Satu Koskinen

KYBERTURVALLISUUDEN TOTEUTUMINEN ALIHANKINTAKETJUISSA

Opinnäytetyö

Tekniikan ylempi ammattikorkeakoulututkinto

Kyberturvallisuuden koulutusohjelma

2023

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri YAMK
Tekijä/Tekijät	Satu Koskinen
Työn nimi	Kyberturvallisuuden toteutuminen alihankintaketjuissa
Toimeksiantaja	YTK
Vuosi	2023
Sivut	75 sivua, liitteitä 4 sivua
Työn ohjaaja	Vesa Kankare

TIIVISTELMÄ

Tutkimuksen tavoitteena oli tutkia, miten ja miksi kyberturvallisuus toteutuu alihankintaketjuissa. Tutkimus sai alkunsa aidosta kiinnostuksesta aihetta kohtaan sekä ajankohtaisista keskusteluista huoltovarmuuskriittisten organisaatioiden kanssa. Aihe on tärkeä, eikä siitä ole riittävästi tutkimustietoa, joten motivaatio ja innostus tutkimuksen tekemiselle oli vahva.

Tutkimusongelman ratkaisemiseksi asetettiin tutkimuskysymyksiä, joihin haettiin vastauksia eri keinoin. Tutkimuksessa selvitettiin muun muassa, mitkä tekijät vaikuttavat siihen, että kyberturvallisuus toteutuu alihankintaketjuissa ja miten kyberturvallisuuden toteutumista alihankintaketjuissa voidaan varmistaa. Lisäksi tutkimuksessa tutkittiin, millaisia tekijöitä tutkimukseen osallistuvat huoltovarmuuskriittiset organisaatiot itse näkevät keskeisinä elementteinä, joilla on vaikutusta kyberturvallisuuden toteutumiseen. Tutkimuksessa peilattiin tutkimuksen tuloksia teoreettiseen viitekehykseen ja tarkasteltiin erilaisten tekijöiden merkitystä kyberturvallisuuden toteutumiseen alihankintaketjuissa.

Tutkimus oli rajattu muutamiin huoltovarmuuskriittisiin toimijoihin alihankintaketjun eri kohdista. Tutkimus toteutettiin monimenetelmäisenä tapaustutkimuksena. Keinoina käytettiin haastatteluja ja kyselytutkimuksia sekä lopputulosten luotettavuuden tarkasteluun yhteen vetävää loppukeskustelua. Monimenetelmäisyys nousi tarpeena varmistaa tutkimuksen luotettavuus ja kattavuus.

Tutkimuksen perusteella voidaan todeta, että johdon sitoutumisella ja resurssien osoittamisella organisaation käyttöön, on erittäin keskeinen merkitys kyberturvallisuuden toteutumisessa alihankintaketjuissa. Johto voi myös omalla toiminnallaan mahdollistaa kulttuurin, jossa kyberturvallisuus otetaan vakavasti ja osana liiketoiminnan kehitystä. Toinen huomio liittyi osaamiseen, jonka merkitys oli myös huomattava. Osaamisen alle on tuloksissa sijoitettu myös hallinnolliset tietoturvan keinot, joihin sisältyvät yrityksen omat tietoturvapolitiikat, ohjeet ja toimintatavat. Kolmantena päähuomiona oli asiakkaiden ja yhteistyökumppaneiden vaatimukset, jotka usein perustuvat lakiin ja asetuksiin. Huoltovarmuuskriittisyys ei noussut esille niin voimakkaasti, kuin tutkimuksen tekijä oletti.

Asiasanat: kyberturvallisuus, alihankintaketjut, huoltovarmuuskriittisyys

South-Eastern Finland University of Applied Sciences

Degree title	Master of Engineering
Author (authors)	Satu Koskinen
Thesis title	Realization of cyber security in subcontracting chains
Commissioned by	YTK
Time	2023
Pages	75 pages, 4 pages of appendices
Supervisor	Vesa Kankare

ABSTRACT

The objective of the thesis was to investigate the realization of cyber security in subcontracting chains of organisations critical to security of supply. The research started out of a genuine interest in the subject, as well as discussions with organizations that are critical to security of supply. The topic is important, and since there is limited research data available, the motivation and enthusiasm to do the research were strong.

The research was carried out as a multi-method case study, utilizing interviews and surveys. The use of multimethodology was necessary to ensure the reliability and comprehensiveness of the research.

Based on the findings, it can be concluded that management's commitment plays a crucial role in the successful realization of cybersecurity in subcontracting chains. Through their own actions, management can enable a culture where cybersecurity is taken seriously and as part of business development. Another significant point that emerged was the importance of the competence. The organization's cybersecurity expertise made important administrative cybersecurity actions possible. The third key aspect that affects the realization of cybersecurity was the influence of demands from different parties, such as customers and partners. Surprisingly, the aspect of security of supply did not arise as strongly as assumed.

The study clearly discovered the factors that affect the realization of cyber security in subcontracting chains. By addressing these issues, the commissioner of the thesis (YTK) and the other participating companies can ensure that cyber security is realized.

Keywords: cybersecurity, subcontracting chains, security of supply

SISÄLLYS

LIITTEET

1 JOHDANTO

1.1 Tutkimuksen tausta

Kyberturvallisuus on noussut vallitsevan geopoliittisen tilanteen vuoksi entistä näkyvämmin niin jokaisen kansalaisen kuin päättäjienkin väliseen keskusteluun. Venäjän hyökättyä Ukrainaan helmikuussa 2022 olemme kuulleet lukuisista kyberiskuista ja niiden aiheuttamista laajoista tuhoista ja haitoista. Toisaalta olemme kuulleet Ukrainan nopeista reagoinneista kyberiskuihin ja innovatiivisista keinoista yhteiskunnan IT-infrastruktuurin turvaamiseksi.

Suomessa kyberturvallisuuden kehittäminen on ollut määrätietoista mutta myös hajautunutta. Suomen ensimmäinen kyberturvallisuusstrategia laadittiin vuonna 2013 ja viimeisin 2019. Tuoreimmassa kyberturvallisuusstrategiassa asetetaan kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi sekä elintärkeiden toimintojen turvaamiseksi. (Turvallisuuskomitea 2019, 4.) Kyberturvallisuudesta puhuttaessa nousee esille kuitenkin suhteellisen harvoin alihankintaketjujen riskit tai toimet, joilla alihankintaketjujen riskejä voitaisiin pienentää. Niin huoltovarmuuskriittisillä organisaatioilla, kun muillakin, on harvoin vain yksi toimittaja tai toimittajia, ilman että toimittaja tai yhteistyökumppani käyttäisi alihankintaa. Kyberturvallisuuden professori Jarmo Limnell on jo lähes kymmenen vuotta sitten todennut, että yhteiskunnan toimivuuden kannalta täytyy huomioida, että kriittinen infrastruktuuri on yli 80-prosenttisesti jonkun muun kuin valtion hallinnassa (Suomen puolustusvoimilla voisi olla kyberjoukot 2014).

Huoltovarmuuskeskuksen Digipooli julkaisi toimialojen kyberkypsyyden selvityksen 14.3.2023 (Huoltovarmuuskeskus 2023). Toimialojen kyberselvitys toteutettiin vuonna 2022 ja se kertoi, että suomalaisten yritysten ja organisaatioiden kyberkyvykkyys on hyvää perustasoa, mutta hajontaa eri toimialojen ja organisaatioiden välillä on havaittavissa. Yksi keskeisistä havainnoista liittyi kumppanihallintaan. Selvityksessä todetaan, että osallistuneet organisaatiot luottavat kumppaneihin kyberturvallisuuden hallinnan ja valvonnan osalta, eivätkä tee valvontatoimenpiteitä raportoinnin lisäksi. Yritykset usein siirtävät vastuun alihankintaketjuissa suorien kumppaneiden vastuulle. Samassa Huol-

tovarmuuskeskuksen selvityksessä todetaan, että kumppanit ja niiden alihankkijat voivat jopa laajentaa yrityksen verkkoa ja mikäli tällaiset riippuvuudet eivät ole tiedossa, on niiden aiheuttama potentiaalinen uhka merkittävä. (Huoltovarmuuskeskus 2023.)

Euroopan unionin kyberturvallisuusviraston (ENISA) julkaiseman raportin mukaan toimitusketjuhyökkäykset ovat kahden yleisimmän kyberuhkan joukossa. Organisaatioiden haavoittuvuus toimitusketjuhyökkäyksille on kasvanut, sillä yhä useammin järjestelmät ovat monimutkaisia ja toimittajia on paljon. (Enisa 2022.) Myös maailman talousjärjestön (Word Economy Forum 2022) mukaan kolmannen osapuolen hyökkäykset ovat kasvussa. Maailman talousfoorumin kyselyyn osallistui 120 kyberturvallisuudesta vastaavaa johtajaa 20 eri maasta. Kyberturvallisuudesta vastaavat johtajat ovat huolissaan hyökkäyksistä, jotka tulevat toimitusketjuista. Toimitusketjuhyökkäyksien kasvu onkin ollut merkittävää ja noussut jo 44 %:sta 61 %:iin muutamassa vuodessa. Lähes puolet kyselyyn osallistuneista toimitusjohtajista näkee, että toimitusketjujen kautta tulevat hyökkäykset ovat keskeisin vaara heidän kyberturvallisuudelleen. Myös luottamus toimittajiin on kärsinyt: lähes 60 % vastaajista koki, että toimittajien ja yhteistyökumppaneiden kyberturvallisuus on huonommalla tasolla kuin heidän omansa. Maailman talousjärjestö suosittaakin käymään oman yhteistyöverkostonsa läpi, keskittymään puolustamisen lisäksi resilienssiin ja vahvistamaan koko ekosysteemin kyberkestävyyttä. Tämän tutkimuksen kannalta merkittävää on myös se, että lähes 90 % johtajista suunnitteli parantavansa kyberresilienssiään eri keinoin johtaakseen kolmansia osapuolia tehokkaammin ja paremmin. (Word Economy Forum 2022.)

Alihankintaketjujen kyberturvallisuuden kehittämisen tärkeys on selvästi maailmanlaajuisesti kuin myös Suomessa hyvin tiedossa. Tarvitaan lisää tutkimusta, määrätietoisia toimia ja lainsäädäntöä tukemaan asian etenemistä. Tämän tutkimuksen tarkoitus on omalta osaltaan tuottaa tietoa päätöksenteon tueksi. On mielenkiintoista nähdä, milloin ja kuinka vahvasti Suomessa, ja millä toimin, asiaa aletaan edistää ja ohjata. Suomi on aktiivisesti mukana Euroopan laajuisten lakien ja asetusten laadinnassa, mutta riittääkö se, vai pitäisikö ottaa vahvempi ote tähän keskeiseen kyberturvallisuuden tasoon vaikuttavaan ongelmakohtaan?

1.2 Tutkimuksen tarkoitus ja tavoitteet

Tässä tutkimuksessa on tarkoitus löytää havaintoja ja huomioita, jotka selittävät kyberturvallisuuden toteutumista alihankintaketjuissa. Kyberturvallisuudessa hyökkäyspinta-alaa kasvattavat alihankintaketjut. Alihankintaketjut muodostavat merkittävän osan yritysten kyberturvallisuuden kokonaisuudesta. Tutkimuksen perusteella toimeksiantaja sekä muut tutkimukseen osallistuvat huoltovarmuuskriittiset yritykset voivat kasvattaa omaa tietoisuuttaan ja pohtia mahdollisesti omia jatkotoimenpiteitään. Toimeksiantajan ensisijainen tavoite on turvata jäsenistölleen turvalliset ja laadukkaat palvelut. Työttömyyskassatoiminta on osa Suomen huoltovarmuuskriittistä toimintaa. Jäsenen turva on YTK:n tärkein tehtävä. (YTK 2023.)

Tutkimuksen toisena tarkoituksena on tuottaa tietoa ja herättää keskustelua tutkittavasta aiheesta. Keskustelun herättämisen lisäksi tarvitaan tutkimuksia, toimenpiteitä, asetuksia ja tarvittavaa tukea yrityksille, jotta he voivat kehittää omaa toimintaansa. Vaikka askeleita on jo otettu, kyberturvallisuuskenttä muuttuu nopeasti ja myös kyberturvallisuuden kasvattamisen keinovalikoiman on oltava laaja ja jatkuvasti kehittyvä. Kolmas tutkimuksen tarkoituksista on tuottaa tietoa jatkotutkimuksia varten, sillä aihetta on syytä tutkia lisää. Tutkimuksella voi olla myös merkitystä yhteiskunnallisiin päätöksiin koskien kansallisia suosituksia, tukea ja jopa tarvittavia lakiasetuksia myöten. Tutkimuksen tuottaman tiedon kautta niin yritykset kuin lainsäätäjätkin voivat kiinnittää huomiota tähän melko vähäisesti tutkittuun, mutta varsin merkittävään kyberturvallisuuteen yhteiskunnassamme vaikuttavaan asiaan.

1.3 Tutkimuksen rakenne

Tämän tutkimuksen johdannossa kuvaan kyberturvallisuuden ajankohtaisuutta ja tärkeyttä Suomessa ja kansainvälisesti. Lisäksi kerron tutkimuksen tarkoituksesta ja tavoitteista. Tutkimusasetelmaksi nimetty luku sisältää tutkimusongelman kuvaamisen sekä tutkimuskysymyksien esittelyn. Lisäksi siinä kuvataan aineiston hankinta- ja analyysitapoja sekä tutkimuksessa noudatettavia eettisyyden periaatteita. Tässä luvussa esittelen myös joitakin tutkimushypoteeseja, jotka perustuvat tietoperustaan ja tutkijan omaan kokemukseen kyberturvallisuuden johtamisesta. Tutkimuksen luvut 3–5 luovat tietoperustaa

työlle pureutuen kyberturvallisuuden määritelmään, alihankintaketjujen tarkasteluun sekä pohdintaan kyberturvallisuuden toteutumisesta. Luvussa 6 esitellään tutkimusjoukon määrittely. Luku 7 käsittelee tutkimuksen toteutusta ja vastauksia teema-alueittain. Luvut 8–10 sisältävät tulokset, johtopäätökset ja pohdinnan.

2 TUTKIMUSASETELMA

2.1 Tutkimusongelma ja tutkimuskysymykset

Tutkimusongelma on selvittää, miten ja miksi kyberturvallisuus toteutuu alihankintaketjuissa. Tutkimuskysymykset koostuvat pääkysymyksestä ja neljästä täydentävästä apukysymyksestä.

Tutkimuksen pääkysymys:
Mitkä tekijät vaikuttavat siihen, että kyberturvallisuus toteutuu alihankintaketjuissa?

Täydentävät apukysymykset:

1. *Onko kyberturvallisuuden määritelmä ymmärrettävä?*
2. *Mitkä asiat vaikuttavat kyberturvallisuuden tasoon?*
3. *Miten kyberturvallisuutta johdetaan alihankintaketjuissa?*
4. *Milloin voidaan todeta, että kyberturvallisuus toteutuu alihankintaketjuissa?*

Ensimmäisen apukysymyksen tarkoitus on tutkia kyberturvallisuuden määritelmän ymmärrettävyyttä. Toisen kysymyksen avulla selvitetään niitä tekijöitä, jotka vaikuttava kyberturvallisuuden tasoon. Näitä voivat olla ihmisiin, työkaluihin tai muihin tekijöihin liittyvät asiat. Kolmas kysymys tarkastelee niitä asioita, jotka liittyvät kyberturvallisuuden johtamiseen alihankintaketjuissa. Vaikuttavia tekijöitä voivat olla, kuten tutkimuskysymyksessä 3, myös ihmiset ja työkalut, mahdollisesti myös sopimukset. Viimeisen apukysymyksen tarkoitus on selvittää, milloin voidaan todeta kyberturvallisuuden toteutuminen alihankintaketjuissa.

Haastattelu- ja kyselytutkimuksen kysymykset on jaettu teema-alueisiin, jotta haastattelu voidaan toteuttaa puolistrukturoituna teemahaastatteluna. Jokaiselle haastattelukysymykselle on määritelty ensisijainen teema-alue, mutta

suurin osa kysymyksistä kattaa muitakin teema-alueita. Kyselytutkimuksen kysymyksille on asetettu jo lähtökohtaisesti useita teema-alueita. Haastattelu- ja kyselytutkimuksen kysymykset teema-alueineen löytyvät tutkimuksen liitteistä 1 ja 2. Oheisessa taulukossa (Taulukko 1) kysymykset on jaoteltu alustavasti arvioiden, mihin tutkimuskysymykseen ne vastaavat.

Taulukko 1. Tutkimuskysymyksien ja haastattelu- ja kyselytutkimuksien suhde

Tutkimuskysymys	Haastattelu-kysymykset	Kyselytutkimuksen kysymykset
1.Onko kyberturvallisuuden määritelmä ymmärrettävä?	H1–H12	K1–K9
2.Mitkä tekijät vaikuttavat kyberturvallisuuden tasoon?	H1–H8, H12	K1, K2, K5
3.Miten kyberturvallisuutta johdetaan alihankintaketjuissa?	H3, H4, H5, H8, H10, H11, H12	K6, K7, K8
4.Milloin voidaan todeta, että kyberturvallisuus toteutuu alihankintaketjuissa?	H10, H12	K1, K5, K6, K7

Teema-alueet:

1. Ihmiset: Yrityksen henkilökunnan vaikutus, myös hallitus
   Alueeseen liittyvät haastattelukysymykset (H) ja kyselytutkimuskysymykset (K) ovat: ***H2****, H3, H5, K4*

2. Osaaminen: Yrityksen osaamisen taso, myös yhteistyökumppanien ja asiakkaiden osaaminen
   Alueeseen liittyvät haastattelukysymykset (H) ja kyselytutkimuskysymykset (K) ovat: ***H5****, H6, H9, H10, K4, K6, K7, K8*

3. Harjoittelu: Kaikki yrityksen sisäinen sekä ulkoinen harjoittelu
   Alueeseen liittyvät haastattelukysymykset (H) ja kyselytutkimuskysymykset (K) ovat: ***H8,*** *H11, K2*

4. Vaatimukset: laista, asetuksista, säädöksistä ja/tai asiakkailta tai yhteistyökumppaneilta tulevat vaatimukset
   Alueeseen liittyvät haastattelukysymykset (H) ja kyselytutkimuskysymykset (K) ovat: ***H12,*** *H3, K5*

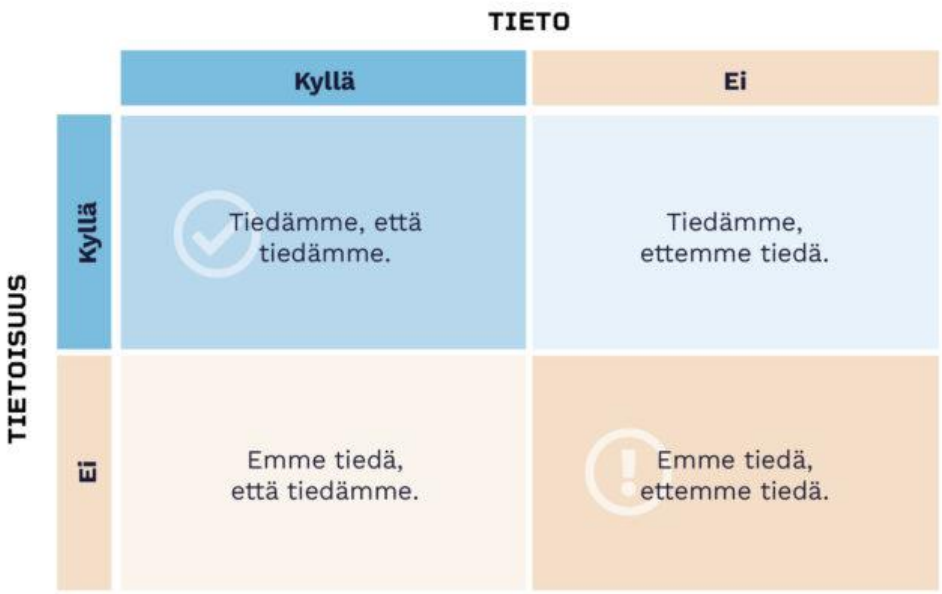
5. Tausta: Yrityksen kyberturvallisuuden kehittymiseen liittyvät tieto tai muu vaikuttava tekijä (budjetti yms.)
   Alueeseen liittyvät haastattelukysymykset (H) ja kyselytutkimuskysymykset (K) ovat: **H1**, H7, K1, K3

6. Hallinto: Yrityksen tapa käsitellä kyberturvallisuutta, hallintomalli, päätöksentekomalli
   Alueeseen liittyvät haastattelukysymykset (H) ja kyselytutkimuskysymykset (K) ovat: **H3,** H10, H11, K2

7. Sopimukset: Yrityksen tapa tehdä sopimuksia sekä huomioida kyberturvallisuus
   *Alueeseen liittyvät haastattelukysymykset (H) ja kyselytutkimuskysymykset (K) ovat: **H4**, H11, K2, K6, K7*

8. Työkalut- ja ohjeistus: Yrityksen käytössä olevat työkalut- ja ohjeistukset, sekä mahdolliset sertifikaatit ja ohjeistukset
   *Alueeseen liittyvät haastattelukysymykset (H) ja kyselytutkimuskysymykset (K) ovat: **H10,** H3, H10, K1, K5, K9*

Tutkimuskysymysten avulla on tarkoitus saada myös näkymää alla olevan jaottelun kautta aiheeseen. Tietoisuuden ja tiedon nelikenttä sopii osuvasti myös kyberturvallisuustietoisuuden pohdintaan siitä näkökulmasta, mikä on tietoisuuden ja ymmärryksen vaikutus kyberturvallisuuden toteutumisessa. Sellaisesta, mitä ei tiedä, on vaikea olla huolissaan. Korkeamman osaamisen vallitessa on helppo ymmärtää, missä kyberturvallisuuden osa-alueella yrityksellä on kehittämistä, tai parhaimmillaan saada kyberturvallisuus sellaiselle tasolle, joka on johdon määrittelemä riittävän kattavan asiantuntijavalmistelun pohjalta. Vaarallisin osa-alue on ensiksi mainittu, jossa tietoisuutta ei ole riittävästi, jotta olisi edes mahdollista ymmärtää tarvittavan tekemisen määrää kyberturvallisuuden saralla.



Kuva 1: Tietoisuuden ja tiedon nelikenttä (Seppänen 2022)

Jokainen yritys ja yksilö hahmottaa omaa kyberturvallisuuden tasoaan omista osaamislähtökohdistaan. Mikäli osaamista on jonkin verran, liikutaan jo oikeasta alalaidasta tietoisuuden ja tiedon nelikentässä oikeaan yläkulmaan. Tuolloin yritys jo mahdollisesti ymmärtää lisäavun tarpeen.

2.2 Tutkimusote

Tutkimusmenetelmiä ovat laadullinen, määrällinen ja prosessuaalinen tutkimus. Tutkimusmenetelmän valinta tulee aina perustella huolellisesti. Perustelut ovat tärkeitä myös työn luotettavuuden ja uskottavuuden kannalta. (Kananen 2015.) Tieteellisessä tutkimuksessa haetaan usein päätuotoksena uutta teoriaa, kun taas tutkimuksellinen kehittäminen paneutuu enemmän käytännön ratkaisuihin. Tämä tutkimus toteutetaan monimenetelmäisenä tapaustutkimuksena. Tapaustutkimuksessa tutustutaan tapaukseen kokonaisvaltaisesti. Siinä usein yhdistellään erilaisia aineistoja, kuten esimerkiksi haastatteluja, tilastoja, tapaukseen liittyviä asiakirjoja tai mediasta löytyviä juttuja. Laadulliset tutkimukset ovat usein lähellä tapaustutkimusta, koska niissäkin tutkittava asia on esimerkki jostakin laajemmasta asiasta. Tutkimuksen kohteena, eli tapauksena, voi näin ollen olla vaikkapa organisaatio, oppilaitos tai projekti tai jopa prosessi (Vuori 2015.)

Tapaustutkimus soveltuu lähestymistavaksi seuraavissa tilanteissa:

• ’Mitä-’, ’miten-’ ja ’miksi-’kysymykset ovat tärkeitä.
• Tutkija ei kontrolloi tai kontrolloi vain vähän tapahtumia itse.
• Aiheen empiirinen tutkimusmäärä on vähäinen.
• Tutkimuskohde on ajankohtainen ilmiö.
(Eriksson ym. 2005.)

