perinteistä tiedustelulajijaottelua paremmin sopivalla tavalla. Yritysvakoilussa käytettäviä yksittäisiä keinoja tunnistettiin näiden kategorioiden sisältä laskentatavasta riippuen 20–30 kappaletta. Yritysvakoilun estämiseen käytettäviä yksittäisiä keinoja tunnistettiin noin 80 kappaletta (Liite 2), jotka jaoteltiin kahdeksaan merkityskategoriaan. Täydentävän tutkimuskysymyksen osalta pystyttiin muodostamaan yritysvakoilua koskeva, suurpiirteinen tilannekuva sekä tunnistamaan varautumiseen yleisellä tasolla liittyviä keskeisiä heikkouksia. Nämä tulokset ja teoriat esitetään kahdessa seuraavassa luvussa, jotka käsittelevät tutkimustulosten tulkintaa.

Koska tutkimuksen tulokset perustuvat kerättyyn aineistoon, ja koska analyyttisen menetelmän käyttäminen on tutkimuksessa ollut johdonmukaista, voidaan tulosten katsoa täyttävän sekä validin että reliaabelin tutkimuksen vaateet. Näiltä osin tutkimus on puolueeton ja luotettava, uskottava ja yleistettävissä oleva, sekä käytäntöön sovellettavissa oleva. Käytetty tutkimusmenetelmä, fenomenografia, soveltui tutkimuksen toteuttamiseen hyvin, joskin tutkimusmenetelmiä koskeva lähdekirjallisuus ilmeni paikoin ristiriitaisena sen suhteen, asemoituuko fenomenografia enemmän analyysimenetelmäksi vai tutkimusmenetelmäksi kokonaisuutena. Käytännön, eli tutkimustulosten muodostamisen kannalta tutkimusaineistoon perustuen ei tällä teoreettisella rajanvedolla kuitenkaan ollut vaikutusta.

5 YRITYSVAKOILUN TILANNEKUVA SUOMESSA

Tämän tutkielman tavoitteena ei ollut selvittää kuinka paljon yritysvakoilua Suomessa tapahtuu tai kuinka isoja menetyksiä siitä aiheutuu yrityksille, mutta siitä huolimatta haastatteluissa luotiin yleiskatsaus yritysvakoilun tämänhetkiseen tilannekuvaan. Valitettavasti kenelläkään haastatelluista asiantuntijoista ei ollut tiedossa tutkimusta, jossa näitä kumpaakaan seikkaa olisi tarkemmin selvitetty. Keskuskauppakamari on kysynyt aiheesta yritysten rikosturvallisuuteen liittyvän tutkimuksen yhteydessä vuosina 2005, 2008, 2012 ja 2017. Näissä tutkimuksissa vakoilun kohteeksi on epäillyt joutuneensa 8–10 % vastaajista (Silen, haastattelu, 10.2.2020). Useat haastatelluista asiantuntijoista olivat kuitenkin sitä mieltä, että yritysvakoilua, varsinkin verkon kautta, saattaa todellisuudessa tapahtua paljon enemmän. Viimeisimmässä, Helsingin seudun kauppakamarin tutkimuksessa loppuvuonna 2020 yritysvakoilulle altistuneiden yritysten määrä olikin kaksinkertaistunut 17 prosenttiin, ja suurista yrityksistä jopa 31 prosenttia katsoi joutuneensa yritysvakoilun kohteeksi (Helsingin seudun kauppakamari, 2020). Vakoilulle erityisen alttiina toimialoina on julkisessa keskustelussa aiempina vuosina mainittu telekommunikaatio, paikannus- ja laserteknologiat sekä bio- ja lääketieteet. Viime vuosina näiden rinnalle on noussut ns. uusia teknologioita, kuten nanomateriaalit, tekoäly ja cleantech. Kokonaiskuvan muodostamisessa haasteeksi nousee se, että näillä toimialoilla toimivien yritysten lukumäärästä ei ole olemassa tarkkaa tietoa. Elinkeinoelämän keskusliiton tutkimuksen mukaan Suomessa oli vuonna 2016 noin 4000 cleantech-alaan jollakin tavalla liittyvää pk-yritystä (EK, 2017). Suomen teknologiateollisuuden selvitys vuodelta 2019 puolestaan kertoo, että tekoälyä kehittäviä yrityksiä Suomessa oli tuolloin noin 250 (Teknologiateollisuus, 2019). Yritysvakoilun yleisyyttä ei kuitenkaan voi päätellä pelkästään sille alttiiden yritysten lukumäärän perusteella, sillä periaatteessa mikä tahansa yritys voi joutua kilpailijavakoilun kohteeksi.

Vielä vaikeampaa, kuin arvioida yritysvakoilun yleisyyttä, on arvioida niitä taloudellisia menetyksiä, joita siitä aiheutuu. Jotakin suuntaa antavaa arviota voidaan saada kansainvälisistä tutkimuksista, joissa arviot vahingoista ovat pahimmillaan 3 % bruttokansantuotteesta (Susi, haastattelu, 18.3.2020). Haasta-

tellut asiantuntijat arvioivat menetysten Suomessa olevan vähintään miljoonia tai kymmeniä miljoonia (Silen, haastattelu, 10.2.2020), tai jopa useita satoja miljoonia (Susi, haastattelu, 18.3.2020). Menetysten arviointi voi olla vaikeaa jopa itse yrityksille, sillä esimerkiksi yksittäisen tuotekehitystiedon päätyminen kilpailijalle on asia, jonka rahallista vaikutusta on hyvin vaikea mitata (Manninen, haastattelu, 13.3.2020). Myös Suojelupoliisin mukaan yrityksiin kohdistuva tiedustelutoiminta on Suomessa jatkuvaa, mutta Supoa haastattelussa edustanut Hakala ei halua avata tarkemmin tietoon tulleiden epäilyjen tai varmistuneiden tapausten lukumääriä. Joka tapauksessa suomalaisten yritysten innovaatiot ja tuotekehitystiedot ovat kansantaloudellemme arvokkaita, ja niiden päätymisestä ulkomaisille kilpailijoille aiheutuu tappioita paitsi kyseiselle yritykselle, myös koko kansantaloudelle. Lisäksi vahinkoa voi aiheutua mainehaitan muodossa, sekä esimerkiksi siitä, että yrityksen koko tietojärjestelmä saatetaan joutua uusimaan haittaohjelman vuoksi. (Hakala, haastattelu, 30.3.2020.)

Yritysvakoilun tilannekuvaan liittyen tutkimuksessa nousi esille myös maamme kriittinen infrastruktuuri, joka on hyvin pitkälle yksityisten yritysten hallussa. Tämän lisäksi on olemassa paljon viranomaisyhteistyötä tekeviä yrityksiä, ja tällaisiin yrityksiin kohdistuva vakoilu saattaa aiheuttaa uhkan myös kansalliselle turvallisuudelle (Hakala, haastattelu, 30.3.2020). F-Securessa työskentelevän Ruohosen mukaan kriittistä infrastruktuuria vastaan tehtävää kyberhyökkäystä saattaa edeltää kybervakoilu, tai vakoilu voi olla kyberhyökkäyksen todellinen tavoite. Suomessa CNI-alalla, Critical National Infrastructure, riskit kuitenkin tiedostetaan hyvin, minkä lisäksi Huoltovarmuuskeskus ja Kyberturvallisuuskeskus tukevat yrityksiä. Suomessa ei ole tapahtunut merkittäviä onnistuneita hyökkäyksiä kriittistä infrastruktuuria vastaan, mikä saattaa kuitenkin johtua siitä, että tarpeeksi vahvaa hyökkäystä ei ole vielä kohdistettu Suomeen. (Ruohonen, haastattelu, 31.1.2020.)

Lisäksi tulee huomata, että koronapandemia on laajentanut kriittisen infrastruktuurin käsitettä esimerkiksi elintarvikehuollossa perinteisestä alkutuotannosta ja varmuusvarastoinnista erilaisiin jakelu-, verkkokauppa- ja kotiinkuljetusratkaisuihin, mikä saattaa lisätä kybervakoiluun- ja hyökkäyksiin huonosti valmistautuneiden yritysten määrää (Cyberwatch, 2020). Vallitseva geopoliittinen ilmapiiri talouspakotteineen ja vakoiluepäilyineen, esimerkkinä Huawei, on hyvä signaali osoittamaan, kuinka syvällä valtarakenteissa yritysvakoilu on, ja kuinka ulkoisten uhkien narratiivit paljastavat myös esimerkiksi USA:n omaa ajattelua vakoilusta ja tiedustelutoiminnasta (Waltzer, haastattelu, 27.2.2020). Suojelupoliisin päällikkö Antti Pelttari onkin todennut, että Suomessa tulisi tarkasti miettiä, minkälaisen luottamuksen varaan uutta kriittistä infrastruktuuria tulisi rakentaa, ja että digitalisaatioon liittyvät kehityskulut tulee ottaa mukaan keskusteluun kansallisesta turvallisuudesta (Pelttari, 2020).

Tilannekuvaan liittyen haastatteluissa pyrittiin luomaan katsetta myös yritysvakoilun tulevaisuudennäkymiin. Mikään tutkimuksessa ilmi tullut seikka ei viittaa siihen, että yritysvakoilun riski olisi vähenemässä, päinvastoin. Suden mukaan yritysvakoilussa on usein kyse geopolitiikasta ja globaalista vaikuttamisesta, jossa taloudellisen tiedustelun keinoin pyritään vaikuttamaan kansain-

väliseen voimatasapainoon. Teknologioita halutaan saada omiin käsiin tai pidettyä omissa käsissä. Toisinaan halutaan estää jonkin teknologian kehittäminen tai pyritään ostamaan uhkaava kilpailija pois markkinoilta, toisinaan taas omaa teknologiaa pyritään levittämään markkinoille hintoja vääristämällä, missä siinäkin yritysvakoilu on merkittävässä roolissa. (Susi, haastattelu, 18.3.2020.) Suomessa yritysvakoilu on todennäköisesti luultua yleisempää, ja korkean teknologian maana olemme erityisen houkutteleva kohde (Manninen, haastattelu, 13.3.2020). Ruohosen mukaan tekoäly tarjoaa jo nyt työkaluja kyberturvallisuuteen liittyen, ja sitä on epäilty hyödynnetyn myös kyberhyökkäyksissä. Se ei vielä tänä päivänä ole merkittävä kyberpelikenttää horjuttava tekijä, mutta jo nykyisin joillakin hyökkäyksiä tekevillä ryhmillä saattaa olla resursseja sen tavoittelemiseen, mikä antaisi hyökkääjille etulyöntiaseman. Myös pilvipalveluihin ja datan toimitusketjuihin kohdistuva kybervakoilu saattaa todennäköisesti tulevaisuudessa lisääntyä. (Ruohonen, haastattelu, 31.1.2020.)

5.1 Yhteiskunnan tuki yrityksille

Mikäli yritys epäilee joutuneensa vakoilun kohteeksi, voi se Hakalan mukaan lähestyä Suojelupoliisia oma-aloitteisesti. Jos vakoilun päätellään olevan valtiotaustaista, hoitaa Supo asian selvittelyn, kun taas yritysten väliset ja työntekijöiden tekemät, tietopääomaan kohdistuvat rikokset tutkii paikallispoliisi tarvittaessa yhteistyössä Keskusrikospoliisin kanssa. Mikäli Supon tutkimissa tapauksissa ylittyisi esitutkintakynnys, vastaisi tutkinnasta KRP, sillä Supolla ei 1.6.2019 alkaen ole ollut esitutkintaoikeutta. Supo myös pyrkii lisäämään tietoisuutta aiheesta erilaista materiaalia jakamalla sekä tapaamalla suoraan yrityksiä. Vuonna 2020 Supo ja Elinkeinoelämän keskusliitto julkaisivat yhdessä sarjan yrityksille suunnattuja videomuotoisia tietoiskuja, joiden keskeinen viesti koski tietopääomaan liittyvää turvallisuutta. (Hakala, haastattelu, 30.3.2020.)

Vuonna 2019 voimaan tulleet tiedustelulait toivat uusia keinoja myös yritysvakoilun estämiseen liittyen. Jo lain valmisteluvaiheessa mukaan kokonaisuuteen otettiin EK:n silloisen johtavan turvallisuusasiantuntijan Mika Suden mukaan nimetty "pykälä Susi", mikä antaa tiedustelua tekevälle viranomaiselle mahdollisuuden luovuttaa tietoa suoraan vakoilun kohteena olevalle yritykselle (Susiluoto, 2020, s. 85). Tämä on erityisen tärkeää akuuteissa tilanteissa, joissa ratkaisut vakoilun estämiseksi tulee tehdä yhteistyössä yrityksen turvallisuustoimintojen kanssa. Muutoinkin lainsäädäntö on Suomessa yritysvakoilun osalta kohdallaan, ja vuonna 2018 voimaan tullut liikesalaisuuslaki on entisestään helpottanut salassapitoon liittyvien tapausten selvittelyä (Lahtinen, haastattelu, 29.1.2020).

Mannisen mukaan Supon lisäksi tukea varautumiseen tarjoavat Kyberturvallisuuskeskus sekä huoltovarmuuskriittisten yritysten osalta Huoltovarmuuskeskus, jopa erittäin yksityiskohtaisella tasolla. Myös Keskusrikospoliisi

tekee tietoverkkorikoksiin liittyvää ennaltaehkäisevää työtä, käyden mm. puhumassa erilaisissa tilaisuuksissa ja osallistuen yritysten harjoitustoiminnan kehittämiseen. KRP on julkaissut yhdessä Kyberturvallisuuskeskuksen kanssa myös oppaan Office365-tietomurroilta suojautumiseen liittyen. (Manninen, haastattelu, 13.3.2020). Kyberturvallisuuteen onkin viime vuosina kiinnitetty kiitettävästi huomiota, mutta yritysvakoilun tunnistamisen ja siltä suojautumisen suhteen olisi kokonaisuutena enemmänkin tehtävissä (Waltzer, haastattelu, 27.2.2020). Kuitenkin liika yhteiskunnan tuki voi myös kääntyä itseään vastaan, sillä verrattuna anglosaksisiin kulttuureihin ja Keski-Euroopan maihin, suomalaisissa yrityksissä luotetaan jo nyt liikaa viranomaisten kykyyn hallita riskejä yritysten itsensä puolesta (Ala-Varvi, haastattelu, 24.3.2020).

5.2 Varautumiseen liittyvät ongelmat

Ensimmäisenä varautumista haittaavana seikkana nousi haastatteluissa esille yritysten puutteellinen riskitietoisuus sekä jopa vääränlainen asennoituminen asiaan. Varsinkin pienissä ja keskisuurissa yrityksissä, joissa tosin riskikin on vähemmän todennäköinen, voi suhtautuminen olla jopa naivia (Ruohonen, haastattelu, 31.1.2020). Koska riskiä ei tunnisteta eikä haluta nähdä, siihen ei myöskään voida varautua riittävästi. Tässä mielessä Suomessa eletään ns. ”ruusun unta” yritysvakoilun suhteen, eikä edes ulkomaalaisten työntekijöiden taustoja selvitetä kunnolla (Waltzer, haastattelu, 27.2.2020). Kun omaa kriittistä tietopääomaa ja kilpailuetua tuovaa osaamista ei tunnisteta ja osata suojata, tulee yritysvakoilun kohteeksi joutuminen yrityksen tietoon usein vasta viiveellä ulkomaisen kilpailijan vallatessa markkinoita halvemmalla hinnalla myytävällä kopiotuotteella (Susi, haastattelu, 18.3.2020).

Niissäkin yrityksissä, joissa riskin olemassaolo tiedostetaan, on varautuminen Ala-Varvin mukaan yleensä heikkoa. Riskienhallintaprosessi on siten pysähtynyt riskin tunnistamiseen eikä arviointia ja käsittelysuunnitelmaa ole tehty. Tähän voi olla monia syitä: saatetaan luottaa liikaa viranomaisten kykyyn havaita yritysvakoilu, varautuminen koetaan liian kalliiksi, tai henkilöstöä ei ole tarpeeksi vaarallisten työyhdistelmien estämiseksi. Tällöin tieto ja käyttöoikeudet kasaantuvat tietyille henkilöille, joilla on usein järjestelmän admintunnukset käytössään. Rikoksesta epäilty löytyykin usein näiden henkilöiden joukosta. Tasapainoilu kaikkien näiden asioiden välillä voi myös johtaa siihen, että asia koetaan liian vaikeaksi ja sille ei tehdä mitään. Kuitenkin toteutuneissa tapauksissa esimerkiksi ICT-ympäristöön tehtävät, korjaavat toimenpiteet ovat olleet kustannuksiltaan vain 10–50 % itse tapauksen tutkintaan kuluneesta rahasummasta. (Ala-Varvi, haastattelu, 24.3.2020.)

Toisena ongelmana varautumisessa voidaan nähdä salailu, joka voi olla paitsi yrityskulttuuriin, myös koko yhteiskunnan liike-elämän kulttuuriin liit-

tyvä ilmiö. Vaikka yritysvakoilu on taloudelliselta merkitykseltään suuri sekä yksittäisille yrityksille että kansantaloudelle, liittyy aiheeseen vaikenemisen kulttuuri, johon kuuluu nolouden tunnetta ja mainehaittojen pelkoa (Susi, haastattelu, 18.3.2020). Mannisen mukaan monet yritykset vaikenevat vakoilun kohteeksi joutumisesta juuri mainehaittojen vuoksi, eikä rikosilmoitusta välttämättä tehdä siitä syystä, että poliisin esitutkinta tulee väistämättä julkiseksi tietyssä vaiheessa prosessia. Kuitenkin esimerkit ovat osoittaneet, että avoimuus olisi ollut peittelyä kannattavampi viestintästrategia, sillä mainehaitta kasvaa huomattavasti peittelyn paljastuessa. Tästä syystä KRP ohjeistaakin yrityksiä tekemään rikosilmoituksen matalla kynnyksellä. Pelkkä epäily rikoksesta riittää, ja KRP:n verkkorikostorjunta myös konsultoi tarvittaessa yrityksiä kybervakoiluun ja ylipäätään tietoverkkorikoksiin liittyvien epäilyjen osalta. (Manninen, haastattelu, 13.3.2020.)

