Mikko Kausto, Eetu Koivistoinen

KYBERTURVALLISUUSOSAAMISEN HALLINTA JA JOHTAMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Kausto, Mikko; Koivistoinen, Eetu
Kyberturvallisuusosaamisen hallinta ja johtaminen
Jyväskylä: Jyväskylän yliopisto, 2024, 107 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Marttiin, Pentti; Hämäläinen, Timo

Tämän pro gradu –tutkielman tavoitteena oli perehtyä kyberturvallisuuden kanssa työskentelevien organisaatioiden kyberturvallisuusosaamisen hallintaan ja johtamiseen liittyviin prosesseihin ja käytänteisiin, sekä selvittää, kuinka tiedolla johtamisen ja osaamisen hallinnan käytänteitä hyödynnetään organisaation toiminnan ohjaamisessa nimenomaan kyberturvallisuuden saralla. Tutkimus toteutettiin laadullisena tutkimuksena, jonka teoriapohjana hyödynnettiin kirjallisuuskatsausta. Laadullisen tutkimuksen aineisto kerättiin puolistrukturoitujen yksilöhaastatteluiden myötä. Tutkimuksiin valikoitui 9 eri organisaatiota. Tulokset analysoitiin laadullisen sisällönanalyysin avulla. Tutkimuksen kirjallisuuskatsauksessa kävi ilmi, että kyberturvallisuus ilmiönä on johdettavissa tiedolla johtamisen ja osaamisen hallinnan käytäntein yhtä lailla muiden organisaation ydintoimintojen tapaan. Laadullinen tutkimus osoitti, että organisaatiot tunnistavat kyberturvallisuuden olevan toden totta johdettavissa ja hallittavissa oleva ilmiö, ja siihen liittyviä prosesseja toteutetaan organisaatioissa jo entuudestaan. Kuitenkin huomattavaa oli se, että tutkimuksessa kävi ilmi, etteivät nämä prosessit välttämättä ole vielä kyberturvallisuuden kohdalla samalla tapaa vakioituja tai dokumentoituja, ja kyberturvallisuusosaamisen johtaminen ja hallinta voisi hyötyä vielä järjestelmällisemmästä lähestymistavasta. Teoreettiseen pohjaan verrattuna huomion arvoista oli myös se, kuinka laadullisen tutkimuksen pohjalta voitiin todeta organisaation sisäisten prosessien olevan valittua mallia monimuotoisempia. Myös ulkoisten tekijöiden merkitys tunnistettiin osana organisaation tiedonkeruuta ja osaamisen kehittämistä, mitä tutkimusta tukeva malli ei tunnistanut. Tutkimuksen tulosten perusteella esitimmekin kattavampaa versiota tutkimukseen valitusta teoreettisesta mallista kyberturvallisuusosaamisen johtamiseen ja hallintaan. Tässä kehitetyssä versiossa prosessien välinen vuorovaikutus sekä ulkoisten tekijöiden merkitys on otettu huomioon.

Asiasanat: tiedolla johtaminen, osaamisen hallinta, kyberturvallisuus, kyberturvallisuusosaaminen

ABSTRACT

Kausto, Mikko; Koivisto Nen, Eetu
Management and leadership of cyber security competence
Jyväskylä: University of Jyväskylä, 2024, 107 pp.
Information Systems, Master's Thesis
Supervisor(s): Marttiin, Pentti; Hämäläinen, Timo

The aim of this master's thesis was to familiarize oneself with the processes and practices related to the management of cyber security competence in organizations working with cyber security, and to find out how knowledge management and competence management practices are utilized in guiding the organization's operations specifically in the field of cyber security. The study was carried out as a qualitative study. However, the theoretical basis of the study was built in the form of a literature review. The data for the qualitative study was collected through semi-structured individual interviews. 9 different organizations were selected for the studies. The results were analyzed using qualitative content analysis. The literature review of the study revealed that cyber security as a phenomenon can be managed through knowledge management and competence management practices just like other core functions of an organization. The qualitative study showed that organizations truly recognize cyber security as a manageable phenomenon, and related processes are already being implemented in organizations. However, it should be noted that the study showed that these processes may not yet be standardized or documented in the same way in cybersecurity, and the management of cybersecurity skills could benefit from an even more systematic approach. Compared to the theoretical basis, it was also worth noting how qualitative research made it possible to conclude that the internal processes of the organization are more diverse than modelled in the framework chosen for the study. The importance of external factors was also recognized as part of the organization's data collection and competence development, which the selected model didn't recognise. Based on the results of the study, we presented a more comprehensive version of the chosen theoretical model for the management of cyber security competence. In this developed version, the interaction between processes, as well as the importance of external factors, are taken into account.

Keywords: knowledge management, competence management, cyber security, cyber security competence

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

1.1 Yleistä

Organisaatiot ovat syvällisesti kiinnostuneita siitä, kuinka erilaisten tekniikoiden avulla työvoiman tehokkuutta nostavaa ilmapiiriä voidaan luoda. Tällä pyritään kasvattamaan kilpailukykyä, innovaatioita ja tehokkuutta. Useita tekijöitä on otettava huomioon onnistuneessa toteutuksessa, sisältäen yrityksen rakenteen, strategian, ympäristön, teknologian ja kulttuurin (Houtzagers, 1999). Tieto itsessään on tärkeä kysymys liiketoimintaorganisaatioille, ja tiedon hallintaa on lähestytty useista eri näkökulmista tutkijoiden ja ammattilaisten toimesta (Gao, Li & Clarke, 2008). Myös McAdam ja McCreedy huomasivat jo vuonna 1999 tiedolla johtamisen (eng. Knowledge Management) olevan yhä enemmän ja enemmän mielenkiintoa herättävä aihealue organisaatioiden ja akatemioiden keskuudessa. Mitä tieto sitten oikeastaan on? Sanan tieto merkitys on monitulkinnainen. Se on aiemmin liitetty vahvasti sanojen data, informaatio, älykkyys, taito, kokemus, asiantuntijuus, idea, intuitio tai käsitys kanssa, riippuen kontekstista, jonka yhteydessä sanaa on käytetty (Gao ym., 2008). Samalla Gao ym. (2008) toteavat, että tiedolla johtaminen puolestaan sisältää paljon monimutkaisemman merkityksen kuin termit tieto ja johtaminen itsessään. Useita eri aiheita eri konteksteissa eri näkökulmin käsitellään tiedolla johtamisen käsitteen alla. Näitä aiheita voidaan jakaa lyhyesti kahteen ryhmään; kovaan ja pehmeään. Tämän tutkimuksen kannalta pehmeä ryhmä on olennaisempi. Pehmeällä ryhmällä Gao ym. (2008) tarkoittavat teorioita, metodologiaa, lähestymistapoja ja työkaluja, jotka keskittyvät ihmiseen ja tiedon luomisen mahdollistamiseen. Wiig (1997) esittää artikkelissaan, ettei tiedolla johtamista tai tiedon hallintaa ole osattu ajatella systemaattisesti liiketoimintatarkoituksiin vielä pitkään, vaikka ihminen onkin pitkään osannut toimia tiedon perusteella ja käyttää sitä hyödykseen toiminnassaan. Kaikessa yksinkertaisuudessaan Wiig:n mukaan tiedolla johtamisen tavoitteet ovat 1) saada yritys toimimaan mahdollisimman älykkäästi turvatakseen sen

elinkelpoisuuden ja kokonaisvaltainen menestymisen sekä 2) muuten realisoida omien tietovoimavarojensa korkein arvo (Wiig, 1997).

Hustad ym. (2004) huomaavat, että henkilöstöjohtaminen on muuttunut yksittäisen työntekijän tuottavuuden mittaamisesta kohti strategista henkilöstön hallintaa keskittyen osaamisen kehittämiseen, ihmisen oppimisen johtamiseen, tiedolla johtamiseen ja oppimisorganisaatioihin. Tämä ajatus tukee pro gradu –tutkimuksemme keskeistä ajatusta siitä, kuinka Keski-Suomen alueella kyberturvallisuutta harjoittavat organisaatiot johtavat ja kehittävät toimintaansa näiden näkökulmien puolesta. Tutkimusalueen rajaaminen kyberturvallisuuden kentälle on mielenkiintoinen, sekä ajankohtainen. Aihealueen rajausta edesauttaa myös Jyväskylän ammattikorkeakoulun (Jamk) ja Jyväskylän yliopiston (JYU) yhteinen kyberturvallisuushanke, jonka tarkoituksena on kehittää Keski-Suomen kyberturvallisuusosaamista ja erityisesti sen tunnettavuutta. Hankkeen nimi 'Keski-Suomen kyberturvallisuusosaamisen tunnettavuuden kasvattaminen' (KSKTK) kuvaa hanketta hyvin. Kyberturvallisuuden merkitys on noussut ihmisten sekä yritysten arjessa digitalisaation ja esineiden internetin kehityksen myötä. Tämän kehityksen johdosta yhteiskunnat ovat yhä enemmän tulevaisuudessa riippuvaisia digitaalisesta ympäristöstä, joten on keskeisen tärkeää varmistaa tietoliikenteen, palvelujen sekä tietoverkkojen ja –varantojen turvallisuus (Pelkonen ym., 2016). Kyberturvallisuus on entistä ajankohtaisempi aihe, erityisesti Venäjän hyökkäyssodan alettua keväällä 2022 sekä valtioiden tullessa mukaan kybermaailmaan. Kyberhyökkäysten määrän kasvu Suomessa ja maailmalla nousee vuosi vuodelta, ja hyökkäykset ovat entistä räätälöidympiä ja kohdistetumpia. Suomessa Traficomin Kyberturvallisuuskeskus on nostanut kyberturvallisuuden uhkatasoa alkuvuodesta 2022 (Traficom, 2022).

Suomen kyberturvallisuusstrategiassa määritetään kolme strategista linjausta, jotka ovat kansainvälinen yhteistyö, johtaminen sekä kyberturvallisuuden osaamisen kehittäminen. KSKTK-hanke tukee näitä kaikkia strategisia linjauksia, kun taas tämän gradututkimuksen painopiste on osaamisen kehittämisessä sekä johtamisessa. Suomen kyberturvallisuusstrategiassa todetaan elinkeinoelämän ja tutkimuksen yhteistyön olevan tärkeässä roolissa uuden merkittävän osaamisen luomisessa. Tiedolla johtaminen ja osaamisen hallinta ovat merkittäviä keinoja osaamiskysymykseen sekä Suomen kilpailukyvyn kehittämiseen (Valtiovarainministeriö, 2019). Nämä edellä mainitut keinot eivät ole varsin uusia käsitteitä, ja niistä on olemassa monia teorioita, mutta niiden soveltamisesta kyberturvallisuuden kontekstissa ei ole paljoa tutkittu. Tällä gradututkimuksella lisätään tärkeää ja arvokasta tietoa kyberturvallisuuden tieteenalalle, mutta myös julkishallinnolle ja elinkeinoelämälle.

Tutkimuksen teoriaosuus toteutetaan kirjallisuuskatsauksena. Teoriaosuudessa hyödynnetään myös muuta aineistoa, kuin pelkästään tieteellisiä artikkeleita tutkimuksen luonteen johdosta. Kirjallisuushakuja tehdään muun muassa seuraavista tietokannoista:

- JYKDOK
- Google Scholar

- IEEE Xploreen
- ScienceDirect

Tärkeitä hakutermejä tulevat olemaan esimerkiksi:

- Knowledge management
- Cyber security
- Management of Cyber security
- Competence management
- Strategic knowledge management
- Strategic competence management.

Myös edellä mainittujen sanojen suomenkielisiä vastineita käytetään hakutermeinä:

- Tiedolla johtaminen
- Tietojohtaminen
- Kyberturvallisuus
- Kyberturvallisuuden johtaminen
- Osaamisen hallinta
- Strateginen tiedolla johtaminen
- Strateginen osaamisen hallinta

Tutkimuksen laadullinen osuus toteutetaan haastattelujen muodossa valittujen kohdeorganisaatioiden avainhenkilöitä haastatellen. Haastatteluihin valikoitui seuraavat organisaatiot:

- Jyväskylän Yliopisto
- Airbus
- Decens
- Huld
- Kela
- Keski-Suomenliitto,
- KPMG
- Millog
- Telia

Haastatteluihin osallistui henkilöitä erilaisista henkilörooleista. Yhteistä näillä rooleilla oli se, että jokainen vastasi omassa organisaatiossa kyberturvallisuudesta jollain tasolla. Haastatteluihin osallistui henkilöitä seuraavista rooleista:

- Tietoturvapäällikkö
- Tietoturvayksikön päällikkö
- Johtaja, Space and Defence
- Kehittämisjohtaja

- Johtaja, teknologiakonsultointi
- Tekninen päällikkö, johtamisjärjestelmät ja kyber
- Pääarkkitehti, verkot ja infrastruktuuri
- Kryptografia-arkkitehti, turvallisuus

1.2 Tutkimuksen tavoitteet ja rajoitteet

Tutkimuksen tavoitteena on kehittää kyberturvallisuusosaamisen hallintaa ja organisaatioiden kyberturvallisuuden johtamista tutkimalla ja analysoimalla heidän nykyisiä käytänteitään ja toimintatapojaan vertaamalla niitä olemassa olevaan teoreettiseen pohjaan. Toisaalta tutkimus myös luo uutta teoriapohjaa ja ymmärrystä siitä, miten olemassa oleva teoria pystyy vastaamaan modernin nopeasti muuttuvan ja kehittyvän maailman tarpeisiin. Tutkielmassa pyritään vastaamaan asetettuihin tutkimuskysymyksiin, jotka ovat:

> *Tunnistetaanko kyberturvallisuusosaamisen olevan hallittavissa ja johdettavissa oleva asia, johon voidaan tiedolla johtamisen ja osaamisen hallinnan menetelmillä vaikuttaa?*
>
> *Miten kyberturvallisuusosaamisen hallintaa ja kehittämistä tulisi toteuttaa organisaatiossa?*

Tutkimuskysymyksiä tarkennetaan seuraavilla alatutkimuskysymyksillä:

> *Mitkä ovat kohdeorganisaatioiden kyberturvallisuusosaamisen hallinnan ja johtamisen strategiat ja prosessit?*
>
> *Mistä tekijöistä kohdeorganisaatioiden osaamisen hallinnan ja johtamisen prosessit koostuvat?*

Tutkimuksen luotettavuuden arvioinnissa on keskitytty sekä validiteetin että reliabiliteetin näkökulmiin. Rajoitteita tuli muun muassa haastateltavien määrässä. Yritimme kasvattaa haastateltavien määrää pitkäjänteisesti, mutta määrä jäi lopulta suunnitellusta tavoitteesta. Lisäksi tutkimukselle muodostui rajoitteita aikataulupaineista ja siitä, että haastateltavat eivät voineet salassapitoasioiden takia kertoa tietyistä asioista niin syvällisesti.

Haasteena tutkimukselle ovat myös käsitteiden kyberturvallisuus, tiedolla johtaminen ja osaamisen hallinnan laajuus sekä käsitteiden useat erilaiset tulkinnat, jotka voivat luoda myös erilaisia näkökulmia ja lähestymistapoja kohdeorganisaatioiden sisällä. Samasta syystä on tärkeää, että tiedonkeruumenetelmänä

käytettävissä haastatteluissa molemmilla osapuolilla, sekä haastattelijalla että haastateltavalla, on yhtenäinen käsitys käytettävien termien merkityksestä. On kuitenkin tärkeä tiedostaa, että täysin yhtenäistä käsitystä haastateltavien välille ei ole mahdollista saavuttaa. Tästä johtuen käsitteiden ja haastattelukysymysten tulkinnassa esiintyy joitakin eroja haastateltavien välillä, mikä voi vaikuttaa tulosten vertailtavuuteen ja tarkkuuteen. Tämä osoittaa tarpeen huolelliselle aineiston analyysille ja tulosten tulkinnalle.

Avoimuus tutkimuksen rajoituksista ja niiden huomioon ottaminen tulosten tulkinnassa ovat tärkeitä tekijöitä tutkimuksen luotettavuuden varmistamisessa. Sillä saavutetaan perusta tuleville tutkimuksille ja se mahdollistaa aiempien tulosten arvioinnin oikeassa kontekstissa. Tarkemmin ja laajemmin tutkimukseen liittyvistä rajoitteista ja haasteista on kerrottu tutkimuksen loppupuolella luvussa kahdeksan.

1.3 Keskeiset käsitteet

Tässä alaluvussa esitellään lyhyesti tutkimuksen kannalta keskeiset käsitteet. Käsitteet esitellään tarkemmin ja monipuolisemmin vielä niille varatuissa omissa luvuissa. Tässä vaiheessa on kuitenkin hyvä hahmottaa minkälaista ilmiötä kukin teorialuku tulee käsittelemään.

1.3.1 Tiedolla johtaminen

Tiedolla johtaminen (eng. Knowledge Management) käsittää erillään olevat mutta keskenään riippuvaiset tiedon luomisen ja ylläpitämisen prosessit, tiedon varastoinnin ja haun, tiedon jakamisen ja tiedon soveltamisen. Minä hetkenä tahansa organisaatio ja sen jäsenet voivat olla mukana useissa tiedolla johtamisen prosessiketjuissa. Täten, tiedolla johtaminen on dynaaminen ja jatkuva organisaationallinen ilmiö (Alavi & Leidner, 2001).

1.3.2 Osaamisen hallinta

Osaamisen hallinnan (eng. Competence Management) tavoitteena on hyödyntää ihmisen taitoa ja tietoa paremmin (Vasconcelos ym., 2016). Laajasti puhuttuna osaamisen hallinta on tapa, jolla organisaatiot hallitsevat yrityksen, ryhmien ja yksilöiden kyvykkyyksiä. Sen päätavoitteena on määrittää ja jatkuvasti ylläpitää kyvykkyyksiä yrityksen tavoitteiden mukaisesti (Berio & Harzallah, 2007). Kyvykkyys puolestaan on tapa laittaa tietoa, taitoa ja asenteita käytäntöön tietyn kontekstin sisällä.

1.3.3 Kyberturvallisuus

Kansallinen turvallisuusjärjestelmä komitea (CNSS) määrittää kyberturvallisuuden (en. Cyber Security) olevan tietokoneiden, elektronisten kommunikaatiojärjestelmien, elektronisten kommunikaatiopalveluiden sekä langallisen ja elektronisen kommunikaation vahingoittumisen estämistä, suojaamista ja restaurointia sisältäen ja varmistaen niiden sisältämän informaation saavutettavuuden, yhtenäisyyden, oikeellisuuden, luotettavuuden ja kiistattomuuden (CNSS, 2022). Lehdon (2022) mukaan kyberturvallisuus on yksinkertaistettuna toimenpiteitä, joilla sekä suojaudutaan että toteutetaan vastatoimenpiteitä kyberhyökkäyksiä vastaan.

1.3.4 Kyberturvallisuusosaaminen

Kyberturvallisuusosaaminen määriteltiin tässä tutkimuksessa kirjallisuuskatsauksen perusteella tiedolla johtamisen, osaamisen hallinnan ja kyberturvallisuuden kirjallisuutta tutkimalla. Kyberturvallisuusosaaminen käsittää kaiken tiedon ja taidon toimia kyberturvallisella tavalla kyberturvallista ympäristöä hyödyntäen.

Lehto (2022) näkee kyberturvallisuuden strategisen johtamisen olevan digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista. Kun taas ajatellaan kyvykkyyksien olevan mitattavissa olevia henkilön piirteitä, joita tarvitaan tietyssä työtilanteessa tietyn työtehtävän suorittamiseen (Klendauer ym., 2012) ja sitä, minkä takia kyvykkyyksien tehokas hallinta on läheisesti yhteydessä erinomaiseen suorituskykyyn, sekä kuinka kyvykkyydet edustavat tietoa, taitoa ja käyttäytymistä, jotka kontribuoivat yrityksen menestykseen (Prahalad & Hamel, 2003), voidaan todeta kyberturvallisuuden olevan sekä yksittäisten ihmisten että organisaatioiden tietoisuutta ja kyvykkyyttä toimia kyberturvallisella tavalla. Täten kyberturvallisuus ja kyberturvallisuusosaaminen linkittyy vahvasti tiedolla johtamisen sekä osaamisen hallinnan prosesseihin, kyberturvallisuuden lähinnä luoden kontekstin johdettaville prosesseille.

1.4 KSKTK-hanke

Tämä tutkimus tehdään Jyväskylän yliopiston ja Jyväskylän ammattikorkeakoulun yhteisen hankkeen ohella sivuten hankkeen tarkoitusta. Keski-Suomen kyberturvallisuusosaamisen tunnettavuuden kasvattamisen (KSKTK) hankkeessa tarkoituksena on kasvattaa kansallista ja kansainvälistä tunnettavuutta. Vastuullisena toteuttajatahona on Jyväskylän ammattikorkeakoulun IT-instituutti ja osatoteuttajana Jyväskylän yliopiston IT-tiedekunta.

Keski-Suomi on erikoistunut kyberturvallisuuden osaamiseen ja on rajallisesti määrin tunnettu kyberturvallisuusosaamisen edelläkävijä niin kansallisesti kuin kansainvälisestikin. Osaamista on erityisesti alueen korkeakouluilla Jyväskylän ammattikorkeakoululla sekä Jyväskylän yliopistolla. Näiden ansioituneiden tutkimus-, kehitys- ja koulutusosaajien lisäksi alueella on kyberturvallisuuteen keskittyneitä toimijoita julkishallinnon ja yritystoiminnan puolelta. Näitä yrityksiä ovat esimerkiksi Puolustusvoimien Johtamisjärjestelmäkeskus, Ilmavoimien Esikunta, KELA, Suomen erillisverkot OY, Elisa, Telia, Airbus Defence and Space, combitech ja KPMG (Jyväskylän Yliopisto & Jyväskylän ammattikorkeakoulu, 2022).

Keski-Suomen alueen erityisosaamista kyberturvallisuuden edelläkävijänä ja osaajana ei vielä tunnisteta valtakunnallisesti riittävän hyvin lukuun ottamatta alan suppeita piirejä. Kompetenssin ja kyberresilienssin kehittäminen on pidetty pimennossa, eikä siitä ole juuri viestitty ulkopuolelle. Erityisesti viimeaikaisten merkittävien muutosten vuoksi kyberturvallisuus on entistä tärkeämmässä roolissa kansakunnan kokonaisturvallisuudessa.

Kyberturvallisuudelle on koko ajan enemmän kysyntää ja sen merkitys kasvaa jatkuvasti, minkä takia erillinen hanke kyberturvallisuuspotentiaalin tunnettavuuden kasvattamiseksi on tarpeen. Hankkeen myötä voimavaroja voidaan tehostaa ja panostaa tunnettavuuden kasvattamiseen, minkä avulla Keski-Suomen alue kykenee menestymään kilpailussa uusien toimijoiden sijoittumisesta alueelle ja toisaalta alueen eri toimijat kilpailussa osaavasta työvoimasta. Tunnettavuuden kasvu mahdollistaa myös lisääntyvän kansallisen, että kansainvälisen investoinnin ja TKI-rahoituksen (Jyväskylän Yliopisto & Jyväskylän ammattikorkeakoulu, 2022).

1.5 Tutkielman rakenne

Rakenteen puolesta tutkielma koostuu johdannosta, teoriaosasta, tutkimusosasta sekä pohdinnasta ja yhteenvedosta. Johdannon tehtävänä on johdattaa lukija tarpeellisen pohjustuksen myötä tutkimuksen asiasisältöön kiinni. Johdanto esittelee tutkimuksen aihealueen ja motivoinnin yleisellä tasolla, avaa tutkimuksen kannalta oleellisia käsitteitä sekä käsittelee tutkimuksen tavoitteet ja mahdolliset rajoitteet. Johdannossa esitellään myös lyhyesti Jyväskylän yliopiston (JYU) ja Jyväskylän Ammattikorkeakoulun (Jamk) yhteinen hanke, Keski-Suomen kyberturvallisuusosaamisen tunnettavuuden kasvattaminen (KSKTK), jonka ohessa ja jonka teemoihin nojaten tämä tutkimus on toteutettu. Johdantoa seuraa teoriaosuus, joka koostuu neljästä teorialuvusta. Jokainen teorialuku käsittelee omaa, tutkimuksen kannalta oleellista käsitettä. Teoria osuus pohjautuu käsitteitä koskettavaan kirjallisuuteen ja tutkimukseen.

Teoriaosuus aloitetaan tiedolla johtamisen osuudella (Luku 2), jossa tarkastellaan tiedon ja tiedolla johtamisen käsitteitä sekä niiden esiintymismuotoja. Luvussa esitetään myös muutamat oleellisimmat teoreettiset viitekehykset niin

tiedolla johtamisen teoriasta kuin tutkimuksen kannalta. Seuraavassa osuudessa määritellään osaamisen hallinnan käsitettä sekä syvennytään aihepiiriin tarkastelemalla osaamisen hallintaa muutamista eri näkökulmista (Luku 3). Tästä siirrytään kyberturvallisuuden määrittelyyn ja sen historiaan sekä kehitykseen. Luvussa ei syvennytä niinkään kyberturvallisuuden teknologioihin vaan tarkastellaan sitä ilmiönä ja enemmänkin hallinnollisen kyberturvallisuuden kannalta. Kyberturvallisuus katsauksen lopussa hahmottelemme kyberturvallisuuden nykytilannetta sekä nykymaailman tarpeita. Kyberturvallisuuden teorialuku (Luku 4) on tutkimuksen kannalta merkittävä, sillä se luo erityisen kontekstin tiedolla johtamiselle ja osaamisen hallinnalle. Tämä seikka todetaan luvussa 5, joka vetää yhteen aiemmat kolme teorialukua, ja luo pohjan koko tutkimuksen teorialle esittämällä, että kyberturvallisuus todella on ilmiö, jota voidaan tiedolla johtamisen ja osaamisen hallinnan käytäntein johtaa.

Tutkimusosa koostuu tutkimusaineiston ja -menetelmän esittelystä (Luku 6), jossa myös kuvataan tutkimuksen teoreettinen viitekehys ja luodaan teorian perusteella pohja laadulliselle tutkimukselle. Tutkimusosan toisessa osiossa omana lukunaan on tutkimustulokset (Luku 7), jossa käsitellään laadullisen tutkimuksen tuloksia.

Lopulta tutkielman lopussa, luvuissa kahdeksan ja yhdeksän, pohditaan tutkimustuloksia, jossa tavoitteena on tunnistaa tutkimustuloksien todellinen merkitys sekä esitellään tutkimuksen pohjalta tehdyt johtopäätökset ja vastataan tutkimuskysymyksiin (Luku 8). Samalla arvioidaan tutkimuksen luotettavuutta ja esitetään mahdolliset jatkotutkimusaiheet. Tutkielman viimeisessä luvussa esitetään tiivis yhteenveto tutkimuksesta (Luku 9).

2 TIEDOLLA JOHTAMINEN

Tiedolla johtamisen konsepti esiteltiin 1990-luvun alussa (Ahmad ym., 2017). Zyngier ja Burstein (2012) ovat määritelleet tiedolla johtamisen perusprosesseiksi tiedon luomisen, tallentamisen, haun, siirtämisen, jakamisen ja soveltamisen organisaation päämäärien ja tavoitteiden saavuttamiseksi. Tieto onkin tietointensiivisten organisaatioiden tärkeä strateginen voimavara, ja se voidaan nähdä tuotteena, minkä avulla organisaatiota voidaan kehittää ja viedä eteenpäin (Almashari, Zairi & Alathari, 2002; Nakash & Bouhnik, 2022).

Ahmad ym. (2017) havaitsivat tutkimuksessaan tiedolla johtamisella olevan merkittävä vaikutus organisaation suorituskykyyn. Organisaatio tulisikin olla varustettuna uusimmilla teknologisilla työkaluilla sekä niiden käyttöön tulisi antaa asianmukaista koulutusta. Tiedolla johtamisen merkittävän strategisen elementin korostaminen näkyy myös muiden tutkijoiden julkaisemissa raporteissa (Nakash, Baruchson-Arbib & Bouhnik, 2021).

Nykypäivän akateemisessa maailmassa ja liike-elämässä tiedolla johtaminen sekä käsitteenä että alana kiinnostaa yhä enemmän. Nykyään organisaatiot elävät lisääntyvän tiedon maailmassa, koska useimmat ihmiset ovat tietotyöntekijöitä ja tieto on ainoa todellinen liiketoiminnan voimavara. Maailmanlaajuiset organisaatiot ovat alkaneet käyttämään tiedolla johtamisen strategioita ja tekniikoita kehittääkseen kilpailukykyään tavoilla, jotka eivät olisi olleet aiemmin mahdollisia (Almashari, Zairi & Alathari, 2002). Tiedolla johtamisesta on tullut merkittävä johtamistrendi, ja sitä pidetään keinona hahmottaa organisaatioiden johtamista uudelleen. Johdon konsultit ovat vahvasti ajaneet eteenpäin tätä kyseistä trendiä (Taylor & Zorn, 2004).

2.1 Mitä tieto on?

Zagzebski (2017) pitää tietoa arvostettuna tilana, jossa ihminen on kognitiivisessa kontaktissa todellisuuden kanssa. Wiigin (1995) mukaan tieto on tietoa,

oivalluksia, ymmärrystä ja käytännön tietotaitoa, jota meillä kaikilla on, ollen perusresurssi, jonka avulla voimme toimia älykkäästi yksilöinä sekä organisaatioina.

Alavi & Leidner (2001) toteavat tiedon olevan laaja ja vaikeatajuinen käsite, joka on määritellyt epistemologista keskustelua länsimaisessa filosofiassa klassisesta kreikkalaisesta aikakaudesta lähtien. Viime vuosien aikana on kuitenkin herännyt eräänlainen kiihkeä kiinnostus tiedon käsittelemiseen merkittävänä organisaation voimavarana. Lisääntynyt kiinnostus organisaation osaamista ja tiedonhallintaa kohtaan kumpuaa siirtymisestä tietotalouteen, jossa tieto on arvonluonnin ja kestävän kilpailuedun päälähde. Organisaation tietämystä ja tiedolla johtamista kohtaan tunnistetun kasvavan kiinnostuksen takia informaatiotutkijat ovat edistäneet tietojärjestelmien luokittelua, jota kutsutaan tiedonhallintajärjestelmiksi (Knowledge management system). Tiedonhallintajärjestelmien tavoitteena on tukea tiedon rakentamista, jakamista ja soveltamista organisaatioissa. Tieto ja tiedonhallinta ovat monimutkaisia ja monitahoisia käsitteitä. Siten, tiedonhallintajärjestelmien tehokas kehittäminen ja käyttöönotto vaatii perustaksi paljon merkityksellistä kirjallisuutta (Alavi & Leidner, 2001).

Davenport & Prusak (1998) puolestaan painottavat, että tieto ei ole dataa eikä informaatiota, vaikka se liittyy molempiin, ja näiden termien erot ovat monesti pieniä. Useimmilla ihmisillä on intuitiivinen käsitys siitä, että tieto on jotain laajempaa, syvempää ja rikkaampaa, kuin data tai informaatio. Ihmiset puhuvat tietävästä yksilöstä ja tarkoittavat sillä jotakuta, jolla on perusteellinen, tietoinen ja luotettava käsitys aiheesta sekä on koulutettu että älykäs. He eivät todennäköisesti puhu muistioista, käsikirjoista tai tietokannoista, vaikka ne olisivatkin asiantuntevien henkilöiden tai ryhmien tuottamia. Tieto on enemmänkin kehystettyjen kokemusten, arvojen, kontekstuaalisen tiedon ja asiantuntijanäkemyksen sulava sekoitus, joka tarjoaa puitteet uusien kokemusten ja tietojen arvioinnille sekä sisällyttämiselle. Se syntyy ja soveltuu tietäjien mielissä. Organisaatioiden osalta se usein uppoutuu dokumenttien tai arkistojen lisäksi myös organisaation rutiineihin, prosesseihin, käytäntöihin ja normeihin (Davenport & Prusak, 1998).

Wiig (1995) huomauttaa tiedon merkityksen vaikuttavan käytännössä katsoen kaikilla päivittäisen ja liiketoiminnan elämän osa-alueilla. Kaksi tietoon liittyvää tekijää onkin olennaisia elinkelpoisuuden ja menestyksen kannalta kaikilla tasoilla. Ensimmäiseksi tekijäksi Wiig on tunnistanut tietovarat, jolla tarkoitetaan arvokasta tietoa, joka on käytettävissä tai hyödynnettävissä. Sitä tulee vaalia, säilyttää ja käyttää mahdollisimman laajasti sekä yksilöiden että organisaatioiden toimesta. Toisena tekijänä on tietoon liittyvät prosessit, joilla tarkoitetaan tiedon luomista, rakentamista, kokoamista, järjestämistä, muuntamista, siirtämistä, yhdistämistä, soveltamista ja suojaamista. Nämä prosessit on hallittava huolellisesti ja selkeästi kaikilla vaikutusalueilla. Toisin sanoen ihmisten ja organisaatioiden tietoa tulisi hallita tehokkaasti, jotta perustavoitteet saavutetaan mahdollisimman pitkälle (Wiig, 1995).

Tieto on ihmisten ja yhteisöjen kykyä jatkuvasti luoda ja uudistua vastatakseen uusiin haasteisiin ja mahdollisuuksiin. Palvelusektorin edistyminen ja

lisääntyvä aineeton työvoiman tarve ovat vaikuttaneet radikaalisti tapaan, jolla tietoa tuotetaan tai luodaan, levitetään ja hyödynnetään (Ahmad ym., 2017).

Erään määritelmän mukaan tieto on olennaista informaatiota, jota voitaisiin kehittää ja siirtää siten, että se olisi helposti oikeiden henkilöiden saatavilla, oikeaan aikaan ja oikeassa paikassa, jotta tulevaisuuden strategisten päätösten tehokkuus säilyy. Tieto on myös dynaaminen ja sujuva virta erikoistuneita kokemuksia, arvoja ja oivalluksia (Ahmad ym., 2017).

Organisaation tieto rakentuu organisaation muodostavien ihmisten kokemuksiin ja heidän oppimiinsa opetuksiin. Nykyisessä tietotaloudessa tämän tiedon tehokas hallinta on merkittävä haaste (Wang & Wang, 2012), sillä ihmiset eivät useinkaan ole tietoisia resursseista, jotka ovat tavallaan piilossa suurten, nykyaikaisten, kansainvälisten organisaatioiden sisällä olevissa sekalaisissa tietovarastoissa (Dzbor ym., 2000).

Wiigin (1995) mukaan tieto on voimavara, joka on organisaation kaikkien muiden osien taustalla. Sen takia sen hallinta vaikuttaa kaikkeen muuhun toimintaan ja kokonaisuuteen. Tämän seurauksena tietotyöntekijöiden on oltava perillä kaikista merkittävistä vaikutuksista ja näkökohdista siihen liittyen (Wiig, 1995).

2.2 Tiedon lajit ja tasot

Ackoff (1989) ja Thierauf (2001) ovat jäsennelleet tietoa eri tasoihin tietotekniikka ja tietojärjestelmäkeskeisessä keskustelussa. Hierarkia on saanut nimekseen DIKW-hierarkia (eng. Knowledge hierarchy) tai viisaushierarkia (eng. Wisdom hierarchy). DIKW-hierarkian (Kuvio 1) alkuperästä tai kehittäjästä ei ole täyttä varmuutta, sillä Sharman (2008) ja Rowleyn (2006) mukaan ensimmäinen maininta hierarkiasta löytyy vuodelta 1934 runoilijan T.S.Eliot toimesta. Ennen Ackoffia hierarkiasta ovat maininneet ainakin Milan Zeleny vuonna 1987, Michael Cooley vuonna 1987, Harlan Cleveland vuonna 1982 ja Adler vuonna 1985 (Frické, 2019). Keskeisimmät pää näkemykset ilmenevät kuitenkin parhaiten perinteisistä Adlerin (1986), Ackoffin (1989) ja Zelenyn (1987) lähteistä.

Frické (2009) arvioi DIKW-hierarkian hyödyllisyyttä sekä älyllistä ja tieteellistä merkitystä. Arviointi keskittyy DIKW-hierarkian näkemyksien ja ilmaisujen paikkansapitävyyteen tutkimalla oletuksia, jotka pohjautuvat kyseiseen hierarkiaan. Frické tunnistaa DIKW-hierarkiassa olevan dilemman. Hän esittää, että hierarkia ei salli induktiivista tai vastaavaa johtopäätöstä eli lausuntoa kuten "Useimmat kalkkarokäärmeet ovat vaarallisia", koska hierarkia hyväksyy vain pyramidin pohjalta tulevat päätelmät, jotka ovat totta. Perustuen siihen, että hierarkian älyllinen tausta on positivismi tai operatiivisuus eli käsitteet, joita ei voi määritellä operaatioilla (instrumentilla karkeasti mitattuna) ovat merkityksettömiä. Tämän takia hierarkiassa käsiteltävä data ja tieto tulisi olla vain totta, mikä on ristiriidassa induktiivisen päättelyn keskeisen ominaisuuden kanssa eli se voi sallia johtopäätökset todellisista premissioista vääriin johtopäätöksiin. Näin

Frické perustelee DIKW-hierarkian olevan rikkinäinen eikä pyramidia ole toisin sanoen rakennettu kiinteälle pohjalle. Frické (2009) esittää kuitenkin arvosteluiden jälkeen omia myönteisiä näkemyksiä hierarkian elementtien luonteista. Data voi olla muutakin kuin pelkkää havaittavissa olevaa tai instrumenttien avulla määritettyä. Informaatio on taas paljon laajempaa kuin data ja vaatii logiikkaa muodostuakseen. Frické toteaa ihmisen voivan olla tietävä sanakirjan avulla, mutta se ei tee vielä kyseisestä ihmisestä viisasta. Viisas ihminen osaa laajan tietämyksen avulla soveltaa toimiaan hankaliin eettisiin ja käytännön ongelmiin.

Baskarada ja Koronios (2013) perustelevat DIKW-hierarkiaa semiotiikan kirjallisuuden avulla sekä tutkivat hierarkian ja sen termien oikeellisuuden välistä suhdetta. He havaitsivat tutkimuksessa DIKW-termejä käytettävän epäjohdonmukaisesti jokapäiväisessä kielessä sekä myös järjestelmäasiantuntijoiden puolesta. Baskarada ja Koronios muodostivat viitekehyksen avulla heidän mielestään selkeät ja yhdenmukaiset määritelmät termeistä:

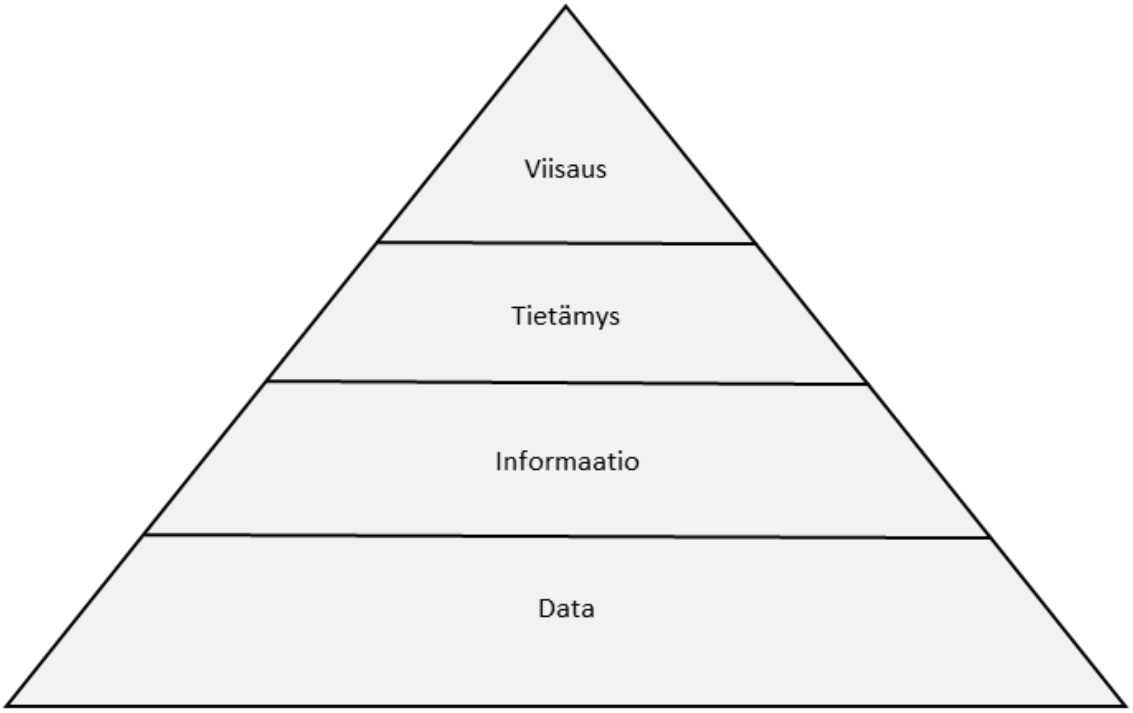
- Viisaus on ihmisen omia normatiivisia käsityksiä, jotka on katsottu sosiaalisesti toivottavaksi.
- Tietämys muodostuu ihmisen uskomuksista, jotka ovat sosiaalisesti arvioitu todenmukaiseksi.
- Informaatio (tai merkitys) tulee esiin tietojen kognitiivisen käsittelyn kautta.
- Data on fyysisiä merkkejä. Niillä ei ole merkitystä, koska ne ovat ihmismielen ulkopuolella.

