Ilona Sutela

KIINTEISTÖ- JA RAKENNUSTOIMIALA YRITYSVA-KOILUN KOHTEENA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Sutela, Ilona
Kiinteistö- ja rakennustoimiala yritysvakoilun kohteena
Jyväskylä: Jyväskylän yliopisto, 2024, 77 s.
Kyberturvallisuus, Kokonaisturvallisuus ja strateginen tiedustelu, pro gradu -tutkielma
Ohjaajat: Kari, J. Martti ja Lehto, Martti

Joulukuussa 2021 valtioneuvosto teki periaatepäätöksen valtion kiinteistöstrategiasta 2030. Kiinteistöstrategian yhdeksi keskeiseksi teemaksi on nostettu kokonaisturvallisuus. Yritysvakoilua voidaan pitää yhtenä merkittävimmistä ja haasteellisimmista kokonaisturvallisuuden uhkista, jolla voidaan vaikuttaa koko yhteiskunnan toimintaan. Toistaiseksi yritysvakoilua on tutkittu Suomessa yleisesti vähäisesti akateemisen tutkimuksen alueella. Kiinteistö- ja rakennustoimialan kontekstista ilmiötä ei ole vielä juurikaan tutkittu. Asiaan on kuitenkin kiinnitetty huomiota Suomen turvallisuusympäristön muuttuessa viimevuosien aikana epävakaammaksi.

Tämän pro gradu -tutkielman tarkoituksena oli tutkia ”miten yritysvakoilu ilmenee kiinteistö- ja rakennustoimialalla”. Tutkimusongelmaa tarkasteltiin kolmen tutkimuskysymyksen avulla ”millä keinoin ja menetelmin yritysvakoilua harjoitetaan kiinteistö- ja rakennustoimialaa kohtaan?”, ”mitkä asiat ovat yritysvakoilun kohteena kiinteistö- ja rakennustoimialalla ja miksi?”, ”miten yritysvakoilua vastaan voidaan varautua ja suojautua kiinteistö- ja rakennustoimialalla?” Tutkielma on rajattu koskemaan Suomen valtion kiinteistökantaa. Tutkielma toteutettiin laadullisena tutkimuksena, jonka aineisto muodostui teemahaastattelujen pohjalta. Haastateltavat edustivat kiinteistönomistajaa, kiinteistön käyttäjää, palveluntuottajaa, tiedusteltuviranomaisia sekä tiedustelu- ja turvallisuusalan että kyberturvallisuuden asiantuntijoita.

Tulosten perusteella voidaan todeta yritysvakoilun ilmenevän kiinteistö- ja rakennustoimialalla monitasoisena ja monimuotoisena uhkana. Tutkielman tulokset osoittavat, miten yritysvakoilu kohdistuu kiinteistö- ja rakennustoimialaan, jolloin sitä vastaan on paremmat mahdollisuudet varautua ja suojautua. Aineiston analyysin tuloksena yritysvakoilun keinojen ja menetelmien voidaan todeta olevan moninaiset ja hyödyntävän fyysistä, sosiaalista sekä digitaalista toimintaympäristöä. Tulokset antavat ymmärryksen siitä, miksi yritysvakoilua kohdistetaan kiinteistö- ja rakennustoimialaa kohtaan ja mitä vaikutusta sillä voi olla organisaatiolle itselleen, sen sidosryhmille ja yhteiskunnalle.

Asiasanat: kiinteistö- ja rakennustoimiala, yritysvakoilut, tiedustelu, organisaatioturvallisuus, kokonaisturvallisuus, tiedustelulajit

ABSTRACT

Sutela, Ilona
Real estate and construction industry as a target of corporate espionage
Jyväskylä: University of Jyväskylä, 2024, 77 pp
Cyber Security, Comprehensive security and strategic intelligence, Master's Thesis
Supervisors: Kari, J. Martti and Lehto, Martti

In December 2021, the Finnish government made a policy decision regarding the State Real Estate Strategy 2030. One of the key themes of the real estate strategy is comprehensive security. Corporate espionage is considered one of the most significant and challenging threats to comprehensive security, with the potential to impact the functioning of the entire society. So far, corporate espionage has been studied relatively little in Finland within the realm of academic research. In the context of the real estate and construction sector, the phenomenon has hardly been researched. However, attention has been drawn to the issue as Finland's security environment has become more unstable in recent years.

The aim of this master's thesis was to examine "how corporate espionage manifests itself in the real estate and construction sector." The research problem was explored through three research questions: "by what means and methods is corporate espionage conducted against the real estate and construction sector?", "what aspects are targeted by corporate espionage in the real estate and construction sector and why?", and "how can the real estate and construction sector prepare for and protect itself against corporate espionage?"

The study was limited to the real estate holdings of the Finnish state. It was conducted by using qualitative research. The empirical data were gathered in semi-structured interviews. The interviewees represented property owner, property user, service provider, intelligence authorities, and experts in the fields of intelligence, security, and cybersecurity.

The results indicate that corporate espionage manifests as a multifaceted and complex threat in the real estate and construction sector. The findings show how corporate espionage targets the real estate and construction sector, thereby providing better opportunities to prepare for and protect against it. The analysis of the data reveals that the means and methods of corporate espionage are diverse, utilizing physical, social, and digital environments. The results provide an understanding of why corporate espionage is directed at the real estate and construction sector and what impact it can have on the organization itself, its stakeholders, and society.

Keywords: Real estate, construction industry, corporate espionage, intelligence, corporate security, comprehensive security, methods of intelligence

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Joulukuussa 2021 valtioneuvosto teki periaatepäätöksen valtion kiinteistöstrategiasta 2030. Samalla päivitettiin valtion toimitilastrategia, jonka tavoitteet tulisi saavuttaa vuoteen 2030 mennessä. Kiinteistöstrategian yhdeksi keskeiseksi teemaksi on nostettu kokonaisturvallisuus. Tällä tarkoitetaan tavoitetilaa, jossa valtion itsenäisyyteen, väestön elinmahdollisuuksiin ja muihin yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat ovat hallittavissa. (Valtiovarainministeriö, 2021:66) Valtion toimitilastrategian 2030 mukaan toimitilojen tulee myös tukea ja mahdollistaa tietoturvallinen työskentely ja luottamuksellisten asioiden käsittely.

Yritysvakoilua voidaan pitää yhtenä merkittävimmistä ja haasteellisimmista kokonaisturvallisuuden uhkista, jolla voidaan vaikuttaa koko yhteiskunnan toimintaan. Koivulan (2020, 77) mukaan voimme menettää jopa 2–3 % bruttokansantuotteesta yritysvakoilun vuoksi. Yritysvakoilun torjunnalla on näin kansakunnallista merkitystä. Toistaiseksi yritysvakoilua on tutkittu Suomessa yleisesti vähäisesti akateemisen tutkimuksen alueella. Kiinteistö- ja rakennustoimialan kontekstista ilmiötä ei ole vielä juurikaan tutkittu. Asiaan on kuitenkin kiinnitetty huomiota eri foorumeissa ja viranomaisissa Suomen turvallisuusympäristön muuttuessa viimevuosien aikana epävakaammaksi. Erityisesti ulkomaalaisten tekemiin kiinteistöostoihin ja maakauppoihin, joissa kauppojen kohteet ovat sijainneet lähellä Suomen maanpuolustuksen kannalta kriittisiä kohteita, tullaan jatkossa arvioimaan turvallisuuskriittisemmin vuonna 2020 voimaantulleen lainsäädäntömuutoksen myötä. (Yle, 2022; Yle, 2016) Lisäksi kyberturvallisuuteen on alettu kiinnittämään enemmän huomioita kiinteistö- ja rakennustoimialan digitalisoitumisen, monipaikkaisen työnteon ja yhteisten monen käyttäjän työympäristöjen lisääntymisen myötä. Tässä tutkielmassa digitaaliseen ympäristöön kohdistuvaa uhkaa tarkastellaan kybervakoilun näkökulmasta.

Tutkielman merkittävimpänä tavoitteena on edistää valtion kiinteistönomistajien ja rakennuttajien sekä heidän eri sidosryhmien (palveluntuottajat, käyttäjät) ymmärrystä sekä valveutuneisuutta yritysvakoilusta ja miten se kohdistuu kiinteistö- ja rakennustoimialaan, jolloin sitä vastaan on paremmat mahdollisuudet suojautua. Lisäksi tutkimuksen avulla saataneen käsitys, miksi

yritysvakoilua kohdistetaan kiinteistö- ja rakennustoimialoihin ja mitä vaikutusta sillä voi olla.

1.1 Tarkoitus ja tavoite, tutkimusongelma

Tutkielman tarkoituksena on selvittää, miten yritysvakoilu eli laiton tiedustelu ilmenee kiinteistö- ja rakennustoimialalla. Tutkimusongelmaa selvitetään seuraavien tutkimuskysymyksien avulla:

1. Millä keinoin ja menetelmin yritysvakoilua harjoitetaan kiinteistö- ja rakennustoimialaa kohtaan?
2. Mitkä asiat ovat yritysvakoilun kohteena kiinteistö- ja rakennustoimialalla ja miksi?
3. Miten yritysvakoilua vastaan voidaan varautua ja suojautua kiinteistö- ja rakennustoimialalla?

Tutkimusaihetta tarkastellaan Suomen valtion omistaman kiinteistökannan näkökulmasta. Rajauksen ulkopuolelle on jätetty Suomen rajojen ulkopuolella olevat kiinteistöt sekä asuinrakennukset ja muut yksityisessä omistuksessa olevat kiinteistöt. Käytännössä tarkastelun keskiössä on Senaatti-konserni, joka hallinnoi valtion omistamia tiloja. Senaatti-konsernin tehtävänä on tuottaa kiinteistö- ja tilapalveluita, tilajohtamisen ja -hallinnon palveluita sekä tilojen hankintaan, hallinnointiin ja luovuttamiseen liittyviä palveluita valtion virastoille ja laitoksille (Laki Senaatti-kiinteistöistä ja Puolustuskiinteistöistä 1018/2020).

1.2 Tutkimuksen rakenne

Tässä alaluvussa kuvataan tämän pro gradu -tutkielman sisältöä ja rakennetta. Tutkielman teoriaosuus (luku 2) on toteutettu kuvailevan kirjallisuuskatsauksen tutkimusmenetelmää hyödyntäen. Salmisen (2011, 3–6) mukaan kuvailevaa kirjallisuuskatsausta voidaan luonnehtia yleiskatsaukseksi, jossa tutkittavaa aihetta pystytään kuvaamaan laajasti ja tutkimusaiheen ominaisuuksia voidaan tarvittaessa luokitella. Kirjallisuuskatsauksen tavoitteena on ollut kuvata tutkielman käsitteellistä taustaa, tutkittavaa kohdetta sekä siihen liittyviä erityispiirteitä tuottaen looginen kokonaiskuva tutkittavasta aiheesta. Lisäksi on pyritty vastaamaan esitettyihin tutkimuskysymyksiin käytetyn kirjallisen aineiston pohjalta. Kirjallisuuskatsauksen tulokset on esitetty luvussa 3, jossa on kuvattuna myös teoriaosuuden pohjalta muodostunut teoreettinen viitekehys. Teoreettisen viitekehyksen synteesi antaa varsinaisen tutkielman tekemiselle lähtökohdan ja kokoaa yhteen teoria osuuden.

Tutkielman toteutus ja tutkimusmetodi on kuvattuna luvussa 4. Tutkimusaineisto on kerätty teemahaastatteluin ja aineisto on analysoitu sisällönanalyysin

menetelmin. Käytetyt menetelmät ja niiden toteutus on pyritty kuvaamaan mahdollisimman kattavasti. Luvussa 5 esitellään haastatteluaineiston analyysin tulokset. Teorian ja haastatteluaineiston analyysin tulosten perusteella muodostuneet johtopäätökset on esitetty luvussa 6. Viimeisessä luvussa on myös tarkasteltu tutkielman luotettavuutta ja miten tutkimuseettiset näkökulmat on huomioitu tutkimusprosessissa. Lisäksi on pohdittu tämän tutkielman hyödynnettävyyttä ja millaisia jatkotutkimusaiheita tätä tutkielmaa tehdessä heräsi.

Tämän tutkielman aineisto koostuu pääasiassa aiheeseen liittyvistä tieteellisistä artikkeleista, viranomaisten sekä tunnettujen yhteisöjen ja järjestöjen julkaisuista, että tiedekirjoista. Lisäksi tutkielmassa on käytetty Senaatti-konsernin tuottamia julkisia lähteitä sekä hyödynnetty julkisuudessa käsiteltyjä tiedustelutoimintaan tai vakoiluun liittyviä tapauksia esimerkinomaisesti sikäli kuin ne ovat olleet tämän tutkielman kannalta relevantteja.

1.3 Aiemmat tutkimukset

Tehdyn kirjallisuuskatsauksen perusteella voidaan todeta, että yleisesti tiedusteluun liittyvää aineistoa on saatavilla paljon, mutta se koostuu pääasiassa disinformaatioon, propagandaan ja kylmään sotaan keskittyvistä historiallisista tutkimuksista. Vakoiluun ja laittomaan tiedusteluun liittyvää aihetta on tutkittu useiden tieteenalojen kuten sotatieteen, oikeustieteen, kasvatustieteen, taloustieteen ja tietojenkäsittelytieteen näkökulmasta. Kansainvälisesti laitonta tiedustelua ovat tutkineet 2000-luvulla muun muassa teollisuus- ja talousvakoilun näkökulmasta kriminologian ja oikeustieteen professori Hedieh Nasheri Kentin yliopistosta ja rikosoikeuden tohtori Daniel J. Benny Campellan yliopistosta. Sisäpiirivakoilua ja sen esiintyvyyttä ovat puolestaan tutkineet psykologian ja kasvatustieteiden näkökulmasta Toronton yliopiston professori Lisa Kramer, entinen CIA:n tiedusteluanalyytikko Richards J.Heuer jr. ja turvallisuustutkija Kent S. Crawford.

Suomessa vastaavia tutkimuksia on tehty vähemmän. Kauppatieteiden tohtori Jan-Peter Paul Helsingin yliopistolta on kirjoittanut teoksen Tiedustelu 2000-luvulla, jossa hän on tutkinut tiedustelun historiaa ja kehityskulkua. Maanpuolustuskorkeakoulussa on tehty useita tutkimuksia sotilastiedusteluun liittyvistä aiheista. Tommi Koivula on toimittanut teoksen Suomalaisen tiedustelukulttuurin jäljillä (2020), jossa tarkastellaan suomalaisen siviili- ja sotilastiedustelun muuttuvaa toimintaympäristöä. Helsingin seudun kauppakamari on tehnyt vuonna 2021 yritysvakoiluun liittyvän selvityksen, jonka avulla voidaan vertailla, minkälaisia yritysvakoilu-uhkia yrityksiin kohdistuu ja millaisia riskienhallinnan keinoja yritykset käyttävät. Selvitys perustuu 192 yrityksen vastauksiin. Vastanneista seitsemän prosenttia edusti rakentamista, 16 % teollisuutta, 38 % palveluita, 10 % kauppaa ja 29 % muuta alaa. Selvityksen tuloksia on myös hyödynnetty tässä tutkielmassa. Suomalaisten korkeakoulujen opinnäytteistä löytyi kaksi yritysvakoiluun keskittyvää pro gradu -tutkielmaa; Marko Meretvuon 2021 kirjoittama ”Yritysvakoilu: Tilannekuva, menetelmät ja estäminen” sekä Juhani

Matilan 2011 kirjoittama ”Yritysvakoilu. Mitä se on ja miten siltä suojaudutaan”. Molemmissa tutkielmissa on selvitetty yritysvakoilun historiaa ja kehityskulkua sekä mitä menetelmiä yritysvakoilussa käytetään ja miten sitä vastaan voi suojautua, joista kahta jälkimmäistä tutkimuskysymystä käsitellään myös tässä tutkimuksessa uudessa kontekstissa.

2 TEORIAOSUUS

Tämän pääluvun tavoitteena on kuvata tutkimuksen kannalta keskeisimmät käsitteet ja niiden väliset suhteet. Ensimmäisessä alaluvussa perehdytään kiinteistö- ja rakennustoimialan ja sen erityispiirteiden kuvaamiseen. Toinen alaluku käsittelee tiedustelun ja laittoman tiedustelun, yritysvakoilun määritelmiä sekä siinä käytettäviä menetelmiä ja mihin ne voivat kohdistua. Kolmannessa alaluvussa avataan kokonaisturvallisuuden ja organisaatioturvallisuuden käsitettä, miten ne nivoutuvat toisiinsa ja miten yritysvakoilun vastatoimia voidaan edistää organisaatioturvallisuuden keinoin.

2.1 Kiinteistö- ja rakennustoimialasta

Tässä alaluvussa kuvataan mitä kiinteistö- ja rakennustoimialla tarkoitetaan, mitkä ovat alan keskeisimpiä erityispiirteitä, mistä Suomen valtion omistama kiinteistökanta muodostuu ja miten sitä hallitaan. Kun ymmärretään tutkimuksen kohde ja alan erityispiirteet, pystymme tarkastelemaan minkälaisia yritysvakoilun keinoja ja menetelmiä kiinteistö- ja rakentamisalaan voi kohdistua. Lisäksi kartutamme ymmärrystä siitä mitkä asiat voivat olla kiinteistö- ja rakentamistoimialan kohteena ja miksi.

2.1.1 Kiinteistö- ja rakennustoimialan määritelmä

Kiinteistö- ja rakennustoimialan merkitys yhteiskunnalle tilojen tarjoajana, kansanvarallisuuden ylläpitäjänä, suurena työllistäjänä ja yhtenä Suomen kansantalouden moottoreista on merkittävä (Rakli, 2014). Alalla on yleisesti keskeinen rooli yhteiskunnan toimivuuden, elinkeinoelämän elinvoimaisuuden ja ihmisten hyvinvoinnin luomisessa. Rakennetun ympäristön voidaan katsoa kattavan kaikki ihmisen rakentama. Se läpi leikkaa yhteiskunnan lukuisia toimintoja kytkeytyen muun muassa liikenne- ja energia-aloihin muodostaen ihmisten, yhteisöjen ja yrityksien jokapäiväiset elin- ja toimintaympäristöt. (Kiinteistö- ja rakentamisfoorumi, 2022.)

Tilastokeskuksen voimassa olevan toimialaluokituksen (2008) mukaan kiinteistöalalla tarkoitetaan kiinteistöjen myyntiin, ostoon, vuokraukseen ja muihin kiinteistöpalveluihin liittyvää toimintaa. Rakennusala puolestaan jakaantuu kolmeen toimintaan, jotka ovat talon rakentaminen, maa- ja vesirakennus ja erikoistunut rakennustoiminta, johon kuuluvat rakennuspaikan valmistelutyöt, rakennusasennus (esimerkiksi LVIS-työt) sekä rakentamisen viimeistelytyöt ja rakennusten purku. Rakennusalan toiminta voi olla uudisrakentamista, korjausrakentamista, perusparannusta ja muutos-, laajennus- tai kunnostustyötä. Kiinteistö- ja rakentamisala muodostavat Suomessa KiRa-klusterin, jonka toimialat ovat sidoksissa toistensa kanssa (Lith, 2022). Tässä tutkielmassa kiinteistö- ja rakennustoimialla tarkoitetaan kiinteistön ostoa, myyntiä, vuokrausta, rakennuttamista, muutos-, laajennus- tai ylläpitotyötä.

2.1.2 Kiinteistö- ja rakennustoimialan erityispiirteistä

Kiinteistö- ja rakennustoimialaa voidaan pitää erittäin verkostoituneena alana, jossa on runsaasti toisten kanssa tekemisissä olevia organisaatioita ja yrityksiä. (Valtioneuvoston kanslia, 2020) Verkostoitumista voidaankin pitää yhtenä keskeisimpänä alan erityispiirteistä. Pelkästään rakennushankkeissa on lukuisia eri osapuolia kuten omistaja, rakennuttaja, käyttäjä, pääurakoitsija, suunnittelijat, urakoitsijat ja heidän aliurakoitsijansa, rakennustuote- ja materiaalitoimittajat sekä viranomaiset. Myös kiinteistön ylläpito- ja puhtaanapitopalveluissa näkyy runsas sidosryhmien käyttö lähtien siivoojista ja vartijoista aina eri järjestelmien ja laitteiden asentajiin sekä huoltohenkilöstöön. (Junnonen & Kankainen, 2022) Esimerkiksi Senaatti-kiinteistöjen työtehtävistä noin 90 % ostetaan toimittajakumppaneilta (Senaatti-kiinteistöt, 2021). Valtioneuvoston kanslian (2020) tutkimusraportin mukaan verkostoitumisesta huolimatta alalle ei ole kuitenkaan syntynyt tiiviitä toimittaja- ja verkostosuhteita kuten valmistavassa teollisuudessa. Tämä johtuu vakiintuneesta käytännöstä hankekohtaisesta hankintojen kilpailutuksesta. Kilpailutuksien myötä osapuolet voivat vaihtua jokaisessa hankkeessa, jolloin rakennuksiin, toimitiloihin ja niiden käyttöön liittyvät tiedot leviävät laajalle.

Toinen keskeisimmistä erityispiirteistä on alan projektiluonteisuus. Suurin osa kiinteistö- ja rakennusalan töistä muodostuu erilaisista projekteista ja hankkeista. Myös Junnosen & Kankaisen (2022) mukaan alalle on tyypillistä hanketasolla toiminnan kertaluonteisuus ja osapuolten jatkuva vaihtuminen. Tätä tukevat myös Peltonen & Kiiras (1998, 32–35), joiden mukaan hankkeet ovat usein monisyisiä ja pitkiä prosesseja vaatien suuria määriä toimijoita eri aloilta ja tahoilta. Tämä edellyttää hajautettujen toimintojen hyvää hallintaa. Alla on listattuna Peltosen & Kiiraksen (1998, 32) kuvaamat rakennustoiminnan erityispiirteet:

- ”Rakennushankkeissa päätäntä on jakautunut rahoittajille, rakennuttajalle, suunnittelijoille, paikallisille viranomaisille sekä urakoitsijoille.
- Suunnittelu- ja rakennustiimit kootaan jokaiseen hankkeeseen erikseen, eivätkä osapuolet ole tottuneet toimimaan yhdessä.
- Jokainen hanke suunnitellaan erikseen.

- Rakennusprojektin toteuttamiseen tarvitaan paljon käsityötä, jossa on aina omat riskinsä verrattuna esimerkiksi tehdasteollisuuteen.
- Toiminta on hajotettu useisiin tilapäisiin kohteisiin.
- Rakennusprosessin pituus ja jokaisen hankkeen ainutkertaisuus vaikeuttavat saatujen kokemusten ja palautteen hyödyntämistä jatkossa."

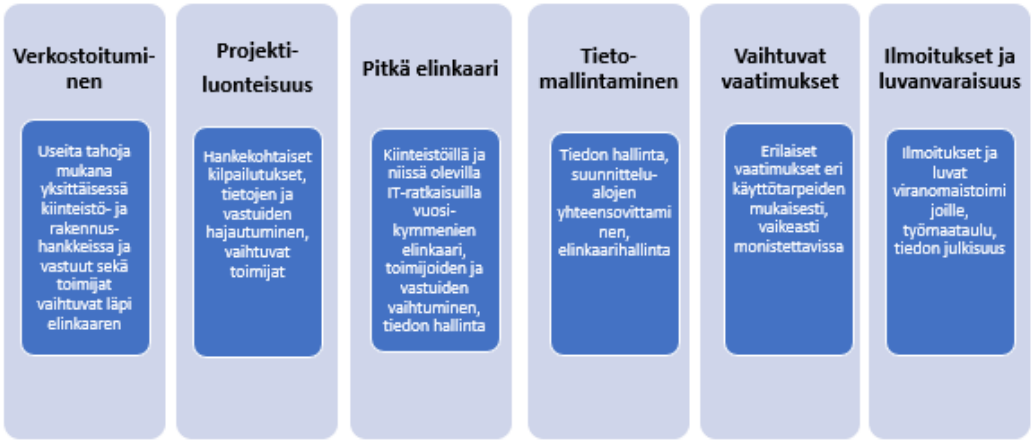
Edellä mainittujen erityispiirteiden lisäksi on huomioitava rakennuksien pitkä elinkaari, mikä muodostuu kolmesta päävaiheesta: rakentamisesta, käyttövaiheesta ja purkaminen. Rakennuksen käyttövaihe vaihtelee kymmenistä vuosista satoihin vuosiin. (Rakennusteollisuus, 2022) Käyttövaiheen aikana on huomioitava rakennuksen ylläpito, huollot ja korjaukset sisältäen talotekniset järjestelmät sekä niihin liittyvät tiedonsiirtoyhteydet. Sähkötieto Ry:n (2022) mukaan tiedonsiirtoa hyödyntävien järjestelmien määrä rakennuksissa on kasvanut viime vuosien aikana ja kasvu vain voimistuu tulevaisuudessa. Taloteknisten järjestelmien ohjaukseen ja säätämiseen käytettävissä rakennusautomaatiojärjestelmissä hyödynnetään yhä yleisemmin tietoverkkoja sekä järjestelmän sisäiseen tiedonsiirtoon että ulkoisen etähallinnan mahdollistamiseen. Yhtenä syynä digitalisaation hyödyntämisessä koko rakennuksen elinkaaren aikana on pyrkimys kustannustehokkuuteen, tuottavuuden kasvuun ja ympäristökuormituksen vähentämiseen (EUBIM Taskgroup, 2018; Rakennusteollisuus, 2022;). Taulukossa 1 on esitetty talotekniset järjestelmät kolmeen pääkategoriaan jaettuna: LVI-, sähkö- ja sähkötekniset tietojärjestelmät. Näiden järjestelmien toimivuudella on merkittävä vaikutus rakennuksen käytön aikaisen toiminnallisuuden varmistamisessa. (Rakennustietosäätiö ym., 2002; Rakennustietosäätiö, 2011)

Taloteknisten järjestelmien digitalisoitumisen lisäksi tietomallintaminen on ollut yhtenä keskeisessä roolissa kiinteistö- ja rakennustoimialan digitaalisessa murroksessa (EUBIM Taskgroup, 2018). Tietomallintamisen lopputuloksena syntyy digitaalisessa muodossa oleva havainnollistava kuvaus rakennetun kohteen toiminnallisista ja fyysisistä ominaisuuksista koko rakennuksen elinkaaren ajalta. (Jäväjä & Lehtoviita, 2016) Tietomalleja on sisällöltään ja käyttötarkoitukseltaan useita erilaisia. Esimerkiksi yhdistelmämallissa yhdistellään eri suunnittelualojen tuottamia tietomalleja ja tehdään yhteensopivuustarkasteluita muun muassa rakenteiden ja järjestelmien tilatarpeiden osalta. (Henttinen, 2012) Tietomalleja voidaan hyödyntää niin rakennetun ympäristön kunnostamisessa, ylläpidossa kuin niihin liittyvässä eri osapuolten välisessä yhteistyössä, muutosten hallinnassa, että päätöksenteossa. Tietomallintaminen mahdollistaa suurten datamäärien käsittelyn ja hallinnan. (Jäväjä & Lehtoviita, 2016; EUBIM Taskgroup, 2018) Sen merkittävyys korostuu erityisesti kiinteistö- ja rakentamisalalla ja se nähdään tässä tutkielmassa yhtenä alan erityispiirteenä.

TAULUKKO 1 Talotekniset järjestelmät kategorioittain

LVI-perusjärjestelmät	**Sähköjärjestelmät**	**Sähkötekniset tietojärjestelmät**
Lämmitysjärjestelmät	Sähkön pääjakelujärjestelmät	Automaatiojärjestelmät
Ilmastointijärjestelmät	Sähkönliitäntäjärjestelmät	Puhelinjärjestelmät
Vesi- ja viemärijärjestelmät	Valaistusjärjestelmät	Viestintäjärjestelmät
Jäähdytysjärjestelmät	Sähkölämmitysjärjestelmät ja -laitteet	Merkinantojärjestelmät
Palontorjuntajärjestelmät		Sähköiset turvallisuusjärjestelmät
Väestönsuojien LVI-järjestelmät		Tietoverkkojärjestelmät
		Integroidut järjestelmät

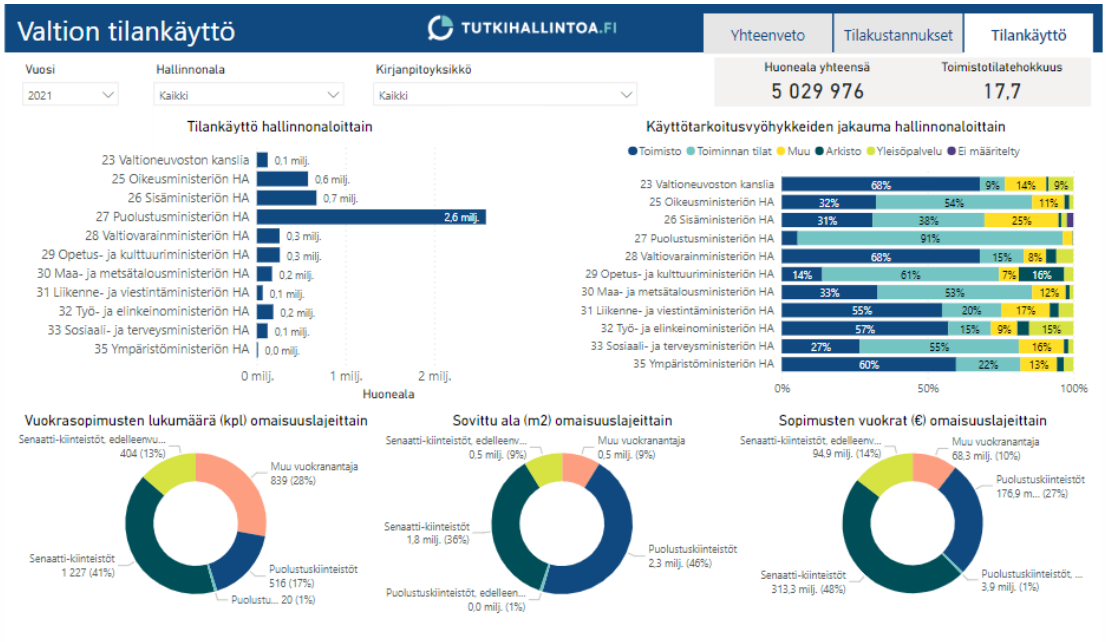
Kiinteistö- ja rakennustoimiala on myös hyvin pitkälti luvanvaraista toimintaa. Lähes poikkeuksetta on haettava esimerkiksi rakennuslupaa tai toimenpidelupaa kunnan rakennusvalvontavirastosta ennen rakennustöiden aloittamista. Oli kyseessä sitten uudisrakentaminen tai korjaus- ja muutostyöt. Lupien lisäksi on tehtävä eri viranomaisille tiedonantoilmoituksia kuten työmaan aloitusilmoitus, urakkatietojen ja työmaalla työskentelevien henkilöiden ilmoittaminen. (Maankäyttö- ja rakennuslaki, 1999) Näiden lisäksi rakentajan on pystytettävä työmaataulu, jossa pitää kertoa suomeksi ja ruotsiksi työn kohde, osoite, rakennushankkeeseen ryhtyvä yhteystietoineen sekä kohteen aloittamis- ja arvioitu valmistumisajankohta (Helsingin kaupunki, 2019). Luvanvaraisen toiminnan takia rakennushankkeisiin liittyviä piirustuksia ja lupa-asiakirjoja voi pyytää määritellyin ehdoin rakennusvalvonnasta. Myös johtojen ja kaapeleiden sijaintitietoja voi tiedustella kaupunkien johtotietopalveluiden tai Erillisverkkojen ylläpitämästä Johtotietopankista. (Helsingin kaupunki, 2022; Johtotietopankki, 2022) Kuviossa 1 on koottuna yhteenveto edellä kuvatusta kiinteistö- ja rakennustoimialan erityispiirteistä. Erityispiirteet linkittyvät toisiinsa ja kuvastavat kokonaisuudessaan kiinteistö- ja rakennustoimialan monimuotoisuutta.