Waltzerin mukaan Suomi on luottamukseen perustuva yhteiskunta, jossa tietoa jaetaan avoimesti, ja luottamuksen hengessä myös yrityksissä ihmisillä on pääsy tietoon, joka ei liity heidän työtehtäviinsä. Tämä voi kostautua myös osaajien siirtyessä organisaatiosta toiseen, mikä onkin edelleen yksinkertaisin ja nopein tapa saada haltuun kilpailevan yrityksen osaamista. Vaikka varsinaisia arkaluontoisia tietoja ei suoraan siirtyisi, niiden pohjalta syntynyt kokemus ja tietotaito siirtyvät. (Waltzer, haastattelu, 27.2.2020.) Suden mukaan samanlainen luottamus näkyy ”sinisilmäisyytenä” myös yrityskauppoihin ja investointeihin liittyvissä tilanteissa, joissa sopimusten sisällöt jäävät epäselviksi ja taloudelliset riippuvuussuhteet tunnistamatta, kun vastapuolesta uskotaan vain hyvää. Tällaisissa tapauksissa koko liiketoiminta voi hävitä maailmalle, minkä lisäksi voi vaarantua myös kansallinen turvallisuus. Pääomaköyhänä maana Suomessa ollaan alttiita uskomaan ulkomaisiin investointeihin, mistä syystä onkin sanottu, että ”Suomessa ei tarvitse vakoilla, Suomessa tarvitaan vain rahaa”. (Susi, haastattelu, 18.3.2020.)

Oma aihealueensa varautumisen ongelmakohdissa on teknisten järjestelmien mahdollisuudet ja toisaalta niiden ristiriita lainsäädännön kanssa. Suomessa yksityisyyden suoja on tiukasti säädeltyä, ja esimerkiksi toimitilojen kameravalvonta ei saa kohdistua työpisteisiin, mikäli tästä ei ole erikseen sovittu työntekijöiden kanssa. Samankaltainen suoja ulottuu myös tietoteknisiin järjestelmiin. Yrityksen tulisi kyetä havaitsemaan poikkeamat verkkoliikenteessä ja käyttäjähallinnassa, ja usein rikostutkinnassa ensimmäisenä havaittava ongelma on puutteellinen järjestelmälokitus (Manninen, haastattelu, 13.3.2020). Kuitenkin poliisin ohje ”kaiken lokittamisesta” ei ole yksityisyydensuojaa noudattavalle yritykselle aina mahdollista (Ala-Varvi, haastattelu, 24.3.2020). Esimerkiksi työntekijöiden internetliikennettä ei lain puitteissa saa valvoa siten, että tunnistetiedot voitaisiin palauttaa yksittäiseen työntekijään, vaikka direktio-oikeuden perusteella työnantaja voi ohjeistaa työvälineiden käyttöä (Lahtinen, haastattelu, 29.1.2020). Kuitenkin on olemassa tapauksia, joissa oikeus on antanut luvan laittomasti hankittujenkin todisteiden hyödyntämiseen (Silen, haastattelu, 10.2.2020). Toinen lokitietoihin liittyvä ongelma ovat yritysten puutteelliset sopimukset alihankkijoiden kanssa sekä alihankintasopimusten sisällön

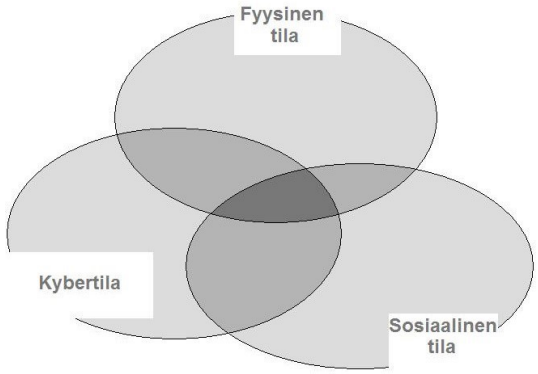
puutteellinen tuntemus. Toisinaan on tullut esille tapauksia, joissa yrityksellä ei ole ollut lainkaan oikeutta päästä oman järjestelmän lokitietoon, jolloin tapahtumien kulun selvittäminen jälkikäteen on ollut mahdotonta (Manninen, haastattelu, 13.3.2020).

Viimeisenä varautumiseen liittyvänä ongelmana voidaan nostaa esille yritysten turvallisuusyksiköiden, tietoturvaan liittyvien tahojen ja viranomaisten väliseen vuoropuheluun liittyvä problematiikka. Suden mukaan viranomaiset pyrkivät tekemään työtä yritysvakoilun estämiseksi ja ovat siinä onnistuneetkin, mutta toisaalta heiltä puuttuu usein oikea käsitys ja kokemus liiketoiminnasta ja sen luonteesta. Turvallisuusviranomainen saattaa katsoa asiaa vain omasta näkökulmastaan ymmärtämättä, että yrityksen päätavoite on kaiken suojaamisen sijaan taloudellisen lisäarvon tuottaminen. Viranomaiset tarvitsisivat enemmän ymmärrystä liiketoiminnasta ja riskienhallinnasta, minkä lisäksi tarvittaisiin lisää vuorovaikutusta julkisen ja yksityisen sektorin välillä. Esimerkiksi yritysvakoilun torjunnan osalta yhteistyörakenteet puuttuvat ja toiminta perustuu yksittäisten henkilöiden keskinäisiin suhteisiin. (Susi, haastattelu, 18.3.2020.)

Suden mukaan myös yritysten sisällä eri tahot, kuten riskienhallinta, yritysturvallisuus ja ICT, ovat erillisiä toimintoja, jotka liiketoiminnan näkökulmasta näyttäytyvät tukifunktioina. Näillä tahoilla on yleensä erilainen koulutustausta ja työhistoria, ja ne puhuvat siten ”eri kieltä”. Juuri yritysvakoilu on se riski, jonka osalta näiden kaikkien tulisi toimia yhdessä, mikä asettaa johtamisen keskeiseen rooliin. Kokonaisriskienhallinnan tulisi olla se käsite ja toiminto, joka nivoo eri tahot yhteen, ja mitä ajattelutapaa ymmärrettäisiin sekä liiketoiminnoissa että tukitoiminnoissa. Suomessa tämä ei yleisesti ottaen toteudu, vaan yrityksissä toimitaan perinteisessä siilomallissa. (Susi, haastattelu, 18.3.2020.)

6 YRITYSVAKOILUN MENETELMÄT JA VASTAMENETELMÄT

Yritysvakoilua toteutetaan monilla keinoilla ja sen onnistuneen estämisen edellytyksenä on näiden keinojen tunteminen. Yritysvakoilun pääkohteena on yrityksen hallussa oleva tietopääoma, jota tietoisesti ulkopuolisilta salassa pidettynä kutsutaan liikesalaisuudeksi. Tämä tietopääoma voi sijaita datana tietojärjestelmissä, dokumentteina tai objekteina fyysisessä tilassa, tai ajatuksina ja tietotaitona ihmisten kognitiivisessa tietoisuudessa. Siksi yritysvakoilun viitekehyksessä on mielekästä jakaa sen toteuttamistavat kolmessa tilassa tai ulottuvuudessa tapahtuviksi: kybertilassa, fyysisessä tilassa ja sosiaalisessa tilassa. Vakoilu voi tapahtua yhdessä näistä tiloista, tai siinä voi yhdistyä elementtejä kahden tai kaikkien kolmen tilan hyödyntämisestä. Tilat ja niiden lomittuminen on esitetty kuviossa 2. Kybervakoilu sellaisenaan on esimerkki yhden tilan hyödyntämisestä, mutta käytännössä useissa vakoilutapauksissa on kybertilan lisäksi hyödynnetty sosiaalista tilaa esimerkiksi käyttäjätunnuksia kalastelemalla, tai fyysistä tilaa esimerkiksi keylogger-laitteita asentamalla, kuten tapahtui Tampereen teknillisellä yliopistolla (Yle uutiset, 2008).



Kuvio 2: Yritysvakoilun kolme ulottuvuutta

Tutkielman puitteissa tehdyt haastattelut, lähdekirjallisuus ja uutislähteissä esiintyneet case-esimerkit ovat tuoneet ilmi suuren joukon erilaisia tapoja toteuttaa yritysvakoilua. Yhteenveto näistä tavoista on esitetty taulukossa 1. Yrityskaappauksiin ja kumppanuushankkeisiin liittyen voitaisiin puhua yritysvakoilun toteuttamisesta taloudellisin tai sopimusteknisin keinoin, mutta koska nämäkin toteuttamistavat liittyvät yritysten ja niiden henkilöstön väliseen vuorovaikutukseen, on ne lokeroitu tässä yhteydessä sosiaaliseen tilaan kuuluviksi.

Menetelmiä fyysisessä tilassa
Tunkeutuminen toimitiloihin, materiaalin varastaminen, tallentaminen tai tarkastelu.
Tunkeutuminen toimitiloihin, salakuunteluun/-katseluun käytettävien laitteiden asentaminen.
Tunkeutuminen toimitiloihin, vakoiluohjelmien asentaminen tietokoneisiin tai muihin laitteisiin.
Toimitiloissa käytävien keskustelujen seuraaminen rakennuksen ulkopuolelta.
Asiakirjojen, tietoteknisten laitteiden tai tallennusvälineiden varastaminen toimipaikan ulkopuolella.
Jätteiden ja muun hävitettävän materiaalin tutkiminen.
Käänteissuunnittelu sitä kautta saadun tiedon hyödyntämiseksi.
Menetelmiä sosiaalisessa tilassa
Avainhenkilöiden rekrytointi salassa pidettävän tiedon ja osaamisen siirtämiseksi omalle yritykselle.
Valetyöhaastattelut.
Esiintyminen asiakkaana ja tiedon kalastelu tarjouspyynnöillä.
Soluttautuminen yrityksen tai alihankkijan työntekijäksi.
Työntekijän värvääminen luovuttamaan salassa pidettävää tietoa työskentelyn jatkuessa.
Tiedon hankkiminen työntekijöiltä elisitaation keinoin vapaa-ajan sosiaalisissa tilanteissa.
Yritysostot, -kaappaukset ja kumppanuushankkeisiin liittyvä yritysvakoilu.
Menetelmiä kybertilassa
Yrityksen tietojärjestelmiin tunkeutuminen.
Haitta- ja vakoiluohjelmat.
Kalasteluviestit ja muu sosiaalinen hakkerointi.
MITM-hyökkäykset, ”sniffing”, valetukiasemat.
Puhelimen etäkuuntelu.
Langattomaan lähiverkkoon tunkeutuminen.
Keyloggereiden ja muiden laitteiden käyttäminen.
Kohdistetut epäsuorat hyökkäykset etätyöhön liittyen esim. IoT-laitteiden kautta.

Taulukko 1: Erilaisia yritysvakoilun menetelmiä

6.1 Menetelmät fyysisessä tilassa

Fyysisessä tilassa yrityksen tietopääoma muodostuu tulostetuista ja käsin kirjoitetuista asiakirjoista ja muista dokumenteista, erilaisista tietoteknisistä tallennusvälineistä ja tietoa sisältävistä laitteista sekä yrityksen liiketoimintaprosessin silmin havaittavista osista, kuten tietokoneiden näytöillä näkyvistä tiedoista, tuotantoprosessiin liittyvistä laitteista, osista ja komponenteista sekä valmiista tuotteista. Kaikkia näitä voidaan joko tarkastella, kuvata, kopioida tai varastaa. Lisäksi fyysisessä tilassa oleva ääni voi sisältää tietopääomaa esimerkiksi neuvottelutilassa käytävän keskustelun muodossa. Fyysisessä tilassa tapahtuva yritysvakoilu ei rajoitu yrityksen toimipaikkaan, vaan sitä voi tapahtua myös autossa, julkisessa liikennevälineessä, kotona tai työmatkalla ulkomailla. Monissa maissa tiedustelupalvelut salakuuntelevat ja -katselevat ulkomaalaisten liikematkustajien hotellihuoneita rutiininomaisesti (Wimmer, 2015, s. 80), ja lisäksi maiden viranomaiset saattavat yrittää kopioida kannettavien tietokoneiden kovalevyjä lentokentällä matkatavaratarkastuksen yhteydessä. Myös yrityksen jätteiden tutkiminen sekä tuotteiden ostaminen käänteissuunnittelua varten ovat fyysisessä tilassa tapahtuvaa yritysvakoilua.

Yksinkertaisin tapa toteuttaa yritysvakoilua on liikkua kohdeyrityksen toimitiloissa tehden havaintoja, tallentaen kuvamateriaalia, varastaen dokumentteja ja jättäen paikalle piilotettuja salakuuntelu- tai katselulaitteita. Yrityksen toimipaikkaan tunkeutuminen voi tapahtua tavanomaisena murtautumisena lukituksia rikkoen. Murtautumista huomaamattomampi tapa on tunkeutua toimitiloihin tiirikoita tai "kloonattuja" kulkukortteja käyttämällä murtojälkiä jättämättä. Mikäli tunkeutuminen tehdään lukituksia näkyvästi rikkoen, voi yritysvakoilun motiivi Wimmerin (2015) mukaan jäädä huomaamatta, jos tapahtumaa pidetään tavanomaisena omaisuusrikoksena. Yleinen tapa tunkeutua toimitiloihin on esiintyä huoltomiehenä, siivoojana tai tärkeän näköisenä johtajana, ja antaa työntekijöiden päästää itsensä sisälle ns. samalla ovenavauksella. Esimerkiksi tietoturvayhtiö Silverskinin Suomessa vuonna 2017 toteuttamissa penetraatiotestauksissa tämän menetelmän onnistumisprosentti oli 100, ja testaajan piti vain kävellä sisään kohdeyrityksiin työntekijäjoukon mukana (Kauppalehti, 2017). Mikäli tiloissa on aulavastaanotto, voidaan siinä työskentelevää vahtimestaria harhauttaa esimerkiksi soittamalla samaan aikaan aulaan puhelu, joka sitoo vahtimestarin huomion. On huomattava, että yritysvakoilu toimitiloissa liikkumalla voi tapahtua myös täysin luvallisesti työnhakijana tai muuna yrityksen vieraana. (Wimmer, 2015, s. 59–73.)

Salakuuntelun ja -katselun käyttäminen yritysvakoilun keinona on lisääntynyt viime vuosina, sillä teknologinen kehitys on tehnyt siihen käytettävistä laitteista yhä pienempiä, ja lisäksi ne ovat tulleet yleisesti saataville internetin verkkokauppojen myötä (Wimmer, 2015, s. 47). Yleisesti saatavissa olevat laitteet ovat esimerkiksi palovaroittimen, kynän, pöytäkellon tai jatkojohdon sisään

kätkettyjä. Ilman harhauttavaa suojakuorta olevat laitteet muodostuvat havaintoa keräävästä anturista, virtalähteestä, lähettimestä ja antenniosasta, ja ovat erittäin pienikokoisia. Ne voidaan kätkeä esimerkiksi pöydän alapintaan, kattopaneelin päälle tai verhon taitososan sisään. Laitteiden toimintaperiaatteet vaihtelevat siten, että ne voivat joko lähettää havaintoaan radiotaajuuksia käyttäen vastaanottajalle, tai ne voivat ainoastaan tallentaa sitä, jolloin vakoilua harjoittava taho joutuu noutamaan laitteen myöhemmin takaisin. Toimitiloihin piilotettujen, kuvaa, ääntä tai molempia tallentavien vakoilulaitteiden lisäksi toimitiloissa käytäviä keskusteluja voidaan seurata rakennuksen ulkopuolelta ikkunalasin värähtelyyn perustuvaa lasermikrofonia käyttäen (Secmeter, 2020). Uusimpana uhkana on viime vuosina noussut esiin droonien käyttäminen kuvaamaan yrityksen sisätiloja ikkunalasin takaa (Sisäministeriö, 21.2.2019). Lisäksi tavanomaisesta matkapuhelimesta tai tietokoneesta voi hakkeroinnin kautta tulla salakuuntelun ja -katselun väline käyttäjän tätä huomaamatta, tai henkilö voi käyttää puhelinta tietoisesti tallentamaan luottamuksellisia keskusteluja (Secmeter, 2020).

Fyysisessä tilassa mutta varsinaisten toimitilojen ulkopuolella tapahtuva vakoilumenetelmä on ”dumpster diving” eli jätteiden tutkiminen. Julkisuudessa esillä olleista yritysvakoilutapauksista Unileverin tapauksessa hyödynnettiin juuri sitä (Crane, 2005, s. 3). Prunckunin (2012) arvion mukaan jopa kaksi kolmasosaa yrityksen jätteistä sisältää tiedonhankintaa harjoittavaa tahoa kiinnostavaa materiaalia. Jätteistä etsitään raportteja, muistiinpanoja, muistioita, kirjeitä, valokuvia, salasanoja, ohjekirjoja, aikatauluja, kuitteja, ja käytännössä kaikkea yrityksen liiketoiminnasta kertovaa materiaalia, jota voidaan suorasti tai epäsuorasti hyödyntää. Jopa tavanomaisella suikalesilppurilla silputut asiakirjat pystytään palauttamaan luettaviksi, kuten tapahtui Iranissa vuonna 1979. Yrityksen heikosti suojatut jätekatokset tai toimitiloissa sijaitsevat turvaroskasäiliöt ovatkin yksi mahdollinen murtautumiskohde. Paperimuotoisen jätteen lisäksi käytöstä poistetut tietokoneet sekä erilaiset massamuistilaitteet ovat yritysvakoilua harjoittavalle taholle arvokasta materiaalia. Tiedostojen näennäinen poistaminen laitteelta ei useinkaan hävitä niitä lopullisesti, sillä laite saattaa olla muodostanut tiedostoista erilaisia vaikeasti löydettäviä varmuus- ja väliaikaistiedostoja. Tärkeää on huomata, että tietokoneiden lisäksi myös muut tietotekniset laitteet, kuten tulostimet, tallentavat käsittelemäänsä materiaalia erilaisille muistiasemille. (Prunckun, 2012, s. 144–147.)