Tähän tutkimukseen tapaustutkimus valikoitui siksi, että aiheesta löytyi vain kohtalainen määrä tutkimuksia ja julkaisuja. Lisäksi miten- ja miksi-kysymykset olivat hyvin keskeisellä sijalla tutkimuksessa. Kehittämistutkimus olisi voinut aiheen huomioon ottaen olla myös vaikea rajata. Pohdittavana oli myös tapaustutkimuksen ja toimintatutkimuksen yhdistäminen, mutta koska toimintatutkimuksen sisällyttäminen mukaan tarkoittaisi osallistumista tutkimusproses-

siin, jossa olisi tutkijan oman taustan vuoksi vaaransa vaikuttaa liikaa tutkimukseen, vaihtoehto ei ollut sopiva. Tapaustutkimus ja toimintatutkimus eroavat toisistaan tutkimuskohteen aineiston keräämisen ja tutkimuskohteen arvioinnin suhteen. Tapaustutkimuksessa ensimmäinen vaihe on toiminta tutkimuskohteessa ja arviointi tapahtuu vasta sen jälkeen. Toimintatutkimuksessa tutkija osallistuu toimintaan, havainnointiin sekä toiminnan arviointiin. Toimintatutkimuksen vahvuus verrattuna tapaustutkimukseen tulee sen reflektiivisyydestä. (Laine ym. 2018.)

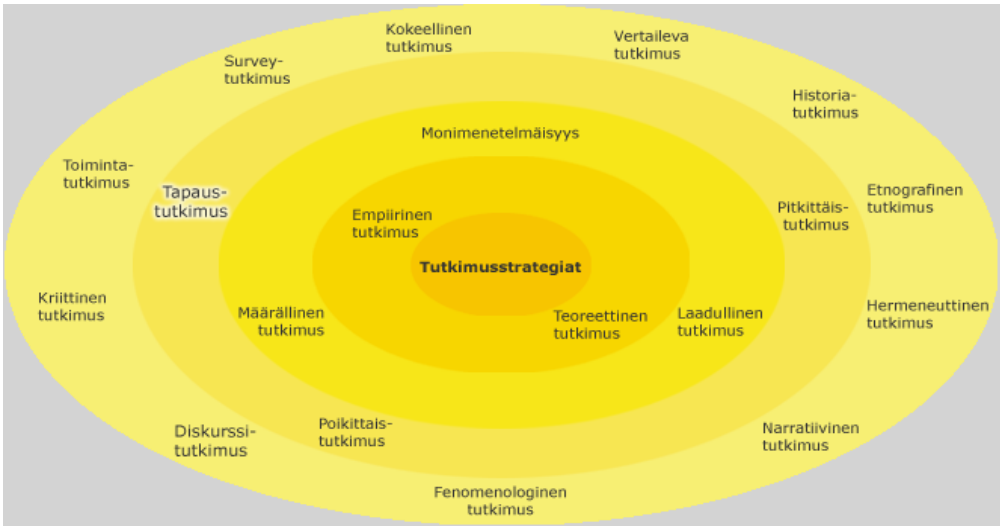
Tapaustutkimuksen käsitettä on usein käytetty virheellisesti viittamaan erilaisiin tutkimusmenetelmiin, jota se ei ole. Tapaustutkimus sisältää lähtökohtaisesti useita tutkimusmenetelmiä, siksi voidaan sanoa, että tapaustutkimus ei ole menetelmä, vaan enemmänkin tutkimustapa tai tutkimusstrategia, jonka sisällä voidaan käyttää erilaisia aineistoja ja menetelmiä. Tapaustutkimuksen päämääränä on tapauksen ymmärtäminen. Tapauksen yleinen merkitys voi ilmetä kahdella tavalla: 1) teoriaa kyseenalaistava tai uutta teoriaa luova tapaus ja 2) yleistys. Tapaustutkimuksessa usein liikutaan induktiivisesti yksityisestä yleiseen, kun taas määrällinen tutkimus etenee deduktiivisesti yleisestä yksityiseen. Induktiivisessa tutkimustavassa lähdetään liikkeelle aineistosta ja se on jo lähtökohtaisesti teoriattomampaa. Deduktiivinen tutkimustapa taas vaatii, että teoria on voitava luoda ennen kuin sen oikeellisuutta voidaan testata. Tapaustutkimuksessa ei tiedetä välttämättä alussa, millaista näkökulmaa kannattaa käyttää, joten teoreettinen näkökulma on valittava, tai ainakin tarkennettava myöhemmin työn edetessä. (Laine ym. 2018, 29.)

Tapaustutkimus voi olla luonteeltaan uutta teoriaa kartoittava tai aiempaa teoriaa laajentava. Uutta teoriaa kartoittava sopii tutkimuksen kohteen oman tilanteen tarkasteluun ja vaatii usein lisätutkimusta. Sen sijaan aiempaa teoriaa laajentava luo jo malleja ja vahvempia ja luotettavampia teorioita. Tapaustutkimuksen lähestymistapa nähdäänkin usein uutta löytävänä tapana. Tarkoitus on tuottaa uusia teoreettisia ideoita tai hypoteeseja niistä syistä, joita tuottavat tietyt käytännöt. Kehittämisen jälkeen näitä voidaan koetalla uusissa tutkimuksissa. Yhden tai muutaman tapauksen tulkitsevaa tutkimusta kutsutaan intensiiviseksi tapaustutkimukseksi. Näissä tutkimuksissa tutkija tarkastelee tapausta osallistuvien näkökulmaa käyttäen, heidän käyttämällään kielellä ja käsitteillä. Sen sijaan ekstensiivinen tapaustutkimus etsii yhteisiä ominaisuuksia,

malleja ja uusia teoreettisia ideoita ja käsitteitä usean tapauksen vertailun avulla. Tapauksia käytetään näin ollen välineinä ilmiön tutkimisessa. (Eriksson ym. 2005.)

Tässä tutkimuksessa käytetään haastatteluja ja kyselyjä. Tutkimuksen luotettavuutta vahvistetaan osallistuvien yritysten välisellä loppukeskustelulla. Haastattelut toteutetaan ensin, jonka jälkeen kyselytutkimuksen kysymyksiä on vielä mahdollista muokata ennen kyselyn lähettämistä osallistujille. Muokkausta tehdään vain, mikäli haastatteluaineiston litteroinnin ja analysoinnin perusteella näyttää siltä, että jokin osa-alue on jäänyt vähäisemmälle käsittelylle. Lisäksi kaikkien osallistujien kesken käydään vapaamuotoisia keskusteluja haastattelujen ja kyselyjen ulkopuolella. Näiden vapaamuotoisten keskustelujen havaintojen ja huomioiden esittämiseen tutkimuksessa pyydetään erikseen lupa jokaiselta osallistuvalta yritykseltä. Näiden keskustelujen tarkoitus on käydä läpi työn edistymiseen liittyviä sovittavia asioita, kuten haastatteluajat, kyselyyn vastaamiset, sekä sen lisäksi havainnoida asioita, joilla voisi olla merkitystä tämän tutkimuksen kannalta.

Tapaustutkimuksen sijoittumista muihin tutkimusstrategioihin nähden voidaan tarkastella oheisen Jyväskylän Yliopiston kuvan (kuva 3) avulla. Kuva havainnollistaa jo aiemmin tässä kappaleessa esille tuotua näkemystä, jossa tapaustutkimus tulee nähdä enemmän tutkimustapana tai strategiana kuin tutkimusmenetelmänä.



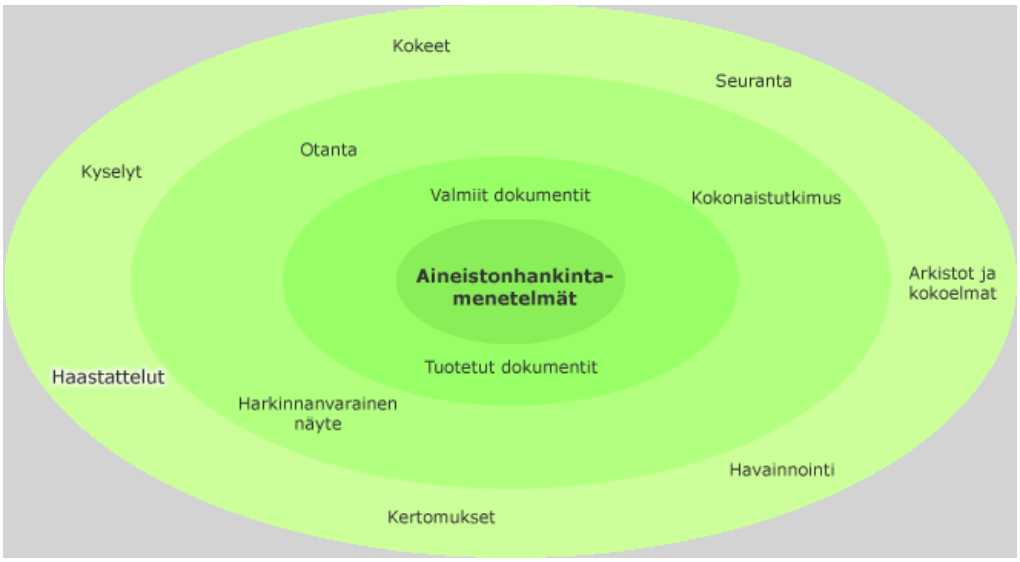
Kuva 2: Tapaustutkimus (Jyväkylän yliopisto 2015.

Tutkimusstrategia koostuu niistä periaatteellisista valinnoista, jolla tutkimus on tarkoitus toteuttaa (Jyväskylän Yliopisto 2015). Keskeistä tutkimuksen teossa on osata valita ja perustella tutkimusstrategian kautta tutkimuksessa käytettävien menetelmien valinta.

2.3 Aineiston hankintatavat

Tutkimuksessa käytetään teoriapohjana muita aiemmin tehtyjä tutkimuksia ja julkaisuja. Tutkimusmenetelminä käytetään haastatteluja ja kyselyjä, ja loppukeskustelu varmistaa tutkimuksen luotettavuutta.

Aineistohankintatavat on valittava niin, että ne tukevat tutkimusongelman ratkaisemista. Aineistonhankintatapoja voi yhdistellä ja valita useita. Oheinen Jyväskylän yliopiston kuva (Kuva 4) havainnollistaa aineistonhankintamenetelmien laajuutta.



Kuva 3. Aineistonhankintamenetelmät (Jyväskylän Yliopisto 2014)

Aineistonhankintamenetelmät jaetaan sekä valmiisiin dokumentteihin että tuotettuihin dokumentteihin. Näitä erilaisia dokumentteja taas löytyy erilaisia ja eri tavalla hankittuja. Voidaan käyttää otantaa, kokonaistutkimusta tai vaikka harkinnanvaraista näytettä. Näitä taas voidaan saada haastatteluilla, havainnoinneilla, kertomuksilla, kokeilla, kyselyillä sekä arkistoista ja kokoelmista.

Haastattelu sopii metodiksi ilmiön tutkimiseen tai silloin, kun tutkitaan intiimejä tai emotionaalisia asioita (Hirsjärvi ym. 2008). Tässä tutkimuksessa tutkitaan aihetta, josta puhuminen on luottamuksellista ja sisältää yritykselle keskeistä ja strategista tietoa. Haastattelu on näin ollen paras tapa käydä luottamuksellista ja avointa keskustelua aiheesta.

Kyselytutkimuksen etuna on taas se, että vastauksien analysointi onnistuu sekä määrällisenä että laadullisesti (Jyväskylän Yliopisto 2015). Lisäksi vastaajalla on oman aikataulunsa mukaisesti väljemmin aikaa pohtia vastauksia kysymyksiin, eikä esimerkiksi jännitys vaikuta vastauksiin, kuten mahdollisesti haastattelussa.

2.4 Haastattelujen ja kyselyjen toteutustapa

Tutkimusta toteutettaessa on hyvä pitää mielessä hyvän tieteellisen käytännön periaatteet. Tutkimukseen osallistuvalle on taattava riittävä tieto tutkimuksesta, jotta hän voi päättää ylipäätään osallistumisesta, mutta myös valmistautua tutkimukseen (Vilkka 2014). Kaikissa käytettävissä menetelmissä on myös tärkeää kertoa osallistuvalle luottamuksellisuudesta ja tietojen huolellisesta käsittelystä. Etukäteen myös kerrotaan selkeästi haastattelupaikka- ja aika, sekä haastattelun kulku sekä koko tutkimustyön aikataulu. Lisäksi kerrotaan, kuinka osallistuva organisaatio saa tutkimuksen lopputuloksista ja havainnoista tietoa. Haastattelussa, kuten kyselyissäkin, on myös tärkeää, ettei tutkija tuo omia näkemyksiään esille tai varsinkaan kysymysten avulla johdattele osallistujaa millään tavalla, jotteivät tutkimustulokset vääristy tai värity.

Haastattelu toteutetaan sekä yksilöhaastatteluna että ryhmähaastatteluna. Tämä riippuu osallistuvan yrityksen toiveesta. Ryhmähaastattelussa osallistujien määrä rajataan vain kahteen, että nauhoitetta olisi helppo jälkikäteen käsitellä, sillä rajatulla osallistujamäärällä pienennetään päälle puhumisen ja sitä kautta vaikeutuvan litteroinnin vaaraa. Yksilöhaastattelu on myös yleisimmin käytetty menetelmä ja ehkäpä jopa helpoin haastattelijan kannalta. Siinä etuna on se, etteivät muut henkilöt vaikuta keskusteluun. Kuitenkin yksilöhaastattelun huonona puolena on se, että haastateltavasta voi tilanne tuntua jännittävältä tai ahdistavalta. (Hirsijärvi ym. 2008, 61.)

Haastatteluihin käytetty aika voi vaihdella. Haastatteluajan vaihtelu johtuu lähinnä haastateltavasta, toki myös tilanteesta ja ulkopuolisista syistä. Ennen kun haastattelu alkaa, on hyvä varata vapaamuotoiselle keskustelulle aikaa. Tämä vähentää mahdollista jännitystä ja lisää luottamuksellisuuden ilmapiiriä. Haastattelutilanteessa on muistettava, että vaikka haastattelijan oma tavoite täyttyy, ei haastattelua pidä silti päättää lyhyesti. (Hirsjärvi ym. 2008.)

Tässä tutkimuksessa käytetään puolistrukturoitua haastattelua eli teemahaastattelua. Muita mahdollisia haastattelun malleja ovat avoin haastattelu, syvä haastattelu ja strukturoitu haastattelu. Valinta kohdistui puolistrukturoituun haastatteluun, koska se mahdollistaa rennomman keskustelun ja ohessa on mahdollista saada hyödyllistä tietoa. Puolistrukturoidussa teemahaastattelussa haastattelukysymykset on mietitty etukäteen, mutta niillä ei ole tarkkaa etenemisjärjestystä. Kaikille haastateltaville esitetään likipitäen samat kysymykset ja samassa järjestyksessä mutta kysymysten järjestystä voidaan myös vaihdella. Yhtenäinen määritys puolistrukturoitujen haastattelujen toteutuksesta puuttuu, mutta useiden määritelmien mukaan niitä voidaan kutsua myös teemahaastatteluiksi (Hirsjärvi ym. 2008).

Kyselytutkimus on enimmäkseen yleensä määrällistä tutkimusta, jossa sovelletaan tilastollisia menetelmiä. Kyselyaineisto koostuu mitatuista luvuista ja numeroista. Sanallisesti voidaan antaa lisätietoja tai täydentäviä tietoja. (Vehkalahti 2014,11.). Tässä tutkimuksessa kyselyssä käytetään hyvin samankaltaisia kysymyksiä kuin haastatteluissa, ja haastattelun jälkeen kyselytutkimuksen kysymyksiä voidaan vielä muokata sen varmistamiseksi, että tutkimusongelmaan saadaan vastaus. Sekä haastattelussa että kyselyssä painotetaan, ettei luottamuksellisia tietoja, kuten yhteistyökumppanien nimiä, sopimuksia, euromääriä tai mitään vastaavia luottamuksellisia tietoja, saa laittaa kyselytutkimuksen tietoihin, eikä mainita haastattelujen aikana.

Kyselytutkimuksen voi osallistua vastaamalla kysymyksiin Webropol -kyselytyökalussa. Tämä väline valikoitui kyselyn toteuttamisen välineeksi siksi, että se täyttää GDPR-vaatimukset ja sen kahdennetut palvelimet sijaitsevat Suomessa. Kyselyyn on kuitenkin mahdollista halutessaan vastata myös muilla tavoilla. Kyselylomake jaetaan haastattelujen jälkeen ja sen voi myös palauttaa

postitse, sähköpostin turvapostilla tai vastaten kyselyyn edellä mainittua työkalua käyttäen. Myös mahdollisuus käydä kyselytutkimuksen kysymyksiä fyysisenä tai Microsoft Teams -etäkokouksena mahdollistetaan.

2.5 Haastattelu- ja kyselytutkimusaineiston analyysitapa

Tässä haastattelututkimuksessa käytetään sanasanaista puhtaaksikirjoitusta eli litterointia. Litterointi voidaan tehdä valikoiden, vain teema-alueista tai vain haastateltavan puheesta tai sitten koko haastatteludialogista. Litterointi suoraan nauhalta on haastavaa ja työlästä ja vaatii tarkkuutta. Litteroinnin aikana voidaan tarkentaa jo annettuja teematunnisteita, jotta samaa teemaa koskevat vastaukset voidaan tunnistaa myöhemmin. On kuitenkin huomioitava, että käsittelyssä on katsottava kokonaisuutta, eikä mentävä liikaan teema-alueiden kautta johtopäätöksiin. Litteroinnin ja teemoituksen jälkeen on tärkeää lukea aineisto vielä kokonaisuutena läpi useita kertoja. Aineiston läpiluku useaan kertaan voi synnyttää uusia ajatuksia, näkökulmia tai jopa kysymyksiä. (Hirsijärvi ym. 2008.)

Teemoituksen jälkeen on vuorossa aineiston luokittelu, yhdistely ja analysointi. Valittujen luokkien perustelu on tärkeää, sillä luokittelu on myös pystyttävä perustelemaan. Hienolta näyttävät luokat, jotka eivät vastaa aineistoa, eivät ole sopivia. Teemahaastatteluja, joihin puolistrukturoitu teemahaastattelu kuuluu, voidaan käsitellä sekä kvantitatiivisesti että kvalitatiivisesti. Haastattelussa saatu materiaali voidaan myös muuntaa kvantitatiivisessa käsittelyssä muuttujiksi. Tällöin menettely muistuttaa tapaa, jota käytetään aineiston kvalitatiivisessa käsittelyssä. Tässä tutkimuksessa käytetään molempia keinoja, tosin kvantitatiivista vain rajallisessa määrin. Aineiston luokittelu ja koodaaminen ei saa kuitenkaan olla kuin välivaihe analyysin rakentamisessa. Tähän pätee esimerkki talon rakennuksesta: taloa rakentaessa tiilet yhdistellään joidenkin periaatteiden mukaisesti ja rakennus syntyy vasta kun koko työ eli talon rakennus on suoritettu ohjeiden mukaan. (Hirsijärvi ym. 2008, 149.)

2.6 Tutkimuksen eettisyyden periaatteet

Tutkimuksen eettisyys on koko tutkimuksen perusta. Tutkimuksen eettisyyteen kuuluu olennaisena osana tutkimuksen luotettavuuden varmistaminen. Eettisyyteen liittyy myös anonymiteetin takaaminen. Tutkimuksen kohteen ollessa

sellainen, jota on vähän tutkittu ja siihen liittyy mahdollisesti geopoliittisen tilanteenkin vuoksi arkuutta vastata, on monimenetelmäinen tapaustutkimus haastattelun ja kyselyn keinoin ja anonymiteetti varmistaen, järkevin valinta. Anonymiteetti taataan käyttämällä keinoja, joilla luottamuksellista tietoa ei pääse ulkopuolisten käsiin ja kuvaamalla tutkimusaineiston käsittely osallistujille. Vilkan (2005, 35) mukaan osallistujalle on joka tilanteessa pystyttävä takaamaan anonymiteetti. Se, ettei tutkija pysty luotettavasti turvaamaan tutkimukseen osallistuvien anonymiteettia, onkin usein tutkimukseen osallistujien suurin pelko. Tutkimusaineiston kohdalla on ehdottomasti turvattava myös se, ettei aineisto joudu vääriin käsiin.

Tässä tutkimuksessa tutkimusaineistoa käsitellään niin, että anonymiteetti säilyy. Osallistuville organisaatioille arvotaan haastattelua varten yksilöivä numerokoodi, jolla myös haastattelun litteroinnissa saadut tiedot tallennetaan tutkijan käytössä olevalle erilliselle, ei internettiin yhteydessä olevalle koneelle. Samoin kyselytutkimuksen osalta vain yksilöivä koodi näkyy kyselytutkimuksen lomakkeen ylälaidassa. Haastattelut nauhoitetaan käyttäen erillistä sanelinta. Haastateltavien tiedot tallennetaan myös yksilöivää numerokoodia käyttäen ulkoiselle kovalevylle, jota säilytetään vain tutkijan tiedossa olevan numerokoodin takana olevassa lukitussa kodin turvalokerossa.

Nauhoitteet ja litteroitu aineisto sekä kyselytutkimuksen tulokset lähtökohtaisesti tuhotaan kokonaan tutkimuksen valmistuttua. Tutkimuksen osalta ei ole löytynyt syytä säilyttää aineistoa, mutta mikäli sellainen syy tulee esille, siihen pyydetään lupa tähän tutkimukseen osallistuvilta yrityksiltä sopien uudesta säilytysajasta. Tutkimuksen aineisto on lähtökohtaisesti tutkimuksen päätyttyä asianmukaisesti hävitettävä, anonymisoitava tai arkistoitava. Jos kuitenkin tutkimusaineistoa täytyy arkistoida, tulee arkistoinnin tarve harkita tarkasti. (Tietosuojavaltuutetun toimisto 2023.)

Triangulaatio on hyvä keino lisätä tutkimuksen luotettavuutta. Triangulaatiolla tarkoitetaan tietolähteiden yhdistämistä, kuten esimerkiksi erilaisten menetelmien tai teorioiden yhdistelyä. Näin saadaan tutkimukseen moninäkökulmaisuutta. Kvantitatiivisen ja kvalitatiivisen tutkimusotteen samanaikainen käyttö on vähäistä, ottaen huomioon mitä etuja se tuo. Menetelmätriangulaatio on toki aikaa ja resursseja vaativa tapa tehdä tutkimusta, mutta se laajentaa ja

syventää tutkimuskohteesta ja tutkimuksesta saatavaa tietoa. Yleisesti triangulaatio jaetaan neljään tyyppiin, jotka ovat: aineistotriangulaatio, tutkijatriangulaatio, teoriatriangulaatio sekä menetelmätriangulaatio. (Tuomi ym. 2004.)

Yhtenä luotettavuutta lisäävänä toimena on myös loppukeskustelujen toteutus. Yhteisessä loppukeskustelussa osallistujien kanssa nostetaan esille sellaisia asioita ja kulmia, jotka vaativat vielä lisätarkastelua ja käydään läpi tutkimuksen tulokset keskustellen. Keskustelu ei kuitenkaan ole ainoastaan tutkimuksen luotettavuuden lisäämisen väline, vaan keskustelun on tarkoitus tuottaa osallistujilleen mahdollisia uusia ajatuksia arjen käytäntöihin tai mahdollisuus jakaa omaa osaamista muiden osallistujien hyödyksi. On erittäin tärkeää, että myös loppukeskusteluissa varmistetaan osallistujien kesken tutkimusten tuloksien osalta anonymiteetti. Osallistujat eivät saa missään olosuhteissa tutkijan toimesta saada selville, mitä kukakin organisaatio on aiemmin vastannut kyselyyn tai kertonut haastattelussa. Loppukeskustelun nauhoittaminen ei ole tarpeen, vaan tutkija poimii keskustelusta vain ne havainnot, joilla voisi olla merkitystä tutkimuksen luotettavuuden kannalta. Loppukeskustelun valmistelu tehdään yhteistyössä osallistuvien yritysten kanssa, jolloin voidaan varmistaa, että se palvelee sekä tutkimusta että osallistuvien yritysten toiveita. On myös syytä muistaa, että luotettavuuteen vaikuttavat myös tallennusten laatu, litteroinnin tasaisuus ja luokittelun säännönmukaisuus (Hirsjärvi ym. 2008, 185).