Frické (2019) pohtii DIKW-pyramidin tasoja hyvin vastaavalla tavalla. Data voi olla numeroita, sanoja, lauseita, tallenteita, oletuksia tai oikeastaan mitä vain muodosta tai lähteestä riippumatta. Informaatio voi olla henkilökohtaista tai julkista tietoa, fyysisiä tiedon ilmentymiä, tilan tai struktuurin muuttaja, epävarmuuden vähentäjä, totuudenmukaista informaatiota, malli, viesti-informaatiota, uutta tietoa tai uskoa johonkin asiaan liittyen tai vaikkapa sisällöllistä informaatiota (Frické, 2019).

Tiedon ero on käsitteiden “tiedostaa että” (eng. know-that) ja “tiedostaa kuinka” (eng. know-how) välillä. Perinteisen filosofian näkemyksen mukaan tieto on kokoelma “tiedostaa-että”-palasia. Esimerkki tästä voisi hyvin olla, että henkilö tietää Eiffel tornin sijaitsevan Pariisissa. Toisaalta sama henkilö voi tietää kuinka pyörällä ajetaan. Tämä tieto on erilaista ja sitä voidaan kutsua taidoksi tai osaamiseksi. Tietoa voidaan myös luokitella vahvaksi tai heikoksi, jolloin vahvalla tiedolla tarkoitetaan oikeutettuja totuudenmukaisia uskomuksia tai yleisiä hyväksyttyjä totuudenmukaisia lausuntoja. Heikko tieto poikkeaa vahvasta tiedosta siinä, että perusteleva komponentti jää pois (Frické, 2019).

Viisaus on tiedon monimuotoisuutta. Se mitä viisaan ihmisen tulee tietää ja ymmärtää muodostaa pitkän listan asioita. Näitä asioita ovat mm. tärkeimmät elämän tavoitteet ja arvot, ikään kuin elämän ultimaattisen maalin, ja sen tavoittelemiseen vaadittavat keinot. Viisaan ihmisen tulisi myös ymmärtää tämän maalin tavoittelemiseen liittyvät vaarat välttääkseen ne. Samalla hänen tulisi

ymmärtää kuinka kehittää itseään sekä yhteyttään muihin ja yhteiskuntaan, kuinka tulla toimeen niin elämän isojen tragedioiden ja dilemmojen kuin hyvienkin asioiden kanssa (Frické, 2019).



KUVIO 1 Tiedon tasot (DIKW-hierarkia) (mukaillen Rowley, 2007)

Frické (2019) esittelee artikkelissaan myös siirtymät tiedon eri tasojen välillä ja toteaa, etteivät siirtymät itsessään ole aina täysin yksinkertaisia. Kaikki data on informaatiota, mutta kuitenkin on olemassa informaatiota, joka ei ole dataa, ja informaatio voi vaihdella paljon suuremmin kuin data ja olla dataa laajamittaisempaa. Avatakseen tätä ajatusta, aiemmin käytetty esimerkki kalkkarokäärmeistä menisi seuraavasti: lause "kaikki kalkkarokäärmeet ovat vaarallisia" on informaatiota, mutta se ei ole käännettävissä dataksi. Ongelma syntyy sanan "kaikki" universaaliuuden kanssa, sillä kaikki data tai dataketjut ovat yksittäisiä. Täten "kalkkarokäärmeet A, B, C ovat vaarallisia" on dataa ja yksittäisiä datan palasia.

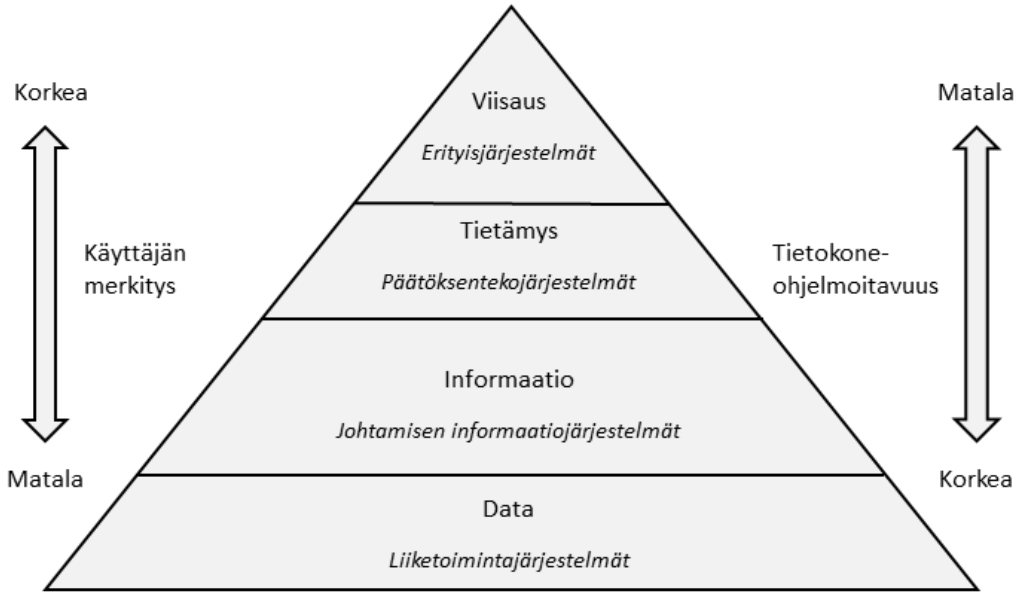
Siirtymä informaatiosta tietoon ei sekään ole täysin yksinkertainen. Jos tieto nähdään "tiedostetaan-että" muodossa, niin jossain valossa tarkasteltuna informaatio ja tieto ovat sama asia, ja tässä tapauksessa siirtymä ei itseasiassa olekaan niin monimutkainen. Kuitenkin DIKW-hierarkian yhteydessä tietoa tarkastellaan usein "tiedostetaan-kuinka" muodossa, mikä tekee siirtymästä haastavan. Otetaan esimerkiksi pyörällä ajaminen. Nuori henkilö ei välttämättä tarvitse mitään informaatiota ajamisen opetteluun tai tarvittavan tiedon määrittäminen voi olla hankalaa. Kuitenkin pyörällä ajaminen on jotain, mitä voidaan opettaa ja

informaatiosta voi olla hyötyä ajamisenkannalta. Taito voi hyötyä informaatiosta. Ongelma sijaitseekin yksityiskohdissa. Kaikki "tiedostetaan-että" muodossa olevat asiat ovat ehdotuksellisia muodoltaan, niille on annettu sopiva ilmaisuun käytettävä kieli, ne voidaan kirjoittaa ylös ja tallentaa tietovaroihin. Sama ei päde "tiedostetaan-kuinka" muodossa oleviin asioihin eli taitoihin. Joitakin taitoja voidaan kirjoittaa ohjemaisesti ylös, mutta ei kaikkia. Esimerkiksi pyörällä ajaminen on yksi näistä asioista, joissa aivot skannaavat ja valitsevat vaihtoehdoista. Näitä taitoja on vaikea taltioida tarkasti.

Viisaus puolestaan on aivan eri kategoriassa datan, informaation ja tiedon kanssa. Viisaus ehdottomasti tarvitsee ja käyttää dataa, informaatiota ja tietoa, mutta se tarvitsee muutakin. Viisaus ei ole datan, informaation ja tiedon "tislaamista". Frické esittääkin, ettei viisaus kuulu DIKW-pyramidin huipulle (Frické, 2019).

Kaikesta DIKW-pyramidin saamasta kritiikistä huolimatta Rowley (2007) esittelee artikkelissaan kuvion 1 DIKW-hierarkian yhteyden myös tietojärjestelmätieteeseen esittämällä, kuinka erilaiset järjestelmät sijoittuvat hierarkian eri tasoille (Kuvio 2). Data-tasolle Rowley sijoittaa liiketoimijärjestelmät. Informaatiotasolle puolestaan sijoittuu johtamisen informaatiojärjestelmät, tietämyksen tasolle päätöksen tekoa tukevat järjestelmät. Korkeimmalle, viisauden tasolle erityisosaamisen ja asiantuntijuuden järjestelmät.

Rowley (2007) esittää samalla, että ihmisen syötteen merkitys nousee hierarkia tasojen myötä, vastavuoroisesti tietokoneohjelmoitavan syötteen määrän laskiessa tasoja noustessa (Kuvio 2). Tämä tarkoittaa sitä, että alemman tason dataa käsittelevät järjestelmät ovat suotuisampia automatisoinnille, kun taas korkeamman tason järjestelmien ja ongelmien yhteydessä käyttäjän rooli kasvaa.



KUVIO 2 DIKW-hierarkia sisältäen järjestelmätasot ja järjestelmien käytön vaativuudet. (Rowley, 2007)

Rowley (2007) pyrki arvioimaan tietojärjestelmä ja tiedonhallinta artikkeleiden pohjalta, onko olemassa selkeää yksimielistä käsitystä hierarkian rakenteesta ja sen elementtien määrittelyssä. Rowleyn tavoitteena oli saada tarkkuutta niihin prosessien kuvauksiin, jotka muuttavat hierarkiassa alempana olevia elementtejä niiden yläpuolella oleviksi. Prosessien kuvauksista ei kuitenkaan löytynyt yksimielistä määritelmää, sillä lähteissä on eri tavoilla kuvattu dataa, informaatiota ja tietämystä. Lisäksi tarkastelussa olevissa teksteissä viitataan vain vähän viisauden elementtiin. Sillä on kuitenkin merkitystä, onko tietoa upotettu järjestelmiin, ihmisten mieliin vai molempiin.

Interazi, Pauleen ja Taskin (2016) puolestaan ovat tutkineet DIKW-hierarkiaa ja sen neljää tasoa siitä, kuinka se informoi ja auttaa johdon päätöksenteossa. Tutkimus osoitti johdon päätöksenteon olevan seurausta kolmen monimutkaisen tekijän dynaamisesta vuorovaikutuksesta, jotka ovat päätöksentekijä (ihminen), päätöstilanne (ongelma) ja kuinka haluttu vastaus kehitetään ja laitetaan paikoilleen (prosessi). Näitä näkökohtia päätöksenteossa pystytään Interazi ym. mukaan tukemaan tiedonhallintajärjestelmällä, jossa on DIKW-lähestymistapa. Tehokas päätöksenteko kuitenkin perustuu DIKW-hierarkian kaikkiin neljään tasoon pyramidissa, eikä vain osaan niistä.

2.3 Tiedolla johtaminen käsitteenä

Tiedolla johtaminen on erittäin laaja käsite, juurtuen moniin eri painopisteen omaaviin tieteenhaaroihin ja käytännön aloihin. Sen lyhyen historian ajan sitä on lähestytty lähinnä seuraavista neljästä näkökulmasta:

1. Filosofinen ja psykologinen näkökulma. Näkökulma tutkii tiedon tyyppejä, niiden vuorovaikutusta ja kognitiivisia prosesseja sekä halua ja motivaatiota töissä. Näkökulma pyrkii vastaamaan siihen, mitä tieto on, mistä se tulee ja mitä mekanismeja sen prosessointi vaatii.
2. Organisaationallinen ja sosiologinen näkökulma. Näkökulma keskittyy organisaatiotason rakenteisiin, oppimiseen ja siihen, kuinka tietoa voidaan luoda ja hallita yhdessä.
3. Taloudellinen ja liiketoiminnallinen näkökulma. Näkökulma keskittyy siihen, kuinka organisaatio voi saavuttaa kilpailuetua tietoa ja innovaatioita luomalla. Se mittaa myös tietoa ja taitoa, ja sitä kuinka tiedosta voidaan saada mitattavissa olevaa arvoa.
4. Teknologinen näkökulma. Näkökulman painopiste on tiedon tehokkaassa säilömisessä, jakamisessa ja “louhimisessa” (Hong & Ståhle, 2005).

Onnistuessaan tiedolla johtamisen pitäisi mahdollistaa ryhmien kyky koordinoida aktiviteettejaan ja jakaa tietoa riippumatta ajasta, funktiosta,

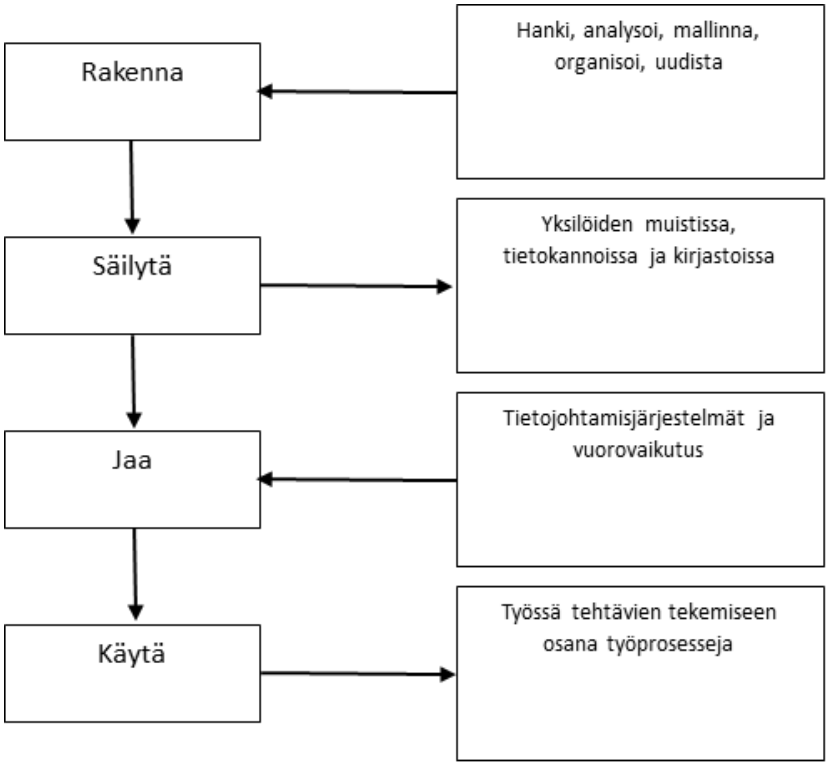
tieteenhaarasta ja liiketoiminnan toimista, vaikka tieto olisikin maantieteellisesti hajautettuna ja säilöttynä useisiin muotoihin (Vasconcelos ym., 2000).

Alavi & Leidner (2001) näkevät, että tieto voi olla hiljaista, eksplisiittistä, se voi viitata johonkin objektiin, kognitiiviseen tilaan tai kyvykkyyteen. Se voi asua yksilöissä, ryhmissä, dokumenteissa, prosesseissa, käytänteissä, fyysisissä paikoissa tai tietokoneiden hakemistoissa. Täten yksittäisen tai täysin optimaalisen ratkaisun kehittäminen organisaation tiedolla johtamiseen tai tiedolla johtamisen järjestelmiin ei ole mahdollista. Organisaatioissa on sovellettava useita tiedolla johtamisen ratkaisuja ja järjestelmiä, jotta hyvin monimuotoisia tiedon tyyppejä ja ominaisuuksia voidaan tehokkaasti hallita (Alavi & Leidner, 2001).

Tiedolla johtaminen käsittää erillään olevat mutta keskenään riippuvaiset tiedon luomisen ja ylläpitämisen prosessit, tiedon varastoinnin ja haun, tiedon jakamisen ja tiedon soveltamisen. Minä hetkenä tahansa organisaatio ja sen jäsenet voivat olla mukana useissa tiedolla johtamisen prosessiketjuissa. Täten, tiedolla johtaminen on dynaaminen ja jatkuva organisaationallinen ilmiö. Lisäksi kompleksisuus, resurssitarpeet ja perustana olevat tiedolla johtamisen työkalut ja lähestymistavat vaihtelevat tiedolla johtamisen prosessin tyypistä, laajuudesta ja prosessin piirteistä riippuen (Alavi & Leidner, 2001).

2.4 Teoreettinen viitekehys

Tietotyöntekijät rakentavat ja käyttävät ammatillista ja yleistä tietoa eri tavoin. He osallistuvat aktiivisesti useisiin tietovirtoihin niin henkilökohtaisella kuin organisaationkin tasolla. He oppivat, organisoivat ja käyttävät tietoaan erilaisiin tarkoituksiin. Oppimista ja muuta tiedon rakentamista tapahtuu, kun tietoa ja informaatiota hankitaan eri lähteistä. Nämä lähteet saattavat sisältää muita ihmisiä, yrityksen tietoja, median, koulutuksen ja harjoittelun, kirjoja ja henkilökohtaisen oppimisen kokemusten kautta niin elämässä yleensä kuin työssäkin. Samalla tapaa on olemassa monia tapoja organisoida, säilyttää, jakaa ja käyttää tietoa tavoilla, jotka ovat sopivia kuhunkin tarkoitusperään (Wiig, 1993). Näitä asioita on esitetty Wiigin tiedolla johtamisen syklissä (Kuvio 3).



KUVIO 3 Wiig:in tiedolla johtamisen sykli. (Wiig, 1993; Kayani & Zia, 2012)

Muutamaa vuotta myöhemmin Wiig (1995) esitteli neljä ulottuvuutta tiedon virtaukseen liittyen. Ne ovat toiminnallisesti erillään ja vastaavat eri tavoitteista. Normaalisti ne ovat eri organisaatioiden osien vastuulla. Tiedon virtauksen neljä ulottuvuutta ovat:

1. Suorita. - Käytä käytettävissä olevaa tietoa laadukkaiden tuotteiden ja palveluiden valmistamiseen.
2. Suorita paremmin. - Tuo uutta operatiivista tietoa työntekijöiden saataville, jotta he voivat suoriutua tehtävistään paremmin.
3. Paranna työtoimintoja ja käytänteitä. - Hyödynnä tietoa muuttaaksesi tuotanto- ja palvelujärjestelmää. Opettele muuttamaan ja kehittämään järjestelmää sekä ottamaan muutoksia käyttöön.
4. Paranna tuotteita ja palveluita. - Hyödynnä tietoa muuttaaksesi ja parantaaksesi tuotteita ja palveluita, sekä kehitä uusia. Rakenna, organisoi ja käytä tietoa näiden toimien suorittamiseksi.

Yksinkertaisesti sanottuna tiedolla johtamisen tavoitteet ovat:

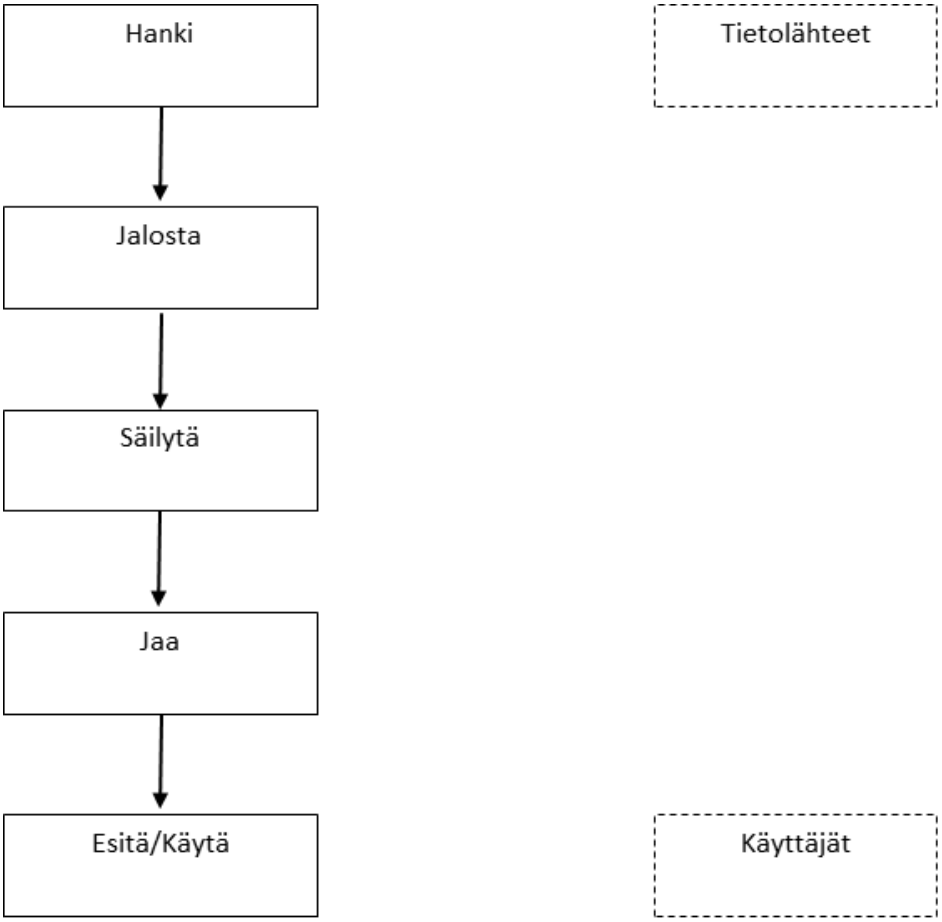
1. Saada organisaatio toimimaan mahdollisimman älykkäästi turvatakseen sen elinkelpoisuuden ja menestymisen.
2. Realisoida organisaation tietovarojen arvo parhaalla mahdollisella tavalla.

Saavuttaakseen nämä tavoitteet edistyneet organisaatiot rakentavat, muuntavat, organisoivat, levittävät ja käyttävät tietovarantoja tehokkaasti (Wiig, 1997). Toisin sanoen, tiedolla johtamisen päätarkoitus on maksimoida organisaation tietoon liittyvä tehokkuus ja tietovarojen tuotot sekä jatkuvasti uudistaa niitä. Tiedolla johtaminen pyrkii ymmärtämään, keskittymään ja johtamaan systemaattista, eksplisiittistä, tarkoituksellista tiedon rakentamista, uudistamista ja käyttöä. Tämä tarkoittaa tehokkaiden tietoprosessien johtamista.

Hallinnollisesta perspektiivistä katsoen systemaattinen tietojohtaminen muodostaa neljä eri osa-aluetta:

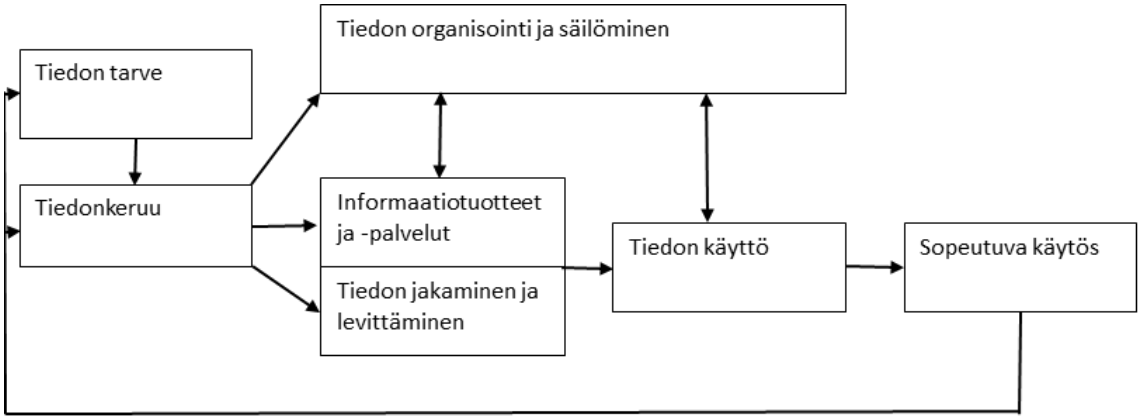
1. Tietoon liittyvien aktiviteettien monitorointia ja fasilitointia.
2. Tietoinfrastruktuurin luominen ja ylläpito.
3. Tietovarojen uudistaminen, organisointi ja transformointi.
4. Tietovarojen käyttö niiden arvon realisoimiseksi (Wiig, 1997).

Meyer ja Zack (1996) kuvaavat tiedolla johtamisen prosessia eräänlaisena syklinä (Kuvio 4). Heidän mallinsa käsittelee sitä, kuinka tieto elää organisaation sisällä ja minkälaisia vaiheita se käy läpi elinkaarensa aikana. Heidän mukaansa tietoa hankitaan tietolähteistä, jonka jälkeen tietoa jalostetaan haluttuun muotoon. Toisin sanoen kerätystä tiedosta poimitaan organisaation toiminnan kannalta oleelliset asiat. Tärkeäksi koettu tieto säilötään tulevaa käyttöä varten. Säilöttyä tietoa jaetaan sen käyttäjien välillä ennen kuin tieto siirtyy käyttöön käyttäjille (Meyer & Zack, 1996).



KUVIO 4 Meyer & Zack tiedolla johtamisen sykli. (Meyer & Zack, 1996; Kayani & Zia, 2012)

Choon (2002) malli (Kuvio 5) käsittelee samoja asioita, kuin Meyer ja Zack (1996), mutta avaa prosesseja tarkemmin. Choon prosessimalli kuvaa tiedon hallintaa jatkuvana syklinä, johon sisältyy kuusi toisilleen hyvin läheistä aktiviteettia; tiedon tarpeen tunnistaminen, tiedon hankkiminen, tiedon organisointi ja säilöntä, tieto ”tuotteiden” ja palveluiden muodostaminen, tiedon jakaminen ja tiedon käyttö. Tiedon hallinnan konseptointi toisiinsa liittyvien informaatioaktiviteettien sykliksi tarjoaa prosessilähtöisen näkökulman informaation hallintaan. Tämä näkökulma täydentää tavanomaisempia informaation hallinnan näkökulmia, joissa puhutaan usein informaatioteknologian hallinnasta tai informaatioresurssien hallinasta. Prosessi alkaa kuvion oikeasta reunasta, syklin lopusta, missä tietoa luodaan organisaation toimien (sopeutuvan käyttäytymisen) kautta. Nämä toimet vaikuttavat yhdessä muiden organisaatioiden ja järjestelmien kanssa muuttaen ympäristöä ja luoden uusia viestejä ja informaatiota (Choo, 2002).



KUVIO 5 Tiedon hallinnan sykli. (Mukaillen Choo, 2002)

Choon (2002) mukaan tiedon tarpeen tunnistamisella tarkoitetaan sitä, kuinka organisaation jäsenet tunnistavat ympäristön epävakauden ja etsivät tietoa sen piirteistä ymmärtääkseen tilanteen ja saadakseen tarvittavan määrän tietoa tukemaan päätöksentekoa ja ongelmanratkaisua. Tiedon tarpeet määrittyvät asia- ja tilannekohtaisesti erilaisten ongelmien ratkaisujen vaatiessa erilaista informaatiota.

Tiedon hankintaa ohjaa tiedon tarpeet. Tiedon hankinnan on myös pystyttävä vastaamaan tiedon tarpeisiin. Organisaatioiden strategiaa ja kasvua koskevat ongelmat vaativat jatkuvasti tarkempaa käsittelyä. Tämän takia olemassa olevia informaatiolähteitä on arvioitava jatkuvasti, uusia lähteitä on löydettävä ja näiden lähteiden yhteensopivuutta on jatkuvasti tarkkailtava.

Tiedon organisointi ja säilöntä prosessin tarkoituksena on luoda organisaatiolle muisti, joka toimii aktiivisena kirjastona organisaation tiedolle ja erikoisosaamiselle. Suurelle volyymille kerättyä ja tuotettua dataa on luotava rakenne, joka vastaa organisaation ja sen jäsenten tarpeita ja tiedon käyttöä. Informaatioteknologia voi nostaa organisaation operatiivisten aktiviteettien tehokkuutta ja luotettavuutta. Informaation hallinnan linjaukset varmistavat, että organisaatioon liittyvä tärkeä tieto niin nykyhetkestä kuin menneisyydestä on suojattuna ja käytettävissä organisaatiotason oppimiseen.

Hankittu ja taltioitu tieto pakataan eritason informaatiotuotteisiin ja palveluihin, joita organisaation eri käyttäjäryhmät ja tiedontarpeet hyödyntävät. Kyse ei ole passiivisesta tiedon uudelleen pakkaamisesta, vaan informaatiotuotteiden arvoa on nostettava informaation laatua ja sopivuutta parantamalla niin, että se vastaa käyttäjän tarpeita ja preferenssejä.

Tiedon jakamisen tavoitteena on kasvattaa tiedon jaettavuutta. Laajalti levitetty tieto kiihdyttää organisaatiotason oppimista sillä tiedon jakaminen luo myös uusia näkökulmia ja tietoa vaikeista ongelmista ja tilanteista. Loppukäyttäjille tulisi antaa parasta mahdollista tietoa, jonka avulla suoriutua töistään ja informaatio tulisi jakaa sellaisten kanavien kautta, jotka sopivat yhteen työntekijän työntapojen kanssa.

Tiedon käytöllä tarkoitetaan tiedon luomista ja soveltamista päätöksenteon ja tulkinnallisten prosessien kautta. Informaation käyttö päätöksenteon

yhteydessä sisältää valikoiman muuttujia, minkä takia informaation muodon ja sisällön tulisi vastata päätöksenteon kineettiseen ja epäsuoraan luonteeseen (Choo, 2002).

2.5 Organisaation sisällönhallinta

"Organisaation strategioiden, työkalujen, prosessien ja taitojen on hallittava sen kaikkia informaatiovaroja niiden elinkaarensa ajan niiden tyypistä riippumatta." (Smith & McKeen, 2003).

Luotujen ja säilöttyjen fyysisten ja virtuaalisten informaatiotuotteiden määrä nykypäivän liikemaailmassa kasvaa eksponentiaalisesti, kun mukaan luetaan myös nopeasti eskaloituva rakenteeton sisältö (Alalwan & Weistroffer, 2012). Organisaation sisällönhallinta (eng. Enterprise content management, ECM) on integroitu lähestymistapa, jonka avulla hallitaan organisaation kaikkea informaatiota, sisältäen organisaation paperiset dokumentit, datan, raportit, verkkosivut ja digitaaliset varat. Organisaation sisällönhallinta sisältää yrityksen informaatiovarojen hallitsemiseen tarvittavat strategiat, työkalut, prosessit ja taidot. Vaikka monet myyjät väittävätkin heidän ohjelmansa olevan ihmeratkaisu ongelmiin, tunnistavat monet tietojohtajat suuremman haasteen hyvän ja kokonaisvaltaisen organisaation sisällönhallintastrategian rakentamisessa, jotta informaation käsittelyyn tarvittavat toimenpiteet ovat kunnollisia ja tehokkaasti integroitu teknologian kanssa sille sopivissa paikoissa (Smith & McKeen, 2003). Kaikki organisaatiot muodostavat, luokittelevat ja arkistoivat informaatiota siten, että se on käytettävissä, kun sitä tarvitaan (Alalwan & Weistroffer, 2012).

Useiden organisaation sisällönhallinnan julkaisujen pohjalta Alalwan & Weistroffer (2012) toteavat yrityksen sisällönhallinnan sisältävän useita hienostuneita ja vuorovaikuttavia teknisiä, sosiaalisia, organisaationallisia ja liiketoiminnallisia näkökulmia. He tiivistävät organisaation sisällönhallinnan kirjallisuuden kolmeen pääpilariin, joista ensimmäinen sisältää neljä sisällönhallinnan ulottuvuutta; työkalut, strategian, prosessin ja ihmiset. Toinen pilari rakentuu yrityksen elinkaaresta sisältäen sisällön omaksumisen, hankinnan, evoluution ja arvioinnin. Kolmas ja viimeinen pilari koostuu puolestaan strategisen johtamisen näkökulmasta sisältäen muutosjohtamisen ja johtamiseen sitoutumisen (Alalwan & Weistroffer, 2012).

Päivärinta ja Munkwold (2005) esittävät, että organisaation sisällönhallinta integroi rakenteellisen, osittain rakenteellisen ja rakenteettoman informaation hallinnan, upotetun ohjelmistokoodin ja metadatan yhteen organisaation sisällön tuottamiseen, julkaisemiseen ja hyödyntämiseen tarkoitetuissa ratkaisuissa. Tiedolla johtamisen tutkimus tunnistaa kolme yleisen tason organisaationallista tietojohtamisen toimenpidettä: parhaiden käytänteiden koodaamisen ja jakamisen; yrityksen tietokirjaston luomisen; sekä tietoverkostojen luomisen. Tietojohtamisjärjestelmät ovat kehitetty tukemaan ja parantamaan tiedon luomisen,

koodaamisen, hyödyntämisen askareita yhdistäen teknologioita, kuten sisäisiä verkkoja, tietolähteitä ja yrityksen hakemistoja. Tiedolla johtamisen tutkimuksen näkökulmasta yrityksen sisällönhallintaa voitaisiin luonnehtia tiedolla johtamisen osa-aihealueeksi, jonka avulla hallitaan eksplisiittisen tiedon hakemistoja. Lisäksi sisällönhallinnan luokittelu- ja metadatatyökalut yltävät aina yrityksen tietoresurssien hallinnan alueelle, johon usein viitataan yrityksen "keltaisina sivuina" ja, jotka sisältyvät tiedolla johtamisen verkostomalliin, joka helpottaa ihmisten välistä kommunikaatiota tietoverkostoissa. Kaiken kaikkiaan, tiedolla johtamisen kenttä on useimmiten liitetty resurssipohjaiseen teoriaan sekä näkökulmaan organisaatioista, joissa tieto on nähty "omaisuuseränä" liittyen tiettyihin organisaationallisiin yksiköihin (Päivärinta & Munkvold, 2005).

Myös Suomen kyberturvallisuusstrategia tunnistaa sisällönhallinnan toimenpiteitä ja tarpeita. Yhteiskunnan elintärkeille toiminnoille välttämättömät tietovarannot, digitaaliset palvelut ja infrastruktuuri tulisi määrittää. Näihin liittyviin toimintoihin ja palveluketjuihin asetetaan kansallisen toiminnan jatkuvuuden hallinnan edellyttämät tavoitetasot strategian mukaan (Valtiovarainministeriö, 2019).

3 OSAAMISEN HALLINTA

Strateginen osaamisen hallinta on enenemissä määrin tärkeää innovatiivisille organisaatioille, ja voi olla jopa kriittistä strategisen kilpailuedun kannalta (Davenport and Prusak 1998). Hustad ym. (2004) painottavat, että organisaatioiden, jotka haluavat saavuttaa pitkäaikaista työllistämistä, toisin sanoen vähäistä vaihtuvuutta, on keskityttävä heidän työntekijöidensä urakehitykseen sekä pitkän aikavälin tavoitteisiin. Tätä varten yleiskuva työntekijöiden osaamiseen ja tietämykseen on välttämätön (Hustad ym., 2004).

Tietointensiivisissä organisaatioissa organisaationallinen tieto on organisaation muodostamien yksilöiden ja työryhmien asiantuntijuuden, kokemuksen ja taidon tuote (Starbuck, 1992; Vasconcelos ym., 2016). Tuo tieto voi olla säilössä yksilön mielessä, selvästi koodattuna ja dokumentoituna yrityksen järjestelmiin tai epäsuorasti upotettuna organisaation kulttuuriin, rituaaleihin, käytänteisiin ja menetelmiin (Alvesson, 1995; Vasconcelos ym., 2016).

Vasconcelos ym. (2016) esittävät aiempaan kirjallisuuteen perustuen, että organisaation sisäiset työryhmät eivät pelkästään voi käyttää parhaita käytännön esimerkkejä, nostaa tehokkuutta ja osallistua kokonaisvaltaiseen organisaatiotason oppimiseen ollakseen toimivia, vaan heidän on myös hallittava jo olemassa olevia taitoja tehokkaasti, kehitettävä mekanismeja ideoiden ja innovaatioiden esiin tuomiseksi, ja identifioitava uusia tiedon lähteitä (Vasconcelos ym., 2016; O'Dell & Grayson, 1998; Zander & Kogut, 1995; Starbuck, 1992; Hansen ym., 2013; Hertog, 2000; Davenport ym., 1996). Hustad ym. (2004) kirjoittavatkin, että systemaattinen ja yleismaailmallinen pääsy yrityksen osaamisresursseihin voi kasvattaa yrityksen innovatiivisuutta ja kiihdyttää uusia oppimisprosesseja. Suomen kyberturvallisuusstrategian mukaan tiiviillä yhteistyöllä, vaihtamalla tietoja asiakastarpeista ja kehittämällä palvelunkehitystä voidaan luoda merkittävää uutta osaamista jo pelkästään kansallisilla sisämarkkinoilla (Valtiovarainministeriö, 2019).

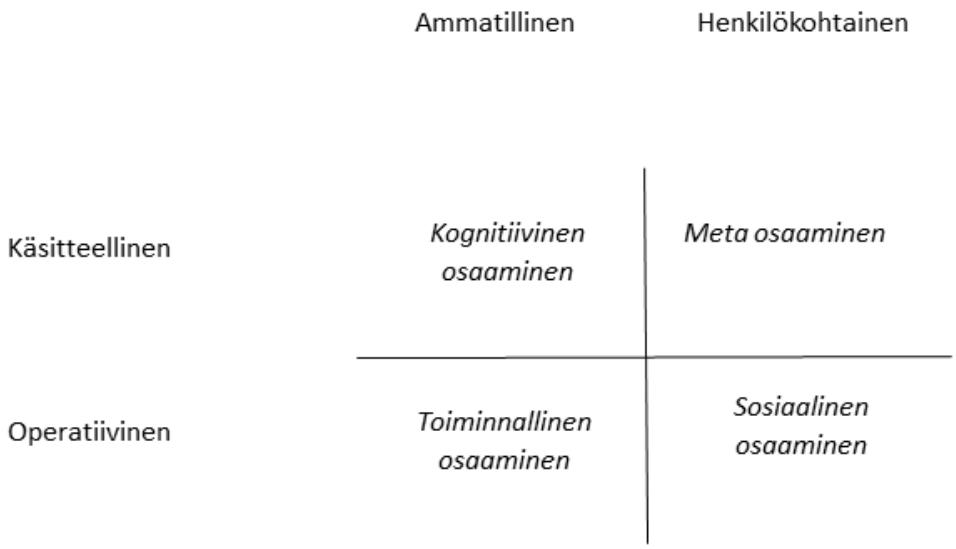
3.1 Mitä osaaminen on?

Osaamisen käsitteen suhteen on paljon hämmennystä ja väittelyä ja sen takia on mahdotonta tunnistaa ja muodostaa yhtenäistä teoriaa tai käsitettä, joka pysyisi sisällyttämään tai täsmentämään kaikki erilaiset tavat, joilla käsitettä osaaminen on käytetty (Le Deist & Winterton, 2005).

Jokaisella organisaatiolla on tietovarantoja aikaisemmista kokemuksista, yksilöllisestä osaamisesta sekä työprosesseista. Mikäli organisaatio haluaa rakentaa toimintaa tehostavan rakenteen, on sen kyettävä pystyttämään arkkitehtuuri, joka palvelee organisaation tietämystä koskien taitoja ja työvoiman kyvykkyyksiä. Organisaation on myös tiedettävä, mitä se haluaa tehostaa tai voimaannuttaa. Toisaalta työntekijöiden on tiedettävä, mitä taitoja tai osaamista eri tehtävissä vaaditaan yrityksen sisällä ja kyettävä valikoitumaan oikeisiin tehtäviin (Houtzagers, 1999).

Le Deist & Winterton (2005) esittivät osaamisen typologiaa alla olevan kuvion 6 mukaisesti. Osaaminen, jota ammatissa tarvitaan, sisältää sekä käsitteellistä osaamista (kognitiivista osaamista, tietoa ja ymmärrystä) sekä operatiivista osaamista (toiminnallista osaamista ja sovellettua taitoa). Yksilökohtaiseen tehokkuuteen liittyvä osaaminen on sekä käsitteellistä (metaosaaminen sisältäen kyvyn oppia) sekä operatiivista osaamista (sosiaalinen osaaminen, käyttäytyminen ja asenteet).

Kognitiivista osaamista on kokemuksen kautta kerätty teoria, konseptit sekä epämuodollinen hiljainen tieto. Tieto ja ymmärrys ovat erotettuja osaamisesta. Toiminnallista osaamista puolestaan ovat ne asiat, joita henkilön jossain tehtävässä tulisi kyettävä tekemään ja demonstroimaan. Metaosaaminen käsittää kyvyn sietää epävarmuutta, mutta myös käsitellä oppimista ja reflektointia. Sosiaalinen kyvykkyys tai osaaminen nähdään taitona tulla toimeen toisten ihmisten kanssa, vuorovaikuttaa ja toimia ryhmässä. Henkilökohtaiseksi osaamiseksi nähdään käytökselliset taidot, joita kuvataan suhteellisen pysyviksi piirteiksi henkilössä, jotka johtavat tehokkaaseen tai erinomaiseen suoriutumiseen työssä (Le Leist & Winterton, 2005).



