Markus Savolainen

”Kaikki tietää että se on semmoinen villi länsi tuo netti vielä”

Narratiivinen tutkimus kyberturvallisuuskulttuurista kaupungin hallinto-organisaatiossa

Pro gradu - tutkielma

Hallintotiede

2022

Lapin yliopisto, yhteiskuntatieteiden tiedekunta

Työn nimi: ”Kaikki tietää että se on semmoinen villi länsi tuo netti vielä” – Narratiivinen tutkimus kyberturvallisuuskulttuurista kaupungin hallinto-organisaatiossa

Tekijä: Markus Savolainen

Koulutusohjelma/oppiaine: Hallintotiede

Työn laji: Pro gradu -tutkielma/Maisteritutkielma_x_ Lisensiaatintutkimus__

Sivumäärä: 120

Vuosi: 2022

Tiivistelmä:

Tämän tutkielman tarkoituksena on kuvailla, millä tavoin kyberturvallisuuskulttuuria ilmentävät inhimilliset piirteet näkyvät tutkielman kohteena olevan organisaation henkilöstön toiminnassa ja asenteissa, sekä toisaalta tarkastella organisaatiokulttuurin ja toimintaympäristön vaikutusta kyberturvallisuuskulttuuriin.

Tutkielmassa kyberturvallisuuskulttuuria ja sen rakentumista organisaatioissa tarkastellaan ihmiskeskeisesti keskittyen ei-teknologisiin tekijöihin, jotka ovat yhteydessä tietoturvan toteutumiseen organisaatioissa. Tutkielman teoreettinen tausta rakentuu kyberturvallisuuskulttuurin, organisaatiokulttuurin ja tietoturvakulttuurin rajapinnoille, hyödyntäen poikkitieteellistä tutkimusta. Kyberturvallisuuskulttuurin avulla voidaan vaikuttaa käyttäjien kautta syntyviin tietoturvauhkiin ja parantaa organisaation suojautumista kyberuhkilta. Aihepiiriä ei tiettävästi ole tutkittu aikaisemmin Suomessa julkisissa organisaatioissa.

Tutkielman aineisto koostuu kahdeksasta kaupunkiorganisaatiosta kerätystä teemahaastattelusta, joita on analysoitu temaattisen narratiivisen analyysin keinoin. Tutkielmassa kysytään: “Millaiset tekijät ja käsitykset ovat vaikuttaneet kyberturvallisuuskulttuurin olemukseen organisaatiossa?”

Tutkielman tulokset tukevat käsitystä siitä, että inhimilliset tekijät on tärkeää huomioida organisaation kyberturvallisuutta kehitettäessä. Merkittäviä kyberturvallisuuskulttuuriin vaikuttavia tekijöitä olivat esimerkiksi tietoisuus, aiemmat kokemukset, sekä henkilö- että ryhmäkohtaiset asenteet ja organisaation julkishallinnollinen toimintaympäristö ja luonne. Narratiivinen tutkimus mahdollistaa kyberturvallisuuskulttuurille annattavien subjektiivisten merkitysten syvemmän ymmärtämisen ja siten paremman ymmärryksen kyberturvallisuuskulttuurista.

Avainsanat: kyberturvallisuus, kyberturvallisuuskulttuuri, organisaatiokulttuuri, narratiivinen tutkimus

SISÄLLYSLUETTELO

SISÄLLYSLUETTELO 3

KUVIOT 4

1 JOHDANTO 5

1.1 Tutkielman tausta ja lähtökohdat 5

1.2 Tutkielman tavoite 8

1.3 Aiempi tutkimus 10

1.4 Tutkielman rakenne 13

2 KULTTUURI JA KYBERTURVALLISUUS – KULTTUURIN VAIKUTUS ARVOIHIN JA KÄYTTÄYTYMISEEN . 15

2.1 Kulttuurin käsite ja mallit 15

2.2 Organisaation kulttuurit ja niiden merkitys turvallisuuteen ja käyttäytymiseen 20

2.2.1 Organisaatiokulttuuriparadigma 20

2.2.2 Organisaatiokulttuuri 23

2.2.3 Julkishallinnollisen organisaation erityispiirteet 26

2.3 Kulttuurin tasojen, arvojen, asenteen ja käyttäytymisen suhde 27

2.3.1 Turvallisuus- ja tietoturvakulttuuri 33

2.4 Kyberturvallisuuskulttuuri 39

3 NARRATIIVISUUS LÄHESTYMISTAPANA ORGANISAATIOTUTKIMUKSESSA 44

4 TUTKIMUSAINEISTO JA MENETELMÄT 49

4.1 Tutkimuskontekstina kuntaorganisaatio 49

4.2 Tutkimusmenetelmänä laadullinen tutkimus 50

4.3 Aineistonkeruumenetelmänä teemahaastattelu 51

4.3.1 Teemahaastatteluiden toteutus 53

4.4 Narratiivinen temaattinen analyysi 55

4.4.1 Aineiston analyysin käytännön toteutus narratiivisen temaattisen analyysin keinoin 58

4.5 Tutkielman eettisyys ja tutkijapositio 61

5 TARINOITA KYBERTURVALLISUUDESTA 64

5.1 Kyberturvallisuuden monet kasvot – narratiivi henkilökohtaisesta kyberturvallisuuskulttuurista 64

5.1.1 Tyyppitarinat henkilökohtaisesta kyberturvallisuuskulttuurista 65

5.2 No me ollaan kuitenkin kuntaorganisaatio – narratiivi organisaatiokulttuurista ja toimintaympäristöstä 74

5.2.1 Tyyppitarinat organisaatiokulttuurista ja toimintaympäristöstä 74

5.3 Narratiivi kyberturvallisuuskulttuurista 81

5.3.1 Tyyppitarinat organisaation kyberturvallisuuskulttuurista 81

6 YHTEENVETO JA KESKUSTELU 93

6.1 Yhteenveto 93

6.1.1 Henkilökohtaisten tekijöiden ja käsitysten vaikutus organisaation kyberturvallisuuskulttuuriin 94

6.1.2 Organisaatiokulttuurin ja toimintaympäristön vaikutus kyberturvallisuuskulttuuriin 98

6.2 Tutkielman kontribuutio ja luotettavuuden arviointi 101

6.3 Jatkotutkimusehdotukset 105

7 LÄHDELUETTELO 107

8 LIITTEET 121

KUVIOT

Kuvio 1. Kulttuurin sipulimalli (mukaillen Hofstede ym., 2010). 18

Kuvio 2. Edgar H. Scheinin (2004) mukaiset kulttuuritasot. 19

Kuvio 3. Arvojen ja käytäntöjen tasapaino kulttuurin eri tasoilla (mukaillen Hofstede, 2010; Karahanna ym., 2005). 29

Kuvio 4. Teoreettinen malli käyttäytymiseen vaikuttavista tekijöistä (mukaillen Karahanna ym., 2005)..... 30

Kuvio 5. Organisaatiokulttuurin ja tietoturvakulttuurin tasot ja esiintyminen Scheinin (2004) mukaisesti (mukaillen Van Niekerk & Von Solms, 2006; 2010). 37

Kuvio 6. Kyberturvallisuuskulttuurin tasot (mukaillen Da Veiga, 2016) 42

1 JOHDANTO

1.1 Tutkielman tausta ja lähtökohdat

Kyberturvallisuudesta on tullut merkittävä ilmiö yhteiskunnissa viimeisen kymmenen vuoden aikana. Luonnonilmiöt ja -katastrofit ovat yhteiskunnalle jo tuttuja, ja niiden hallitsemiseksi ja torjumiseksi on kehitetty erilaisia toimintatapoja sekä lainsäädäntöä. Digitalisaation myötä yhteiskuntia koetelleet erilaiset katastrofit ovat kuitenkin viimeisen kahdenkymmenen vuoden saaneet rinnalleen digitaalisen maailman vastineen, kyberkatastrofin. Kyseessä on merkittävä yhteiskunnallinen muutos, jonka perustavanlaatuisia vaikutuksia olemme päässeet todistamaan vasta viimeisten vuosien aikana. Digitalisaatio on tarkoittanut digitaalisen tiedonkäsittelytekniikan käyttöönottoa jokaisella yhteiskunnan osa-alueella, joka on puolestaan auttanut tehostamaan yhteiskunnan kannalta keskeisiä asioita kuten työtä ja hallintoa. Toisaalta se on tarkoittanut myös perinteisten uhkakuvien muuttumista digitaaliseen maailmaan sopiviksi. Digitalisaatio ei tarkoita pelkästään sitä, että yhä useampi asia hoidetaan tietoteknisten välineiden avulla, vaan myös hallinto- ja organisaatiorakenteiden muuttumista. Yhteiskunnan palvelut ja prosessit ovat sähköistyneet, uudet palvelut suunnitellaan alusta alkaen pelkästään tietokoneiden välityksellä suoritettaviksi ja organisaatioissa työn apuna käytetään entistä enemmän digitaalisia työkaluja.

Elinkeinoelämän tutkimuslaitoksen tutkimuksen mukaan kyberuhkien tilannekuva on mullistunut lyhyessä ajassa. Poliisin tietoon tullut kyberrikollisuus on kasvanut voimakkaasti varsinkin tietomurtojen osalta, joiden lukumäärä on yli tuplaantunut kahdessa vuodessa. Lisäksi suomessa kyberturvallisuusongelmia kokeneiden yritysten määrä oli keskiarvoltaan muita EU-maita hieman korkeampi. Lähes joka kuudes suomalainen suuryritys on joutunut tietovuodon kohteeksi. (Mattila, Ali-Yrkkö & Seppälä, 2020.) Hyökkäykset eivät kohdistu vain yksityiselle sektorille, vaan myös julkinen sektori on saanut niistä osansa. Esimerkiksi vuonna 2021 Turun kaupungin opetuksen verkkopalveluihin kohdistui tietomurto kiristyshaittaohjelman levittämisesi (Hiltunen, 2021) ja satojen Turun kumppaneiden ja työntekijöiden tiedot olivat vaarassa vuotaa tietomurtajien saadessa

käsiinsä käyttäjätunnustietoja (Pihkala, 2021). Myös Lappeenrannan kaupungin työntekijän sähköpostiin kohdistui tietomurto (Pohjalainen, 2021).

Digi- ja väestötietoviraston (DVV, 2021a) (myöhemmin DVV) raportissa julkisen hallinnon digitaalisen turvallisuuden nykytilasta nostetaan esiin, että kunnat ovat keskimäärin hieman jäljessä digitaalisen turvallisuuden toimeenpanossa verrattuna muuhun julkiseen hallintoon. Digitaalisen turvallisuuden osalta on tunnistettu muun muassa vaje digitaalisen turvallisuuden kehittämisen resursseissa, jonka vuoksi digitaalisen turvallisuuden jalkauttaminen, kouluttaminen ja vakinaistaminen ovat epävakaita. Lisäksi johdon haastetta luovat johdon ymmärryksen ja sitoutumisen puute. (DVV, 2021b.) Myös Kuntaliiton (2020) tilaama tutkimus nostaa esiin useita kehityskohteita kuntien tietoturvallisuuden pelikentällä, kuten sen että tietoturvallisuus ei ole koko organisaation yhteinen asia.

Kyberturvallisuuden tutkiminen onkin tärkeää, jotta uudenlaisiin kyberuhkiin varautuminen, sekä niiden torjunta sekä organisaatiotasolla että esimerkiksi lainsäädännön kautta olisi mahdollista. Tietoturvauhkien estämiseksi kehitetyt tekniset ratkaisut ovat kehittyneet, ja kyberrikolliset ovat alkaneet etsiä uusia keinoja rikollisten tavoitteidensa saavuttamiseksi. Pelkät teknologiset menetelmät ja työkalut eivät välttämättä olekaan tarpeeksi tehokkaita organisaation tietovarantojen suojaamiseen (Siponen, ym., 2008). On tärkeää ymmärtää yksilöiden ja organisaatiotasolla työntekijöiden tietoturvakäyttäytymistä, jotta kyberuhkia voidaan ehkäistä, ja jotta tietojärjestelmien suunnittelussa ja laadinnassa voidaan huomioida inhimillisiä ominaisuuksia (Gonzalez & Sawicka, 2021; Krombholz ym., 2014).

Työntekijöillä ja heidän toimintapäätöksillään on merkittävä rooli tietoturvan toteutumisessa (Parsons ym., 2015). Jopa 75 prosenttia organisaatioiden tietoturvahaavoittuvuuksista kumpuaa organisaation sisältä (D'Arcy, Hovav & Galletta, 2009). Inhimilliset tekijät voivat mahdollistaa tietoturvaloukkauksien toteutumisen (Grobler, Gaire & Nepal, 2021), esimerkiksi työntekijän päättäessä vastata tietojenkalastelusähköpostiin (Parson ym., 2015). Vuonna 2021 jopa yli 75 prosenttia kaikista tietoturvauhkista alkoikin organisaatioiden työntekijöille lähetetyistä sähköposteista. (Trend Micro, 2022). Kyberturvallisuuskeskuksen vuosikatsauksen mukaan yleisimmät tietoturvauhkat ovat juuri huijausviestit, kiristyshaittaohjelmat ja tietojenkalastelu, joilla voidaan saada haltuun esimerkiksi liikesalaisuuksia (Traficom 2019).

Kyberturvallisuuskulttuurin käsitteessä korostuu ajatus siitä, että organisaatioiden tulisi huomioida työntekijöidensä tietoturvaan liittyvät arvot, asenteet, käyttäytyminen, merkitykset, uskomukset tiedot ja taidot organisaation tietovarantoja suojellessaan. Kyberturvallisuuskulttuuri pohjautuu ajatukseen organisaatiokulttuurista ja tietoturvakulttuurista, painottaen tietoturvakulttuurin tiedonhallintaan liittyvän näkökulman sijaan kokonaisvaltaista näkemystä ihmisen käyttäytymisestä tietotekniikan kontekstissa. (Da Veiga, 2016.) Tutkimuksessa tarkastellaan monimerkityksellistä ilmiötä, kulttuuria, joka näkyy Scheinin (2004) mukaisesti eri tasoilla. Tasoilla viitataan niiden havaitsemiseen: ne sisältävät näkyviä ja näkymättömiä elementtejä, jotka vaikuttavat organisaation toimintaan (Schein, 2004).

Kyberturvallisuuskulttuurin tutkimusta tarvitaan, koska tietoverkkojen ja -järjestelmien käyttäjät ovat yksi merkittävimmistä hyökkäyksien kohteista. Jo hieman kuluneen, mutta edelleen ajankohtaisen sanonnan mukaan ihminen on tietoturvan heikoin lenkki (ks. esim. Vroom & Von Solms, 2004; Bulgurcu ym., 2010). Kyberturvallisuuden ja laajemmin tietoverkkojen ja -järjestelmien turvallisuuden kehittäminen vaatii ymmärrystä ihmisen toiminnasta, roolista ja vaikutuksista (Siponen, 2005; Mishra & Dhillon, 2006; Dhillon ym., 2016). Aiemman tutkimuksen tarkastelun perusteella voidaan todeta, että Suomessa ei vielä ole tehty sellaista tutkimusta, joka käsittelee kyberturvallisuuskulttuuria julkisorganisaatioissa.

Tämä tutkielma edistää osaltaan ymmärrystä kyberturvallisuuskulttuurista ja sen rakentumisesta Suomalaisessa julkisorganisaatiossa. Tutkielman keskiössä ovat ihmiskeskeiset, pääosin ei-teknologiset tekijät, jotka ovat yhteydessä tietoturvan toteutumiseen organisaatioissa. Tekijät ilmenevät työntekijöiden käyttäytymisessä tietotekniikan kontekstissa, niin henkilökohtaisella kuin myös organisaatiotasolla. Tutkielman viitekehyksenä ja ohjaavina käsitteinä toimivat organisaatiokulttuuri ja kyberturvallisuuskulttuuri. Kyberturvallisuuskulttuuri limittyy turvallisuus- ja tietoturvallisuuskulttuurien käsitteisiin ja tutkimuksessa sitä määritellään niiden rajapintojen kautta.

Tutkielman analyysi on toteutettu laadullisen narratiivisen analyysin keinoin. Tutkielmassa aineiston sisältöjä analysoimalla pyritään selvittämään kyberturvallisuuskulttuuria kuvailevia tekijöitä ja käsityksiä aineistosta ja muodostamaan niistä tyyppitarinoita.

Tutkielmaan sisältyy ajattelutapa, jonka mukaan organisaation tapahtumista ei ole olemassa eikä siten voida muodostaa yhtä oikeaa totuutta, eikä sen selvittäminen siten olisi tarkoituksenmukaista. Tutkielmaan sisältyy ajatus narratiivisen tietämisen tavasta, eikä siinä yritetä etsiä oikeiksi tai vääriksi miellettyjä kausaalisuhteita, vaan esittää tulkinta tutkittavasta ilmiöstä sellaisena, kuin se tutkijalle näyttäytyy. Tarinallinen lähestymistapa rajoittaa yleistämistä ja tutkielman tuloksiin on vaikuttanut vahvasti tutkijan tekemä tulkinta. Tarinallisuus on nähtävissä yhdeksi mahdolliseksi lähestymistavaksi, kun kulttuurillista ilmiötä pyritään tulkitsemaan. Vaikka tutkimustulokset eivät ole suoraan yleistettävissä muihin organisaatioihin, voi tutkimusasetelma tapauskohtaisesti harkiten toimia esimerkkinä kyberturvallisuuskulttuurin tarkastelemisesta muissa julkisen sektorin organisaatioissa.

1.2 Tutkielman tavoite

Tämän tutkielman tarkoituksena on kuvailla, millä tavoin kyberturvallisuuskulttuuria ilmentävät inhimilliset piirteet näkyvät tutkimuksen kohteena olevan organisaation henkilöstön toiminnassa ja asenteissa, sekä toisaalta tarkastella organisaatiokulttuurin ja toimintaympäristön vaikutusta kyberturvallisuuskulttuuriin. Tässä tutkielmassa kyberturvallisuuskulttuuria ja sen rakentumista organisaatioissa tarkastellaan ihmiskeskeisesti. Tämä tarkoittaa ei-teknologisia tekijöitä, jotka ovat yhteydessä tietoturvan toteutumiseen organisaatioissa, kuten esillä olevia ja piileviä käsityksiä, arvoja, uskomuksia, asenteita, normeja ja oletuksia kyberturvallisuudesta ja miten ne ilmenevät työntekijöiden käyttäytymisessä tietotekniikan kontekstissa, niin henkilökohtaisella kuin myös organisaatiotasolla.

Tutkielmassa tutkitaan kyberturvallisuuskulttuuria erään kaupungin hallinto-organisaatiossa. Tarkemmat tiedot tutkielman kohteena olevasta organisaatiosta jätetään julkaisematta tässä tutkielmassa, jotta organisaation anonyymiys säilyy. Tutkielma pureutuu erityisesti seuraavaan tutkimuskysymykseen:

Millaiset tekijät ja käsitykset ovat vaikuttaneet kyberturvallisuuskulttuurin olemukseen organisaatiossa?

Tutkimuskysymykseen pyritään vastaamaan muodostamalla ja analysoimalla haastatteluaineistosta ilmiötä kuvaavia tyyppitarinoita. Tyyppitarinat kuvaavat asioita, tapahtumia ja käsityksiä, jotka ovat vaikuttaneet kyberturvallisuuteen, ja jotka ilmentävät organisaation kyberturvallisuuskulttuuria. Tutkielma pyrkii tunnistamaan aikaisempaan tutkimukseen nojaten henkilöstön henkilökohtaisia ja kollektiivisia arvoja, toimintatapoja kybertoimintaympäristössä ja muodostamaan niistä yleistä, yhteistä ajattelumaailmaa, jonka kautta organisaatiossa tulkitaan ympäröivää maailmaa.

Tutkielman laajempana tieteellisenä tavoitteena on tuoda esiin kyberturvallisuuden ja kyberturvallisuuskulttuurin käsitettä osana hallintotieteellistä organisaatiokulttuurin tutkimusta ja narratiivisen organisaatiotutkimuksen kenttää. Tutkielmassa lähdetään ajatuksesta, että kyberturvallisuuskulttuuri on osa organisaatiokulttuuria. Tutkielmassa viitataan narratiivisen tietämisen tapaan, joka tarkoittaa Brunerin (1986) mukaisesti tarinoihin perustuvaa ymmärryksen tapaa. Toisin sanoen, narratiivisuuden nähdään olevan tapa ajatella, ymmärtää ja selittää inhimillistä elämää ja ihmisten keskinäisiä suhteita (Hänninen, Mönkkönen & Puusa, 2020, 241).

Konstruktiivinen ajattelutapa tukee tutkielman tavoitteita. Kyberturvallisuuskulttuurin ei nähdä olevan muuttumaton ilmiö, vaan sen uskotaan muodostuvan tapauskohtaisesti ihmisten tuottamien tietojen ja totuuksien pohjalta sekä olevan lopulta tutkijan eli minun rakentama kokonaisuus. Narratiivinen tutkimus korostaakin pluralismia, relativismia ja subjektiivisuutta. Sen perusolettamuksena on, että se ei etsi yhtä ainoaa oikeaa totuutta, eikä se tarjoa yhtä oikeaa tapaa käsitellä aineistoa. (Lieblich ym., 1998, 2.)

Tämän tutkielman aihe koskettaa perinteistä hallintotieteellisen tutkimuksen sekä ihmistutkimuksen, teknologiantutkimuksen ja käyttäytymiseen liittyvän tietojärjestelmien turvallisuuden hallinnoinnin tutkimusparadigmaa. Tutkielmassa viitataan laajasti erilaisiin tutkimuksiin eri tieteenaloilta. Kyberturvallisuuskulttuurin käsitettä rakennettaessa on tarpeellista selvittää ihmisen suhdetta teknologiaan, niin arvojen kuin myös käyttäytymisen kontekstissa. Oleellista on myös organisaatiokulttuurin ja tietoturvallisuuden tutkimus, varsinkin tietoturvakulttuurin osalta, joka on nähtävissä kyberturvallisuuskulttuurin lähikäsitteeksi (Da Veiga, 2016). Kyberturvallisuuskulttuuri on käsitteenä melko uusi ja siihen liittyvää tutkimusta ei ole olemassa kovin paljoa. Oman piirteensä tutkielmaan tuo ilmiön käsittely julkishallinnollisen organisaation kontekstissa sekä sen narratiivinen

tutkimusote. Organisaation kulttuureista, kuten myös tietoturvallisuudesta löytyy sen sijaan reilusti aikaisempaa kirjallisuutta. Näitä lähteitä hyödyntäen tutkielma muodostaa pohjan kyberturvallisuuskulttuurin käsitteelle ja sen tutkimiselle.

Tämä tutkielma käsittelee tutkimustehtävää kvalitatiivisella eli laadullisella tutkimusotteella. Tutkimuksen tavoitteena on ymmärtää valittua ilmiötä eli kyberturvallisuuskulttuuria kohdehenkilöiden tai tahojen näkökulmasta. Tutkielmassa ollaan siis kiinnostuneita ajatuksista, kokemuksista, tunteista ja merkityksistä, joita kohdehenkilöt antavat kyberturvallisuuskulttuurille. (Puusa & Juuti 2020, 9.) Tutkielman lähtökohtana on haastateltavien todellisen elämän kuvaaminen. Tutkielmassa ei etsitä totuuksia, vaan yksilöllisten kokemusten kautta yhteisiä piirteitä kohdeorganisaation kyberturvallisuuskulttuurista. (Hirsjärvi, Remes & Sajavaara, 2009.) Tutkimustehtävään vastataan narratiivisen temaattisen analyysin avulla analysoimalla aineistosta muodostettuja tyyppitarinoita.

1.3 Aiempi tutkimus

Suomessa kyberturvallisuuskulttuuria ei tiettävästi ole tutkittu julkisen sektorin organisaatioissa aikaisemmin. Kansalliskirjasto ylläpitämästä Finna-palvelun kokoelmista hakusanalla ”kyberturvallisuuskulttuuri” ei löydy yhtään vertaisarvioitua tulosta. Sen sijaan kyberturvallisuuskulttuurista on tiettävästi tehty joitain pro gradu -tason tutkielmia. Kyberturvallisuuskulttuurin lähikäsitteenä voidaan nähdä olevan turvallisuus- ja tietoturvallisuuskulttuuri. Myöskään haku ”tietoturvakulttuuri” Finna-palvelun kokoelmista ei tuota yhtään vertaisarvioitua tulosta. Turvallisuuskulttuuri sen sijaan tuottaa niukasti hakutuloksia.

Turvallisuuskulttuuria ovat tutkineet esimerkiksi Mannila & Laajalahti (2021) sairaalojen kontekstissa, erityisesti kriisiviestinnän kautta. Artikkeli tarkastelee turvallisuuskulttuurin rakentumista. Heidän mukaansa turvallisuuskulttuuria voidaan kehittää sairaaloissa 1) jaettua ymmärrystä turvallisuudesta synnyttämällä, 2) turvallisuusnäkökulmat kaikessa tekemisessä huomioimalla, 3) ohjeistuksia kehittämällä, 4) yhteistyötä tukemalla ja pirstaloitumista ehkäisemällä, 5) työntekijöitä osallistamalla sekä 6) johtamista kehittämällä.

Kulttuuri käsite on hyperkompleksinen, eikä tieteellisessä kentässä ole onnistuttu saavuttamaan yhteistä tulkintaa sen tulkinnasta tai käsitteestä. Aiemmassa tutkimuksessa on esimerkiksi väitetty, että kulttuuria ei voi aistia osana fyysistä maailmaa, vaikkakin jotkin sosiaalisen maailman muodot ovat osa kulttuurillista toimintaa ja saaneen näin kulttuurillisen leiman. (Pirnes, 2008) Kulttuurin käsitteen moniulotteisuuden ja erilaisten tulkintojen myötä kulttuuriksi voidaan käytännössä laskea kuuluvan lähes kaikki ihmiselävään liittyvä (Benjamin, 2014, 61–62).

Organisaatiokulttuuriteorioita ovat tutkineet esimerkiksi Huhtala & Laakso (2007). Heidän tutkimuksensa oli kirjallisuuskatsauksen muodossa ja sen tarkoitus oli selvittää, mitkä ovat kulttuuriparadigman pääsuuntaukset ja miten niistä on keskusteltu alan kansainvälisissä julkaisuissa. Heidän mukaansa organisaatiokulttuuriparadigman nähdään olevan yksi viidestä merkittävimmästä 1900-luvun organisaatio- ja johtamisparadigmasta. Organisaatiokulttuuriteoriat juontavat juurensa 1970- ja 1980-lukujen akateemiseen keskusteluun, jolloin organisaatioita alettiin tutkia symbolisen interaktionismin ja antropologian näkökulmista, toisin sanoen sosiaalisesti rakentuneina merkitysjärjestelminä, sekä 1980-luvulle Yhdysvaltoihin, jolloin kasvavan kilpailun vuoksi etsittiin uusia keinoja kilpailukyvyn kasvattamiseksi. Keskeiseksi ajatukseksi nousivat työyhteisöjen muuttaminen joustaviksi, luoviksi ja työntekijää paremmin motivoiviksi, jotka saavutettaisiin organisaatiokulttuurin sitoutumisen ja laadun ideologioista. Kulttuuriparadigman pääsuuntaukset koostuvat kahdesta näkemyksestä: kulttuuri muuttujana ja kulttuuri metaforana.

Kaksi kenties tunnetuinta organisaatiokulttuurin tutkijaa ovat E. Schein sekä G. Hofstede. Hofstede ym., (2010) määrittää kulttuurin merkitysten verkoksi, jonka kautta ihmiset tulkitsevat kokemuksiaan ja joka ohjaa ihmisten toimintaa. Useat eri tutkijat hahmottavat kulttuurin eri tasojen kautta. Hofstede ym. (2010) hahmottaa kulttuurin luomansa sipulimallin avulla, jonka kerrokset koostuvat arvoista, rituaaleista, sankareista symboleista ja käytännöistä. Schein (2004) puolestaan näkee kulttuurin tasojen muodostuvan kolmesta eri tasosta: artefakteista ja luomuksista, arvoista ja uskomuksista sekä perusolettamuksista. Scheinin (2008) määritelmän mukaan kulttuurin ytimessä ovat perusolettamukset: mikäli jokin ratkaisu toimii toistuvasti, siitä muodostuu kyseenalaistamaton itsestäänselvyys. Nämä perusolettamukset ovat välttämättömiä kulttuurin näkyvien osien tulkitsemiseksi. (Schein, 2008.)

Tässä tutkielmassa kulttuuri ymmärretään Scheinin (2004) määritelmän tavoin, jolloin kulttuuri nähdään dynaamisena ilmiönä, joka ympyröi meitä ja jota luodaan ja sovelletaan vuorovaikutuksessa muiden kanssa. Kulttuuriin nähdään kuuluvan myös käyttäytymistä ohjaavia ja rajoittavia myös rakenteita, rutiineja, sääntöjä ja normeja (Schein, 2008, 14). Scheinin (2008) määritelmän mukaan kulttuurin ytimessä ovat perusolettamukset: mikäli jokin ratkaisu toimii toistuvasti, siitä muodostuu kyseenalaistamaton itsestäänselvyys. Nämä perusolettamukset ovat välttämättömiä kulttuurin näkyvien osien tulkitsemiseksi. (Schein, 2008.)

Organisaatiokulttuurin voidaan nähdä olevan monitahoinen ja vaikeaselkoinen ilmiö, jolla ei ole yhtenäistä määritelmää. Useimmat tutkijat näkevät, että organisaatiokulttuuria määrittävät kokonaisvaltaisuus, historia, rituaalit ja symbolit, sosiaalinen rakentuminen (Hofstede, 2010). Scheinin (2004, 21) mukaan kulttuuri on jaettujen kokemusten muotoutumista perusoletuksiksi organisaation jäsenille ja millä tahansa ryhmällä, jolla on yhteistä keskeytymätöntä historiaa, on myös kulttuuria. Nämä perusoletukset puolestaan ohjaavat organisaation jäsenten käyttäytymistä. Organisaatiokulttuuri auttaa ymmärtämään miksi organisaatiot tekevät tiettyjä asioita ja miksi niillä on tiettyjä haasteita. (Schein, 2004.)

Kyberturvallisuutta on tutkinut esimerkiksi Da Veiga (2016). Hänen mukaansa, kuin monen muunkin tutkijan mukaan kyberturvallisuudelle ei ole olemassa yhtenäistä määritelmää (Da Veiga, 2016). Kyberturvallisuuskulttuuria määrittelyssä voidaan hyödyntää tietoturvakulttuurin tutkimusta sekä organisaatiokulttuurimalleja ja määritelmiä (Da Veiga & Eloff, 2010; Von Solms & Van Niekerk, 2013; Da Veiga 2016). Tietoturvakulttuurin nähdään keskittyvän rajattuun kontekstiin sekä usein tiedon hallintaan ja turvaamiseen organisaation sisäisesti. Kyberturvallisuuskulttuurin nähdään olevan tietoturva- ja turvallisuuskulttuureja huomattavasti laajempi kokonaisuus, kattaen kokonaisuuden yksilöstä, yksittäisestä tietoteknisestä laitteesta, yhteiskunnan kriittiseen infrastruktuuriin. (Da Veiga, 2016.)

Organisaatiolla tulisi olla asianmukainen hallintorakenne sekä selvät prosessit ja käytännöt organisaation sekä sen työntekijöiden ja asiakkaiden suojelemiseksi. Kyberturvallisuuskulttuuria ja sen arviointia voidaan hyödyntää esimerkiksi tietoturvariskien hallinnan osalta inhimillisen riskien ymmärtämiseen organisaatioissa. Lisäksi sen avulla voidaan havainnoida häiriötilanteisiin reagointia käyttäjän näkökulmasta

sekä sitä voidaan hyödyntää erilaisten koulutusten kohdentamiseen esimerkiksi käyttäjille, joiden parissa kulttuuri ei ole vaaditulla tasolla. (Da Veiga, 2016.)

1.4 Tutkielman rakenne

Tutkielma koostuu kuudesta pääluvusta. Ensimmäisessä johdantoluvussa käydään läpi tutkimuksen tausta, tavoite, tutkimuskysymys, käsitteellinen viitekehys sekä rajaukset. Ensimmäisen luvun alussa pyritään antamaan yleiskuva tutkielmasta.

Tutkielman toinen luku käsittelee teoreettista viitekehystä, joka koostuu organisaatiokulttuurista, kyberturvallisuudesta ja kyberturvallisuuskulttuurista. Kulttuurin käsittely on tärkeä osa tutkielmaa, koska ihmiset tulkitsevat sen kautta maailmaa (Hofstede ym., 2010). Organisaatiokulttuurin käsittely on puolestaan tärkeää siksi, koska se auttaa selittämään organisatorisia ilmiöitä (Schein, 2004).

Tutkielman kolmas luku kuvaa tutkimuksen narratiivista lähestymistapaa organisaatiotutkimukseen. Narratiivisuus luo tässä tutkimuksessa mahdollisuuden tarkastella tutkimuksen kohteena olevaa ilmiötä yksityiskohtaisesti. Tutkimuksen kohteena oleva ilmiö ikään kuin herätetään henkiin kertomusten avulla. (Rhodes & Brown, 2005.)

Neljännessä eli empiirisessä luvussa kuvataan, miten tutkimuskysymykseen on vastattu. Empiria käsittelee tutkimuksen laadullista tutkimustapaa, teemahaastatteluilla kerättyä tutkimusaineistoa, analyysimenetelmää eli temaattista analyysiä sekä eettisyyttä ja tutkijapositiota. Luvun tarkoitus on lisätä tuloksien luotettavuutta sekä selkeyttää niitä lukijalle selittämällä yksityiskohtaisesti, miten aineisto on kerätty ja analyysi toteutettu.

Tutkielman viidennessä luvussa esitetään tutkimuksen tulokset narratiivisina tyyppitarinoina. Tuloksien ensimmäinen narratiivi kuvaa henkilökohtaista kyberturvallisuuskulttuuria sekä henkilökohtaisia käsityksiä kyberturvallisuudesta. Tulososion toinen narratiivi kuvaa hallinto-organisaation organisaatiokulttuuria ja toimintaympäristöä pureutuen kohdeorganisaation organisaatiokulttuuriin ja sen ominaispiirteisin. Kolmas narratiivi kuvaa kyberturvallisuuskulttuuria yleisemmin.

Viimeisessä eli kuudennessa luvussa esitetään tutkielman yhteenveto sekä kontribuutio. Johtopäätöksissä kuvataan myös tutkielman keskeiset rajoitukset, luotettavuuden arviointi sekä jatkotutkimusehdotukset.

2 KULTTUURI JA KYBERTURVALLISUUS – KULTTUURIN VAIKUTUS ARVOIHIN JA KÄYTTÄYTYMISEEN

2.1 Kulttuurin käsite ja mallit

Kulttuuria voidaan tulkita useissa erilaisissa merkityksissä. Sen laajimmassa merkityksessä voidaan puhua sivilisaatioista, eli valtioiden, kansojen tai jopa koko yhteiskunnan elämäntavasta. Pienemmässä mittakaavassa kulttuurista voidaan puhua esimerkiksi yksittäisen maan, siellä olevan ryhmän tai organisaation näkökulmasta. (Hofstede ym., 2010.) Seuraavissa alaluvuissa käsitellään kulttuurin käsitettä, organisaatiokulttuuria ja tietoturvakulttuuria sekä kyberturvallisuuskulttuuria.

Kulttuurin käsitettä voidaan kutsua hyperkompleksiseksi. Sitä on verrattu rinnettä alas pyörivään lumipalloon, joka pyöriessään kätkee sisäänsä uusia merkityksiä. (Everitt 1999; Pirnes 2008) Pirneksen (2008, 14) mukaan kulttuurin hahmottamisen tekee hankalaksi se, että aistihavainnolla tunnistettavaa kulttuuri-nimistä fyysisen maailman kappaletta tai henkisen maailman oliota ei ole olemassa. Jotkin sosiaalisen toiminnan muodot on liitetty kulttuurin käsitteen mukaiseen toimintaan, ja ne ovat saaneet kulttuurisen leiman. Näistä tulkinnoista on muodostunut yhteisiä sopimuksia kulttuurin käsitteen merkityksestä. On kuitenkin huomattava, että mitään yksimielisyyttä käsitteestä ja sen tulkinnoista ei ole, jolloin yhteiskunnassa esiintyy aina erimielisyyksiä siitä, mitä kulttuurilla tarkoitetaan. (Pirnes, 2008, 14.) Benjaminin (2014, 60–61) mukaan yleiskielessä kulttuurilla tarkoitetaan ”sellaisia tapoja, käytäntöjä, kieliä, arvoja ja maailmankatsomuksia, jotka määrittävät ihmisryhmää esimerkiksi kansallisuuden, etnisyyden, alueen tai yhteisen mielenkiinnonkohteen perusteella”. Kulttuuria on kuitenkin vaikeaa havainnoida, sillä suurin osa siitä näyttäytyy pinnan alla olevana arvojen, uskomusten ja käsitteiden monimutkaisena järjestelmänä. Lisäksi kulttuurin käsitteen moniulotteisuuden ja erilaisten tulkintojen myötä kulttuuriksi voidaan laskea kuuluvan lähes kaikki ihmiselävään liittyvä (Benjamin, 2014, 61–62.)

Hofstede ym. (2010) puolestaan määrittelee kulttuurin ”merkitysten verkostoksi, jonka kautta ihmiset tulkitsevat kokemuksiaan ja joka ohjaa heidän toimintaansa”. Hofstede on eräs kulttuurintutkimuksen tunnetuimmista tutkijoista. Hän jakaa kulttuurin kahteen osaan ja kuvaa kulttuuria ohjelmointianalogian kautta (Hofstede, ym., 2010, 5). Hänen mukaansa kulttuuri, joskin suppeassa merkityksessä, viittaa länsimaisissa kielissä mielen jalostumiseen ja sivistykseen sekä ennen kaikkea jalostumisen lopputuloksiin, kuten koulutukseen, taiteeseen ja kirjallisuuteen. Laajemmassa mielessä hän kuvaa kulttuuria mielen kollektiiviseksi ohjelmoinniksi, jonka lähteet ovat sosiaalisessa ympäristössä, jossa ihminen on kasvanut ja saanut elämänkokemuksensa. Ohjelmointi on alkanut perheessä ja jatkunut henkilön ollessa vuorovaikutuksessa ympäristön toimijoiden kanssa. Ohjelmat myös vaihtuvat sen ympäristön mukaan, missä ne on saatu. Hofstede ym., (2010) korostaa kulttuurin olevan sosiaalisesta ympäristöstä peräisin ja olevan siten opittua. Hänen mukaansa kulttuuriset piirteet on aiemmin liitetty perinnöllisyyteen puutteellisen osaamisen vuoksi ja perinnöllisyyden roolia on liioiteltu aiemmissa ”pseudoteorioissa”. (Hofstede ym., 2010, 6–7.)

Edellä kuvatun analogian mukaisesti Hofstede ym., (2010, 5) paikallistaa kulttuurin ihmismieleen. Hänen mukaansa kulttuuri on mielen kollektiivista ohjelmointia ja joka erottaa yhden ryhmän tai ryhmien jäsenet muista ryhmistä. Kulttuuri on kollektiivinen ilmiö, joka ilmenee ja on jaettu ainakin osittain muiden samassa sosiaalisessa ympäristössä elävien ihmisten kanssa. Hänen näkemyksensä mukaan kulttuuri viittaa kaikkiin tunne-, ajattelu- ja toimintamalleihin, sekä myös arkisempiin asioihin, kuten tervehtimiseen, syömiseen ja tunteiden osoittamiseen, joiden voidaan osoittaa olevan jossain määrin yhteneväisiä jossain tietyssä sosiaalisesti ja/tai maantieteellisesti rajatussa ryhmässä. (Hofstede ym., 2010, 5–6.)