2.7 Tutkimushypoteesit

Hypoteesi tarkoittaa tutkimuksessa ehdotusta tutkimuksen tuloksista. Tutkimuksessa testataan ja todennetaan, pitävätkö hypoteesit paikkaansa. Hypoteesit usein syntyvät, kun tutkija muotoilee ongelmanasettelua ja tutkimuskysymyksiä ja pohtii aineiston analyysin toteutusta ja tuloksia. Hypoteesit kertovat prosessin oletetuista päätöksistä. Hypoteesin käsitettä käytetään erityisesti määrällisessä tutkimuksessa, mutta laadullisen tutkimuksen ”oletus” tarkoittaa samaa. (Trochim 2006.)

Teoreettisen viitekehyksen kautta ja tutkijan oman tietopohjan yhdistelmänä syntyi joitakin tutkimushypoteeseja, eli oletuksia työn lopputuloksista.

Tutkimushypoteesi 1. Huoltovarmuuskriittisyys vaikuttaa vahvasti kyberturvallisuuden toteutumiseen alihankintaketjuissa. Perusteluna tälle hypoteesille

oli se, että kriittisille organisaatioille on paljon enemmän tukea ja apua saatavissa kyberturvallisuusasioissa kuin muissa yrityksissä. Usein huoltovarmuuskriittisillä yrityksillä on myös osaamista omasta takaa huolehtia kyberturvallisuusasioista.

Tutkimushypoteesi 2. Johdon tuki on erittäin merkittävässä asemassa kyberturvallisuuden toteutumista alihankintaketjuissa arvioitaessa. Tämä hypoteesi perustui teoriapohjaan ja tutkijan omiin huomioihin keskusteluista eri organisaatioiden johdon ja hallituksen jäsenten kanssa.

Tutkimushypoteesi 3. Organisaation kyberosaajilla on merkittävä rooli kyberturvallisuuden toteutumisessa alihankintaketjuissa. Hypoteesin perustelut ovat samat kuin toisessa tutkimushypoteesissa.

3 KYBERTURVALLISUUDEN MÄÄRITTELY

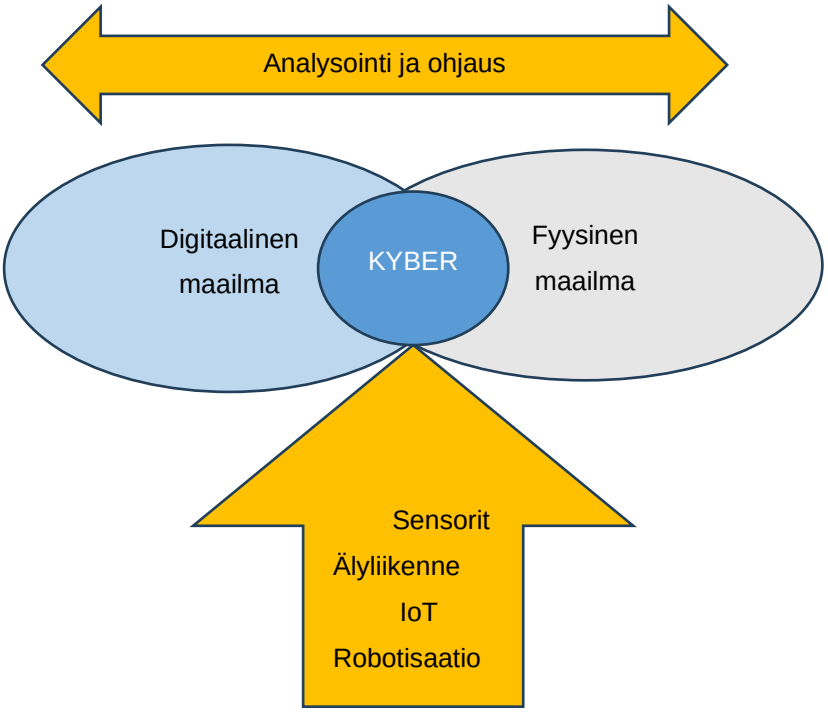
3.1 Kyberturvallisuus käsitteenä

Kyberturvallisuuden uhkakuvat ovat uutisissa jatkuvasti kärjistyneen geopoliittisen tilanteen vuoksi. Kyberturvallisuus oli vielä joitakin vuosia sitten valtaosalle kansalaisia lähes tuntematon käsite, mutta nyt sen ollessa jatkuvasti otsikoissa ja puheissa, siitä on tullut vakiintuneempi ja arkikäytössä oleva sana. Kyber-etuliitteen historia on aina 1940-luvulta peräisin, jolloin sitä käytti ensimmäisenä Nober Wiener teoksessa Cybernetics: Or Control and communication in the Animal and the Machine (1948). Teoksessaan Wiener totesi, että ihmisen rooli koneiden hallinnassa oli iso ja nimesi uuden tienhaaran kyberetiikaksi kreikan kielen sanan kybernētēs mukaan. Sana tarkoittaa ohjaamista, opastamista ja hallitsemista (Sanastokeskus, 2018). Vuosien saatossa kyberille on pyritty löytämään muita samaa tarkoittavia sanoja, mutta kyber on pitänyt pintansa sitkeästi.

Järvisen (2018) mukaan se tarkoittaa yhteiskunnan arkipäiväisten järjestelmien suojaamista ja kuinka niiden toiminta turvataan. Voidaan myös määritellä, että kyberturvallisuus kuvaa tavoitetilaa, jossa kybertoimintaympäristö on luotettava ja toiminta siellä on turvattua (Turvallisuuskomitea 2018). Kyberturvallisuuden termi tuli Suomeen vuonna 2011, kun valtioneuvosto päätti laittaa

käyntiin kansallisen kyberturvallisuusstrategian laatimisen. Tämä on havaintojen mukaan ensimmäinen kerta, kun kyberturvallisuus sanaa käytettiin Suomessa tässä merkityksessä. (Järvinen 2018, 13.)

Kyberin määritelmää voidaan Kasvin (2016) mukaan ajatella myös digitaalisen ja fyysisen maailman yhtymäkohtana.



Kuva 4. Kyber on bittien ja atomien vuorovaikutusta (Kasvi 2016)

Kuvassa olevat sensorit, älyliikenne, IoT, robotisaatio ja automaatio ovat kaikki herkkiä kyberhäiriöille. Myös niiden kyberturvallisuudesta on huolehdittava. Suomen Turvallisuuskomitea linjasi termin määrityksen Kyberturvallisuusstrategiassa vuonna 2013 näin:

> ”Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoiminta ympäristöön voidaan luottaa ja jossa sen toiminta turvataan.” (Turvallisuuskomitea, 2013).

Kyberturvallisuuden sanastossa Turvallisuuskomitea (2018) täydensi kyberturvallisuuden määritelmää ja toi vertailukohdaksi tietoturvan. Kyseisessä sanastossa tietoturva nähdään tiedon saatavuuden, eheyden ja luottamuksellisuuden terminä, kyberturvallisuus painottuu digitaalisen ja verkottuneen yhteiskunnan ja organisaation turvallisuuteen. Kyberturvallisuus voidaan myös

nähdä toimenpiteinä, joilla suojaudutaan kyberhyökkäyksiä vastaan ja toteutetaan tarvittavat vastatoimenpiteet (Lehto ym. 2015, 8).

Yhdysvaltain kansallinen standardien ja teknologian instituutti (NIST) linjaa termin sanakirjassaan tarkoittamaan kykyä puolustaa kyberulottuvuudessa olevia resursseja kyberhyökkäyksiltä (NIST 2020). Suomessa käsitteet ”digiturva”, ”kyberturvallisuus” ja ”tietoturvallisuus” eivät ole täysin vakiintuneita. Digitaalinen turvallisuus ja kyberturvallisuus ajatellaan usein synonyymeina. Ruotsissa käytetään myös digitaalinen turvallisuus -termiä, mutta muualla maailmassa tämän termin käyttäminen on vähäistä. Toisaalta eri maissa käytettävät kyberturvallisuuden määritelmät eivät poikkea toisistaan merkittävästi. (Valtiovarainministeriö 2020.) Käsitteiden epämääräisyys voi aiheuttaa myös käytännön toimenpiteiden vaikeutumista ja sitoutumista kyberturvallisuuden kehittämiseen. Kaikista oleellisinta on kuitenkin ymmärtää fyysisen ja digitaalisen maailman kietoutuminen toisiinsa. (Lehto ym. 2017.)

Tutkijan oma näkemys on, että kyberturvallisuus koostuu toimenpiteistä, joilla kyberympäristön järjestelmiä, prosesseja ja toimijoita voidaan turvata. Voidaan myös yleisesti sanoa, että kyberturvallisuus on osa kokonaisturvallisuutta. Se käsittää tietoturvallisuuden ja jatkuvuuden hallinnan sekä varautumisen. Vaikka kyberturvallisuuden määritelmät eroavatkin toisistaan, on niissä löydettävissä selkeä yhteneväisyys. Kyberturvallisuuden tarkoitus on kuitenkin lopulta luotettavan, tietoturvallisen ja häiriöttömän yhteiskunnan toiminnan turvaaminen.

3.2 Suomen kyberturvallisuusstrategia ja kansainvälinen vertailu

Suomessa kyberturvallisuuden kehittäminen on ollut määrätietoista mutta myös hajautunutta. Suomen ensimmäinen kyberturvallisuusstrategia laadittiin vuonna 2013 ja viimeisin 2019. Vuonna 2019 laaditussa kyberturvallisuusstrategiassa asetetaan kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi sekä elintärkeiden toimintojen turvaamiseksi. (Turvallisuuskomitea 2019, 4.) Kansallisen kyberturvallisuuden kehittämisen linjauksiin on otettu jo aikanaan Sanna Marinin hallitusohjelmassa kantaa, joten tuki kyberturvallisuuden kehittämiselle on tullut jo hallitustasolta.

Suomen kyberturvallisuuden kehittäminen perustuu ohjelmaan, jossa vuosittain arvioidaan toimenpiteitä ja päivitetään niitä. Yksi keskeisimmistä kehittämistä tukevista ohjelmista on Haukka-ohjelma, jossa kehitetään julkisen hallinnon digitaalisen turvallisuuden palveluita (Valtiovarainministeriö 2020). Lisäksi toisena tärkeänä kehitysohjelmana on Titukri, eli raportti lainsäädännön muutostarpeista ja muista toimenpiteistä, joilla tietoturvaa ja tietosuojaa voidaan parantaa yhteiskunnan kriittisillä toimialoilla (Liikenne- ja viestintäministeriö 2021). Digitaalinen turvallisuus 2030 on ohjelma, jonka tehtävänä on yhteiskunnan digitaalisen infrastruktuurin ja sen palvelujen häiriönsiedon ja kyberturvallisuuden kehittäminen (Huoltovarmuuskeskus 2021). Haasteena Suomen kyberturvallisuuden johtamisessa on hajautuminen. Kyberympäristömme suojaaminen on jakaantunut monille eri hallinnonaloille. Kuitenkin kyberuhkiin reagoiminen vaatii yhteistyötä, sillä kybertoimintaympäristön turvallisuutta vaarantava tapahtuma voi olla tietoturvauhka, rikos tai peräti maanpuolustusta vaarantava tapahtuma, jolla on vaikutuksia myös ulko- ja turvallisuuspolitiikkaan (Soikkeli 2023).

Kansainvälisesti tarkasteltuna jo yli 80 valtiolla on kyberturvallisuusstrategia. Joillakin mailla strategia on vasta ensimmäinen ja jotkut valmistelevat jo kolmatta tai neljättä strategiaansa (CCDCOE 2016). Naapurimaistamme Ruotsin ja Norjan viimeisimmät kyberturvallisuusstrategiat ovat vuodelta 2017 ja 2019. Venäjän kyberturvallisuusstrategia on vuodelta 2011, tosin sitä on päivitetty Naton kyberpuolustuksen osaamiskeskuksen (CCDCOE) sivujen mukaan runsaasti erilaisin asetuksin ja lisäselvityksin lähes joka vuosi.

KPMG toteutti digitaalisen turvallisuuden vertailun vuonna 2020. Vertailussa kerättiin tietoa osallistuvista maista niin julkisista dokumenteista kuin kyselyjen avulla. Kysymykset laadittiin KPMG:n ja Valtiovarainministeriön yhteistyönä. Digitaalisella turvallisuudella tarkoitettiin tässä tutkimuksessa riskienhallintaa, jatkuvuudenhallintaa sekä varautumista. Mukaan kutsutut maat olivat: Alankomaat, Australia, Iso-Britannia, Israel, Ruotsi, Saksa, Venäjä ja Viro. Vertailun yksi huomioista oli digitaalisen turvallisuuden terminologian kirjavuus. Myöskään Suomessa digitaalinen turvallisuus, kyberturvallisuus tai tietoturvallisuus eivät ole aukottomasti kaikille samaa tarkoittavia asioita. Lainsäädäntö oli verrokkimaissa tutkimuksen mukaan vaihtelevaa, mutta EU:n laajuiset yhteiset

asetukset ja direktiivit, kuten tietosuoja-asetus (GDPR) ja tietoverkkodirektiivi (NIS) ovat tuoneet käytänteisiin yhtenäisyyttä (Valtiovarainministeriö 2020.)

Palosen (2019) pro gradu -työssä tarkasteltiin kyberturvallisuuden kärkimaiden Viron, Alankomaiden ja Israelin kyberturvallisuuden johtamista ja etsittiin niitä tekijöitä, joista voisi olla apua Suomen kansallisen kyberturvallisuuden kehittämiseen. Palonen oli nostanut edellä mainitut maat tarkasteluun käyttäen International Telecommunication Unionin (ITU) Global Cybersecurity Indexiä (GCI) sekä ABI Researchin kyberturvallisuusindeksiä. Viro, Alankomaat ja Israel olivat vuoden 2017 indeksin mukaan korkeammalla sijoituksissa kuin Suomi. Palosen tutkimus nosti esille useita kehityskohteita kansallisen kyberturvallisuuden kehittämiseen. Keskeisimpinä havaintoina tutkimuksessa nousi esille selkeän kansallisen kyberturvallisuuden johtamisrakenteen luominen ja nykyisten organisaatiorakenteiden yksinkertaistaminen ripeämmän päätöksenteon ja tiedonkulun saavuttamiseksi. Myös riittävien kyberturvallisuuden resurssien määrittely nousi esille. Muita huomioita olivat: tilannetietoa keräävän keskuksen perustaminen, kyberturvallisuuskeskuksen toimivaltuuksien laajentaminen ja laajemman joukon osallistuttaminen kyberturvallisuuden strategiseen johtamiseen. Viimeisinä kohtina tutkimus nosti esille ylipäätään kyberturvallisuuden tietoisuustason nostamisen, harjoittelun ja koulutuksen lisätarpeen.

Kirjavat lainsäädännöt ja termien vakiintumattomuus aiheuttavat EU- tasoiselle yhteistyölle haastetta. Kuitenkin EU:ssa halutaan tehdä yhteistyötä tietoturvallisuuden, tietosuojan ja kyberturvallisuuden saralla ja Suomi haluaa olla siinä työssä uusimman kyberturvallisuustrategian mukaan aktiivinen toimija.

3.3 Kyberturvallisuus huoltovarmuuskriittisissä organisaatioissa

Huoltovarmuudella tarkoitetaan varautumista kriiseihin ja häiriötilanteisiin sekä jatkuvuudenhallintaa poikkeusoloissa (Huoltovarmuuskeskus 2023). Elintärkeiden toimintojen turvaaminen on yhteiskunnan toimivuuden kannalta kriittistä, ihmisten turvallisen arjen takaamiseksi. Suomessa huoltovarmuustyöhön osallistuu niin julkinen, yksityinen kun kolmas sektori ja se koskee kriittistä tuotantoa, palveluja sekä infrastruktuuripalvelujen turvaamista. Huoltovarmuustyössä on huomioitava lisäksi kohdemaan ilmasto, sijainti, kuljetusetäisyydet-

ja mahdollisuudet sekä muu infrastruktuuri. Huoltovarmuuteen vaikuttaa myös moni muu asia, kuten teknologian kehitys, globalisaatio sekä erilaiset liiketoimintarakenteiden muutokset. Samoin väestön terveydellä ja mahdollisilla luonnonkatastrofaaleilla on merkitystä. (Huoltovarmuuskeskus 2023.)

Huoltovarmuuskriittiseksi katsotaan organisaatio, joka on turvaamassa yllä olevia toimintoja. Moni yritys osallistuu sopimuskumppanina tai alihankkijan roolissa kuitenkin huoltovarmuuskriittisten toimijoiden toimintaan merkittävästi. Huoltovarmuustoiminta on jaettu seitsemään eri sektoriin, joita ovat: energiahuolto, elintarvikehuolto, finanssiala, logistiikka, teollisuus, terveydenhuolto, sekä tietoyhteiskunta. Huoltovarmuuskeskus järjestää poolitoimintaa, missä jaetaan tietoa ja opastetaan niin tietoturvan, jatkuvuuden, kyberturvallisuuden kun tietosuojankin asioissa. Ennakoinnin merkitys on kasvanut, joten kaikille toimialoille on tehty yhteiset jatkuvuuden turvaavat ohjeet. Huoltovarmuuskriittisillä organisaatioilla on pääsy HVO Extranet -portaaliin, joka tarjoaa organisaatioille varautumiseen ja jatkuvuudenhallintaan ohjeita. Lisäksi portaali sisältää tietoa ajankohtaisista tapahtumista ja muista asioista. Portaalin yhtenä tarkoituksena on myös yritys- ja henkilötietokannan avulla pitää huoltovarmuuskriittisten organisaatioiden vastuuhenkilöiden tietoja yllä. (Huoltovarmuuskeskus 2023.)

Huoltovarmuuskriittisten organisaatioiden erilaisten yhteistyöpoolien ja heihin kohdistuvan valvonnan ja raportointivelvoitteiden vuoksi voisi helposti olettaa, että huoltovarmuuskriittiset organisaatiot ovat keskimäärin paremmin tietoisia kyberturvallisuudestaan. Tämä onkin yksi tutkimuksen hypoteeseista.

3.4 Politiikat, viitekehykset ja standardit kyberturvallisuuden tason määrittelyssä

Kyberturvallisuuden määrittämiseen, yhteismitallistamiseen ja kehittämiseen on tarjolla erilaisia viitekehyksiä ja standardeja. Tässä työssä esittelen niistä suomalaisissa organisaatioissa yleisimpiä ja tunnetuimpia käytössä olevia. Usein yrityksessä on jo ennen viitekehyksien tai sertifiointien toteuttamista tehty kyberturvallisuusstrategia ja politiikka. Strategia määrittelee keskeiset isot strategiset toimintalinjat ja tavoitteet. Kyberturvallisuuspolitiikka tuo ne

konkreettisemmalle tasolle, toimintalinjoiksi. Kyberturvallisuupolitiikasta asioiden pitäisi tarvittavien tehtävien ja toimenpiteiden siirtyä sujuvasti osaksi yrityksen toimintasuunnitelmia. Yrityksen johdon ja hallituksen vastuu myös kyberturvallisuuden saralla on laaja, siksi hallituksen kannattaa myös vaatia kyberturvallisuusstrategian ja politiikan käsittelyä hallituksessa (Kyberturvallisuuskeskus 2023).

Yksi tunnetuimmista ja paljon organisaatioiden tietoturvallisuuden tason määrittelyssä käytetty, on ISO 27001 -standardi. Standardin laatijat ovat ISO (international Organization for Standardization) ja IEC (International Electrotechnical Comission) muodostama organisaatio. ISO 27000 -standardiperhe, joka sisältää useita standardeja. Standardin osa 27000 on yleiskatsaus standardiin, jossa myös sanasto määritellään. Tärkein kyberturvallisuuteen liittyvä alastandardi on ISO 27001, sillä se kuvaa vaatimukset informaatioteknologioille, turvallisuustekniikoille ja tietoturvallisuuden hallintajärjestelmille. ISO 27002 sisältää menettelyohjeita tietoturvallisuuteen. Standardin osassa ISO 27003 annetaan ohjeita hallintajärjestelmän toteuttamiselle ja osassa ISO 27004 ohjeistetaan hallintamenetelmien toiminnan mittaamiseen. Viimeisin, eli ISO 27005 määrittää tietoturvariskien hallinnan vaatimuksia. ISO 27001 sisältää 114 kpl hyviä hallintakeinoja, joita organisaatio voi käyttää arvioidessaan omaa tietoturvallisuuden toteutumisen tasoaan. Lisäksi ISO 27001 auttaa organisaatioita tietoturvan hallinnassa ja tietomurtoriskien vähentämisessä. Sertifikaatilla organisaatio haluaa myös usein viestittää, että se on luotettava kumppani ja käsittelee organisaation hallussa olevaa dataa asiaankuuluvasti. (SFS 2022.)

KATAKRI on hyvä auditointityökalu arvioitaessa yrityksen turvallisuusjärjestelyjä ja viranomaiset käyttävätkin työkalua ahkerasti. Sitä voidaan toki käyttää myös tavallisten yritysten turvallisuustyössä. Tarkoituksena on varmistaa, että organisaatiolla on riittävät turvallisuusjärjestelyt, jotta viranomaisten salassa pidettävä tieto ei paljastu. KATAKRI soveltuu myös kansainvälisiin hankkeisiin käytettäväksi, sillä siihen on koottu kansallisiin ja kansainvälisiin velvoitteisiin liittyvät vähimmäisvaatimukset. Vähimmäisvaatimukset perustuvat lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Kansallisesta lainsäädännöstä ovat laki julkisen hallinnon tiedonhallinnosta (906/2019)

ja valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Kansainvälisiin lähteisiin kuuluu EU:n turvallisuussäännöt (2013/488/EU), jossa on määritelty EU:n turvallisuusluokitellun tiedon suojaamista koskevat perusperiaatteet ja vähimmäisvaatimukset. Suomen Ulkoministeriön Kansallinen turvallisuusviranomainen (National Security Authority) vastaa KATAKRI:sta. KATAKRI:sta on julkaistu neljä versiota, joista viimeisin vuonna 2020, joten julkaisutahtia ei voida sanoa kovinkaan nopeaksi. Ensimmäinen versio laadittiin 2009 hallituksen turvallisuusohjelman osana, jonka jälkeen vastuu siirtyi sisäministeriölle. Toinen versio KATAKRI:sta julkaistiin vuonna 2011. Kolmas versio näki päivänvalon 2015 Kansallisen turvallisuusviranomaisen johtamana. Neljättä versiota saatiin odottaa 5 vuotta ja se valmistui 2020 (Kansallinen turvallisuusviranomainen 2020). Uusin versio sisältää parannuksia rakenteeseen ja terminologiaan Kyberturvallisuuskeskus myöntää yrityksille pätevyyden suorittaa KATAKRI arviointeja yrityksille. Tämän opinnäytetyön kirjoitushetkellä Suomessa on kaksi organisaatiota, joilla on pätevyys suorittaa KATAKRI 2020 sertifiointi. Ne ovat KPMG IT Sertifiointi Oy, joka sai pätevyyden vuonna 2022 ja Nixu Certification Oy, jolla pätevyys on ollut jo vuodesta 2021 (Kyberturvallisuuskeskus 2022). Katakrista löytyy kolme eri osa-aluetta, jotka ovat Turvallisuusjohtamisen osa-alue (T), Fyysisen turvallisuuden osa-alue (F) sekä teknistä tietoturvallisuutta koskeva alue (I). Kuhunkin kolmesta osa-alueesta on kuvattu vaatimuksia, jotka mahdollistavat erilaisia toteutustapoja, sekä toteutusesimerkit auttavat ymmärtämään, miten useimmissa ympäristöissä saavutetaan hyväksyttävä suojausten vähimmäistaso (Ulkoministeriö 2020).

VAHTI-ohje on varsinkin julkisen puolen toimijoille tuttu työkalu tietoturvallisuuden tason määrittelyyn ja ohjeiksi. Työkalua voidaan käyttää hyvin myös yksityisellä puolella. VAHTI-ohjeen on tuottanut julkisen hallinnon digitaalisen turvallisuuden johtoryhmä. VAHTI-ohje sisältää paljon tietoturvaan ja tietosuojaan liittyviä ohjeita. Sisältö koostuu ohjeista liittyen auditointiin, tiloihin, salauksiin, henkilöstöön ja järjestelmäkehitykseen, sekä jatkuvuuteen. (Valtiovarainministeriö 2020.)