Prunckunin (2012) mukaan käänteissuunnittelulla, reverse engineering, tarkoitetaan laitteen tai järjestelmän takaisinmallinnusta eli purkamista osiin ja sitä kautta rakenteen, ominaisuuksien ja toimintaperiaatteiden selvittämistä. Tällä tavalla pyritään selvittämään kilpailijan mahdollisia uusia innovaatioita, eikä menettely sinänsä ole laitonta. Mikäli tuotteessa käytettyä tekniikkaa aletaan kopioida tai käänteissuunnittelun kautta syntynyttä tietoa muutoin levittää, saatetaan syyllistyä immateriaalioikeuksien rikkomiseen. (Prunckun, 2012, s. 141.) Kansainvälisillä markkinoilla immateriaalioikeuksien rikkominen on kuitenkin varsin yleistä, eikä syyllisiä ole aina helppo saada vastuuseen. Yritysvakoilun suhteen erityisen alttiilla toimialoilla kilpaileva tuote saatetaan pyrkiä

saamaan haltuun laittomia keinoja käyttäen jo ennen sen markkinoille tuloa. Tämä voi tapahtua esimerkiksi tilanteessa, jossa tuotteiden mallikappaleita esitellään messuilla tai luovutetaan testikäyttöön alan lehdistölle. Prunckun (2012, s. 141) huomauttaa lisäksi, että käänteissuunnittelun tulisi olla osa yrityksen omaa offensiivista vastatiedustelua, sillä vain tutkimalla itse kilpailijoiden tuotteita pystytään selvittämään, onko omaa patenttioikeutta rikottu.

6.2 Menetelmät sosiaalisessa tilassa

Sosiaalisessa tilassa tapahtuvilla yritysvakoilun menetelmillä tarkoitetaan sellaisia keinoja, joilla tavoitellaan ihmisen mielessä olevaa tietoa. Tällainen tieto ei ole silmin havaittavassa tai korvin kuultavassa muodossa ennen kuin se saadaan ääneen lausutuksi esimerkiksi kysymisen kautta. Yritysvakoilu sosiaalisessa ulottuvuudessa edellyttää aina ihmisten välistä vuorovaikutusta, joka voi tapahtua joko kasvotusten tai erilaisten viestivälineiden, kuten puhelimen, sähköpostin tai sosiaalisen median kautta. Toisin kuin fyysisen tai kybertilan kohdalla, tieto ei ole yksipuolisesti havainnoitavissa, vaan se pyritään saamaan kohdehenkilöltä joko tämän tietäen tai tietämättä.

Mikäli tiedon luovuttaminen yrityksen ulkopuolelle tapahtuu tietoisesti, puhutaan ns. insider- eli sisäpiiriuhkasta (Jääskeläinen, 2018, s. 6). Insideruhkalla voidaan liikesalaisuuksiin kohdistuvan uhkan lisäksi tarkoittaa mitä tahansa työntekijän yritykselle aiheuttamaa vahingon uhkaa. Lisäksi liikesalaisuuksiin kohdistuva insider-uhka ei aina liity yritysvakoiluun vaan sen motiivina voi olla yrityssalaisuuden rikkominen ja väärinkäyttö. Yritysvakoilun menetelmiä ja niihin varautumista tutkittaessa insider-uhka onkin liian laaja käsite, ja se tulee purkaa osakokonaisuuksiin sen mukaan, miten tiedon luovuttaminen yrityksen ulkopuolelle tapahtuu: työntekijä voidaan rekrytoida tietotaitoineen kilpailijan palvelukseen, hänet voi olla alun perinkin solutettu yritykseen töihin yritysvakoilun tarkoituksessa, tai hänet voidaan värvätä luovuttamaan tietoa yrityksestä työskentelyn yhä jatkuessa siellä.

Kilpailijalta rekrytointi on edelleen yleisin tapa siirtää osaamista kilpailijalta omalle yritykselle (Waltzer, haastattelu, 27.2.2020). Mikäli yrityksellä on hallussaan sellaista erityisosaamista, jota ei suoraan voi kopioida teknisiä yksityiskohtia jäljittelemällä, on se myös ainoa keino saada haltuun kilpailijan tietotaitoa. Sinänsä rekrytointi ei ole laitonta, mutta muodostuu ongelmalliseksi tilanteissa, joissa rikotaan kilpailukielto- tai salassapitosopimuksia. Wimmer (2015, s. 85–97) huomauttaa, että työntekijän lisäksi insider-uhka voi muodostua kenestä tahansa yrityksen sisällä toimivasta: johtajasta, yhteistyökumppanista, siivoojasta, huoltomiehestä tai vartijasta. Hänen mukaansa se on yksi vaarallisimpia uhkia yrityksen liikesalaisuuksille, sillä siihen on kaikkein vaikeinta varautua, eivätkä yritykset useinkaan halua epäillä omaa henkilökuntaansa.

Tiedustelun maailmassa perinteinen, mutta yritysvakoiluun liittyen vähemmän esillä ollut henkilötiedustelumenetelmä, on henkilön värvääminen. Siinä kohdehenkilö suostuu – aluksi yleensä tiedostamattaan mutta lopulta tietoisesti – luovuttamaan hallussaan olevaa tai hankkimaansa tietoa kolmannelle osapuolelle työskentelyn yhä jatkuessa yrityksessä. Henkilön värväämisen motiivin luokitteluun voidaan käyttää ns. MICE-mallia, joka tulee sanoista money, ideology, compromise, ego (Wimmer, 2015, s.13–16). Mikäli yritysvakoilua harjoittava taho noudattaa henkilötiedustelussa yleisesti käytettyä värväysprosessia, on ensimmäinen vaihe sopivan henkilön löytäminen. Brown (2011) kirjoittaa aiheesta yritysvakoilua harjoittavan tahon näkökulmasta, ja hänen mukaansa tietojen luovuttajaksi ei tavallisesti valita voimakastahtoista, tasapainoista ja menestyvää henkilöä. Sen sijaan huomio kiinnitetään henkilön elämäntilanteesta tai persoonasta löytyviin heikkouksiin. Tällaisia voivat olla taloudelliset ongelmat, avioelämän ongelmat, hiljattain tapahtuneet elämänmullistukset, päihdeongelmat, mielenterveysongelmat, suhteet toiseen valtioon, antikapitalistisen ideologian kannattaminen, alipalkkaus tai turvattomuuden ja aliarvostettavuuden kokemukset. (Brown, 2011, s. 283.)

Liike-elämään liittyen raha sekä egon kautta syntyvä kostomotiivi uralla etenemiseen liittyvän pettymyksen vuoksi ovat lähdeaineiston perusteella yleisimpiä motiiveja värväykselle. Kuitenkin myös ideologia, esimerkiksi työntekijän kulttuuriseen taustaan liittyen, tai altistuminen kiristykselle jonkin kyseenalaisen toiminnan seurauksena ovat mahdollisia. Tällainen toiminta voi liittyä huumausaineiden käyttämiseen, muuhun laittomaan toimintaan tai sukupuolielämään, ja tilanne voi olla joko spontaanisti tapahtunut tai ennalta järjestetty. Brownin mukaan (2011, s. 40) ns. “honey and powder” -ansat ovat yleisiä tietyissä maissa, joissa yritysvakoilua harjoittavat tahot toimivat kiinteässä yhteistyössä järjestäytyneen rikollisuuden kanssa. Niin sanotut ”hunaja-ansat”, joissa hyödynnetään vastakkaisen sukupuolen viehätysvoimaa, ja joissa henkilö yritetään houkutella salaa kuvattavaan sukupuoliseen kanssakäymiseen, ovat tulleet aikoinaan suomalaisille liikemiehillekin tutuiksi idänkauppaan liittyvillä ulkomaanmatkoilla.

Brownin (2011) mukaan vakoiluoperaatiot, joissa henkilö värvätään luovuttamaan salassa pidettävää tietoa, voidaan jakaa ajallisesti lyhyt- ja pitkäaikaisiin. Pitkäaikaisessa operaatiossa tietojen luovuttaminen saattaa jatkua jopa vuosia. Yritysvakoilua harjoittavan kannalta tämä on kuitenkin haastavaa, sillä sopivan henkilön löytämisen lisäksi ko. henkilöä tulee opastaa huomaamattomaan kanssakäymiseen värvääjän kanssa, ja tiedon luotettavuutta tulee jatkuvasti arvioida useasta lähteestä siltä varalta, että värvätty on jäänyt kiinni tai yrittää rahastaa värvääjää keksityillä tiedoilla. Riski sekä värvätyn että värvääjän kiinnijäämisen on suuri, sillä henkilö saattaa kokea merkittävää psykologista stressiä väärin toimimisen ja salailun seurauksena. Lyhytaikaisissa operaatioissa tällaisia riskejä ei ole, ja värväys voi tapahtua jopa kertaluonteisena kohtaamisena. Lähes jokaisesta yrityksestä löytyy Brownin mukaan henkilöitä, joiden suhtautuminen omaan työnantajaan on syystä tai toisesta negatiivista. Suurehkon käteissumman tarjoaminen tällaiselle henkilölle käyttäjätunnusta ja salasa-

naa vastaan voi muodostua työntekijälle ylitsepääsemättömäksi kiusaukseksi, varsinkin jos kohtaaminen tapahtuu yllättäen, päihteiden siivittämänä, eikä henkilölle anneta aikaa harkita asiaa. (Brown, 2011, s. 26–38.)

Kun tietoa hankitaan sosiaalisessa kanssakäymisessä henkilön tietämättä tai tiedonhankinnan todellinen motiivi piilottaen, käytetään siitä termiä ”elisitaatio”. Laineen (2018) mukaan se voi tilanteesta riippuen olla joko keskustelua, haastattelua tai kuulustelua. Näiden kolmen eroavaisuus syntyy kohdehenkilön asemasta suhteessa elisitaation harjoittajaan: keskustelussa molempien asema on näennäisen tasa-arvoinen, haastattelussa tietoa hankkiva johtaa keskustelua ja kuulustelussa kohdehenkilö on jo selkeästi alisteisessa asemassa kuulustelijaan nähden. (Laine, 2018, s. 1–11.)

Esimerkkinä keskustelusta elisitaation muotona yritysvakoilun yhteydessä voidaan pitää yrityksen työntekijän seuraan hakeutumista vaikkapa messuilla, lounasravintolassa tai vapaa-ajan harrastuksen yhteydessä ja keskustelun ohjaamista tilanteeseen, jossa henkilö yritetään saada huomaamattaan paljastamaan liikesalaisuuden piiriin kuuluvaa tietoa (Tolvanen, 2015, s. 35–36). Haastattelua voidaan yritysvakoilun yhteydessä toteuttaa valetyöhaastattelun muodossa, jonka aikana työntekijää yritetään saada, yleensä oman pätevyytensä osoittamisen kautta, julkituomaan nykyisen työnantajansa tietopääomaa. Haastattelu voidaan toteuttaa fyysisesti, mutta nykyisin yhä useammin etäyhteyden kautta, jolloin haastattelijan todellisen identiteetin jäljittäminen on hyvin vaikeaa. Esimerkiksi Kiinan tiedetään lähestyneen ihmisiä LinkedIn-palvelussa erilaisten kulissiyritysten nimissä (BBC News, 2020). Kuulustelu elisitaation muotona voi äärimmillään tulla yritysvakoilun yhteydessä kyseeseen ulkomailla tapahtuvana viranomaiskuulusteluna. Kuitenkin liike-elämässä tavanomainen tarjouspyyntöprosessi voidaan osin tässä yhteydessä rinnastaa kuulusteluun, sillä käytännössä tarjouksen pyytäjällä on usein tilanteessa yliote myyvänä toimivaan osapuoleen nähden. Potentiaalisena asiakkaana esiintyminen onkin yksi tehokas tapa toteuttaa yritysvakoilua, sillä yritykset eivät kaupantekoa tavoitellessaan malta aina olla kertomatta jopa puhelimitse liikesalaisuuden piiriin kuuluvia tietoja asiakasta esittävän niitä kysyessä (Ala-Varvi, haastattelu 24.3.2020).

Hyvin erilaisin keinoin, mutta periaatteessa sosiaalisessa ympäristössä, tapahtuvaa yritysvakoilua ovat yritysostot ja -kaappaukset sekä joint venture- eli kumppanuushankkeiden kautta toteutettava tiedonhankinta. Tutkimushaastatteluissa tuli esille erityisesti suomalaisten yritysten luottavainen suhtautuminen tällaisiin taloudellisiin hankkeisiin. Monen suomalaisen yrityksen immateriaalioikeudet on kaapattu ulkomaille heti yritystoiminnan alkuvaiheessa ostamalla yritys houkuttelevalla mutta kansainvälisellä tasolla katsottuna vaatimattomalla tarjouksella (Waltzer, haastattelu 27.2.2020). Nopean rahan toivossa myyvien omistajien näkökulmasta asiassa ei sinänsä tapahdu mitään laitonta, mutta kansantalouden kannalta uusien innovaatioiden patenttioikeuksien päätyminen ulkomaille voi olla ongelmallista. Kumppanuushankkeissa yritysvakoilun riski on havaittu myös Suomessa, ja sopimussakkolausekkeista huolimatta sopimuk-

set suojaavat yritysvakoilulta huonosti (Silen, haastattelu 10.2.2020). Myös patentteihin liittyviä kanteita voidaan yrittää käyttää yritysvakoilussa. Menetelmä perustuu siihen, että kanteen saanut yritys saattaa pyrkiä todistelemaan sen perusteettomaksi esittämällä sellaisia teknillisiä tai menetelmällisiä yksityiskohtia, jotka muutoin kuuluisivat liikesalaisuuden piiriin.

6.3 Menetelmät kybertilassa

Kybertilassa sijaitsevalla tietopääomalla tarkoitetaan sellaista tietoa, johon on mahdollista päästä käsiksi tietoverkkojen välityksellä. Kybervakoilu on muuttanut tiedustelun toimintaympäristöä ja menetelmiä laajasti, sillä tietoverkkojen kautta on mahdollista hankkia tietoa aiempaa nopeammin ja helpommin, minkä lisäksi kyberympäristöä voidaan hyödyntää henkilö- ja avointen lähteiden tiedustelussa (Cyberwatch & EK, 2018, s. 8).

Kuten Koivula (2015) kirjoittaa Iovaniin ja Dinuun (2014) perustuen, tietoturvayhtiö McAfee arvioi jo vuonna 2014, että kybervakoilusta ja muusta kyberrikollisuudesta aiheutuu maailmanlaajuisesti biljoonan Yhdysvaltain dollarin suuruiset tappiot. Esimerkiksi vuonna 2013 löydetty NetTraveler-vakoiluohjelma oli toiminut vuodesta 2004 asti, tunkeutuen ainakin 350 organisaatioon 40 maassa, kohteinaan mm. nano-, laser-, tietoliikenne-, energia- ja lääketeollisuus (Lehto, 2020, s. 48). Kybertilasta on tullut maailmanlaajuisessa teollisuusvakoilussa eniten käytetty ulottuvuus, minkä lisäksi tekoälyn hyödyntäminen ja IoT-laitteiden yleistyminen tulevat lähitulevaisuudessa lisäämään kybervakoilua entisestään (NCSC, 2018, s. 4).

Ruohosen mukaan kybervakoilutapausten tunnistamista haittaa se, että yritysvakoilun motiivia on usein vaikea tunnistaa, ja se saatetaan tietoisestikin naamioida muunlaiseksi kyberhyökkäykseksi, kuten kiristyshaittaohjelmaksi. Hyökkäys voi alkaa julkisessa verkossa olevien palvelujen haavoittuvuuksien kautta. Palvelimilta hyökkääjä saa käyttäjätunnuksia, ja pääsee sitä kautta levittäytymään yrityksen sisäverkkoon, asentaen samalla takaovia työasemille. Tässä vaiheessa vakoilija yrittää pysyä näkymättömänä mahdollisimman pitkään, seuraten erilaisia sisäisiä kommunikaatiokanavia, kuten sähköpostia. Yrityksen sähköpostiin voidaan asentaa huomaamatta kopiointi- ja uudelleenohjaustoiminto, ja viestit saattavat huomaamatta vuotaa ulkopuolisille jopa vuosien ajan. Takaoven kautta vakoilija voi vierailla huomaamatta sisäverkossa varastamassa tiedostoja tiedostopalvelimilta, ja tarpeeksi suuret käyttövaltuudet saatuaan luoda itselleen uusia käyttäjäprofiileita. Tällöin se pystyy lähettämään sähköpostia yrityksen sisäisestä osoitteesta, huijaten työntekijöitä luovuttamaan edelleen lisää tietoa. Esimerkkitapauksessa hyökkääjä saavutti korkeimmat mahdolliset valtuudet ja sillä oli pääsy mihin tahansa sisäverkon osaan. Tällöin se aloitti näkyvän toiminnan yrityksen tuotteiden lähdekoodin etsimiseksi, valitsi haluamansa tiedostot, pakkasi ja suojasi ne salasanalla, ja lähetti sitten julkiseen

pilvipalveluun, josta ne oli helppo ladata edelleen hyökkääjän komentopalvelimeen. (Ruohonen, haastattelu 31.1.2020.)

