Mustonen Lassi

KYBERTURVALLISUUDEN HALLINTORAKENTEEN TOIMINNAN ANALYYSI – TAPAUS KRIITTISEN INFRASTRUKTUURIN ORGANISAATIOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Mustonen, Lassi
Kyberturvallisuuden hallintorakenteen toiminnan analyysi – tapaus kriittisen infrastruktuurin organisaatiossa
Jyväskylä: Jyväskylän yliopisto, 2021, 69 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaajat: Pöyhönen, Jouni; Nuojua, Viivi

Kyberturvallisuudella mahdollistetaan modernien organisaatioiden digitaalinen toiminta ja sitä kautta myös yhteiskunnan toiminta. Keskeisessä roolissa ovat organisaatiot, jotka toimivat kriittisen infrastruktuurin parissa. Tässä tapaustutkimuksessa tarkasteltiin kriittisen infrastruktuurin parissa toimivan organisaation kyberturvallisuuden hallintorakennetta. Organisaatiot voivat muodostaa kyberturvallisuuden hallintorakenteen monella tavalla. Tässä tutkimuksessa käydään läpi yksi tapa, joka toimii hyvin tämän organisaation kontekstissa ja mahdollisesti myös muissa organisaatioissa. Tutkimuksen tavoitteena on selvittää, miten kyberturvallisuuden hallintorakenne vaikuttaa kyberturvallisuuden hallintaan. Tutkimusta täydentävät alatutkimuskysymyksistä muodostuvat näkökulmat viestinnän ja tiedonhallinnan osalta. Tutkimuksen metodologinen lähestyminen on laadullinen. Tutkimus toteutettiin tapaustutkimuksena keskisuuressa kriittisen infrastruktuurin parissa toimivassa organisaatiossa. Empiirinen aineisto hankittiin puoliksi rakenteellisten haastattelujen avulla. Haastatteluaineistoanalysoitiin temaattisella analyysillä. Empiiriseen aineistoon kuului myös tutkittavan organisaation tietoturvaorganisaation rakennekaavio. Tutkimuksen tuloksissa nousi esiin kolme merkittävää löytöä. Organisaation toimijat, eli ihmiset ja ryhmät, voidaan jakaa kolmelle päätöksentekotasolle ja teknisen tai hallinnollisen tietoturvan puolelle. Toinen löytö oli organisaation muodostamat yhteistyöryhmät, joissa oli edustusta kaikista päätöksentekotasoista, sekä tekniseltä että hallinnolliselta puolelta. Tutkimuksen kolmas löytö liittyy läheisesti yhteistyöryhmiin ja se oli henkilöstön osallistaminen kyberturvallisuuden toteutukseen.

Asiasanat: kyberturvallisuus, hallintorakenne, tiedonhallinta, tilannekuva, organisaatio, osallistaminen

ABSTRACT

Mustonen, Lassi
Cybersecurity governance structure performance analysis - case in critical infrastructure organization
Jyväskylä: University of Jyväskylä, 2021, 69 pp.
Cyber Security, Master's Thesis
Supervisors: Pöyhönen, Jouni; Nuojua, Viivi

Cybersecurity enables the digital operations of modern organizations and society. Organizations that work in critical infrastructure play a key role in ensuring the functioning of modern society. This case study examined the cybersecurity governance structure of an organization operating on critical infrastructure. Organizations can form a cybersecurity governance structure in multiple ways. This study reviews one specific way that works well in the context of this organization and possibly in other organizations. The study aims to find out how the structure of a cybersecurity management organization affects cybersecurity management. The research is complemented with sub-research questions regarding communication and knowledge-management. The methodological approach of the study is qualitative. The study is a case study in a medium-sized organization operating on critical infrastructure. The empirical material was obtained through semi-structural interviews, which were then analyzed by thematic analysis. The empirical material also contained an organizational chart of the organization's cybersecurity management structure. The results of the study revealed three significant findings. The actors in an organization i.e., people and groups, can be divided into three levels of decision making and technical or administrative cybersecurity. The second discovery was the co-operation groups formed by the organization. Groups had representation from all levels of decision-making and both the technical and the administrative sides of cybersecurity. The third finding of the study is closely related to the collaboration groups. It was the involvement of staff in the implementation of information security.

Keywords: cybersecurity, governance structure, knowledge-management, situational awareness, organization, employee involvement

KUVIOT

TAULUKOT

SISÄLLYS

1 Johdanto

Moderni yhteiskunta on digitalisaation mukana ajautunut kyberriippuvaiseen tilaan (Limnell, Majewski & Salminen, 2014). Tämän kyberriippuvuuden mukana on kasvanut tarve kyberturvallisuudelle. Kyberturvallisuutta on tutkittu paljon sitä mukaan, kun kybermaailma on laajentunut digitalisaation ohessa. Kyseessä on kuitenkin suhteellisen uusi ilmiö, joten kaikkia kyberturvallisuuden osa-alueita ei ole vielä tutkimuksissa ehditty perinpohjaisesti tarkastelemaan.

Tämän tutkimuksen kohde on kyberturvallisuuden hallintorakenne organisaatiossa. Tavoitteena on tuottaa lisätietoa siitä, miten organisaatioiden tulisi muodostaa kyberturvallisuuden hallintorakenne. Aikaisemmat tutkimukset ovat muussa kontekstissa tuoneet tietoa kyberturvallisuuden hallintorakenteesta, jota voidaan hyödyntää, mutta pääasiallista keskittymistä kyberturvallisuuden hallintorakenteeseen ei ole tutkijan tietojen mukaan toteutettu. Tässä tutkimuksessa pyritään täyttämään tätä aukkoa.

Suomen 2013 julkaistussa kyberturvallisuusstrategiassa mainitaan, että ”kyberturvallisuus käsittää kaikki ne yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia tilanteissa, joista voi aiheutua merkittävää haittaa tai vaaraa Suomelle tai sen väestölle” (Turvallisuuskomitea, 2013).

Tutkimus on tapaustutkimus kriittisen infrastruktuurin parissa työskentelevästä keskisuuresta suomalaisesta organisaatiosta. Organisaation kyberturvallisuuden ja haastateltavien anonymiteetin turvaamiseksi tarkemmat yksityiskohdat organisaatiosta on pidetty salassa. Salassapidon vaikutus tutkimukseen on kuitenkin minimaalinen, sillä tutkimuksen kannalta oleelliset tiedot saatiin esiin ilman organisaation nimeämistä.

Tutkittava organisaatio on ollut mukana useissa valtakunnallisissa sekä toimialan sisäisissä kyberyhteistyöhankkeissa ja -ryhmissä. Organisaatiolla on siis selvä motivaatio kehittää omaa toimintaa myös tutkimushankkeiden kautta. Näiden tutkimusten avulla voidaan myös kehittää muiden organisaatioiden kyberturvallisuus tasoa Suomessa ja tätä kautta nostaa suomalaisen kyberturvallisuuden tasoa.

Tutkimuksen haastatteluista voidaan todeta, että tutkittavan organisaation kyberkypsyys on korkealla tasolla ja kyberturvallisuuteen panostetaan paljon. Myös motivaatio osallistua kyberyhteistyöhankkeisiin on merkkinä siitä, että kyberturvallisuus otetaan organisaatiossa tosissaan. Koska tutkittavan organisaation kyberkypsyys on kehittynyt korkealle tasolle, tämän tutkimuksen tuloksista voidaan saada hyviä toimintamalleja muille organisaatioille, joiden kyberkypsyys on vasta alkuvaiheessa.

Organisaatiossa on kehitetty hallintorakenne, jonka tavoitteena on mahdollistaa kyberturvallisuuden tuottaminen tehokkaasti ja tässä tutkimuksessa pyritään selvittämään miten hallintorakenne toteuttaa tämän tehtävän. Tutkimuksen pääkysymys on ”**Miten tietoturvan hallintorakenne vaikuttaa kyberturvallisuuden hallintaan?**” Pääkysymyksen lisäksi tutkimukseen otetaan kaksi alakysymystä, jotka ottavat viestinnällisen/tiedonhallinnallisen näkökulman tutkimukseen.

- **Miten tietoturvan hallintorakenne vaikuttaa tietoturvainformaation kulkuun?**

- **Miten tiedonhallinnalla voidaan tehostaa informaation kulkua hallintorakenteessa?**

Empiirinen data kerättiin puoliksi rakenteellisilla haastatteluilla. Haastatteluihin osallistui henkilöitä eri puolilta ja tasoilta organisaation kyberhallintorakenteesta, niin teknisistä, kuin hallinnollisista tehtävistä.

Tutkimuksen tuloksissa selviää, miten tutkittava organisaatio on muodostanut kyberturvallisuuden hallintorakenteen heidän organisaatioonsa ja mitkä sen vaikutukset ovat kyberturvallisuuden hallintaan ja viestintään tämän hallintorakenteen sisällä. Keskeisiä löytöjä olivat, että hallintorakenne jakautuu organisaation kolmen päätöksenteko tason mukaisesti ja tämän lisäksi hallinnolliseen ja tekniseen puoleen. Yhteistyöryhmät olivat toinen keskeinen löytö, jotka yhdistivät näitä jakaumia siten, että ryhmissä oli edustusta eri tasoilta, sekä hallinnolliselta ja tekniseltä puolelta. Kolmas löytö oli, että organisaatio osallistaa työntekijöitä rakenteen tasolla kyberturvallisuuden toteutukseen esimerkiksi edellä mainittujen yhteistyöryhmien kautta.

Tutkimuksen luvut kaksi ja kolme koostavat tutkimuksen kirjallisuuskatsauksen. Kirjallisuus katsauksessa käsitellään ensimmäisenä kyberturvallisuutta yleisesti ja tämän jälkeen syvennytään kyberturvallisuuteen kriittisen infrastruktuurin organisaatiossa ja tilannetietoisuuteen. Luvun kaksi toinen keskeinen teema on organisoitumismallit ja niiden teoriat ja kehittyminen. Näiden jälkeen tarkastellaan miten kyberturvallisuus ja organisaatiomallit vaikuttavat toisiinsa. Kirjallisuus katsauksen toinen luku, luku kolme, käsittelee tiedonhallintaa organisaatiossa. Luvussa tarkastellaan viestinnän ja tiedonhallinnan kannalta oleellista kirjallisuutta tämän tutkimuksen kontekstissa. Neljännessä luvussa käydään läpi tutkimusmenetelmä ja tulosten analysointi, sekä tarkastellaan tutkimuksen luotettavuutta. Viidennessä luvussa käydään läpi tulokset ja peilataan tuloksia kirjallisuuskatsaukseen. Kuudennessa luvussa vastataan tutkimuskysymyksiin

ja keskustellaan tulosten merkityksistä. Viimeisenä lukuna on yhteenveto, jossa kootaan tutkimuksen keskeiset löydöt ja ehdotetaan suuntaa tuleviin tutkimuksiin.

2 Kyberturvallisuus ja organisoitumismallit

Tässä luvussa käsitellään kyberturvallisuutta, kybertoimintaympäristöä ja organisoitumismalleja, sekä näiden välisiä yhteyksiä. Ensimmäinen alaluku käsittelee kyberturvallisuutta yleisesti ja tämän jälkeen tarkennetaan aihetta kyberturvallisuuteen kriittisen infrastruktuurin yrityksissä. Kolmas kyberturvallisuuteen liittyvä aihe on tilannetietoisuus. Toinen alaluku käsittelee organisoitumismallien teorioita. Tässä alaluvussa käydään läpi organisaatioteorioita, organisaatiomallien kehittymistä ja tietopohjaista organisaatiota. Viimeisessä alaluvussa käsitellään organisaatiomallien merkitystä kyberturvallisuuden kontekstissa. Alaluvussa käsitellään tarkemmin systeemiteoriaa, osallistamista ja organisaation kolmea päätöksentekotasoa, sekä ohjaus/kontrolli sykliä.

2.1 Kyberturvallisuus

Digitalisaatio on ajanut yhteiskunnan kyberriippuvaiseen tilaan. Digitalisaatio on lisännyt eri toimijoiden kyberpotentiaalia, eli kykyä ja osaamista toimia kybermaailmassa. Kyberpotentiaalin lisääntyminen johtaa kyberuhille altistumiseen. Liiketoimintaprosessien siirtäminen kybermaailmaan mahdollistaa digitalisoinnin avulla paremman tehokkuuden, mutta altistaa prosessin samalla kyberuhille. (Limnell, Majewski & Salminen, 2014)

Kyber-sanaa käytetään yleensä yhdyssanan määriteosana. Sana kyber tulee kreikan kielen sanasta ”kybereo”, joka tarkoittaa ohjata, opastaa, hallita. Kyber viittaa yleensä digitaalisessa muodossa olevan informaation käsittelyyn. Kyberturvallisuuden sanastossa kyberturvallisuuden määritelmä on seuraava: ”tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. (Turvallisuuskomitea, 2018)

Pöyhösen (2020) mukaan kyberturvallisuus on yksi kokonaisturvallisuuden osa-alueista, jonka tavoitteena on turvata digitalisoituneen yhteiskunnan kriittiset toiminnot. Organisaatiot muodostavat kyberkyvykkyytensä ihmisten osaamisella, käytänteillä, prosesseilla ja teknologioilla, joilla voidaan suojata verkkoja, järjestelmiä, ohjelmia ja dataa kybermaailman uhkia vastaan (Pöyhönen, 2020). Kyberturvallisuudella pyritään luomaan luotettava ja turvallinen kybertoimitaympäristö. Tähän tavoitetilaan pääseminen on jatkuva iteratiivinen prosessi yritysten ja erehtymisien kautta (Kim, 2017). Menestyksekkään kyberturvallisuuden tuottamiseksi jatkuva kehitys on dynaamisen ja nopeasti muuttuvan kybertoimintaympäristön takia välttämätöntä.

Suomen kyberturvallisuusstrategian (2013) liitteessä kuvataan kyberturvallisuusprosessia viisivaiheisesti. Ensimmäinen vaihe on analyysi, joka tarkoittaa oman aseman hahmottamista suhteessa toimintaympäristöön. Toisessa vaiheessa, eli suunnitteluvaiheessa, suunnitellaan kyberturvallisuuden visio, eli miten haluttuun tavoitetilaan päästään hallussa olevilla resursseilla.

Suunnitteluvaiheessa luodaan useita vaihtoehtoisia suunnitelmia, joilla tavoitteeseen voidaan päästä. Päätösvaiheessa valitaan yksi suunnitelmista ja määritetään halutut kybersuorituskyvyt ja toimenpiteen niiden luomiseksi. Tuottamisvaiheessa määritellään konkreettiset tavoitteet ja vastuut, sekä kyberturvallisuusstrategian rakenne. Viimeisenä toimenpanovaiheessa, kun aikaisempien vaiheiden tuottama strategia on hyväksytty, viedään strategian käytäntöön. Tämän jälkeen sykli alkaa alusta. (Turvallisuuskomitea, 2013)

Kyberturvallisuuden ja tietoturvallisuuden käsitteet menevät monesti sekaisin. Solmssin ja Niekerkin mukaan (2013) kyberturvallisuus ja tietoturvallisuus mielletään monesti synonyymeina, mutta asia ei näin ole. Tietoturvallisuus ja kyberturvallisuus eivät ole sama asia, vaikka termeillä onkin paljon yhteistä (Von Solms & Van Niekerk, 2013). Kyberturvallisuuskomitean sanastossa määritellään tietoturvallisuus seuraavasti: ”järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus” (Turvallisuuskomitea, 2018).

Tietoturvallisuuden tavoitteena on ylläpitää tiedon saatavuus, luottamuksellisuus ja eheys. Saatavuus tarkoittaa, että tieto on käytettävissä haluttuun aikaan, eheys tarkoittaa, että tieto on yhtäpitävää alkuperäisen tiedon kanssa ja luottamuksellisuus tarkoittaa, että kukaan ulkopuolinen ei saa tietoa käsiinsä (Turvallisuuskomitea, 2018).

Tietoturvallisuus keskittyy tiedon turvaamiseen, joten tiedon ei tarvitse olla digitaalista. Kyberturvallisuus keskittyy kybertoimintaympäristön suojaamiseen ja myös kybertoimintaympäristössä toimivien henkilöiden ja sen kautta saavutettavan omaisuuden suojaamiseen (Von Solms & Van Niekerk, 2013).

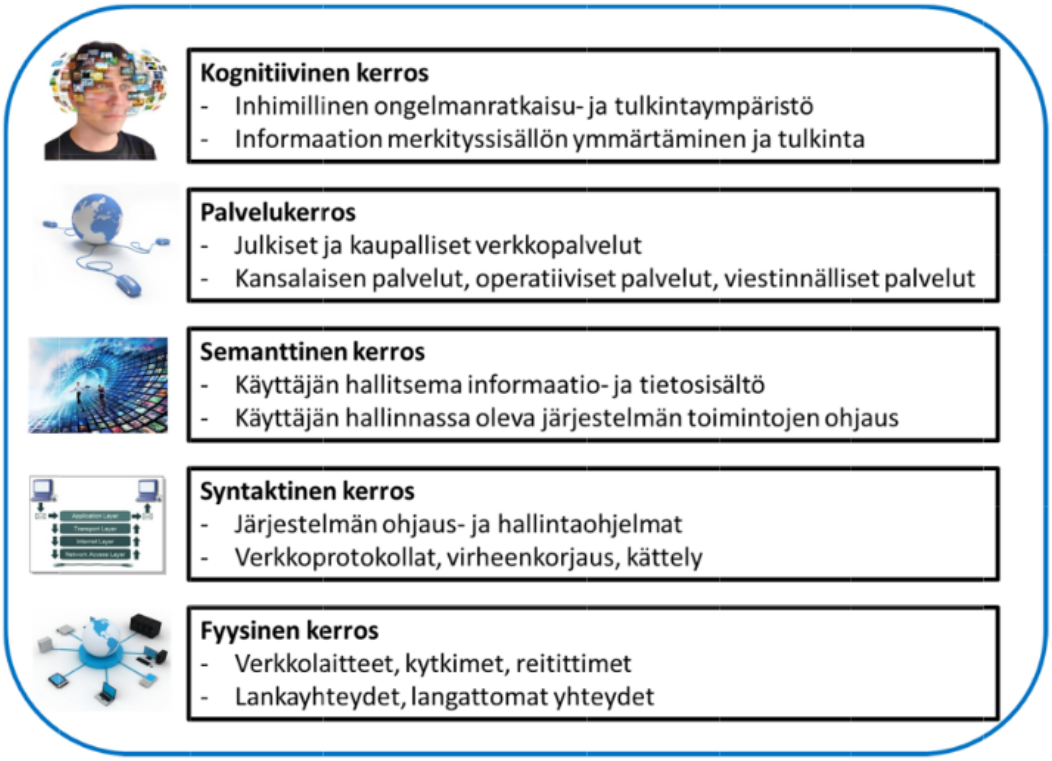
Suomen turvallisuuskomitean sanastossa (2018) määritellään kybertoimintaympäristö seuraavasti:

> yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö
>
> Kybertoimintaympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet.

Kybertoimintaympäristöön kuuluu siis myös fyysiset rakenteet, joten kybertoimintaympäristöä ei saa ajatella pelkästään bittienmaailmana, vaikka siellä kybertoimet yleensä tapahtuvatkin. Täyden kyberturvallisuuden toteuttamiseksi on pystyttävä takaamaan myös fyysisten rakenteiden turvallisuus, joihin kuuluu esimerkiksi reitittimet, tietokoneet, teollisuudenhallintajärjestelmät ja sähkölukot.

Libicki (2007) on luonut OSI-malliin (Open Systems Interconnection model) pohjautuvan kybermaailman tasorakenteen, joka perustuu neljään kybermaailman kerrokseen. Alkuperäisessä OSI-mallissa on seitsemän kerrosta. Kuten OSI-mallissa Libickin kybermaailman rakenteen eri kerrokset käyttävät palveluita, joita alempi kerros tarjoaa ja tarjoavat itse palveluja ylemmille kerroksille (Libicki, 2007). Jyväskylän yliopiston professori Martti Lehto on muokannut tätä mallia

lisäämällä siihen viidennen kerroksen, eli palvelukerroksen, organisaation verkostoitumistarpeiden huomioimiseksi (Pöyhönen & Lehto, 2020). Tämä päivitetty tasomalli on esillä kuvassa 1.



KUVIO 1 Kybermaailman tasomalli (Lehto & Kähkönen, 2015)

Kybermaailman alin kerros on fyysinen kerros, jossa eri laitteet ja verkot toimivat. Syntaktisella kerroksella on järjestelmien ohjaus- ja hallintaohjelmat, verkkoprotokollat ja kättelyt. Keskimmäinen kerros on semanttinen kerros, joka sisältää käyttäjän hallintaan liittyvät tiedot ja järjestelmät. Palvelukerroksella on julkiset ja kaupalliset verkkopalvelut, sekä kansalaisen-, operatiiviset- ja viestinnälliset palvelut. Viimeisenä ja ylimpänä kerroksena on kognitiivinen kerros, joka on inhimillinen kerros. Kognitiivisella kerroksella voidaan ratkaista ongelmia ja tulkita ympäristöä, sekä tulkita ja ymmärtää informaatio sisältöä. (Lehto & Kähkönen, 2015)

Kyberturvallisuutta voidaan myös hahmottaa organisaation kolmen päätöksentekotason kautta. Nämä tasot ovat: strateginen taso, operatiivinen taso ja taktinen/teknillinen taso (Pöyhönen, 2020, s. 135). Strateginen taso määrittää toiminnan suunnan, jota operatiivisella tasolla toteutetaan ja asetetaan resurssit strategisen tason suunnan mukaisesti. Taktisella / teknillisellä tasolla pyritään näiden resurssien optimaaliseen käyttöön. Alemmat tasot antavat informaatiota ylöspäin, jotta strategia voidaan suunnata uudelleen alemman tason havaintoihin pohjautuen. Tätä kutsutaan ohjaus/kontrolli sykliksi, jota tarkastellaan tarkemmin alaluvussa 2.3.