NCWF-viitekehys (NICE Cybersecurity Workforce Framework) on vähemmän Suomessa tunnettu, tosin sillä on myös erilainen tarkoitus kuin KATAKRI:lla ja ISO27001:lla. NCWF kehitettiin alun perin osana Yhdysvaltain standardi- ja

teknologian instituutin (NIST) kansallista kyberturvallisuuden koulutusohjelmaa, jonka nimi oli National Initiative for Cyber Education (NICE). Hanketta johti National Institute of Standars and Technology (NIST) ja se oli hyvin laaja, koostuen valtion ja yritysten yhteisistä edustajista. Sillä oli myös erittäin kunnianhimoinen tavoite. Tarkoituksena oli kehittää maailmanlaajuinen yhteistyöverkosto ja uusi ekosysteemi kyberturvallisuuden osaamisen kehittämiseen. Hanke tuotti NCWF-viitekehyksen, jolla pyrittiin vastaamaan organisaatioiden kyberturvallisuuden tarpeisiin yhtenäistää sanastoa ja tehtävärooleja. NCWF-viitekehys koostuu kategorioista, jotka jakaantuvat erityisalueisiin. Erityisalueet jakaantuvat työrooleihin, jonka sisällä on tehtäviä, jotka taas vaativat taitoja, kykyjä ja tietoa. (NIST 2023.)

IISP Skills Framework-viitekehys edustaa samantyyppistä viitekehystä kuin NCWF-viitekehys. Se on englantilaisen Institute of Information Security Professionalsin (IISP) vuonna 2007 tuottama kehys, jolla pyritään kuvaamaan kyberturvallisuuden osaamista kompetenssien ja vaatimusten kautta. Tietoturvallisuuden toimialueet jaetaan kategorioihin ja niihin liittyviin osaamisalueisiin. IISP:tä löytyy myös osaamisen viitekehys (Knowledge framework) sekä tehtäviin ja rooleihin liittyvä viitekehys (IIS Roles framework). (IISP 2010.)

NIST Cybersecurity Framework (NIST CSF) antaa ohjeita organisaatioille kyberturvallisuusriskien vähentämiseksi ja tarjoaa hyvän pohjan kyberturvallisuuden toteuttamiselle. Viitekehys on vaihtoehtoinen tapa kehittää kyberturvaa verrattuna ISO 27001:een. Viitekehys auttaa ymmärtämään, priorisoimaan ja kommunikoimaan kyberturvallisuuden tehtäviä. Viitekehys ei kuitenkaan tarkasti määrittele, miten tulokset pitäisi saavuttaa, eikä sitä vasten myöskään sertifioiduta. (NIST 2023.)

Kyberturvallisuuskeskuksen kybermittari on myös hyvä apuväline organisaation kyberturvallisuuden tason ymmärtämiseen, kehittämiseen ja toteutumisen seurantaan (Kyberturvallisuuskeskus 2022). Kybermittari on laajasti tunnettu ja yhä enemmän organisaatioiden käyttämä työkalu oman kyberturvallisuuden kypsyystason arviointiin. Esittelen kybermittarin tässä tutkimuksessa tarkemmin muihin viitekehyksiin ja työkaluihin nähden sen tunnettuuden vuoksi.

Kybermittari kertoo saavutetun kypsyystason ja esittää seuraavalle tasolle vaadittavat kehitysalueet. Mittarin käyttöä tukee mittauksista saatavat vertailukelpoiset tulokset. Mittarin avulla saa myös vertailukohtaa, missä oma taso vertautuu toimialan keskiarvoon. Kybermittarin kehittämisessä on ollut mukana Kyberturvallisuuskeskuksen lisäksi Huoltovarmuuskeskus ja muita kriittisen infrastruktuurin organisaatioita, yrityksiä, asiantuntijoita sekä viranomaisia. Pohjana kybermittarille on toiminut edellä esitelty NIST Cybersecurity Framework sekä C2M2 (Cybersecurity Capability Maturity Model. (Kyberturvallisuuskeskus 2022.) Kybermittarin avulla saa hyviä vinkkejä myös kyberturvallisuuden johtamiseen, kehityskohteiden tunnistamiseen, sekä tavoitteiden asettamiseen oikeisiin kohteisiin ja oikealle tasolle. Kybermittariin perustuvia arviointeja toteuttavat Kyberturvallisuuskeskuksen mukaan 2NS – Second Nature Security Oy, Accenture Oy, Atea Oy Finland Oy, Cinia Oy, Deloitte Finland Oy, Digia Oy, Fraktal Oy, Insta Group Oyj, KPMG Oy Ab sekä Netum Oy. Kyberturvallisuuskeskus järjestää myös kybermittariin liittyviä koulutuksia, niin organisaatioille, kuin palveluntarjoajillekin. (Kyberturvallisuuskeskus 2022.)

Kybermittarissa on 11 eri osiota, jotka ovat;

Kriittisten palvelujen suojaaminen (CRITICAL)
Omaisuuden, muutosten ja konfiguraation hallinta (ASSET)
Uhkien ja haavoittuvuuksien hallinta (THREAT)
Riskienhallinta (RISK)
Identiteetin- ja pääsynhallinta (ACCESS)
Tilannekuva (SITUATION)
Tapahtumien ja häiriöiden hallinta, toiminnan jatkuvuus (RESPONSE)
Kumppaniverkoston riskien hallinta (THIRDPARTY)
Henkilöstön johtaminen ja kehittäminen (WORKFORCE)
Kyberturvallisuusarkkitehtuuri (ARCHITECTUORE)
Kyberturvallisuuden hallinta (PROGRAM)

Tämän tutkimuksen kannalta osio, joka käsittelee kumppaniverkoston riskien hallintaa (THIRDPARTY), on mielenkiintoisin. Osio koostuu kolmesta kokonai-

suudesta, joista ensimmäinen on kumppaniverkoston tunnistaminen ja priorisointi. Toisena on kumppaniverkostoon liittyvien riskien hallinta ja kolmantena Yleisiä hallintatoimia.

Ensimmäinen kokonaisuus, eli kumppaniverkoston tunnistaminen ja priorisointi pitää sisällään nimensä mukaisesti tunnistamiseen liittyviä kysymyksiä. Osioon sisältyvissä kysymyksissä selvitetään, ovatko kumppaniverkoston toimijat priorisoitu tärkeyden ja vaikuttavuuden mukaan ja onko priorisointi aikataulutettu ja tehdäänkö sitä säännöllisesti. Toinen kokonaisuus antaa ohjeita kumppaniverkoston riskien hallintaan. Tämän kokonaisuuden kysymyksien avulla arvioidaan toimittajien ja muiden kumppaniverkoston organisaatioiden kyberturvallisuuden tasoa. Myös mahdollisten tuotteiden tai palvelujen kyberkyvykkyyksien tasoa arvioidaan. Suojatoimien arviointitarkastelu kuuluu myös tähän kokonaisuuteen, sekä verkoston kyberturvallisuusvaatimusten täyttökyky. Kolmas kokonaisuus, eli yleiset hallintatoimet, ottaa kantaa siihen, onko olemassa dokumentoituja ohjeistuksia kumppaniverkoston hallintaan ja ohjataanko sitä vaatimuksilla. Lisäksi osiossa selvitetään ovatko vastuut ja valta selkeitä kumppaniverkoston ohjaamisessa. Osio sisältää myös arvioinnin siitä, miten tämän vaikuttavuutta arvioidaan ja seurataan. (Kyberturvallisuuskeskus 2023.)

Viitekehyksiä ja standardeja on paljon ja niiden noudattaminen vaatii osaamista, aikaa ja rahaa, mutta toisaalta ne tuottavat määrämuotoista tietoa. Ne myös eroavat toisistaan päivitystahdin, sisällön ja vaativuuden osalta. Riippuen muun muassa toimialan luonteesta, lainsäädännöstä, viitekehysten ja standardien markkina-arvosta yritykselle, organisaation on tehtävä tietoinen ja harkittu päätös mitä se niistä näkee järkeväksi käyttää. Mikään politiikka, viitekehys tai standardi ei sinällään vielä täysin luotettavasti kerro, onko yrityksessä hoidettu tietoturva tai kyberturva hyvin, mutta ne antavat jo vahvan viestin asiasta.

3.5 Kyberturvallisuus ja riskienhallinta

Kyberturvallisuudesta huolehtiminen tarkoittaa tietojen saatavuudesta, eheydestä ja luottamuksellisuudesta huolehtimista. Organisaation on suojaudut-

tava pystyäkseen turvaamaan edellä mainittujen asioiden toteutuminen. Suojautuminen vaatii toimintojen suojaamista ja varautumista. Nämä taas vaativat riskienhallintaa. Digitaalisen turvallisuuden viitekehys koostuu Digi- ja väestötietoviraston (2021) mukaan viidestä eri osa-alueesta, joita ovat: johtaminen ja riskienhallinta, jatkuvuudenhallinta, tietoturvallisuus, tietosuoja ja kyberturvallisuus. Riskienhallinnassa on otettava myös uudet asiat huomioon. Esimerkiksi tekoäly on ollut viime vuosina huomion kohteena. Se tuokin mukanaan uusia mahdollisuuksia, mutta myös vastuita ja haasteita. Tekoälyyn liittyvien tietoturvariskien tunnistaminen ja hallinta on tärkeä asia, jotta sekä hyöty että turvallisuus toteutuvat. (Traficom 2021.)

Kyberturvallisuusyhtiö Nixun (2022) tutkimuksen mukaan päättäjät eivät näe riskienhallintaa kyberturvallisuuskyvykkyytenä. Toisena tutkimuksen huomiona oli toimitusketjujen kyberturvallisuuden liian vähäinen huomiointi. Tutkimus toteutettiin osallistuttamalla 180 yrityspäättäjää eri toimialoilta ja pyytämällä heitä arvioimaan oman organisaationsa kyberturvallisuuden nykytilaa. Huoltovarmuuskeskuksen (2023) tekemän toimialojen kyberkypsyyden selvitys vuodelta 2022 nosti esille samat huomiot. Tutkimuksen mukaan yrityksen riskienhallintaa ei useinkaan sisällä kyberriskejä. Huoltovarmuuskeskuksen tekemään tutkimukseen osallistui 12 toimialalta 121 toimijaa, joten otos oli kattava tässäkin tutkimuksessa.

Kyberturvallisuuden edistäminen tulisikin vahvasti kytkeä osaksi johtamista ja riskienhallintaa. Näin siitä tulee näkyvää ja ymmärrettävää. Riskienhallintaa tarkastellaan jo suomalaisten organisaatioiden hallituksissa totutusti, mutta kyberturvallisuuden osalta ollaan vasta suhteellisen uuden asian äärellä.

4 ALIHANKINTAKETJUJEN KYBERTURVALLISUUS

4.1 Alihankintaketjun määritelmä ja riskit

Alihankkija määritellään henkilöksi tai yhtiöksi, joka on sitoutunut tekemään määrätyn työn päähankkijan lukuun. Päähankkija on sopimusvastuuosapuoli tilaajaan eli asiakkaaseen päin. Alihankintaketjuilla tarkoitetaan kaikkia niitä yrityksiä, joita varsinainen pääyhteistyökumppani eli sopimusosapuoli asiakkaan suuntaan, käyttää apunaan toimitusta tai palvelua toimitettaessa. Ky-

seessä voi olla yksittäinen toimitus tai jatkuvaluonteinen palvelu. Teknologiateollisuuden (2023) mukaan alihankintateollisuuden kokonaisvolyymi on Suomessa 2,6 miljardia euroa ja se työllistää yli 16 000 henkilöä. Suurin osa alihankkijayrityksistä on pieniä tai keskisuuria perheyrityksiä. Alihankkijat toimivat eritavoin pääkumppanin kanssa, alihankkija voi olla järjestelmien toimittaja, sopimusvalmistaja, osavalmistaja tai vaikka kapasiteettialihankkija.

IT-toimialalla alihankkijoiden käyttö on hyvin yleistä, näin ollen kyberturvallisuuden toteutumista arvioitaessa sillä on merkittävä vaikutus. Organisaatiot ovat riippuvaisia toisistaan nykyaikaisessa yhteiskunnassa monilla tavoin, ja yritysten olisikin hyvä selvittää osana riskienhallintaa, mistä kaikesta yritys on riippuvainen ja ketä sen verkostoon kuuluu. IT-maailmassa ohjelmistot ja järjestelmät muodostavat pitkiä ketjuja, joiden eri toimijoista ja rooleista on tärkeää olla tietoinen.

Alihankintaketjuissa hyökkääjä voi hyökätä jonkin ketjun toimijan järjestelmiin ja levittää sinne vaikka haittaohjelman. Alihankintaketjussa haittaohjelma lähtee leviämään helpommin, kun hyökkääjä hyödyntää organisaation luottamusta yhteistyökumppaneihin ja uhrina onkin nopeasti laajempi joukko yrityksiä kuin vain alkuperäinen hyökkäyksen kohdeyritys. On erittäin tärkeää, että toimitusketjuhyökkäykset huomataan ripeästi, sillä vahinko voi laajentua suureksi nopeasti. Myöskään yritys, joka ei havainnoi riskejään huolellisesti, ei varmasti ole verkostossa luotettavan yhteistyökumppanin maineessa jatkossa. Tärkeintä kuitenkin on, tapahtuman havaitessa, olla nopea ja avoin tiedottamisessa, sillä voi paikata paljon.

Huoltovarmuuskeskuksen Digipooli julkaisi toimialojen kyberkypsyyden selvityksen 14.3.2023. Toimialojen kyberselvitys kertoi, että suomalaisten yritysten ja organisaatioiden kyberkyvykkyys on hyvällä perustasolla, mutta hajontaa eri toimialojen ja organisaatioiden välillä on havaittavissa. Yksi keskeisistä havainnoista liittyi kumppanihallintaan. Selvityksessä todetaan, että osallistuneet organisaatiot luottavat kumppaneihin kyberturvallisuuden hallinnan ja valvonnan osalta, eivätkä tee valvontatoimenpiteitä raportoinnin lisäksi. Yritykset usein siirtävät vastuun alihankintaketjuissa suorien kumppaneiden vastuulle. (Huoltovarmuuskeskus 2023.). Samassa Huoltovarmuuskeskuksen selvityk-

sessä todetaan että, kumppanit ja niiden alihankkijat voivat jopa laajentaa yrityksen verkkoa ja mikäli tällaiset riippuvuudet eivät ole tiedossa, on niiden aiheuttama potentiaalinen uhka merkittävä.

Alihankintaketjut voivat olla hyvin pitkiä, eikä välttämättä palvelusta tai asiasta vastaava henkilö edes tiedä, ketä kaikkia palvelun tarjoamiseen osallistuu. IT-toimittajalla voi olla sopimus konesalitoimittajan kanssa, konesalitoimittajalla voi olla sopimus asennustyötä toimittavan yrityksen kanssa ja siivotakin pitäisi vielä jonkun yrityksen edustajan. Myös yritysten lisääntynyt globaali hankinta aiheuttaa pitkiä toimitusketjuja, joissa osapuolten määrä kasvaa. Toimitusketjujen kyberturvallisuuteen liittyvässä tutkimuksessa (Creazza ym. 2022) tutkittiin toimitusketjun johtajien käsityksiä kybertoimitusketjun kyberturvallisuutta lisäävistä elementeistä. Tutkimuksen tuloksina oli selvästi nähtävissä, että toimitusketjujen kyberturvallisuuden avaintekijöinä on syytä nähdä ihmiset. Yritysten on pohdittava tarkoin inhimillisten tekijöiden merkityksellisyyttä riskien lähteenä. Tutkimuksessa nousee myös esille kyberturvallisuusstrategian tärkeys.

Alihankintaketjujen kyberturvallisuus on osa yrityksen kokonaisturvallisuutta. Organisaatioiden tulisikin panostaa alihankintaketjujen kyberturvallisuuden johtamiseen ei vain itsensä vuoksi, vaan myös koko toimitusketjun ja siihen osallistuvien muiden organisaatioiden turvallisuuden vuoksi. Myös Supo (2021), varoittaa toimitusketjuhyökkäyksistä, joissa käytetään hyväksi luottamussuhdetta. Yhteistyökumppanin verkkoon päästessään, yritetään pian luottamussuhteen avulla päästä kohti kohdeyrityksen verkkoa. Kyberturvallisuuden varmistaminen toimitusketjuissa on näin ollen erittäin tärkeää.

Tunnettu esimerkki historian siihen saakka suurimmista toimitusketjuhyökkäyksistä oli Kaseyan etähallintaohjelmiston haavoittuvuuden aiheuttama kaaos. Tunkeutujat käyttivät hyväkseen etäkäyttöohjelman nollapäivän haavoittuvuutta ja lisäsivät ohjelmistoon haitallista koodia. Vaikka Kaseya-palvelu irrotettiinkin verkosta, se ehti aiheuttaa mittavat vahingot, sillä Kaseyaa käyttivät organisaatiot, joilla oli laaja määrä asiakkaita itsellään, kymmenistä eri maista. FBI alkoi tutkia tapausta välittömästi. (Cybernews 2021.) Euroopassa

tästä kärsi muun muassa Cooper-niminen ruotsalainen päivittäistavarakauppa, kun sen kassajärjestelmä ei enää toiminut ja liikkeet oli suljettava (Bergström ym. 2021).

Toimitusketjuhyökkäykset voivat olla vaikutuksiltaan merkittäviä ja laajoja. Verkottuneessa yhteiskunnassa hyökkäyspinta-ala kasvaa. Tulevaisuudessa tullaan varmasti näkemään organisaatioiden tekevän entistä enemmän valintoja yhteistyökumppaneistaan ja toimittajistaan sen perusteella, miten niiden kyberturvallisuus on hoidettu.

4.2 Alihankintaketjujen kyberturvallisuuden lainsäädäntö ja ohjeistus

Alihankintaketjuihin liittyy niitä koskevia lakeja ja asetuksia sekä suosituksia ja ohjeita. Tässä luvussa tutustutaan niistä keskeisimpiin. Esitellyt lait ovat kyberturvallisuutta koskevia ja ne sisältävät kannanottoja myös toimitusketjujen riskien hallintaan ja liittyvät sitä kautta alihankintaketjujen kyberturvallisuuteen.

Alihankintaketjuja koskevasta lainsäädännöstä yksi tuoreimmista on vuoden 2023 alussa voimaan tullut DORA. DORA tulee sanoista Digital Operational Resilience Act. Sen tavoite on yhtenäistä digitaalista resilienssiä ja IT-riskienhallinnan vaatimuksia. DORA koskee mittavaa määrää Euroopan finanssialan toimijoista ja IT-palveluntarjoajista ja se on sitova lainsäädäntö, ei ohje tai suositus. Asetuksen soveltaminen alkaa tammikuussa 2025. DORA on yksi 14 regulaatioaloitteesta ja osa EU:n strategiaa. (EUR-Lex 2022.) Muita Euroopan digisäätelyä ohjaavia säädöksiä ovat digipalvelusäädös (Digital Services Act), datasäädös (Data Act) ja tekoälyasetus (AI Act). Nämä kaikki koskevat finanssiorganisaatiota, joten seurattavaa ja arvioitavaa riittää.

DORA-asetus tuo sitovia sääntöjä IT-riskienhallinnalle, raportoinnille, häiriösietokyvyn testaamiselle sekä kolmansien osapuolien riskienhallinnalle. DORA:n kolmansien osapuolten tarjoamiin palveluihin liittyvien riskien hallinta asettaa lukuisia velvoitteita organisaatioille. Rahoitusalan toimijoiden on muun muassa seurattava aktiivisesti riskejä, jotka liittyvät siihen, että ICT-palveluja toimittavat kolmannet osapuolet. Tähän kuuluu myös ilmoitusvelvollisuus kaikista ulkoistetuista toimista. Myös ulkoistamisen riskit on huomioitava ja toimit-

tava yhdenmukaisella tavalla IT-palvelujen ulkoistamisessa ja keskittämisessä. Sopimuksiin on huolehdittava kaikki palvelun seurantaan ja saatavuuteen liittyvät asiat, kuten palvelutasokuvaukset ja tietojen säilytys- ja käsittelypaikat. (EUR-Lex 2022.)

Joulukuussa 2022 voimaan tullut NIS2 on kyberturvallisuusdirektiivi, joka määrittää kyberturvallisuusriskien hallintatoimenpiteet, raportointivelvoitteet ja valvontatoimenpiteet. NIS1:een verrattuna direktiivin soveltamisalat ovat laajemmat. Vanhassa direktiivissä velvoitettiin ilmoittamaan poikkeuksista, mutta nyt direktiiviin on lisätty myös tietoturvakäytännöistä huolehtiminen. Jokaisen EU-maan tulee viedä säädökset lainsäädäntöön vuoden 2024 lokakuuhun mennessä. Julkisten toimijoiden lisäksi direktiiviä tulee noudattaa kriittisillä toimialoilla toimivien suurien ja keskisuurien yritysten. Kriittisiksi aloiksi katsotaan direktiivin mukaan esimerkiksi finanssi-, energia-, terveydenhuolto-, liikennesektori sekä digitaalinen infrastruktuuri. Direktiivin keskeisin asia on varmistaa kyberriskien hallintatoimenpiteet ja raportointivelvoitteista vastataan organisaatiossa johdossa saakka. Direktiivissä on velvoitteita siksi yritysten hallintoelimille. Suomessa tämä tarkoittanee yritysten hallituksia. Direktiivi myös edellyttää, että yritysten hallintoelimet osallistuvat kyberturvan koulutuksiin, jotta osaisivat tunnista kyberturvallisuusriskejä ja arvioida hallintatoimenpiteitä paremmin. Direktiiviin kuuluu myös vahvempi henkilökohtainen vastuu hallintoelimissä vaikuttavien henkilöiden osalta. (EUR-Lex 2022.)

Hallintatoimenpiteet tarkentuvat vielä, mutta siellä tulee olemaan myös toimitusketjujen turvallisuuden varmistaminen. Toimitusketjujen turvallisuuden varmistaminen tarkoittaa, että tunnistaa ja tuntee toimitusketjut, joten työ kannattaa aloittaa ajoissa. Lisäksi muita hallintatoimenpiteitä ovat tietojärjestelmien turvallisuutta koskevat politiikat, kyberhygieniakäytännöt, poikkeamien käsittely ja toiminnan jatkuvuuden ja kriisien hallinta. NIS2 vaatii organisaatiolta aktiivisia toimia. Se ei kuitenkaan pakota sertifioitumaan sinällään mihinkään. Vaihtoehtona voi olla oman tietoturvan hallintajärjestelmän päivitys ja huolehtiminen muutoin, että direktiiviä noudatetaan. (EUR-Lex 2023.)

Toimitusketjujen riskejä käsiteltäessä, kyberturvallisuuden osaajien keskuudessa hyvin tunnettu on C-SCRM (Cyber Supply Chain Risk Management) on prosessi, jossa tunnistetaan, arvioidaan ja lievennetään toimitusketjuriskejä (NIST 2017). Työn takana on Yhdysvaltain standardointi- ja teknologiainstituutti eli NIST. C-SCRM- työ käynnistyi 2008 ja on siitä asti jatkunut tähän päivään saakka.

NIST:n (nd) ”Software security in supply chains” julkaisu tuo hyvinkin konkreettisia ohjeita alihankintaketjun eri osapuolille (NIST n.d). Koko toimitusketjun on oltava hereillä ja huolehdittava, että ymmärrys käytettävistä ohjelmistoista on kaikilla tiedossa. EU- tasoisesti tästä löytyy ehdotus säädökseksi nimeltä Cyber Resilience Act (Fox 2022). Säädös ei kuitenkaan ole vielä lainvoimainen on herättänyt paljon keskustelua erityisesti avoimien lähdekoodien ohjelmistojen osalta.

4.3 Alihankintaketjujen kyberturvallisuutta koskevia tutkimuksia

Tutkimuksien haku toteutettiin kahdella eri hakuvälineellä, jotka olivat Google Scholar sekä IEEE Xplore. Google Scholar on Googlen tuottama maksuton hakupalvelu tieteellisille julkaisuille. IEEE Xplore on sähkö- ja tietotekniikan keskeinen tietokanta, josta löytyy aineistoa muu muassa yli 260 tekniikan alan johtavalta lehdeltä. Käytettävät hakupalvelut on valittu arvioiden niiden sopivuutta tarkastelemalla yleistasolla ja kokeilunomaisesti eri hakupalveluilla tehtyjen hakujen tuloksia.