Yrityksen tietojärjestelmiin voidaan tunkeutua tietoverkkojen kautta hyvin erilaisia hyökkäysvektoreita käyttäen. Yllä kuvatun lisäksi tunkeutuminen voi tapahtua langattoman lähiverkon tai IoT-laitteiden kautta. Viime vuosina kyberhyökkäyksiä on tapahtunut paljon mm. reitittimissä olevia heikkouksia hyödyntäen. Kohdistetuissa epäsuorissa hyökkäyksissä pääsy yrityksen verkkoon tapahtuu etätyössä, kodin huonosti suojattujen laitteiden ja perheenjäsenten varomattoman nettikäyttäytymisen kautta. Myös mobiililaitteiden vakoiluun on olemassa omat menetelmänsä, kuten valetukiasemat. Perinteinen analogisten puhelinkeskustelujen salakuuntelu on Suomessa jo historiaan jäänyt asia, mutta joissakin maissa sekin saattaa edelleen olla mahdollista.

Usein organisaatioihin kohdistuvat kyberhyökkäykset ovat monivaiheisia ja monien eri toimijoiden toteuttamia: yksi taho tekee alkuperäisen tunkeutumisen, myy pääsyoikeuden toiselle taholle, joka varastaa tietoja yrityksestä myydäkseen niitä eteenpäin ja luovuttaakseen lopuksi pääsyn kolmannelle osapuolelle, joka käynnistää verkossa kryptovaluuttojen louhimisen tai kiristyshaittaohjelman (Manninen, haastattelu 13.3.2020). Yritys saattaa ymmärtää joutuneensa yritysvakoilun kohteeksi vasta huomatessaan liikesalaisuutensa olevan myytävänä Darknetin markkinapaikoilla (Ruohonen, haastattelu 31.1.2020). Mannisen mukaan tällaista ammattimaista kyberrikollisuutta harjoittavat ryhmät hyödyntävät usein nollapäivähaavoittuvuuksia sekä korjauspäivityksen jälkeen verkosta pitkään löytyviä, päivittämättömiä palveluita. Toisinaan yritys saattaakin joutua kohteeksi pelkästään sen perusteella, että haavoittuvuus on edelleen hyödynnettävissä heidän verkossaan. Viime vuosina tällaisia haavoittuvuuksia on ollut mm. Citrix-, RDP-, Confluence- ja Pulse Secure VPN -palveluissa ja sovelluksissa. Office365-ympäristössä tietomurrot on taas yleisimmin tehty tunnusten kalastelua hyödyntäen. Tällaisen tietoverkkorikollisuuden kohteena voivat yritysten liikesalaisuuksien lisäksi olla henkilötiedot sekä luottokortti- ja laskutustiedot. (Manninen, haastattelu 13.3.2020.)

Elokuussa 2020 paljastunut, yritysvakoiluun erikoistunut APT-ryhmä ”RedCurl” oli aloittanut kyberhyökkäyksensä kalasteluviesteillä HR-henkilöstönä esiintyen. Näihin viesteihin oli liitetty linkki, joka johti toimivaan ja lailliseen pilvipalveluun, mutta joka käyttäjän huomaamatta latasi koneelle ns. troijalaisen haittaohjelman. Tämän tarkoitus oli avata hyökkääjälle pääsy yritysten sisäverkkoon yhä uusien haittaohjelmien asentamiseksi, joiden avulla voitiin mm. lukea ja kopioida tiedostoja ja sähköpostiviestejä. Hyökkääjä viipyi kohdeyritysten verkossa kahdesta kuuteen kuukauteen, etsien sopimusasiakirjoja, taloustietoja, työntekijöiden henkilötietoja ja tietoa yrityksen käynnistämistä juridisista toimenpiteistä. Kohteina oli yhtiöitä monilta eri aloilta, kuten vakuutus-, rakennus- ja finanssialalta, asianajoyhtiöitä ja matkatoimistoja. (Infosecurity, 14.8.2020.) Rikollisten tahojen lisäksi yritysvakoiluun tähtääviä APT-hyökkäyksiä tekevät myös valtiolliset tiedusteluorganisaatiot, ja yrityksillä on todennetusti vaikeuksia havaita tällaisia suunnitelmallisia ja kehittyneitä hyökkäyksiä (Lehto ym., 2018, s. 41).

6.4 Yhdistetyt menetelmät

Tietoturvariskeistä puhuttaessa nousee usein esiin ns. social engineering eli sosiaalinen hakkerointi, jossa tietoteknisiin hyökkäysvektoreihin yhdistetään käyttäjän manipulointia erehdyttämällä tätä antamaan tietoa tai tekemään haitallisia toimenpiteitä. Esimerkiksi moniin onnistuneisiin APT-hyökkäyksiin näyttää tapauksista kertovien uutistietojen mukaan liittyneen käyttäjän manipulointia klikkaamaan haitallista linkkiä sähköpostissa tai antamaan käyttäjätunnuksensa ja salasanansa puhelimessa käytöntukena esiintyneelle henkilölle. Sosiaalinen hakkerointi yritysvakoilussa on esimerkki kyber- ja sosiaalisen tilan yhtäaikaisesta hyödyntämisestä, ja kybervakoilun menetelmiä tutkittaessa pitää huomata, että vakoilutapauksissa käytetään yleensä useita erilaisia hyökkäysvektoreita sosiaalinen hakkerointi mukaan lukien. Brown (2011) korostaa, että huippuluokan tekninen tietoturva voidaan ohittaa helposti yksinkertaisesti ostamalla kohdeyrityksen työntekijältä pääsyoikeus järjestelmään. Myös fyysistä tilaa voidaan hyödyntää kybervakoilussa, ja tietokoneisiin muistitikulta asennettavia vakoiluohjelmia saattaa olla vaikea havaita tavanomaisilla virustorjuntaohjelmistoilla.

Sosiaalisen ja fyysisen tilan yhdistämistä yritysvakoilun menetelmissä tapahtuu esimerkiksi silloin, kun yrityksen työntekijä houkutellaan varastamaan tai kopioimaan hänelle kuulumattomia asiakirjoja tai asentamaan työtiloihin salakuunteluun- tai katseluun käytettäviä laitteita. Brownin (2011, 42–43) mukaan erityisesti kohdeyrityksen käyttämissä alihankintayrityksissä, kuten tavarantoimittajissa, kiinteistönhuollossa ja jätehuoltoyhtiöissä, työskentelee määräaikaisissa ja alipalkatuissa työsuhteissa olevia ihmisiä, jotka ovat valmiita tällaisiin toimiin hyvinkin pientä korvausta vastaan. Mikäli tällainen henkilö houkutellaan asentamaan fyysisesti päätelaitteissa käytettäviä vakoiluohjelmistoja, voidaan katsoa yritysvakoilussa hyödynnettävän kaikkia kolmea, fyysistä, sosiaalista ja kybertilaa. Samoin on tilanteessa, jossa sosiaalista hakkerointia sisältävä kybervakoiluhyökkäys toteutetaan langattoman lähiverkon kautta kohdeyrityksen välittömässä läheisyydessä oleskellen.

6.5 Yritysvakoiluun varautuminen

Yritysvakoiluun varautuminen rakentuu yrityksen tietopääoman ja liikesalaisuuksien tunnistamisen varaan. Mikäli yrityksessä ei tunnisteta salassapitointressin alaista tietoa tai tiedetä missä tämä tieto sijaitsee, on kontrollitoimien

pystyttäminenkin tällöin hakuammuntaa. Kun liikesalaisuudet on tunnistettu, tulee yrityksen arvioida niihin kohdistuvat riskit, yritysvakoilun riski mukaan lukien. Sekä Wimmerin (2015) että Prunckunin (2012) mukaan tämä prosessi alkaa uhka-arviolla, jossa yrityksen tulee arvioida, syntyykö yritysvakoilun uhka esimerkiksi kilpailijoiden, rikollisten vai valtiollisten tiedustelupalveluiden taholta. Nykyisen kaltaisessa kompleksisessa toimintaympäristössä tämä saattaa kuitenkin olla vaikeaa, sillä tiedustelupalvelut saattavat tukea omien valtioidensa yrityksiä hyvin moninaisilla aloilla. Riskinä on tällöin uhkan aliarviointi, kun oletetaan, että oma ala ei ole tarpeeksi merkittävä, jotta siihen kohdistuisi valtiollisten tiedustelupalveluiden kiinnostusta. Lisäksi kybervakoilun yleistyminen ja hakkeriryhmien verkottuminen tiedustelutoimijoihin on vaikeuttanut uhkan arvioimista näin suoraviivaisilla tavoilla.

Uhka-arvion jälkeen yrityksessä tulee tehdä varsinainen riskianalyysi, jossa punnitaan sekä riskin toteutumisen todennäköisyyttä että niitä menetyksiä, joita riskin toteutumisesta aiheutuu. Kun riski on analysoitu, päätetään seuraavaksi riskienhallintakeinoista, eli niistä kontrollitoimista, joilla sekä toteutumisen todennäköisyyttä että menetysten suuruutta pyritään vähentämään. (Leppänen, 2006, s. 29–31, 167). Koko tämä prosessi tulee olla kirjattuna eksplisiittisesti yrityksen riskienhallinta- ja turvallisuussuunnitelmiin, minkä lisäksi kontrollitoimien toteuttaminen pitää aloittaa johdonmukaisesti ja määrätietoisesti. Yritysvakoiluun varautuminen ei saa jäädä ainoastaan yrityksen riskienhallinnasta tai turvallisuudesta vastaavien toimijoiden asiaksi, vaan koko yritysjohdon tulee sitoutua varautumisprosessiin allokoimalla sitä varten tarvittavia resursseja sekä luomalla oikeanlaista turvallisuuskulttuuria myös omalla esimerkillään (Wimmer, 2015).

Sijaitsee yrityksen kriittinen tieto sitten tietojärjestelmissä tai fyysisissä dokumenteissa, tulee se turvaluokitella. Sandbergin mukaan (2015), joka nojautuu Tankardiin (2011), tämä prosessi aloitetaan kaikkien tietoaineistojen läpikäymisellä, tunnistamalla tärkeät tiedot, ja päättämällä minkälaista tietoturvapolitiikkaa niiden suhteen noudatetaan. Hänen mukaansa prosessissa tulee huomioida, onko tieto sensitiivistä vai ei, mikä on sen taloudellinen arvo, ja mitkä olisivat sen vaarantumisen seuraukset. Leppänen (2006, s. 262–287) painottaa tiedon käsittelyyn liittyvien ohjeiden tärkeyttä kaikissa eri turvaluokissa. Toisin sanoen tietoa käsittelevän tulee tietää, miten kyseisen turvaluokituksen tietoa saa tulostaa, siirtää, säilyttää, ja miten se tulee hävittää. Kaikella tiedolla tulee organisaation sisällä olla omistaja, joka määrittelee kyseisen tiedon turvaluokituksen, valvoo sen noudattamista ja tarvittaessa puuttuu virheellisiin menetelmiin.

6.5.1 Vastamenetelmät fyysisessä tilassa

Tekninen murtosuojaus ja sitä täydentävät hälytys-, kulunvalvonta- ja kameravalvontajärjestelmät muodostavat pohjan toimitiloihin kohdistuvien tavan-

omaisten rikosten lisäksi myös fyysisessä tilassa tapahtuvalle yritysvakoilun torjunnalle. Insider-uhkia silmällä pitäen toimitilojen kulunvalvontajärjestelmät tulisi suunnitella turvallisuusvyöhykkeittäin siten, että kullakin työntekijällä on kulkuoikeus vain niihin työtiloihin, joita hän säännöllisesti käyttää. Lisäksi tiettyihin teknisiin tiloihin, kuten palvelin- ja teletiloihin tulisi olla pääsyoikeus vain niitä käyttävällä huoltohenkilökunnalla (Leppänen, 2006, s. 355). Tavallisesti kulkuoikeudet toimivat kuvallisen henkilökortin kautta, johon on liitetty tunniste etälukijaa varten. Biometrisen tunnisteen, kuten sormenjälki-, verkkokalvo-, ääni- tai kasvotunnisteen lisääminen tähän kokonaisuuteen parantaa kulunvalvonnan tehokkuutta, sillä kulkukorttiin perustuva järjestelmä ei tosiasiallisesti tunnista käyttäjää vaan ainoastaan kortin haltijan (Leppänen, 2006, s. 367–368). Tallentamiseen perustuva toimitilojen kameravalvonta saattaa olla monille yrityksille riittävä ratkaisu tavanomaisen rikollisuuden suhteen, mutta ei yritysvakoilun osalta ole paras mahdollinen. Jotta turvallisuusvyöhykkeillä asiattomasti liikkuvat henkilöt voitaisiin havaita etupainotteisesti, tulisi turvallisuushenkilöstön havainnoida videokuvaa reaaliajassa (Wimmer, 2015, s. 180).

Yrityksen tiloissa liikkuvat vierailijat muodostavat yritysvakoilun näkökulmasta erityisen uhkan. Vierailijoita ovat mm. liikekumppanit, työnhakijat, erilaiset tutustumiskäynneillä olevat ryhmät sekä epäsäännöllisesti vieraileva huoltohenkilöstö. Yrityksellä itsellään ei ole käytännössä mahdollisuutta selvittää kaikkien näiden henkilöiden taustoja, eivätkä kaikki heistä kuulu työsopimuksiin sisältyvien vaitiolosäädösten piiriin. Tästä syystä vierailijoilla tulisi aina tiloissa liikkuessaan olla mukana saattaja, ja heidän tulisi allekirjoittaa ennen vierailua erillinen salassapitosopimus. Lisäksi olisi hyvä, mikäli vierailijoita opastettaisiin sulkemaan matkapuhelimensa tai pitämään ne suljetussa laukussa koko vierailun ajan. Kaikki kuvaaminen toimitiloissa tulisi olla kiellettyä.

Leppäsen (2006) mukaan vierailijoiksi hyväksymisen periaatteet tulisi olla kirjattu erikseen ylös, minkä lisäksi kaikki vierailijat tulisi henkilöllisyystodistuksen perusteella kirjata vierailijarekisteriin. Koska tällaisesta rekisteristä voi itsessään muodostua yritysvakoilun kohde, tulisi sen suojaamiseen kiinnittää erityistä huomiota. Tilapäisiä kulkuoikeuksia, joiden avulla vierailija pystyy itsenäisesti liikkumaan toimitiloissa, tulisi myöntää vain poikkeustapauksissa. Lisäksi vierailijoiden tulisi aina käyttää kuvallista vierailijakorttia, samoin kuin henkilöstölläkin tulisi olla kuvallinen henkilökortti aina näkyvillä. Tätä kautta kaikki ilman kyseisiä kortteja tiloissa liikkuvat henkilöt olisi helppo tunnistaa, ja työntekijöiden tulisikin kiinnittää erityistä huomiota siihen, että tällaisia henkilöitä ei päästetä liikkumaan mistään lukitusta ovesta ”samalla ovenavauksella”. (Leppänen, 2006, s. 204–206.)

Yrityksessä käytössä oleva clean desk-periaate estää ulkopuolisia näkemästä pöydällä olevien asiakirjojen sisältöä, mutta myös vaikeuttaa teknisten salakuunteluun- ja katseluun käytettävien laitteiden asentamista toimitiloihin. Tämä tulisi huomioida myös yrityksen sisustussäännöissä, joissa kaikki ylimääräiset tekniset laitteet, koriste-esineet, kasvit ja tekstiilit tulisi olla kielletty (Wimmer, 2015, s. 171). ”TSCM-lakaisu” tai ”nuohous” eli teknisten valvontalaitteiden etsintä tulisi suorittaa säännöllisesti koko yrityksen tiloissa, ja lisäksi

tehostetusti erityisen tärkeissä tuotekehitystiloissa, neuvotteluhuoneissa ja yritysjohdon huoneissa. TSCM, technical surveillance countermeasures, tulisi aina olla siihen pätevöityneen tahon suorittama ja tunnettujen valmistajien välineitä käyttäen tehty. Internetin verkkokaupoissa myytävillä etsintälaitteilla on mahdollista löytää kaupallisesti myytäviä salakuuntelulaitteita, mutta tiedustelupalveluiden käyttämät laitteet saattavat lähettää tallentamansa tiedot vaihtelevia taajuuksia pitkin tai vain tiettynä hetkenä vuorokaudesta, jolloin laite ei ole havaittavissa muina aikoina radiosignaalien etsimiseen perustuvalla etsintälaitteella. TSCM-palvelua tarjoavat ammattilaiset käyttävätkin etsinnässä aina käsin ja silmin tehtävän tarkastelun lisäksi sekä radiolähetyksiä etsivää laitetta, spektrianalysaattoria että NLJD-laitetta, joka havaitsee rakenteiden sisälle kätketyt puolijohteet, vaikka mikropiiri ei olisi aktiivisessa tilassa. (Wimmer, 2015, s. 149–156). Koska nykyisin myös tavanomaisesta matkapuhelimesta voidaan hakkeroida vakoilulaite, tulisi tärkeimmät neuvottelutilat pitää kokonaan matkapuhelinvapaina vyöhykkeinä. Lisäksi neuvottelutilat tulisi suojata rakennuksen ulkopuolelta tehtävältä lasermikrofonikuuntelulta kohinageneraattoreilla tai erityisillä verho- ja ikkunaratkaisuilla (Secmeter, 2020).