Kybertoimintaympäristöön liittyy mahdollisuuksien lisäksi aina myös uhkia. Valtioneuvoston selvityksessä (2017) on tutkittu kyberuhkien trendejä (Lehto, Limnéll, Innola, Pöyhönen, Rusi & Salminen, 2017, s.12). Trendejä olivat:

- kiristyshaittaohjelmien kasvu
- haavoittuvuuksien hyödyntäminen
- laitteistoihin kohdistuvat uhkat
- yrityksen sisäpiiri hyökkäyskanavana
- liiketoiminnan tuhoamiseen tähtäävät hyökkäykset
- henkilötietojen varastamiseen tähtäävät hyökkäykset
- huijaukset ja tietojen kalastelut
- palvelunestohyökkäykset
- kohdistetut hyökkäykset
- jatkuvat hyökkäykset

Kyberuhkiksi voidaan katsoa ne toimenpiteet, joilla yritetään vahingoittaa tai tuhota tietoverkkoja, tietojärjestelmiä, päätelaitteita tai vaikuttaa niiden käyttömahdollisuuksiin tai tietosisältöihin (Lehto ym., 2017, s. 12). Nämä toimenpiteet voivat kohdistua kaikkiin viiteen kybermaailman tasoon, jotka luvussa aikaisemmin esiteltiin (ks. KUVIO 1).

2.1.1 Kyberturvallisuus kriittisen infrastruktuurin organisaatiossa

Kriittinen infrastruktuuri koostuu monista järjestelmistä, jotka muodostavat teknillisesti monimutkaisen ja kompleksisen kokonaisuuden (Pöyhönen, 2020, s. 66). Kyberturvallisuus vaatimukset ovat korkeammat, kun kyseessä on kriittisen infrastruktuurin alueella toimiva organisaatio. Kriittisen infrastruktuurin alueella toimivien yritysten on kyettävä varmistamaan toimintaprosessien jatkuvuus.

Nykyään miljoonat laitteet, jotka kontrolloivat turvallisuuden kannalta kriittisiä järjestelmiä, on kytketty internetiin. Esineiden internet (Internet of Things) on nouseva avainteknologia, joka raivaa tietä seuraavan sukupolven teollisille tuotantojärjestelmille. Viime vuosikymmeninä klassinen tuotantotekniikka, automaatio ja älykkäät laskentajärjestelmät sulautuivat teolliseen esineiden internetiin. Ohjelmoitavat logiikkayksiköt korvataan kehittyneemmillä kyberfyysisillä järjestelmillä (Cyber Physical Systems), jotka ovat vapaasti ohjelmoitavia sulautettuja laitteita. Nämä laitteet ohjaavat fysikaalisia prosesseja. Olemassa olevien tietoturvakäsitteiden mukauttaminen kyberfyysisiin tuotantojärjestelmiin ei ole yksinkertaista. Esimerkiksi verkkohyökkäyksen kohdistuessa IT-järjestelmiin, kyseiset IT-järjestelmät poistetaan yleensä käytöstä ja palautetaan toimintaan hyökkäyksen jälkeen. Tätä lähestymistapaa ei kuitenkaan voida soveltaa kyberfyysiseen tuotantojärjestelmään, jossa toimintaa ei voida keskeyttää yhtä helposti. (Sadeghi, Wachsmann, & Waidner, 2015)

Modernit ICS-järjestelmät (Industrial Control System) eli teollisuuden automaatiojärjestelmät käyttävät informaatio ja kommunikointi teknologioita teollisten prosessien kontrolloimiseen ja automatisaatioon. Teollisuuden

automaatiojärjestelmät yhdistävät, valvovat ja ohjaavat prosesseja useilla toimialoilla, kuten sähköntuotanto, siirto ja jakelu, kemiallinen tuotanto, öljy ja kaasu, jalostus ja veden suolanpoisto. ICS-järjestelmät ovat siirtyneet yhä enemmän internetiin, joten niihin kohdistuvat kyberhyökkäykset ovat mahdollisia esimerkiksi protokollien ja laitteiden kautta. (McLaughlin ym., 2016)

SCADA-järjestelmät (Supervisory control and data acquisition) ovat tietojärjestelmiä, joilla monitoroidaan ja kontrolloidaan teollisia prosesseja. Suurin tietoturvauhka teollisilla prosesseilla on, kun hyökkääjä pääsee käsiksi SCADA-järjestelmään valvojan roolissa ja hyökkääjä kykenee kontrolloimaan järjestelmän eri osia (Ten, Liu & Manimaran, 2008).

Suomen kyberturvallisuusstrategiassa (2019) on nostettu esiin kyberturvallisuuden merkityksen kasvaminen erityisesti aloilla, joiden varsinainen liiketoiminta on kyberturvallisuuden ulkopuolella, mutta joiden toimintaan kyberturvallisuus ja kybertoimintaympäristön häiriöt vaikuttavat merkittävästi. Tällaisia toimialoja ovat tietoliikenne, energiantuotanto ja -jakelu, finanssi- ja vakuutusala ja terveydenhuolto (Turvallisuuskomitea, 2019). Euroopan neuvoston 2016 hyväksymässä verkko- ja tietoturvadirektiivissä (NIS-direktiivi) asetettiin tavoitteeksi parantaa EU:n jäsenvaltioiden yhteistyötä ja asettaa turvallisuus velvoitteita keskeisten palvelujen tarjoajille, sekä digitaalisten palvelujen tarjoajille (Euroopan unioni, 2016). Kriittisen infrastruktuurin alueella toimiville yrityksille on siis asetettu vaatimuksia niin EU:n kuin Suomenkin osalta.

Kansallisen kriittisen infrastruktuurin kyberturvallisuuden taso on Suomessa hyvä erityisesti suurimmissa organisaatioissa. Näissä organisaatioissa tunnistetaan kyberuhkia, osataan kyberturvallisuuden tilannetietoisuuden järjestelyt, hallitaan häiriötilanteiden analysointikyky ja osataan vaihtaa uhkakuviin liittyviä tietoja verkostoja käyttäen. (Pöyhönen, 2020, s. 183)

Valtionneuvoston selvityksessä (2017) nostettiin esiin heikkouksia ja vahvuuksia eri alueilta kriittisen infrastruktuurin parissa työskenteleviltä organisaatioita. Kategoriat olivat: johtaminen, tilannekuva, henkilöstön osaaminen, tuotteet ja palvelut, asiantuntija palvelut ja jatkuvuuden varmistaminen (Lehto ym., 2017, s. 42–43). Näitä osa-alueita käytetään myös tämän tutkimuksen tulosten tarkastelussa.

2.1.2 Tilannetietoisuus

Tehokkaan kyberturvallisuuden toteuttamiseksi tarvitaan tilannetietoisuutta kybertoimintaympäristöstä. Kuten aiemmin jo kyberturvallisuustoimintaympäristöstä todettiin, että se on dynaaminen ja nopeasti muuttuva ympäristö, joten toimijoiden on pystyttävä rakentamaan jatkuvaa tilannekuvaa tehokkaiden päätösten tekemiseksi.

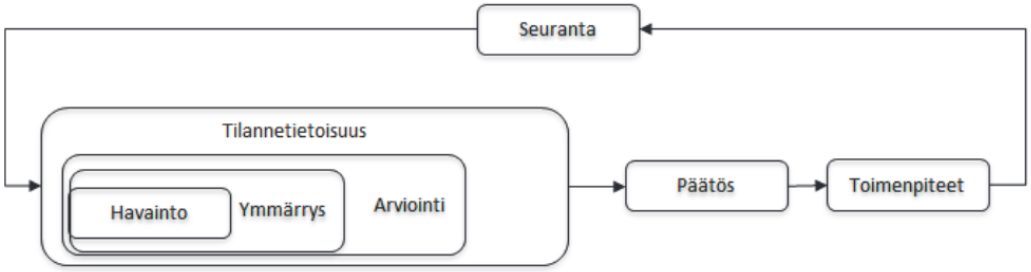
Tilannetietoisuuden konsepti on ensimmäisen kerran havaittu ensimmäisen maailmansodan aikana ja käsite on noussut valokeilaan uudelleen 1980 luvun loppupuolella ilmailualan piirissä, jossa tilannetietoisuuden tarve on dynaamisen toimintaympäristön takia merkittävä tekijä turvallisuuden kannalta. Jos

systeemin tilasta halutaan pysyä tietoisina, on ihmisten pidettävä kirjaa tapahtumien muutoksesta. (Stanton, Chambers & Piggott, 2001)

Tilannetietoisuudesta on kolme pää määritelmää ja tässä tutkimuksessa keskitytään Endsleyn (1988) luomaan määritelmään, jossa keskeistä on ympäristön havainnointi, ymmärtäminen ja ennustaminen (Stanton, Chambers & Piggott, 2001).

Tilannetietoisuus on keskeinen tekijä päätöksentekoprosessissa. Tilanne tietoisuus on henkilön tietojen tila dynaamisessa ympäristössä. Tilannetietoisuus sisältää havainnot relevanteista elementeistä, arvioinnin näiden merkityksestä yhdistettynä toimijan tavoitteisiin ja heijastumana tulevaisuuden tiloihin ympäristössä tähän informaatioon perustuen. Toimijat, joilla on hyvä tilannetietoisuus tekevät todennäköisemmin parempia päätöksiä ja pärjäävät hyvin dynaamisissa järjestelmissä. (Endsley, 1995)

Endsleyn (1995) malli on havainnollistettu kuviossa 2. Tilannetietoisuus on syklinen prosessi. Päätökset ja toimenpiteet vaikuttavat ympäristöön ja näitä seuraamalla saadaan uutta tilannetietoisuutta. Tilannetietoisuus muodostuu havaintojen, ymmärryksen ja arvioinnin kautta.



KUVIO 2 Tilannetietoisuus ja päätöksentekomalli (Endsley, 1995, muokattu)

Aikaisemmin mainitut kolme organisaation päätöksentekotasoa esiintyvät tässä mallissa seuraavasti. Tavoitteena on aikaansaada kaikkia päätöksentekotasoja palveleva havainnointikyky. Havainnoista muodostuu tilannekuva, jota analysoimalla voidaan ymmärtää havaintojen merkitys. Tämä ymmärryksen avulla voidaan arvioida eri vaihtoehtoja ja tehdä päätöksiä. Havaintotietojen luokittelulla mahdollistetaan tietojen siirto eri tasojen välillä ja tämä mahdollistaa kokonaiskuvan hahmottamisen. (Pöyhönen, 2020 s. 88–89)

Teknillinen/taktinen kerros tarvitsee eri informaatiota päätöksentekemisessä, kuin strateginen taso. Strategisen tason tietovaatimuksen ovat abstraktimpia kuin teknisellä tasolla. Operatiivisella tasolla tarvittava tiedon abstraktisuus on jotain näiden kahden välistä. Alaluvussa 3.1 käsitellään tarkemmin tiedon tasoja.

Haaste kyberturvallisuuden tilannekuvan ja tilannetietoisuuden kehittämisessä on erityisesti kyberrakenteen teknillisellä tasolla kuten ICT- ja automaatiojärjestelmissä. Tilannetietoisuuden muodostamisessa keskeisessä asemassa on organisaation henkilöstön kyberkyvykkyydet ja -osaaminen. (Pöyhönen, 2020, s. 136, 183)

2.2 Organisoitumismallien teoriat

”Jokaisen organisaation tehtävänä on omaksua itselleen sellainen rakenne, joka palvelee parhaiten ja tehokkaimmin sen perimmäisiä tavoitteita” (Harisalo, 2008 s. 76). Organisaatiorakenteet koskevat organisaation eri jäsenten suhteita toisiinsa. Tähän eivät kuulu vain johtamis- ja raportointisuhteet. Organisaatiorakenteet kertovat meille, kenellä on resurssit, kuka puhuu kenelle, kuka on vastuussa mistäkin, mitä voi tehdä yksin ja mitä on tehtävä muiden kanssa, millaisia urapolkuja on käytettävissä ja miten tieto virtaa organisaatiossa. Jotkut näistä rakenteista on kirjattu virallisesti organisaatiokaavioon ja muihin menettelyihin. Monet näistä ovat epävirallisia, vaikka ne liittyvät usein myös muodollisiin rakenteisiin. Organisaatiorakenteet ovat olennainen osa strategian toteuttamista ja minkä tahansa tavoitteen saavuttamista organisaatiossa. (Whittington, 2006)

2.2.1 Organisaatioteoriat

Organisaatioteoriat voidaan jakaa ajallisesti. Ajallisessa jakamisessa tulee ottaa huomioon, että uudet teoriat eivät korvaa vanhoja, vaan kehittyvät rinnakkain ja muutoskykyisinä. Harisalon (2008) kirjan mukaan teoriat ajallisessa järjestyksessä ovat:

- tieteellinen liikkeenjohto, 1910
- klassinen organisaatioteoria, 1915
- ihmissuhteiden koulukunta, 1920
- byrokratia- ja rakennekoulukunta, 1920
- päätöksentekoteoria, 1950
- järjestelmäteoria, 1950
- valtateoria, 1960
- kontingenssiteoria, 1965
- strategisen johtamisen teoria, 1970
- organisaatiokulttuuriteoria, 1980
- innovaatioteoria, 1990

Tieteellistä liikkeenjohtoa pidetään ensimmäisenä johdonmukaisena teoriana ymmärtää organisaatiota. Tieteellisessä liikkeenjohdossa keskeistä on työntekijöiden fyysisten kykyjen ja työolosuhteiden tutkiminen, sekä motivointi materiaalisten palkkioiden avulla. Klassisessa organisaatioteoriassa keskityttiin selvittämään organisaation rakentamisen periaatteita, eli miten hallinnon järjestelyillä tehostetaan organisaatiota. Klassisen teorian jälkeen lähes kaikissa organisaatioteorioissa organisaatiorakenne on ollut keskeinen tekijä. (Harisalo, 2008 s. 37–40)

Ihmissuhteiden koulukunta lähestyi organisaatiota nimensä mukaisesti ihmisen näkökulmasta, joka tieteellisessä liikkeenjohdossa oli pienemmällä huomiolla. Byrokratiateoriassa nähdään organisaatio rationaalisuuden mahdollistavana järjestelmänä, jossa pyritään ymmärtämään hallinnollisia tekijöitä, jotka

edistävät ja rajoittavat rationaalista toimintaa. Päätösteoriassa keskityttiin prosessiin, jossa suunnitellaan toiminnan järjestämistä ja tulevaisuutta. Tässä teoriassa analysoitiin ensimmäisen kerran organisaatiota dynaamisena prosessina. (Harisalo, 2008 s. 37–40)

Järjestelmäteoriassa, toiselta nimeltään systeemiteoriassa, mahdollistettiin organisaation analysointi osana itseään laajempia järjestelmiä. Järjestelmäteoriassa on tärkeää ymmärtää eri osatekijöiden välisiä riippuvuus- ja vuorovaikutussuhteita. Järjestelmäteoria yhdisti organisaation rakenteen ja prosessit sen toimintaympäristöön. Valtateoriassa keskeinen kysymys on, millaista valtaa organisaatio käyttää ja kuka tätä käyttää organisaatiossa. (Harisalo, 2008 s. 37–40)

Kontingenssiteoriassa otettiin huomioon ympäristön merkitys organisaation rakenteeseen ja käytäntöihin. Kontingenssiteorian mukaan ei ole olemassa yhtä oikeaa tapaa hallinnoida yritystä, vaan yrityksen rakenne, johtaminen ja päätöksenteko tulee suhteuttaa toimintaympäristöön. (Harisalo, 2008 s. 37–40)

Strateginen johtaminen korosti, että jotkut päätökset ovat merkittävimpiä, kuin toiset. Merkittäviä päätöksiä ovat strategiset päätökset ja vähemmän merkittävät ovat operatiivisia. Organisaatiokulttuuriteoria painotti kulttuurin merkitystä organisaation toiminnassa. Kulttuuri ohjaa toimintaa näkymättömästi, mutta vaikuttavasti. Innovaatioteoriassa kohdistettiin huomio organisaation muuttumiseen ja uudistumiseen. Tällä teorialla pyrittiin ymmärtämään organisaatioiden halu ja haluttomuus innovoida. (Harisalo, 2008 s. 37–40)

2.2.2 Organisaatiomallien kehitys

Siitä lähtien, kun moderni liikeyritys syntyi, Yhdysvaltojen sisällissodan ja Ranskan ja Preussin sodan jälkeen organisaatioiden käsitteessä ja rakenteessa on tapahtunut kaksi merkittävää muutosta kahdeksankymmentäluvun loppuun mennessä. Ensimmäinen tapahtui kymmenessä vuodessa vuosina 1895–1905. Siinä erotettiin johto omistuksesta ja vakiintunut johto itsenäisenä työnä ja tehtävänä. Toinen evoluutiomuutos tapahtui 20 vuotta myöhemmin. Modernimman yrityksen näkemyksen kehitys alkoi Pierre S. du Pontin perheyrityksen uudelleenjärjestelyllä 20-luvun alussa ja jatkui Alfred P. Sloanin General Motorsin muutoksella muutama vuosi myöhemmin. Tämä otti käyttöön silloin yleisen komentoja valvontaorganisaation. Tämä vaihe huipentui General Electricin massiiviseen uudelleenorganisointiin 1950-luvun alussa, joka täydellisti tätä mallia, jota useimmat suuryritykset ympäri maailmaa seurasivat vielä kahdeksankymmentäluvun loppu puolella. (Drucker, 1988).

Tiernan (1993) on tehnyt huomion jo yhdeksänkymmentäluvun alkupuolella, että organisaatiorakenne on muuttunut nopeasti viime vuosina, ja näyttää todennäköiseltä, että tämä suuntaus jatkuu. Tärkein ajuri on tullut muutoksista liiketoimintaympäristössä, joka on siirtynyt suhteellisen vakaan ja staattisen tilasta modernimpaan toimintaympäristöön, jolle on ominaista monimutkaisuus, epävarmuus, dynaamisuus ja kilpailu. Liiketoimintaympäristössä on tapahtunut muutoksia neljällä pääalueella - poliittisella, taloudellisella, teknologisella ja sosiaalisella. Trendit organisaationrakenteessa ovat henkilöstön vähentäminen,

muutokset työtehtävien suunnittelussa, tiimimekanismeissa ja lisääntynyt vastuu ja päätöksenteko. (Tiernan, 1993).

2.2.3 Organisaatiomallien konteksti ja ulottuvuudet

Organisaatiorakenteessa on vahva yhteys toiminnan ja kontekstin välillä. Daltonin ym. (1980) mukaan organisaatiorakenne ohjaa ihmisten toimintaa organisaation sisällä. "Organisaatioarkkitehdit" suunnittelevat rakenteensa vastaamaan toimintaa. Vaikka organisaatioiden rakenteessa on vaihteluita, ne ovat monesti pieniä, joten rakenteesta johtuvassa suorituskyvyssä ei ole eroa (Dalton ym., 1980). Pughin, Hicksonin, Hiningsin ja Turnerin (1969) tutkimuksessa havaittiin, että organisaation rakenne liittyy läheisesti kontekstiin, jossa se toimii ja suuri osa organisaation rakenteiden vaihteluista voidaan selittää kontekstiin liittyvillä tekijöillä, kuten organisaation koko, käytettävät teknologiat, sosiaalinen toiminta ja riippuvuus suhteet muiden organisaatioiden kanssa. Kaikkia näitä tekijöitä on ehdotettu ensisijaisen tärkeiksi vaikuttajiksi organisaation rakenteeseen ja sen toimintaan (Pugh, Hickson, Hinings & Turner, 1969).

Organisaatioteorian kirjallisuuden perusteella organisaation rakenteesta löydettiin kuusi ensisijaista ulottuvuutta: erikoistuminen, standardointi, formalisointi, keskittäminen, kokoonpano ja joustavuus, joista viisi ensimmäistä oli mukana tässä määritelmässä. Erikoistuminen määritellään organisaation sisällä suoritettavien eri ammattinimikkeiden tai erilaisten toiminnallisten tehtävien lukumääränä. Formalisointi viittaa siihen, missä määrin sopiva käytös kuvataan kirjallisesti. Standardointi määrää tai rajoittaa organisaation jäsenten käyttäytymistä ja menettelytapoja. Keskittämiseen liittyy auktoriteettien päätöksentekoon organisaatioissa. Jos esimerkiksi valta tehdä päätöksiä on yhdellä tai muutamalla henkilöllä, rakennetta pidetään keskitettynä. Kokoonpano on roolirakenteen "muoto". Sen tiedot sisältyisivät kattavaan ja yksityiskohtaiseen organisaatiokaavioon, joka sisältäisi kirjaimellisesti kaikki roolit organisaatiossa. (Pugh, Hickson, Hinings & Turner, 1968).

Edellä mainittu viisijakoinen määritelmä kuvaa organisaatiosta vain sisäistä toimintaa. Tämän luvun alussa todettiin, että organisaatioiden toiminta ja rakenne muuttaa vahvasti ympäristön muutosten mukana. Ympäristön ja organisaation väliseen hahmottamiseen tarvitaan näkökulma, joka ottaa myös organisaation ympäristön huomioon. Systeemiteoria ottaa organisaation ympäristön huomioon ja sitä tarkastellaan alaluvussa 2.3.2.

2.2.4 Tietopohjainen organisaatio

Tietopohjainen organisaatio vaatii kokonaisuudessaan paljon enemmän asiantuntijoita, kuin mitä nähdään perinteisissä komento- ja valvontaorganisaatioissa. Lisäksi asiantuntijat löytyvät operointi tasolta, ei yrityksen pääkonttorista. Operatiivisesta organisaatiosta tulee kaikenlaisten asiantuntijoiden organisaatio. Tietopohjaiset organisaatiot tarvitsevat keskeistä operatiivista työtä, kuten lakineuvontaa, PR-toimintaa ja työsuhteita yhtä paljon, kuin aina ennenkin. Mutta tarve

palveluhenkilöstölle, toisin sanoen ihmisille, joilla ei ole toiminnallista vastuuta, jotka vain neuvovat tai koordinoivat, kutistuu rajusti. Tietopohjainen organisaatio tarvitsee keskushallinnossa vain vähän, jos ollenkaan, asiantuntijoita. (Drucker, 1988).

Suuri osa työstä tehdään eri tavalla tietopohjaisessa organisaatiossa. Perinteiset osastot toimivat standardien vartijoina, koulutuskeskuksina ja asiantuntijoiden tehtävänjakajina. Ne eivät ole siellä, missä työ tehdään. Se tapahtuu suurelta osin tehtäväkeskeisissä tiimeissä. (Drucker, 1988).