KUVIO 1 Kiinteistö- ja rakennustoimialan erityispiirteitä

2.1.3 Suomen valtion omistama kiinteistökanta ja niiden hallinta

Valtiovarainministeriön (2021) mukaan Suomen valtiolla on omistuksessaan noin 9000 rakennusta, joiden kiinteistöomaisuuden arvo noin 4,2 miljardia. Kaikkiaan erilaisia toimitiloja on vajaat kuusi miljoonaa neliömetriä. Näistä viidennes on toimistotilaa ja loput erilaisia toiminnon tiloja kuten laboratorioita, poliisilaitoksia, oikeussaleja, museoita ja erilaisia varastoja. Puolustusvoimien käytössä on lähes puolet kokonaisneliömäärästä. Kuviossa 2 on graafisessa muodossa hallinnonaloittain tilojen jakauma käyttötarkoituksineen. Valtion kiinteistötiedot perustuvat Senaatti-kiinteistöjen Hallinnan tilahallinnan (HTH) -tietopalvelun tietoihin, jotka ovat julkisesti saatavilla Valtiokonttorin ylläpitämästä ”tutkihallintoa.fi”-sivuston kautta, jossa kootaan yhteen osoitteeseen tietoa kuntakentän ja valtionhallinnon tiedoista.



KUVIO 2 Valtion tilankäyttö

Senaatti-kiinteistöt vastaa valtion kiinteistöomaisuuden hallinnasta, kehittämisestä ja valtiolle tarpeettoman tilan myynnistä. Lisäksi Senaatti-kiinteistöt toimii valtion tilahankintayksikkönä. Tiloja voidaan vuokrata joko valtion tai ulkopuolisen vuokranantajan tiloista kuten kuvion 2 vuokrasopimuksen omaisuuslajeista nähdään. Puolustuskiinteistöt toimii puolestaan tilanhankintayksikkönä Puolustusvoimille ja tukee Puolustusvoimien valmiutta, varautumista ja turvallisuutta toimitilojen tarjoaman suojan ja käytettävyyden kautta. (Valtiovarainministeriö, 2022; Valtioneuvosto, 2021) Molemmat liikelaitokset tuottavat myös rakennuttamiseen ja peruskorjaukseen liittyviä palveluita. Nämä kaksi liikelaitosta muodostavat Senaatti-konsernin, jonka tehtävänä on tuottaa kiinteistö- ja tilapalveluita, tilajohtamisen ja -hallinnon palveluita sekä tilojen hankintaan, hallinnointiin ja luovuttamiseen liittyviä palveluita valtion virastoille ja laitoksille (Laki Senaatti-kiinteistöistä ja Puolustuskiinteistöistä 1018/2020). Tämän tutkimuksen tarkastelun keskiössä on Senaatti-konserni ja sen omistama kiinteistökanta Suomessa.

2.2 Tiedustelun määritelmästä

Lähdekirjallisuuden mukaan ei ole olemassa yksiselitteistä määritelmää mitä tarkoitetaan organisaatioihin ja yrityksiin liittyvällä tiedustelutoiminnalla. Useamman lähteen perusteella voidaan todeta, että tiedustelu on jokapäiväistä, jatkuvaa, laaja-alaisesti monilla eri sektoreilla ja keinoilla tapahtuvaa tiedon hankintaa, keräämistä ja analysointia. Sen avulla tuotetaan varmistettua ja ennakoivaa tietoa valitusta kohteesta sekä toimintaympäristöstä niin operatiivisen kuin strategisen päätöksenteon tueksi. Tiedustelun tavoitteena on tuottaa analysoitua tietoa päättäjille oikea-aikaisesti mahdollisista toimeksiantajaa kohtaavista uhkista tai mahdollisuuksista, jotka se voi ottaa huomioon päätöksenteossa varmistaen toimintansa jatkuvuuden tai vahvistaen omaa asemaansa suhteessa muihin kilpaileviin toimijoihin. (Lowenthal (2002); McDowell, 2009; Kupcikas, 2013)

Lowenthalin (2002) mukaan tiedustelu on olemassa, koska hallitukset pyrkivät salaamaan joitakin tietoja muilta hallituksilta, jotka puolestaan yrittävät löytää salattua tietoa salatuin keinoin. Tämä sama väittämä pätee yhtä hyvin myös muihin organisaatioihin ja yksityisiin yrityksiin. Jokaisella organisaatiolla on tietoa, joka voidaan luokitella kolmeen pääkategoriaan: julkiseen tietoon, harmaaseen tietoon, mikä on tarkoitettu vain rajatulle henkilöryhmälle ja salassa pidettävään tietoon. Näitä tietoja hankintaan tiedustelun keinoin. (Elinkeinoelämän keskusliitto, 2017) Tässä tutkielmassa tiedustelu jaetaan lailliseen tiedusteluun ja laittomaan tiedusteluun eli yritysvakoiluun, jolla pyritään hankkimaan erityisesti toisen organisaation salassa pidettävää tietoa. Seuraavassa luvussa tarkastellaan tarkemmin mitä yritysvakoilulla tarkoitetaan.

2.2.1 Yritysvakoilu

Kuten edellä on todettu yrityksiin ja organisaatioihin kohdistuvaa tiedonhankintaa voidaan pitää yleisenä jokapäiväisenä tapahtumana. Tietoa voidaan hankkia muun muassa yrityksen tai organisaation julkisista tietolähteistä, joista saa talouteen, organisaatioon, henkilöstöön, strategiaan, palveluihin ja järjestelmiin liittyvää tietoa suhteellisen kattavasti. Lisäksi tietoa voidaan hankkia markkinointikatsauksista ja avoimista kaupallisista tutkimuksista. Avoin tieto toimii myös hyvänä kanavana vakoilutarkoituksiin. Käytännössä voi olla välillä vaikeaa hahmottaa mikä on laillista ja mikä laitonta tiedon keräämistä. Myös tietojen keräämisen valvonta on haastavaa. Oleellista on kuitenkin millä keinoin ja mihin tarkoitukseen tietoa käytetään. (Cyberwatch & Elinkeinoelämän keskusliitto, 2018)

Kun toisen omistuksessa olevaa tietoa hankitaan oikeudetta, kyseenalaisin tai laittomin keinoin, kutsutaan sitä pääsääntöisesti vakoiluksi tai yritysvakoiluksi. Kirjallisuuslähteiden perusteella englannin kielellä vastaavaa toimintaa voidaan kuvata useilla termeillä kuten ”corporate espionage”, ”industrial espionage”, ”economic espionage” ja ”business espionage”, riippuen siitä mihin vakoilutoimenpiteitä kohdistetaan. Tässä tutkielmassa määritelmä perustuu Suomen lakiin ja kohteena voi olla julkishallinnon organisaatio tai yksityinen yritys, koska kiinteistö- ja rakentamistoimialalla molemmat sektorit tulee huomioida tämän tutkimuksen aiheessa, vaikka keskiössä tarkastellaankin valtion omistamaa kiinteistökantaa.

Suomen rikoslain (578/1995) mukaan vakoiluksi luetaan teko, jossa vierasta valtiota hyödyntääkseen tai Suomea vahingoittaakseen hankkii tiedon sellaisesta Suomen maanpuolustusta tai muuta poikkeuksellisiin oloihin varautumista, Suomen ulkomaansuhteita, valtiontaloutta, ulkomaankauppaa tai energiahuoltoa koskevasta taikka muusta niihin rinnastettavasta, Suomen turvallisuuteen vaikuttavasta seikasta, jonka tuleminen vieraan valtion tietoon voi aiheuttaa vahinkoa Suomen maanpuolustukselle, turvallisuudelle, ulkomaansuhteille tai kansantaloudelle. Yritysvakoiluksi luetaan puolestaan teko, jossa oikeudettomasti hankitaan toiselle kuuluvaa liikesalaisuutta, tunkeudutaan ulkopuolisilta suljettuun paikkaan taikka tietojärjestelmään, hankitaan haltuunsa tai jäljennetään asiakirjan tai muun tallenteen taikka muulla siihen rinnastettavalla tavalla tai käyttämällä teknistä erikoislaitetta (Rikoslaki 605/2018).

Kehittyneissä tietoyhteiskunnissa vakoilun menetelmät ovat muuttaneet muotoaan. Niin valtiollista vakoilua kuin yritysvakoilua tehdään yhä enemmän kyberympäristössä, tietoverkkoja ja niihin liitettyjä laitteita sekä ohjelmistoja hyödyntäen. Tätä oikeudettomasti ja laittomasti tehtävää tiedonkeruuta kyberympäristössä kutsutaan yleisesti kybervakoiluksi. Suomessa kybervakoilu on kansallisen lainsäädännön mukaan pääsääntöisesti lainvastaista toimintaa, vaikka sitä ei sellaisenaan tunneta rikoslaissa. (Turvallisuuskomitea, 2018, 26) Tässä tutkielmassa kybervakoilu on osa yritysvakoilua.

Kybervakoilun, jossa luvatta käytetään tai murtaudutaan toisen omistamaan tietojärjestelmään tai laitteeseen, voidaan yleisesti katsoa kuuluvan kyberrikollisuuden kontekstiin. Kyberrikollisuus määritellään Euroopan komissiossa (Euroopan komissio, 2016) rikoksiksi, jotka tehdään sähköisiä viestintäverkkoja

ja tietojärjestelmiä käyttäen. Kyberrikollisuus voidaan komission mukaan luokitella kolmeen alaryhmään, jossa ensimmäinen kattaa perinteiset rikollisuuden muodot, jotka on tehty käyttäen sähköisiä viestintäverkkoja ja tietojärjestelmiä. Toiseen ryhmään kuuluu laittoman sisällön julkaiseminen sähköisissä viestimissä ja kolmas ryhmä kattaa rikokset, joita esiintyy ainoastaan sähköisissä verkoissa, kuten hyökkäykset tietojärjestelmiä vastaan, palvelunesto ja hakkerointi. On kuitenkin huomioitava, että kyberrikollisuus käsitettä ei tunneta Suomen rikoslaissa ja termiä käytetään lähinnä kattoterminä kaikelle verkkovälitteiselle rikollisuudelle ja rikoskäyttäytymiselle. (Niemi, 2017)

Weissbrodtin (2013) mukaan kybervakoilu tulee ottaa vakavana uhkana, koska siinä on aiempaa suurempi kapasiteetti käsitellä ja analysoida kerättyä tietoa. Myös kiinnijäämisen riski on muihin keinoihin nähden pienempi ja voitonmahdollisuudet suuret. Kybervakoilu on valtioiden rajat ylittävää, kansainvälistä ja vakoojan löytäminen sekä riittävän näytön todentaminen on vaikeaa. Sitä voidaankin pitää matalariskisenä ja kustannustehokkaana vakoiluoperaationa. (Weissbrodt, 2013; Gunneriusson & Ottis, 2013)

Myös Cyberwatch Finland (2021) mukaan kybervakoiluun liittyvien operaatioiden valmistelua on useimmiten vaikea havaita ja toimijoiden jäljittäminen on aikaa vievää sekä haastavaa. Kybervakoilussa hyökkääjän tavoitteena onkin pyrkiä olemaan kohdejärjestelmässä mahdollisimman huomaamattomana ja pitkäaikaisesti keräten tietoja organisaation toiminnasta.

Kybervakoilua harjoittavat toimijat voivat toimia teknisiä laitteita ja tietoverkkoja hyödyntäen kansallisista rajoista, etäisyyksistä ja sijainneista välittämättä. Tekijät voivat olla niin yksittäisiä hakkereita tai ryhmittymiä, järjestäytynyttä rikollisuutta tai valtioiden ja yrityksien toimeksiannosta toimivia vakoilijoita. (Enisa, 2020) Erilaisia hybridi- ja kyberoperaatioita edeltää yhä useammin kybervakoilu. Tarkoituksena on luoda edellytykset muille operaatioille ja täydentää muita vakoilun sekä tiedonhankinnan menetelmiä. Vakoilun kokonaiskapasiteetin on todettu useiden lähteiden mukaan kasvaneen viimeisten vuosien aikana. (Cyberwatch Finland, 2021) Suomessa kybervakoilu on sekä laaja-alaista että systemaattista toimintaa ja se voi kohdistua kaikkiin yhteiskunnan toimijoihin. (Suojelupoliisi, 2018)

2.2.2 Yritysvakoilun motiivit ja kohteet

Yleisimmin yritysvakoilun motiiveina ovat taloudellinen hyöty, tiedon saanti, poliittiset motiivit, yhteiskunnallinen tai ideologinen vaikuttaminen. Yritysvakoilun tavoitteena on pääsääntöisesti hankkia salassa pidettävää tietoa, jolla tekijä voi parantaa oman valtionsa tai tietyn yrityksen asemaa globaalissa kilpailussa tai kaventaa kohteena olevan valtion tai yrityksen liikkumatilaa. (Suojelupoliisi, 2021) Suojelupoliisin (2018) mukaan poliittisesti motivoituneessa yritysvakoilussa tavoitteena on kerätä poliittisen päätöksenteon kannalta kriittistä ja salassa pidettävää tietoa. Tällaista tietoa voi olla esimerkiksi ulko- ja turvallisuuspoliittista päätöksentekoa koskeva tieto, johon kohdistui Suomessa vuonna 2020 koronatilanteen vuoksi poikkeuksellisen voimakasta valtiollista kybervakoiluyritystä. Näissäkin tapauksissa kohteena voivat olla julkishallinnon

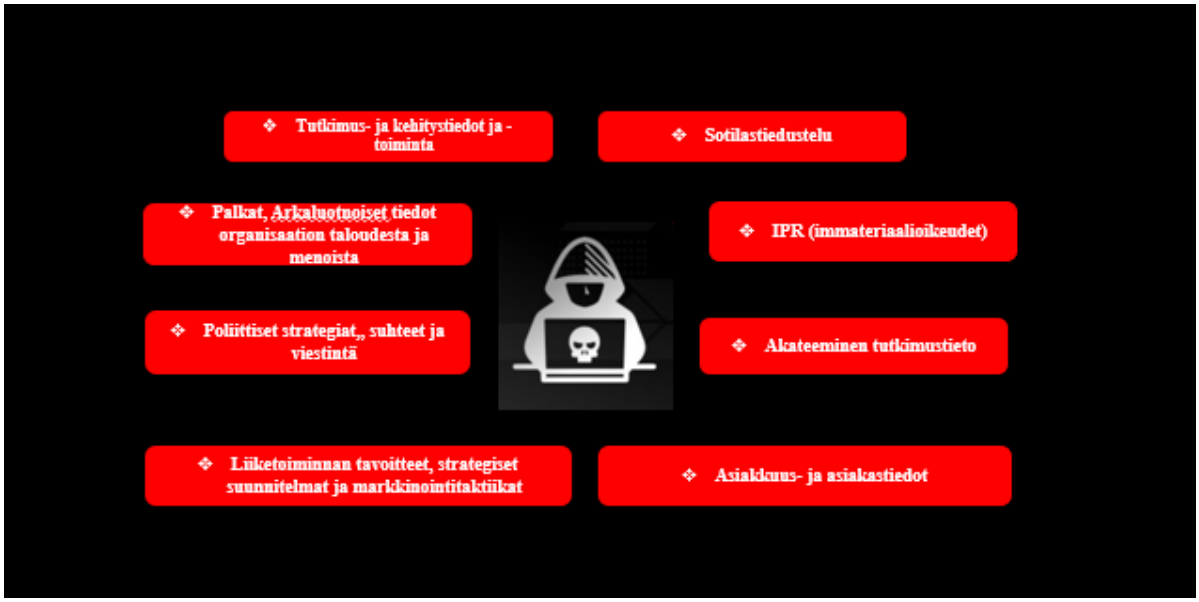
organisaatioiden lisäksi myös yritykset, joiden kautta haluttuihin tietoihin pyritään pääsemään välillisesti. Tämä tarkoittaa sitä, että yritysvakoilua ei kohdisteta välttämättä suoraan pääkohteena olevaan organisaation, vaan sen lähellä oleviin henkilöihin ja yrityksiin, jotka eivät ole asiaan välttämättä varautuneet ja tiedostaneet tietoturvan merkitystä vastaavasti kuin varsinainen pääkohde. Yhä useampi yritys ja organisaatio ovat ulkoistaneet ydintoimintojen ulkopuolelle lukeutuvia palveluja kuten tietojärjestelmiensä ylläpidon ja kiinteistöjen huolto- ja ylläpitotyöt palveluntarjoajille. Molemmilla tahoilla on työtehtäviensä puolesta laajat pääsyoikeudet useisiin tiloihin ja tietoverkkoihin. Salassa pidettävästä tiedosta kiinnostuneille tunkeutujille nämä tahot ovat kullanarvoisia. Yrityksien toiminnan jatkuvuuden kannalta tämä on huomionarvioinen havainto ja se on hyvä tiedostaa. (Viestintävirasto, 2017) Yritysvakoilulla loukataan usein myös kohdevaltion väestön perusoikeuksia kuten oikeutta luottamukselliseen viestintään ja yksityisyyteen. Tällaisissa tilanteissa, joissa loukataan toisen valtion suvereniteettia, toimijoina ovat yleensä autoritääriset valtiot kuten Kiina ja Venäjä, jotka harjoittavat vakoilua muun muassa Suomea vastaan. (Suojelupoliisi, 2021; Suojelupoliisi, 2020)

Yritysvakoilua voidaan käyttää myös sotilasoperaatioiden yhteydessä tai terrorismin toimena. Pahimmillaan yritysvakoilun vaikutukset voivat johtaa ihmishenkien menetyksiin, julkisten palveluiden ja infrastruktuurin häiriintymiseen, etenkin silloin kun se on osa laajempaa sotilaallista tai poliittista kampanjaa. Tulevaisuudessa tällaisissa tapauksissa kohteena voivat olla yhä useammin ne tahot, joiden omistuksessa ja operoinnissa on Suomen yhteiskunnalle kriittistä infrastruktuuria. (Cyberwatch & Elinkeinoelämän keskusliitto, 2018) Tähän kohdejoukkoon voidaan lukea myös kiinteistö- ja rakennusalan toimijat, jotka omistavat, rakentavat ja ylläpitävät kriittisiä kohteita ja niissä olevaa infrastruktuuria.

Erityisesti kybervakoilulle on tyypillistä kohdennetut hyökkäykset, joita voidaan toteuttaa yksittäisiä henkilöitä kuten merkittäviä poliittisia johtajia, virkamiehiä, yritysjohtajia tai yrityksessä toimivia asiantuntijoita ja muita tarkoitukseen tarvittavia henkilöitä vastaan. Hyökkäyksen kohteesta voidaan kerätä tietoja jopa vuosia ennen kuin varsinaiseen tietomurtoon edetään. (Viestintävirasto, 2017; Sisäministeriö, 2017) Kohdennetut hyökkäykset ovat lisääntyneet viime vuosien aikana ja niiden takana ovat pääsääntöisesti yritys- tai valtiojohtoinen toimija. Arvokkaan ja salassa pidettävän tiedon keräämisen lisäksi, pyrkimyksenä voi olla vaikuttaa kohteena olevan henkilön ja organisaation toimintaan tekijälle suotuisalla tavalla. Joissakin tapauksissa loukkauksen tarkoituksena on yksinkertaisesti vahingoittaa kohteen mainetta ja brändiä paljastamalla yksityisiä tietoja tai kyseenalaisia liiketoimintakäytäntöjä. (Euroopan tilintarkastus tuomioistuin, 2019)

Kuten aiemmin on todettu yleisimpiä yritysvakoilun kohteita ovat suuret yritykset ja valtion organisaatiot. Näiden lisäksi mikä tahansa yritys, yliopisto, ajatushautomo tai muu organisaatio, jolla on pääsy tietoon, tietojärjestelmiin tai omistuksessa arvokasta tietoa, jonka avulla voidaan luoda kilpailuetua suoraan tai välillisesti toiselle organisaatiolle tai valtiolle voivat joutua yritysvakoilun kohteeksi. Tietoturvayritys Crowdstrike (2021) on kuvannut (Kuvio 3) yleisimpiä

kybervakoilun tietoresursseja, joihin vakoilija pyrkii useimmiten pääsemään käsiksi. Näitä ovat muun muassa tutkimus- ja kehitystiedot, huipputeknologia, sotilastiedustelu, tuotekehitykseen liittyvät suunnitelmat, rakennesuunnitelmat, immateriaalioikeuksiin liittyvät tiedot kuten tuotekaavat tai suunnitelmat, arkaluontoiset taloustiedot ja palkat, asiakkuus- ja asiakastiedot sekä maksurakenteet, yrityksen liiketoiminnan tavoitteet, strategiset suunnitelmat ja markkinointitaktiikat.



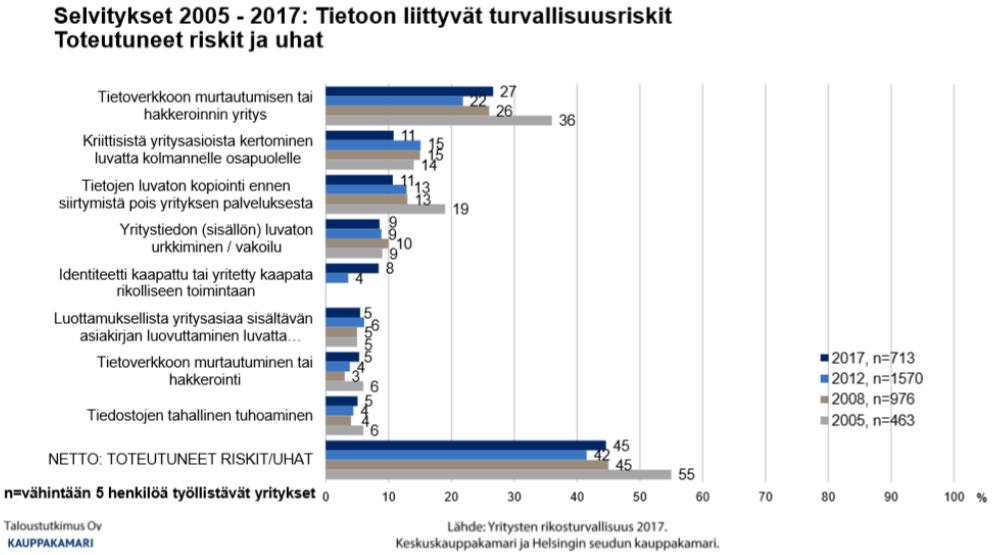
KUVIO 3 Esimerkkejä kybervakoilun kohteista

Vastaavanlaiset yritysvakoilun mielenkiinnon kohteet tulivat ilmi myös Helsingin seudun kauppakamarin Yritysvakoilu 2021 -selvityksessä, mikä perustuu 192 suomalaisen yrityksen vastauksiin. Näiden lisäksi vakoilijaa kiinnostaa poliittiset strategiat sekä niihin liittyvät suhteet ja viestintä sekä yrityksen mahdollinen linkittyminen yhteiskunnan kriittiseen toimintaan. (Helsingin seudun kauppakamari, 2021)

Yrityksiin kohdistuvien yritysvakoiluoperaatioiden osalta on saatavilla heikosti tilastointia. Yhtenä syynä tähän on se, että yrityksissä pelätään negatiivista julkisuutta ja epäilystä ei raportoida poliisiviranomaiselle tai yleensäkään ulkopuolelle ollenkaan. Toiseksi osa ei luota viranomaisen kykyyn pitää asiaa luottamuksellisena tai kykyyn tutkia asiaa. Ilmoittamisen hyötyä ei myöskään nähdä, vaikka se parantaisi tilannekuvaa ja toimivaltaisen viranomaisen olisi helpompi ratkaista tapauksia. (Korva-Perämäki, 2017) Toukokuussa 2018 voimaan tullut EU:n tietosuojadirektiivi tulee kuitenkin muuttamaan tätä tilannetta osittain, kun direktiivi pakottaa ilmoittamaan tiettyjä internetissä toimivia palveluntarjoajia tietomurroista tietosuojaviranomaiselle ja asiakkailleen (GDPR, 2016).

Yrityksiin kohdistuvaa vakoilua on pyritty myös selvittämään yrityskyselyiden perusteella. Kauppakamari julkaisee muutaman vuoden välein tehdyn Yritysturvallisuus kyselyn, jossa kartoitetaan muun muassa yrityksien tietopääomaan kohdistuvia toteutuneita turvallisuusriskejä alla olevan Kuvion 4

mukaisesti. Kyselyyn osallistuvien yrityksien antamista vastauksista suurimpana riskinä koetaan tietoverkkoon murtautuminen tai hakkeroinnin yritys. (Keskuskauppakamari, 2017) Vuoden 2021 tehdyssä Yritysvakoilu -selvityksessä (Helsingin seudun kauppakamari, 2021) yli puolet kaikista (191) vastaajista pitivät kybervakoilua yleisimpänä yrityksiin kohdistuvana vakoilun keinona ja toiseksi yleisempänä viestinnän laitonta sieppausta (puhelut, sähköposti, muut viestit), mikä toisaalta voidaan lukea kuuluvan osaksi kybervakoilua. Seuraavassa luvussa tarkastellaan tarkemmin yritysvakoilussa käytettäviä keinoja ja menetelmiä, joita kiinteistö- ja rakennustoimialalla toimivat voivat kohdata.



KUVIO 4 Yritysturvallisuus kyselyn vastauksien vertailut eri vuosilta

2.2.3 Tiedustelulajit; keinot ja menetelmät yritysvakoilussa

Edellisen luvun perusteella voidaan todeta, että yritysvakoilun keskeisimpänä tavoitteena on hankkia tietopääomaa, jonka avulla toimeksiantaja voi parantaa omaa asemaansa, edistää tavoitteitaan tai heikentää kohteena olevan liikkumatilaa tai kilpailuetua. Tietopääoma voi sijaita dokumentteina ja objekteina fyysisessä tilassa, ajatuksina ja tietotaitona ihmisten kognitiivisessa tietoisuudessa tai datana tietojärjestelmissä. Meretvuon (2021, 39) mukaan vakoilun voidaan katsoa toteutuvan kolmessa ulottuvuudessa: fyysisessä tilassa, sosiaalisessa tilassa ja kybertilassa. Kiinteistö- ja rakentamistoimialalla tätä kolmijakoa voidaan soveltaa Valtion toimitilastrategian mukaisesti fyysisen, sosiaalisen ja digitaalisen toimintaympäristön näkökulmasta. Edellä mainitut ulottuvuudet limittyvät toisiinsa ja yritysvakoilussa tietopääomaa voidaan hankkia monin eri keinoin yhden tai useamman toimintaympäristön elementtejä hyödyntäen. Yritysvakoilussa keinot ja menetelmät voivat olla tiedustelutoiminnassa käytettävien eri tiedustelulajien kaltaisia riippumatta siitä, onko tekijä yritys vai valtiollinen toimija. (Elinkeinoelämän keskusliitto, 2017)

Tiedustelulajilla tarkoitetaan määriteltyä tiedon hankinnan tapaa. Tiedustelulajien menetelmiä voidaan tarpeen mukaisesti yhdistää tai käyttää pelkästään yhtä menetelmää, mikäli sillä saavutetaan haluttu tulos. Se missä laajuudessa tiedustelulajeja ja menetelmiä yritysvakoiluoperaatiossa käytetään, riippuu siitä, onko toteuttavana osapuolena vieras valtio, muu organisaatio vai yksittäinen henkilö tai ryhmittymä. Valtiollisilla toimijoilla on huomattavasti laajemmat resurssit käytettävissään kuin esimerkiksi yksittäisillä yrityksillä. (Puolustusvoimat, 2021)

Tiedustelutoiminnan menetelmiä on vuosien varrella kehitetty tiedon hankkimiseksi ja analysoimiseksi. Tässä tutkielmassa tarkastellaan Lowenthalin ja Clarken (2015) jaon mukaisesti tiedustelulajien viittä päälajia, joita pidetään alan tutkimuskirjallisuuden mukaan klassisina tiedustelulajeina. Nämä päälajit ovat lueteltuna alla. Luettelossa tiedustelulajit ovat sekä suomeksi että englanniksi, koska tiedustelulajien englanninkieliset lyhenteet ovat vakiintuneet jo länsimaissa käytännöksi.

- Henkilötiedustelu (engl. Human Intelligence, HUMINT)
- Signaalitiedustelu (engl. Signals Intelligence, SIGINT) (ml.Kyber)
- Geotiedustelu eli paikka- ja olosuhdetiedustelu (engl. Geospatial Intelligence, GEOINT)
- Mittaus- ja tunnusmerkkitiedustelu (engl. Measurement and Signatures Intelligence, MASINT)
- Avointen lähteiden tiedustelu (engl. Open-Source Intelligence, OSINT)

Henkilötiedustelu (HUMINT) ja siinä käytettävät menetelmät ovat vanhin tiedonkeräyksen muoto, jossa tiedot saadaan suoraan henkilölähteeltä. Yhdysvaltojen kansallisen tiedusteluoppaan (2009) mukaan näillä lähteillä on yleensä pääsy sellaiseen tietoon, jota ei ole saatavissa muilla keinoilla. Tietojen saanti henkilöiltä voi olla toisinaan helpompaa kuin murtautuminen esimerkiksi tiloihin tai tietojärjestelmiin. Henkilötiedustelu on ainut tiedustelulaji, jossa tiedon kerääjät kommunikoivat suoraan tietolähteen kanssa, pyrkien hallitsemaan kommunikoinnin aihetta ja ohjaamaan lähteen toimintaa.