KUVIO 6 Osaamisen typologia (mukaillen Le Deist & Winterton, 2005)

Hong ja Ståhle (2005) esittelivät artikkelissaan neljä erilaista osaamisen tyyppiä. Näitä ovat yksilön osaaminen, yrityksen laajuinen strateginen osaaminen, tiimin tai projektin yhteistyöhön perustuva osaaminen sekä verkostollinen osaaminen. Yksilöllinen tai työntekijäkohtainen osaaminen liittyy useissa organisaatioissa tiedolla johtamiseen. Yksilökohtainen osaaminen keskittyy täysin työntekijöiden henkilökohtaisiin ja kognitiivisiin piirteisiin suhteessa heidän suoriutumiseensa työssään (Hong & Ståhle, 2005). Yksilöiden osaaminen on ratkaisevassa osassa yrityksen kilpailukykyä ja yritysten täytyykin löytää uusia keinoja, joilla huippuosaajat saadaan pidettyä yrityksessä (Valtiovarainministeriö, 2019).

Yrityksen laajuinen strateginen osaaminen sisältää tiedolla johtamisen konsepteja, kuten ydinosaamisen, kyvykkyysperusteisen kilpailun, osaamisperusteisen strategisen johtamisen, dynaamiset kyvykkyydet sekä vastaanottamiskapasiteetin. On selvää, että ydinosaaminen nähdään yhdistelmänä tuotantotaitoja sekä teknologiaa. Tämä ajatus ohjaa osaamisen hallinnan näkökulman pois yksilöstä ja laajentaa sen koskemaan koko organisaatiota, luoden samalla resurssilähtöisen näkökulman, jossa osaaminen on avainasemassa yrityksen kasvua ajatellen (Hong & Ståhle, 2005).

Tiimin tai projektin yhteistyöhön perustuva osaaminen käsittää hyvin yksiselitteisesti jonkin tietyn yhdessä työskentelevän tiimin osaamisen. Osaava tiimi koostuu poikkeuksetta vaihtelevalla tasolla osaamattomista yksilöistä. Keskeinen asia onkin ryhmän kyky työskennellä yhdessä yhteisen tavoitteen eteen. Tämä sisältää kyvyn ratkaista ongelmia yhdessä, yksilöllistä taitoa työskennellä eri yksilöiden kanssa tiedon ja vastuiden jakamisen mahdollistavan ilmapiirin säilyttämiseksi sekä ryhmän sisäistä tietoa ja yhteisiä toimintatapoja työn kontekstissa (Vartiainen ym., 2003; Hong & Ståhle, 2005)

Verkostollisen osaamisen tieteenala keskittyy erityisesti organisaatioiden välisiin suhteisiin ja vuorovaikutukseen yrityksen osaamisen rakentamisessa.

Nykypäivän jatkuvasti muuttuvassa ja kompleksissa liikemaailmassa eritasojen kyvykkyyksien ja osaamisen hallinta tulee olemaan erityisen tärkeää organisaatioissa (Hong & Ståhle, 2005).

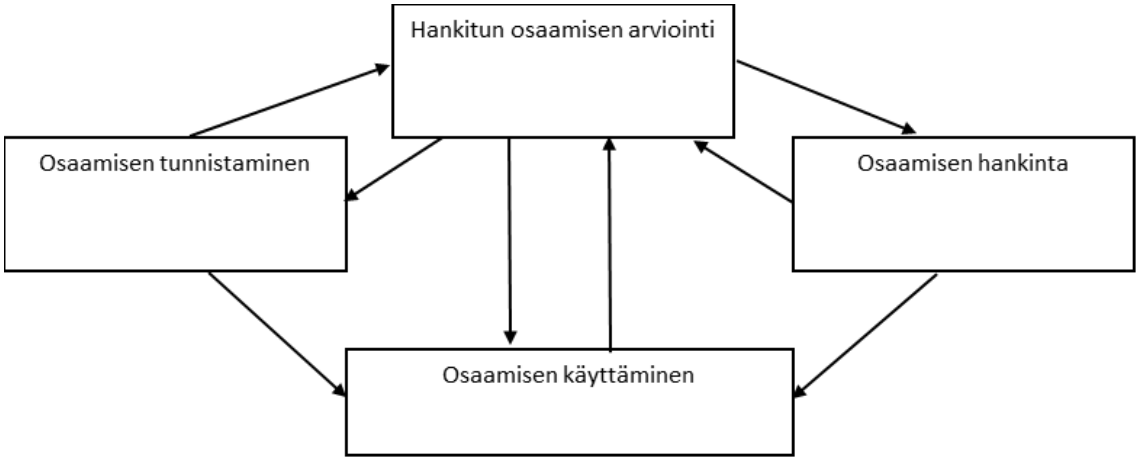
3.2 Osaamisen hallinta käsitteenä

Kyberturvallisuuden yhteydessä osaamisen hallinta on määritelty prosessien ja työkalujen hallinnaksi, joiden avulla organisaatio voi tunnistaa, dokumentoida ja käyttää henkistä pääomaa ja tietosisältöä (Newhouse ym., 2017). Osaamisen hallinnan tavoitteena on hyödyntää ihmisen taitoa ja tietoa paremmin (Vasconcelos ym., 2016). Laajasti tarkasteltuna osaamisen hallinta on tapa, jolla organisaatiot hallitsevat yrityksen, ryhmien ja yksilöiden kyvykkyyksiä. Sen päätavoitteena on määrittää ja jatkuvasti ylläpitää kyvykkyyksiä yrityksen tavoitteiden mukaisesti (Berio & Harzallah, 2007). Kyvykkyys puolestaan on tapa viedä tietoa, taitoa ja asenteita käytäntöön tietyn kontekstin sisällä. Osaamisen hallinnasta on tulossa entistä tärkeämpää, sillä osaamisen on tunnistettu olevan erittäin tärkeää yrityksen tavoitteiden saavuttamiselle ja edesauttavaa ydinliiketoimintaprosesseille, asiakassuhteille ja taloudellisille tuloksille (Berio & Harzallah, 2005; Hamel & Prahalad, 1994; Kaplan & Norton, 1996).

Kyvykkyydet ovat niitä mitattavissa olevia henkilön piirteitä, joita tarvitaan tietyssä työtilanteessa tietyn työtehtävän suorittamiseen (Klendauer ym., 2012), minkä takia kyvykkyyksien tehokas hallinta on läheisesti yhteydessä erinomaiseen suorituskykyyn, sillä kyvykkyydet edustavat tietoa, taitoa ja käyttäytymistä, jotka kontribuoivat yrityksen menestykseen (Prahalad and Hamel 2003).

Berio & Harzallah (2007) esittivät, että osaamisen hallintaa voidaan organisoida neljän eri prosessin mukaisesti, huomaten kuitenkin, että jokaisen neljän pääprosessin sisällä voi tapahtua useita prosesseja (Kuvio 7). Osaamisen tunnistaminen käsittää sen, milloin ja miten osaamista tunnistetaan ja kuinka osaamista määritetään nykyhetkessä tai tulevaisuudessa askareiden ja tehtävien tekemisen ja strategioiden käyttöönoton saavuttamiseksi.

Osaamisen arvioinnilla tarkoitetaan Berion ja Harzallahin (2007) mukaan sitä, kuinka ja milloin yksilöiden hankkimaa osaamista tunnistetaan ja määritetään, ja kuinka yritys voi päättää yksilön saavuttaneen tietyn osaamisen. Osaamisen hankinnalla puolestaan tarkoitetaan sitä, kuinka yritys suunnittelee ja päättää milloin ja miten osaamista hankitaan. Osaamisen käyttämisen prosessi vastaa siitä, kuinka tunnistamisen, arvioinnin ja hankinnan kautta tuotettua ja muodostettu osaamista käytetään. Tämä voi tarkoittaa esimerkiksi sitä, kuinka tunnistaa rakoja tarvitun ja hankitun osaamisen välillä, kenen tulisi osallistua tarvittuun koulutukseen, kuinka löydetään avaintyöntekijöitä, jotka omaavat avainasemassa olevaa osaamista ja kuinka arvioidaan tärkeimpiä suuntauksia taidoissa organisaatioiden eri osien välillä (Berio & Harzallah, 2007).



KUVIO 7 Osaamisen hallinnan neljä prosessia (mukaillen Berio & Harzallah, 2005).

4 KYBERTURVALLISUUS

Tässä luvussa käsitellään kyberturvallisuuden käsitettä, kyberturvallisuuden kehitystä ja modernin maailman tarpeita kyberturvallisuuden suhteen. O'Connell (2012) toteaa sanan 'kyber' olevan yksi useimmiten käytetyistä sanoista kansainvälisessä turvallisuuskeskustelussa tänä päivänä.

Kaikessa turvallisuudessa on kyse omaisuuden suojaamisesta tiettyjen luontaisten haavoittuvuuksien aiheuttamilta erilaisilta uhkilta. Suojausprosessit käsittelevät yleensä turvallisuuskontrollien ja vastatoimien valintaa sekä käyttöönottoa, jotka auttavat vähentämään näiden haavoittuvuuksien aiheuttamaa riskiä (Von Solms & Van Niekerk, 2013).

Lehto (2022) toteaa kyberturvallisuuden rakentuvan monista erilaisista toimintamalleista ja dokumenteista, joihin sisältyy turvallisuutta ohjaavia strategioita, arkkitehtuureja ja suunnitelmia. Arviointimenettelyt ja raportointi ovat tärkeässä osassa kyberturvallisuuden jatkuvassa toteuttamisessa. Turvatoimien tehokkuutta ja tarkoituksenmukaisuutta tulisi organisaatioissa seurata ja arvioida säännöllisesti. Apuna yleensä toimii hallintajärjestelmä, joka toteuttaa organisaation strategiaa. Kyberturvallisuudella monesti viitataankin kykyyn hallinnoida pääsyä verkossa oleviin järjestelmiin ja informaatioon, joita ne sisältävät, joten kyberturvallisuutta voidaan kutsua myös informaatioteknologian turvallisuudeksi (Lehto, 2022).

Lehto (2022) määrittelee kyberturvallisuuden kokonaisturvallisuuden osa-alueeksi, jonka kokonaistavoitteena on digitalisoituneen ja verkotetun yhteiskunnan turvallisuus. Yhteiskunnan kriittisissä toiminnoissa yhdistyvät kyberturvallisuuden osa-alueita kuten tietoturva, toimintojen jatkuvuuden hallinta ja häiriötilanteisiin varautuminen. Kyberavaruutta voi myös sen sisältämien uhkakuvien lisäksi pitää varmana, joustavana ja luotettavana digitaalisena infrastruktuurina, jos kyberturvallisuuden kontrollit ja kyvykkyydet ovat tehokkaita. Tarkemmin tarkasteltuna kyberturvallisuus on teknologioiden, prosessien ja käytänteiden yhdistelmä, jonka avulla verkkoja, laitteita, ohjelmia ja dataa suojellaan hyökkäyksiltä, vahingoilta tai luvattomalta käytöltä (Lehto, 2022).

Rikoslaki, EU:n tietosuoja-asetus, NIS2-direktiivi, joka on EU:n laajuinen kyberturvallisuutta koskeva lainsäädäntö (EU-komissio, 2023) sekä VAHTI-

ohjeistus, josta Digi- ja väestötietovirasto vastaa, ja ohjaa ohjeistuksella julkisen hallinnon digitaalisen turvallisuuden kehittämistä ja varmistamista (Digi- ja väestötietovirasto, 2024), ovat organisaation johdon apuna, mutta samalla Lehto (2022) toteaa niiden antavan velvoitteita ja juridisia perusteita toteuttaa kyberturvallisuutta. Organisaation johdon vastuulla on laatia, kehittää ja jalkauttaa organisaatiolle sen vaativa toimiva kyberturvallisuusstrategia, jossa määritellään kyberturvallinen toimintatapamalli. Kyberturvallisuusstrategiassa on päämäärät, periaatteet, toimintatavat ja linjaus siitä, kuinka kyberturvallisuus otetaan huomioon, suunnitellaan ja toimeenpannaan organisaation kaikilla eri tasoilla. Myös kyberturvallisuuden johtaminen tulisi olla koko organisaation läpi ulottuvaa, jotta prosessien osatekijät ja niiden riskit voidaan tunnistaa kokonaisturvallisuuden kehittämiseksi. Kyberturvallisuusstrategia täytyy saada aina strategiselta tasolta toiminnan tasolle asti (Lehto, 2022).

4.1 Kyberturvallisuuden määritelmä

"Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoiminta ympäristöön voidaan luottaa ja jossa sen toiminta turvataan" (Suomen kyberturvallisuusstrategia ja taustamuistio, 2013).

Lehdon (2022) mukaan kyberturvallisuus on yksinkertaistettuna toimenpiteitä, joilla sekä suojaudutaan että toteutetaan vastatoimenpiteitä kyberhyökkäyksiä vastaan. Uhka-analyysit, joita organisaatiot sekä instituutiot muodostavat ovat avainasemassa kyberturvallisuuden rakentumisessa, sillä niissä arvioidut uhkatekijät ja riskit muodostavat organisaation kyberturvallisuusstrategian- ja ohjelman rakenteen sekä elementit. Kybertoimintaympäristö on nykypäivänä erittäin laaja ja ulottuva, joten monesti organisaatiot joutuvat laatimaan useita tarkemmin kohdistettuja kyberturvallisuusstrategioita ja -ohjeita. Thakur ym., (2015) määrittelevät kyberturvallisuuden toimenpiteiksi, joilla suojataan tietokonejärjestelmiä, verkkoja ja tietoja häiriöiltä tai luvattomilta pääsyiltä, käytöiltä, paljastumisilta, muuttumisilta tai tuhoutumiselta.

Kansallinen turvallisuusjärjestelmäkomitea (CNSS) määrittää kyberturvallisuuden olevan tietokoneiden, elektronisten kommunikaatiojärjestelmien ja –palveluiden sekä langallisen ja elektronisen kommunikaation vahingoittumisen estämistä, suojaamista ja restaurointia sisältäen ja varmistaen niiden sisältämän informaation saavutettavuuden, yhtenäisyyden, oikeellisuuden, luotettavuuden ja kiistattomuuden (CNSS, 2022). Craigen ym. (2014) määrittelevät käsitteen kyberturvallisuus resurssien, prosessien ja rakenteiden organisoinniksi ja kokoelmaksi, jonka tehtävänä on suojata kyberavaruutta ja kyberavaruuteen liittyviä järjestelmiä kyberrikollisuudelta. Kyberturvallisuuden toimenpiteillä yritetään estää tapahtumia, jotka ovat oikeudellisesti ristiriidassa tosiasiallisten omistusoikeuksien kanssa (Craigen ym., 2014).

Thakur ym. (2015) huomasivat kyberturvallisuuden termiä käytettävän vaihtoehtona tietoturvan termille, vaikka heidän mielestään tietoturva korostaa enemmän ihmisen roolia turvallisuusprosesseissa, kun taas kyberturvallisuudessa ihmisen rooli nähdään lisäulottuvuutena, mutta myös samalla potentiaalisena kohteena kybertoiminta ympäristössä. Thakur ym. (2015) pitävät keskustelua kyberturvallisuudesta merkittävänä, sillä se keskittyy koko yhteiskunnan eettiseen osaan. He samalla toteavat selkeyden ja yksimielisyyden puuttuvan kyberturvallisuus termiltä, sillä määritelmät keskittyvät eri näkökohtiin, kuten suojattu jakaminen, luottamuksellisuus tai tiedon saatavuus (Thakur ym., 2015). Myös Schatzin ym. (2017) huomauttavat terminologian käytön kehityksen aiheuttavan ongelmia, koska termistä 'kyberturvallisuus' puuttuu esimerkiksi 'tietokoneturvallisuuden' määrittävä selkeys. Heidän mielestään tämä voi johtaa sekaannukseen ja väärinkäsityksiin, jos osapuolilla on erilaiset oletukset siitä, mitä termi edustaa.

Qiu ym. (2013) havaitsivat tutkimuksessaan kyberturvallisuuden osoittavan kolme tärkeää tekijää. Ensimmäisenä tietotekniikan suojausmenetelmät, toisena data itsessään ja kolmantena fyysiset ja virtuaaliset asetukset datan käsittelyssä. Näiden toimenpiteiden avulla on mahdollista saavuttaa suojauksen taso ja niihin liittyvät ammatilliset näkökohdat. Myös Lehto (2022) toteaa kyberturvallisuuden olevan erilaisia suojausmenetelmiä haitallisia hyökkäyksiä vastaan. Menetelmät koskevat tietokoneita ja palvelimia, mobiililaitteita, elektronisia järjestelmiä, verkkoja ja dataa. Kyberturvallisuuden termi onkin hyvin laaja-alainen ja se soveltuu kaikkeen tietokoneiden kokonaisturvallisuudesta katastrofeista toipumiseen ja loppukäyttäjien koulutukseen asti.

Kyberturvallisuus on sekä epävarmuutta, joka on syntynyt uuden alueen ja ulottuvuuden myötä, että myös käytänteitä ja prosesseja, joilla tämä tila saadaan turvallisemmaksi. Kyberturvallisuus viittaa joukkoon aktiviteetteja ja toimenpiteitä niin teknisiä kuin epäteknisiä, joiden avulla suojataan kaikilta mahdollisilta uhilta ympäristöä ja dataa, jota se sisältää ja kuljettaa (Cavelty, 2010).

Schatz ym. (2017) kirjoittavat artikkelissaan Etelä-Afrikan kyberturvallisuusstrategian määrittelevän kyberturvallisuuden käsitteen kaikista parhaiten. "Kyberturvallisuus on kokoelma työkaluja, linjauksia, turvallisuuskonsepteja, turvallisuussuojia, ohjeistuksia, riskinhallinnan lähestymistapoja, toimia, harjoitusta, parhaita käytänteitä, varmuutta ja teknologiaa, joita voidaan käyttää kyberympäristön, organisaatioiden ja sen varojen turvaamiseen." (Schatz ym., 2017)

Schatz ym. (2017) esittävät tutkimuksensa pohjalta myös oman parannellun versionsa kyberturvallisuuden määritelmästä: "Lähestymistapa ja toimet, jotka ovat yhteydessä organisaatioiden ja valtioiden turvallisuusriskien hallintaprosesseihin, joilla suojataan datan ja omaisuusvarojen luottamuksellisuus, yhtenäisyys ja saavutettavuus kyberavaruudessa. Konsepti sisältää ohjenuorat, linjaukset, kokoelman suojia, teknologian, työkalut sekä koulutuksen mahdollistaakseen parhaan suojan kyberympäristölle ja sen käyttäjille." (Schatz ym., 2017)

Organisaatio ja käyttäjävarannot sisältävät yhdistetyt tietokoneet, henkilöstön, infrastruktuurin, sovellukset, palvelut, telekommunikaatiojärjestelmät sekä

kokonaisuudessa että välitetyn ja/tai säilötyn informaation kyberympäristössä. Kyberturvallisuus ponnistelee varmistaakseen organisaation turvallisuusominaisuuksien ja käyttäjän varantojen saavuttamisen ja ylläpitämisen vastaten oleellisiin turvallisuusriskeihin kyberympäristössä. Yleiset turvallisuuden tavoitteet käsittävät saavutettavuuden, yhtenäisyyden ja luotettavuuden (ITU, 2008).

National Institute of Standards (NIST) on National Initiative for Cybersecurity Education -ohjelmassaan luonut viitekehyksen (Taulukko 1), joka kuvaa kyberturvallisuuden työtä ja osaamista, niin julkisella, yksityisellä kuin akateemisella sektorilla. Viitekehystä kutsutaan yleisesti NICE-viitekehykseksi (Workforce Framework for Cybersecurity). Viitekehys koostuu seitsemästä korkeamman tason kyberturvallisuustoimintojen ja -osaamisen ryhmittelystä, joihin sisältyy 33 alemman tason osa-aluetta. Lisäksi viitekehyksessä on kyberturvallisuustyö jaoteltu yhteensä 52 eri ryhmään, jotka koostuvat tietyistä taidoista, tiedoista ja kyvyistä, joita tarvitaan työroolin suorittamiseen. Viitekehyksen avulla saa tarkemman kuvan kyberturvallisuudesta ja siihen liittyvistä toiminnallisista osa-alueista. Taulukossa 1 esittelemme korkeamman tason ryhmittelyt sekä alemman tason osa-alueet (Newhouse ym., 2017).

TAULUKKO 1 Kyberturvallisuuden työvoimakehys (NICE Framework) (Newhouse ym., 2017)

Osaamisen pääluokat (7)	**Erityisosaamisalueet (33)**
Analysointi	Kaikkien lähteiden analysointi, hyödyntämisen analyysi, kielianalyysi, kohdeanalyysi ja uhka-analyysi
Tiedonkeruu ja operointi	Keräystoiminnot, kyberoperaation suunnittelu ja kyberoperaatiot
Tutkinta	Kybertutkinta ja digitaalinen rikostekninen tutkimus
Operointi ja ylläpito	Asiakaspalvelu ja tekninen tuki, tietojen hallinta, osaamisen hallinta, verkkopalvelut, järjestelmän hallinta ja järjestelmäanalyysi
Kokonaisuuden valvonta ja johtaminen	Kyberturvallisuuden hallinta, toimeenpaneva johtajuus, oikeudellinen neuvonta ja asianajo, projektin hallinta ja hankinta, strateginen suunnittelu ja politiikka sekä harjoittelu, koulutus ja tietoisuus
Suojaus ja puolustus	Kyberpuolustusanalyysi, kyberpuolustusinfrastruktuurin tuki, tapahtumiin vastaus ja haavoittuvuuksien arviointi ja hallinta
Turvallinen tuotanto	Riskienhallinta, ohjelmistokehitys, järjestelmäarkkitehtuuri, järjestelmäkehitys, järjestelmävaatimusten suunnittelu, teknologian tutkimus ja kehitys sekä testaus ja arviointi

4.2 Kyberturvallisuuden historia ja kehitys

Tässä alaluvussa esitellään kyberturvallisuuden kehitystä ajan saatossa sekä merkittäviä tapahtumia, jotka ovat muovanneet tai edesauttaneet kyberturvallisuuden kehitystä.

4.2.1 Informaatioturvallisuudesta kyberturvallisuuteen

Digitaalisten laitteiden ja tiedon turvallisuusnäkökohtien käsittelyssä käytetty terminologia on muuttunut huomattavasti viime vuosina. Lehto (2022) huomauttaa, että käsitteitä kyberturvallisuus, digitaalinen turvallisuus ja tietoturvallisuus käytetään usein rinnakkaisina käsitteinä eikä niille ole yhteisesti hyväksyttyä määrittelyä. Schatz ym. (2017) toteavat vuosisadan alussa tässä yhteydessä käytetyimpien termien olleen tietokoneturvallisuus, IT-suojaus tai tietoturva. Näillä termeillä on vivahteita, joita alalla työskentelevät ammattilaiset ymmärtävät, mutta termit eivät ole kuitenkaan olleet riittävän konkreettisia ollakseen merkityksellisiä laajemmalle väestölle. Schatz ym. pohtivat pitäisikö yleistä keskustelua käydä ja suunnitelmia tehdä yhteisymmärryksen pohjalta siitä, mitä nämä termit tarkoittavat, mutta toteavat ensimmäisen vuosikymmenen lopulla uudesta kyberterminologiasta tulleen yhä suositumpi 'kyberturvallisuus' termin käytön myötä. Viimeistään vuonna 2009 termi 'kyber' vakiinnutti paikkansa, kun Yhdysvaltojen presidentti Barack Obama piti puheen kansalaisille kyberinfrastruktuurista. Puheessaan Obama kannusti kaikkia kyberturvallisuuteen ja julisti aloittavansa kampanjan, jossa pyritään edistämään kyberturvallisuustietoisuutta ja digitaalista lukutaitoa niin organisaatioissa kuin kouluissakin. Samalla Obama huomautti Yhdysvaltojen taloudellisen vaurauden 2000-luvulla riippuvan kyberturvallisuudesta sekä digitaalisen työvoiman rakentamisesta (Obama, 2009; Schatz ym., 2017).

Sana 'kyber' on yksi yleisimmin käytetyistä termeistä kansainvälisissä turvallisuuskeskusteluissa nykypäivänä. Se on myös varmasti kasvava termi kansainvälisen asianajajan sanakirjassa mutta se ei kuitenkaan ole O'Connellin (2012) mukaan uusi termi kansainvälisessä oikeudessa, sillä kansainväliset asianajajat ovat keskustelleet tietokoneista ja niiden käyttöä sääntelevästä laista useiden vuosikymmenien ajan. Kyberavaruuden turvallisuudesta keskusteltaessa on alustavasti huomioitava, että kyberavaruus on kansainvälistä tilaa. Toimiessa kyberavaruudessa ja siihen liittyvässä kansallisessa lainsäädännössä on noudatettava asiaa koskevaa kansainvälistä oikeutta (O'Connel, 2012).

Tietoturvallisuus on hyödykkeenä olevan tiedon suojaamista erilaisten uhkien ja haavoittuvuuksien aiheuttamilta mahdollisilta haitoilta. Kyberturvallisuus puolestaan ei välttämättä ole vain kyberavaruuden suojaamista, vaan myös kyberavaruudessa toimivien ja niiden kyberavaruuden kautta tavoitettavissa

olevien resurssien suojaamista (Von Solms & Van Niekerk, 2013). Valtiovarainministeriö (Valtiovarainministeriön julkaisuja 2020:23) on määritellyt digitaalisen turvallisuuden laajemmaksi viitekehykseksi, johon sisältyy riskien hallinta, toiminnan jatkuvuuden hallinta ja varautuminen, tietoturvallisuus, tietosuoja ja kyberturvallisuus.

4.2.2 Kybermaailman uhkia ja merkittäviä tapahtumia

Turvallisuusongelmat ovat yhtä vanhoja kuin internet on itse (O'Connell, 2012), mutta seuraavaksi esittelemme kuitenkin tiettyjä merkittävämpiä kybermaailman tapahtumia, jotka ovat osaltaan vaikuttaneet kyberturvallisuuden kehityskulkuun ja maailman politiikkaan. Sen jälkeen tarkastellaan nykypäivän kybermaailman uhkia ja tilannetta.

Vuonna 2007 Viro koki laajoja tietokonehakkerointihyökkäyksiä, jotka kestivät useita viikkoja ja joilla oli lähes tuhoisa vaikutus maahan (Kumar & Carley, 2016; O'Connell, 2012). Siitä lähtien tuki kyberturvallisuutta kohtaan on kasvanut, jotta kyberturvallisuusongelmien sotilaalliset ratkaisut ovat etusijalla. NATO:n vastaus hyökkäykseen oli alkaa kehittämään kyberturvallisuuteen tähtäävää politiikkaa ja kapasiteettia. Georgian ja Venäjän sodassa vuonna 2008 Georgia koki vastaavanlaisia kyberhyökkäyksiä kuin Viro aikaisempana vuotena (O'Connell, 2012). Vuonna 2009 Yhdysvallat aloitti Obaman hallituskaudella julkaisemaan useita kyberturvallisuuteen liittyviä poliittisia linjauksia ja virkoja, jotka olivat pääosin sotilaallisia (Obama, 2009). Lisäksi vuonna 2009 yksi tai useampi hallitus, todennäköisimmin Yhdysvallat ja Israel, julkaisi tietokonehaittaohjelmia, jotka tunnetaan nimellä Stuxnet-mato, joiden tavoitteena oli hidastaa Iranin ydinohjelman etenemistä. Vuonna 2011 Yhdysvaltojen kongressi aloitti keskustelun uudesta lainsäädännöstä, joka antaisi puolustusministeriölle entistä enemmän toimivaltaa kyberturvallisuuden alalla (O'Connell, 2012). 2010-luvun tienoilla valtiot alkoivat julkaisemaan kansallisia kyberturvallisuusstrategioita. Norja oli ensimmäisiä maita Yhdysvaltojen kanssa, jolla oli kansallinen kyberturvallisuusstrategia jo vuonna 2003. Muun muassa Viro julkaisi omansa vuonna 2008, Ruotsi ja Kanada vuonna 2010, Saksa ja Ranska vuonna 2011 ja Suomi vuonna 2013. Jokainen edellä mainittu valtio on päivittänyt myöhemmin 2020-luvulle tultaessa vähintään kerran kansallista kyberturvallisuusstrategiaa vastaamaan kybermaailman kehitykseen (Public Safety Canada, 2018; ANSSI, 2015; Federal Ministry of the Interior and Community, Germany, 2021; Valtiovarainministeriö, 2019; Ministeries, Norway, 2019; Ministry of Economic Affairs and Communication, Estonia, 2019; Goverment Offices of Sweden, 2016; White House, United States, 2003). Euroopan unionin kyberturvallisuusvirasto toteaa raportissaan jatkuvan kehityksen näkyvän etenkin puolustusstrategioissa ja kyberfyysisten järjestelmien kehityksessä (Marinos ym., 2016).

Euroopan unionin kyberturvallisuusviraston (ENISA) selvityksen mukaan kyberturvallisuushyökkäykset jatkoivat kasvuaan vuosien 2021 ja 2022 aikana, ei vain eri sektoreilla ja lukumääriltään, mutta myös kokonaisvaikutusten osalta. Venäjän ja Ukrainan kriisi on puskenut kybersodankäynnin ja hacktivismin

roolin sekä vaikutuksen konflikteihin uudelle aikakaudelle. Valtioiden- ja muiden toimijoiden kyberoperaatiot kuitenkin sopeutuvat tilanteeseen, jolloin ne pystyvät hyödyntämään sodan tuomia uusia mahdollisuuksia ja haasteita. Sota on kuitenkin tuonut uuden paradigman kyberavaruuden kansainvälisiin normeihin ja erityisesti kyberhyökkäyksiä koskevaan valtion sponsorointiin sekä hyökkäysten kohdistamista kriittistä infrastruktuuria vastaan. Virasto odottaakin lähi- ja keskipitkällä aikavälillä havaitsevan enemmän geopolitiikan ohjaamaa kybertoimintaa. Geopoliittinen tilanne saattaa laukaista kyberoperaatioita ja haitallisia kyberhyökkäyksiä. Näin ollen epävakaa tilanne ja jatkuva haitallisen kybertoiminnan ylläpitäminen voi johtaa lisääntyneisiin vahinkoihin maailmanlaajuisesti (Ifigeneia ym., 2022).

Lehto ja Limnéll (2017) määrittivät kyberuhkien aiheuttajiksi sisäpiiriläiset, kybervandaalit, kybervakoilijat sekä kyberterroristit ja –sotilaat. Sisäpiirillisiksi luokitellaan kaikki nykyiset ja entiset työntekijät, urakoitsijat ja liikekumppanit, jotka voivat muodostaa uhan. Käytännössä kuka tahansa henkilö, jolla on pääsy yrityksen tietokonejärjestelmiin ja tietoihin, voi olla vahingollinen. Sisäpiiriläiset vaihtelevat motivaation, tietoisuuden, pääsyn tason ja aikomusten osalta (IBM, 2023). Sisäpiiriuhka onkin yksi merkittävimmistä kyberuhkista. Ayodele (2022) on listannut toimenpiteitä, joilla sisäpiiriuhkan muodostaa riskiä voidaan organisaatioissa hallita paremmin sekä toteaa organisaatioiden ajattelutavan tarvitsevan muutosta, jossa kyberturvallisuus nähtäisiin kaikkien sidosryhmien roolina ja vastuuna. Kybervandaaleita ovat hakkerit, haktivistit, script kiddiet ja yksinäiset sudet. Näiden toimijoiden motiivit, työkalut ja toimintatavat vaihtelevat paljon, mutta kaikki toiminta on enemmän tai vähemmän hyökkäävää. Kyberrikollisuudelle on nyt ominaista erikoistuminen ja ammattimaisuus, jossa yksilöt tarjoavat tavallaan, kuin à la carte kyberrikollisuuspalveluita (Paquet-Clouston & Garcia, 2022). Marinos ym. (2016) pohtivat Euroopan unionin kyberturvallisuusvirastolle muodostamassaan raportissa, että olisi tarpeen miettiä kuinka ystävällismielisiä kybertoimijoita ja -toimintaryhmiä voitaisiin luoda ja mobilisoida toimimaan aktiivisesti kyberpuolustuksessa. Näillä toimijoilla on valtavasti osaamista, joten he olisivat tärkeä vastatoimi koko yhteiskuntaa vaarantavissa kyberuhkissa. Kybervakoilua toteuttavat sekä valtiot että yritykset, jotka ovat kiinnostuneita aineettomasta omaisuudesta, liikesalaisuuksista, kansallisista salaisuuksista, sotilaallisesta luottamuksellisesta tiedosta sekä valtioiden politiikkaan vaikuttamisesta (Lehto ja Limnéll, 2017). Kybervakoiluun käytettävä keino- ja taitovalikoima kehittyy jatkuvasti eikä aina ole varmuutta onko vakoilun takana valtio vai teollinen toimija. Esimerkiksi Kiinan valtioon yhdistettäviä valtiollisia kyber- ja hakkeriryhmiä on tunnistettu ainakin 87 ja Venäjän valtioon yhdistettäviä 20 (Kim, K., Alfouzan, F.A. ja Kim, H., 2021).

Kyberrikos palveluna (Cybercrime-as-a-service (Caas)) on kriittinen kehitys suunta kyberrikollisuudessa. Maanalaisten markkinapaikkojen ja räätälöityjen verkkosivustojen ohella kyberrikollisuusfoorumit ovat tärkeä kanava CaaS-toimittajille houkutella asiakkaita (Akyazi, van Eeten & Gañán, 2021). Internetin foorumeilla tarjotaan erilaisia as-a-service-toimintoja, mukaan lukien botnettien vuokraus palvelunestohyökkäyksiä (DDoS) varten (Santanna ym., 2015) ja

yleisten tietojenkalasteluhyökkäysten luomista (Hyslip, 2020). Huang ym. (2018) kehitti viitekehyksen, jossa on 24 hypoteettista arvoketjua eli eri palvelujen kohdistamista kyberhyökkäyksen luomiseksi. Tässä viitekehyksessä erotetaan ensisijaiset toiminnot, jotka edustavat kyberhyökkäyksen ydintä (esim. hyökkäyspalvelut) ja tukitoimintoja, jotka auttavat toimintaa (esim. toiminnan hämärtäminen palveluna). Eri toimintojen kohdistamisen kautta yksilöt voivat erikoistua yhteen taitoon, kaupallistaa sen ja tehdä yhteistyötä muiden kanssa suorittaakseen monimutkaisempia kyberrikollisuuteen liittyviä tehtäviä tai kyberrikollisuuden arvoketjuja. Tällaisen yhteistyön ja koordinoinnin kautta tuottavuus ja kannattavuus on lisääntynyt kyberrikollisuuden toimitusketjun eri tasoilla toimivien toimijoiden osalta tutkijoiden mukaan (Lusthaus 2018; Huang ym., 2018; Thomas ym., 2015; Paquet-Clouston & Garcia, 2022). Vuoden 2022 Euroopan unionin kyberturvallisuusviraston uhkamaisema raportissa onkin tunnistettu kahdeksan merkittävintä kyberuhkaa (Ifigeneia ym., 2022):

1. kiristysohjelmat
2. haittaohjelmat
3. käyttäjän manipulointi (eng. social engineering)
4. dataan kohdistuvat uhkaukset
5. Käytettävyyteen kohdistuvat uhkaukset: palvelunestohyökkäykset
6. käytettävyyttä koskevat uhat: internet uhat
7. disinformaatio - väärä tieto
8. hyökkäykset toimitusketjuihin.

Vihollisen tai kohdistetun hyökkäyksen taustalla olevan motivaation ymmärtäminen on tärkeää, koska se voi määrittää, mitä vastapuoli tavoittelee. Ymmärtääkseen kyberhyökkäysten taustalla olevia tekijöitä Gandhi ym. (2011) selvittivät, että kyberhyökkäykset liittyvät sosiaalisiin, poliittisiin, taloudellisiin ja kulttuurisiin konflikteihin ja he väittivät, että kyberhyökkäysten ehkäisyssä on otettava huomioon kyberhyökkääjien sosioteknologinen kehittyneisyys, tausta ja motivaatio. Organisaatio tasolla motiivien tunnistaminen ja tunteminen voi auttaa määrittämään ja priorisoimaan, mitä ja miten suojellaan. Sillä saadaan myös käsitys hyökkääjien aikeista ja todennäköisistä hyökkäysskenaarioista.

Ifigeneia ym. (2022) ovatkin tunnistaneet Euroopan unionin kyberturvallisuusviraston vuotuisessa raportissa neljä keskeisintä motivaatiota, jotka voidaan yhdistää edellä mainittuihin uhkatekijöihin. Tutkimuksessa huomattiin merkittävimpien uhkien kuuluvan yhden tai useamman motivaation alle melko tasaisesti. Ensimmäinen on monetisointi, johon luokitellaan kaikki ne kyberrikollisryhmien suorittamat toimet, joissa on taloudellinen motivaatio takana. Esimerkkinä kiristyshaittaohjelma, joka on tehty puhtaasti taloudellisen hyödyn vuoksi (Ifigeneia ym., 2022). Tästä on myös kehittynyt kannattava ja tuottava liiketoimintamalli (ransomware-as-a-service), jossa erikoistunut ryhmä tarjoaa tytäryhtiöille tai jopa yksittäisille henkilöille infrastruktuurin ja teknologian kiristyshaittaohjelmien käynnistämiseen (Paquet-Clouston & Garcia, 2022). Geopolitiikka ja vakoilu on toinen iso motivaation lähde, jossa tavoitteena on tiedon hankkiminen immateriaalioikeuksista sekä arkaluonteisista- ja turvaluokitelluista tiedoista.

Yleensä valtion tukemat ryhmittymät ovat näiden toimien takana. Kolmantena motivaatiotekijänä on geopolitiikkaan liittyvä häirintä eli mikä tahansa geopolitiikan nimissä tehty häiritsevä toiminta. Nämä toimet ovat myös useimmiten valtion tukemien ryhmittymien suorittamia. Ideologia on neljäs motivaatiotekijä, johon luokitellaan kaikki sellainen toiminta, jonka taustalla on ideologia (Ifigeneia ym., 2022).

4.3 Haasteita

Kyberturvallisuus on enemmän kuin yksittäinen askel. Sitä voisi kuvata jatkuvaksi prosessiksi, jossa on opittava, tarkkailtava, analysoitava, päätettävä ja reagoitava. Prosessia tulee soveltaa liiketoiminnan omaisuuteen ja toiminnan kestävyyteen kohdistuvien riskien yhteydessä (O'Connell, 2012). Lehto (2022) mainitsee kyberturvallisuuden ja –huoltovarmuuden turvaamisen sekä varmistamisen haasteena olevan toimintaympäristön hajanaisuus, muutosten nopeus ja vaikeasti ennustettava kehitys. Nykypäivän kyberympäristön kehitysvauhti on lujaa, johon organisaatioiden täytyy pystyä vastaaman (Lehto, 2022). Teollinen Internet of Things (IIot) -teknologia mahdollistaa yhä älykkäämpiä automatisoituja laitteita ja prosesseja, mutta samalla näiden hyödyntäminen lisää kyberhyökkäysten riskiä (Gonzalez-Wertz ym., 2019). Kyberavaruus ylittää myös kansalliset rajat. Teknologian toimitusketjut ja kriittiset riippuvuudet ovat yhä globaalimpia, kyberrikolliset ja valtiolliset toimijat toimivat ympäri maailmaa, tehokkaat teknologiayritykset vievät tuotteitaan ja asettavat standardinsa, ja kyberavaruutta ja internetiä ohjaavista säännöistä ja normeista päätetään kansainvälisillä foorumeilla. Kyberavaruus kehittyy myös jatkuvasti tekniikan ja ihmisten käyttötapojen muuttuessa, mikä vaatii omaksumaan ketterän ja reagoivan lähestymistavan (HM Goverment, United Kingdom, 2022).

Internetin ansiosta tietojen varastaminen etänä on helpottunut. Älypuhelinten lisääntyminen ja työntekijöiden taipumus liittää henkilökohtaiset laitteet työpaikan verkkoihin ja kerätä organisaatiolle kuuluvaa tietoa, on entisestään lisännyt tietoturva haasteita. Tämän seurauksena kyberhygieniastandardit ovat kohonneet erityisesti niille, joilla on pääsy elintärkeisiin tietoihin (O'Connell, 2012). Kumar ja Carley (2016) huomasivat tutkimuksessaan, että korkeampi korruptio ja suurempi internetin kaistanleveys suosii hyökkäysten aloittamista. He huomasivat myös, että maihin, joissa BKT asukasta kohden on suurempi ja joissa on parempi tieto- ja viestintäteknologian infrastruktuuri, kohdennetaan hyökkäyksiä useammin.

Gonzalez-Wertz ym. (2019) havaitsivat suurimpina haastein IIoT-tekniikan käyttöönottojen turvaamisessa olevan kyberturvallisuusosaajien puute sekä lisäksi nopeus ja mittakaava yhdistettynä datan kanssa. Tutkimus toteutettiin 700 teollisuus- ja energiaorganisaatiolle 18 maassa. Vaikka sähköyhtiöiden kyberturvallisuusohjelmat ovat keskimääräistä kypsemmät, kohtaavat ne myös suuria haasteita IIoT-teknologioiden kyberturvallisuudessa.