Druckerin (1988) mukaan tietopohjainen organisaatio asettaa myös omat erityiset johtamisongelmansa:

1. Palkintojen, tunnustamisen ja uramahdollisuuksien kehittäminen asiantuntijoille.
2. Yhtenäisen vision luominen asiantuntijaorganisaatiossa.
3. Hallintorakenteen suunnittelu työryhmien organisaatiolle.
4. Ylimmän johdon henkilöiden saatavuus, valmistautuminen ja testaaminen.

Chasen (1997) toteuttamassa kyselytutkimuksessa havaittiin, että organisaatiot tunnistavat tiedon luomisen, hallinnan ja siirtämisen tärkeyden, mutta ne eivät ole toistaiseksi pystyneet muuntamaan näitä tarpeita strategioiksi (Chase, 1997). Organisaatiot siis tunnistavat jo tiedon merkityksen, mutta eivät vielä 2000-luvun vaihteessa ole onnistuneet toteuttamaan tietopohjaisia strategioita.

Bennet ja Bennet (2004) mainitsevat kirjassa: ”The rise of the knowledge organization”, että tiedon tärkeyden nykyinen tunnistaminen ja suosio, organisaation menestymiselle on vain alku todella älykkäiden organisaatioiden luomiselle. Tulevaisuuden perimmäinen haaste on vapauttaa ja vahvistaa kaikkien organisaation jäsenten tietoa ja luovuutta. Sillä yksin heissä elää älykkyyden ja viisauden lähde ja voima, jotka mahdollistavat tietopohjaisen organisaation nousun (Bennet & Bennet, 2004).

2.2.5 Tietotyö ja tietotyöntekijä

Druckerin (1999) kirjoituksessa “Knowledge-Worker Productivity: The Biggest Challenge” hän nosta esiin, että 2000-luvun suurimpana hallinnollisena haasteena tulee olemaan tietotyön ja tietotyöntekijöiden tehokkuuden kasvattaminen. 2000-luvun organisaation arvokkain voimavara tulee olemaan tietotyöntekijät ja heidän tuottavuutensa (Drucker, 1999).

Pöyriän (2005) mukaan tietotyö termin selkeä ja ytimekäs määrittely on osoittautunut vaikeaksi. Tietyt teemat, kuten korkea koulutustaso, korkea osaaminen ja tietotekniikan käyttö, ovat kuitenkin tulleet yhä yleisemmiksi, sekä empiirisessä, että teoreettisessa kirjallisuudessa (Pöyriä, 2005). Tietotyö voidaan määritellä työnä, joka luo, tulkitsee tai soveltaa uutta tietoa. Tämä määritelmä on melko kapea, joten vain pieni prosenttiosuus organisaatioissa tehtävästä työstä luokitellaan tietotyöksi (Maier, 2007). Kelloway ja Barling (2000) ehdottavat

artikkelissaan, että tietotyö tulisi nähdä työn ulottuvuutena. Kun tietotyö nähdään ulottuvuutena voi työtehtävä olla osittain tietotyötä ja osittain manuaalista työtä. Manuaalisen ja tietotyön suhde voidaan nähdä jatkumona (Kelloway & Barling, 2000).

Maierin (2007) mukaan tietotyön ominaisuuksia voidaan määritellä seuraavasti:

- **kohde**: ratkaisee hankalasti jäsenneltyjä ongelmia monimutkaisilla aloilla, joilla on paljon vaihtelevuutta ja poikkeuksia
- **sisältö**: on luovaa työtä, vaatii tiedon luomista, hankkimista, soveltamista ja jakamista. Sisääntulot ja ulostulot perustuvat pääosin dataan ja informaatioon
- **työtapa**: koostuu useista erityisistä toimintatavoista, kuten uuden tiedon luomisesta, tulkitsemisesta, integroinnista, esittämisestä, säilyttämisestä ja turvaamisesta, tiedon tuottamisesta ja toistamisesta
- **henkilökohtaiset taidot ja kyvyt**: fyysisten kykyjen sijaan tietotyö käyttää älyllisiä kykyjä ja asiantuntijuutta ja vaatii korkeaa koulutusta ja kokemuksia, jotka johtavat taitoihin ja asiantuntemukseen
- **organisaatio**: se on usein organisoitu hajautetusti käyttämällä uusia organisaation metaforia, kuten erikoistuneiden tietotyöntekijöiden yhteisöjä, sillä on vahvat viestintä-, koordinointi- ja yhteistyötarpeet ja se on erittäin liikkuva, joustava ja hajautettu
- **ICT**: vaatii vahvaa, mutta joustavaa henkilökohtaista tukea tieto- ja viestintätekniikoiden avulla

Tietovastuun merkitys muille työntekijöille ymmärretään yhä paremmin, erityisesti keskisuurissa yrityksissä. Mutta tietovastuu itselleen on edelleen suurelta osin unohdettu. Eli jokaisen henkilön organisaatiossa tulisi jatkuvasti miettiä, mitä tietoja hän tarvitsee oman työn tekemiseen ja panoksen antamiseen. (Drucker, 1988)

Tietoturvatehtävissä työskentelevien henkilöiden työ perustuu vahvasti informaation käsittelyyn, joten tietoturva-alalla työskentelevät ovat siis tietotyöntekijöitä. Datan, informaation ja tiedon avulla tehdään päätöksiä tietoturva toimien toteuttamiseksi. Jos tietotyöntekijä haluaa olla tehokas, on hänellä oltava tarvittavat tiedot työn toteuttamiseen. Informaation hallinnan efektiivisyys selittää 41 prosenttia tietotyöntekijän tehokkuudesta (Hwang, Kettinger, & Yi, 2015). Kyseessä on siis merkittävä tekijä kaikkien tietotyöntekijöiden keskuudessa.

2.3 Organisaatiomallit ja kyberturvallisuuden hallinta

Tietoturvallisuuden hallinta on kehittynyt kolmen vaiheen kautta. Ensimmäisessä vaiheessa it-ympäristöä suojattiin lähinnä teknisin keinoin. Ajan myötä organisaatioiden "tekniset ihmiset" alkoivat ymmärtää, että johtamisella oli merkittävä rooli tietoturvassa ja, että ylimmän johdon on myös osallistuttava

tietoturvan toteuttamiseen. Tämä johti toiseen vaiheeseen, jossa tietoturva sisällytettiin organisaatiorakenteisiin. Tietoturvan kehityksen kolmas vaihe korostaa, että tietoturva tulisi sisällyttää jokapäiväisiin käytäntöihin, jotka suoritetaan osana työntekijän työtä, jotta siitä tulisi elämäntapa ja siten kehitettäisiin tehokasta tietoturvakulttuuria koko organisaatiossa. (Veiga & Eloff, 2007)

Julisch (2013) on löytänyt tutkimuksessaan neljä merkittävää heikkoutta organisaatioiden kyberturvallisuudesta. Ensimmäisenä on intuitioon ja kognitiivisiin ennakkoluuloihin perustuva päätöksenteko. Toinen heikkous on perus tietoturvakontrollien puute. Kolmas on liiallinen painotus staattisiin uhkatietoihin, kuten virusskannereihin ja vähäinen investointi dynaamiseen kybertiedusteluun. Viimeinen ongelma on heikko hallinto, joka jättää aukkoja siihen, miten päätöksiä tehdään ja kyberturvallisuuskontrolleja hallitaan (Julisch, 2013).

Julischin (2013) mukaan organisaatioiden on määriteltävä selkeät hallintorakenteet. Hallinnoinnin vaikeus on, että ei ole olemassa yhtä ainoaa optimaalista tapaa hallinnoida. Organisaation strategiasta, rakenteesta ja kulttuurista riippuen eri hallintorakenteet toimivat parhaiten. Sopivan hallintorakenteen kehittämiseksi organisaatioita kehotetaan noudattamaan systemaattista lähestymistapaa, kuten seuraavaa, joka perustuu Weillin ja Rossin (2004, 2005) kirjaan ja artikkeliin aiheesta:

1. Määritä tärkeimmät päätökset, jotka on tehtävä kyberturvallisuuden suhteen (esim. budjetti, turvallisuuskontrollien valinta ja suunnittelu, turvallisuuskontrollien hallinta ja valvonta, turvallisuuskontrollien toteutus jne.).
2. Määritä näiden päätösten tekemiseen liittyvät roolit (liiketoiminta vs. IT-roolit ja tiedottaja vs. päättäjä).
3. Määritä valvontamekanismit, jotka määrittävät, kuinka näiden roolien haltioita mitataan ja pidetään vastuussa.
4. Käytä hallintomekanismeja, kuten hyväksymisprosesseja keinona vakiinnuttaa roolit ja mittaukset.
5. Suunnittele erilliset mutta toisiinsa liittyvät hallintajärjestelmät, joita voi olla olemassa useilla organisaatiotasoilla (esim. yritys-, liiketoimintayksikkö- ja ryhmä- / aluetasolla) toistamalla vaiheet 1–4.
6. Lopuksi poistu tieltä ja anna tietoturva henkilöstön tehdä todelliset päätökset.

Systemaattinen lähestymistapa, kuten edellä mainittu lista mahdollistaa kaikkien hallintoon liittyvien tekijöiden huomioon ottamisen. Näitä vaiheita seuraten organisaatiot pystyvät rakentamaan itselleen sopivan hallintorakenteen. Vastuu henkilöiden määrääminen auttaa toiminnan hallitsemisessa. Valvontamekanismit auttavat päätösten tehokkuuden mittaamisessa. Etenkin isoissa organisaatioissa on viisasta tehdä useita hallintajärjestelmiä, jotta toiminnan kaikki osa-alueet tulevat katetuksi. Viimeisenä listalla mainitaan sivuun astuminen tietoturva henkilöstön edestä, sillä heillä on ammattitaito tehdä päätöksiä ja johdon tehtävänä on vain asettaa rajoitteet ja resurssit näille päätöksille.

2.3.1 Organisaation kolme päätöksentekotasoa ja ohjaus/kontrolli sykli

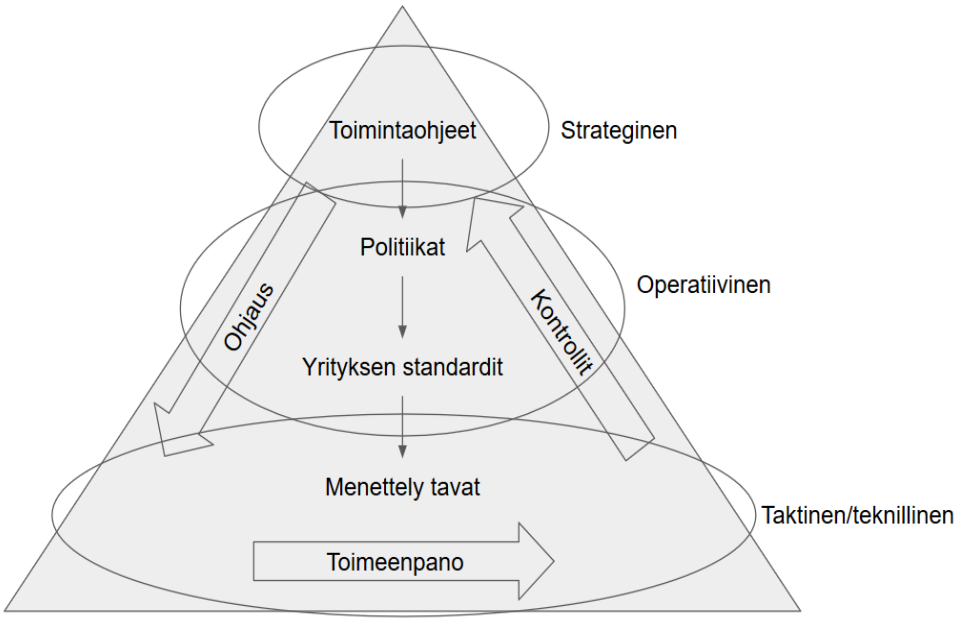
Koska yritysten kyberturvallisuuden tuottamiseksi ei ole yhtä oikeaa mallia tai tapaa (Julisch, 2013), on perusteltua tarkastella asiaa jonkin viitekehyksen kautta, joka mahdollistaa eri mallien ja tapojen hahmottamisen helpommin. Seuraavaksi tarkastellaan eri malleja, joissa on havaittavissa organisaation kolme päätöksentekotasoa.

Yritysten ICT-hallintorakenteista on havaittavissa organisaation kolme päätöksentekotasoa. Jouko Selkälän väitöskirjan (2016) mukaan yritysten, joilla on kansainvälisiä toimintoja, globaalissa ICT-hallintorakenteessa on kolme tasoa. Nämä kolme tasoa ovat vastaavat kuin aiemmin mainitut: strateginen, operatiivinen ja taktinen/teknillinen. Taktinen/teknillinen taso varmistaa sujuvan päivittäisen toiminnan, operatiivinen taso varmistaa suorituskyvyn ja strateginen taso parantaa IT:n arvoa (Selkälä, 2016). Vastaavia tasoja voidaan käyttää myös kyberhallinnossa.

Kolmea päätöksentekotasoa ovat myös esillä Veigan ja Eloffin (2007) ehdottamassa tietoturvallisuuden hallinnan viitekehyksessä. Strategiselle tasolle kuuluu johtajuus ja hallinto. Operatiiviselle tasolle kuuluvat turvallisuuden hallinta ja organisointi, turvallisuuspolitiikat, tietoturvaohjelmien hallinta ja käyttäjien tietoturvan hallinta. Taktisella/teknillisellä tasolla on teknologian ja toiminnan suojaaminen (Veiga ja Eloff, 2007).

Myös Solms & Solms (2008) ehdottavat, että organisaation työntekijät voidaan jakaa kolmelle eri tasolle organisaation hallinnan näkökulmasta. Tasoja ovat: hallitus ja johto, ylempi- ja keskijohto, sekä alempijohto ja hallinto. Nämä voidaan myös katekorisoita kolmen organisaation päätöksentekotason avulla, jossa hallitus ja ylin johto kuuluvat strategiselle tasolle. Ylempi- ja keskijohto kuuluvat operatiiviselle tasolle ja alempijohto ja hallinto kuuluvat taktiselle/teknilliselle tasolle (Solms & Solms, 2008).

Solms ja Solms (2008) mukaan yritysten hallinnon määritelmistä löytyy aina kaksi tekijää, jotka ovat toiminnan ohjaaminen ja kontrollointi. Tätä voidaan kutsua ohjaus/kontrolli sykliksi, joka on esitetty muokattuna kuviossa 3. Toiminnanohjaus vaiheessa ohjataan, suunnitellaan tai asetetaan vastuita ja kontrolli vaiheessa kontrolloidaan lopputulemaa, toimeenpanoa ja varmistetaan näiden toteutuminen (Solms & Solms, 2008).



KUVIO 3 Ohjaus/kontrolli sykli (Solms & Solms 2008, muokattu)

Solms ja Solms (2008) kuvaavat ohjaus/kontrolli sykliä seuraavasti. Yrityksen strategisella tasolla ohjataan yrityksen toimintaa ja asetetaan toimintaohjeita, joiden perusteella luodaan politiikkoja ja standardeja yritykseen operatiivisella tasolla. Näistä dokumenteista muodostuu yrityksen menettelytavat, joita toimeen pannaan yrityksen taktisella/teknillisellä tasolla. Kontrollien nuoli osoittaa kuviossa ylöspäin. Kontrollien tavoitteena on tuottaa ylimmälle johdolle tietoa siitä, että ohjaus toimii halutulla tavalla. (Solms & Solms, 2008).

2.3.2 Systeemiteoria

Systeemiteoria on järjestelmäteorian synonyymi. Systeemiteoria on yksi organisaatioteorioista, joka mainittiin aikaisemmin organisaatioteorioiden yhteydessä. Systeemiteorian mukaan organisaation on järjestelmä, joka on jatkuvasti vuorovaikutuksessa muiden organisaatioiden ja oman toimintaympäristönsä kanssa. Systeemiteoria mahdollisia organisaation ja sen ympäristön välisten suhteiden tutkimisen. Systeemiteoria on siirtänyt huomion yksittäisten tekijöiden analysoinnista kokonaisuuden analysointiin. (Harisalo, 2008 s. 195)

Systeemi määritellään kokonaisuudeksi kokonaisuuksia, jotka toimivat yhdessä tietyn tarkoituksen suorittamiseksi. Systeemillä on rajat, jotka erottavat sen ympäristöstään. Systeemin sisälle päästään syötteiden (input) kautta ja ulos systeemistä päästään ulostulojen (output) kautta. Järjestelmä voi sisältää säätökomponentteja, joilla voidaan säädellä ulostuloa sisääntulojen perusteella. (Ashby, 1961)

Kybertoimintaympäristön kompleksisuus ulottuu tietoturvaratkaisujen suunnitteluun. Systeemitiede tarjoaa tietoa siitä, kuinka monimutkaiset

järjestelmät ovat vuorovaikutuksessa ympäristönsä kanssa, ja tätä voidaan soveltaa turvallisuusarkkitehtuurien suunnitteluun. Turvajärjestelmien analysointi ja suunnittelu systeemiteorian avulla tarjoaa uuden polun vähentää kompleksisuutta. (Conklin & Dietrich, 2008)

Systeemiin kohdistuvien uhkien tutkiminen yksittäisten tekijöiden kokoelmana erikseen ei tarjoa asianmukaista tietoa riittävän vahvan puolustuksen luomiseksi. Sen lisäksi, että pelkästään listataan uhkia ja niiden mekanismeja, tarvitaan ymmärrys järjestelmätasosta, joka antaa turvasuunnittelijalle mahdollisuuden käyttää useita kerroksia puolustuksia, joilla on kyky vaikuttaa uhkaan tehokkaammin. (Conklin & Dietrich, 2008)

Organisaation kyberturvallisuutta voidaan siis tarkastella systeeminä, joka toimii edellisessä luvussa mainitulla organisaation kolmella päätöksentekotasolla. Systeemi vaikuttaa myös kaikilla kyberturvallisuuden viidellä tasolla. Päätöksenteko asettuu kognitiiviselle, eli ylimmälle tasolle, mutta päätösten vaikutus voi ulottua aina fyysiseen tasoon asti.

2.3.3 Osallistaminen

Tietoturvaan liittyvä kirjallisuus kuvaa käyttäjiä usein heikkona linkkinä, mutta käyttäjät voivat olla myös arvokas resurssi tietoturvaan tarjoamalla tarvittavaa liiketoimintatietoa, joka edistää tehokkaampia turvatoimia. Käyttäjien osallistaminen on myös keino sitouttaa käyttäjät suojaamaan arkaluonteisia tietoja liiketoimintaprosesseissa. (Spears & Barki, 2010)

On ainakin kaksi syytä, miksi käyttäjien osallistaminen tietoturvan hallintaan voi olla arvokasta. Ensinnäkin käyttäjien tietämyksen lisääminen tietoturvaan liittyvistä riskeistä uskotaan yleisesti olevan tehokkaan turvallisuuden perusta. Toiseksi tietoturvan kontrollit on sovitettava yhteen liiketoiminnan tavoitteiden kanssa, jotta ne olisivat tehokkaita. Tällainen linjaus edellyttää ymmärrystä tiedon suhteellisesta arvosta ja siitä, miten tietoa käytetään liiketoimintaprosesseissa ja niiden välillä, ja missä prosessin arkaluontoiset tiedot ovat haavoittuvimpia. Käyttäjien osallistuminen tietoturvariskien analysointiin ja tietoturvakontrollien suunnitteluun voi tarjota tarvittavaa liiketoimintatietoa ja edistää siten tehokkaampia turvatoimia. (Spears & Barki, 2010)

Käyttäjien havaittiin lisäävän arvoa tietoturvariskien hallintaan, kun he osallistuivat liiketoimintaprosessien käyttäjiin liittyvien kontrollien priorisointiin, analysointiin, suunnitteluun, toteuttamiseen, testaamiseen ja seurantaan. Käyttäjien osallistuminen lisää organisaation tietoisuutta tietoturvariskeistä ja kontrolleista liiketoimintaprosesseissa, mikä puolestaan edistää turvallisuuden valvonnan kehittämistä ja suorituskykyä. Tarve noudattaa käytäntöjä voi kannustaa käyttäjiä osallistumaan tietoturva riskienhallintaan liiketoimintaprosesseissa. Turvallisuuspäälliköt voivat hyödyntää sääntelyn noudattamista mahdollisuutena sitouttaa käyttäjät, lisätä organisaation tietoisuutta turvallisuudesta ja yhdenmukaistaa turvallisuustoimenpiteitä paremmin liiketoiminnan tavoitteiden kanssa. (Spears & Barki, 2010)

Käyttäjien osallistamista on tutkittu myös tietoturvapolitiikan toteutumisen kontekstissa. Karyda, Kiountouzis & Kokolakis (2005) toteavat, että organisaatiorakenteella on tärkeä rooli turvallisuuspolitiikan onnistuneessa toteuttamisessa ja hyväksymisessä. Organisaatiot, joissa on työntekijöitä, jotka osallistuvat erilaisiin tietoturvaan liittyviin aktiviteetteihin ja joilla on lisääntynyt vastuullisuus, kehittävät todennäköisemmin turvallisuuskulttuuria ja luovat henkilöstölleen korkean turvallisuustietoisuuden. Jäykkä hierarkkinen rakenne voi olla ongelma tietoturvan hallinnassa, koska turvallisuuspolitiikan soveltaminen vaatii usein organisaation joustavuutta, mukaan lukien uusien roolien luomista tai olemassa olevien muokkaamista. (Karyda, Kiountouzis & Kokolakis, 2005)

Yksi tärkeä kysymys on organisaation johdon aktiivinen osallistuminen ja näkyvä tuki. Tietoturvapolitiikan laatiminen ja toteuttaminen edellyttää yleensä paljon ylimääräistä työtä, ei vain IT-henkilöstöltä, vaan myös käyttäjiltä, joiden on ryhdyttävä uusiin työtapoihin ja hylättävä tai muutettava vanhoja. Tästä syystä johdon osallistuminen tietoturvan toteutukseen voi vaikuttaa merkittävästi tietoturvapolitiikan onnistumiseen. Pätevä tietoturvapäällikkö voi myös auttaa tietoturvapolitiikan toteutumisessa. Käyttäjät ottavat todennäköisemmin käyttöön turvallisuuspolitiikan menettelyt, kun politiikka on yhdenmukainen heidän ammatillisten tavoitteidensa kanssa ja auttaa täyttämään tehtävänsä tehokkaammin. (Karyda, Kiountouzis & Kokolakis, 2005)