Tarkemmin tarkasteluun nostettaville tutkimuksille ja julkaisuille asetettiin seuraavat sisäänottokriteerit;

1. Tutkimukseen liittyvien viittausten määrä >10
2. Hakutuloksissa sopivuudeltaan Google Scholarin 20 sopivimmaksi ehdotetun joukossa
3. Tutkimus on tehty vuoden 2020 jälkeen
4. Julkaisukieli: suomi tai englanti
5. Lähdeluettelo saatavilla, nimetty organisaatio tai henkilö
6. Aineisto on saatavissa maksuttomasti

Sisäänottokriteerejä käyttäen, kahdella eri hakuvälineellä tehty haku, neljän eri hakusanayhdistelmän avulla tuotti paljon tuloksia. Hakutulosten runsaan määrän vuoksi oli arvioitava tutkimuksia silmämääräisesti pelkän otsikon perusteella ja käytävä läpi vain kaikista hyödyllisimmiltä ja luotettavimmilta kuulostavien hakutulosten kautta saatujen tutkimusten sisältö. Luotettavuuden arvioinnissa käytettiin lisäksi tutkimuksessa esitettyjen väitteiden tai tulosten uskottavuutta ja perusteluja, sekä niihin liittyviä lähteitä.

Hyödyllisyyttä on myös arvioitu tutkimukseen liittyvien viittausten määrällä. Viittausten määrä on usein, ei kuitenkaan aina, osoitus siitä, että tutkimusta on luettu ja sitä pidetään luotettavana. Google Scholar löysi hyvin sopivimmat tutkimukset kärkeen, joten kriteerin 2 asetus jätettiin tiukaksi. Lisäksi vuoden 2020 jälkeen läpikäydyssä tutkimusmateriaalissa alkoi selvästi näkyä alihankintaketjujen kyberturvallisuuden riskitason huomattava nousu ja ketjujen monimutkaistuminen, joten hakuehto asetettiin siihen.

Sisäänottokriteerien avulla löydettyjen aineistojen sopivuutta tämän tutkimuksen tietolähteinä käytettäväksi olen arvioinut viisiportaisella asteikolla. Asteikossa 1–3 eivät ole tämän tutkimuksen kannalta järkeviä tarkasteltavia ja ne sivuutettiin, vaikka täyttivätkin sisäänottokriteerit. Asteikossa 3 on jo osittain hyödyllistä tietoa, 4 katsotaan hyödylliseksi ja 5 erittäin hyödylliseksi. Sopivaksi tätä tutkimusta varten katsottiin tutkimukset, joiden hyödyllisyys arvioitiin 3–5 tasolle. Suurimman osan sopiviksi arvioiduista tutkimuksista sijoittui tasolle 3. On kuitenkin huomattavaa, että mielenkiintoisia ja mahdollisesti hyödyllisiä tutkimuksia jäi paljon maksumuurin taakse. Sopiviksi katsotuista tutkimuksista löytyy hakutaulukon jälkeen kaksi nostoa. Ne ovat merkittyinä hakuvälineen ja hakusanan yhtymäkohdasta numerolla ja *-merkillä.

Enemmän julkaisuihin, konferenssimateriaaleihin ja kirjoihin keskittyvä haku IEEE Xplore-välineellä taas antoi runsaasti osumia julkaisuista kyberturvallisuuden alihankintaketjuihin liittyen. Silmämääräisesti hyödyllisyyttä arvioiden tässä tutkimuksessa tarkasteltiin niistä vain 10 julkaisua. Niistä ei kuitenkaan löytynyt mitään erityistä nostettavaa tähän tutkimukseen. Alla olevassa taulukossa on kuvattu tutkimusta varten tehtyä hakua tarkemmin. Tutkimuksien sisäänottokriteerit on esitelty aiemmin tässä luvussa.

Taulukko 2. Tutkimusten haku koskien kyberturvallisuuden alihankintaketjuja

Hakuväline	**Hakusanat 1**	**Hakusanat 2**	**Hakusanat 3**	**Hakusanat 4**
Google Scholar	Kyberturvallisuus alihankintaketjut ***Esimerkkinosto: 1****	Cybersecurity supply chains ***Esimerkkinosto: 2****	Cybersecurity in outsourcing chains	Cybersecurity third party
IEEE Xplore	Kyberturvallisuus alihankintaketjut	Cybersecurity supply chains	Cybersecurity in outsourcing chains	Cybersecurity third party

Hakusanoina on käytetty seuraavia sanaliittoja:

1) Kyberturvallisuus alihankintaketjut
2) Cybersecurity supply chains
3) Cybersecurity in outsourcing chains
4) Cybersecurity third party

Kokonaisuutena materiaalia, niin tutkimuksia kuin julkaisua, oli paljon. Sopivia ja saatavilla olevia sen sijaan vain kohtalainen määrä. Yleisenä huomiona löydetyistä tutkimuksista voidaan todeta, että niissä oli käytetty tapaustutkimusta tutkimusstrategiana huomattavan paljon. Aineistoa haettaessa on hyvä muistaa myös lähdekritiikki. Tutkijan on arvioitava aineisto ennen kuin hän käyttää sitä tutkimuksessaan. Lähdekritiikin merkitys on suuri, sillä tutkimuksessa käytetyn aineiston laatu vaikuttaa suoraan tutkimuksen luotettavuuteen (Vilkka 2007).

Tutkimusnosto 1*

Järvisen (2020) pro gradu-tutkimuksessa, joka selvitti kyberturvallisuuden nykyisiä ja tulevia osaamistarpeita valitussa ohjelmistoyrityksessä käyttäen apuna NCWF-viitekehystä. Tutkimuksen tuloksena hän nostaa esille seuraavia huomioita alihankintaketjujen hallintaan;

”Alihankintaketjun hallinta nähtiin aineiston perusteella tarpeellisena ja keskeisenä osaamisalueena turvallisen tuotannon kategoriassa. Sen voitiin ajatella olevan siis ydinkompetenssin yksi osaalue. Kyberturvallisen toimintamallin nähtiin kohdistuvan vaatimuksena aina koko alihankintaketjuun. Toimittajaan (kohdeyritys) kohdistuvat vaatimukset nähtiin vyörytettävän aina myös toiminnassa mukana oleville alihankkijoille. Ohjelmistotoimittajan nähtiin vastaavan alihankkijan työstä aina kuten omasta työstään. Kohdeyrityksen laatujärjestelmän todettiin myös sisältävän ohjeistuksen ja prosessikuvauksen alihankintaketjun hallintaan ja siihen liittyviin toimenpiteisiin”

Tutkimusnosto 2*

Solfan (2022) tutkimuksessa todettiin, että liiketoiminnan on kehitettävä kykyään vastata alihankintaketjujen muodostamiin riskeihin. Tämä onnistuu tutkimuksen mukaan lisäämällä läpinäkyvyyttä alihankintaketjuista. Läpinäkyvyys mahdollistaa paremman riskienhallinnan ja vahvemman kyberresilienssin. Tutkimus toteutettiin kohdentaen tutkimus lääketeollisuuden sektorille, kooten vastauksia 14 eri kohdealueen yrityksestä ja 243 henkilöltä. Tutkimus osoitti vahvasti merkittävän positiivisen yhteyden kyberturvallisuuden ja toimitusketjujen riskienhallinnan välillä.

Tässä tutkimuksessa käytettiin yleisesti kyberturvallisuuteen liittyvien aineistojen hankinnassa lisäksi theseus.fi-palvelua, josta löytyy ammattikorkeakoulujen lopputöitä ja julkaisuja. Alihankintaketjujen kyberturvallisuuteen liittyviä ja tähän tutkimukseen sopivia ja lisäarvoa tuottavia töitä, sieltä ei suoraan löytynyt. Hakusanoilla ”kyberturvallisuus alihankintaketjut” ja ”kyberturvallisuuden toteutuminen”, ”kyberturvallisuus toimitusketjut” sekä ”cybersecurity subcontracting chain” löytyi joitakin osumia, mutta ei uutta kulmaa tähän tutkimukseen tuovia tutkimuksia.

4.4 Alihankintaketjujen kyberturvallisuuden sopimusjuridiikka

Sopimuksissa on hyvin tyypillisesti varsinkin isoissa yrityksissä maininta, jossa palvelun tuottaja vastaa alihankkijoista kuin omistaan. Kuinka hyvin palvelun tuottaja sitten lopulta huolehtii ja vastaa käyttämiensä alihankkijoiden kyberturvallisuudesta, on toinen asia. Pääsopimuksen osapuoli ei myöskään välttämättä halua asiakkaan olevan aktiivisesti mukana alihankintaketjujen sopimustarkasteluissa, sillä pääsopimuskumppani haluaa hoitaa tuon vastuun itse omalla tavallaan.

Tutkijan oman pitkän tietohallintojohtajakokemuksen mukaan suuret yritykset osaavat usein sopimusten laadinnan ja heillä on käytössään juristeja ja muita sopimusjuridiikkaa tuntevia henkilöitä. Keskeisin ja tunnetuin pykälä koskien alihankintaa on se, että pääsopimuspuoli vastaa alihankkijoistaan kuin omistaan. Käytännössä kuitenkin valvominen ja toimenpiteiden osoittaminen alihankinnan valvontaan voivat olla haastavia eri syistä. Sopimuksissa voidaan hyvin mainita alihankkijat jopa nimeltä, mutta käytännössä alihankkijoiden vaihtuessa niitä ei yleensä päivitetä sopimuksiin, eikä niistä välttämättä edes informoida alkuperäistä asiakasta. Asiakkaan puolella aikataulupaineet, kiinnostuksen puute, tietoisuuden puute sekä asian ulkoistaminen voivat aiheuttaa sen, ettei asia edes nouse arjessa esille. Erilaisissa IT-tarkastuksissa ja vastuuhenkilöiden vaihtuessa yrityksissä voidaan hyvin törmätä tilanteeseen, jossa pitkiä alihankintaketjuja lähdetään tarkastelemaan vasta, kun joku asiakas tai yhteistyökumppani nostaa asian esille. Alihankintaketjun läpikäynti vaatii myös aikaa ja sitkeyttä, joten siihen pitää olla osoitettuna riittävä määrä osaavia resursseja.

Alihankintaketjut voivat muodostaa pitkiä ja monimutkaisiaketjutuksia, joiden kuvaaminen voi saada organisaation heräämään riskien suuruuteen. Alihankintaketjut kasvattavat riskipinta-alaa huomattavasti. Ketjutus voi mennä niinkin pitkälle, ettei varsinainen pääsopimuskumppani toimita itse mitään sopimukseen kuuluvia velvoitteita, vaan on ulkoistanut ne täysin usealle tai useille alihankkijoille. Alihankkijalla on kuitenkin tietysti solmimaansa sopimukseen perustuva suoritus- ja mahdollinen vahingonkorvausvastuu, mutta tämä vastuu on vain sopimuskumppaniaan kohtaan, varsinaista tilaajaa eli asiakasta,

jonka kanssa pääsopimuskumppanilla on sopimus. (Kyberturvallisuuskeskus 2023.)

Tiedonhallintalautakunta (2023) julkaisi tämän tutkimuksen kirjoitushetkellä suosituksen viranomaisille ja hankintayksiköille erityisesti tietojärjestelmien hankintoja varten ohjeistusta tietoturvallisuusvaatimusten määrittelystä ja toteutumisen varmistamisesta. Oheistus perustuu Julkisen hallinnon tietoturvallisuuden arviointikriteeristöön (Julkri). Ohjeistus sisältää paljon hyödynnettävää tietoa myös kyberturvallisuuden osa-alueelle.

Toimitusketjun hallintaa tutkivissa aineistoissa niin Suomessa kuin kansainvälisissäkin aineistoissa nousee kuitenkin yllättävän vähän esille sopimukselliset asiat. Sopimus ei takaa onnistumista, mutta se tuo turvaa niin lainsäädäntöä vasten, kuin helpottaa arjen johtamista. On kuitenkin muistettava, että sopimus tuo lisäarvoa vasta, kun sen noudattamista ohjataan ja valvotaan.

5 KYBERTURVALLISUUDEN TOTEUTUMINEN

5.1 Toteutumisen määritelmiä

Kyberturvallisuuden toteutumiselle on esitetty erilaisia epävirallisia määritelmiä. Tutkijan oma näkökulma on, että kyberturvallisuus on toteutunut silloin, kun yritys on saavuttanut siltä lainsäädännön edellyttämän ja lisäksi omaan tilanteeseensa sopivan ja perustellun tason. Lisäksi on tärkeää, että asiantuntijat ja johto sitoutuvat tuohon sovittuun tasoon yhteisesti. Joku yritys taas voi tulkita kyberturvallisuuden toteutuneeksi vasta, kun se on hyvällä tasolla tai korkealla tasolla. Myös hyvä tai korkea taso, tai ylipäätään mikä taso tahansa, vaatii, että se määritellään. Finanssivalvonta vaatii esimerkiksi työttömyyskassoja, joihin YTK kuuluu, määräys- ja ohjekokoelmassaan (MOK) huolehtimaan, että tietoturva noudattaa korkeaa tasoa (Finanssivalvonta 2021).

Tutkijan oman näkemyksen mukaan yrityksen on tehtävä johtotasolla päätös, millaista kyberturvan tasoa tavoitellaan. Tämä on sidoksissa siihen, miten liiketoiminta halutaan turvata ja paljonko se saa maksaa. Yksinkertaisuudessaan kyse on riskeistä ja halusta lieventää riskien todennäköisyyttä ja vaikutusta tai kokonaan poistaa riskejä. Halutaanko tehdä kaikki tehtävissä oleva

vai päädytäänkö tekemään toimenpiteitä, jotka alentavat riskin todennäköisyyttä tai vaikutusta jonkin verran, on yrityksen päätettävä ja linjattava johdossa. Kyberturvallisuus on aina yrityksen johdon ja viime kädessä hallituksen vastuulla (Traficom 2020).

Laaksosen (2018) mukaan kyberturvallisuus on oikealla tavalla huomioitu, kun organisaatiossa kyberturvallisuuden asiat ovat selkeästi vastuutetut ja yhteistyö eri vastuualueiden välillä on aktiivista ja toimivaa. Lisäksi Laaksonen toteaa, että kyberturvallisuus ei silloin ole vain osasto tai ryhmä ihmisiä, vaan asenne. Kyberturvallisuus ei myöskään ole vain tekniikkaa, vaan prosesseja, toimintatapoja ja ongelmatilanteisiin varautumista.

Kyberturvallisuuden toteutumiselle ei ole esitetty yhtä virallista määritelmää, vaikka se on olennainen asia esimerkiksi yrityksen hallituksen kannalta. Kyberturvallisuuden toteutuminen ei kuitenkaan voi missään olosuhteissa tai määritelmällä tarkoittaa sitä, ettei kyberriskejä olisi. Kyberriskejä on aina ja kyberturvallisuudesta vastaavilla on ikuinen kilpajuoksu käynnissä pystyäkseen torjumaan tunnistettujen kyberriskien toteutumisen.

5.2 Toteutumisen arviointi

Organisaatiossa voidaan erilaisten viitekehysten tai standardien avulla määrittää omaa kyberturvallisuuden toteutumisen tilannetta. Luvussa 3.4 on läpikäyty useampia viitekehyksiä ja standardeja. Edellä mainitusta luvussa on esitelty myös kyberturvallisuuskeskuksen kybermittari. Se on matalan kynnyksen työkalu, jolla moni organisaatio usein aloittaa oman kyberturvallisuuden tason määrittelynsä. Kyberturvallisuuskeskus onkin tehnyt merkittävää työtä lisätäkseen organisaatioiden kybertuvallisuutta tämän työkalun avulla. Kybermittarin käyttäminen ja hyödyntäminen vaatii kuitenkin myös osaamista. Kaikilla yrityksillä ei ole riittävää määrää osaajia käytössään tai muutoin mahdollisuutta hyödyntää työkalua, vaikka itse työkalu onkin ilmainen.

6 TUTKIMUSJOUKON MÄÄRITTELY JA VALINTA

6.1 Valintakriteerit

Tutkimuksen aluksi asetettiin kriteerit osallistuville yrityksille. Organisaatioiden tulisi olla huoltovarmuuskriittisiä ja heillä tulisi olla aikaa lähteä mukaan tutkimukseen ja käydä tutkimuksen lopuksi tuloksia läpi osana tutkimuksen luotettavuuden varmistamista. Haastatteluihin tulisi kulumaan useita tunteja ja kyselytutkimuskin veisi lähes saman verran aikaa.

Tutkimuksen luotettavuuden kannalta mukana olisi hyvä olla riittävä määrä yrityksiä, mutta ei myöskään liian paljon, sillä tulosten analysointi voisi käydä liian raskaaksi. Haastattelu- ja kyselytutkimuksen toteuttaminen ja analysointi tulisivat viemään kuitenkin jo muutaman osallistuvan organisaation osalta useita viikkoja työaikaa. Tutkimuksen luotettavuuden kannalta tutkija piti riittävänä, että yrityksiä olisi mukana kolme ja ne voisivat toimia huoltovarmuuden eri sektoreissakin. Myöskään sillä, toimittivatko organisaatiot palveluja tai tuotteita kuluttajille vai toisille yrityksille, ei ollut merkitystä. Jokaisella osallistuvalla yrityksellä tuli kuitenkin olla selkeästi merkittävissä määrin alihankintaa, joka voi olla hankkijan näkökulmasta tai sitten organisaatio toimii itse osana alihankintaketjua. Organisaation henkilöstön määrä tuli olla myös yli 50 henkilöä, jolloin ne lukeutuisivat keskisuuriin tai suuriin yrityksiin. Suomen yrittäjien (2023) mukaan keskisuuria yrityksiä ovat henkilömäärältään 50–249 henkilön yritykset ja vähintään 250 henkilöä työllistävät yritykset ovat suuryrityksiä. Suomalaisista yrityksistä on 0,6 % yli 50 henkilöä työllistäviä yrityksiä (Tilastokeskus 2023). Liikevaihdon tuli olla yli 10 miljoonaa euroa, jolla varmistettiin myös, että alihankinta on merkittävän kokoista.

Kriteerit yritysten mukaan ottamiselle;

1. Huoltovarmuuskriittinen
2. Aikaa osallistua tutkimukseen ja käydä tuloksia läpi
3. Merkittävissä määrin alihankintakokemusta, osana alihankintaketjua tai hankkijana
4. Henkilöstömäärä yli 50 henkilöä
5. Liikevaihto yli 10 miljoonaa euroa

6.2 Tutkimukseen osallistuvat yritykset

Mukaan valikoidut yritykset kasattiin yllä kuvatuilla kriteereillä käyttäen tutkijan omia työelämän verkostoja apuna. Kaikki yritykset täyttivät valintakriteerit ja sitoutuivat käyttämään aikaansa tutkimukseen sovitun mukaisesti.

Osallistuvat yritykset olivat YTK, Fujitsu ja anonyymina pysyttelevä yritys. Alla lyhyet esittelyt jokaisesta yrityksestä.

YTK on Suomen suurin työttömyyskassa, jolla on yli 500 000 jäsentä. YTK:n tehtävänä on järjestää ansioturva jäsenilleen. YTK turvaa jäsenten toimeentulon työttömyyden, lomautuksen, osa-aikatyön, sivutoimisen yritystoiminnan sekä vuorotteluvapaan aikana. YTK haluaa tehdä monimutkaisesta työttömyysturvasta ymmärrettävää ja tuottaa parasta ja ystävällisintä palvelua jäsenilleen. YTK:lle tietoturva, tietosuoja ja kyberturvallisuus ovat erittäin tärkeitä asioita, sillä se käsittelee jäsentensä arkaluonteista tietoa järjestelmissään. YTK:n osallistuja tutkimuksessa oli Tietoturvapäällikkö Matti Laakso.

Fujitsu on globaali tietotekniikan palveluyhtiö, joka tarjoaa vahvan paikallisen palvelukyvyn. Fujitsu Finland Oy toimii Suomessa yli 20 paikkakunnalla. Pääkonttori sijaitsee Helsingissä ja suurimmat aluetoimipisteet ovat Tampereella, Turussa ja Lahdessa. Suomessa ja Virossa palveluksessa on noin 2 000 työntekijää. Fujitsulta tutkimukseen osallistuivat Tietoturvajohtaja Marko Remes ja Alihankintavastaava Petteri Lehtonen.

Anonyymi yritys
Yhteiskunnan toiminnan kannalta huoltovarmuuskriittinen yritys, jolla on merkittävät toimintavelvoitteet myös häiriötilanteissa ja poikkeusoloissa. Yritys kuuluu kokoluokaltaan suuryrityksiin ja se hallinnoi mittavaa alihankintaverkostoa. Yrityksen osallistujia tutkimuksessa olivat valmiuden ja kyberturvallisuuden asiantuntijat turvallisuusorganisaatiosta.

Jäljempänä tutkimuksessa, yllä luetelluille osallistuville yrityksille on arvottu satunnaisesti numerokoodi, käyttäen lukuja 1–10. Luottamuksellisuuden säilyttämiseksi yrityksen nimeä ja koodinumeroa ei tässä tutkimuksessa julkaista.

Numerokoodeina käytetään numeroita 5, 8 ja 10. Jäljempänä käytetään lyhenteinä: osallistuva yritys nro 5 = OS5, osallistuva yritys nro 8= OS8, osallistuva yritys nro 10 = OS10. Näin turvattiin osallistuvien organisaatioiden anonymiteetti.

7 TUTKIMUKSEN TOTEUTUS

7.1 Haastattelu- ja kyselytutkimuksen toteutusvaiheet

Ensimmäisenä vaiheena toteutettiin tutkimushaastattelu. Haastattelu pidettiin fyysisenä tapaamisena kahden osallistuvan yrityksen osalta ja yhden osalta Microsoft Teams -välinettä käyttäen. Yrityksen, joka ei voi osallistua tähän tutkimukseen nimellään, haastattelu pidettiin fyysisenä tapaamisena 17.5.2023. Läsnä haastattelussa oli kaksi yrityksen valmiuden ja kyberturvallisuuden asiantuntijaa. YTK:n Tietoturvapäällikön haastattelu toteutettiin 25.5.2023 ja Fujitsun Tietoturvajohtajan ja Alihankintavastaavan haastattelu 16.6.2023.

Haastattelua sovittaessa ja sen aikana kävi ilmi, että yksi yrityksistä halusi vastata kyselytutkimuksen kysymyksiin etätapaamista käyttäen ja kahdelle voitiin toimittaa kysymykset sähköpostilla, jättäen heille arvioinnin tekemisen siitä, voivatko he vastata siihen myös sähköpostilla vai edellyttääkö se vahvempia turvatoimia. Kysymysten ollessa kuitenkin melko ylätasoisia, molemmat yritykset päätyivät toimittamaan vastaukset sähköpostilla. Kahden yrityksen kanssa haastatteluissa otettiin jo mukaan kyselytutkimuksen kysymyksiä, joten kirjallisesti vastattavaa eri jäänyt kovinkaan paljon.

Kaikille haastateltaville toimitettiin haastattelukysymykset merkittyine teema-alueineen vähintään viikkoa ennen haastattelua etukäteen tutustuttavaksi (Liite 1). Tällä varmistettiin se, että haastattelu sujuisi jouhevasti ja haastateltavat saisivat arvioida kysymyksiin vastaamisen tasoa jo ennen haastattelua. Kyberturvallisuudesta puhuttaessa ollaan hyvin helposti jopa salaisen tiedon äärellä, joten tämä keino antoi haastateltaville mahdollisuuden valmistautua rauhassa. Lähtökohtaisesti sovittiin jo ennen tutkimuksen aloitusta, ettei salaista tietoa käsitellä ollenkaan, vaan tieto kuuluu korkeintaan luottamuksellisen tiedon piiriin. Myöskään mitään muita henkilötietoja kuin haastateltavien tietoja, ei käsitellä. Kaikki tutkimuksessa käsitelty luottamuksellinen tieto on anonymisoitua.