Riskianalyysit ovat olennainen kyberturvallisuuden menetelmä, koska sen avulla organisaatiot voivat käsitellä asioita heihin mahdollisesti vaikuttavien kyberuhkien kanssa, priorisoida omaisuuden puolustamista ja päättää mitä turvatoimenpiteitä tulisi toteuttaa. Rios Insua ym. (2021) huomasivat tutkimuksessaan nykyisten riskianalyysikehyksien tarjoavan nopean mutta alkeellisen uhkien kartoittamisen, sillä ne eivät ole riittävän muodollisia tai kattavia nykypäivänä. He kehittivät sen pohjalta uuden riskianalyysikehyksen kyberturvallisuudelle, joka tarjoaa kattavamman menetelmän ja yksityiskohtaisemman riskien mallinnuksen, mutta vaativamman ja resursseja vievän analyysin. Monissa organisaatioissa ja erityisesti kriittisen infrastruktuurin sektorilla panokset ovat niin suuret, että lisätyö ja resurssien lisääminen pitäisi olla vaivan arvoista. Lähes puolet ISACAn (2022) tutkimista yrityksistä tekevät vuosittaisella syklillä riskinarviointianalyysin, joka on liian pitkä väli. Se sallii liikaa aikaa merkittävien kyberympäristöpoikkeamien esiintymiselle, mikä voi mahdollisesti heikentää yrityksen vastatoimisuunnitelmia ja joustavuutta reagointiin. Organisaation johdolla onkin vastuu sovittaa sopiva aikaväli riskinarviointianalyysien toteuttamiselle, jotta se vastaa muutosympäristön nopeaan kehittymiseen, mutta on kuitenkin tehty laadukkaasti ja tarpeeksi kattavasti.

4.4 Modernin maailman tarpeet

Suomen kyberturvallisuusstrategiassa (Valtiovarainministeriö, 2019) on määritelty kolme strategista linjausta, jotka ovat kansainvälisen yhteistyön kehittäminen, kyberturvallisuuden johtaminen sekä kyberturvallisuuden osaamisen kehittäminen. Suomen keskeinen tavoite on jatkaa vahvaa kyberturvallisuus osaamista ja olla siinä kärkiosaajien joukossa. Nämä kolme strategista linjausta voidaan nähdä myös modernin maailman tarpeina.

On erityisen tärkeää saada kyberturvallisuus osaksi myös yrityksiä, jotka eivät tuota kyberturvallisuustuotteita, -palveluita ja ratkaisuja. Sillä näiden yritysten rooli tulee olemaan tulevaisuudessa yhä isommassa merkityksessä kyberturvallisuuden kokonaisuudessa. Kansallisen tason kyberturvallisuus rakentuu ja muodostuu viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten tiiviissä yhteistyössä, jossa jokainen voi vaikuttaa yhteiseen kyberturvallisuuteen (Valtiovarainministeriö, 2019). Kyberturvallisuus onkin tiimityöskentelyä monien osapuolten kesken. Teollisuuden ja kaupallisten sektorien on työskenneltävä yhdessä hallituksen kanssa jakaakseen ja levittääkseen informaatiota, vahvistaakseen kyberälykästä kyvykkyyttä ja ehkäistäkseen tulevaisuuden kyberkonfliktit (Borum ym., 2015).

Eri maiden kyberturvallisuusstrategioissa toistuu kolme keskeistä asiaa, jotka ovat kansainvälisen ja kansallisen yhteistyön merkityksen kasvu ja sen kehittämisen tarpeellisuus. Toisena asiana yksityisen ja julkisen sektorin yhteistyön ja tiedonjakamisen kehittäminen ja tehostaminen. Kolmantena asiana kyberturvallisuusjohtamisen heikkous tai sen puuttuminen. (Public Safety Canada, 2018;

ANSSI, 2015; Federal Ministry of the Interior and Community, Germany, 2021; Valtiovarainministeriö, 2019; Ministeries, Norway, 2019; Ministry of Economic Affairs and Communication, Estonia, 2019; Goverment Offices of Sweden, 2016; White House, United States, 2003). EU:n kyberturvallisuustrategian (EU-komissio, 2020) kolme kehittämiskohdetta puolestaan ovat 1. Häiriönsietokyky, teknologinen riippumattomuus ja johtajuus, 2. Operatiivisten valmiuksien kehittäminen uhkien ehkäisemiseksi, torjumiseksi ja niihin vastaamiseksi ja 3. Maailmanlaajuisen ja avoimen kybertoimintaympäristön edistäminen yhteistyötä lisäämällä.

Uhkatoimijoihin liittyvien trendien, motivaatioiden ja kohteiden ymmärtäminen auttaa merkittävästi kyberturvallisuuden puolustus- ja lieventämisstrategioiden suunnittelussa (Ifigeneia ym., 2022). Huang ym. (2018) esittävät kahta strategiaa vastaamaan tehokkaammin kyberhyökkäyksiä vastaan. Ensimmäisenä pimeän puolen kriittisten hallintapisteiden tunnistaminen ja vastuiden jakaminen eri toimijoille yhteistyön tehostamiseksi. Havaitsemalla kyberrikollisuuden ekosysteemin tärkeitä kontrollipisteitä, jotka ohjaavat kyberuhkien lisäarvopolkuja ja joista toimintaa hallinnoidaan, pystytään ymmärtämään paremmin taustalla olevaa taloutta, verkkorikollisuutta ja toimijoiden profiileita. Tällaisen ekosysteemikehyksen muodostaminen auttaisi lainvalvojia keräämään kriittisiä todisteita kyberrikollisten tuomitsemiseksi ja iskemään kyberrikollisuuden ytimeen. Toisena strategiana on vastuiden jakaminen toimijoille sekä yhteistyön syventäminen iskeäkseen kyberuhkien toimitusketjuun. Kyberturvallisuuden jättäminen pelkästään yksilöiden ja yritysten vastuulle ei ole toimivaa, vaan toimet vaativat sekä kansallista että kansainvälistä politiikkaa. Politiikalla on erityinen rooli kyberturvallisuuteen liittyvien henkilöstömarkkinoiden puutteiden korjaamisessa, millä tarkoitetaan ammattitaitoisten henkilöiden houkuttelua ja niiden kannustimien poistamista, jotka ajavat kyberrikollisuuteen.

Lähes jokainen kriittinen järjestelmä nojaa informaatio- ja kommunikaatioteknologiaan. Borum ym. (2015) huomauttavatkin, että kyberriskit jatkavat lisääntymistään, jolloin organisaatioiden sekä julkisella että yksityisellä sektorilla on toimittava puolustaakseen ja suojatakseen tärkeitä informaatiovarojaan. Teknologiaan, palomuureihin ja tunkeutumisen tunnistamisjärjestelmiin investoiminen on paikallaan, muttei itsessään riittävää (Borum ym., 2015). Työntekijöiden kyberturvallisuuden koulutuksella lisätään tietoisuutta sekä parannetaan turvatoimien tehokkuutta (Gonzalez-Wertz ym., 2019). Kuten monien muidenkin monimutkaisten turvallisuusuhkien kanssa, älykkyys on avain asemassa. Kyberälykkyys korostaa ennaltaehkäisyä ja ennakointia kyberturvallisuustoimien suhteen (Borum ym., 2015).

Gonzalez-Wertz ym. (2019) suosittelevat kaksiosaista lähestymistapaa sulkemaan kyberturvallisuuden aukkoa kansainvälisessä kentässä. Ensimmäisenä organisaatioiden tulisi keskittyä vahvan IIot-kyberturvallisuuden perustan rakentamiseen ja perustavanlaatuisen kyberhygienian luomiseen. Kyberhygienia tarkoittaa peruskyberkäytäntöjä, joita organisaatiot käyttävät kyberturvallisuusohjelmissaan ja –strategioissaan. Käytännöt koskettavat organisaatiota, tietokoneiden käyttäjiä sekä muita laitteita, jotka ovat avainasemassa

verkkoturvallisuuden ylläpidossa ja parantamisessa. Kuten fyysinen hygienia, kyberhygienia on säännöllistä ja rutiininomaista, jolla estetään luonnollista rappeutumista ja suojaudutaan uhkilta. Erilaisten sairauksien, kuten myös tietokonevirusten ja uhkien leviäminen on aivan liian monimutkaista ja tarpeetonta useimmille käyttäjille. Tärkeintä on olla tietoinen hygienian tarpeellisuudesta ja osata toteuttaa hygieniakäytäntöjä niin sairauksien estämisessä kuin kyberympäristössä (Cain ym., 2018; Gonzalez-Wertz ym., 2019; Vishwanath ym., 2020). Kun kyberturvallisuuden perusta on muodostettu, organisaatiot voivat toisena lähestymistapana keskittyä kehittyneempien tietoturvaominaisuuksien kehittämiseen tekoälyn ja automaation avulla. Näiden lähestymistapojen avulla varmistetaan toimintojen ja palveluiden jatkuvuus (Gonzalez-Wertz ym., 2019).

Peslak ja Hunsinger (2019) tutkivat mitä taitoja työnantajat etsivät ja odottavat työnhakijoilta. Tutkimuksesta kävi ilmi, että kyberturvallisuus on alana hyvin monipuolinen ja siten erilaisia taitoja tarvitaan, vaikkakin lähtökohtaisesti yleiset tekniset taidot olivat välttämättömiä lähes jokaisessa työnhakuilmoituksessa. Yhtenäisiä taitoja hakijoilta ei odoteta, sillä kuten todettu kyberturvallisuuden alalla on tarvetta monipuolisille ja erityistaitoja omaaville ammattilaisille. Työnantajat arvostivat vuosien työkokemusta sekä tutkintoa, ja ne ovatkin suurimpia organisaatioiden tarpeita nykyään, kun tarvittavista osaajista on pulaa. ISACAn (2022) (Information Systems Audit and Control Association) kyberturvallisuudentila tutkimuksesta kuitenkin selviää, että työvoimapula ei ole häviämässä vaan jopa pahenemassa. Työnhakijat pitävät joustavuutta avainasemassa, jolloin yritysten täytyy mahdollistaa etätyö sekä joustavammat työajat. Osaajapula on myös pakottanut yrityksiä laskemaan vaatimuksia työnhaussa, kuten tutkintovaatimuksen edellytystä, jolloin työntekijöiden koulutus jää myös osittain yritysten harteille.

ISACAn (2022) vuosittaisessa globaalissa kyberturvallisuuden tila tutkimuksessa tulokset osoittivat yritysten kamppailevan edelleen osaavasta henkilöstöstä kyberuhkien torjumiseksi. Jopa 60 prosenttia kyselyyn vastanneista yrityksistä kokee vaikeuksia pätevien kyberturvallisuuden ammattilaisten pitämisessä sekä 63 prosentilla vastaajista on kyberturvallisuuteen liittyviä työpaikkoja täyttämättä. Vastaajien mukaan viisi tärkeintä turvallisuus- ja kybertaitoa, joita organisaation kyber- ja tietoturva-ammattilaiset tarvitsevat nykypäivänä ovat:

- Pilvilaskenta
- Datan suojelu
- Identiteetin ja pääsyn hallinta (IAM)
- Poikkeamiin vastaaminen
- DevSecOps

Viisi tärkeintä pehmeää taitoa (eng. soft skills), joita organisaation kyber- ja tietoturva-ammattilaiset tarvitsevat nykypäivänä ovat:

- Viestintä (kuuntelu- ja puhumistaito)
- Kriittinen ajattelu
- Ongelmanratkaisu

- Ryhmätyöskentely ja yhteistyö
- Silmää yksityiskohdille

Yhtenä nostona voisi ottaa rehellisyyden taidon, sillä vain 16 prosenttia vastaajista valitsi rehellisyyden yhdeksi tärkeimmistä organisaatiossaan tarvittavista turvallisuustaidoista, mikä on yllättävä havainto, kun huomioidaan sen merkitys suojeluammateissa ja etenkin kyberturvallisuudessa (ISACA, 2022).

Kuten jo aikaisemmin on mainittu, kyberturvallisuusalalla on valtava osaajapula. Liikenne- ja viestintäministeriölle tehdyssä kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimuksella (Lehto, 2022) selvitettiin laaja-alaisesti osaamisen määrällinen ja laadullinen kehittäminen Suomessa. Osaajapula on valtava eikä nykyisillä resursseilla pystytä kattamaan kaikkia rekrytointitarpeita. Selvityksen mukaan osaajapulaan tarvitaan julkista panostusta vuosittain arviolta noin 8–9 miljoonaa euroa vuodessa.

ISACAn (2022) tutkimuksesta selviää globaalisti yliopistosta vastavalmistuneilla olevan osaamispuutteita etenkin pehmeissä taidoissa (esim. joustavuudessa ja johtajuudessa), tietoturva-arviointien toteuttamisessa, verkkotoiminnoissa (esim. konfiguroinnissa ja suorituskyvyn seurannassa), järjestelmän kovettamisessa eli haavoittuvuuksien pinta-alan vähentämisessä sekä verkon arkkitehtuuriin, osoitteisiin ja verkkokomponentteihin liittyvissä asioissa.

Kyberresilienssi viittaa kykyyn, jossa päästään haluttuun lopputulokseen jatkuvasti haitallisista kybertapahtumista huolimatta (Björck ym., 2015). Roege ym. (2017) ovat määritelleet kyberturvallisuus resilienssin ominaisuuksiksi muun muassa vikaturvallisuuden, kriittiset toiminnot, nopean toipumisen, sopeutumisen ja oppimisen. Yhteiskunnan turvallisuuden ja resilienssin parantamiseksi löytyy myös ISO standardi, sillä ISO standardi 22316:2017 (International Organization for Standardization, 2017) tarjoaa ohjeita kaiken kokoisten organisaatioiden resilienssin parantamiseen, eikä se edistä vain yhdenmukaista lähestymistapaa kaikkiin organisaatioihin, koska yksilölliset tavoitteet ja aloitteet räätälöidään yksittäisen organisaation tarpeisiin.

Kyberturvallisuus- ja laajemman resilienssin kehittämistoimet tulisi olla Roege ym. (2017) mielestä integroitu paremmin johtajien, sidosryhmien ja asiantuntijoiden avulla. Etenkin kriittisen infrastruktuurin toiminnallisiin näkökohtiin, niin inhimillisiin kuin fyysisiin, tietoalan ammattilaiset sekä kyberturvallisuustoimijat täytyisi saada osallistumaan aktiivisesti liiketoiminta- ja valmiussuunniteluun. Kyberturvallisuudesta vastaavien tulisi resilienssiajattelun avulla miettiä uusia lähestymistapoja kyberriskien hallintaan organisaatiotasolla. Heidän osallistumisensa yritystason analyyseihin auttaa ymmärtämään yleisiä liiketoimintaprosesseja ja haavoittuvuuksia, jolloin on mahdollista tunnistaa kybertoimialueen toimenpiteitä, jotka tukevat kestävämpiä yritysprosesseja ja edistävät kansallista resilienssiä (Roege ym., 2017).

Kyberrikollisuudesta ilmoittaminen poliisille, tekijän löytäminen ja tuomitseminen on vielä haasteellista. Kyberrikosten ilmoittamisesta poliisille on tutkittu van de Weijer ym. (2020) toimesta. Tutkimuksen mukaan ne, jotka pelkäävät joutua enemmän kyberrikollisuuden uhriksi ja joilla on myönteisempi asenne poliisia kohtaan, ilmoittavat todennäköisemmin verkkorikollisuuden uhriksi

joutumisesta. Myös aiemmin verkkorikoksesta poliisille ilmoittaneilla oli enemmän aikomuksia ilmoittaa uhriksi joutumisesta poliisille. Kuitenkin lähes puolet uhreista oli tyytymättömiä tapaan, jolla poliisi käsitteli heidän ilmoituksiaan, lähinnä siksi, että ongelmaa ei ratkaistu ja koska poliisi reagoi välinpitämättömästi. Yleisin motiivi olla ilmoittamatta poliisille rikoksesta, oli uhrien näkemys, että poliisi ei kuitenkaan tee asialle mitään. Van de Weijer ym. ehdottavatkin ratkaisuksi ongelmaan sitä, että poliisin tulisi aktiivisesti työskennellä yhdessä muiden asiaankuuluvien julkisten ja yksityisten organisaatioiden, kuten pankkien, luottokorttiyhtiöiden ja verkkokauppojen kanssa. He perustelevat ratkaisuaan sillä, että useimmiten verkkorikosten uhrit ilmoittavat uhriksi joutumisesta useammin tällaisille organisaatioille tai järjestöille poliisin sijaan. Tällä tavoin poliisi voisi saada paremman käsityksen verkkorikosten yleisyydestä ja suuntauksista. Digi- ja väestötietoviraston digitaitoraportissa (2022) tarkasteltiin Suomen tilannetta, josta selvisi suomalaisten kaipaavan apua verkkorikoksista ilmoittamiseen ja lähes puolet tutkimukseen vastanneista haluaisikin oppia enemmän siitä, miten toimia, jos joutuu verkkorikoksen uhriksi.

5 KYBERTURVALLISUUSOSAAMISEN JOHTAMINEN JA HALLINTA

Kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista (Lehto, 2022). Craigen ym. (2014) määrittelevät käsitteen kyberturvallisuus resurssien, prosessien ja rakenteiden organisoinniksi ja kokoelmaksi, jonka tehtävänä on suojata kyberavaruutta ja kyberavaruuteen liittyviä järjestelmiä kyberrikollisuudelta. Sekä Lehto että Craigen ym. viittaavat kirjoituksissaan tietynlaisten prosessien johtamiseen ja hallitsemiseen. Hyvin vastaavanlaisesti prosessien hallintaa käsittelee tiedolla johtaminen, ja toisaalta myös osaamisen hallinnan tutkimus.

Alavi & Leidner (2001) esittävät tiedolla johtamisen käsittävän erillään olevat mutta keskenään riippuvaiset tiedon luomisen ja ylläpitämisen prosessit, tiedon varastoinnin ja haun prosessit sekä tiedon jakamisen ja tiedon soveltamisen prosessit. Samoin Berion & Harzallahin (2005) osaamisen hallinnan neljä prosessia (Kuvio 7) tunnistaa samantapaisia piirteitä osaamisen tunnistamisen, arvioinnin ja käyttämisen suhteen, joista Lehto (2022) kirjoittaa kyberturvallisuuden luomisen ja hallitsemisen suhteen.

Boyce ym. (2011) kirjoittavat, että ihmisen rooli järjestelmähaavoittuvuuksien luomisessa ja selättämisessä on identifioitava eri järjestelmien kohdalla järjestelmän käytön vaatimuksiin perustuen. Nämä vaatimukset sisältävät ajan, jossa tehtävä valmistuu, vaaditun tarkkuuden ja luotettavuustason, minkä tahansa sääntöjen ja ohjeiden ohjaaman ihmisen osallistumisen, teknologian saavutettavuuden, tarvittavan informaation, käyttäjän tiedon ja taidon sekä päätöksen tekoon liittyvät vaatimukset. Tehokas ihmisen suorituskyky on kriittistä onnistuneiden kyberturvallisuuden prosessien, fasiliteettien ja varustelun käyttöönoton ja toiminnan suhteen (Boyce ym., 2011).

Kun taas ajatellaan kyvykkyyksien olevan niitä mitattavissa olevia henkilön piirteitä, joita tarvitaan tietyssä työtilanteessa tietyn työtehtävän suorittamiseen (Klendauer ym., 2012) ja sitä, minkä takia kyvykkyyksien tehokas hallinta on läheisesti yhteydessä erinomaiseen suorituskykyyn, sekä kuinka kyvykkyydet

edustavat tietoa, taitoa ja käyttäytymistä, jotka kontribuoivat yrityksen menestykseen (Prahalad & Hamel, 2003), voidaan tämän tutkimuksen kannalta todeta kyberturvallisuuden olevan sekä yksittäisten ihmisten että organisaatioiden tietoisuutta ja kyvykkyyttä toimia kyberturvallisella tavalla. Näistä asioista mm. Lehto (2022) puhuu toimenpiteinä, joilla sekä suojaudutaan että toteutetaan vastatoimenpiteitä kyberhyökkäyksiä vastaan.

Täten kyberturvallisuus ja kyberturvallisuusosaaminen linkittyy vahvasti tiedolla johtamisen sekä osaamisen hallinnan prosesseihin, kyberturvallisuuden lähinnä luoden kontekstin johdettaville prosesseille. Myös Wang ja Wang (2019) huomaavat, että tiedolla johtaminen on merkittävässä roolissa kyberturvallisuudessa. Kyberturvallisuusosaamisen kattaessa sekä tietoa että taitoa, on tutkimuksen kannalta järkevää tarkastella kyberturvallisuusosaamisen johtamisen ja hallinnan prosesseja yhdessä hyödyntäen juuri tiedolla johtamisen ja osaamisen hallinnan vuorovaikuttamiseen keskittyvää teoreettista mallia. Seuraava luku esittelee tämän tutkimuksen kannalta oleellisen teoreettisen viitekehyksen ja mallin, joka onnistuneesti tunnistaa tiedolla johtamisen ja osaamisen hallinnan läheisen yhteyden.

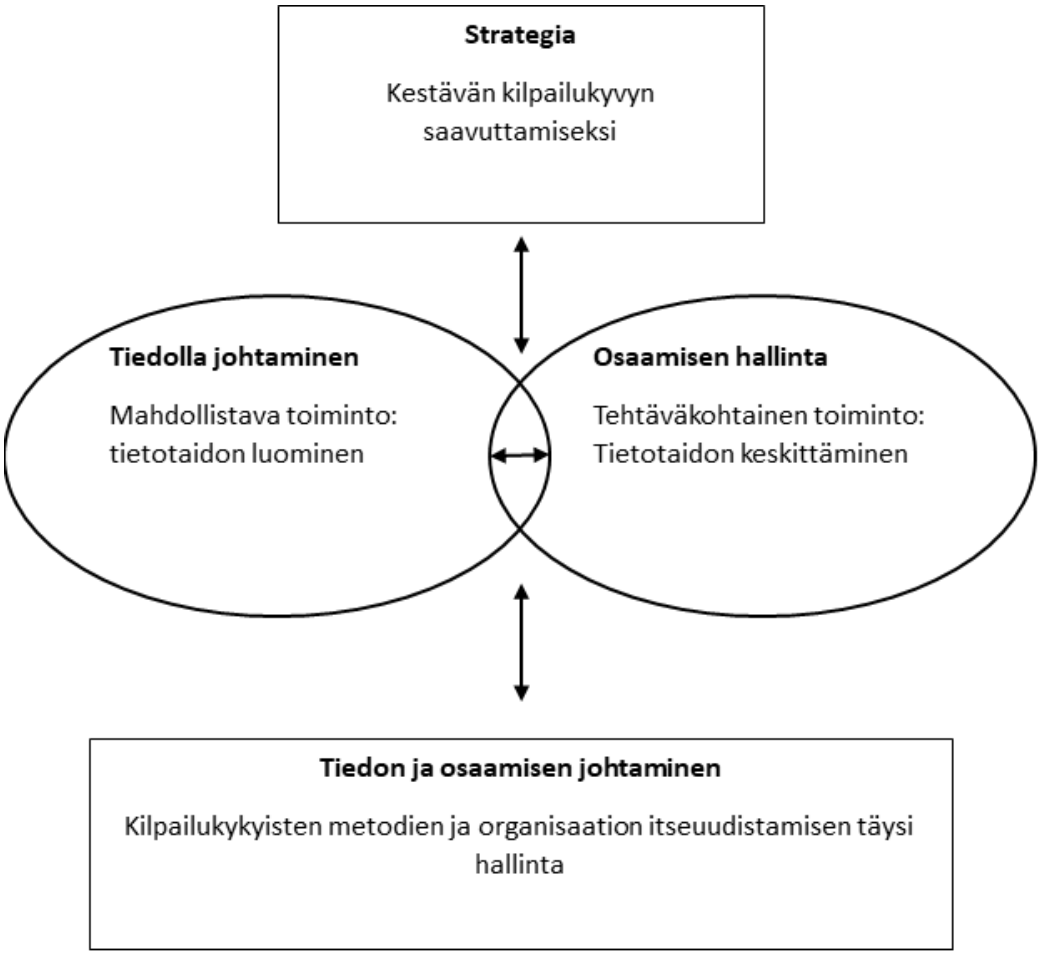
6 TUTKIMUSAINEISTO JA -MENETELMÄ

6.1 Tutkimuksen teoreettinen viitekehys

Tässä alaluvussa esitellään edellä esitellyn teorian pohjalta muodostettu teoreettinen malli, jonka avulla pyritään mallintamaan teoreettisesti osaamisen hallinnan ja tiedolla johtamisen prosessia. Mallin pohjana hyödynnetään Hongin ja Ståhlen (2005) mallia (Kuvio 8), jossa tiedolla johtaminen ja osaamisen hallinta on sisällytetty yhteen malliin.

Hong ja Ståhle (2005) kirjoittavat, että kiinnostus niin tietoa, kuin osaamista kohtaan on ollut kasvussa viimeaikaisessa tutkimuskirjallisuudessa sekä organisaatioiden toiminnassa. Erottamaton ja yhteinen suhde tiedon ja osaamisen välillä sekä niiden merkittävät seuraukset strategiseen johtamiseen ovat puhuttaneet tutkijoita. Kuitenkin käsitteellinen määritelmä ja selvennys tiedon ja osaamisen hallinnasta sekä näiden käsitteiden eroavaisuuksista ja suhteesta uupuu (Hong & Ståhle, 2005).

Tiedolla johtaminen ja osaamisen hallinta jakavat yhteisen piirteen kehityksellisen kaaren muodossa. Molemmat käsitteet ovat käyneet läpi saman muutoksen siirtäessään keskittymisensä ja kiinnostuksensa dokumentoinnista ja identifioinnista integraatioon ja vaikutukseen ja lopulta sekä tiedon että osaamisen tuottamiseen. Tuottamisprosessissa sekä tiedolla johtaminen että osaamisen hallinta ovat näyttäneet samankaltaisia piirteitä. Näihin yhtäläisyyksiin liittyen Hong ja Ståhle (2005) esittävät artikkelissaan uuden lähestymistavan, jossa sekä tiedolla johtamista että osaamisen hallintaa ja niiden välistä suhdetta kuvataan termillä tiedon ja osaamisen hallinta/johtaminen (eng. Knowledge and competence management). Tämä näkökulma yhdistää molempien, sekä tiedolla johtamisen, että osaamisen hallinnan ponnistelut, lisäten kokonaisvaltaisesti koko organisaation kyvykkyyttä tarkoituksenaan parantaa systemaattista tehokkuutta organisaation strategian mukaisesti.



KUVIO 8 Tiedon ja osaamisen johtamisen malli. (Hong & Ståhle, 2005)

Tiedon ja osaamisen johtaminen voitaisiin nähdä teknologisena ja sosiaalisena järjestelmänä, jonka avulla kilpailukykyisten metodien ja organisaation itseuudistumista pyritään hallitsemaan. Sekä tiedolla johtaminen että osaamisen hallinta käsittelevät organisaation tietotaitoa omalta kantiltaan, kuitenkin mennen limittäin vuorovaikutuksen myötä (Hong & Ståhle, 2005).

Mallin (Kuvio 8) mukaisesti organisaation strategia osoittaa toiminnalle rajat ja tavoitteet, jonka mukaan tiedolla johtamisen periaatteita sovelletaan organisaation sisäisen tietotaidon kehittämiseksi. Osaamisen hallinnan periaatteita puolestaan hyödynnetään tehtäväkohtaisemmin suorittamaan tehtäviä, kohdentaen luotua tietotaitoa.

Tältä osin voidaan huomata paljon yhtäläisyyksiä Berion ja Harzallahin (2005) osaamisen hallinnan malliin (Kuvio 7), jossa osaamisen hankinta, tunnistaminen ja arviointi mahdollistavat osaamisen käytön. Samaan tapaan vuorovaikutus yhdistää nämä kaksi osaa toisiinsa luoden tiedon ja osaamisen johtamisen kokonaisuuden. Samalla tapaa Wiigin (1993) sekä Meyerin ja Zackin (1996)

tiedolla johtamisen syklit noudattavat samantapaista kaavaa, jossa tietoa ensin hankintaan ja rakennetaan, sittemmin säilötään, jaetaan ja lopulta käytetään osana organisaation prosesseja. Yhtä lailla Choon (2002) malli tunnistaa samoja piirteitä. Tämä tukee myös Hongin ja Ståhlen ajatusta näiden prosessien yhdistämisestä ja "tietotaidon" johtamisesta.

Kyberturvallisuuden näkökulmasta edellä esitellyn mallin (Kuvio 7) keskeisiin käsitteisiin voidaan sisällyttää tiedolla johtamisen alle esimerkiksi kyberturvallisen toiminnan mahdollistavat jatkuvasti päivitettävät tietoturvallisuusohjeet ja määräykset sekä muun kyberturvallisuutta koskevan informaation sekä organisaation sisäisen perehdytyksen ja koulutuksen aiheisiin, toisin sanoen informaation jakamisen, mikäli peilaamme prosessia Meyerin & Zackin (1996) tiedolla johtamisen sykliin (Kuvio 4). Osaamisen hallinnan puolelle luonnollisesti sijoittuu edellä mainitun tietotaidon soveltaminen ja kyberturvallisesti toimiminen kaikkine prosesseineen. Näiden osa-alueiden välinen vuorovaikutus mahdollistaa molempien osa-alueiden kehityksen ja tästä seuraten kilpailukykyisten metodien syntymisen ja käyttämisen sekä organisaation jatkuvan uudistumisen ja kehityksen.

Tutkimuksessa perehdytään erityisesti näihin vuorovaikuttaviin prosesseihin niin tiedolla johtamisen, osaamisen hallinnan kuin kokonaiskuvan saralla, ja tutkimuksesta saatua aineistoa verrataan lopulta yllä olevaan malliin selvittäen, kuinka tiedolla johtamisen ja osaamisen hallinnan prosessit käytännössä toteutuvat kohdeorganisaatioissa.

6.2 Aineisto ja menetelmä

Tutkimus toteutetaan laadullisena tutkimuksena kohdeorganisaatioiden avainhenkilöitä haastatellen. Haastattelut toteutettiin puolistrukturoituina yksilöhaastatteluina, mikä mahdollisti haastatteluihin tietyn joustavuuden tarkentaa tai lisätä mieleen tulevia asioita osaksi haastattelua, mikä osaltaan mahdollistaa laadukkaan tutkimusaineiston keräämisen, jossa haastattelurunko ei estä organisaatioiden välisien eroavaisuuksien esille tulemista. Näin tutkimus pystyy ketterästi vastaamaan asetettuihin tutkimuskysymyksiin organisaatiosta riippumatta.

Syy laadullisen tutkimuksen tekemiseen puolistrukturoidun yksilöhaastattelun muodossa piilee myös tutkittavien asioiden luonteessa. Määrällinen tutkimus soveltuu hyvin faktuaalisen tiedon selvittämiseen, mutta kun tietoa etsitään jonkun kokemuksista tai näkökulmista eikä data ole laskettavissa tai mitattavissa laadullinen tutkimus on sopivampi metodi. Laadullisten tutkimusmenetelmien avulla voidaan etsiä näkökulmia valittuun aiheeseen, kokemuksiin, taustatietoihin tai instituution perspektiiviin (Hammarberg, Kirkman & Lacey, 2016). Tutkimuskysymysten luonteen takia niihin saatavat vastaukset eivät ole myöskään suoraan mitattavissa, ja vaativat tarkempaa tapauskohtaista analyysiä, jotta organisaation toimintaa voidaan ymmärtää, joten laadulliselle tutkimukselle on täydet perusteet.

On kuitenkin huomattava, että tutkimusmenetelmän ketteryys voi luoda vaihtelevuutta vastausten välille haastatteluita vertaillessa, minkä takia tarkka yleistäminen tai tulosten analysoiminen tarkoiksi tilastoiksi voi olla hankalaa. Kuitenkin asetettujen tutkimuskysymysten ja tutkimuksen laadun puitteissa mahdollisimman kattava osaamisen hallinnan ilmiön tutkiminen organisaatioiden prosessien ja strategian yhteydessä on perusteltua.

Tutkimuksen aineisto kerättiin haastatteluilla, haastatteluja varten ennalta määriteltyä haastattelurunkoa (Liite 1) hyödyntäen. Puolistrukturoidun haastattelun myötä haastatteluissa ilmeni myös jossain määrin vapaata pohdintaa ja haastateltava- sekä organisaatiokohtaisia erovaisuuksia.

Haastatteluita varten mietittiin ja kerättiin lista mahdollisista kohdeorganisaatioista. Organisaatioita kertyi listaukseen yhteensä 25 kappaletta, joista kaikkia lähestyttiin haastattelukutsun muodossa (Liite 1). Haastatteluihin osallistui lopulta ja haastatteluja tehtiin yhteensä yhdeksän kappaletta maaliskuun ja heinäkuun välillä vuonna 2023. Haastattelut olivat kestoltaan noin 40–60 minuuttia. Haastateltaviin organisaatioihin valikoitui lopulta Jyväskylän Yliopisto, Airbus, Decens, Huld, Kela, Keski-Suomenliitto, KPMG, Millog ja Telia. Näistä organisaatioista haastateltaviksi määräytyi henkilöitä seuraavista henkilörooleista:

1. Tietoturvapäällikkö
2. Tietoturvayksikön päällikkö
3. Johtaja, Space and Defence
4. Kehittämisjohtaja
5. Johtaja, teknologiakonsultointi
6. Tekninen päällikkö, johtamisjärjestelmät ja kyber
7. Pääarkkitehti, verkot ja infrastruktuuri
8. Kryptografia-arkkitehti, turvallisuus

Haastatteluissa kerätty materiaali litteroitiin laadukkaan analysoinnin helpottamiseksi. Litteroituna materiaalia kertyi 99 sivua. Anonymiteetin varmistamiseksi henkilörooleja ja organisaatioita ei yhdistetä keskenään, eikä haastattelumateriaaleihin viitatessa ole myöskään yhdistettävissä mistä organisaatiosta on kyse. Tämä varmistetaan siten, että haastattelumateriaalin yhteydessä viitataan haastateltaviin henkilöihin, jotka ovat satunnaisesti numeroitu 1–9 välillä.

7 TULOKSET

Tässä luvussa esitellään tutkimuksen tulokset. Tuloksia tarkastellaan neljässä alaluvussa aihealueittain, jotka on muodostettu tutkimuskysymysten ja haastattelurungon perusteella. Haastattelurunko koostui niin ikään kolmesta osiosta. Ensimmäinen osio käsitteli kyberturvallisuuden, tiedolla johtamisen ja osaamisen hallinnan käsitteitä. Toinen osio otti kyberturvallisuusosaamisen rinnalle mukaan organisaation strategian ja tavoitteen, ja pyrki selvittämään näiden tekijöiden välistä suhdetta. Kolmas osio ja aihealue keskittyi kyberturvallisuusosaamisen hallinnan ja johtamisen prosesseihin eli siihen, kuinka tiedolla johtamisen ja osaamisen hallinnan asioita toteutetaan kyberturvallisuuden kohdalla kohdeorganisaatiossa. Neljännessä alaluvussa pohditaan tiedon ja osaamisen välistä suhdetta ja vuorovaikutusta Hongin ja Ståhlen (2005) mallin mukaisesti.

7.1 Kyberturvallisuus, tiedolla johtaminen ja osaamisen hallinta organisaatioissa

Tämä alaluku käsittelee haastattelurungon mukaisesti kyberturvallisuutta, tiedolla johtamista sekä osaamisen hallintaa käsitteiden valossa kohdeorganisaatioissa. Haastateltavia pyydettiin haastattelun ensimmäisessä osiossa määrittelemään edellä mainitut käsitteet juuri siltä kannalta, miten he ymmärsivät ne omissa organisaatioissaan. Käsitteiden määrittely haastattelun alussa johdatteli haastateltavan haastattelun aihealueeseen kiinni, ja toisaalta luo pohjan sille, että myös seuraavat osiot haastattelusta on järkevä toteuttaa. Haastattelukysymykset olivat seuraavanlaiset:

Mitä kyberturvallisuus sinulle tarkoittaa? Millaisia asioita tai kokonaisuuksia se mielestäsi sisältää?

Mitä koet osaamisen hallinnan ja tiedolla johtamisen olevan? Miten määrittelisit ne?

Miten määrittelisit kyberturvallisuusosaamisen hallinnan ja johtamisen? Poikkeaako se muusta osaamisesta jollain tapaa?

Näillä kysymyksillä pyrittiin johdattelemaan haastateltavia aiheeseen, ja toisaalta luomaan pohjaa myös tulevien haastattelukysymysten vastauksille. Toisaalta on myös mielenkiintoista selvittää, kuinka käsitteiden merkitys eroaa käytännön ja teorian tasoilla.

7.1.1 Kyberturvallisuus käsitteenä

Kyberturvallisuuden määritteleminen koettiin haastateltavien keskuudessa usein haastavana sen laajuuden vuoksi. Samoin haastateltavat tunnistavat, että käsite kyberturvallisuus voidaan ymmärtää eri tavoilla ja sen voidaan tulkita käsittävän eri asioita. Useammat haastateltavat huomauttivat, että usein kyberturvallisuudella tarkoitetaan hyvin samoja asioita, mitä tietoturvallisuudellakin. Yksi yhdistävä tekijä oli se, että ympäristön huomattiin olevan jollain tapaa älykäs tai sähköinen. Myös käsitteen turvallisuus määrittäminen saattoi olla haastavaa.

> Nojoo nämä on nämä käsiteasiat sillein vähä haastavia, että noin niinku yleiskielessä ja yleisesti, kun puhutaan kyberturvallisuudesta, niin sillä tarkotetaan, voisi sanoa lähes kaikkea samaa mitä tietoturvallisuudella. (Haastateltava 9)

> No sehän on tämmöinen niinku hauska termi, että sen voi jokainen vähän määritellä eri tavalla. (Haastateltava 4)

> No jaa, sillohan kun mä aloitin nää hommat niin puhuttiin tietoturvallisuudesta… …jos puhutaan kyberturvallisuudesta niin sillo on väkisin, mun mielestä ollaan niinku sähköisessä maailmassa, IT-maailmassa, ja sitten oikeastihan se on, niinku mun mielestä, se on sähköisen maailman tietoturvallisuutta. Näin niinku tiivistetysti. (Haastateltava 6)

> Sehän on aika laaja käsite kyllä loppujen lopuksi... ...jollain tapaa mä nyt ymmärrän sen semmoiseksi tietoturvallisuuden tai ylipäänsä turvallisuuden osaksi, missä niinku jonkun sortin älystä tai jostain muusta on kyse, että tota se nyt ei ole välttämättä sitten semmoista niinku aitojen rakentamista, mutta ehkä jos siihen aitaan liittyy jotain älykästä, niin sitten se voi olla kyberturvallisuutta, mutta se turvallisuus on kuitenkin semmoinen kokonaisuus, niin en mä koskaan osannut oikein kuvata sitä silleen niinku kovin hyvin. (Haastateltava 3)

Ero perinteiseen tietoturvallisuuteen nähtiin pitkälti siinä, kuinka kyberturvallisuuden koettiin käsittävän myös erilaisten tärkeiden infrastruktuurien suojaamisen. Näin ollen kyberturvallisuus koettiin ehkä tietoturvallisuutta laajemmaksi

käsitteeksi sen käsittäessä myös erilaisten järjestelmien ympärillä olevan teknisen ympäristön ja jopa maan laajuisen infrastruktuurin.

> Mä näen sen, että se on niinku se on sitä sen infrastruktuurin turvaamista. (Haastateltava 8)

> Me puhutaan digiturvallisuudesta ja sen osana on kyberturvallisuus. Ja siellä se sitten ehkä enemmänki rajautuu nimenomaan tälläseen vaikkapa johonkin infraan vaikuttamiseen... (Haastateltava 9)

> Nykyään, kun puhutaan paljon laaja-alaisestakin vaikuttamisesta niin niin tota, jos tietoturva nyt enemmän oli sitten sinne niinku sähköisiin järjestelmiin ja miksei nyt myöskin johonkin niin kun niinku paperilla oleviin dokumentteihin, niin tää kyber sitten niinku liittää siihen myöskin sitä ympäröivää maailmaa ja niitä ihmisiä ja sitä tekemistä. (Haastateltava 7)

Tämän lisäksi esiin nousi usein ajatus kyvykkyydestä suojautua erilaisia uhkia tai hyökkäyksiä vastaan eikä pelkästään järjestelmien tai infrastruktuurin kestävyyttä sellaisenaan. Sana kyvykkyys liittää ihmisen osaksi kyberturvallisuutta. Myös sanan kyvykkyys nouseminen esiin osana kyberturvallisuuden käsitteen määrittelyä antaa tälle tutkimukselle hyvät lähtökohdat.

> Teknistä kyvykkyyttä suojata yrityksen organisaation luottamuksellisia tietoja ja henkilötietoja, ja ennen kaikkea ja havaita erilaisia poikkeamia ja kykyä reagoida niihin. (Haastateltava 2)

> Sehän on tavallaan sitä karkuun juoksemista elikkä tota pyritään olemaan selvillä missä kunnossa oma verkko ja omat serverit ja laitteet on, ja tota mikä on niinku tilannekuva. (Haastateltava 5)

> Tähän kyber-teemaan tavallaan liittyy niinkun kaks tämmöistä niinkun isompaa asiaa. Toinen on nimenomaan se osuus, jota nyt enemmän itse edustan, elikkä ne palvelut ja ne tavallaan niinkun kyvykkyydet, mitä me niinkun organisaationa tuotetaan tuonne asiakkaalle. (Haastateltava 7)

7.1.2 Tiedolla johtaminen ja osaamisen hallinta käsitteenä

Haastateltavia pyydettiin samaan tapaan, kuin kyberturvallisuutta, määrittelemään tutkimuksen kannalta oleellisia ilmiöitä, tiedolla johtamista ja osaamisen hallintaa. Tarkoituksena oli johdatella haastateltavia aiheeseen ja herätellä ajatuksia valmiiksi tulevia haastattelukysymyksiä varten. Toki samalla pääsemme vertaamaan, kuinka käsitteiden määritelmät mahdollisesti poikkeavat käytännön ja teorian välillä.