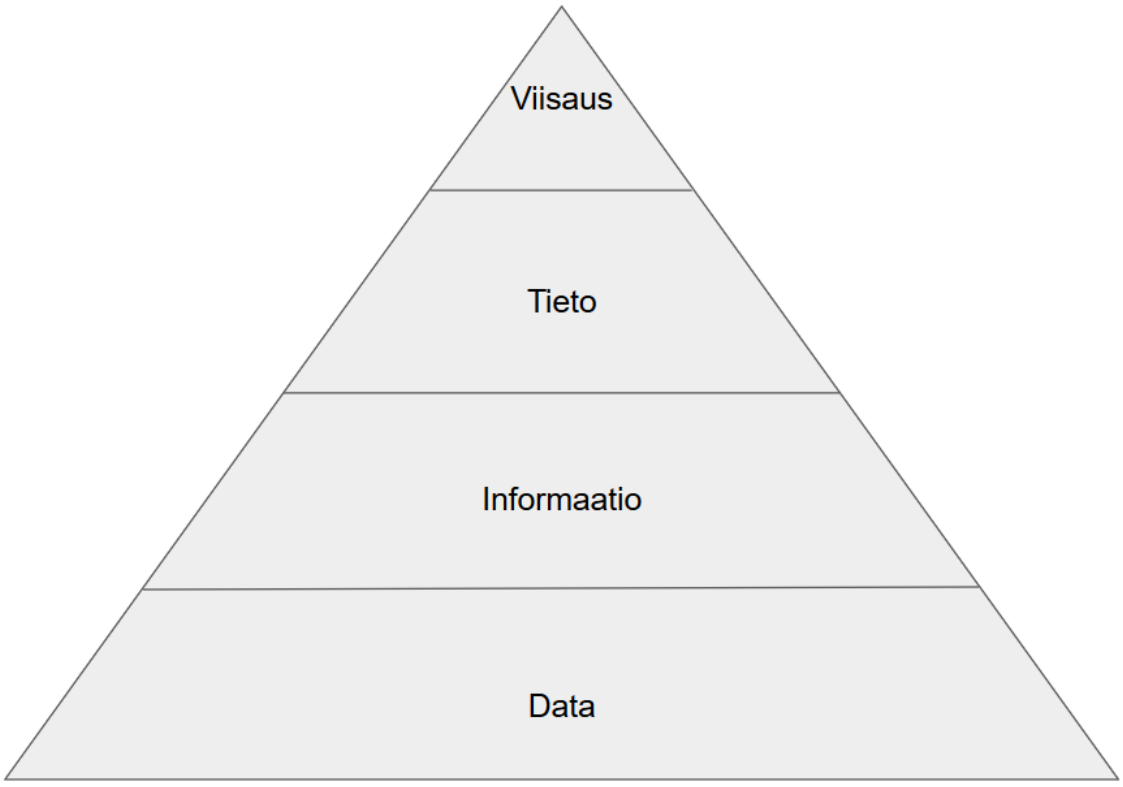
Organisaatioilla, joilla on johdonmukainen kulttuuri, varsinkin kun heidän työntekijänsä noudattavat toimintaohjeita tai eettisiä sääntöjä, on myös paremmat mahdollisuudet toteuttaa ja ottaa käyttöön tietoturvapolitiikka. Tietoturvapolitiikan onnistunut hyväksyminen edellyttää työntekijöiden keskinäisen yhteisymmärryksen ja yhteisten merkitysten kehittämistä. Tätä helpottaa aikaisempi kokemus noudattaa yhteisiä käytännesääntöjä. (Karyda, Kiountouzis & Kokolakis, 2005)

3 Tieto ja tiedonhallinta

Luvun aiheena on tiedonhallinta, joten ensimmäisenä vastataan kysymykseen siitä, että mitä tieto ylipäätään on ja määritellään eri tasoja, millä tietoa voi esiintyä. Alaluvussa 3.2 katsotaan, miten organisaatiot luovat tietoa ja alaluvussa 3.3 käsitellään tiedonhallinnan teorioita ja tiedonhallintaa kyberturvallisuuden kontekstissa, sekä tietotyötä ja tietotyölle ominaisia asioita. Viimeisessä alaluvussa käsitellään tiedonhallinnan järjestelmiä ja niille tyypillisiä ominaisuuksia.

3.1 Mitä tieto on?

Data-, informaatio-, tieto-, viisaushierarkia on yksi perustavista malleista tieto- ja informaatiokirjallisuudessa. Rowleyn (2007) mukaan hierarkia tunnetaan myös nimillä tietohierarkia, informaatiohierarkia ja tietopyramidi. Tuoreemmassa kirjallisuudessa kirjoittajat mainitsevat usein Ackoffin 1989 tutkimuksen hierarkian lähteenä. Ackoffin (1989) artikkeli ”From data to wisdom” ehdotti hierarkiaa seuraavilla tasoilla: data, informaatio, tieto, ymmärrys ja viisaus. Ackoff sisällytti ymmärryksen hierarkiaansa, mutta tuoreemmat kommentit hierarkiasta ovat kiistäneet, että ymmärtäminen on erillinen taso. Näiden kommenttien mukaan ymmärtäminen on mukana aina, kun siirrytään alemmalta tasolta seuraavalle (Rowley, 2007). Viisaushierarkia on esitetty kuviossa 4.



KUVIO 4 Viisaushierarkia (Ackoff, 1989, muokattu)

Ackoffin (1989) määritelmien mukaan data, informaatio, tieto ja viisaus määritellään seuraavasti:

- Data määritellään symboleina, jotka edustavat esineiden, tapahtumien ja niiden ympäristön ominaisuuksia, ja ne ovat havainnon tuloksia. Mutta niistä ei ole hyötyä, ennen kuin ne ovat käyttökelpoisessa (ts. merkityksellisessä) muodossa. Datan ja informaation välinen ero on toiminnallinen, ei rakenteellinen.
- Informaatio sisältyy kuvauksiin ja kysymysten vastauksiin, jotka alkavat sellaisilla sanoilla kuten: kuka, mitä, milloin ja kuinka monta. Tietojärjestelmät tuottavat, tallentavat, hakevat ja käsittelevät tietoja. Informaatio päätellään datasta.
- Tieto on taitotietoa, ja se tekee mahdolliseksi muuntaa informaatio ohjeiksi. Tieto voidaan saada joko toiselta henkilöltä, ohjeesta tai oppimalla se kokemuksesta.
- Viisaus on kyky lisätä efektiivisyyttä.

Ackoffin (1989) maaliin pohjautuva kuvio toimii alhaalta ylöspäin. Alimmalla tasolla dataa on paljon, mutta sillä ei ole juurikaan rakennetta tai merkitystä. Ylimmällä tasolla viisautta on vähän ja se on vahvasti merkityksellistä ja rakenteellista. Alemman tason resurssia tarvitaan aina enemmän, kun siirrytään ylemmälle tasolle ja siitä saadaan ymmärryksen kautta rakennettua seuraavan tason resurssi.

3.2 Miten organisaatio luo tietoa

Organisaatioteoriaa on pitkään dominoinut paradigma, jossa käsitellään organisaatiota järjestelmänä, joka käsittelee tietoa tai ratkaisee ongelmia. Keskeistä tässä paradigmassa on oletus, että organisaation perustehtävä on se, kuinka tehokkaasti se pystyy käsittelemään tietoja ja päätöksiä epävarmassa ympäristössä. Tämä paradigma viittaa siihen, että ratkaisu on hierarkkisen tietojenkäsittelyn sisääntulo ulostulo sekvenssissä. Tämän paradigman ongelmana on sen passiivinen ja staattinen näkymä organisaatioon. Tietojenkäsittelyä pidetään ongelmanratkaisutoimintana, joka keskittyy organisaatiolle annettavaan tietoon, ottamatta huomioon tietoa, jota organisaatio itse luo. Kaikkien organisaatioiden, jotka käsittelevät dynaamisesti muuttuvaa ympäristöä, ei pitäisi vain käsitellä tietoa tehokkaasti, vaan myös luoda informaatiota ja tietoa. (Nonaka, 1994)

Vaikka ideat muodostuvat yksilön mielessä, yksilöiden välisellä vuorovaikutuksella on kriittinen rooli näiden ideoiden kehittämisessä. Toisin sanoen "vuorovaikutusyhteisöt" myötävaikuttavat uuden tiedon lisääntymiseen ja kehittämiseen. Organisaatio ei voi luoda tietoa ilman yksilöitä. Organisaatio tukee luovia yksilöitä tai tarjoaa kontekstin henkilöille tiedon luomiseen. Siksi organisaation tietotaidon luominen tulisi ymmärtää prosessina, joka organisatorisesti

vahvistaa yksilöiden luomaa tietoa ja kiteyttää sen osaksi organisaation tietämystä. (Nonaka, 1994)

Tieto voidaan jakaa kahteen eri kategoriaan, eksplisiittiseen ja hiljaiseen tietoon. Eksplisiittisellä tai kodifioidulla tiedolla tarkoitetaan tietoa, joka on siirrettävissä muodollisella, systemaattisella kielellä. Hiljaisella tiedolla on henkilökohtainen ominaisuus, mikä vaikeuttaa virallistamista ja kommunikointia. Hiljainen tieto juurtuu syvälle toimintaan, sitoutumiseen ja osallistumiseen tietyssä kontekstissa. (Nonaka, 1994)

Nonakan (1994) matriisi hiljaisen ja eksplisiittisen tiedon muuttumisesta on esillä kuviossa 5.

KUVIO 5 Hiljaisen tiedon siirtyminen ja muuttuminen eksplisiittiseksi (Nonaka, 1994)

Sosialisointi on prosessi, jonka avulla voimme siirtää hiljaista tietoa yksilöiden välisen vuorovaikutuksen avulla. Yksi huomioitava asia on, että henkilö voi hankkia hiljaisen tiedon ilman kieltä. Oppisopimuskoulutuksen harjoittajat työskentelevät mentoreidensa kanssa ja oppivat käsityötä tarkkailemalla, jäljittelemällä ja harjoittelemalla. Yritysympäristössä työharjoitteluissa käytetään samaa periaatetta. Avain hiljaisen tiedon hankkimiseen on kokemus. (Nonaka, 1994)

Toinen tiedonmuunnostapa, eli yhdistäminen sisältää sosiaalisten prosessien käytön yksilöiden hallussa olevan eksplisiittisen tiedon eri kappaleiden yhdistämiseksi. Yksilöt vaihtavat ja yhdistävät tietoa sellaisten vaihtomekanismien kautta, kuten esimerkiksi kokoukset ja puhelinkeskustelut. Olemassa olevan tiedon uudelleen konfigurointi, lajittelu, lisääminen, uudelleen kategorisointi ja tekstittäminen voi johtaa uuteen eksplisiittiseen tietoon. Yhdistämisessä eksplisiittinen tieto muuttuu uudeksi eksplisiittiseksi tiedoksi. (Nonaka, 1994)

Kolmas ja neljäs tiedonmuunnostapa liittyvät muunnosmalleihin, joihin sisältyy sekä hiljaista että eksplisiittistä tietoa. Nämä muuntamistavat vangitsevat

ajatuksen siitä, että hiljainen ja eksplisiittinen tieto ovat täydentäviä ja voivat laajentua ajan myötä keskinäisen vuorovaikutuksen kautta. Tämä vuorovaikutus käsittää kaksi erilaista operaatiota. Ensimmäinen on hiljaisen tiedon muuntaminen eksplisiittiseksi tiedoksi, jota kutsutaan ulkoistamiseksi. Toinen on eksplisiittisen tiedon muuntaminen hiljaiseksi tiedoksi, jota kutsutaan sisäistämiseksi. (Nonaka, 1994)

3.3 Tiedonhallinnan teoriat ja järjestelmät

Tiedonhallintakyky on organisaation kyvykkyyden mahdollistaja. Tiedonhallintakyky tarjoaa peruskyvykkyyden, jonka avulla organisaatiot voivat rakentaa korkeamman tason valmiuksia. Nämä korkealaatuisemmat ominaisuudet puolestaan vaikuttavat erilaisiin organisaation suorituskyvyn mittareihin. (Hwang, Kettinger & Yi, 2015; Maier, 2007; Rubenstein-Montano ym., 2001).

Tiedonhallinta sisältää paljon enemmän, kuin vain teknologiat tiedon jakamisen helpottamiseksi. Organisaation ihmiset ja kulttuuri ovat tekijöitä, jotka lopulta määrittävät tiedonhallinnan onnistumisen ja epäonnistumisen. Teknologia monesti ohjaa kapeaan näkemykseen, joka voi estää tiedonhallinnan kasvun ja pysyvyyden. (Rubenstein-Montano ym., 2001).

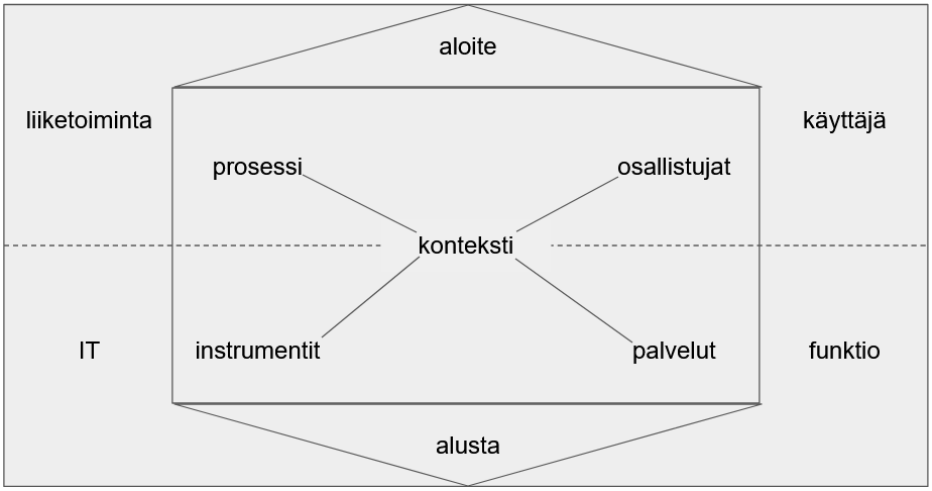
Tiedonhallinta käsittää erilliset, mutta toisistaan riippuvat tiedon tuottamisen, tallennuksen ja noutamisen, tiedon siirron ja tiedon soveltamisen prosessit. Organisaatio ja sen jäsenet voivat milloin tahansa olla mukana useissa tiedonhallinnan prosessiketjuissa. Tiedonhallinta ei ole selkeä kokonaisuus vaan dynaaminen ja jatkuva organisaatioilmiö. Lisäksi tiedonhallintaprosessien monimutkaisuus, resurssivaatimukset, taustalla olevat työkalut ja lähestymistavat vaihtelevat tietohallintoprosessien tyypin, laajuuden ja ominaisuuksien mukaan. (Alavi & Leidner, 2001)

3.3.1 Tiedonhallinnan järjestelmät

Tiedonhallintajärjestelmät viittaavat tietojärjestelmien luokkaan, jota käytetään organisaation tiedonhallintaan. Toisin sanoen ne ovat IT-pohjaisia järjestelmiä, jotka on kehitetty tukemaan ja parantamaan organisaatioprosesseja tiedon luomisen, tallentamisen/hakemisen, siirron ja soveltamisen osalta. Tiedonhallintajärjestelmät voivat hyödyntää erilaisia IT-työkaluja ja -ominaisuuksia käyttämällä erilaisia rooleja organisaation tietohallintaprosessien tukemisessa. Tarkasteltaessa kirjallisuutta, jossa keskustellaan tietotekniikan soveltamista organisaation tiedonhallinnan aloitteisiin, paljastuu kolme yleistä sovellusta: parhaiden käytäntöjen kirjaaminen ja jakaminen, yritysten tietohakemistojen luominen ja tiedon verkostojen luominen. (Alavi & Leidner, 2001)

Tiedonhallintajärjestelmiä voidaan hahmottaa niiden ominaisuuksien kautta. Kuvio 4 antaa yleiskuvan näistä ominaisuuksista. Kolme ominaisuutta: aloite, prosessi ja osallistujat voidaan osoittaa liiketoiminnalle ja käyttäjälle.

Instrumentit, palvelut ja alusta ovat IT- tai toimintokeskeisiä ominaisuuksia. Konteksti on yhdistävä asia, joka yhdistää liiketoiminnan ja IT: n sekä käyttäjä- ja toiminto ominaisuudet. Aloitteen tavoitteet auttavat määrittelemään prosessit ja osallistujat, jotka toteutetaan tiedonhallinnan työvälineiden avulla, joita tiedonhallintajärjestelmän palveluiden tulisi tukea kattavan alustan pohjalta ja valvoa niiden käyttöönottoa. Osallistujat ja yhteisöt ovat kohdennettuja käyttäjäryhmiä, jotka ovat vuorovaikutuksessa tiedonhallintajärjestelmän kanssa tehtävien suorittamiseksi. (Maier, 2007)



KUVIO 6 Tiedonhallintajärjestelmän ominaisuudet (Maier, 2007)

Kuviossa esiteltyjen ominaisuuksien voidaan katsoa väittävän tiettyjä palveluja. Alusta edellyttää infrastruktuurin palvelujen sisällyttämistä varastointiin, viestintään, pääsyyn ja tietoturvaan, joka perustuu data- ja tietolähteisiin. Konteksti vaatii kontekstualisoitujen tietojen käsittelyä, mikä edellyttää integrointipalveluja, jotka kuvaavat resursseja, jotka on koottu yhteen useista lähteistä. Palvelut rakentuvat näiden integraatiopalvelujen päälle ja tarjoavat tukea työvälineille. Näiden tietopalvelujen on tuettava kaikkia tiedonhallinta-aloitteessa määriteltyjä hankinta- ja käyttöönottoprosesseja. Tieto- ja viestintätekniikan näkökulmasta nämä ovat julkaisun, yhteistyön, oppimisen ja löytämisen palveluja. Tietopalvelut on räätälöitävä osallistujien yksilöllisiin tarpeisiin ja toisaalta niiden prosessien ja projektien vaatimuksiin, joita he suorittavat. Tämä edellyttää personointipalveluja. Osallistujat voivat halutessaan käyttää tiedonhallintajärjestelmää useilla laitteilla ja sovelluksilla. (Maier, 2007)

Konkreettinen tiedonhallinnan työkalu kyberturvallisuudessa on tiketöinti järjestelmä. Tiketöintijärjestelmään kirjataan tietoturvatapahtumista raportteja, eli tikettejä. Tiketöintijärjestelmän avulla voidaan keskittää tietoturvatapahtumien raportointi yhteen järjestelmään.

3.3.2 Tiedonhallinta kyberturvallisuudessa

Kyberturvallisuus on erityisesti tiedonhallinnan ongelma. On paljon tietoa, jota on tulkittava, jotta päätökset voidaan tehdä ajoissa. Tähän prosessiin osallistuu useita sidosryhmiä, joilla on erilaiset taustat. Usein näillä ryhmillä on oma ammattikieli, kulttuuri ja standardit. Kyberturvallisuus on monimutkaista, ja siihen sisältyy kokonaisvaltainen lähestymistapa, jossa useimmat organisaatiot tarvitsevat tietyntyyppisiä liiketoimintatiedon hyödyntämis- ja analyyttisiä prosesseja, sekä työkaluja sen hallintaan. (Tisdale, 2015)

Kyberturvallisuudessa vaaditaan parempaa tietojen jakamista ja automatisointia. Nykyiset käytännöt ja niitä tukevat teknologiat rajoittavat organisaatioiden kykyä hyödyntää täysimääräisesti henkilöstönsä asiantuntemusta ja luottamussuhteita, joiden avulla he pyrkivät turvaamaan organisaation tietojärjestelmät. Rajoituksiin kuuluvat yhteen toimivien standardien puuttuminen, mekanismien puuttuminen arkaluontoisten tietojen käytön hallitsemiseksi ja valvomiseksi, sekä ongelmat tietojen laadun vahvistamiseksi. (Dandurand & Serrano, 2013).