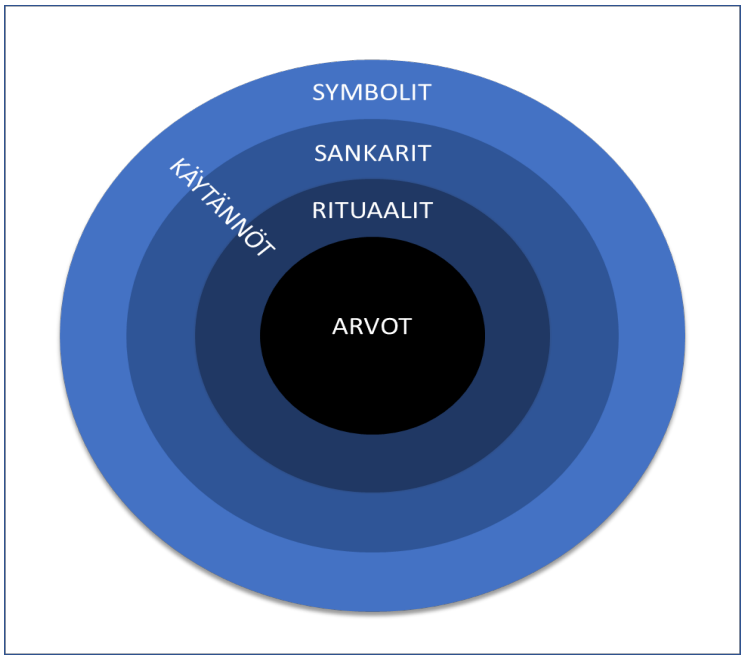
Toisen tunnetun kulttuurintutkijan Scheinin (2004) mukaan kulttuuri on dynaaminen ilmiö, joka ympäröi meitä jatkuvasti ja jota luodaan ja sovelletaan vuorovaikutuksessa muiden kanssa sekä joukko rakenteita, rutiineja, sääntöjä ja normeja, jotka ohjaavat ja rajoittavat käyttäytymistä. Kulttuuri onkin jaettujen kokemusten päätymistä perusoletuksiksi organisaation jäsenille ja millä tahansa ryhmällä, jolla on jonkinlainen yhteistä historiaa, on myös kulttuuria, jonka vahvuus riippuu sen olemassaolon pituudesta ja jaetuista menneistä kokemuksista. (Schein, 2004, 1–16.) Scheinin dynaamisen kulttuurin määritelmä kuuluukin näin:

“Jaettujen perusolettamusten malli, jonka ryhmä on oppinut ratkaistessaan ulkoiseen sopeutumiseen ja sisäiseen integraatioon liittyviä ongelmiaan ja joka on toiminut riittävän hyvin, jotta sitä voidaan pitää pätevänä ja näin ollen opettaa se uusille jäsenille oikeana tapana hahmottaa, ajatella ja tuntea suhteessa näihin ongelmiin.” (Schein, 2004, 17)

Scheinin mukaan kulttuurin ydintä ovat siis perusolettamukset, jotka ovat muodostuneet yhteisön ongelmanratkaisussa. Mikäli ratkaisu toimii toistuvasti, se otetaan itsestäänselvyytenä, ja sitä ei kyseenalaisteta. Mikäli taustalla olevia perusolettamuksia ei ymmärretä, ei voida tietää, miten artefakteja, eli kulttuurin näkyviä osia tulisi tulkita tai kuinka paljon uskoa artikuloituihin arvoihin. Kulttuurin merkitys on siis perusolettamuksien mallissa ja vasta niiden ymmärtäminen mahdollistaa muiden pinnallisempien tasojen ymmärtämisen. (Schein, 2004.)

Schenin mukaan useita eri kulttuurin määrittelyjä tarkastelemalla saadaan käsitys, jonka mukaan kulttuuri kattaa lähes kaiken, minkä ryhmä on oppinut kehittyessään (Schein, 2004, 1). Scheinin mukaan ihmisellä on siis aktiivinen rooli kulttuurin muotoutumisessa ja oppimisessa, mikä viittaa siihen, että kulttuuri ei ole yhtä stagnaattinen luomus, kuin millaisena Hofstede ym. (2010) sen ymmärtää.

Kulttuurin ilmenemistä voidaan havaita useilla eri tasoilla, joilla viitataan siihen, missä määrin kulttuuri ilmiönä on havaittavissa. Sekä Hofstede ym. (2010) että Schein (2004) ovat esitelleet kulttuurin muodostumista mallien kautta, jotka havainnoitavat näitä tasoja. Hofsteden ym. (2010, 7–8) mukaan kulttuurin ilmenemismuotoja on kuvattu monin eri tavoin, mutta hänestä kulttuuria voidaan kuvata hyvin sipulimallin kautta neljän keskeisen kokonaiskäsitteen avulla: symbolien, sankarien, rituaalien ja arvojen (ks. kuvio 1). Kulttuurinen ohjelmointi näkyy tämän luokittelun kautta käsitteiden omaksumisena. Mallin mukaan sipulin kuorien mukaisesti symbolit kuvaavat kulttuurin näkyvimpiä ilmenemismuotoja, arvojen ollessa syvimmällä. (Hofstede ym., 2010.)



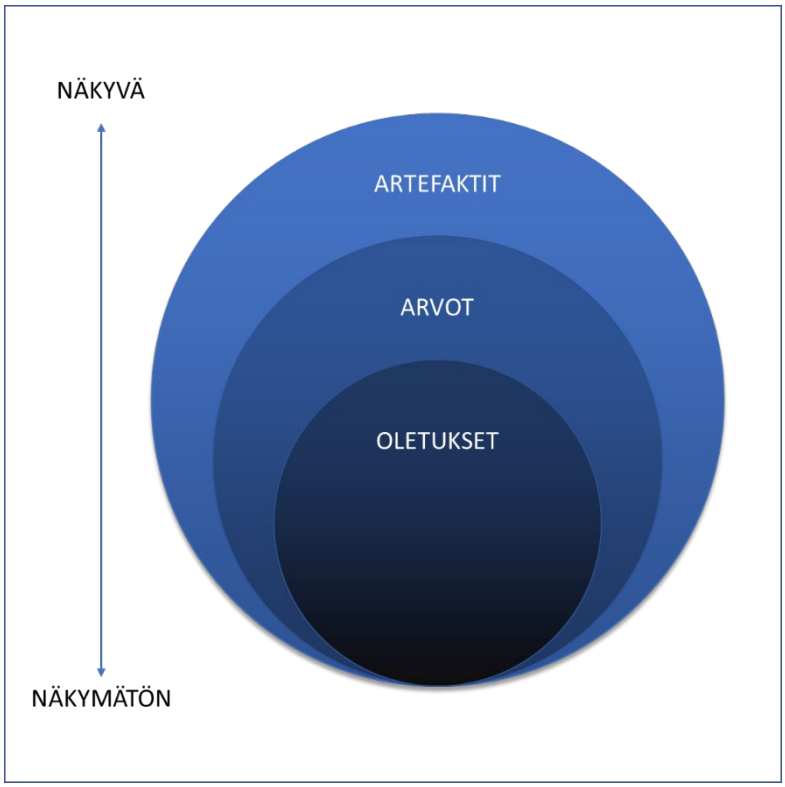
Kuvio 1. Kulttuurin sipulimalli (mukaillen Hofstede ym., 2010).

Symbolit ovat sanoja, eleitä, kuvia tai kielikuvia ja esineitä, jotka kantavat tiettyä merkitystä. Tämän merkityksen tunnistavat vain ne, jotka jakavat kulttuurin. Sankarit ovat eläviä tai kuolleita, todellisia tai kuvitteellisia henkilöitä, joilla on kulttuurissa arvostettuja ominaisuuksia ja joita pidetään siten käyttäytymismalleina. Rituaalit ovat kollektiivisia toimintoja, joilla ei ole varsinaista merkitystä, mutta joita pidetään kulttuurissa sosiaalisesti välttämättöminä. Niitä toteutetaan itsensä vuoksi, esimerkkinä tapa osoittaa kunnioitusta toiselle. Rituaaleihin kuuluu myös kielenkäytön tapa, diskurssi, jolla kieltä käytetään tekstissä ja puheessa sekä päivittäisessä vuorovaikutuksessa. Sipulimallissa Hofstede on koonnut kolme käsitettä, symbolit, sankarit ja rituaalit käytännön toimien käsitteen alle. Tällä hän tarkoittaa sitä, että vain tällaisina ne näkyvät ulkopuolisen silmin, jolloin niiden kulttuurin merkitys on näkymätön. Kulttuurinen merkitys näkyy ainoastaan siinä, miten sisäpiiriläiset tulkitsevat näitä käytäntöjä. Kulttuurinen muutos alkaa yleensä käytännöistä, sillä ne eivät ole niin syvälle juurtuneita käsityksiä. Uusia käytäntöjä voidaan oppia koko elämän ajan. (Hofstede, 2010, 7–9, 19.)

Hofsteden mukaan kulttuurin ytimen muodostavat arvot. Ne ovat ikään kuin asioiden sisäisiä merkityksiä, tunteita, joita suositaan toistensa yli. Arvot muodostuvat ikään kuin alitajuisiksi uskomuksiksi. Arvot muotoutuvat ihmiselle nuoressa iässä, samalla kun opimme muita asioita. Arvot jäävät tämän vuoksi usein tiedostamattomiksi asioiksi, joista ei voida keskustella tai joita muut eivät voi havainnoida. Arvot näkyvät vain erilaisina

toimintamalleina, jotka ilmenevät eri olosuhteissa. (Hofstede, 2010, 19–20.) Arvojen muutos on hidasta, sillä ne on opittu lapsena vanhemmilta, jotka ovat omaksuneet ne lapsena. Tämän myötä yhteiskunnassa vaikuttavat perusarvot ovat paljon vakaampia ja muuttumattomia, vaikka käytännöt muuttuisivat.

Schein (2004) sen sijaan näkee kulttuurin tasojen muodostuvan kolmesta eri tasosta: artefakteista ja luomuksista, arvoista ja uskomuksista sekä perusolettamuksista (ks. Kuvio 2). Tasoilla viitataan niiden havaitsemiseen: ne sisältävät näkyviä ja näkymättömiä elementtejä, jotka vaikuttavat toimintaan. Ensimmäinen taso sisältää kulttuurin ulkoisen säilymisen tekijät, toinen taso kulttuurin sisäisen yhdentymisen ja kolmas taso kulttuurin syvät perusolettamukset. (Schein, 2004.)



Kuvio 2. Edgar H. Scheinin (2004) mukaiset kulttuuritasot.

Artefaktit ja luomukset ovat kulttuurin näkyviä asioita, kirjaimellisesti mitä voidaan nähdä, kokea ja kuulla. Niihin kuuluvat ryhmän fyysinen ympäristö, fyysiset asiat kuten käytetyt tuotteet, pukeutumiskoodi, käyttäytymisen ja puhuttelun mallit sekä kieli. Artefaktien havaitseminen on helppoa, mutta niiden tulkitseminen on hankalaa omien ennakkokäsitysten vuoksi. (Schein, 2004, 25–36.)

Scheinin määritelmän toisen tason muodostavat arvot ja uskomukset. Taso koostuu uskomuksista, strategioista, tavoitteista, arvoista, jotka ohjaavat jonkin ryhmän toimintaa. Kuvaavaa on, että arvot ja uskomukset voivat olla niin abstrakteja, että ne voivat olla ristiriidassa keskenään. Arvot ovat kuitenkin tiedostettuja ja näkyviä, koska niitä käytetään esimerkiksi organisaation toiminnan johtamiseen. Tämän vuoksi esimerkiksi strategiaan sisältyvillä arvoilla tulisi olla selkä suhde organisaation johtamistapoihin, jotta ne edesauttaisivat tehokkaasti organisaation toimintaa. (Schein, 2004, 28–30.)

Kolmas taso koostuu jaetuista perusoletuksista. Ne ovat tiedostamattomia ja näkymättömiä asioita, joita pidetään niin itsestään selvinä ja yleisesti hyväksyttyinä, että niihin ei kiinnitetä huomiota ja täten niitä on hankala muuttaa. Niistä muodostuu olettamuksia, alitajuisia malleja, joilla on perustavanlaatuisia vaikutuksia ihmisen toimintaan. Perusoletukset ovat organisaation identiteetin perusta. (Schein, 2004, 30–36.)

Edellä käsitellyt määritelmät kulttuurista muodostavat tällekin tutkielmalle sen ominaisen käsityksen kulttuurista: Kulttuuri on subjektiivisesti koettu kollektiivinen ilmiö, jolla on historiallinen luonne ja se näyttäytyy tietylle ryhmälle ominaisina artefakteina, arvoina ja oletuksina.

2.2 Organisaation kulttuurit ja niiden merkitys turvallisuuteen ja käyttäytymiseen

2.2.1 Organisaatiokulttuuriparadigma

Kuten kappaleen alussa kerrottiin, kulttuuria voidaan tulkita useissa erilaisissa merkityksissä ja sen käsite on hyperkompleksinen. Etuliite ‘organisaatio’ monipuolistaa sen merkitystä entisestään. Organisaatiokulttuurin tutkimusta tehtiin jo 1950-luvulla, mutta se yleistyi vasta kaksi vuosikymmentä myöhemmin. Yhdet ensimmäisistä tutkijoista, kuten Elliot Jaques ja Isabel Menzies (1951; 1952) tutkivat organisaatiokulttuuria psykodynaamisesta näkökulmasta. Jaques näki, että organisaatiossa tapahtuu jatkuvasti vuorovaikutusta rakenteen, kulttuurin ja persoonallisuuden välillä (Jaques, 1951). Toiset tutkijat, kuten Philip Selznick (1957), painottivat sosiologisen viitekehyksen näkökulmaa. Hänen näki

institutionalisoitumisprosessin kautta organisaatiossa muodostuvan sääntöjä ja periaatteita, jotka vaikuttavat toimintatapoihin (Selznick, 1957). Kuitenkin vasta 1970-luvun loppupuolella organisaationkulttuurin käsite yleistyi. Ponnahduslautana tähän oli Pettigrewin (1979) tutkimus, jossa käytettiin kulttuuriviitekehystä organisaation tutkimiseen. Tämä johti siihen, että kun näkökulma organisaatioihin tuli kulttuuriviitekehyksen kautta, ne käsitettiin sosiaalisina rakenteina vanhan luonnontieteellisen ihmistoimijoista riippumattomien objektiivisten merkitysten sijaan. (Puusa & Juuti, 2020, 68–69.)

Organisaatiokulttuuriparadigman nähdään olevan yksi viidestä merkittävimmästä 1900-luvun organisaatio- ja johtamisparadigmasta. Organisaatiokulttuuriteoriat juontavat juurensa 1970- ja 1980-lukujen akateemiseen keskusteluun, jolloin organisaatioita alettiin tutkia symbolisen interaktionismin ja antropologian näkökulmista, toisin sanoen sosiaalisesti rakentuneina merkitysjärjestelminä, sekä 1980-luvulle Yhdysvaltoihin, jolloin kasvavan kilpailun vuoksi etsittiin uusia keinoja kilpailukyvyn kasvattamiseksi. Keskeiseksi ajatukseksi nousivat työyhteisöjen muuttaminen joustaviksi, luoviksi ja työntekijää paremmin motivoiviksi, jotka saavutettaisiin organisaatiokulttuurin sitoutumisen ja laadun ideologioista. (Huhtala & Laakso, 2007, 13–15.)

Suomeen erilaiset kulttuuriteoriat rantautuivat 1980-luvulta alkaen ja kulttuurinäkökulman tunnistettiin 1990-luvulla vaikuttaneen keskusteluun yritys- ja julkisista organisaatioista. Kulttuuriparadigma on säilyttänyt monitahoisen ja moniteemaisen luonteensa. Kulttuuria on tutkittu työkaluna tavoitteiden ja tehokkuuden saavuttamiseen. Toisaalta keskustelussa on säilynyt mukana kritiikki kulttuuriteorioiden hyötyyn tähtäävään toimintaan. (Huhtala & Laakso, 2007, 25.) Organisaatiokulttuurin tarkastelu on mahdollistanut tutkijoille syvemmän teoreettisen ymmärryksen organisaatioista (Puusa & Juuti, 2020).

Kulttuurinäkökulmien yleistyessä 1980-luvulla ne jakaantuivat kahteen kenttään: organisatorisen symbolismin tutkijoihin, jonka mukaan organisaatioita tulisi tutkia sosiaalisesti rakentuneina merkitysjärjestelminä ja joka syntyi vastalauseena toiselle kulttuurinäkökulmalle eli rakenneanalyyttiselle paradigmalle sekä pragmaattiselle rintamalle, jonka tavoitteena oli hyötyä kulttuurintutkimuksesta ja jonka sanoma puhutteli liike-elämän toimijoita. (Huhtala & Laakso, 2007, 14–15.) Alvensson (1990, 34) jakoi kulttuurinäkökulman edustajat puritaaneihin, pragmaatikkoihin ja akateemisiin

pragmaatikkoihin, joista ensimmäiseksi mainittu edustaa organisatorisen symbolismin tutkijoita. Puritaanien, eli akateemisen siiven mukaan kulttuureita ei voi eikä niitä tulisi yrittää hallinnoida. Pragmaatikot eli ei-akateemiset kirjoittajat ja akateemiset pragmaatikot pyrkivät sen sijaan tuottamaan tietoa siitä, kuinka kulttuureja hallinnoidaan. (Huhtala & Laakso, 2007, 14–19.)

Linda Smirch (1983) tunnistaa organisaatioiden tutkimuksesta edellä mainitun mukaisesti kaksi erilaista kulttuurinäkökulmaa organisaatioon. Ensimmäisessä lähestymistavassa kulttuuri nähdään metaforana, jonka kautta organisaation toimintaa voidaan selittää ja ymmärtää (Huhtala & Laakso, 2007, 21.) Tällöin kulttuuri nähdään organisaation ominaisuudeksi, ollen jotain sellaista mitä organisaatiolla on. Organisaatiot ovat kulttuurin tuotteita, johon myös siihen kuuluvien ihmisten on sopeuduttava ja jota heidän on hyvin vaikeaa muuttaa. Kulttuuria ei voi valita, vaan ihmiset ikään kuin kohtaavat sen ja sopeutuvat siihen. (Harisalo, 2008, 272.) Toinen lähestymistapa näkee kulttuurin muuttujana, jota voidaan mitata ja hallita (Huhtala & Laakso, 2007, 21). Sen mukaan organisaatioilla on kulttuuri, jonka muokkaaminen ja kehittäminen haluttuun suuntaan on mahdollista. Kulttuuri näyttelee täten tärkeää osaa organisaation menestyksessä suuntaamalla ajattelutapoja ja toimintaa haluttua suuntaa kohti. (Harisalo, 2008, 273.)

Tässä tutkielmassa organisaatiokulttuurin nähdään sijoittuvan kahden edellä mainitun kulttuurinäkökulman, kulttuurin muuttujana ja kulttuurin organisaation ominaisuutena, välimaastoon. Tutkielman lähtökohta on, että organisaatioon tullessaan henkilö sopeutuu vallitsevaan kulttuuriin, mutta toisaalta kulttuuria voidaan jossain määrin mitata ja kehittää haluttuun suuntaan. Kuten Alvensson (2002) kuvailee, nämä kaksi näkökulmaa organisaatiokulttuurista ovat lähestulkoon toistensa ääripäitä. Jotkut tutkijat noudattavat hyvin selvästi vain toista näkökulmaa, mutta useimmat tutkijat asemoituvat näiden kahden välille ja välttelevät pelkistämästä kulttuuria muuttujaksi tarkastelematta organisaatiota täysin kulttuurina. (Alvensson, 2002.)

2.2.2 Organisaatiokulttuuri

Organisaatiokulttuuri on monitahoinen ja vaikeaselkoinen ilmiö, joka auttaa ymmärtämään miksi organisaatiot tekevät joitain asioita ja miksi organisaatioilla on tietynlaisia haasteita. Organisaatiokulttuuri auttaa selittämään organisatorisia ilmiöitä. (Schein, 2004.) Organisaatioissa vallitseva kulttuuri kehittyy pitkän ajan kuluessa, ja ihmiset tarkastelevat sen varassa työnjaollisia rakenteita, käytäntöjä ja prosesseja. Kulttuuri voi niin vahvistaa kuin heikentääkin näiden rakenteiden, käytäntöjen ja prosessien toimivuutta. (Harisalo, 2008, 264–266.)

Astuessaan uuteen organisaatioon työntekijä oppii ajan mittaan sekä tietoisesti että tiedostamatta organisaation kulttuuria seuraamalla muiden käyttäytymistä. Opittuihin asioihin kuuluu syy- ja seuraussuhteiden näkeminen tietyllä tavoin, tiettyjen asioiden arvostaminen ja toisten väheksyminen. Työntekijä oppii myös käyttäytymään ja ajattelemaan tavalla, joka ei ole ristiriidassa muiden organisaatioiden organisaation jäsenten kanssa. (Harisalo, 2008, 264–266.)

Harisalo (2008) näkee kulttuurin muuttujana. Organisaatiokulttuuri ohjaa organisaation johtoa arvioimaan tekijöitä, joiden avulla organisaatioita voidaan kehittää ja johtaa. Kyseisten tekijöiden pohdinta voi saada johtajat huomaamaan rakenteellisten tekijöiden tehottomuuden. Moitteettomastikaan rakennettu organisaatio ei ole riittävä, jos se ei kosketa ihmisten sydäntä ja henkeä. (Harisalo, 2008, 264–266.)

Organisaatiokulttuurin käsitteeseen sisältyy hyvin paljon erilaisia näkökulmia. Näkökulmiin tulee vielä enemmän vaihtelua, jos käsitteen kulttuuri erilaiset määritelmät otetaan huomioon. Lisäksi organisaatiokulttuurin termin ongelmana on sen käyttö yleispätevänä terminä kuvaamaan pintatason sosiaalista toimintaa, vaikka kyseisille tapauksille löytyisikin tarkempi termi. Tämä on johtanut matalaan kynnykseen käyttää termiä, joka on johtanut ympäripyöreisiin määritelmiin. Kulttuuri on ”hankala konsepti, koska sillä tarkoitetaan kaikkea ja tämän vuoksi, ei oikeastaan mitään”. (Alvensson, 2002, 3.) Määritelmiä tuntuukin olevan lähes yhtä monta kuin on sen tutkijoita. Edgar Schein (2004, 14–16) on esimerkiksi koonnut yhteen muiden tutkijoiden kulttuuria ilmentäviä tekijöitä. Hänen mukaansa niitä ovat esimerkiksi säännönmukaiset käyttäytymismallit, jotka ilmenevät ihmisten välisessä vuorovaikutuksessa, ryhmien säännöt, ryhmien arvot, muodolliset ja julkituodut säännöt,

organisaation sisäiset kirjoittamattomat säännöt, tunnelma ja/tai ilmapiiri, sisäistetyt ryhmän taidot, ajattelutavat, henkiset mallit ja/tai kielen tulkinnat, jaetut merkitykset, symbolit sekä ryhmän juhlalliset rituaalit ja juhlatavat. Scheinin (2004) mukaan käsitykset organisaatiokulttuurista poikkeavat toisistaan: kaikki listatut asiat ilmentävät kulttuuria, mutta eivät riitä muodostamaan sitä yksinään. Kulttuuri perustuukin oletukselle, että tietyt asiat, kuten säännöt, arvot, ajatukset ja käyttäytyminen, ovat jollekin ryhmälle kollektiivisia ja ohjaavat ryhmän toimintaa, usein tiedostamattomalla tavalla.

Yksi tunnetuimmista organisaatiokulttuurin teorioista on Scheinin organisaatiokulttuurin malli. Scheinin (2004) mukaan organisaatiokulttuuri näkyy kolmella tasolla. Alimmalla tasolla ovat perusolettamukset, jotka ovat kulttuurin jäsenten käyttäytymistä ohjaavia piileviä oletuksia. Perusolettamukset ovat organisaatiokulttuurin tärkein taso, jonka kautta muita organisaatiokulttuurin muita tasoja on mahdollista ymmärtää. Nämä kulttuurin ytimenä toimivat perusolettamukset kertovat kulttuurin jäsenelle mihin kiinnittää huomiota, mitkä ovat asioiden merkitykset ja miten tulee toimia ja tuntea. Peruolettamukset ovat ikään kuin itsestään selviä, ja niiden vastaisesti toimiminen voidaan nähdä käsittämättömänä. (Schein, 2004) Scheinin organisaatiokulttuurin mallista kerrotaan tarkemmin kulttuurin tasojen kautta luvussa 2.1.

Schein näkee, että kulttuurin määrittelyt ovat relevantteja vain makrokulttuureja tarkastellessa ja kuvataksemme kulttuuria tarkemmin, tarvitaan käyttökelpoinen integroiva ja dynaaminen kulttuurin määritelmä, jossa korostetaan, miten kulttuuri muodostuu ja kehittyy organisaatioissa ja alakulttuureissa. Scheinin (2004, 21) mukaan kulttuuri onkin jaettujen kokemusten päätymistä perusoletuksiksi organisaation jäsenille ja millä tahansa ryhmällä, jolla on yhteistä keskeytymätöntä historiaa, on myös kulttuuria. Scheinin dynaamisen kulttuurin määritelmä kuuluukin näin:

”Ryhmän kulttuuri voidaan määritellä ryhmän kertyneeksi jaetuksi oppimiseksi, kun se ratkaisee ulkoiseen sopeutumiseen ja sisäiseen integroitumiseen liittyviä ongelmiaan. Oppiminen on toiminut riittävän hyvin, jotta sitä voidaan pitää pätevänä ja siten opettaa uusille jäsenille oikeana tapana hahmottaa, ajatella, tuntea ja käyttäytyä suhteessa näihin ongelmiin. Tämä kertynyt oppiminen on uskomusten, arvojen ja käyttäytymisnormien malli tai järjestelmä, jota pidetään itsestäänselvyytenä perusolettamuksina ja joka lopulta häviää tietoisuudesta.” (Schein, 2004)

Hofstede (2010, 344) alleviivaa myös, että organisaatiokulttuurilla tai yrityskulttuurilla ei ole yhtenäistä määritelmää. Hänen mukaansa useimmat tutkijat ovat kuitenkin sitä mieltä, että organisaatiokulttuuria määrittävät seuraavat asiat, joista ensimmäinen on kokonaisvaltaisuus, joka viittaa kokonaisuuteen, joka on enemmän kuin osiensa summa. Toisekseen historiallinen määräytyneisyys tarkoittaa organisaatioin historian heijastamista. Kolmanneksi organisaatiokulttuuri liittyy antropologien tutkimiin asioihin, kuten rituaaleihin ja symboleihin. Neljänneksi se on sosiaalisesti rakentunutta, eli organisaatioin muodostaman ihmisryhmän luomaa ja ylläpitämää. Viides organisaatiokulttuuria määrittävä asia on se, että sitä on vaikea muuttaa.

Hofstede (2010) korostaa, että vaikka kulttuuri -sanan käyttäminen saattaisi näyttää yhdistävän erilaisia kulttuurityyppejä, eivät esimerkiksi kansallinen kulttuuri ja organisaatiokulttuuri ole identtisiä ilmiöitä. Tämä johtuu siitä, että siinä missä kansallinen kulttuuri muodostuu nuorena, perheessä ja asuinympäristössä ja koulussa ja se sisältää suurimman osan perusarvoistamme, organisaatiokulttuurit hankitaan kun liitymme organisaatioon, yleisesti nuorina aikuisina, jolloin arvomme ovat jo muotoutuneet. Tällöin organisaatiokulttuuri koostuu käytännössä organisaation käytännöistä, jotka ovat pinnallisempia ja siten muuttuvaisempia. (Hofstede, 2010, 346.)

Harisalo (2008, 266–267) ymmärtää organisaatiokulttuurin suhteellisen laajasti omaksutuksi henkiseksi syvärakenteeksi, jonka varassa organisaatiossa ajatellaan, toimitaan ja strukturoidaan mahdollisuuksia. Hänen mukaansa jostain asiasta tulee laajasti hyväksyttyä, luonnollista ja kiistatonta, jos se on yleisesti omaksuttua. Sen sijaan, jos asialla on kielteisiä merkityksiä ja se ei ole enää luonnollista tai kiistatonta, voivat työntekijät suhtautua kaikkeen asiaan liittyvään kriittisesti. Hatchin (1997) mukaan organisaatiossa ei välttämättä vallitse yksimielisyys ja hyväksyntä kulttuurillisista merkityksistä, vaan yhteinen tulkinta tarkoittaa, että jäsen jakaa kulttuurilliset merkitykset muiden kanssa ja osallistuu kulttuurin tuottamiseen. Smircichin (1983) mukaan organisaatiokulttuuri on kokoelma jaettuja keskeisiä arvoja ja uskomuksia, sekä mukaan lukien prosessit ja käytösmallit. Scheinin (2004) mallin ollessa yksi käytetyimmistä organisaatiokulttuurin kuvauksista, on se saanut myös kritiikkiä osakseen. Hatch (1997) mukaan mallissa ei huomioida tarpeeksi kulttuurin dynaamista ja symbolista luonnetta. Martinin (2002) mukaan Scheinin (2004) kulttuurimalli ei ota huomioon sitä, että kulttuuri ei ole yhtenäinen kokonaisuus.

Esittelin edellä erilaisia lähestymistapoja organisaatiokulttuuriin ja kerroin, mitä kaikkea organisaatiokulttuurin käsitteen ajatellaan sisältävän. Olen myös esitellyt Scheinin (2004) tunnetun organisaatiokulttuurin jaottelun kolmeen eri tasoon – artefakteihin, omaksuttuihin arvoihin ja perusoletuksiin (ks. Kuvio 2) sekä Hofsteden (2010) organisaatiokulttuuria määrittävät asiat. Tässä tutkielmassa painotetaan Scheinin (2004) organisaatiokulttuurimallia, sillä sitä on sovellettu turvallisuus- ja tietoturvakulttuurin tutkimuksessa. Tästä kerrotaan lisää myöhemmin luvussa 2.3.

2.2.3 Julkishallinnollisen organisaation erityispiirteet

Tässä tutkielmassa tutkittava ilmiö sijoittuu julkishallinnollisen organisaation sisäiseen maailmaan, jonka merkitseviä erityspiirteitä voivat olla muun muassa organisaatio- ja henkilöstörakenne ja muut julkishallinnollisen organisaation erityispiirteet. Tämän vuoksi on syytä käydä läpi tutkielman kohdeorganisaation organisaatiokulttuurin erityispiirteitä.

Hallinnon käsitteellä voidaan viitata toimintaan, jolla ihmiset pyrkivät saavuttamaan yhteisiä tavoitteita, tai toiminnan järjestykseen yhteiskunnassa. Hallintoa voidaan tarkastella ihmisten toimintana organisaatioiden sisällä tai laajemmin organisaation toimintana. Hallinnon jäsenten rooli hallinnossa on toimia suunnitellun ja johtamisen mukaan. Organisaation, johtamisen ja organisaatio- ja johtamiskulttuurin käsitteet liittyvät vahvasti hallinnon tarkasteluun. Julkishallinto voidaan sen sijaan määrittää usealla eri tavalla. Sen voidaan nähdä määrittyvän yleisesti hyväksyttyjen arvojen ja politiikan toteutuksen kautta. Toisaalta julkisen sektorin tehtävät määrittävät julkista hallintoa. Julkisen sektorin tehtävät kertovat, mistä tehtäviä julkisen hallinnon odotetaan toteuttavan ja mitkä asiat kuuluvat sen piiriin. Eri maiden ja kulttuurien välillä on eroa julkisen vallan laajuudessa ja sen tehtävissä. (Salminen, 2004.)

Julkisjohtamisen käsite pohjaa johtamiseen sekä julkisen johtamisen eroihin verrattuna yksityisen sektorin johtamiseen. Näistä ensimmäisen, eli johtamisen käsitteen, sisältöön ovat vaikuttaneet eri johtamisperiaatteita eri näkökulmista kuvaavat teoriat ja koulukunnat. Johtamisen voidaan nähdä olevan hallinnon käytännön toimintaa, jolla on samoja piirteitä niin yksityisellä kuin julkisellakin sektorilla, vaikkakin julkisen organisaation johtamisessa on useita eri piirteitä, jotka eivät ole tyypillisiä yksityisten organisaatioiden johtamiselle.

(Salminen, 2004.) Näitä piirteitä ovat esimerkiksi julkisen organisaation toimintaa ylhäältäpäin tuleva ohjaus. Tämä ohjaus muodostuu poliittisesta tilanteesta, yhteiskunnassa vallitsevista arvoista sekä yleisistä intresseistä. Julkiset organisaatiot vastaavat vaikeasti määriteltävistä ja mitattavista yleishyödyllisistä palveluista, toiminnoista ja tavoitteista, joita muun muassa turvallisuus on. Tällaisista julkisen hallinnon tehtävistä ja tavoitteista on usein säädetty lailla, joka voi myös rajoittaa toimivaltaisen julkisen johtajan toimivaltaa. (Virtanen & Stenvall, 2010.) Esimerkiksi hallintolailla ja hyvän hallinnon periaatteilla on olennainen vaikutus julkisen hallinnon viranomaisten toimintaan, sillä se asettaa vastuita, rajoja ja laatuvaatimuksia viranomaisen vallankäytölle ja toiminnalle. (Laakso, 2009.) Lisäksi julkiset johtajat voivat olla organisaation jäsenten muodostaman paineen lisäksi poliittisten päättäjien ja kansalaisten ristipaineessa. (Virtanen & Stenvall, 2010.)

Julkisen hallinnon nykytilanteeseen vaikuttaa siltä kaivatut asiat, kuten ketteryys, uudistuminen ja ratkaisukeskeisyys, joiden vuoksi julkisen hallinnon ohjaus- ja johtamistapoja on edelleen tarpeellista kehittää. Uudet johtamisopit eivät kuitenkaan ole korvanneet julkisen hallinnon kokonaisrakenteita, vaan tilalle on tullut uusien ja vanhojen mallien ja toimintatapojen eri yhdistelmiä, sillä uusia malleja on sovellettu vanhoissa hierarkkisissa organisaatioissa. (Peters & Pierre, 1998; Nyholm ym., 2016.) Vallallaan olevat hallintoideologian vaikuttavatkin julkiset sektorin toimintaan. Eri hallintoideologiat voivat esiintyä yhtäaikaisesti ja limittyä toisiinsa, ja niitä voi olla vaikeaa havaita. (Osborne, 2010; Nyholm ym., 2016.) Julkisessa hallinnossa tasapainoillaan edelleen byrokraattisen hallinnon ja uuden julkisen johtamisen välillä juurikin toisiinsa limittyvien hallintoideologioiden takia (Ikonen, 2015). Kuntaorganisaatioiden kompleksisuutta lisää entisestään kuntien monitahoinen hallinto ja laaja toimintakenttä (Haveri & Rönkkö, 2007, 67, 176.)

2.3 Kulttuurin tasojen, arvojen, asenteen ja käyttäytymisen suhde

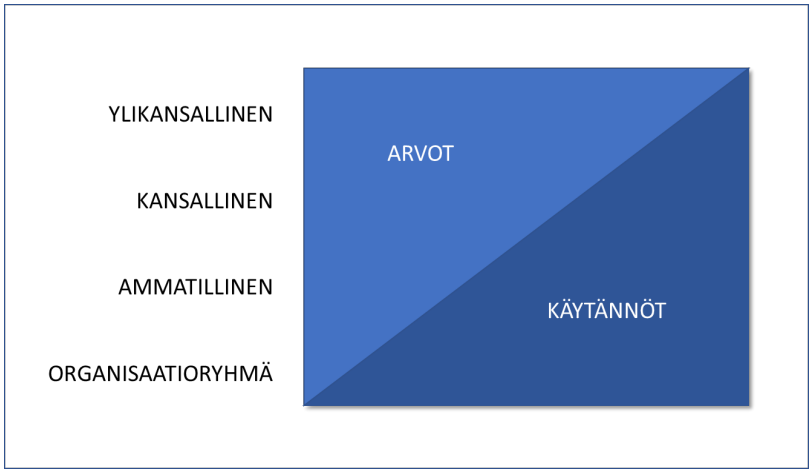
Edellä esitettyjen teorioiden pohjalta voidaankin todeta, että kulttuuri on ilmiö, joka tarkoittaa toisaalta ihmisryhmää määrittäviä tapoja, käytäntöjä, arvoja ja maailmankatsomuksia. Toisaalta se on myös ilmiö, joka ympäröi meitä jatkuvasti ja jonka kautta elämme. Se on myös joukko rakenteita, rutiineja, sääntöjä ja normeja, jotka ohjaavat

ja rajoittavat käyttäytymistä. Scheinille kulttuuri merkitsee sitä, miten rituaalit, ilmapiiri, arvot ja käyttäytyminen nivoutuvat yhdenmukaiseksi kokonaisuudeksi. Kyseinen nivoutunut kokonaisuus on se ydin, mitä kulttuurilla tarkoitetaan (Schein, 2004, 15). Schein toteaa, että kulttuurin käsitteen kenties mielenkiintoisin puoli on sen kyky osoittaa ne näkymättömät ja tiedostamattomat ilmiöt, jotka ohjaavat ihmisten toimintaa. Kulttuuri voidaan tässä mielessä nähdä ryhmän persoonallisuutena tai luonteena. Yksilön käyttäytymistä voi havainnoida, mutta käytöstä määrittäviä tekijöitä ei. Kulttuuri ohjaa sekä rajoittaa muiden tekijöiden ohella ryhmän ja sen jäsenen käyttäytymistä ryhmässä vallitsevien yhteisten normien kautta. (Schein, 2004, 8.)

Kulttuureista puhuttaessa saatetaan niiden olettaa tarkoittavan samaa asiaa, asia ei ole näin yksinkertainen. Termiä kulttuuri käytetään niin kansallisessa kuin organisaatiokontekstissa ja vaikka niiden taustalla voidaan nähdä olevan samankaltaisia tekijöitä, ovat kulttuurityypit Hofsteden mukaan silti luonteeltaan erilaisia. Kansalliset kulttuurit muodostuvat ihmisten elämän kymmenen ensimmäisen vuoden aikana ja ne koostuvat suurimmaksi osaksi arvoista ja uskomuksista, organisaatiokulttuurien rakentuessa enemmän käytännön muotoon, ollen enemmän pinnallisia. (Hofstede ym., 2010, s. 346.)

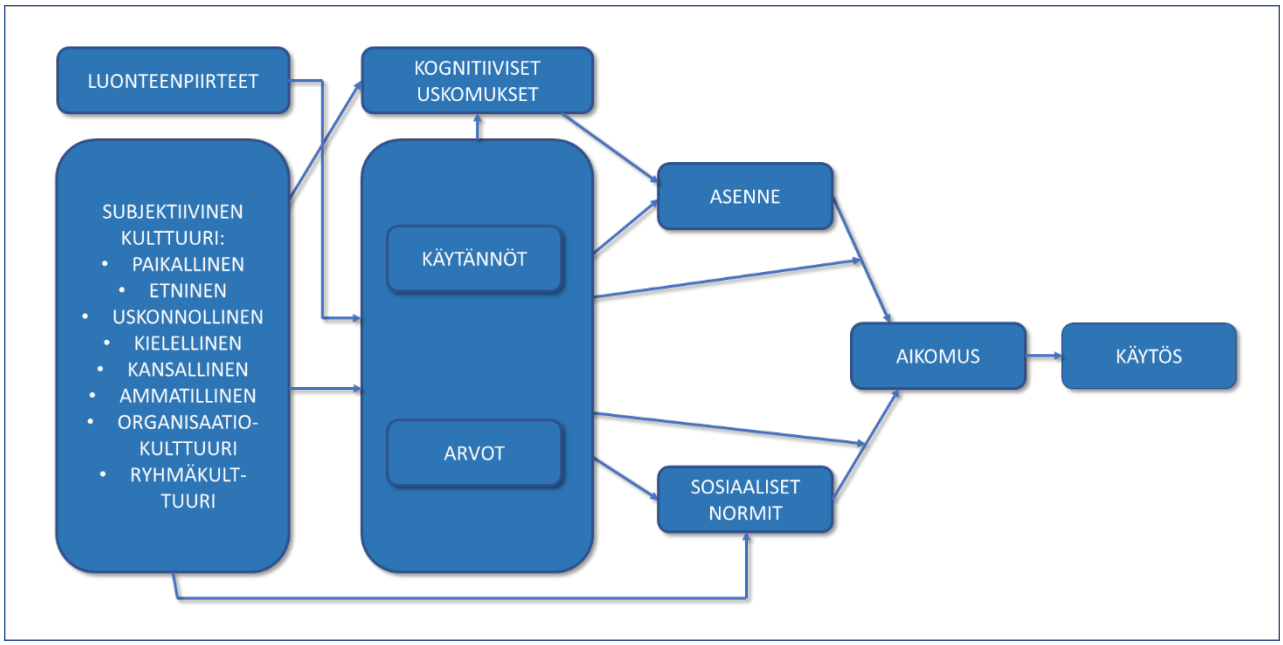
Hofsteden mukaan kulttuurin merkitys arvoihin ja käytäntöihin on erilaista kulttuurin eri tasoilla (ks. kuvio 3). Hänen mukaansa lähes jokainen ihminen kuuluu samanaikaisesti useisiin eri ryhmiin ja yhteisöihin. Jokaisen ryhmällä tai yhteisöllä on oma kulttuurinsa, joka on muodostunut ryhmälle tai luokalle yhteisistä henkisistä ohjelmista. Tämän vuoksi meissä on useita eri kerrostumia eli kulttuurin tasoja, joita ovat muun muassa 1. kansallinen taso, joka perustuu kotimaahan tai kotimaihin, 2. alueellinen, etninen, uskonnollinen tai kielellinen taso, 3. sukupuoli, 4. sukupolvien väliset erot, 5. sosiaalinen luokka, joka liittyy koulutusmahdollisuuksiin ja ammatilliseen asemaan ja 6. työssäkäyvien osalta organisaatiokulttuurien väliset erot organisaatioiden ja osastojen tasolla, sen mukaan miten työntekijä on sosialisoitunut työyhteisöön. (Hofstede ym., 2010, 18.) Edellä mainitut kerrostumat voivat olla keskenään ristiriitaisia, varsinkin modernissa yhteiskunnassa uskonnolliset arvot ja käytännöt saattavat olla ristiriidassa sukupolvien mukaan muotoutuneiden arvojen ja käytänteiden kanssa. Tällaiset ristiriidat kerrostumien välillä voivat hankaloittaa ihmisten käyttäytymisen ennakointia uudessa tilanteessa. (Hofstede ym., 2010, 18.)