6.5.2 Vastamenetelmät sosiaalisessa tilassa

On paradoksaalista, että yrityksen omat työntekijät ovat samaan aikaan sekä yrityksen suurin voimavara, että merkittävin uhka luottamukselliselle tietopääomalle. Esimerkiksi Verizonin tekemässä tutkimuksessa 77 prosenttia käyttöoikeuksien väärinkäytöksistä oli yrityksen sisäpiiriläisten tekemiä, ja niistä 25 prosentissa motiivina oli yritysvakoilu (Lehto ym., 2017, s. 13). Sosiaalista ulottuvuutta hyödyntävään yritysvakoiluun on myös kaikkein vaikeinta varautua etukäteen suojauksia rakentamalla. Tästä huolimatta yritysvakoilun riski tulisi huomioida työntekijöiden työsuhteen elinkaaren kaikissa vaiheissa jo rekrytoinnista alkaen. Mahdollisimman hyvät taustatarkistukset, mukaan lukien luottotiedot, rikoshistoria ja huumausainetestaus, edesauttavat valitsemaan yritykselle työntekijöitä, joilla on mahdollisimman vähän alttiutta joutua ulkopuolisen toimijan värväämäksi (Bressler, 2015, s. 29). Suomessa Suojelupoliisin turvallisuusselvitysmenettely on yksi varteenotettava tapa tarkastaa työnhakijan taustoja. Kaikissa taustatarkistuksissa tulee huomioida voimassa oleva lainsäädäntö yksityisyyden suojasta työelämässä. Esimerkiksi tiedon hankkimisen "googlettamalla" ilman työnhakijan lupaa voidaan katsoa rikkovan tätä lakia.

Rehellisyyttä ja lojaaliutta korostavat luonteenpiirteet tulisi huomioida myös soveltuvuustestauksissa. Työsuhteen alkaessa työntekijän tulisi allekirjoittaa erillinen salassapito- ja/tai kilpailukieltosopimus. Vaikka työsuhteen aikaisten tietojen salassapito sisältyy sinänsä työsopimukseen, voidaan erillisellä salassapitosopimuksella alleviivata tätä näkökulmaa työntekijöille. Työsuhteen alkuun sijoittuvaan työtehtävään perehdyttämiseen tulisi myös sisällyttää ohjeet tietopääoman salassa pitämiseen liittyen. Luonnollisesti työntekijällä tu-

lisi tietojärjestelmissä olla käyttövaltuudet vain sellaisiin tietoihin, joita hän työtehtävässään tarvitsee. Näillä toimenpiteillä paitsi ohjataan työntekijää kohti oikeita toimintatapoja, myös pienennetään insider-uhkaa osoittamalla, että yritys pyrkii aktiivisesti suojaamaan liikesalaisuutensa myös omien työntekijöiden muodostamalta uhkalta. Lisäksi työntekijöitä tulisi rohkaista antamaan mahdolliset värväysyritykset ja muita työntekijöitä koskevat epäilyttävät havainnot ilmi jopa rahallisia palkkioita lupaamalla (Brown, 2011, s. 284).

Työntekijän värväämistä luovuttamaan tietoja tai tietojen urkkimista elisitaation keinoin vapaa-ajalla työpaikan ulkopuolella on käytännössä mahdotonta ehkäistä muutoin, kuin kouluttamalla henkilöstölle yritysvakoiluun liittyvää riskitietoisuutta. Sandberg (2015) esittää Hadnagyyn (2010) nojautuen, että yrityksen turvallisuustietoisuusohjelman tulisi olla lähestymistavaltaan holistinen, joustava ja huomioida sekä tiedonhankinnassa käytettävät keinot että niiden kohteena oleva tieto. Riskialttiissa yrityksissä koko henkilökunnan tulisi olla tietoisia yleisimmistä yritysvakoilun menetelmistä, joita heihin voidaan yrityksen kontrollitoimien ulkopuolella kohdistaa, kuten värväysyrityksistä ja valetyöhaastattelujen mahdollisuudesta. Samoin työntekijöillä tulisi olla ymmärrys päivittäisten työtehtävien tietoturvakäytäntöjen syistä ja niiden laiminlyömisen mahdollisista seurauksista, clean desk -periaatteesta alkaen asiakirjojen oikeaoppiseen hävittämiseen asti. Linjaorganisaation esimiesten tulisi valvoa sääntöjen noudattamista johdonmukaisesti päivittäin, ja huomauttaa laiminlyönneistä työntekijöille. Vastaavasti turvallisuuspäällikön tai muun turvallisuudesta vastaavan tahon tulisi havainnoida sääntöjen noudattamista ainakin pistokoeluontoisesti.

Mikäli työntekijä on joko tietoisesti tai tahtomattaan alkanut luovuttaa tietoja yrityksen ulkopuolelle, voi tämä näkyä henkilön käyttäytymisessä ja toiminnassa. Brownin mukaan (2011, s. 281) tällaisia merkkejä ovat mm. selvä varallisuuden lisääntyminen, salaileva käytös, työn tekeminen poikkeuksellisina aikoina, mielialojen vaihtelu, hermostuneisuus sekä poikkeuksellinen kiinnostuneisuus oman toimenkuvan ulkopuolisia asioita ja työntekijöitä kohtaan. Sekä turvallisuustoimijoiden että lähiesimiesten tulisi osata kiinnittää huomiota tällaisiin muutoksiin työntekijöissä. Tietopääomaan kohdistuvien rikosten lisäksi samat muutokset voivat merkitä myös omaisuus- tai petosrikosten suunnittelua tai toteuttamista. Sinänsä tällaiset muutokset eivät kuitenkaan välttämättä kerro rikollisesta toiminnasta, vaan niiden taustalla voi olla monenlaisia syitä.

Työsuhteen päättyminen muodostaa yritykselle erityisen riskin yritysvakoilun ja muiden tietopääomaan kohdistuvien rikkomusten näkökulmasta. Työntekijän kostomotiivi saattaa olla korkea, mikäli irtisanominen ei ole tapahtunut hänen aloitteestaan, tai irtisanoutumisen taustalla voi olla siirtyminen kilpailijan palvelukseen. Molemmissa tapauksissa työntekijällä saattaa herätä kiusaus viedä mukanaan hänelle kuulumatonta tietoa, tai pahimmillaan rekrytointi kilpailijan palvelukseen on tapahtunut juuri tätä edellyttäen. Tästä syystä työntekijän työvelvoite tulisi päättää heti irtisanoutumisen tultua ilmi, ja työntekijä tulisi saattaa valvotusti ulos toimitiloista. Irtisanomiskeskustelun yhteydessä työntekijää tulisi muistuttaa salassapitovelvollisuudesta ja sen rikkomiseen liit-

tyvistä seuraamuksista. Kaikki käyttö- ja kulkuoikeudet tulisi lakkauttaa mahdollisimman pian. Koska työntekijä on voinut toteuttaa yritysvakoilua jo ennen irtisanoutumisesta kertomista, tulisi lokitietoja hyödyntäen selvittää, mitä tiedostoja hän on viimeisten viikkojen aikana katsellut, tallentanut ja tulostanut. Mikäli tilanteessa on syytä epäillä kilpailukieltosopimuksen rikkomista, tulisi asia varmistaa tarvittaessa yksityisetsivän palveluita hyödyntäen.

6.5.3 Vastamenetelmät kybertilassa

Varautuminen yritysvakoiluun kybertilassa noudattaa hyvin pitkälle samoja periaatteita, kuin varautuminen muihinkin kyberuhkiin. Tietoverkkojen kautta tapahtuvan tunkeutumisen estämisen perustan muodostavat asianmukaiset palomuuri- ja virustorjuntaohjelmistot sekä käyttövaltuuksien- ja pääsynhallinta salasanakontrolleineen. Salasanojen tulee pakotetusti olla vahvoja ja niiden vaihtaminen säännöllisin väliajoin varmistettua. Järjestelmälokituksen tulee mahdollistaa tapahtumien tarkastelu jälkikäteen käyttäjäkohtaisella tasolla. Verkkosivujen suojausprotokollien tulee olla ajan tasalla, järjestelmäpäivitysten automaattisia ja sähköpostiliikenteen suojattua. Teknisten kontrollitoimien ohella yhtä tärkeää on kuitenkin myös käyttäjien turvallisuustietoisuudesta huolehtiminen, mikä on käytännössä ainoa tapa suojautua kalasteluviesteiltä ja sosiaaliselta hakkeroinnilta. Uusista uhkista ja kalastelumenetelmistä tulisi tiedottaa päivittäin, minkä lisäksi laajempia turvallisuustietoisuuskoulutuksia tulisi järjestää säännöllisin väliajoin.

Mikäli yrityksellä on syytä varautua kybervakoiluun näitä perustason toimenpiteitä laajemmin, on Ruohosen mukaan suositeltavaa ottaa käyttöön EDR- ja SIEM-tyyppisiä verkonvalvontatyökaluja. Niiden avulla voidaan parantaa havaitsemiskyvykkyyttä tilanteissa, joissa hyökkääjä on jo saanut muodostettua takaoven yrityksen sisäverkkoon. Tutkimus- ja tuotekehitystyötä olisi hyvä tehdä näihin toimintoihin erikseen varatuilla työasemilla, joita ei käytettäisi mihinkään muuhun, ja jotka toimisivat eri käyttäjätunnuksilla ja eri aliverkossa kuin muut työasemat. Tiedostojen tulisi tallentua automaattisesti luotettavaan pilvipalveluun VPN-suojatulla yhteydellä ilman lokaalia kopiota. Vaihtoehtoisesti tutkimustyötä voidaan tehdä myös täysin tietoverkoista irrotetuilla työasemilla, jolloin varmuuskopiointikin pitää tehdä manuaalisesti. Tällöin riskiksi muodostuu laitteiden fyysinen varastaminen tai tietojen kopiointi massamuistilaitteille. Työasemien kovalevyt tulisikin olla kryptattu fyysisen varkauden varalta. (Ruohonen, haastattelu 31.1. ja 12.2.2020.)

Mikäli yritysvakoilun riski on yrityksessä suuri, tulisi suojauksien ja poikkeavan toiminnan havainnointikykyjen lisäksi kiinnittää huomiota käytössä olevien järjestelmien "koventamiseen". Tällä tarkoitetaan kykyä ICT-infran kokonaishallintaan, aitoa "päästä-päähän" salausta sekä Linuxin kaltaisia avoimen lähdekoodin ohjelmistoja. Käytetyt laitteet eivät siten voi olla "kaupan hyllystä" ostettuja, sillä niiden sisältöä komponenttitasolla ei täysin tunneta.

Myöskään salaukset eivät voi olla kolmannen osapuolen tuottamia, eikä näkyvyys lähdekoodiin voi olla puutteellista, kuten esimerkiksi Windows-pohjaisissa ohjelmistoissa. (Lehto, 2020). Ainoastaan tällä "kolmannen tason" suojautumisella organisaatio pystyy suojautumaan laitteistoihin valmistusvaiheessa syntyneiltä riskeiltä sekä toimitusketjuhyökkäysten tapaisilta hyökkäysvektoreilta.

Kyberympäristössä insider-uhkalta voi pyrkiä suojautumaan myös vaarallisia työyhdistelmiä minimoimalla, kierrättämällä työtehtäviä ja ketjuttamalla työvaiheita useille työntekijöille (Sandberg, 2015, s. 67). Tällä pyritään siihen, että työntekijä ei yksin ja muiden huomaamatta pysty käsittelemään ja kopioimaan kriittisiä tietoja, vaan toiset työntekijät samassa ketjussa huomaavat epäilyttävän toiminnan. Käytännössä tämä on vaikeaa, mutta ainakin se pakottaa laittomaan toimintaan pyrkivän huomioimaan asian ja nostaa kynnystä toimia laittomasti. Työtehtävien kierrättämisellä pyritään siihen, että samaa työtä seuraavaksi tekemään tuleva huomaa edellisen mahdolliset väärinkäytökset. Kuitenkin tehtävien kierrättämisessä on myös riskinsä, sillä se saattaa tarjota tietoa laittomasti keräävälle pääsyn entistä suurempiin tietomääriin.

Useimmiten yritys ulkoistaa tietoturvapalvelunsa asiaan erikoistuneelle palveluntarjoajalle, mikä saattaa itsessään muodostua riskiksi, sikäli kun palveluntarjoajan kykyyn suojata yritystä kaikilta kyberuhkilta luotetaan liikaa. Tietoturvayhtiöt harjoittavat itsekin liiketoimintaa, ja tuottavat asiakkaalle siten vain ja ainoastaan niitä palveluita, joista sopimusta tehdessä on sovittu. Lisäksi sopimusten hallinta kaikkien tietojärjestelmiin liittyvien palveluntarjoajien kanssa tulee tehdä yritysvakoilun riski huomioiden, jotta esimerkiksi lokitietoihin pääsy on tarvittaessa nopeaa ja vaivatonta. Mahdollisissa yritysvakoiluepäilyissä tulee olla käytettävissä myös tietotekniseen forensiikkaan erikoistunut taho, joka pystyy selvittämään, mitä laitteilla on milloinkin tehty ja kenen toimesta. Tällaisissa tilanteissa näytön hankkiminen mahdollisimman pitkälle itse on tärkeää, sillä poliisin esitutkintaresurssit ovat niukkoja, minkä lisäksi tutkintapyynnön tekemisessä kannattaa hyödyntää lakimiestä (Silen, haastattelu, 10.2.2020).

Etupainotteista varautumista varten on syytä käyttää penetraatiotestaukseen ja red teaming -toimintaan erikoistunutta palveluntarjoajaa, joka testaa "valkohattuhakkeroinnin" keinoin yrityksen kyberturvallisuuden toimivuutta käytännössä. Tämä on kriittisen tärkeää yrityksen tietoturvan kannalta, ja tunkeutumisen testaaminen palvelee yritystä konkreettisten haavoittuvuuksien löytämisen lisäksi myös turvallisuustietoisuuden ja yritysvakoilua harjoittavien tahojen toimintamenetelmien tuntemisen lisääjänä (Sandberg, 2015, s. 77). Sosiaalinen hakkerointi huomioiden tällainen testaustoiminta tulee kyberulottuvuuden lisäksi toteuttaa aina myös sosiaalisessa ja fyysisessä tilassa. Hadnagy (2010) on tunnistanut viisi erilaista haavoittuvuuksien kategoriaa, joita yrityksessä tulisi testata sosiaaliseen hakkerointiin liittyen. Nämä voidaan muotoilla kysymyksiksi:

- Avaako henkilöstö tuntemattomilta lähettäjiltä tulevien sähköpostien linkkejä tai liitetiedostoja?

- Meneekö henkilöstö huijaustarkoituksessa luoduille internetsivuille ja syöttää tietokenttiin yritystä koskevaa tai henkilökohtaista tietoa?

- Kuinka paljon henkilöstö on valmis luovuttamaan yritystä koskevaa tietoa puhelimessa tai kasvotusten työpaikan ulkopuolella?

- Miten yrityksen lukitukset, kulunvalvonta ja vartiointi kykenee estämään asiattoman liikkumisen toimitiloissa?

- Onko henkilöstö altis laittamaan työasemiin USB-tikkuja tai DVD-levykkeitä, joiden sisältö ja alkuperä on heille tuntematon?

6.5.4 Muita vastamenetelmiä

Yrityksen tietoaineistoihin kohdistuva uhka voi toteutua sekä fyysistä-, sosiaalista- että kybertilaa hyödyntäen, sijaitsivat nämä aineistot sitten dokumentteina työpisteillä tai tietokoneiden ja tallennusvälineiden sisällä. Itsestään selvää tulisi olla, että kaikki turvaluokitellut dokumentit tulisi sijoittaa lukittuihin kaappeihin ja laatikostoihin. Myös tietokoneet tulisi varastamisen vaikeuttamiseksi ja kovalevyn irrottamisen estämiseksi suojakoteloida ja telakoida työpisteisiin. Sivusta tapahtuvan silmäilyn estämiseksi näytöissä tulisi käyttää tietosuojakalvoja, ja hakkeroinnin kautta syntyvään salakatseluun tulisi varautua käyttämällä manuaalisia webkameran peittimiä. Paperidokumenttien turvallisuudesta tulisi huolehtia koko niiden elinkaaren ajan tulostamisesta hävittämiseen asti. Yhteistulostimien tulisi toimia turvatulostusperiaatteella, ja dokumenttien hävittämistä varten tulisi olla joko ristiinleikkaavat silppurit tai lukitut turvasäiliöt. Käytöstä poistettujen tietoteknisten laitteiden kovalevyt tulisi puhdistaa usealla päällekirjoituskerralla, rikkomalla manuaalisesti tai antamalla luotettavan alihankkijan tehtäväksi. Kaikki yrityksestä talon ulkopuolelle lähtevä jäte tulisi sijaita lukituissa jätekatoksissa.

Erityistä huomiota tulisi kiinnittää ulkomailla matkustamiseen liittyvään yritysvakoilun uhkaan. Ennen matkalle lähtöä turvallisuudesta vastaavan tahon tulisi järjestää palaveri, jossa käydään läpi kyseisen maan turvallisuustilanne, viranomaisten luotettavuus, yritysvakoiluun käytettävät menetelmät kuten värväysyritykset sekä toimintaohjeet epäilyttävissä tilanteissa (Wimmer, 2015, s. 75–83). Koska kannettaviin tietokoneisiin ja mobiililaitteisiin kohdistuva varkauden uhka on monissa maissa korkea, tulisi laitteiden suojaukset, varkaudenestotoiminnot ja kovalevyjen kryptaukset olla kunnossa. Huomaamatta tapahtuva laitteisiin kajoaminen tulisi estää lentokentillä ja hotellihuoneissa niin sanotuilla hygieniapusseilla, joiden sisään laite sinetöidään. Pussin avaamisen

huomaamista voi edesauttaa sijoittamalla muovin liimaosaan roskia, joiden tarkka sijoittuminen valokuvataan. Julkisia WiFi-verkkoja ei missään tilanteessa tulisi käyttää, ja muutoinkin kaikkea kriittistä tietoa tulisi välttää ulkomailta Suomeen tapahtuvassa viestinnässä. Erityisen tärkeät neuvottelut tulisi suojata oman turvallisuushenkilöstön tekemällä TSCM-skannauksella, joskin joissakin maissa tämä saattaa olla kiellettyä.