Kyselytutkimuksen kysymykset (Liite 2) toimitettiin kaikille osallistujille sähköpostilla haastattelututkimuksen suorittamisen jälkeen. Kyselytutkimuskysymyksistä poimittiin vain ne, joita ei huomioitu haastattelututkimuksen yhteydessä. Kyselytutkimuksen osalta palautusaika sovittiin jokaisen osallistujan kesken erikseen. Haastattelun- ja kyselytutkimuksen jälkeen sovittiin osallistuvien organisaatioiden yhteisestä loppukeskustelusta. Loppukeskustelun ajankohdaksi valikoitui 28.8.2023.

Haastattelu- ja kyselytutkimuksessa kysymykset oli jaettu teema-alueisiin. Teema-aluejako perustui lopulta sellaisiin teemoihin, jotka alkoivat muotoutua jo haastatteluun valmistautuessa, sekä teoreettisesta viitekehyksestä että alustavista keskusteluista osallistuvien yritysten kanssa. Haastattelun aikana mainitsin teemaluokan aina ennen kysymystä ja samalla kannustin laajempaan vastaamiseen kuin vain pelkkä haastattelukysymys.

Haastatteluissa kokonaisuutena pysyttiin hyvin teema-alueissa ja vastattiin kaikkiin etukäteen lähetettyihin kysymyksiin. Otin myös muutamia lisäkysymyksiä esille kyselytutkimuksen puolelta ja kerroin, että niihin ei ole pakko vastata, koska ne eivät kuuluneet etukäteisaineistoon. Lähes poikkeuksetta myös esille ottamat kyselytutkimuksen kysymykset käsiteltiin haastattelun aikana. Lisäkysymysten esille otto liittyi haastattelukysymyksien aikana esille tulleisiin, läheisesti kyselytutkimuksessa olleisiin kysymyksiin. Näin ollen oli perusteltua mutta vapaaehtoista vastata niihin haastatteluhetkellä.

Haastattelujen virallinen nauhoitettu osuus kesti keskimäärin 58 minuuttia. Etäyhteyden kautta toteutettu haastattelu kesti hiukan vähemmän aikaa kuin muut haastattelut, vain 46 minuuttia. Kaikkien haastateltavien kanssa haastatteluaikaa oli varattu riittävästi, eikä muitakaan häiriöitä tullut esille haastattelun aikana. Nauhuri toimi moitteetta ja nauhoitus oli hyvälaatuinen. Nauhoituksen osalta merkillepantavaa oli se, ettei yksikään osallistuja vahingossa maininnut yrityksen tai henkilöiden nimiä nauhoituksen aikana, vaan jokainen osallistuja muisti ohjeistukset asian suhteen. Myös haastattelija pysyi ohjeistuksessa poikkeuksetta.

7.2 Haastattelu- ja kyselytutkimuksen aineiston käsittely

Kolmen haastattelun osalta kertyi Arial fontilla fonttikoolla 12 litteroitua tekstiä 33 sivua. Kyselytutkimuksen vastausten puhtaaksikirjoitus ja yhdistäminen toi kuusi sivua lisää samalla fontilla ja fonttikoolla kirjoittaen. Yhteensä materiaalia kertyi 39 sivua. Analysoidessani materiaalia säilytin sitä sähköisessä muodossa, enkä turvallisuussyistä tulostanut sitä paperille. Paperille tulostaminen olisi voinut helpottaa materiaalin läpikäymistä, mutta turvallisuussyyt menivät päätöksen edelle. Tulostettu materiaali olisi pitänyt säilöä turvalokerossa, eikä käytössäni ollut turvalokero ollut riittävän suuri. Turvalokerossa oli tilaa vain haastatteluaineison sisältävälle nauhurille ja osallistujien tiedot sisältävälle ulkoiselle kovalevylle.

Litteroitunani kaikki haastattelut luin ne läpi kaksi kertaa ilman muistiinpanojen tai huomioiden tekemistä. Kolmannella kerralla lähdin pohtimaan teema-alueiden sopivuutta luokittelun perusteena ja tein alustavia havaintoja litteroituun materiaaliin. Lisäksi kuuntelin kaikki nauhoitteet läpi kaksi kertaa. Kyselytutkimuksen materiaalien läpiluku oli nopeampaa ja lukukertoja kertyikin yhteensä neljä. Aikaa materiaalin analysointivaiheeseen litterointeineen kului yhteensä työaikaa yli kaksi viikkoa. Huolellinen tutkimusaineiston käsittely ja analysointi on kuitenkin merkittävä osa tutkimuksen luotettavuutta, joten siihen käytetystä ajasta ei kannata tinkiä. Hirsijärven ym. (2008) mukaan luotettavuuteen vaikuttaa tallennusten laatu, litteroinnin tasaisuus ja luokittelun säännönmukaisuus.

Haastattelu- ja kyselytutkimuksen materiaalin litteroinnin ja puhtaaksikirjoituksen jälkeen pohdin erilaisia aineiston luokittelutapoja. Päädyin kuitenkin käyttämään tutkimusongelman pääkysymystä sekä alikysymyksiä luokittelun perusteella, sillä kun haastattelu- ja kyselytutkimuksen kysymykset oli laadittu vastaamaan tutkimusongelmaan.

Usein kvalitatiivista tutkimusta tekevä tutkija joutuukin pohtimaan, miten luokkia luodaan, mutta siihen ei ole yksiselitteistä vastausta. Luokkien muodostamisen kriteerit ovat tiukasti yhteydessä tutkimustehtävään, aineiston laatuun ja tutkijan teoreettiseen osaamiseen ja kykyyn käyttää tietoa. Aineiston luokitteluun voidaan käyttää tutkimusongelmaa ja alaongelmia, tutkimusvälinettä tai menetelmiä, käsitteitä tai luokkia. Tutkijan kannattaa myös selvittää millaisia

luokkia muut tutkijat ovat vastaavissa tutkimuksissa käyttäneet (Hirsijärvi ym. 2008, 148).

7.3 Haastattelu- ja kyselytutkimuksen vastaukset teema-alueittain

Haastattelussa ja kyselytutkimuksessa olevat teema-alueet (Taulukko 3) ovat lueteltuina alla, sekä ovat merkittyinä myös haastattelu- ja kyselytutkimuslomakkeisiin (Liite 1 ja 2)

Taulukko 3. Tutkimushaastattelun- ja kyselyn teema-alueet

Teema-alueet ja niiden kuvaus
1. Ihmiset Yrityksen henkilökunnan vaikutus, myös hallitus
2. Osaaminen Yrityksen osaamisen taso, myös yhteistyökumppanien ja asiakkaiden osaaminen
3. Harjoittelu Kaikki yrityksen sisäinen sekä ulkoinen harjoittelu
4. Vaatimukset Laista, asetuksista, säädöksistä ja/tai asiakkailta tai yhteistyökumppaneilta tulevat vaatimukset
5. Tausta Yrityksen kyberturvallisuuden kehittymiseen liittyvät tieto tai muu vaikuttava tekijä
6. Hallinto Yrityksen tapa käsitellä kyberturvallisuutta, hallintomalli, päätöksentekomalli
7. Sopimukset Yrityksen tapa tehdä sopimuksia, sekä huomioida kyberturvallisuus
8. Työkalut- ja ohjeistus Yrityksen käytössä olevat työkalut- ja ohjeistukset, sekä mahdolliset sertifikaatit, markkinoilla olevien työkalujen tuntemus ja esille nostaminen

Teema-alueittain purettuna löydökset olivat alla kuvattuja. Kuten tämän tutkimuksen kappaleessa kuusi on kerrottu, osallistuville yrityksille on arvottu satunnaisesti numerokoodi, käyttäen lukuja 1–10. Luottamuksellisuuden säilyttämiseksi yrityksen nimeä ja siihen arpomalla yhdistettyä koodinumeroa ei tutkimuksessa julkaista.

7.3.1 Ihmiset (teema-alue 1)

Ihmiset (teema-alue 1) muodostavat selkeän ja ison kokonaisuuden vaikutuksiltaan siinä, miten kyberturvallisuus toteutuu. Johdon tuen merkitys oli kaikissa tutkittavissa organisaatiossa erittäin suuri. Johdon edustuksella tarkoitetaan tässä hallitusta, johtoryhmää, sekä myös alueesta operatiivisessa arjessa vastaavaa henkilöä. Erityistä kyberlähettilästä ei nouse esille, vaan enemmän on kyse kaikkien osallistuvien yritysten osalta pitkästä matkasta, jossa kyberosaaminen on kehittynyt vuosien varrella siihen kypsyystasoon, jossa se nyt on. Empiirisinä havaintoina nousi esille innokkuus ja kiinnostus aiheeseen, joka oli selkeästi näkyvissä kaikkien osallistuvien organisaatioiden osallistujien osalta. Yksittäinen osallistuja nosti esille myös oman roolinsa, jonka hän näki olevan myös merkittävä asia kyberturvallisuuskulttuurin luomisessa yrityksessä.

Kyberturvallisuuden osalta henkilökunta on pääosin omaa, mutta erikoistilanteissa ja tiettyä kapea-alaista osaamista tarvittaessa käytetään myös ulkopuolista apua. Häiriönhallinta ja uhkatilanteen analysointi haluttiin pitää omissa käsissä, sekä tilanneymmärrys, jota jokainen osallistuva yritys korosti.

OS8, kertoi vastauksena kysymykseen; Onko organisaatiossanne ns. kyberturvallisuuslähettilästä, jolla on ollut erityinen rooli kyberturvallisuuden tason kasvattamisessa, että:

> *”Kun me tiedotetaan asioista ja niin kuin tavallaan kerrotaan uhkista ja asioista, voidaan me kyllä sanoa, että ollaan niin kuin kyberlähettiläitä”*

Tähän teema-alueeseen liittyivät lähtökohtaisesti kysymykset: H2, H3, H5 ja K4.

7.3.2 Osaaminen (teema-alue 2)

Osaaminen (teema-alue 2) kyberturvallisuuden osalta kokonaisuutena, sekä myös alihankintaketjujen vastuiden ymmärtämisen osalta, näyttäytyi kaikkien osallistuvien yritysten osalta vahvana. Kaikilla haastateltavilla henkilöillä oli vastuualueestaan pitkää kokemusta, ja he tunsivat selvästi tekevänsä tärkeää ja vastuullista työtä. Tärkeimpinä asioina kyberturvallisuuteen vaikuttavina asioina vastaajat lähes yksimielisesti nostivat esille johdon tuen, kontrollit, politiikat ja koulutuksen. Kaikissa yrityksessä johdon tuki ja yhteiset läpikäynnit vaikuttivat selvästi kyberturvallisuustoimiin. Yksittäisenä huomiona todettakoon, että yhdellä osallistuvista yrityksistä, kyberturvallisuuskeskuksen kybersää tuli jopa johdon sähköposteihin.

Alihankintaketjujen valvominen ja johtaminen koettiin tärkeänä asiana, joskin vaikka vastuut olivat selkeitä kaikille osallistuville yrityksille, että rekisterinpitäjä on aina vastuussa alihankintaketjun loppuun saakka, aiheutti paljon pohdintaa, kuinka pitkälle ketjua käytännössä pystytään valvomaan toimintaa. Parhaina keinoina varmistua alihankintaketjujen turvallisuutta pidetiin sopimuksia ja auditointeja, mutta myös harjoittelua. Kysymysten kääntyessä kyberturvallisuuden tärkeyteen vastaukset olivat myös yhteneväisiä. Rikollisten ammattimaisuus on lisääntynyt ja kyberturvallisuudesta on tullut pakko ja edellytys. Auditoinnit ja vaatimukset tulevat lisääntymään. Yksi yritys nosti esille myös sen, että kehityssuunta kyberturvallisuudessa ei voi olla vaikuttamatta lakeihin.

Yksittäinen osallistuja yritys kertoi, että jokainen alihankintaketju katsotaan tarkasti loppuun saakka, yhden osalta satunnaisemmin ja tarpeen mukaan ja yhden osallistuvan yrityksen osalta muutama alihankintaketjuporras eteenpäin.

OS10 nostaa esimerkin alihankintaketjujen valvonnan tärkeydestä:

> *”Jos nyt vaikka tavarantoimittaja joutuisi kyberhyökkäyksen kohteeksi eikä voisi toimittaja tavaraa, niin ei putkifirmaan voi hoitaa*

omia vastuitaan. Tässä sitten käy niin että ei myöskään se putkifirmalta apua pyytänyt firma saa putkiaan kuntoon ja mahdollisesti senkin toiminta keskeytyy".

Tähän teema-alueeseen liittyvät lähtökohtaisesti kysymykset: H5, H6, H10, K4, K6, K7, K8

7.3.3 Harjoittelu (teema-alue 3)

Harjoittelu (teema-alue 3) ja sen merkitys nousi esille jokaisen vastaajan osalta. Osa oli jopa sitä mieltä, että ilman harjoittelua ei voida edes todentaa kyberturvallisuuden tasoa, sillä muuten kaikki on vain paperinmakuista. Harjoittelu näyttäytyi osallistuvissa yrityksissä positiivisena ja aktiivisena toimena. Kahdella osallistuvalla yrityksellä oli paljon ulkopuolisiin harjoituksiin osallistumisia. Kaikilla vastaajilla vaihdettiin ainakin osittain harjoituksiin osallistujia eri harjoituskerroilla oppimisen laajentamiseksi.

OS5 kertoo että:

"Harjoituksissa pyritään kierrättämään henkilöitä kokemuksen kartuttamiseksi, näin ollen osaaminen laajenee isommalle joukolle".

Lisäksi OS8 jatkaa:

"Uhkaskenaariotoiminta on monipuolista, se ollaan mukana tuolla oman sektorin harjoituksessa ja sitten on omia kommervenkkejä. Me polkastaan käyntiin vaikka harjoitus, jos ei vaikka ole mitään erityistä menossa, kun meille on johtokin antanut siihen luvan, eli keksitään harjoitus kun on niinku hiljasta"

Kyselytutkimuksen kysymys nro 2, liittyvät huomiot tulivat katetuksi jo teema-aluessa nro 2, joten niitä ei käsitellä tässä kohtaa.

Tähän teema-alueeseen liittyvät lähtökohtaisesti kysymykset: H8, H11, K2

7.3.4 Vaatimukset (teema-alue 4)

Vaatimukset (teema-alue 4) eri tahoilta, olivatpa ne yrityksen johto tai yrityksen asiakkaat, tai yhteistyötahot, nousivat erittäin keskeisinä asioina esille vastauksissa. Erityisesti asiakassuunnan vaatimukset ovat koventuneet ja tarkentuneet viime aikoina. Tosin kaksi vastaajaa myös kertoi, että asiakaspuolella ei välttämättä aina ihan tarkasti osata purkaa vaadittuja kyberturvallisuuden vaatimuksia auki, vaan laatimassa on ollut ehkä juristi tai konsulttiapua, jota ei ole enää saatavilla, eikä asiakas itse ymmärrä ihan tarkasti miksi jotakin asiaa on vaadittu.

Yrityksen omat hallinnollisen tietoturvan asiat nousivat vahvasti esille. Kyberturvallisuuteen liittyvät politiikat, käytännöt, ohjeistukset ja vuosikellot rytmittivät vastaajien mielestä arkea kaikista vahvimmin.

Oman kyberturvallisuuden tason arviointiin oli käytetty työkaluja apuna, mutta mitenkään erityisen korostetusti niiden tuottamaa hyötyä ei tuotu esille. Selkeästi sen sijaan esille nousi mahdollisten sertifikaattien mukaisten toimenpiteiden noudattamisen pakollisuus, sekä oma arviointi kyberturvallisuuden tilasta, jota pidettiin tärkeänä.

Haastattelututkimuksen kysymys 12, jossa kysyttiin ”Vaativatko/kysyvätkö asiakkaanne alihankintaketjujen kyberturvallisuudesta?”, tuli kaikilta osallistuvilta yrityksiltä kyllä -vastaus lisäkuvauksineen. Tämä kertoo siitä, että asia on asiakkailla ja yhteistyökumppaneilla tiedossa, mutta kuten yllä todettu, ei välttämättä aina ymmärretä kuitenkaan mitä vaaditaan.

OS5: ”Kyllä,…”, OS8: ”Kyllä,…” ja OS10: ”Kyllä,..”

Tähän teema-alueeseen liittyvät lähtökohtaisesti kysymykset: H12, H3, K5

7.3.5 Tausta (teema-alue 5)

Tausta (teema-alue 5) aihealuetta läpikäytäessä laaja-alaisesti esille nousi se, että kyberturvallisuuden eteen on osallistuvissa yrityksissä tehty työtä jo pitkään. Välttämättä jokaisen osallistuvan yrityksen osalta historia kyberturvallisuudesta ei ollut täysin kirkkaana tiedossa henkilövaihdosten takia. Erilaiset jo kauan aikaa sitten päivätyt dokumentit ja selvitykset osoittivat, että työtä on tehty pitkäjänteisesti.

Omaa selkeää budjettia pelkästään kyberturvalle ei ollut, mutta sen sijaan tietoturvakokonaisuudelle kyllä. Osalla se oli jakaantunut eri liiketoiminta-alueisiin. Kysyttäessä kuinka tärkeää varautuminen ja jatkuvuus ovat asteikolla 1–10 yrityksellenne, vastaukset sijoittuivat välillä 8–10. Alempaa kuin 10 arviota perusteltiin sillä, että arvio 10 haluttaisiin antaa vain toimiessa maanpuolustuksen tai erittäin muun erittäin kriittisen sektorin toiminnassa.

OS5 kertoo, että:

> *”Kyllä se kymppi on, vaikea sitä on kovin montaa toimijaa kotimaassa tietää, missä se olisi näin tärkeä. Se on niin kuin olemassaolon edellytys”*

Kyselytutkimuksen kysymys nro 1, liittyvät huomiot tulivat katetuksi jo teema-alueessa nro 4, kysymyksen 5 yhteydessä, joten niitä ei käsitellä tässä kohtaa.

Tähän teema-alueeseen liittyvät lähtökohtaisesti kysymykset: H1, H7, K1, K3

7.3.6 Hallinto (teema-alue 6)

Hallinto (teema-alue 6) osa-alue piti sisällään keskustelua siitä vahvasti kyberturvallisuus näkyy johtamisessa ja miten johto on sitoutunut edistämään asioita. Kaikilla osallistuvilla yrityksillä kyberturvallisuuden asioita käsiteltiin säännöllisesti yrityksen johdossa, osalla osana muuta suurempaa kokonaisuutta, kuten turvallisuuden kokonaistilannetta sekä riskien läpikäyntiä. Hallituksen

osalta näkymä oli jo vähän sumuisempi, kuitenkin niin, että tiedettiin asioita käsiteltävän hallituksessakin aika-ajoin.

OS10 kertoi, että johtoryhmälle menee säännöllisesti raportti tietoturvan tilanteesta osana koko IT:n raportointikokonaisuutta.

OS8 kertoi, että:

> *”Kokonaisuutena raportoidaan tästä kaikesta. Johto haluaa toimintakykyyn liittyviä asioita ja ennakointia. Ei ehkä tapahtumien määrä, vaan se laajempi kokonaisuus. Kokonaisuuden tilanne. Riskikartan kautta ja sillä lailla”.*

Kyselytutkimuksen kysymys nro 2, liittyvät huomiot tulivat katetuksi jo teema-alueissa nro 2,3 ja 4, joten niitä ei käsitellä tässä kohtaa.

Tähän teema-alueeseen liittyvät lähtökohtaisesti kysymykset: H3, H10, H11, K2

7.3.7 Sopimukset (teema-alue 7)

Sopimukset (teema-alue 7) sekä asiakassuuntaan että toimittajasuuntaan, nousivat vahvoina esille kaikkien haastateltavien kanssa. Jokaisella oli omien toimittajiensa sopimuksia, joissa tietosuoja, tietoturva ja kyberturvallisuus huomioitiin. Apuna käytettiin muun muassa vastuumatriiseja, jossa yksiselitteisesti kerrotaan, kenen vastuulla tekeminen on ja ketkä siihen osallistuvat ja kenelle siitä pitää raportoida. Tämän työkalun käyttö nousi esille kahden eri osallistuvan yrityksen toimesta ja käyttivät sitä aktiivisesti.

Tietoturvavaatimukset ja kyberturvavaatimukset tulivat laista, asetuksista, sertifikaattien kautta, asiakkaiden vaatimuksista ja yhteistyökumppanien vaatimuksista. Suurelta osin vaatimukset pohjautuivat lakeihin, vain harva asiakas- tai yhteistyökumppani vaati mitään erityistä. Kuitenkin se, mitä milloinkin pitäisi vaatia tietyn tuotteen tai palvelun osalta, herätti ajatuksia.

OS8 kertoo, että:

> *”Meillä on keskeisimpien toimittajien kanssa sopimukset, joissa on keskeisinä asiana kybervaatimukset”*

Lisäksi OS10 toteaa, että:

> *”Näkyy sopimuksissa ja ehkä enemmänkin henkilötietonäkökulmasta. Mutta aina kun hankintaan uutta, niin tehdään aina tietoturvaliite ja siellä on käytetty hyödyksi esimerkiksi VAHTI-määrittelyä”.*

Tähän teema-alueeseen liittyvät lähtökohtaisesti kysymykset: H4, H11, K2, K6, K7

7.3.8 Työkalut ja ohjeistus (teema-alue 8)

Oman kyberturvallisuuden tason arviointiin oli käytetty erilaisia työkaluja apuna, mutta mitenkään erityisen korostetusti niitä ei tuotu esille. Selkeästi sen sijaan esille nousi mahdollisten sertifikaattien mukaisten toimenpiteiden noudattamisen pakollisuus, sekä oma arviointi kyberturvallisuuden tilasta, jota pidettiin tärkeänä. Oman kyberturvallisuuden tason ja toteutumisen mittaamiseen käytettiin hallinnollisen kyberturvallisuuden erilaisia käytänteitä ja toimintatapoja. Teema-alueen läpikäynnissä korostui prosessit ja käytännöt, sekä raportointi ja harjoittelun merkitys.

Tukea ja ohjeistusta kyberturvallisuuden osalta kaivattiin rautalankamallisena tarkistuslistana asioista, jotka tulee olla kunnossa, että palautuminen kybervaikuttamisesta onnistuu ja että esimerkiksi viranomaisilla on edellytykset tutkia tapausta.

Tähän teema-alueeseen liittyvät lähtökohtaisesti kysymykset: H3, H10, K1, K5, K9

7.4 Teema-alueisiin liittyvät erilliset huomiot

Yksittäisinä vahvoina esille nousseina asioina, vaikka ne teema-alueiden sisäänkin menisivät, on syytä tarkastella neljää huomiota, jotka tulivat haastatteluun osallistuvilta yrityksiltä useaan kertaan mainituiksi.

1. On tärkeää tuntea oma toimintaympäristönsä hyvin. Mitä järjestelmiä meillä on, kuka vastaa niiden päivityksistä ja seuraa että toimitaan ohjeiden mukaan? (maininta kaikilta osallistuvilta yrityksiltä).
2. Hallinnollinen kyberturva ei riitä, on osattava myös teknistä kyberturvaa. Myös toisinpäin, tekninen osaaminen ei auta, jos ei hallinnollinen tietoturva ole kunnossa (maininta kahdelta osallistuvalta yritykseltä).
3. Kyberturvallisuudesta huolehtiminen nähtiin tärkeänä koko yhteiskuntamme kannalta. Kun ymmärtää oman osansa yhtenä tekijänä koko Suomen kyberturvallisuudessa, on sillä vaikutusta myös motivaatioon edistää kyberturvallisuuden asioita. Eli on syytä varmistaa, että jokainen yrityksessä ymmärtää miksi kyberturvallisuutta kannattaa edistää. (maininta kahdelta osallistuvalta yritykseltä).
4. Kyberturvallisuus lähtee jo ohjelmistokehityksestä ja sen johtamisesta, kun alusta pitäen tietoturva ja kyberturvallisuus huomioidaan, on sitten tuotannon aikanakin helpompaa (maininta kahdelta osallistuvalta yritykseltä).

Tutkimuksen eri vaiheissa kävin myös vapaamuotoisia keskusteluja osallistuvien yritysten kanssa. Keskustelut tapahtuivat sovittaessa tapaamisaikoja, lisätietokyselyjen yhteydessä tai haastattelujen yhteydessä, kun nauhoitus ei ollut vielä alkanut, tai kun nauhoitus oli jo päättynyt. Sain osallistuvilta yrityksiltä luvan nostaa noista hetkistä muutaman huomion tähän tutkimukseen.