Käytännöt ovat merkityksellisempiä alimman tason kulttuureissa, kuten ryhmä- ja organisaatiokulttuureissa. Yksilön arvoihin vaikuttavat enemmän kulttuurin korkeammat tasot, kuten ylikansalliset, etniset ja uskonnolliset kulttuurit. Yksilön käytäntöihin sen sijaan vaikuttavat ammatti- ja organisaatiokulttuurit. (Karahanna, Evaristo, Srite, 2005; Hofstede, 2010.) Karahanna, ym. (2005) laajentavat käsitystä informaatioteknologian alalle sijoittuvassa tutkimuksessaan, jossa he tarkastelevat kulttuurityypin vaikuttamista käyttäytymiseen. He pohjaavat näkemyksensä Hofsteden (2010) näkemykseen eri kulttuurin tasojen vaikutuksesta arvoihin ja käytäntöihin, mutta vievät ajattelutavan pidemmälle ja integroivat Hofsteden (2010) mukaiset kulttuurin eri tasot tunnustamalla, että yksilöiden käyttäytyminen työpaikalla on kaikkien eri kulttuurien funktio samanaikaisesti.



Kuvio 3. Arvojen ja käytäntöjen tasapaino kulttuurin eri tasoilla (mukaillen Hofstede, 2010; Karahanna ym., 2005).

Karahanna ym., (2005) uskovat, että käyttäytymisen aikomukset tiettyä käyttäytymistä kohtaan ovat käyttäytymisen parhaita ennustajia. Käyttäytymiseen kohdistuvat vallitsevat asenteet ja tärkeiden viiteryhmien aiheuttamat normatiiviset käyttäytymistä koskevat paineet vaikuttavat aikomuksiin. Asenteeseen vaikuttavat puolestaan käyttäytymisen seurauksiin kohdistuvat kognitiiviset uskomukset. Empiirisen näytön mukaan esimerkiksi käsitykset teknologian hyödyllisyydestä ja helppokäyttöisyydestä ovat kognitiivisia uskomuksia ja samalla teknologian hyväksyntämallin keskeisiä konstruktioita. Nämä kognitiiviset uskomukset edeltävät tietotekniikan käyttöä kohtaan kumpuavia asenteita ja käyttäytymisaikomuksia. Osana tutkimustaan Karahanna ym., (2005) kehittivät teoreettisen käyttäytymismallin käyttäytymiseen vaikuttavista tekijöistä (ks. Kuvio 4). Mallissa arvojen nähdään olevan sosiaalisten normien, asenteiden ja kognitiivisten uskomusten ja näin ollen käyttäytymisen tärkeitä ennakko-odotuksia. (Karahanna ym., 2005.)



Kuvio 4. Teoreettinen malli käyttäytymiseen vaikuttavista tekijöistä (mukaillen Karahanna ym., 2005).

Kulttuurien voidaan siis nähdä jakautuvan muun muaassa arvoihin ja käytänteisiin, joita kulttuurista omaksutaan ja jotka vaikuttavat käyttäytymiseen. Esimerkiksi Rokeach (1973) ja Schwartz & Blisky (1993) määrittelevät arvot uskomuksiksi halutusta tahtotilasta, jolloin arvot toimivat ohjaavana tekijänä henkilön käyttäytymiselle. Kulttuurin on todettu vaikuttavan esimerkiksi käytökseen ja asenteeseen tietoturvaa kohtaan, mikä kertoo kulttuurin merkityksestä tieto- ja informaatioteknologian kontekstissa. Mishra & Dhillon (2006) tunnistavat käyttäytymiseen perustuvan tietoturvan hallinnoinnin (behavioral information security governance) tutkimuksessa kulttuurin vaikuttavan poikkeavaan käytökseen ryhmässä ja korostavat turvallisuuskulttuurin tärkeyttä paremman hallintatuloksen kannalta. Dinev ym., (2009) tutkivat käyttäjien käyttäytymistä suojaavaa tieto- ja informaatioteknologiaa kohtaan testaamalla empiirisesti käyttäytymismallin avulla Yhdysvalloissa ja Etelä-Koreassa vastaajilta kerättyjä aineistoa sekä käyttäen Hofsteden (2010) kansallista kulttuuri-indeksiä moderoivana muuttujana. Heidän mukaansa on syytä uskoa, että kaikkiin tapauksiin sopivaa tietoturvallisuusstrategiaa tai menettelyä ei ole mahdollista olla olemassa, mikä osoittaa, että organisaatioiden tulisi ottaa huomioon kulttuuriset tekijät turvallisuuttaan parantaessa. Crossler ym,. (2013) argumentoi myös, että kulttuurilla on todennäköisesti vahva vaikutus tietoturvan eri osatekijöihin sekä Rocha & Flores (2014) tunnistavat kulttuurin merkityksen tehokkaiden tietoturvaohjelmien suunnittelussa.

Jo hieman kuluneen, mutta silti edelleen merkityksellisen sanonnan mukaan ihminen on tietoturvan heikoin lenkki (ks. esim. Vroom & Von Solms, 2004; Bulgurcu ym., 2010). Pelkät teknologiset menetelmät ja työkalut eivät välttämättä olekaan tarpeeksi tehokkaita organisaation tietovarantojen suojaamiseen (Siponen, ym., 2008). Eräänä lähestymistapana organisaation tietoturvaan on käytetty tietoturvakäyttäytymistä, eli asioita joita käyttäjät tekevät tai jättävät tekemättä (Da Veiga & Eloff, 2010), tai toisin sanoen toimintaa ja käyttäytymistä, joka vaikuttaa yksikön tai organisaation tietoturvallisuuteen (Guo, 2013). Tietoturvakäyttäytymisen huomioiminen voi olla haastavaa, sillä yksilöillä on erilaisia käsityksiä tietoturvasta ja siihen liittyvistä ohjeista (Herath & Rao, 2009).

Tietoturvakäyttäytymisen tutkimuskenttä on laaja ja hajanainen ja sitä on tutkittu useista erilaisista näkökulmista. Tietoturvallista käyttäytymistä on esimerkiksi mahdollista ennustaa motivaatiolla tietoturvaan liittyvien uhkien välttämiseen. Motivaatioon puolestaan vaikuttavat uhkiin liittyvä ymmärrys ja henkilön mahdollisuus vaikuttaa tilanteeseen. Tietoturvaan liittyviä uhkia pystyy havainnoimaan, mikäli henkilö ymmärtää häntä koskettavan uhan. (Huigang & Yajiong, 2010.) Bulgurcu ym., (2010) huomasivat tietoturvapolitiikan noudattamiseen keskittyvässä tutkimuksessaan, että asenne, normatiiviset uskomukset ja noudattamisen itsetehokkuus vaikuttivat työntekijän aikomukseen noudattaa tietoturvapolitiikkaa. Heidän mukaansa asenteeseen vaikuttavat noudattamisesta saatu hyöty sekä sen aiheuttamat kustannukset, kuin myös noudattamatta jättämisestä aiheutuvat kustannukset. He kuvaavat edellä mainittuja tulosuskomuksiksi, jotka syntyvät noudattamisen tai noudattamatta jättämisen seuraamuksien arvioinnista. (Bulgurcu ym., 2010.) Siponen, Mahmood & Pahnila, (2014) puolestaan osoittivat tutkimuksessaan, että koettujen uhkien vakavuus, havaitut haavoittuvuudet, tietoturvakäytäntöjen noudattamiseen ja soveltamiseen liitetyt uskomukset, tietoturvakäytäntöjen noudattamiseen liittyvä asenne, ja käytänteiden noudattamiseen liittyvät sosiaaliset normit vaikuttivat positiivisesti aikomukseen noudattaa tietoturvapolitiikkaa. Aikomuksella puolestaan oli merkittävä vaikutus siihen, kuinka käytäntöjä noudatettiin. (Siponen ym., 2014.) Ifinedo (2012) puolestaan esittää tietoturvapolitiikan noudattamista koskevassa tutkimuksessaan tutkimustulosten viittaavan siihen, että työntekijöiden asenteet ja työkavereiden näkemykset vaikuttivat tietoturvakäyttäytymiseen. Lisäksi Galvez ym., (2015) osoittivat, että toisten ihmisten kannustuksella, itsetehokkuudella ja tietoturvakäytännöillä oli positiivinen vaikutus tietoturvan tulosuskomuksiin, motivoiden yksilöitä jatkamaan käyttäytymistä, jos he

uskovat, että heidän toimintansa tuottaa toivottuja tuloksia. Tam ym., (2010) puolestaan tutkivat käyttäjien salasanojen hallintaa. Heidän mukaansa käyttäjät valitsevat heikkoja salasanoja, koska mukavuuden ja käytännöllisyyden eli lyhyen ja helpon salasanan ja turvallisuuden eli pitkän ja monimutkaisen salasanan käytön ja muistamisen välinen kompromissi on tärkeä. Muiksi käyttäytymiseen vaikuttaviksi tekijöiksi on tunnistettu esimerkiksi turvallisuutta parantavan asian koettu hyödyllisyys (Ng & Rahim, 2005) sekä asenteen vaikutus (Ng & Rahim, 2005; Anderson & Agarwal, 2010).

Merkittäväksi tietoturvaan vaikuttavaksi tekijäksi on tunnistettu myös tietoturvatietoisuus (information security awareness) ja useat tutkimukset osoittavat, että tietoturvaan on mahdollista vaikuttaa tietoturvatietoisuutta kasvattamalla (ks. esim. Siponen, 2000; Puhakainen, 2006; Siponen ym., 2007). Tietoturvatietoisuudella tarkoitetaan Siposen (2000) mukaan ”viittaamaan tilaan, jossa organisaation käyttäjät ovat tietoisia - ja mieluiten sitoutuneita – tietoturvatehtäväänsä”. Myös muita määritelmiä on ilmaantunut, ja esimerkiksi Shaw ym., (2009) mukaan tietoturvatietoisuudella viitataan tietoturvan merkityksen ymmärtämiseen sekä henkilökohtaisen toiminnan vaikutukseen tietoturvan toteutumisessa. Shaw ym., (2009) mukaan tietoturvauhkien ja tietoturvakäytäntöjen kehnon tietoisuuden on havaittu vaikuttavan tietoturvan toteutumiseen negatiivisesti. Abawajyn (2014) mukaan tietoturvatietoisuuden kehittämisen kautta voidaan vaikuttaa asenteisiin ja siten tietoturvakäytäntöihin. Bulgurcu ym., (2010) tunnistivat, että tietoturvatietoisuudella on myönteinen vaikutus henkilöiden asenteisiin tietoturvallisuutta kohtaan. Parsons ym., (2014) tutkivat työtietokoneen käytön yhteydessä käytäntöjä ja menettelytapoja koskevan tietoisuuden, käytäntöjä ja menettelytapoja koskevan asenteen ja käyttäytymisen välistä suhdetta. Heidän mukaansa tietoturvatietoisuus vaikutti positiivisesti asenteeseen tietototurvakäytänteitä kohtaan. (Parsons ym., 2014.) Farooq ym., (2015) tutkivat suomalaisten yliopisto-opiskelijoiden tietoturvatietoisuutta tiedon ja käyttäytymisen yhdistelmänä ja selvittivät, miten yksilölliset tekijät, kuten ikä, sukupuoli ja koulutustaso, opiskeluala, kansalaisuus, asuinalue, työkokemus ja tietoturvaan liittyvä koulutus, vaikuttivat opiskelijoiden tietoturvatietoisuuden tasoon. Tutkimuksen mukaan mitatulla tietoisuudella havaittiin olevan vaikutus turvallisuuskäyttäytymiseen, mutta todellisen vaikutuksen kuvailtiin olleen vähäinen. Yksilöllisten tekijöiden osalta sukupuolella nähtiin olleen suurin vaikutus tietoturvatietoisuuteen, miespuolisten saaden parempia tuloksia. Tietoisuus oli kattavinta IT-opiskelijoiden keskuudessa, mutta tällöin sukupuolella ei ollut merkitystä. (Farooq ym., 2015.)

Edellä esitettiin kulttuurin, asenteiden, aikomuksien ja käyttäytymisen vaikutusta tietoturvallisuuteen. Tietoturvakäyttäytyminen on kuitenkin monimutkainen ilmiö, jota on vain pintaraapaistu tässä tutkielmassa ja jota on tutkittu useiden teorioiden avulla ja jolla on useita lähikäsitteitä (ks. Lebek, 2013). Tietoturvakäyttäytymiseen ja tietoturvaan liittyvässä kirjallisuudessa esitetään, että organisaation tietovarantoja suojellakseen niiden täytyisi huomioida työntekijöiden käyttäytymistä, arvoja ja uskomuksia (Kolkowska, 2011; Siponen, 2005; Mishra & Dhillon, 2006). Dhillon ym., (2016) mukaan organisaatiossa työskentelevien kulttuurinen asenne ja sen mukaiset toimet ovat merkityksellisiä tekijöitä tietoturvan kannalta. Heidän mukaansa sosiotekninen ympäristö, joka muodostuu ihmisen ja teknologian suhteesta, eli esimerkiksi organisaation normeista, käyttäytymismalleista sekä uskomuksista ja sen teknologisesta infrastruktuurista, tulisi ottaa huomioon muun muassa tietoturvarikkomuksia käsitellessä. (Dhillon ym., 2016.) Ei voida sanoa, että pelkästään kulttuuri vaikuttaa käyttäytymiseen, mutta sen voidaan aiemman tutkimuksen perusteella olettaa olevan yksi mahdollinen käyttäytymiseen vaikuttava tekijä.

Tieto- ja informaatioteknologian inhimillisen puolen parantamista kohtaan on kehittynyt kyberturvallisuuskulttuurin käsite, joka limittyy organisaatiokulttuurin, turvallisuuskulttuurin ja tietoturvakulttuurin käsitteisiin. Seuraavassa kappaleessa pohjustetaan turvallisuus- ja tietoturvallisuuskulttuurien käsitteitä, josta edetään kyberturvallisuutta ja kyberturvallisuuskulttuuria käsittelevään lukuun.

2.3.1 Turvallisuus- ja tietoturvakulttuuri

Organisaatiokulttuurin oheen on noussut näkemys turvallisuuskulttuurista, joka voidaan käsittää yhdeksi organisaatiokulttuurin osaksi tai vaihtoehtoisesti turvallisuutta korostavana organisaatiokulttuurina (Reiman ym., 2008). Turvallisuuskulttuurin käsite syntyi vuonna 1986 Tšernobylin ydinvoimalaonnettomuuden tutkinnan yhteydessä. Sitä käytettiin kansainvälisen atomienergiajärjestön (ent. INSAG) raportissa havainnollistamaan, että onnettomuuksien taustalla ei ole pelkästään teknisiä vikoja tai yksittäisten ihmisten virheitä. Turvallisuuskulttuurin käsite toi ajatteluun mukaan kokonaan uusia ulottuvuuksia: se toi esiin, että onnettomuuksien syntyyn voivat vaikuttaa johtamiseen, organisaatioon, työyhteisöön tai jopa yhteiskuntaan liittyvät tekijät. (Reiman ym., 2008, 18.)

Turvallisuuskulttuurin käsitettä vaivaavat samat ongelmat, kuin muitakin kulttuuriin liittyviä käsitteitä – määritelmiä on useita, eikä yhtä selkeää määritelmää ole olemassa. Yhteistä määritelmille on kuitenkin, että ne korostavat yksilöiden ja ryhmien ja organisaatioiden asenteita, käsityksiä ja käyttäytymistä turvallisuutta kohtaan. Turvallisuuskulttuuri näyttäytyykin yksilön ja organisaation kykynä ja tahtona ymmärtää turvallisen toiminnan periaatteita. (Reiman ym., 2008, 18.) Reiman & Oedewald, (2004) määrittelevät turvallisuuskulttuurin osaksi organisaatiokulttuuria, joka käsittää kulttuurin turvallisuuteen liittyvät tekijät. Heidän mukaansa jokaisessa organisaatiossa voidaan nähdä muodostuvan jonkin tasoinen turvallisuuskulttuuri osana organisaatiokulttuuria.

Turvallisuuskulttuurin käsityksiä on alettu soveltamaan myös tietotekniikan osalta, jossa turvallisuuskulttuurin periaatteiden nähdään olevan tärkeä tekijä organisaation tietoturvan ylläpitämisessä ja että turvallisuuskulttuurin kultivoiminen vakiinnuttaa tietoturvalliset käyttäytymismallit organisaation toimintaan (Thomson ym., 2006).

Tietoturvallisuuteen liittyvissä tutkimuksissa sosiaalisissa ympäristöissä, kuten yhteisöissä, vallitsevien normien ja asenteiden on tunnistettu voivan vaikuttaa käyttäytymiseen (Pahnila, Siponen & Mahmood, 2007) ja työntekijöiden käyttäytyminen sekä arvot ja uskomukset nähdään merkityksellisiksi organisaation tietovarantoja suojellessa (esimerkiksi Mishra & Dhillon, 2006; Bulgurcu ym., 2010; Crossler ym., 2013). Tällainen ihmislähtöinen tietoturvallisuuden ajattelutapa onkin yleistynyt ja esimerkiksi Karydan ym., (2005) sekä Grobler ym., (2021) mukaan tietoturvan yhteydessä pitäisi huomioida sen inhimillinen sekä teknologinen ulottuvuus. Yksilöt kytkeytyvät teknologiaan aina joko suunnittelun, käytön, huollon tai asentamisen kautta. Tämä puolestaan mahdollistaa ihmisen aiheuttamat tahalliset tai tahattomat virheet, jotka altistavat organisaation tietoturvauhkille. (Schultz, 2005.)

Greenen & D'Arcyn (2010) mukaan turvallisuuskulttuuri vaikuttaa organisaation henkilöstön turvallisuusohjeiden noudattamiseen. He havaitsivat myös korkean tyytyväisyyden vaikuttavan positiivisesti turvallisuusohjeiden noudattamiseen. Heidän mukaansa tietoturvallisuuden lisäämiseksi organisaatio voi pyrkiä vaikuttamaan työntekijöiden asenteisiin ja uskomuksiin turvallisuuskulttuuria ylläpitämällä. Da Veiga & Martins, (2015) huomioivat, että tietoturvakoulutuksella voi olla myönteinen vaikutus tietoturvakulttuuriin. Kearneyn (2010) mukaan jotta henkilö voidaan sitouttaa turvallisiin toimintatapoihin ja jotta turvallisuudesta tulisi yksi hallitsevista arvoista,

turvallisuuskulttuurin tulisi käsittää toimenpiteitä, jotka tukevat ymmärrystä tietoturvan uhkista ja vastuun jaosta organisaation tietojen suojaamisessa. Näkemystä tukee Greenen & D'Arcyn (2010) tutkimus, jonka mukaan työntekijät, jotka kokivat saavansa vahvaa tukea organisaation turvallisuusyksikön taholta, saattoivat kokea tietoturvallisuuden olevan pääsääntöisesti IT-osaston hoidettavissa, jolloin heidän oma panoksensa turvallisuuteen ei ole niin tärkeää. Kyse on *risk homeostasis* ilmiöstä, joka kuvaa ihmisten käyttäytymisen muuttuvan, kun he tuntevat olevansa turvallisessa ympäristössä (ks. Wilde, 1982).

Tietoturva ja muut tieto- ja informaatioteknologiaan liittyvät käsitteet ovat usein aiheeseen perehtymättömälle haastavia hahmottaa ja ymmärtää. Tietoturvasta puhuttaessa nousee usein esille myös tietosuojan ja kyberturvallisuuden käsitteet. Tietoturvalla (eng. information security) viitataan tiedon saatavuuteen, eheyteen ja sen luottamuksellisuuteen (Whitman & Mattord, 2017). He määrittelevät tietoturvan ”tiedon ja niiden kriittisten osien suojaamiseksi, mukaan lukien järjestelmät ja laitteistot, jotka käyttävät, tallentavat ja välittävät tietoa.” (Whitman & Mattord, 2017). Tietosuojalla tarkoitetaan oikeustieteellisessä kirjallisuudessa henkilötietojen suojaa tietosuojalainsäädännön avulla. Tietosuojan tarkoituksena on suojata luonnollisia henkilöitä ja heidän oikeuksia, mutta ei tietoa itsessään. (Saarenpää, 2012.) Tietosuojavaltuutetun toimiston mukaan tietosuojalla tarkoitetaan ”perusoikeutta, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.” (Tietosuojavaltuutetun toimisto, 2022). Kyberturvallisuuden käsitteelle ei ole olemassa vakiintunutta ja yhtenäistä merkitystä, mutta sillä viitataan digitaalisen toimintaympäristön turvallisuuteen (Suomen kyberturvallisuuden strategia, 2013; 2019; Laari ym., 2019). Julkisella sektorilla käytetään yleisesti digitaalisen turvallisuuden käsitettä, jolla tarkoitetaan usein samaa kuin kyberturvallisuudella (Valtiovarainministeriö, 2020). Tässä tutkielmassa käytetään kyberturvallisuuden käsitettä, jota käsitellään laajemmin seuraavassa luvussa.

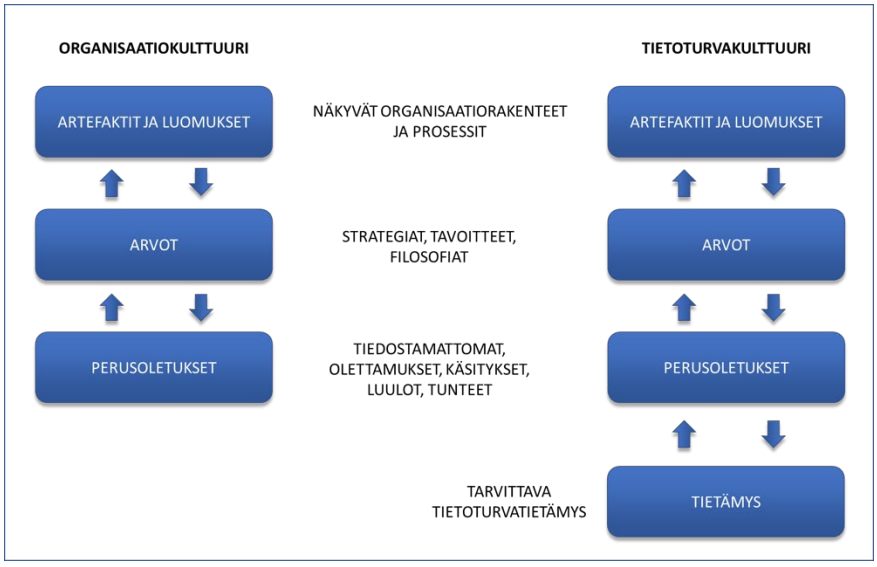
Organisaatioiden on mahdollista vaikuttaa turvalliseen käyttäytymiseen kehittämällä tietoturvakulttuuria, joka nostaa esiin turvallisuustietoista päätöksentekoa ja turvallisuusohjeistusten noudattamista. Tietoturvakulttuurin tavoitteena on siis vahvistaa ja ylläpitää organisaation tietoturvan tasoa. (von Solms & von Solms, 2004; Vroom & von Solms, 2004.) Kuten olemme huomanneet jo aiemmista kappaleista, kulttuurisen käsitteen määrittelyongelmat ovat yleisiä ja koskevat myös tietoturvakulttuuria, sillä sille ei ole toistaiseksi olemassa yhtenäiseksi miellettyä määritelmää (da Veiga ym., 2020).

Tietoturvakulttuuria on määritelty useiden muilta tieteenaloilta lainattujen teorioiden avulla ja useat viitekehykset nojaavat Scheinin (2004; 2010) organisaatiokulttuurin tutkimukseen (Mahfufh ym., 2017). Iivonen (2011) huomioi, että tietoturvakulttuurin käsite on melko uusi ja sen määritelmät ovat samankaltaisia. Käsitteen määrittelyä hankaloittavat kuitenkin sen yhteydessä käytetyt termit ja niiden päällekkäisyydet, kuten tietoturvatietoisuus (information security awareness), (ks. Siponen, 2000; Siponen, ym., 2007) ja tietoturvakuuliaisuus (information security obedience), (ks. Thomson, ym., 2006). Tietoturvakulttuurilla kuitenkin viitataan tietoturvallisuuden näkymiseen organisaation toiminnassa ja siihen, millainen käyttäytyminen on hyväksyttävää. (Iivonen, 2011.) Glaspie & Karwowski (2017) puolestaan tunnistivat viiden ihmistekijään liittyvän asian vaikuttavan tietoturvakulttuuriin. Näitä asioita olivat tietoturvapolitiikka, pelotteet ja kannustimet, asenteet ja osallistuminen, koulutus ja tietoisuus sekä johdon tuki.

Vroomin & Von Solmsin (2004) ideaalisessa tietoturvakulttuurin määritelmässä vapaaehtoinen ja itseohjautuva tietoturvallinen toiminta sekä käytös ovat osa organisaation päivittäistä toimintaa. Myös Schlienger & Teufel (2003) näkevät käsitteen samankaltaisesti: tietoturvakulttuuri käsittää sosiaaliset ja kulttuuriset tekijät, jotka vaikuttavat tekniseen tietoturvaan. Martins & Eloff (2002) puolestaan määrittelevät tietoturvakulttuurin olevan olettamus hyväksytyksi katsotusta ja kannustetusta tietoturvakäyttäytymisestä, jonka kautta tietoturva otetaan osaksi organisaation toimintatapoja. Da Veiga ym., (2020) puolestaan määrittelevät tietoturvakulttuurin laajemmin kirjallisuuskatsauksen pohjalta: ”Tietoturvakulttuuri liittyy ihmisten käyttäytymiseen organisaatiokontekstissa organisaation hallussa olevien tietojen suojaamiseksi noudattamalla tietoturvapolitiikkaa ja -menettelyjä sekä ymmärtämällä, miten vaatimukset pannaan täytäntöön varovaisesti ja huolellisesti, kuten säännöllisessä viestinnässä, tietoisuudessa, koulutuksessa ja koulutusaloitteissa on todettu. Käyttäytymisestä tulee ajan mittaan osa toimintatapaa, joka on seurausta työntekijöiden oletuksista, arvoista ja uskomuksista, heidän tietämyksestään ja asenteestaan tietovarojen suojaamista kohtaan sekä heidän käsityksestään tietovarojen suojaamisesta. Joka tapauksessa vaikka tietoturvakulttuurin määritelmiä on useita, on määritelmissä useita yhteisiä näkökulmia. Niissä viitataan työntekijöiden arvoihin, perusoletuksiin ja käyttäytymiseen, jotka näkyvät artefakteissa. (Da Veiga ym., 2020.)

Useat tutkijat sisällyttävät organisaatiokulttuurin turvallisuuskulttuurin määritelmään ja Scheinin (2004) organisaatiokulttuurin mallia (Ks. kuvio 2) onkin sovellettu

turvallisuuskulttuuria ja tietoturvakulttuuria käsittelevissä tutkimuksissa (kuten esimerkiksi Guldenmund, 2000; Schlienger & Teufel, 2003; Vroom & von Solms, 2004; Reiman ym., 2008; Da Veiga & Eloff, 2010; Da Veiga ym., 2020). Tietoturvakulttuurin muodostumista Scheinin (2004) organisaatiokulttuurin mallin mukaan tarkastelivat myös Chen, Ramamurthy & Wenn (2015). Heidän mukaansa organisaation perusolettamuksiin tietoturvasta vaikuttavat muun muassa tietoturvakoulutukset, tietoturvatietoisuus ja organisaation arvot tietoturvasta. (Chen ym., 2015.) Van Niekerk & Von Solms, (2006; 2010) ovat soveltaneet tietoturvakulttuurin tutkimuksessa Scheinin (2004) organisaatiokulttuurin mallia (ks. myös kuvio 2). Alla kuviossa 6. Van Niekerkin ja Von Solmsin (2006; 2010) mukainen tietoturvakulttuurin malli, johon lisätty neljänneksi tasoksi tieto, joka ei sisälly Scheinin malliin, mutta on Van Niekerk & Von Solms (2006; 2010) mukaan oleellinen, sillä tietoturvaa ei voida taata ilman riittävää tietämystä.



Kuvio 5. Organisaatiokulttuurin ja tietoturvakulttuurin tasot ja esiintyminen Scheinin (2004) mukaisesti (mukaillen Van Niekerk & Von Solms, 2006; 2010).

Taustalla on ajatus siitä, että jokaisen organisaation kulttuuri on seurausta jokaisesta kolmesta Scheinin (2004) mukaisesta organisaatiokulttuurin tasosta. Näiden tasojen voidaan katsoa vastaavan organisaation tietoturvan niin sanottuun inhimillisen tekijän käyttäytymisnäkökohtaan, joka koostuu tietämyksestä ja käyttäytymisestä, ja jotka liittyvät läheisesti toisiinsa. Näiden kahden ulottuvuuden seuraussuhteen vuoksi tieto tai sen puute on otettava huomioon organisaation tietoturvakulttuurissa. Yleisesti organisaatiokulttuurin määritelmissä ei oteta huomioon työtehtäviin liittyvää tietämystä, sillä työntekijällä

oletetaan olevan tarvittava tietämys tehtäviensä hoitamiseksi. (Van Niekerk & Von Solms, 2010.)

Van Niekerk & Von Solms (2010) esittävät myös, että tietoturvaan liittyvää tietämystä ei välttämättä tarvitse normaalien työtehtävien puitteissa. Tietoturvan tietämystä tarvitaan vain silloin, kun se on tarpeellista työtehtävien suorittamiseksi tietoturvakäytäntöjen mukaisella tavalla, eikä toisaalta voida olettaa, että jokaisella työntekijällä olisi vaadittava tietämys työnsä tekemisesti turvallisesti. Kaiken tavanomaisen toiminnan tulisi myös noudattaa hyvää tietoturvakäytäntöä, mikäli organisaatio haluaa edistää tietoturvakulttuuria. Riittävän tietämyksen voidaan siis katsoa olevan edellytys tietoturvalliselle toiminnalle ja siten tietoturvatietämyksen tai sen puutteen voidaan katsoa saavan paikkansa tietoturvakulttuurin neljäntenä tasona. Tietoturvakulttuurissa esitetyt neljä tasoa vaikuttavat toisiinsa, jolloin näkyvä toiminta, kuten käyttäytyminen, on seurausta arvojen, perusolettamuksien ja tietoturvatietämyksen vaikutuksesta. (Van Niekerk & Von Solms, 2010.)

Kun halutaan suojata organisaatiota tietoturvauhkilta, eräänä keinona nähdään siis olevan turvallisuus- ja tietoturvallisuuskulttuurien ylläpito. Tietoturvan katsotaan kuitenkin olevan käsitteenä riittämätön käsittelemään fyysisen ja digitaalisen maailman sulautumista ja niiden turvallisuutta (Limnéll ym., 2014). Seuraavassa luvussa pureudutaan kyber-käsitteeseen, joka on muodostunut tietoturvakäsitteen sivuttaen määriteosaksi yhdyssanoihin, joilla viitataan fyysisen ja digitaalisen maailman turvallisuuteen (Limnéll ym., 2014; Laari ym., 2019). Lisäksi luvussa käsitellään yhtä tämän tutkielman pääkäsitettä, kyberturvallisuuskulttuuria.

2.4 Kyberturvallisuuskulttuuri

Limnéll, Majewski & Salmisen (2014) mukaan maailmasta on olemassa ikään kuin kaksi eri versiota: fyysinen, konkreettisesti havaittava maailma ja bittien kyllästämä, keinotekoinen digitaalinen maailma. Heidän mukaansa kyber tarkoittaa nimenomaan tätä digitaalista maailmaa, mutta yksittäisenä sanana sitä ei juuri käytetä, sillä se saa merkityksensä yleensä siihen liitettävästä loppuosasta. Kyber on siis nähtävissä enemmänkin yhdyssanan etuliitteeksi, jonka merkitys muotoutuu vasta kokonaisuudesta, kuten kyberturvallisuus, kyberrikollisuus tai kybertoimintaympäristö. (Limnéll ym., 2014.) Myös Laari ym., (2019) mukaan kyber -sana on nähtävissä yhdyssanan määriteosana, jonka merkitys liittyy ”digitaalisessa muodossa olevan informaation käsittelyyn: tietotekniikkaan, digitaaliseen viestintään, tiedonsiirtoon ja tietojärjestelmiin. Yleensä vasta koko yhdyssanalla voidaan ajatella olevan oma merkityksensä” (Laari ym., 2019, 9). Digitaalinen ja fyysinen maailma eivät kuitenkaan ole toisistaan täysin erillisiä, sillä ne integroituvat koko ajan enemmän yhteen ja ovat riippuvaisia toisistaan. Yhteiskuntaa tai siellä olevien yritysten palveluja on haastavaa kuvitella ilman digitaalisen maailman ominaisuuksia. Olemmekin riippuvaisia tässä fyysisessä maailmassa sen toisen, digitaalisen maailman toimivuudesta, eli kyberturvallisuudesta. (Limnéll ym., 2014.)

Kyberturvallisuudelle ei ole toistaiseksi olemassa yhtenäistä määritelmää. Luiijf ym., (2013) vertailivat 19 eri maan kyberturvallisuusstrategioita ja huomasivat, että yhtenäistä määritelmää kyberturvallisuudelle ei ollut. Euroopan unionin kyberturvallisuusvirasto Enisa, (2016) huomauttaa myös, että ei ole olemassa yleisesti määriteltyä ja hyväksyttyä määritelmää kyberturvallisuuden termille, koska termin määrittelyt liikkuvat useilla tasoilla ja erilaisilla konteksteilla. Myös Limnéll ym., (2014) huomioivat, että kyber-käsitteelle löytyy satoja erilaisia määritelmiä. Heidän mukaansa kyber-sana syntyi tarpeesta kuvata uutta toimintaympäristöä, siis fyysisen ja digitaalisen maailman yhteyttä. Tietoturva-termi ei tähän riittänyt, sillä sen merkitys oli jo vakiintunut kuvaamaan niin fyysisen kuin digitaalisen tiedon säilömisen turvaamista ja siihen liittyviä menettelytapoja (ks. myös Von Solms & Van Niekerk, 2013). Nykyisessä digitaalisessa maailmassa turvallisuus ei ole enää vain tietojen turvallisuutta, vaan se on koko kyberfyysisen maailman turvallisuutta, yhdistäen fyysisen ja digitaalisen maailman rajapinnat (Limnéll ym., 2014). Limnéll ym., (2014) määrittelevät kyberturvallisuuden tärkeimpien tekijöiden kautta: ”Kyberturvallisuus

tarkoittaa digitaalisen maailman tilaa, jossa vallitsee sekä ymmärryksen myötä tuotettu luottamuksen tunne että käytännön toimenpitein saavutettu kyky ennakoivasti hallita sekä sietää kyberuhkia ja niiden vaikutuksia”. (Limnéll ym., 2014.) Kokonaisturvallisuuden sanasto määrittää myös kyberturvallisuuden ja tietoturvallisuuden yhteen toteamalla, että ”kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä” (Sanastokeskus TSK, 2017). Laari ym., (2019) ja Suomen kyberturvallisuuden strategia (2013; 2019) määrittelevät kyberturvallisuuden ”tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Da Veiga (2016) puolestaan esittää kyberturvallisuuden tarkoittavan: ”Tietoresurssien ja ihmisten suojelemiseksi tarkoituksellisten ja tahattomien uhkien minimoimisena, lieventämisenä ja niihin reagoimisena kyberavaruudessa.” ISO/IEC:n standardissa 27032 (ISO/IEC, 2012), joka virallisesti käsittelee "kyberturvallisuutta" tai "kyberavaruuden suojausta", määritellään kyberturvallisuus "tietojen luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseksi kyberavaruudessa".

Von Solms & Von Niekerk (2013) ovat havainneet, että kyberturvallisuuden ja tietoturvan käsitteitä käytetään usein synonyymeina. Heidän mukaansa ne eroavat kuitenkin usealla tavalla: Tietoturvan osalta inhimillisellä tekijällä viitataan yleensä ihmisen rooliin tietoturvaprosessissa. Kyberturvallisuudessa inhimillisellä tekijällä viitataan sen lisäksi ihmisiin kyberhyökkäyksien kohteena tai tietämättään niihin osallistuvina subjekteina. Heidän mukaansa tällä lisäulottuvuudella on eettisiä vaikutuksia koko yhteiskuntaan, sillä tiettyjen haavoittuvien ryhmien, esimerkiksi lasten, suojelu voidaan nähdä yhteiskunnallisena vastuuna. Lisäksi, kun tietoturvan voidaan katsoa käsittävän lähtökohtaisesti vain tiedon turvaamisen, kyberturvallisuus ei ole vain kyberavaruuden suojaamista, vaan käsittää myös siellä toimivien henkilöiden ja omaisuuden suojaamisen. (Von Solms & Van Niekerk, 2013.)

Kuten sanottua, kyber -etuliitteeseen liitetään usein toimintaympäristö, muodostaen kybertoimintaympäristö -sanan. Kybertoimintaympäristöllä viitataan laajemmin ”ekosysteemiin, jonka osajärjestelmiä yhteiskuntien eri toimijat ovat” (Limnéll ym., 2014, 65). Laari ym., (2019) määrittelevät kybertoimintaympäristön olevan ”digitaalisista tietojärjestelmistä muodostuva toimintaympäristö, johon kuuluvat myös fyysiset rakenteet sekä kaikki toimintaympäristön toimijat.” Jotkut tahot käyttävät myös kyberavaruuden

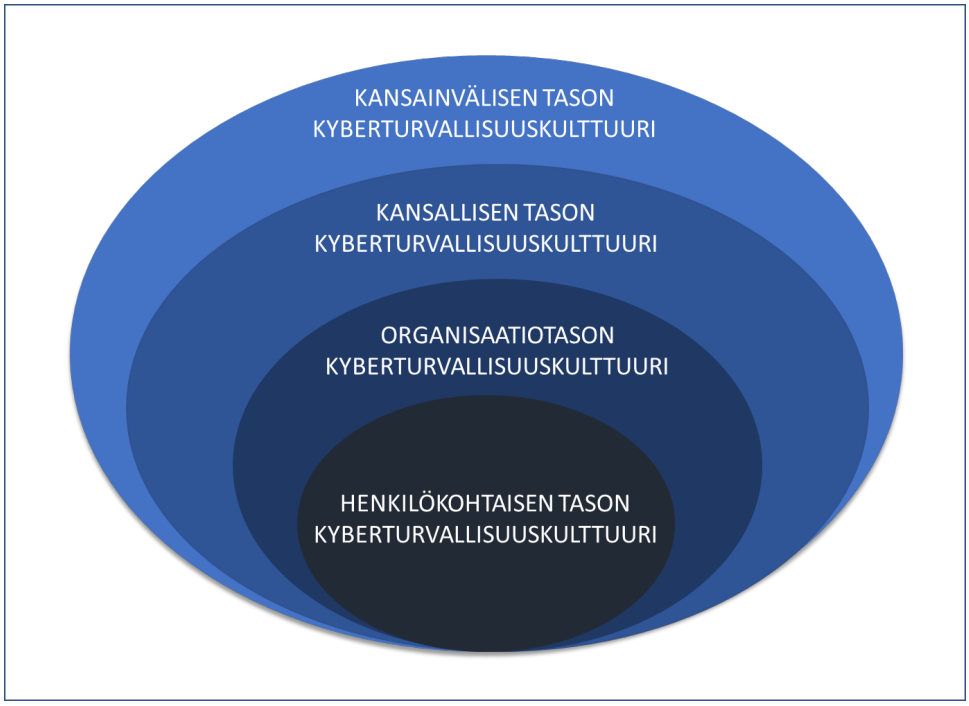
käsitettä (esim. Da Veiga, 2016), jolla puolestaan viitataan ihmisen ja digitaalisen ympäristön vuorovaikutukseen: "kyberavaruus määritellään "monimutkaiseksi ympäristöksi, joka syntyy ihmisten, ohjelmistojen ja palvelujen vuorovaikutuksesta internetissä siihen liitettyjen teknisten laitteiden ja verkkojen avulla, jota ei ole missään fyysisessä muodossa" (ENISA, 2016, 14–15).