Haastateltavat tunnistivat usein tiedolla johtamisen olevan yleisesti sitä, että organisaation toimintaa ohjataan niin, että päätökset perustuvat johonkin tietoon, ja nimenomaan johonkin "dataan", jota on pystytty keräämään ja, jonka avulla tehtyjä voidaan tukea faktaan. Haastateltavat huomasivat myös yleisesti sen, että pelkästään tiedon olemassa oleminen tai sen kerääminen ei riitä. Tietoa tai dataa on pystyttävä analysoimaan, jotta siitä voitaisiin johtaa päätöksiä organisaation toiminnan tueksi. Myös yksittäisiä viittauksia ilmeni siihen, kuinka tieto ei aina välttämättä ole dataa tai numeroita, vaan tietolähteenä voidaan pitää myös asiantuntijuutta ja ihmisen omistamaa tietoa, jota ei aina välttämättä ole kirjattuna mihinkään. Haastateltavat tunnistivat myös vaihtoehtoiseksi tavaksi niin sanotun Mutu-johtamisen tai fiiliksellä johtamisen, mikä osoittaa vastakohdan kautta heidän ymmärrystään tiedolla johtamisen käsitteestä tai sen periaatteista.

> Tiedolla johtaminen olisi se, että kaikki päätökset ja tekeminen perustus johonkin tietoon. Ja että niinku kerätään, käsitellään, analysoidaan tietoja. Tehdään sitten päätöksiä ja johdetaan toimintaa niiden perusteella. Kai toi vaihtoehtoinen tapaisi sitten tällainen mutulla johtaminen, että mennään fiiliksen pohjalta. (Haastateltava 6)

> Toi tiedolla johtaminen mun mielestä niiku ihan sananmukaisesti on juuri sitä, että kun johdetaan, tehdään päätöksiä ja toimitaan, niin se perustuu aina tietoon eikä niiku tämmöseen mutuun. Joskus tieto ei ole välttämättä korvaa faktista tietoa vaan se voi olla tämmönen niiku arvio, joka ehkä konsensus periaatteella on saatu aikaseksi. Tiedolla johtamisessa keskeistä on se, että se myöskin on dokumentoitua se tieto et se ei ole pelkästään sellaista, että se kulkee jonkun nahkakantisissa vaan tietoa kerätään ja hallitaan ja sitä käytetään hyväksi johtamisessa ja päätöksen teossa. (Haastateltava 9)

> …päätöksiä pitäisi tehdä sillä tavalla, että se perustuu jollain tavalla siihen tietoon. Toki siis informaatioalalla, kun me ollaan niin silloin tietoon pitää mielellään perustua kaikki päättäminen ja vielä sitten se, että se tieto muuttuu paljon. Sitten meillä on hurja määrä dataa, joka muuttuu informaatioksi ja sitten se, että se data ei itsessään välttämättä ole suojattua, mutta sitten kun se muuttuu informaation se saattaa muuttaa sun ajatukset. (Haastateltava 8)

> Joku ajattelee sitä semmoiseksi niinku numeroilla johtamiseksi, mutta ymmärryksellä johtamisen fani, että pitäisi sitten myös niinku tajuta sitä kokonaisuutta, että siinä on vähän kahta koulukuntaa, että jotkut ajattelee sen tiedolla johtamisen semmoiseksi niinku numeroihin perustuvaksi, että pitää tehdä niinku mittareita ja sitten niitä seurataan ja tehdään käppyröitä. Mutta ehkä se on pikkuhiljaa menossa siihen, että ymmärretään niitä tämmöisiä ei niin numeroilla kuvattavia juttuja siinä tiedolla johtamisessa, mutta ehkä siinä pääpointti on kuitenkin se, että yrittää ymmärtää niinku taustalla olevia juttuja jotenkin. Ei mennä ihan tunteella, että saadaan jotain faktaa kaivettua jostakin asioista. (Haastateltava 3)

> No hyvin paljon niin kuin asiantuntijaorganisaatioissa on tota tämmöistä asiantuntijajohtajuutta, että ne jotka niinkun tietää enempi asiasta pystyy tavallaan sitten määrittelemään, kuinka tota joku asia sitten pitää tehdä... (Haastateltava 1)

Osaamisen hallinnan määritteleminen tuntui sekin olevan haastateltavilla käsitteenä suhteellisen hyvin hallussa. Haastateltavat tunnistivat osaamisen hallinnan organisaation kannalta organisaation jäsenten osaamisen ja tietotason ylläpitämiseksi ja kehittämiseksi.

> …osaamisen hallinta, niin se olisi niin kun tavallaan henkilöstön semmoinen niin kun tietotason ajalla pitäminen ja sen niinku siitä vastuussa oleminen. (Haastateltava 1)

Osaamisen hallinnan merkitys tunnistettiin organisaation tasolla myös toiminnan jatkuvuuden kannalta, niin toiminnan suojaamisen kuin jatkuvan kehittymisen myötä. Tämä on osaltaan myös tutkimuksen kannalta merkittävää, sillä nämä määritelmät tunnistavat Hongin ja Ståhlen (2005) mallin viimeisen vaiheen, jossa organisaatio on kykeneväinen uudistumaan itsenäisesti. Mielenkiintoisena havaintona nousi esiin se, kuinka haastateltavien puheista nousi esille osaamisen tason hahmottaminen ja mittaaminen, eli tiedon kerääminen osaamisen tasosta, mikä puolestaan sopii hyvin Hongin ja Ståhlen (2005) malliin tiedon ja osaamisen vuorovaikutuksen puolesta.

> Osaamisen hallinta mun näkökulmasta, se tarkottaa sitä, että me pyritään jollakin tavalla varmistamaan ja kontrolloimaan, meidän käyttäjät… …ymmärtää nyt tietenkin tässä tapauksessa tietoturvaan liittyviä keskeisiä periaatteita ja asioita ja tietää ohjeet ja niin poispäin. Elikkä me pyritään niiku kontrolloimaan sitä että henkilöt saavat niiku tämmösen minimiosaamistason saavuttavat niillä ohjeilla ja kursseilla ja koulutuksilla mitä meilllä on tarjota. Pyritään varmistamaan se, että kukaan ei ainakaan niinku osaamattomuuden takia tee mitään sellaista joka vaarantaa organisaation toiminnan tai järjestelmien toiminnan. (Haastateltava 9)

> Oleellista tietenkin tunnistaa, että millaista osaamista me liiketoiminnassa tässä tarvitaan, mitkä on ne tulevaisuuden tarpeet. Mitä meillä tällä hetkellä mimmoista osaamista meillä tällä hetkellä on, miten se tulee muuttumaan? Mitä koulutuksia ja kaikkea pitää järjestää? Käytännössä siis se, että analysoidaan ja ennakoidaan. Mitä osaamista tarvitaan? Sitten käydään läpi mitä on ja mietitään, että mitä pitää tehdä esimerkiksi koulutusmielessä tai muuten jotta tota on sitten jatkossakin oikeanlaista osaamista organisaatiossa. (Haastateltava 6)

> Osaamisen hallinnan määrittelisin niin, että se on tämmöinen, niin kun proaktiivinen, suunnitelmallinen tapa kehittää ja seurata jonkun organisaation tai jonkun ryhmän tai jonkun kokonaisuuden sen osaamisen nykytilaa suhteessa tavoitetilaan. Mitä toimia sinne voidaan tehdä. (Haastateltava 4)

> …jos organisaatiosta puhutaan, niin se on sitten sitä, että sehän tulee jo siitä, että mitä me niinku yrityksenä tarvitaan, jotta me voidaan tehdä sitä liiketoimintaa, että se lähtee ihan sieltä mitä yritys haluaa tehdä. Ja varmistetaan, että se osaaminen on ja sitten yksilötasolla tavallaan sitä, että miten sinne sitten päästään, jos havaitaan jotain

> puutteita ja siihen liittyy sitten taas yksilön omat tavoitteet. Ja mitä se yksilö sitten haluaa olla isona ja muuta, että siinä on aika monta näkökulmaa. (Haastateltava 3)

Eräs haastateltavista nosti myös suoraan esiin yhteyden määriteltävien käsitteiden, eli tiedolla johtamisen ja osaamisen hallinnan välillä. Tämä havainto tukee suoraan Hongin ja Ståhlen (2005) mallia siinä, kuinka tiedolla johtaminen ja osaamisen hallinta nähdään kahtena erillisenä, mutta vuorovaikutteisena osa-alueena organisaation toiminnan johtamisessa.

> …että sitä tietoa pystytään tuottamaan, niin siellä täytyy olla jonkinlaista osaamista taustalla ja sitten sitä tietoa taas kertyy. (Haastateltava 2)

7.1.3 Kyberturvallisuusosaamisen hallinta ja johtaminen käsitteenä

Kolmantena käsitteenä haastateltavia pyydettiin määritteleмään edellisten käsitteiden yhdistelmä ja tämän tutkimuksen avainkäsite eli kyberturvallisuusosaamisen johtaminen ja hallinta. Haastateltavilta kysyttiin, kuinka he näkevät kyseisen käsitteen ja poikkeaako kyberturvallisuusosaamisen johtaminen ja hallinta jollain tapaa ensin määritellyistä käsitteistä. Tutkimuksen teoriapohjan ja siitä tehtyjen johtopäätösten kannalta oli ilahduttavaa huomata, että haastateltavien näkemys mukaili pitkälti tehtyjä havaintoja. Haastateltavat eivät tunnistaneet kyberturvallisuusosaamisen hallinnan ja johtamisen poikkeavan muusta osaamisen hallinnasta millään tapaa. He tulkitsivat kyberturvallisuuden luovan osaamisen johtamiselle ja hallinnalle kontekstin ja kyberturvallisuuden lähinnä olevan se johdettava asia käsitteen tapauksessa. Tämä tukee aiemmin luvussa 5 tehtyä johtopäätöstä siitä, kuinka kyberturvallisuus ei itsessään ilmiönä ole poikkeava muista organisaation toimintaan vaikuttavista asioista, joita organisaation tulee kyetä hallitsemaan, ja joita organisaation olisi hyvä aktiivisesti johtaa.

> No ei se varmaan ylätasolla katsottuna poikkea. (Haastateltava 3)

> No mun mielestä perusperiaate on sama, että tokihan se on niinku aihealue vähän, kun vaihtuu niin sitten se taso tai ne asiat mitä seurataan, niin vaihtuu. Mutta mun mielestä ei merkittäviä eroja… (Haastateltava 4)

> Ei siinä niin kun sanotaako teknisesti mitään eroa ole. (Haastateltava 5)

> Ei, sillä kun mä luin näitä teidän kysymyksiä, niin vähän mietinkin tätä. Ja jotenkin mä tulin silloin kyllä siihen tulokseen, että no, ei se kyllä oikeastaan poikkea, että tietenkin se konteksti on niinku erilainen… … Mutta ei käytännössä mun mielestä ei poikkea. (Haastateltava 6)

> No jos niiku mentäs määritelmän mukaan niinku se nyt varmaan oppikirjoissa määritellään niin kyllä siinä pitäisi olla eroa mutta niiku tossa aluks oli puhetta, kun se kyberturvallisuus on melkein synonyymi tietoturvallisuudelle niin mä en sen takia niiku nää siinä mitää erityistä eroa. (Haastateltava 9)

Haastateltavat osasivat kuitenkin nostaa esiin kyberturvallisuudelle ominaisia piirteitä, jotka saattavat omalta osaltaan vaikuttaa siihen, kuinka kyberturvallisuuden alalla osaamisen hallintaa tai johtamista toteutetaan, tai mitkä tekijät saattavat hankaloittaa sitä oleellisesti. Yhtenä asiana haastateltavat nostivat kyberturvallisuuteen liittyvän nopean kehityksen ja kovan vauhdin, jolla tieto muuttuu tai uutta syntyy ja olemassa oleva vanhenee. Haastateltavien mukaan on oleellista, että kyberturvallisuuden pelikentällä on oltava jatkuvasti hereillä, jotta käytössä oleva tieto on varmasti ajan tasalla.

> Puhutaan kyberturvallisuudesta niin sehän on alueena semmoinen missä se tieto vanhenee aika nopeastikin tai pitää olla ajan hermolla. Elikkä se tota hallinta ja sitten tiedon hankkiminen niin se pitää olla semmoista jatkuvaa, jotta ei jää jälkeen siitä ajan hermolla olemisesta. (Haastateltava 1)

> Kyllä tuntuu että toi kyberin puoli kuitenkin on semmoinen missä pitää olla aika hereillä. Että pysyy tavallaan siinä mukana siinä hommassa, että jotkut asiat on vähän stabiilimpia. Että ehkä se suurin juttu on niinku tavallaan se vauhti. Miten tulee uusia asioita ja sitten se on yllättävän laaja alainen se mitä pitää niinku tietää, jotta voi ottaa kantaa siihen turvallisuuteen. Varsinkin niinku teknisen puolen jutut. Sitten tämmöinen hallinnollinen puoli on ehkä vähän rauhallisempaa siinä suhteessa. (Haastateltava 3)

Myös loputtomasta tiedon määrästä juuri organisaation toiminnalle relevantin tiedon tunnistamisen haastavuus nousi esille. Koska tietoa on tarjolla paljon, on organisaatioiden kyettävä tulkitsemaan sitä niin, että tietoon pohjautuvat päätökset pohjautuvat myös oikeaan ja merkitykselliseen tietoon. Tietoa on pystyttävä analysoimaan ja tulkitsemaan tehokkaasti. Kyberturvallisuuden käsitteen määrittelyssäkin tunnistettu käsitteen laajuus tuo myös käytännön tasolla haasteita kyberturvallisuuden johtamiseen ja hallintaan.

> Haaste siinä tietopohjassa on se, että se pohja on, se on pohjaton. siis tietoa on ihan tolkuton määrä ja se haaste on se että kun tehään päätöksiä tietoon perustuen niin miten me voidaan varmistaa, että me, meillä on niiku se relevantein tieto käsillä. Sillonkun se perustuu meidän omiin havaintoihin, joita tapahtuu niikun meidän ympäristössä, niin se on tietenki helppo sanoo, että tää on meidän havainto tää, tää on niiku fakta. Mut sillonkun se perustuu vaikkapa tämmösen ulkoisen lähteen välittämään tietoon tai jonkun yhteistyöverkoston jakamaan tietoon niin sillon sitä pitää aina arvioida, että miten tää nyt suhteutuu tähän meidän ympäristöön, et onks tää sellanen joka vaikuttaa meihin ja pitääkö tää ottaa niiku pohjaksi johonkin päätöksenteolle. Elikkä tota tietopohjasta sanosin että jos sitä pitää kiteyttää niin hajanainen tieto, josta pitäisi

> pystyä kiteyttämään se oleellinen tieto ja se haaste on nimenomaan se, että miten se kiteyttäminen onnistuu niin että se on riittävän oikeaan osunut se tieto mikä otetaan hyötykäyttöön. (Haastateltava 9)

> Laaja alaisuus oikeastaan, että kyberturvahan on paljon muuta kuin tietokoneella työskentelyä, että se on sitä fyysistä tietoturvaa ja ympäristöhavainnointia ja yleensäkin valppautta ja valveutuneisuutta monenlaisiin asioihin. (Haastateltava 2)

Myös eroavaisuuksia tunnistettiin. Eräs haastateltavista osasi tunnistaa yhdeksi mahdolliseksi eroavaisuudeksi sen, että kyberturvallisuuden ala on siihen johtavien koulutusten puitteissa vielä kovin nuori, eikä taustaa ole kovin pitkältä ajalta. Eroavaisuus ei siis välttämättä synny ilmiön johtamiseen liittyvissä prosesseissa, mutta itsessään ilmiön uutuus saattaa luoda eron, koska tietoa ja osaamista ei ole vielä kovin pitkältä ajalta.

> Ainut ehkä tietenkin miten se voisi ajatella, että poikkeaa, niin tietenkin aina tällaista, että mimmoista, koulutusta tai tutkimusta ja mitäkin on niinku olemassa tai saatavilla ja miten niitä on saatavilla ja mistä on saatavilla niin tolla tavalla ehkä jotenkin poikkeaa. Jos ajattelee vähän pidemmälle, vaikka että kyberturvallisuutta, niin eihän Suomessa hirveän pitkään ollut mitään hirveän laajoja koulutuksia esimerkiksi yliopistopuolella siihen, että kyllähän ne ihan vastata tässä mennä vuosina tullut nää kaikki kyberturvallisuuden koulutusohjelmat, maisteriohjelmat. (Haastateltava 6)

7.2 Kyberturvallisuusosaamisen hallinta ja johtaminen suhteessa organisaation strategiaan

Tämä alaluku käsittelee haastattelurungon toista osiota sekä Hongin ja Ståhlen (2005) mallia (kuvio 8), jossa paneuduttiin tarkemmin kyberturvallisuusosaamisen hallintaan ja johtamiseen ja sen suhteeseen haastateltavan edustaman organisaation strategiaan. Haastateltavia pyydettiin kuvailemaan organisaation strategiaa ja siitä johdettuja tavoitteita. Heitä pyydettiin tämän jälkeen pohtimaan, kuinka kyberturvallisuus mukailee näitä tavoitteita. Tämän lisäksi haastateltavia pyydetiin kuvailemaan, kuinka kyberturvallisuusosaamista pyrittiin hallitsemaan ja johtamaan ja sitä, minkälainen rooli kyberturvallisuudella on organisaation toiminannan kannalta. Haastattelukysymykset olivat toisessa osiossa seuraavanlaiset:

Miten kuvailisit organisaation strategiaa? Onko toiminnassanne niistä johdettuja tavoitteita, joita seurataan? Mitä nämä ovat ja kuinka niitä seurataan?

Kuinka kyberturvallisuus mukailee tai liittyy näihin tavoitteisiin? Miten kyberturvallisuuden käytännöt tukevat organisaation strategian toteutumista?

Miten kyberturvallisuusosaamisen hallintaa ja johtamista toteutetaan? Onko olemassa erityistä suunnitelmaa tai kirjoitettuja ohjeita, pelisääntöjä tai mallia?

Millainen rooli kyberturvallisuusosaamisella on toimintanne kannalta?

Oletteko tunnistaneet toiminnassanne ns. suorituskyvyn aukkoja tai puutteita, joita voitaisiin pyrkiä kuromaan umpeen paremmalla kyberturvallisuusosaamisella?

7.2.1 Organisaation strategia ja tavoitteet kyberturvallisuuden näkökulmasta

Strategiaan liittyvissä kysymyksissä haastateltavien osalla esiintyi eroavaisuuksia siinä, kuinka kyberturvallisuus on löytänyt tiensä heidän edustamiensa organisaatioiden strategian tasolle. Haastateltavilta kysyttäessä, kuinka kyberturvallisuus näyttäytyy heidän edustamansa organisaation strategiassa tai siitä johdetuissa tavoitteissa, totesi muutama haastateltava strategian olevan ylätason käsitteenä sellainen, että siellä kyberturvallisuus ei välttämättä suoraan näy. Kuitenkin strategiset linjaukset näkyivät sitten kyberturvallisuuden parissa työskentelevien ihmisten työssä jollain tapaa, vaikka kyberturvallisuutta ei suoraan strategian tasolla erityisesti tunnistettukaan.

> Meillä on semmonen väljä kytkös sinne ylätason strategiaan, koska siellä on kuitenkin tietenki yks keskeinen asia on osaaminen, ja sit meillä on digiohjelma, joka pyrkii taas niiku jalkauttamaan sitä strategiaa tänne digitalisaation maailmaan. Ja nyt sen ikään kuin alapuolella on sitten tämmönen digiturvaohjelma, jossa sitten tää osaaminen on yks keskeinen osa-alue… mun ehkä aavistuksen hankala osottaa suoraa kytköstä sinne strategiaan, mutta jos puhutaan siitä, miten johto ilmaisee näitä tarpeita liittyen tietoturvaosaamiseen niin sieltä se kumpuaa myöskin se, että meillä on niiku selkee tavote siellä omassa digiturvaohjelmassa henkilöstön osaamisen kehittäminen. (Haastateltava 9)

> Eihän meidän strategiassa esimerkiksi suoraan siinä niinku ylätasolla näe mitään kyberturvallisuutta, eikä paljon muutakaan tämmöistä niinku esimerkiksi osaamisalueita tai teknisiä juttuja, että ne on niinku, ehkä se tulee siitä sitten, että miten se ylemmän tason strategia sitten näkyy pienemmissä tiimeissä ja porukoissa, niin siellä sitä pitää vähän pureskella ja muuta. Mutta, että kyllä me niinku kyllä me seurataan kyllä sitä. (Haastateltava 3)

Toisaalta myös suuri osa haastateltavista löysi hyvin suoriakin kytköksiä organisaation strategian ja kyberturvallisuuden välillä. Osittain eroavaisuuksia varmasti selittää organisaatioiden liiketoiminnan malli ja kyberturvallisuuden rooli osana liiketoimintaa. Osalla organisaatioista kyberturvallisuus on oman toiminnan varmistamisen lisäksi tuotettavaa palvelua ja tuotteita, jolloin voidaan olettaakin kyberturvallisuuden olevan organisaation kannalta erityisen merkittävä ja laaja-alainen käsite, jonka alle organisaation ydintoiminnot muodostuvat.

> No kyberturvallisuusmielessä, no meillähän tuotteet, mitä tehdään, niin on tarkoitettu tämmöiseen viranomaiskommunikaatiooon, ja sehän on luonteeltaan hyvin niinkun arkaluontoista ja tota tavallaan se ohjaa jo meidän strategiaa ja toimintatapoja siihen, että nää security asiat pitää ottaa hyvinkin vakavasti ja niinpä niinkun meidän security policy ohjaa meidän meidän tota jokapäiväistä tekemistä. (Haastateltava 1)

> Yksi strategian osa on hyvät ja koko ajan kehittyvät ja tietoturvalliset palvelut asiakkaille ja, että me pystytään olemaan kilpailukykyinen palvelutalo asiakkaille ICT-alalla, niin se tarkoittaa käytännössä sitä, että se tietoturvan pitää olla kunnossa, joten tätä tietoturvallisuuden tilaa palveluissa ja ohjelmassa toiminnassa seurataan ihan johdon katselmuksessa säännöllisesti muutaman kerran vuodessa eli kyllä se on ihan tuota strategiatasolla ja käytännön tasolla kunnossa. (Haastateltava 2)

Mielenkiintoisena sanana haastateltavien suusta kuului myös sana “luottamus”. Haastateltavat tunnistivat luottamuksen olevan tärkeä arvo kyberturvallisuuden alalla toimiessa. Myös erilaisia vastuita ja velvoitteita tunnistettiin osaksi toimialalla toimimista. Vastuiksi ja velvoitteiksi tunnistettiin muun muassa velvollisuus toimia oikein ja esimerkiksi tiedonkäsittelyn puolesta vastuullisesti, mutta organisaatioilla tunnistettiin myös olevan yhteiskunnallisia velvoitteita esimerkiksi poikkeustilanteita ajatellen.

> Tällä hetkellä strategiana on luottamus, tieto ja turva on niinku ne kolme sanaa. Ja tää meidän bisneshän on tämmöinen luottamusbisnes niinku lähtökohtaisesti monestakin näkökulmasta. Eli siinä on se, että ihmisten pitää pystyä luottamaan siihen, että asioita hoidetaan oikein. (Haastateltava 4)

> Yleensä kuitenkin kaikki noi tommoiset strategiat niin meillä ehkä tehdään noin 3–5 vuoden tähtäimellä, ja sitten aina tällaiset tavoitteet asetetaan yleensä aina tilikausittain tietenkin huomioiden se, että ne jokaisen tilikauden tavoitteet vie meitä kohti sitä, tarkoitus on tukea sen strategian implementointia käytännössä ihan jokaiselle ihmiselle ketä meillä on töissä. Me asetetaan tavoitteita ja mittareita, jotka lähtee sieltä strategiasta ja koettaa tukee sitä strategian jalkauttamista... … yksi osa meidän liiketoimintaa on myydä kyberturvallisuuteen liittyviä palveluita... ...Meidän pitää koko ajan pysyä kärryillä siitä, että mihin suuntaan niinku riskit ja mahdollisuudet organisaatioissa on menossa. Elikkä kyberturvallisuus niinku jakaantuu siinäkin sitten että se on tiedon suojaamista monella eri kulmalla, ja siellä on meilläkin velvoitteita, mutta sitten just tää strateginen liiketoimintastrategiakulma, jossa me halutaan olla luotettu toimija. (Haastateltava 6)

> Meillähän on niin, kun varmaan kaikilla muillakin yrityksillä, niin on tietenkin olemassa niinkun strategia ja sitä tota niin strategiajakso on 4 vuotta ja tarpeen vaatiessa sitten päivitellään siinä välissä... ...me ollaan oikeasti tässä niinku semmoisella toimialalla, että se kyber ja tämmöinen niinku valmiussuunnittelu ja varautuminen niin sehän on niinkun osa tätä meidän DNA:ta, että nyt kun toimitaan tällä toimialalla ja meillä on tosiaan velvoitteet kyetä toimimaan niinku kaikissa olosuhteissa, niin meillähän on tää koko organisaatio rakennettu sillä tavalla, että me niinkun huomioidaan tämmöiset uhkakuvat (Haastateltava 7)

Maininnan arvoista on myös erään haastateltavan ja tämän edustaman organisaation oivallus siitä, kuinka kyberturvallisuus koskettaa oikeastaan kaikkea organisaation toimintaa läpileikkaavana ilmiönä, vaikka kyberturvallisuus nostettaisiinkin yhdeksi strategiseksi elementiksi tai vaikka jokin toinen asia nostettaisiin kehityksessä niin sanotusti keihään kärjeksi.

> Mehän on tehty strategia, jossa kyber nostettu yhdeksi kärjeksi... ...Vielä siihen voisi sanoa, että me on määritelty, että kyberturvallisuus on kaikkea leikkaava elementti. Elikkä se liittyy kaikkiin, jos meillä on jotenkin kehittämisen kärkeä, niinku horisontaalisesta niin siis anteeksi vertikaalisessa, niin se kyber menee horisontaalisesti kaikkien läpi. Elikkä kaikissa pitää ottaa huomioon se. Se on meidän strategiassa kuvattukin. (Haastateltava 5)

7.2.2 Kyberturvallisuusosaamisen rooli organisaatiossa

Kyberturvallisuusosaamisen merkitystä organisaatioissa pyrittiin selvittämään, jotta saataisiin käsitys siitä, kokevatko organisaatiot kyberturvallisuusosaamisen olevan todella merkityksellinen seikka, johon kannattaa panostaa, eikä vain pakollinen velvollisuus. Haastateltavat vastasivat kysymykseen siitä, minkälainen merkitys kyberturvallisuusosaamisella on heidän organisaationsa toiminnan kannalta. Selvää oli jo ennakkoon, että kyberturvallisuuden alalla toimivien organisaatioiden toiminnan kannalta kyberturvallisuusosaaminen poikkeaa monella tapaa ja voi merkitä eri asioita. Osalle se on tärkeää liiketoiminnan kannalta tuotettuna palveluna tai tuotteena, mutta mielenkiintoista on selvittää tunnistavatko organisaatiot myös kyberturvallisuuden merkityksen sisäisesti oman toiminnan mahdollistajana.

Eräs haastateltavista nosti hyvin esille juuri tuon kyseisen asian, että jokaisen on ymmärrettävä perusasiat ja osattava toimia oikein. Käyttäjän merkityksen nostaminen keskeiseen rooliin tietoturvallisuudessa on tärkeää.

> Tietenkin omalta kannalta se on hyvin tärkeä ja keskeinen, toki pakko myöntää, että eihän tuo tietoturvallisuus tai kyberturvallisuus ole meidän niin sanottua ydinosaamista, mutta noin niiku laajemmassa perspektiivissä, kun katsoo, niin se on tukeva

> toiminto, jolla pyritään varmistamaan tiedon turvallisuus tai saatavuus ja järjestelmien turvallisuus. eli kyllä se on keskeisen tärkeää, että kaikki osaavat ja ymmärtävät perusasiat... … se loppukäyttäjän merkitys ja rooli tietoturvassa on ihan keskeisen tärkeä. (Haastateltava 9)

Haastateltavat tunnistivat myös organisaation sisäisen osaamisen tärkeyden heidän uskottavuutensa puolesta. Haastateltavat tunnistivat, kuinka sisäinen osaamattomuus näkyy herkästi myös heidän asiakkailleen, mikäli asiat eivät ole kunnossa organisaation sisällä. Myös liiketoiminnan ja kyberturvallisuuden palveluiden tuottamisen puolesta osaaminen tunnistettiin hyvin tärkeäksi, jotta palveluita voidaan tuottaa ja liiketoimintaa ylläpitää halutulla ja kilpailukykyisellä tasolla.

> Hyvin merkittävä, eli se on jo pelkästään mainekysymyskin ja maineriski meidän kaltaiselle firmalle, että jos ei ole hyvällä tolalla asiat, ihan henkilöstön osaamisessa, niin tuota kyllä se äkkiä näkyy sitten asiakkaille. (Haastateltava 2)

> No se on, se on tota erittäin tärkeää, koska me tehdään tämmöisiä tuotteita millä välitetään tämmöistä sensitiivistä informaatiota, niin niin, se niinku asennoituminen jo siihen, niin on hyvin tärkeä. (Haastateltava 1)

> No ei me pystytä tekemään mitään meidän palveluita, jos meillä ei ole sitä osaamista, meillä pitäisi käytännössä olla alan paras osaaminen tästä kyberturvallisuudesta, jotta me ollaan uskottava palveluntarjoajia meidän asiakkaille, ja tietenkin pitää olla semmoista koko ajan kehittyvää osaamista, kun maailma ja regulaatio ja kaikki muuttuu. (Haastateltava 6)

7.3 Kyberturvallisuusosaamisen hallinnan ja johtamisen prosessit

Kolmas alaluku käsittelee haastattelurungon (Liite 1) kolmannen osion mukaisesti kyberturvallisuusosaamisen johtamiseen ja hallintaan liittyviä prosesseja organisaatioissa. Hongin ja Ståhlen (2005) malliin (Kuvio 8) tämä sijoittuu keskelle mallia tiedolla johtamisen ja osaamisen hallinnan prosessien kohdalle. Haastatteluosion tarkoituksena oli kartoittaa, kuinka kyberturvallisuusosaamista käytännön tasolla johdetaan tai hallitaan organisaatioissa. Osiossa pyrittiin selvittämään muun muassa kyberturvallisuusosaamiseen liittyviä henkilörooleja sekä johtamisen ja hallinnan toimintamalleja ja käytänteitä. Haastateltavilta kysyttiin myös, kuinka ja mitä tietoa organisaatio kerää nopeasti muuttuvassa kyberturvallisuuden maailmassa sekä kuinka osaamista kehitetään organisaation sisällä, ja kuinka alati muuttuvan maailman haasteisiin pystytään vastaamaan.

7.3.1 Tiedon ja osaamisen kartoittaminen

Seuraavat haastattelulainaukset kuvaavat sitä, kuinka haastateltavien organisaatioissa kyberturvallisuutta mitataan ja seurataan sekä tiedon tarvetta kartoitetaan. Haastateltavien vastauksista nousi esille tietoturvatestit ja arvioinnit, joiden avulla saadaan tietoa siitä, kuinka hyvin henkilöstö hallitsee tiettyjä asioita, missä on tarvetta lisäkoulutukselle tai missä henkilöstöllä on selkeitä vaikeuksia tai puutteita. Haastateltavien mukaan tietotaidon mittaaminen ja raportointi on yksi keino siinä, kuinka tietoa kerätään ja kuinka tieto auttaa päätöksenteossa ja priorisoinnissa. Erilaiset mittarit olivat haastateltavien vastauksissa keskeisessä roolissa organisaation kyberturvallisuustason mittaamisessa. Tiedon tarvetta kartoitetaan myös asiakkaiden puolelta keräämällä palautetta sekä ennakoimalla ja vastaamalla kysyntään. Asiakaspalautteiden avulla pystytään seuraamaan kilpailukykyä sekä sitä, missä organisaation mahdolliset vahvuudet ja heikkoudet ovat. Haastateltavat kertoivat asiakaspalautteiden ja markkinoiden vaatimusten seuraamisen olevan tärkeää, sillä niiden perusteella voidaan tehdä muutoksia esimerkiksi koulutuksiin sekä ennakoimaan markkinoita, ja täten vastaamaan tehokkaammin kysyntään. Tämän lisäksi tiedon tarvetta kartoitetaan myös erilaisten harjoitusten avulla. Kuvitteellisten tai simuloitujen tilanteiden järjestämisellä harjoituksissa voidaan mitata organisaation reagointi- ja kriisinhallintakykyä. Haastateltavat nostavat samassa yhteydessä esille laadukkaan tiedottamisen merkityksen.

> Nojoo toki sillä tavalla, että kun mä sanon, että me pyritään varmistamaan niin jotenkinhan meidän pitää pyrkiä sitä myös mittaamaan ja se perustuu sit siihen tietoon mitä me saadaan niistä koulutuksista. Esimerkiksi henkilöstöllä oli tossa viime syksynä, avattiin tämmönen tietoturvatesti, jolla me pyrittiin arvioimaan, että kuinka hyvin ihmiset näitä perusasioita osaa. Ja sit siitä on kerätty tietoa, että mikä mahollisesti olis semmonen niiku kompastuskivi niiku mikä yleisimmin nousee esiin semmosena hankaluutena mitä ihmiset ei ehkä osaa tai ymmärrä et sillä tavalla liittyy toki tiedolla johtamiseen. (Haastateltava 9)

> Totta kai niinku jokainen firma eli tää on asioita mitä me seurataan ja mittaroidaan täällä ja koitetaan sitten viestiä johdolle, että näihin meidän pitää panostaa sitten tässä seuraavan vuoden aikana esimerkiksi. Eli joo toi on jatkuva prosessi. Sitä kartoitetaan ihan esimerkiksi, kun me suunnitellaan aina koulutuspolku säännöllinen tyyliin vuodeksi eteenpäin, että mitä väelle koulutetaan, niin sitten eräänlainen seuranta on se, että ne koulutukset on tehty läpi ja hyväksytysti läpi, että siellä on vastaanotto tietynlaisiin arviointikysymyksiin sitten, että on ymmärretty se aihe. Sitten taas tiettyjä omia ohjeita me niitä vastuutetaan lukemaan ja pyydetään kuittaus, että onko luettu ja ymmärretty... (Haastateltava 2)

> No kyllä ehkä se karu todellisuus on, että se feedback saadaan aika hyvin siitä, että miten kauppa käy, että niinku sen näkee aika hyvin siinä kohtaa, että ollaanko me niinku ikään kuin kilpailukykyisiä, että jos rupeaa aina tulee häviöitä ja palautetta, että kilpailijalla oli parempi osaaminen ja muuta niin se on niinku semmoinen viimeinen

> hälytyskello. Mutta se nyt yleensä näkee jo vähän aikaisemmin, että missä se kysyntä tavallaan on, niin se on niinku se ennakointi näkökulma, että mitä kysytään ja mitä on tarve niin se niinku ohjaa käytännössä sitä hommaa. Ja sitten me aika helposti nähdään kyllä, että onko meillä niinku sen tyyppistä osaamista. Että kyllä se aika niinku suoraviivaisesti tulee mun mielestä sieltä myynnin ja asiakkaiden kautta se semmoinen niinku ohjaus, että tota siitä se sitten jotenkin niinku menee, että ei meillä semmoisia niinku mitään excel matriiseja ole kauheasti viritelty että tossa on aukko, että kyllä se vielä on niinku jotenkin pysynyt hallussa. (Haastateltava 3)

> Me käytiin myöskin tämmöinen taistoharjoitus. Elikkä kuvitteellinen tilanne että meidän verkkoon hyökättiin ja tota DVV kanssa sekin. Juurikin viime vuonna itse asiassa harjoiteltiin sitä, että mitäs sitten jos joku hyökkää, niin mitä meidän pitäisi sen jälkeen tehdä niin kyllä se tiedottaminen, tiedottaminen, tiedottaminen oli niin kun nousi kyllä sieltä niin esille, että tiedonkulku ja oikean tiedon saaminen on ihan ykkösjuttu. (Haastateltava 5)

Mielenkiintoisina nostoina haastateltavat nostivat edellisten havaintojen lisäksi pari konkreettista mittaria ja toimenpidettä, joilla organisaatio arvioi ja seuraa kyberturvallisuustaitoja ja reagointikykyä. Näiden käytäntöjen hyödyntäminen heijastaa organisaation sitoutumista jatkuvaan oppimiseen ja kyberresilienssin kehittämiseen. Tietojenkalastelusimulaation avulla pystytään arvioimaan, kuinka hyvin henkilöstö käsittelee ja toimii kyberuhkiin liittyvissä skenaarioissa. Yhden organisaation edustaja huomautti, että poikkeamien raportointitiheyttä seuraamalla voidaan tulkita myös osaamisen tasoa. Vähäinen määrä ilmoitettuja poikkeamia on huono asia, sillä se ei tarkoita sitä, etteikö ongelmia olisi, vaan pikemminkin sitä, että niitä ei raportoida. Tämä korostaa avoimen tiedonkulun ja raportoinnin tärkeyttä kyberturvallisuudessa.

> Säännöllinen tietojenkalastelu simulaatio on yksi sitten sellainen konkreettinen mittari, mikä meillä näyttää kyseiseen asiaan sitten tarkkaakin mittarointia, että kuinka meidän väki toimii, toimii missäkin skenaariossa. (Haastateltava 2)

> Se oli ainakin hänelle (edellinen security officer) tärkeä se, että organisaatio pysty tota niin kun oppimaan itse itseltä, että tämmöisiä security incidentteja tapahtui, että ne niinku raportoitiin ja niistä sitten pyrittiin oppimaan ja sitten se oli enempi niin kun huolestuttavaa, että jos ei tullut yhtään niin security incidenttia kuukaudessa, niin silloin se ei ollut hänen mielestään hyvä tilanne, että se ei tarkoittanut sitä, että etteikö niitä tule vaan sitten, että kukaan ei raportoinut. (Haastateltava 1).

7.3.2 Osaamisen kehittäminen ja hallinta

Haastateltavia pyydettiin haastatteluissa myös avaamaan osaamisen kehittämisen ja hallinnan prosesseja. Mielenkiintoista oli selvittää, kuinka he ja heidän edustamansa organisaatio pyrkii kehittämään toimintaansa nimenomaan osaamisen hallinnan kautta. Erityisesti, kun osaamisen hallinta tunnistettiin tärkeäksi

käsitteeksi ja kyberturvallisuus myös ilmiönä soveltuvaksi osaamisen hallinnan ja johtamisen prosessien alle. Suurimpana asiana, täysin oletettavasti, haastateltavat nostivat esille koulutusten merkityksen. Mutta koulutukseen haastateltavat tunnistivat myös liittyvän muutamia haasteita ja toisaalta velvollisuuksia myös organisaation jäsenten toimesta. Koulutuksista on haasteellista tehdä sopivia monille eri osaamisen tasolla oleville henkilöille sekä monesti koulutusten käyminen ja suorittaminen jäi yksilöiden vastuulle. Vastauksista pystyi ymmärtämään, että kontakti ja paikallaolo koulutuksia kaivataan ihan yhtä lailla, kuin helpommin suoritettavia verkkokoulutuksia.