Kyberturvallisuuteen liittyvää organisaatiotietoa ei voida kuvata kaikkien sisäisten organisaation toimijoiden tietämyksen ja uskomusten summaksi, vaan se on toimijoiden, uskomusten ja ympäristön välisten rakenteiden vuorovaikutusten funktio. Tämä funktio toimii sopeutumisen/kalibroinnin lähteenä jatkokäyttäytymiseen. Tiedon tulkinnan jakaminen on keskeinen tekijä monitieteisessä kokonaisuudessa, jota tarvitaan organisaation kyberturvallisuustoimien tukemiseksi. (Sallos, Garcia-Perez, Bedford & Orlando, 2019)

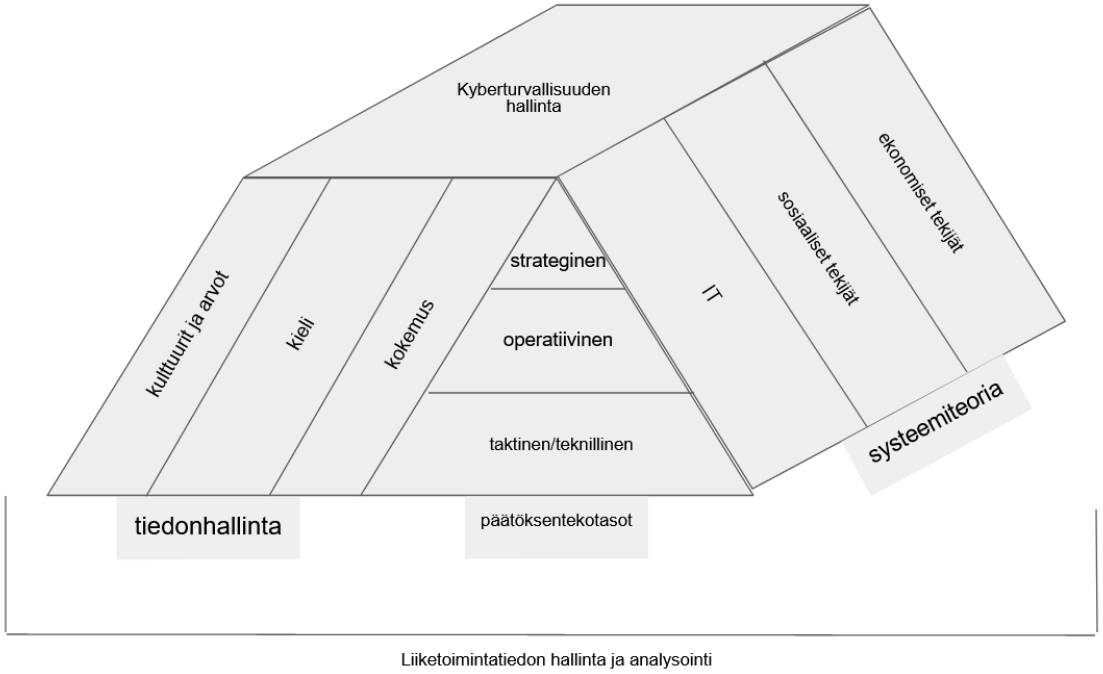
Kyberturvallisuuden hallinta on haastava ulottuvuus nykyaikaisessa organisaatioympäristössä, ja se vaatii huomiointia strategioissa, arvoissa, rakenteissa ja käytännöissä. Sen merkitystä korostavat organisaatiomallit, joissa hyödynnetään aineetonta omaisuutta ja henkistä pääomaa ensisijaisena alustana arvonmuodostuksessa. Kyberturvallisuusstrategialla, joka perustuu tehokkaisiin tietohallintakäytäntöihin, on mahdollisuus kanavoida organisaation henkinen pääoma ja sen operatiivisuus kohti arvonluontia. (Sallos, Garcia-Perez, Bedford & Orlando, 2019)

Tisdalen (2015) mukaan kyberturvallisuuden hallitsemiseksi paremmin seuraavat kohdat tulisi ottaa huomioon:

- teknologia näkökulma ei ole tarpeeksi kattava kyberturvallisuuden toteutukseen
- organisaatio tulisi nähdä monimutkaisena systeeminä
- työntekijöiden on kaikilla tasoilla osallistuttava tiedonhallintaprosessiin sekä luotava ja jaettava tietoja organisaatiossa
- organisaatio voi hyötyä kyberturvallisuuden hallintojohtajasta, joka on taitava useilla organisaation toiminta-alueilla
- kyberturvallisuustoiminnot ja -järjestelmät voidaan tunnistaa katsomalla ensin liiketoimintaongelman tietojen, niiden prioriteetin ja niihin liittyvien tietojärjestelmien kautta

Tisdalen (2015) listassa korostuu systeemi ajattelu, sekä tiedonhallinta ja -luominen organisaatiossa. Tietohallintaprosessiin osallistuminen kaikilla tasoilla mahdollistaa oikean tiedon kulkeutumisen oikeille henkilöille. Drucker (1988) toteaa, että työntekijät ymmärtävät hyvin, mitä tietoa heidän tulee jakaa muille, mutta tiedon vaatiminen oman työn tekemiseksi on puutteellista. Hallintojohtaja, joka on moniosaaja organisaation toimialueilla voi luonnollisesti allokoida resursseja ja tulkita tilannekuvaa tehokkaammin, jos hän ymmärtää organisaation toimintaa monipuolisesti.

Kuviossa 7, esitellään Tisdalen (2015) viitekehykseen perustuva malli kyberturvallisuuden hallinnasta, johon sisältyy tiedonhallinta, systeemiteoria, organisaation kolme päätöksentekotasoa ja liiketoimintatiedonhallinta.



KUVIO 7 Kyberturvallisuuden hallintamalli (Tisdale, 2015, muokattu)

Kuviossa vasemmalla näkyy tiedonhallinnan osuus ja oikealla näkyy systeemiteoriaan sisältyvät tekijät. Näihin molempiin sisältyy organisaation kolme päätöksentekotasoa. Alkuperäisessä mallissa puhuttiin päätöksentekotasojen sijasta kompleksisuus teoriasta, mutta siinäkin esiintyy kolme tasoa. Nämä kaikki kuuluvat organisaation liiketoimintatiedonhallintaan ja tästä kokonaisuudesta muodostuu kyberturvallisuuden hallinta.

Tietojen hallitsemiseksi johtajien on toimittava oikeaan aikaan, asianmukaisella tiedolla ja asianmukaisilla resursseilla. Jokainen kerros pitää toiset kerrokset informoituina ja milloin tahansa yhdestä organisaation päätöksentekotasosta voi tulla liikkeellepaneva voima. Esimerkiksi tietoturvaloukkaus voi johtaa siihen, että operatiiviset näkökohdat ovat etusijalla ja päivittäiset tehtävät jätetään hetkellisesti sivummalle. Strategisissa päätöksissä voidaan ohjata toiminta kriittisen

haavoittuvuuden korjaamiseen riippumatta kustannuksista tai aikatauluista. (Tisdale, 2015)

Wang & Wang (2019) ehdottavat, että yritysten kyberturvallisuuden tiedonhallinnalla on erikoistunut organisaatiorakenne. Toisin kuin perinteisessä tiedonhallintamallissa, yritysten kyberturvallisuuden tiedonhallinnassa on perustettava erikoistuneita tiedonhallintaryhmiä, jotka jakavat tietoa ulkopuolisten organisaatioiden kanssa organisaation rajojen yli. Toiseksi yritysten kyberturvallisuuden tiedonhallinnalliset tietovirrat korostavat spesifiä, selittävää ja eksplisiittistä tietoa. Kolmanneksi kyberturvallisuudessa tiedonhallinnalla on selkeät arviointitoimenpiteet, joiden avulla tiedonhallinnan tuloksia mitataan kyberturvallisuuden suorituskykymittareiden kehityksen ja soveltamisen osalta organisaatiossa. (Wang & Wang, 2019)

4 Tutkimusmenetelmä ja aineiston analyysi

Tutkimus toteutettiin tapaustutkimuksena. Tapaustutkimus soveltuu hyvin tilanteisiin, joissa tutkitaan ilmiötä sen luonnollisessa ympäristössä (Hunter, 2004; Metsämuuronen, 2008 s.14). Empiirinen data hankittiin puoliksi rakenteellisilla haastatteluilla.

Tutkittava organisaation on keskisuuri kriittisen infrastruktuurin parissa toimiva organisaatio. Organisaation kyberturvallisuuden ja haastateltavien anonymiteetin turvaamiseksi tarkemmat yksityiskohdat organisaatiosta on pidetty salassa. Salassapidon vaikutus tutkimukseen on kuitenkin minimaalinen, sillä tutkimuksen kannalta oleelliset tiedot saatiin esiin ilman organisaation nimeämistä.

Organisaatiosta on oleellista tietää tämän tutkimuksen kontekstissa tietoturvaorganisaation rakennekaavio, joka esitellään myöhemmin. Muita olennaisia ominaisuuksia ovat, että organisaatio on keskisuuri. Lisäksi on huomioitava se, että organisaatiossa on muutamia eri organisaatioyksiköitä, jotka toimivat eri alueiden parissa.

4.1 Luotettavuuden arviointi

Hirsijärven, Remeksen ja Sajavaaran (2009) mukaan kaiken tutkimuksen luotettavuutta on arvioitava, vaikka tapaustutkimuksen arviointi voikin olla haastavaa (Hirsijärvi ym. 2009 s. 232). Tutkimuksen luotettavuutta pyrittiin vahvistamaan kuvaamalla suoritetut vaiheet riittävällä tarkkuudella. Hirsijärvi ym. (2009) painottavat, että laadullisen tutkimuksen luotettavuus paranee, kun tutkija selostaa tarkasti tutkimuksen kaikki vaiheet. Näin ollen lukija pystyy arvioimaan käytettyjä menetelmiä. Kuten aikaisemmin mainittiin, tutkimus toteutettiin tapaustutkimuksena, jolla on omat haasteensa luotettavuuden kanssa. Tutkittavia kohteita oli tässä tutkimuksessa vain yksi, joten yksistään tämä on tekijä, joka heikentää luotettavuutta ja etenkin toistettavuutta.

Toistettavuuden osalta on todettava, että tämän tutkimuksen tulokset liittyvät vahvasti kontekstiin, jossa tutkimus on toteutettu, eli organisaation toimintaympäristöön. Toistettavuutta ei välttämättä ainakaan matalalla tasolla ole saavutettavissa eri organisaatioissa. Tämä tulisi ottaa huomioon tulevissa tutkimuksissa.

Yksi luotettavuutta heikentävä tekijä oli otannan rajallisuus. Kaikista hallintorakenteen keskeisistä rooleista ei saatu haastateltavia tähän tutkimukseen, joten tämä on voinut vaikuttaa tutkimuksen tuloksiin. Haastateltavista puuttui edustus johtoryhmän ja tietohallintopäällikön osalta.

Haastatteluaineiston lisäksi tässä tutkimuksessa on käytössää dokumentteja, joten tutkimuksessa oli käytössä triangulaatiota. Kun aineisto koostuu kahdesta tai useammasta lähteestä voidaan puhua aineistotriangulaatiosta

(Hirsijärvi ym. 2009 s. 233). Tutkittavat organisaation tietoturvaorganisaation rakennekaavio oli yksi osa tutkimuksen aineistoa. Triangulaatio tarkoittaa esimerkiksi useamman eri tutkimusmetodin tai datalähteen käyttämistä yhdessä tutkimuksessa. Tässä tutkimuksessa käytettiin yhtä metodia, mutta aineiston lähteinä käytettiin haastattelujen lisäksi edellä mainittua dokumenttia. Tutkimukset, jotka käyttävät vain yhtä menetelmää, ovat haavoittuvampia virheille, jotka liittyvät kyseiseen menetelmään (esim. johdattelevat haastattelukysymykset, puolueelliset tai epätodelliset vastaukset) kuin tutkimukset, joissa käytetään useita menetelmiä, joissa erityyppiset tiedot varmistavat tietojen pätevyyden (Patton, 1999).

Tässä tutkimuksessa rakennekaavion mukaan ottamisen pääasiallinen tavoite oli laittaa haastateltavien roolit tietoturvaorganisaation rakenteen kontekstiin, sekä mahdollistaa rakenteen analysoiminen tämän dokumentin kautta, mutta näiden tavoitteiden lisäksi tämä toimenpide lisäsi tutkimuksen luotettavuutta hieman. Rakennekaavio on esitelty tarkemmin tulosten yhteydessä.

4.2 Aineiston kerääminen

Tutkimuksen empiirinen aineisto kerättiin puoliksi rakenteellisilla haastatteluilla. Puoliksi rakenteellinen haastattelu antaa hyvän tasapainon vastausten vapaudelle ja aiheessa pysymiselle (Noor, 2008). Puoliksi rakenteellinen haastattelu mahdollisti kysymyslistan ulkopuolisten kysymysten kysymisen haastattelutilanteen aikana, joka mahdollisti erilaisten kiinnostavien kommenttien seuraamisen haastattelun aikana. Metsämuurosen (2008) mukaan puoliksi rakenteellista haastattelua voidaan kutsua myös teemahaastatteluksi (Metsämuuronen, 2008 s. 41).

Haastattelut toteutettiin 2020 joulukuun ja 2021 tammikuun aikana. COVID-19 epidemian takia haastattelut päätettiin pitää etänä turvallisuus syistä. Kaikki haastattelut järjestettiin Microsoft Teams-sovelluksessa. Haastattelujen aikana ei käytetty videota vaan haastattelijan ja haastateltavan välillä oli käytössä pelkkä ääniyhteys.

Yksi haaste haastatteluissa oli salassa pidettävän materiaalin julkituleminen. Yksi haastattelututkimuksen ominaispiirteistä on luottamuksellisuus (Metsämuuronen, 2008 s. 39). Luottamus ja salassapito pyrittiin turvaamaan haastattelujen aikana kahdella tavalla. Ensinnäkin haastattelijoille mainittiin, että haastattelut ovat julkisia (vaikka ovatkin anonyymejä), toiseksi litteroidut haastattelut käytäisiin läpi ja salassapidon alainen materiaali poistettaisiin. Näillä toimenpiteillä haastattelut saatiin toteutettua niin, että haastateltavien ja heidän mainitsemien henkilöiden anonymiteetti säilyi. Näiden toimien lisäksi haastattelujen tallenteen säilytettiin turvallisessa sijainnissa, missä riski haastattelujen vuotamisesta ulkopuolisten käsiin oli minimoitu.

Ennen haastattelun aloittamista haastateltaville kerrottiin, että haastattelu tullaan nauhoittamaan Microsoft Teamssin nauhoitus ominaisuuden avulla. Tämän lisäksi haastateltaville kerrottiin, että haastattelut pro gradu tutkimuksiin

liittyen ovat julkisia ja kaikkea salassapidon alaista asiaa tulisi välttää. Tämän jälkeen mainittiin, että organisaation edustaja tulee vielä tarkastamaan haastattelujen sisällön salassapidon alaisilta asioilta, ja tällaiset asiat poistetaan analyysiin vietävistä haastatteluista. Tämän lisäksi haastateltaville kerrottiin kysymysten määrä ja haastattelun arvioitu kesto. Kun edellä mainitut asiat olivat mainittu, aloitettiin tallennus ja haastattelu.

Haastattelujen kesto oli keskiarvoltaan noin 22 minuuttia. Lyhin haastattelu kesti 13 minuuttia ja pisin noin 30 minuuttia. Haastateltavia tutkimuksessa oli kuusi eri henkilöä. Haastattelut pidettiin haastateltaville sopivina aikoina 08:00 ja 16:00 välillä arkipäivinä.

Henkilöt toimivat eri tehtävissä eri puolella organisaatiota. Kaikki heistä kuului tietoturvaorganisaatioon ja heidät valittiin eri puolelta tietoturvaorganisaation osia. Haastatteluihin valittiin henkilöitä kaikilta kolmelta organisaation päätöksentekotasolta. Kybermaailman viidestä tasosta oli myös kaikki edustettuna, sillä osa haastateltavien tehtävistä ulottui fyysiselle kerrokselle asti. Lopullisen haastateltavien valinnan toteutti yrityksen edustaja, joka toimi keskeisessä roolissa tietoturvaorganisaatiossa. Haastatteluihin osallistuminen oli kuitenkin vapaaehtoista. Kaikista tietoturvaorganisaation osista ei saatu haastatteluihin haastateltavia. Johtoryhmän ja tietohallintopäällikön edustus jäi tästä tutkimuksesta puuttumaan. Yksi haastateltavista teki kuitenkin läheistä yhteistyötä johtoryhmän kanssa ja täten pystyi osittain paikkaamaan tätä puutetta.

Haastatteluihin osallistui kuusi henkilöä. Tyypillisesti teemahaastatteluissa haastateltavien määrä on pieni (Metsämuuronen, 2008 s.41). Kaksi näistä henkilöistä toimi teknisen asiantuntujan tehtävässä eri organisaatioyksiköissä. Yksi haastateltavista toimi järjestelmäasiantuntia tehtävänimikkeellä. Järjestelmäasiantuntijan tehtävä oli vahvasti tietoturvaan liittyvä, mutta kahden muun tehtävät eivät olleet päätoimisesti tietoturvaan liittyviä, vaan muita teknisiä tehtäviä. Neljäs haastateltava oli IT-päällikkö. IT-päällikön tehtävänkuvaus oli osittain hallinnollinen ja osittain tekninen. Viides haastateltava toimi tietoturva-asiantuntijan roolissa, joka keskittyi hallinnolliseen puoleen. Viimeinen haastateltava oli tietoturvapäällikkö, jonka vastuualueella oli hallinnollinen kyberturvallisuus. Haastateltavissa oli siis jako hallinnollisiin tehtäviin ja teknisiin tehtäviin. IT-päällikkö oli haastattelujen perusteella sekä teknisessä, että hallinnollisessa roolissa organisaatiossa.

Haastattelukysymykset valittiin sen mukaan, että saataisiin avoimia vastauksia tutkimuskysymysten aihepiireihin. Haastattelukysymyksiä oli 12 kolmessa eri teemassa. Teemat kysymyksiin muodostuivat tutkimuskysymysten kautta. Jokaisessa teemassa oli neljä kysymystä. Teemat ja kysymyksen on nähtävissä liitteessä 1. Haastattelujen aikana kysyttiin myös kysymyksiä haastattelurungon ulkopuolelta. Haastattelujen aikana tuli esiin monia eri kommentteja, joita seurattiin jatkokysymyksillä. Haastattelija saattoi kysyä käytännön esimerkkiä tietyistä tilanteista, mitä haastateltavat mainitsivat. Näin pyrittiin tarkentamaan ja ymmärtämään vastauksia ja niiden kontekstia paremmin. Kysymys rungon ulkopuolelta kysytyissä kysymyksissä pyrittiin ottamaan huomioon

johdattelematon sävy, mutta jatkokysymysten kysyminen väkisin ohjaa haastattelua tiettyyn suuntaan, joten tämä ei täysin toteutunut haastatteluissa.

4.2.1 Litterointi

Haastattelunauhoitukset litteroitiin tekstiksi kokonaisuudessaan. Hirsijärven ym. (2009) mukaan litterointi on tyypillisesti tarkoituksen mukaista. Litteroinnin tarkkuudesta ei ole yksiselitteistä ohjetta, mutta tutkimuksen analyysi metodi, aineisto ja käytettävät työkalut vaikuttavat siihen (Hirsijärvi ym., 2009 s. 222). Litteroinnin tarkkuus pidettiin tässä tutkimuksessa, sillä tasolla, että haastateltavien sanomat asiat eivät vääristyneet. Sanojen toistot, naurahdukset ja muut vastaavat poistettiin osittain ensimmäisestä litterointiversiosta, sillä näiden analysoimisessa ei nähty lisäarvoa tämän tutkimuksen kontekstissa. Tavoitteena tässä tutkimuksessa ei ole selvittää miten jokin asia on sanottu vaan tärkeämpää on keskittyä sisältöön. Litteroinnit käytiin läpi vielä toiseen kertaan ensimmäisen kirjauksen jälkeen kirjoitus- ja muiden virheiden varalta. Seuraavassa vaiheessa aineistosta poistettiin salassapidonalaisia asioita, kuten yritysten nimiä, henkilöiden nimiä, järjestelmien nimiä ja muuta, mikä saattaisi vaarantaa tutkittavan organisaation kyberturvallisuutta. Näillä toimenpiteillä haastatteluaineisto saatiin muotoon, jossa sitä voitiin alkaa analysoimaan vapaasti.

4.2.2 Koodaus

Koodaus työkaluna käytettiin Altlasti pilvi versiota, joka on laadullisen datan analysointi työkalu. Työkalun pääasiallinen tehtävä oli koodauksen helpottaminen. Atlasti mahdollistaa koodien, viittauksien ja koodiryhmien hallinnan sovelluksen kautta ja tämä helpottaa tukijan työtä, sekä vähentää manuaalisen tavan aiheuttamia virheitä. Koodaus tehtiin kuitenkin sovelluksessa käsin, eikä automaattikoodausominaisuuksia käytetty, sillä tämä voi mahdollisesti johtaa erilaisiin virheisiin koodausprosessissa.

Koodausvaihe tutkimuksesta alkoi jo osittain haastattelujen aikana, sillä jo siinä vaiheessa alettiin vertaamaan haastattelun sisältöä ja kirjallisuuskatsauksen teorioita toisiinsa. Tämä on tyypillistä laadullisessa tutkimuksessa, että aineiston keruu ja analyysi tapahtuvat päällekkäin (Metsämuuronen, 2008 s. 48). Lisäksi tässä vaiheessa muodostui jo jotain hahmotelmia siitä, mitä koodeiksi mahdollisesti muodostuu. Haastattelujen aikana tehdyt muistiinpanot ja mahdolliset koodit olivat kuitenkin vasta hahmotelmia ja eivät kovin kattavia. Tästä saatiin kuitenkin hyvä pohja haastatteluaineistoon tutustumiseen, jonka kautta varsinainen koodaus pystyttiin aloittamaan hieman sujuvammin.

Koodausprosessi aloitettiin käymällä kaikki haastattelut läpi systemaattisesti ja samalla etsittiin niistä koodeja, joita voi pitää tämän tutkimuksen kontekstissa merkittävänä. Keskiarvoltaan yhdessä haastattelussa oli 45 viittausta, jotka merkattiin koodeilla. Yhdessä haastattelussa oli keskimäärin 33 uniikkia koodia. Ensimmäisen koodauksen päätteeksi kuudesta haastattelusta ilmeni yhteensä 116 uniikkia koodia ja viittauksia haastatteluissa oli yhteensä 268.

Ensimmäisellä koodauskerralla pyrittiin löytämään eri teemoja, kokonaisuuksia ja kategorioita datasta, mutta tässä vaiheessa pääpaino oli kuitenkin tutustua aineistoon ja alkaa hahmottelemaan sieltä esiin nousevia kokonaisuuksia. Ensimmäisen koodauskerran jälkeen koodit käytiin läpi ja niistä etsittiin erilaisia yhteneväisyyksiä toisten koodien kanssa ja hahmoteltiin alustavia kategorioita. Tämän jälkeen, kun merkittävimmän koodit ja kategoriat oli kirjattu ylös, aloitettiin toinen koodauskierros, aikaisemmat koodit ja kategoriat mielessä.

Toinen koodauskierros alkoi kuitenkin lähes tyhjältä pöydältä, sillä vielä tässä vaiheessa ei haluttu sitoutua ensimmäisen vaiheen koodeihin ja kategorioihin liikaa, eli jos uusia koodeja tai kategorioita nousi esiin, niin ne lisättiin dataanalyysi sovellukseen. Ensimmäinen kierros siis ohjasi toisen kierroksen koodausta. Näin päästin vähemmän hajanaiseen lopputulokseen, mutta saatiin kuitenkin uusia koodeja ja huomioita datasta esiin.

Toisen koodauskierroksen jälkeen kokonaisuudessa koodeja tuli 140 jotka viittasivat 316 eri viittaukseen haastatteluaineistossa. Koodien ja viittausten määrä siis hieman lisääntyi toisen koodauskierroksen aikana. Toinen koodauskierros oli viimeinen, jossa lähdettiin lähes tyhjältä alustalta tarkastelemaan aineistoa. Toisen kierroksen jälkeen tehdyt iteroinnin pohjautuivat toisen koodauskierroksen koodeihin.

Kolmas iteraatio oli rakentaa edellisessä vaiheesta tulleista koodeista kategorioita, joiden avulla saatiin datasta poimittua siinä muodostuvia teemoja esiin tehokkaammin. Eri kategorioita muodostui tässä vaiheessa 25. Eri koodit sijoiteltiin näihin kategorioihin ja näitä kategorioita alettiin muokkaamaan, joko yhdistämällä tai jakamalla niitä.