Kuten aiemmin on sanottu, organisaation turvallisuutta voidaan parantaa turvallisuuskulttuuria ylläpitämällä (von Solms & von Solms, 2004; Vroom & von Solms, 2004; Thomson ym., 2006; Mishra & Dhillon, 2006). Sikäli, että tietoturvakulttuurin nähdään keskittyvän enemmän rajattuun kontekstiin sekä usein tiedon hallintaan ja turvaamiseen organisaation sisäisesti, kyberturvallisuuskulttuurin nähdään olevan tietoturva- ja turvallisuuskulttuureja huomattavasti laajempi kokonaisuus, kattaen kokonaisuuden yksilöstä, yksittäisestä tietoteknisestä laitteesta, yhteiskunnan kriittiseen infrastruktuuriin. (Da Veiga, 2016.)

Kyberturvallisuuskulttuurin avulla voidaan vaikuttaa käyttäjien kautta syntyviin tietoturvauhkiin ja parantaa organisaation suojautumista kyberuhkilta. Kyberturvallisuuskulttuuria ja sen arviointia voidaan hyödyntää esimerkiksi tietoturvariskien hallinnan osalta inhimillisen riskien ymmärtämiseen organisaatioissa. Lisäksi sen avulla voidaan havainnoida häiriötilanteisiin reagointia käyttäjän näkökulmasta sekä sitä voidaan hyödyntää erilaisten koulutusten kohdentamiseen esimerkiksi käyttäjille, joiden parissa kulttuuri ei ole vaaditulla tasolla. (Da Veiga, 2016.)

Euroopan unionin kyberturvallisuusviraston mukaan kyberturvallisuuskulttuurin käsite viittaa ihmisten tietoon, uskomuksiin, käsityksiin, asenteisiin, oletuksiin, normeihin ja arvoihin kyberturvallisuudesta ja siihen, miten ne ilmenevät ihmisten käyttäytymisessä tieto- ja informaatioteknologian kontekstissa (ENISA, 2017). Da Veiga (2016) puolestaan määrittelee kyberturvallisuuskulttuurin Da Veiga & Eloff (2010) tietoturvakulttuurimallin pohjalta. Kyberturvallisuuskulttuuri määritellään tarkoituksellisiksi ja tahattomaksi tavaksi, jolla kyberavaruutta hyödynnetään kansainvälisestä, kansallisesta, organisatorisesta tai yksilöllisestä näkökulmasta kyberkäyttäjän asenteiden, oletusten, uskomusten, arvojen ja tietämyksen yhteydessä. Syntyvästä kyberturvallisuuskulttuurista tulee tapa, jolla asioita tehdään vuorovaikutuksessa kyberavaruudessa, ja se voi joko edistää tai estää yksilöiden, organisaatioiden tai valtioiden, yksityisyyttä ja kansalaisvapauksia.

Kyberturvallisuuskulttuuri on siis moniulotteinen ilmiö, joka voidaan nähdä useilla eri tasoilla (Ks. kuvio 7.). (Da Veiga, 2016.)



Kuvio 6. Kyberturvallisuuskulttuurin tasot (mukaillen Da Veiga, 2016)

Yksilö, joka toimii kyberavaruudessa, on vuorovaikutuksessa kaikkien kyberturvallisuuskulttuurin tasojen kanssa. Organisaation näkökulmasta sen on keskeistä pyrkiä suojaamaan omaa toimintaansa minimoimalla kyberavaruuden aiheuttamia riskejä. Organisaation tasolla, kuin myös muilla tasoilla tarvitaan kyberturvallisuuskulttuuria, jonka kautta kyberavaruuden kanssa ollaan vuorovaikutuksessa tavalla, jossa yksilöiden käyttäytyminen edistää jokaisen tahon tietoturvallisuutta. Kyberavaruudessa henkilö voi aiheuttaa toiminnallaan riskiä niin omalle organisaatiolleen, muille henkilöille kuin myös itselleen, minkä vuoksi kyberavaruudessa toimivien henkilöiden asenteiden, oletuksien, uskomuksien, arvojen ja tietämyksen on keskeistä edistää turvallisuutta kyberavaruudessa. (Da Veiga, 2016.)

Kyberturvallisuuskulttuurin määritelmä käsittää siis tieto- ja viestintäteknologian, yksilöiden suojelun sekä organisaatiokulttuurin ja käyttäytymisen ymmärtämistä. Organisaatiolla tulisi olla asianmukainen hallintorakenne sekä selvät prosessit ja käytännöt, joilla organisaatiota sekä sen työntekijöitä ja asiakkaita suojellaan. (Da Veiga, 2016.) Kyberturvallisuuskulttuuria tarkastelemalla tietoturvakulttuurin ja organisaatiokulttuurien

rajapintojen kautta voidaan pyrkiä havainnoimaan organisaation henkilöstön tietoturvallista käyttäytymistä, asenteita, olettamuksia ja tietoisuutta ja pyrkiä vaikuttamaan niihin organisaation kyberturvallisuuden parantamiseksi ja kyberturvallisuuskulttuurin kehittämiseksi.

3 NARRATIIVISUUS LÄHESTYMISTAPANA ORGANISAATIOTUTKIMUKSESSA

Tutkielman alkuvaiheessa pohdittiin tutkimuksen näkökulmaa. Tämä tutkielman narratiivinen lähestymistapa sai innoituksensa ajatuksesta, jossa pohdittiin, millaisena ilmiönä kyberturvallisuuskulttuuri tutkijalle itselleen näyttäytyy. Kyberturvallisuuskulttuuri näyttäytyi tutkijalle kompleksisena ja moniäänisenä ilmiönä, josta ei ole olemassa yhtä tai edes useaa totuutta, vaan joka rakentuu organisaation ja ihmisten arvoissa ja sille antamissa merkityksissä. Kyseinen lähestymistapa kyberturvallisuuskulttuuriin sopii hyvin yhteen narratiivisen organisaatiotutkimuksen kanssa, jonka mukaan pelkät organisaatiokaaviot tai mekaaniset mallit eivät riitä tulkitsemaan nykyisiä suuria, kompleksisia ja dynaamisia organisaatioita. Tässä tutkielmassa päädyttiinkin narratiiviseen näkökulmaan, koska ihmisten johtamisessa ja tutkimisessa tarvitaan myös ymmärrystä tarinoista, jotka edellä mainitun mukaisesti toimivat keinona kommunikoida, järjestää, selittää ja ymmärtää inhimillistä elämää sekä ihmisten keskinäisiä suhteita, ja joiden kautta ihmiset tulkitsevat sosiaalista ympäristöään. (Puusa & Juuti, 2020, 243.)

Tämän tutkielman metodologisena lähtökohtana toimii narratiivinen tutkimuskenttä. Narratiiviseen tutkimukseen ei ole suoraa tietä – yhden suuntauksen sijaan se on kuin monitieteinen laadullinen tutkimusverkosto ja se käsittää useita erilaisia lähestymistapoja (Hänninen, 2018, 211). Narratiivisen tutkimuksen perusajatuksena on, että narratiivit eli kertomukset ja tarinat toimivat keinona kommunikoida, järjestää, selittää ja ymmärtää inhimillistä elämää ja ihmisten keskinäisiä suhteita. Elämän kulkua on luonteenomaista jäsentää kuin tarinoiden tai kertomusten kautta, kuvaten erilaisia tapahtumakulkuja lähtötilanteesta lopputilanteeseen. (Hänninen, Mönkkönen, Puusa, 2020, 241–242.) Kertomusten tutkiminen onkin keskeinen tapa ymmärtää ihmistä ja niiden toimintaa, sillä kertomukseen punoutuu ihmisen kokemus elämästä (Heikkinen, 2018, 190). Tarinat ovat myös olennainen vuorovaikutuksen väline, sillä kertomalla toisille jotain ”jaetaan ja tehdään ymmärrettäväksi kokemuksia, luodaan luottamusta ja ylläpidetään ryhmiä” (Hyvärinen & Löyttyniemi, 2005). Narratiivisen tutkimuksen ollessa hyvin monitieteinen, saatetaan siitä käyttää termejä narratiivinen, kerronnallinen, kertomuksellinen ja tarinallinen tutkimus (Heikkinen, 2018, 190). Heikkinen (2018) argumentoi, että osuvin suomennos käsitteestä olisi kerronnallinen tutkimus. Tässä tutkielmassa käytetään ja puhutaan selvyyden vuoksi

kuitenkin narratiivisesta tutkimuksesta, jolla viitataan nimenomaan tarinalliseen tutkimukseen.

Laadullisessa tutkimuksessa narratiivisuutta on hyödynnetty laajasti (Hirsjärvi, Remes & Sajavaara, 2007, 218). Tutkimuskirjallisuudessa narratiivisuus ja sen lähikäsitteet yleistyivät 1980-luvulla (Heikkinen, 2018, 190). Narratiivinen tutkimus nojasi postmoderniin aatteeseen ja pyrki erottautumaan tällöin vallalla olleesta positivistisesta tieteenkäsityksestä, jonka mukaan tieteen tulisi yrittää paljastaa yksiselitteisiä tosiasioita, jotka tuotettiin määrällisten tutkimusmenetelmien avulla (Puusa ym., 2020). Kyseessä oli laajempi tieto- ja tiedekäsityksen muutos kohti konstruktivismia. Se on ikään kuin vastakkainen näkemys positivismille. Se ilmentää relativismia, jonka mukaan tieto ja totuus ovat suhteellisia ympäristöön, jossa niitä tuotetaan, eikä yksiselitteistä tietoa siten ole olemassa. (Heikkinen, 2018, 198.) Tätä tiedekäsityksen muutosta on kuvailtu myös ”kielelliseksi käänteeksi”. Sen taustalla oli sosiaalisen konstruktionismin tutkimuksellinen viitekehys, joka katsoi todellisuuden rakentuvan kielellisessä vuorovaikutuksessa. (Kuortti, Mäntynen, Pietikäinen, 2008.)

Narratiivinen tutkimus on monitieteellistä ja moniulotteista (Riessman, 2008). Kertomuksia voidaan tarkastella monista eri tieteenaloista ja erilaisin näkemyksin. Tämä tutkielma sijoittuu narratiiviseen lähestymistapaan organisaatiotutkimuksessa. Organisaatio- ja johtamistutkimuksen parissa narratiivinen tutkimusote monipuolistui 2000-luvulla, ja narratiivit tunnistetaankin nykyään pelkän tutkimusaineiston sijaan myös metodiseksi lähtökohdaksi (Somers, 1994; Rhodes & Brown, 2005).

Eräs syy valita tähän tutkielmaan narratiivinen lähestymistapa oli sen edustama konstruktiivinen näkökulma. Sekä narratiivisuuden ja tutkijan ajattelutavat ovat toisaalta relativistisia: tutkija ei usko absoluuttisiin totuuksiin, vaan näkee, että totuus tai tieto rakentuvat kontekstissa, suhteessa sosiaaliseen ympäristöön. Tällöin nähdään, että on oleellista ymmärtää niitä tarinoita, joiden kautta ihmisen tulkitsevat sosiaalista ympäristöään. Kuten Riessmann (2008, 3) sanoo, kertomukset ja tarinat ovat aina tietyssä hetkessä, paikassa ja tietylle joukolle suunnattuja. Tämän vuoksi tarinat eivät heijasta täydellistä, kontekstista riippumatonta totuutta. Narratiivinen tutkimus korostaakin pluralismia, relativismia ja subjektiivisuutta. Sen perusolettamuksena on, että se ei etsi yhtä

ainoaa oikeaa totuutta, eikä se tarjoa yhtä oikeaa tapaa käsitellä aineistoa. (Lieblich ym., 1998, 2.)

Narratiivisuudella voidaan tarkoittaa montaa eri asiaa ja siitä puhutaan usein käyttäen päällekkäisiä käsitteitä. Narratiivisessa tutkimuksessa voidaan kuitenkin tunnistaa kaksi keskeistä käsitettä. Tässäkin kappaleessa aiemmin käytettyjä käsitteitä *tarina* ja *kertomus* käytetään toistensa synonyymeinä arkikielessä, mutta tutkimuksen osalta kirjallisuustieteen parissa tutkijat erottavat nämä käsitteet toisistaan ja näin on syytä tehdä tässäkin tutkielmassa. Tarinalla viitataan kertomuksen tapahtumarakenteeseen, eli tapahtumien kulkuun. (Hyvärinen & Löyttyniemi, 2005, 189; Heikkinen, 2018, 192.) Tarina muodostuu joukosta perättäisiä tapahtumia ja olevaisista. Kun näistä tapahtumista luodaan tulkinta, syntyy ajassa etenevä tapahtumakulku eli tarina, joka vastaa kysymykseen *mitä on tapahtunut?* Tapahtumat voivat olla tahallisia ja tarkoituksellisia tekoja sekä tahattomia sattumuksia, joiden tekijät eivät ole intentionaalisia olentoja eikä taustalla ole tietoista tai tarkoituksellista toimintaa. Olevaiset ovat tarkoituksellisia toimijoita, eli tarinan henkilöhahmoja, jotka ovat kykeneviä tarkoitukselliseen toimintaan sekä tapahtumapaikkoja, eli ympäristöjä, joissa tapahtumat tapahtuvat ja henkilöhahmot toimivat. (Hänninen, 2018; Heikkinen, 2018, 195.)

Yhdestä tarinasta voi olla olemassa useita erilaisia kertomuksia. Tämä tarkoittaa sitä, että tarina voidaan kertoa monella erilaisella tavalla sekä erilaisessa järjestyksessä, tarinan itsessään ollen kuitenkin jokaisessa tapauksessa sama. Tällaisia erilaisia kertomuksia voidaan kertoa esimerkiksi suullisesti, kirjallisesti tai kokonaan ilman näitä esimerkiksi kuvien ja liikkeen välityksellä. (Heikkinen, 2018, 192–193.) Hännisen (2018) mukaan kertomus on tarinan esitys erilaisten symbolien avulla: peräkkäisinä sanoina, kuvina tai liikkeinä. Kertomus esittää tarinan vastaanottajille ja se pyrkii saamaan nämä eläytymään tarinan tapahtumiin päähenkilön näkökulmasta. Kertomus kuvaa kerronnan keinoin tapahtumiin liittyviä tunteita ja muita kokemuksia. (Hänninen, 2018.) Abbottin (2009, 19) mukaan kertomus muodostuu, kun tapahtumakulku esitetään kerronnan avulla.

Heikkinen (2000; 2001; 2018, 195), joka käyttää narratiivisuudesta termiä *kerronnallisuus*, on tunnistanut, että kerronnallisuudella voidaan tarkoittaa neljää asiaa: Se voi viitata tietämisen tapaan ja tiedon luonteeseen sekä toisaalta kerätyn tutkimusaineiston luonteeseen. Se voi myös viitata aineiston analyysitapoihin tai tutkimuksen käytännön merkitykseen.

Kerronnallisuus tietämisen tapana ja tiedon luonteena viittaa konstruktiiviseen ja tulkinnalliseen tutkimusotteeseen. Kerronnallisuus nähdään ihmisiä kautta historian ja kulttuurien yhdistävänä tekijänä (Barthes, 1966; Heikkinen, 2018), ja kertomuksen voidaan nähdä olevan keino, jonka avulla ihminen ymmärtää elämäänsä (Hardy, 1987; Heikkinen, 2018). Tutkimusaineiston luonteena narratiivisuus viittaa kertomusluontoiseen kielenkäyttöön. Aineisto on tällöin kerrontaa suullisesti tai kirjallisesti esitetyssä muodossa. Käytännössä aineiston tunnuspiirteinä voidaan tällöin pitää myös muita kertomuksen tunnuspiirteitä, kuten ajassa etenevää juonta tai alku- tai loppupistettä, mutta yksinkertaisimmillaan narratiivinen aineisto voi olla mitä tahansa kerronnallista aineistoa. Aineiston analyysitapana narratiivisuus viittaa kahteen erilaiseen käsittelytapaan. Tästä kerrotaan lisää kappaleessa 4.3. Lopuksi, kerronnallisuus käytännön merkityksenä viittaa sen soveltamiseen ammatillisena työvälineenä. Usein tämä perustuu näkemykseen siitä, että ihmisen identiteetti muotoutuu kertomusten kautta. (Heikkinen, 2018, 195–204.)

Narratiivit paljastavat asioita yhteisön kulttuurista, moraalijäsennyksistä sekä tapahtumien merkityksestä narratiivin kertojalle (Cortazzi, 2001; Hänninen, 1999). Tarinat ja narratiivit tuovat tarinallisuudessaan esiin asioita yhteisön kulttuurista, ja saavat myös ihmisen ymmärtämään omaa elämäänsä kulttuurin tarjoamien tarinallisten mallien avulla. Tarinalliset rakenteet voivat myös paljastaa vallitsevan yhteisön uskomuksia ja moraalijäsennyksiä. (Hänninen, 1999.) Vaikka narratiivit paljastavat edellä kuvatun tavoin asioita kulttuurista ja yhteisöstä, eivät ne kuitenkaan ole suoria kuvauksia todellisuudesta, vaan versioita tai näkökulmia tapahtuneesta, jotka kuvaavat tapahtuman merkitystä ja tärkeyttä narratiivin kertojalle (Cortazzi, 2001). Asioiden kuvaamisen lisäksi narratiivit ovat myös keino jäsentää kertojan paikkaa maailmassa suhteessa itseensä ja muihin. Kertomukset toimivatkin erilaisten tunteiden, kokemusten ja tulkintojen sanoittajia sen lisäksi, että ne vain selittäisivät ympäröivää maailmaa, yhteisöjä ja kulttuureja. (Hyvärinen, 2006.)

Narratiivinen lähestymistapa hyödyttää tätä tutkielmaa luomalla mahdollisuuden tarkastella organisaatioita yksityiskohtaisesti korostaen toistuvia ominaispiirteitä, jolloin organisaation muutoksiin liittyvät syy-seuraussuhteet voivat paljastua. Organisaatio voidaan herättää henkiin kertomusten avulla, joista organisaation jäsenet voivat luoda merkityksiä tai rakentaa identiteettiään suhteessa kokemuksiinsa, tapahtumiin tai itse organisaatioon. (Rhodes & Brown, 2005.) Narratiivit voivat myös rikastuttaa näkemyksiä sosiaalisen elämän rakentumisesta (Czarniawska, 2004.)

Tässä tutkielmassa ei haluta testata teoriaa tai etsiä oikeiksi tai vääriksi miellettyjä asioita, vaan selvittää tyyppitarinoiden keinoin millaiset tekijät ja käsitykset ovat vaikuttaneet kyberturvallisuuskulttuurin olemukseen organisaatiossa. Kyberturvallisuuskulttuuri näyttäytyy tutkijalle kompleksisena ilmiönä, josta ei nähdä olevan olemassa yhtä tai useampaa totuutta. Kyberturvallisuus rakentuu haastateltavien sille antamissa merkityksissä, mikä sopii hyvin yhteen narratiivisen organisaatiotutkimuksen lähestymistavan kanssa.

4 TUTKIMUSAINEISTO JA MENETELMÄT

4.1 Tutkimuskontekstina kuntaorganisaatio

Tutkielman kohteen vuoksi on tarkoituksenmukaista avata sitä, minkä tyyppinen organisaatio kuntaorganisaatio on, mitkä ovat sen mahdollisia erityispiirteitä ja minkälaisessa toimintaympäristössä se toimii. Kappaleen tavoitteena ei ole luoda kokonaisvaltaista kuvaa kuntaorganisaatioiden maailmasta, vaan keskittyä lyhyesti taustoittamaan sitä kontekstia, missä tämä tutkielma on tehty.

Kunnalla tarkoitetaan Suomessa olevaa hallinnollista organisaatiota ja alueellista yksikköä. Kunnan olemus on ainakin kaksijakoinen, sillä se on yhtä aikaa paikallistasolla toimiva hallinto-organisaatio sekä paikallinen yhdyskunta. Kuntaa voidaan tarkastella kummankin olemuksen kautta. Kuntaorganisaation tasolla kunta nähdään organisaatioksi, joka koostuu kuntalaisten valitsemista luottamushenkilöistä sekä työ- ja virkasuhteisista työntekijöistä, ja jolla on omat rakenteet, prosessit ja organisaatiokulttuurit. Yhteisön tasolla kuntaorganisaatio käsitetään osaksi laajempaa paikallista yhteisöä, johon kuuluvat myös muut paikalliset instituutiot kuten kuntalaiset, järjestöt, yritykset ja valtion organisaatiot. Kummatkin tasot ovat monin eri tavoin kytkeytyneet toisiinsa. Kuntaa määrittelevät myös esimerkiksi maantieteellinen sijainti, yhdyskuntarakenne, väestön määrää, sosiaalinen rakenne, historia, arvot, kulttuuri ja identiteetti. (Rönkkö, 2003, 12–13; Anttiroiko ym., 2007; Haveri & Rönkkö, 2007.)

Kunnalla viitataan tässä tutkielmassa suomalaiseen julkisen hallinnon paikallistason hallinto-organisaatioon, joka käyttää alueellaan itsehallintoa ja lainsäädännön rajoissa sille määriteltyä julkista valtaa. Kunta tuottaa julkisia palveluja, joiden tuottaminen perustuu erityislakeihin (lakisääteiset tehtävät) tai vapaaehtoisuuteen. Kuntien toimintaa säädellään usein eri tavoin, mutta keskeisin toimintaa määrittävä laki on kuntalaki (KL 410/2015). Kuntalain tarkoituksena on luoda edellytykset kunnan asukkaiden itsehallinnon sekä osallistumis- ja vaikuttamismahdollisuuksien toteutumiselle kunnan toiminnassa (KL 410/2015 1§). Kuntalaki määrittelee kuntaorganisaation tehtävät, rakenteen sekä päätöksentekoprosessin. (Anttiroiko ym., 2007.)

Organisaatio on yhteistoimintatoimintajärjestelmä, jonka tarkoituksena on yhdistää resurssit jonkin tarkoituksen toteuttamiseksi. Yleisin tapa määritellä organisaatiota on tavoite- ja tehokkuusmalli, jonka näkökulmasta organisaatio on tarkasti suunniteltu järjestelmä, jonka tehtävä on toteuttaa sille asetetut tavoitteet. (Harisalo, 2007, 17, 31.) Haverin & Rönkön (2007, 67) mukaan organisaatiot muodostuvat tavoitteista ja päämääristä, rakenteista, jotka on muodostettu niiden saavuttamiseksi, ihmisistä ja toiminnoista sekä myös kulttuurista, joka ei välttämättä mukaile täysin tavoitteita. Kunnan päämäärät ja tavoitteet määritellään organisaation ylimmällä tasolla, kuntalain (KL 410/2015, § 14) mukaisesti ylintä päätösvaltaa käyttävässä elimessä eli kunnanvaltuustossa. Toisaalta kunnan tehtävät tulevat paljolti lainsäädännöstä, jolloin tavoitteiden ja päämäärien tulisi täsmentyä sitä kautta. Valtuusto koostuu kunnan asukkaiden valitsemista luottamushenkilöistä, jolloin kunnan johtamisen voidaan katsoa olevan luonteeltaan edustuksellista demokraattista johtamista. (Haveri & Rönkkö, 2007, 67.) Päätösvalta perustuu kunnissa hallintosääntöön, jonka kunnanvaltuusto määrittelee, ja jossa määrätään kunnan eri viranomaisen toimivallan jaosta ja tehtävistä. Päätösvallalla tarkoitetaan kunnan hoidettavaksi lain mukaan tai muuten kuuluvia asioita, joissa kunta voi tehdä tai joissa sen edellytetään tekevän päätöksiä. (Myllymäki, 2021; KL 410/2015, 14 §, 90 §.)

Tutkielman kohdeorganisaatio on Etelä-Suomessa sijaitsevan kaupungin hallinto-organisaatio. Kooltaan kaupunki sijoittuu kuntien kärkipäähän koossa mitattuna.

4.2 Tutkimusmenetelmänä laadullinen tutkimus

Tämä kuntaorganisaation kyberturvallisuuskulttuuria tutkiva tutkielma toteutetaan laadullisen eli kvalitatiivisen tutkimuksen keinoin. Laadullisen tutkimuksen tyypillinen piirre on, että sen tavoitteena on usein ymmärtää tarkasteluun valittua ilmiötä kohdehenkilöiden näkökulmasta. Tutkimuksessa ollaan siis kiinnostuneita kohdehenkilöiden ajatuksista, kokemuksista ja tunteista sekä merkityksistä, joita kohdehenkilöt ilmiölle antavat. (Puusa & Juuti 2020, 9.) Laadullisessa tutkimuksessa tutkimuskohteen kokonaisvaltaisen tutkimuksen avulla pyritään todellisen elämän kuvaamiseen. Tämä ajattelutapa toimii laadullisen tutkimuksen lähtökohtana. (Hirsjärvi, Remes, Sajavaara 2013, 161.) Alasuutarin (2011, 88) mukaan laadullinen tutkimus ja sen

aineisto on ”pala tutkittavaa maailmaa”, koska se on näyte tutkimuksen kohteena olevasta kielestä ja kulttuurista.

Teoria on olennainen osa laadullista tutkimusta (Tuomi & Sarajärvi, 2018, 21). Tässä tutkimuksessa viitataan laajasti erilaisiin tutkimuksiin eri tieteenaloilta. Tämän tutkielman aihe koskettaa perinteistä hallintotieteellisen tutkimuksen sekä ihmistutkimuksen, teknologiantutkimuksen ja käyttäytymiseen liittyvän tietojärjestelmien turvallisuuden hallinnoinnin tutkimusparadigmaa.

Tutkielman empiirinen aineisto ja tulokset ovat molemmat laadullisia. Empiirinen aineisto muodostuu kahdeksasta teemahaastattelusta, joista kerrotaan tarkemmin luvussa 4.3. Laadullisen tutkimuksen tulokset ovat yksityiskohtaisia tulkintoja tutkimusaiheesta, jotka tässä tutkielmassa tarjoavat kuvauksia henkilökohtaisesta kyberturvallisuuskulttuurista, organisaatiokulttuurista ja toimintaympäristöstä, kappaleessa 6.

4.3 Aineistonkeruumenetelmänä teemahaastattelu

Laadulliselle tutkimukselle on tyypillistä, että siinä pyritään tuottamaan rikasta ja yksityiskohtaista tietoa jostakin ilmiöstä. Tällaista tietoa pyritään hankkimaan ihmisiltä, jotka toimivat luonnollisissa ympäristöissään. (Puusa & Juuti 2020, 11.) Haastattelu on menetelmä, joka hyödyntää keskustelua ja vuorovaikutusta tuottaakseen tutkimusaineistoa, johon tutkimus perustuu ja josta tutkimustuloksia pyritään erilaisten analyysikeinoin tuottamaan. Kun haluamme ymmärtää ihmisten tapaa toimia, heidän mielipiteitänsä, käsityksiä ja uskomuksia, kerätä heistä tietoa sekä selvittää miten he arvottavat erilaisia asioita, on luonnollista keskustella ihmisten kanssa. Esimerkiksi vapaamuotoiset keskustelut voivat paljastaa sellaista tietoa, jota ei muuten saataisi selville. (Hirsjärvi & Hurme 2018, 10–11.) Haastattelu on hyvin joustava tutkimusmenetelmä ja se sopii erilaisiin tutkimustarkoituksiin. Sen aineistonkeruu on joustavaa ja sen ohessa voi esittää lisäkysymyksiä, jotka auttavat syventymään tutkimusaiheeseen. (Hirsjärvi & Hurme, 2018, 34.)

Tutkimushaastattelun lajeja on useita. Niistä käytettyjen nimikkeiden valikoima on osin jopa sekava ja samoilla nimillä saatetaan puhua erilaisista tai samankaltaisista menetelmistä. (Hirsjärvi & Hurme, 2018, 44.) Haastattelutyypit eroavat toisistaan lähinnä niiden ohjailevuuden perusteella eli sillä, kuinka vapaamuotoisesti haastattelu etenee (Puusa, 2020, 123). Keskeisimmät haastattelutyypit ovat strukturoitu ja standardoitu lomakehaastattelu, puolistrukturoitu haastattelu, teemahaastattelu, avoin eli strukturoimaton haastattelu ja syvähaastattelu (Hirsjärvi & Hurme, 2018, 44; Puusa, 2020, 123).

Strukturoitu haastattelu on käytetyin haastattelutapa. Siinä kysymysten ja väitteiden muoto ja esittämisjärjestys on määrätty ja se on kaikille vastaajille sama. Menetelmänä se on helppo ja tehokas tapa haastatella, sillä se vastaa käytännössä kyselylomakkeen täyttämistä ohjatusti. Puolistrukturoidussa haastattelussa tutkijalla on silloinkin etukäteen laaditut kysymykset, mutta joihin vastaukset tutkija saa haastateltavan sanoittamina. (Hirsjärvi & Hurme, 2018) Puolistrukturoitua haastattelua saatetaan joskus kutsua teemahaastatteluksi, vaikka ne eroavat toisistaan (Puusa, 2020). Täysin strukturoimattomasta eli avoimesta haastattelusta käytetään myös nimitystä syvähaastattelu, kliininen haastattelu, asiakaskeskeinen haastattelu ja keskustelunomainen haastattelu. Avoin haastattelu on keskustelun kaltainen tilanne, joka pyrkii pitämään haastattelun mahdollisimman vapaamuotoisena ja avoimena, mutta jossa aiheena on tutkijan etukäteen päättämä aihepiiri. (Tuomi & Sarajärvi, 2009) Tässä tutkielmassa haastattelut toteutettiin teemahaastatteluna, jossa kuitenkin pyrittiin mahdollisimman kattavaan avoimuuteen. Haastatteluita haluttiin ohjata pysymään teemassa, kuitenkin mahdollistaen haastattelutilanteen narratiivisuuden toteutumisen mahdollisimman hyvin.

Haastattelu on kansainvälisesti suosituin tapa kerätä ihmistieteellistä narratiivista aineistoa. Kaikkein toimivamman haastattelutavan nähdään tässä kontekstissa olevan narratiivinen haastattelu, jossa haastateltavaa pyydetään kertomaan oma tarinansa tutkimuksen kohteena olevasta asiasta. Kertominen on vapaamuotoista ja haastattelijan tehtäväksi jää aktiivinen kuuntelijan rooli, joka pyrkii kannattelemaan tarinan etenemistä. Lopuksi haastattelija voi myös esittää tarkentavia lisäkysymyksiä sekä täydentää kokonaisuutta esittämällä kysymyksiä asioista, jotka eivät ole nousseet esiin. (Hänninen, 2018.)

Vaikka laadullisessa tutkimuksessa on tavoitteena saada selville mahdollisimman autenttisesti tutkimuskohteiden kokemuksia, on tärkeää huomioida, että edes narratiivinen

haastattelumuoto ei tuo suoraa ikkunaa tarinan kertojan kokemuksiin ja tunteisiin. Tarinan kertoja ottaa aina huomioon vastapuolen odotukset, jolloin haastattelussa kuin haastattelussa toteutuneen tarinankerronnan voidaan nähdä olevan vuorovuorovaikutuksen tulosta. (Hänninen, 2018; Puusa & Juuti, 2020.) Lisäksi haasteena on, että tutkielman kohteena olevat henkilöt saataisiin puhumaan avoimesti omista kokemuksistaan. Puusan ja Juutin (2020) mukaan onkin tärkeää, että tutkija säilyttää neutraalin asemansa ja esiintyä luotettavana yhteistyökumppanina, jonka tarkoitusperät ovat hyvät.

4.3.1 Teemahaastatteluiden toteutus

Tässä tutkielmassa aineisto kerättiin kohdeorganisaatiosta teemahaastattelun muodossa. Vaikka narratiivinen haastattelu saatetaan nähdä sopivimmaksi haastattelutavaksi narratiivisen aineiston keräämiseen, tämän tutkielman osalta se ei palvellut tarkoitustaan. Ongelmaksi muodostui haastateltavien puutteellinen käsitys tutkielmassa käytettävistä käsitteistä sekä aihepiiristä, jonka vuoksi tutkija joutui ohjaamaan haastatteluja haluttua enemmän ja vaikuttamaan sen kulkuun. Teemahaastattelun keinoin kerätystä aineistosta voidaan nostaa esiin narratiivisia tulkintoja. Tällöin on tärkeää, että huomiota kiinnitetään teemahaastattelusta syntyvän tarinan luonteeseen. Tarina on ikään kuin haastattelijan ja haastateltavan yhteistä tuotosta, sillä se on syntynyt heidän välisessään vuorovaikutuksessa. (Hyvärinen & Löyttyniemi, 2005; Puusa ym., 2020.)

Haastateltavat hankittiin kohdeorganisaatiosta yleiseen jakoon julkaistun tiedotteen sekä suorien osallistumispyyntöjen avulla. Yleisen osallistumiskutsun jakaminen kohdeorganisaation sisäisesti on helppoa, mutta melko tehotonta. Yleinen kutsu ei puhuttele yksittäistä osallistujaa kovinkaan syvällisesti ja se on helppo ohittaa. Hirsjärven ja Hurmeen (2018, 85) mukaan yhteydenottaminen haastateltavaan onkin käytännössä hänen motivointiaan osallistumaan tutkimukseen. Kun tutkimuksesta kertoo potentiaaliselle haastateltavalle tarkemmin, se voi jopa innostaa haastateltavaa osallistumaan tutkimukseen. Suorien yhteydenottojen etuna ovat myös erilaisten suostuttelutekniikoiden hyödyntäminen, kuten jokaisen haastateltavan tärkeyden ja ainutlaatuisuuden korostaminen. (Hirsjärvi & Hurme, 2018.)

Teemahaastattelu sopii monenlaisten ilmiöiden tutkimiseen. Sen keskeisenä ajatuksena on, että tutkittavat ovat käyneet läpi tietyn asian tai prosessin, ja että tutkija selvittää tutkimuskohteen olennaisimmat tekijät kirjallisuuteen huolellisesti tutustumalla ja muotoilemalla niistä etukäteen teemoja ja tarkentavia kysymyksiä, joiden avulla teemahaastattelua viedään eteenpäin. Ratkaisevin asia onkin, että tutkija ymmärtää käsiteltävän ilmiön tarpeeksi hyvin ja kykenee näin purkamaan sen teemojen avulla osa-alueisiin, joiden sisältöä ja merkityksiä haastattelussa pyritään ymmärtämään. Teemahaastattelun on kuitenkin tarkoitus olla vapaamuotoinen ja joustava haastattelumenetelmä, eikä sen tarkoituksena ole edetä täysin suunnitelman mukaan johdonmukaisesti, vaan haastateltavaa kannustetaan kertomaan aiheesta vapaasti. (Puusa, 2020, 124–125.)

Teemahaastattelua käytettäessä yksi tärkeimmistä tehtävistä onkin haastatteluteemojen suunnittelu. Haastattelurunkoa laatiessa ei ole syytä laatia yksityiskohtaista kysymysluetteloa, vaan teema-alueluettelo. Ne ovat yksityiskohtaisempia kuin ongelmat ja ovat alueita, joihin haastattelukysymykset kohdistetaan. Haastattelutilanteessa niiden tarkoituksena on olla haastattelijan muistilista, sekä toimia keskustelua ohjaavana rakenteena. Teemat suunniteltiin aiempien tutkimusten ja kirjallisuuden perusteella sekä Adele Da Veigan (2016) mukaisen kyberturvallisuuskulttuurin käsitteen ja sen tasojen kautta (Ks. Kuvio 7).

Haastattelurunko (LIITE 1) sisälsi neljä teemaa:

1. Henkilön tausta
2. Henkilökohtainen kyberturvallisuuskulttuuri (henkilökohtainen suhtautuminen kyberturvallisuuteen)
3. Organisaatiokulttuuri (näkemykset organisaatiokulttuurista ja toimintaympäristöstä)
4. Organisaation kyberturvallisuuskulttuuri ja koettu kyberturvallisuus (Arvot, asenteet, merkitykset kyberturvallisuutta kohtaan)

Teema-alueet tarkennetaan kysymyksillä, joiden tarkentajana voi toimia niin tutkittava kuin tutkija – tällöin ilmiöön liittyvät moninaiset seikat paljastuvat mahdollisimman hyvin (Hirsjärvi & Hurme, 2018, 66). Tutkielmassa tätä asiaa pohdittiin tarkoin, sillä tutkimukseen tarvittiin haastattelumetodi, joka olisi ohjaavampi kuin avoin haastattelu, mutta jonka tulisi silti mahdollistaa aineiston narratiivisuus. Tutkielmassa suunniteltiin teemat neljään osa-

alueeseen ja niistä muotoiltiin melko abstrakteja. Teemojen tueksi suunniteltiin joitain ohjaavia kysymyksiä, joiden tarkoituksena oli toimia minulle ikään kuin muistilistana sekä myös tarpeen tullen ohjata keskustelua oikeaan suuntaan.

Haastattelutilaisuus aloitettiin esittäytymällä ja kertomalla tutkielman aihe. Sen jälkeen vuorovaikutuksen lisäämiseksi pyrittiin rakentamaan luottamussuhteen haastateltavan ja tutkijan välille (Ruusuvuori & Tiittula, 2005). Tavoitteena oli luoda vapaamuotoinen ja keskusteleva haastattelutilanne, jossa haastateltava tuntisi olonsa turvalliseksi. Tutkielmassa pyritään selvittämään kohteena olevien henkilöiden kokemuksia. Osa näistä kokemuksista voi olla arkaluontoisia. Tämän vuoksi haastattelutapahtuman täytyi tuntua turvalliselta ja luotettavalta. Tutkielmassa oli tärkeää, että tutkija ei ala rajaamaan keskustelun aiheita, jotta keskustelu saadaan pidettyä luontevana. Tutkijan tulee myös pystyä esittämään aiheesta selvästi muotoiltuja kysymyksiä, jotka haastateltava ymmärtää. Tutkija pyrkikin säilyttämään neutraalin aseman ja esiintymään luotettavana yhteistyökumppanina, jonka tarkoitusperät olivat hyvät. (Puusa & Juuti, 2020.)

Haastatteluita kertyi kahdeksan kappaletta ja niiden pituus vaihteli 50–70 minuutin välillä, joista syntyi litteroinnin jälkeen noin 120 sivua aineistoa. Tutkielmassa tavoitteena oli saada 10 haastattelua, mutta aikataulullisista syistä pitäydyttiin kahdeksassa haastattelussa. Kaikki haastatellut työskentelivät erään kaupunkiorganisaation hallinto-organisaatiossa. Haastateltavat haettiin avoimen yhteydenottopyynnön avulla ja sen perusteella, että heidän tuli toimia vähintään asiantuntijatason tehtävissä ja heidän tulisi olla työskennellyt organisaatiossa vähintään vuoden. Viimeiseksi mainittu ei toteutunut yhden haastateltavan kohdalla.

4.4 Narratiivinen temaattinen analyysi

Tässä tutkielmassa aineisto analysoidaan narratiivisen tutkimuskentän moninaisia menetelmiä mukaillen. Tutkimuksen analyysitapana käytettävässä narratiivisessa analyysissä on kyse laadullisesta menetelmästä, jossa analysoidaan aineistoa, joka kuvailee sattumia, tapahtumia ja tekoja. Narratiivisen analyysin kohteena voivat olla esimerkiksi erilaiset tekstit, kuvat, elokuvat, musiikki tai ympäristö, jotka nähdään kertomuksena ja niitä

tulkitaan tapahtumien kautta. (Hänninen, Mönkkönen, Puusa, 2020.) Tässä tutkielmassa mielenkiinto kohdistuu temaattisen analyysin tavoin erityisesti aineiston kertomusten sisällön merkityksiin, joita yksilöt muodostavat kokemilleen asioille oman elämäänsä liittyvien tarinoiden kautta. Tämän vuoksi analyysi tehdään narratiivisena temaattisena analyysina.

Narratiivisia analyysimenetelmiä on olemassa suuri ja jatkuvasti laajentuva joukko, ja niitä voidaan luokitella moniin erilaisiin päätyyppeihin. Luokittelussa keskeiseksi näkökulmaksi on muodostunut Hännisen (2018) mukaan se, ollaanko analyysissä kiinnostuneita sen sisällön merkityksistä vai ulkoisista piirteistä. Tässä tutkielmassa tarkastellaan kertomuksen sisällön merkitystä, jolloin ollaan kiinnostuneita kertomuksien sisällöistä. Toisinaan narratiivisessa analyysissa tarkastellaan kertomuksen ulkoisia piirteitä, jolloin kiinnostus kohdistuu kertomisen tapaan. (Hänninen, 2018, 218.) Myös Riesmann (2008) tunnistaa narratiivisen analyysin jakaantuvan kahteen leiriin, jotka ovat temaattinen ja rakenteellinen analyysi. Temaattisessa analyysissä keskitytään kertomuksen sisältöön, kuten sisällön merkityksien tutkimisessa. Rakenteellisessa analyysissa kohteena ovat kertomuksen rakenteelliset muodot, kuten kenelle kerrotaan, miten kerrotaan ja miksi kerrotaan. (Riesmann, 2008.) Tämän tutkielman analyysivaihe on toteutettu temaattisena analyysinä keskittyen tarinoiden sisällön merkityksiin.