Henkilötiedustelun kohteeksi voi valikoitua niin valtion virkamies kuin yrityksen tai sen alihankkijan työntekijä, jolla on tietoa tai pääsy tietoon, tilaan tai tietojärjestelmään tai hänen kauttaan pyritään vaikuttamaan asiaan mikä hyödyntää tekijätahoa. Kohdehenkilö ei välttämättä edes ymmärrä auttavansa ulkopuolista tahoa tai luovuttavansa organisaationsa salassa pidettävää tietoa ulkopuoliselle taholle. Tekijä pyrkii käyttämään kohdehenkilön luottavaisuutta hyväkseen ja manipuloimaan hänen toimintaansa. Apunaan tekijä käyttää avoimesti julkisista lähteistä ja sosiaalisesta mediasta keräämiään tietoja kohdehenkilöstä, hänen elämäntilanteestaan (taloustilanne, ihmissuhteet, päihderiippuvuus/väärinkäyttö), työpaikastaan (asema, suhde työnantajaan), työskentelytiloista, työtehtävistä, kollegoista, kaveripiiristä ja harrastuksista. (Elinkeinoelämän keskusliitto, 2017)

Muihin tiedustelulajeihin verrattuna henkilötiedustelu on riskialtis ja aikaa vievä menettely tiedon keräämiseksi. Kaminski (2019) korostaakin, että

arvokkaan henkilölähteen saaminen on monimutkainen operaatio. Voi kestää vuosia luoda luotettava ja tuottava yhteys. Hänen mukaansa henkilölähteiden käyttö vaatii erityistä varovaisuutta ja siihen liittyy valtava riski. Muun muassa vastatiedustelupalveluiden paljastamia henkilöitä voidaan syyttää vakoilusta, jolloin vaarana on pitkät vankeusrangaistukset tai pahimmillaan kuolemantuomio. Lisäksi henkilötiedustelua suorittavan on huomioitava, että hänen lähteensä voi osoittautua kaksoisagentiksi, joka työskentelee toiselle tiedustelupalvelulle. Henkilötiedustelua voivat tehdä kilpailevan yrityksen, rikollisorganisaation tai tiedustelupalveluiden edustajat peiteroolissa keräten tietoa salassa tai avoimesti esimerkiksi diplomaatin roolissa. (Wirtz & Rosenwasset, 2010)

Henkilön luovuttaessa yrityksen tai organisaation tietoa tietämättömyyttään, välinpitämättömyyttään tai tietoisesti joko omaehtoisesti, harhautetusti tai pakotetusti ilman tiedon omistajan lupaa, puhutaan **sisäpiiriuhkasta (engl. Insider Threath)**. Sisäpiiriuhka määritellään lähdekirjallisuuden mukaan yleisesti organisaation sisältä lähtöisin olevaan uhkaan, jossa tekijöinä voivat olla kaikki henkilöt (työsuhteiset, alihankkijat, urakoitsijat, liikekumppanit), joilla on valtuutettu eli laillinen pääsy organisaation resursseihin kuten kiinteistöihin, tiloihin, laitteisiin, tietojärjestelmiin, salassa pidettäviin tietoihin tai tietovarantoihin ja, jotka käyttävät niitä rikollisiin tai tahallisiin luvattomiin tekoihin tai edistää niiden suorittamista. Sisäpiiriläinen voi toimia yksin tai yhdessä muiden sisäpiiriläisten kanssa. (IAEA, 2020; NATO, 2015; Schultz, 2002;)

Yritysvakoilun keinoja ja niihin suojautumista tarkasteltaessa tulee kiinnittää huomioita miten tiedon luovuttaminen organisaation ulkopuolelle tapahtuu sisäpiiriläisen toimesta. Tekijä on voitu värvätä tai hänet on tarkoituksellisesti solutettu organisaatioon sisälle valtiollisen tiedustelupalvelun, rikollisjärjestön tai kilpailevan suuryrityksen toimesta (esimerkiksi kiristys, taloudellinen hyöty, ideologia) tai hän toimii itsenäisesti ajaen omia tarkoitusperiään (esimerkiksi taloudellisen hyödyn tavoittelu) tai hän tietämättömyyttään aiheuttaa toiminnallaan organisaatiolleen haittaa (esimerkiksi puutteellinen turvallisuustietoisuus). Sisäpiiriteossa voidaan hyödyntää eri tiedustelulajien menetelmiä tarkoituksen mukaisesti tavoitteen saavuttamiseksi. Lähdekirjallisuuden mukaan sisäpiiriläisen haitallisen teon käynnistämiseen on useita motiiveja kuten raha, ideologia, kosto, ego, pakottaminen tai näiden motiivien yhdistelmä. (Nasheri, 2005)

Wimmerin (2015) mukaan sisäpiiriuhka muodostaa yhden vakavimmista uhkista organisaation salassa pidettäville tiedoille sekä toimintojen jatkuvuudelle, ja siihen on vaikea varautua. Tätä väittämää vahvistavat myös Jalil ja Hassan (2020, 208), joiden mukaan tämä johtuu siitä, että sisäpiiriläiset tietävät ja ovat tietoisia organisaation politiikoista, menettelytavoista ja käytössä olevasta tekniikasta. He myös tietävät organisaation haavoittuvuuksista ja voivat ohittaa turvatoimenpiteet käyttämällä tietojaan sekä pääsyä organisaation omistamiin järjestelmiin. Tässä suhteessa sisäpiiriläisillä on merkittävä etu ulkopuolisiin tai ulkopuolisiin hyökkääjiin verrattuna. Myös IAEA (2020, 3–4) listaa kolme sisäpiiritekijöiden ominaisuutta, jotka tarjoavat etuja ulkopuolisiin tekijöiden nähden, kun he yrittävät tehdä haitallisia toimia:

1. Pääsy: Sisäpiiriläisillä on valtuutettu pääsy työnsä suorittamiseen tarvittaviin tiloihin, laitteisiin ja tietoihin. Pääsy sisältää fyysisen pääsyn kiinteistöihin; näihin liittyvät järjestelmät, komponentit ja laitteet; ja tietokonejärjestelmät sekä mahdollinen pääsy sensitiiviseen tietoon. Pääsyllä tarkoitetaan myös tietokoneiden etäpääsyä kiinteistössä oleviin järjestelmiin, kuten tietokonejärjestelmiin ja verkkoihin, jotka ohjaavat prosesseja, turvallisuutta, sisältävät sensitiivisiä tietoja. Kiinteistö- ja rakentamistoimialalla tämä voi näyttäytyä esimerkiksi pääsynä kriittistä infraa tuottavan kiinteistön tiloihin tai siellä oleviin taloautomaatiojärjestelmiin tai näitä koskeviin suunnittelutietoihin.
2. Valtuus: Sisäpiiriläiset voivat suorittaa toimintoja osana heille osoitettuja työtehtäviä, ja heillä voi myös olla valtuudet ohjata muita työntekijöitä. Tätä valtuutusta voidaan käyttää tukemaan haitallisia toimia, mukaan lukien joko fyysiset tai digitaaliset toimet, kuten tiedostojen tai prosessien manipulointi.
3. Tieto: Sisäpiiriläisillä voi olla tietoa kohteesta, siihen liittyvistä toiminnoista tai järjestelmistä rajallisesta tiedosta aina asiantuntijatietoon. Tämä voi sisältää tietoa, jonka avulla sisäpiiriläinen voi ohittaa tai kumota esimerkiksi fyysiset suoja- ja valvontajärjestelmät, kirjanpitojärjestelmät ja muut tavoitetta edistävät toimintamenettelyt.

Lisäksi yritykset ja organisaatiot lähtökohtaisesti luottavat omiin työntekijöihinsä. Sisäpiiriläisten uhka on siksi todellinen ja voi olla merkittävä. Sisäpiiriuhka on myös kasvanut monin kertaisesti työntekemisen tapojen muuttuessa ja etätyöskentelyn lisääntyessä vuoden 2020 COVID -viruspandemian jälkeen. Etä- ja hybridityöskentelyn myötä sisäpiiriteko on myös entistä helpompaa, kun tietoa ja laitteita liikkuu enemmän työpaikan ja kodin/etätyöpisteen välillä vaikeuttaen työnantajan näkökulmasta tiedon ja tietojärjestelmien käytönhallintaa ja valvontaa (pääsy, käsittely, siirtäminen, säilytys).

Yle (2014) ja Ilta-Sanomat (2002) uutisoivat Wärtsilässä 2000-luvun alussa tapahtuneesta yritysvakoilusta, jossa yrityksen pitkäaikaisessa palveluksessa ollut vartija oli kopioinut rahallista palkkiota vastaan toista tuhatta piirustusta ja toimittanut ne metalliyritykselle. Tekoa oli jatkunut neljän vuoden ajan. Yrittäjän tavoitteena oli tehdä Wärtsilän valmistamiin koneisiin perushuoltoa mahdollisimman edullisia varaosia käyttäen, johon hän oli tarvinnut piirustukset.

Geotiedustelu eli paikka- ja olosuhdetiedustelussa (GEOINT) käsitellään maantieteelliseen paikkaan sidottua informaatiota, jonka avulla kuvataan ja arvioida kohteena olevan ominaisuuksia kuten fyysisiä piirteitä. Geotiedustelu muodostuu paikkatietotiedustelusta ja kuva-aineistojen analysoinnista. (Puolustusvoimat, 2021) Analysoitavat kuvat saadaan useimmiten ilmasta muun muassa satelliittien, tiedustelukoneiden ja miehittämättömien ilma-aluksien avulla. Satelliitit ja tiedustelukoneet pystyvät ottamaan kuvia etäältä, jolloin henkilöstöä ja laitteita ei tarvitse vaarantaa tehtävän hoitamiseen. Huomioitavaa on, että kuvat eivät sisällä henkilötiedustelun henkilölähteistä käsin otettuja kuvia ja kuvissa näkyy vain kuvanottohetkellä vallitseva tilanne, jolloin ne voivat muuttua

myöhemmin. Lisäksi on huomioitava sään, naamiointi- ja väistötekniikoiden mahdolliset vaikutukset saatujen kuvien hyödyllisyyteen. (Writz & Rosenwasset, 2010)

Paikkatiedon avulla tunnistetaan maantieteellisten tai rakennettujen piirteiden ja rajojen maantieteellinen sijainti ja ominaisuudet. Maan alla tapahtuva toiminta voi olla yläpuolella olevien kuvien ulottumattomissa, vaikka tiedusteluanalyytikot voivat ymmärtää mitä tapahtuu maan alla seuraamalla epäiltyjen rakennuksien/laitosten lähellä tapahtuvaa elinkaaritoimintoa. Geotiedustelun täysimittainen hyöty saadaankin kolmen elementin integraatiosta ja käytöstä: kuvat, kuvatiedustelu (engl. Imagery intelligence, IMINT) ja paikkatieto. Tämä synergia mahdollistaa kokonaisvaltaisemman näkökulman ja toimintaympäristön syvemmän ymmärtämisen. (Kaminski, 2019)

Signaalitiedustelulla (SIGINT) tarkoitetaan sähkömagneettisiin signaaleihin kohdistettua tiedustelua. Sähkömagneettisia signaaleja pyritään sieppaamaan ja tarkkailemaan tutkien sekä mittauslaitteiden avulla. Tyypillisesti signaalitiedustelu on jaettu kahteen luokkaan: viestintään kohdistuvaan viestitiedusteluun (engl. Communication intelligence, COMINT) ja tutkien signaaliin kohdistuvaan mittaustiedusteluun (ELINT). (Puolustusvoimat, 2021)

Viestitiedustelu on seurausta ihmisten välisen viestinnän sieppauksesta mukaan lukien puhelut, sähköpostit, pikaviestit ja muut viestintäjärjestelmät. Näitä voidaan valvoa avaruudessa, ilmassa, maassa ja meren alla toimivilla kuuntelulaitteilla. Signaalitiedustelun menetelmiin voi liittyä myös salainen tunkeutuminen kielletylle alueelle ja tiettyihin tiloihin. Viestitiedustelussa tärkeässä roolissa on myös liikenneanalyysi, joka sisältää muun muassa puhelun osapuolten tunnistamisen ja niiden tarkan sijainnin, millä laitteilla ja menetelmillä he ovat yhteydessä toisiinsa, viestintätapa ja puhelujen tiheys. Kommunikaatiomallit voivat paljastaa kohteena olevan toiminnasta paljon. Mittaustiedustelu sen sijaan ei sisällä ihmisten välistä viestintää, vaan sen tieto on peräisin pääasiallisesti elektronisten signaalien kuten tutkasignaalien sieppauksesta. (Writz & Rosenwasset, 2010) Bathin (1998) mukaan kyky salakuunnella muiden keskusteluja heidän tietämättään on korvaamaton voimavara tiedustelutietojen tuotannossa. Se voi tarjota näkemyksiä suunnitelmista ja aikomuksista sekä tarjota valtavia etuja sille osapuolelle, joka voi valvoa salaisesti kohteen viestintää.

Writz & Rosenwasset (2010) mainitsevat muutamia keinoja, joiden avulla signaalitiedustelua voi heikentää. Tällaisia vastatoimia ovat muun muassa kuriirien käyttö, suojatut lankaliittymät, monimutkaiset koodikielet. Nämä toimenpiteet lisäävät käyttökustannuksia ja voivat hidastaa toimintaa. Nopeus ei kuitenkaan ole menestymisen edellytys.

Mittaus- ja tunnusmerkkitiedustelun (MASINT), josta käytetään myös ominaispiirre- ja tunnistetiedustelu nimeä, tarkoituksena on tunnistaa tai havaita kohde, seurata sitä ja kuvata sen ominaispiirteet. Ominaispiiteiden tunnistamiseen voidaan hyödyntää esimerkiksi seismologisten, magneettisten tai akustisten sensoreiden tuottamaa tietoa. (Puolustusvoimat, 2021) Sensoreita voidaan myös

käyttää näytteiden ottamiseen ympäristöstä esimerkiksi havaitsemaan radiologisia, biologisia ja kemiallisia vaaroja. Mittaus- ja tunnusmerkkitiedustelua käytetään yleensä varmistamaan ja tarkentamaan muista tiedustelulajeista saatuja lähteitä. (Richelson, 2007)

Avointen lähteiden tiedustelu (OSINT) luo perustan yritysvakoilutoiminnalle, sillä suurin osa tiedustelutoiminnasta perustuu avointen lähteiden hyödyntämiseen ja sen merkitys on kasvanut viime vuosien aikana entisestään. Digitaaliset lähteet tuottavat yhä enemmän ja uudenlaista tietoa. (Suojelupoliisi, 2024) Avointen lähteiden tiedustelua on määritelty hallituksen esityksessä eduskunnalle (HE 203/2017), jonka mukaisesti menetelmällä saatu tietämys perustuu avoimista lähteistä hankittuun analysoituun ja arvioituun informaatioon, jotka ovat laillisesti jokaisen kansalaisen mahdollista itse havainnoida tai pyytää. Wirtzin & Rosenwasserin (2010, 736–737) mukaan avointen lähteiden tiedustelulajin vahvuutena on lähteiden nopea saatavuus, edullisuus sekä maantieteellinen rajoittamattomuus. Se antaa myös mahdollisuuden kerätä tietoja tulevista tapahtumista. Heikkoutena voidaan pitää suurta datan määrää, väärän ja harhaanjohtavan tiedon mahdollisuutta. Tätä voidaan kuitenkin nykyaikana vähentää tekoälyä hyödyntämällä. Tietolähteinä ovat esimerkiksi erilaiset lehdet, kirjallisuus, julkaisut ja tilastot, kartat, sosiaalisen median sisällöt sekä radio- ja televisiolähetykset. Tällaisten lähteiden kautta hankittu tiedustelutieto on muita tiedustelulajeja riskittömämpää ja tiedon käytettävyys on parempi sen julkisuusasteen vuoksi. Avointen lähteiden tiedustelulla tuetaan yleensä muita tiedustelulajeja. Omana itsenäisenä tiedustelulajina sitä käytetään silloin, kun muiden tiedustelulajien käyttö ei ole mahdollista. (HE 203/2017)

Esimerkiksi Yle (2016) uutisoi Suomen ulkoministeriön tietojärjestelmiin tehdyistä murroista vuonna 2013. Tapahtumaketju alkoi verkkovakoilijoiden aloittamalla tiedon hankinnalla kohteesta muun muassa asiat, joiden parissa kohteen työntekijät työskentelevät ja keiden kanssa he ovat tyypillisesti tekemisissä. Kohdetta tiedustellessaan vakoilijat selvittivät taustatietoja ihmisistä muun muassa sosiaalisesta mediasta ja muista julkisista lähteistä. Kohteena olleet työntekijät saivat tämän jälkeen sähköpostin, jossa oli linkki tavalliselle verkkosivulle, mikä liittyi henkilön arkeen ja, jossa hän vieraili työnsä puolesta. Uutisen mukaan pelkkä sivulla vierailu riitti saastuttamaan kohteen koneen haittaohjelmalla, jota kautta hyökkääjät pääsivät etenemään verkossa ja varastamaan haluamiaan tietoja. Seuraavassa luvussa käsitellään tarkemmin mitä kokonaisturvallisuudella ja organisaatioturvallisuudella tarkoitetaan. Lisäksi tarkastellaan yleisellä tasolla miten yritysvakoilulta voidaan suojautua ja millaista tukea yhteiskunnalta voi tähän saada.

2.3 Organisaatioturvallisuus osana kokonaisturvallisuutta ja yritysvakoilun torjuntaa

Joulukuussa 2021 valtioneuvosto teki periaatepäätöksen valtion kiinteistöstrategiasta 2030. Samalla päivitettiin valtion toimitilastrategia, jonka tavoitteet tulisi saavuttaa vuoteen 2030 mennessä. Kiinteistöstrategian yhdeksi keskeiseksi teemaksi on nostettu kokonaisturvallisuus. Tällä tarkoitetaan tavoitetilaa, jossa valtion itsenäisyyteen, väestön elinmahdollisuuksiin ja muihin yhteiskunnan elintärkeisiin toimintoihin kohdistuvat uhkat ovat hallittavissa. (Valtiovarainministeriö, 2021:66) Turvallisuuskomitea (2017, 15) määrittelee kokonaisturvallisuuden käsitteen tilana, jossa yhteiskunnan elintärkeisiin toimintoihin kohdistuviin uhkiin ja riskeihin on varauduttu yhdessä elinkeinoelämän, viranomaisten ja järjestöjen kanssa. Tavoitteena on edistää yhteiskunnan vakautta ja hyvinvointia luomalla kestävä ja vahva turvallisuuskulttuuri, jonka avulla pystytään reagoimaan tehokkaasti erilaisiin yhteiskuntaan kohdistuviin uhkiin.

Yhteiskunta on riippuvainen organisaatioiden ja yrityksien tuottamien palvelujen häiriöttömästä toiminnasta. Organisaatiot lähtökohtaisesti joko edistävät tai heikentävät yhteiskunnan turvallisuutta riippuen siitä miten niissä hoidetaan turvallisuutta ja hallitaan niihin kohdistuvia riskejä. (Sisäasiainministeriö 2012, 4.) Tarkasteltaessa turvallisuutta organisaation näkökulmasta käytetään termiä organisaatioturvallisuus tai sen synonyymiä yritysturvallisuus. (Lanne, 2007) Tässä tutkielmassa käytetään termiä organisaatioturvallisuus, mikä koostuu useista turvallisuuden osa-alueista kuten Elinkeinoelämässä kehitetyssä yritysturvallisuusmallissa on kuvattuna (Kuvio 5). Osa-alueet limittyvät toisiinsa, jolloin kokonaisvaltainen turvallisuudenhallinta edellyttää, että organisaatioturvallisuuden osa-alueita tarkastellaan kokonaisuutena. Turvallisuuden osa-alueiden keinovalikoimaa käyttämällä pyritään saavuttamaan asetetut tavoitteet kustannustehokkaasti. Organisaatioturvallisuudella tavoitellaan organisaation toiminnan jatkuvuuden varmistamista suojaamalla tietoa, omaisuutta, ihmisiä ja ympäristöä vahingoilta, onnettomuuksilta ja rikolliselta toiminnalta kaikissa tilanteissa niin normaali- kuin kriisiaikana. Suojaustoimenpiteillä tuetaan ja edistetään organisaation toiminnan tavoitteita, kilpailukykyä ja positiivista imagoa. (Miettinen 2002; Puolustusministeriö - Puolustushallinnon turvallisuus; Lanne 2007; Kauppakamari 2012; Turvallisuuskomitea 2017, 15)

KUVIO 5 Yritysturvallisuusmalli

2.3.1 Yritysvakoilulta suojautuminen

Aiemmissa luvuissa on kuvattuna mitä yritysvakoilulla tarkoitetaan, millä tavoin ja keiden toimesta sitä voidaan harjoittaa. Yritysvakoilua voidaankin pitää yhtenä merkittävimmistä ja haasteellisimmista kokonaisturvallisuuden uhkista, jolla voidaan vaikuttaa koko yhteiskunnan toimintaan. Koivulan (2020, 77) mukaan voimme menettää jopa 2–3 % bruttokansantuotteesta yritysvakoilun vuoksi. Yritysvakoilun torjunnalla on näin kansallista merkitystä. Teknologiakehityksen myötä kybervakoilusta on tullut yksi vakavimmista tietopääomaan kohdistuvista uhkista, jota vastaan kaikkien organisaatioiden tulee varautua. Kybervakoilu aiheuttaa vähintään neljäsosan kaikista kyberhäiriöistä ja suurimman osan kustannuksista. (Euroopan tilintarkastustuomioistuin, 2019)

Yritysvakoilulta suojautumisessa on kyse kokonaisvaltaisesta organisaation liiketoiminnan jatkuvuuden suunnittelusta, jossa on huomioitava kriittisten kohteiden kuten avainhenkilöiden sekä sidosryhmien, tietojen, tilojen, tietojärjestelmien ja -laitteiden tunnistaminen ja suojaaminen sekä niihin kohdistuvien uhkien ja riskien hallinta. Myös tilannekuvan ymmärtäminen, kyky havainnoida ja seurata toimintaympäristöön kohdistuvia uhkia ovat olennainen osa suojautumista. (Cyberwatch & Elinkeinoelämän keskusliitto, 2018) Yritysvakoilua vastaan voidaankin suojautua organisaatioturvallisuuden menetelmin, joilla pyritään takaamaan organisaation tiedon, henkilöstön, materiaalin, ympäristön ja infrastruktuurin turvallisuus. Tähän tavoitteeseen päästäkseen pääpainon tulee olla riskilähtöisessä ennakoivassa toiminnassa, jolla pyritään havaitsemaan, tunnistamaan, estämään ja hallitsemaan toimintaa uhkaavat tekijät.

Limnell (2019) mukaan yrityksen turvallisuuskulttuurin ja henkilöstön turvallisuustietoisuuden vahvistaminen ovat avainasemassa kybervakoilun torjunnassa. Lanne (2007, 33) vahvistaa organisaation turvallisuuskulttuurin muodostavan pohjan turvallisuusasenteille ja turvalliselle käyttäytymiselle, mikä puolestaan vaikuttaa turvallisuuden hallintaan. Turvallisuuskulttuuria voidaankin näin pitää yritysvakoilulta suojautumisen perustana. Asianmukaiset turvallisuuspolitiikat, tietojen luokitteluun liittyvät riskiperusteiset käytänteet pääsyoikeuksien, tiedon käsittelyn ja säilytyksen osalta ovat osa hyvää turvallisuuskulttuuria. Organisaation tulee myös ymmärtää miksi he voivat olla yritysvakoilun kohteena. Minkälaista tietoa heidän kauttaan voi saada ja miten tätä tietoa voidaan käyttää, kenen hyväksi organisaatiota voidaan vakoilla ja mitä siitä voi aiheutua organisaatiolle itselleen, yhteistyökumppaneille tai yhteiskunnalle. Valveutuneen henkilöstön lisäksi niin fyysinen kuin tekninen ympäristö tulee olla kunnossa. Teknisen ympäristön osalta avainasemassa on ennakoiva toiminta ja järjestelmien tietoturvallinen suunnittelu sekä käyttäjien kouluttaminen ennen järjestelmän tai laitteen käyttöönottoa. Lisäksi ajantasaiset ohjelmistoversiot, tietoturvapäivitykset, järjestelmien koventaminen, käyttöoikeuksien hallinta ja muutoksien seuranta tulee olla määriteltynä. Myös verkkojen ja tietokokonaisuuksien eriyttäminen, havainnointikyky ja poikkeamienhallintaan liittyvät toimenpiteet on linjattu sekä lokitietojen taltiointi että siihen liittyvä seurantaprosessi ja suojaus ovat määritelty. Näiden lisäksi alihankkijoiden ja yhteistyökumppaneiden turvallisuuskulttuurin ja taustojen selvittäminen ovat olennaista yritysvakoilulta suojautumisessa. (Kyberturvallisuuskeskus, 2014; Cyberwatch & Elinkeinoelämän keskusliitto, 2018)

2.3.2 Yhteiskunnan tuki yrityksille ja organisaatioille

Suomalainen yritys ja organisaatio voi olla Suojelupoliisiin yhteydessä, mikäli se epäilee joutuneensa yritysvakoilun kohteeksi. Suojelupoliisi hoitaa asian selvittelyn, mikäli tekijän päätellään olevan valtiotaustainen. Asian selvittelyä tehdään yhteistyössä kohdeorganisaation turvallisuustoiminnon kanssa. Muissa tapauksissa rikostutkinnasta vastaa Suomessa alueperiaatteen mukaisesti poliisilaitokset sekä Keskusrikospoliisin kyberrikostorjuntakeskus, jossa pääasiallisesti tutkitaan tietoverkkoympäristössä tehtyjä laajempia kansainvälisiä rikoskokonaisuuksia yhteistyössä Europolin ja Yhdysvaltojen (FBI) kanssa. (Sisäministeriö, 2017) Kuten aiemmin todettiin rikoslaki ei tunne kybervakoilua ja kyberrikollisuutta käsitteenä eikä sitä ole sinne virallisesti määritelty. Mutta kyberrikoksissa yhdistyy usein muita rikosnimikkeitä kuten törkeä kiristys (Rikoslaki 31:4), petos (Rikoslaki 36:1), vakoilu (Rikoslaki 12:5) tai yritysvakoilu (Rikoslaki 30:4), jolloin ne voidaan ottaa tutkinnan alle.

Viranomaiset suosittelevat yrityksiä ja organisaatioita ilmoittamaan yritysvakoiluepäilyistä matalalla kynnyksellä, vaikka niitä on yrityksen näkökulmasta haastava todentaa. Kybervakoilun ja yleisesti tietoverkkorikoksiin liittyvien epäilyjen osalta Keskusrikospoliisi konsultoi tarvittaessa yrityksiä ja organisaatioita. Kansainvälinen viranomaisyhteistyö varsinkin valtioiden organisoimien kybervakoilutapauksien tutkinnan osalta on haastavaa. Vaikka tapahtuma

täyttää useammankin rikoksen tunnusmerkistön, tekoa ei voida selvittää käytännössä rikosoikeuden kontekstissa. Tämä johtuu siitä, että tekijöiden selvittäminen edellyttäisi oikeusapua valtiolta, josta käsin he ovat toimineet. Oikeusapua ei ole odotettavissa, mikäli tekijät toimivat sijaintivaltionsa lukuun. (Sisäministeriö, 2017) Kansainväliset lait ja säädökset ovat myös yleisesti kybervakoilun estämisen osalta epäselviä (Poliisiammattikorkeakoulu, 2021).

On kuitenkin huomioitava, että Suomessa viranomaisten, organisaatioiden ja yksityisten yrityksien välistä kyberrikoksien torjuntaa koskevaa yhteistyötä sekä tiedonvaihtoa voidaan kuitenkin pitää vielä alkuvaiheessa olevana. Esimerkiksi yritykset, jotka tuottava SOC-palvelua (engl. Security Operation Center) on viranomaistoimijaa tiiviimmässä yhteistyössä asiakasorganisaatioihinsa. Näin ollen he ovat ensimmäinen taho, jonka puoleen asiakasorganisaatio ottaa yhteyttä turvallisuuspoikkeamatilanteessa. SOC-palvelua tuottaville kertyykin hyvä tilannekuva suomalaisiin yrityksiin ja organisaatioihin kohdistuvista uhkista. Yhteistyötä on pyritty lisäämään entisestään lisääntyvien kyberoperaatioiden myötä. (Poliisiammattikorkeakoulu, 2021)

3 YHTEENVETO TEORIAOSUUDESTA

Kirjallisuuskatsauksen tuloksena saatiin kuvattua tämän tutkielman kannalta keskeisimmät käsitteet sekä tutkittavaa kohdetta että siihen liittyvän alan erityispiirteitä. Lisäksi saatiin yleisestä näkökulmasta vastaukset tutkimuskysymyksiin millä keinoin ja menetelmin yritysvakoilua harjoitetaan, mitkä asiat ovat sen kohteena ja miten sitä vastaan voidaan suojautua. Näitä tutkimuskysymyksiä täydennetään kiinteistö- ja rakennustoimialan näkökulmasta empiirisessä osiossa. Kirjallisuuskatsauksen tulokset on koottu yhteen alla olevaan taulukkoon 2.

TAULUKKO 2 Yhteenveto kirjallisuuskatsauksen tuloksista

<table>
<tr><th>Kiinteistö- ja rakentamistoimiala (KIRA):</th><th colspan="4">Yritysvakoilu:</th></tr>
<tr><td>Tarkoitetaan kiinteistön ostoa, myyntiä, vuokrausta, rakennuttamista, muutos-, laajennus- tai ylläpitotyötä.