Tässä vaiheessa myös koodien päällekkäisyyttä pyrittiin poistamaan. Moni koodauksen aikana esiin noussut koodi voitiin yhdistää johonkin toiseen koodiin, joiden merkitys oli lähellä toisiaan ja koodien pitäminen erillään ei tuonut dataanalyysiin lisäarvoa. Liikkeelle lähdettiin 140 koodilla ja koodien yhdistämisellä, poistamisella ja muutaman uuden lisäämisellä lopputuloksena oli 120 koodia, jotka liittyivät 327 viittaukseen. Viittausten määrä siis hieman kasvoi, mutta koodien määrä väheni.

4.2.3 Teemat

Tässä alaluvussa tarkastellaan, miten koodeista muodostui teemoja. Selkeyden vuoksi pienempiä teemoja kutsutaan kategorioiksi. Isommat kokonaisuudet, jotka muodostuvat näistä kategorioista ovat teemoja.

Haastatteluaineistosta löytyi yhteensä 24 eri kategoriaa. Kategoriat löytyivät yhdistämällä samaa aihealuetta käsitteleviä koodeja toisiinsa. Tämä oli iteratiivinen ja syklinen prosessi, joka käytiin läpi useaan kertaan. Tämä on tyypillinen toimintatapa aineiston analyysissä (Hirsijärvi ym., 2009 s. 224). Tarkkaa iteraatioiden määrää on vaikea sanoa, sillä tähän prosessiin palattiin aina tarvittaessa tekemään pieniä muutoksia. Koodeja siirrettiin kategorioista toisiin ja kategorioita nimettiin uudelleen, poistettiin ja lisättiin tarpeen mukaan. Näin päädyttiin lopullisiin kategorioihin, jotka parhaiten edustivat datassa olevia koodeja.

Haastatteluaineistosta löytyi yhteensä 24 eri kategoriaa. Kategorioiden sisällä olevien koodien määrä vaihteli paljon. Kategoriat olivat seuraavat:

- Yhteistyö ulkoinen
- Yhteistyö sisäinen
- Tiedonvälitystavat
- Tietoturvan kehittäminen
- Yhteistyö sisäinen
- Tilannekuvan kommunikointi
- Tilannekuvan tuottaminen
- Tietoturvan toteutumisen valvominen
- Tiedonhallinnan haasteet
- Koulutuksen järjestäminen
- Koulutus tarpeet
- Johtoryhmän toiminta
- Osallistaminen
- Hallintorakenteen vaikutuksia
- Toimintaroolit
- Toiveet
- Kontrollitieto
- Haasteet
- Viestintä
- Toiminnan ohjaaminen
- Tilannekuvan taso
- Toimivat asiat
- Muut
- Tietoturvan ylläpito
- Toimintatavat

Kategorioiden sisällä olevien koodien ja sitaattien määrä vaihteli paljon. Esimerkiksi hallintorakenteen merkityksiä, koodin alla oli 11 eri koodia ja kontrollitieto kategorian alla oli vain kaksi, eli mitään tasapainoa kategorian koodien esiintymisellä ei ollut.

Koodit, joita ei saatu sovitettua mihinkään kategoriaan lisättiin muut kategorian alle. Nämä irralliset koodit säilytettiin kuitenkin tässä vaiheessa, sillä tarkemman analyysin aikana niistä saattaisi löytyä jotain tutkimuskysymysten kannalta relevanttia tietoa. Muut kategoriaan oli 10 viittausta muutamasta koodista. Jälkeenpäin voidaan todeta, että tästä kategoriasta ei noussut tuloksissa esiin mitään mielenkiintoista ja niitä ei otettu huomioon seuraavaksi käsiteltävissä teemoissa.

Kun kategoriat oli saatu hahmoteltua, alettiin niistä muodostamaan vielä korkeatasoisempia teemoja. Tässä vaiheessa pyrittiin yhdistämään kategoriat aina yhden teeman alle. Alustavat teemat löytyivät kategorioista helposti, sillä näitä oli jo aikaisempien vaiheiden aikana alustavasti hahmoteltu. Teemojen muodostuminen oli myös iteratiivinen prosessi. Teemat muodostuivat

kategorioista melko vaivattomasti. Tässä vaiheessa saatiin nopeasti teemat kasattua kategorioista ja muutoksia ensimmäiseen versioon ei juuri tarvinnut tehdä. Alla esitetyssä taulukossa on listattu teemat vasemmalle ja teeman alle asettuvat kategoriat oikealle.

TAULUKKO 1 Haastatteluista löydetyt teemat

Teema	**Kategoria**
Yhteistyö	Yhteistyö ulkoinen Yhteistyö sisäinen
Koulutus	Koulutuksen järjestäminen Koulutus tarpeet
Tilannekuva	Tilannekuvan kommunikointi Tilannekuvan tuottaminen Tilannekuvan taso
Viestintä ja tiedonvälitystavat	Tiedonvälitystavat Viestintä Tiedonhallinnan haasteet
Tietoturvan ylläpito ja kehitys	Tietoturvan kehittäminen Tietoturvan toteutumisen valvominen Tietoturvan ylläpito
Kehityskohteet ja toimivat asiat	Haasteet Toiveet Toimivat asiat
Ohjaus kontrolli	Kontrollitieto Toiminnan ohjaaminen Toimintatavat
Rakenteen vaikutukset	Johtoryhmän toiminta Hallintorakenteen vaikutuksia Osallistaminen Toimintaroolit

Teemoja löytyi haastatteluista kahdeksan. Taulukosta voidaan nähdä, että teemoissa on päällekkäisyyttä. Esimerkiksi tilannekuvan kommunikointi voitaisiin hyvin asettaa viestintä ja tiedonvälitystavat teeman alle. Tässä kuitenkin päädyttiin siihen, että tilannekuvan tuottaminen käsitellään omana teemanaan, jotta data edustaa paremmin haastatteluja ja pystyy vastaamaan tutkimuskysymyksiin tehokkaammin.

Nämä kahdeksan teemaa olivat haastatteluissa edustettuina eri painoilla. Seuraavassa taulukossa esitetään, että kuinka monta viittausta kuhunkin teemaan liittyy ja kuinka monta uniikkia koodia kyseiseen teemaan kuului.

TAULUKKO 2 Viittausten ja koodien määrä teemoissa

TEEMA	Viittaukset	Koodit
Yhteistyö	30	8
Koulutus	13	5
Tilannekuva	61	13
Viestintä ja tiedonvälitystavat	58	22
Tietoturvan ylläpito ja kehitys	38	13
Kehityskohteet ja toimivat asiat	42	16
Ohjaus kontrolli	30	10
Rakenteen vaikutukset	90	28

4.3 Temaattinen analyysi

Hirsijärven ym. (2009) mukaan tutkimuksen tulosten analysointi voidaan toteuttaa karkeasti kahdella tavalla, selittävällä ja ymmärtävällä tavalla. Ymmärtävä tapa on tyypillistä laadullisissa tutkimuksissa ja siitä syystä tässä tutkimuksessa on käytetty selittävää analyysimetodia, eli temaattista analyysiä. Braunin ja Clarken (2006) mukaan temaattiseen analyysiin sisältyy kuusi vaihetta:

1. dataan tutustuminen
2. alustavien koodien luominen
3. teemojen etsintä
4. teemojen arviointi
5. teemojen määrittely ja nimeäminen
6. raportin kirjoittaminen

Dataan tutustumisvaiheessa tutkijan tavoitteena on tutustua aineistoon tarkemmin ja luoda alustavia ideoita eri koodeista ja teemoista. Tutustuminen voi tapahtua lukemalla tai kuuntelemalla haastatteludataa tai litteroidessa. Toinen vaihe on alustavien koodien luominen. Etsitään aineistosta mielenkiintoisia huomioita ja koodataan ne systemaattisesti koko aineiston sisällöstä. Kolmannessa vaiheessa etsitään alustavat teemat. Edellisen vaiheen tuottamien koodien avulla niistä aletaan etsiä esiin nousevia teemoja. Neljäs vaihe on teemojen arviointi. Tässä tavoitteena on tarkastaa toimivatko teemat koodi tasolla ja koko aineiston tasolla. Viides vaihe on teemojen määrittely ja nimeäminen. Tässä määritellään teemat tarkasti ja nimetään ne määritelmien mukaan mahdollisimman edustaviksi. Viimeinen vaihe tässä prosessissa on raportin kirjoittaminen, mikä on viimeinen mahdollisuus toteuttaa analyysiä. (Braun & Clarke, 2006).

5 Tulokset

Tässä vaiheessa tutkimusta siirrytään tulosten analysointiin. Edellisessä vaiheessa selitettiin, miten haastatteluaineistosta saatiin selville eri koodit, joista muodostui kategorioita ja lopulta teemoja. Tässä vaiheessa tavoitteena on käyttää edellisessä vaiheessa kuvattujen prosessien tuottamaa materiaalia empiiristen tulosten analysoimiseen korkeammalla tasolla.

Tämän luvun tarkoituksena on esittää tutkimuksen empiiriset löydöt. Suuri osa tämän luvun löydöistä syntyy suoraan empiirisestä tutkimusmateriaalista, eli osallistujien haastatteluista. Nämä ovat joko yksittäisen haastateltavan vastauksia tai yhdistelmiä useista vastauksista. Jotkut oivallukset ovat kuitenkin epäsuorempia ja syntyvät tutkijan käsityksistä. Nämä oivallukset perustuvat koko tutkimuksen kontekstiin, josta voidaan tehdä päätelmiä yhdistämällä tutkimuksen teoria- ja empiriaosuuksia toisiinsa. Empiriasta on siis osittain luotu epäsuoria päätelmiä, joiden tavoitteena on avata datan merkityksellisyyttä.

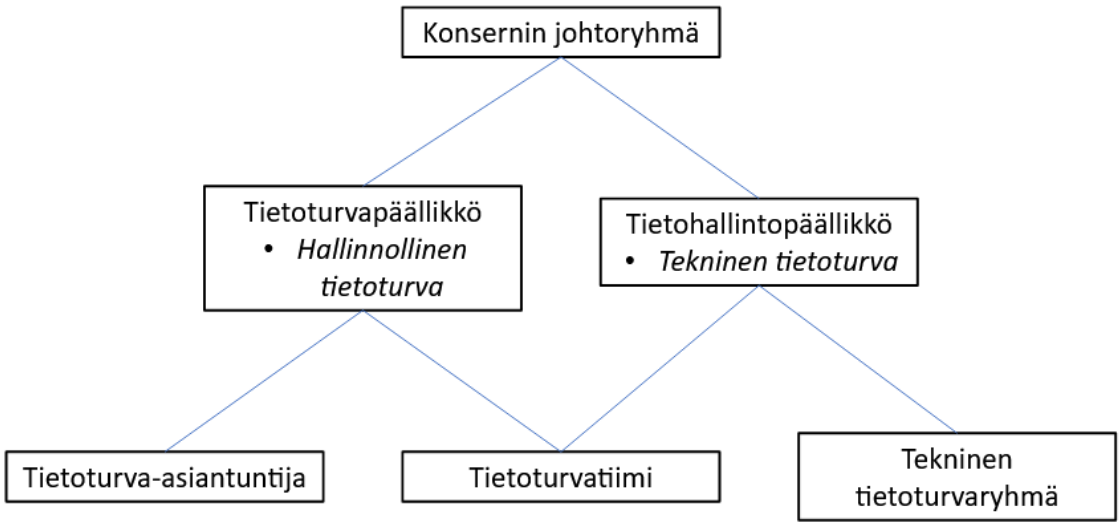
Tutkimuksen pääasiallisena tavoitteena oli tarkastella hallintorakenteen toimivuutta. Haastateltavien roolit olivat jaettavissa teknisiin ja hallinnollisiin tehtäviin, joten tulosten tulkinnassa otettiin käyttöön näkökulma hallinnollisten ja teknisten tehtävien välillä. Täysin teknisiä tehtäviä oli haastateltavissa kuudesta kolme ja täysin hallinnollisia kaksi. Yksi haastateltavista asettui molempiin, tekniseen sekä hallinnolliseen tehtävään. Tästä saadaan lopputulokseksi neljä teknistä tehtävää ja kolme hallinnollista, sillä yksi tehtävä esiintyy molemmista. Näitä eroja tarkastellaan teemoissa, jos sieltä on löytynyt merkittäviä eroja näiden kahden välillä.

Tutkimus keskittyy pääosin kybermaailman tasorakenteen kognitiiviselle tasolle (ks. KUVA 1). Tavoitteen mukaisesti keskityttiin siis ihmisten toimintaan teknologian ympäröimässä kontekstissa.

Tässä luvussa käsitellään löydöt teemakohtaisesti. Yhden teeman löydöt käsitellään omassa alaluvussaan ja osittainen päällekkäisyys teemoissa otetaan huomioon jokaisessa alaluvussa tarvittaessa. Yksittäisiin koodeihin pureudutaan tuloksissa tarvittaessa. Tavoitteena tulosten analysoinnissa on pysyä teema ja kategoria tasolla, sillä koodattu data sisältää paljon yksittäisiä koodeja, joiden esiintyvyys datassa on vähäistä, niin kategorioilla saadaan nämäkin koodit mukaan tulosten analysoimiseen. Tämän pääluvun ensimmäinen alaluku käsittelee organisaation tietoturvaorganisaation hallintorakennekaaviota, jossa käydään eri hallintorakenteen osat läpi. Tämän jälkeen tarkastellaan haastatteludatan teemoja ja viimeisenä verrataan rakennekaaviota haastatteludatasta löytyneisiin huomioihin ja analysoidaan rakennekaaviota uudelleen haastatteludatan löytöjen valossa.

5.1 Rakennekaavio

Kuviossa 8 on esitetty organisaation tarjoama dokumentti tietoturvaorganisaation rakenteesta. Tässä vaiheessa on tämän tutkimuksen kyberturvallisuuden ja tietoturvallisuuden määritelmiin vedoten (ks. luku 2.1) on todettava, että tutkittavan organisaation tietoturvaorganisaatio on todellisuudessa lähempänä kyberturvallisuusorganisaatiota. Sama voidaan todeta myös tiimeistä ja tehtävänimikkeistä, että niihin sopisi tämän tutkimuksen kontekstissa paremmin kyber-etuliite. Tuloksissa käytetään kuitenkin alkuperäisiä nimiä, mitä organisaatiossa on määritetty näihin tehtäviin.



KUVIO 8 Tietoturvaorganisaation hallintorakennekaavio

Konsernin johtoryhmä toimii tietoturvallisuuden ohjausryhmänä. Tietoturvapäällikön vastuulla on hallinnollinen kyberturvallisuus. Tietohallintopäällikkö vetää tietohallintoa ja hänen vastuualueisiinsa kuuluu kyberturvallisuuden osalta tekniset asiat. Nämä tehtävät ovat organisaatiossa samalla tasolla, ja tässä tulee esiin jako hallinnollisen ja teknisen kyberturvallisuuden välillä.

Tekninen tietoturvaryhmä, joka on eri organisaatioyksiköiden operatiivisista asiantuntijoista koostuva kyberasioiden tiedonvaihtoryhmä, joka kokoontuu noin kerran kvartaalissa. Teknisen tietoturvaryhmän jäsenet tehtävänimiketasolla:

- tietohallintopäällikkö
- tietoturvapäällikkö
- tietoturva-asiantuntija
- IT-päällikkö
- järjestelmäasiantuntija x 2
- ICT-asiantuntija
- tietojärjestelmäasiantuntija

- tekninen asiantuntija x 6

Tietoturvatiimi on kyberturvallisuuden kannalta keskeisimpien henkilöiden muodostama virtuaalitiimi. Tietoturvatiimi kokoontuu kahdella eri tavalla. Ensimmäinen on tietoturvan kuukausipalaverit. Toinen on IT-haavoittuvuuksien läpikäyntipalaverit joka toinen viikko. Tietoturvatiimin jäsenet tehtävänimiketasolla:

- tietoturvapäällikkö
- tietoturva-asiantuntija
- tietohallintopäällikkö
- IT-päällikkö
- järjestelmäasiantuntija
- *järjestelmäasiantuntija*
- ICT-asiantuntija
- *tietoarkkitehti*

Tietoturvan kuukausipalavereissa ja IT-haavoittuvuuksien läpikäyntipalavereissa ei ole täysin sama kokoonpano. Tietoturvan kuukausipalavereihin osallistuvat tietoturvatiimin ei-kursivoidut jäsenet ja IT-haavoittuvuuksien läpikäyntipalaveriin osallistuvat kaikki tietoturvatiimin jäsenet, mutta kaikki eivät osallistu joka kerta.

5.2 Yhteistyö

Yhteistyö teemassa oli havaittavissa useita mielenkiintoisia huomioita. Ensimmäinen ja yksi suurimmista huomioista oli, että ulkoinen yhteistyö nousi esiin useassa eri haastatteluissa eri tavoilla. Haastattelu rungossa ei kysytty mitään ulkoisesta yhteistyöstä, mutta haastateltavat nostivat ulkoisen yhteistyön asioita silti useasti esiin. Muutamassa haastattelussa haastateltavat kysyivät, että voivatko mainita ulkoisia yhteistyö asioita ja haastattelija rohkaisi heitä kertomaan myös näistä.

Vaikka tämän tutkimuksen pääasiallinen tavoite onkin tutkia organisaation sisäistä kyberhallintorakennetta, on tärkeää ottaa huomioon nämä ulkoiset yhteistyö elementit, jotka vaikuttavat myös sisäiseen toimintaan eri tavoilla. Tisdalen (2015) mukaan organisaatio tulisi nähdä avoimena systeeminä kyberturvallisuuden kontekstissa. Avoimeen systeemiin liittyy siis myös ulkoiset tekijät.

Yhteistyötä tehtiin muun muassa muiden alan toimijoiden, viranomaisten ja laitetoimittajien kanssa. Yksi keskeinen yhteistyön tapa mikä nousi esiin, oli tilannekuvan hankkiminen ulkoisen yhteistyönkautta. Tätä tarkastellaan tarkemmin tilannekuvaan liittyvässä alaluvussa.

Sisäinen yhteistyö nousi esiin jokaisessa haastattelussa, mikä oli oletettavaa. Ulkoinen yhteistyö oli mainittu kaikissa paitsi yhdessä teknisen asiantuntijan

haastattelussa. Ulkoista yhteistyötä tapahtuu siis monilla eri organisaation tasoilla. Alla olevassa taulukossa on listattuna kategorioiden esiintymisen jako hallinnollisen- ja teknisen tehtävien välillä.

TAULUKKO 3 Yhteistyö teeman koodien jakautuminen

Kategoria	Hallinnollinen tehtävä	Tekninen tehtävä
Yhteistyö sisäinen	12	7
Yhteistyö ulkoinen	10	9

Tästä huomataan, että hallinnon puolen tehtävissä käydään hieman enemmän yhteistyötä, sekä sisäisesti, että ulkoisesti. Hallinnollisissa tehtävissä toimivat henkilöt kuuluivat myös useampaan hallintorakenteen osaan samanaikaisesti, joten tämä selittää osittain isomman yhteistyö määrän. Hallinnollisia tehtäviä oli kolmella haastateltavalla ja teknisiä neljällä, joten tämä on myös syytä ottaa huomioon näiden lukujen tulkinnassa.

Kuten tutkimuksen kirjallisuuskatsauksessa aikaisemmin mainittiin, että yritysten kyberturvallisuuden tiedonhallinnalla on erikoistunut organisaatiorakenne. Toisin kuin perinteisessä tiedonhallintamallissa, yritysten kyberturvallisuuden tiedonhallinnassa on perustettava erikoistuneita tiedonhallintaryhmiä, jotka jakavat tietoa ulkopuolisten organisaatioiden kanssa organisaation rajojen yli. (Wang & Wang, 2019)

Tämä on havaittavissa myös tämän tutkimuksen haastatteludatasta. Tiedonjako tapahtuu ulkopuolisten organisaatioiden kanssa ainakin yksilötasolla. Sisäisiä tiedonjakoryhmiä on organisaatiossa useampia ja haastatteluista ilmenee, että yksilöt tekevät yhteistyötä ulkoisten toimijoiden kanssa aina tarpeen mukaan. Varsinaisia tiedonhallintaryhmiä, jotka keskittyvät ulkopuoliseen tiedonjakoon ei suoraan voitu haastatteluista kuitenkaan havaita.

Organisaatiossa on paljon eri tiedonvaihtoryhmiä, jotka näkyvät kyberturvallisuuden hallintorakenteessakin. Yhteenvetona tässä vaiheessa organisaation kyberturvallisuuden yhteistyötoimista voidaan sanoa, että sisäisen yhteistyön lisäksi sitä tapahtuu huomattavasti myös organisaatiorajojen ulkopuolella muiden organisaatioiden kanssa.

5.3 Rakenteen vaikutukset

Rakenteen vaikutukset teemassa olevat koodit ja kategoriat liittyivät siihen, miten rakenne vaikuttaa toimintaan organisaatiossa. Tässä teemassa kaksi tärkeintä kategoriaa olivat osallistaminen ja hallintorakenteen vaikutukset. Lisäksi johtoryhmän toiminnasta ja toimintarooleista oli tämän teeman alla mielenkiintoisia mainintoja. Taulukossa neljä on nähtävillä, miten koodit jakautuivat hallinnollinen-/tekninen tehtävä akselilla.

TAULUKKO 4 Rakenteen vaikutukset teeman koodien jakautuminen

Kategoria	Hallinnollinen tehtävä	Tekninen tehtävä
hallintorakenteen vaikutuksia	33	21
johtoryhmän toiminta	10	3
osallistaminen	16	9
toimintaroolit	10	9

Hallintorakenteen vaikutuksia kategorialla tarkoitettiin asioita, jotka vaikuttivat haastateltavan toimintaan rakenteen kautta. Esimerkiksi eri yhteistyöryhmiin osallistuminen laskettiin tähän kategoriaan. Vaikutus näyttäisi olevan suurempi hallinnollisissa tehtävissä kuin teknisissä. Tässä on kuitenkin hyvä ottaa huomioon, että hallinnolliseen tehtävänkuvaan liittyy useampi toimintoja, jota voidaan laskea tämän kategorian alle. Tämän lisäksi hallinnollisissa rooleissa toimivat henkilöt osallistuivat useisiin eri yhteistyöryhmiin ja teknisissä tehtävissä toimivat henkilöt kuuluivat pääosin vain tekniseen tietoturvaryhmään.