Bruner (1986) on erottanut toisistaan kaksi eri tietämisen tapaa. Narratiivisuus tietämisen tapana keskittyy Brunerin mukaan muun muassa siihen, kuinka elämän eri vaiheita, toimintaa, kokemuksia, vastoinkäymisiä ja niiden seurauksia selitetään, paikallistetaan, ajallistetaan ja liitetään toisiinsa, joista myös tässä tutkielmassa ollaan kiinnostuneita. Narratiivinen tietämisen tapa ja täten myös tämä tutkielma keskittyvätkin tapahtumien välisiin yhteyksiin, eivätkä paljastamaan kausaalisia syy-seuraussuhteita tai käsitteellistämään ilmiöitä. Se pyrkii oivaltamaan, ymmärtämään ja hahmottamaan maailmaa kokonaisvaltaisesti. (Bruner, 1986; Heikkinen, 2018.) Samoin Polkinghorne (1988) on todennut narratiivien olevan ensisijainen yksilön kokemusten merkityksellistämisen muoto, ja käsittänyt ne keskeiseksi osaksi kulttuurista ja sosiaalista ympäristöämme. Polkinghornen (1988) mukaan kieli on tiedon muodostamisen, järjestelyn, suodattamisen ja merkitysten luomisen perusta. (Polkinghorne, 1988; Heikkinen, 2018.)

Polkinghorne (1995) on myös erottanut, että narratiivisuus voidaan nähdä aineiston analyysitapana kahdella eri tavalla: narratiivien analyysinä ja narratiivisena analyysinä (Polkinghorne 1995; Heikkinen, 2018). Jaottelu perustuu Brunerin (1986) tapaan erotella toisistaan kaksi erilaista tietämisen tapaa. Brunerin (1986) mukaan kertomukseen perustuvaa ymmärryksen muotoa kutsutaan narratiiviseksi tiedon muodoksi ja loogisten propositioiden avulla esitettävää tietoa loogis-tieteelliseksi tai paradigmaattiseksi tietämisen muodoksi. Jaottelu narratiivien ja narratiiviseen analyysiin pohjautuu näihin kahteen tietämisen tapaan. Kun aineistoa luokitellaan ja järjestellään erilaisiin kategorioihin ja tapaustyyppeihin, sovelletaan analyysissä pragmaattista tietämistä eli narratiivien analyysiä. Pragmaattiselle tietämiselle ominaista on matematiikan ja logiikan täsmällinen argumentaatio ja käsitteiden määrittely. (Bruner, 1986; Heikkinen, 2018, 202.) Narratiivisessa analyysissa keskitytään siis kerrontaan ja se käyttää eri tekniikoita edellä mainitun mukaisesti analysoidessaan esimerkiksi kerronnan tapaa, juonta tai kertomuksen rakennetta (Eriksson & Kovalainen, 2008, 217). Narratiiviselle tietämiselle ominaista on sen sijaan kertomuksen tuottaminen temaattisesti ja johdonmukaisesti. Kun tavoitteena on kokonaisnäkemyksen muodostaminen, jonka tarkoituksena on pilkkomisen sijaan kokonaisuuden rakentaminen, sovelletaan narratiivista tietämistä eli narratiivista analyysiä. (Heikkinen, 2018, 202.) Tällöin narratiivinen analyysi pyrkii järjestelemään ja tulkitsemaan empiiristä aineistoa, jossa on sattumia, tapahtumia ja tarinankulkuja ja muodostamaan niistä yhden tai useamman kertomuksen, jota tulkitaan ja josta keskustellaan eri tavoin (Eriksson & Kovalainen, 2008, 217). Tässä tutkielmassa aineisto analysoidaan narratiivisena analyysina.

Empiirisen aineiston analyysi on toteutettu narratiivista temaattista analyysia eli käytännössä sisällönanalyysia soveltaen. Narratiivisessa tutkimuksessa temaattisella analyysillä voidaan tarkoittaa kahta hieman erilaista analyysitapaa. Ensimmäisen tavan mukaisesti empiirisestä aineistosta koostetaan teemoja, joista tutkija muodostaa tarinankerronnan ja teemat, jotka yhdistetään tarinoiksi. Toinen vaihtoehto on temaattisen analyysin tapa, jossa analysoidaan muiden toimijoiden tuottamia narratiiveja, kuten esimerkiksi omaelämänkertoja, joista pyritään etsimään yhteisiä teemoja tai toistuvia toimintamalleja. (Eriksson & Kovalainen, 2008, 217–218.) Temaattisessa analyysissa ei yleensä kiinnitetä huomiota kieleen, sen muotoon tai vuorovaikutukseen haastattelutilanteessa. Kaikessa narratiivisessa tutkimuksessa keskitytään jollain tapaa sisältöön, kuten esimerkiksi siihen mitä on sanottu, kirjoitettu tai näytetty, mutta temaattisessa analyysissa tutkija on ainoastaan kiinnostunut siitä, mitä sanotaan. (Kohler Riessman, 2008, 53–59.)

Tässä tutkielmassa seuraan pääsääntöisesti ensimmäiseksi mainittua temaattisen analyysin mallia. Tällöin on huomattava, että tutkijan rooli narratiivien muodostamisessa on suuri. Narratiivit ovat tutkijan rakentamia, jolloin tutkijan tulkinta näkyy selvästi, eikä siltä voi välttyä tuloksissa. (Eriksson & Kovalainen, 2008, 217–218.) Tässä tutkielmassa ollaan kiinnostuneita ainoastaan siitä, mitä haastattelujen sisältö kertoo ja miten se vastaa tutkimuskysymykseeni. Aihepiirin ollessa haastateltaville jossain määrin tuntematon ja käytettyjen käsitteiden ollessa vakiintumattomia ja teknisiä, saatettiin niitä käyttää kuvaamaan hyvin erilaisia asioita. Tässä mielessä puheen tavan analysointi ei olisi kovin mielekästä ja sisällön merkitys korostuu.

Tämän tutkielman temaattinen analyysi etenee käytännössä aineistolähtöisen sisällönanalyysin prosessin mukaisesti. Temaattinen analyysi ja sisällönanalyysi ovat melko samanlaisia analyysitapoja, mutta niiden välillä on kuitenkin eroja. Käytännössä ne kummatkin noudattavat samoja periaatteita ja logiikkaa ja molemmat voivat olla joko aineisto- tai teorialähtöisiä. Aineistolähtöinen analyysi ei nojaa mihinkään etukäteen valittuun teoriaan, eikä siinä ole ennalta muotoiltuja analyysiyksiköitä. Tutkija valitsee analyysiyksilöt aineistosta. (Tuomi & Sarajärvi, 2018, 146.) Tuomen ja Sarajärven (2018) mukaan keskeinen ero näiden kahden analyysitavan välillä on, että sisällönanalyysissa aineisto pilkotaan pelkistetyksi palasiksi, jonka jälkeen se kootaan alaluokkien ja yläluokkien muodostamaksi hierarkiaksi. Temaattisessa analyysissa sen sijaan tunnistetaan johtoajatuksia, joista koostetaan esimerkiksi käsitekartan mukainen teemaan liittyvä kokonaisuus. Olennaista on, että teemat eivät ikään kuin itsestään nouse aineistosta, vaan ne ovat aina tutkijan oman tulkinnan ja päätelmän mukaisia. Tällöin tulkinta on hyvin paljon riippuvaista tutkijasta ja samasta aineistosta on mahdollista saada erilaisia tulkintoja. (Tuomi & Sarajärvi, 2018, 147–148.)

4.4.1 Aineiston analyysin käytännön toteutus narratiivisen temaattisen analyysin keinoin

Tutkimuksen aineiston analyysin käytännön toteutuksessa apuna käytettiin Tuomen ja Sarajärven (2018) esittelemää Milesin ja Hubermanin (1994) mukaista aineistolähtöisen laadullisen aineiston analyysiprosessia sekä Braun ja Clarken (2006) mukaista temaattisen analyysin runkoa. Aineistolähtöinen sisällönanalyysi koostuu käytännössä kolmivaiheisesta analyysiprosessista: 1) aineiston redusointi eli pelkistäminen, 2) aineiston klusterointi eli

ryhmittely ja 3) abstrahointi eli teoreettisten käsitteiden luominen. (Tuomi & Sarajärvi, 2018.) Mainittuja analyysiprosesseja seurattiin siksi, jotta analyysi olisi säännönmukaisempaa, eikä etenisi pelkästään intuition varassa.

Aineiston analyysi alkoi jossain määrin jo haastatteluiden aikana. Tukija muodosti jo haastatteluiden aikana itselleen kokonaiskuvaa aineistosta, ja siitä mitä haastatteluissa kerrottiin. Jotta aineistoa olisi mahdollista analysoida täytyi tallenteet litteroida. Jokainen haastattelu pyrittiin litteroimaan kokonaisuudessaan jo ennen seuraavaa haastattelua. Tämä ei onnistunut muutaman haastattelun kohdalla, mutta muutoin se auttoi haastatteluiden sisällön hahmottamisessa, kun uutta tallennetta litteroidessa saattoi jo hahmottaa yhdistäviä teemoja. Litterointitapoja on myös olemassa erilaisia. Tällä viitataan litteroinnin tarkkuuteen, eli asioihin, joita litteroinnissa otetaan huomioon. Tarkka litterointi voi ottaa huomioon eleilmaisun piirteitä, tai se voi olla vain hyvin yksityiskohtaisesti eli sanatarkasti tehty. Mikäli aineistoa analysoidaan vuorovaikutuksen kannalta, on litteroinnin tarkkuus hyvin tärkeää. Litterointiin voi myös sisällyttää sanojen lisäksi äänenvoimakkuutta, painotuksia ja taukoja. (Hyvärinen & Lyöttyniemi, 2005, 16, 178.)

Koska tutkielmassa ollaan kiinnostuneita aineiston sisällöstä ja myös piilevistä merkityksistä, tallenteet litteroitiin sanatarkasti. Litterointiin ei sisällytetty muita ulottuvuuksia kuin sanat, koska tutkielmassa ei ollut tarkoitus tutkia esimerkiksi vuorovaikutukseen liittyviä asioita, eikä sitä, miten asioista kerrotaan. Tutkielma keskittyi sisällön ymmärtämiseen, asioihin, joita haastatellut kertoivat. Haastattelut olivat kokonaisuudessaan hyvälaatuisia, vaikkakin joitain kertoja yhteyden pätkimisen vuoksi haastateltavien ääni puuroutui.

Aineistoon tutustuttiin lukemalla se läpi useaan otteeseen ja toisella lukukerralla tutkija alkoi muodostamaan parempaa kokonaiskuvaa aineistosta. Tutkija kiinnitti jälleen erityistä huomiota siihen, ettei hän anna omien ennakkoasenteideni vaikuttaa lukemaansa ja pyrki välttämään johtopäätöksien muodostamista. Seuraavaksi tutkija siirtyi aineiston pelkistämiseen ja ryhmittelyyn, pyrkien poimimaan aineistosta kaikki olennaiset asiat. Aineistoa pelkistettiin värittämällä samaa tarkoittavat ilmaisut, jonka jälkeen ne ryhmiteltiin koodaamalla ne yhden koodin alle. Aineistolähtöisen analyysin merkityksessä aineistoa koodattiin hyvin reilulla kädellä ja vapaasti. Koodauksen edetessä järjesteltiin myös samaa tarkoittavia koodeja toisiinsa sekä karsittiin pois epäolennaisia.

Analyysin kolmantena vaiheena oli aineiston ryhmittely teemoihin ja sen tyypittely. Nämä käsitellään samassa kappaleessa, sillä tyypittely edellyttää jonkin tarinajoukon määrittelyä, kuten esimerkiksi teemoittelua (Eskola & Suoranta, 1998, 153). Näitä menetelmiä mukaillen muodostui analyysin kolmas ja viimeinen vaihe. Aineisto teemoiteltiin Puusan & Juutin (2020, 171) mukaisesti tunnistamalla aineistosta usealle haastatellulle yhteisiä ja säännönmukaisia piirteitä.

Tässä vaiheessa tyypittely tuntui loogiselta jatkumolta analyysiin. Puusan & Juutin (2020, 172) mukaan tyypittelyllä voidaan etsiä niin yleisiä, kuin myös tyypillisestä poikkeavia ilmiöitä. Tyypittely mahdollisti myös analyysin tuloksien kuvaamisen tarinamaisessa muodossa. Sen pohjalta muodostin tyyppitarinoita, jotka eivät muodostu yhden haastateltavan vastauksista, vaan ne on koostettu useiden haastateltujen vastauksista yhdistävien tekijöiden pohjalta. Pyrkimyksenä oli tuoda esiin ilmiön monipuolisuus kohdeorganisaation kontekstissa, jolloin tyyppitarinat mahdollistivat kattavamman ja helpommin luettavan kuvauksen ilmiöstä organisaation kontekstissa, tuomalla esiin kutakin joukkoa kohden yhden tarinan. Kuten Eskola & Suoranta (1998, 137) ilmaisevat, ”*Laadullisen aineiston analyysin tarkoitus on luoda aineistoon selkeyttä ja siten tuottaa uutta tietoa tutkittavasta asiasta. Analyysilla pyritään aineisto tiivistämään kadottamatta silti sen sisältämää informaatiota; päinvastoin pyritään informaatioarvon kasvattamiseen luomalla hajanaisesta aineistosta selkeää ja mielekästä*.”

Tyyppitarinoiden koostamisessa on mahdollista, että tarinoiden ulkopuolelle jää paljon sellaista, mitä tyyppitarinaan ei voitu liittää. Tutkijan oman tulkinnan kautta näin ei kuitenkaan tapahtunut, vaan jaottelemalla tyyppitarinat kolmen kuvailevan narratiivin alle, tyyppitarinat saatiin rajattua suppeiksi kuvauksiksi ilmiöstä. On kuitenkin huomattava, että narratiivisen tutkimusmenetelmän suoman vapauden turvin tyyppitarina on osittain fiktiivinen ja hyvin pelkistetty kuvaus ilmiöstä. Tutkija on luonut ilmiölle tyyppikertomukset, jotka sisältävät elementtejä yhden tai useamman vastaajan teemoista. Tyyppitarinat eivät siis ole lainauksia tutkielman aineistosta, vaan niiden tarkoitus on kuvata analyysissä muodostuneita teemoja ja siten ilmiön piirteitä. Tyyppitarina on tutkijan luoma ja sisältää siis tutkijan tulkintaa ja tekemiä valintoja. En väitä, että jokainen haastateltava tunnistaisi oman kokemuksensa tekemistäni tulkinnoista. Lopulta tulkinnan tekeminen on juuri lukijan vastuulla. Tyyppitarinat muodostettiin teemojen kautta esittämällä aineistolle

seuraavia kysymyksiä: Mikä on haastateltavan tausta? Missä työtehtävässä hän työskenteli? Mikä on teeman pääsanoma?

Analyysin pohjalta muodostettiin lopulta kolme narratiivia, jotka kuvaavat henkilökohtaista kyberturvallisuuskulttuuria, organisaatiokulttuuria ja toimintaympäristöä sekä kyberturvallisuuskulttuuria. Narratiivi on siis tässä tapauksessa yksi iso tarinallinen kokonaisuus, joka muodostuu haastatteluista muodostetuista teemoista ja niistä koostetuista tyyppitarinoista. On korostettava, että tyyppitarinat eivät ole sitaatteja haastateltujen kertomuksista, vaan ne ovat osittain fiktiivisiä ja ovat koostettu usean eri haastatellun kertomuksista.

Tyyppitarinan jälkeen analyysissa syvennytään nostamaan litteroidusta haastatteluaineistosta esiin tyyppitarinaan liittyviä aineistositaatteja, joilla saadaan luotua tarinoihin syvyyttä sekä tuotua tutkijan tekemiä tulkintoja. Sitaatit antavat myös lukijalle näkemyksen aineistoon ja lisäävät täten tutkimuksen luotettavuutta. Huomionarvoista on kuitenkin se, että yksittäiset sitaatit eivät todenna koko aineiston sisältöä eivätkä ne riitä perustelemaan tutkielman tuloksia tai johtopäätöksiä (Puusa & Juuti, 2020, 173). Tekstissä olevat sitaatit liittyvät niitä edellisiin lauseisiin. On huomattava, että sitaateissa oleva teksti saattaisi sopia myös toiseen kohtaan. Sitaatit ovat sisennetty ja kirjoitettu kursivoidulla tekstillä, jotta ne olisi helppo erottaa. Ne on muutettu osittain yleiskielisiksi ja niistä on poistettu kaikki mahdolliset tunnistetiedot, säilyttäen kuitenkin sitaatin alkuperäisen merkityksen mahdollisimman tarkkaan. Kolmoispiste sitaatin sisällä tarkoittaa, että sen edestä, välistä tai lopusta on poistettu tekstiä.

4.5 Tutkielman eettisyys ja tutkijapositio

Tutkielmassa ja tulosten raportoinnissa noudatettiin Tutkimuseettisen neuvottelukunnan hyvä tieteellinen käytäntö -ohjetta (ks. Tenk, 2013). Tutkielmassa kiinnitettiin erityistä huomiota huolellisuuteen ja rehellisyyteen sekä kunnioitin muiden tekemää työtä merkitsemällä lähdeviitteet aikaisempaan tutkimukseen tarkoituksenmukaisella tavalla. Tutkielman kohteena olevalta organisaatiolta haettiin tutkimuslupa ennen aineiston keräämistä. Tutkielman alusta alkaen haastattelupyyntöjä suunnitellessa tutkija halusi olla

haastateltaville mahdollisimman avoin. Haastattelupyyntöjen ohessa haastateltaville jaettiin tutkimuksen esittelylomake sekä tietosuojalomake, johon tutkija oli pyrkinyt avaamaan tutkimuksessa tehtyjä valintoja mahdollisimman selväsanaisesti. Samalla haastateltavilta kerättiin kirjallinen suostumus tutkielmaan osallistumiseksi. Tutkielmasta kerrottiin haastateltaville helposti ymmärrettävällä kielellä, mainiten myös haastateltavan oikeudet sekä yksityisyydensuojaan liittyvät asiat. Tämä oli tärkeää, jotta tutkija sai luotua mahdollisimman luotettavan suhteen itsensä ja haastateltavan välille. Haastattelutilanteen alkuun tutkija oli myös varannut hieman ylimääräistä aikaa yleiselle keskustelulle, jolloin haastateltava saattoi esittää tutkijalle haluamiaan kysymyksiä. Samalla sen oli tarkoitus tuoda tilanteeseen luonnollisuutta ja aloittaa tutkijan sekä haastateltavan välinen vuorovaikutussuhde.

Tutkielmassa tärkeäksi periaatteeksi nousi haastateltavien anonymiteetti. Haastattelutilanteessa saatettiin käsitellä haastateltaville sensitiivisiä asioita, jonka vuoksi kunkin haastatellun anonymiteetti oli turvattava. Lisäksi oli oleellista, että tutkielmaan osallistujille ei koituisi henkisiä, taloudellisia tai sosiaalisia haittoja. Jokaiselle haastateltavalle kerrottiin anonymiteettiin liittyvistä seikoista. Haastattelutilanteet nauhoitettiin ja tallennettiin tutkijan tietokoneelle. Haastattelutallenteet olivat aluksi videomuodossa, sisältäen jatkuvan videokuvan haastattelutilanteesta. Tallenteista eriytettiin pelkkä ääni ja videomuotoiset tallenteet poistettiin, koska tutkielmassa oltiin kiinnostuneita vain haastateltavien puheessa antamista merkityksistä. Haastattelutallenteita säilytettiin ajantasaisia tietoturvallisia menettelyjä käyttäen tutkijan henkilökohtaisella tietokoneella lokaalisti, salatussa salananoin suojatussa järjestelmäosiossa sekä varmuuskopiona erillisellä salatulla muistilevyllä. Aineisto säilytettiin siten, että muilla henkilöillä ei ollut pääsyä siihen. Haastattelutallenteiden litteroinnin ohessa aineisto anonymisoitiin poistamalla tai koodaamalla aineistosta kaikki tunnistetiedot siten, että yksittäistä henkilöä ei voi aineistosta tunnistaa. Tutkielman lopuksi haastatteluaineisto tuhottiin. Narratiivisen tutkimuksen keskeisenä piirteenä oleva tarina voi myös olla haastava tekijä anonymisoinnin kanssa. Vaikka tuloksissa käytettyjen aineistositaattien osalta olisi toteutettu hyvin tarkka anonymisointi, voi henkilön puhetyyli tai tarina olla silti tunnistettavissa (Hänninen, 2018, 227). Tutkija päätyi vähentämään tätä mahdollisuutta yleiskielistämällä aineistositaatit, kuitenkin säilyttämällä sitaatin alkuperäisen merkityksen mahdollisimman hyvin. Lisäksi tutkielmassa kerrotaan haastateltavista mahdollisimman yleisluontoisella tavalla, välttäen tarkkoja luokitteluja.

Narratiivisessa tutkimuksessa tutkijan rooli on hyvin korostunut. Hyvin monitieteisenä tutkimusalana ja erilaisten analyysimenetelmien kyllästämänä tutkijalla on paljon valtaa siihen, kuinka hän lopulta tutkimuksensa suorittaa ja millaisia tulkintoja hän tekee (Heikkinen, 2018). Heikkisen (2018, 200) mukaan narratiivinen tutkimus on ymmärtämisen ja tulkinnallisuuden vuoksi melko lähellä fenomenologista ja hermeneuttista tutkimusta. Kuten fenomenologisessa ja myös muussa laadullisessa tutkimuksessa, on tutkijan ollut syytä pohtia avoimuuttaan tutkimusta kohtaan. Eskolan ja Suorannan (1998) mukaan laadullisessa tutkimuksessa tutkijalla ei tulisi olla ennakko-olettamuksia tutkimuksen tuloksista tai tutkimuskohteesta. Toisaalta nykyaikaisemman käsityksen mukaan laadullinen tutkimus ei koskaan voi olla täysin vapaata ennakkokäsityksistä, koska tutkijan arvot ja ennakkokäsitykset ohjaavat tulkintoja (Hirsjärvi ym., 2007). Tämän vuoksi tutkija on pyrkinyt huomioimaan tutkimusprosessissa omia ennakko-oletuksiaan tutkimusaiheesta kirjaamalla niitä ylös tutkimuksen edetessä. Tavoitteenani ei ollut niinkään fenomenologisen reduktion kaltainen prosessi, vaan pikemminkin se nähtiin keinona parantaa omaa ymmärtämistä ja tulkintaa aineistosta. Tämä korostui varsinkin analyysiosiossa, jolloin tutkija nosti esiin aineistosta oman tulkintansa kautta merkityksellisiä teemoja. Teemoja pohtiessani tutkija piti ennakkokäsitykset selkeästi mielessään koko prosessin ajan. Tutkija oli tutkittavan organisaation ulkopuolinen, eikä hänellä ollut varsinaista ennakkokäsitystä kohdeorganisaatiosta. Tutkija on myös itse kiinnostunut kyberturvallisuudesta ja kuluttaa paljon aihepiiriin liittyvää mediaa – siten hänellä oli ennakkokäsityksiä siitä, millaisia tarinoita aihepiiristä saattaisi tulla ilmi. Kokonaisuudessaan tärkeää oli ymmärtää omien kokemusten ja käsitysten vaikuttavan tutkimusprosessin keskeisiin osiin.

5 TARINOITA KYBERTURVALLISUUDESTA

5.1 Kyberturvallisuuden monet kasvot – narratiivi henkilökohtaisesta kyberturvallisuuskulttuurista

Ensimmäinen analyysissä muodostunut narratiivi kuvaa henkilökohtaista kyberturvallisuuskulttuuria ja henkilökohtaisia käsityksiä kyberturvallisuudesta. Narratiivi koostuu kolmesta erilaisesta tyyppitarinasta. Tyyppitarinat kuvaavat ilmiötä kolmesta eri näkökulmasta. Kyberturvallisuus näyttäytyy laajana ja ihmisten puheessa erilaisia merkityksiä saavana asiana. Tarinoissa kyberturvallisuuteen suhtaudutaan vaihtelevasti: siitä muodostetaan merkityksiä työkokemuksen, koulutuksen ja henkilökohtaisen elämän kautta ja käsitykset kyberturvallisuudesta ja siihen kuuluvista osa-alueista vaihtelivat haastateltujen kertomuksissa. Kyberturvallisuuteen liitetään eri asioita vastaajasta riippuen. Esiin nousivat niin sosiaalinen media, tietosuoja, tietoturva ja yleinen turvallisuus, ja käsitteet saivat haastatteluissa myös päällekkäisiä merkityksiä. Sekaannusta aiheutti esimerkiksi kyberturvallisuuden ja tietosuojan päällekkäisyydet ja erot. Useimmat haastateltavat myös pitivät kyberturvallisuutta ja tietoturvallisuutta lähes samana asiana.

Yleisesti ottaen epävarmuus on vahvasti läsnä henkilökohtaisessa kyberturvallisuudessa ja luottamus kybermaailmaa kohtaan on arkailevaa. Työntekijän arjessa epävarmuus ja luottamuksen puute kybermaailmaa kohtaan näkyy jatkuvana epäilyksenä omia teknologisia taitoja kohtaan. Haastateltavat epäilivät myös teknologisten laitteiden sekä ohjelmistojen turvallisuutta. Tietoturvallisuuteen liittyvät työtehtävät vaikuttivat työntekijöiden tulkintoihin kyberturvallisuudesta. Toisaalta vähäinen tai epäsuora kosketuspinta kyberturvallisuuteen johti kyberturvallisuuden kokemiseen epäselkeänä kokonaisuutena. Haastateltavien työkokemuksesta kumpuava tietämys siis yleisesti ottaen lisäsi tietämystä kyberturvallisuudesta. Henkilökohtaisen kyberturvallisuuskulttuurin ominaisuuksia kuvataan tarkemmin Tuukan, Tiinan ja Artun tyyppitarinoiden avulla.

5.1.1 Tyyppitarinat henkilökohtaisesta kyberturvallisuuskulttuurista

Tuukka Tavallisen tyyppitarina

Tuukka Tavallinen herää aamulla kotonaan. Tänään on etätyöpäivä. Rutiininomaisesti Tuukka avaa työtietokoneensa ja menee hakemaan keittiöstä kupin kahvia. Käyttäjätilille kirjautuessaan Tuukka muistaa VPN-yhteyden, mutta ei viitsi tällä kertaa laittaa sitä päälle. Sehän hidastaa yhteyksiäkin.

Sähköpostin avattuaan Tuukka huomaa ilmoituksen tietoturvakoulutuksesta ja lukee sen. Ilmoitus ei ole ensimmäinen Tuukalle saapunut, mutta nyt määräaika koulutuksen suorittamiseen on umpeutumassa. Se täytyisi suorittaa tänään. Hän on työskennellyt tässä työpaikassa jo useita vuosia. Hänen tehtävänkuvaansa ei kuulu mitään turvallisuuteen liittyvää, mutta koulutus on hänestä silti tärkeä. Sitä on vain jotenkin vaivaannuttavaa tehdä. Koulutuksessa Tuukkaa pyydetään arvioimaan omat teknologiset taitonsa. Tuukka vastaa uskovansa pärjäävänsä arjessa, mutta epäröivänsä internetin käyttöä silti ja olevansa hyvin skeptinen. Tuukka huolehtii aina, että tietokoneella on virustorjuntaohjelmisto. Koulutus päättyy kysymykseen siitä, mistä Tuukka kaipaisi lisää tietoa. Hän ei tiedä, sillä kokee ettei oikein ymmärrä kybermaailmaa, eikä pysy teknologisen kehityksen perässä.

Lounastauolla Tuukka lukee mahdollisen Nato-jäsenyyden aiheuttamista kyberuhkista. Uutisessa listataan asiantuntijoiden vinkkejä uhkiin varautumiseen. Viranomaisten ja asiantuntijoiden näkemykset kyberturvallisuuden uhkakuvista ovat Tuukan mielestä tärkeä asia varsinkin tässä maailmanpoliittisessa tilanteessa. Tuukka on yrittänyt kiinnittää huomiota sosiaalisen median tiliensä suojaukseen, ettei niistä vuotaisi tietoja ja jotta niitä ei voitaisi hakkeroida, esimerkiksi ottamalla käyttöön kaksivaiheisen tunnistautumisen ja päivittämällä laitteensa säännöllisesti. Tuukka ei kuitenkaan osaa olla huolissaan siitä, että sosiaalisen median alustoilla kerättävää tietoa saatetaan myydä kolmansille osapuolille. Tuukka suhtautuu pelokkaasti virheisiin ja hänelle on tärkeää, että hänen laitteensa toimivat hänen haluamallaan tavalla, eikä niissä ole viruksia.

Tuukan tyyppitarina kuvaa henkilöä, jolla ei ole työssään tai vapaa-ajallaan suoraa kosketuspintaa kyberturvallisuuteen tai siihen liittyviin lähikäsitteisiin. Hänelle kyberturvallisuus tarkoittaa tietosuojaa, sosiaalista mediaa, hakkerointia, viruksia ja yleistä

internetin ja laitteiden turvallisuutta. Kosketuspinta kyberturvallisuuteen voi muodostua esimerkiksi median, asiantuntijoiden sekä viranomaisten näkemysten kautta, mutta myös sosiaalinen ympäristö saattaa vaikuttaa henkilökohtaisen kyberturvallisuuskulttuurin muodostumiseen. Henkilö kiinnittää huomiota siihen, että hänen laitteensa toimivat halutulla tavalla.

> *…jos mulla on tietokone, se ei kaatuile koko ajan ja jos olen tehnyt tekstidokumentin, kun tallennan sen, saan sen auki uudelleen ja se ei ole kadonnut tai että niinku se toimii…*

> *Turvallisuus on myös sitä, että jos julkaisen sosiaalisessa mediassa jotain tai käyn verkkokaupassa, niin toivoisin että se laite ei ole seurannut toimintaani…*

Kyberturvallisuutta pidetään tärkeänä aihepiirinä. Tärkeys on tarinassa kuitenkin suhteellinen käsite, sillä lopulta kyberturvallisuuteen suhtautuminen näyttää olevan sidoksissa henkilön asenteeseen ja kyberturvallisuudelle antamiin merkityksiin. Tarinassa henkilön suhtautuminen kyberturvallisuuteen rakentuu ulkopuolisten vaikutteiden varaan: siihen vaikuttavat esimerkiksi media ja maailmanpoliittiset tapahtumat. Covid-19 -viruksen myötä kasvanut verkkorikollisuus on saanut mediassa paljon palstatilaa. Esillä ovat olleet muun muassa niin kalasteluviestit, identiteettivarkaudet kuin valeuutiset. Hän kokee kybertoimintaympäristön muuttuneen turvattomammaksi.

> *Kaikki uutiset, miten huijataan ihmisten luottokorttitiedot ja kaikki muut niin tämähän on ihan käsittämätöntä touhua nykyään.*

Vaikka kyberturvallisuutta pidetään tärkeänä, turvallisista toimintatavoista saatetaan silti luistaa, mikäli ne hidastavat toimintaa tai koetaan, ettei niitä jostain syystä tarvitse noudattaa. Henkilö saattaa kokea turvalliset toimintatavat vaivalloisiksi ja pitää kyberuhan riskiä pienenä. Esimerkiksi tietovuodon uhkaa ei välttämättä pidetä lopulta kovinkaan vakavana, mikäli koetaan, että käsitellyn tiedon vuotaminen ei olisi vaarallista. Samoin tietoturvakoulutusta pidetään tärkeänä, mutta silti sen kanssa saatetaan olla hieman huolettomia. Vaikka henkilö pitää kyberuhkia huolestuttavina ongelmina, riskit eivät kuitenkaan konkretisoidu hänen omassa arjessaan. Siksi hänen henkilökohtainen asenteensa kyberturvallisuutta kohtaan on välillä huoleton.

> *En usko, että kauheasti käytetään VPN-yhteyksiä esimerkiksi etätöissä, ehkä koetaan, että ei käsitellä sellaista tietoa mikä olisi kauhean haavoittuvaista ja sitten se hidastaa meidän etäyhteyksiä.*

Henkilö kokee omien teknologisten taitojensa olevan arjessa riittävät, tavalliset, mutta ei silti varsinaisesti luota niihin. Epävarmuus teknologisista taidoista kytkeytyy tietämyksen puutteeseen. Hän toimii työtehtävässä, jossa ei varsinaisesti käsitellä kyberturvallisuutta, tietosuojaa tai muita läheisiä aihepiirejä, eikä tieto- ja informaatioteknologian koulutuskaan ei ole relevantti. Osaamisensa hän on saanut pitkälti vain kokemuksen kautta. Henkilö suhtautuu hänelle arvaamattomana näyttäytyvään kybermaailmaan skeptisesti ja varauksella, sillä hän ei välttämättä luota omaan arvioonsa turvallisuudesta. Hän kokee, ettei puutteellisen ymmärryksensä vuoksi myöskään oikein tiedä, kuinka hänen tulisi kehittyä tai mitä hänen tulisi oppia lisää.

> *Niitähän on sitten semmoisia klikkejä että se viesti on niinku täysin asiallisen oloinen että klikkaat väärin ja sitten täytyy sanoa, että mun tietoteknisillä taidoilla niin en välttämättä niinku tietäisi että jos se mun laitteeni toimii suhteellisen normaalisti niin mistäpä minä tiedän että mikä siellä taustalla hyrrää.*

> *Tuo on kuitenkin aika vieras maailma minulle, et on hankala sanoa mitkä on sellaisia mistä meitä tavallisia tallukoita kannattaisi informoida, et onko se oma käytös, miten sinä missäkin käyttäydyt, vai onko meillä nyt ollut kuinka paljon tietomurtoja täällä, saakohan niitä edes kertoa.*

Skeptisen asenteen lisäksi henkilö on tehnyt joitakin konkreettisia parannuksia henkilökohtaiseen kyberturvallisuuteensa. Hän mainitsee muuttaneensa sosiaalisen median asetuksia, käyttävän kaksivaiheista tunnistautumista ja päivittävän laitteitaan säännöllisesti. Tärkeintä hänelle on kuitenkin se, että kybermaailmassa asiat toimivat hänen tottumustensa mukaisesti.

> *Hmm, no miten, kyllä nyt siis sellaisia kaksivaiheisen tunnistautumisen tyylisiä ottanut käyttöön, en mä oikein muuta.*

Tiina Tunnollisen tyyppitarina

Tiina on lähdössä työpaikaltaan kotiin. Hän on pitänyt töissä koulutuksen, jossa käsiteltiin muiden aiheiden ohella myös tietosuojaa ja tietoturvaa. Tiina kertoi esimerkin siitä, mitä tapahtuisi jos hän huomaisi tai avaisi epähuomiossa epämääräisen sähköpostin liitteen. "Mikäli mä huomaisin sen heti, olisin varmasti tyytyväinen itseeni. Mikäli en, muhun saattaisi hyökyä häpeän ja epäuskon tunne. Ikään kuin olisin tehnyt jotain pahaa, vaikka kyseessä olisikin ollut silkka vahinko", Tiina kuvailee. Hän kertoi myös, että tunteikkaan reagoimisen jälkeen hän olisi kuitenkin ilmoittanut asiasta esimiehelleen. Vaikka hän kokee omien tietoteknisten taitojensa olevan melko hyvät, hän saattaa silti kokea joskus epävarmuuden tunnetta. Vahinkoja voi aina sattua.

Tiina pitää koulutuksien järjestämisestä, sillä tietosuoja ja tietoturva ovat hänestä hyvin tärkeitä aihepiirejä. Hän muistaa vuosien takaisesta työpaikastaan ensimmäisen kosketuksensa tietosuojaan ja tietoturvallisuuteen. Perehdytys oli ollut jännittävä ja antanut hänelle arvostavan tunteen siitä, että työpaikalla ei väheksytä ketään turvallisuuden noudattamisessa. Sen jälkeen hän oli suhtautunut tietoturvallisuuteen ja tietosuojaan paljon jämerämmin.

Tänään Tiinalle kuitenkin jäi koulutuksen pitämisen jälkeen epämiellyttävä tunne. Hän on huomannut, että kyberturvallisuus tai siihen liittyvät aihepiirit eivät olleet oikein kiinnostaneet muita työntekijöitä. Melko vasta hän oli keskustellut ystäviensä kanssa salasanamanagerien käytöstä ja yksityisyyttä kunnioittavaan pikaviestipalveluun siirtymisestä. Turhaan, sillä sitä ei pidetty tärkeänä. Ajatus palaa hänen mieleensä, ja hän on turhautunut, sillä kokee ettei voi tehdä tarpeeksi asian eteen. Kybermaailma epäilyttää häntä, varsinkin nykyään, ja hän uskoo, että mikään ei ole internetissä täysin turvassa ja että jokaiseen tietojärjestelmään voidaan lopulta tunkeutua. Tiina pohtii, että onko turvallisuuden tunteeseen tuudittautuminen lopulta vain näennäistä ja voiko turvallisuuden tunteeseen todellisuudessa luottaa?

Tyyppitarinan päähenkilö Tiina työskentelee organisaatiossa tehtävässä, joka ei varsinaisesti liity tietosuojaan tai tietoturvallisuuteen, mutta jossa sivutaan jossain määrin sitä. Hän pitää kyberturvallisuutta ja tietosuojaa hyvin tärkeinä aihepiireinä. Tiinalla ei ole tieto- ja informaatioteknologian koulutusta. Tiina on kuitenkin työnsä puolesta perehtynyt

turvallisuuden ja tietosuojan asioihin jonkin verran. Tarinassa Tiina kokee koulutuksien järjestämisen tärkeäksi. Hän sai ensimmäisen kosketuksensa tietoturvallisuuteen ja tietosuojaan vuosien takaisessa työpaikassaan. Kokemus oli positiivinen ja sillä oli vaikutus siihen, minkälaiseksi Tiinan asenne muodostui tietosuojaa ja tietoturvaa kohtaan. Usealla haastatellulla aikaisemmat kokemukset tietoturvasta tai tietosuojasta näkyivät positiivisina asenteina tietoturvaa kohtaan.

> *Ensimmäinen kosketus semmoiseen tietoturva-asioihin oli ehkä kun olin töissä … ja siellä meille pidettiin aika tiukka turvallisuuskoulutus ja siellä oli tosi tiukat säännöt esimerkiksi siihen että miten töitä sai tehdä kotoa käsin… koin, että meille haluttiin tarjota työvälineet tähän niinku turvallisuuteen ja opettaa siihen kulttuuriin.*

Tiinan asenne koskettaa myös henkilökohtaista elämää. Tarina kuvaa, kuinka tietoturvaan ja tietosuojaan liittyvät asenteet näkyvät myös henkilökohtaisessa elämässä. Tiinalle on tärkeää, että hän toimii näiden asenteiden mukaisesti ja hän on valmis myös keskustelemaan aihepiiristä myös muiden kanssa. Sosiaalisessa piirissään Tiina on muita tarkempi tietoturvasta ja –suojasta. Hän kokee, että muita nämä asiat eivät kiinnosta, eivätkä he pidä niitä niin merkityksellisinä, että lähtisivät muuttamaan omia toimintatapojaan. Tämä turhauttaa Tiinaa.

> *Olen pitkään tehnyt tämän asian parissa töitä ja se on ehkä vaikuttanut tähän mun käyttäytymiseen ihan niin kuin yksityiselämässäkin, että on hankittu sellaiset laitteet jotka ovat turvallisempia.*

> *Tulee ihan joka päivä tulee vastaan se esimerkiksi kun minä juttelen kavereiden kanssa, kun mä en ole pitkään aikaan käyttänyt erästä palvelua ja esiin tulee et ei ne osaa, ei ymmärrä tästä yhtään mitään, et en mä nyt lähde siirtymään mihinkään muuhun palveluun… Välillä olen vähän kyllästynyt tähän kaikkeen, koska, sä et juurikaan, tai et aina pysty vaikuttamaan, teit sit mitä vaan niin aina jotain sattuu ja tapahtuu, ja sitten kun sä et pysty niinku muiden käyttäytymiseen sitten millään tapaa vaikuttamaan.*

Tarinassa Tiina kertoo, kuinka hän suhtautuisi tietoturvapoikkeamaan. Epäilyttävän viestin tai muun asian huomaaminen olisi positiivista ja selkeä onnistuminen. Sen sijaan uhkan tunnistamatta jättämiseen tai sellaiseen lankeamisen hän kokisi noloksi, ahdistavaksi ja surullisen tunteikkaaksi, mutta ei ylitsepääsemättömäksi hetkeksi. Työtehtävään liittyvä virhe voi tuntua henkilökohtaiselta epäonnistumiselta, mikäli henkilö kokee, että virhe olisi ollut vältettävissä huolellisemmalla toiminnalla. Mikäli yleensä kokee olevansa tarkka tietoturvallisuuteen ja tietosuojaan liittyvien hyvien toimintatapojen noudattamisessa, hän saattaa syyttää vahingosta tai virheestä itseään. Tiina kokee olevansa henkilökohtaisesti vastuussa omasta kyberturvallisuudestaan, jonka hän tunnistaa vaikuttavan myös muihin työntekijöihin sekä organisaatioon.