Kiinteistö- ja rakentamisala muodostavat Suomessa KiRa-klusterin, jonka toimialat ovat sidoksissa toistensa kanssa</td><td>Teko, jossa oikeudettomasti hankitaan toiselle kuuluvaa liikesalaisuutta ja otetaan se omaan käyttöön tai ilmaistaan oikeudettomasti ulkopuoliselle, joko tunkeutumalla ulkopuolisilta suljettuun paikkaan tai tietojärjestelmään, hankkimalla tietoja haltuunsa tai jäljentämällä tai käyttämällä teknistä erikoislaitetta. Kybervakoilu on osa yritysvakoilua.</td><td>Tekijätahot

• Valtiolliset toimijat
• Rikolliset toimijat
• Valtiollisten ja rikollisten yhteen liittymät
• Yksityiset yritykset tai organisaatiot
• Yksittäiset henkilöt</td><td>Motiivit ja kohteet

• Taloudellinen hyöty
• Poliittiset motiivit
• Yhteiskunnallinen tai ideologinen vaikuttaminen
• Tiedon saanti
• Pyrkimys edistää omaa asemaansa, tavoitteitaan tai heikentää kohteena olevan liikkumaa tai kilpailuetua
• Kohteena voivat olla niin fyysiset rakennukset, tilat, laitteet, järjestelmät, verkkoympäristöt kuin ihmiset</td><td>Menetelmät ja keinot

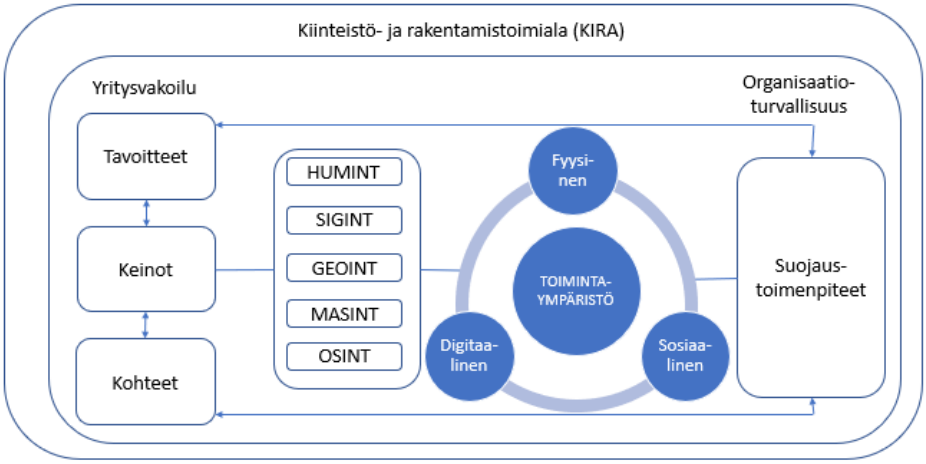
Tiedustelutoiminnan menetelmät

• Henkilötiedustelu (HUMINT)
• Signaalitiedustelu (SIGINT)
• Geotiedustelu eli paikka- ja olosuhdetiedustelu (GEOINT)
• Mittaus- ja tunnusmerkkitiedustelu (MASINT)
• Avointen lähteiden tiedustelu (OSINT)</td></tr>
<tr><td colspan="2">Erityispiirteet ja alan keskeisimmät haasteet:
• Verkostoituminen
• Projektiluonteisuus
• Pitkä elinkaari
• Tietomallintaminen
• Vaihtuvat vaatimukset
• Ilmoitukset ja luvanvaraisuus</td><td colspan="3">Organisaatioturvallisuuden mukaiset suojaustoimenpiteet
(EK:n yritysturvallisuuden malli)</td></tr>
</table>

Yritysvakoilulla tarkoitetaan pohjimmiltaan laitonta ja epäeettistä toimintaa, johon valtiolliset tai yksityiset organisaatiot, rikolliset ryhmittymät tai yksittäiset henkilöt ryhtyvät kerätäkseen, analysoidakseen ja hallitakseen järjestelmällisesti tietoa heikentääkseen kohteena olevan liikkumatilaa tai kilpailuetua. Tavoiteltava tietopääoma voi sijaita dokumentteina ja objekteina fyysisessä tilassa, ajatuksina ja tietotaitona ihmisten kognitiivisessa tietoisuudessa tai datana tietojärjestelmissä. Kiinteistö- ja rakentamistoimialan kontekstissa tätä kolmijakoa tarkastellaan fyysisen, sosiaalisen ja digitaalisen toimintaympäristön näkökulmasta.

Yritysvakoilussa keinot ja menetelmät voivat olla tiedustelutoiminnassa käytettävien eri tiedustelulajien kaltaisia riippumatta siitä, onko tekijä valtiollinen vai ei-valtiollinen toimija. Tässä tutkielmassa keinovalikoiman viitekehyksenä voidaan pitää Lowenthalin ja Clarken (2015) jaon mukaista tiedustelulajien viittä päälajia (HUMINT, SIGINT, GEOINT, MASINT, OSINT), selvitettäessä tarkemmin millä menetelmillä yritysvakoilua harjoitetaan kiinteistö- ja rakennustoimialaa kohtaan. Näitä viittä tiedustelulajia tarkastellaan toimintaympäristön kolmen ulottuvuuden ja kiinteistö- ja rakentamistoimialan erityispiirteiden näkökulmasta. Erityispiirteiksi tunnistettiin verkostoituminen, projektiluonteisuus, pitkä elinkaari, tietomallintaminen, vaihtuvat vaatimukset sekä ilmoitukset ja luvanvaraisuus. Erityispiirteet linkittyvät toisiinsa ja kuvastavat kokonaisuudessaan kiinteistö- ja rakennustoimialan monimuotoisuutta.

Yritysvakoilusta tai tiedustelutoiminnasta tehdyistä aiemmista tutkimuksista ei löytynyt kirjallisuuskatsauksen perusteella teoreettista viitekehystä, jota olisi voinut soveltaa tässä tutkielmassa. Kuviossa 6 on kuvattuna teoriaosuuden synteesi, jota on käytetty empiirisen osion viitekehyksenä.



KUVIO 6 Teoreettinen synteesi

4 TUTKIMUKSEN TOTEUTUS JA TUTKIMUSMETODI

Tämä pro gradu -tutkielma on toteutettu laadullisena eli kvalitatiivisena tutkimuksena. Laadullisen tutkimuksen menetelmät soveltuvat käytettäväksi silloin, kun halutaan tutkia arkaluontoisia ja ennalta vierasta aihetta, jota ei ole tutkittu aiemmin. Lisäksi menetelmä auttaa ymmärtämään tutkittavaa ilmiötä tarkemmin ja se auttaa luomaan kokonaisvaltaisen ja syvällisemmän käsityksen ilmiöstä. (Tuomi & Sarajärvi, 2018). Tämän tutkimuksen tarkoituksena on selvittää, miten yritysvakoilu ilmenee kiinteistö- ja rakennustoimialalla. Tutkimuksessa käsitellään asioita, jotka koetaan arkaluontoisiksi ja lisäksi aihetta tarkastellaan uudesta kontekstista, jonka vuoksi kvalitatiivisen tutkimuksen metodien käyttö on perusteltua.

Päätös pro gradu -tutkielman aiheesta ja rajauksesta valmistui vuoden 2021 lopulla, jolloin alkoi myös alustava aiheeseen tutustuminen. Seuraavan vuoden keväällä valmistui tutkimussuunnitelma. Tutkielman teoriaosuus on toteutettu kuvailevan kirjallisuuskatsauksen tutkimusmenetelmää hyödyntäen. Salmisen (2011, 3–6) mukaan kuvailevaa kirjallisuuskatsausta voidaan luonnehtia yleiskatsaukseksi, jossa tutkittavaa aihetta pystytään kuvaamaan laajasti ja tutkimusaiheen ominaisuuksia voidaan tarvittaessa luokitella. Kirjallisuuskatsauksen tavoitteena on ollut kuvata tämän tutkielman käsitteellistä taustaa, tutkittavaa kohdetta sekä siihen liittyviä erityispiirteitä tuottaen looginen kokonaiskuva tutkittavasta aiheesta. Lisäksi on pyritty vastaamaan esitettyihin tutkimuskysymyksiin käytetyn kirjallisen aineiston pohjalta. Aineiston keruussa on hyödynnetty sekä sähköisiä tietokantoja kuten JYKDOK, Google Scholar, Helmet (E-kirjasto) että kirjallisuuslähteitä kirjastoista. Sähköisissä tietokannoissa hakusanoina käytettiin muun muassa

- englanninkieliset: corporate espionage, illegal intelligence, industrial espionage, cyber espionage, real estate industry, critical infrastructure

- suomenkieliset: yritysvakoilu, laiton tiedustelu, tiedustelutoiminta, teollisuusvakoilu, kybervakoilu, kiinteistötoimiala, rakennusala, kriittinen infrastruktuuri

Kirjallisuuskatsauksen avulla teoriaosuuden tuloksena muodostui viitekehys, joka on toiminut tämän tutkimuksen empiirisen tutkimusosion perustana. Empiirisen osion aineisto on muodostunut haastatteluista, jotka toteutettiin kevään 2024 aikana. Aineistonkeruumenetelmänä on käytetty teemahaastattelua, jonka avulla vaikeasti tutkittavaa aihetta on voitu tarkastella kiinteistö- ja rakennustoimialan näkökulmasta. Seuraavissa alaluvuissa on kerrottu tarkemmin empiirisen osion aineiston keruusta ja analysoinnista.

4.1 Tutkimusmetodin valinta ja aineiston keruu

Kvalitatiivisen tutkimuksen yksi yleisimmistä tiedonkeruumenetelmistä on haastattelut. Haastattelumenetelmät voidaan jakaa yleisesti strukturoituihin, strukturoimattomiin ja puolistrukturoituihin haastatteluihin. (DiCicco-Bloom & Crabtree, 2006). Tässä tutkimuksessa empiirisen osion aineiston keruussa on käytetty teemahaastattelua eli puolistrukturoitua haastattelumetodia.

Hirsjärvi, Remes ja Sajavaara (2001) mukaan teemahaastattelun käyttö on perustelua, kun halutaan kuulla ihmisten käsityksiä, mielipiteitä ja uskomuksia, joita on helpompi käsitellä, kun ollaan haastateltavan kanssa suorassa vuorovaikutuksessa. Syvälliset ja vapaamuotoiset keskustelut voivat paljastaa asioita, joita ei voisi saada selville muilla tavoin. Vaikeasti tutkittavia asioita onkin mahdollista lähestyä keskustelutyyppisissä haastatteluissa. Haastattelujen aikana voidaan myös tarkentaa ja syventää annettuja vastauksia sekä oikaista mahdollisia väärinymmärryksiä. Lisäksi haastateltaviin on mahdollista ottaa yhteyttä haastattelun jälkeen, mikäli aineistoa on tarvetta täydentää. (Tuomi & Sarajärvi, 2018). Metsämuurosen (2005, 226) mukaan teemahaastattelua käytetäänkin usein, kun halutaan selvittää vähän tiedettyjä ja tunnettuja asioita tai, kun on kyseessä arka aihe kuten tässä tutkielmassa. Esimerkiksi harva organisaatio edelleenkään nykypäivänä tuo julkisuuteen, mikäli on joutunut yritysvakoilun tai tiedustelun kohteeksi. Haastattelumetodia on myös perusteltua käyttää silloin, kun halutaan syventää aiemmin tutkittuja aiheita kuten miten yritysvakoilu ilmenee kiinteistö- ja rakentamistoimialalla, josta ei ole aiempaa tutkimustietoa saatavilla.

Teemahaastattelua pidetään avoimen ja lomakehaastattelun välimuotona. Tämä tarkoittaa, ettei menetelmässä käytetä strukturoidulle haastattelulle ominaisia tarkkoja kysymysmuotoja ja -järjestystä, vaan haastattelun pääteemat ovat tiedossa etukäteen. Teemat johdetaan yleensä käsiteltävän aiheen teoreettisesta analyysistä. Haastattelijan tehtäväksi jää varmistaa, että kaikki suunnitellut teemat käsitellään ja keskustelua voidaan syventää niin pitkälle kuin tutkimusintressit edellyttävät ja haastateltavan edellytykset sallivat. (Hirsjärvi ja Hurme, 1995).

Tässä tutkielmassa teemahaastattelun pääteemat johdettiin tutkimuskysymyksistä ja teoreettisesta viitekehyksestä (Kuvio 5), mikä nopeutti aineiston myöhempää analysointia. Haastattelurunko sisälsi tosiasia- ja mielipidekysymyksiä, jotka ovat Hirsjärven ja Hurmeen (1995) mukaan teemahaastatteluille tyypillisiä kysymystyyppejä. Tosiasiakysymykset pitävät sisällään taustoittavia kysymyksiä ja tietokysymyksiä, jotka käsittelevät sitä mitä haastateltava tietää aiheesta. Taustoittavien kysymyksien avulla selvitettiin haastateltavien työkokemus- ja osaamistaustaa, kokemuksia kiinteistö- ja rakennustoimialaan sekä tiedusteluun että yritysvakoilun ja laittoman tiedustelun torjuntaan. Näiden kysymyksien avulla saatiin muodostettua käsitys haastateltavien ymmärryksestä tutkittavasta aiheesta. Lisäksi haastateltavia haastettiin kriittiseen ajatteluun pyytämällä kuvaamaan yksityiskohtaisesti tapahtunutta tai keskusteltua asiaa ja miksi haastateltava pitää tapausta tai asiaa kriittisenä. Tätä toimintatapaa käytettiin haastattelun siinä vaiheessa, kun haastateltavalta haluttiin kehittämisnäkemyksiä tutkivaan aiheeseen liittyen.

Teoreettisesta viitekehyksestä johdettu haastattelurunko koostui seuraavista teemoista:

- Taustatiedot
- Uhka- ja riskikuva
- Yritysvakoilun tavoitteet ja kohteet
- Yritysvakoilun keinot ja menetelmät
- Varautuminen ja suojautuminen yritysvakoilulta
- Tulevaisuuden trendit, haasteet ja jatkotutkimusaiheet

Haastattelurunko on kuvattuna liitteessä 1.

Haastattelumenetelmän vahvuutena voidaan pitää tässä tutkielmassa, että se avasi väylän keskustella haastateltavien kanssa edellä kuvatuista teemoista kiinteistö- ja rakennustoimialan kontekstissa eri tahojen tietojen ja kokemuksien mukaan. Lisäksi haastatteluissa käydyissä keskusteluissa pystyttiin huomioimaan miten haastateltavat kokevat kiinteistö- ja rakennustoimialan erityispiirteet. Miten ne mahdollisesti näkyvät kiinteistö- ja rakennustoimialaan kohdistuvassa yritysvakoilussa, tiedustelussa, eri toimintaympäristöt (fyysinen, sosiaalinen, digitaalinen) ja kiinteistön elinkaaren eri vaiheet huomioiden, jolloin haastateltava pääsi pureutumaan varsinaiseen tutkimusongelmaan.

4.1.1 Haastatteluiden toteutus

Teemahaastattelut pidettiin helmi-maaliskuun 2024 aikana. Ennen varsinaisten haastatteluiden aloittamista pidettiin joulukuun 2023 lopulla yksi esihaastattelu, jolla testattiin haastattelurunkoa, aihepiirien järjestystä ja kysymyksien muotoiluja. Samalla saatiin kellotettua haastattelun keskimääräinen kesto. Esihaastattelun jälkeen haastattelurunkoon tehtiin muutamia muutoksia ja käsiteltävien aiheiden järjestystä muutettiin siten, että taustatietoja koskevan keskustelun jälkeen tulee tutkittavaa aihetta yleisesti käsittelevä teema, josta haastateltavan oli alkuun helppo kertoa.

Esihaastattelun jälkeen alkoi haastateltavien alustava valinta kartoittamalla ensin Senaatti-konsernista, heidän asiakkuuksistaan ja palvelutuottajista sopivia ehdokkaita. Tutkielman kannalta oli tärkeää, että haastateltaviksi saatiin kiinteistön omistajan, käyttäjän ja palveluntuottajan edustajat. Kiinteistössä toimivien tahojen lisäksi oli oleellista saada haastateltua tiedusteluviranomaisten niin sotilas- kuin siviilitiedustelun edustajia sekä asiantuntijahaastatteluja vastatiedustelun ja kyberturvallisuuden osalta. Tarkoituksena oli saada mahdollisimman kokonaisvaltainen kuva tutkittavasta aiheesta eri näkökulmat huomioiden.

Haastateltavia organisaatioita ja henkilöitä lähestyttiin sähköpostitse, jossa taustoitettiin tutkimusaihetta ja tavoitteita, kerrottiin tutkimuseettisistä näkökulmista, tutkimuksen julkisuusasteesta sekä tiedusteltiin haastateltavien halukkuutta osallistua etänä toteutettaviin haastatteluihin, jotka tallennettaisiin. Varsinainen haastatteluajankohta sovittiin erikseen haastateltavan kanssa puhelimitse tai sähköpostitse. Kaikki suostuivat haastatteluihin yhtä organisaatiota lukuun ottamatta. Tämä puuttuva organisaatio korvattiin yksityisen sektorin asiantuntijahaastattelulla, koska tutkimuksen toteutukseen varattuaika oli rajallinen. Haastateltavia oli yhteensä seitsemän, jotka ovat kuvattuna seuraavassa alaluvussa tarkemmin. Alun perin tarkoituksena oli haastatella kaksi henkilöä kustakin eri roolista, mutta tästä luovuttiin rajallisten resurssien vuoksi. Sen sijaan panostettiin sopivien haastateltavien valintaan.

Kaikki haastattelut toteutettiin yksilöhaastatteluina Teams -videokokouksena, jonka kutsun yhteydessä kaikille haastateltaville lähetettiin vielä kertaalleen saatekirje tutkimuksen tavoitteista, aiheesta ja rajauksesta sekä tutkimuksessa käytettävistä keskeisimmistä käsitteistä. Saatekirjeessä kerrottiin myös lyhyesti miten haastattelu tullaan toteuttamaan mistä teemoista on tarkoitus keskustella kiinteistö- ja rakennustoimialan kontekstissa. Haastateltavia kannustettiin myös kertomaan mahdollisia todellisuudessa tapahtuneita case-esimerkkejä mahdollisuuksien mukaisesti vaikka karkeutetusti. Lopussa muistutettiin vielä tutkimuseettisistä näkökulmista, jotka otetaan huomioon tutkimusprosessin aikana kuten henkilötietojen anonymisointi ja pseudonymisointi.

Haastatteluiden kesto oli 60–90 minuuttia. Haastattelija oli valinnut mahdollisimman häiriöttömän haastatteluympäristön siten, ettei tilassa ollut muita henkilöitä ja äänen kuuluminen ympäristöön oli estetty käyttämällä kuulokkeita. Haastattelija ja haastateltavat, kahta lukuun ottamatta, pitivät kuvayhteyden, jolloin haastattelija pystyi tulkitsemaan myös haastateltavien kehonkieltä.

Haastatteluiden alussa kerrattiin vielä haastattelun tarkoitus ja tutkimuksen tavoitteet sekä tutkimuseettiset näkökulmat. Lisäksi muistutettiin, että tutkielman loppuraportti on julkinen, mutta työ tehdään luottamuksellisena, haastateltavien nimiä ja organisaatioita ei mainita ja haastatteluaineistoa käsittelee ainoastaan haastattelija. Kaikki haastattelut tallennettiin haastateltavien luvalla.

Haastattelutilanteet etenivät suppilotekniikan mukaisesti helpoista ja laajoista yleisistä kysymyksistä spesifisimpiin kysymyksiin. Tällä pyrittiin varmistamaan, että haastateltavat kokevat osaavansa vastata kysymyksiin ja keskustelu tuntuu mielekkäältä. Hirsjärven ja Hurmeen (2000) mukaan kysymysten laaja-alaisuus antaa haastateltavalle mahdollisuuden käsitellä aihetta kykyjään

vastaavalla ja häntä kiinnostavasta näkökulmasta. Laaja-alaisilla kysymyksillä pyrittiin myös siihen, että haastattelija ei ohjaa haastateltavaa liiaksi, jotta haastateltavan oma tietämys ja kokemus tutkittavasta aiheesta tulisi mahdollisimman hyvin esille. Haastatteluteemojen käsittelyjärjestys saattoi muuttua haastattelun aikana haastateltavan mukaan. Haastateltavat rohkaistuivat kertomaan enemmän konkreettisemmista asioista haastattelun edetessä ja heille esitettiin haastatteluroolin mukaisia tarkentavia lisäkysymyksiä.

Haastatteluiden päätteeksi haastateltavat antoivat lisätietoja keskustelluista aiheista ja suosittelivat henkilöitä, joilta voi tarvittaessa pyytää lisätietoja. Saadut lisätiedot ja huomiot kirjattiin haastattelupäiväkirjaan, jota ylläpidettiin jokaisesta haastattelusta. Päiväkirjaan kirjattiin haastattelupäivä ja kesto aloitus- ja lopetuskellonaikoineen sekä huomiot haastateltavasta että keskustelluista asioista, jotka on hyvä nostaa tarvittaessa esiin myös muissa haastatteluissa. Pääasiassa haastatteluista annettiin positiivista palautetta ja osassa haastateltavissa haastattelu oli herättänyt pohtimaan turvallisuusasioita eri näkökulmasta, mikä koettiin hyvänä.

4.1.2 Haastateltavat

Haastateltavien edustamat organisaatiot olivat Senaatti-konsernin kanssa yhteistyötä tekeviä tahoja, jotka edustivat kiinteistön omistajaa, kiinteistön käyttäjää, palveluntuottajaa, tiedusteluviranomaista tai asiantuntijatahoa. Tämä mahdollisti yritysvakoilun tarkastelun mahdollisimman laaja-alaisesti kiinteistö- ja rakennustoimialan kontekstissa huomioiden eri toimijoiden näkökulmat tutkimuksen rajaus huomioiden. Tällä tavoin haastatteluvastaukset myös täydensivät toinen toisiaan ja eri roolissa olevan haastateltavan antamaa näkemystä pystyttiin testaamaan toisessa roolissa olevalla.

Koska haastateltavien määrä oli rajallinen, käytettiin aikaa haastateltavien valintaan. Haastateltavaksi valittiin henkilöitä, joilla oli pitkäaikaista substanssiasiantuntijuutta organisaatioturvallisuudesta tai kyberturvallisuudesta ja tiedustelutoiminnasta. Lisäksi kiinteistönomistajan, kiinteistön käyttäjän ja palveluntuottajien edustajien tuli olla tutkimuksen rajauksen mukaisesti sidoksissa Suomen valtion omistamaan kiinteistökantaan. Osalla haastateltavista oli kokemusta tutkimuksen kannalta eri rooleissa toimimisesta kuten esimerkiksi kiinteistön käyttäjän turvallisuusorganisaatiossa sekä kiinteistön omistajan palveluntuottajana toimimisesta, jolloin he pystyivät antamaan vastauksensa laaja-alaisemmasta ja monipuolisemmasta näkökulmasta. Tiedusteluviranomaisten osalta toinen haastateltavista edusti siviilitiedustelua ja toinen sotilastiedustelua. Asiantuntijahaastattelun antaneilla toisella henkilöllä on pitkä työkokemus poliisihallinnosta ja toisella puolustushallinnosta kunnes ovat siirtyneet yksityiselle sektorille. Melkein kaikilla haastateltavista oli yli kahdenkymmenen vuoden kokemus turvallisuus- ja/tai tiedustelualaan liittyvistä asiantuntijatehtävistä. Haastateltavien roolit (näkökulma) ja työtehtävät vastuualueineen ovat kuvattuna taulukossa kolme.

TAULUKKO 3 Tutkielmaan osallistuneet haastateltavat

Haastattelu	Tehtävä, vastuualue	Rooli tutkimuksessa
H1	Asiantuntija, tiedustelu ja turvallisuus	Asiantuntija
H2	Päällikkö, organisaatio-turvallisuus ja valmius	Kiinteistön käyttäjä (kokemus useammasta valtion organisaatiosta)
H3	Päällikkö, organisaatio-turvallisuus ja jatkuvuu-denhallinta	Palveluntuottaja, kiinteistön käyttäjä
H4	Erikoistutkija	Tiedusteluviranomaisen edustaja
H5	Päällikkö	Tiedusteluviranomaisen edustaja
H6	Päällikkö, organisaatio-turvallisuus ja valmius	Kiinteistönomistaja, kiinteistön käyttäjä
H7	Asiantuntija, kyberturvallisuus	Asiantuntija

4.2 Aineiston analyysi

Tutkimuksen empiirisen aineiston eli haastatteluin kerätyn datan analysoinnissa on käytetty sisällönanalyysimenetelmää. Menetelmä sopii käytettäväksi kaikissa laadullisissa tutkimuksissa vaikkakin se koetaan yleisesti työlääksi. Sitä voi käyttää haastatteluiden, nauhoitettujen puheiden, kirjoitetun tekstin sekä kuvaa että ääntä sisältävien aineistojen analyysiin. (Tuomi & Sarajärvi, 2018).

Sisällönanalyysin tarkoituksena on luoda tutkittavasta ilmiöstä selkeä ja sanallinen kuvaus, johon aineisto tarjoaa näkymän. Tuomen & Sarajärven (2018) mukaan aineisto järjestetään analyysissä tiiviiseen ja selkeään muotoon kadottamatta siinä olevaa informaatiota. Sisällönanalyysi voidaan toteuttaa kolmella tavalla, joko aineistolähtöisesti, teorialähtöisesti tai näiden yhdistelmällä. Aineisotlähtöisessä analyysissä tutkivasta aiheesta kertoavia kohtia etsitään aineiston ehdoin. Teorialähtöisessä analyysissa aineiston analyysiä ohjaa aikaisemman tiedon perusteella luotu teoria, jolloin useimmiten testataan aikaisempaa tietoa uudessa kontekstissa. Kolmantena analyysimenetelmänä on kahden aiemman yhdistelmä. (Tuomi & Sarajärvi, 2018, 108–110). Tässä tutkielmassa on käytetty yhdistelmämenetelmää, jossa analyysin apuna käytettiin teemahaastattelun pääteemoja. Pääteemat johdettiin tutkimuskysymyksistä ja teoreettisesta viitekehyksestä.

Analyysin tekemiseen ei kuitenkaan ole mitään yhtä yleispätevää ohjetta. Olennaista on, että aineiston koodaus ja luokittelu on systemaattista, jossa aineiston samankaltaisuudet ja eroavaisuudet on tunnistettu. Yleensä toimiva

koodausrunko edellyttää useampaan kertaan tehtyä aineiston huolellista läpikäyntiä. Hirsjärvi & Hurme (2000) mukaan onnistuneen tulkinnan kriteerinä voidaan pitää sitä, kun lukija löytää saman näkökulman kuin tutkija. Huomioitavaa on, että lukija lukee tulkinnan haastatteluista tutkijan kirjoittaman tulkinnan pohjalta eikä haastatteluaineiston. Tämän vuoksi onkin tärkeää, että tutkija kirjoittaa tarkan kuvauksen, miten tulkintoihin päädyttiin.

Aineiston analysointi alkoi haastattelutallenteiden sanatarkalla litteroinnilla. Litteroinnit tehtiin heti haastatteluiden jälkeen, jolloin haastatteluaineisto oli vielä tuore. Tämä mahdollisti myös aineiston tarkennukset haastateltavalta, mikäli tähän oli tarvetta. Yhden haastatteluaineiston litterointiin kului aikaa useampi tunti. Analysoitavaa aineistoa muodostui yli kaksisataa sivua.

Litteroinnin jälkeen tekstistä poistettiin täytesanat, jotta aineisto saatiin luettavampaan muotoon. Haastattelun aikana tehdyt muistiinpanot vertailtiin kirjoitettuun tekstiin. Samalla haettiin alustavaa tuntumaa aineistoon.

Aineiston alustavan tutustumisen jälkeen aloitettiin aineiston luokittelu. Luokittelussa käytettiin apuna Mindmap -ohjelmaa, mikä helpotti aineiston kokonaisuuden käsittelyä. Aineiston luokittelun pohjalla käytettiin teemahaastatteluiden pääteemoja. Pääteemat oli aiemmin todetun mukaisesti johdettu tutkimuskysymyksistä ja teoreettisesta viitekehyksestä. Tämän pohjalta kaikki haastatteluaineistot luokiteltiin ensin teemahaastattelun pääteemojenmukaisiin luokkiin: uhka- ja riskikuva, yritysvakoilun tavoitteet ja kohteet, keinot ja menetelmät, varautuminen ja suojautuminen ja tulevaisuuden trendit, haasteet, jatkotutkimusaiheet. Tämän jälkeen alkoi aineiston tarkempi analyysi ja aineistoa alettiin luokitella tarkempiin alaluokkiin. Esimerkiksi yritysvakoilun keinot ja menetelmät luokiteltiin tiedustelulajeihin ja toimintaympäristöihin, jotka jatko luokiteltiin eri tiedustelulajeittain (OSINT, HUMINT, GEOINT, SIGNINT/KYBINT) ja eri toimintaympäristöihin (fyysinen, sosiaalinen, digitaalinen, yhdistelmät). Samalla tunnistettiin haastateltavien vastauksista samankaltaisuudet, eriävät ja mahdolliset kriittiset näkökulmat sekä kehitettävät asiat. Luokiteltuja tietoja verrattiin toisiinsa ja tunnistettiin yhtymäkohdat sekä syy-seuraus-yhteydet. Esimerkiksi aineistosta nousi kiinteistö- ja rakennustoimialan erityispiirteitä, jotka altistivat yritysvakoilulle, ja joihin kohdistettiin yritysvakoilun keinovalikoimaa eri toimintaympäristöissä.

Luokittelumalli tuntui loogiselta ja mahdollisti aineiston systemaattisen läpikäynnin. Lisäksi aineistosta voitiin tunnistaa tutkittavan aiheen kannalta relevantit tiedot. Käytetty luokittelutapa ei välttämättä ole ainut ja oikea, mutta tällä tavalla koettiin saadun vastaukset tutkimusongelmaan ja -kysymyksiin. Kaikki seitsemän haastatteluaineistoa luokiteltiin ja analysointiin tarkasti ja samalla mekanismilla. Haastatteluaineistoista oli tunnistettavissa perusasioiden osalta yhtäläisyyksiä, joita haastateltavat täydensivät oman roolinsa näkökulmasta. Tämä mahdollisti sen, että aineistosta saatiin kokonaisvaltaisempi tutkittavan kohteen osalta.

5 TULOKSET

Tässä luvussa tarkastellaan teemahaastatteluiden pohjalta tehdyn analyysin tuloksia. Tuloksien avulla saadaan käsitys miten yritysvakoilu eli laiton tiedustelu ilmenee kiinteistö- ja rakennustoimialalla erityisesti valtion kiinteistökannan kontekstista tarkasteltuna. Haastatteluaineiston analyysin tuloksena nousi neljä pääteemaa, jotka ovat yritysvakoilun uhka, yritysvakoilun motiivit ja kohteet kiinteistö- ja rakennustoimialalla, yritysvakoilun keinot ja menetelmät sekä yritysvakoiluun varautuminen ja suojaustoimet.

Yritysvakoilun keinot ja menetelmät pääteema on luokiteltu edelleen kolmeen alateemaan, joita ovat fyysinen toimintaympäristö, sosiaalinen toimintaympäristö ja digitaalinen toimintaympäristö. Samoin yritysvakoilun varautuminen ja suojaustoimet pääteema sisältää kolme alateemaa, mitkä täydentävät varautumis- ja suojaustoimia erityisesti kiinteistö- ja rakennustoimialan näkökulmasta. Nämä alateemat ovat turvallisuuden hallinta, kiinteistön elinkaarenaikaiset turvallisuusmenettelyt ja sidosryhmäyhteistyö. Analysoinnin tuloksena voidaan osoittaa mitkä asiat ovat yritysvakoilun kohteena kiinteistö- ja rakennustoimialalla ja miksi, millä keinoin ja menetelmin yritysvakoilua harjoitetaan ja miten sitä vastaan voidaan varautua ja suojautua kiinteistö- ja rakennustoimialalla.