6.6 Vastatiedustelullinen näkökulma

Prunckun (2012, s. 41) jakaa vastatiedustelun neljään osa-alueeseen, jotka ovat estäminen, havaitseminen, harhauttaminen ja neutralisoiminen. Yllä käsitellyt yritysvakoilun vastamenetelmät kuuluvat pääasiallisesti ensimmäisen eli estämisen alle. Yhtä tärkeää kuin yritysvakoilun estäminen, on myös sen havaitseminen, mikä näyttää haastattelututkimuksen valossa olevan tällä hetkellä ongelma monille yrityksille. Prunckunin mukaan (2012, s. 171–185) havaitseminen muodostuu vastatiedustelun kontekstissa seuraavista vaiheista:

- Tapahtuneen asian tunnistaminen.
- Tapahtumaan liittyvien henkilöiden tunnistaminen.
- Näihin henkilöihin liittyvien organisaatioiden tunnistaminen.
- Näiden henkilöiden tämänhetkisen olinpaikan tunnistaminen.
- Todisteiden kerääminen henkilöiden liittämiseksi tapahtuneeseen.

Prunckun liittää havaitsemisprosessiin sellaisia toimia, kuten alustava tutkinta, rikospaikkatutkinta ja rikospaikkatietojen tallentaminen, tietokoneisiin liittyvä forensiikka sekä henkilöihin ja toimitiloihin kohdistuvan tarkkailun havaitseminen vastatarkkailun, ”surveillance detection”, keinoilla. Mikäli yritys ei turvaudu viranomaisiin yritysvakoilutapausten selvittelyssä, tulee sillä itsellään silloin olla kyky toteuttaa näitä toimia. Wimmer (2015, s. 7) liittää havaitsemisprosessiin myös tyypillisiä yritysturvallisuuden keinoja, kuten valvontakamerajärjestelmät ja paikallisvartiointi. Sinänsä minkä tahansa estävän kontrollitoimen, kuten lukituksen, tarkoitus on estämisen lisäksi osoittaa, mikäli kontrollitoimi on onnistuttu läpäisemään. Erotuksena yllä käsitellyistä estävistä toimista yritysvakoilun erityiset havaitsemistoimet voidaankin nähdä nimenomaan aktiivisena etsimisenä ja havaitun tapahtuman tutkintana.

Asiantuntijahaastattelut toivat esiin joitakin hyviä tapoja havaita, mikäli yritys on joutunut yritysvakoilun kohteeksi. Yksi niistä on havainnoida Darknetin markkinapaikkoja ja hakkeripalstoja, joissa kybervakoilun keinoin varastettuja liikesalaisuuksia myydään eteenpäin, ja ylipäätään seurata kilpailijoiden

liikkeelle laskemia tuotteita (Manninen, haastattelu 13.3.2020). Eräänlaisena "punaisena lippuna" eli indikaattorina mahdollisesta yritysvakoilusta voidaan pitää myös epätavallista markkinaosuuksien heilahtelua tai asiakkaiden menetystä (Susi, haastattelu, 18.3.2020). Mikäli yritys häviää tarjouskilpailut pienellä marginaalilla, menettää avainhenkilöstöä kilpailijoille, kilpailijat tuntuvat olevan aina "askeleen edellä" tai sijoittavat osaavat ennakoida yrityksen tuloksia ennen tulosjulkistusta, voi yritys olla joutunut kilpailijavakoilun kohteeksi (Brown, 2011, 294). Oman toimintaympäristön lisäksi tulee seurata aktiivisesti koko toimialaa, sillä mikäli esimerkiksi kilpailijan viestintä alkaa muistuttaa omaa, voi se olla merkki siitä, että omaan toimintaan kohdistuu mielenkiintoa (Ala-Varvi, haastattelu 24.3.2020).

ICT-ympäristössä oman normaalitoiminnan ja toimintalogiikan tunteminen on oleellista, jotta poikkeamat pystyttäisiin heti havaitsemaan. Usein tämä ei toteudu, vaan alihankkijoilta palveluita ostettaessa sopimusehtoja ei lueta, alihankkijoihin luotetaan liikaa eikä heidän toimintaansa seurata, ja pääsyoikeuksia myönnetään kaikille. Pahimmillaan ei tiedetä, kenelle käyttövaltuuksia on annettu, eikä niitä poisteta irtisanotuilta työntekijöiltä. (Ala-Varvi, haastattelu 24.3.2020.)

Myös Wimmer (2015) pitää oman ICT-ympäristön seuraamista tärkeänä, ja järjestelmissä tulisikin olla hälytykset tiettyjen poikkeuksellisten toimien, kuten epänormaaleina aikoina tapahtuvan käytön tai suurten tulostusmäärien osalta. Maasberg (2014) on tutkinut artikkelissaan sekä sosiaalisia että teknisiä indikaattoreita, joita on havaittu tunnettuihin insider-vakoilutapauksiin liittyen. Hän jaottelee tekniset indikaattorit neljään ryhmään, jotka ovat tiedon etsiminen, tiedon hankkiminen, tiedon valmistelu siirtämistä varten ja viimeisenä tiedon siirtäminen yrityksen ulkopuolelle. Yritysvakoilua suunnitteleva työntekijä etenee tyypillisesti kaikkien näiden vaiheiden läpi, ja niihin sisältyviä indikaattoreita ovat mm. hakujen tekeminen tietokannoissa, tiedostojen tallentaminen, tiedostojen kryptaaminen sekä tiedostojen tulostaminen, siirtäminen massamuistilaitteille tai liittäminen sähköpostiin. Sosiaalisia ja psykologisia indikaattoreita ovat mm. epätavalliset poissaolot ja myöhästymiset, sosiaaliset konfliktit, huono suoriutuminen työssä, sääntöjen rikkominen ja tyytymättömyys työhön.

Kahta viimeistä vastatiedustelun osa-aluetta, harhauttamista ja neutralisoimista, voisi helposti ajatella viranomaistoiminnan piiriin kuuluviksi asioiksi. Tosiasia kuitenkin on, että iso osa yritysvakoilun kohteeksi joutuneista yrityksistä ei vie asiaa viranomaisille vaan pyrkii hallitsemaan tilannetta omatoimisesti. Tässä tapauksessa yrityksellä tulee siten itsellään olla kyvykkyydet hoitaa tilanne siten, että yritysvakoilu kyseisen tekijän osalta päättyy. Yksinkertaisimmillaan neutralisointi voi tapahtua työsuhteen päättämisen tai järjestelmään pääsyn sulkemisen kautta. Wimmer (2015, s. 147) pitää myös harhauttavan tiedon antamista vakoilua toteuttaville tahoille yhtenä mahdollisena keinona. Esimerkiksi Applen epäillään käyttäneen harhauttavaa tietoa yhtiöön soluttautuneen "myyrän" paljastamiseksi (Bressler, 2015, s. 30). Mikäli yritys päättää laskea liikkeelle harhauttavaa tietoa, liittyy asiaan kuitenkin juridisia riskejä (Silen, haastattelu 10.2.2020). Mikäli työntekijä on epäilyn kohteena, voidaan

hänen omalla suostumuksellaan tutkimuksessa hyödyntää myös polygrafi- eli valheenpaljastustestausta (Wimmer, 2015, s. 132).

Vastatiedustelua yritysvakoilun yhteydessä voidaan tarkastella myös kriminologian ja rikostiedustelun näkökulmasta. Leppäsen (2006) mukaan kriminologiassa rikostorjunta jakautuu rikostorjuntastrategiaan, preventiiviseen taktiikkaan ja reaktiivisiin teknisiin rikostorjuntakeinoihin. Usein juuri tekniset menetelmät painottuvat ennaltaehkäisyn ja strategian kustannuksella. Rikostorjuntastrategia muodostuu erilaisista preventiomalleista. Tekijäpreventio kohdistuu potentiaalisiin rikoksentekijöihin, kuten yrityksen omaan henkilökuntaan, uhripreventio rikoksen uhriksi todennäköisesti joutuviin, sekä tilannepreventio itse rikostapahtumaan ja sen toteuttamiseen. Yrityksen rikostorjuntastrategiassa tulisi tunnistaa alueet, joihin yritys itse voi joko suoraan tai välillisesti vaikuttaa. (Leppänen, 2006, 257–258.) Juuri tekijä- ja uhripreventio voidaan tässä yhteydessä nähdä tärkeinä mutta vähemmän hyödynnettyinä tapoina sekä tuottaa tietoa mahdollisesta tietopääomaan kohdistuvasta rikoksesta että suojata yrityksen liikesalaisuuksia erityisesti sosiaalisessa tilassa tapahtuvalta yritysvakoilulta.

7 POHDINTA

Tämän tutkielman päätarkoitus oli selvittää yritysvakoilussa käytettäviä menetelmiä ja vastamenetelmiä. Lisäksi tavoitteena oli selvittää yritysvakoilun tämänhetkistä tilannekuvaa Suomessa sekä riskiin varautumiseen liittyviä ongelmakohtia. Tavoitteena oli tuloksiin perustuen myös esittää ratkaisuehdotuksia tunnistettuihin ongelmiin sekä tarjota todellisia menetelmiä yrityksille yritysvakoilun estämiseksi käytännössä. Lähdeaineistosta Podszymalow (2012) on esittänyt yrityksille kolme keinoa yhä tehokkaampaan yritysvakoilun torjuntaan. Ensimmäinen on liikesalaisuuden tunnistaminen, sen arvon määritteleminen ja tiedon suojaaminen. Toinen keino on henkilöstön kouluttaminen riskitietoisuuden lisäämiseksi ja kolmas simuloitujen hyökkäysten toteuttaminen toiminnan kehittämiseksi.

Myös Wimmer (2015) painottaa, että yritysvakoiluun varautumisen ei tulisi olla ainoastaan suojauksien rakentamista ja jälkikäteisreagointia, vaan proaktiivista ja etupainotteista työtä. Hän esittää teoksessaan useita hyviä keinoja tämän toteuttamiseen, joista ainakin kolmea voisivat hyödyntää myös sellaiset suomalaisyritykset, joissa yritysvakoilun riski on kohtuullinen tai suurempi. Ensimmäiseksi yrityksen tulisi perustaa tietopääoman suojaamisen ohjausryhmä, jossa olisi edustajia turvallisuusyksiköstä, IT-osastolta, henkilöstöhallinnosta ja liiketoiminnoista. Ryhmässä tulisi olla mukana myös juridiikan asiantuntija sekä ylimmän johdon edustaja, ja sen tulisi kokoontua säännöllisesti arvioimaan yritysvakoilun riskiä, tilannekuvaa ja varautumistoimenpiteiden tasoa. Toiseksi, tämän ryhmän tulisi koordinoida yrityksen johtoryhmän sitoutuneella tuella koko henkilöstölle järjestettäviä koulutuksia ja tietoiskuja yritysvakoilun uhkasta. Kolmanneksi, yrityksen tulisi perustaa kaikki toimipaikat käsittävä tietoturvallisuuden suojeluorganisaatio, joka toimisi turvallisuuspäällikön tai ohjausryhmän silminä ja korvina ruohonjuuritasolla. Organisaatio toimisi OTO-periaatteella vapaaehtoisesti, ja sen tehtävä olisi havainnoida, että clean desk -periaatetta noudatetaan, laatikostot ja kaapit ovat lukittuna, asiakirjat hävitetään oikeaoppisesti ja työtiloihin ei tule työntekijöiden mukana ulkopuolisia ”samalla oven avauksella”. (Wimmer, 2015, s. 101–172.) Suomessa isommissa yrityksissä on jo valmiina paloturvallisuuteen liittyvät suojeluorganisaatiot,

joista löytyy jokaisessa kerroksessa ja osastossa toimiva suojeluvalvoja. Näiden organisaatioiden toimenkuvan laajentaminen tietoturvallisuusohjeiden noudattamisen valvontaan oli helppo tapa hallita yritysvakoilun ja muihin tietopääomaan kohdistuvien rikosten riskiä.

Yhteiskunnan tasolla yksi tutkimuksessa esille tulleista ongelmista oli se, että Suomessa ei ole olemassa tahoa, jonka päätehtävä olisi seurata yritysvakoilun tilannekuvaa ja koordinoida varautumista, vaan yritysten ja viranomaisten välinen yhteistyö perustuu lähinnä henkilösuhteisiin. Ratkaisuna tähän ongelmaan olisi perustaa tietopääoman suojaamisen koordinointiryhmä, joka toimisi varautumisessa linkkinä eri toimijoiden, kuten Supon, KRP:n, Kyberturvallisuuskeskuksen, Huoltovarmuuskeskuksen, Elinkeinoelämän keskusliiton, kauppakamareiden, kyberturvallisuusalan klusteriorganisaatio FISC:n, turvallisuusalan yhtiöiden ja yksittäisten yritysten välillä. Tällaisen organisaation tehtäviä voisivat olla tilannekuvan muodostaminen suomalaisiin yrityksiin kohdistuvasta yritysvakoilusta, aiheesta tiedottaminen sekä erilaisten koulutusten ja seminaarien järjestäminen. Mikäli Keskuskauppakamarin aiemmat tutkimukset pitävät paikkansa, ja jopa kymmenesosa suomalaisista yrityksistä on jonkinlaisen yritysvakoilun kohteena, eivät tällaisen ryhmän perustamiseen ja ylläpitämiseen käytettävät resurssit varmasti olisi liioiteltuja.

7.1 Riskin arvioiminen

Jo tutkimuksen alkuvaiheessa näytti siltä, että yrityksillä yleisesti ottaen saattaisi olla vaikeuksia arvioida yritysvakoilun riskiä. Tutkimuksen aikana tämä oletus osoittautui paikkansa pitäväksi, eikä spesifisti yritysvakoiluun käytettävää riskiarviomenetelmää ollut löydettävissä lähdekirjallisuudesta tai aiemmista tutkimuksista. Jotta yritys voisi suhteuttaa yritysvakoilun estämiseen käytettävät resurssit oikein, tulisi sen ensin voida arvioida yritysvakoilun kohteeksi joutumisen todennäköisyyttä, sekä sen seurauksena tapahtuvien menetysten vakavuutta. Menetykset voivat olla joko suoraa taloudellista tappiota esimerkiksi saamatta jääneestä myynnistä, mutta myös vaikeasti mitattavaa maineen menetystä. Yrityksen liikesalaisuuden joutuminen yritysvakoilijan haltuun ei kuitenkaan välttämättä aiheuta minkäänlaista tappiota yritykselle (Lamberg, henkilökohtainen tiedonanto 6.4.2020). Tämä voi johtua monestakin syystä: kyseessä oleva innovaatio saattaa olla liian vaikea kopioida suunnittelutiedoista huolimatta, alkuperäisellä suunnittelijalla on vakiintunut jalansija markkinoilla eikä kopiotuotteelle olisi kysyntää, tai liikesalaisuus liittyy enemmän kriittisen infrastruktuurin heikkouksien selvittämiseen kuin taloudelliseen hyödyntavoitteluun. Tästä syystä riskin vakavuuden arviointi tulee aina toteuttaa yritys- ja tilannekohtaisesti. Sen sijaan yritysvakoilun kohteeksi joutumisen todennäköisyyden arvioimiseen on mahdollista muodostaa arviointimalli, joka on esitetty taulukossa 2. Siinä riskin todennäköisyys voidaan arvioida neljää kysymystä

käyttämällä: onko yrityksellä liikesalaisuutta, toimiiko se kotimaisilla vai kansainvälisillä markkinoilla, onko sillä fyysisesti toimintaa myös ulkomailla, ja onko sen liikesalaisuuksilla sotilaallista tai erityisen suurta taloudellista arvoa.

0	ei riskiä	ei liikesalaisuutta, jolla taloudellista arvoa
1	pieni	kilpailuetua tuova arvo ainoastaan Suomessa
2	matala	kilpailuetua tuova arvo kansainvälisillä markkinoilla, toimintaa vain Suomessa
3	kohtuullinen	kilpailuetua tuova arvo kansainvälisillä markkinoilla, toimintaa ulkomailla
4	korkea	merkittävä taloudellinen/sotilaallinen arvo, toimintaa vain Suomessa
5	kriittinen	merkittävä taloudellinen/sotilaallinen arvo, toimintaa ulkomailla

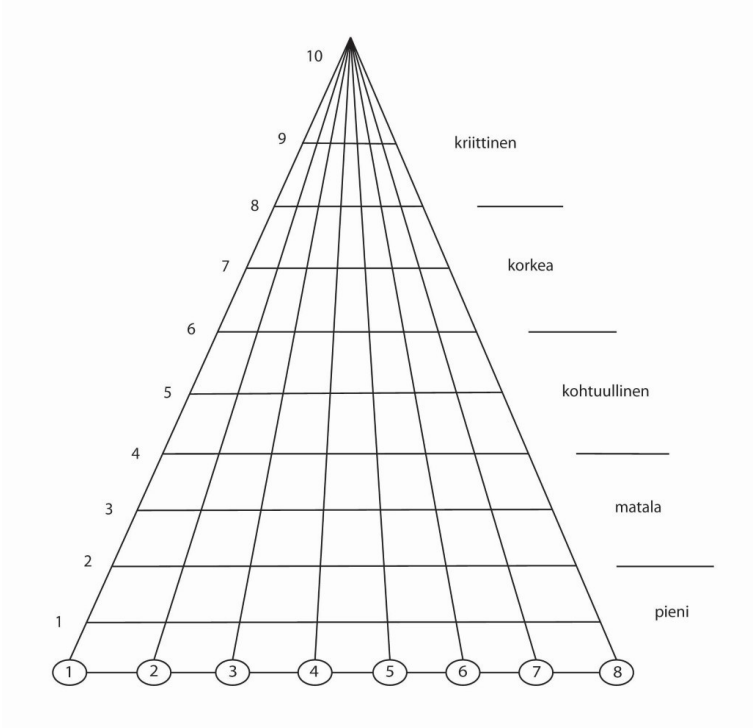
Taulukko 2: Yritysvakoilun riskin todennäköisyyden arvioiminen

Teoreettisesti ajateltuna yrityksellä ei välttämättä ole mitään sellaista tietoa, jota se haluaisi salata kilpailijoiltaan tai miltään muultakaan taholta. Tällöin yrityksellä ei olisi lainkaan riskiä joutua yritysvakoilun kohteeksi. Koska liikesalaisuudet kuuluvat lähtökohtaisesti liiketoiminnan luonteeseen, on tämä mahdollisuus käytännössä hyvin epätodennäköinen. Esimerkiksi Kähkönen (2015, s. 1–2) kirjoittaa, että lähes kaikkeen liiketoimintaan liittyy nykyaikana sellaista erityislaatuista ja arvokasta tietoa, että sitä hallussa pitävälle taholle syntyy intressi salassapitoon. Wimmerin (2015) mukaan yritys, jolla ei ole ketään kiinnostavaa liikesalaisuutta, ei ole olemassa vuoden kuluttua, sillä se ei tällöin toimi kovin kilpailullisesti. Vastaavasti liikesalaisuuden paljastumisuhka on jatkuvasti kasvanut, ja Euroopan komission tilaamassa tutkimuksessa vuonna 2013 joka viidenneltä yritykseltä oli yritetty varastaa tietoa kuluneen kymmenen vuoden aikana (Kähkönen, 2015, s. 1–2).