> *Varmaan niinku kauhistuisin siinä ja mua nolottaisi hirveästi ja niinku nolottaisi et mä oon niinku haksahtanut siihen, mutta kyllä mä siitä kertoisin heti, että en lähtisi sitä niinku silleen peittelemään, toivotaan parasta tyyliin, vaan kyllä mä sitten ihan heti ilmoittaisin esimiehelle ja tietoturvapäällikölle että olen klikannut tällaista linkkiä ja tutkikaa mun kone että onko täällä nyt jotain viruksia.*

Vaikka Tiina kokee tietoteknisten taitojensa olevan melko hyvät, herättää kybermaailma hänessä silti epävarmuuden tunnetta. Hän liittää tunteeseen maailmanpoliittisen tilanteen sekä kasvaneen kyberrikollisuuden ja kybervaikuttamisen. Internetissä mikään ei tunnu olevan täysin turvassa, eikä omaan turvallisuuden tunteeseen voi välttämättä luottaa. Henkilö saattaa tietämyksensä perusteella tunnistaa aukkoja esimerkiksi ohjelmistojen tai laitteiden tietoturvassa ja siksi pohtia, että voivatko luotettavaksi mielletyt palvelut todellisuudessa vastata niistä muodostettuja käsityksiä.

> *… loppujen lopuksi jollain tasolla pystytään tunkeutumaan tietoihin, se on aivan fakta, niinku en mä sataprosenttisesti kyllä luota tähän… kaikki se mitä nyt tehdään mediassa ja mitä olen nähnyt omassa organisaatiossa, että vaikka kuinka yritetään, niin kyllä se kaikki mitä on tapahtunut on vaikuttanut, että ilman muuta se rikkoo sitä luottamusta että niinku päästään toimimaan vaikka ollaan olevinaan niinku tehty parhaamme ja asiat olisi hyvin.*

…ei se varmaan turvallisuutta, enemmän mä mietin sitä että onko se sellaista oikeaa turvallisuutta vai onko se vaan semmoista savuverhoa, että jossain säiliössähän vaikka ne Applen hienot pitkät tunnukset ovat ja se Applen palvelu muistaa ne, mutta että onko siellä kuitenkin kanssa joku takaportti sitten johonkin ja käytetäänkö niitä, et ainakaan millään tavalla mediassa se ei ole vielä noussut, että tällaista pitäisi epäillä mutta että mikään maailmassa ei ole varmaa.

Arttu Asiantuntijan tyyppitarina

Arttu Asiantuntija istuu työpaikan ruokalassa lounaalla. Artun kollega kertoo hänelle jälleen eräästä huijausviestistä, jonka oli saanut. Häntä naurattaa, koska sähköpostin roskapostikansiosta löytynyt viesti oli niin epäuskottava. Arttu huomauttaa, että organisaation sisällä olisi kuitenkin ehkä syytä varoittaa uudenlaisesta huijausviestistä. Lounaan jälkeen Arttu suuntaa takaisin työpisteelleen. Hän ajautui työskentelemään tietotekniikan parissa suoritettuaan siihen liittyvän korkeakoulututkinnon. Työnsä puolesta Arttu seuraa tietoturvaan ja –suojaan liittyviä aihepiiriä edelleen läheisesti, sillä teknologian nopean kehityksen vuoksi omaa ammattitaitoa on pidettävä aktiivisesti yllä.

Artulle on tullut ilmoitus sähköpostiin tietoturvakoulutuksesta. Hän naputtelee sen läpi kuin huomaamattaan. Koulutuksessa läpikäytävät asiat ovat Artulle tuttuja ja rutiininomaisia. Tässäkö tämä oli, hän miettii. Artun mielestä koulutuksen sisältöjä olisi ehkä voitu avata laajemminkin. Arttu jää pohtimaan koulutusta, ja miettii, että kyberturvallisuus on ikään kuin sähköisen maailman turvallisuutta, jonka kanssa hän on vuorovaikutuksessa. Työssä se on tarkoittanut hänelle tietoturvallisuutta ja tietosuojaa. Hän joutuu välillä punnitsemaan tietosuojaan ja -turvaan liittyviä asioita syvällisestikin, esimerkiksi kun halutaan hyödyntää dataa kehitystyössä. Tällöin on pystyttävä punnitsemaan datan käytön eettisyyttä, oikeutusta ja siitä seuraavaa hyötyä.

Arttu lopettaa tänään päivänsä ajoissa, sillä tänään täytyy tehdä vielä henkilökohtaiseen elämään liittyviä vapaaehtoistöitä. Hän pitää niistä, ja kokee ammattitaidostaan olevan niissä hyötyä. Joskus hän kuitenkin tuntee, että muut saattavat pitää tietoturvaan ja tietosuojaan liittyviä huomionarvoisia asioita pilkunviilauksena.

Artun tyyppitarina kertoo henkilöstä, joka työskentelee tietoteknisten asioiden parissa. Hän ei ole niin peloissaan kybermaailmasta, sillä se on hänelle arkinen ympäristö, johon hän suhtautuu rationaalisesti. Artun kaltainen henkilö ymmärtää kyberturvallisuuden taustansa ja työtehtävänsä kautta. Hänen asenteeseensa voi vaikuttaa relevantti koulutustausta ja hänen kerryttämänsä työkokemus tietoturvaan ja tietosuojaan liittyvistä työtehtävistä. Hänellä voi olla yksityiskohtaista tietoa teknologiasta, laitteista ja ohjelmistoista, ja sen myötä hän luottaa omiin teknologisiin taitoihinsa.

> *… oli yksi tapaus, missä minusta tuli se pilkunviilaaja tietosuoja-asioissa, koska mä nyt satun tietämään niistä aika paljon työn roolin kautta.*

> *Ammatillinen tausta auttaa siinä, että tunnistaa niitä tilanteita missä kannattaa olla tarkkana ja jos on joku verkkosivu missä on mainoksia, joissa sanotaan että klikkaa tästä, niin ei klikkaa siitä, että osaa erottaa mikä on niinku sivuston oikeaa sisältöä mitkä on niitä houkuttimia siinä.*

Asenteeseen voi vaikuttaa tiedon lisäksi myös nykyinen työtehtävä. Tietoturvallisuus ja tietosuojan kysymykset voivat olla välillä vastakkain työtehtävien kanssa. Henkilön työtehtävä esimerkiksi kehitystyössä voi olla sellainen, että siinä on kyettävä punnitsemaan tietosuojaan ja -turvaan liittyviä toimenpiteitä suhteessa siihen, mitä haluttaisiin tehdä tai saavuttaa, esim. laajemmalla tietojenkäsittelyllä. Tietosuoja on Artun kaltaiselle henkilölle tärkeää, mutta asetettujen vaatimuksien tulisi olla hänen mielestään kohtuullisia.

> *Tietoturvaan ja tähän tietosuojaan liittyvät, etenkin tietosuojaan liittyen sanoisin että ne arvot joutuu, sitten edistyksellisyys ja sitten tää tietosuojakin menee vastakkain välillä.*

> *Omassa työssä huomaa sen että jos tosi kovasti vaan salataan ja noudatetaan lakia niinku ihan pilkun tarkkaan niin silloin kyllä helposti ollaan siinä tilanteessa että ihan hirveän innovatiivista tai uutta asiaa varsinkin julkisessa toiminnassa on vaikea toteuttaa tai kehittää…*

> *… siinä pitäisi saavuttaa enemmän balanssia, pitäisi pystyä tunnistamaan ne tiedot mitkä on oikeasti riskialttiita ja arvokkaita ja niiden käsittelyssä pitää*

> *ehdottomasti olla myös huolellinen mutta sitten pitää pystyä tekemään myös vähän ketterämpiä, oikeasti punnitsemaan, että siinä ei ole niin suuria riskejä.*

Arttu pystyy kokemuksensa perusteella paitsi arvioimaan tietoturvaan ja –suojaan liittyviä kysymyksiä sekä kyberuhkia, myös punnitsemaan erilaisia ratkaisuja ja varautumismahdollisuuksia. Hän myös saattaa työnsä puolesta olla vastuussa turvallisuudesta ainakin joiltain osin. Hän kokee, että tunnistaessaan puutteita tai ongelmakohtia organisaation sisäisessä kyberturvallisuuskulttuurissa, hänen on puututtava niihin. Artun kaltainen henkilö tunnistaa puutteellisten tietojen ja taitojen mahdollisen vaikutuksen kyberturvallisuudelle.

> *... koen että siitä seuraa tietty vastuu, jos siellä muilla ei ole tietoa että nämäkin pitäisi huomioida niin ikävä kyllä niistä niinku täytyy mielestäni sitten vähän niinku kertoa ja huomauttaa että kyllä tarvitsisi huomioida ja ainakin jollain tavalla pyrkii niitä huomioimaan, että joo siis et pidän noin lähtökohtaisesti tärkeänä kyllä.*

Arttu suhtautuu tietoturvapoikkeamaan rationaalisesti, eikä tunteilla. Arttu ymmärtää, että kyberuhkat koskettavat kaikkia ja että kaikille sattuu joskus inhimillisiä virheitä. Arttu kuitenkin ymmärtää, että omilla toimintatavoilla kyberuhkia voi ehkäistä ja niihin voi varautua. Olennaista on se, että hyviä toimintatapoja noudatetaan, vaikka ne tuntuisivatkin joskus turhilta tai vaivalloisilta. Artun mielestä on hyvä, että tietoturvakoulutuksia pidetään säännöllisesti, sillä yhteiset toimintatavat ja -säännöt parantavat organisaation turvallisuutta. Käytäntöjä on myös hyvä päivittää tasaisin väliajoin.

> *Kyllä mä uskon että vastaavassa asemassa paljon tietotyötä tekevät ja kehittämistyötä tekevät ja korkeakoulututkinnon käyneet varmaan allekirjoittaa tämän ajatuksen että se tietoturvakoulutus oli aika niinku yleispätevää tietoa että ei siitä ehkä nyt ihan hirveän hullua hurskaammaksi tullut.*

> *...mutta kyllä sitten mä sanoisin että palvelee tarkoitustaan juuri sitten vaikka tällaisille ihmisille, joiden osaaminen on niinku ihan jotain muuta ja sitten niinku joiden pitää tavallaan saada se peruspaketti näistä asioista, tosin mä*

olen itse käynyt vaan kliksuttelemassa sen läpi koska itselleni ne on kuitenkin aika tuttuja asioita.

No ehkä itsellä on työkokemuksen kautta sitten enemmän tietoa vielä asiasta kun kollegoille että ehkä sen kautta vielä tarkemmin tietyssä mielessä tai huolellisemmin mutta tieto lisää tuskaa tyyppisesti.

5.2 No me ollaan kuitenkin kuntaorganisaatio – narratiivi organisaatiokulttuurista ja toimintaympäristöstä

Toinen analyysissa muodostunut narratiivi kuvaa hallinto-organisaation organisaatiokulttuuria ja toimintaympäristöä. Tämä narratiivi pureutuu kohdeorganisaation organisaatiokulttuuriin ja sen ominaispiirteisiin. Narratiivi koostuu kahdesta tyyppitarinasta. Toimintaympäristöä kuvailtiin kompleksiseksi: kuntaorganisaation laajuus ja monitoimialainen hallinto ovat tekijöitä, jotka vaikuttavat toimintakentän haasteellisuuteen. Oman mausteensa keittoon tuovat myös muut julkisen sektorin organisaatioihin liittyvät erityispiirteet, kuten byrokraattisuus, hallintolähtöinen organisaatiokulttuuri ja lainsäädäntö. Organisaation ja toimintaympäristön ominaispiireet vaikuttivat organisaatiokulttuuriin, jonka tulkinta sai erilaisia merkityksiä sen suhteen, mikä oli henkilöiden tausta ja missä osassa organisaatiota he olivat töissä.

5.2.1 Tyyppitarinat organisaatiokulttuurista ja toimintaympäristöstä

Pekka Perusteellisen tyyppitarina

Pekan vastuulla on hanke, joka koskettaa kymmeniä organisaatiossa työskenteleviä ihmisiä. Hänen työnään on määritellä uusia toimintatapoja ja varmistaa, että organisaatiossa toimitaan lainsäädäntöä noudattaen.

On osoittautunut, että työntekijöiden toimintatavat poikkeavat huomattavasti toisistaan: kaikki työntekijät eivät välttämättä tiedä tai välitä oikeista toimintatavoista. Pekalla on

aiempaa työkokemusta suurista organisaatioista, joten asenteiden, taustojen ja motivaatioiden moninaisuus ei ole yllättänyt häntä. Pekan mielestä moninaisuus on varsin ymmärrettävää. Organisaation ollessa varsin suuri ja siiloutunut, ovat työntekijöiden taustatkin toisistaan hyvin poikkeavia. Vaikka lainsäädäntö ja oikeiden toimintatapojen noudattaminen ovat Pekan työn keskiössä, asian merkittävyys ei ole lopulta kovin suuri muille työntekijöille.

Organisaatiotasolla ongelma on Pekan mielestä mittava, mutta sitä on vaikea ratkaista. Pekan mielestä organisaatiossa ei järjestetä riittävästi perehdytystä tai koulutusta asioihin, ja työntekijöiltä vaadittu osaaminen on laaja-alaista, esimerkiksi lainsäädännöstä johtuen. Lainsäädännön kannalta asia on Pekan mielestä kuitenkin erityisen ongelmallinen – hän on tottunut noudattamaan lainsäädäntöä ja lainsäädäntö määrittelee organisaation toimintaa huomattavasti. Onhan kyseessä kuitenkin julkinen organisaatio.

Pekka tiedostaa että lainsäädäntö on muuttunut ja muuttuu myös tulevaisuudessa, kun parempia toimintatapoja kehitetään. Organisaatiotasolla on kuitenkin vaikea muuttaa vanhoja ja pinttyneitä toimintatapoja. Pekalle on tärkeää, että organisaatiossa ei toimittaisi lainvastaisesti, vaikka kyseessä olisikin kokonaisuuteen nähden pienen pieni asia. Hänen mielestään suurissa organisaatioissa olisi hyödyllistä kouluttaa työntekijöitä systemaattisemmin ja säännöllisemmin, jotta hyvät toimintatavat saataisiin osaksi organisaation kulttuuria.

Tyyppitarina kuvaa kaupungin hallinto-organisaatiota ja sen erityispiirteitä. Organisaatio on varsin laaja kokonaisuus, sillä kaupungin lakisääteiset ja vapaaehtoiset tehtävät tarkoittavat, että erilaisia palveluja ja täten eri tehtävissä eri taustoista tulevia työskenteleviä henkilöitä on paljon. Tarinassa Pekka on huomannut, että organisaation sisällä on useita toisistaan poikkeavia toimintatapoja ja asenteita, esimerkiksi eri ryhmien välillä. Eri ryhmien väliset toimintatavat voivat korostua esimerkiksi organisaation siiloutumisen vuoksi. Tällä tarkoitetaan sitä, että sen sisäisten ryhmien, suurien tai pienien, yhteistyö vähenee ja ne pyrkivät toimimaan enemmissä määrin erillisinä itsenäisinä ryhminä. Siiloutuminen nähdään haasteena, joka hankaloittaa organisaation päivittäistä toimintaa. Lisäksi sen nähdään olevan kaupunkiorganisaatiolle jollain tavalla perinteistä tai normaalia.

> *Mä uskon, että meidän organisaatiossa haaste on enemmän siinä, että me ollaan aika perinteiseen tapaan aika siiloissa, meillä on hyvin erilaista tekemistä erilaisissa yksiköissä, että ja hyvin eri ikäistä siis sekä väkeä erilaisella osaamisella.*

Eri ryhmien välillä koetaan olevan eroja esimerkiksi heidän ammattitaustansa tai -alan kautta. Ryhmille tunnistetaan erityisiä kulttuurillisesti ominaisia piirteitä, jotka vaikuttavat esimerkiksi siihen, kuinka heidän kanssaan toimitaan.

> *Vaikka et jos tuolla terveydenhuollon ammattilaisten kanssa jostain sovitaan, niin se pitää sitten niinku pilkulleen paikkansa… ja sitten insinöörit on niinku oma kastinsa ja rehtorit on jo tottunut johtamaan sitä koulua kuin pientä universumia, ja jos rehtorille menee sanomaan, että pitäisi näin tehdä, rehtori on kyllä sitä mieltä, että hän osaa opettaa ja jalkauttaa. Että kyllä sitä ihan aina huomaa, että erilaisten verkostojen kanssa tässä tehdään.*

Kuntaorganisaatiossa keskeisenä toimintaympäristöä määrittelevänä tekijänä on myös lainsäädäntö. Kuntaa koskettavat julkisen hallinnon erityispiirteet, kuten se että toiminnan tulisi perustua lakiin, sekä se että toimintaa määrittävä laaja sääntely. Lainmukainen toiminta onkin yksi organisaation kulmakivistä. Sen noudattaminen ei kuitenkaan ole yksiselitteistä, sillä kaikki lainsäädäntökään ei ole yksiselitteistä.

> *…lainmukaisuus menee kaikkein tärkeimmäksi, että se on niinku tärkeintä että toimitaan lain mukaan, tietysti kaikki lainsäädäntö ei ole niinku niin selkeää ja voidaan joutua tekemään tulkintaa ja kysyä juristilta, että miten tämä pitäisi tulkita ja sitten eri juristitkin voi antaa eri näkemyksiä siitä että miten se kannattaisi tulkita…*

Tarinassa nousee esiin joidenkin henkilöiden tai ryhmien erilainen asenne lainnoudattamista kohtaan. Vaikka asia on tapauskohtainen, se kuvaa erilaisia asenteita organisaation sisällä. Sitä kuvaillaan vähäiseksi, mutta silti ongelmalliseksi ajattelutavaksi. Yleisesti ottaen haastatellut näkivät, että monet uudet toimintatavat saatetaan kokea hankaliksi, tai vaihtoehtoisesti niiden opettelu koetaan epämiellyttäväksi. Asiaa kuitenkin monimutkaistaa myös se, että lainsäädäntö voi myös joissain tapauksissa ja joistain syistä johtuen onnistua

yllättämään organisaation vaatimuksillaan, jolloin osaamisvajeen aiheuttajasta voidaan olla montaa mieltä.

> *Ainahan välistä sitä voi nurista, että on tässä nämä omatkin työt hoidettavana, että ehtiikö sitä kaikkea opiskella. Kuntahallinnossahan tulee tosi paljon lainsäädännöstä ja säädöksistä velvoitteita, joita kunnan työntekijän pitää tehdä. Minun omassa työssä juuri edellisessä kokouksessa puhuttiin lainsäädännöstä ja sehän on tullut silleen, että hups heijaa, nyt kaikkien kaupungin työntekijöiden pitäisi osata ja hallita tämä, niin kyllä mä sen ymmärrän hyvin että kun sulla on se arjen työ, niin ihan nyt välttämättä et ole ehtinyt perehtyä tähän lainsäädäntöön, mutta se on lainsäädäntö.*

Pekka kokee myös, että hänen asenteensa eroaa muista taustansa vuoksi. Hänen kokemukset ja työhistoria ovat vaikuttaneet siihen, kuinka hän asennoituu ja mitkä ovat hänen toimintatapansa jotain asiaa kohtaan. Pekka tapauksissa koki, että hänen asenteensa eroaa jollain tavalla organisaatiossa tai omassa ryhmässä yleisesti vallitsevasta asenteesta.

> *Se juontaa varmaan sieltä aikaisemmista kokemuksistani, että kun tässä sääntöjä on opittu noudattamaan...*

Hanna Hallinnon tyyppitarina

Hanna on työstänyt organisaation henkilökunnalle uuden ohjeistuksen. Hanna on tyytyväinen työhönsä, ja odottaa, että ohjeistus saataisiin otettua käytäntöön. On kuitenkin kulunut jo useita kuukausia, kun Hanna sai työnsä päätökseen. Asia tulee puheeksi kahvipöydässä ja kollega kyselee Hannalta, onko asia edennyt mitenkään? Hanna vastaa, että ei ole. Tiedäthän, tässä koronan ja muiden asioiden keskellä se ei ole vielä edes päässyt sinne hyväksyntämyllyn kokouslistoille. Enkä ole päässyt tapaamaan heitä, joilla voisi olla vaikutusvaltaa asiaan. Eiköhän se sinne vielä saada, Hanna sanoo äänessään hieman optimisuutta. Hän on jo tottunut organisaation kankeuteen ja toisaalta ymmärtää prosessin merkityksen. Se on kuitenkin Hannan mielestä jossain määrin tarpeellista, sillä julkisella sektorilla hyvän hallinnon noudattaminen on tärkeää, jotta lain- ja oikeudenmukaisuus voidaan taata.

Kollega toteaa Hannalle, että kuulostaa ankealta, mutta vähän tutulta. Minä onneksi koen asiat vähän eri tavalla kuin sinä, meillä on jotenkin rennompaa ja itseohjautuvampaa, toki erilaisissa töissä ollaan myös. Toisaalta tulevathan ne tietyt asiat meillekin ylhäältä, mutta joka tapauksessa. Joo, ja kyllähän se perinteinen byrokraattisuus on jotenkin vähentynyt, kun nykyään toimitaan laajasti erilaisissa verkostoissa, Hanna mainitsee. Vaikka meidän yksiköt saattavat hieman erottua toisistaan, on meillä kuitenkin selkeä strategia taustalla määrittämässä toimintaa ja samanlaisen arvomaailman omaavat ihmiset töissä.

Tyyppitarina kuvailee organisaatiossa koettua kankeutta ja itseohjautuvuutta. Hannan työtehtävänä ollut asia on jäänyt päätöksentekoprosessin jalkoihin. Hän kuvailee tarinassaan päätöksentekoprosessia *hyväksyntämyllyksi*. Tällä hän viittaa siihen, että käsiteltävän asian tulee käydä läpi monia eri tahoja, ennen kuin se pääsee käytäntöön organisaation elämässä. Jotkut toimintamallit näyttäytyvät hänelle turhan byrokraattisina, hitaina ja vanhanaikaisina. Se luo joillekin haastatelluille turhautumisen tunnetta ja toivetta muutoksesta.

> *…hidastaa niin kuin asioiden eteenpäin viemistä että… niin kuin tietyt muut asiat nyt painaa enemmän vaakakupissa, on ollut koronaa ja on ollut vaikka mitä niin siellä on tietyt toimielimet, minkä kautta pitää mennä sen hyväksyntämyllyn läpi niin se ei koskaan kerkeä tai pääse sinne kokouslistoille edes, että kyllä se tavallaan vähän turhauttaa välillä... että kyllä se näyttäytyy siinä omassakin arjessakin ikävä kyllä.*

> *…mä olen sen verran tässä organisaatiossa viihtynyt, että ei tämä pelkkää huonoa ole ollut, mutta ehkä toivoisin sellaista niin kuin organisaatiokulttuurin näkökulmasta, että ruvettaisiin vähän enemmän vielä lähestymään sitä semmoista avoimempaa ja ei niin semmoista hierarkkista johtamista etenkin.*

Hanna suhtautui päätöksentekoprosessiin osaltaan turhautuneesti, mutta ymmärsi sen merkityksen. Organisaation toimintaa säätelevät lait sekä lain määrittelemät, mutta organisaation itsensä tarkentamat ohjeistukset, kuten hallintosääntö. Vaikka nämä asiat tuovat organisaation elämään kankeutta, niiden merkitys ymmärretään. Organisaatiokulttuuria kuvailtiin hallintolähtöiseksi, jolla viitattiin siihen, että työskentelyn tapoja ja tehtäviä asioita määrittää vahvasti julkishallinnollisena organisaationa hyvä

hallinto, julkishallinnolliset arvot, lainsäädäntö, ja oikeusturva, jotka ovat tärkeitä elementtejä.

> *Mulla tulee mieleen ekana tuollainen hallintolähtöinen [kulttuuri], että jos ajattelee koko organisaatiota, niin onhan se semmoinen hallintolähtöinen. Hallintolähtöisyyshän nyt tulee ihan lainsäädännöstä ja julkisen hallinnon kulttuurista ja se oikeusturvakin tavallaan, että pyritään välttämään niitä virkavirheitä.. on myös hyvä että kaikesta on joku jäljitettävyys, kuka päätti mitä ja missä kohtaa, kun sillä [päätöksellä] voi olla vaikutuksia johonkin henkilöön tai firmaan tai jonkun poikkeuksiin tai asemaan.*

Tyyppitarinassa Hanna kokee kankeuden vaikuttavan varsinkin hänen yksikköönsä, kun taas Kollegan käsitys oman yksikkönsä kulttuurista eroaa varsin paljon. Organisaation eri yksiköiden tai tiimien välillä koettiin olevan eroavaisuuksia esimerkiksi työtapojen osalta. Kulttuureja ei kuitenkaan nähdä täysin erillisiksi, sillä niitä koskettavat samat organisaation erityispiirteet, kuin muitakin. Itseohjautuvassa yksikössä yhteisenä eetoksena on pyrkiä tuomaan organisaatioon muutosta, myös kulttuurin kautta.

> *…sitten jos vielä ajattelee tarkemmin sitä, että mistä on helpompi puhua, niin siitä omasta yksiköstä, yksiköstä jossa työskentelen niin siellä on varmaan aika semmonen vahvaan yksilön asiantuntijuuteen pohjaava kulttuuri. Hyvin itseohjautuvaa, asiantuntijuutta arvostavaa kulttuuria ja sitten kanssa tämmöistä aika avointa kulttuuria, jossa halutaan avata sitä organisaatiota, halutaan murtaa niitä organisaation siiloja ja rajoja, tehdä yhteistyötä.*

> *…sellainen tietyllä lailla jäyhä, hidas ja byrokraattinen, vähän sellaista vanhanaikaista hierarkiaa vielä ilmenee. Varsinkin meidän hallinnossa, että minä en saa mennä suoraan puhumaan jollekin johtajalle vaan minun täytyy hoitaa asiat esihenkilön kautta. Minulle se näyttäytyy vähän vanhanaikaisena. Kaiken kaikkiaan sanotaan, että kun kyseessä on kaupunki ja näin paljon kuntalaisia ja palvelut pitää yrittää pitää, niin kyllä mä kuitenkin näen, että kaupunki onnistuu aika monessa asiassa hyvin.*

Tarinassa Hannan ja kollegan näkemykset oman yksikkönsä toiminnasta ovat varsin erilaiset, vaikka he kuitenkin toimivat samassa organisaatiossa. Vaikka Hanna kokee organisaation jossain määrin jäyhänä ja byrokraattisena, tunnistaa hän että niiden rinnalle on tullut enemmän verkostoihin nojautuvaa toimintaa.

> *…siihen miten me toimitaan haluttaisiin varmaan matriisimaisuutta, mutta että [nyt] tietyt asiat tulee kuitenkin silleen että kaupungin johtoryhmä päättää ja johtoryhmästä ohjeet menee sitten toimialajohdolle ja toimialajohto sitten puhuu lähiesimiesten kanssa ja lähimmät esimiehet vie sen sitten arkeen.*

> *Julkishallinnossa puhutaan myös siitä että ei niinku siilouduttaisi ja toimittaisiin verkostomaisesti, tai mehän toimitaan siis verkostoissa ja varsinkin tämä meidän hallinnossa koko toimintahan on sitä että me koko kokoustetaan joko toimialojen ihmisten kanssa, kokoustetaan konserninhallinnon yksiköiden kesken tai sitten mitä me tehdään tosi paljon ja mikä meille kuuluu on se että pidetään yhteyttä naapureihin tai siis kuntasektori valtionhallintoon tai sitten ihan globaalisti, kuitenkin ollaan se yksi suomen suurimmista kaupungeista…*

Hanna kokee, että organisaation toimintaa määrittää vahvasti myös sen strategia. Strategiaa kuvattiin selkeäksi päämääräksi, joka määrittää organisaation arvoja ja tavoitteita. Strategia mainittiin useita kertoja haastatteluissa, ja vaikka sen sanoituksen koettiin olevan melko laaja, pidettiin sitä silti tärkeänä ohjaavana elementtinä, jonka mukaisesti kaupungissa toimintaa. Hanna myös tunnistaa, että organisaatiolla ja siellä olevilla ihmisillä on samankaltainen arvomaailma. Arvojen koettiin näkyvän esimerkiksi siten, että organisaatioon tulevilla ja siellä olevilla työntekijöillä on yhteinen eetos tehdä yhteistä hyvää, työskennellä jonkin yhteisen merkityksellisen asian puolesta.

> *Meidän kaupungin strategia, joka meidän toimintaa ohjaa on minusta kuitenkin hyvä, vaikka se sanoitus on tosi laaja niin se antaa meille kaikille sen tarttumapinnan ja sitten kuitenkin sanoisin, että meidän kaupungin tasolla niin kuin ymmärretään se tärkeys ja että miksi sitä tehdään.*

Voisin ajatella että tietyllä tavalla julkiselle sektorille ajautuu tai päätyy sellaisia ihmisiä, jotka ajattelee että haluaa tehdä yhteisen hyvän edestä töitä. Joku tämmöinen niinku yhteisen hyvän ja vähän pehmeämpien arvojen ajattelumaailma et kuntasektorilla paljon on myös just tätä varhaiskasvatuksen, sivistystoimen, sosiaali- ja terveyspalvelujen väkeä, jossa on tällainen yhteisen hyvän tekemisen ajattelumaailma varmasti vielä enemmän läsnä.

5.3 Narratiivi kyberturvallisuuskulttuurista

Tutkielmassa muodostettu kolmas ja viimeinen narratiivi kuvaa organisaation kyberturvallisuuskulttuuria. Narratiivi koostuu kolmesta tyyppitarinasta. Toimintaympäristön haasteellisuudesta huolimatta organisaation kyberturvallisuuden tilaa pidettiin pääsääntöisesti hyvänä. Organisaation toimenpiteitä kyberturvallisuuden parantamiseksi pidettiin erittäin tärkeinä. Kyberturvallisuuskulttuuri nähtiin positiivisessa mielessä, vaikka parantamisen varaakin olisi: kyberturvallisuuden taso ole organisaation kokoon suhteutettuna tarpeeksi hyvällä tasolla. Toisaalta tunnistettiin, että virheisiin suhtaudutaan rakentavasti, eikä niistä piikitellä. Turvallisuuteen suhtautumisen koettiin myös kehittyneen viime vuosien aikana huomattavasti.

5.3.1 Tyyppitarinat organisaation kyberturvallisuuskulttuurista

Jaska Jämerän tyyppitarina

Jaska huomaa työmatkallaan unohtaneensa kulkulätkän kotiin, mutta päättää silti mennä toimistolle. Hän pohtii käyvänsä hakemassa aulasta väliaikaisen kulkuluvan. Hän saapuu toimistolle samaan aikaan erään vanhemman työtuttavan kanssa, ja he menevät yhtä aikaa sisälle. Jaska sanoo käyvänsä hakemassa kulkulätkän ja tulevansa sitten perästä. Tuttava kuitenkin hymähtää ja sanoo, että kyllähän me nyt sut tunnetaan, ei näitä ennen vanhaan tarvittu. Jaska välttää vastaamasta ja suuntaa aulaan hakemaan kulkulupaa. Hänen

mielestään tällaisilla toimintatavoilla on syynsä ja niitä tulisi noudattaa. Mitä jos kaikki toimisivat niitä vastoin?

Jaskan mielestä turvallisuuteen suhtautuminen ja siten myös turvallisuuskäytännöt ovat muuttuneet viimeisen kymmenen vuoden aikana parempaan suuntaan. Jaska on muutaman kerran tavannut tahoja, jotka vastaavat organisaation tietoturvallisuudesta. Hän pitää heistä ja arvostaa heitä, mutta tietää myös toisin ajattelevia henkilöitä ja heitä, keillä ei ole mitään hajua ketä turvallisuudesta vastaavat henkilöt ovat. Hänen mielestään tietoturvallisuudesta tai muusta kybermaailman turvallisuudesta ei puhuta organisaatiossa tarpeeksi. Hän on kyllä nähnyt jonkin uutisen intranetissä johonkin tietoturvallisuuteen liittyvästä asiasta, sekä osallistunut turvallisuusinfoihin, mutta hänen mielestään näitä saisi kyllä olla enemmän.

Tarinassa esiintyvien merkitysten taustalla olleet haastatellut olivat henkilöitä, joilla on jotain kosketuspintaa organisaation turvallisuuteen, tietoturvallisuuteen tai tietosuojaan. Tarina alkaa siitä, kun Jaska on unohtanut kulkulupansa kotiin mennessään toimistolle. Hän tiedostaa sen ja ymmärtää että turvallisuusmekanismit ovat tärkeitä, eikä niitä kuuluisi rikkoa. Jaska tunnistaa oman panoksensa merkityksen turvallisuuteen, sillä hän kokee, että hänen itsensäkin käyttäytymisellä on merkitys organisaation turvallisuuteen. Haastatellut myös yleisesti ottaen kokivat, että heidän omalla toiminnallaan on merkitys organisaation turvallisuutta kohtaan. He tunnistivat omasta työstään rooleja, joilla edistävät organisaation kyberturvallisuutta tai tietosuojaa.

> *Minun pitäisi toimia siinä linkkinä, minä vien omalle porukalle tietoa tästä, että mitä tietoturvaan ja tietosuojaa liittyvissä ryhmissä keskustellaan ja yritän myös sitä jalkauttaa.*

Jaska kuitenkin tapaa vanhemman työtuttavansa, jonka suhtautuminen turvallisuuteen on erilaista. Hän on valmis joustamaan toimintatavoista käytännöllisyyden vuoksi. Hän myös vetoaa organisaation aikaisempaan turvallisuuteen suhtautumiseen, joka viittaa siihen, että hän ei välttämättä arvosta nykyistä suhtautumista turvallisuuteen, eikä toisaalta haluaisi asioiden muuttuvan. Haastatteluissa mainittiin, että näkemyserot turvallisuutta kohtaan liittyvät esimerkiksi siihen, kuinka kauan henkilö on ollut töissä organisaatiossa. Lisäksi haastatteluissa tunnistettiin, että organisaatiossa on ryhmiä tai yksittäisiä henkilöitä, joiden suhtautuminen turvallisuuteen voi olla negatiivista. Sen koettiin osaltaan johtuvan

toimintatapojen muutoksista, kun toimintaa kehitetään turvallisempaan suuntaan sekä arvoista, joiden pohjalta turvallisuutta ei välttämättä pidetä kovin merkityksellisenä asiana. Turvallisuuteen liittyvien arvojen koettiin olevan kuitenkin haastateltujen mukaan suurimmalla osalla nykyisestä henkilöstöstä, varsinkin uusilla ja nuoremmilla työntekijöillä, hyvät.

> *Niitä ihmisiä on paljon, jotka ovat olleet kymmeniä vuosia kaupungilla, sillä kaupunki on tyypillisesti semmoinen työnantaja että sä oot pitkään siellä, että kun ne on aloittanut työnsä vielä lintukotovaiheessa, jolloin kaupungintalolle pääsi kuka tahansa, eikä siellä ollut mitään leimauksia väliovissa. On tämä kuitenkin kehittynyt paljon ja mä uskoisin että henkilöstön osalta näillä uudemmilla ja nuoremmilla työntekijöillä on ehkä hyvä suhtautuminen, mutta sitten on tietysti näitä, joita kutsuisin asennevikaisiksi, jotka ovat sokeita niille uhkille ja keskittyvät ehkä vähän niin kuin läpät silmillä tekemään vaan sitä omaa työtä, eivätkä näe sitä organisaation turvallisuusetua.*

Tarinassa työtuttavan asennoituminen turvallisuutta kohtaan voi johtua myös erilaisesta suhtautumisesta turvallisuuden parissa työskenteleviin tahoihin. Haastatteluissa mainittiin, että jotkut organisaation jäsenet eivät välttämättä suhtaudu turvallisuuden parissa työskentelevään henkilökuntaan kovinkaan positiivisesti. Heidät saatetaan nähdä pelottavina tai uhkaavina. Samalla kuitenkin korostettiin sitä, että koska kyseessä on suhteellisen iso organisaatio, on siellä myös hajonta laajaa ja siten paljon erilaisia asenteita ja toimintatapoja.

> *…huomaa sen, että jotkut ihmiset, varsinkin jotka tulee uutena, vähän aristeleekin meidän porukkaa, ne ajattelee, että tässä nyt istuu tämä turvallisuusporukka, kohta ne tulee ja sanomaan jotakin… joskus on käynyt niin, että kun on joutunut puuttumaan johonkin räikeään, esimerkiksi työturvallisuutta uhkaavaan tilanteeseen, niin on kerran todettu yhdessä kokouksessa, että teillä ei ole mitään muuta kuin uhkakuvia ja te olette koko himskatin jengi aivan täyttä p*skaa. Että kyllä se tavallaan sellainen roolikin mitä joudumme tekemään vaikuttaa kyllä siihen, että se voi olla minunkin esihenkilöltä tietoinen veto ettei se halua, että me näyttäydytä minään pelleinä.*

Toiminnan kuvailtiin kuitenkin olevan sellaista, kuin sen kuuluisi organisaation virallisten ohjeistuksien mukaan olevan.

> *kyllähän isossa organisaatiossa on ties mitä tapoja toimia, mutta kyllä mun mielestä arjessakin ihan siellä kahvipöydässä tai muutenkin, että kun me työskennellään avokonttorissa ja meitä on aika paljon siinä kerroksessa ja me ei välttämättä tunneta toisiamme, jos sinä et kulje lätkän kanssa, niin kyllä sieltä niinku joku sit kysyy että et anteeksi millä asioilla sinä olet, kuka sinä olet? Kyllä mun mielestä se miten me toimitaan on aika lailla sen mukaista mitä niinku myös virallisesti halutaan.*

Suhtautuminen tietoturvallisuuteen on muuttunut varsinkin muutaman vuoden sisällä. Organisaatiossa on ymmärretty, että miksi turvallisuutta tarvitaan ja miksi sitä koordinoivia ja sen parissa tekeviä työntekijöitä tarvitaan. Käytännössä jokainen haastateltu näki nykyisen kehityskulun positiivisena.

> *Suhtautuminen on varmaan muuttunut niinku mä sanoin tässä näiden kahden kolmen vuoden aikana kyllä niinku että yhtäkkiä onkin ymmärrys, että miksi me olemme olemassa ja tavallaan että miksi turvallisuutta tarvitaan tai miksi siihen tarvitaan työntekijöitä, jotka sitä oikeasti koordinoi ja yrittää saada vielä vaan paremmaksi, mä uskon että tuossa meidän organisaatiossa se ymmärrys on kyllä kasvanut aivan huimasti.*

Tyyppitarinassa Jaska kertoi arvostavansa turvallisuuden ja tietoturvallisuuden parissa työskenteleviä ihmisiä. Jokainen haastateltu ilmaisi arvostavansa turvallisuuden ja tietoturvallisuuden parissa työskenteleviä. Noin puolet haastatelluista kertoivat tunnistavansa vastuutahot varsinkin sen kautta, että vastuut ovat julkisessa hallinnossa tarkkaan määriteltyjä ja niitä määritellään muun muassa kaupungin hallintosäännössä sekä valtuuston hyväksymässä toimintaohjeessa, ja tietävänsä, keitä nämä henkilöt olivat, puolet olivat epävarmoja. Haastatellut kuitenkin uskoivat, että suuri osa organisaation henkilöstöstä tuskin tietää mahdolliset vastuutahot.

> *... mä oon vähän nyt huono kohdehenkilö veikkaan, että jos mennään niinku vähänkin alemmaksi kuin johtoryhmään ja muualle, niin voi alkaa olla jo vähän heikkoa se tietämys sitten siltä osin.*

Jaska kokee, että organisaatiossa ei puhuta tietoturvasta tarpeeksi. Tietoturvaan tai kyberturvaan liittyvät asiat eivät juuri näy organisaation elämässä, muutoin kuin ajoittaisina, melko harvoina ilmoituksina ja sähköpostiviesteinä.