5.1 Yritysvakoilun uhka

Yritysvakoilun uhka -teema sisältää kaikki ne haastatteluiden keskustelut, joissa haastateltavat ovat tuoneet esiin millaisena uhkana ja riskinä he näkevät yritysvakoilun kiinteistö- ja rakennustoimialan kontekstissa ja mitkä tahot voivat olla sen taustalla. Teema sisältää myös ne keskustelut, joissa haastateltavat pohtivat miten uhka ymmärretään alalla ja sen toimijoiden keskuudessa. Lisäksi haastateltavat kertoivat minkälaisia seuraamuksia yritysvakoilusta voi pahimmillaan aiheutua niin yhteiskunnalle kuin valtionhallinnon organisaatioille.

Analyysin tuloksena voidaan todeta yritysvakoilun uhkan olevan merkittävä Suomen valtion omistaman kiinteistökannan näkökulmasta. Kiinteistö- ja

rakennustoimialan ei itsessään nähty olevan uhkan pääkohteena, vaan yritysvakoilun koettiin muodostavan konkreettisen uhkan erityisesti kriittiselle infrastruktuurille ja viranomaisten kohteille ja niissä toimiville valtionhallinnon organisaatioille, joille uhka on todellinen ja päivittäinen. Kybervakoilun koettiin korostuneen viimeisten vuosien aikana ja olevan kasvava uhka myös kiinteistö- ja rakennustoimialalle. Yhtenä syynä nähtiin tiedustelumenetelmien kehittyminen kustannustehokkaammaksi sekä aikaan ja paikkaan sitomattomiksi. Myös Weissbrodtin (2013) mukaan kybervakoilu tulee ottaa vakavana uhkana aiempaa suuremman kapasiteetin, kustannustehokkuuden ja matalariskisyyden vuoksi.

Uhkan merkittävyyden nähtiin korostuvan Ukrainan tilanteeseen peilaten kriisitilanteissa ja poikkeusoloissa, jolloin valtionhallinnon toimintaan pyritään vaikuttamaan joko fyysisesti lamauttamalla kriittisiä toimintoja tai hybridivaikuttamisen keinoin. Pahimmillaan haastateltavat kokivat vakoiluoperaatioiden seuraamuksien voivan olla fataalit niin yksittäiselle organisaatiolle, valtionhallinnolle kuin koko yhteiskunnalle. Palveluntuottajille uhkan merkittävyys näkyy puolestaan kiinteistönomistajan ja loppuasiakkaan asettamilla turvallisuusvaatimuksilla tietojen käsittelylle ja säilyttämiselle. Samalla he ovat itse tiedostaneet olevansa potentiaalinen yritysvakoilun kohde tuottaessaan palveluita ja ratkaisuja valtiollisille toimijoille kriittisiin kohteisiin.

”Valtiohallinnon piirissä tiedustelun uhka on todellinen ja sitähän tapahtuu koko ajan, joka päivä. Tiedustelutoiminta on kehittynyt huomattavasti vuosien varrella ja se on tullut kustannuksiltaan hyvin edulliseksi ja on kaikkien käytettävissä, mikä tekee siitä entistä haastavamman.” (H2)

”Uhka on merkittävä. Näkyy asiakkaalta tulevien ohjeistuksien ja vaatimuksien kautta tiedon käsittelyyn ja säilyttämiseen liittyen. Kun toimitetaan palveluita tai ratkaisuja valtiollisille toimijoille, niin ihan samaan tapaan meihin kohdistuu sitten laittoman tiedustelun uhka.” (H3)

”Pahimmillaanhan siinä puhutaan sellaisesta tiedosta, joka voi vaarantaa satojentuhansien ihmisten hengen. Jos ajatellaan nyt siis ihan meidän maanpuolustukseen liittyvää tietoa esimerkiksi ja Suomen ulko- ja turvallisuuspolitiikkaan liittyviä tietoja.” (H4)

"Uhka on konkreettinen. Jos julkisiin lähteisiin peilaan, että mitä esimerkiksi ukrainassa on tehty, niin kyllähän kriittinen infra ja viranomaisten kohteet on sellaisia mihin poikkeusoloissa pitää pystyä vaikuttamaan joko kineettisesti tai sitten jotenkin muuten lamauttamalla sitä hybridivaikuttamisen kautta." (H5)

"Yritysvakoilun uhka on merkittävä. Kyllä nämä kohteet, valtion kriittiset toimijat, ihan varmasti ovat tiedustelun kohteena ja ovat olleet jo vuosikymmeniä." (H6)

”Kyllähän se kybervakoilu on kasvava uhka myös kiinteistöalalla.”(H7)

Suojelupoliisin vuosikertomuksessa 2023 korostetaan Venäjän toiminnan olevan Suomen kansallisen turvallisuuden suurin uhka. Tutkimuksen konteksti huomioiden myös haastateltavat pitivät yritysvakoilun uhkan syntyvän todennäköisimpänä valtiollisten toimijoiden taholta, erityisesti Venäjä korostui keskusteluissa. Lisäksi Kiina, Iran ja Yhdysvallat mainittiin potentiaalisina valtiollisina toimijoina. Toisena toimijana nähtiin rikolliset kuten yksittäiset henkilöt, hakkerit, järjestäytyneen rikollisuuden edustajat tai valtiollisen toimijan värväämät henkilöt ja ryhmät kuten APT-ryhmät. Käyttäjälle rikollisryhmittymät ja heidän luomien peiteyrityksien käyttö näkyi erityisesti rakennushankkeissa. Kolmantena tahona nostettiin myös kilpailevat yritykset, jotka pyrkivät saamaan toisen yrityksen tietoa, osaamista tai teknologiaa.

”Mä puhun tiedustelusta valtiollisen toimijan ja sitten toisaalta tämmöisen rikostiedustelun näkökulmasta, että kohteethan saattavat sisältää tiedon lisäksi jotain materiaalia kuten rikollisia kiinnostavia aseita, räjähteitä tai muuta arvokasta omaisuutta.” (H1)

”Yhtenä esimerkkinä voin kertoa missä järjestäytyneen rikollisuuden edustajia oli mukana. Saneerattiin yhtä kohdetta, niin kaikki ne tiedot mitä siellä oli, niin on nyt osa rikollisten tiedossa. Mutta se että mitenkä niitä on käytetty ja missä ne ovat ja kenelle ne on vuodettu, sitähän ei tiedä. Meillähän oli useamman kuukauden seuranta tässä tapauksessa ennen kuin ne otettiin kiinni, kun niitä seurattiin kymmeniä yrityksiä. Mutta ei kukaan voi tietää mitä tietoa ne saivat ja mihin tarkoitukseen lopulta, kun eihän ne kerro.” (H2)

”Hakkeriryhmät, jotka toimivat valtiollisten toimijoiden alihankkijoina, työrukkasina. Kilpailevat yritykset, jotka pyrkivät saamaan meidän tietoa, osaamista ja teknologiaa.” (H3)

”Vähemmän Suomessa on näkynyt ei valtiollisten toimijoiden tai ääriliiketoimijoiden uhkaa toistaiseksi kriittisiin kohteisiin." (H4)

”Esimerkiksi APT-ryhmiä, jotka ovat ammattimaisia kyberrikollisia Venäjä tukee, ohjaa ja antaa heille kohteita. Valtiolliset toimijat kyllä, samoin Kiinassa, Iranissa on vastaavia ryhmiä, jotka saa sieltä tehtäviä ja resursseja.” (H7)

Osa haastateltavista nosti yhdeksi huolenaiheeksi ja konkreettiseksi uhkaksi erityisesti Venäjän tiedustelupalveluiden historian saatossa harjoittaman kyber- ja tiedustelutoiminnan. Nämä kohdistuivat Suomen yhteiskunnan toiminnan jatkuvuuden kannalta kriittisiin kohteisiin ja järjestelmiin, joista saadut tiedot voivat olla edelleen käytettävissä tulevaisuuden konfliktitilanteissa. Haastateltavat painottivat aiemmin menetetyn tiedon huomioonottamisen varautumistoimenpiteissä ja uusia kohteita rakentaessa.

"Jos puhutaan suojatiloista ja vitaaleista tiloista ja mikä liittyy esimerkiksi valtion jatkuvaan toimintaa kaikissa olosuhteissa, oli se sitten sota taikka mikä hyvänsä, niin ne tiedothan on kerätty varmasti. Tämmöinen ystävällismielinen itänaapurimmekin, mutta eihän niitä tietoja käytetä vasta, kun siinä vaiheessa, jos eskaloituu sota esimerkiksi. Mutta kyllä niillä ne tiedot siellä ovat, siihen on hyvä varautua." (H2)

”Uskon, että sitä tietoa, se perustieto, on jo silloin kerätty. Aikoinaan vierailevalle Venäläiselle delegaatiolle näytettiin erään kaupungin vesiverkostokuvat ja annettiin vielä ne ystävällisesti mukaan. Voi vaan miettiä minkälaisia vaikuttamisen mahdollisuuksia sitten tulee kaupungin vesiverkostoon.” (H6)

”Kyllähän Venäjä on, paitsi nyt vuoden 2020 jälkeen, mutta paljon sitä ennenkin, niin kartoittanut tasan tarkkaan, että missä menee kaapeleita ja missä on siirtoja ja minkälaisia rakennuksia sijaitsee missäkin.” (H7)

Edellä kuvatun mukaisesti yritysvakoilun uhkaa voidaan pitää todellisena. Tästä huolimatta osa haastateltavista nosti esiin, että edelleen kaikki organisaatiot kiinteistö- ja rakennustoimialalla eivät tiedosta ja ymmärrä yritysvakoilun uhkaa tai sitä vähätellään. Näihin organisaatioihin katsottiin kuuluvan niin kiinteistönomistajia kuin toimitusketjussa olevia palveluntuottajia. Haastatteluissa koettiin uhkatietoisuuden vaihtelevan myös valtionhallinnon sisällä ja avainhenkilöiden keskuudessa. Toisaalta haastatteluissa todettiin turvallisuustietoisuuden parantuneen viime vuosien aikana.

”Esimerkiksi erään valtionviraston korkea-arvoinen virkamies sanoi, kun olin sinne tekemässä turvallisuusjärjestelyitä, että minkä ihmeen takia tämmöistä tehdään, kun eihän meillä ole mitään varastettavaa. Tästä on nyt toki aikaa ja tilanne on parantunut.” (H2)

”Kaikki eivät ymmärrä sitä, että suojataan omaa bisnestä, muiden meille antamaa tietoa vastustajalta, joka voi olla valtiollinen taho, jolla on kyvykkyyttä tehdä asioita." (H5)

”Ja sitten, kun välttämättä ei ymmärretä just sitä, että voidaan olla välillisenä kohteena.” (H7)

"Esimerkiksi erään ison kumppanimme johtoryhmän jäseniä oli riskiarvioinnissa mukana ja silloin, kun tuotiin näitä erilaisia tiedusteluriskejä esiin, niin yhdeltä johtoryhmänjäseneltä tuli kommentti, että eikös nämä ole Remes -juttuja, että eihän nämä ole totta." (H3)

5.2 Yritysvakoilun motiivit ja kohteet kiinteistö- ja rakennustoimialalla

Vaikka kiinteistö- ja rakennustoimialan ei itsessään nähty olevan yritysvakoilun varsinainen kohde, sen merkitys välillisenä tiedustelun kohteena kasvaa sitä mukaan mitä kriittisempiä käyttäjiä, toimintoja, tietoja, järjestelmiä kiinteistöissä ja sille kuuluvissa maa- ja vesialueilla on. Yritysvakoilun ja tiedustelutoiminnan ensisijaisena tavoitteena nähtiin tiedonhankinta, jonka avulla kiinteistön käyttäjiin ja toiminnallisuuksiin voidaan kohdistaa poliittista, taloudellista ja toiminnallista vaikuttamista tai mahdollistaa toiminnan lamauttaminen tai tavoitellaan puhtaasti taloudellista hyötyä. Yritysvakoilun toimeksiantajan pyrkimyksenä on aina oman asemansa vahvistaminen ja tavoitteidensa edistäminen.

”Tiedustelulla ja laittomalla tiedustelulla, yritysvakoilulla pyritään yleisesti hankkimaan salassa pidettävää tai luottamuksellista tietoa. Toisinaan tavoitteena voi olla myös taloudellisten tai talouspoliittisten neuvotteluiden taustatietojen hankkiminen, jotta omalla maalla olisi etulyöntiasema neuvotteluissa. Lisäksi sotilaalliset tavoitteet voivat olla osa tiedustelutoimintaa, kuten sotilaallisen kyvykkyyden ja puolustusvalmiuden tiedustelu.”(H4)

Haastatteluaineistojen perusteella kiinteistö- ja rakennustoimiala tarjoaa useita kohteita ja mahdollisuuksia yritysvakoilulle. Haastatteluaineiston analyysin pohjalta voitiin muodostaa viisi asiakokonaisuutta, jotka altistavat yritysvakoilulle. Yksi merkittävä tekijä on **asiakkaat, ne valtion organisaatiot tai henkilöt**, joille kiinteistö- ja rakennustoimialan palveluita tuotetaan. Esimerkiksi, jos asiakkaat ovat itse valtiollisen tiedustelun kohteita tai heillä on tietoa, jota vieraat tahot haluavat saada haltuunsa, tämä voi tehdä palvelutuotantoketjussa olevasta toimijasta potentiaalisen kohteen tiedustelulle.

"Kiinteistö- ja rakennustoimiala sinänsä ei ole niin kiinnostava vaan se kiinnostaa, että kuka tulee sitä rakennusta käyttämään. Vakoilua harjoitetaan sekä yritysten että ulkomaisten toimijoiden kuten Venäjän, Kiinan ja Yhdysvallat taholta, ja se kohdistuu sekä poliittiseen että taloudelliseen tiedusteluun. Taloudellinen vakoilu voi vaikuttaa valtion päätöksiin ja yritystoimintaan merkittävästi, erityisesti EU-yhteyksissä. Valtiohan käsittelee suuria kokonaisuuksia yritystoiminnan kannalta. Ja niitä käsitellään valtion kiinteistöissä ja se kiinnostaa, koska siinä kysymyshän on miljardeista." (H2)

”Onko asiakkailla jotain sellaista tietoa tai toimintaa ja mihin kaikkeen asiakkaissa voidaan päästä teidän kautta käsiksi. Mihin kaikkiin suojattuihin toimitiloihin kiinteistö- ja rakennustoimialan toimijoilla on pääsy.” (H4)

Toiseksi merkittäväksi tekijäksi nähtiin **valtion kriittiset kohteet ja rakennukset**, joita pyritään saamaan selville niin valtiollisten toimijoiden kuin rikollisten

kautta. Kriittisiksi kohteiksi haastateltavat mainitsivat suojatilat, johtamiskeskukset ja johtamispaikat, konesalit, laite- ja palvelintilat sekä tilat, joissa voidaan käsitellä ja säilyttää turvaluokiteltua tietoa. Lisäksi mainittiin ase, ammus ja räjähdevarastot, jotka voivat olla erityisesti rikollisten toimijoiden kiinnostuksen kohteena. Tiedusteluviranomaisten ja asiantuntijahaastatteluiden mukaan tiedustelutoiminnot pyrkivät saamaan kriittisistä rakennuksista paikkatiedot, rakennustekniset tiedot, rakenne- ja pohjapiirustukset.

” Kiinteistö- ja rakennusalan kohteet voivat olla strategisesti tärkeitä kansalliselle turvallisuudelle, kuten esimerkiksi Puolustusvoimien ja Valtioneuvoston kohteet. Niiden kautta voi olla mahdollista vaikuttaa valtion toimintaan tai turvallisuuteen.” (H2)

”Turvallisuuskriittisten viranomaisten tiedot ja toiminnot, johtaminen, johtamiskeskukset, -paikat ja näihin liittyvät kriittiset kiinteistöt.” (H6)

"Jos ajatellaan sotilaallista tiedustelua tai ei valtiollisten toimijoiden kybervakoilua niin silloinhan kiinteistöalalla on iso rooli siinä, että yritetään selvittää kohteita, joiden kautta voidaan vaikuttaa valtion tai yhteiskunnan toimintaan tai ainakin vaikeuttaa sitä." (H7)

Kolmanneksi tekijäksi haastatteluissa nostettiin **kiinteistön ja rakennuksen kriittiset järjestelmät**, jotka nähtiin keskeisiksi yritysvakoilun kohteiksi, joiden kautta voidaan vaikeuttaa tai lamauttaa kohteen toimintaa tai mahdollistaa pääsy tiloihin tai järjestelmiin. Kriittisiksi järjestelmiksi mainittiin talotekniset järjestelmät (Taulukko 1) eli LVIS-järjestelmät sekä sähkötekniset tietojärjestelmät, joista korostettiin tietoverkkojärjestelmiä, turvallisuusjärjestelmiä sekä rakennus- ja kiinteistöautomaatiojärjestelmiä, joiden kautta voi ohjata ja valvoa muun muassa rakennuksen olosuhteita. Järjestelmistä pyritään lisäksi selvittämään niiden käyttöikä, sähkön ja veden tulopisteet ja millaiset varautumis- ja varajärjestelmät on rakennettu.

”Merkitys on siinä, että jos valtiollinen toimija vaikka nyt rikollisjärjestön kautta saisi rakennepiirustukset tai tietää ja ymmärtää turvallisuusjärjestelmistä ja mitä meillä on käytössä. Kyllähän se merkittävän uhkan muodostaa siinä, että vastustaja pääsee vaikuttamaan liian helposti. Ei tarvitse fyysisesti vaikuttaa mihinkään luolatilaan, jos sen pystyy lamauttamaan muuten sähköjärjestelmämme kautta.” (H5)

Kaikki haastateltavat toivat esiin myös **kiinteistönomistajan ja sen palveluntuottajan omassa käytössä olevat tilat ja järjestelmät**, joissa säilytetään ja käsitellään valtion kohteiden edellä mainittuja tietoja tai hallinnoidaan kohteessa olevia järjestelmiä, joita voidaan käyttää väylänä varsinaisen tavoitteen saavuttamiseksi. Lisäksi haastateltavat nostivat **yhteiskunnan kriittisen infrastruktuurin** (sähkön, veden, lämmön tuotanto ja jakelu, tiedonsiirto), mikä

pääsääntöisesti on yksityisen sektorin hallussa, mutta on huomioitava oleellisena osana kiinteistöjen ja rakennuksien toimintakykyä. Vastaavasti Meretvuon (2021) tutkimuksessa yritysvakoilun nähtiin kohdistuvan kriittiseen infrastruktuuriin saattaen sitä kautta aiheuttaa uhkan myös Suomen kansalliselle turvallisuudelle.

”Kiinteistönomistajan omassa käytössä olevat tilat ja järjestelmät, joissa em. tietoja kuten rakennusteknisiä tietoja säilytetään ja käsitellään.” (H6)

”Salassa pidettävä tieto kuten esimerkiksi asiakkaiden turvallisuusjärjestelmiin liittyvät tiedot sekä meidän tuotteiden ja ratkaisujen haavoittuvuudet.” (H3)

"Valtion kiinteistöt, mitkä oletettavasti voisivat joutua vaikutuksen kohteeksi, niin kyllähän se tieto mitä teillä on eri paikoista, pyritään saamaan selville tai kartoittamaan, että mitä järjestelmiä, kuinka vanhoja, miten niihin on varauduttu, mistä sähköt tulee, mistä vesi tulee." (H5)

”Kun tehdään sitä tiedustelua, niin siinä valmistellaan koko ajan sitten sitä kuinka pystytään lamauttamaan kohde ja sehän voi kohdistua sitten jonnekin LVIS-järjestelmään tai jätevesi ja energia ja tämän tyyppisiin asioihin, joilla pystytään hankaloittamaan huomattavasti muuta kuin verkkoinfraa, sitä palvelua. Jos se kohdistuu tämmöisiin, niin näillähän suorat vaikutukset myös yhteiskunnallisesti.”(H7)

Yhteenvetona yritysvakoilun motiivit ja kohteet -teemasta voidaan todeta valtion kiinteistöjen ja rakennuksien sekä siellä toimivien ja siihen yhdistyvien henkilöiden että järjestelmien muodostavan otollisen alustan yritysvakoilulle. Suomen valtion kiinteistö- ja rakennusinfrasta kartoitetut haavoittuvuudet ja kriittiset kohteet mahdollistavat yhteiskunnan toimintojen vaikeutumisen, Suomen päätöksentekojärjestelmään vaikuttamisen ja johtamistoiminnan lamauttamisen, mikäli kriittisiä tiloja ja tietojärjestelmiä ei kyetä pitämään käytettävissä ja toimintakuntoisina. Yritysvakoilun keinoin ja menetelmin saatujen tietojen pohjalta luodaan edellytykset muille operaatioille, jotka erityisesti kriisitilanteissa ja poikkeusoloissa voivat olla kohteelle katastrofaaliset.

"Eli jos tulisi se, että me ollaan vaikka sodassa Venäjän kanssa, niin heidän pitää ymmärtää se, että mitä on rakennettu, minne, mikä pitää lamauttaa ja mitä se vaatii." (H5)

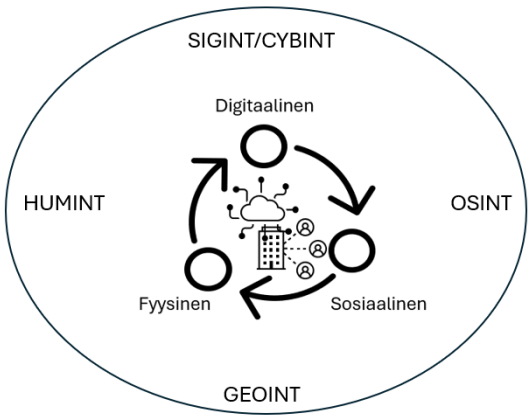
5.3 Yritysvakoilun keinot ja menetelmät

Yritysvakoilun keinot ja menetelmät -teema sisältää kaikki ne haastattelukeskustelut, joissa haastateltavat ovat tuoneet esiin millä keinoin ja menetelmin yritysvakoilua voidaan toteuttaa kiinteistö- ja rakennustoimialalla sen erityispiirteiden tuomia haavoittuvuuksia hyödyntäen. Keinot ja menetelmät ovat luokiteltu

edelleen kolmeen alateemaan, jotka ovat Valtion toimitilastrategiaa mukaillen fyysinen toimintaympäristö, sosiaalinen toimintaympäristö ja digitaalinen toimintaympäristö. Analyysin tuloksena voidaan todeta yritysvakoilua toteutettavan monin eri keinoin, eri tiedustelulajien keinovalikoimia ja toimintaympäristöjä yhdistelemällä. Tätä on havainnollistettu kuviossa 7. Tiedustelulajeista ainoastaan mittaus- ja tunnusmerkkitiedustelu (MASINT) ei noussut suoranaisesti haastatteluissa, jonka vuoksi sitä ei ole huomioituna alla olevassa kuviossa.

Tiedustelulajeista oleellisimpana tiedonhankintakeinona nähtiin kaikkien haastateltavien mukaan avointenlähteiden tiedustelu (OSINT) erityisesti, kun asiaa tarkastellaan kiinteistö- ja rakennustoimialan ja suomalaisen avoimen yhteiskunnan näkökulmasta. Avointen lähteiden tiedustelu muodostaa myös pohjan kaikille muille tiedustelulajeille ja sisältyy kaikkiin toimintaympäristöihin.

Tiedusteluviranomaisten ja asiantuntijoiden haastatteluissa korostettiin tiedustelulajien ja menetelmien menevän limittäin ja ristiin. Toinen menetelmä vahvistaa toista menetelmää tai täydentää toisesta toimintaympäristöstä saatua tietoa. Yleensä tiedusteluoperaatiot aloitetaan avointen lähteiden tiedustelulla eli selvitetään mitä tietoja on jo saatavilla julkisista, kaikille avoimista lähteistä. Saatua tietoa voidaan sen jälkeen tarvittaessa täydentää esimerkiksi kybertiedustelun ja henkilötiedustelun keinoin, jotta saadaan kattavampi kuva halutusta asiasta. Haastatteluiden mukaan koko yritysvakoilun keinovalikoima on käytössä, riippumatta siitä onko kyseessä valtiollinen toimija tai ei-valtiollinen toimija.



KUVIO 7 Tiedustelulajit ja toimintaympäristöt

” Käytetään useita eri tiedustelulajeja ja näiden tiedot yhdistämällä saadaan tieto tai ainakin osa tieto siihen tiedustelukysymykseen mitä tietoa ollaan hakemassa. Sitä ei ole syytä ajatella aina yksipuolisesti, että yhdellä keinolla tehtäisiin joku asia, vaan yleensä esimerkiksi kyberkeino vaatii paljon avoimien lähteiden tiedustelua, henkilötiedusteluosaamista niin, että se toimenpide edes onnistuu.” (H1)

”Tiedustelupalveluiden tarve perimmältään on ollut sama, että sitä tietoa hankitaan kaikilla mahdollisilla keinoilla, tiedustelulajeista ja julkiset lähteet siellä se ihan ykkösprioriteetti.” (H6)

5.3.1 Fyysinen toimintaympäristö

Wimmerin (2015) mukaan yritysvakoilu ja tiedustelu ei rajoitu fyysisessä toimintaympäristössä pelkästään organisaation toimipaikkaan, vaan sitä voi tapahtua esimerkiksi kotona, matkoilla ja liikennevälineissä. Tämä mikä todettiin myös haastateltavien taholta. Haastatteluaineistosta yhtenä keinona nousi fyysinen tarkkailu ja havainnointi, jossa voidaan hyödyntää teknisiä laitteita kuten droneja. Ihmisten, kiinteistöjen ja rakennuksien, rakennustyömaiden sekä niiden ympäristöjen **fyysisen tarkkailun ja havainnoinnin** kautta saadaan selvitettyä tietoa kohteen heikkouksista, työntekijöistä, palveluntuottajista, urakoitsijoista, rakenteista, kaapeleista ja toiminnasta. Muun muassa rakennuskyltit, jotka ovat kaikkien nähtävillä, tuotiin käyttäjähaastattelussa esiin. Rakennuskylteissä kerrotaan mitä rakennetaan, kuka rakentaa, millä aikataululla ja kenelle.

Toisena keinona nähtiin **rakennukseen, tilaan tai työmaalle tunkeutuminen**, joko fyysisesti murtautumalla, toisen henkilön avustuksella tai soluttautumalla. **Soluttautumisen** koettiin olevan mahdollista hyödyntäen kiinteistö- ja rakennustoimialan laajaa toimittajaverkostoa ja toimitusketjua. Esimerkkeinä nostettiin kiinteistön huoltoa, ylläpitoa, valvontaa tekevän palveluntuottajan työntekijäksi tai työmaaurakoitsijaksi tekeytyminen toimittajien logolla olevia vaatteita ja varusteita hyödyntäen. Erityisesti rakennustyömaat nähtiin otollisiksi hetkiksi soluttautumisille, jolloin työmaalla liikkuu yhtäaikaisesti useita toimijoita lyhyillä aikajaksoilla, jolloin materiaalivirrat ja henkilöliikenne on suurimmillaan.

”Kun näitä kiinteistöjä rakennetaan, niin silloinhan ujutetaan niitä ihmisiä sinne töihin, että ne saa ne kaikki tiedot. Tästä on jo vuosia, mutta oli venäläinen naisinsinööri, mikä oli rakennussiivoojana ja, kun rakennussaneeraus valmistui, niin hän häipyi Venäjälle. Ja varmaan vei kaikki mahdolliset tiedot.” (H2)

"Lukkoliikkeiden ja raksafirmojen huolto- ja asennusautot ja huoltoautot. Nehän on perinteisen rikollisuuden suuressa suosiossa, että siellä on työkaluja mitkä on helppo muuttaa rahaksi. Parisen vuotta takaperin oli jälleen kerran korkattu yksi huoltoauto, mutta sieltä ei oltu viety mitään muuta kuin työvaatteita. Kaikki muu jätetty paikoilleen. Tämä herättää omat epäilynsä mitä tavoiteltu, mutta vaikea todeta onko nyt tiedustelumielessä vai rikoksentekomielessä viety vaatteet. Mutta kyllähän turvasuojakamppeet päällä on päässyt aika pitkälle ja sen jälkeen tuli meillekin sitten muutos, ettei työvaatteita säilytetä autossa eikä muutenkaan niin, että niihin on ulkopuolelta pääsy." (H3)

”Taannoin kahteen vedenpuhdistamoon murtauduttiin saman yön aikana ja niistä varastettiin etäohjausyksiköt. Yritys, joka oli tehnyt vedenpuhdistamon automaatiojärjestelmän tuottaa palveluita myös eräälle valtion organisaatiolle.

Samaan aikaan lähistöllä oli havaittu olevan ulkomaisen valtion omistuksessa olevia puhelimia. Voi vaan taas miettiä oliko sattumaa ja kyseessä vaan normi murto…" (H5)

Kolmantena keinona haastateltavat nostivat **fyysisen kontaktoitumisen** ja kohdehenkilön lähipiiriin pääsemisen. Fyysisessä ympäristössä keinon tavoitteena on haastattelujen perusteella löytää henkilö, jolla on pääsy tietoon tai pääsy halutulle alueelle, rakennukseen, tilaan tai laitteelle. Kontaktoituminen ei katso aikaa tai paikkaa ja voi tapahtua esimerkiksi harrastustoiminnan parissa. Tiedusteluviranomaisten edustajat toivat myös esiin, ettei kohdehenkilöllä itsellään välttämättä tarvitse olla suoraa pääsyä kriittiseen tilaan tai salassa pidettävään tietoon. Toisinaan pääsy kohdeorganisaation toimitiloihin riittää edistämään operaatiota. Henkilön avulla voidaan **varastaa tai kopioida** tietoja kuten fyysisiä rakennus- ja rakennepiirustuksia, järjestelmäpiirustuksia tai laitteita ja muuta omaisuutta. Sisällä olevan henkilön avulla voidaan myös ottaa tallenteita rakenteista, tiloista, laitteista, kaapeleista ja tiloissa olevista henkilöistä, joita voidaan tarvittaessa käyttää lisätietojen saannissa. Lisäksi kohdehenkilön kautta tiloihin, kaapeleihin ja rakenteisiin tai laitteisiin voidaan **asentaa teknisiä häirintä- tai valvontalaitteita**, jotka aiheuttavat tilassa oleville laitteille häiriötä tai lähettävät tietoja tilan ulkopuolelle. Hän voi myös mahdollistaa ulkopuoliselle henkilölle pääsyn kohteeseen.