Yhtenä keskeisenä huomiona nousi esille työmäärä. Kyberturvallisuuden saralla on koko ajan pysyttävä hereillä ja opiskeltava uutta. Tämä voi olla myös stressaavaa, pääosin kuitenkin työhön kohdistuva vankkumaton mielenkiinto ja innostus korvasivat kiireen ja paineen. Toisena huomiona nousi esille asiakaspaineet. Asiakkaat ja myös yhteistyökumppanit voivat olla vaativia ja eivätkä ole selvästikään aina ihan varmoja itsekään, millaisia asioita pyydettyyn palveluun tai tuotteeseen tietoturva- tai kyberturvallisuuden suhteen pitäisi vaatia. Kolmas huomio koski osaavan henkilökunnan rekrytointia. Kaksi yrityksistä kertoi olevan haastavaa saada houkuteltua osaavia kyberturvallisuuden ammattilaisia tai ammattilaiseksi haluavia yritykseen.

Tutkimuksen kannalta vapaamuotoiset keskustelut tutkimuksen eri vaiheissa syvensivät ymmärrystä ja luottamusta osallistuvien yritysten haasteista kyberturvallisuuden saralla. Kuitenkin tutkimuksen eettisyyden kannalta on erittäin tärkeää varmistaa osallistuvilta yrityksiltä saako näistä epävirallisista keskusteluista tutkimuksessa mainita, sillä pahimmillaan tutkija tekee siinä räikeän tutkimusvirheen. Tässä tutkimuksessa, kuten aiemmin jo todettu, asia varmistettiin kaikilta osallistuvilta organisaatioilta.

7.5 Haastatteluaineiston käsittely kvantitatiivisesti

Tein litteroidulle aineistolle myös kvantitatiivista analyysia, poimien haastatteluaineistosta viisi eniten mainittua substantiivia tai substantiiviparia, joilla oli sisältömerkitys ja joilla viitattiin kyberturvallisuuden toteutumiseen. Yhdistelin selkeästi samaa tarkoittavat sanat. Varmistin vielä kuuntelemalla uudelleen nauhoitukset, litteroidun tekstin lukemisen lisäksi, jotta varmasti olin tulkinnut samaa tarkoittavat sanat oikealla tavalla.

Eniten mainitut substantiivit tai substantiiviparit olivat:

1. Johdon tuki, johdon vaatimus, johdon seuranta
2. Tietoturvapolitiikka, kontrollit, sisäiset tietoturvaohjeet, auditointi
3. Asiakkaiden tai yhteistyökumppaneiden vaatimukset
4. Henkilöstön osaaminen
5. Huoltovarmuuskriittisyys

Huoltovarmuuskriittisyys otettiin selkeästi keskeisenä teemana esille, mutta se mainittiin sanana vain kuusi kertaa kolmen eri haastatteluna aikana, kun taas johdon tuki –sanapari sai 16 mainintaa. Tietoturvapolitiikan, kontrollien, sisäisten tietoturvaohjeiden ja auditoinnin muodostavat sanat saivat yhteensä 14 mainintaa, eli toiseksi eniten. Asiakkaiden ja yhteistyökumppaneiden vaatimukset, hieman eri sanoin ilmaistuina eri kerroilla, saivat yhteensä 13 kertaa maininnan kolmen haastattelun aikana. Henkilöstön osaaminen mainittiin yhteensä 11 kertaa. Kuitenkin näiden asioiden maininta johtuu vahvasti myös puolistrukturoidun teemahaastattelun teemojen nimistä ja myös siitä, että kysymyksissä mainitaan yllä kuvattuja sanoja. Näin ollen yllä oleva analyysi on ehkä enemmänkin mielenkiintoinen huomio kuin tutkimuksellisesti täysin luotettavana pidettävä tieto.

Eri teema-alueiden alla saatettiin käsitellä muihinkin teema-alueisiin liittyviä asioita ja kysymyksiä, jolloin siirsin sellaisten kommenttien osalta näkemykset ja huomiot oikean teema-alueen alle.

8 TUTKIMUKSEN TULOKSET

8.1 Kyberturvallisuuden toteutumiseen vaikuttavat tekijät

Tutkimusongelma koostui pääkysymyksestä sekä neljästä apukysymyksestä. Tutkimuksen pääkysymykseen: ”Mitkä tekijät vaikuttavat siihen, että kyberturvallisuus toteutuu alihankintaketjuissa?”, haettiin vastausta apukysymysten avulla. Keskeiset haastattelu- ja kyselytutkimuksesta poimitut tulokset on jaoteltu alla tutkimuskysymysten alle.

Tutkimuskysymys 1: *Onko kyberturvallisuuden määritelmä ymmärrettävä?*

Kyberturvallisuuden määritelmä vastasi haastattelu- ja kyselytutkimuksen perusteella kyberturvallisuudesta sekä arkikielessä että tutkimuksen tietoperustassa esiteltyjä määritelmiä. Tähän vaikuttaa varmasti osallistuvien organisaatioiden kyberturvan vankka osaaminen, jota käsiteltiin teema-alueessa ”Osaaminen”. Kyberturvallisuus haluttiin nähdä osana kokonaisturvallisuutta. Kyberturvallisuuden määritelmän osalta ei noussut tarvetta tarkentaa sitä, eikä se myöskään luonut tutkimuksen toteuttamiselle riskiä, sillä sen määritelmä oli hyvinkin selkeä osallistuville organisaatioille, vaikka erojakin sen kuvaamisessa oli selvästi havaittavissa osallistuvien organisaatioiden kesken.

Tutkimuskysymys 2: *Mitkä asiat vaikuttavat kyberturvallisuuden tasoon?*

Kyberturvallisuuden tasoon vaikuttivat eniten johdon tuki ja oma osaaminen. Organisaation oman osaamisen kautta luodut hallintomallit kyberturvallisuuden johtamiseen näyttäytyivät jokaisen haastattelussa läpikäydyn teema-alueen osalta vahvoina. Lakien ja asetusten sekä erilaisten sitovien määräyksien vaikutus koettiin vahvana. Liiketoiminnan ja kyberturvallisuuden kytkeminen yhteen samaa päämäärää kohti koettiin vahvana vaikuttavana tekijänä kyberturvallisuuden tason määrittelyssä ja toteutumisessa.

Tutkimuskysymys 3. *Miten kyberturvallisuutta johdetaan alihankintaketjuissa?*

Alihankintaketjujen johtaminen nähtiin tärkeänä ja itsestään selvänä osana kyberturvallisuuden johtamista. Kaikki osallistuva yritykset olivat hyvin perillä vastuistaan rekisterinpitäjänä. Hallinnollisen kyberturvallisuuden johtamisen käytännöt olivat mittavassa roolissa. Ymmärrys tarvittavista teknisistä kyberturvallisuutta vahvistavista toimista nousi myös esille.

Tutkimuskysymys 4: *Milloin voidaan todeta, että kyberturvallisuus toteutuu alihankintaketjuissa?*

Kyberturvallisuuden toteutumista määriteltäessä kävi ilmi, että kyberturvallisuuden toteutuminen ei tarkoita yhdenkään osallistuvan yrityksen mielestä sitä, että kyberhäiriöitä ei voisi esiintyä. Sataprosenttista varmuutta ei olekaan ja sen kanssa on elettävä. Toteutuminen koettiin tilannetajuna. Ymmärretään riskitasot yrityksen johtoa myöten ja kannetaan päätöksistä vastuu. Lakien- ja asetusten noudattaminen koettiin tärkeänä, samoin organisaation johdon ja hallituksen ymmärrys kyberturvallisuuden tilanteesta, aina alihankintaketjujen kyberturvallisuuden johtamista myöten. Asiakkaiden- ja yhteistyökumppaneiden välinen yhteistyö ja aktiivinen toimenpiteiden seuranta nousi vahvana havaintoja esille. Yhteisissä läpikäynneissä oli usein kyberturvallisuuden asiat mukana, joka hyvin säännöllisesti tai melko säännöllisesti. Harjoittelun merkitys nousi usean teema-alueen osalta haastattelussa vahvana esille. Jokainen organisaatio toi esille, että ilman harjoittelua kyberturvallisuuden toteutumisen todentaminen, on hankalaa tai mahdotonta. Auditoinnit toivat myös osallistuvien organisaatioiden mielestä toimintaan ryhtiä ja uskottavuutta.

Kvantitatiivisesti haastattelu- ja kyselytutkimuksen aineistoa käsiteltäessä esille nousi taulukossa (Taulukko 4) luetellut 5 teemaa, jotka pääosin noudattelivat aineiston kvalitatiivisen käsittelyn tuloksia.

Taulukko 4. Kyberturvallisuuden toteutumiseen vaikuttavat sanaparit

Johdon tuki, johdon vaatimus, johdon seuranta	16
Tietoturvapolitiikka, kontrollit, sisäiset tietoturvaohjeet, auditointi	14
Asiakkaiden tai yhteistyökumppaneiden vaatimukset	13
Henkilöstön osaaminen	11
Huoltovarmuuskriittisyys	6

Suurimman mainintamäärän sai erimuodoissaan johdon tuki. Omat hallinnollisen tietoturvan- ja kyberturvallisuuden toimet saivat lukuisan määrän mainintoja. Tähän kategoriaan nousi kaikki sellaiset havainnot, joissa mainittiin politiikka, kontrollit, ohjeet, auditointi, yhteiset läpikäynnit organisaation sisällä tai omien IT-toimittajien kanssa, sekä sertifiointeihin liittyvät maininnat. Asiakkaiden ja yhteistyökumppaneiden vaatimukset toistuivat lähes yhtä monta kertaa. Tähän kategoriaan poimittiin sanat ja sanaparit, joissa toistui asiakasvaatimus, yhteistyökumppanien vaatimat velvoitteet, asiakkaan sopimusvaatimukset, sekä muut vastaavantyyppiset samaa tarkoittavat sanat tai sanaparit.

Tutkimuksen tuloksena ja vastauksena tutkimusongelmaan ”Miten ja miksi kyberturvallisuus toteutuu alihankintaketjuissa?” on haastattelu- ja kyselytutkimuksen aineiston kvalitatiivisen ja kvantitatiivisen analysoinnin perusteella seuraava:

1. **Johdon mahdollistama kyberturvallisuuden aktiivinen kehitys**

Mitä valveutuneempi johto on kyberturvallisuusasioissa, sitä varmemmin kyberturvallisuus toteutuu alihankintaketjuissa. Kun johto näkee kyberturvallisuuden liiketoiminnan mahdollistajana, ovat edellytykset kyberturvallisuuden toteutumiselle hyvät. Johto asettaa resurssit ja seuraa kyberturvallisuuden toteutumista kokonaisuutena, joko osana kokonaisturvallisuutta, tai jopa sellaisenaan. On tärkeää, että kyberturvallisuus on johdon agendalla säännöllisesti ja vuorovaikutus toimii asiantuntijasta hallitukseen. Resurssien asettamisella johto turvaa osaamisen, joka on merkittävä tekijä kyberturvallisuuden toteutumisessa. Kun johto pitää kyberturvallisuutta tärkeänä asiana, myös ihmiset

motivoituvat, hankkivat osaamista ja kouluttautuvat. Osaaminen johtaa ymmärrykseen vastuista. Vastuiden ymmärrys riittävän budjetin kautta johtaa parempaan kyberturvallisuuden johtamiseen yleisesti ja sitä kautta myös alihankintaketjujen kyberturvallisuuden johtamiseen. Kyberturvallisuus vaatii osaamista ja rahaa. Mikäli johto mahdollista molemmat, organisaatiolla on mahdollisuudet luoda käytäntöjä, prosesseja, työvälineitä ja muita tapoja, joilla kyberturvallisuutta johdetaan.

2. **Osaamisen taso ja sitoutuneisuus**

Yrityksen omilla hallinnollisilla kyberturvallisuuteen liittyvillä käytännöillä on iso merkitys. Sisäiset tietoturvapolitiikat ja -ohjeet ohjaavat arjen tekemistä vahvasti. Säännöllisyys ja selkeät vastuut auttavat siinä, että kyberturvallisuuden asiat tulevat käsitellyiksi oikealla tavalla ja oikea-aikaisesti. Näiden takana on kuitenkin ihmiset, joilla on tarvittava osaaminen hallussaan. Osaamisen tasoon ja sitoutuneisuuteen liittyy vahvasti johdon mahdollistama kyberturvallisuuden kehitys, joka olikin ensimmäinen tutkimuksen tuloksista. Hallinnolliset tietoturvan tai kyberturvan toimet eivät tule itsestään, eivätkä toteudu edes pelkällä johdon johon tuella, vaan tarvitaan myös johdon seurantaa ja aktiivista ja kiinnostunutta otetta. Sitoutunut, osaava ja asiastaan kiinnostunut kyberturvallisuuden osaajajoukko on merkittävässä roolissa organisaation kyberturvallisuuden toteutumisessa.

3. **Asiakkaiden ja yhteistyökumppaneiden vaatimukset**

Asiakkaiden ja yhteistyökumppaneiden vaatimukset ovat myös hyvin keskeinen ja merkittävä tekijä ylipäätään kyberturvallisuuden toteutumisessa, mutta myös suoraan alihankintaketjujen turvallisuuteen vaikuttava tekijä. Kyberturvallisuudesta tulee tätä kautta pakko ja selviö, jota ilman liiketoimintaa ei voi toimia tai se on hyvin riskialtista. Asiakkaiden ja yhteistyökumppaneiden vaatimuksiin vaikuttavat samat asiat kuin organisaation omiin ohjeisiin ja linjauksiin. Lait ja asetukset koskevat kaikki yrityksiä tietoturvallisuuden, tietosuojan ja kyberturvallisuuden osalta. Joillakin yrityksillä noudatettavia lakeja ja asetuksia ja säädöksiä on enemmän, johtuen toiminnan luonteesta. Asiakkaiden ja yhteistyökumppaneiden vaatimuksista löytyi huomio, joka korostaa jatkotut-

kimuksen tarvetta. On selkeä tarve eri osapuolten kouluttamiselle ja opastamiselle, mitä kyberturvallisuuden osalta kannattaa vaatia. Johdolla on myös tässä keskustelussa myös merkittävä rooli vuoropuhelussa asiantuntijoiden kanssa.

Näiden kolmen keskeisen tuloksen välisten riippuvuussuhteiden analysointi on monimutkaista ja tuloksia voidaankin ajatella useassa eri järjestyksessä.

Vaihtoehto 1. Johdon mahdollistama kyberturvallisuuden kehitys johtaa osaamisen tason ja sitoutuneisuuden nousuun ja sitä kautta asiakkaiden ja yhteistyökumppaneiden vaatimusten noudattamiseen.

Vaihtoehto 2. Organisaation kyberturvallisuuden osaaminen ja sitoutuneisuus lisää johdon tietoisuutta vastuistaan ja saa johdon mahdollistamaan kyberturvallisuuden aktiivisen kehityksen ja mahdollistaa näin asiakkaiden ja yhteistyökumppaneiden vaatimuksiin vastaamisen.

Vaihtoehto 3. Asiakkaiden ja yhteistyökumppaneiden vaatimukset saavat johdon sitoutumaan kyberturvallisuuden noudattamiseen ja mahdollistamaan organisaation kyberturvallisuuden aktiivisen kehityksen, joka johtaa osaamisen tason ja sitoutuneisuuden nousuun.

Riippuen organisaatiosta vaihtoehdot voivat toteutua missä järjestyksessä vaan. Kuitenkin organisaatioiden peruslähtökohtana on aina liiketoiminnan turvaaminen, joten taustalla on aina otettava huomioon lait ja asetukset. Tutkimukseen osallistuvissa organisaatioissa oli kussakin hieman erilainen kyberturvallisuuden historia ja kehityspolku. Tutkimukseen kuuluvassa loppukeskustelussa ja mahdollisissa jatkotapaamisissa osallistuvien organisaatioiden kesken käydään tästä aiheesta lisäkeskusteluja.

8.2 Osallistuvien organisaatioiden omat kehityshuomiot

Tutkimuksen yksi huomioista oli myös se, miten haastattelujen aikana osallistuvat yritykset tekivät havaintoja omasta toiminnastaan kertoessaan siitä haastattelijalle. Syntyi ideoita ja huomioita, joiden uskon hyödyttävän osallistuvia organisaatioita. Yksi osallistuvista organisaatioista kertoi, että jatkossa IT-

toimittajan tai yhteistyökumppanin kanssa läpikäynteihin otetaan entistä säännöllisemmin kyberturvallisuusasiat ohjausryhmän tai johtoryhmän kokouksiin. Tässäkin tapauksessa alihankintaketjujen valvonta oli muutoin erinomaisella tasolla ja muita käytäntöjä ja rutiineja oli tukemassa puuttuvaa säännöllistä kyberturvan läpikäyntiä toimittajaohjausryhmässä. Toinen osallistuva yritys lähti pohtimaan kyberturvallisuuden lisäkoulutuksen tarvetta omalle henkilökunnalleen, vaikka sitäkin työtä oli jo yrityksessä tehty määrätietoisesti ja pitkään.

Tutkimuksen haastattelujen aikana nousi myös esille muutama huomionarvoinen ja huumorinsävyttämäkin termi ja viisaus, joista molemmista kunnia kuuluu Fujitsun Tietoturvajohtaja Marko Remekselle. Ensimmäinen niistä on kybermakaroonipaketti. Tämän termin taustalla oli Remeksen ajatus siitä, että kun jotakin tapahtuu, kaikilla yrityksessä olisi tiedossa, mitä pitää tehdä, ikään kuin valmiuspaketti, kuten kotona elintarvikevarasto varmuusvarana.

Toinen Marko Remeksen esille nostama ajatus liittyi maalaisjärkeen. Remes totesi, että on maalaisjärkeen käypää huolehtia ja tulla tietoiseksi ”mitä tietoa yrityksellä on ja noudattaa mitä on sovittu”.

9 JOHTOPÄÄTÖKSET

9.1 Tuloksien ja tietopohjan vuoropuhelu

Johtopäätökset tutkimusten tulosten ja teoreettisen viitekehyksen perustella ovat selkeitä. Tiivistetysti voidaan todeta, että, kyberturvallisuus toteutuu, kun yrityksessä on tehty tietoisia päätöksiä hyvin valmisteltujen, ymmärrettävien ja esitettyjen tietojen valossa ajantasaista tilannekuvaa vasten. Tämä vaatii johdon päätöksiä, sitoutumista ja seurantaa. Keskeistä johdon osalta on mahdollistaa kyberturvallisuuden toteutuminen asettamalla asialle tarvittavat resurssit. Resurssit mahdollistavat hallinnollisen kyberturvallisuuden toteutumisen, jotka johtavat myös teknisen kyberturvallisuuden toteutumiseen ja lakien ja asetusten noudattamiseen. Asiakkaiden ja yhteistyökumppaneiden vaatimukset liittyvät suurimmaksi osaksi lakeihin ja asetuksiin. Kuten tuloksissa on todettu, jossakin organisaatioissa tämä kolmen kärjen malli voi lähteä liikkeelle eri kärjellä kuin toisessa organisaatiossa.

Tuloksia tarkastellessa on mielenkiintoista huomata, että sekä kvalitatiivisesti että kvantitatiivisesti käsitellyt aineistot tuottivat hyvin samanlaiset tulokset ja johtopäätökset. Tutkimuksessa hyödynnetty muu aineisto, haastattelu- ja kyselytutkimuksen lisänä, puoltaa näitä näkökulmia erityisesti johdon tuen osalta, sekä kyberturvallisuuden osaamisen näkökulmalta. Useissa tutkimuksissa ja julkaisuissa on myös nostettu vahvasti esille hallinnollisen tietoturvan merkitys, joista tutkimuksessakin on esimerkkeinä erilaisia viitekehyksiä ja standardeja. Erilaisissa viitekehyksissä, standardeissa ja sertifikaateissa, nostetaan esille kolmannen osapuolen johtaminen. Pelkästään hallinnolliset kyberturvallisuuden toimet eivät myöskään riitä, vaan tarvitsevat rinnalleen teknisiä toimia. Tutkimuksen tietoperustassa esitetyistä laista ja asetuksista löytyy myös useita velvoitteita alihankintaketjujen kyberturvallisuudesta huolehtimiseen.

9.2 Tutkimushypoteesien tarkastelu

Tutkimuksessa asetettiin kolme tutkimushypoteesia. Ensimmäisenä hypoteeseina oli, että kyberturvallisuuden toteutumiseen alihankintaketjuissa vaikuttaa merkittävissä määrin huoltovarmuuskriittisyys. Toinen hypoteesi oli johdon tuen suuri merkitys ja kolmas hypoteesi painotti kyberlähettiläinen keskeistä roolia organisaatiossa.

Hypoteesit osoittautuivat suurimaksi osaksi oikeiksi. Johdon tuella on iso rooli kyberturvallisuuden toteutumisen varmistamisessa, ja kyberlähettiläät edustavat osittain tutkimuksessa esille noussutta vahvaa osaamisasiaa. Huoltovarmuuskriittisyys ei sen sijaan noussut kovin vahvana esille, mutta se linkittyy vahvasti lakiin ja asetuksiin ja osoittautuu hypoteesina siltä osin oikeaksi.

10 POHDINTA

10.1 Onnistumiset ja kehityskohteet

Tutkimus vastasi tutkimusongelmaan ja tutkimuksen tietopohja tuki työtä. Osallistuvien yritysten kanssa yhteydenpito oli sujuvaa ja niin viralliset kuin vapaamuotoiset keskustelutkin mielenkiintoisia. Aineistoa oli melko kattava määrä ja siitä sai hyvin johdettua tulokset. Kehityskohteina tutkimuksen osalta nousi selvästi kaksi asiaa. Näistä ensimmäinen oli ajankäyttö. Tutkimukseen

osallistuvien yritysten valitsemiseen meni liikaa aikaa. Moni organisaatio oli kiinnostunut, mutta lopulta aikataulusyistä tai aiheen luottamuksellisuuden vuoksi ei lähtenyt mukaan. Tämä viivästytti tutkimuksen etenemistä ja aiheutti aikataulupainetta. Tutkimuksen suorittaminen myöhästyi kuitenkin vain joitakin kuukausia, eikä sillä ollut lopputuloksiin juurikaan vaikutusta. Toisena kehityskohteena nousee esille työn rajaamisen haasteet. Mikäli aikaa olisi ollut käytössä enemmän, olisi tutkimusta voinut laajentaa käyden kansainvälisiä tutkimuksia laajemmin läpi, mikä olisi lisännyt työn luotettavuutta ja tuonut työlle vielä enemmän lisäarvoa. Myös haastattelu- ja kyselytutkimus olisi voinut olla laajempi, vastaten vielä paremmin tutkimuskysymyksiin.

10.2 Tutkimuksen luotettavuus

Tutkimuksen luotettavuutta on pyritty vahvistamaan käyttämällä monimenetelmäistä tapaustutkimusta ja valitsemalla hyvin erityyppisiä yrityksiä alihankintaketjujen eri kohdista mukaan. Myös aineistoa on käsitelty usealla tavalla. Tutkimuksessa toteutui aineistotriangulaatio sekä menetelmätriangulaatio. Aineistossa on käytetty olemassa olevaa aiheeseen liittyvää materiaalia sekä haastattelusta ja kyselystä saatuja aineistoja. Menetelmätriangulaatio toteutuu myös, sillä tiedon hankinnassa ja analysoinnissa on yhdistetty eri menetelmiä, joskin kvantitatiivinen analyysi aineistolle on hyvin suppea. Teoriatriangulaatio olisi ollut myös erittäin mielenkiintoinen ja varteen otettava tämän tutkimuksen osalta, mutta sitä ei tämän tutkimuksen osalta tehty. Mahdollisia jatkotutkimuksia silmällä pitäen nämä keinot on hyvä pitää mielessä, sillä triangulaatiolla voidaan lisätä merkittävästi tutkimuksen luotettavuutta. Tutkimuksessa suojattiin osallistuvien yritysten osalta anonymiteetti luotettavasti, eikä huolta noussut tämän osalta esille myöskään tutkimuksen valmistuttua.