Mikäli yritys toimii vain Suomessa ja liikesalaisuuden joutumisella vääriin käsiin olisi taloudellista arvoa vain yrityksen suomalaisille kilpailijoille, voidaan yritysvakoilun riskiä pitää pienenä. Kilpailijavakoilu suomalaisten yritysten välillä on nimittäin tutkimuksen valossa hyvin harvinaista. Vaikka yritys toimisi vain Suomessa, voi liikesalaisuudella kuitenkin olla kilpailuetua tuovaa arvoa kansainvälisillä markkinoilla, kuten esimerkiksi erilaisten teknisten innovaatioiden kyseessä ollessa usein on. Tällöin yritysvakoilun riski on matala mutta jo toiminnassa huomioitava, sillä kybervakoilu tarjoaa ulkomaalaisille toimijoille helpon tavan hankkia tietoa yrityksen tietojärjestelmiin tunkeutumalla. Kohtuulliseksi riski muodostuu, mikäli tällaisella yrityksellä on toimintaa ulkomailla joko toimipaikan tai säännöllisen matkustamisen muodossa. Tällöin kynnys toteuttaa yritysvakoilua kyberulottuvuuden lisäksi fyysisessä ja sosiaalisessa ulottuvuudessa madaltuu. Korkeaksi yritysvakoilun riski muodostuu silloin, kun yrityksen liikesalaisuuksilla on merkittävää taloudellista tai sotilaallista arvoa, vaikka yritys fyysisesti toimisi vain Suomessa. Merkittävällä arvolla tarkoitetaan tässä yhteydessä satojen miljoonien eurojen arvoisia tuoteinnovaatioita, sotilas- tai kaksoiskäyttöteknologiaa, tai sellaista kriittistä infra-

struktuuria, jonka teknisten yksityiskohtien joutuminen vieraan valtion käsiin aiheuttaisi merkittävää vaaraa yhteiskunnalle mahdollisen sotilaallisen kriisin aikana. Mikäli tällaisella yrityksellä on fyysisesti toimintaa myös ulkomailla, voidaan yritysvakoilun riskiä pitää kriittisenä.

Yrityksen varautumistoimet laittoman tiedonhankinnan estämiseksi ovat hyvin moninaisia, eikä yksiselitteistä ja tyhjentävää luetteloa yritysten tilanteen ja toiminnan luonteen vaihtelevuudesta johtuen voida kehittää. Tutkimuksen aikana sekä haastattelujen että lähdemateriaalin perusteella on kuitenkin koottu tarkistuslista, jossa esitetään kahdeksankymmentä keinoa yritysvakoilun riskin hallitsemiseksi käytännössä (kontrollitoimien tarkistuslista, liite 2). Koska varautumiseen käytettävien resurssien tulee olla suhteessa riskiin, voidaan tarkistuslistaa käyttää yhdessä alla olevan matriisin kanssa (kuvio 3). Tarkistuslistan perusteella yritys sijoittaa saamansa pisteet kustakin kahdeksasta osa-alueesta matriisiin. Osa-alueiden numerot ovat kuvassa alla, pisteytys vasemmassa reunassa. Tulosten suhteuttaminen riskiin näkyy kuvan oikeassa reunassa ihanteellisena tavoitetasona. Jos esimerkiksi yritys arvioi yllä mainittua menetelmää käyttäen riskin olevan kriittisellä tasolla, tulisi valtaosan tuloksista sijaita kolmion yläpäässä kahdeksan ja kymmenen välillä. Mikäli yrityksen tulokset tarkistuslistan läpikäynnin jälkeen jäävät riskiä vastaavan tavoitetason alapuolelle, tulisi yrityksen toteuttaa kontrollitoimia, jolla varautumista tehostetaan kyseisellä osa-alueella. Tämä menetelmä tarjoaa nopean ja yksinkertaisen tavan arvioida yrityksen varautumisen tasoa sekä kiinnittää huomiota niihin seikkoihin, joiden osalta varautuminen ei vastaa arvioitua riskiä. Menetelmää voivat hyödyntää sekä yritysten turvallisuustoiminnoista vastaavat ammattilaiset että ulkopuoliset turvallisuuskonsultit.



Kuvio 3: Matriisi tarkistuslistan tuloksille

7.2 Lisätutkimuksen aiheita

Tässä tutkielmassa on selvitetty yritysvakoilussa käytettäviä keinoja sekä niihin varautumista erilaisten vastamenetelmien kautta. Tutkimusprosessin aikana on tullut ilmi kolme erilaista lisätutkimuksen aihetta, joita jatkossa olisi syytä selvittää Suomeen kohdistuvan yritysvakoilun ja siihen varautumisen osalta. Ensimmäiseksi esille on noussut yritysvakoilun laajuus ilmiönä. Vaikka joitakin viitteitä siihen liittyen on olemassa mm. Keskuskauppakamarin tutkimusten kautta, tulisi aiheesta tehdä oma, pelkästään siihen keskittyvä tutkimus, joka kattaisi merkittävän joukon suomalaisia yrityksiä toimialasta, koosta ja sijainnista riippumatta. Helsingin seudun kauppakamari onkin käynnistänyt tällaisen tutkimuksen alkuvuodesta 2021. Yritysvakoilu yhteiskunnallisena uhkana on todellinen ja jopa merkittävä, mistä huolimatta kenelläkään ei ole tarkkaa käsitystä ilmiön todellisesta laajuudesta. Resurssien ohjaaminen yritysvakoilun torjuntaan niin yhteiskunnan kuin yksittäisten yritystenkin taholla on vaikeaa, mikäli sen laajuus on vain arvailujen varassa. Paras lähde yritysvakoilun yleisyyttä tutkittaessa voisivat olla tietoturvayhtiöt sekä yritysten turvallisuustoiminnoista vastaavat tahot ja toimitusjohtajat.

Toinen lisätutkimuksen aihe olisi yritysten riskitietoisuus, jota olisi hyvä mitata niin yritysten johdon, turvallisuustoimintojen kuin liiketoimintojenkin osalta. Riskien hahmottaminen on riskienhallinnan teoriassa asia, johon lukuisilla tekijöillä on vaikutusta. Juvosen, Korhosen, Ojalan, Salosen ja Vuoren (2005) mukaa esimerkiksi paljon mediahuomiota saavia riskejä pidetään tyypillisesti merkittävämpinä kuin niitä, joita käsitellään vain vähän julkisuudessa. Toisaalta kuitenkin riskejä, joista on saatavilla vähän tietoa, pidetään suurempina kuin niitä, joista on saatavilla paljon luotettavaa tietoa. Yritysvakoilun osalta riskin arvottamista voivat pienentää esimerkiksi se, että kyseessä on hengen ja terveyden sijaan taloudellinen menetys, asia on tuttu ja tunnettu, ja siihen voi sopeutua. Lisäksi riskin hallintaan liittyviä päätöksiä tekevän henkilökohtaisella taustalla ja yksilöllisillä tekijöillä on huomattu olevan merkittävää vaikutusta riskin hahmottamiseen. (Juvonen ym., 2005, s. 14–15.) Kuten yritysvakoilun yleisyyttä, myös riskitietoisuutta yritysvakoilun suhteen voisi tutkia kyselytutkimuksen avulla.

Kolmas aihe, jota olisi syytä tutkia, on yritysten onnistuminen yritysvakoilun ehkäisemiseen liittyvien toimintamenetelmien jalkauttamisessa yrityksen kaikkiin prosesseihin. Osalla yrityksistä yritysvakoilun riski on kirjattu riskienhallinta- ja turvallisuussuunnitelmiin, osalla ei, ja pienimmillä yrityksillä ei välttämättä edes ole muuta kuin toimitiloihin liittyvät pelastussuunnitelmat. Tämä ei kuitenkaan tarkoita sitä, että ilman riskin kirjaamista suunnitelmiin sen torjunnassa automaattisesti epäonnistuttaisiin, sillä riskiä saatetaan hallita implisiittisellä, ääneen sanomattomalla tasolla. Työntekijät saattavat noudattaa annettuja ohjeita, vaikka kaikkia syitä niiden olemassaoloon ei tiedettäisi tai tiedostettaisi. Olisikin syytä tutkia, kuinka riskin hallinnassa ja yritysvakoilun ehkäisemiseen liittyvien toimintatapojen jalkauttamisessa ovat onnistuneet toi-

saalta yritykset, jotka ovat ilmaisseet riskin eksplisiittisesti, ja toisaalta ne, jotka eivät ole näin toimineet. Tällaista tutkimusta voisi suorittaa observoinnin kautta.

LÄHTEET

Ahonen, S., Saari, S., Syrjälä, L. & Syrjäläinen, E. (1994). *Laadullisen tutkimuksen työpajoja*. Rauma: Kirjayhtymä.

Alasuutari, P. (1993). *Laadullinen tutkimus*. Helsinki: Gummerus.

Alonso-Trabanco, J. (2020). The Emerging Nexus of Strategic Intelligence, Geopolitics, and Finance. *Geopolitical Monitor, Situation Reports May 19, 2020*. Haettu osoitteesta https://www.geopoliticalmonitor.com/the-emerging-nexus-of-strategic-intelligence-geopolitics-and-finance/

BBC News (26.7.2020). How a Chinese agent used LinkedIn to hunt for targets. Haettu osoitteesta https://www.bbc.com/news/world-asia-53544505

Benny, D. (2014). *Industrial Espionage. Developing a Counterespionage Program*. Boca Raton: CRC Press.

Billand, P., Bravard, C., Chakrabarti, S. & Sarangi, S. (2009). Corporate Espionage. *DIW Berlin Discussion Papers 854*. Haettu osoitteesta https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1430908

Bressler, M. (2015). Protecting your company's intellectual property assests from cyber-espionage. *Journal of Legal, Ethical and Regulatory Issues*, *vol. 18, no. 1*. Haettu osoitteesta https://www.questia.com/library/journal/1G1-423819243/protecting-your-company-s-intellectual-property-assets

Brown, A. (2011). *The Grey Line: Modern Corporate espionage and Counterintelligence*. CreateSpace Independent Publishing Platform.

Budiono, G. & Sawitri N. (2017). Strategic business espionage: an ethics and business practices to gain opportunity or community problems. *Studies in Business and Economics no. 12(1)/2017*. Haettu osoitteesta https://www.researchgate.net/publication/318156412_Strategic_Business_Espionage_An_Ethics_and_Business_Practices_to_Gain_Opportunity_or_Community_Problems

Carlisle, R. (2005). *Encyclopedia of Intelligence and Counterintelligence*. London: Routledge.

Clark, R. & Lowenthal, M. (2016). *The 5 disciplines of intelligence collection*. Washington: SAGE Publications.

Crane, A. (2005). In the company of spies: when competitive intelligence turns into industrial espionage. *Business Horizons 48 (3)*. Haettu osoitteesta https://www.academia.edu/27131253/In_the_company_of_spies_When_competitive_intelligence_gathering_becomes_industrial_espionage

Cyberwatch & EK (2018). Kybervakoilu – mitä jokaisen yrityksen tulisi tietää? Haettu osoitteesta https://ek.fi/wp-content/uploads/Kybervakoilu2018.pdf

Cyberwatch Finland Magazine, quarterly review Q2 (2020). Haettu osoitteesta https://www.cyberwatchfinland.fi/news/cyberwatch-finland-q2-magazine-a-passion-for-a-cyber-safe-world/

Ehrman, J. (2009). Toward a theory of CI. What are we talking about when we talk about counterintelligence. *Studies in intelligence, vol. 57*. Haettu osoitteesta https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/pdfs/U-%20Ehrman-Theory%20of%20CI.pdf

Elinkeinoelämän keskusliitto (2017). Yritys – miten olet suojannut tietopääomasi? Haettu osoitteesta https://ek.fi/wp-content/uploads/Tietopaaoman-turvaaminen.pdf

Elinkeinoelämän keskusliitto (3.2.2017). EK tutki: Cleantech-alalla jo 4 000 pk-yritystä. Haettu osoitteesta https://ek.fi/ajankohtaista/tiedotteet/2017/02/03/ek-tutki-cleantech-alalla-jo-4-000-pk-yritysta/

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

Fink, S. (2003). *Sticky Fingers: Managing the Global Risk of Economic Epionage*. Indiana: IUniverse.

Grossmann, W. (2015). *Fundamentals od Business Intelligence*. New York: Springer.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. New Jersey: John Wiley & Sons. Siteerattu teoksesta Sandberg, J. (2015). *Human element of corporate espionage risk management – literature review on assessment and control of outsider and insider threats*. Pro gradu –tutkielma, Tampereen yliopisto.

Harris, J. (1998). *Industrial espionage and technology transfer: Britain and France in the eighteenth century*. Farnham: Ashgate.

Harrison, J. & Andrii, A. (2017). A Literature Review: Industrial Espionage. School of Business and Engineering Halmstad University, Sweden. Haettu

osoitteesta https://www.researchgate.net/publication/318816635_A_Literature_Review_Industrial_Espionage

Helsingin seudun kauppakamari (14.12.2020). Yritysvakoilu ja tietoriskit yleistyneet yrityksissä. Haettu osoitteesta https://helsinki.chamber.fi/release/yritysvakoilu-ja-tietoriskit-yleistyneet-yrityksissa/#baa2bc65

Heuer, R. (1999). *Psychology of Intelligence Analysis*. Reston: Pherson Associates.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2016). *Tutki ja kirjoita*. Helsinki: Kustannusosakeyhtiö Tammi.

Holmström, L. (2010). Industrial espionage and corporate security: the Ericsson case. *Reports of the police college of Finland 87/2010*. Haettu osoitteesta https://www.theseus.fi/bitstream/handle/10024/86735/Rapotteja_87_holmstrom.pdf?isAllowed=y&sequence=1

Infosecurity (14.8.2020). RedCurl Emerges as a Corporate Espionage APT. Haettu osoitteesta https://www.infosecurity-magazine.com/news/redcurl-emerges-as-a-corporate/

Iovan, S. & Dinu, M.B. (2014). Impact of the loss and theft of electronic data on companies. *Fiability & Durability/Fiabilitate si Durabilitate 1*, 39-45. Siteerattu tutkielmasta Koivula, N. (2015), *Kiinan suorittaman kybervakoilun aiheuttamat pitkäaikaiset haitat KIBS-yrityksille*. Kandidaatintutkielma, Jyväskylän yliopisto.

Javers, E. (2011). Secrets and Lies. The Rise of Corporate Espionage in a Global Economy. *Georgetown Journal Vol. 12 No. 1, 2011*. Haettu osoitteesta https://www.slideshare.net/easa71/secrets-and-lies-the-rise-of-corporate-espionage-in-a-global-economy

Johnson, L.K. (1996) *Secret Agencies: U.S. Intelligence in a Hostile World*. New Haven, CT, and London: Yale University Press, p 147. Siteerattu artikkelista Trim, P. (2002) *Counteracting Industrial Espionage through Counterintelligence: The Case for a Corporate Intelligence Unit and Collaboration with Government Agencies*. Perpetuity Press.

Johnson, L.K (2007). *Handbook of intelligence studies*. Abingdon: Routledge.

Johnson, M., Long, T. (2000). Rigour, reliability and validity in qualitative research. *Clinical Effectiveness in Nursing, Volume 4, Issue 1*. Haettu osoitteesta https://www.sciencedirect.com/science/article/abs/pii/S1361900400901067

Juvonen, M., Korhonen, H., Ojala, V-M., Salonen, T. & Vuori, H. (2005). *Yrityksen riskienhallinta*. Helsinki: Suomen vakuutusalan koulutus ja kustannus Oy.

Jyväskylän yliopisto, opinto-opas 2020-2023, TSAS7036. Haettu osoitteesta: https://opinto-opas.jyu.fi/2020/fi/opintojakso/tsas7036/

Jääskeläinen, V. (2018). Liikesalaisuuksiin kohdistuvien insider-riskien hallinta. *Suojelupoliisin julkaisusarja 1/2018*. Haettu osoitteesta https://ek.fi/wp-content/uploads/Liikesalaisuuksiin-kohdistuvien-insider-riskien-hallinta.pdf

Kahaner, L. (1998). *Competitive Intelligence: How to gather, analyze and use information to move your business to the top*. New York: Touchstone.