"Huolto- ja korjaustoimintaan, kiinteistötekniseen toimintaan, liittyvä henkilö, joka toimii ulkovaltojen tiedustelupalvelun tai rikollistoiminnan lukuun, hankkiakseen sieltä kohteesta tietoa esimerkiksi missä kohdassa siellä kiinteistössä on todennäköisesti se parhaiten suojattu paikka eli mihin ei pääse ilman saattajaa, mihin on lukitukset tai kulunvalvonta rakennettu niin, että sinne ei selvästikään pääse kuten vapaille vyöhykkeille pääse." (H1)

"Sillä ei välttämättä ole edes tiedustelupalvelun kannalta niin kauheasti aina väliä, että pääseekö henkilö suoraan johonkin suojattavan tietoon, että ihan pelkästään se pääsy kohdeorganisaation verkkoon voi riittää. Mutta myös se pääsy kohde organisaation toimitiloihin voi riittää joissain tapauksissa." (H4)

5.3.2 Sosiaalinen toimintaympäristö

Sosiaalisessa toimintaympäristössä tapahtuvat yritysvakoilun menetelmät edellyttävät ihmisten kanssa käytävää vuorovaikutusta. Vuorovaikutustilanteet voivat tapahtua fyysisesti kasvokkain, viestintävälineitä tai sosiaalisenmedian alustoja käyttämällä. Sosiaalisesta toimintaympäristöstä tulevat riskit koettiin haastatteluissa merkittävinä, jossa ihminen kaikkine heikkouksineen ja vahvuuksineen on keskiössä. Käytettävinä yritysvakoilua edistävinä keinoina korostuivat haastattelujen pohjalta **maalittaminen, sosiaalinen manipulointi ja kiristys, värvääminen ja sisäpiiritoimija**. Näitä keinoja edeltää kohdehenkilön taustatietojen, toimintatapojen, heikkouksien ja mieltymyksien selvittäminen pääsääntöisesti avoimia lähteitä käyttäen. Lisäksi kohdehenkilön etnisen taustan tai

sukulaissuhteen kerrottiin voivan altistaa yhteistyöhön painostamisen tai kiristyksen keinoin. Erityisesti haastateltavat mainitsivat Venäjän ja Kiinan kansalaisten tai kaksoiskansalaisiin kohdistuvan uhkan.

Tiedusteluviranomaisten edustajat toivat lisäksi erityisenä huolena myös sosiaalisessa mediassa organisaatioiden ja henkilöiden julkaisemat tiedot (kuvat, kirjoitukset) esimerkiksi liikekumppaneista, rakennushankkeista, työtehtävistä ja projekteista, joissa ovat mukana ja voivat näin tahattomasti paljastaa arkaluontoista tietoa. Nämä tiedot voivat itsessään herättää mielenkiinnon tiedustelupalveluissa ja rikollisissa toimijoissa altistaen organisaatiot ja henkilöt maalittamisen ja yritysvakoilun kohteeksi.

"Monissa työpaikoissa ihmisiä myös kannustetaan jakamaan tietoa itsestään ja työstään aika paljon, että se on semmoinen mikä tavallaan altistaa. Kannattaa miettiä kuinka avoimesti organisaatiot haluaa esimerkiksi työntekijätietoja, yhteystietoja ja työntekijöitä vaikkapa tehtävänkuvia jaella verkossa" (H4)

”Mitä ihmiset kertovat itse työtehtävistään, työpaikoistaan, jossa työskentelevät. Joillakin oli esimerkiksi muutama vuosi takaperin valtava tarve kertoa meidän strategisista kumppaneistamme ja toimivansa eräässä merkittävässä hankkeessa." (H5)

Haastatteluiden perusteella yhdeksi keskeiseksi keinoksi nousi henkilön värväämineN. Vaikka se voi tapahtua myös fyysisessä toimintaympäristössä korostui haastateltavien keskusteluissa sosiaalisen median alustojen kuten LinkedIn käyttö henkilön vaikuttamis- ja värväyskanavana. Tällöin henkilöä voidaan lähestyä valeprofiilien kautta, jolloin kohteella ei ole todellista tietoa kenen ja minkä tahon kanssa on vuorovaikutuksessa. Tiedusteluviranomaisten ja asiantuntijoiden mukaan tämä antaa tekijälle myös suojan ja tekee värväysprosessista riskittömämmän verrattuna fyysisessä toimintaympäristössä tehtävään värväykseen. Värväyksen kohteina voivat olla suoraan kohdeorganisaatiossa toimivat henkilöt tai toimittajaverkostossa olevat kuten kriittisten palvelinten ylläpitäjät ja pääkäyttäjät, rakennuttajakonsultit, suunnittelijat ja muut henkilöt, joilla on tieto salassa pidettävistä tiedoista. Sisäpiiritoimijaa (engl. insider) pidettiin haastatteluiden perusteella kaikkein merkittävimpänä uhkana. Tällöin henkilö toimii tietoisesti omaa työnantajaansa tai tilaajaansa vastoin omaten laillisen pääsyn tietoon tai tilaan ja tuntee kohteen toimintatavat. Lisäksi haastatteluissa tuotiin esiin valtiollisten toimijoiden voivan värvätä myös rikollistoimijoita, joilla ensi sijassa ei ole aiempaa rikosrekisteriä. Pyrkimyksenä on asettaa näitä henkilöitä valtion kohteisiin eri tehtäviin kuten vartijoiksi ja siivoojiksi, hyödyntäen heitä omien tarkoitusperien saavuttamiseksi. Haastateltavat myös kertoivat, että sisäpiiritoimijaa on ennakkoon vaikea havaita, mikä entisestään korostaa uhkan merkittävyyttä. Yleensä tilanne havaitaan vasta siinä vaiheessa, kun jotain on jo tapahtunut. Sisäpiiriuhkaa onkin haastateltavien mielestä käytännössä vaikea estää kokonaan, mutta sitä voidaan minimoida ennakoivalla riskienhallinnalla.

”Henkilötiedustelua voidaan tehdä myös sosiaalisessa mediassa, eli voidaan käyttää esimerkiksi LinkedIniä. Valeprofiilin kautta voidaan pyrkiä myös loppukädessä värväämään henkilöä toimimaan tiedustelupalvelun hyväksi.” (H4)

"Yksi vaarallisimpia asioita mitä on olemassa. Insider on aina uhka varsinkin, jos se on admin tai vastaavassa tehtävässä missä se pääsee liikaan tietoon käsiksi.” (H5)

”Rikollisuuden edustaja joko peiteyritysten kautta pystyy toimittamaan työntekijöitä toimitusketjuun ja peiteyritys saattaa olla tiedustelupalvelun värväämä. Siitä on merkkejä maailmalla, että valtiollinen toimija on käyttänyt rikollisjärjestöjä oman toimintansa peittämiseen ja sen tehtävän toteuttamiseen. Myös sen rikollisjärjestön oma intressi voi olla jos kysymyksessä.” (H1)

"Valtiolliset toimijat värväävät rikollistoimijoita. Nehän hakee sellaisia henkilöitä, joilla on puhtaat taustat ja ne asettaa niitä erilaisiin esimerkiksi valtion työpaikkoihin ja kohteisiin. Niitä voi olla siivoojat, vartijat ja kaikki mitkä käsittelee tietoa tai saa pääsyn tilaan, niin nehän yrittää ujuttaa niitä sisälle sinne. Sehän on ihan todettu se toiminta ja siinähän on kärähtänytkin näitä ihmisiä." (H2)

"Eniten olisin huolissani social engineeristä. Saa olla todella hereillä, että sellaisen tunnistamaan, jos teon takana on valtiollinen toimija." (H3)

Huomioiden kiinteistö- ja rakennustoimialan laajat toimittajaverkostot useamman haastateltavan näkökulmasta yhdeksi merkittäväksi tiedonhankinta ja vaikuttamiskeinoksi koettiin sosiaalinen manipulointi (engl. Social Engineering). Manipulointitekniikassa hyödynnetään inhimillistä virhettä tiedon, pääsyn tai muun asian saamiseksi. Mann (2017) mukaan tavoitteena on saada kohdehenkilö tekemään hänen etujensa vastaisia asioita kuten paljastamaan tietoja, levittämään haittaohjelmatartuntoja tai antamaan pääsyn rajoitettuihin järjestelmiin. Sosiaalisessa manipulaatiossa hyödynnetään kohdehenkilöstä kartoitettuja haavoittuvuuksia ja se tapahtuu yleensä yhdistämällä yhtäaikaisesti sosiaalista ja digitaalista toimintaympäristöä.

5.3.3 Digitaalinen toimintaympäristö

Digitaalisessa toimintaympäristössä tapahtuvissa yritysvakoilun menetelmissä ja keinoissa hyödynnetään digitaalista (kyber) ympäristöä, tietoverkkoja ja niihin liitettyjä laitteita sekä ohjelmistoja. Tehtäviä toimenpiteitä voidaan kohdistaa digitaalisen toimintaympäristön lisäksi myös fyysiseen ja sosiaaliseen toimintaympäristöön. Haastateltavien mukaan digitaalisessa toimintaympäristössä tapahtuvien menetelmien ja teknologioiden kehittyessä kybertiedustelun ja -vakoilun uhka on entisestään kasvava myös kiinteistö- ja rakennustoimialalla. Tätä selittää osaltaan digitaalisten järjestelmien ja palveluiden käytön laajeneminen, jolloin haavoittuvuuspinta-ala on aiempaa suurempi. Esimerkkinä haastatteluissa

nostettiin LVIS-järjestelmien ja laitteiden liittäminen verkkoon (engl. IoT, Internet of Things).

Asiantuntijahaastattelun mukaan IoT-alustaan kohdistuu laajenevissa määrin kyberrikollisuuden ja erityisesti kybervakoilun uhkaa sen tietoturvahaavoittuvuuksien vuoksi. Kybervakoilun näkökulmasta osa valmistajista voi jättää laitteisiin tahallisesti haavoittuvuuksia toimiessaan jonkin yrityksen tai valtion lukuun. Esimerkiksi kiinteistöautomaatiojärjestelmän kautta voidaan tunkeutua kohdeorganisaation muuhun verkkoon tai pyrkiä lamaannuttamaan kohteen toiminta. Tietoturvayhtiö Kasperskyn mukaan IoT-järjestelmiin kohdistui vuoden 2021 alkupuoliskon aikana 1,51 miljardia kyberhyökkäystä.

”Meillä yleensä kaikki toimii verkossa rakennusautomaation kautta ja, jos pääsee rakennusautomaation sisälle, niin sen koko kiinteistön toiminta pystytään lamauttamaan.” (H2)

"Se on tavallaan iso osa verkkoa, mikä tulee IoT -laitteiden kanssa. Ja kaikkihan säädetään nykyaikaisessa kiinteistössä verkon kautta ja, jos pääset vaikuttamaan sinne, niin tuota kaksi toiminen vielä, että sitä kautta pystyy vaikuttamaan konkreettisesti kiinteistön toimintaan ja pyrkiä lamauttamaan toiminto, mutta sitä kautta pystyy myös pääsemään harjoittaman kybervakoilua." (H7)

Haastateltavat korostivat poikkeuksetta **avointen lähteiden tiedustelua** ensisijaisena tiedonhankintakeinona digitaalisessa toimintaympäristössä. Merkittävä osa Suomen valtion kiinteistö- ja rakennustiedoista sekä yhteiskunnan kriittiseen infraan liittyvästä tiedosta saadaan haettua avoimesti internetistä. Tällaisina tietoina nähtiin haastattelujen perusteella rakennusvalvonnan rakennuspiirustukset ja suunnitelmat, maa- ja merikaapeleiden sijainnit, energiaverkostot, kiinteistörekisteri sekä kartta- ja paikkatiedot että pelastussuunnitelmat. Kun näihin yhdistetään vielä asiantuntijahaastattelun mukaisesti signaali- ja geotiedustelulajien menetelmin saatuja viestiliikennetietoja sekä satelliitti- ja ilmakuvia, on vastapuolen tiedustelupalvelulla varsin kattava kuva Suomen infrastruktuurista. Lisäksi valtionhallinnon näkökulmasta mainittiin myös julkisten hankintojen palvelu Hilma, jonka kautta saa tietoa julkisen sektorin käynnissä olevista ja tulevista hankkeista ja hankinnoista sekä päättyneiden kilpailutuksien tuloksista.

”Viime aikoina näitä merellisen infran turvallisuutta pyöritelty julkisesti ja siellä on aina hyvin selkeästi tietoliikennekaapelitkin mitä Itämerellä kulkee. Ne on iloisesti siellä aina kaikissa kartoissa. Meidän yhteiskuntamme nojaa hirveän paljon avoimuuteen. Meillä on kaikkien kriittisten kohteiden tiedot avoimesti netissä, mutta tarvitseeko niiden välttämättä olla, siihen keskusteluun ollaan ehkä nyt herätty.” (H4)

”Julkiset hankinnat mitä meilläkin tehdään, niin ovat julkisia lähteitä, joita kautta tiedustelupalvelut kollaavat niitäkin sivustoja ja hakevat tietoa ja myös sitä verkostoitumisen mahdollisuutta.” (H6)

”Suomihan on aika avoin yhteiskunta, että jos palaan tähän kiinteistö- ja rakennustoimialaan, niin kaikki rakennusluvat ja johtotiet ja kaikki on suurin piirtein kaikkien saatavilla. Ilmaiseksi netistä tyyliin löytyy, että sehän on tässä mielessä pöyristyttävä kääntöpuoli tälle avoimelle yhteiskunnalle." (H7)

Haastateltavien mukaan avoimen yhteiskunnan kääntöpuolena on sen tuomat riskit yhteiskunnan kokonaisturvallisuudelle. Valtiollisille tiedustelupalveluille ja rikollistoimijoille on mahdollistettu tehokas ja riskitön, luvanvarainen, tiedonhankinta, jonka avulla voidaan kartoittaa niin yhteiskunnan kuin valtion kiinteistökannan sekä niihin liittyvien palveluiden haavoittuvuuksia. Näitä haavoittuvuuksia vastapuoli voi halutessaan käyttää vaikuttamiseen ja toimintojen lamauttamiseen.

”Esimerkki, eräs virasto jakoi taannoin matalavesiväylien kaikki kartastot. Se oli viikon verran näkyvissä. Sittenhän se poistettiin, mutta… Meillä ei välttämättä viranomaistahot ymmärrä tai sitten virkamiehistö ei ymmärrä sitä, että miten voi vastustaja hyödyntää erinäisiä julkisia lähteitä mitä on olemassa..., niin kyllä mä väitän silloin, että me ollaan liian avoin." (H5)

”Tiedustelupalvelut lukevat niitä kuin avointa kirjaa ja sieltä on aika helppo niitä raportteja tehdä ja etsiä tämän yhteiskunnan haavoittuvuuksia, kun halutaan vaikuttaa.” (H6)

Kuten aiemmin on todettu valtiolliset toimijat ja rikolliset ovat yhä enenemissä määrin siirtyneet hyödyntämään verkkoympäristöä. Verkkoympäristö tuo rikollisille toimijoille suojan. Tällä tarkoitetaan teon kiistettävyyttä, jolloin tekijätahoa ei voida osoittaa suoraan, mikä on tiedusteluviranomaisten mukaan erityisesti valtiollisille toimijoille tärkeää. Kybervakoilu ja -hyökkäysoperaatioiden tekeminen on myös helpottunut viimeisten vuosien aikana. Asiantuntijahaastattelun mukaan tekijällä ei tarvitse olla enää omaa osaamista vaan hän voi ostaa sen palveluna. I-Lead:n (2020) mukaan toimintamalli on tällä hetkellä yksi kasvavista trendeistä kyberrikollisuuden piirissä. **CaaS (engl. Crime-as-a-Service) -palvelun** tavoitteena on tarjota vähemmän koulutetuille kyberrikollisille kyvykkyyttä kyberoperaatioiden suorittamiseen. Palvelusta voi ostaa vahinkoihin nähden edulliseen hintaan esimerkiksi haittaohjelmia ja varastettuja henkilö- ja taloustietoja. Tämä mahdollistaa perinteisten rikollisten keinovalikoiman laajenemisen.

Haastatteluiden perusteella keskeisimmiksi kybervakoilu ja -hyökkäysoperaatioiden keinoiksi nousivat **kohdennetut hyökkäykset, kiristys- ja haittaohjelmat**. Kybervakoilun yhtenä petollisimpana menetelmänä voidaan haastatteluiden mukaan pitää kohdistettua hyökkäystä eli APT (engl. Advanced Persistent Threat) -hyökkäystä. APT-hyökkäyksien takana on ammattimaiset

kyberrikolliset, joita valtiolliset toimijat tukevat. Venäjän valtio käyttää kybertoimintansa ja osaamisensa kehittämiseen toimijoiden verkostoa, johon kuuluu muun muassa kyberrikollisia, valtion luomia peiteyrityksiä, yksittäisiä ICT-kehittäjiä ja hakkereita (Aitel&Co, 2022). ECIPE:n vuonna 2018 tekemän tutkimuksen mukaan kohdennettu hyökkäys on erittäin pitkälle kehitetty ja jatkuva prosessi, johon kuuluu pitkän aikavälin tietojen seuranta ja varastaminen kohteesta. Tyypillisesti siihen liittyy pääsyn jatkuva vahvistaminen ja syventäminen ajan myötä. Kehittyneisyytensä vuoksi kohdistettua hyökkäystä on vaikea havaita ja se voi kestää useita vuosia huomaamattomana. Asiantuntijahaastattelussa tuotiinkin esiin, etteivät kohteeksi joutuneet organisaatiot välttämättä edes huomaa olevansa kybervakoilun kohteena. Myös Lehdon ym. (2018) mukaan rikollistahojen lisäksi yritysvakoiluun tähtääviä APT-hyökkäyksiä tekevät myös valtiolliset tiedusteluorganisaatiot, ja organisaatioilla on todennetusti vaikeuksia havaita tällaisia suunnitelmallisia ja kehittyneitä hyökkäyksiä. Potentiaalisina kohteina nähtiin toimittajaverkostossa olevat yritykset, joiden kybermaturiteetti ei ole samalla tasolla kuin arvoketjun kovimmalla brändillä. Toimittajien kautta pyritään etsimään reittiä varsinaiseen kohteeseen tai tietoon. Esimerkiksi rakennushankkeiden suunnitelmista ja tietomalleista, joiden avulla voidaan hahmottaa yksityiskohtaisesti rakennuskohteiden ja niiden ominaisuustietoja kolmiulotteisesti.

”Tehokkain tapa päästä sisään on se APT-toimija, joka käy korkkaamassa sen alihankintaketjutuksen. Pyrkien löytämään sieltä hyökkäysvektorin ja varsinaiseen kohteeseen. ...Yhdessä tapauksessa meidän sopimuskumppaneita ei korkattu, mutta sitten löytyy yhtäkkiä heti saman päivän aikana kolme alihankintaketjutuksessa ollutta yritystä ja yksi niistä oli esimerkiksi arkkitehtiyritys, joka tekee rakennepiirustukset tiettyihin kohteisiin.” (H5)

”Esimerkiksi APT-ryhmiä, jotka ovat ammattimaisia kyberrikollisia, joita Venäjä tukee, ohjaa ja antaa heille kohteita. Samoin Kiinassa, Iranissa on vastaavia ryhmiä, jotka saa sieltä tehtäviä ja resursseja.” (H7)

”Ainahan se on minusta helpompaa tulla palvelutuotantoketjun kautta, koska ne turvallisuuskontrollit eivät ihan niin hyvät ole, kun viranomaisella itsellä." (H6)

Kybervakoilun ja -operaation nähtiin haastattelujen perusteella alkavan yleensä huijausviestillä, jonka kautta haittaohjelma ujutetaan kohdeorganisaationa olleen tietoverkkoon. Viestin kohteena olevan henkilön asemalla tai tehtävällä ei nähty olevan merkitystä. Asiantuntijahaastattelun mukaan esimerkiksi kiristyshaittaohjelmaa voidaan käyttää myös hämäyksenä järjestelmään pääsemiseksi ja tietojen saamiseksi. Tiedusteluviranomaisten haastatteluissa nostettiinkin kiristyshaittaohjelmiin varautuminen yhdeksi asiaksi, johon kiinteistö- ja rakennustoimialan kannustettiin kiinnittävän huomiota erityisesti, jos joutuu valtiollisen toimijan kohteeksi.

”Tehtävätasosta riippumatta henkilöstölle tulevat tämmöiset hyvinkin räätälöidyt haittaohjelmaviestit eli varsin aidon näköiset kalasteluviestit, joissa sitten todellisuudessa taustalla onkin valtiollisen toimijan haittaohjelma. Ei tarvitse olla mikään johtotason tai avainhenkilötason työntekijä vaan pääsy sinne organisaation tietoverkkoon riittää, koska silloin henkilön kautta voi pyrkiä tällainen pahis uimaan sisään.” (H4)

”Tyypillisin keino on se, että ujutetaan jotain kautta haittaohjelma yrityksen järjestelmiin, siellä kerätään tietoa ja tiedustellaan. Se voi olla pitkänkin ajan järjestelmissä, vuoden kaksi, tiedusteluvaihetta tai se voi jatkua koko ajan ennen kuin sitten joku antaa merkit, että pitää jotain tehdä. Mutta kyllä ne ihan samalla tavalla kuin vaikka kiristyshaittaohjelmat toimivat ja kiristyshaittaohjelmiakin voidaan käyttää hämäykseksi siihen, että päästään sinne järjestelmiin ja saadaan sieltä tietoa. Sitten dumpataan ulos jne. ” (H7)

Asiantuntijahaastattelussa tuotiin esiin yhtenä esimerkkitapauksena Iranin ydinvoimalaitokseen vuonna 2010 kohdistettu Stuxnet kyberhyökkäys. Ylen (2011) ja Suomen kuvalehden (2010) mukaan Stuxnet-mato oli suunniteltu aiheuttamaan fyysistä tuhoa laitoksen teollisuusautomaatiojärjestelmän taajuusmuuntimiin. Haittaohjelma oli tunkeutunut järjestelmään, joka ohjaa rikastamisessa käytettäviä sentrifugeja ja koko laitos oli onnistuttu lamauttamaan. Kohteena ollutta ydinvoimalaitosta ei ollut tuolloin kytkettynä internettiin, joten haittaohjelma oli viety laitoksen palvelimille ulkoisen kovalevyn kuten muistitikun kautta. Suomen kuvalehden (2010) mukaan hyökkäyksen taustalla ollut taho oli onnistunut salakuljettamaan saastutettuja muistitikkuja ydinohjelmassa työskennelleiden venäläisten teknikkojen tarvikevarastoon. Kun teknikot käyttivät muistitikkujaan, pääsi Stuxnet -haittaohjelma ydinlaitoksen palvelimille. Ylen (2011) artikkelin mukaan Stuxnet-matoa käytettiin myös vakoiluun lähettäen tietoja laitoksesta kahdelle muulle palvelimelle. Madon löydyttyä siitä toimitettiin tiedot tietoturvayrityksien hälytyssivuille, jotka joutuivat puolestaan verkkohyökkäyksen kohteiksi ja haittaohjelman levittäjä ehti sillä aikaa hävittää jäljet itsestään.

Edellä kuvattu esimerkkitapaus kokoaa hyvin yhteen yritysvakoilun keinojen ja menetelmien monitahoisuuden. Se on erinomainen kuvaus kompleksisesta vakoiluoperaatiosta, jonka tavoitteena oli lamauttaa kriittisen infrastruktuurin kohde teollisuusautomaatiojärjestelmän kautta. Ja, jossa oli käytetty sosiaalisen, digitaalisen ja fyysisen toimintaympäristön yritysvakoilun keinoja.

5.4 Yritysvakoiluun varautuminen ja suojaustoimet

Yritysvakoiluun varautuminen ja suojaustoimet -teema sisältää kaikki ne haastattelukeskustelut, joissa haastateltavat ovat tuoneet esiin miten yritysvakoilua vastaan voidaan varautua ja millaisia suojaustoimenpiteitä tulee ottaa huomioon. Teema sisältää myös ne keskustelut, joissa haastateltavat pohtivat minkälaisiin riskeihin on hyvä varautua kiinteistön elinkaarenaikana ja miten

sidosryhmäyhteistyöllä voidaan edistää yritysvakoilun torjuntaa kiinteistö- ja rakennustoimialalla. Varautuminen ja suojaustoimenpiteet on edelleen luokiteltu kolmeen alateemaan, jotka ovat turvallisuuden hallinta, kiinteistön elinkaarenaikaiset turvallisuusmenettelyt ja sidosryhmäyhteistyö.

5.4.1 Turvallisuuden hallinta

Yritysvakoilun torjunnan perustana nähtiin **organisaation turvallisuuskulttuuri**, mikä antaa pohjan toimintatavoille ja henkilöstön käyttäytymiselle. Haastateltavien mukaan on luotava avoin ja kannustava turvallisuuskulttuuri, jossa henkilöstö uskaltaa ilmoittaa epäilyttävistä tilanteista ja virheistä pyritään oppimaan niin yksilö- kuin organisaatiotasolla. Osana turvallisuuskulttuuria korostui organisaation turvallisuusuhkien tiedostamisen merkitys. Kaikilla henkilöstötasoilla niin johdon kuin työntekijöiden tulee ymmärtää, että organisaatio voi olla yritysvakoilun kohteena joko suoraan tai välillisesti, väylänä muihin organisaatioihin. Tiedusteluviranomaisten haastatteluiden mukaan ihmisten on vaikea mieltää yritysvakoilun uhkaa, koska se tuntuu epätodennäköiseltä ja kaukaiselta, jolloin siihen ei ole osattu varautua. Henkilöstön turvallisuustietoisuutta voidaan edistää henkilöstölle järjestettävillä **turvallisuuskoulutuksilla ja -harjoituksilla**. Turvallisuuskoulutuksien ja -harjoituksien tulee haastateltavien mukaan olla säännöllisiä ja kattavia. Koulutuksien avulla henkilöstöä autetaan ymmärtämään suojattava arvo, tunnistamaan ja välttämään yritysvakoilun riskit ja toimimaan oikein poikkeamatilanteissa vahinkojen rajoittamiseksi ja estämiseksi. Haastateltavien mukaan selkeät ohjeistukset ja prosessit edistävät organisaation turvallisuuskulttuuria.

”Organisaation turvallisuuskulttuuri on lähtökohta ja siinä on tunnistettu haasteita. Henkilökunta ei aina välttämättä ymmärrä vakoilun uhkaa.” (H2)

” Työntekijät ymmärtäisi, että organisaatiossa on jotain suojattavaa tietoa, että siihen voi kohdistua myös ulkopuolista asiatonta mielenkiintoa ja just ennen kaikkea, että omakin organisaatio voi olla valtiollisen tiedustelun mielenkiinnon kohteena tai toimitaan väylänä sitten johonkin toiseen organisaatioon. Tiedustelutoiminnan uhka on usein sellainen, jota ihmisten on tosi hankala mieltää, että se tuntuu jotenkin sellaiselta epätodennäköiseltä. " (H4)

Kolmantena keskeisenä toimenpiteenä haastateltavat toivat esiin **työsuhteen elinkaaren aikaiset turvallisuustoimenpiteet**, jotka ovat myös sisäpiiriuhkan torjunnan näkökulmasta oleellisia. Tällaisina toimenpiteinä nähtiin ennen työsuhteen aloitusta riittävien taustaselvityksien (turvallisuusselvityksien) tekeminen, salassapitosopimuksen laadinta ja turvallisuusperehdytys työsuhteen alussa. Työsuhteen aikana työtehtävän mukaisten pääsyoikeuksien anto tietoihin, tiloihin ja järjestelmiin. Erityisen tärkeänä haastateltavat näkivät pääsyoikeuksien päivittämisen muutoksien yhteydessä, taustaselvityksien uusinnat lain sallimissa puitteissa kriittisten tehtävien osalta ja jatkuvat säännölliset

turvallisuuskoulutukset. Työsuhteen päättymisen jälkeen korostettiin omaisuuden ja tietojen palauttamista sekä pääsyoikeuksien päättämistä.

”Yritysvakoilulta suojautumisen kannalta on tärkeää, että kaikki työntekijät olivat sitten kiinteistöomistajan tai heidän palveluntuottajien, erityisesti ne, jotka käsittelevät luokiteltuja asiakirjoja tai toimivat yhteisissä työympäristöissä, tarkastetaan ja että heille annetaan asianmukainen turvallisuuskoulutus.” (H2)

”Pääsynhallinta tietoihin ja, kun meillä on avaintehtävä tiedossa, pitää olla keinot siihen, että näitä henkilöitä, kun rekrytoidaan, tehdään riittävät taustaselvitykset, joita pitää myös päivittää.” (H7)

Neljäntenä varautumistoimenpiteenä haastatteluista nousi **tilannekuvan ylläpito, uhkien seuranta ja turvallisuushavainnoista ilmoittaminen**. Koska yritysvakoilua on vaikea havaita, tulee haastateltavien mukaan organisaatioilla olla selkeä kuva omasta ekosysteemistä eli verkkoympäristöstä ja toimintaympäristöstä. Näin turvallisuuden hallinnassa huomioidaan kaikki toimintaan liittyvät asiat. Kokonaisvaltainen tilannekuva organisaation ekosysteemistä mahdollistaa haavoittuvuuksien tunnistamisen ja niihin liittyvien riskien arvioinnin. Lisäksi mahdollistetaan riskiperusteisten turvallisuustoimenpiteiden toteuttamisen sekä poikkeavan toiminnan havaitsemisen. Kybertiedustelulta suojautumisen osalta asiantuntijahaastattelussa korostettiin **verkkoinfrastruktuurin kyberhygieniasta**, laitteistojen ja ohjelmistopäivityksistä ja varmuuskopioinneista huolehtimisesta. Myös verkkojen ja tietokokonaisuuksien eriyttäminen sekä organisaation tekninen valmius poikkeamien havaitsemiseksi hälytysjärjestelmien ja kontrollien avulla nähtiin tärkeäksi. Lisäksi korostettiin muuttuvien uhkakuvien seurantaa ja tilannekuvan ylläpitoa. Haastateltavien mukaan organisaatiolla on hyvä olla luotuna selkeä mekanismi turvallisuushavaintojen ja väärinkäytöksien ilmoittamiselle, seurannalle, analysoinnille ja raportoinnille osana kokonaisvaltaista turvallisuudenhallintaa.