Tutkimuksen luotettavuuden kannalta kehityskohteena nousee tutkijan oman roolin vaikutus tutkimukseen. Tutkija toimii tietohallintojohtajana ja vastaa yhden osallistuvan yrityksen osalta myös kyberturvallisuudesta. Haastateltava henkilö työskentelee tutkijan vetämässä yksikössä. Toisen osallistuvan yrityksen osalta tutkija toimii mahdollisen palveluja hankkivan roolissa, joskin tutkimuksen haastattelujen toteutushetkellä ei ollut käynnissä mitään tuotteiden tai palvelujen hankintaan liittyviä yhteisiä asioita. Kolmannen osallistuvan yrityksen osalta tutkijalla ja yrityksellä ei ole mitään sidettä keskenään. Toisena

pohdittavana asiana nousee esille tutkijan oman kiinnostuksen ja osaamisen vaikutus tutkimustuloksiin. On mahdollista, että tutkija teki myös vääriä johtopäätöksiä omasta kokemuspohjastaan ja näkemyksistään johtuen. Muihin kuin tutkijaan liittyviä kehityskohteita luotettavuuden osalta ovat mahdollisesti laajemman aineiston kvantitatiivisen analyysin tekeminen, sekä tasaisempi haastattelu- ja kyselytutkimusten jakaantuminen tutkimuskysymysten ympärille.

Tutkimuksen luotettavuuden kannalta myös laajempi aineistohaku olisi voinut tuottaa hyviä huomioita tutkimukseen ja lisätä sen luotettavuutta. Monimenetelmäinen tapaustutkimus on kuitenkin näinkin laajan tutkimusongelman osalta melko työläs, joten tässä tutkimuksessa oli järkevää rajata aineisto suppeammin.

10.3 Jatkotutkimusideat

Kyberturvallisuuden toteutuminen alihankintaketjuissa on melko vähän tutkittu, mutta sitäkin tärkeämpi kyberturvallisuuden osa-alue. Tutkimusten tulosten ja aiempien tutkimuksien perusteella voidaan löytää useita jatkotutkimusmahdollisuuksia. Jatkotutkimuksista saman aiheen osalta olisi järkevää jatkaa, käyttäen mahdollisesti muita tutkimusstrategioita ja -menetelmiä.

Tutkimuksen laajentaminen koskemaan kattavampaa joukkoa huoltovarmuuskriittisten organisaatioiden eri sektoreilla voisi olla yksi vaihtoehto. Lisäksi vastaavantyyppisen tutkimuksen suuntaaminen pk-sektorille voisi tuoda arvokasta ja erilaista tietoa verrattuna tähän tutkimukseen. Tutkimusjoukon laajentamisen ja rajaamisen lisäksi jatkotutkimukset voisivat kohdentua tämän tutkimuksen tulosten ympärille. Esimerkiksi johdon tuen tarkempi tarkastelu kyberturvallisuuden toteutumisen yhtenä tekijänä voisi olla jo pelkästään yksinäänkin jatkotutkimuksen kohde. Erilaisia viitekehyksiä ja standardeja kyberturvallisuuden määrittelyyn ja mittaamisen löytyy paljon. Niiden ymmärtäminen ja käyttömukavuus voi vaihdella organisaation kyberturvallisuuden osaamisen tason vuoksi paljonkin. Jatkotutkimuksissa olisi sijaa myös toiminnan kehittämisen tutkimuksille tällä alueella. Voisiko joku yksinkertaisempi ohjeistus ja malli tuoda enemmän lisäarvoa ja nostaa yritysten kyberturvallisuuden tasoa nopeammin ja tehokkaammin? Jatkotutkimusaiheena voisi hyvin olla myös kyberturvallisuuden toteutumisen virallisen määritelmän pohtiminen.

Tapaustutkimusta kritisoidaan joskus siitä, ettei sen avulla voida tehdä yleistyksiä. Tapaustutkimuksen avulla voidaan kyllä tuottaa teoreettisia yleistyksiä, mutta tärkein tapaustutkimuksen tarkoitus on täsmentävän tiedon tuottaminen valitusta aiheesta käyttäen tapauksia apuna. Teoriaa kehittävät tapaustutkimukset perustuvat usein enemmän kuin yhteen tapaukseen ja niiden järjestelmälliseen vertailuun. (Eriksson ym. 2005.)

Tämä tutkimus lähti liikkeelle tavoitteesta tuottaa uutta teoriaa valitsemalla tutkimukseen riittävä määrä tapauksia (osallistuvat organisaatiot), käyttämällä erilaisia tutkimusmenetelmiä, riittävää tietoperustaa ja huolellista aineiston käsittelyä ja analysointia. Tutkijan mielestä tämä tavoite onnistui ja jatkotutkimusmahdollisuudet ovat laajat.

LÄHTEET

Bergström, G. & Ericson, A. 2021. Coop-butiker stängs efter it-attack. Aftonbladet. WWW-dokumentti. Saatavissa: https://www.aftonbladet.se/minekonomi/a/86bQQw/coop-butiker-stangs-efter-it-attack [viitattu 11.8.2023]

CCDCOE. (s.a.). NATO Cooperative Cyber Defence Centre of Excellence. WWW-dokumentti. Saatavissa: https://ccdcoe.org/library/strategy-and-governance/ [viitattu 9.8.2023]

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. 2022. Who cares? Supply chain manager's perceptions regarding cyber supply chain risk management in the digital transformation era. WWW-dokumentti. Saatavissa: https://www.emerald.com/insight/content/doi/10.1108/SCM-02-2020-0073/full/pdf?title=who-cares-supply-chain-managers-perceptions-regarding-cyber-supply-chain-risk-management-in-the-digital-transformation-era [viitattu 26.7.2023]

Cybernews. 2021. An in-depth analysis of the Kaseya ramsomware attach: here's what you need to know. WWW-dokumentti. Saatavissa: https://cybernews.com/security/kaseya-ransomware-attack-heres-what-you-need-to-know/ [viitattu 12.8.2023]

Digi- ja väestötietovirasto (s.a.) WWW- dokumentti. Mitä on digiturva? Saatavissa: https://dvv.fi/mita-on-digiturva [viitattu 13.8.2023]

Enisa. 2022. Threat landscape 2022. WWW-dokumentti. Saatavissa: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [viitattu 8.8.2023]

Eriksson, P. & Koistinen, K. 2005. Monenlainen tapaustutkimus. Kuluttajatutkimuskeskus. PDF-dokumentti. Saatavissa: https://helda.helsinki.fi/server/api/core/bitstreams/a8adc2c5-9541-449d-88f9-72e97cf60a7a/content [viitattu 26.7.2023]

EUR-Lex. 2022. DORA 2022. WWW-dokumentti. Saatavissa: EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu) [viitattu 29.1.2023]

EUR-Lex. 2022. NIS2. WWW-dokumentti. Saatavissa: https://eur-lex.europa.eu/eli/dir/2022/2555 [viitattu 29.1.2023]

Finanssivalvonta. 2021. Työttömyyskassoja koskevat määräykset ja ohjeet. PDF-dokumentti: Saatavissa: https://www.finanssivalvonta.fi/globalassets/fi/saantely/maarayskokoelma/2021/03_2021/3_2021.m1.pdf [viitattu 12.6.2023]

Fox, J. 2022. EU Cyber Resilience Act: Good for Software Supply Chain Security, Bad for Open Source? WWW- dokumentti. Saatavissa: https://sonatype.com [viitattu 12.6.2023]

Hirsjärvi, S. & Hurme, H. 2008. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino [viitattu 29.1.2023]

Huoltovarmuuskeskus. 2021.Digitaalinen turvallisuus 2030. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/huoltovarmuuskeskus/4962-2/digitaalinen-turvallisuus-2030 [viitattu 29.1.2023]

Huoltovarmuuskeskus. 2023. Toimialat. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/toimialat [viitattu 29.1.2023]

Huoltovarmuuskeskus. 2023. Tietoa huoltovarmuudesta. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta [viitattu 29.1.2023]

IISP. 2010. Information security skills framework. PDF-dokumentti. Saatavissa: https://apmg-international.com/sites/default/files/documents/products/iisp_skills_framework_v1_0.pdf [viitattu 29.1.2023]

Julkisten hankintojen neuvontayksikkö. 2021. Alihankinta. WWW-dokumentti. Saatavissa: https://www.hankinnat.fi/eu-hankinta/ehdokkaiden-ja-tarjoajien-sovel-tuvuus/alihankinta [viitattu 29.1.2023]

Jyväskylän Yliopisto. 2014. Aineistonhankintamenetelmät. WWW-dokumentti. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/johdanto [viitattu 29.1.2023]

Jyväskylän Yliopisto. 2015. Tapaustutkimus. WWW-dokumentti. Muokattu 23.4.2015. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/tapaustutkimus [viitattu 29.1.2023]

Järvinen, H. 2020. Kyberturvallisuuden nykyiset ja tulevat osaamistarpeet ohjelmistoyrityksessä -tapaustutkimus. Saatavissa: https://jyx.jyu.fi/bitstream/handle/123456789/69152/URN%3aNBN%3afi%3ajyu-202005253405.pdf?sequence=1&isAllowed=y [viitattu 29.1.2023]

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Jyväskylä: Docento. [viitattu 29.1.2023]

Kansallinen turvallisuusviranomainen. 2020. Saatavissa: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246 [viitattu 29.1.2023]

Kasvi, J. 2016. Kyberturvallisuus koskettaa meitä jokaista. PDF-dokumentti. Saatavissa: https://www.slideshare.net/JyrkiKasvi/kyberturvallisuus-koskettaa-meit-jokaista [viitattu 29.1.2023]

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä. Suomen Yliopistopaino - Juvenes Print. [viitattu 12.7.2023]

Kyberturvallisuuskeskus. 2022. Hyväksytyt tietoturvallisuuden arviointilaitokset. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset [viitattu 29.1.2023]

Kyberturvallisuuskeskus. 2023.Teletoiminnan tutkintaesimerkkejä. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/teletoiminnan-tulkintaesimerkkeja?toggle=1.2%20Alihankinta [viitattu 29.1.2023]

Laaksonen, M. 2018. Kyberturvallisuus kuuluu johdon agendalle. PDF-dokumentti. Saatavissa: https://dif.fi/wp-content/uploads/2018/06/BV-1-2018-Mika-Laaksonen-Kyberturvallisuus-kuuluu-kaikille.pdf [viitattu 29.1.2023]

Laine, M., Bamberg, J. & Jokinen, P. 2018. Tapaustutkimuksen taito. 3.painos. Helsinki: Unigrafia Oy. [viitattu 29.1.2023]

Lehto, M, & Kähkönen, A. 2015. Kyberturvallisuuden kansallinen osaaminen. Informaatioteknologian tiedekunnan julkaisuja No.20/2015. PDF-dokumentti. Jyväskylä: Jyväskylän Yliopistopaino. Saatavissa: http://urn.fi/URN:ISBN:978-951-39-6105-3 [viitattu 20.8.2023]

Lehto, M., Limnell, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. PDF- dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-287-368-2 [viitattu 16.8.2023]

Liikenne- ja viestintäministeriö. 2021. Kyberturvallisuuden kehittämisohjelma. WWW dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163219/LVM_2021_7.pdf [viitattu 29.1.2023]

Liikenne- ja viestintäministeriö. 2022. Valtioneuvostolta tukea yritysten tietoturvan kehittämiseen. WWW dokumentti. Saatavissa: https://valtioneuvosto.fi/-/valtioneuvostolta-tukea-yritysten-tietoturvan-kehittamiseen [viitattu 29.1.2023]

NIST. 2017. Cyber supply chain risk management (C-SCRM). WWW-dokumentti. Saatavissa: https://csrc.nist.rip/scrm/ [viitattu 22.8.2023]

NIST. (n.d.). Guidance on Supply Chain Security, under EO 14028 Section 4c-4d. WWW- dokumentti. Saatavissa: https://www.nist.gov [viitattu 12.6.2023]

NIST. 2021. Key Practices in Cyber Supply Chain Risk Management. PDF-dokumentti. Saatavissa: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf [viitattu 12.6.2023]

NIST. 2023. The NIST Cybersecurity Framework 2.0. WWW- dokumentti. Saatavissa: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd [viitattu 13.6.2023]

Nixu. 2022. Cybersecurity Index 2022. PDF-dokumentti. Saatavissa: https://www2.nixu.com/NIXU_Cybersecurity_Index_Report_2022.pdf [viitattu 15.8.2023]

Palonen, O. 2019. Kyberturvallisuuden johtaminen Virossa, Israelissa ja Alankomaissa – mitä voimme oppia? Jyväskylän Yliopisto. Tietojenkäsittelytieteiden laitos. Pro gradu -työ. PDF-dokumentti. Saatavissa: https://jyx.jyu.fi/bitstream/handle/123456789/65430/1/URN%3ANBN%3Afi%3Ajyu-201909064032.pdf [viitattu 11.8.2023]

SFS. 2022. ISO/IEC 27000 Tietoturvallisuuden standardisarja. Suomen standardisoimisliitto SFS. WWW-dokumentti. Saatavissa: https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/ [viitattu 11.8.2023]

Seppänen, P. 2022. Tietoisuuden ja tiedon nelikenttä. WWW-dokumentti. Saatavissa: https://millog.fi/varmistamalla-kyberturvallisuden-varmistat-yritystoiminnan-jatkuvuuden/ *[viitattu 25.7.2023]*

Sisäministeriö. 2023. Selvitys: Suomen kyberturvallisuutta tulee kehittää määrätietoisesti, viranomaisten yhteistyötä ja prosesseja tulee edelleen parantaa. WWW-dokumentti. Saatavissa: https://intermin.fi/-/selvitys-suomen-kyberturvallisuutta-tulee-kehittaa-maaratietoisesti-viranomaisten-yhteistyota-ja-prosesseja-pitaa-edelleen-parantaa [viitattu 25.7.2023]

Solfa, D. 2022. Impacts of cyber security and supply chain risk on digital operations: evidence from the UAE pharmaceutical industry. WWW-dokumentti. Saatavissa: http://sedici.unlp.edu.ar/bitstream/handle/10915/152337/Documento_completo.pdf?sequence=1 [viitattu 25.7.2023]

Suojelupoliisi. 2021. Kolumni: Onko organisaatiosi suojautunut toimitusketjuhyökkäyksiltä? Saatavissa: https://supo.fi/-/kolumni-onko-organisaatiosi-suojautunut-toimitusketjuhyokkaykselta-nailla-vinkeilla-paaset-alkuun [viitattu 25.7.2023]

Suomen puolustusvoimilla voisi olla kyberjoukot. 2014.Verkkolehti. MTV. 8.12.2014. Saatavissa: https://www.mtvuutiset.fi/artikkeli/professori-suomen-puolustusvoimilla-voisi-olla-kyberjoukot/4592080#gs.nxkbb2 [viitattu 29.1.2023]

Teknologiateollisuus. 2023. Alihankkijat- toimialaryhmä. WWW-dokumentti. Saatavissa: https://teknologiateollisuus.fi/fi/teknologiateollisuus/toimialaryhmat/alihankkijat-toimialaryhma [viitattu 1.8.2023]

Tietosuojavaltuutetun toimisto. 2023. WWW-dokumentti. Saatavissa: https://tietosuoja.fi/aineiston-havittaminen-anonymisointi-tai-arkistointi-tutkimuksen-paattyessa [viitattu 6.8.2023]

Tilastokeskus. 2023. WWW-dokumentti. Saatavissa: https://www.tilastokeskus.fi/tup/suoluk/suoluk_yritykset.html [viitattu 1.8.2023]

Traficom. 2020.Kyberturvallisuus ja yrityksen hallituksen vastuu. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf [viitattu 29.1.2023]

Traficom. 2021. Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta. PDF-dokumentti. Saatavissa: https://www.traficom.fi/sites/default/files/media/publication/Teko%C3%A4lyn%20soveltamisen%20kyberturvallisuus%20ja%20riskienhallinta.pdf [viitattu 13.8.2023]

Trochim, W. 2006. Hypotheses. Research Methods Knowledge Base. Saatavissa: http://www.socialresearchmethods.net/kb/hypothes.php [viitattu 15.8.2023]

Tuomi, J. & Sarajärvi, A. 2004. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi. [viitattu 29.7.2023]

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. PDF-dokumentti. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf [viitattu 29.1.2023]

Turvallisuuskomitea. 2019. Suomen kyberturvallisuusstrategia. PDF-dokumentti. Päivitetty 3.10.2019. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf [viitattu 29.1.2023]

Ulkoministeriö. 2020. Katakri 2020. Tietoturvallisuuden auditointityökalu viranomaisille. Traficomin julkaisusarja 232/2020. PDF-dokumentti. Saatavissa: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246 [viitattu 11.8.2023]

Valtioneuvosto. 2019. Suomen kyberturvallisuusstrategia. PDF-dokumentti. Saatavissa: Suomen kyberturvallisuusstrategia 2019 (valtioneuvosto.fi) [viitattu 11.8.2023]

Valtiovarainministeriö. 2020. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka). PDF-dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162191/VM_2020_33.pdf?sequence=1&isAllowed=y [viitattu 29.1.2023]

Valtionvarainministeriö. 2020. Digitaalisen turvallisuuden kansainvälinen vertailu. Saatavissa: https://vm.fi/documents/10623/307681/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu/7aafe82e-86e7-7450-358c-f1adfeecb3e5/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu.pdf [viitattu 29.1.2023]

Vehkalahti, K. 2014. Kyselytutkimuksen mittarit ja menetelmät. WWW-dokumentti. Saatavissa: https://helda.helsinki.fi/server/api/core/bitstreams/bc1c2c8a-0eb8-4881-ba8f-510ce386b810/content *[viitattu 13.8.2023]*

Vilkka, H. 2007. Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Saatavissa: https://trepo.tuni.fi/bitstream/handle/10024/98723/Tutki-ja-mittaa_2007.pdf?sequence=1&isAllowed=y *[viitattu 29.1.2023]*

Vilkka, H. 2005. Tutkimusmenetelmiä ammattilaiselle kentälle. WWW-dokumentti. Saatavissa: http://hanna.vilkka.fi/wp-content/uploads/2014/02/Tutki-ja-kehit%C3%A4.pdf [viitattu 29.6.2023]

Vuori, J. Tapaustutkimus. 2015. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/kvaliohjeet/#Viittausohje *[viitattu 29.1.2023]*

World Economy Forum. 2022. PDF-dokumentti. Saatavissa: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf *[viitattu 8.8.2023]*

YTK. 2023. WWW sivut. Saatavissa: https://ytk.fi/tietoa-meilta/tietoa-meista [viitattu 29.1.2023]

Yrittäjäjärjestö. 2023. WWW-sivut. Saatavissa: https://www.yrittajat.fi/yrittajajarjesto/tietoa-yrittajista/yrittajyys-suomessa/ [viitattu 29.1.2023]

Liite 1

Haastattelukysymykset

Taustakysymykset

Onko organisaationne huoltovarmuuskriittinen?

Mihin huoltovarmuuskriittisyyden osa-alueeseen toimintanne kuuluu? (esimerkiksi finanssiala tai energiahuolto)

Kuinka monta henkilöä organisaationne työllistää?

Tunnistatteko toiminnassanne riippuvuuksia alihankintaketjuihin?

1. Milloin ja miten yrityksenne kyberturvallisuustietoisuus sai alkunsa? /Mitkä tekijät ovat vaikuttaneet yrityksenne kyberturvallisuustietoisuuteen? (TAUSTA)
2. Onko organisaatiossanne ns. kyberturvallisuuslähettilästä, jolla ollut erityinen rooli kyberturvallisuuden tason kasvamisessa? (IHMISET)
3. Onko kyberturvallisuus johdon ja hallituksen säännöllisissä läpikäynneissä mukana? (HALLINTO)
4. Näkyykö kyberturvallisuus sopimuksissa saakka? (omat toimittajat sekä asiakkaanne) (SOPIMUKSET)
5. Onko teknisen/ hallinnollisen kyberturvallisuuden osaajat omaa henkilökuntaa vaiko ulkoistettuja osaajia tai niiden kombinaatio? (IHMISET, OSAAMINEN)
6. Osaisitteko nimetä yksittäisen kyberturvallisuutta parantavan asian? (OSAAMINEN)
7. Onko varautuminen ja jatkuvuus asteikolla 1–10, kuinka tärkeää yritykselle ja miksi? (TAUSTA)
8. Harjoitteletteko säännöllisesti erilaisten kybertapahtumien varalta? (HARJOITTELU)
9. Mitä ajattelette kyberturvallisuudesta, sen tärkeydestä, vastuusta ja tulevaisuudesta (OSAAMINEN)
10. Onko alihankintaketjut tunnistettu osittain, suurimmaksi osaksi tai kaikki? (OSAAMINEN)

11. Käyttekö tai teettekö säännöllisesti, satunnaisesti tai ei ollenkaan läpi alihankintaketjujen sopimuspykäliä, konkreettisia tarkistuksia tai auditointeja? (SOPIMUKSET)

12. Vaativatko /kysyvätkö asiakkaanne alihankintaketjujen turvallisuudesta (vain BtoB)? (VAATIMUKSET)

Liite 2

Kyselytutkimus

Taustakysymykset

Onko organisaationne huoltovarmuuskriittinen?

Mihin huoltovarmuuskriittisyyden osa-alueeseen toimintanne kuuluu?

Kuinka monta henkilöä organisaationne työllistää?

Tunnistatteko toiminnassanne riippuvuuksia alihankintaketjuihin?

Kyberturvallisuus (Kyllä /Ei)

1. Osaisitko määritellä mitä kyberturvallisuus tarkoittaa?
2. Onko organisaatiossanne selvää, kuka vastaa eri tasoilla kyberturvallisuudesta?
3. Onko kyberturvallisuusasioita käsitelty hallituksessanne viimeisen vuoden aikana?
4. Vaativatko /velvoittavatko asiakkaanne tai osa asiakkaista, teiltä raportointia kyberturvallisuusasioista?
5. Onko rekisterinpitäjyys ja alikäsittelijänä toimiminen tuttuja asioita teille tai edustamallenne organisaatiolle?

Kyberturvallisuus (sanalliset vastaukset)

1. Oletteko käyttäneet jotakin työkaluja kyberturvallisuuden tasonne arviointiin? jos olette niin mitä? (TAUSTA, TYÖKALUT)

2. Jos teidän pitäisi nimetä 5 tärkeintä asiaa, joilla on ollut merkitys kyberturvallisuuden tasoon yrityksessänne, mitä ne olisivat? (esimerkkeinä: henkilöstön osaaminen, lainsäädäntö, vaatimukset asiakkailta, yrityksenne hallituksen vaatimukset, julkisen keskustelun paine, hyvien työkalujen myötä tullut ymmärryksen lisäys, jne) (OSAAMINEN, HARJOITTELU, HALLINTO, SOPIMUKSET)

3. Onko kyberturvallisuudelle määritelty oma budjetti? (älä mainitse tähän euromääräisiä arvioita). Mikä budjetin suuruuteen on vaikuttanut eniten? (esimerkiksi: tietoisuus, sattuneet kyberturvallisuutta vaarantaneet tapahtumat, yrityksen hallituksen vaatimus, jonkun yksittäisen ihmisen rooli budjetin laadinnassa? jne.) (TAUSTA)

4. Käytättekö kyberturvallisuuden osaamisen lisäämisessä ulkopuolista apua? esimerkiksi koulutuksia, kohdennettuja palveluostoja jne. Luetelkaa käyttämänne keinot. (IHMISET, OSAAMINEN)

5. Miten määrittelette kyberturvallisuuden tasonne? Tapahtuuko se työkalujen avulla, onko se oma arvio vai hyödynnättekö jotakin muuta menetelmää? (VAATIMUKSET, TYÖKALUT)

6. Kuinka hyvin mielestänne toimitusketjuissanne tunnistetaan vastuut ja velvoitteet kyberturvallisuuden osalta ja miksi? (OSAAMINEN, SOPIMUKSET)

7. Mikä on mielestänne paras keino valvoa kyberturvallisuuden toteutumista alihankintaketjuissa? käytättekö sitä säännöllisesti tai edes satunnaisesti? (OSAAMINEN, SOPIMUKSET)

8. Miksi kyberturvallisuuden toteutumista alihankintaketjuissa on syytä valvoa ja johtaa, jos on? (OSAAMINEN)

9. Millaisia ohjeita tai tukea kaipaisitte yrityksille kyberturvallisuusasioissa? (TYÖKALUT)