> Sitä on pyritty koulutuksella parantamaan mut sitten tietenkin nää haasteet tulee siitä, että monesti toi kouluttautuminen tai lyhyenkin kurssin käyminen on se sitten tämmönen moodle tai joku muu sähkönen digitaalinen kurssi, niin ihmiset, henkilökunta varsinkin monesti kertoo, että ei heillä ole aikaa tän tyyppisiin, vaikka tunnistavat ehkä sen tärkeyden. (Haastateltava 9)

> Tietenkin yritys kouluttaa. Yrityksellä on verkkokursseja ja sitten on myös tota tietenkin tämmöistä työssä oppimista. Ja sitten on ihan niin kun mahdollisuus käydä jotain ulkopuolisia koulutuksia, että siinä mielessä yritys kyllä panostaa tuohon koulutuspuoleen, tietenkin sitten sen lisäksi on jokaisen työntekijän, voisiko sanoa pieni velvollisuus sitten, että niinkuin omatoimisesti sitten seuraa uutisia ja nettikirjoittelua, että pysyy sitten ajan hermolla. (Haastateltava 1)

> Tiimin vetäjät niin niitten tehtävä on niinku sen tiimin osaamista niinku ikään kuin olla kartalla ja keskustella henkilöiden kanssa ja sitten myös niinku myynnin ynnä muiden kanssa, että mitä sen suhteen tehtäisiin ja sitten meillä on, se on semmoinen treeni tai brain-konsepti että siinä on ihan selkeät budjetit henkilötasolla ja muuta että paljonko saa käyttää niinku opiskelua ja sitä just niitten sitten niiden tiiminvetäjä ja muiden kanssa yksin pohditaan, että mitä kukakin tekee, että kyllä nyt jonkunlainen semmoinen malli on olemassa. (Haastateltava 3)

> Meillä on monenlaisia tapoja ja siinä on niinku sille, että siellä tota meillä on aika aika löyhiä ne niinku sen osaamisen kartuttamisen käytänteet osittain sen takia, että jos me päätetään edeltäpäin, että tää on se niinku se tapa millä me kartoitetaan osaamista niin samalla me blokataan mahdollisesti ulos jotain tiettyä osaamista mitä kartoittaa, että niinkun semmoinen löyhäprosessi on... ...kun koulutuksia on tarjolla, koulutuksiin pääsee, mutta se on niinku kuitenkin yksilön vastuulla aika paljon se, että mitä se kokee niinku tarvitsevansa sitä, niin sitä niinku sitä osaamista ja sitä tuetaan toki, sitä niinku sitä oppimista paljon meillä, on niinku on kaikennäköistä online-kuviota ja sitten toki ihan tämmöisiä oikeita face-to-face kursseja. (Haastateltava 8)

Haastateltavat tunnistivat haasteiksi muun muassa työntekijän kiireellisyyden. Työkuorma voi olla yksittäisellä työntekijällä niin suuri, että tämä joutuu priorisoimaan työaikaansa muihin tehtäviin, jolloin omalla ajalla tehtävät koulutukset ja kurssit jäävät tekemättä, vaikka tähän saisikin käyttää työaikaa ja koulutuksen tärkeys tunnistettaisiinkin. Eräs haastateltavista nosti myös esiin sen, että osaamisen kartuttamista ei pitäisi liian tarkkaan suunnitella edeltä käsin tai pyrkiä

päättämään ennakkoon mikä on tärkeää ja mikä ei, jotta ei "kävellä laput silmillä" jonkin tärkeän asian ohi. Sama haastateltava nosti yhdessä muiden kanssa myös työntekijän oman vastuun haluta oppia ja tunnistaa hänelle tärkeitä asioita opittaviksi. Vastuu osaamisen kartoittamisesta nähtiin siis molemmin puoleiseksi niin työntekijän ja työnantajan puolesta.

Kyberturvallisuusosaamisen hallinnan johtamiseen ja hallintaan liittyen haastateltavat nostivat esiin erilaisia kirjoitettuja ohjeita kuten ISO 27001 standardin ja siihen liittyvät standardin mukaiset toimenpiteet. Myös sisäiset tietoturvaohjeet todettiin käytänteiksi, joiden avulla kyberturvallisuutta pyritään hallitsemaan sisäisten koulutusten ja kurssien lisäksi. Organisaatioiden välillä ilmeni pientä vaihtelua käytännön toteutuksen suhteen, mutta yleisesti ottaen organisaatiosta riippumatta koko henkilöstön osaamisen hallintaan liittyy jonkinlainen koulutus ja koulutuksen seuraaminen, jotta osaamisen tasosta voidaan varmistua.

> Yleisesti henkilöstöllä, niin meillä on tietysti pitää kuvatakin ihan jo vaatimuksiin liittyen se, että miten me koulutetaan meidän henkilöstöä, että kyberturva asiat on tuttuja koko henkilöstölle. Ja ne roolin mukaisella syvyydellä sitten vielä kaiken lisäksi elikkä me tuota, kun koulutussuunnitelma tai siis tietoturvatietoisuus -ohjelma on meillä olemassa ja se on dokumentoitu ja sisältää säännöllistä toimintaa. Meillä myöskin huomioidaan koko työntekijän elinkaaren riittävä koulutus. Erityisiä pelisääntöjä, niin en nyt tiedä onko, että meillä on politiikka olemassa, että miten tai mitä me vaaditaan, että meidän käyttäjät on koulutettu tietyiltä osin aina, että siitä ei poikkeuksia ole, se koskee koko firmaa ja sitten taas minä omassa roolissani vastaan siitä, että koulutus on riittävällä tasolla ja sitä seurataan... ...Säännöllisyys ja mitattavuus luonnollisesti ja mehän tehdään ISO 27001 mukaan näitä hommia muun muassa näitä koulutusasioita. Sieltä tulee se meidän johtamismalli yleensäkin tietoturvaan. Se on se hyvä, ja johtamisen käytäntö siellä mikä vastuuttaa sitten huolehtimaan siitä, että se koulutus on säännöllistä ja, että se kattaa myös koko henkilöstön johtoporrasta myöden. Että se on se sieltä periytyvä hyvä malli meilläkin käytössä. Ja sitten toi viestintä tärkeänä. (Haastateltava 2)

> Pitää tehdä niinku määrätietoisesti ja määrämuotoisesti asioita, että monessa paikkaa se lähtee niinku ehkä siitä, että pitää niinku joku yksittäinen asia saada organisaation opittua tai se saatua niinku tieto läpi. Siis tätä lähestytään liikaa sen yksittäisen asian kautta eikä ajatella sitä semmoisena niinku pitkänä jatkumona, että sun pitää aina niinku huolehtia siitä, että se pohja on semmoinen, jonka päälle voidaan rakentaa, niin se on ehkä semmoinen hyvä käytäntö, mikä täällä on ollut pitkään. (Haastateltava 4)

Osa haastateltavista osasi erotella erilaisia vaatimustasoja kyberturvallisuusosaamiselle eri tehtävissä, ja yhdessä organisaatiossa oli erillinen kolmiportainen malli käytössä, jonka avulla eri henkilöstöryhmien osaamisen tarpeet voitiin tunnistaa ja niihin vastata. Myös tehtävä- tai projektikohtainen koulutus tunnistettiin tärkeäksi, unohtamatta sitä, että työntekijöitä on osattava myös käsitellä yksilöinä, jokaisen yksilön omat tarpeet huomioiden.

> Ja ja hyvin yksinkertaisesti meillä semmoiset niinku tavallaan prosessit tai käytännöt sitten on, että ne ei ole mitään niinku rakettitiedettä, että ne on niitä esimiehiä henkilön välisiä keskusteluja ja vähän peilataan siihen, että onko löytynyt töitä vai pitäisikö tehdä jotain ja onko se työ semmoista, mikä kiinnostaa, että siinähän se käytäntö periaatteessa niinku on meillä sitten on. En osaa tarkentaa käydäänkö täällä näitä keskusteluita niinku ihan viikko-, kuukausi-, vuositasolla tota riippuu ihan henkilöstä. Jotkut ei halua koko aikaa esimiehen kanssa niinku lässyttää ja jotkut tarvitsee enemmän tukea, että se on niinku pelisilmää sitten. Ja jotkut sanoo ihan suoraan, kun ei tarvitse, että kyllä mä pärjään ja jotkut sitten tarvitsee apua vähän joka viikkoa. (Haastateltava 3)

> Tota meillä on tota niin semmoinen osaamisen kehittämisen suunnitelma ja se, että kun meillä on niin kun erinäköisiä henkilöstöryhmiä niin tää on niinku jaettu nyt niinku tavallaan elikkä meillä on me käytetään semmoista kolmiportaistapyramidimallia... (Haastateltava 7)

> No joo niinku tossa äsken viittasit, meillä on tietenkin se ISMS, joka tulee sieltä ISO 27001 puolelta... ...sitten tietenkin Security Policy on yks, mikä on semmoinen kirjoitettu ohje. Sitten meillä myöskin on koulutusta ja sillain että, että meillä on tämmöinen Security Awareness -koulutus, mikä pitää tehdä vähintään joka kolmas vuosi. Se tehdään meillä verkossa ja sitten on tämmöisiä niinkun puhuin tuossa äsken noista sensitiivisyyshankkeista, niin jokaista hanketta ennen niin siihen annetaan hankekohtainen koulutus. (Haastateltava 1)

Haastatteluissa nousi myös esille osaamisen hallintaan liittyvä liiketoimintanäkökulma. Muutamat organisaatiot tunnistivat nimittäin myös kilpailun ja markkinoiden vaikuttavan siihen, minkälaista osaamista organisaatio tarvitsee, jotta muuttuvaan ja kovasti kilpaillun pelikentän muutoksiin voidaan vastata. Eli tarvittavia osaamistarpeita ammennetaankin suoraan markkinoilta analysoimalla ja ennustamalla sitä, mihin suuntaan maailma on menossa, ja mitkä ovat ne trendit, jotka nousevat pintaan ja joissa organisaation on kyettävä pysymään mukana.

> Se lähtee niinku siitä asiakkaiden kysynnästä käytännössä ihan selkeästi, että mihin suuntaan kauppa niinku käy ja sitten siitä se sitten niinku tavallaan muotoutuu et, nähdään, että onko meillä riittävästi osaajia ja minkälaista osaamista niillä on, missä on puutteita ja se näkyy sitten niinku rekrytoinnissa myös, ei pelkästään siinä osaamisen kehittämisessä, mutta mille on kysyntää niin se ohjaa aika pitkälti sitten sitä kaikkeen siihen osaamiseen liittyvää. Toki siellä sitten niinku yritetään saada ihmisten omatkin suunnitelmat jotenkin mukaan siihen kuvioon. Mutta kyllä se niinku rehellisyyden nimissä niin se tulee sieltä niinku asiakkailta sitten loppujen lopuksi... ...tässä on varmaan monta mielipidettäkin, mutta itse tykkään siitä, että aina olisi se semmoinen “bisnes ensin” tyyppinen lähestyminen, ettei tehdä turhaa jotakin asiaa, että yksi hyvä käytäntö on kyllä niinku saada vastauksia siltä asiakkaalta siihen, että mihin päin mennään. En mä tiedä onko se ihan käytäntö, mutta siis semmoinen periaate kuitenkin. (Haastateltavava 3)

> Me koko ajan analysoidaan ja tehdään niinku markkina-analyysiä siitä, että mimmoisia trendejä kyberturvallisuuden alalla on niinku. nyt ja nähtävissä, jos on nyt ottaa jonkun esimerkin niin vaikka tällainen taas asioita siirretään pilvipalveluihin tai siirron trust-jutut ja tän tyyppiset niin tollaisia niinku merkittävimpiä muutoksia niinku trendeissä pyritään olla riittävän ajoissa niiden päällä sitten kaikki regulaatiot mitä tulee, vaikka joku DORA tai NIS2 niin, että tiedetään mitä regulaatiota on tulossa ja niin mimmoisia muutoksia ne tulee aiheuttamaan. Ja sitten tuolta pohjaltahan meidän pitää miettiä, että mimmoista osaamista noi asiat nyt sitten tulee vaatimaan ja, että onko meillä semmoista osaamista? Jos ei ole, niin mistä me sitten saadaan sitä, että semmoisia mahdollisuuksia vaikka kouluttaa ihmisiä noihin tai pitääkö palkata jotain uusia ihmisiä ja näin pois? Monia asioitahan on sellaisia myöskin mihin ei hirveästi oo saatavilla mitään niinku hirveän fiksuja koulutuksia niin sitten pitää itsekin tehdä niitä koulutuksia ja kouluttaa ihmisiä. (Haastateltava 6)

7.3.3 Muuttuvan maailman haasteisiin vastaaminen

Haastateltavilta nousi vastauksissa esille seuraavia keskeisimpiä näkökohtia siihen, kuinka organisaatio pyrkii pysymään ajan tasalla ja vastaamaan kyberturvallisuuden haasteisiin. Ensimmäisenä ja isoimpana havaintona haastateltavat näkivät uhkatiedon hankinnan ja tilannekuvan muodostamisen. Haastateltavat kertoivat hankkivansa uhkatietoa eri lähteistä, kuten viranomaisilta (mm. Traficom), valmistajilta ja erilaisten jakelulistojen kautta kuten mm. ISAC-toiminto, mikä käsittää kyberturvallisuuskeskuksen eri toimialoille perustamia kyberturvallisuuden tiedonvaihtoryhmiä. Haastateltavien organisaatiot pyrkivät näiden ulkoisten tietolähteiden avulla muodostamaan kokonaiskuvaa kyberuhkista seuraamalla tilannetta maailmalla ja Suomessa. Organisaatiot hyödyntävät myös teknisiä valvontatyökaluja sekä riskianalyysejä yhdessä ulkoisten lähteiden kanssa rikastaakseen tilannekuvaa. Niiden avulla yritetään pysyä ajan tasalla sekä reagoimaan ja suunnittelemaan toimenpiteitä mahdollisesti jo etukäteen. Seuraavina asioina nousi esille koulutus ja kybertietoisuuden ylläpito sekä viestintä henkilöstölle. Haastateltavien edustamat organisaatiot panostavat koulutuksiin ja yleissivistykseen kyberturvallisuuden saralla esimerkiksi tietoisuuden lisäämisellä koskien huijausviestejä ja tietoturvauhkia. Säännöllisellä viestinnällä kuten tietoiskuilla ja tiedotteilla, jotka käsittelevät ajankohtaisia uhkia, haavoittuvuuksia ja tapahtumia pystytään haastateltavien mukaan pitämään henkilöstö ajan tasalla. Kolmantena havaintona haastateltavat nostivat yhteistyön toimittajien ja valmistajien kanssa, joka liittyy osaltaan ensimmäiseen havaintoon tiedonlähteiden ja uhkatiedon hankintaan liittyen. Yhteistyö on kuitenkin nostettava asiana omakseen, sillä hyvä yhteistyö auttaa haasteisiin vastaamisessa. Yhteistyössä noudatetaan kahdenvälisiä sopimuksia ja hyödynnetään esimerkiksi Katakri-auditointivaatimuksia. Neljäntenä näkökohtana on tutkimus ja kehitystyö. Yhden haastateltavan edustamalla organisaatiolla on käytössä jopa oma tutkimusosastonsa, joka vastaa uuden tiedon hankinnasta, työkalujen kehittämisestä

ja uusien tapojen oppimisesta, joita sitten jalkautetaan organisaation toimintaan. Vastaavanlaista toteutustapaa ei ilmennyt muiden haastateltavien puheista, mutta haastattelujen pohjalta pystyi ymmärtämään, että tutkimusta ja kehitystyötä tehdään muissakin organisaatioissa.

> Aina sitä pyritään ajankohtaisia ilmiöitä sitten viestinnällä tuomaan esiin kaikille työntekijöille, että tällaistakin taas tapahtuu. Niin uhkatietoa tulee sitten ihan tuota niin niin viranomaiselta traficomilta esimerkiksi ja sitten erilaisilta valmistajilta. Siellä tulee esim. tietoja haavoittuvuuksista ja muista hyökkäys- tai sähköpostikampanjoista. (Haastateltava 2)

> Aika laaja asia sinällään et jos niiku ajatellaan et niiku sanoit et me pyritään tommosen niiku uhkakuvan kautta muodostamaan sitä käsitystä, että mikä on sellasta mihin pitäs reagoida tai mitä pitäs kehittää niin ne lähteethän on, niitähän on tietenkin lukematon määrä maailmassa. Alkaen nyt vaikkapa lähimpänä kyberturvallisuuskeskuksen erilaiset jakelulistat ja nyt on ihan äskettäin perustettu myös organisaatioiden ISAC-toiminto ja sit tota kun me käytetään tuolla teknisessä valvonnassa työkaluja niin niihin voidaan, sitä voidaan niiku rikastaa sitä oman tilannekuvan, sisäisen tilannekuvan muodostamista erilaisilla ulkoisilla lähteillä, joita sitten käytetään, kun pyritään arvioimaan, että minkälaisia uhkia on olemassa. Elikkä tavallaan se dokumentoituu sitä kautta ummm semmosta, tää niikku kiteytyy minun mielestä tämmöseen tilannekuvan muodostamiseen. (Haastateltava 9)

> Seuraamalla aktiivista, että mihin suuntaan maailma on menossa, että sehän se on se paras tapa ja sitten tuota tietysti tämmöinen niinku aktiivinen tiedonvaihto sekä meidän kumppaniyritysten että viranomaisten kesken. Sillä tavalla niinku pysytään kartalla siitä mitä muut on tekemässä. Se on ehkä ne keskeisimmät keinot. (Haastateltava 4)

> Meillä on tämmöinen niin kun tavallaan tutkimusosasto, se ei sillä nimellä kulje, mutta niinku se tutkimusosasto, joka vastaa siitä, että siellä on tätä tietoa, kehitetään työkaluja ja niinku opitaan uutta ja sitten jalkautetaan siihen turvaorganisaatioon. (Haastateltava 8)

> Siis pyritään kouluttamaan koko henkilökunta, että ihmiset havaitsisi, jos nyt sitten tulee vaikka jostakin oudosta sähköpostiosoitteesta postia tai tämmöisiä huijausviestiyrityksiä tai niin pyritään pitämään yleissivistystä porukalla, että ne on hereillä, että nyt ei kannata ehkä tota linkkiä klikata, että se ei ole pankin välttämättä virallinen osoite mihin sen jälkeen menee. Että näitä erilaisia tietoiskutyyppisiä meillä on joka toinen viikko. Henkilöstötunti, jossa on aina yksi vakioaihe. Aiheena on nämä IT asiat, jos siellä on jotain meneillään jotain huijauksia tai jotakin on tapahtunut niin siitä samantien tiedotetaan ihmisille ja pyritään pitämään ajan tasalla. Että se on ehkä se meidän rooli enemmänkin, että ylläpitää sitä, määritellä sitä osaamista koko jengillä. ...ja me pyritään pysymään ajan tasalla. Tavallaan jonkinnäköistä, ei sitten ole riskianalyysiä, mutta sen tapaisella ajattelulla, että pyritään pysymään ajan tasalla tilanteesta ja tekemään toimenpiteitä, mitä voidaan etukäteen tehdä. (Haastateltava 5)

> Joo mä joudun tähän nyt vähän vastaamaan sillain niin kun kieli keskellä suuta elikkä tuota niin. Tietenkin meillä niin kun on tota ICT toimittajien kanssa on niinku hyvin läheiset, läheistä yhteistyötä. Ja nythän kun me ollaan Katakri auditoitu yritys ja sitten

mikäli meillä nyt on semmoisia ICT toimittajia, jotka sitten ylläpitää, vaikka meille semmoisia järjestelmiä, jossa on niinku tietoturvaluokiteltuja aineistoja, niin myöskin nää meidän alihankkijatoimittajat on sitten velvoitettuja ja toimimaan Katakrin mukaan. Ja siellähän on niinku tietyt vaatimukset sille, miten niinku pysytään ajan tasalla. No sen lisäksi tietenkin luonnollisesti, niin meille tulee nää certin (Kyberturvallisuuskeskuksen CERT-toiminto) ja Traficomin kaikki tiedotteet missä sitten on niin kun, on tota näitä haavoittuvuuksia ja mitä nyt maailmalla on nähty. Mutta sitten tota, kun me ollaan nyt tässä, kuitenkin kohtuullisen lähellä tätä pääasiakasta toimitaan, niin meillä saattaa olla sitten jotain semmoisia kanaviakin missä niinku tilannekuva liikkuu kumpaankin suuntaan, että me saatetaan se toimittaa sitten jollekin viranomaiselle ja me saadaan taas sieltä semmoisia niinku indikaatioita, että nyt on niinku nähty siellä tämmöistä ja tuolla tommoista, että pitäkää silmänne auki, että tota niin sanoisin, että meillä on niin kun hyvin valveutunut tää verkosto ja tää tilannekuva. (Haastateltava 7)

7.3.4 Osaajapula

Haastatteluissa kävi ilmi, että kyberturvallisuuden osaajista on pulaa. Kovin syvälle osaajapula keskusteluun ei haastatteluissa päästy, mutta suhteellisen selvästi tuli esille se, että työtä olisi tarjolla, mutta sopivia hakijoita ja osaajia ei löydy halutulla tavalla. Etenkin erikoisosaamista ja niin sanottuja kovemman luokan tekijöitä kaivataan. Osaajapulaan liittyvässä keskustelussa nousi esille mielenkiintoinen ongelma. Työnhakijoilla voi olla osaamista eri osa-alueilla, mutta kokonaiskuvassa osaaminen saattaa jäädä kuitenkin vajavaiseksi, joko teknisten niin sanottujen kovien taitojen tai pehmeiden taitojen ontuessa.

Vaan se fakta, että semmoisia kovan luokan, vaikka teknisen tietoturvan osaajia niitä ja niitä niinku maailmassakaan nyt niinku ihan joka nurkassa ole, että tietysti sen tietyn tyyppiset semmoiset niinku kärki etenevät niin niitä aina vähän vaikeampi sitten löytää ja niitä nyt on, mutta että saisi niitä olla enemmänkin. (Haastateltava 3)

...olisi duunia vaikka kuinka paljon niinku koko ajan tuntuu, että puuttuu asiantuntijoita, aina tarvitsisi lisää. Sitten mistä sä saat niitä niin en tiedä tai mistään. (Haastateltava 6)

Mä voisin puhua yleensä ottaen siitä, miten niinku se työmarkkina näyttäytyy meille, niin siellä on. Siellä on niin kun selvästi havaittavissa puutteita siinä, että niinku niillä ihmisillä, jotka hakeutuu kyberturvatehtäviin, on hyvin vaillinainen verkko osaaminen. Joka on niinku todella kriittistä. Kuitenkin sitten, jos niinku yleensä ottaen jos kyberturvaa tehdään niin jossainhan se kulkee se kyberuhka ja se tuppaa olemaan tietoverkko missä se kulkee. Jos et sä ymmärrä miten se toimii se tietoverkko niin sä et pysty sitten lopulta niinku kovinkaan hyvin mitigoimaan sitä. (Haastateltava 8)

...tilanne on tällä hetkellä sellanen, että niiku tietoturva tai kyberturvaosaajista, tämmösistä kovista teknisistä osaajista on huutava pula. (Haastateltava 9)

Eräs haastateltavista nosti esille tärkeän ja mielenkiintoisen havainnon pehmeiden taitojen osaamisen osa-alueesta, joissa on puutetta kyberturvallisuuden alalla töitä hakevilla. Vaikka hakijalla olisi tekninen kyberturvallisuusosaaminen kunnossa, saattaa puutteita olla perustaidoissa, kuten yhteistyötaidoissa, kirjoittamisessa tai puhumisessa eli ihmisten välisissä vuorovaikutustaidoissa.

> Ja sitten yksi mitä ehkä niinku unohtanut tässä korostaa, niin varsinkin tämmöisessä konsultointityössä. Niin tota vaikka se on kyberturvallisuus tai mikä tahansa se aihe, niin siellähän korostuu tosi paljon semmoiset osaamiset niinku ihan, että osaako puhua kirjoittaa, kuunnella ja esittää asiansa. Ja ne on yllättävän tärkeitä taitoja, että tota kyllä se puute saattaa olla ihan näissä perustaidoissa sit. (Haastateltava 3)

7.3.5 Henkilöroolit

Osa haastateltavista tunnisti kyberturvallisuusosaamisen hallintaan ja tiedolla johtamiseen liittyviä henkilörooleja, mutta toteutustavat haastateltavien organisaatioiden välillä vaihteli merkittävästi. Muutama haastateltava tunnisti organisaatiostaan yhden tai kaksi henkilöä, joiden vastuulla on kyberturvallisuuden tiedolla johtaminen sekä osaamisen hallinta. Kun taas muutamassa organisaatiossa henkilöitä on selvästi useampia jaettuna vastaamaan pienemmistä osa-alueista, jolloin kyberturvallisuusosaamisen hallinnan ja tiedolla johtamisen kokonaisuus muodostuu näistä pienemmistä osa-alueista ja useammista henkilöroolesta. Eroavaisuuksiin on todennäköisesti vaikuttanut organisaatioiden koko. Osa haastateltavista osasi vastauksessaan erottaa osaamisen hallinnan tiedolla johtamisesta ja kuvailla kuinka ne on toteutettu eri roolien kautta. Esimerkiksi yhden haastateltavan mukaan on henkilöitä, jotka omistavat dataa ja sitten on niitä, jotka tuottavat dataa, eivätkä nämä ole samoja henkilörooleja.

> Se on minun roolissani ja sitten mulla on tossa, meillä on pieni tiimi, niin mulla on tossa toinen henkilö, joka on osallistunut aktiivisesti myös tähän niiku osaamisen kehittämiseen ja hallintaaan. Elikkä käytännössä jos nyt pitää sanoa henkilötyömääriä niin meit on puoltoista henkilöö joilla on tietenkin paljon muitaki tehtäviä mutta joiden vastuulla se on se osaamisen hallinta. (Haastateltava 9)

> Rooli on varmaan mulla nyt, jos puhutaan siitä, että joka on vastuussa henkilöstön perusturvan osaamisen kouluttamisesta, esimerkiksi että se taso on riittävä, niin sehän vastuu on mulla. Eli tietoturvapäällikkö ja siihen sitten tota mua ylemmät tahot on sitten vastuussa, että siihen riittävä budjetointi löytyy ja minä viestin sitten tätä asiaa yleiesti alas ja sivuille. (Haastateltava 2)

> Meillä menee niin, että että tota niin kuin tietysti jokaisella esihenkilöllä on se oman osa alueensa. Se vastuu siitä, mutta sitten sen lisäksi niin kun esimerkiksi tässä kyberissä niin koulutus sisältöihin ja muihin niin tästä mun yksiköstä tulee sitä ohjausta ja samaten sitten meillä on myös erikseen turvallisuusyksikkö, joka vastaa niinku niin

> sanotusti siitä organisaatioturvallisuuspuolesta niin sieltä tulee myös näitä niinku johtamiseen liittyviä rooleja. (Haastateltava 4)

> Joo, onhan meillä joitain ihmisiä, joiden tehtävä on ihan niinku koko firma tasolla, ei pelkästään keskittyä niinku tietoturvallisuuteen vaan kaikkeen niinku koulutukseen ja osaamiseen. Niin koordinoida näitä erinäköisiä koulutuksia ja osaamisen kehittämistä mitä mitä me firmassa tehdään. Eli meillä on ihan niinku kokopäivä toimisia ihmisiä, jotka tota tekee sitä, mutta sitten jos ajattelee tätä kyberturvallisuutta. Niin tietenkin meillä on ensinnäkin globaalisti ihmisiä, jotka tekee ja järjestelee erinäköisiä koulutuksia... No meillä ehkä sitten enemmän, jos ajattelee sitä tiedolla johtamista, niin se olisi enemmän sitä niinku liiketoiminnan niinku numeroilla johtamista, että miten tota miten tässä noin niinku numeroiden valossa menee. (Haastateltava 6)

> On joo, kyllä on. Joo en voi avata tarkemmin. Eli lähinnä vaan se, että niitä on myös erillään tai ehkä vähän on eri puolilla eri puolilla organisaatiota, että on niitä, jotka huolehtii tai omistaa dataa ja sitten on niitä, jotka tavallaan tuottaa dataa ja ne ei ole samoja henkilöitä. (Haastateltava 8)

Tunnistetuissa kyberturvallisuuden tiedolla johtamisen sekä osaamisen hallinnan henkilörooleissa ei juuri vaadittu rooliin valitulta henkilöltä etukäteen suoritettuja sertifikaatteja tai yleisiä standardeja. Muutama haastateltava koki, että yleisesti ottaen sertifikaattien avulla käsitteet tulevat tutuksi ja perusymmärrys kyseisen aihepiirin asioista näkyvämmäksi mutta ne eivät välttämättä tee henkilöä paremmaksi työssään. Suoritetut sertifikaatit nähtiin olevan hakijan etu mutta niitä ei pidetty pakollisena. Haastateltavat kertoivat yrityksen kouluttavan henkilöstöään ja tukevan halukkaita sertifikaattien suorittamiseen. Kuitenkin yleisesti ottaen vastauksista selviää, että osaaminen pitää jollain tavalla todentaa jo rekrytointivaiheessa.

> No sertifikaatteja meillä ei oo kovin aktiivisesti suoritettu, itseasiassa itselläkään ei taida olla, kun yks ainoo sertifikaatti ja sekin on jo vanhentunut. Niin tota ei, ei pidetä kirjaa, kun ei meillä niitä ole. Me ei, ihan hirveesti noihin sertifikaatteihin uskota. En sano, etteikö niistä olis jotain hyötyä ja nehän on tämmösiä hyviä, niihin liittyy monesti tää niiku käsitteiden harmonisointi ja se on niiku hyvä asia niissä sertifikaateissa mut ei meillä oo siihen panostettu eikä oo pidetty sitä erityisen tärkeänä asiana. (Haastateltava 9)

> Kyllä meillä on rekryn vaatimuksia, että pitää olla jollain tavalla osoitettua osaamista tietyistä asioista ja sertifikaatit ei välttämättä ole aina vaatimuksena, mutta ne on ehdottomasti eduksi. Tai jollain muulla tavalla osoitettu kokemus sitten samoista asioista. (Haastateltava 2)

> Ei ole. Ei ole ollut silleen, että niinku tuossa vähän mainitsin, että meillä ehkä mitataan sitä niinku asian ymmärrystä vähän niinku niitten sertifikaattien ulkopuolelta. Että toki sitten jos sulla on joku siisti tai mitä näitä nyt onkaan niin se antaa tietyn perusymmärryksen tason niinkun näkyväksi. Mutta sitten niin kun tekeekö siitä ihmisestä paremman siinä työssä niin ei. (Haastateltava 4)

> Ei käsittääkseni hakuvaiheessa taideta vaatia, mutta ne on aina niinku ehdoton plussa, että jos niitä on, niin kyllähän semmoinen hakija aina menee ohi... ... tärkeämpää on se että siellä on niinku laaja alaista osaamista kuin se että on sertifikaatteja. (Haastateltava 8)

> On käytössä elikkä meillä asiakas saattaa vaatia tiettyjä sertifikaatteja ja tietenkin mielellään rohkaistaan omaa henkilöstöä sitten käymään tota niin sen tyyppisiä koulutuksia. Eli siis tota niin kyllä meillä niinku lähdetään siitä, että me koulutetaan sitten henkilöstölle ne kelpoisuudet ja sertifikaatit mitä he työssään tarvitsee, että ei meillä ole ollut ainakaan rekrytointien osalta niin kovia vaatimuksia, että vielä siinä kohtaa niinku vaadittaisi semmoista tiettyä sertifikaattia. (Haastateltava 7)

7.4 Tiedon ja osaamisen välinen vuorovaikutus

Hongin ja Ståhlen mallin (Kuvio 8) mukaisesti organisaation strategia osoittaa toiminnalle rajat ja tavoitteet, jonka mukaan niin tiedolla johtamisen ja osaamisen hallinnan periaatteita sovelletaan organisaation sisäisen tietotaidon kehittämiseksi ja sen kohdentamiseksi. Mallin mukaan vuorovaikutus yhdistää tiedolla johtamisen ja osaamisen hallinnan toisiinsa luoden tiedon ja osaamisen johtamisen kokonaisuuden. Tästä syystä vuorovaikutuksen ymmärtäminen on erittäin tärkeää. Haastateltavilta kysyttiin haastatteluissa sitä, mikä on heidän mielestään tiedon ja osaamisen välinen suhde ja kuinka kerätty tai omattu tieto muunnetaan osaamiseksi.

Keskeistä oli, että haastateltavat ensinnäkin tunnistivat, että tiedon lähteitä on useita, ja tietoa saadaan ja kerätään niin talon sisältä kuin sen ulkopuoleltakin. Haastateltavien vastauksista nousi myös esille aktiivisen tiedonkeruun ja tulkinnan tarve. On tärkeää, että toiminnan kannalta oleellista tietoa aktiivisesti pyritään kääntämään osaamiseksi. Tämä tarkoittaa haastateltaville sitä, että saatua tietoa pyrittiin tulkitsemaan ja jakamaan tehokkaasti. Yleisesti ottaen havaintona vastausten laadusta sekä haastateltavien ulosannista paistoi läpi halu kehittyä ja oppia uutta.

> Tietoahan saadaan talon ulkopuolelta. Erilaisin tavoin. On tota semmoista asiakkailta saatua tietoa ja kokemusperäistä tietoa ja opittua tietoa. Viranomaismääräykset. Ja tota, tietenkin vähän riippuen, että mihinkä tota osa-alueelle aina mikäkin tieto sitten vaikuttaa, mutta kumminkin niin. Se ehkä eniten on sitä työssäoppimista ja tiedon jakamista siinä työn tekemisen ohessa, että se niinkun voisi sanoa, että niinku tämmöinen asiantuntijaorganisaatio on enemmän ku yksilöiden summa. (Haastateltava 1)

> No mä ehkä koko ajan ajattelen sitä samasta vinkkelistä, että se tieto mitä kerättäisi olisi niinkun tavallaan markkinoiden tarpeita ja sitten siinä on se linkki, että osaamisen pitäisi vastata niihin tarpeisiin, että meidän tyyppisessä liiketoiminnassa menee aika suoraan yleisesti näin, että tiivistetysti siinä se vastaus, että pitäisi olla niinku hereillä siellä ihan niinku koko ketjun, että myynnistä valuu tieto sitten sinne niinku tiimeihin

ja esimiehille ja muille, että OK tämmöiselle nyt meidän mielestä on kysyntää, ja ollaanko me valmiita vastaamaan. (Haastateltava 3)

Siinä on se vissi ero, että saadaanko se tieto sidottua osaksi sitä päivittäistä tekemistä. Niin jos me kerrotaan niille ihmisille siellä, että älkää laittako tunnuksia tänne ja älkää klikatko niinku klikatko niitä linkkejä. Niin he on saanut sen tiedon. Mutta sitten se on osaaminen siinä vaiheessa, kun he osaa toimia sen tiedon pohjalta... ... se pohjautuu siihen koulutukseen. (Haastateltava 4)

Kaikki tämmöinen niinku kerätty tieto niin sitähän ei välttämättä ihan tälleen niinku koulutusmielessä edes niinku muuteta osaamiseksi, jos niikun ajattelee, että tämmöinen kerätty tieto mitä tota niinkun millä johdetaan liiketoimintaa. Totta kai siinäkin nyt osaaminen kehittyy, kun sä seurailet, että miten tää bisnes menee ja näin. Mutta jos puhutaan tällaisesta niinku ihmisten substanssiosaamista ja siitä, että vaikka meidän asiantuntijat osaa jotain tiettyjä turvallisuuteen liittyviä asioita tai tekniikoita ja näin. Ja sitten kun siihen liittyen kerätään jotain tietoa vaikka jostain uudesta regulaatiota tai suunnasta, mihin joku tietty bisnesalue on menossa tai tota vaikka toimiala on menossa että joku ja jollain toimialalla nähdään, että niiden sitten ympäristö tulee muuttumaan tällä ja tällä tavalla ja sillä on tällaista ja tällaista regulaatiota, niin niin tommoinen tietohan sitten pitäisi jatkojalostaa osaamiseksi ehkä niin, että meidän pitää ensinnäkin kertoa kaikille ihmisille jollain tavalla ja yleensä me koitetaan tehdä tällaisia. Mikähän se suomenkielinen termi nyt sille olisi… tällaisia niinku leadership papereita eli jotain niinku, en minä tiedä mikä se on Suomessa, mutta siis jotain sellaista niinku että missä kerrotaan että tää toimiala on menossa tähän suuntaan. Täältä tulee tällaista ja tällaista regulaatiota ja me pyritään sitten tuolla tavalla kouluttaa sekä niinku meidän asiakkaita ymmärtämään, että tällaisia asioita tulee tapahtumaan lähitulevaisuudessa teidän toimialalle ja sitten meidän omia ihmisiä siihen, että maailma on nyt menossa tonne suuntaan, että katsokaa tota ja pysyä itsekin kärryillä siitä, että tuonne suuntaan on menossa ja sitten meidän pitää tietysti miettiä, että mimmoisia koulutuksia on jostain saatavilla tai itse järjestettävä. (Haastateltava 6)

Se tieto niin niin kyllä me se käännetään saman tien sitten sinne niinku sillä tavalla että mitä se vaatii tavallaan niinkun että siitä koko organisaatio osaa ottaa sitten opikseen. (Haastateltava 7)

Mielenkiintoinen asia nousi myös esille erään haastateltavan kohdalla liittyen ihmisten johtamisen taitoihin, ja taitoon tunnistaa ihmisluonteelle tyypillisiä käyttäytymistapoja. Haastateltava tunnisti koulutusten järjestämisen olevan hyvä tapa muuttaa tietoa osaamiseksi, mutta tunnisti samalla, että koulutettavan asenne ja suhtautuminen koulutukseen voi muuttua sen perusteella kuka kyseistä koulutusta pitää vaikka asiasisältö olisikin sama.

Sekin on jännä juttu, että jos minä menen pitämään koulutusta tai tulee ulkopuolinen asiantuntija, vaikka me puhuttaisiin täsmälleen samalla tavalla, mutta se herättää heti niinku mielenkiintoa, kun tulee nyt ulkoa joku, että hetkinen nyt taitaa olla ihan vakavasti otettava juttu. Ja tota ja sitä kautta, kun se kaveri sitä omaa tietoa jakaa niin sitä osaamista rupeaa syntymään. (Haastateltava 5)

Hongin ja Ståhlen (2005) mallin sisältämään vuorovaikutukseen saatiin myös hyvin suoria viitteitä, kun haastateltava kertoi organisaationsa toimivan hyvin mallin mukaisesti kehittäen aktiivisesti toimintaansa niin, että tiedolla johtamisen ja osaamisen hallinnan periaatteet vuorovaikuttavat keskenään johtaen siihen, että organisaatio itsessään pystyy uusiutumaan ja kehittämään toimintaansa.

> "Meillä on niin se pyritään tiimeihin kouluttamaan hyvät opitut asiat. Kun me mitataan jotain esimerkiksi poikkeamien hallinnassa. Siellä on meillä sitten yleispalaveri vaikkapa sitten prosessin lopuksi, että mikä meillä meni vikaan, missä meillä kesti kauan, mikä meillä ei onnistunut. Me kerätään siitä dataa. Sitten me kehitetään osaaminen niihin kohtiin, muokataan omaa toimintaa, että se niinkun kuuluu prosessiin meillä esimerkiksi poikkeamien hallinnassa. Se on pakko ottaa siihen että eihän se muuten kerätty tieto valu mihinkään kentälle sitten, jos ei huolehdittaisi että se sinne menee." (Haastateltava 2)

> "Voiko rivien välistä lukea, että siellä on keskusteleva ilmapiiri?" (Haastattelija)

> "No kyllä joo, että se upotetaan nimenomaan se jatkuva parantaminen osaksi prosessia, että näin vastaisin. Onneksi meidän firmassa näistä sitten keskustellaan eri tiimien välillä, että mikä toimii mikä ei tai, että nyt näyttää siltä, että tässä on vähän tekemistä." (Haastateltava 2)

> Koetko keskustelun tärkeäksi? (Haastattelija)

> Erittäin. (Haastateltava 2)

8 POHDINTA JA JOHTOPÄÄTÖKSET

Tässä luvussa edetään tutkimuksen kannalta ensimmäisessä alaluvussa pohdintaan, jossa syvennytään pohtimaan tarkemmin edellisessä luvussa esiteltyjen tuloksien merkitystä yleisesti teoriaan nähden sekä suhteessa ennalta asetettuihin tutkimuskysymyksiin. Tavoitteena on tunnistaa tutkimustuloksien todellinen merkitys. Toinen alaluku pyrkii tekemään tutkimuksen kannalta oleelliset johtopäätökset pohjautuen pohdinnan lopputuloksiin. Tarkoituksena on luoda lopullinen vastaus asetettuihin tutkimuskysymyksiin ja saattaa tutkimus tulosten pohjalta päätökseen.

Kaksi viimeistä alalukua ottavat kantaa tutkimuksen rajoittaviin tekijöihin sekä mahdollisiin jatkotutkimusaiheisiin. Rajoittavien tekijöiden kriittinen tarkastelu on tutkimuksen kannalta yhtä oleellista kuin itse tulosten tulkitseminen, sillä tutkimuksen tekemiseen liittyvät rajoittavat tekijät vaikuttavat yhtä lailla tuloksiin, pahimmassa tapauksessa jopa sysäten tutkimuksen pois raiteiltaan tai vääristäen tuloksia esimerkiksi liian suppean tai väärin kohdistetun aineiston takia. Myös tutkimuksen mahdollisia jatkotutkimusaiheita on syytä pohtia, jotta tutkittavaa ilmiötä tai siihen liittyvää toista ilmiötä voidaan jatkotutkia ja näin ollen syventää tietoisuutta entisestään.