"Organisaation oman tilannekuvan kannalta olisi tärkeätä, että olisi aidosti käsitys siitä, että minkä tyyppisiä tapahtumia on." (H4)

”Huolehtii siitä, että minkälainen on se oma verkkoinfrastruktuurin. Ja miltä se vaikuttaa ulkopuolisen tarkastajan näkökulmasta. Siellä voi olla avoimia portteja, unohtuneita palvelimia. Niitä säännönmukaisesti löydetään ja sitä kautta sitten ja niitä etsii pahantahtoiset toimijat." (H7)

Viidentenä keskeisenä toimenpiteenä nähtiin **tiedon luokittelu ja hallinta**. Kaikkien haastateltavien mielestä on tarve löytää tasapaino avoimuuden ja turvallisuuden välille erityisesti turvallisuuskriittisten kohteiden tiedonhallinnassa. Nykyinen lainsäädäntö ohjaa voimakkaasti avoimuuteen ja kaikki tieto on lähtökohtaisesti julkista, jollei sitä ole erikseen salattu. Haastatteluissa tuotiin esiin tarve ymmärtää tiedon suojaamisen merkitys. Erityisesti korostettiin kriittisen tiedon

tunnistamista, jotta ne eivät ole avoimena saatavilla ja niitä säilytetään ja käsitellään turvallisesti ja niihin pääsyä valvotaan. Konkreettisina tiedonhallinta keinoina nostettiin myös tiedon karkeuttaminen sekä puolustus- ja turvallisuushankintalain käyttö niitä koskevien hankintojen osalta. Osa haastateltavista toi myös esiin organisaatioiden ja työntekijöiden digitaalisen jalanjäljen tunnistamisen ja tiedostamisen. Lisäksi tulee olla ymmärrys siitä mitä tietoa organisaatiosta on julkisesti saatavilla, jota vastapuoli voi hyödyntää kybertiedustelussa ja vaikuttamisessa. Haastateltavat kokivat myös tarpeelliseksi, että organisaatioissa sovittaisiin mitä tietoja saa jakaa eri viestintäkanavissa.

”Organisaatioiden on tärkeää olla tietoisia siitä, mitä tietoa jaetaan avoimesti, sekä omilla verkkosivuilla että työntekijöiden sometileillä. Lyhyesti sanottuna avoimia lähteitä käytetään tosi paljon ja organisaatioiden on hyvä olla hereillä sen suhteen, että olisi jonkinlainen näppituntuma siitä mitä ja millaista tietoa sen organisaation toiminnasta, asiakkaista organisaation mahdollisesti suojattavaan toimintaan liittyvistä asioista jaetaan ihan avoimesti vaikka organisaation omilla verkkosivuilla.” (H4)

”Kriittisen tiedon määrää verkossa pitää koko ajan arvioida.” (H7)

Kuudentena varautumistoimenpiteenä korostettiin **toimittajaverkoston hallintaa**. Haastateltavien mukaan kiinteistö- ja rakennustoimialalla toimitusketjut ovat usein pitkiä ja monimutkaisia, mikä lisää haavoittuvuuksia yritysvakoilun uhkalle. Toimitusketjujen heikkouksien tunnistaminen sekä kumppaneiden ja alihankkijoiden varmistaminen koettiin tärkeäksi, sillä uhkat voivat muodostua toimitusketjun tai toimittajaverkoston läpinäkymättömistä osista. Erityisesti kriittiset toimittajat tulee luokitella ja heidän kanssaan laatia turvallisuussopimukset sekä varmistaa turvallisuuden vaatimuksien mukaisuus esimerkiksi auditoinnein.

”Toimitusketjun turvallisuus on keskeinen osa turvallisuutta. Organisaation on tunnettava kumppaninsa ja varmistettava, että toimittajat täyttävät tarvittavat turvallisuusvaatimukset.” (H2)

Yleisesti haastateltavat korostivat **turvallisuuden perusasioiden** merkitystä yritysvakoilulta suojautumisessa. Kansallista turvallisuusauditointi kriteeristöä (KATAKRI) pidettiin hyvänä pohjana turvallisuuden perustalle kaikille organisaatioille tiedusteluviranomaisten näkökulmasta. Lisäksi säännöllisten tietoturva- ja turvallisuusauditointien koettiin auttavan tunnistamaan mahdolliset heikkoudet ja puutteet organisaation suojausjärjestelmissä.

”Perusasioiden kuntoon laittaminen, että ne perus henkilöstöturvallisuuden periaatteet sekä tila- ja tietoturvallisuuden perusasiat olisi kunnossa.” (H4)

”KATAKRI on mun mielestä hyvä. Se antaa sen aloituspaketin ja sitten se ymmärrys siitä, että mikä teillä on se kriittinen asia. Mitä te haluatte suojata.” (H5)

5.4.2 Kiinteistön elinkaaren aikaiset turvallisuusmenettelyt

Haastatteluaineiston analyysin perusteella valtion kiinteistökantaa hallitsevan tulee ottaa huomioon yritysvakoilun uhka ja sen torjuntaan liittyvät turvallisuusmenettelyt kiinteistön elinkaaren eri vaiheissa. Näistä vaiheista korostuivat aineistosta rakentamis- ja kunnossapitovaihe sekä kiinteistön ostoon, vuokraukseen ja myyntiin liittyvät vaiheet. Yhtenä tärkeimpänä nähtiin **rakentamis- ja kunnossapito**, jolloin rakennetaan uusia tiloja ja asennetaan uudenlaista tekniikkaa, mikä lisää valtiollisen tai ei-valtiollisen toimijan kiinnostusta. Rakentamisvaiheessa tulee ottaa huomioon kaksi asiaa yritysvakoilulta suojautumiseen liittyen. Turvallisuustoimenpiteet rakentamishankkeen aikana, mutta samalla varaudutaan rakennuksen ja tilojen käytön aikaiseen turvallisuuteen. Tällöin huomioidaan muun muassa tilaturvallisuus- ja rakenteelliset ratkaisut, tilojen sijoittelu, hajasäteilysuojaukset ja kaapeleiden suojaukset.

”Silloin, kun rakennetaan tai saneerataan, niin silloinhan laitetaan uudenlaista tekniikkaa ja muuta, niin sehän kiinnostaa huomattavasti näitä vakoojia. Rakentamisvaiheessa otetaan huomioon miten pystytään parhaiten suojautumaan laittomalta tiedustelulta ja tiedustelulta yleisesti.” (H2)

”Rakennushankkeen aloitus ja suunnitteluvaiheessa tulee olla tarkkana, jotta salassa pidettävät tiedot pysyvät vain niitä tarvitsevilla. Kontrollit pitää olla tosi hyvin hoidettuna silloin, kun meillä on kriittinen asiakkuus ja tärkeät tilat suunnitteilla.” (H6)

Haastateltavien mukaan on tärkeää huolehtia kokonaisvaltaisesta riskienhallinnasta, huolellisesta tiedonhallinnasta ja turvallisuustoimenpiteistä kuten pääsynhallinnasta heti rakennushankkeen alusta lähtien käyttöönottoon asti. Erityisesti suojattavien kriittisten tietojen ja tilojen tunnistaminen nähtiin tärkeäksi, joihin tulee kohdistaa tarkemmat turvallisuuskontrollit. Haastateltavien mukaan rakentamisvaiheessa tapahtuvien turvallisuuskontrollien pettäminen voi luoda pohjan käytönaikaiselle tiedustelutoiminnalle ja toiminnan vaikuttamiselle.

”Riskiarvio on pakko tehdä, koska sen perusteella tehdään turvallisuustoimenpiteitä. Loppukäyttäjä määrittelee yhdessä kiinteistönomistajan kanssa hankkeen turvallisuusmenettelyt ja prosessit huomioiden käyttäjältä tulevat turvallisuusvaatimukset.” (H2)

”Rakennusvaiheen näkisin riskialtteimpana palveluntuottajan näkökulmasta. Haalarit päällä pääsee kulkemaan ihan jokaiseen tilaan. Välillä valvottuna

ja välillä ei. Moni huomaa, jos jotain on viety, mutta harva huomaa, jos jotain on lisätty.” (H3)

”Mikä on se kriittisin tieto, mitä meidän pitäisi suojata? Mitä me emme saa menettää? Mutta, jos me olemme menettäneet alkuvaiheessa, kun rakennetaan jotain tilaa tai järjestelmää jo se tieto, että mitä meillä on siellä sisällä ja vastustaja pystyy hyödyntämään sitä, niin se meidän tilaturvallisuusajattelu, niin se menee hukkaan, että siitä ei ole hyötyä.” (H5)

Kiinteistön osto, vuokraus ja myynti nähtiin keskeisinä vaiheina, jolloin turvallisuusnäkökohdat tulee ottaa haastateltavien mukaan vakavasti huomioon. Kiinteistöä ostettaessa ja vuokrattaessa valtion käyttöön tulee lähtökohtana huomioida aina kuka kiinteistöä tulee käyttämään, mihin tarkoitukseen ja mikä on suojattava arvo. Haastatteluissa painotettiin ennakoivan riskienarvioinnin tärkeyttä ennen kaupallistasopimusta. Tämä sisältää tilojen aiemman käytön, mahdollisten suojatoimenpiteiden, naapuruston ja muiden kiinteistön käyttäjien sekä ympäristön vaikutusten ja uhkien arvioinnin.

”Ainakin tulee huomioida kuka sitä tilaa tulee käyttämään ja minkä turvaluokan tietoa siellä tilassa tullaan käsittelemään. Se on ensimmäinen lähtökohta eli mä itse kääntäisin sen niin, että sitä tilaa pitäisi lähteä etsimään tämä käyttötarve ja käyttäjä edellä." (H1)

”Tunnistetaan toimintaympäristössä olevien toimijoiden rooli, jotka voi olla ihan siltä kiinteistön omistajalta saatavaa tietoa niistä kiinteistön muista vuokralaisista. Haastattelemalla sitä, että onko tiedossa muutoksia. Onko tästä lähdössä toimijoita pois? Ovatko kauan olleet siellä ja arvioidaan etniset taustat? Ja sitten voidaan kysyä apuja riskianalyysin tekemisen helpottamiseksi viranomaisilta tai muilta asiantuntijaorganisaatioilta.” (H1)

Kiinteistöä myytäessä tai vuokrattaessa valtion ulkopuolelle korostettiin käyttäjälähtöistä tarkastelutapaa. Tällä haastateltavat tarkoittivat, että yhdessä käyttäjän kanssa kartoitetaan kohteen suojattava arvo, mahdolliset purettavat ja muutettavat rakenteet ja järjestelmät. Toisena asiana tulee huomioida voiko myytävän kohteen kautta vaikuttaa toisen kiinteistön toimintaan tai ympäristössä olevaan muuhun kriittiseen toimintaan. Lisäksi haastateltavat painottivat kriittisen tiedon suojaamista, erityisesti sellaisen tiedon, joka liittyy turvallisuuteen ja jonka paljastuminen voisi aiheuttaa riskejä niin aiemmalle käyttäjälle kuin yhteiskunnan kokonaisturvallisuudelle. Tämä sisältää muun muassa tilojen suojarakenteiden ja teknisten järjestelmien yksityiskohtien salaamisen mahdollisilta ostajaehdokkailta. Yleisesti kiinteistön ostoa, myyntiä tai vuokrausta tehtäessä korostettiin käyttäjän, kiinteistönomistajan ja viranomaisten välistä yhteistyötä. Viranomaiset voivat tarvittaessa antaa asiantuntija-apua turvallisuusriskien tunnistamisessa ja hallinnassa erityisesti valtion omistamien kiinteistökauppojen

yhteydessä. Yhteistyöllä voidaan varmistaa, että kaikki turvallisuusnäkökohdat tulevat huomioiduiksi asianmukaisesti.

”Tilan käyttäjälle kysymys mitä tässä tilassa, vaikka siellä on ne tavallaan omat tavarat poissa, niin onko tässä tilassa jotain sellaista, jota te haluatte, että ei paljasteta mahdolliselle ostajaehdokkaille ja jos siellä jotain sellaista rakennetta tai jotain muuta, niin sitten kysymys tuleeko sieltä purkaa tai muuntaa jotain rakennetta tai ratkaisua niin, että sen käyttöperiaate tai se suojattava arvo, jota se viimeinen käyttäjä on siellä todennut, niin ei paljastuisi.” (H1)

”Huomioitava myytävän kiinteistön toimintaympäristö, voiko toisen kiinteistön kautta lamauttaa toisen kiinteistön. Esimerkkinä eräässä myynti-ilmoituksessa luki, että rasitteena tulee kiinteistön ostajalle se, että rakennuksen läpi kulkee erään valtion organisaation tietoliikenteen solmukohta sekä sähköjärjestelmän merkityksellinen solmukohta,” (H5)

Haastatteluissa mainittiin esimerkkinä miten valtiolliset toimijat voivat pyrkiä vaikuttamaan kiinteistö- ja rakennustoimialan kohteisiin kiinteistökauppojen kautta. Erityisesti aineistosta nousi viime vuosien aikana julkisuudessakin olleet venäläisten tekemät kiinteistökaupat, joissa kiinteistöjä on ostettu läheltä strategisesti merkittäviä kohteita kuten Puolustusvoimien tai kriittisen infrastruktuurin kohteita. Tällä tavoin valtiollinen toimija voi pyrkiä vaikuttamaan maanpuolustukseen ja kokonaisturvallisuuteen liittyviin asioihin. Kiinteistöjen ostaminen on yksi tapa, jolla ulkoiset toimijat voivat hankkia vaikutusvaltaa ja tiedustelutietoa tärkeistä kohteista.

”Sotilaallisella tiedustelulla kartoittaa kohteita ja toimintamalleja. Kyllähän tässä laajaa keskustelua käydään esimerkiksi siitä miten Venäläiset ostaa kiinteistöjä läheltä valtion kiinteistöjä, joilla on sitten kriittistä merkitystä maanpuolustuksen ja kokonaisturvallisuuden kannalta. Että ihan hyvin keskeinen homma.” (H7)

”Tässä kiinteistöjen ostossa ja myynnissä on paljon sellaista mietittävää, joka on syytä ottaa vakavasti huomioon ja siihen keinoja on olemassa.” (H1)

5.4.3 Sidosryhmäyhteistyö

Haastatteluiden perusteella sidosryhmäyhteistyö on olennainen osa yritysvakoilulta suojautumista. Yritysvakoilu ja siihen liittyvät uhkat ovat monimuotoisia ja monitasoisia, rajat ylittäviä, jolloin yhteistyö kiinteistönomistajien, käyttäjien, palveluntuottajien, viranomaisten ja asiantuntijaorganisaatioiden välillä koettiin tärkeäksi. Tiedonvaihto tunnistetuista uhkista, havaituista tapauksista, uusimmista vakoilutekniikoista ja -trendeistä sekä vakoilun torjuntaan liittyvistä teknologioista ja suojausratkaisuista auttavat ennaltaehkäisemään yritysvakoilun uhkaa.

”Yhteistoiminta on säännöllistä eri viranomaistoimijoiden kanssa tiedustelu-uhkaan liittyen. Tiedusteluviranomaisilta saadaan tietoa uhkaympäristön muutoksista ja mahdollisista uusista tiedustelu menetelmistä esimerkiksi teknisistä ratkaisuista, jotka on hyvä ottaa suojaustoimissa huomioon.” (H2)

”Jos me viranomaisena havaitaan itse jotain suomalaiseen organisaatioon kohdistuvaa toimintaa, niin kyllähän me proaktiivisesti ollaan siitä yhteydessä. Meille voi myös matalalla kynnyksellä laittaa havaintoja.” (H4)

Viranomaisten antaman koulutustuen ja uhka-arvioiden koettiin auttavan organisaatioiden henkilöstöä tunnistamaan ja reagoimaan entistä paremmin yritysvakoilun uhkaan. Osa haastateltavista koki myös haasteita organisaatioiden välisessä tiedonkulussa. Tiedon ei välttämättä koettu saavuttavan kaikkia tarvittavia tahoja oikea-aikaisesti, mikä vaikuttaa yhteneväisen tilannekuvan muodostamiseen. Toisaalta kiinteistönomistajan sekä palveluntuottajan edustajat kaipasivat konkreettisempaa tietoa tiedustelun uhkasta ja tapahtumista.

”Kun viranomainen on aloittanut ennaltaehkäisevän toiminnan ja kun aktiivista koulutustukea on sidosryhmille annettu, niin se on johtanut siihen, että näiden sidosryhmien työntekijät ovat enemmän valppaana.” (H1)

”Se aina herättää, kun ulkopuolinen tulee kertomaan ja jos vielä pystyttäisiin käytännön esimerkein tuomaan, niin varmasti parantaisi sitä meidän tilannekuvaamme, mutta varmasti vähän parannettavaa on koulutuksen kautta ja voisivat vieläkin terävämmin niin kun tavallaan meitä valistaa ja tuoda sitä tiedustelun uhkaa vielä selkeämmin esille.” (H6)

5.5 Yhteenveto tuloksista

Edellä kuvattujen tulosten perusteella voidaan todeta, että yritysvakoilu ilmenee kiinteistö- ja rakennustoimialalla monitasoisena ja monimuotoisena uhkana. Alla olevassa taulukossa 4 on yhteenveto tuloksista. Tutkielman tuloksien perusteella yritysvakoilua toteutetaan pääsääntöisesti yhdistelemällä eri tiedustelulajien keinovalikoimia ja toimintaympäristöjä. Kiinteistö- ja rakennustoimialan osalta keskeisenä tiedonhankintakeinona on avointen lähteiden tiedustelu. Merkittävä osa Suomen valtion kiinteistö- ja rakennustiedoista sekä yhteiskunnan kriittiseen infraan liittyvästä tiedosta saadaan haettua avoimesti internetistä.

TAULUKKO 4 Yritysvakoilu kiinteistö- ja rakennustoimialalla

Kiinteistö- ja rakentamistoimiala (KIRA):	**Yritysvakoilu:**			
Tarkoitetaan kiinteistön ostoa, myyntiä, vuokrausta, rakennuttamista, muutos-, laajennus- tai ylläpitotyötä. Kiinteistö- ja rakentamisala muodostavat Suomessa KiRa-klusterin, jonka toimialat ovat sidoksissa toistensa kanssa	Teko, jossa oikeudettomasti hankitaan toiselle kuuluvaa liikesalaisuutta ja otetaan se omaan käyttöön tai ilmaistaan oikeudettomasti ulkopuoliselle, joko tunkeutumalla ulkopuolisilta suljettuun paikkaan tai tietojärjestelmään, hankkimalla tietoja haltuunsa tai jäljentämällä tai käyttämällä teknistä erikoislaitetta. Kybervakoilu on osa yritysvakoilua.	**Tekijätahot** • Valtiolliset toimijat • Rikolliset toimijat • Valtiollisten ja rikollisten yhteen liittymät • Yksityiset yritykset tai organisaatiot • Yksittäiset henkilöt	**Motiivit ja kohteet** • Tiedon saanti • Taloudellinen hyöty • Poliittiset motiivit • Yhteiskunnallinen vaikuttaminen • Pyrkimys edistää omaa asemaansa, tavoitteitaan tai heikentää kohteena olevan liikkumaa (toiminnan lamauttaminen, häirintä) --- • Asiakkaat (valtion organisaatiot, henkilöt) • Valtion kriittiset kohteet ja rakennukset • Kiinteistön ja rakennuksen kriittiset järjestelmät • Kiinteistönomistajan, palveluntuottajan tilat ja järjestelmät • Yhteiskunnan kriittinen infrastruktuuri	**Menetelmät ja keinot** Tiedustelulajit • ***Avointen lähteiden tiedustelu (OSINT)*** • Kybertiedustelu/Signaalitiedustelu (KYBINT/SIGINT) • Henkilötiedustelu (HUMINT) • Geotiedustelu eli paikka- ja olosuhdetiedustelu (GEOINT) Fyysinen toimintaympäristö: • Fyysinen tarkkailu ja havainnointi • Tunteutuminen • Soluttautuminen • Fyysinen kontaktoituminen • Varastaminen, kopioiminen • Teknisten häirintä- ja valvontalaitteiden asentaminen Sosiaalinen toimintaympäristö: • Maalittaminen • Sosiaalinen manipulointi • Kiristys • Värvääminen • Sisäpiiritoimija Digitaalinen toimintaympäristö: • CaaS • Kohdennetut hyökkäykset • Kiristys- ja haittaohjelmat Menetelmien, keinojen ja toimintaympäristöjen limittäin ja ristiin käyttö
Erityispiirteet ja alan keskeisimmät haasteet: • Verkostoituminen (Toimittajaverkostot) • Projektiluonteisuus • Pitkä elinkaari • Tietomallintaminen • Vaihtuvat vaatimukset • Ilmoitukset ja luvanvaraisuus	**Organisaatioturvallisuuden mukaiset suojaustoimenpiteet** 1. Turvallisuuden hallinta: • Turvallisuuskulttuuri • Turvallisuuskoulutukset ja –harjoitukset • Työsuhteen elinkaaren aikaiset turvallisuustoimenpiteet • Tilannekuvan ylläpito, uhkien seuranta • Turvallisuushavainnoista ilmoittaminen • Verkkoinfrastruktuurin kyberhygienia • Tiedon luokittelu ja hallinta		2. Kiinteistön elinkaaren aikaiset turvallisuusmenettelyt 3. Sidosryhmäyhteistyö	

6 JOHTOPÄÄTÖKSET JA POHDINTA

Tämän Pro gradu -tutkielman tarkoituksena oli selvittää, miten yritysvakoilu eli laiton tiedustelu ilmenee kiinteistö- ja rakennustoimialalla. Tutkimusongelmaa selvitettiin kolmen tutkimuskysymyksen avulla; mitkä asiat ovat yritysvakoilun kohteena kiinteistö- ja rakennustoimialalla ja miksi, millä keinoin ja menetelmin yritysvakoilua harjoitetaan kiinteistö- ja rakennustoimialaa kohtaan sekä miten yritysvakoilua vastaan voidaan varautua ja suojautua kiinteistö- ja rakennustoimialalla. Tutkielman tutkimusongelmaan ja tutkimuskysymyksiin saatiin vastaukset ja tulokset ovat kuvattuna luvussa 5.

Johtopäätelmänä tutkielman tulosten perusteella voidaan todeta yritysvakoilun ilmenevän kiinteistö- ja rakennustoimialalla monitasoisena ja monimuotoisena uhkana. Erityisesti Suomen valtion omistaman kiinteistökannan näkökulmasta yritysvakoilun uhka nähtiin merkittävänä. Vaikka kiinteistö- ja rakennustoimiala ei itsessään ole yritysvakoilun varsinainen kohde, sen merkitys välillisenä tiedustelun kohteena kasvaa mitä kriittisempiä käyttäjiä, toimintoja, tietoja ja järjestelmiä kiinteistöissä sekä siihen kuuluvissa maa- ja vesialueilla on. Yritysvakoilun ja tiedustelutoiminnan ensisijaisena tavoitteena nähtiin tiedonhankinta, jonka avulla kiinteistön käyttäjiin ja toiminnallisuuksiin voidaan kohdistaa poliittista, taloudellista ja toiminnallista vaikuttamista tai mahdollistaa toiminnan lamauttaminen.

Valtion kiinteistöjen ja rakennuksien, niissä toimivien ja niihin palvelua tuottavien henkilöiden ja järjestelmien voidaan katsoa muodostavan otollisen alustan yritysvakoilulle. Tähän voi vaikuttaa tutkimuksen teoriaosuuden ja empiirisen osion tulosten perusteella kiinteistö- ja rakennustoimialan erityispiirteiden kuten laajojen toimittajaverkostojen, projektiluonteisuuksien, kiinteistön elinkaaren, tietomallintamisen sekä luvanvaraisuuden tuomat haavoittuvuudet. Lisäksi taloteknisten järjestelmien suuri määrä ja digitalisoituminen tuovat lisähaasteita yritysvakoilun uhkalta suojautumiseen.

Suomen valtion kiinteistö- ja rakennusinfrasta sekä kriittisistä kohteista kartoitetut haavoittuvuudet altistavat yhteiskuntamme toiminnot häiriötilanteille. Lisäksi Suomen päätöksentekojärjestelmään vaikuttaminen ja johtamistoiminnan lamauttaminen mahdollistuvat, mikäli kriittisiä tiloja ja taloteknisiä

järjestelmiä ei kyetä suojaamaan ja ylläpitämään käyttö- ja toimintakuntoisina. Yritysvakoilun keinoin ja menetelmin saatujen tietojen pohjalta luodaankin edellytykset operaatioille, jotka erityisesti kriisitilanteissa ja poikkeusoloissa voivat olla kohteelle katastrofaaliset. Esimerkiksi sodan aikana tiedetään, mitä rakennuksia ja järjestelmiä tulee lamauttaa kohteiden toimintojen estämiseksi. Tutkielman tulosten perusteella voidaan osoittaa, että yritysvakoilu kiinteistö- ja rakennustoimialalla muodostaa merkittävän uhkan niin valtion kokonaisturvallisuudelle kuin yhteiskunnan toiminnalle. Tätä päätelmää tukee muun muassa Venäjän hyökkäyssota Ukrainaan vuonna 2022. Microsoftin (2022a) raportin mukaan Venäjän tiedustelupalvelu kohdisti sodan alkuvaiheessa massiivisia kyberoperaatioita juuri kriittistä infrastruktuuria ja valtion strategisia kohteita kohtaan.

Yritysvakoilun keinojen ja menetelmien voidaan todeta olevan moninaiset ja hyödyntävän fyysistä, sosiaalista sekä digitaalista toimintaympäristöä. Tutkielman tuloksien perusteella yritysvakoilua toteutetaan pääsääntöisesti yhdistelemällä eri tiedustelulajien keinovalikoimia ja toimintaympäristöjä. Vastaavanlainen johtopäätös oli tehty Meretvuon (2021) tutkielmassa, jonka mukaan tiedustelulajien ja -menetelmien limittäminen ja ristiin käyttö mahdollistaa mahdollisimman kattavan kuvan saamisen halutusta asiasta.

Yhtenä keskeisenä tiedonhankintakeinona tuloksien perusteella nousi avointen lähteiden tiedustelu. Merkittävä osa Suomen valtion kiinteistö- ja rakennustiedoista sekä yhteiskunnan kriittiseen infraan liittyvästä tiedosta saadaan haettua avoimesti internetistä. Tämä osoittaa sen, ettei avoimesti jaettujen tietojen tuomia haavoittuvuuksia ole ymmärretty ja tiedostettu. Samoin yritysvakoilun tuomaa uhkaa valtion kokonaisturvallisuudelle ei ole välttämättä ymmärretty kiinteistö- ja rakennustoimialan kontekstissa. Tosin yritysvakoilu on sen kompleksisuuden vuoksi vaikeasti hahmotettavissa ja toisaalta organisaatiot eivät ole välttämättä tiedostaneet omien tietojensa ja tuotteidensa suojattavaa arvoa.

Vaikka tiedon avoin saatavuus on monella tavalla hyödyllistä, on tärkeää löytää tasapaino avoimen yhteiskunnan periaatteiden ja kansallisen turvallisuuden välillä. Liiallinen avoimuus voi altistaa yhteiskunnan riskeille, kun taas liiallinen sulkeutuneisuus voi heikentää avoimuuden ja demokratian periaatteita. Nykyinen lainsäädäntö ohjaa kuitenkin voimakkaasti avoimuuteen, mikä tuo omat haasteensa erityisesti turvallisuuskriittisten kohteiden tietojen suojaamiselle. Lainsäädäntö edellyttäisikin uudelleen tarkastelua, jotta se mahdollistaisi kriittisten tietojen salassapidon nykyistä selkeämmin.

Avointen lähteiden tiedustelun lisäksi tutkielman tulosten perusteella keskeisinä yritysvakoilun keinoina voidaan pitää sosiaalista manipulointia, kyberhyökkäyksiä ja sisäpiiritoimijoita, joita vastaan on tarpeen kehittää kokonaisturvallisuuden suojaustoimia huomioiden eri toimintaympäristöjen ulottuvuudet. Erityisesti sisäpiiriuhka koetaan merkittäväksi uhkaksi ja haasteelliseksi varautumisen näkökulmasta. Myös Wimmerin (2015) mukaan sisäpiiriuhka muodostaa yhden vakavimmista uhkista organisaation salassa pidettävälle tiedolle ja toimintojen jatkuvuudelle. Kiinteistö- ja rakennustoimialalla uhkaa voidaan pitää potentiaalisena huomioiden laajat toimittajaverkostot, jolloin

kontrolloitavien toimijoiden määrä on suuri. Tämä edellyttää etenkin kiinteistönomistajalta omasta ekosysteemistään selkeää tilannekuvaa, systemaattisia pääsynhallintamenettelyitä sekä turvallisuuskontrolleja heikkojen signaalien ja poikkeamien havaitsemiseksi sekä niihin reagoimiseksi. Toisaalta toimittajaverkon hallinta voi olla haastavaa mahdollisten pitkien toimitusketjujen vuoksi. Tämä nostaa entisestään riskin suuruutta.

Yksinkertaisimmillaan yritysvakoilulta varautuminen ja suojautuminen edellyttää kiinteistö- ja rakennustoimialan organisaatioiden turvallisuuskulttuurin ja henkilöstön turvallisuustietoisuuden vahvistamista sekä organisaatioturvallisuuden perusasioiden hallintaa. Vastaavasti kuten teoriaosuudessa on todettu, voidaan myös tämän tutkielman tulosten perusteella todeta, että organisaatioiden ja henkilöstön ymmärrys miksi he voivat olla yritysvakoilun kohteena on perusta onnistuneelle varautumiselle ja suojaustoimille. On hyvä ymmärtää minkälaista tietoa organisaation ja työntekijöiden kautta voidaan saada ja miten tätä tietoa voidaan käyttää. Kenen hyväksi organisaatiota voidaan vakoilla ja mitä siitä voi aiheutua organisaatiolle itselleen, sidosryhmille tai yhteiskunnalle. Ihminen on kuitenkin viimekädessä aina toiminnan keskiössä ja laukaisevana tekijänä positiiviselle tai negatiiviselle tapahtumalle. Oli kyseessä sitten oven avaaminen, linkin klikkaaminen tai tiedon jakaminen.

Tarkasteltaessa yritysvakoilua valtion kiinteistökannan ja -hallinnan näkökulmasta, tulee varautumis- ja suojaustoimenpiteissä huomioida edellisten lisäksi kolme näkökulmaa. Ensin on tiedostettava historian saatossa jo menetetty tieto, jota valtiolliset toimijat ja rikolliset voivat hyödyntää omiin tarkoitusperiinsä. Ja toisaalta, kun rakennetaan uutta ja olemassa olevia tiloja sekä järjestelmiä uudistetaan, huolehditaan alusta lähtien tiedon ja toiminnan turvallisuuden hallinnasta koko kiinteistön elinkaaren ajan. Tämä sama pätee yhteiskunnan kriittisen infran osalta valtion ja yhteiskunnan kokonaisturvallisuuden edistämiseksi ja resilienssin vahvistamiseksi. Kolmanneksi on tiedostettava yritysvakoilun monimuotoisuus, rajat ylittävä toiminta ja tehokkaampi järjestyminen, jossa valtiolliset ja ei-valtiolliset toimijat yhteistyössä muodostavat entistä vaarallisempia uhkia. Yritysvakoilulta suojautuminen edellyttää yhteistyötä kiinteistönomistajien, käyttäjien, palveluntuottajien, viranomaisten ja asiantuntijaorganisaatioiden välillä. On tärkeää ylläpitää jatkuvaa ja avointa tiedonkulua sekä tilannekuvaa eri toimijoiden välillä varautuen uusiin uhkamuotoihin teknologiakehityksen myötä.