Kaikkonen, P. (2017). *Liiketoimintatiedon hallinnan suorituskyvyn muodostaminen ja mittaaminen PK-yrityksissä*. Pro gradu -tutkielma, Itä-Suomen yliopisto. Haettu osoitteesta https://epublications.uef.fi/pub/urn_nbn_fi_uef-20170582/urn_nbn_fi_uef-20170582.pdf

Kauppalehti (4.9.2017). Yritysvakoilusimulaatio paljasti suomalaisyritysten tietoturva-aukot - ”Tulokset ovat jäätäviä”. Haettu osoitteesta https://www.kauppalehti.fi/uutiset/yritysvakoilusimulaatio-paljasti-suomalaisyritysten-tietoturva-aukot-tulokset-ovat-jaatavia/1319bad7-ea7b-3b3a-9833-1642cadcf8a6

Koivula, J. (2010). *RE: VS: Aineistot s-postilla? Sähköposti aineistonkeruun välineenä yhteiskuntatieteellisessä tutkimuksessa*. Pro gradu –tutkielma, Jyväskylän yliopisto. Haettu osoitteesta https://jyx.jyu.fi/bitstream/handle/123456789/22987/1/URN%3ANBN%3Afi%3Ajyu-201002241276.pdf

Kupi, E. & Lanne, M. (2014). Miten hahmottaa Security-alaa? VTT.

KvaliMOTV, menetelmäopetuksen tietovaranto, 9.9.2020. Haettu osoitteesta https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3_2.html

Kähkönen, H. (2015). *Liikesalaisuuksien salassapidosta sopiminen työsuhteessa*. Pro gradu -tutkielma, Tampereen yliopisto. Haettu osoitteesta http://urn.fi/URN:NBN:fi:uta-201505131427

Laine, H. (2018). *Kuulustelua, haastattelua vai keskustelua? Käsiteanalyysi elisitaatiosta henkilötiedustelun tiedonhankinnan viitekehyksessä*. Pro gradu –tutkielma, Maanpuolustuskorkeakoulu. Haettu osoitteesta https://core.ac.uk/download/pdf/160038264.pdf

Lamberg, J-A. (2019). Business intelligence, luento Jyväskylän yliopistossa 12.11.2019.

Lehto, M. (2020). Digitaalinen maailma ja turvallisuus. Luento Jyväskylän yliopistossa 24.10.2020.

Lehto, M. (2020). Digitaalisen kybermaailman ilmiöitä ja määrittelyjä, V. 12.0. Jyväskylä: Jyväskylän yliopisto.

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. *Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018*. Haettu osoitteesta http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf?sequence=1&isAllowed=y

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. *Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017.* Haettu osoitteesta https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf?version=1.0&t=1487318599000

Leppänen, J. (2006). *Yritysturvallisuus käytännössä*. Helsinki: Talentum.

Lohse, M. & Viitanen, M. (2019). *Johdatus tiedusteluun*. Helsinki: Alma Talent.

Lowenthal, M. (2011). *Intelligence: from Secrets to Policy*. Washington: CQ Press.

Maasmerg, M. (2014). Insider Espionage: Recognizing Ritualistic Behavior by Abstracting Technical Indicators from Past Cases. AMCIS 2014 Proceedings. Haettu osoitteesta https://aisel.aisnet.org/amcis2014/Posters/ISSecurity/26/

Martelius, J. (1999). Tiedusteluympäristö kylmän sodan jälkeen. Teoksesta Simola, M. & Sirviö, T. (toim.), (1999). *Isänmaan puolesta, Suojelupoliisi 50 vuotta* (s. 233-252). Helsinki: Gummerus.

Matila, J. (2011). *Yritysvakoilu. Mitä se on ja miten siltä suojaudutaan?* Pro gradu -tutkielma, Oulun yliopisto.

Mayers, M & Newman, M. (2006). The qualitative interview in IS research: Examining the craft. *Information and Organization Vol. 17.* Haettu osoitteesta

https://www.sciencedirect.com/science/article/abs/pii/S1471772706000352

NCSC, National Counterintelligence and Security Center (2018). Haettu osoitteesta https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

Pelttari, Antti (13.3.2020). Uudet uhkat 2020-seminaari. Ulkopolitis.fi

Podszywalow, M. (2012). Preventing corporate espionage. *Risk Management vol. 59*. Haettu osoitteesta https://www.natlawreview.com/article/preventing-corporate-espionage

Pourteus, S. (1994). Economic espionage 2. *Canadian Security Intelligence Service, Commentary Number 46*. Siteerattu artikkelista Holmström, L. (2010). Industrial espionage and corporate security: the Ericsson case. *Reports of the police college of Finland 87/2010*.

Prescott, J. & Miller, S. (2001). *Proven Strategies in Competitive Intelligence – Lessons From the Trenches*. New Jersey: John Wiley & Sons.

Prunckun, H. (2012). *Counterintelligence, theory and practice*. Lanham, Maryland: Rowman & Littlefield Publishers.

Rikoslaki 39/1889 30 luku: Elinkeinorikoksista. Viitattu 22.12.2020. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Sandberg, J. (2015). *Human element of corporate espionage risk management – literature review on assessment and control of outsider and insider threats*. Pro gradu –tutkielma,
Tampereen yliopisto. Haettu osoitteesta https://trepo.tuni.fi/handle/10024/97116

Secmeter (29.11.2020). Haettu osoitteesta https://secmeter.com/home.php

Shing, M. & Spence, L. (2002). Investigating the limits of competitive intelligence gathering: is mystery shopping ethical? *Business Ethics, a European Review 11 (4)*. Haettu osoitteesta http://web.a.ebscohost.com.ezproxy.jyu.fi/ehost/pdfviewer/pdfviewer?vid=1&sid=dbdd4492-8888-4158-9458-145d61e0c4ec%40sessionmgr4006

Simola, M. (toim.), (2009). *Ratakatu 12. Suojelupoliisi 1949–2009*. Helsinki: WSOY.

Sisäministeriö, tiedote (21.2.2019). Poliisi voi jatkossa puuttua dronejen lennättämiseen tietyissä tilanteissa. Haettu osoitteesta

https://valtioneuvosto.fi/-/1410869/poliisi-voi-jatkossa-puuttuja-dronejen-lennattamiseen-tietyissa-tilanteissa

Søilen, K. S. (2016). Economic and industrial espionage at the start of the 21st century–Status quaestionis. *Journal of Intelligence Studies in Business, 6(3)*. Haettu osoitteesta http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1061073&dswid=-4594

Suojelupoliisi (2019). Kansallisen turvallisuuden katsaus. Haettu osoitteesta https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/78653_20191205_Supo_kansallinen_turvallisuus_web.pdf?7d32519b6979d788

Susiluoto, T. (2020). Elinkeinoelämän ja tiedustelun kohtalonyhteys. Teoksesta Koivula, T. (toim.) *Suomalaisen tiedustelukulttuurin jäljillä*. Maanpuolustuskorkeakoulu. Haettu osoitteesta https://www.doria.fi/handle/10024/177568

Tankard, C. (2011). Advanced Persistent threats and how to monitor and deter them. *Network security 2011*. Siteerattu teoksesta Sandberg, J. (2015). *Human element of corporate espionage risk management – literature review on assessment and control of outsider and insider threats.* Pro gradu –tutkielma, Tampereen yliopisto.

Teknologiateollisuus (12.11.2019). Suomalaisten tekoäly-yritysten huiput listattiin jälleen. Haettu osoitteesta https://teknologiateollisuus.fi/fi/ajankohtaista/tiedote/suomalaisten-tekoaly-yritysten-huiput-listattiin-jalleen-listalla-jo-30

Trim, P. (2002). *Counteracting Industrial Espionage through Counterintelligence: The Case for a Corporate Intelligence Unit and Collaboration with Government Agencies*. Leicester: Perpetuity Press.

Tolvanen, T. (2015). *Yrityksen kilpailutoimintatiedon suojaaminen henkilötiedustelun peitetyn tiedonhankinnan uhalta*. Opinnäytetyä, Laurea-ammattikorkeakoulu. Haettu osoitteesta https://docplayer.fi/14899612-Yrityksen-kilpailutoimintatiedon-suojaaminen-henkilotiedustelun-peitetyn-tiedonhankinnan-uhalta.html

Van Cleave, M.K. (2007). Strategic Counterintelligence: What Is It, and What Should We Do About It? *Studies in intelligence, vol. 51, no. 2*. Haettu osoitteesta https://apps.dtic.mil/dtic/tr/fulltext/u2/a498042.pdf#page=7

Van Cleave, M.K. (2013). What is counterintelligence? *Journal of U.S. intelligence studies, 20 (2)*. Haettu

osoitteesta https://www.afio.com/publications/VAN%20CLEAVE%20Pages%20from%20INTEL_FALLWINTER2013_Vol20_No2.pdf

West, C. (2001). *Competitive Intelligence*. London: Palgrave Macmillan.

Wimmer, B. (2015). *Business Espionage. Risks, Threats and Countermeasures*. Amsterdam: Elsevier.

Yle uutiset (11.6.2008). Yliopiston mikroluokasta löytyi vakoilulaite. Haettu osoitteesta https://yle.fi/uutiset/3-5839100

Yle uutiset (19.6.2019) Entisillä työntekijöillä oli tuhansia Nokian renkaiden tiedostoja – hovioikeus lievensi hieman tuomioita Suomen suurimmassa yrityssalaisuusjutussa. Haettu osoitteesta https://yle.fi/uutiset/3-10837850

HAASTATTELUT JA HENKILÖKOHTAISET TIEDONANNOT

Ahonen, Anna-Maija. Koulutusohjelman johtaja, Aalto Pro. Sähköpostihaastattelu 10.2.2020.

Ala-Varvi, Jari. Tietosuojavastaava, Opsec Oy. Sähköpostihaastattelu 24.3.2020.

Hakala, Lotta. Suunnittelija, Suojelupoliisi. Sähköpostihaastattelu 30.3.2020.

Lahtinen, Mika. Lakimies, Helsingin seudun kauppakamari. Sähköpostihaastattelu 29.1.2020.

Lamberg, Juha-Antti. Professori, Jyväskylän yliopisto. Sähköpostihaastattelu 6.4.2020.

Manninen, Otso. Rikosylikonstaapeli, Keskusrikospoliisi. Sähköpostihaastattelu 13.3.2020.

Rajamäki, Markku. Johtava asiantuntija, Elinkeinoelämän keskusliitto. Sähköpostihaastattelu 2.4.2020.

Ruohonen, Sami. Service Owner, F-Secure. Sähköpostihaastattelu 31.1.2020 ja 12.2.2020.

Silen, Marko. Johtaja, Helsingin seudun kauppakamari. Sähköpostihaastattelu 10.2.2020.

Susi, Mika. Toiminnanjohtaja, FISC ry. Sähköpostihaastattelu 18.3.2020.

Waltzer, Kim. Analyytikko, Cyberwatch Finland. Sähköpostihaastattelu 27.2.2020.

LIITE 1

HAASTATTELUKYSYMYSTEN MALLIRUNKO

1. Miten yritysvakoilu on näkynyt työssäsi? Minkälaisiin tapauksiin olet törmännyt, minkälaisia keinoja vakoiluun on käytännössä käytetty, miten ne ovat paljastuneet, ketkä ovat olleet syyllisiä?

2. Miten näet suomalaisten yritysten varautumisen yritysvakoiluun, mitä on tehty ja mitä voisi tehdä paremmin?

3. Onko sinulla kokonaisarviota siitä, kuinka paljon laitonta tiedonhankintaa suomalaisyrityksiin kohdistuu ja minkälaisia menetyksiä siitä aiheutuu?

4. Entä tukeeko yhteiskunta yrityksiä tähän asiaan liittyen tarpeeksi, esim. Supo, kyberturvallisuuskeskus jne.?

5. Yritysvakoilun kohteeksi joutumista on usein vaikea huomata. Osaatko antaa vinkkejä, mistä yritys voisi päätellä joutuneensa vakoilun kohteeksi?

6. Asiantuntijan organisaation ja työtehtävän mukaisesti kohdennettu kysymys.

7. Mitä muuta haluaisit sanoa aiheeseen liittyen?

LIITE 2

KONTROLLITOIMIEN TARKISTUSLISTA

1. Turvallisuusjohtaminen **Kyllä** **Ei**

- Liikesalaisuudet on määritelty
- Yritysvakoilun riski on tunnistettu
- Riski on arvioitu ja analysoitu
- Asia on kirjattu riskienhallinta- ja turvallisuussuunnitelmiin
- Kontrollitoimiin on ryhdytty suunnitelmallisesti
- Turvallisuustietoisuutta aiheesta lisätään kouluttamalla ja ohjeistamalla
- Ohjeiden noudattamista havainnoidaan
- Puutteista huomautetaan henkilöstölle ja esimiehelle
- Yrityksen johto on sitoutunut ohjaamaan resursseja yritysvakoilun estämiseen
- Yrityksen johto pyrkii luomaan turvallisuuskulttuuria, jossa tietopääoma huomioidaan

2. Henkilöstö **Kyllä** **Ei**

- Uusien työntekijöiden työhistoria tarkistetaan
- Luottotiedot tarkistetaan
- Huumausainetestit tehdään
- Turvallisuusselvitysmenettely on käytössä
- Yritysvakoilu riskinä huomioidaan soveltuvuustesteissä
- Erillinen salassapitosopimus on käytössä
- Kilpailukieltosopimus on käytössä
- Tietopääomaan kohdistuvat riskit huomioidaan perehdytyksessä
- Käyttövaltuuksien hallinta tietojärjestelmissä on kunnossa
- Työsuhteen päättyminen tapahtuu hallitusti

3. Toimitilat **Kyllä** **Ei**

- Lukitukset, murtosuojaus ja hälytysjärjestelmät ovat käytössä
- Kameravalvonta on käytössä
- Kulunvalvontajärjestelmät ovat käytössä
- Kulkuoikeudet on määritelty turvallisuusvyöhykkeittäin
- Matkapuhelinvapaat tilat on määritelty
- Palvelin- ja teletilat on lukittu myös työntekijöiltä
- Yritysvakoilu on huomioitu sisustussäännöissä
- Clean desk -periaate on käytössä ja sitä noudatetaan
- TSCM-lakaisut toteutetaan säännöllisesti
- Neuvotteluhuoneet on suojattu kohinageneraattoreilla

4. Vierailijat **Kyllä** **Ei**

- Vierailuperiaatteet löytyvät kirjallisessa muodossa
- Vierailijat kirjataan vierailijarekisteriin
- Asiaton pääsy vierailijarekisteriin on estetty
- Vierailijat allekirjoittavat salassapitosopimuksen
- Vierailijoilla on yksilöity vierailijakortti
- Vierailijoilla on aina saattaja
- Vierailijoiden käytössä olevat turvallisuusvyöhykkeet on määritelty
- Matkapuhelimen ym. laitteiden käytöstä ohjeistetaan
- Tilapäisiä kulkuoikeuksia annetaan vain poikkeuksellisesti
- Työntekijät eivät päästä tuntemattomia mukanaan lukituista ovista

5. Tietoaineistot ja laitteet	**Kyllä**	**Ei**
• Tiedon turvallisuusluokittelu ja käyttöoikeudet on määritelty		
• Tietoaineistot säilytetään lukituissa kaapeissa ja laatikoissa		
• Kriittiset tietokoneet on suojakoteloitu tai lukittu telakkaan		
• Tietosuojakalvot ovat käytössä		
• Web-kameran sulkimet ovat käytössä		
• Tulostuksen kontrollitoimet ovat käytössä		
• Dokumenttien hävittämiseen käytetään silppureita		
• Dokumenttien hävittämiseen käytetään turvasäiliöitä		
• Tietoteknisten laitteiden hävittäminen on kontrolloitua		
• Jätesäiliöt ja katokset rakennuksen ulkopuolella on lukittu		

6. Tietojärjestelmät	**Kyllä**	**Ei**
• Päätelaitelukitukset ovat käytössä		
• Käyttäjän tunnistus on käytössä		
• Salasanakontrolli on käytössä ja sitä noudatetaan		
• Palomuuri ja virustorjunta on hoidettu		
• Järjestelmälokitus on kunnossa		
• Verkonvalvonta on käytössä		
• Sähköpostiliikenne on aina suojattua		
• Verkkosivujen suojausprotokollat ovat kunnossa		
• Käyttäjien turvallisuustietoisuudesta huolehditaan säännöllisesti		
• Näkyvyys sekä komponentteihin ja lähdekoodiin on varmistettu		

7. Työskentely toimipaikan ulkopuolella ja matkustaminen **Kyllä** **Ei**

- Mobiililaitteiden suojaus ja varkaudenesto on kunnossa
- Tietoturvallisuudesta huolehditaan myös etätyössä
- Turvallisuusasiat käydään läpi ennen ja jälkeen matkan myös
- yritysvakoilu huomioiden.
- Paikallisten viranomaisten luotettavuus on selvitetty
- Epäilyttävien tilanteiden ilmoittamisesta on ohjeistettu
- Teknisten laitteiden lukitukset ja kryptaukset on varmistettu
- Julkisia WiFi-verkkoja ei käytetä
- Hygieniapussit ovat käytössä lentokentillä ja hotelleissa
- Puhelin- ja sähköpostiliikenteen sisältöä on rajoitettu ulkomailla
- TSCM on käytössä majoitus- ja kokoustiloissa

8. Aktiiviset toimenpiteet **Kyllä** **Ei**

- Kilpailijoiden toimintaa seurataan yritysvakoilun näkökulmasta
- Darknetin markkinapaikkoja seurataan
- Vastatarkkailua toimipaikoissa toteutetaan
- Rikostiedustelua harjoitetaan tiedonkeruun havaitsemiseksi
- Liikekumppanien taustat selvitetään ulkomaansidonnaisuuksien osalta
- Joint venture -hankkeissa pyydetään konsultaatioapua tarvittaessa Suojelupoliisilta
- Polygrafitestit ovat tarvittaessa käytössä
- Epäilyttävät tapaukset kyetään selvittämään forensiikan keinoin näytön hankkimiseksi
- Penetraatiotestausta toteutetaan fyysisesti ja tietoverkossa
- Red-Teamingia toteutetaan

Pisteet yhteensä: _____ / 80