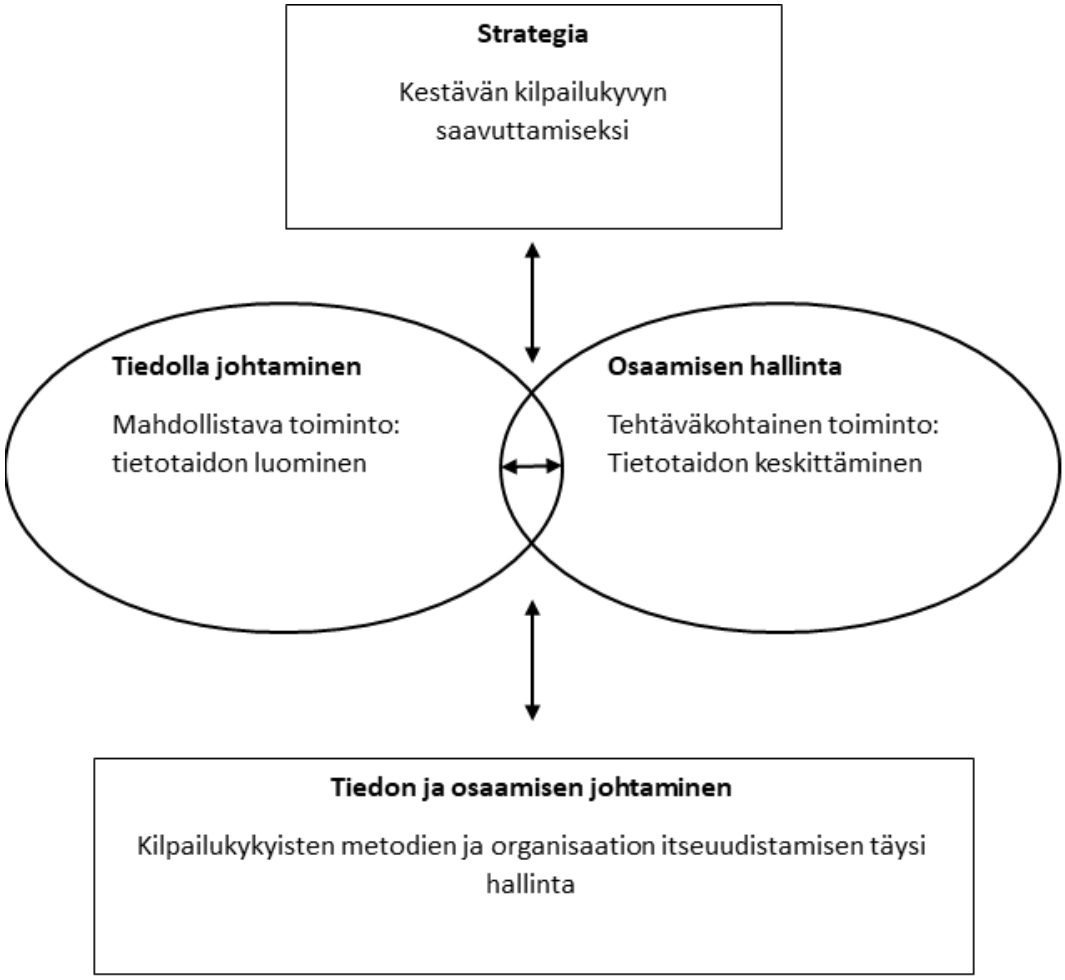
8.1 Pohdinta

Tutkimusraportin luvussa 5 teimme ensimmäisen teoriapohjaan perustuvan johtopäätöksen. Esitimme, että kyberturvallisuus on ilmiö, joka on johdettavissa ja hallittavissa, kyberturvallisuuden lähinnä luoden kontekstin, jossa osaamisen hallinnan ja tiedolla johtamisen käytänteitä voidaan soveltaa. Otamme tähän väliin lyhyen kertauksen siihen, miksi tulimme tähän johtopäätökseen.

Kirjallisuuskatsaus tutkimuksen kannalta tärkeisiin kolmeen aihealueeseen osoitti ensinnäkin sen, kuinka tiedolla johtamisen ja osaamisen hallinnan teoria mukailee vahvasti toisiaan näiden kahden ilmiön sisältäen monia yhteneväisiä prosesseja. Olennaista on myös tiedon ja osaamisen välinen suhde.

Kyvykkyyksien ajatellaan olevan niitä mitattavissa olevia henkilön piirteitä, joita tarvitaan tietyssä työtilanteessa tietyn työtehtävän suorittamiseen (Klendauer ym., 2012). Kyvykkyyksien tehokas hallinta on puolestaan läheisesti yhteydessä erinomaiseen suorituskykyyn, ja kyvykkyydet itsessään edustavat tietoa, taitoa ja käyttäytymistä, jotka kontribuoivat yrityksen menestykseen (Prahalad & Hamel, 2003). Näin ollen voidaan tämän tutkimuksen kannalta todeta kyberturvallisuuden olevan sekä yksittäisten ihmisten että organisaatioiden tietoisuutta ja kyvykkyyttä toimia kyberturvallisella tavalla. Näistä asioista mm. Lehto (2022) puhuu toimenpiteinä, joilla sekä suojaudutaan että toteutetaan vastatoimenpiteitä kyberhyökkäyksiä vastaan. Kyberturvallisuusosaamisen johtamisesta ja hallinnasta on entuudestaan hyvin vähän tutkimusta, mutta onneksemme Wang ja Wang (2019) ovat tutkineet tiedolla johtamista kyberturvallisuuden näkökulmasta, ja voimme käyttää heidän tutkimustaan jollain tapaa vertailukohteena saatujen havaintojen suhteen. Kyberturvallisuusosaamisen kattaessa sekä tietoa että taitoa, on tutkimuksen kannalta järkevää tarkastella kyberturvallisuusosaamisen johtamisen ja hallinnan prosesseja yhdessä.

Tästä syystä päädyimme käyttämään tutkimuksen teoreettisena viitekehyksenä Hongin & Ståhlen (2005) muodostamaa mallia (Kuvio 9), joka käsittää sekä tiedolla johtamisen että osaamisen hallinnan käsitteet ja linkittää onnistuneesti kaksi ilmiötä yhdeksi tutkittavaksi kokonaisuudeksi. Mallin (Kuvio 9) mukaisesti organisaation strategia osoittaa toiminnalle rajat ja tavoitteet, jonka mukaan tiedolla johtamisen periaatteita sovelletaan organisaation sisäisen tietotaidon kehittämiseksi. Osaamisen hallinnan periaatteita puolestaan hyödynnetään tehtäväkohtaisemmin suorittamaan tehtäviä, kohdentaen luotua tietotaitoa.



KUVIO 9 Tiedon ja osaamisen johtamisen malli. (Hong & Ståhle, 2005)

Hong ja Ståhle (2005) korostavat näiden kahden ilmiön välistä vuorovaikutusta, ja tunnistavat tiedolla johtamisen ja osaamisen hallinnan yhtäläisyydet sekä toisiaan täydentävät piirteet. Näin ollen he sijoittavat molemmat käsitteet saman mallin sisään ja käsittelevät molempia ilmiöitä organisaation toiminnan tukipilareina. Mallin perusteella onnistuneella tiedon ja osaamisen johtamisella organisaatio voi saavuttaa sen strategian määrittämät tavoitteet kilpailukykyisten metodien ja itseuudistumisen kautta.

Tämän tutkimuksen tutkimuskysymykset on muodostettu tutkimaan mallin mukaisesti niitä prosesseja ja käytänteitä, joita organisaatiot käyttävät johtaessaan toimintaansa kyberturvallisuuden saralla. Tutkimuskysymykset käsittelivät teorian pohjalta tehtyä johtopäätöstä kyberturvallisuuden johdettavuudesta sekä kyberturvallisuusosaamisen johtamisen ja hallinnan prosesseja, ja näiden prosessien kehittämistä ja toteuttamista. Hyvin vastaavalla tavalla oman tutkimuksensa laadullisen osion toteuttivat Wang ja Wang vuonna 2019. Haastatteluin toteutetussa tutkimusmateriaalin keruussa yleisenä havaintona huomattiin haastateltavien olevan hyvin tietoisia käsitteiden määritelmistä, vaikka eivät välttämättä niitä olleet tietoisesti aiemmin määritelleetkään. Keskeisten,

teoriaosiossakin esiteltyjen, käsitteiden yhtenäinen selvyys on omalta osaltaan tutkimuksen kannalta tärkeää, jotta myös tiedolla johtamisen ja osaamisen hallinnan prosessien tutkiminen organisaatioiden välillä on järkevää. Haastateltavat osasivat määritellä keskeiset käsitteet hyvin ja löysivät samoja yhtäläisyyksiä, ja toisaalta samoja vivahde-eroja, kuin Hong ja Ståhle (2005) mallissaan. Haastatteluissa aiheeseen johdatteleva osio todisti sen, että organisaatioiden edustajat ymmärtävät organisaatioidensa kannalta oleelliset ilmiöt sekä antoi viitteitä siitä, että tiedolla johtamisen ja osaamisen hallinnan prosesseja hyödynnetään organisaatioiden sisällä yleisellä tasolla. Tutkimuksen ensimmäiseksi päätutkimuskysymykseksi asetettiin kysymys:

> *Tunnistetaanko kyberturvallisuusosaamisen olevan hallittavissa ja johdettavissa oleva asia, johon voidaan tiedolla johtamisen ja osaamisen hallinnan menetelmillä vaikuttaa?*

Tutkimuksen kannalta on oleellista, että organisaatiot tunnistavat kyberturvallisuuden olevan sellainen asia, johon he voivat näillä tiedolla johtamisen ja osaamisen hallinnan prosesseilla vaikuttaa samoin kuin esimerkiksi muihin liiketoimintaan vaikuttaviin tekijöihin. Tämä tutkimuskysymys on tutkimuksen kannalta oleellinen siksi, että se luo pohjan Hongin ja Ståhlen (2005) mallin hyödyntämiselle. Mikäli organisaatio ei tunnista kyberturvallisuusosaamisen roolia tai näe sitä osana organisaation toimintaa, jota he voivat tiedolla johtamisen tai osaamisen hallinnan käytänteiden avulla johtaa, ei organisaation toimintaa voida tutkia mallia hyödyntäen tämän tutkimuksen rajoissa. Iloinen yllätys oli, että organisaatioiden edustajat tunnistivat kyllä, että kyberturvallisuuden ja sen tuottaminen vaativat tietoa ja osaamista, ja on täten yhtä lailla johdettavissa oleva tärkeä osa organisaation toimintaa, eivätkä haastateltavat nähneet kyberturvallisuusosaamisen poikkeavan muusta osaamisesta millään tapaa. Asiaan voi toki vaikuttaa myös se, että tutkimukseen valittiin Keski-Suomen alueelta juuri jollain tapaa kyberturvallisuuden kanssa tekemisissä olevia yrityksiä, joista osalla kyberturvallisuus on organisaation liiketoiminnan ydinosaamista. Mutta myös organisaatiot, jotka tunnistivat kyberturvallisuuden olevan toiminnan kannalta mahdollistava ja tukeva tekijä, tunnistivat kyberturvallisuusosaamisen jopa organisaation strategian tasolla, joten pelkästä vientituotteen kehittämisestä ei kyberturvallisuusosaamisen hallinnan ja johtamisen kohdalla voida kuitenkaan puhua.

Hongin ja Ståhlen malli etenee strategian tasolta tiedolla johtamisen ja osaamisen hallinnan prosesseihin ja näiden kahden väliseen vuorovaikutukseen organisaation sisällä. Tätä osaa mallista vastaa tämän tutkimuksen kaksi apututkimuskysymystä.

> *Mitkä ovat kohdeorganisaatioiden kyberturvallisuusosaamisen hallinnan ja johtamisen strategiat ja prosessit?*

Mistä tekijöistä kohdeorganisaatioiden osaamisen hallinnan ja johtamisen prosessit koostuvat?

Nämä tutkimuskysymykset lähestyivät asiaa juuri aiemmin mainitun strategian sekä sen pohjalta luotujen prosessien kautta. Hongin ja Ståhlen (2005) mallin mukaan strategia luodaan kestävän kilpailukyvyn saavuttamiseksi. Käytännössä tämä tarkoittaa sitä, että organisaatio määrittää sille merkitykselliset arvot tai maalit, joita se pyrkii toiminnallaan toteuttamaan tai saavuttamaan.

Haastateltavilta kysyttiin, kuinka kyberturvallisuus kytkeytyy organisaation strategiaan, ja kuinka tämä näkyy organisaation toiminnassa. Osa haastateltavista kertoi, ettei kyberturvallisuus suoraan näyttäydy heidän strategiassaan, mutta kuitenkin strategiasta johdetut tavoitteet ohjaavat myös kyberturvallisuuteen liittyviä prosesseja. Kysymys organisaation strategiasta lienee hankala juuri sen ylätasoisuutensa takia, minkä osa haastateltavistakin tunnisti. Voidaan ajatella, että kyberturvallisuustuotteita ja -palveluita tuottava organisaatio tunnistaa strategiassaan juuri esimerkiksi ylätason liiketoiminnallisia, eettisiä tai ekologisia arvoja, joiden perusteella organisaation toimintaa ja juuri kyberturvallisuusosaamistakin sitten johdetaan ilman, että kyberturvallisuutta erikseen strategiassa mainitaan. Tällaisen organisaation kohdalla voidaan ajatella, että strategia on luotu kyberturvallisuuskuplan sisään, kun taas toisenlaisessa organisaatiossa kyberturvallisuus nähdään tuotettavan palvelun tai tuotteen sijaan toiminnan mahdollistajana ja toimintaa suojaavana tekijänä. Tällöin strategiaa ei ole luotu kyberkuplan sisään vaan kyberturvallisuus tuodaan osaksi strategiaa esimerkiksi turvallisuusnäkökulmasta. Eräs haastateltavista esitti kyberturvallisuuden olevan koko organisaation toiminnan läpileikkaava käsite. Kyseisen haastateltavan organisaatio tunnisti kyberturvallisuuden merkityksen myös strategian tasolla, mutta sen lisäksi se nähdään organisaation toiminnan kannalta merkittävänä tukipilarina.

Tutkimuksen kannalta, kun näitä havaintoja peilataan Hongin ja Ståhlen (2005) malliin, voidaan todeta, että kaikki tutkimukseen osallistuneet organisaatiot olivat määrittäneet mallin mukaisesti strategian avulla raamit, joiden sisällä toimintaa johdetaan. Strategia viittaakin terminä monimutkaiseen ajatusten verkkoon, ideoihin, kokemuksiin, tavoitteisiin, asiantuntijuuteen, muistoihin, havaintoihin ja odotuksiin, jotka muodostavat ohjeistuksen tietyille toimille tiettyjen lopputulosten saavuttamiseksi (Nickols, 2012). Haastateltavat kykenivät määrittämään organisaatioidensa omaavan strategian, joka edellä mainitun määritelmänkin mukaisesti luo ohjeet ja tavoitteet organisaation toiminnalle isossa kuvassa.

Entä kuinka strategia sitten jalkautuu käytännön prosesseihin organisaatioissa? Haastateltavat tunnistivat, että strategian pohjalta on luotava tavoitteita, ja näille tavoitteille mittareita, jotta voidaan mitata organisaation edistyminen tavoitteiden suhteen. Strategiaa ja prosesseja käsittelevässä haastatteluosiossa nousi esiin kolme selvää teemaa; tiedon ja osaamisen kartoittaminen, osaamisen kehittäminen ja hallinta sekä muuttuvan maailman haasteisiin vastaaminen.

Organisaatioiden edustajat kertoivat tiedon ja osaamisen kartoittamisen tarkoittavan usein sitä, että organisaation henkilöstön osaamista mitataan

erilaisin testein. Näin organisaatiot pyrkivät selvittämään henkilöstönsä sen hetkisen osaamisen tason. Tämän lisäksi haastatteluissa haastateltavat kertoivat, ettei tiedon ja osaamisen kartoittaminen rajoitu pelkästään organisaation sisälle, vaan tiedon ja osaamisen tarvetta kartoitetaan myös ulkoisista lähteistä kuten markkinoilta ja seuraamalla ja ennustamalla trendejä ja muutoksia ”kentällä”. Haastateltavien kuvaama prosessi tiedon keruusta täyttää tiedolla johtamisen teorian kuvaukset. Luvussa 2.4 esitelty Choon (2002) tiedon hallinnan sykli (Kuvio 5) käsittää juuri tämän asian ensimmäisenä vaiheena.

Choon malli etenee tiedon kartoittamisesta ja keruusta tiedon organisointiin ja säilömiseen, tiedon jakamiseen, palveluiden tuottamiseen sekä tiedon varsinaiseen käyttöön. Tähän samaan kategoriaan kuuluu myös haastatteluissa tunnistettu osaamisen kehittäminen. Kartoitusvaiheessa saatua tietoa osaamisen tasosta hyödynnetään pohjana tuleville kehitystoimille, kuten koulutustarpeiden tunnistamiseen ja niiden pohjalta luotuihin henkilöstökoulutuksiin. Nämä vaiheet edustavat Choon mallissa tiedon käyttöä. Choo esittää, että tiedon käyttöä seuraa sopeutuva käytös, kunnes sykli pyörähtää jälleen uudelle kierrokselle. Haastatteluissa organisaatioiden edustajat tunnistivat erilaisten koulutusten olevan keskeinen tapa edistää osaamispohjaa samalla, kun organisaatio pyrkii aktiivisesti pysymään ajan hermoilla ja tunnistamaan tarvittavia osaamistarpeita.

Samat teemat toistuvat myös osaamisen hallinnan teorian puolella. Berio & Harzallah (2005) tunnistavat osaamisen hallinnan neljä prosessia (Kuvio 7); osaamisen tunnistaminen, hankitun osaamisen arviointi, osaamisen hankinta ja osaamisen käyttäminen. Nämä neljä prosessia kulkevat lähes käsi kädessä Choon (2002) mallin kanssa, mikä puolestaan vahvistaa entisestään Hongin ja Ståhlen (2005) ajatusta siitä, kuinka tiedolla johtaminen ja osaamisen hallinta vuorovaikuttavat paljon keskenään organisaation etsiessä keinoja oman toimintansa kehittämiseen. Tämän tutkimuksen sisällä viitteitä siitä voidaan huomata edellä mainitusta prosessikulusta. Organisaatio kerää *tietoa* omaamansa *osaamisen* tasosta, ja käyttää tätä *tietoa* hyväksi *osaamisen* kehittämisessä. Osaamisen kehittämisen kautta uusien taitojen implementoitua syntyy uutta *tietoa osaamisen* tasosta ja kehitys jatkuu. Tutkimusta tehtäessä huomattiin siis, että nämä teoreettiset mallit toteutuvat toden totta organisaatioiden sisällä. Huomattavaa on kuitenkin se, että haastateltavien puheista pystyi tulkitsemaan kilpailukyvyn säilyttämisen olevan hyvin vahva eteenpäin potkiva voima, joka ikään kuin pakottaa organisaatioita keräämään tietoa ja jalostamaan sitä osaamiseksi. Täten aikaisempi huomio siitä, että strategia luodaan kestävän kilpailukyvyn saavuttamiseksi ei ole pelkästään ainoa ohjaava tekijä, vaan Hongin ja Ståhlen (2005) mallin viimeinen palikka ”Tiedon ja osaamisen johtaminen - Kilpailukykyisten metodien ja itseuusiutumisen täysi hallinta” tavoitteena ohjaa ja jopa osittain pakottaa tavoitteenaan organisaatiot toimimaan tehokkaasti.

Toki on muistettava, ettei sisäisen tiedon kartoittaminen ole ainoa tapa kerätä tietoa, ja monet haastateltavista mainitsivatkin, että tietoa täytyy kerätä myös ulkoisista lähteistä, kuten erilaisilta foorumeilta ja markkinoilta sekä seuraamalla uusia lakeja tai muita regulaatiouudistuksia. Kaikki saatu informaatio on tärkeää, mutta tärkeää on myös se, että tunnistetaan suuresta määrästä tietoa

juuri se oikea ja oleellinen tieto, jota sitten jatkojalostetaan osaamiseksi. Haastatteluissa oleellisena havaintona kävi selväksi, että tiedon keruussa ja sen jatkojalostamisessa on oltava aktiivinen ja organisaation on omaksuttava kyky haluta oppia.

Haastateltavilta kysyttiin, kuinka organisaatioissa sitten toteutetaan kyberturvallisuusosaamisen hallintaa ja kehitystä. Hongin ja Ståhlen (2005) malliin viitaten tämä kysymys kattaa mallin alimman nuolen ja viimeisen osan, eli sen, kuinka organisaatio kykenee uudistumaan ja pysymään kilpailukykyisenä. Haastatteluissa kävi ilmi, että organisaatiot luottavat erilaisten koulutusten voimaan henkilöstön osaamisen kehittämisessä. Tämä lienee kaikista yksinkertaisin ja oletettavin tapa kehittää yksilön osaamista. Itse koulutuksen järjestämistä haastateltavat eivät tunnista haasteeksi, pikemminkin oikean koulutustarpeen ja -aiheen tunnistamisen. Tässä muutamat haastateltavat löysivät jälleen suoran yhteyden markkinoille. Tieto osaamistarpeista valuu heidän mukaansa aina myynnistä saakka organisaatiolle, ja organisaation on kyettävä vastaamaan kysyntään, jolloin henkilöstöä on koulutettava tarpeen mukaisesti. Haastatteluissa tunnistettiin tarve osata johtaa ihmisiä yksilöinä, jotta heidän henkilökohtaiset mielenkiinnon kohteensa ja koulutustarpeensa voidaan tunnistaa. Mansaray (2019) esittää, että työntekijälle tulisi tarjota "mahdollistava" työympäristö, joka mahdollistaa työntekijän käyttävän ammattiosaamistaan. Ihmisläheinen lähestymistapa ruokkii työntekijän motivaatiota, jolla on suora yhteys työntekijän oma-aloitteisuuteen, joka sekin tunnistettiin haastatteluissa tärkeäksi tekijäksi osaamisen kehittämissä.

Kuten myös aiemmin todettiin, on osaamista mitattava ja täten kerättävä tietoa osaamisen tasosta. Sama pätee myös prosessien hallintaan. Eräs haastateltavista osasikin hienosti nostaa esille sen, että myös kokonaisia prosesseja on arvioitava kriittisesti. Tietoa onnistumisista ja epäonnistumisista on analysoitava, jotta prosesseja ja toimintaa voidaan kehittää. Toisin sanoen tiedon ja osaamisen hallintaa on tehtävä useissa eri tasoissa. Tämän tunnisti myös eräs haastateltavista esitellessään organisaationsa kolmitasoista koulutusohjelmaa, jossa erilaisia taitoja ja tietoja koulutetaan eri rooleissa oleville ihmisille, jotka toimivat organisaatioissa erilaisten toimintojen ja prosessien sisällä.

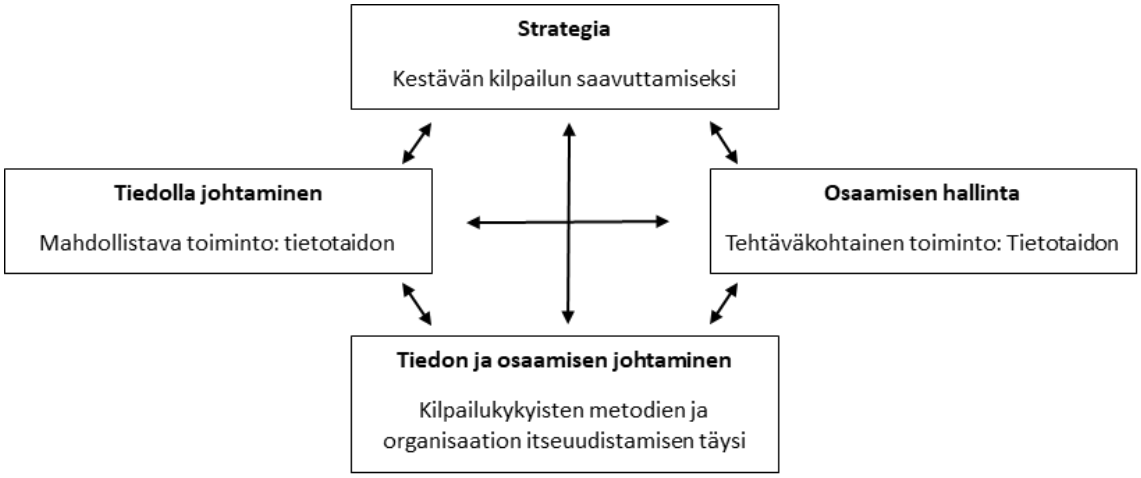
Lopulta on syytä pohtia, kuinka hyvin tutkimukseen valittu teoreettinen viitekehys eli Hongin ja Ståhlen (2005) malli toimii käytännössä. Tähän kysymykseen vastausta etsii myös tutkimuksen toinen päätutkimuskysymys.

> *Miten kyberturvallisuusosaamisen hallintaa ja kehittämistä tulisi toteuttaa organisaatiossa?*

Lyhyesti ja ytimekkäästi kuvattuna haastattelujen perusteella voidaan todeta, että organisaatiot ovat määrittäneet korkean tason strategian, jonka pohjalta organisaatio on luonut toiminnalleen tavoitteet niin organisaation tasolla, kuin pienemmilläkin yksikkö tai tiimitasolla. Strategia siis ohjaa organisaation toimintaa ja määrittää ikään kuin kehyksen, jossa organisaatio toimii. Aivan kuten Hongin ja Ståhlen malli asian ilmaisee. Organisaation prosessien voidaan todeta olevan hyvin johdettuja ja hyvin vuorovaikutteisia kuten aiemmin jo todettiin. Tietoa

kerätään ja tulkitaan, sen pohjalta pyritään kehittämään osaamispohjaa ja jota jälleen analysoidaan uuden tiedon saavuttamiseksi. Samoin ulkoisia tiedonlähteitä pyritään jalostamaan osaamiseksi parhaan mukaan. Kuten Hong ja Ståhle kuvaavatkin mallissaan, ovat tiedolla johtamisen ja osaamisen hallinnan prosessit ja käytänteet hyvin toisiinsa kiinnittyneitä ja vuorovaikutteisia keskenään. Tästä seuraa mallin mukaan tiedon ja osaamisen kokonaisvaltainen johtaminen, ja organisaatio on kykenevä itseuudistumaan ja hallitsemaan kilpailukykyiset metodit, joka voidaan tutkimukseen osallistuvien organisaatioiden kohdalla todeta olevan totta. Asianhan voisi esittää myös niin, että mikäli organisaatiot eivät tähän kykenisi, olisivat ne myös mallin puitteissa kykenemättömiä selviytymään markkinoilla. Mallin voidaan siis todeta olevan kohtuullisen tarkka myös käytännössä.

Kuitenkin mallin osa-alueet ovat kuvattu olevan yhteydessä toisiinsa suhteellisen lineaarisesti, joskin tutkimuksenkin pohjalta voidaan tunnistaa tiedon ja osaamisen johtamisen toimivan hyvin syklimäisesti, kuten myös Choo (2002) on tiedon hallinnan syklissään kuvannut. Tämä havainto perustuu haastatteluissa ilmenneeseen jatkuvaan hereillä olemiseen ja kehittämiseen, jotta organisaatio pysyy kilpailukykyisenä. Hong ja Ståhle ovat kuvanneet mallissaan kyllä vaikutussuhteet kaksisuuntaisina, mutta mielestämme se ei kuvaa tiedon ja osaamisen hallinnan prosesseja täydellisesti. Choon lisäksi myös Berio ja Harzallah (2005) tunnistavat monisuuntaisemman vuorovaikutuksen osaamisen hallinnan neljän prosessin kuvauksessaan. Hongin ja Ståhlen malli voisi siis tämän tutkimuksen perusteella näyttää seuraavanlaiselta (Kuvio 10). Myös haastatteluissa ilmennyt asia esimerkiksi jatkuvasta hereillä olemisesta ja ajantasaisen tiedon ylläpitämisestä puoltaa syklimäisempää ja jatkuvaa prosessia.



KUVIO 10 Päivitetty tiedon ja osaamisen johtamisen malli (mukaillen Hong & Ståhle, 2005)

Näin saadaan muodostettua Hongin ja Ståhlen mallista niin tutkimuksessa todetun kuin teorian pohjalta muodostettujen johtopäätösten mukainen malli, joka käsittelee tiedon ja osaamisen johtamisen prosesseja aiempaa syklimäisemmin, huomioiden kaikkien elementtien välisen vuorovaikutuksen.

Esitetyt havainnot ovat hyvin samantapaisia kuin Wangin ja Wangin (2019) tekemässä tutkimuksessa. He totesivat kyberturvallisuuden hyötyvän tiedolla johtamisen käytänteistä, kun informaation jakaminen on tärkeää kyberturvallisuuden kehittämisessä, ja kun puhutaan ihmisen roolista kyberturvallisuudessa. Wang ja Wang kehittivät tutkimuksessaan myös mallin kuvaamaan tiedolla johtamista kyberturvallisuudessa, sillä huolimatta synergisesti suhteestaan ei tiedolla johtamista ja kyberturvallisuutta ole juuri mallinnettu. Wang ja Wang toteavat tutkimuksessaan, että organisaatioiden tulisi luoda selkeät mallit ja rakenteet kyberturvallisuuden johtamiselle tiedolla johtamisen käytänteitä hyödyntäen. Heidän mallinsa pyrkii juuri siihen, ja kuvaakin informaatiovirtoja hyvin eri toimijoiden välillä ottaen myös ulkoisia tekijöitä huomioon. Ulkoiset tekijät nousivat esille tämän tutkimuksen aikana, ja niihin otetaankin kantaa seuraavassa alaluvussa, jossa tehdään tutkimuksen lopulliset johtopäätökset.

8.2 Johtopäätökset

Tässä luvussa esitellään tiiviisti tutkimuksen tulosten sekä teorian pohjalta tehdyt johtopäätökset. Johtopäätökset ovat linjassa tutkimuskysymyksiin, mutta haastatteluiden ja kirjallisuuskatsauksen perusteella voitiin tehdä muitakin johtopäätöksiä kyberturvallisuusosaamisen johtamiseen ja hallintaan liittyen.

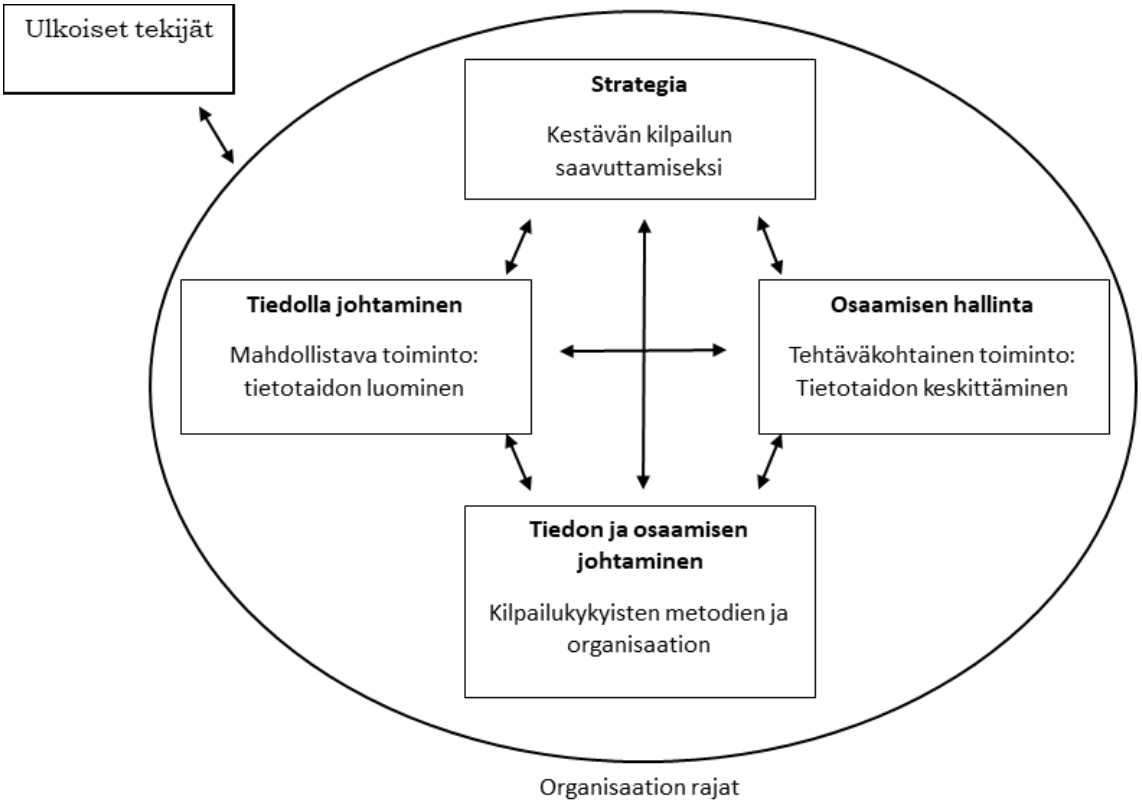
Kirjallisuuskatsauksen perusteella tehty ensimmäinen johtopäätös loi oikeastaan pohjan muulle tutkimukselle. Aikaisemman tutkimuksen perusteella voitiin todeta, että kyberturvallisuus on ilmiönä yhtä lailla johdettavissa ja hallittavissa oleva asia kuin muutkin organisaation ydintoiminnot. Tämä tarkoittaa toisaalta sitä, että sen johtamiseen ja hallitsemiseen tulisi olla myös selkeät prosessit, joiden mukaan organisaatio toimii. Lähdimme selvittämään, kuinka organisaatiot tässä onnistuvat ja tunnistavatko he kyberturvallisuusosaamisen merkityksen tai roolin osana organisaation toimintaa.

Haastatteluiden perusteella voidaan todeta, että organisaatiot tunnistivat kyllä kyberturvallisuuden käsitteenä olevan sellainen asia, että sitä voidaan toden totta johtaa tiedolla johtamisen ja osaamisen hallinnan käytäntein eikä kyberturvallisuusosaaminen poikkea muusta osaamisesta. Huomattavaa oli kuitenkin, että kyberturvallisuusosaamisen johtamiseen liittyviä vakioituja käytänteitä tai selkeitä prosesseja ei välttämättä ollut täysin määriteltynä, joilla kyberturvallisuusosaamista hallittaisiin. Tämä voi johtua siitä, että kyberturvallisuus on ilmiönä vielä suhteellisen nuori ja nopeasti kehittyvä. Toisaalta mahdollista on myös, ettei haastateltavat osanneet haastatteluissa mainita tai tuoda esille hallinnan prosesseja kokonaisvaltaisesti. Joka tapauksessa yhdistävä tekijä oli asian tärkeyden tunnistaminen, vaikka sana kyberturvallisuus ei vielä organisaation strategia tasolla tai johdetuissa prosessikuvauksissa täysimittaisesti näkyisikään. Välillä oli jopa havaittavissa, että kyberturvallisuusosaamista johdettiin hyvinkin Hongin ja Ståhlen (2005) mallin mukaisesti, joskin jossain määrin jopa tiedostamatta. Tästä voidaan päätellä, että organisaation toiminta tunnistaa kyllä tiedolla johtamisen ja osaamisen hallinnan käytänteet toiminnassaan, mutta

kyberturvallisuuden puitteissa niitä käytänteitä ei ole täysin vakioitu tai dokumentoitu. Seuraava askel voisi siis olla kyberturvallisuusstrategian luominen sekä sen implementoiminen osaksi organisaation järjestelmällistä toimintaa.

Kuten aiemmin jo todettiin, Hongin ja Ståhlen (2005) malli on käytännön tasolle vietynä hieman liian lineaarinen. Tutkimuksen perusteella voidaan todeta, että todellisuudessa mallin eri osa-alueiden välillä käydään lopulta enemmän vuorovaikutusta. Tutkimuksessa nousi myös esille ulkoisten tekijöiden vaikutus organisaation toimintaan. Tätä Hongin ja Ståhlen malli ei sellaisenaan tunnista. Haastateltavien puheista nousi esille toistuvasti se, kuinka vahvasti markkinat säätelevät organisaation sisäisiä prosesseja myös kyberturvallisuuteen nähden. Markkinoita tutkimalla organisaatiot pystyvät tunnistamaan osaamistarpeita ja vastaamaan kysyntään vahvistamalla omaa osaamistaan tarpeiden mukaan. Näin organisaatio pyrkii pysymään kilpailukykyisenä hyvin kilpailuilla markkinoilla. Toisaalta haastateltavien esiin tuoma mainehaitta, joka voi syntyä huonon osaamisen takia, on myös merkittävä tekijä, ja vaikuttaa suoraan organisaation kilpailukykyyn. Tarve osaamiselle on siis sekä vientituotteena että oman toiminnan turvaajana ja luotettavuuden merkkinä. Voidaan siis todeta kilpailun olevan vahva motivaattori organisaation toiminnan kehittämiselle, ja täten merkittävä tekijä ohjaamaan organisaation sisäisiä prosesseja.

Tästä syystä päivitimme vielä kerran Hongin ja Ståhlen (2005) mallia ottamaan paremmin huomioon ulkoiset tekijät, jotka vaikuttavat organisaation toimintaan. Uusin versio (Kuvio 11) käsittää nyt sisäisten prosessien laajempien vuorovaikutussuhteiden lisäksi organisaation ulkoiset tekijät, jotka vahvasti ohjaavat organisaation toimintaa. Näitä ulkoisia tekijöitä ovat esimerkiksi lait ja regulaatiot, markkinat sekä kyberalan jatkuva kehitys.



KUVIO 11 Päivitetty tiedon ja osaamisen johtamisen malli huomioiden ulkoiset tekijät

Yhtenä haasteena kyberturvallisuuden alalla oli haastateltavien mukaan tekijöiden puute. Kyberturvallisuusalalla on pulaa osaajista, mutta mielenkiintoisena asiana kävi ilmi se, että näillä osaajillakin on puutetta teoriaosuudessakin mainituista pehmeistä taidoista eli kuuntelu- ja puhumistaidosta, kriittisistä ajattelutaidoista, ongelmaratkaisutaidoista sekä vuorovaikutus- ja yhteistyötaidoista. Juontaako tämä juurensa siitä, ettei tietokoneiden parissa työskentelevät ihmiset välttämättä ole sosiaalisesti yhtä vilkkaita kuin esimerkiksi asiakasrajapinnassa työskentelevät ihmiset? Onko etätyöskentely mahdollisuus haitannut entisestään sosiaalisten taitojen kehittymistä vai onko jopa korkeakouluopinnoissa tarvetta lisätä yhteistyötaitojen kehittämistä, jotta työelämään siirtyvät osaajat todella tulevat toimeen organisaatioissa ja pystyvät aktiivisesti osallistumaan organisaation toimintaan myös työyhteisön hyvinvoinnin puolesta.

8.3 Tutkimuksen rajoitteet

Tutkimuksia arvioidaan tyypillisesti kahden näkökulman kautta: validiteetin ja reliabiliteetin. Validiteetti kuvaa sitä, kuinka hyvin tutkimus mittaa tarkasteltavia ilmiöitä eli tutkii sitä, mitä se lupaa mitata. Toisin sanoen se arvioi tutkimuksen pätevyyttä ja sitä, kuinka hyvin se vastaa tutkimuskysymyksiin tai tavoitteisiin. Reliabiliteetilla tarkoitetaan tutkimuksen tulosten toistettavuutta eli sitä, kuinka luotettavia ja vakaita tulokset ovat, kun tutkimusta suoritetaan uudelleen

samanlaisissa olosuhteissa. Näiden kahden käsitteen avulla pyritään tässä luvussa lyhyesti arvioimaan tämän tutkimuksen luotettavuutta, käyttäen näitä validiteetin ja reliabiliteetin näkökulmia.

Tutkimuksen suorittamiseen liittyi useita merkittäviä rajoitteita, joilla saattaa olla vaikutusta tulosten luotettavuuteen, tarkkuuteen tai laajuuteen. Ensinnäkin haastateltavien määrä jäi vähäiseksi siihen nähden mikä alun perin oli tutkimuksen tavoitteena. Syynä tähän oli se, että tietyt organisaatiot ja henkilöt eivät vastanneet haastattelukutsuun, eivät halunneet osallistua tai eivät voineet mielestään tarjota kaivattua tietoa. Haastattelukutsuja lähetettiin lähes 30 henkilölle ja organisaatiolle muutaman kuukauden ajan ja lopulta saimme 9 haastattelua järjestettyä. Koska haastattelu perustui vapaaehtoisuuteen ja saimme hieman tavoitetta vähemmän vastauksia, on mahdollista, että saaduissa vastauksissa painottuvat enemmän ne ihmiset, jotka ovat jo valmiiksi kiinnostuneita kyseisestä aiheesta. Toisin sanoen ne, jotka tuntevat aiheen entuudestaan, ovat todennäköisemmin osallistuneet haastatteluun. Samalla ne, joille aihe ei ole tuttu, saattoivat jättää helpommin osallistumatta haastatteluun. Tämä voi vaikuttaa tuloksiin siten, että tulokset eivät välttämättä edusta koko perusjoukkoa tasapuolisesti, vaan heijastelevat enemmän niiden näkemyksiä, jotka jo valmiiksi tuntevat aiheen. On tärkeää mainita, että pyrimme aktiivisesti laajentamaan haastateltavien lukumäärää, mutta edellä mainituista syistä haastatteluiden määrä jäi toivottua pienemmäksi. Haastateltavia saimme kuitenkin lopulta sen verran, että tutkimus oli järkevää saattaa loppuun asti. Toteutuneiden haastatteluiden avulla saimme kuitenkin lopulta hyvää ja laadukasta tutkimusmateriaalia, sillä se oli sisällöltään laajaa, kohtuullisen syvää ja rikasta. Haastateltavien henkilöiden näkemykset aihepiiristä saatiin haastatteluiden aikana selkeästi ilmi ja tutkimusmateriaali vastasi pitkälti tutkimuskysymyksiin, joten tutkimuksen validiteetin voi sanoa siten onnistuneen.