6.1 Tutkimuksen luotettavuus ja tutkimusetiikka

Tässä pro gradu -tutkielmassa tutkimuseettiset näkökulmat ja hyvän tieteellisen käytännön perusperiaatteet on otettu huomioon koko tutkimusprosessin aikana. Tutkimuseettisen neuvottelukunnan (2024) ohjeistuksen mukaan hyvän tieteellisen käytännön periaatteet muodostuvat luotettavuudesta, rehellisyydestä, arvostuksesta ja vastuunkannosta. Tutkimuksen toteutus ja käytettävä tutkimusmetodi on pyritty kuvaamaan mahdollisimman tarkkaan luvussa 4.

Tämä tutkielma on tehty laadullisena tutkimuksena. Tutkimusmetodina on käytetty teemahaastattelua ja aineisto on analysoitu aineisto- ja teorialähtöisen sisällönanalyysin yhdistelmämenetelmällä. Laadullisen tutkimuksen luotettavuuden arviointiin ei ole olemassa yksiselitteistä menetelmää. Usein luotettavuutta arvioidaan reliabiliteetin eli tutkimuksen tulosten toistettavuuden ja validiteetin eli tutkimusmenetelmien soveltuvuus tutkittavaan ilmiöön. (Hirsjärvi ym., 2009). Teemahaastattelussa tilanne on ainutkertainen, ja saman henkilön haastatteleminen toistamiseen muuttaisi sen keinotekoiseksi. Joten tämän tutkielman luotettavuuden arvioiminen reliabiliteetin keinoin ei ole mielekästä. Tutkielman luotettavuuden arviointia tarkastellaan Tuomen & Sarajärven (2018, 163–164) esittämien näkökulmien kautta.

Tutkimuksen kohteena oli selvittää, miten yritysvakoilu ilmenee kiinteistö- ja rakennustoimialalla. Tavoitteena on edistää alan ymmärrystä yritysvakoilusta ja miten sitä vastaan voidaan suojautua. Aihe oli rajattu koskemaan Suomen valtion omistamaa kiinteistökantaa, mikä jäsensi aineiston käsittelyä. Teoriaosuuden kirjallisuuskatsauksen avulla saatiin kuvattua tutkielman keskeisimmät käsitteet, tutkittavaa kohdetta sekä siihen liittyviä erityispiirteitä tuottaen looginen kokonaiskuva tutkittavasta aiheesta. Hirsjärven & Hurmeen (1995, 129) mukaan luotettavuuteen vaikuttaa miten hyvin tutkittavasta ilmiöstä on pystytty johtamaan olennaiset piirteet ja keskeiset käsitteet.

Aineiston keruu tehtiin teemahaastatteluin. Metodin valintaperustelut ja aineiston keruuprosessi on kuvattuna luvussa 4.1. Etäyhteydellä toteutetut haastattelut eivät välttämättä olleet paras mahdollinen ratkaisu, sillä se saattoi vaikuttaa haastateltavien antamiin vastauksiin. Mahdollisesti syvällisempiä vastauksia olisi saanut läsnäolohaastatteluina. Teemahaastattelun pääteemat johdettiin tutkimuskysymyksistä ja teoreettisesta viitekehyksestä, jolloin haastattelut eivät jääneet aiheesta irrallisiksi ja käsitellyt teemat vastasivat sisällöltään tutkittavaa ilmiötä. Tutkija oli onneksi varautunut riittäviin lisäkysymyksiin, jotta kysymyksen haluttu merkitys saavutettiin. Toisaalta haastateltavien valinnalla oli merkitystä, koska tutkittava aihe on haastava ja ainoastaan asiaa tuntevat ja riittävää kokemusta omaavat henkilöt soveltuivat haastateltaviksi. Haastateltavien valinta on kuvattuna luvussa 4.1.2. Luotettavuutta edistää, että yksi tutkija toteutti kaikki haastattelut, litterointeineen sekä analysointeineen. Tällä varmistettiin, ettei muodostunut tulkinnallisia eroavaisuuksia ja varmistettiin tiedon muuttumattomuus. Samalla huolehdittiin aineiston luottamuksellisesta käsittelystä.

Tutkimuksen tiedonantajat eli haastateltavien määrä (n=7) olisi voinut olla suurempi. Toisaalta analysoitavaa aineistoa kertyi yli 200 sivua ja haastatteluista saatu tieto alkoi kertautua. Aineiston kyllääntyessä sitä voidaan pitää riittävänä (Hirsjärvi ym., 2009). Tutkittavaa ilmiötä tarkasteltiin myös eri näkökulmista eli huomioitiin niin kiinteistönomistajan, käyttäjän, palveluntuottajan, tiedusteluviranomaisten sekä tiedustelu- ja kyberturvallisuuden asiantuntijoiden näkemykset, jolloin tuloksista saatiin mahdollisimman kokonaisvaltainen näkemys. Tulokset olisivat jääneet varmasti suppeammiksi, mikäli kaikkien tahojen näkemyksiä ei olisi huomioitu.

Tutkijan ja tiedonantajien välinen suhde saattoi vaikuttaa tutkielman luotettavuuteen. Tutkija ja osa haastateltavista olivat entuudestaan tuttuja. Toisaalta tämä loi haastattelutilanteeseen luotettavan ilmapiirin.

Tutkimusaineiston käsittely ja analysointi litterointeineen tehtiin suojatussa ympäristössä. Tällä tarkoitetaan, ettei tutkimusaineistoa käsitelty muiden läsnä ollessa. Samalla varmistettiin, etteivät sivulliset kuule ja näe litteroitavaa tekstiä ja aineistoja. Tutkimusaineistoa on säilytetty koko tutkimusprosessin ajan siten, että vain tutkijalla on pääsy aineistoon. Tutkimuksessa ei myöskään käsitellä tarpeettomia henkilötietoja ja niiden osalta tutkimusaineistossa huomioitiin tietojen anonymisointi ja pseudonymisointi tarvittavilta osin. Osaa haastatteluissa esiin tulleista asioista ei ole voitu tuoda julkiseen tutkimusraporttiin, koska näiden katsottiin voivan vaikuttaa tai aiheuttaa haittaa valtion organisaatiolle tai sidosryhmälle. Muutoin tutkimuksessa käsitellyt ja julkaistut asiat ovat sellaisia, joiden ei ole katsottu aiheuttavan haittaa organisaatioille ja yhteiskunnalle. Haastattelukertomuksista on myös poistettu yksityiskohtia, jotta niitä ei voida sellaisenaan liittää mihinkään tiettyyn kohteeseen tai henkilöön.

Yleisesti huomioituna tutkielman luotettavuutta voi heikentää tutkijan mielenkiinto tutkittavaa aihetta kohtaan ja tutkijan työskentely kiinteistö- ja rakennustoimialan organisaatiossa. Toisaalta tämä auttoi hahmottamaan tutkivaa aihetta ja tuki haastatteluiden onnistumista. Tutkija on kuitenkin pyrkinyt käsittelemään aineistoa mahdollisimman objektiivisesti ja tulokset pohjautuvat aineistoista saatuihin tietoihin. Tältä osin luotettavuutta ja tuloksien uskottavuutta on pyritty osoittamaan haastateltavien suorilla lainauksilla.

6.2 Tutkimuksen hyödyntäminen ja jatkotutkimusaiheet

Yritysvakoilua käsittelevää tutkimusaineistoa kiinteistö- ja rakennustoimialan kontekstista ei ollut saatavilla tätä pro gradu -tutkielmaa kirjoittaessa. Meretvuon (2021) ja Matilan (2011) tutkimukset käsittelevät yritysvakoilua yleisesti. Tämän tutkielman voidaankin todeta täydentävän yritysvakoilua käsittelevää tutkimusaineistoa kiinteistö- ja rakennustoimialan näkökulmasta. Tutkimalla yritysvakoilua uudesta, tietyn alan näkökulmasta, saadaan muodostettua konkreettisempi kuva muutoin kompleksisesta ja vaikeasti hahmotettavasta aiheesta. Kun tutkittava aihe on sidottu lukijalle tuttuun kontekstiin, se voi auttaa ymmärryksen edistämisessä.

Tämän tutkielman avulla voidaan edistää valtion kiinteistönomistajan ja rakennuttajien sekä heidän eri sidosryhmien (viranomaiset, palveluntuottajat) ymmärrystä ja valveutuneisuutta yritysvakoilusta. Tutkielman tulosten perusteella voidaan osoittaa, miten yritysvakoilu kohdistuu kiinteistö- ja rakennustoimialaan, jolloin sitä vastaan on paremmat mahdollisuudet varautua ja suojautua. Lisäksi saadaan käsitys, miksi yritysvakoilua kohdistetaan kiinteistö- ja rakennustoimialaa kohtaan ja mitä vaikutusta sillä voi olla organisaatiolle itselleen, sen sidosryhmille ja yhteiskunnalle.

Verrattaessa tätä tutkielmaa esimerkiksi Meretvuon (2021) tutkimukseen, voidaan havaita yritysvakoilun keinovalikoimassa tapahtuneen muutosta. Erityisesti valtiollisten toimijoiden ja rikollistoimijoiden välinen yhteistyö on tiivistynyt. Lisäksi rikollistoimijat ovat alkaneet palvelullistamaan toimintaansa, tarjoten vähemmän koulutetuille kyberrikollisille kyvykkyyttä kyberoperaatioiden suorittamiseen. Tämä voi enteillä vakoilu- ja kyberoperaatioiden kasvua tulevaisuudessa entisestään.

Vaikka tutkimus on tehty valtion kiinteistökannan näkökulmasta, tuloksia voidaan hyödyntää yleisesti kiinteistö- ja rakennustoimialan organisaatioiden turvallisuuden kehittämisessä. Tämä sama pätee yhteiskunnan kriittisen infran osalta valtion ja yhteiskunnan kokonaisturvallisuuden edistämiseksi ja resilienssin vahvistamiseksi. Tutkielma tukee osaltaan valtioneuvoston periaatepäätöstä valtion kiinteistöstrategiasta 2030 kokonaisturvallisuuden edistämisen osalta.

Tutkielmassa käsiteltävä aihe on erittäin ajankohtainen. Venäjän hyökkäyssota Ukrainaan on vielä käynnissä. Julkisuudessa on nostettu viime päivien aikana esiin Suomen avoimen yhteiskunnan tuomia haavoittuvuuksia erityisesti kriittisen infrastruktuurin näkökulmasta. Vastaava asia nostetaan esiin myös tässä tutkielmassa. Lainsäädäntömme edellyttäisikin uudelleen tarkastelua, jotta se mahdollistaisi kriittisten tietojen salassapidon nykyistä selkeämmin. Olisi hyvä tutkia miten kriittistä tietoa voidaan hallinnoida siten, ettei se muodosta liian isoa uhkaa yhteiskunnalle ja kokonaismaanpuolustukselle. Samalla olisi hyvä selvittää miten muissa pohjoismaissa ja EU-maissa vastaavia tietoja käsitellään, onko lainsäädännöllisesti eroavaisuuksia ja onko havaittu vastaavanlaisia haasteita kuin Suomessa. Toiseksi olisi hyvä tutkia ja selvittää miten voidaan hallinnoida laajoja toimittajaverkostoja ja pitkiä toimitusketjuja kyberturvallisuuden ja yritysvakoilulta suojautumisen näkökulmasta. Toimittajaverkoston ja toimitusketjujen turvallisuuden hallinnan haasteet nousivat esiin erityisesti kiinteistö- ja rakennustoimialalla. Näihin liittyviä vaatimuksia on tulossa myös EU:n kyberturvallisuusdirektiivin NIS2.0 myötä. Kolmanneksi olisi mielenkiintoista tehdä tutkimus tapahtuneista yritysvakoilu-, tiedusteluoperaatioista, mitä vahinkoa ja millaisia seuraamuksia niistä aiheutui. Miten niitä on käytännössä pystytty ratkomaan. Minkälaisia vaikutuksia tapauksilla on ollut tai voi olla yksittäisen valtion toimintaan. Tätä voi olla haastava tutkia, mutta aiheena olisi mielenkiintoinen ja edistäisi vakoilulta varautumista.

LÄHTEET

Aitel, D., dÁntoine, S., Garwin, T., Roos, I., Rostow, N., Sherman, J., & Wagner, A. (2022). Russia´s Cyber Operations. A Threat to American National Security. Margin Research LLC. Full Report. Haettu: https://margin.re/russias-cyber-operations-are-a-threat-to-american-national-security/

Baldwin, D.A. (1985). Economic Statecraft. Priceton University Press, New Jersey.

Bath, A.H. (1998). Tracking the Axis Enemy: The Triumph of Anglo-American Naval Intelligence (Lawrence: University of Kansas Press 1998).

CGI (2018). Paikkatiedot ovat kriittistä infrastruktuuria – miten huolehtia niiden toimintavarmuudesta ja turvallisuudesta? Blogi 1.11.2018. Haettu: https://www.cgi.com/fi/fi/blogi/paikkatiedot-ovat-kriittista-infrastruktuuria-miten-huolehtia-niiden-toimintavarmuudesta-ja-turvallisuudesta

Crowdstrike. (2021) What is cyber espionage? Haettu: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

Cyberwathc Finland (2021). Cyberwatch Finland. (2021) Mitäs me sanottiinkaan ? Haettu: https://www.cyberwatchfinland.fi/fi/mitas-me-sanottiinkaan/

Cyberwatch & Elinkeinoelämän keskusliitto (2018). Kybervakoilu – mitä jokaisen yrityksen tulisi tietää? Haettu osoitteesta https://ek.fi/wpcontent/uploads/Kybervakoilu2018.pdf

Cyrus, C, IoT Cyberattacks Escalate in 2021, According to Kaspersky, 17.9.2021, Haettu osoitteesta https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/#

DiCicco-Bloom, B. & Crabtree B.F. (2006). The qualitative research interview. Medical Education 2006. 40: 314–321. doi:10.1111/j.1365-2929.2006.02418.x

Elinkeinoelämän keskusliitto (2017). Yritys – miten olet suojannut tietopääomasi.

Enisa (2020). ENISA threat landscape 2020 - cyber espionage. European Union Agency for Network and Information Security. Haettu osoitteesta https://www.enisa.europa.eu/publications/enisa-threatlandscape-2020-cyber-espionage

EUBIM Taskgroup (2018). Käsikirja tietomallintamisen käyttöön ottamisesta Euroopan julkisella sektorilla. Pdf-tiedosto. Haettu osoitteesta http://www.eubim.eu/wp-content/uploads/2018/10/GROW-2017-01356-00-00-FI-TRA-00.pdf

Euroopan komissio (2007). Komission tiedonanto neuvostolle, Euroopan parlamentille ja alueiden komitealle. Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi. Bryssel 22.5.2007. Luettavissa : http://ec.europa.eu/transparency/regdoc/rep/1/2007/FI/1-2007-267-FI-F1-1.Pdf

Euroopan tilintarkastus tuomioistuin (2019). EU:n kyberturvallisuuspolitiikan vaikuttavuuteen liittyvät haasteet. Aihekohtainen katsaus, maaliskuu 2019. Haettu:

https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_FI.pdf

European Centre for Political Economy (ECIPE), Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness? Occasional Paper No 2/18, helmikuu 2018.

GDPR (2016). The General Data Protection Regulation (EU) 2016/679. ("GDPR")

Gunneriusson, H. & Ottis, R. (2013). Cyberspace from the hybrid threat perspective. Journal of Information Warfare, 12(3), 67-77.

Hakonen, K. (2021). Sotilastiedustelun tiedustelulajit sekä siviili- ja sotilastiedustelun tiedustelumenetelmät. Haettu: https://tiedusteluvalvonta.fi/-/sotilastiedustelun-tiedustelulajit-seka-siviili-ja-sotilastiedustelun-tiedustelumenetelmat

HE 203/2017. Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi. Haettu: https://www.finlex.fi/fi/esitykset/he/2017/20170203

Henttinen, T. (2012). Yleiset tietomallivaatimukset YTV 2012.

Helsingin kaupunki. (2022). Johtotietopalvelut. Haettu: https://www.hel.fi/helsinki/fi/kaupunki-ja-hallinto/hallinto/palvelut/palvelukuvaus?id=3282

Helsingin kaupunki. (2019). Työmaan ilmoitukset 6.12.2019. Haettu: https://www.hel.fi/helsinki/fi/asuminen-ja-ymparisto/rakentaminen/tyomaavaihe/tyomaan-ilmoitukset/

Helsingin seudun kauppakamari. (2021). Yritysvakoilu 2021 -selvitys. Helsinki.

Hirsjärvi, S., Hurme, H. (2000). Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino

Hirsjärvi, S., Hurme, H. (1995). Teemahaastattelu. Helsinki: Yliopistopaino

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). Tutki ja kirjoita. Helsinki: Tammi

IAEA. (2020). Prevent and Protective Measures against Insider Threats. IAEA Nuclear Security Series No. 8-G (Rev.1)

I-LEAD. (2020). Crime as a service – Market & research scan 2019-2020. Haettu: https://enlets.eu/wp-content/uploads/2022/09/CaaS-1.pdf

Iltasanomat. (2018). Asiantuntijat: Airiston Helmi saattaa olla hybridivaikuttamista – ”Venäjän korruptioverkosto on iso, tämä voisi liittyä siihen”. Artikkeli julkaistu 30.9.2018. Haettu: https://www.is.fi/kotimaa/art-2000005846962.html

Iltasanomat. (2018). Venäjän tiedustelupalveluiden sabotaasitoiminnalla on pitkäperinne Haettu: https://www.is.fi/ulkomaat/art-2000005846969.html

Jalil, A.J., Hassan, H. (2020). Protecting trade secret from theft and corporate espionage: some legal and administrative measures. International Journal of Business and Society, Vol. 21 S1, 2020, 205-218

Johtotietopankki. (2022) Johtotietopankki.fi -palvelu. Haettu: https://johtotietopankki.fi/

Junnonen, J-M., Kankainen, J. (2020). Rakennuttaminen. Rakennustieto Oy. Helsinki. 6.painos.

Jäväjä, P. & Lehtoviita, T. (2016). Tietomallintaminen talorakennustyömaalla. Pieksän print. Pieksämäki.

Keskuskauppakamari., Helsingin seudun kauppakamari. (2017). Yritysten rikosturvallisuus 2017: Riskit ja niiden hallinta. Keskuskauppakamari.

Kiinteistö- ja rakentamisfoorumi (2022). Kiinteistö- ja rakentamisalan kasvuohjelma. Haettu: https://kirafoorumi.fi/wp-content/uploads/2022/02/KIRAfoorumi_Kasvuraportti_2022_FINAL.pdf

Koivula, T. (2020). Suomalaisen tiedustelukulttuurin jäljillä. Maanpuolustuskorkeakoulu sotataidon laitos. Julkaisusarja 2: Tutkimusselosteita nro7.

Korva-Perämäki, M. (2017). Kyberrikostorjuntakeskuksen tavoitteena on pysäyttää kyberrikollisuus. RIKU-lehti 2/2017.

Kupcikas, K. (2013). The Importance of Intelligence to International Security. E-International Relations. ISSN 2053-8626. Loughborough University. Haettu https://www.e-ir.info/2013/11/08/importance-of-intelligence-to-international-security/

Kyberturvallisuuskeskus (2014). Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti, Viestintävirasto 2014, Haettu: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf

Lanne, M. (2007). Yhteistyö turvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa. VTT Publications 632. Espoo: VTT.

Laki Senaatti-kiinteistöistä ja Puolustuskiinteistöistä 1018/2020

Lanne, M. 2007. Yhteistyö turvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa. VTT Publications 632. Espoo: VTT.

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

Limnell (2019). Verkkovakoilu uhkaa suomalaisyrityksiä. Haettu: https://www.kaleva.fi/verkkovakoilu-uhkaa-suomalaisyrityksia/1697587

Lith, P. (2022). Kiinteistöala Suomen kansantaloudessa. Raportti kiinteistöalan yritystoiminnasta, markkinoista ja kehityslinjoista 2021-22. Helsinki 18.8.2022,

Lowenthal. M.M. & Clark, R. M. (2015). The 5 Disciplines of Intelligence Collection.

Lowenthal, M. M. (2002). Intelligence: From Secrets to Policy. Washington DC: CQ Press.

Maanmittauslaitos. (2020). Ulkomaalaisten kiinteistön ostot muuttuivat luvanvaraisiksi. Artikkeli 11.2.2020. Haettu: https://www.maanmittauslaitos.fi/ajankohtaista/ulkomaalaisten-kiinteiston-ostot-muuttuivat-luvanvaraisiksi

Maankäyttö- ja rakennuslaki 5.2.1999/132. Luettavissa: Ajantasainen lainsäädäntö – Finlex. Haettu: https://www.finlex.fi/fi/laki/ajantasa/1999/19990132

Mann,I. (2017) Hacking the Human. Social Engineering Techniques and Security Countermeasures. eBook Published 15.10.2017. Haettu: https://doi.org/10.4324/9781351156882

McDowell,D. (2009). Strategic intelligence. A Handbook for Practitioners, Managers, and Users. Revised Edition. The Scarecrow press, Inc.

Meretvuo, M. (2021). Yritysvakoilu: Tilannekuva, menetelmät ja estäminen. Jyväskylän yliopisto. Informaatioteknologian tiedekunta.

Microsoft (2022a, April 27). Special Report: Ukraine, An overview of Russia's cyberattack activity in Ukraine. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Nasheri, H. (2005). Economic Espionage and Industrial Spying. Cambridge University Press.

Niemi, H. (2017). Rikollisuustilanne 2017. Rikollisuuskehitys tilastojen ja tutkimusten valossa, Helsingin yliopisto, Kriminologian ja oikeuspolitiikan instituutti. Katsauksia 29/2018, 147-158.

Peltonen, T. & Kiiras, J. 1998. Rakennuttajan riskit eri urakkamuodoissa. Rakennustieto Oy. Gummerus kirjapaino Oy.

Poliisiammattikorkeakoulu (2021) Kyberrikos on poliisiasia. Opas yrityksille kyberrikostutkinnan kulusta. Haettu: https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212?t=1616740405258

Puolustusministeriö (2020). EU- ja ETA-alueiden ulkopuolisten ostajien lupa kiinteistökauppoihin. Haettu: https://www.defmin.fi/luvat_ja_asiointi/kiinteistonostajien_luvat#af6e3d00

Puolustusvoimat. (2021). Sotilastiedustelu. Julkinen katsaus 2021. Pääesikunta.

Rakennustietosäätiö., LVI-Keskusliitto ry., Sähkötieto ry. & Rakennustieto ry. (2002). Talotekniikka RYL.

Rakennustietosäätiö. (2011). LVI2010-NIMIKKEISTÖ.

Rakennusteollisuus (2022). Rakennuksen elinkaari kestävän rakentamisen lähtökohtana. Haettu: https://www.rakennusteollisuus.fi/Tietoa-alasta/Ilmasto-ymparisto-ja-energia/Kestava-rakentaminen/Rakennuksen-elinkaari/

Rakli (2014). Kiinteistöalan yhteiskunnallinen ja kansantaloudellinen merkitys. KTI Kiinteistötieto Oy.

Richelson, J. (2007) The technical collection of intelligence.

Rikoslaki 19.12.1889/39. Luettavissa : Ajantasainen lainsäädäntö – Finlex. Haettu: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Salminen, A. (2011). Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja. Vaasa: Vaasan yliopisto

Senaatti-kiinteistöt (2021). Tilinpäätös Senaatti-kiinteistöt 2021. https://www.senaatti.fi/app/uploads/2022/03/Tilinpaatos-Senaatti-kiinteistot-2021-1.pdf

Sisäministeriö (2017). Tietoverkkorikollisuuden torjuntaa koskeva selvitys, Sisäministeriön julkaisu 14/2017, s16, 21, 22. Haettu osoitteesta: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf

Sisäasiainministeriö (2012). Liiketoimintaa turvallisesti. Kansallinen strategia yritystoiminnan turvallisuuden parantamiseksi. Sisäasiainministeriön julkaisusarja 30/2012. Helsinki: Sisäasiainministeriö.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. Computers & Security, 21(6), 526–531. https://doi.org/10.1016/S0167-4048(02)01009-X

Suojelupoliisi (2024). Supo vuosikirja 2023. Haettu osoitteesta https://vuosikirja.supo.fi/documents/62399122/66519032/SUPO+Vuosikirja+2023.pdf/b86c9a6d-8a29-165e-6abe-c10447e66d71/SUPO+Vuosikirja+2023.pdf?t=1711366634612

Suojelupoliisi (2021). Suojelupoliisin kirjallinen asiantuntijalausunto, 11.2.2021 Dnro SUPO 50/01.04.04.00/2021, Haettu osoitteesta https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2021-AK-362832.pdf

Suojelupoliisi. Supo 2020 vuosikirja, 2020, s18, Haettu osoitteesta https://vuosikirja.supo.fi/vakoilun-painopiste-verkkoon

Suojelupoliisi (2018). Suojelupoliisin juhlavuosikirja 2018. Haettu osoitteesta https://supo.fi/documents/38197657/40760236/2018_Supo_Juhlavuosikirja-70.pdf/d986a8e0-65d5-5bf6-0857-b516d1c8907d/2018_Supo_Juhlavuosikirja-70.pdf?t=1602665751133

Suojelupoliisi (2016). Hallintovaliokunnan lausuntopyyntö VNS 2/2016 ja VNS 5/2016. 27.9.2016 Dnro 343/2016. Haettu https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2016-AK-75745.pdf

Suomen kuvalehti (2010). Ilmestyskirjan mato: Stuxnet on yhä arvoitus, lue taustat kybersodan aseesta. Artikkeli 10.11.2010. Haettu: https://suomenkuvalehti.fi/ulkomaat/ilmestyskirjan-mato-stuxnet-on-yha-arvoitus-lue-taustat-kybersodan-aseesta/

Sähkötieto ry (2022). Taloteknisten järjestelmien tiedonsiirto. Tietotekniset järjestelmät. ST-käsikirja 21.

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

Turvallisuuskomitea (2018). Kyberturvallisuuden sanasto, 26. Haettu https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Turvallisuuskomitea (2017). Kokonaisturvallisuuden sanasto, 15. Haettu https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Tutkimuseettinen neuvottelukunta (2024). Hyvä tieteellinen käytäntö (HTK). Haettu 18.5.2024 https://tenk.fi/fi/hyva-tieteellinen-kaytanto-htk

Valtiokonttori (2022). Toimitilat. Haettu: https://www.tutkihallintoa.fi/valtio/valtio-toimitilat/

Valtioneuvosto. (2021). Valtioneuvoston puolustusselonteko VNS 8/2021 vp. Valtioneuvosto. Helsinki. Haettu: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/VNS_8+2021.pdf

Valtioneuvoston kanslia (2020). Rakennusalan kilpailukyky ja rakentamisen laatu Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2020:24. Helsinki.

Valtiovarainministeriö (2022). Kiinteistöt ja toimitilat. Haettu: https://vm.fi/kiinteistot-ja-toimitilat

Valtiovarainministeriö (2021). Ehdotus valtion toimitilastrategiaksi 2030. Valtion toimitilastrategian uudistamishankkeen työryhmä. Valtiovarainministeriön julkaisuja 2021:66. Helsinki. Haettu: https://urn.fi/URN:ISBN:978-952-367-901-6

Valtiovarainministeriö (2021). Valtioneuvoston periaatepäätös valtion kiinteistöstrategiaksi 2030. Periaatepäätös 16.12.2021. VN/6761/2021

Vashiskt,A. & Kumar,A. (2013) Corporate espionage: The insider threat. Sage journals. Research Article published July 12, 2013. Haettu: https://doi.org/10.1177/0266382113491816

Viestintävirasto (2017). Tietoturvan vuosi 2017, Viestintäviraston julkaisu 001/2018

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. Minnesota Journal of International Law, 22, 347

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

Wirtz, J., Rosenwasset, J. (2010). From Combined Arms to Combined Intelligence: Philosphy, Doctrine and Operations. Intelligence and National Security. Volume 25, 2010, 25-743. Haettu: https://doi.org/10.1080/02684527.2010.537870

Yle (2011). Israel testasi Stuxnet-matoa ennen verkkohyökkäystä Iraniin. Uutisartikkeli 16.1.2011. Haettu: https://yle.fi/a/3-5306825

Yle (2016). Venäläisen verkkovakoojan 12 askelta Suomen ulkoministeriön koneille ja jälkien peittämiseen. Haettu: https://yle.fi/a/3-8591034

Yle (2016). Analyysi: Venäläisten maakauppoja hyssyteltiin pitkään – vasta Ukrainan sota herätti päättäjät. Uutisartikkeli 15.2.2016. Haettu: https://yle.fi/uutiset/3-8673869

Yle (2022). Venäläisten Suomesta ostamien kiinteistöjen määrä on kasvanut rajusti viime aikoina – katso, paljonko kotikunnastasi on myyty itänaapuriin. Uutisartikkeli 2.3.2022. Haettu: https://yle.fi/uutiset/3-12339022

LIITE 1 HAASTATTELURUNKO

Alla on ote haastatteluiden perusrungosta, mikä oli kaikille haastateltaville sama. Tarkentavia teemakohtaisia ja haastatteluroolin mukaisia lisäkysymyksiä ei ole sisällytettynä tähän.

1. Johdanto ja taustaa
   - Haastattelijan esittäytyminen
   - Pro gradu -tutkielman aiheen esittely ja haastattelun tarkoitus
   - Tutkimusetiikka
   - Tutkielman loppuraportin julkisuusaste
   - Lupa haastattelun tallennukselle

2. Haastateltavan tausta:
   - Työhistoria/tehtävä ja asema organisaatiossa
   - Vastuualue ja toimenkuva
   - Tiedustelu- ja turvallisuusalan sekä vastatoimien tuntemus
   - Kiinteistö- ja rakennustoimialan tuntemus

3. TEEMAT
   A. Uhka- ja riskikuva
   B. Yritysvakoilun/laittoman tiedustelun kohteet, tavoitteet
   C. Yritysvakoilun keinot ja menetelmät (sisältää tekijätahot)
   D. Varautuminen ja suojautuminen yritysvakoilulta
   E. Tulevaisuuden trendit, haasteet ja jatkotutkimusaiheet