> *Mutta ei näistä asioista yleisesti puhuta tai niinku sanota et menkää tuonne, lukekaa ja tutkikaa tätä ja selvittäkää, katsokaa, opetelkaa käyttäytymään näin.*

Joukon tyyppitarina

Joku koputtaa Joukon ovea. Jouko kutsuu hänet sisään. Mun pitäis tarkistaa yks juttu, tiedätkö sä mistä mä nämä materiaalit löytäisin, eräs kollega kysyy. Jouko katsoo hänelle näytettyä puhelimen ruutua, ja pohtii ääneen – nämähän liittyvät tietoturvallisuuteen. Jouko opastaa hänet oikealle sivulle, kollega kiittää ja poistuu huoneesta. Jouko miettii, että kyllähän noi nyt pitäisi tietää, tai ainakin mistä ne löytyvät. Noin vuosi sitten Jouko havaitsi työtietokoneensa käyttäytyvän oudosti ja epäili, että siinä on mahdollisesti jokin haittaohjelma. Jouko säikähti ja häpesi hieman, mutta lopulta ilmoitettuaan asiasta eteenpäin hän huomasi, että asiaan suhtauduttiin vakavasti, mutta positiivisesti. Jouko ei ollut tiennyt, mitä tietoturvapoikkeamasta ilmoittamisen jälkeen tapahtuisi ja kuinka siihen reagoitaisiin. Jouko oli kuitenkin osannut olla hereillä, sillä vasta joku oli näyttänyt hänelle hyvin tehdyn huijausviestin ja hän oli huomannut organisaation sisäistä viestintää aiheesta ja lukenut aiheesta itse intranetistä löytyvältä sivulta. Jouko ei kuitenkaan kaipaa lisää ainakaan henkilökohtaisesti saapuvaa viestintää, sillä hän kokee olevansa asiantuntijaroolissa vastuussa yleisen viestinnän seuraamisesta sekä asioihin perehtymisestä, mikäli kokee sen tarpeelliseksi. Liika viestintä ja muistuttelu saattaisi myös tuntua ärsyttävältä roskapostitukselta.

Tyyppitarinan alussa kollega tulee kysymään Joukolta, mistä eräät tietoturvallisuuteen liittyvät materiaalit löytyisivät. Jouko tietää, mistä ne löytyvät ja kertoo kollegalle. Jouko hieman ihmettelee, miksei hän tietänyt näitä asioita, tai että mistä ne löytyisivät. Tarinassa

Jouko on perillä tietoturvallisuuteen liittyvistä ohjeistuksista ja materiaaleista sekä mistä ne löytyisivät. Haastatteluissa nousi kuitenkin esiin epäilys siitä, että isommassa mittakaavassa organisaation sisällä tieto näiden asioiden olemassaolosta ja niiden sijainnista saattaa olla kehnoa.

Jouko on seurannut aihepiiriin liittyvää organisaation sisäistä viestintää ja kokee, että se on hänen velvoitteensa. Jouko pitää viestinnän tasoa riittävänä, eikä kaipaa ainakaan lisää henkilökohtaista viestintää aihepiiristä. Hän kokee, että on asiantuntijaroolissa itse työskentelevänä velvollinen seuraamaan viestintää ja ottamaan asioista selvää tarpeen vaatiessa. Liiallinen viestintä saatetaan kokea epämukavaksi.

> *Minä saattaisin kokea sen spämmiksi, että minun mielestä tässäkin tullaan just siihen yksilön omaan harkintaan ja vastuuseen, että minä en itse koe että se tietoturvan taso paranisi sillä että ihmisiä spämmätään joillakin sähköpostin muistutuksilla, se sitten saattaa aika nopeasti päätyä siihen että se koetetaan vaan ärsyttäväksi. Että jos sä oikeasti käsittelet arkaluonteista tietoa niin sitten se on se niinku esimiehen varmistettava että alaiset on sen järjestelmän ja sen tiedon osalta tilanteen tasalla… ja sitten muut jotka työskentelee asiantuntijaroolissa ja joutuu niinku tekemään sitä tapauskohtaista harkintaa niin on heidän omalla vastuullaan sitten seurata sitä viestintää muun muassa siellä intranetissä ja perehtyä asioihin sitten tarpeen vaatiessa.*

> *Minä koen, että se [tieto] on niinku saatavissa ja että ei sitä varmaan niin paljoa tule niinku annettuna, että siinä mun mielestä taas mennään tähän yksilön harkintaan, että varmaan siinä niin kuin uudessa roolissa tai tehtävässä aloittaessa saa semmoisen peruspaketin tietoturvakoulutuksen kautta ja sitten kaikki extra on niinku sun oman aktiivisuuden piirissä että kyllä se tieto on löydettävissä mutta ei se niinku sillä tavalla kotiovelle tule.*

Jouko myös kokee, että turvallisuuteen suhtaudutaan henkilöstön osaamista ja tietotaitoa kunnioittaen. Kulttuuri ei kuitenkaan ole varovaisuutta korostava, vaan peilaa yksilön harkintaan, tiukkojen ohjeistuksien sijaan.

> *Suhtaudutaan tiedostaen, että suurin osa siellä on kuitenkin korkeasti koulutettuja ja silleen valveutuneita, paljon tietotyötä tekeviä henkilöitä, eli uskon että sellainen yleinen tietoisuus on aika niinku vahvaa, mutta sitten taas ehkä se kulttuuri ei ole mielestäni sellainen varovaisuutta korostava, että mielestäni se palaa ehkä enemmän siihen yksilön harkintaan ja yksilön maalaisjärkeen, kuin siihen että olisi joku valvonta tai tiukka ohjeistus jota sitten kaikki noudattaisivat.*

Tarinassa nousee esiin, että Jouko ja joku muu työntekijä ovat keskustelleet mahdolliseen kyberuhkaan liittyvistä asiasta. Tietoturvaan liittyvistä asioista vaihdetaan tietoa organisaatiossa ja esimerkiksi mahdollisista uhkista varoitetaan toisia työntekijöitä.

> *ollut että joku niinku oikealta yhteystiedoista näyttävä on jakanut sinulle Microsoftin pilvessä jonkun tiedoston ja se on näyttänyt niinku ihan sellaiselta Microsoftin lähettämältä se koko viesti, niin muistan että kun se tuli mun yhdelle kollegalleni niin hän sitten kaikille näytti sen viestin niinku tiedoksi, että tällainen ja se oli niinku oikeasti vakuuttavan näköinen.*

> *Mä olen välillä ihmetellyt että kun meillä on paljon puhuttu siitä että saattaa tulla paljon tällaisia kalasteluviestejä ja hämäriä sähköposteja. Mulle ei niitä kyllä juurikaan tule, toisille tulee sitten enemmän, mutta mä oon miettinyt että voisikohan se olla sitten se [etten ole jakanut niin paljoa yhteystietoja] ja olen ymmärtänyt että kollegoille saattaa tulla paljon enemmän roskapostia.*

Jouko on kokee, että tietoturvapoikkeamasta ilmoittaminen oli positiivinen prosessi, jossa häneen sekä ilmoitukseen suhtauduttiin asiallisesti ja tarpeen vaatimalla vakavuudella. Jouko ei kuitenkaan ollut tiennyt, mitä ilmoittamisen jälkeen tapahtuisi, joka oli puolestaan vaikuttanut hänen suhtautumiseensa ilmoittamiseen. Haastatteluissa nousi esiin, että ilmoittamisen jälkeiseen prosessiin nähdään sisältyvän epäselvyyksiä.

> *Luulen että yleisesti ottaen kaikki ajattelisi vaan niin että ”ei hemmetti että mitä tästä opitaan” -tyyppisesti, en usko että siitä olisi kukaan lähtenyt mitään haukkumaan tai pitämään idioottina. Tämä juttu on niin muuttuvaa koko ajan,*

niinku että tekevällehän sattuu. Luulen että enemmän niinku tota linjaa olisi, kunhan kertoo sen eikä yritä salata.

Vähän epäilen ettei välttämättä ole kaikille ihan selvä, että he ehkä tietää sen mihin se pitää ilmoittaa koska sitä niin monessa paikassa kyllä meillä tiedotetaan ja muistutetaan. Mutta voi olla että olisi syytä ehkä avata vähän tarkemmin että mitä sitten tapahtuu…

Haastatteluissa nostettiin myös esille, joillekin henkilöille tietoturvapoikkeamasta ilmoittaminen ei välttämättä tunnu tärkeältä ja että siihen liittyvien tunteiden vuoksi ilmoittamista saatetaan pohtia ja välttää.

Häpeä varmaan on se, mä mokasin ja että ei tätä kukaan huomaa, antaa olla. Et niinku mä uskoisin että häpeä ja sitten se toinen voi olla pelko, että tuleeko mulle jotain kustannuksia tästä, menikö nyt joku juttu nyt kyykkyyn ja pitää tilata kalliit korjaajat sinne, tai että saastui koneita…

Ehkä juuri tämä tietämys siitä että pitää ilmoittaa ne pienetkin epäilyt itseä huolestuttaa, mutta kyllä mä uskon että siellä on niitä jotka vähän niinku pelkääkin sitä.
Että jos tosiaan on mennyt sitten avaamaan linkin tai muuta niinku et mitä seuraamuksia itsellä on. Olen jutellut muutamien kanssa joskus siis silloin kun oltiin vielä kahvitauoilla yhdessä, niin jossain kahvipöydässä muistan että kyllä niinku moni koki sen niin että jättäisi kertomatta, vähän niinku antaa olla vaan

Tuula Turvallisuuden tyyppitarina

Tuula kuuluu osana työtehtäviään erilaisiin verkostoihin, joissa käsitellään tietosuojaan ja tietoturvallisuuteen liittyviä asioita. Verkostoissa on viime aikoina käsitelty perehdyttämiseen, koulutukseen ja tietoturvan koordinointiin liittyviä asioita. Siellä ollaan huolissaan siitä, että organisaatiossa on paljon henkilöitä, jotka eivät ole suorittaneet pakollista tietoturvakoulutusta. Ongelmaksi on tullut kuitenkin se, että vaikka koulutuksen suorituksia seurataan läpi organisaation, ei sen tekemättä jättämisestä ole varsinaisesti

mitään seuraamuksia. Tuula myös epäilee, ettei osaamisen taso lopulta ole kovinkaan hyvä, eikä yleisesti ottaen koulutuksiin suhtautuminen ole myöskään sieltä parhaimmasta päästä. Tietoturvakoulutuksia järjestetään ja vaikka ne ovat hänen mielestään hieman yksinkertaisia, uskoo hän niistä olevan jotain hyötyä.

Tuula pohtii, että ikään kuin organisaatio ei haluaisi velvoittaa, tai että sillä ei ole välineitä velvoittaa työntekijöitään suorittamaan koulutusta. Toisaalta realiteetit, kuten kuntatalouden kireys ja lakisääteisten velvoitteiden noudattaminen painavat muiden asioiden tekemisen pienimmälle mahdolliselle tasolle. Tuula tunnistaa, että asioita on haastavaa viedä eteenpäin, sillä resurssien puute ja toisaalta tahtotila ei mahdollista työmäärän kasvattamista halutulle tasolle. Hän kokee henkilöstön olevan tärkein voimavara ja että heihin tulisi panostaa. Tuula kokee yhdessä muiden verkostoon kuuluvien ihmisten kanssa, että turvallisuuteen suhtaudutaan vakavasti, mutta organisaation rakenteet ja toimintaympäristö vaikeuttavat ongelmien puuttumista ja toimintaa. Hän toivoo, että sääntely asiaa kohtaan kasvaisi, jolloin asioiden vaatiminen ja vähimmäistason nostaminen olisi helpompaa.

Tyyppitarina alkaa esittämällä huolenaiheen organisaation tietoturvakoulutusta kohtaan. Tyyppitarinassa organisaation tietoturvakoulutuksen toteutusta ei pidetä riittävänä ja siihen suhtaudutaan kehnosti. Esiin nousi näkemys, jonka mukaan jotkut suhtautuvat tietoturvakoulutuksiin, kuin ne olisivat epämieluista ylimääräistä tehtävää, kun taas ne, jotka seuraavat tapahtumia ja mediaa, näkevät tietoturvakoulutukset positiivisena asiana. Tietoturvakoulutuksiin kytkeytyvä henkilö puolestaan kokee niiden olevan liian helppoja, sellaisia että ne eivät täytä niille asetettuja tavoitteita.

> *Niinku kaikkeen tällaiseen niin sanotusti oman työn ylimääräiseen tehtävään, ne niinku yleensä jätetään sitten viime tinkaan ja vähän sellaista [asennetta], että kaikennäköistä tässä pitää tehdä... mutta kyllä oikeasti huomaa sen että ne jotka seuraa maailmaa laajemmin ja lukee mediaa ja muuta niin he sitten taas näkee sen positiivisena, että hienoa että meillä on tällaista, mutta he taas ei ehkä osaa ajatella sitä niinku minä ajattelen, että se on liian helppoa ja tavallaan se, että sä saat jatkaa sitten kun sä olet tehnyt sen yhden tentin, eikä ole mitään välitsekkejä… siitä olen myös huolissani, että kun tulee uusi työntekijä tai harjoittelija tai joku, niin miten se perehdytys oikeasti hoidetaan.*

Haastatteluissa henkilöstön turvallisuuden osaamistasoa pidettiin vajavaisena, varsinkin suhteessa siihen, että kyseessä on varsin suuri organisaatio. Syynä tähän pidettiin esimerkiksi kouluttamisen jalkauttamista sekä sitä, että pakollisen tietoturvakoulutuksen käyneiden määrän arvellaan olevan melko alhainen.

> *Tällä hetkellä ymmärrys ei varmaan ole sillä tasolla, millä sen pitäisi olla tämän kokoisessa organisaatiossa. Sen tiedon kouluttamisen jalkauttaminen on ollut aika hidasta, kun se silloin aikanaan muutama vuosi sitten tietosuoja-asetusten myötä tuli ikään kuin pakolliseksi.*

Useissa haastatteluissa nostettiin esille, että tietoturvakoulutuksen käyneiden määrä on melko alhainen. Koulutuksen mainittiin olevan ’niin sanotusti pakollinen’, sillä ilmeisesti sen suorittamisen valvonta on tapauskohtaista ja heikkoa ja koulutuksen suorittamatta jättämisestä ei tule seuraamuksia.

> *Niin se on ilmeisesti alhainen se prosentti mitä meidän henkilöstöstä on tällä hetkellä sen pakollisen, niin sanotun pakollisen, koulutuksen käynyt.*

Tietoturvakoulutusta pidettiin varsin tärkeänä tekijänä turvallisuuden edistämisessä, mutta sen kuvailtiin olevan ikään kuin lapsenkengissä.

> *Kyllähän aika lapsenkengissä on ne meidän koulutukset. Minä itse olen ne suorittanut aina, koska ne ovat pakolliset, niin kyllä ne on aika lailla sellaiset että vasemmalla kädellä voi vähän heitellä sinne vastauksia, mun mielestä ne on liian helpot, siinä ei niinku tavallaan vaadita sitä osaamista, että sä pystyt jopa niinku päättelemään tiettyjä asioita, mutta toivottavasti nyt tilanne tulee muuttumaan*

Resurssien puute tunnistettiin myös olennaiseksi vaikuttavaksi tekijäksi kyberturvallisuuden kehittämisessä ja jalkauttamisessa. Resurssien osalta merkittäväksi tekijäksi tunnistettiin kuntatalouden kireys ja resurssien suuntaaminen muualle, kuin turvallisuustyöhön.

> *Pitäisi olla ensinnäkin enemmän henkilöitä, jotka pystyy näitä sisäisiä koulutuksia ja infoja pitämään. Ei tällä porukalla, jolla jokaisella on ikään*

> *kuin se oma vastuualueensa pystytä vastaamaan tuohon työyksikkö määrään tai työpaikka määrään mikä meillä on, että toki meillä on sitten erilaisia verkostoja mihin me yritetään jalkautua… Että kyllä tuota noin niin ehdottomasti tarvittaisiin resursseja lisää siihen työhön*

> *Turvallisuus ei saisi maksaa, mitään se ei saa näkyä, haista, maistua, että se on niinku vähän siellä takavasemmalla oleva välttämätön paha, mutta sitten kun jotain tapahtuu niin kysytään, että miksi tämä asia ei ollut kunnossa. Niinku osa tavallaan pitää sitä välttämättömänä pahana ja ei halua satsata siihen ja se pidetään minimissä. Satsataan niihin omiin ideologioihin tai oman toimialan toimintaan, koska resurssit on aika niukat tänä päivänä. Oikeasti kuntatalous on aika kireällä, että tehdään ne lakisääteiset velvoitteet, satsataan niihin ja hoidetaan sitten nämä muut niinku minimillä.*

Turvallisuustyötä hankaloittavana tekijänä nähtiin myös se, että nykyisellä tietoturvallisuutta koordinoivalla ja valvovalla taholla ei ole suoraa johto-oikeutta mihinkään käytännön työtä tekevään yksikköön. Tämä on johtanut siihen, että toiminta on vaikeutunut ja hidastunut sekä toiminnan vaikutus ei ole halutulla tasolla.

> *Jos ajatellaan kyberturvallisuutta ylipäätänsä niin kyllähän tämän yksikön niinku ohjattavana ja valvottavana on, mutta operatiivista puolta hoitaa sitten tietohallinto joka on sitten eri yksikön alaisuudessa, et tästä on tullut vähän sellaista että kun ei ole suoraa johto-oikeutta niinku tiettyyn yksikköön, niin voidaan vaan niinku todeta ja muuta, niin kyllä se vähän hidastaa ja vaikeuttaa, et asiat saadaan eteenpäin ja joutuu niinku monen päättäjän kanssa asiasta keskustelemaan.*

Haastatteluissa esiin nousi myös näkemys, jonka mukaan organisaatiolla ei ole halua tai välineitä vaatia, tässä tapauksessa tietoturvakoulutuksen suorittamista, henkilöstöltä. Haastatteluissa toivottiinkin lainsäädännön kasvattamista ja sen nähtiin antavan organisaatiolle sen tarvitsemaa selkärankaa asioiden vaatimiselle.

meidän pitäisi uskaltaa organisaationa oikeasti ruveta vaatimaan enemmän eikä ajatella niin, että työntekijät tästä mielensä pahoittaa, että kyllä meidän pitäisi ymmärtää, mitä meidän pitää osata.

Kaipaisin ehkä lisää jonkinnäköistä kuntiin kohdistuvaa [lainsäädäntöä] valtion hallinnolta. Tietoturvalakihan uudistuu nyt ensi vuoden vaihteessa, että se antaa nyt selkänojaa, että me voidaan vaatia että nämä asiat tulee kuntoon, koska se laki edellyttää sitä. Se on hyvä että tulee lakiin, niin nyt on pakko laittaa ne asiat kuntoon, mitkä on retuperällä.

Kun ei ole suoraa sitä niinku linjajohtoa johonkin yksikköön, niin nyt kuitenkin on se laki joka sitten rupeaa vaatimaan meiltä tiettyjä asioita.

Organisaatiossa tunnistetaan laajalti kyberturvallisuuden ylläpitämiseen ja kehittämiseen liittyviä ongelmia ja yhteisenä päämääränä nähdään olevan kyberturvallisuuden kehittäminen. Organisaatiossa tunnistetaan, että kyberturvallisuuden kehittämiseen suunnataan paljon voimavaroja.

Mielestäni täällä kyllä kovasti yritetään ja pyritään parantamaan kyberturvallisuutta näin niinku yleisellä tasolla mutta ongelma on edelleen se, että on tosi iso organisaatio, on tosi vaikea jalkauttaa ja jokainen asia vaatii sitä omaa aikaansa, ja pitäisi ehkä panostaa siihenkin että on joku välitaso siinä välissä olisi niinku viestittämässä tätä ja jalkakauttamassa sitä työtä. Mitä kyllä kovasti tehdään.

Kyllä se tänä päivänä on noussut niinku arvoon arvaamattomaan, että ihan selkeästi nyt niinku kaiken tämän kahden ja puolen vuoden aikana on tehty aika lailla kehitystyötä asian eteen ja tehdään edelleenkin ja toki sitten on tiettyjä lakivelvoitteitakin mitä tulee jatkuvasti eli joudutaan alkamaan selvittelemään asioita eri lailla. Kyllä siihen on selkeästi nyt on tahtotila että sitä halutaan kehittää.

6 YHTEENVETO JA KESKUSTELU

6.1 Yhteenveto

Tämän tutkielman tarkoituksena on kuvailla, millä tavoin kyberturvallisuuskulttuuria ilmentävät inhimilliset piirteet näkyvät tutkielman kohteena olevan organisaation henkilöstön toiminnassa ja asenteissa, sekä toisaalta tarkastella organisaatiokulttuurin ja toimintaympäristön vaikutusta kyberturvallisuuskulttuuriin. Organisaation näkökulmasta sen on keskeistä pyrkiä suojaamaan omaa toimintaansa varautumalla kyberuhkiin. Organisaatiossa toimivat työntekijät ovat tavallisia henkilöitä, jotka ovat vuorovaikutuksessa organisaation kyberinfrastruktuuriin niin omien asenteidensa, käyttäytymisensä ja uskomustensa, eli toisin sanoen henkilökohtaisen kyberturvallisuuskulttuurinsa, kuin myös organisaation tietoturvapolitiikan, organisaation sisäisten asenteiden, olettamuksien ja toimintatapojen kautta. (Da Veiga, 2016.) Yleisesti ottaen organisaatiossa tunnistetaan laajasti kyberturvallisuuden ylläpitämiseen ja kehittämiseen liittyviä ongelmia. Kyberturvallisuuden kehittäminen on yhteinen päämäärä ja siihen suunnataan paljon rajallisia voimavaroja.

Ihmiset antavat kyberturvallisuudelle erilaisia merkityksiä ja heidän asenteensa kyberturvallisuutta kohtaan on yksilökohtaista. Asenteiden on tunnistettu vaikuttavan tietoturvakäyttäytymiseen (Ng & Rahim, 2005; Anderson & Agarwal, 2010; Ifinedo, 2012), jolla puolestaan on merkittävä vaikutus organisaation kyberturvallisuuteen (Mishra & Dhillon, 2006; Bulgurcu ym., 2010; Crossler ym., 2013). Ihmistä pidetään usein tietoturvan heikoimpana lenkkinä (Bulgurcu ym., 2010) inhimillisten tekijöiden mahdollistaessa tietoturvaloukkauksien toteutumisen (Grobler ym., 2021). Pelkät teknologiset menetelmät ja työkalut eivät välttämättä takaa organisaation tietovarantojen suojelemista (Siponen ym., 2008). Työntekijöiden käyttäytyminen, arvot ja uskomukset nähdäänkin merkityksellisiksi organisaation tietovarantoja suojellessa (Mishra & Dhillon, 2006; Bulgurcu ym., 2010; Crossler ym., 2013), jotta inhimillisen tekijän uhka saadaan minimoitua. Tässä luvussa pyritään aiempaa kirjallisuutta huomioiden vastaamaan johdantoluvussa esiteltyyn tutkimuskysymykseen “Millaiset tekijät ja käsitykset ovat vaikuttaneet kyberturvallisuuskulttuurin olemukseen organisaatiossa?”.

Tutkielman tuloksia ja tutkimuskysymystä tarkastellaan ja pohditaan seuraavissa alaluvuissa. Ensin käsitellään henkilökohtaisten tekijöiden ja käsitysten vaikutusta organisaation kyberturvallisuuskulttuuriin ja sitten organisaatiokulttuurin ja toimintaympäristön vaikutus kyberturvallisuuskulttuuriin.

6.1.1 Henkilökohtaisten tekijöiden ja käsitysten vaikutus organisaation kyberturvallisuuskulttuuriin

Tutkielman tuloksien mukaan henkilökohtainen kyberturvallisuuskulttuuri koskettaa sekä henkilökohtaista että työhön liittyvää elämää. Suurin osa haastateltavista kertoi toimivansa ja ajattelevansa samalla tavoin työssä ja vapaa-ajalla. Siviilielämässä kyberturvallisuutta koskettaviin kysymyksiin kiinnitettiin sitä enemmän huomioita, mitä enemmän tietoa aihepiiristä oli. Organisaatioon kohdistuvat uhkat koettiin kuitenkin vakavimpina, kuin henkilökohtaiseen elämään kohdistuvat uhkat.

Aiemman tutkimuksen mukaan tietoturvatietoisuudella, jolla viitataan tietoturvan merkityksen ymmärtämiseen, on positiivinen vaikutus henkilön käyttäytymiseen (Shaw ym., 2009; Farooq ym., 2015) sekä tietoturvaan liittyvien uhkien kattavampaan havainnointiin (Huigang & Yajiong, 2010). Heikko tietoturvatietoisuus puolestaan on merkittävä syy tietoturvauhkille (Siponen ym., 2007; D'Arcy ym., 2009). Tämän tutkielman tulosten perusteella aiemmat tai nykyiset työkokemukset, koulutus ja muu osaaminen tai niiden puute vaikuttavat kyberturvallisuudelle annettaviin käsityksiin.

Tutkielman tulokset osoittavat, että henkilökohtaisen kyberturvallisuuskulttuurin tasolla näkyi aiemman tutkimuksen esiin nostama kyberturvallisuuden käsitteen vakiintumattomuus (Limnéll ym., 2014). Tutkielman tulokset tukevat myös Von Solmsin ja Von Niekerkin (2013) havaintoja siitä, että kyberturvallisuuden ja tietoturvallisuuden käsitteitä käytetään usein synonyymeinä. Kyberturvallisuuden käsitteelle annetaan lähes yhtä monta määritelmää kuin kuinka monta haastateltavaa tutkielmassa on, ja siihen viitattiin esimerkiksi puhumalla tietosuojasta, tietojen kalastelusta, tietoturvasta, sosiaalisesta mediasta, kyberrikollisuudesta ja yleisesti internetin käytön turvallisuudesta.

Aiemmat työkokemukset ja koulutus, joiden kautta kyberturvallisuuteen oli saatu kosketuspintaa, lisäsivät tietoa kyberturvallisuudesta. Tällöin kyberturvallisuuden nähtiin tarkoittavan sähköisen maailman tai sähköisen ympäristön turvallisuutta, jonka kanssa ollaan vuorovaikutuksessa. Henkilöt, joilla oli taustallaan tieto- ja viestintäteknologiaan liittyvä koulutus tai muuta keskeistä kyberturvallisuuteen liittyvää osaamista, kokivat osaavansa toimia tietoteknisessä ympäristössä, suhtautuivat kyberuhkiin realistisesti ja pystyivät käymään läpi erilaisia uhkakuvia sekä niihin sopeutumismalleja ja toimenpiteitä. Ammatillisen taustan kautta saadun kokemuksen, tiedon ja ymmärryksen koettiin vaikuttavan käyttäytymiseen kybermaailmassa, jossa se auttoi erilaisten uhkakuvien tunnistamisessa.

Vähäinen kokemus ja tieto kyberturvallisuudesta tai siihen liittyvistä aihepiireistä rajasi kyberturvallisuuden merkityksen arkielämässä käytettyjen sähköisten palveluiden sujuvuuteen. Lisäksi kokemus omien taitojen tai teknologisen kompetenssin riittämättömyydestä lisäsi epävarmuuden tunnetta haastateltavissa. Yleisesti ottaen haastateltavat kokivat omien teknologisten taitojensa olevan riittävät päivittäiseen toimimiseen, mutta omia taitoja ei pidetty varsinaisesti kovin hyvinäkään. Omaan ymmärrykseen sekä tietoihin ja taitoihin ei luotettu niin paljoa, että voitaisiin uskoa olevan varmasti turvassa kybermaailmassa.

Epävarmuus näkyi haastatteluissa käsityksenä siitä, että mikään tieto ei ole internetissä täysin turvassa ja lopulta mihin tahansa tietojärjestelmään voidaan tunkeutua. Turvallisuuteen luottaminen voi luoda vain näennäistä turvallisuuden tunnetta, jolloin vaarana on siihen tuudittautuminen. Epävarmuus vaikuttaa myös käyttäytymiseen kybermaailmassa niin henkilökohtaisella kuin organisaatiotasolla, sillä kaikkea epävarmaksi koettua, kuten outoja palveluita pyritään välttämään ja outoihin tapahtumiin, kuten arveluttaviin sosiaalisen median kaveripyyntöihin ja sähköpostin liitetiedostoihin kiinnitetään paljon huomiota. Epävarmuutta lisäsi myös maailmanpoliittinen tilanne. Esimerkiksi Venäjän sotatoimet Ukrainassa, muut henkilökohtaiset ja yhteiskuntaa koskettavat kyberuhkat, kyberrikollisuus sekä käyttäjien seuranta ja tiedonkerääminen niin yksityisten palveluiden kuin valtioiden toimesta tuovat henkilökohtaiseen kyberturvallisuuskulttuuriin negatiivisempia ja uhkaavampia merkityksiä. Näitä merkityksiä ovat muun muassa epäluottamus internetissä toimimiseen ja yleinen epävarmuus kybermaailmaa ja sen turvallisuutta kohtaan.

Tutkielmaan haastatelluista noin puolella on jokin henkilökohtainen kokemus kyberturvallisuuteen liittyvästä uhkasta, kuten epäilyttävän liitteen tai kalasteluviestin huomaamisesta ja siitä ilmoittamisesta. Epäilyttävän viestin tai muun tietoturvapoikkeaman huomaaminen koetaan positiivisena ja selkeästi onnistumisena. Jos tietoturvapoikkeama jää huomaamatta, se koetaan pääsääntöisesti noloksi, ahdistavaksi ja surulliseksi, mutta ei ylitsepääsemättömäksi hetkeksi. Haastatteluissa kävi myös ilmi, että organisaation henkilöstö keskustelee kyberturvallisuuteen liittyvistä aihepiireistä ja jakaa kyberturvallisuuteen liittyvää tietoa esimerkiksi kyberturvallisuuteen liittyvistä uhkista. Tiedon jakaminen organisaatiossa kasvattaa toisten työntekijöiden tietoutta sekä mahdollistaa siten paremman uhkakuvien tunnistamisen. Kyberturvallisuuskulttuuri on ilmiö, joka näkyy useilla eri tasoilla ja organisaation kyberturvallisuuskulttuuriin vaikuttaa sen henkilöstön kyberturvallisuuskulttuurit (Da Veiga, 2016).

Tutkielman tulosten mukaan haastateltujen asenteet kyberturvallisuutta kohtaan koskivat niin henkilökohtaista kuin työelämää. Ne vaikuttivat Da Veigan (2016) mukaisesti käyttäjän vuorovaikutukseen kyberavaruudessa niin henkilökohtaisella, kuin organisaatiotasolla. Aiemmat hyvät kokemukset kyberturvallisuudesta vaikuttivat asenteeseen positiivisesti. Positiivinen asenne korostui henkilöillä, jotka olivat aikaisemmin työskennelleet alalla, jolla tietoturva- ja tietosuojasääntely sekä yleinen turvallisuus olivat olleet merkittävässä roolissa. Asenteeseen vaikutti myös haastatellun nykyinen työtehtävä. Tietoturvallisuuteen ja tietosuojaan liittyvät arvot saattoivat olla jossain määrin vastakkain työtehtävien kanssa, jolloin niitä yritettiin ikään kuin sovittaa toisiinsa. Tällöin tietoturvallisuuden ja tietosuojan tärkeyttä korostettiin, mutta niiden asettamien vaatimuksien toivottiin olevan kohtuullisia. Tutkielmaan osallistujat kuvailivat asenteiden olevan myönteisiä hänen henkilöpiirissään, mutta uskoivat niiden olevan mahdollisesti negatiivisia muualla organisaatiossa.

Tutkielmassa haastateltujen asenne oli pääsääntöisesti hyvä niin henkilökohtaisessa, kuin myös työelämässä, mutta esiin nousee myös toimintamalleja, jotka eivät tue tätä johtopäätöstä. Aikaisempi tutkimus osoittaa, että asenne liittyy toiminnan tekemisen aikomukseen, joka on käyttäytymistä ennustava tekijä (Karahanna ym., 2005; Mishra & Dhillon, 2006). Haastateltavat havaitsivat itsensä ja muiden toimivan tietoturvan vaarantavalla tavalla, jos se sujuvoitti työntekoa. Esimerkiksi VPN-yhteyden koettiin joskus hidastavan datayhteyttä niin paljon, että sen käyttöä välteltiin. Erinäisiin palveluihin pääsy saatettiin kokea hankalaksi, jolloin samoja käyttäjätunnuksia jaettiin. Lisäksi tunnistetaan,

että joitain työhön käytettäviä työkaluja käytetään henkilökohtaisilla tunnuksilla, jolloin riski työ- ja henkilökohtaisten asioiden sekoittumiselle kasvoi. Tutkielman tulosten mukaan näissä tapauksissa henkilöiden asenne turvallista toimintaa kohtaan voi olla jollain tavoin puutteellinen. Selittävää tekijää voidaan hakea esimerkiksi Tamin ym., (2010) tutkimuksesta, jonka mukaan salasanojen turvallisuus oli kompromissi mukavuuden ja käytännöllisyyden kanssa. Ng & Rahim (2005) puolestaan totesivat, että käyttäytymiseen vaikuttaa esimerkiksi turvallisuutta parantavan asian koettu hyödyllisyys. Tulosten pohjalta voidaan nähdä, että kompromisseja turvallisuuden ja käytettävyyden välillä tehdään ja joissain tapauksissa turvallisuutta parantavia asioita ei koettu niin hyödyllisiksi, että niitä käytettäisiin, vaikka se haittaisi käyttäjäkokemusta. Epäselväksi jää kuitenkin lopulta se asenne, joka johtaa edellä mainitun kahden vaihtoehdon väliseen pohdintaan.

Kyberturvallisuuden ja tietosuojan merkitys kuitenkin tiedostetaan päivittäisessä toiminnassa. Omien asenteiden tärkeyttä painotettiin, sillä kyberturvallisuuden ei koeta olevan yleisesti kiinnostava aihepiiri. Varsinkin henkilöiden kertomuksissa, joilla oli suoraa kokemusta kyberturvallisuuden tai tietosuojan aihepiirin ympärillä työskentelystä korostuu näkemys, jonka mukaan kyberturvallisuus ei kiinnosta joitain ihmisiä ollenkaan, eivätkä ihmiset yleisesti ottaen ajattele kyberturvallisuutta. Tutkielman mukaan omaa asennetta kyberturvallisuutta kohtaan korostetaan, niin henkilökohtaisella kuin organisaatiotasolla, suhteessa henkilöihin, joiden asenne ei ole niin hyvä. Asennetta pidetään tärkeänä tekijänä, joka lopulta kuvaa sitä, miten henkilö on vuorovaikutuksessa kyberturvallisuuden kanssa. Haastatellut toivat esille erilaisia toimenpiteitä ja tapoja, joilla pyrittiin huolehtimaan arjen turvallisuudesta. Erityisesti tietosuojaan liittyviä toimenpiteitä arvostettiin ja pidettiin tärkeinä. Joissain tapauksissa taustalla oli pelko identiteettivarkaudesta, joka koettiin pelottavaksi ja raskaaksi koettelemukseksi.

Tutkielman tulosten mukaan lähes jokainen haastateltava oli tietoinen erinäisistä toimintatavoista ja keinoista, joita käytetään laitteiden tietoturvallisuuden parantamiseen heidän organisaatiossaan sekä toimintatapoja ja keinoja, joilla he pyrkivät parantamaan suojaustaan henkilökohtaisesti. Keinot olivat sekä teknisiä, että myös erilaisia toimintatapoja. Jokainen haastateltu tiedostaa ja ymmärtää turvallisuusmekanismien tärkeyden sekä oman käyttäytymisen merkityksen organisaation turvallisuutta kohtaan. Omalla toiminnalla koettiin olevan merkitys organisaation turvallisuutta kohtaan. Toiminta kuvaileekin Vroomin & Von Solmsin (2004) ideaalista tietoturvakulttuurin määritelmää,

jonka mukaan vapaaehtoinen ja itseohjautuva tietoturvallinen toiminta sekä käytös ovat osa organisaation päivittäistä toimintaa. Lisäksi haastatellut tunnistavat omaan työhönsä liittyviä rooleja, joiden kautta he edistävät organisaation kyberturvallisuutta tai tietosuojaa.

6.1.2 Organisaatiokulttuurin ja toimintaympäristön vaikutus kyberturvallisuuskulttuuriin

Kyberturvallisuuskulttuuri on jossain määrin päällekkäinen organisaatiokulttuurin kanssa, sillä molemmat kulttuurit käsittävät arvoja ja uskomuksia, jotka vaikuttavat organisaation sisäiseen maailmaan ja toimintaan (Da Veiga, 2016). Kyberturvallisuuskulttuurin käsitteen määrittelyssä on myös hyödynnetty tietoturvakulttuurin määritelmää, organisaatiokulttuurimallia sekä organisaatiokulttuurin määritelmiä (Van Niekerk & Von Solms, 2006; 2010; Da Veiga & Eloff, 2010; Da Veiga, 2016). Tämän tutkielman mukaan organisaatio erityispiirteineen ei tue parhaan mahdollisen kyberturvallisuuskulttuurin kehittämistä.

Tutkielman kohdeorganisaatio on julkishallinnollinen kaupunkiorganisaatio. Julkishallinnolliselle organisaatiolle tyypillistä on, että se käyttää julkista valtaa lainsäädännön rajoissa. Kuntien toimintaa säädellään muun muassa kuntalaissa (KL 410/2015). Tutkielman analyysin ohessa tunnistettiin kaupungin julkishallinnollisen toimintaympäristön merkitys kyberturvallisuuskulttuurin olemukselle, jonka vuoksi sitä käsitellään tässä tutkielmassa.

Tutkielman tuloksien mukaan organisaatiossa on toisistaan poikkeavia toimintatapoja ja asenteita. Organisaatiossa työskentelee henkilöitä useista eri ammattiryhmistä, joihin liitetään erilaisia kulttuurisia piirteitä esimerkiksi arvojen, asenteiden ja toimintatapojen kautta. Tässä tutkielmassa aiemmin esitettyjen johtopäätösten mukaan kyberturvallisuuteen liittyviin asenteisiin vaikuttavat esimerkiksi aiemmat työkokemukset sekä nykyiset työtehtävät, jolloin organisaatiossa kyberturvallisuuteen liittyvät asenteet voivat vaihdella pelkästään jo eri ammattiryhmien välillä ja siten myös organisaation yksiköiden välillä. Yleisesti ottaen turvallisuuteen liittyvien arvojen koetaan olevan hyvät, mutta tunnistetaan organisaatiossa silti olevan henkilöitä tai ryhmiä, joiden asenne turvallisuutta kohtaan voi olla negatiivinen. Asenteisiin vaikuttaa esimerkiksi muutosvastaisuus, jolla viitataan organisaatiossa ajan saatossa muuttuneisiin turvallisuuskäytäntöihin. Esimerkiksi joidenkin

vanhempien työntekijöiden koetaan toimivan vanhojen toimintatapojen ja asenteiden mukaisesti. Eri ryhmien toimintatavat korostuvat organisaation siiloutuneisuuden vuoksi. Siiloutumisella viitataan siihen, että sisäisten ryhmien yhteistyö vähenee ja ne pyrkivät toimimaan enemmissä määrin erillisinä itsenäisinä ryhminä. Siiloutumisen koetaan olevan kaupunkiorganisaatiolle perinteinen ongelma ja se hankaloittaa organisaation päivittäistä toimintaa. Siiloutuneessa organisaatiossa voi muodostua kyberturvallisuuskulttuurin kuplia, joissa yleisiä toimintatapoja voi olla vaikeampi ylläpitää ja kehittää, koska ryhmäkohtaiset arvot ja asenteet voivat erota toisistaan.

Turvallisuuteen liittyviin asenteisiin koetaan vaikuttavan myös suhtautuminen turvallisuuden parissa työskenteleviin tahoihin. Turvallisuuden parissa työskentelevät henkilöt saattavat kokea, että heidät nähdä pelottavina tai uhkaavina, joka puolestaan vaikuttaa negatiivisesti siihen, kuinka turvallisuuteen asennoidutaan. Samalla painotetaan kuitenkin sitä, että kyseessä on iso organisaatio, johon mahtuu paljon erilaisia asenteita, eikä edellä mainittua voida yleistää organisaation kontekstissa.