Karyda, Kiountouzis & Kokolakis (2005) toteavat, että organisaatiorakenteella on tärkeä rooli turvallisuuspolitiikan onnistuneessa toteuttamisessa ja hyväksymisessä. Jäykkä hierarkkinen rakenne voi olla ongelma tietoturvan hallinnassa, koska turvallisuuspolitiikan soveltaminen vaatii usein organisaation joustavuutta, mukaan lukien uusien roolien luominen tai olemassa olevien mukauttaminen (Karyda, Kiountouzis & Kokolakis, 2005). Vaikka edellä viitattu tutkimus keskittyikin politiikan onnistumiseen, voidaan sitä pitää myös oleellisena tämän tutkimuksen kontekstissa. Tässä organisaatiossa on luotu uusia rooleja, esimerkiksi teknisen tietoturvaryhmän kautta, johon osallistuvat henkilöt ottavat uuden roolin oman päätoimisen roolin ohelle. Rakenteen joustavuuteen ei tämän haastatteludatan kannalta voida ottaa kantaa.

Johtoryhmän toiminta kirjattiin myös tämän teeman alle, sillä se voidaan ainakin osittain nähdä johtuvan rakenteesta. Tässä huomattiin, että johtoryhmän osallistuminen kyberturvallisuuden toteutukseen on kyseisessä organisaatiossa vahvaa. Tietoturvapäällikkö mainitsi haastattelussaan johtoryhmästä seuraavaa:

> ” …johtoryhmän tietoturva taso on hyvä ja ymmärtävät asian merkityksen ja sen vaikutuksen meidän liiketoiminnan jatkuvuudelle, niin on helppoa operoida johtoryhmän kanssa. Johtoryhmä, myös toimitusjohtaja ohjaa vahvasti organisaatiota tietoturvalliseen käyttäytymiseen mikä on iso juttu sitouttamisen kannalta.”

Organisaatiossa on siis ymmärretty johtoryhmän osallistumisen tärkeys ja tämä on varmasti yksi syy sille, että yrityksessä on vahva tietoturvataso. Haastatteluissa selvisi myös, että johtoryhmä on aktiivisesti selvittämässä tietoturva-asioita aina tarpeen mukaan ja johtoryhmä pidetään tilannekuvasta ajan tasalla.

Yksi huomio haastatteluista oli se, että tietoturvapäällikkö toimii solmuna johtoryhmään, eli viestintä johtoryhmään ja sieltä ulos kulkee suurelta osin tietoturvapäällikön kautta. Tietoturvapäällikön tasolla tapahtuu tiedon suodattamista johtoryhmälle sopivaksi, sillä yksityiskohtien merkityksellisyys laskee johtoryhmän tarkastellessa asiaa. Ackoffin (1989) viisaus pyramidiin (ks. KUVIO 4)

verrattuna tässä tiivistetään alempia tietotasoja ylempiin, eli johtoryhmän tarpeisiin sopivammaksi.

Karyda, Kiountouzis & Kokolakis (2005) mainitsevat, että tietoturvapäällikkö on keskeinen tekijä tietoturvapolitiikan onnistumisessa ja Tisdalen (2015) mukaan organisaatio voi hyötyä kyberturvallisuuden hallintojohtajasta, joka on taitava useilla organisaation toiminta-alueilla. Suomalaisissa kriittisen infrastruktuurin parissa työskentelevissä organisaatioissa on havaittu johtamisen haasteeksi se, että johtoryhmästä puuttuu tietoturvasta vastaava henkilö (Lehto ym. s.42–43 2017). Kyberturvallisuudesta/tietoturvasta vastaavan keskeisen henkilön merkitys on siis noussut teoriaosuudessa esiin kolmessa eri lähteessä. Haastatteludata ja rakennekaavio osoittavat, että tutkitussa organisaatiossa tämä toteutuu hyvin, sillä organisaatiossa on tietoturvapäällikkö, joka ymmärtää eri organisaation osien toimintoja tekemällä läheistä yhteistyötä heidän kanssaan. Lisäksi tietoturvapäällikön apuna on tietoturva-asiantuntija. Organisaatio on keskisuuri, joten tietoturvapäällikön vastuiden täyttäminen voi yksittäiselle henkilölle olla haastavaa. Organisaation koon takia ei välttämättä tarvita johtoryhmään erillistä tietoturvasta vastaavaa CISO edustajaa, vaan tietoturvapäällikkö voi täyttää tämän roolin, vaikka ei varsinaisesti johtoryhmään kuulukaan.

Osallistaminen oli yksi merkittävä löytö haastatteluaineistosta. Osallistaminen tuli vahvasti esiin sekä teknisten tehtävien, että hallinnollisten tehtävien haastatteluista. Veiga & Eloff (2007) totesivat, että tietoturva tulisi sisällyttää jokapäiväisiin käytäntöihin, jotka suoritetaan osana työntekijän työtä, jotta siitä tulisi elämäntapa ja siten kehitettäisiin tehokasta tietoturvakulttuuria koko organisaatiossa (Veiga & Eloff, 2007). Organisaatiossa on käytössä esimerkiksi tekninen tietoturva ryhmä, johon kuuluu eri organisaatioyksiköiden operatiivisista asiantuntijoista koostuva tietoturva-asioiden tiedonvaihtoryhmä. Suurin osa näistä henkilöistä ei työskentele tietoturvan kanssa päätoimisesti, vaan heidät on osallistettu tietoturvan toteutukseen oman päätoimisen roolin ohella.

Tutkittavassa organisaatiossa on otettu kyberturvallisuuden integrointi huomioon yhteistyöryhmien kautta. Julischin (2013) mukaan tehokkaan kyberturvallisuuden toteuttamiseksi organisaatioiden on luotava erilliset, mutta toisiinsa liittyvät hallintajärjestelmät, joita voi olla olemassa eri organisaatio tasoilla. Tämän tutkimuksen kontekstissa voidaan nähdä, että nämä yhteistyöryhmät ajavat tätä asiaa tässä organisaatiossa.

Kirjallisuuskatsauksessa todettiin, että käyttäjät voivat olla arvokas resurssi tietoturvaan tarjoamalla tarvittavaa liiketoimintatietoa, joka edistää tehokkaampia turvatoimia. Käyttäjien osallistaminen on myös keino sitouttaa käyttäjät suojaamaan arkaluonteisia tietoja liiketoimintaprosesseissa (Spears & Barki, 2010). Tekninen tietoturvaryhmä tekee juuri tätä, mitä Spears ja Barki (2010) tutkimuksessaan ehdottavat. Tutkittavalla organisaatiolla on muutamia eri organisaatioyksiköitä, joissa on omia erityispiirteitään. Näiden yksiköiden henkilöstöllä on ammattiosaaminen omasta tehtävästään, mikä kyberasiantuntijoilta puuttuu. Näiden avainhenkilöiden integrointi kyberturvallisuuden tuottamiseen on yksi tutkitun organisaation kyberrakenteen vahvuuksista.

Kyberturvallisuuteen osallistetaan siis työntekijöitä, joiden pääasiallinen tehtävä ja asiantuntijuus ei ole tietoturvassa vaan jossain muualla. Näillä toimilla organisaatio vahvistaa omaa tietoturva kulttuuriaan, kuten Veiga ja Eloff (2007) totesivat. Kulttuurin merkitys havaittiin kirjallisuudessa myös tietoturvapolitiikan kontekstissa. Karyda, Kiountouzis & Kokolakis (2005) totesivat tutkimuksessaan, että organisaatiot, joissa on työntekijöitä, jotka osallistuvat erilaisiin aktiviteetteihin ja joilla on lisääntynyt vastuullisuus, kehittävät todennäköisemmin turvallisuuskulttuuria ja luovat henkilöstölleen korkean turvallisuustietoisuuden (Karyda, Kiountouzis & Kokolakis, 2005).

Osallistaminen on huomioitu organisaatiossa myös muilla tavoilla, kuten tietoturva huomioiden arvostamisella. Tämä nousi esiin molemmissa sekä tietoturvapäällikön, että tietoturva-asiantuntijan haastatteluissa, joiden tehtävän kuvaan liittyy muun henkilöstön kouluttaminen ja tietoturvaosaamisen ylläpitäminen. Tietoturvapäällikkö toteaa haastattelussa seuraavasti:

> No jokainen työskentelee tietoturvan kanssa päivittäin, koska oma toiminta vaikuttaa olennaisesti siihen kokonaissuoriutumiseen, mutta he tietävät ohjeistukset, käytännöt ja politiikat, jotka säätelevät käyttäjän roolissa sitä tietoturvaa.

Organisaation henkilöstön osallistumista eri tietoturva asioihin arvostetaan, joka mahdollistaa tietoturvallisen kulttuurin kehityksen. Esimieskunta on myös osallistettu organisaatiossa valvomaan tietoturvakäyttäytymistä. Haastatteluissa tuli myös ilmi, että haasteena nähdään se, että ihmisten ilmoituskynnystä pidetään turhan korkeana kyberasioihin liittyen. Tietoturva-asiantuntija mainitsi haastattelussa toiveensa siitä, että ilmoituksia annettaisiin erittäin matalalla kynnyksellä kaikista tietoturvaan liittyvistä asioista.

> No ehkä vähän enemmän toivoisin vielä aktiivisuutta siellä tiketöintijärjestelmässä, että ihmiset ottaisivat sen vielä paremmin käyttöön. Toki se on ihan hyvin käytössä, mutta ilmoittaisivat siellä mahdollisimman matalalla kynnyksellä kaikista tietoturva- ja tietosuojahavainnoista ja kysyisivät sieltä lomakkeiden kautta, jos on jotain kysyttävää esim. tietosuojaan liittyen. Niin ihan rohkeasti laittaisivat sinne viestiä, et ehkä vähän semmoista uskallusta ja aktiivisuutta toivos vielä muilta työntekijöiltä, että saisivat sitten meidät kiinni silloin kun on meille asiaa, niin rohkaistuisivat käyttämään näitä tämmöisiä välineitä minkä kautta saisi sitten paremmin yhteyttä.

Myös eri roolit kirjattiin tämän teeman alle. Yksi havainto oli, että tietoturvatapahtumien varalle oli ennalta määritellyt roolit, joiden mukaan vastuut jakaantuivat tietoturvatapahtuman sattuessa. Yhdessä haastatteluista mainittiin myös roolien epäselvyydestä tällaisissa tilanteissa. Tämän lisäksi tietoturva- ja it-päällikkö mainitsivat, että heillä on johtovastuita tietoturvatapahtumien sattuessa.

Seuraavana käsitellään ohjaus/kontrolli syklin teemaa, joka liittyy vahvasti rakenteen vaikutus teemaan. Nämä teemat olisi voinut yhdistää yhdeksi teemaksi, mutta päätettiin kuitenkin käsitellä nämä teemat erikseen, jotta saatiin tarkasteltua asioita matalammalla tasolla.

5.4 Ohjaus/kontrolli sykli

Tämä teema muodostui tutkimuksen teoriaosuudesta. Haastattelujen aikana huomattiin erilaisia ohjaus ja kontrolli toimenpiteitä, joita organisaatiossa tapahtui ja kirjallisuuskatsauksessa esiin noussut ohjaus/kontrolli sykli antoi suunnan tämän teeman valitsemiselle tutkimukseen.

Rakenteesta voidaan tässä vaiheessa mainita organisaation kolmeen päätöksentekotasoon liittyviä huomioita. Johtoryhmä toimii luonnollisesti strategisella tasolla, jossa asetetaan organisaation toimintaohjeet. Tietoturvapäällikön, tietoturva-asiantuntijan ja it-päällikön roolit asettuvat kaikki operatiiviselle tasolle. Tekniset asiantuntijat ja järjestelmäasiantuntia asettuivat taktiselle/teknilliselle tasolle. Tämä jakautuminen voidaan sijoittaa Solms ja Solms (2008) malliin, jossa tasoja ovat: hallitus ja johto, ylempi- ja keskijohto, sekä alempijohto ja hallinto. Tässä tutkimuksessa nämä on nimetty kolmen organisaation päätöksenteko tason mukaan, jossa hallitus ja ylin johto kuuluvat strategiselle tasolle. Ylempi- ja keskijohto kuuluvat operatiiviselle tasolle ja viimeisenä alempijohto ja hallinto kuuluvat taktiselle/teknilliselle tasolle. Solmssin ja Solmssin (2008) malli toimii isossa organisaatiossa näillä nimityksillä, mutta tässä tutkimuksessa oli kyseessä keskisuuri organisaatio ja siitä vielä organisaation osa, eli tietoturvaorganisaatio. Tämän takia tasojen määritelmiä on syytä hieman soveltaa tässä kontekstissa. Veigan ja Eloffin (2007) kolmitasoisen jaon mukaan strategiselle tasolle kuuluu johtajuus ja hallinto. Operatiiviselle tasolle kuuluvat turvallisuuden hallinta ja organisointi, turvallisuuspolitiikat, tietoturvaohjelmien hallinta ja käyttäjien tietoturvan hallinta. Taktisella/teknillisellä tasolla on teknologian ja toiminnan suojaaminen (Veiga & Eloff, 2007). Näiden määritelmien mukaan Veigan ja Eloffin (2007) määritelmä sopii paremmin tämän tutkimuksen kontekstiin.

Alla olevasta taulukosta nähdään, että jakauma hallinnollisen ja teknisen tehtävän välillä on muuten, niin kuin voisi teorian perusteella olettaa, mutta kontrolli tietoa ei ole mainittu kertaakaan teknisissä tehtävissä. Tähän yksi syy voi olla siinä, että tilannekuvan tuottamista ei koodauksessa laskettu kontrollitiedoksi, sillä se ei välttämättä ole tietoturva kontrollien tuottamaa dataa, joten se käsiteltiin erillisenä teemana. IT-päällikön haastattelussa mainittiin, että he käyttävät työkaluja, jotka tuottavat haavoittuvuus tietoja, joita välitetään eteenpäin. Tämä voitaisiin hyvin lukea kontrolli tiedon tuottamiseksi, mutta päätettiin jättää ne kokonaisuudessaan tilannekuva teeman alle.

TAULUKKO 5 Rakenteen vaikutukset teeman koodien jakautuminen

Kategoria	**Hallinnollinen tehtävä**	**Tekninen tehtävä**
kontrollitieto	9	0
toiminnan ohjaaminen	14	0
toimintatavat	0	7

Tietoturvapäällikkö ja tietoturva-asiantuntija mainitsivat molemman kontrolli tiedon tuottamiseen ja välittämiseen liittyviä asioita. Nämä kontrollitiedot tulivat pääosin henkilöstön kouluttamiseen liittyvistä toimenpiteistä, joista saatiin dataa, jolla osaamista mitattiin, esimerkiksi tietojen kalasteluun liittyvästä koulutusohjelmasta. Näitä kontrollitietoja jaetaan organisaatiossa koko henkilöstölle ja tiivistettyinä raportteina johtoryhmälle.

Toiminnanohjaus toimenpiteitä oli havaittavissa johtoryhmästä käsin ja operatiiviselta tasolta tietoturvapäällikön ja -asiantuntijan osalta. Tietoturvapäällikkö ja -asiantuntija välittivät johtoryhmältä saatuja toimintaohjeita eteenpäin, sekä loivat itse toimintaohjeita. Toimintaa ohjattiin pääosin luomalla toimintaohjeita, joita jaettiin henkilöstölle eteenpäin. Tarve näihin saattoi syntyä tietoturva huomioista, joita joku henkilöstön jäsen teki esimerkiksi kysymällä tietystä kyberturvallisuuteen liittyvästä asiasta.

Toimintatavat tulivat esille teknisissä tehtävissä toimivilla henkilöillä. Toimintatavoista keskusteleminen ja niiden muodostaminen tapahtui taktisella/teknillisellä tasolla. Solms ja Solms (2008) kuvaamassa ohjaus/kontrolli syklissä näitä kutsuttiin menettely tavoiksi ja myös heidän kaaviossaan nämä menettely tavat muodostuivat taktisella/teknillisellä tasolla. Kirjallisuuskatsauksessa todettiin myös, että tiedon tulkinnan jakaminen on keskeinen tekijä monitieteisessä kokonaisuudessa, jota tarvitaan organisaation kyberturvallisuustoimien tukemiseksi (Sallos, Garcia-Perez, Bedford & Orlando, 2019). Toimintatapojen jakamista voidaan pitää juuri tiedon tulkinnan jakamisena.

Näiden toimintatapojen jakaminen ja raportointi voidaan myös nähdä hiljaisen tiedon muuttamisena eksplisiittiseksi tiedoksi. Nonaka (1994) kutsuu tätä prosessia ulkoistamiseksi, jossa hiljaisesta tiedosta tehdään eksplisiittistä kirjaamalla se ylös systemaattisesti välitettävään muotoon. Lisäksi näistä toimintatavoista keskusteleminen voidaan nähdä myös sosialisointina, joka Nonakan (1994) mukaan tarkoittaa hiljaisen tiedon siirtämistä toiselle henkilölle ilman, että tieto muuttuu eksplisiittiseksi. Seuraavassa luvussa tarkastellaan tarkemmin, miten tätä prosessia voitaisiin muovata siihen suuntaa, että hiljainen tieto muuttuisi tehokkaammin eksplisiittiseksi tiedonhallinnallisilla keinoilla.

5.5 Viestintä- ja tiedonvälitystavat

Tässä alaluvussa käydään läpi tiedonvälitykseen, viestintään ja tiedonhallintaan liittyvät löydöt. Mayer (2007) mukaan tietotyöhön pohjautuva organisaatio on usein organisoitu hajautetusti, sillä on vahvat viestintä-, koordinointi ja yhteistyötarpeet ja se on erittäin liikkuva, joustava ja hajautettu. Voidaan siis olettaa, että tutkittavassa organisaatiossa on vahvat viestintätarpeet ja alaluvun tuloksissa nähdään, miten näihin tarpeisiin on vastattu.

5.5.1 Tiedonvälityskanavat

Yhdessä haastattelukysymyksistä pyrittiin selvittämään millaisia työkaluja/tapoja haastateltavat käyttävät tiedonvälittämiseen ja vastaanottamiseen. Vastauksissa nousi esiin useita eri työkaluja, joita viestintään käytettiin. Alle on listattu eri viestintätavat, joita oli käytössä:

- kokoukset
- keskustelut
- puhelin
- dokumenttienhallintajärjestelmä
- Teams: kokoukset
- Teams: chatti
- intra
- sähköposti
- tietoturvaloukkauslomake
- tiketöintijärjestelmä
- ulkoiset viestintäkanavat (kyberturvallisuuskeskus, Twitter)

Yllä olevasta listasta huomataan, että käytössä on perinteisiä viestintä tapoja paljon ja näiden lisäksi organisaatio on itse panostanut eri järjestelmiin, joilla viestintää voidaan hoitaa tehokkaammin. Microsoft Teams oli yksi kaikissa haastatteluissa esiin tullut työkalu, joka toimi pääväylänä tietoturvaorganisaation tiedonvaihdossa chatin ja kokousten muodossa. Organisaatiossa on myös käytössä intranet sisäiseen viestintään. Intranet tuli esiin vain kahdessa haastattelussa.

5.5.2 Tiedonhallinta

Organisaatiolla oli käytössä kaksi pääasiallista tiedonhallinta työkalua, jotka liittyivät kyberturvallisuuteen. Ensimmäinen näistä oli tiketöintijärjestelmä ja toinen dokumenttienhallintajärjestelmä.

Tiketöintijärjestelmä on työkalu, jolla voidaan koota kybertapahtumat ja havainnot yhden järjestelmän sisälle. Havainnot, eli tässä kontekstissa tiketit ovat keskitetysti yhdessä järjestelmässä. Tiketöintijärjestelmä voidaan nähdä tilannekuvan tuottamis- ja hallinnointi työkaluna, mutta samalla se toimii tiedonhallinnanjärjestelmänä. Tiketöintijärjestelmä avulla voidaan hallita ja yhdistää kybertapahtumia. Kybertoimintaympäristö on kompleksinen ja kyberhyökkäyksen sattuessa voi hyökkäys kohdistua useisiin järjestelmiin yhtäaikaisesti. On mahdollista, että yksittäinen poikkeama jossain järjestelmässä jää pienelle huomiolle, mutta yhdistämällä useat ilmoitukset voi kokonaiskuva näyttää jotain yksittäistä tapahtumaa merkittävämpää.

Haastatteluista havaittiin, että järjestelmäasiantuntija ja tekniset asiantuntijat eivät maininneet tiketöintiä viestintätyökaluna. Lopuissa haastatteluissa tiketöinti nousi esiin. Tiketöinti ei siis näyttäisi olevan teknisten asiantuntijoiden pääasiallisena työkaluna ilmoittaa tietoturvatapahtumista, mikä voi johtua siitä, että

mahdollisuudet kommunikoida kybertapahtumia ovat kattavampia, kuin muulla henkilöstöllä. On myös mahdollista, että tekniset asiantuntijat yksinkertaisesti unohtivat mainita tämän viestintätyökalun haastattelujen aikana.

Tietoturvaloukkauslomake, joka toimii osana tiketöintijärjestelmää, on organisaatiossa tapana ilmoittaa eri kyberhavainnoista kyberasiantuntijoille lomakkeen kautta. Tämä lomake nousi esiin tiedonvälitystapana vain tietoturvapäällikön ja -asiantuntijan vastauksissa. Tietoturvaloukkauslomake toimi myös helppona kanavana osallistaa henkilöstöä tietoturva asioihin, joskin sen käytön aktiivisuutta toivottiin vielä lisää.

Dokumenttienhallintajärjestelmässä on organisaation kaikki dokumentit. Siellä välitetään esimerkiksi kyberturvallisuuteen liittyviä toimintaohjeita henkilöstölle. Dokumenttienhallintajärjestelmä mainittiin kolmessa haastattelussa tiedonvälitystyökaluna. Yhden teknisen asiantuntijan haastattelussa todettiin, että hän käyttää ennemmin sähköpostia dokumenttienhallintajärjestelmän sijaan, sillä kokemusta tämän järjestelmän käytöstä on vielä suhteellisen vähän. ”Niin kun ei ole vielä dokumenttienhallintajärjestelmää niin paljoa tullut itse käytettyä, niin sähköpostin käyttäminen on jotenkin yksinkertaisempaa vielä ainakin.”