Haastateltavat eivät voineet kertoa kaikesta, sillä tutkimuksen aihe ja tutkimuskysymykset liittyivät osittain heidän edustamien organisaatioiden salassa pidettäviin sekä arkaluonteisiin tietoihin. Se asetti rajoituksia siihen, miten hyvin pystyimme ymmärtämään tutkimuskohteita ja haastateltavia. Rajoitteen takia on mahdollista, että saimme vain osittaisen kuvan käsiteltävistä aiheista, koska haastateltavat eivät voineet niin avoimesti tai pureutuvasti kertoa tietyistä asioista. Haastatteluiden aikana kuitenkin vain muutaman kerran haastateltava joutui toteamaan, että ei voi kertoa tarkemmin. Sovimme ennen haastatteluita käytännön, että haastateltavat kertovat, kun eivät voi vastata tarkemmin tai ollenkaan esitettyyn kysymykseen. Tällaisen rajoitteen takia emme välttämättä saaneet täysin syvällistä näkökulmaa tai vastausta haastattelukysymykseen kaikilta haastateltavilta jokaiseen käsiteltyyn aiheeseen.

Tutkimustulosten luotettavuuteen vaikuttaa merkittävästi se, kuinka haastateltavat ymmärtävät eri käsitteet. Jos haastateltavat ymmärtävät eri tavalla käsitteet, voi sillä olla vaikutusta tutkimustuloksiin, koska ei välttämättä puhuta samoista asioista. Vaikka pyrimme varmistamaan, että haastatteluiden pohjalta ei ilmennyt huomattavia eroja, käsitteiden tulkinta haastateltavien välillä voi vaihdella, mikä saattaa vaikuttaa tulosten tarkkuuteen ja vertailtavuuteen. Tässä

tapauksessa voidaan huomata, että haastatteluiden perusteella ei ilmennyt merkittäviä eroja, mikä on positiivista. On kuitenkin huomionarvoista, että täydellisesti toisen henkilön ajatuksiin pääseminen ei ole mahdollista, mikä asettaa rajat täyden varmuuden saavuttamiselle asiasta.

Käsitteiden lisäksi haastattelukysymykset ovat aina toki sellaisia, että haastateltavat voivat ymmärtää niitä hieman eri tavalla eikä rajoitetussa ajassa pystytä käymään kaikkia eri näkökulmia asioihin jokaisen haastateltavan kanssa. Esimerkiksi yksi haastateltava voi nähdä ensimmäisenä kaupallisen näkökulman eikä sen ulkopuolelle poistu vastauksissaan, kun taas toinen haastateltava näkee organisaation oman toiminnan suojaamisen eikä tämän takia puhuta täysin samoista asioista välttämättä. Haastateltavan organisaatio on vaikuttava tekijä eikä voi olettaa, että puhuttaisiin samoista asioista mutta vivahde-erot selittynevät tällä. Myös jokainen keskustelu on yksilöllinen puolistrukturoiduissa haastatteluissa eikä siksi tarjoa täysin vakioituja vastauksia.

Tulosten analysointiin eli tässä tutkimuksessa laadulliseen sisältöanalyysin liittyy oleellisesti subjektiivisuuden riski, koska laadullisessa sisältöanalyysissa vaaditaan tutkijan tulkintaa ja arviointia aiheesta. Se voi johtaa subjektiivisuuteen, sillä eri tutkijat voivat tulkita aineistoa eri tavoin eri ajankohtina. Tätä riskiä pystyimme pienentämään jo lähtökohtaisesti suorittamalla tutkimus kahden tutkijan toimesta mutta myös huolellisella tulosten analysoinnilla eri ajankohtina ja eri näkökulmista. Haastattelukysymyksien laadinnassa hyödynnettiin pitkälti aiheen taustalla olevaa teoriaa sekä kysymysten muotoilua ja asettelua mietittiin luotettavuuden ja toistettavuuden kannalta. Laadullisessa tutkimuksessa tutkijan omat kokemukset, ennakkokäsitykset ja asenteet voivat vaikuttaa tuloksiin niin tulosten analysointivaiheessa kuin jo haastatteluvaiheessa, sillä haastattelut pidettiin puolistrukturoituina sekä tyyliltään keskustelevina. Tätäkin rajoitetta hieman pienentää kahden tutkijan rooli, mutta ollen kuitenkin sen verran merkittävä rajoite, että se täytyi vain hyväksyä laadullisen tutkimuksen ominaispiirteenä.

Tutkimuksemme etenemistä sävytti myös pieni aikapaine, sillä haastatteluiden suorittamiseen ei ollut muutamaa kuukautta enempää aikaa, jotta pääsimme analysoimaan haastatteluiden tuloksia. Tämä aikarajoite vaikutti monin tavoin tutkimuksen kulkuun ja vaati huolellista aikataulutusta ja resurssien hallintaa. Jos aikaa olisi ollut enemmän olisimme voineet saada hieman enemmän haastateltavia, mutta toisaalta ehdimme tuossa ajassa lähestyä potentiaalisia haastateltavia moneen kertaan tuloksetta. Joten aikaa haastatteluiden pitämiselle olisi ollut mielestämme riittävästi, mutta haastateltavien saaminen osoittautui jopa ennakoitua vaikeammaksi.

Lopuksi on hyvä huomauttaa, että vaikka tämän tutkimuksen tulokset tarjoavat arvokasta tietoa, sen tuloksia tulisi tulkita ottaen huomioon edellä mainitut rajoitukset. Avoimuus ja rehellisyys tutkimuksen rajoitteista mahdollistaa tarkan käsityksen näiden tutkimustulosten luotettavuudesta ja antaa perustan mahdollisten tulevien tutkimusten suunnittelulle.

8.4 Jatkotutkimusaiheet

Yhtenä jatkotutkimusaiheena voisi keskittyä järjestelmällisen hallintaprosessin jalkauttamisen vaikutuksiin esimerkiksi yhden organisaation sisällä. Selkeät tavoitteet ja strategiat luovat mahdollisuuden vaikuttaviin prosesseihin, joita sitten mitattaisiin ja edelleen kehitettäisiin mittaustulosten perusteella. Näiden eri osa-alueiden vaikuttavuutta organisaation suorituskykyyn, tehokkuuteen ja tuloksellisuuteen voisi tutkimuksessa selvittää. Tärkeänä kuitenkin arvioida, miten nämä käytännöt ja prosessit käytännössä toteutetaan ja miten ne vaikuttavat organisaation toimintaan.

Jatkotutkimusaiheiden lisäksi huomasimme kehitystoimia tutkimuksen toteuttamisessa. Laaja-alaisemmassa tutkimuksessa pystyisi tarkastelemaan määrällisesti enemmän erilaisia organisaatioita ja niiden hallintaprosessien käytäntöjä. Tässä yhteydessä tutkimuksessa tulisi ottaa huomioon haasteet, kuten palveluiden ulkoistamisen vaikutukset ja miten ne mahdollisesti vaikuttaisivat hallintaprosessien suunnitteluun ja toteutukseen eri organisaatioissa. Kun taas monimenetelmällisen tutkimuksen avulla voi saada syvällistä ymmärrystä eri organisaatioiden käytännöistä sekä kokemuksista. Monimenetelmätutkimuksessa voisi hyödyntää haastatteluja yhdistettynä esimerkiksi kyselytutkimukseen, dokumenttianalyysiin tai havainnointiin saadakseen monipuolisempaa näkökulmaa kyberturvallisuusosaamisen johtamisesta ja hallinnasta. Tällainen lähestymistapa voi auttaa varmistamaan tutkimustulosten luotettavuuden sekä antaa mahdollisuuden syvällisempään analyysiin ja ymmärrykseen.

Kokonaisuudessaan laaja-alaisempi tutkimus tai monimenetelmätutkimus tarjoaisi laadukkaasti toteutettuna arvokasta tietoa kyberturvallisuusosaamisen johtamisen ja hallintaprosessien tehokkaasta suunnittelusta ja toteutuksesta organisaatioissa sekä antaisi suuntaviivoja käytännön kehittämistoimille ja jopa tuleville tutkimuksille.

9 YHTEENVETO

Tutkielman tavoitteena oli selvittää, kuinka kyberturvallisuusosaamisen hallintaa ja kyberturvallisuuden johtamista tulisi johtaa ja kuinka sitä voitaisiin organisaatioissa kehittää. Lähestymistapana oli tutkia ja analysoida organisaatioiden nykyisiä käytänteitä ja toimintatapoja vertaamalla niitä olemassa olevaan teoriapohjaan. Tutkielmassa onnistuimme selvittämään, kuinka kyberturvallisuusosaamisen hallintaa ja johtamista toteutetaan organisaatioissa, kuinka sitä tulisi tehdä, ja kuinka sitä voisi kehittää. Vaikka kyberala on murroksessa ja ala kehittyy koko ajan, on kyberturvallisuusosaamisen hallinnassa ja johtamisessa samat lainalaisuudet, kuin muissakin osaamisen johtamisen ja hallinnan konteksteissa. Toisaalta tutkimus onnistui luomaan uutta teoriapohjaa ja ymmärrystä kehittäen sitä, miten olemassa oleva teoria pystyy vastaamaan modernin, nopeasti muuttuvan ja kehittyvän maailman tarpeisiin tunnistamalla myös organisaatioiden toimintaan vaikuttavat ulkoiset tekijät sekä niiden vaikutuksen myös organisaation sisäisiin prosesseihin.

Teoriaosuudessa tarkasteltiin tiedolla johtamista, osaamisen hallintaa ja kyberturvallisuutta olemassa olevan kirjallisuuden ja tutkimusten avulla. Näistä kolmesta käsitteestä muodostui kolme omaa lukuaan sekä raamit tutkimukselle aihepiirien osalta. Kolme edellä mainittua teorialukua yhdistyi omaksi kokonaisuudeksi "kyberturvallisuusosaamisen johtaminen ja hallinta" luvussa 5. Teoriaosuuden tavoitteena oli johdattaa lukija tutkimuksen äärelle, ja samalla perehdyttää niin lukijat, että tutkijat aiheeseen. Teoriaosuus on lisäksi tärkeässä asemassa tässä tutkielmassa siksi, että sen pohjalta muodostui vertailtavaa aineistoa itse tutkimukseen.

Tutkimukseen haastateltaviksi haluttiin ensisijaisesti sellaisia kyberturvallisuuden alalla vaikuttavia organisaatioita, joilla on toimipiste myös Keski-Suomessa. Mahdollisia kohdeorganisaatioita löytyi 25 kappaletta, joista kaikkia lähestyttiin haastattelukutsun muodossa. Lopulta haastatteluja tutkimuksessa saatiin tehtyä yhdeksän kappaletta. Empiirinen tutkimus toteutettiin laadullisena tutkimuksena kohdeorganisaatioiden avainhenkilöitä haastatellen. Haastatteluiden menetelmänä käytettiin puolistrukturoituja yksilöhaastatteluita, jolla

varmistettiin haastatteluiden joustavuus ja tutkimusaineiston mahdollisimman tehokas ja laadukas kerääminen suhteessa ennalta määriteltyihin tutkimuskysymyksiin. Valituilla tutkimusmenetelmillä vaihtelevuutta voi kuitenkin esiintyä haastatteluvastausten välillä, jolloin tulosten muodostamiseen tarkoiksi tilastoiksi ei ole mahdollisuutta. Toisaalta tarkkaa mitattavaa dataa tuottava määrällinen tutkimus olisi saattanut jättää paljastamatta organisaatioiden todellisia prosesseja eikä esimerkiksi organisaatioiden kulttuuriin olisi päästy samalla tavalla kiinni. Kun tutkimuksen aiheena ja kohteena oli kyberturvallisuusosaamisen hallinnan ja johtamisen ilmiön tutkiminen kokonaisuudessaan, olivat valitut tutkimusmenetelmät perusteltuja.

Kirjallisuuskatsauksessa tarkasteltiin tarkemmin tiedolla johtamisen, osaamisen hallinnan ja kyberturvallisuuden käsitteitä. Aiemman tutkimuksen perusteella selvisi, että sekä tiedolla johtamista että osaamisen hallintaa kuvataan hyvin samanlaisin teoreettisin mallein ja, että käsitteiden sisältämät prosessit mukailevat ja täydentävät vahvasti toisiaan. Tämä voidaan nähdä esimerkiksi siinä, kuinka tiedon elinkaarta kuvataan hyvin syklimäisenä. Tietoa kerätään, analysoidaan, jatkojalostetaan ja lopulta käytetään. Tämän jälkeen prosessi alkaa uudelleen nykytilaa arvioimalla. Osaamisen hallinta käyttäytyy samalla tavalla. Seuraava lause esittänee kahden käsitteen yhteyden varsin tehokkaasti. Organisaation halutessa kehittää toimintaansa, on osaamisen tasosta kerättävä tietoa. Tietoa on analysoitava ja tulkittava uusien kehityskohteiden löytämiseksi. Analyysin pohjalta voidaan kehittää toimenpiteitä, joiden kautta kerättyä tietoa voidaan muuttaa osaamiseksi. Hong ja Ståhle (2005) tunnistavat näiden käsitteiden yhtäläisyyden, minkä takia tämän tutkimuksen teoreettiseksi malliksi valittiin heidän esittämänsä malli (Kuvio 8). Mallin soveltuvuus kyberturvallisuuden kontekstiin todettiin mahdolliseksi kirjallisuuskatsauksen pohjalta. Kyberturvallisuuden todettiin olevan tietoa ja taitoa toimia kyberturvallisin tavoin ja laittein, minkä takia Hongin ja Ståhlen 'Tiedon ja osaamisen hallinnan mallia' voidaan hyödyntää ilmiön tutkimiseen. Tärkein johtopäätös kirjallisuuskatsauksen pohjalta olikin juuri se, että kyberturvallisuus ei itsessään poikkea muista johdettavista tai hallittavista ilmiöistä, vaan luo omanlaisensa kontekstin tiedolla johtamiseen ja osaamisen hallintaan.

Laadullinen tutkimus osoitti, että organisaatiot tunnistavat kyberturvallisuuden olevan toden totta johdettavissa ja hallittavissa oleva ilmiö, ja siihen liittyviä prosesseja toteutetaan organisaatioissa jo jossain määrin ja joskus jopa osittain tiedostamatta. Huomattavaa oli nimenomaan se, että tutkimuksessa kävi ilmi, etteivät nämä prosessit välttämättä ole vielä kyberturvallisuuden kohdalla samalla tapaa vakioituja tai dokumentoituja kuin esimerkiksi muut organisaation perustoiminnot, ja kyberturvallisuusosaamisen johtaminen ja hallinta voisi hyötyä vielä järjestelmällisemmästä lähestymistavasta. Teoreettiseen pohjaan verrattuna huomion arvoista oli myös se, kuinka laadullisen tutkimuksen pohjalta voitiin todeta organisaation sisäisten prosessien olevan valittua mallia monimuotoisempia. Myös ulkoisten tekijöiden merkitys tunnistettiin osana organisaation tiedon keruuta ja osaamisen kehittämistä sekä organisaation toimintaa säätelevinä tekijöinä. Tutkimuksen tulosten perusteella esitimmekin

kattavampaa versiota tutkimukseen valitusta teoreettisesta mallista kyberturvallisuusosaamisen johtamiseen ja hallintaan. Tässä kehitetyssä versiossa prosessien välinen vuorovaikutus sekä ulkoisten tekijöiden merkitys on otettu huomioon.

Tutkimuksen rajoitteiden ja luotettavuuden arvioinnissa keskityttiin sekä validiteetin että reliabiliteetin näkökulmiin. Validiteetin osalta on huomioitu, että tutkimus onnistui hyvin vastaamaan ennalta määriteltyihin tutkimuskysymyksiin ja tavoitteisiin. Vaikka haastateltavien määrä jäi alkuperäisestä suunnitelmasta, saadut haastatteluvastaukset olivat laajoja, syvällisiä ja jopa rikasta materiaalia, mikä vahvisti tutkimuksen pätevyyttä. Yleisesti ottaen haastattelujen perusteella saatiin selkeästi ilmi haastateltavien näkemykset aihepiiristä, mikä tukee tutkimuksen validiteettia. Toisaalta reliabiliteetin osalta on havaittu rajoituksia, erityisesti haastateltavien lukumäärän ja aikarajoitteiden vuoksi. Pieni haastateltavien määrä ja rajallinen aikaväli voivat vaikuttaa tulosten toistettavuuteen ja luotettavuuteen. Laadulliseen sisältöanalyysiin liittyy subjektiivisuuden riski, mikä myös tässä tutkimuksessa jouduttiin hyväksymään ominaispiirteenä, mutta riskiä kuitenkin pienensi kahden tutkijan rooli. Lisäksi haastatteluiden aikana ilmeni joitakin rajoituksia, kuten haastateltavien kykenemättömyys kertoa tietyistä asioista, jotka ovat organisaation sisäisiä tai salassa pidettäviä asioita. Tämä saattaa rajoittaa tutkimuksen syvällisyyttä ja kattavuutta. Käsitteiden ja haastattelukysymysten tulkinnassa esiintyi myös joitakin eroja haastateltavien välillä, mikä voi vaikuttaa tulosten vertailtavuuteen ja tarkkuuteen.

Osaamisen hallinnasta ja johtamisesta on saatavilla lukuisasti, joskin hieman vanhaa tutkimusta ja teoriaa moderniin ja nopeasti muuttuvaan nykymaailmaan. Kyberturvallisuuden kontekstissa vastaavaa tutkimusta ei juurikaan ole, joten tämän tutkimuksen voidaan todeta edistävän kyberturvallisuusosaamisen hallinnan ja johtamisen tutkimusta ja teoriapohjaa sekä luovan perustaa mahdollisille jatkotutkimuksille. Tuloksia voivat hyödyntää sekä organisaatiot että yksityishenkilöt ja tutkijat. Organisaatiot pystyvät tulosten avulla kehittämään omia kyberturvallisuusosaamisen hallinnan ja johtamisen prosesseja. Tutkimustulosten mukaan osaamisen hallinnan ja johtamisen lainalaisuudet säilyvät samoina riippumatta kontekstista, jolloin myös muille aloille tästä tutkimuksesta voi olla käytännön hyötyjä, myös kyberturvallisuuden ulkopuolella.

Hyvä jatkotutkimuksen aihe olisi tutkia järjestelmällisen hallintaprosessin jalkauttamisen vaikutuksia yhden organisaation sisällä. Tutkimuksessa keskityttäisiin organisaation tavoitteiden ja strategioiden muodostamien prosessien mittaukseen ja kehittämiseen. Tutkimuksessa selviäisi, kuinka hallintaprosessin eri osa-alueet vaikuttavat organisaation suorituskykyyn, tehokkuuteen ja tuloksellisuuteen, jolloin käytännön hyötynä voisi saada selvyyttä siitä, kuinka hallintaprosessit tulisi toteuttaa kyseisessä organisaatiossa mutta mahdollisesti myös muissa organisaatioissa.

Jatkotutkimusaiheiden lisäksi tutkimuksen toteuttamisessa nousi esille myös kehityskohteita. Kehittämällä aiheen tutkimuksen toteutusta ja menetelmää voisi pienentää tässä tutkimuksessa nousseita reliabiliteetin ja validiteetin rajoitteita, kuten tulosten vaikuttavuutta, luotettavuutta ja syvyyttä. Jatkotutkimusten menetelminä voisi hyödyntää laaja-alaisempaa tutkimusta tai

monimenetelmätutkimusta. Laaja-alaisemmassa tutkimuksessa tutkittavien organisaatioiden määrää olisi mahdollista lisätä, mutta ennen kaikkea laajentaa hallintaprosessien ja erilaisten käytäntöjen tutkimusta. Monimenetelmätutkimus tehostaisi organisaatioiden hallintaprosessien, käytäntöjen ja kokemusten tutkimusta, jolloin syvempää ymmärrystä kyberturvallisuusosaamisen hallintaprosesseista voitaisiin saavuttaa.

LÄHTEET

Ackoff, R. L. (1989). From data to wisdom. *Journal of applied systems analysis*, *16(1)*, 3-9.

Adler, M. J. (1986). *A guidebook to learning: for a lifelong pursuit of wisdom*. Macmillan Publishing Company.

Ahmad, N., Lodhi, M. S., Zaman, K., & Naseem, I. (2017). Knowledge management: a gateway for organizational performance. *Journal of the knowledge economy*, *8,* 859-876.

Akyazi, U., van Eeten, M., & Gañán, C. H. (2021, July). Measuring cybercrime as a service (CaaS) offerings in a cybercrime forum. *In Workshop on the Economics of Information Security* (pp. 1-15).

Alalwan, J. A., & Weistroffer, H. R. (2012). Enterprise content management research: a comprehensive review. *Journal of Enterprise Information Management.*

Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: *Conceptual foundations and research issues. MIS quarterly*, 107-136.

Almashari, M., Zairi, M., & Alathari, A. (2002). An empirical study of the impact of knowledge management on organizational performance. *Journal of Computer Information Systems, 42(5)*, 74-82.

Alvesson, M. (1995). *Management of knowledge-intensive companies*. de Gruyter.

ANSSI, French Cybersecurity Agency. (2015). French national digital security strategy.

Ayodele, C. (2022). *Mitigating cybersecurity insider threat in the hiring stage of the employee lifecycle*.

Baskarada, S., & Koronios, A. (2013). Data, information, knowledge, wisdom (DIKW): a semiotic theoretical and empirical exploration of the hierarchy and its quality dimension. *Australasian Journal of Information Systems, 18(1)*.

Berio, G., & Harzallah, M. (2005). Knowledge management for competence management. *Journal of Universal Knowledge Management, 1,* 21-28.

Berio, G., & Harzallah, M. (2007). Towards an integrating architecture for competence management. *Computers in Industry, 58(2),* 199-209.

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security, 23(3),* 317-332.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011, September). Human performance in cybersecurity: a research agenda. *In Proceedings of the Human Factors and*

Ergonomics Society annual meeting (Vol. 55, No. 1, pp. 1115-1119). Sage CA: Los Angeles, CA: SAGE Publications.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications, 42,* 36-45.

Cavelty, M. D. (2010). Cyber-security. *In The Routledge handbook of new security studies* (pp. 154-162). Routledge.

Choo, C. W. (2002). Information management for the intelligent organization: the art of scanning the environment. *Information Today, Inc.*.

CNSS. 2022. Committee on National Security Systems (CNSS). *Committee on National Security Systems Glossary. Instruction No. 4009*. Haettu 21.12.2022 sivulta https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4(10).*

Davenport, T., Jarvenpaa, S., & Beers, M. (1996). Improving knowledge work processes. *MIT Sloan Management Review*.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.

Digi- ja väestötietovirasto (DVV). (2022). Digitaitoraportti 2022. Haettu 23.3.2023 sivulta https://dvv.fi/digiosaamisen-tilannekuva

Digi- ja väestötietovirasto (DVV). (2024). VAHTI-verkosto kehittää digitaalista turvallisuutta. Haettu 13.3.2024 sivulta https://dvv.fi/vahti

Dzbor, M., Paralic, J., & Paralic, M. (2000). Knowledge management in a distributed organisation. *Advances in Networked Enterprises: Virtual Organizations, Balanced Automation, and Systems Integration*, 339-348.

EU-komissio. (2023). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Haettu 13.3.2024 sivulta https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

EU-komissio. (2020). Euroopan kyberturvallisuusstrategia, COM(2020), 605 final, Bryssell, 27.4.2020.

Federal Ministry of the Interior and Community, Germany (2021). Cyber Security Strategy for Germany 2021.

Frické, M. (2009). The knowledge pyramid: a critique of the DIKW hierarchy. *Journal of information science, 35(2),* 131-142.

Frické, M. (2019). The knowledge pyramid: the DIKW hierarchy. *Ko Knowledge organization, 46(1),* 33-46.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine, 30(1),* 28-38.

Gao, F., Li, M., & Clarke, S. (2008). Knowledge, management, and knowledge management in business operations. *Journal of knowledge management, 12(2),* 3-17.

Gonzalez-Wertz, C., Fisher, L., Dougherty, S. & Holt, M. (2019). *Mind the utilities cybersecurity gap.* IBM Institute for Business Value.

Government Offices of Sweden. (2016). A national cyber security strategy.

Hamel, G., & Prahalad, C. K. (1994). Competing for the future. *Harvard business review, 72(4),* 122-128.

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them. *Human reproduction, 31(3),* 498-501.

Hansen, M. T., Nohria, N., & Tierney, T. (2013). What's your strategy for managing knowledge?. *In The knowledge management yearbook 2000-2001* (pp. 55-69). Routledge.

Hertog, P. D. (2000). Knowledge-intensive business services as co-producers of innovation. *International journal of innovation management, 4(04),* 491-528.

HM Government, United Kingdom. (2022). National Cyber Strategy 2022. Pioneering a cyber future with the whole of the UK.

Hong, J., & Stahle, P. (2005). The coevolution of knowledge and competence management. *International Journal of Management Concepts and Philosophy, 1(2),* 129-145

Houtzagers, G. (1999). Empowerment, using skills and competence management. Participation and Empowerment: *An International Journal, 7(2),* 27-32.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR), 51(4),* 1-36.

Hustad, E., Munkvold, B. E., & Moll, B. V. (2004). *Using IT for strategic competence management: potential benefits and challenges.*

Hyslip, T. S. (2020). Cybercrime-as-a-service operations. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 815-846.

IBM (2023). Nettiartikkeli. Haettu 12.3.2023 osoitteesta https://www.ibm.com/topics/insider-threats

Ifigeneia, L., Tsekmezoglou, E., Naydenov, R., Ciobanu, C., Malatras, A., & Theocharidou, M. (2022). *Enisa threat landscape 2022.* European Union Agency for Network and Information Security.

International Organization for Standardization. (2017). Security and resilience — Organizational resilience — Principles and attributes (ISO Standard No.

ISO 22316:2017). Haettu 23..3.2023 osoitteesta https://www.iso.org/standard/50053.html

Intezari, A., Pauleen, D. J., & Taskin, N. (2016, January). The DIKW hierarchy and management decision-making. *In 2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4193-4201). IEEE.

ISACA (2022). Tutkimusraportti. State of cybersecurity 2022. Haettu: 17.2.2024 osoitteesta https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/state-of-cybersecurity-2022_whpsc22_res_eng_0322.pdf?mod=djemCybersecruityPro&tpl=cy

ITU (International Telecommunications Union) 2008. *ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008*.

Jyväskylän ammattikorkeakoulu (2022). KSKTK-projektisivu. Haettu 14.3.2023 osoitteesta https://www.jamk.fi/fi/tutkimus-ja-kehitys/tki-projektit/keski-suomen-kyberturvallisuusosaamisen-tunnettavuuden-kasvattaminen.

Jyväskylän Yliopisto, Converis (2022). KSKTK-projektisivu. Haettu 14.3.2023 osoitteesta https://converis.jyu.fi/converis/portal/detail/Project/147402535?auxfun=&lang=fi_FI.

Kaplan, R. S., & Norton, D. P. (1996). *The balanced scorecard: translating strategy into action.* Harvard business press.

Kayani, J., & Zia, M. Q. (2012). The analysis of knowledge, knowledge management and knowledge management cycles: A broad review. *International Journal of Academic Research in Economics and Management Sciences, 1(6).*

Kim, K., Alfouzan, F. A., & Kim, H. (2021). Cyber-attack scoring model based on the offensive cybersecurity framework. *Applied Sciences, 11(16),* 7738.

Klendauer, R., Berkovich, M., Gelvin, R., Leimeister, J. M., & Krcmar, H. (2012). Towards a competency model for requirements analysts. *Information Systems Journal, 22(6),* 475-503.

Kumar, S., & Carley, K. M. (2016, September). Approaches to understanding the motivations behind cyber attacks. *In 2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 307-309). IEEE.

Le Deist, F. D., & Winterton, J. (2005). What is competence?. *Human resource development international, 8(1),* 27-46.

Lehto, M. (2022). Digitaalisen kybermaailman ilmiöitä ja määrittelyjä. *Kyber on kaikkialla–Jyväskylän yliopisto, tiedeblogi, 15,* 19-125.

Lehto, M., & Limnéll, J. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.

Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime.* Harvard University Press.

Mansaray, H. E. (2019). The role of human resource management in employee motivation and performance-An overview. *Budapest International Research and Critics Institute (BIRCI) Journal, 2(3),* 183-194.

Marinos, L., Belmonte, A., & Rekleitis, E. (2016). Enisa threat landscape 2015. *European Union Agency for Network and Information Security, 18.*

Mayer, M., & Zack, M. (1996). The design and implementation of information products. *Sloan Management Review, 37(3),* 45-59.

McAdam, R., & McCreedy, S. (1999). *A critical review of knowledge management models.* The learning organization.

Ministeries, Norway (2019). National Cyber Security Strategy for Norway.

Ministry of Economic Affairs and Communication, Estonia. (2019). Cybersecurity strategy.

Nakash, M., Baruchson-Arbib, S., & Bouhnik, D. (2022). A holistic model of the role, development, and future of knowledge management: Proposal for exploratory research. *Knowledge and Process Management, 29(1),* 23-30.

Nakash, M., & Bouhnik, D. (2022). "A system that will do magic": organizational perspective on the technological layer in knowledge management. *Aslib Journal of Information Management*.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST special publication, 800(2017),* 181.

Nickols, F. (2012). Definitions & meanings. *Distance Consulting, 200,* 2-10.

Obama, B. (2009). Remarks by the President on securing our nation's cyber infrastructure. Washington, DC, 29.

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict and Security Law, 17(2),* 187-209.

O'dell, C., & Grayson, C. J. (1998). If only we knew what we know: Identification and transfer of internal best practices. *California management review, 40(3),* 154-174.

Paquet-Clouston, M., & García, S. (2022). On the motivations and challenges of affiliates involved in cybercrime. *Trends in Organized Crime, 1-30.*

Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Savola, R., Salonen, J., ... & Remes, J. (2016). *Kyberosaaminen Suomessa–Nykytila ja tiekartta tulevaisuuteen.*

Peslak, A., & Hunsinger, D. S. (2019). What is cybersecurity and what cybersecurity skills are employers seeking?. *Issues in Information Systems, 20(2).*

Prahalad, C. K., & Hamel, G. (2003). The core competence of the corporation. *International Library of Critical Writings in Economics, 163,* 210-222.

Prusak, L., & Davenport, T. (1998). *Working knowledge: How organizations manage what they know.*

Puplic Safety Canada. (2018). National Cyber Security Strategy. Minister of Public Safety and Emergency.

Päivärinta, T., & Munkvold, B. E. (2005, January). Enterprise content management: an integrated perspective on information management. *In Proceedings of the 38th annual hawaii international conference on system sciences* (pp. 96-96). IEEE.

Qiu, M., Zhang, L., Ming, Z., Chen, Z., Qin, X., & Yang, L. T. (2013). Security-aware optimization for ubiquitous computing systems with SEAT graph approach. *Journal of Computer and System Sciences, 79(5),* 518-529.

Rios Insua, D., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & G. Rasines, D. (2021). An adversarial risk analysis framework for cybersecurity. *Risk Analysis, 41(1),* 16-36.

Roege, P. E., Collier, Z. A., Chevardin, V., Chouinard, P., Florin, M. V., Lambert, J. H., ... & Todorovic, B. (2017). Bridging the gap from cyber security to resilience. *In Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains* (pp. 383-414). Springer Netherlands.

Rowley, J. (2006). *What do we need to know about wisdom?.* Management decision.

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of information science, 33(2),* 163-180.

Santanna, J. J., van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015, May). Booters—An analysis of DDoS-as-a-service attacks. *In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (pp. 243-251). IEEE.

Sharma, N. (2008). The origin of data information knowledge wisdom (DIKW) hierarchy. *Preuzeto, 25,* 2021.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12(2), 8.*

Smith, H. A., & McKeen, J. D. (2003). Developments in practice VIII: Enterprise content management. *The Communications of the Association for Information Systems, 11(1), 41.*

Starbuck, W. H. (1992). Learning by knowledge-intensive firms. *Journal of management Studies, 29(6),* 713-740.

Suomen kyberturvallisuusstrategia ja taustamuistio (2013), Valtioneuvoston periaatepäätös, Turvallisuuskomitean sihteeristö, Helsinki, 24.1.2013.

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. *In 2015 IEEE 2nd international conference on cyber security and cloud computing* (pp. 307-311). IEEE.

Thierauf, R. J. (2001). *Effective business intelligence systems.* Greenwood Publishing Group.

Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T. J., ... & Vigna, G. (2015). *Framing dependencies introduced by underground commoditization.*

Traficom (2022). Nettisivu. Haettu 8.12.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt.

Valtiovarainministeriö, julkisen hallinnon ICT. (2020). Julkisen hallinnon digitaalinen turvallisuus. Valtiovarainministeriön julkaisuja 2020:23. Haettu 29.3.2023 osoitteesta http://urn.fi/URN:ISBN:978-952-287-857-1

Valtiovarainministeriö, Turvallisuuskomitea (2019). Suomen kyberturvallisuusstrategia 2019. Haettu 12.12.2022 osoitteesta https://vm.fi/kyberturvallisuusstrategia.

van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal.*

Vartiainen, M., Kokko, N., & Hakonen, M. (2003). Competences in virtual organizations. *In Proceedings of the 3rd International Conference on Researching Work and Learning, Book I, Tampere, Finland, 25-27 July 2003* (pp. 209-219).

Vasconcelos, J., Kimble, C., Gouveia, F., & Kudenko, D. (2000, October). A group memory system for corporate knowledge management: an ontological approach. *In Proceedings of the 1st European Conference on Knowledge Management (ECKM'2000) Bled School of Management, Slovenia* (pp. 91-99).

Vasconcelos, J. B., Kimble, C., & Rocha, Á. (2016). A special issue on knowledge and competence management: Developing Enterprise solutions. *Information Systems Frontiers, 18,* 1035-1039.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128, 113160.*

Von Solms, R., & Van Niekerk, J. (2013). *From information security to cyber security. computers & security, 38,* 97-102.

Wang, S., & Wang, H. (2019). Knowledge management for cybersecurity in business organizations: a case study. *Journal of Computer Information Systems.*

Wang, Z., & Wang, N. (2012). Knowledge sharing, innovation and firm performance. *Expert systems with applications, 39(10),* 8899-8908.

Wiig, K. M. (1993). *Knowledge management foundations: thinking about thinking-how people and organizations represent, create, and use knowledge.* Schema Press, Limited.

Wiig, K. M. (1995). *Knowledge management methods.* Arlington (TX).

Wiig, K. M. (1997). Knowledge management: an introduction and perspective. *Journal of knowledge Management, 1(1),* 6-14.

White House, United States. President (2001-2009: Bush). (2003). The national strategy to secure cyberspace.

Zagzebski, L. (2017). What is knowledge?. *The Blackwell guide to epistemology,* 92-116.

Zander, U., & Kogut, B. (1995). Knowledge and the speed of the transfer and imitation of organizational capabilities: An empirical test. *Organization science, 6(1),* 76-92.

Zeleny, M. (1987). Management support systems: Towards integrated knowledge management. *Human systems management, 7(1),* 59-70.

Zorn, T. E., & Taylor, J. R. (2004). Knowledge management and/as organizational communication: Theodore E. Zorn and James R. Taylor. *In Key issues in organizational communication* (pp. 109-125). Routledge.

Zyngier, S., & Burstein, F. (2012). Knowledge management governance: the road to continuous benefits realization. *Journal of Information Technology, 27(2),* 140-155.

LIITE 1 TUTKIMUKSEN KUTSU, SAATEKIRJE JA HAASTATTELURUNKO

Hei!

Tämä haastattelu on osa Jyväskylän yliopistossa tehtävää pro gradu –tutkielmaa sivuten samalla Keski-Suomen liiton rahoittamaa 'Keski-Suomen kyberturvallisuusosaamisen tunnettavuuden kehittäminen' (KSKTK) hanketta. Haastattelu ja tutkimukseen osallistuminen on vapaaehtoista. Tutkimus toteutetaan puolistrukturoituna yksilöhaastatteluna. Tutkimuksen myötä saatuja tuloksia käytetään tutkielman toteutusta ja toiminnan kehittämistä varten.

Haastattelut nauhoitetaan ja tallenteet tuhotaan tutkimuksen tulosten analysoinnin jälkeen. Haastateltavien nimiä, titteleitä tai muuta yksilöivää/tunnistettavaa tietoa ei tutkielmaan jätetä.

Tutkielman aiheena on kyberturvallisuusosaamisen hallinta ja johtaminen. Tavoitteena on selvittää, miten Keski-Suomen alueella toimivissa alan yrityksissä hallitaan ja johdetaan kyberturvallisuusosaamista: Mitä strategiaa kyberturvallisuusosaamisen hallinta noudattaa ja millaisista tekijöistä tämä strategia muodostuu sekä minkälaisia prosesseja osaamisen hallintaan liittyy.

Alla haastattelukysymykset, joihin voi halutessaan tutustua jo etukäteen. Haastattelussa pyritään noudattamaan alla kuvattua järjestystä, mutta tarvittaessa voidaan esittää myös tarkentavia lisäkysymyksiä. Haastattelussa voit myös nostaa esille sellaisia asioita, joita ei alla ole kuvattu tai kysytty suoraan.

Tulokset ovat käytettävissä tutkimuksen valmistuessa ja niistä voidaan sopia tarvittaessa myös henkilökohtainen läpikäynti. Nähdään haastattelussa!

Ystävällisin terveisin,

Mikko Kausto & Eetu Koivistoinen
Tutkimusavustajat
Jyväskylän Yliopisto
Informaatioteknologian tiedekunta

Taustatiedot:

- Mikä on työtittelisi ja kuinka kauan olet toiminut kyseissä tehtävässä.

Osio 1: Aiheeseen johdattelu: Kyberturvallisuus, tiedolla johtaminen & osaamisen hallinta

- Mitä kyberturvallisuus sinulle tarkoittaa? Millaisia asioita tai kokonaisuuksia se mielestäsi sisältää?
- Mitä koet osaamisen hallinnan ja tiedolla johtamisen olevan? Miten määrittelisit ne?
- Miten määrittelisit kyberturvallisuusosaamisen hallinnan ja johtamisen? Poikkeaako se muusta osaamisesta jollain tapaa?

Osio 2: Kyberturvallisuusosaamisen hallinta ja johtaminen suhteessa organisaation strategiaan

- Miten kuvailisit organisaation strategiaa? Onko toiminnassanne niistä johdettuja tavoitteita, joita seurataan? Mitä nämä ovat ja kuinka niitä seurataan?
- Kuinka kyberturvallisuus mukailee tai liittyy näihin tavoitteisiin? Miten kyberturvallisuuden käytännöt tukevat organisaation strategian toteutumista?
- Miten kyberturvallisuusosaamisen hallintaa ja johtamista toteutetaan? Onko olemassa erityistä suunnitelmaa tai kirjoitettuja ohjeita, pelisääntöjä tai mallia?
- Millainen rooli kyberturvallisuusosaamisella on toimintanne kannalta?
- Oletteko tunnistaneet toiminnassanne ns. suorituskyvyn aukkoja tai puutteita, joita voitaisiin pyrkiä kuromaan umpeen paremmalla kyberturvallisuusosaamisella?

Osio 3: Kyberturvallisuusosaamisen hallinnan ja johtamisen prosessit

- Onko yrityksessä kyberturvallisuusosaamisen hallintaan liittyviä henkilörooleja? Jos on, montako? Ja minkälaisia (kyber-)osaamis- ja kyvykkyysvaatimuksia näihin henkilörooleihin on liitetty?
- Entä kyberturvallisuuden tiedolla johtamiseen liittyviä henkilörooleja? Jos on, montako? Minkälaisia (kyber-)osaamis- ja kyvykkyysvaatimuksia näihin henkilörooleihin on liitetty?
- Vaaditaanko sertifikaatteja, tai onko yleisiä standardeja, joilla osaaminen todennetaan edellä mainituissa henkilörooleissa, mikäli niitä on?
- Onko yksikössäsi käytössä tiedolla johtamisen toimintamalleja tai -käytänteitä?
- Millaista tietoa kyberturvallisuudesta ja kyberturvallisuusosaamisen tasosta kerätään tai hyödynnetään? Miten tiedon tarvetta kartoitetaan?

- Kuinka organisaatio pyrkii pysymään ajan tasalla ja vastaamaan kyberturvallisuuden haasteisiin? Kuinka tietoa kerätään?
- Miten kuvailisit käytössä olevaa osaamis- ja tietopohjaa?
- Ketkä kyberturvallisuustietoa ja -osaamista käyttävät ja miten?
- Kuinka osaamista kehitetään? Koulutus tms.?
- Millaisia hyviä kyberturvallisuusosaamisen johtamisen ja hallinnan käytänteitä olette löytäneet?
- Entä millaisia ongelmia olette kohdanneet?
- Millainen on tiedon ja osaamisen välinen suhde? Kuinka kerätty tai omattu tieto muunnetaan osaamiseksi?