Organisaation toiminnan kulmakivinä nousi esille julkisen hallinnon erityispiirteitä, kuten että toimintaa ohjaa laajamittainen sääntely ja toiminnan tulee perustua lakiin. Toimintaa säätelevät lait sekä lain määrittelemät, mutta organisaation itsensä tarkentamat ohjeistukset, kuten hallintosääntö. Näiden asioiden koetaan tuovan organisaation elämään kankeutta, mutta niiden merkitys esimerkiksi lainmukaisuuden ja hyvän hallinnon noudattamisen osalta ymmärretään. Organisaatiossa työskentelevät henkilöt ovat tottuneet pitkiin päätöksentekoprosesseihin, joihin viitataan esimerkiksi “hyväksyntämyllynä”. Niiden nähdään olevan osaltaan turhan byrokraattisia, hitaita ja vanhanaikaisia. Organisaatiossa toiminnan kankeus vaikuttaa myös kyberturvallisuuskulttuuriin, sillä tavat ja toimintamallit vaikuttavat väistämättä myös siihen, kuinka kyberavaruuden kanssa ollaan vuorovaikutuksessa. Toimintamallien nähtiin hidastavan muun muassa kyberturvallisuutta edistävää työtä, jolla puolestaan on vaikutus kyberturvallisuuskulttuurin kehittymiseen. Päätöksentekoprosessien ymmärretään olevan tarpeellisia julkisen sektorin organisaatiossa, mutta niihin suhtaudutaan silti turhautuneesti ja niiden osalta toivottiin muutosta.

Organisaatiokulttuurista esitetään eroavaisia näkemyksiä. Organisaatiokulttuuria kuvataan hallintolähtöiseksi ja byrokraattiseksi, jolla viitataan siihen, että arvoja, työskentelyn tapoja ja tehtäviä asioita määrittää vahvasti julkishallinnollisena organisaationa hyvä hallinto,

raskas päätöksentekoprosessi, julkishallinnolliset arvot ja lainsäädäntö. Organisaatiokulttuuria kuvataan toisaalta myös melko avoimeksi ja itseohjautuvaksi, asiantuntijuuteen pohjautuvaksi kulttuuriksi. Haastateltujen välillä on eroja siinä, millaiseksi he kokevat oman yksikkönsä toiminnan ja kulttuurin. Lisäksi molempia piirteitä, hallintolähtöistä byrokraattisuutta ja itseohjautuvuutta, saatetaan tunnistaa yhdessä. Enemmän avointa ja itseohjautuvaa toimintaa kokevat, että kyberturvallisuutta tuodaan esiin organisaatiossa tarpeeksi. Tähän liittyy näkemys, jonka mukaan henkilöllä, varsinkin asiantuntijatasolla työskentelevänä, on velvollisuus itse seurata viestintää ja kehittää omaa osaamistaan tarpeen vaatiessa. Aiheeseen liittyvän tiedon nähdään olevan saatavissa ja vapaasti hyödynnettävissä. Toisaalta taas haastatteluissa yleisen näkemyksen mukaan kyberturvallisuuteen liittyvien asioiden koettiin näkyvän organisaation arjessa liian vähän, ajoittaisina ilmoituksina ja sähköpostiviesteinä. Haastatellut kokevat, että on organisaation edun mukaista tuoda kyberturvallisuutta enemmän esiin. Organisaation koettiin suhtautuvan kyberturvallisuuteen henkilön osaamista ja tietotaitoa kunnioittaen, antaen yksilölle enemmän vastuuta. Toisaalta taas nähtiin, että henkilöstön kyberturvallisuuden osaamistaso on vajavaista, varsinkin organisaation kokoon nähden, joka viittaa siihen, että toimenpiteitä ja organisaation henkilöstöön kohdistunutta turvallisuustyötä pidetään riittämättömänä. Erilaiset näkemykset siitä, kuinka organisaation tulisi edistää kyberturvallisuutta voivat aiheuttaa kitkaa organisaation sisällä ja vaikuttaa kyberturvallisuuteen liittyviin asenteisiin ja siten myös käyttäytymiseen.

Tutkielman tulosten mukaan organisaation työntekijät ymmärtävät hallintolähtöisen kulttuurin merkityksen ja kokevat organisaation toimintaa määrittävän strategian selkeäksi ja yhteiseksi päämääräksi. Lisäksi organisaatiossa työskentelevillä tunnistetaan voivan olla yhteisen hyvän ja pehmeämpien arvojen kautta muodostuva arvomaailma. Voidaankin olettaa että työntekijöiden arvot ovat ainakin jossain määrin samankaltaisia organisaation arvojen kanssa. Samankaltaiset arvot vahvistavat organisaation ja henkilöstön suhdetta. Scheinin (2004) mukaan arvoilla tulisi olla selkeä suhde organisaation johtamistapoihin, jotta ne edesauttavat organisaation toimintaa. Harisaloa (2008) mukaillen, jostain asiasta tulee laajasti hyväksyttyä ja luonnollista ja kiistatonta, jos se on yleisesti omaksuttua. Tutkielman tulosten perusteella voidaan nähdä, että hallintolähtöistä kulttuuria pidetään organisaatiolle ominaisena perusrakenteena ja itseohjautuvuutta, avoimuutta ja verkostomaisuutta pidetään arvoina ja tavoitteina, jotka pyrkivät ohjaamaan organisaation tai siellä olevien yksiköiden toimintaa.

Tutkielman tulosten mukaan organisaation kyberturvallisuuskulttuurin kehittämiseen vaikuttaa organisaation julkishallinnollinen toimintaympäristö ja luonne. Organisaatiolta koetaan puuttuvan halu tai välineet, tai kummatkin organisaation kyberturvallisuuden kehittämiseksi. Organisaation tietoturvaa koordinoivan tahon toiminnan sen koetaan olevan vaikeutunutta ja hidastunutta johto-oikeuden puutteen vuoksi. Tämän vuoksi koetaan, että sen toiminnan vaikutus ei ole halutulla tasolla. Organisaation tietoturvakoulutusta ja sen toteuttamista pidetään heikkotasoisena. Tutkielman tuloksissa kuvaillaan, kuinka organisaatio jollain tavoin ei halua tai pysty vaatimaan tietoturvakoulutuksen suorittamista. Lainsäädännön nähdään lisäävän ja myös toivottiin lisäävän vaatimuksia tietoturvallisuuden osalta ja siten myös parantavan tilannetta. Tietoturvakoulutuksilla voi olla myönteinen vaikutus organisaation kyberturvallisuuskulttuuriin (Da Veiga & Martins, 2015). Kyberturvallisuuden kehittämiseen suunnatuista resursseista on pulaa. Resurssien osalta merkittäväksi tekijäksi tunnistettiin kuntatalouden kireys ja resurssien suuntaaminen muualle, kuin turvallisuustyöhön. Tulos tukee myös DVVn (2021) digitaalisen turvallisuuden nykytilan raporttia, jonka mukaan kuntien digitaalisen turvallisuuden kehittämisen resursseissa on tunnistettu vajetta.

6.2 Tutkielman kontribuutio ja luotettavuuden arviointi

Tämä tutkielma auttaa osaltaan ymmärtämään millaiset tekijät ja käsitykset vaikuttavat kyberturvallisuuskulttuurin olemukseen sekä millaisena ilmiönä se näkyy julkisessa organisaatiossa. Kyberturvallisuuskulttuurin parempi ymmärrys voi auttaa julkisia organisaatioita kehittämään kyberturvallisuuskulttuuria ja toisaalta kitkemään sitä horjuttavia tekijöitä. Aikaisempi tutkimus korostaa inhimillisten tekijöiden merkitystä tietoturvauhkien synnyssä (esim. Parson ym., 2015; Grobler, Gaire & Nepal 2021). Ymmärrys yksilöiden ja organisaatiotasolla työntekijöiden tietoturvakäyttäytymisestä voi auttaa ehkäisemään kyberuhkia (Gonzalez & Sawicka, 2021; Krombholz ym., 2014), jota tämä tutkielma edistää.

Kyberturvallisuuskulttuuri näkyy sekä henkilökohtaisella että laajemmin organisaatiotasolla. Se sitoutuukin henkikohtaisen kulttuurin lisäksi organisaatiokulttuuriin esimerkiksi organisaation siiloutumisen kautta. Kyberturvallisuudelle annettavat

merkitykset ja asenteet ovat moninaisia ja riippuvat henkilökohtaisesta taustasta, nykyisestä työstä ja jopa maailmanpoliittisesta tilanteesta. Tässä tutkielmassa organisaation kyberturvallisuuskulttuuria tutkittiin narratiivisella tutkimusotteella. Narratiivista tutkimusta ei ole tutkijan tiedon mukaan aikaisemmin hyödynnetty kyberturvallisuuskulttuurin tutkimuksessa. Tutkielma tuo esiin narratiivisen tutkimuksen hyödyntämistä organisaation kyberturvallisuuskulttuurin tutkimuksessa. Narratiivinen tutkimus mahdollistaa kyberturvallisuuskulttuurille annattavien subjektiivisten merkitysten syvemmän ymmärtämisen ja siten paremman ymmärryksen kyberturvallisuuskulttuurista.

Julkisen organisaation siiloutuminen voi vaikuttaa organisaation sisäisten ryhmien välisiin näkemyseroihin kyberturvallisuudesta. Vaikka tutkimustulokset eivät ole suoraan yleistettävissä muihin organisaatioihin, toimii tutkimusasetelma ja narratiivinen tutkimusote esimerkkinä kyberturvallisuuskulttuurin tarkastelemisesta muissa julkisen sektorin organisaatioissa.

Laadullisella tutkimuksella ei lähtökohtaisesti haeta yleistävyyttä, vaan sillä pyritään esimerkiksi kuvaamaan käsiteltävää ilmiötä, ymmärtämään jotain toimintaa syvällisesti tai teorian tuella luomaan tulkintaa käsiteltävästä ilmiöstä (Tuomi & Sarajärvi, 2018). Lincoln & Guban (1985) mukaan kvantitatiivisen tutkimusparadigman mukaisen tiedon luonne on erilainen kuin naturalistisen (kvalitatiivisen) paradigman mukaisen tiedon. Heidän mukaansa kvantitatiivisessa tutkimuksessa yleisesti käytetyt luotettavuuden käsitteet validiteetti ja reliabiliteetti perustuvat kvantitatiivisen paradigman käsitykseen yhdistä konkreettisesta todellisuudesta. Heidän mukaansa todellisuudesta on kuitenkin olemassa erilaisia konstruktioita, eivätkä toiselle paradigmalle kehitetyt luotettavuuden käsitteet sovi toiselle. (Lincoln & Guba, 1985; Tuomi & Sarajärvi, 2018.) Tuomen & Sarajärven (2018) mukaan luotettavuuden arviointiin laadullisessa tutkimuksessa ei ole olemassa selkeitä ohjeita. Tämän tutkielman luotettavuutta arvioidaan käyttäen hyväksi Tuomen & Sarajärven (2018, 171) luotettavuuden arvioinnin listaa ja narratiivisen tutkimuksen lähteitä (Kohler-Riesmann, 2008; Heikkinen, 2018). Tutkielman luotettavuutta arvioitiin tutkijan sitoutumisen, aineiston keruun, analyysin, tulkinnan, tutkimuksen tiedonantajien ja siirrettävyyden kautta.

Laadullisen tutkimusotteen vuoksi tämän tutkielman tuloksiin ovat vaikuttaneet tutkijan subjektiivinen käsitys tutkittavasta ilmiöstä, sillä tutkija on päättänyt tutkimusasetelmasta

oman ymmärryksensä varassa (Tuomi & Sarajärvi, 2018). Tulkintojen tekeminen on olennainen osa laadullista tutkimusta. Tutkijan tekemät tulkinnat korostuivat narratiivien muodostamisessa, tulosten kirjoittamisessa ja johtopäätösten tekemisessä, jolloin niihin ovat vaikuttaneet tutkijan omat ennakko-oletukset ja -käsitykset. Tutkielmassa on kuitenkin pyritty avaamaan mahdollisimman tarkasti tutkimuksen toteuttamisen eri vaiheet ja niihin vaikuttaneet tekijät, jotta tutkimuksen luotettavuus paranisi. Tutkielman luotettavuutta ja läpinäkyvyyttä pyrittiin lisäämään myös lisäämällä tutkielman liitteisiin haastattelukysymykset sekä lisäämällä tulososioon suoria, mutta yleiskieliseksi muunnettuja lainauksia haastateltavien puheesta. Lisäksi analyysia pyrittiin kuvailemaan tarkasti, huomioiden myös tutkijan ennakko-olettamuksia.

Tutkimusaineisto koostuu kahdeksasta teemahaastattelusta, jotka on toteutettu samassa kaupunkiorganisaatiossa. Tutkielman aineiston koosta ja hankkimistavasta johtuen on syytä pohtia, sitä voidaanko sen perusteella tutkielman kohteena olevaa ilmiötä kuvata syvällisesti. Tutkimusaineiston pienuus mahdollisti tarkan syventymisen kunkin haastattelun sisältöön, jolloin niistä oli mahdollista tehdä yksityiskohtaisia havaintoja. Tämä on oleellista myös tutkimuksessa käsitellyn ilmiön, kulttuurin, tutkimisen puolesta.

Tutkimuksen toteuttamisvaiheessa heräsi epäilys, että avoimen satunnaisen otannan vuoksi tutkielmaan osallistujat olivat jollain tavoin kiinnostuneita kyberturvallisuudesta, minkä vuoksi he olivat valmiimpia osallistumaan tutkimukseen, kuin he, joita aihepiiri ei puhutellut. Aihepiiristä keskustelu saatettiin myös kokea vaikeiden käsitteiden kautta haastavaksi, vaikka tämä otettiin huomioon haastatteluja suunnitellessa. Huomioita tukee myös johtopäätöksissä esiin tuotu näkemys, jonka mukaan haastatellut uskoivat asioista ajateltavan toisin heidän työlähipiirinsä ulkopuolella. Samalla tämä näkemys kuitenkin kuvaa näkemyksiä muualla organisaatiossa, eikä ole syytä olettaa heidän olevan epärehellisiä tai pitää arvioita epäluotettavina. Tutkielmaan osallistujien joukossa oli myös henkilöitä eri puolilta organisaatiota ja tutkielman aineisto toi esiin kattavasti erilaisia näkemyksiä eri puolilta organisaatiota, joka tukee näkemystä, että tutkielmassa ilmiötä onnistuttiin ymmärtämään kokonaisvaltaisesti kohdeorganisaatiossa.

Edellä mainittu kytkeytyy osittain siis myös Heikkisen (2018) ja Kohler-Riesmanin (2008) huomioihin narratiivisen tutkimuksen luotettavuudesta. Tutkimusaineistona toimivista haastatteluista muodostettiin narratiivisia tyyppitarinoita. Narratiivista tutkimusta tehdessä

ei voi olla ohittamatta ajatusta siitä, kuinka narratiivisuus vaikuttaa tutkimuksen luotettavuuteen ja kuinka luotettavia kerrotut tarinat olivat. Heikkisen (2018, 205) mukaan keskeisin narratiivisen tutkimuksen ongelma on kysymys sen luotettavuudesta. Luotettavuutta on perinteisesti tutkittu realistisen maailmankuvan kautta käsitteillä validiteetti ja reliabiliteetti. Termit merkitsevät sitä, kuinka hyvin mittari mittaa sitä, mitä sen on tarkoitus mitata, sekä että tuloksiin eivät vaikuta satunnaiset tekijät, kuten mittaaja itse. Mittaus on luotettavaa, mikäli se voidaan toistaa samoin tuloksin toisten mittaajien avulla. Toisin sanoen, tutkija erillisenä tietävänä objektina esittää jonkin väittämän ulkoisesta objektista. Käsitteet eivät kuitenkaan sovi tulkinnalliseen ja konstruktiiviseen tutkimukseen, kuten myös Lincoln & Guba (1985) näkevät. Monen muun laadullisen tutkimusmenetelmän tapaan narratiivinen tutkimus ei muodosta toistettavaa tietoa, eikä tutkijaa ei voi erottaa erilliseksi olennoksi todellisuudesta. Tieto ja todellisuus voidaan nähdä olevan tutkijan rakentamia ja olevan tutkijan tulkintaa. Jotta tutkija voisi ymmärtää tutkimuskohdettaan, tulisi hänen tulkintansa syntyä vuorovaikutuksessa tutkimuskohteen kanssa. (Heikkinen, 2018.) Lisäksi on huomioitava, että kukin lukija voi tulkita valitsemiani aineistositaatteja omalla tavallaan. Tämän vuoksi tulkintoja voi olla yhtä monia kuin lukijoita.

Kysymys luotettavuudesta voi koskea myös tarinoita itsessään. Kerronta todellistaa kokemuksia ja tarjoaa yksilöille tapoja ymmärtää menneisyyttä (Kohler-Riessman, 2008, 11). Haastattelut ovatkin kertomuksia menneisyydestä – toisin sanoen yksilön tulkintaa omasta menneisyydestä. Tässä mielessä tarinoiden luotettavuutta voidaan myös kyseenalaistaa – mistä tiedän että haastateltava puhuu totta? Mahdollista on myös, että haastateltava on kokenut jonkin aihepiirin araksi ja on epäröinyt totuuden kertomisessa ja jättänyt haastattelusta pois joitain oleellisia yksityiskohtia. Puhui haastateltava totta tai ei, narratiivista aineistoa analysoidessa ei ole oleellista tietää, ovatko kerrotut asiat oikeasti tapahtuneet haastatellulle. Sen sijaan keskeistä on se, mikä näiden tapahtumien merkitys oli kertojalle. (Polkinghorne, 2007, 471–486.)

Tutkielman kohteena oli yksittäinen organisaatio, ja siinä tutkittiin organisaation ja sen henkilöiden maailmassa olevaa ilmiötä. Tutkielman tuloksissa nousi kuitenkin esiin tekijöitä, jotka voivat olla yhteneväisiä muissa samankaltaisissa organisaatioissa. Vaikka tutkielma keskittyy yhden kaupunkiorganisaation kontekstiin, voi tuloksien hyödyntämistä

toisiin kuntiin harkita tapauskohtaisesti, mikäli kunnista tunnistetaan yhdistäviä tuloksiin vaikuttaneita tekijöitä.

Aiemmissa tutkimuksissa on osoitettu, että joillain demografisilla tekijöillä, kuten iällä tai sukupuolella voi olla vaikutusta tietoturvakäyttäytymiseen. Tässä tutkielmassa ei kuitenkaan pienen otannan vuoksi voitu eritellä demografisten tekijöiden vaikutusta kyberturvallisuuskulttuuriin.

6.3 Jatkotutkimusehdotukset

Tässä tutkielmassa tutkittiin kyberturvallisuuskulttuurin rakentumista erään kaupungin hallinto-organisaatiossa. Tutkielman toteutus ja tutkijan tekemät rajaukset toivat esiin uusia mielenkiintoisia jatkotutkimusehdotuksia.

Tässä tutkielmassa haastateltaviksi valikoitui satunnaisen otannan ja suorien yhteydenottojen kautta todennäköisesti vain kyberturvallisuudesta kiinnostuneita henkilöitä. Tästä syystä jatkotutkimusehdotuksena esitetään satunnaista otantaa suunnattuna joihinkin etukäteen tarkasti määriteltyihin ryhmiin. Toisaalta haastateltavien kohdejoukko voitaisiin jatkotutkimuksissa rajata tarkasti kahteen eri joukkoon, joiden kautta voitaisiin verrata kulttuurin eroja eri ryhmien välillä. Mahdollisia ryhmiä voisivat olla esimerkiksi tietohallinnon edustajat ja yksikkö, jonka työtehtäviin turvallisuus ei suoranaisesti kuulu.

Aiemmassa tutkimuksessa nostettiin esiin demografisten tekijöiden, asenteiden ja tietoisuuden merkitys kyberturvallisuuskulttuurille (Bulgurcu ym., 2010; Farooq ym., 2015; Da Veiga, 2016). Tästä syystä tutkimusaineiston rajaus koskemaan esimerkiksi tietyn opintotaustan tai työhistorian omaavia henkilöitä toisi mahdollisuuden tutkia kyseisiin ryhmään kuuluvien ihmisten muodostaman kulttuurin ominaispiirteitä. Toisaalta tutkimus voitaisiin rajata myös jonkin organisaatioin tiettyyn yksikköön, jolloin tutkimuksessa päästäisiin paneutumaan tietyn yksikön kyberturvallisuuskulttuuriin yksityiskohtaisemmin.

Tutkimusaineiston kerääminen suuremmalta joukolta haastateltavia useammasta organisaatiosta voisi mahdollistaa paneutumisen eri tilanteissa näkyviksi tuleviin

kulttuurieroihin sekä ihmisten kokemuksiin niistä. Tutkimuksen tulokset olisivat myös paremmin yleistettävissä, jos aineiston keruuta ei olisi rajattu yhteen organisaatioon. Tällöin voitaisiin nähdä eroja myös julkisten ja yksityisten organisaatioiden kyberturvallisuuskulttuurien eroissa. Tällöin tutkimuksen toteuttaminen kvantitatiivisena eli määrällisenä tutkimuksen voi olla hyvä ratkaisu laajemman tutkimusjoukon tavoittamiseksi.

7 LÄHDELUETTELO

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology,* 33(3), 237–248.

Ali-Yrkkö, Mattila, Mäkäräinen, Pajarinen, Seppälä, & Tervo, (2020). *Digibarometri 2020: Kyberturvan tilannekuva Suomessa.* Helsinki: Taloustieto Oy.

Anderson, C. L., Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. Management Information Systems: Mis Quarterly, 34(3), 613-643.

Anttiroiko, A.-V., Haveri, A., Karhu, V., Ryynänen, A., & Siitonen, P. (2007). Kuntien toiminta, johtaminen ja hallintasuhteet (3. uud. p.). *Tampere University Press.* http://urn.fi/urn:isbn:978-951-44-8768-2.

Barthes, R. (1966). Introduction to the structural analysis of the narrative.

Benjamin, S. (2014). Kulttuuri-identiteetti–Merkitys kehitykselle ja kotoutumiselle. Teoksessa Laine, Marja (toim.) *Kulttuuri-identiteetti & kasvatus: Kulttuuriperintökasvatus kotoutumisen tukena.* Tallinna: K-Print, 56-105.

Boss. (2007). Control, perceived risk and information security precautions: External and internal motivations for security behavior. *ProQuest Dissertations Publishing.*

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34(3), 523–548.

Brown, A. D., & Humphreys, M. (2003). Epic and tragic tales Making sense of change. *The Journal of Applied Behavioral Science*, 39(2), 121-144.

Bruner, J. (1986). Actual Minds, Possible Words. Harvard University Press, Cambridge.

Chen, Ramamurthy, K. (Ram), & Wen, K.-W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *The Journal of Computer Information Systems*, 55(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767.

Cortazzi, M. (2001). Narrative analysis in ethnography. *Handbook of ethnography,* 384, 394.

Currie, G., & Brown, A. D. (2003). A narratological approach to understanding processes of organizing in a UK hospital. Human Relations, 56(5), 563-586.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security,* 32 (1), 90–101.

Czarniawska, B. (2004). Narratives in social science research. Sage.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713.

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72–94. https://doi.org/10.1016/j.cose.2017.05.002.

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *2016 SAI Computing Conference* (SAI), 1006–1015.

Da Veiga, A. & Eloff, J. H. P. (2010). A framework and assessment instrument for Information Security Culture. *Computer Security*, vol. 2010, no. 29, pp. 196-207.

D'Arcy, J. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security* 22 (5), 474–489.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research,* 20(1), 79-98.

Dhillon, G., Samonas, S., & Etudo, U. (2016). Developing a human activity model for insider IS security breaches using action design research. In *IFIP International Conference on ICT Systems Security and Privacy Protection* (pp. 49-61). Springer.

Digi- ja Väestötietovirasto. (2021a). Julkisen hallinnon digitaalisen turvallisuuden nykytilan selvitys. Haettu 1.7.2022 osoitteesta https://dvv.fi/documents/16079645/17634906/Raportti+-+Julkisen+hallinnon+digitaalisen+turvallisuuden+nykytilan+selvitys.pdf/595ba46a-1a15-6089-92c1a019c5e47475/Raportti++Julkisen+hallinnon+digitaalisen+turvallisuuden+nykytilan+selvitys.pdf?t=1616745361082.

Digi- ja Väestötietovirasto. (2021b). Kuntien digitaalisen turvallisuuden selvitys. Haettu 1.7.2022 osoitteesta https://dvv.fi/documents/16079645/17634906/Raportti+-+Kuntien+digitaalisen+turvallisuuden+selvitys.pdf/ede8c7c4-9509-8977-92c8-9127a0fd091e/Raportti+-+Kuntien+digitaalisen+turvallisuuden+selvitys.pdf?t=1616745436358.

Dinev, T., Goo J., Hu Q., & Nam., K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal.* 2009, 19(4), 391—412.

European Network and Information Security Agency. (2015). Definition of cybersecurity: Gaps and overlaps in standardisation. Publications Office. Haettu 1.6.2022 osoitteesta https://data.europa.eu/doi/10.2824/4069.

European Union Agency for Network and Information Security. (2017). Cyber security culture in organisations. Publications Office. Haettu 1.6.2022 osoitteesta https://data.europa.eu/doi/10.2824/10543.

Eriksson, & Kovalainen, A. (2008). *Qualitative methods in business research.* SAGE.

Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. 4. Painos. Vastapaino.

Everitt, A. (1999). The governance of culture: approaches to integrated cultural planning and policies. Policy Note No. 5, September 1999. Council of Europe.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. *2015 IEEE Trustcom/BigDataSE/ISPA*, 352–359. https://doi.org/10.1109/Trustcom.2015.394.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001.

Galvez, S. M., Shackman, J. D., Guzman, I. R., & Ho, S. M. (2015). Factors affecting individual information security practices. *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* (pp. 135-144).

Glaspie, H. W., & Karwowski, W. (2017). Human factors in information security culture: A literature review. *International Conference on Applied Human Factors and Ergonomics* (pp. 269-280). Springer, Cham.

Gonzalez, J., & Sawicka, A. (2021). A framework for human factors in information security. 2002.

Greene, G. & D'Arcy J. (2010). Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance. *5th Annual Symposium on Information Assurance* (ASIA-2010).

Grobler, Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, 4, 583723–583723. https://doi.org/10.3389/fdata.2021.583723.

Guldenmund, F. (2000). The nature of safety culture: a review of theory and research. *The Netherlands: Safety Science Group* 34 (2000), 215–257.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, 32, 242-251.

Harisalo, R. (2008). *Organisaatioteoriat.* Tampere University Press.

Hatch, M. J. (1993). The Dynamics of Organizational Culture. *The Academy of Management Review,* 18(4), 657. https://doi.org/10.2307/258594.

Hatch, M. J. (1997). Organization theory: Modern, symbolic and postmodern perspectives. Oxford UP.

Hardy, B. (1977). Narrative as a primary act of mind. Teoksessa M. Meek, A. Warlow & G. Barton (toim.) The cool web: The patterns of children's reading. London: The Bodley Head, 12–23.

Haveri, A., Karhu, V., Ryynänen, A., Siitonen, P., & Anttiroiko, A.-V. (2007). *Kuntien toiminta, johtaminen ja hallintasuhteet (3. uud. p.).* Tampere University Press. http://urn.fi/urn:isbn:978-951-44-8768-2.

Haveri, A., & Rönkkö, P. (2007). Kuntaorganisaatio ja sen johtaminen. Teoksessa A.-V. Anttiroiko, A. Haveri, V. Karhu, A. Ryynänen, & P. Siitonen (Toim.), *Kuntien toiminta, johtaminen ja hallintasuhteet* (3. uud. p.). Tampere University Press. http://urn.fi/urn:isbn:978-951-44-8768-2.

Heikkinen, H. (2018). Kerronnallinen tutkimus. Teoksessa R. Valli (Toim.), Ikkunoita tutkimusmetodeihin 2: Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. 5. p., 170–187. PS-kustannus.

Herath, T. & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems.* 47(2). 154–165.

Hiltunen, Tarja. (2021). Turun opetuksen verkkopalveluihin kohdistettu tietomurto pystyttiin estämään – varotoimenpiteenä tulee vaihtaa salasana. Haettu 21.8.2022 osoitteesta https://yle.fi/uutiset/3-11883275.

Hirsjärvi, S., & Hurme, H. (2018). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. *Gaudeamus Helsinki University Press.* https://doi.org/10.1109/SAI.2016.7556102.

Hirsjärvi, S., Remes, P., Sajavaara, P. & Sinivuori, E. (2009). *Tutki ja kirjoita* (15. uud. p.). Tammi.

Hofstede, G. H., Hofstede, G. J., & Minkov, M. (2010). Cultures and organizations: Software of the mind: intercultural cooperation and its importance for survival (3rd ed). McGraw-Hill.

Huhtala, H., & Laakso, A. (2007). Kirjallisuuskatsaus organisaatiokulttuuriteorioihin: mitä ne ovat ja miten niistä on keskusteltu kansainvälisissä ja suomalaisissa tieteellisissä journaaleissa?. *Hallinnon tutkimus,* 26(2).

Huigang, L. & X. Yajiong (2010). Understanding security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information Systems.* 11(7). 394–413.

Hyvärinen, M. (2006). Kerronnallinen tutkimus. Haettu 15.5.2022 osoitteessa http://www.hyvarinen.info/material/Hyvarinen-Kerronnallinen_tutkimus.pdf.

Hyvärinen, M., & Löyttyniemi, V. (2005). Kerronnallinen haastattelu. Teoksessa L. Tiittula & J. Ruusuvuori (Toim.), *Haastattelu: Tutkimus, tilanteet ja vuorovaikutus,* 189–222. Vastapaino.

Hänninen, V. (1999). Sisäinen tarina, elämä ja muutos. *Tampere University Press.*

IAEA. (2002). International Atomic Energy Agency. Safety culture in nuclear installations: Guidance for use in the enhancement of safety culture. *Vienna: International Atomic Energy Agency* (IAEA).

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.

Ilvonen, I. (2011). Information Security Culture or Information Safety Culture-What do Words Convey? In European Conference on Cyber Warfare and Security. Academic Conferences International Limited.

ISO/IEC 27032. (2012). Information Technology – Security Techniques – Guidelines for Cybersecurity.

Karahanna, Evaristo, J. R., & Srite, M. (2005). Levels of Culture and Individual Behavior: An Investigative Perspective. *Journal of Global Information Management,* 13(2), 1–20. https://doi.org/10.4018/jgim.2005040101.

Karjalainen, M. (2011). Improving employees' information systems (IS) security behavior. Acta Univ. Oul. A 579, 2011.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security,* 24(3), 246–260. https://doi.org/10.1016/j.cose.2004.08.011.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly executive,* 9(3).

Kearney, P. (2010). Security: The Human Factor. *Cambridgeshire: IT Governance Publishing.*

KL 410/2015. Kuntalaki. Viimeisin muutos 419/2021. Ajantasainen lainsäädäntö. Haettu 6.6.2022 osoitteesta: https://www.finlex.fi/fi/laki/ajantasa/2015/20150410.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

Kuntaliitto. (2020). 9 digiturvaan liittyvää haastetta kuntajohdolta, loppuraportti. Haettu 2.8.2022 osoitteesta https://www.kuntaliitto.fi/sites/default/files/media/file/9%20digiturvaan%20liittyvää%20haastetta%20kuntajohdolta%20-loppuraportti.pdf

Kuortti J., Mäntynen, A., & Pietikäinen, S. (2008). Kielen rakennustelineillä: kielellisen ja yhteiskunnallisen käänteen merkitys. *Media & Viestintä,* 31(3). https://doi.org/10.23983/mv.63021.

Laakso, S. (2009). Julkisen hallinnon oikeudellinen sääntely. Teoksessa Karppi, I., & Sinervo, L. M. (2009). Governance: uuden hallintatavan jäsentyminen. Tampereen yliopisto, Tampere.

Laari, T., Flyktman, J., Härmä, K., Timonen, J. & Tuovinen, J. (2019). *#Kyberpuolustus: Kyberkäsikirja Puolustusvoimien henkilöstölle*. Maanpuolustuskorkeakoulu, Sotataidon laitos.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. In 2013 46th Hawaii International Conference on System Sciences. 2978-2987. IEEE.

Lieblich, A. &, Tuval-Mashiach, R. & Zilber, T. (1998) Narrative Research. Reading, Analysis and Interpretation. *Applied Social Research Methods Series*. Vol. 47. Thousand Oaks, Ca.: Sage.

Liikenne- ja viestintävirasto. (2020). Kyberturvallisuus ja yrityksen hallituksen vastuu -opas. Haettu 6.5.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. sage.

Limnéll, J., Majewski, K. & Salminen, M. (2014). Kyberturvallisuus. Docendo.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6*, *9*(1-2), 3-31.

Mahfuth, A., Yussof, S., Baker, A.A., Ali, N. (2017). A systematic literature review: Information security culture. Proceedings of the 5th International Conference on Research and Innovation in Information Systems - Social Transformation through Data Science, 2017.

Martin, J. (2002). *Organizational Culture: Mapping the Terrain.* SAGE. https://doi.org/10.4135/9781483328478.

Martins, A., & Elofe, J. (2002). Information security culture. In Security in the information society (pp. 203-214). Springer, Boston, MA.

Mattila, Ali-Yrkkö & Seppälä. (2020). Elinkeinoelämän tutkimuslaitos. ”Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät?”.

Mishra, S. & Dhillon, G. (2006). Developing Theoretical Base for Studying Governance: The Case of Information Security.

Myllymäki, R. (Toim.). (2021). Kunnan hallintosääntö. Suomen Kuntaliitto. Haettu 16.6.2022 osoitteesta https://www.kuntaliitto.fi/julkaisut/2021/2072-kunnan-hallintosaanto.

Ng, B.-Y., & Rahim, M. (2005). A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security. 15.

Nyholm, I., Stenvall, J., Airaksinen, J., Pekkola, E., Haveri, A., Ursin, K. a. & Tiihonen, S. (2016). Julkinen hallinto Suomessa. Tietosanoma.

Ojanperä, S. (2019). Kyberhyökkäys on maksanut Lahden kaupungille lähes 690 000 euroa. Yleisradio. https://yle.fi/uutiset/3-10914550.

Osborne, Stephen. (2010). Public governance and public services delivery: a research agenda for the future. Teoksessa Stephen Osborne (toim.) The New Public Governance? Emerging Perspectives on the Theory and Practice of Public Governance. Lontoo: Routledge. 413–428.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences.* IEEE.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security, 42, 165-176.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making,* 9(2), 117-129.

Peters, G. B. & Pierre, J. (1998): Governance without Government? Rethinking Public Administration. Journal of Public Administration Research and Theory 8 (2), s. 223–243.

Pihkala, Esko. (2021). Laaja tietomurto: Satojen Turun työntekijöiden ja kumppaneiden tietoja voinut päätyä rikollisiin käsiin. Haettu 21.8.2022 osoitteesta https://www.ts.fi/uutiset/5255986.

Pirnes, E. (2008). Merkityksellinen kulttuuri ja kulttuuripolitiikka: laaja kulttuurin käsite kulttuuripolitiikan perusteluna (No. 327). Jyväskylän yliopisto.

Pohjalainen, Ilkka. (2021). Lappeenrannan kaupungin työntekijän sähköpostiin kohdistui tietomurto – Kaupunki selvittää onko jotain tietoja päätynyt vääriin käsiin. Haettu 21.8.2022 osoitteesta https://www.esaimaa.fi/paikalliset/4145064.

Polkinghorne, D. (1988). *Narrative Knowing and the Human Sciences.* Albany: State University of New York Press.

Polkinghorne. (2007). Validity Issues in Narrative Research. *Qualitative Inquiry,* 13(4), 471–486. https://doi.org/10.1177/1077800406297670.

Puhakainen, P. (2006). A design theory for information security awareness. University of Oulu.

Puusa, A. (2020). Haastattelutyypit ja niiden metodiset ominaisuudet. Teoksessa A. Puusa & P. Juuti (Toim.), *Laadullisen tutkimuksen näkökulmat ja menetelmät,* 113–130. Gaudeamus.

Puusa, A., & Juuti, P. (Toim.). (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät.* Gaudeamus. Quarterly, 28(3), 339. https://doi.org/10.2307/2392246.

Puusa, A., Hänninen, V., & Mönkkönen, K. (2020). Narratiivinen lähestymistapa organisaatiotutkimuksessa. Teoksessa A. Puusa & P. Juuti (Toim.), *Laadullisen tutkimuksen näkökulmat ja menetelmät.* Gaudeamus.

Reiman, T. & Oedewald, P. (2008). Turvallisuuskriittiset organisaatiot: Onnettomuudet, kulttuuri ja johtaminen. Edita.

Reiman, T. Pietikäinen, E. Oedewald P. (2008). *Turvallisuuskulttuuri.*

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: its influence on end users' information security practice behavior. Computers & Security. 28(8). 816–826.

Rhodes, C., & Brown, A. D. (2005). Narrative, organizations and research. *International journal of management reviews,* 7(3), 167-188.

Riessman, C. K. (2007). Narrative Methods for the Human Sciences. SAGE Publications.

Rokeach, M. (1973). *The nature of human values.* New York: Free Press.

Rönkkö, Pentti. (2007). Kunta osana suomalaista yhteiskuntaa. Teoksessa Anttiroiko Ari-Veikko, Haveri Arto, Karhu Veli, Ryynänen Aimo & Siitonen Pentti (toim.), *Kuntien toiminta, johtaminen ja hallintasuhteet.* Tampereen yliopisto.

Saarenpää, A. (2008). Henkilö- ja persoonallisuusoikeus. Teoksessa Halttunen, R., Kuusikko, K., Tammi-Salminen, E., Mikkola, T., Mäkelä, S., Saarenpää, A. & Tammilehto, T. (2012). Oikeusjärjestys: Osa I (8. täyd. p.). Lapin yliopisto.

Salminen, A. (2004). Julkisen toiminnan johtaminen: Hallintotieteen perusteet. Edita.

Sanastokeskus TSK. (2017). ”Kyberturvallisuus”. Kokonaisturvallisuuden sanasto. Sanastokeskus TSK ry. Haettu osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Schein, E. H. (2004). *Organizational culture and leadership* (3th ed). Jossey-Bass.

Schlienger, T., & Teufel, S. (2002). Information Security Culture. Teoksessa M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Toim.), *Security in the Information Society* (Vsk. 86, ss. 191–201). Springer US. https://doi.org/10.1007/978-0-387-35586-3_15.

Schultz, E. (2005). The human factor in security. *Computers & Security,* 24(6), 425–426. https://doi.org/10.1016/j.cose.2005.07.002.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education,* 52(1), 92-100.

Siponen, M. (2005). An analysis of the traditional IS security approaches: implications for research
and practice. European Journal of Information Systems, 14(3), 303-315.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees’ adherence to information security policies: an empirical study. *IFIP International Information Security Conference*, 133-144. Springer.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management,* 51(2), 217-224.

Smircich, L. (1983). Concepts of Culture and Organizational Analysis. *Administrative Science Quarterly,* 28(3), 339–358. https://doi.org/10.2307/2392246.

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology,* 29(3), 233-244.

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security,* 2006(10), 7–11.

Tietosuojavaltuutetun toimisto. (2022). Tietosuoja. Haettu osoitteesta: https://tietosuoja.fi/tietosuoja

Traficom. (2019). Tietoturvan vuosi 2019 - Kyberturvallisuuskeskuksen vuosikatsaus. Traficomin julkaisuja 5/2020.

Trend Micro. (2022). Navigating New Frontiers: Trend Micro 2021 Annual Cybersecurity Report. Trend Micro Research.

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

Turvallisuuskomitea. (2019). Suomen Kyberturvallisuusstrategia. https://turvallisuuskomitea.fi/suomen- kyberturvallisuusstrategia-2019/.

Tutkimuseettinen neuvottelukunta (TENK). (2013). Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa: Tutkimuseettisen neuvottelukunnan ohje 2012. http://www.tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & security, 29(4), 476–486.

Van Niekerk, J., & Von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. ISSA, 1–10.

Virtanen, P. & Stenvall, J. (2010). Julkinen johtaminen. Tietosanoma.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security,* 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004.

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security,* 23(4), 275–279. https://doi.org/10.1016/j.cose.2004.01.013.

Vroom, C. & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security,* 23(3), 191–198. https://doi.org/10.1016/j.cose.2004.01.012.

Whitman, M. E. & Mattord, H. J. (2017). *Principles of information security*. Cengage learning, Boston, MA.

Wilde, G. J. (1982). The theory of risk homeostasis: implications for safety and health. Risk analysis, 2(4), 209–225.

8 Liitteet

Liite 1: Haastatteluteemat

1. *Henkilön tausta*
2. *Henkilökohtainen kyberturvallisuuskulttuuri (henkilökohtainen suhtautuminen kyberturvallisuuteen)*
3. *Organisaatiokulttuuri (näkemykset organisaatiokulttuurista ja toimintaympäristöstä)*
4. *Organisaation kyberturvallisuuskulttuuri ja koettu kyberturvallisuus (Arvot, asenteet, merkitykset kyberturvallisuutta kohtaan)*