5.5.3 Viestintä

Positiivinen huomio haastatteluista oli se, että kaikkien haastateltavien haastatteluista löytyi koodi, joka kertoi, että viestintä koetaan toimivana. Kaikki haastateltavat jollakin tapaa sanoivat, että viestintä ja tavat viestiä toimivat tietoturvaorganisaatiossa. Tämän lisäksi tietoturvapäällikkö mainitsi, että ”sisäinen tiedonvaihto meidän organisaatiossa on lisääntynyt merkittävästi”. Tähän on siis panostettu ja tulokset näyttäisivät hyviltä.

5.6 Koulutus

Koulutus teeman alta haastatteluista löytyi kaksi merkittävää huomiota. Ensimmäinen oli se, että organisaatio panostaa reilusti henkilöstön tietoturvakoulutukseen ja toinen oli koulutustarpeiden ja koulutuksen järjestämisen välillä oleva kitka. Taulukosta kuusi nähdään taas koodien jakautuminen hallinnollisten ja teknisten tehtävien välillä.

TAULUKKO 6 Koulutus teeman koodien jakautuminen

Kategoria	Hallinnollinen tehtävä	Tekninen tehtävä
Koulutuksen järjestäminen	7	0
Koulutus tarpeet	3	6

Tietoturva-asiantuntijan haastattelussa puhuttiin koulutustarpeista ja niiden kuuntelusta seuraavasti: ”Koulutustarpeita tietysti kuunnellaan, jos halutaan

vaikka jotain kohdennetumpaa tietosuojakoulutusta tai tietoturvakoulutusta niin mielellään järjestetään semmoista."

Organisaatiossa siis kuunnellaan ja toteutetaan koulutusta aina tarpeen mukaan ja sitä toteutetaan mielellään. Mielenkiintoinen havainto oli tässä, että koulutustarpeet nousivat teknisiin tehtäviin kuuluvien haastatteluissa esiin kuusi kertaa, kolmessa haastattelussa neljästä. Koulutuksen tarve siis tunnistetaan yksilö tasolla ja organisaatio tiedostaa koulutuksen toteuttamisen hyödyllisyyden, mutta silti nämä koulutus toiveet eivät ainakaan täysin ole täyttyneet haastateltavien osalta. Tämän datan perusteella on mahdotonta sanoa, mistä tämä epätasapaino johtuu. Kyseessä voi olla esimerkiksi ajan puute, joka monesti työtehtävissä on, eli ei ole aikaa kouluttautua, vaikka koulutusta olisikin tarjolla.

Muun henkilöstön koulutusta, eli henkilöt, jotka eivät kuulu tietoturvaorganisaatioon järjestetään myös tässä organisaatiossa paljon. Henkilöstön kyberkyvykkyydet ja -osaaminen ovat keskeinen tekijä etenkin kyberturvallisuuden tilannekuvan luomisessa (Pöyhönen, 2020, s. 136, 183). Tietoturva-asiantuntija mainitsi esimerkiksi verkkokoulutusjärjestelmän, joka on organisaatiossa käytössä: "Tietenkin toi verkkokoulutusjärjestelmä, kun meillä on noita verkkokoulutuksia niin sekin on tavallaan semmoinen väline, kun sieltä kautta opetetaan ihmisiä." Tietoturvapäällikkö mainitsi seuraavan asian, kun häneltä kysyttiin, että millaisella tietoturvaan liittymällä tiedolla voisit hoitaa tehtäväsi tehokkaammin? "varmaan käyttäjäkunnan kouluttaminen ja sen tietoisuuden lisääminen on tärkeintä." Rakenteen hallinnollisella puolella siis ymmärretään koulutuksen tarpeellisuus ja hyödyllisyys erittäin hyvin ja siihen panostetaan organisaatiossa reilusti. Organisaatiossa on siis huomioitu haaste, joka nousi esiin Lehdon ym. (2017) tutkimuksessa, että koko henkilöstön kouluttaminen on haastavaa.

5.7 Tilannekuva

Tilannekuvaan liittyviä vastauksia oli haastatteluissa huomattavan paljon. Tilannekuvaan liittyviä kysymyksiä oli kysymysrungossa kaksi suoraan ja lisäksi siihen liittyviä kysymyksiä, jotka pääosin liittyivät tiedon välittämiseen, oli kahdeksan. Tämä on yksi syy, miksi haastatteluaineistosta nousi tilannekuviin liittyviä vastauksia paljon. Taulukossa 7 on nähtävissä koodien jakautumien kategorioiden ja teknisen-/hallinnollisen tehtävän välillä.

TAULUKKO 7 Tilannekuva teeman koodien jakautuminen

Kategoria	Hallinnollinen tehtävä	Tekninen tehtävä
tilannekuvan kommunikointi	26	25
tilannekuvan taso	6	5
tilannekuvan tuottaminen	13	15

Tilannekuvan kommunikoinnissa ei juuri ollut eroja hallinnollisen ja teknisen jaon välillä. ”Tilannekuvan vastaanottaminen” koodissa teknisessä tehtävässä oli seitsemän mainintaa, kun hallinnollisessa tehtävissä vain neljä. Tilannekuvan tuottamista oli teknisessä kolme ja hallinnollisessa kuusi. Tämä voi kertoa siitä, että tilannekuva kootaan hallinnollisella puolella ja välitetään sieltä eteenpäin muualle organisaatioon tietoturva parissa työskenteleville. Tämä voidaan nähdä myös havaintotietojen luokitteluna, jonka Pöyhönen (2020) nosti väitöskirjassaan esiin. Havaintotietojen luokittelulla mahdollistetaan tietojen siirto eri tasojen välillä ja tämä mahdollistaa kokonaiskuvan hahmottamisen (Pöyhönen, 2020 s. 88–89).

Yksi tutkimuksen pienemmistä tavoitteista oli selvittää, että onko eri haastateltavilla riittävä tilannekuva muiden tietoturvaorganisaation osien toiminnasta. Tähän kaikilla haastateltavilla oli positiivinen vastaus. Osa kuitenkin mainitsi, että tilanne voisi olla vielä entistä parempi ja osa kertoi, että ylläpitää aktiivisesti tilannekuvaa muiden toimista, kuten seuraavasta sitaatista nähdään, kun kysyttiin, onko tilannekuva riittävä muiden osien toiminnasta.

> Kyllä on mutta tietenkin siinä pitää pysyä mukana esimerkiksi eri organisaatioyksiköiden kanssa työskennellään, että pysyy tuo tilannetietoisuus. Vähän semmoisia kenttä hommia välillä, että tietää mitä siellä tapahtuu ja missäkin. Mitä kehitetään minnekin.

Pöyhösen (2020) mukaan tilannekuvan tuottamisen tavoitteena on aikaansaada kaikkia päätöksentekotasoja palveleva havainnointikyky. Havainnoista muodostuu tilannekuva, jota analysoimalla voidaan ymmärtää havaintojen merkitys. Tämä ymmärryksen avulla voidaan arvioida eri vaihtoehtoja ja tehdä päätöksiä (Pöyhönen, 2020 s. 88–89).

Tilannekuvan tuottamista tapahtuu sekä teknisten tehtävien, että hallinnollisten tehtävien tasolla ja kuten aikaisemmin tässä alaluvussa arveltiin, että tilannekuvaa kootaan hallinnollisella puolella ja tiivistetään siitä johtoryhmälle. Näin saadaan muodostettua tilannekuvaa ja havainnointikykyä, joka palvelee kaikkia päätöksentekotasoja. Seuraavassa IT-päällikön sitaatissa nähdään hyvä esimerkki havainnoinnista ja sitten analysoinnista.

> No minä annan esimerkiksi tietoja meidän ympäristöstämme, jos vaikka havaitaan haavoittuvuuksia, niin meidän kautta tarvitaan tietoa sitten siihen, kun arvioidaan sitä, että miten se liittyy meidän ympäristöön vai liittyykö.

Sisäisen tilannekuvan hankkimisen lisäksi organisaatio saa sitä myös ulkopuolelta, kuten yhteistyö alaluvussa mainittiin. Esimerkiksi eri uhka ja haavoittuvuustietoa tulee suoraan yhteistyökumppaneilta ja kyberturvallisuuskeskukselta. Tilannekuvaa tuotetaan siis ulkoa ja sisältä saaduilla tiedoilla, jotka täydentävät toisiaan. Tämä on hyvin havaittavissa seuraavassa sitaatissa.

> Kumppanit, joiden kautta saadaan vaikka sitä haavoittuvuus tietoa… Sitten meillä on semmoisia täydentäviä työkaluja, jotka ovat meidän itse pystyttämiä. Me saadaan

niistä semmoista varmistus tietoa, joka täydentää sitä kuvaa ja sitä välitetään sitten tarvittaessa eteenpäin, jos sieltä paljastuu jotain.

Wangin & Wangin (2019) huomio tulee myös tässä esiin, että organisaation tulee kommunikoida tietoa ulkopuolisten organisaatioiden kanssa organisaation rajojen yli. Organisaatiossa on siis otettu huomioon ulkoisten tiedonlähteiden arvokkuus tilannekuvan tuottamisessa.

Haaste kyberturvallisuuden tilannekuvan kehittämisessä on erityisesti kyberrakenteen teknillisellä tasolla kuten ICT- ja automaatiojärjestelmissä. Tilannetietoisuuden muodostamisessa keskeisessä asemassa on organisaation henkilöstön kyberkyvykkyydet ja -osaaminen. (Pöyhönen, 2020, s. 136, 183)

Tämä Pöyhösen (2020) mainitsema tilannekuvan haaste on tässä organisaatiossa otettu huomioon integroimalla eri organisaatioyksiköiden edustajia mukaan kyberturvallisuuden tuottamiseen. Tässä keskeisessä roolissa on aikaisemmin mainittu tekninen tietoturvaryhmä, jossa on edustusta eri puolilta organisaatiota. Toinen haaste, eli organisaation henkilöstön kyberkyvykkyydet ja -osaaminen, mistä keskustellaan tarkemmin koulutus alaluvussa, on myös tässä organisaatiossa otettu huomioon ja siihen on panostettu.

5.8 Tietoturvan ylläpito ja kehitys

Kybertoimintaympäristö on monimutkainen ja dynaaminen toiminta kenttä, joten siellä onnistuminen turvallisuuden osalta vaatii jatkuvaa kehitystä ja ylläpitoa. Tässäkin tutkimuksessa yhdeksi teemaksi nousi esiin tietoturvan kehitys ja ylläpito toimet. Taulukosta kahdeksan nähdään koodien jakautuminen kategorioihin ja teknisen-/hallinnollisen tehtävän välillä.

TAULUKKO 8 Tietoturvan ylläpito ja kehitys teeman koodien jakautuminen

Kategoria	Hallinnollinen tehtävä	Tekninen tehtävä
tietoturvan kehittäminen	19	4
tietoturvan toteutumisen valvominen	4	0
tietoturvan ylläpito	8	15

Mielenkiintoisia huomioita hallinnollisen ja teknisten tehtävien välillä oli havaittavissa esimerkiksi kehittämisen osalta. Tietoturvan kehitys painottui vahvasti hallinnollisten tehtävien puolelle. Kehittämiskohteita ja tapoja hallinnollisella puolella olivat esimerkiksi:

- henkilöstön osaamisen nostaminen
- tietoturva road-mappien toteuttaminen
- henkilöstön tilannekuvan nostaminen tietoturvaorganisaation toiminnasta
- henkilöstön kyberymmärryksen nostaminen

- sisäiset auditoinnit

Tietoturvan kehittäminen asettui vahvasti hallinnollisten tehtävien puolella ja tämäkin on teorian kanssa yhteensopivaa, sillä kehitys toimia voidaan myös ajatella ohjaus/kontrolli syklin kontekstissa ohjaaviksi toimenpiteiksi. Tämän lisäksi vastuu kehityksestä on hallinnollisissa tehtävissä. Tietoturva-asiantuntija sanoi kuuluvansa kehityspuolelle, joten tämä on yksi syy, miksi jako on painottunut hallinnolliselle puolelle.

Tietoturvan toteutumisen valvominen keskittyi myös täysin hallinnolliselle puolelle. Tämä jako on oletettavissa, sillä teknisissä tehtävissä taas keskitytään ylläpitoon. Yksi maininta toteutumisen valvonnasta liittyi myös osallistamiseen, sillä esimieskunta on osallistettu tietoturvan toteutumisen valvontaan, kuten seuraavassa sitaatissa tulee ilmi. ”Sitten yksi tärkeä viiteryhmä on meidän esimieskunta joidenka vastuulla on heidän omien tiimiensä toimiminen näitten annettujen ohjeiden mukaisesti.”

Kyberturvallisuuden ylläpidolliset toimenpiteet taas keskittyivät teknisten tehtävien puolelle. Näissä havainnoissa oli hyvin tyypillisiä esimerkkejä siitä, miten organisaatioissa pidetään kyberturvallisuutta yllä. Yksi teknisistä asiantuntijoista kuvasi aihetta seuraavasti. ”No se vois olla esimerkiksi tietokoneiden päivityksistä huolehtimista ja virussuojauksien ylläpitoa.”
Ylläpidolliset tehtävät toteutuvat siis pääosin teknisissä tehtävissä. Ylläpidollisia toimenpiteitä on organisaatiossa säännöllisesti. Ylläpidolliset asiat liittyvät myös mahdollisesti tilannekuvan ylläpitoon, mutta nämä kaksi asiaa ovat hyvin lähellä toisiaan joka tapauksessa. IT-päällikkö sanoi ylläpidosta seuraavasti.

> Toki meillä on niin kun ajatus se, että me käydään näissä säännöllisissä palavereissa näitä asioita läpi, niin kuin viimeistään sitten, jos on jotain auki olevia asioita, parin viikon välein.

Haastattelujen perusteella organisaatiossa on jatkuvaa kehitystä kyberturvallisuuden osalta ja tämän lisäksi kyberturvallisuuden toteutumista valvotaan ja kyberturvallisuutta ylläpidetään systemaattisesti. Nämä toimet varmistavat, että kyberturvallisuuden taso pysyy riittävän korkeana, vaikka toimintaympäristössä tapahtuisikin muutoksia.

5.9 Kehityskohteet ja toimivat asiat

Yksi teema oli kehityskohteet ja toimivat asiat, jossa pyrittiin poimimaan haastatteluista kehityskohtia ja toimivia asioita. Taulukosta 9 nähdään, miten teeman kategoriat jakautuivat hallinnollisten ja teknisten tehtävien välillä.

TAULUKKO 9 Kehityskohteet ja toimivat asiat teeman koodien jakautuminen

Kategoriat	Hallinnollinen tehtävä	Tekninen tehtävä
Haasteet	4	10
toimivat asiat	11	12
Toiveet	11	4

Haasteisiin kirjattiin kolme eri koodia, jota olivat ajan puute, kommunikointi haasteet ja toimintamallien epäselvyys. Ajan puute nousi esiin kahdessa haastattelussa. Molemmissa haastatteluissa ilmaistiin, että oman tehtävän voisi hoitaa paremmin, jos sille annettaisiin enemmän aikaa. Molemmissa haastatteluissa mainittiin myös tarve koulutukselle, joten ajan puute voi olla yksi syy minkä takia koulutus tarpeita ei saada täytettyä, kuten aikaisemmin tuloksissa mainittiin.

Kommunikointi haasteet ja toimintamallien epäselvyys nousivat esiin vain yhdessä teknisen roolin haastattelussa. Sitaatista huomaa, että valmiiksi suunniteltu toimintamalli ei ole täysin selkeä ainakaan kyseiselle haastateltavalle.

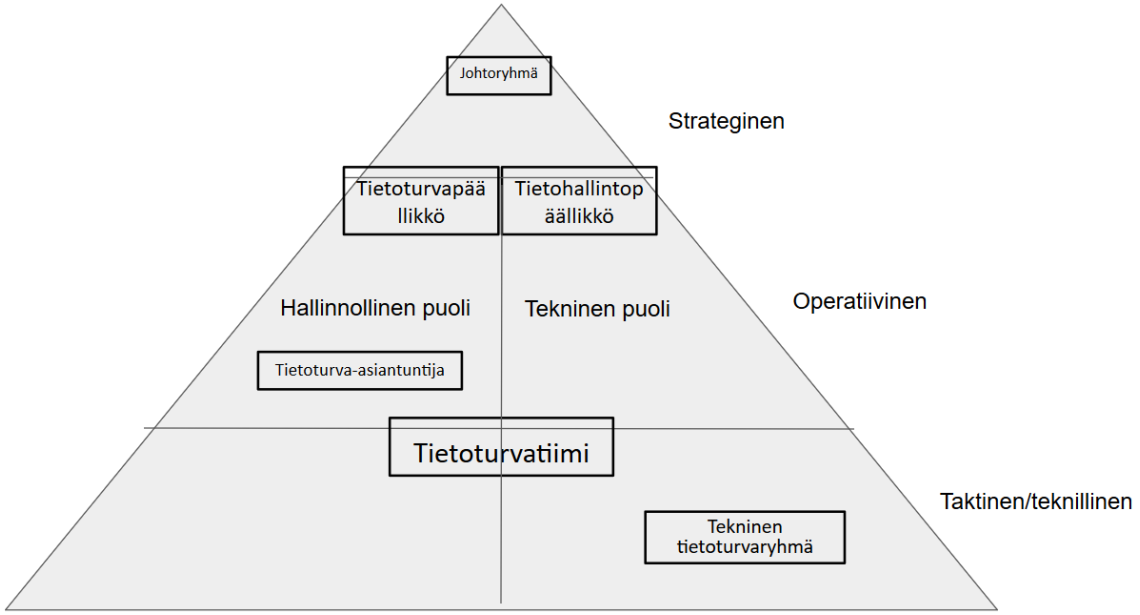
> No tietenkin, jos joku poikkeama tapahtuu, niin ketkä kaikki siinä on sitten mukana ja miten siinä saadaan se ryhmä kasaan ja miten siinä sitten edetään. Vaikka itse jonkun poikkeaman huomaa, niin ketä kaikkia siitä pitäisi sitten informoida.

Toimivista asioista nousi kaksi merkittävää huomiota, jotka olivat toimiva viestintä ja tiketöinti. Kuten viestintä alaluvussa jo todettiin, että kaikki mainitsivat viestinnän toimivana haastatteluissaan ainakin kerran. Toinen huomio oli tiketöinti, jota pidettiin toimivana. Tiketöinnnistä sanottiin, että se vähentää sähköposteja, joita tyypillisesti tulee paljon ja tätä pidettiin positiivisena asiana.

Toiveita haastatteluista nousi esiin useimmiten tietoturva huomioiden antaminen. Hallinnollisella puolella toivottiin, että annetaan enemmän huomioita eri kyberturvallisuus asioista kehityksen ja ylläpidon saavuttamiseksi. Tiketöintiä toivottiin myös lisää, joka voidaan myös nähdä kyberhuomiona. Hallinnollisella puolella mainittiin toive, että kerrottaisiin ohjeistustarpeista. Teknisellä puolella toivottiin, että toimintaohjeita tulisi lisää. Tässä on kanssa yksi tarve ja toive, jotka kohtaavat, mutta eivät ole toteutuneet. Maininnat olivat molemmissa yksittäisiä ja vain yhdessä haastattelussa. Näiden lisäksi toivottiin enemmän toimintatapojen jakamista, lisää tiedonvaihtoa ja ulkoista yhteistyötä.

5.10 Rakennekaavion analyysi

Rakennekaavio voidaan sovittaa tämän tutkimuksen teoriaviitekehyksiin muokkaamalla sitä hieman. Rakenne on jaettu organisaation kolmeen päätöksentekotasoon ja lisäksi se on jaettu hallinnolliseen ja tekniseen puoleen.



KUVIO 9 Tietoturvaorganisaation hallintorakenne sijoiteltuna teoreettiseen viitekehykseen

Kun hallintorakenteen eri osat asetetaan teoriaviitekehyksen mukaisesti kaavioon, on havaittavissa seuraavia huomioita. Johtoryhmä on oletetusti strategisella tasolla, missä tapahtuu tietoturvan ohjaustoimenpiteitä. Lisäksi strategisella tasolla on tietoturvapäällikkö ja tietohallintopäällikkö. Nämä eivät ole vain strategisia tehtäviä, vaan toimivat myös operatiivisella tasolla. Edellä mainitut tehtävät ovat kuitenkin keskeisesti mukana tietoturvan ohjaustoimenpiteissä myös strategisella tasolla. Operatiiviselle tasolle asettuu tietoturva-asiantuntija ja tietoturvatiimi. Tietoturvatiimi toimii vain osittain operatiivisella tasolla, mutta myös taktisella/teknillisellä tasolla. Viimeiseksi tekninen tietoturvaryhmä toimii lähes täysin taktisella/teknisellä tasolla.

Tietoturvatiimi on siis yhdistävä tekijä niin hallinnollisen ja teknisen jaon välillä ja myös taktisen/operatiivisen rajapinnan yhdistävä yhteistyöryhmä. Tietoturvatiimin vaikutus ulottuu myös strategiselle kerrokselle siinä mielessä, että tietoturvapäällikkö ja tietohallintopäällikkö kuuluvat tähän kokoonpanoon. Tietoturvatiimin ansiosta hallintorakenteen eri osista voidaan vaihtaa tietoa ja tehdä yhteistyötä eri hallintorakenteen alueiden kanssa.

Tekninen tietoturvaryhmä on kokoonpanoltaan hieman poikkeava tietoturvatiimistä. Siinä painotus on kallistunut enemmän tekniselle puolelle. Teknisen tietoturvaryhmän erityisominaisuus on se, että siihen on sisällytetty eri organisaatioyksiköiden edustajia. Tekninen tietoturvaryhmä siis hyödyntää henkilöstön osallistamista tietoturvaan tuomalla organisaatioyksiköstä henkilöitä, joilla on kultakin toiminta-alueelta spesifiä tietoa.

IT/ICS-kokonaisuuden osaaminen on haaste kriittisen infrastruktuurin parissa työskentelevillä organisaatioilla (Lehto ym. s.42–43 2017). Tällaisten yhteistyöryhmien avulla voidaan mahdollistaa kommunikaatio näiden kahden alueen välillä.

Yksi huomioitava tekijä on se, että nämä yhteistyöryhmät on nostettu esiin organisaation rakennekaavioon. Pughin, Hicksonin, Hiningsin ja Turnerin (1968)

mukaan formalisointi, tarkoittaa kuinka paljon organisaatiossa kuvataan jäsenten käyttäytymistä ja menettelytapoja. Standardointi määrää tai rajoittaa organisaation jäsenten käyttäytymistä ja menettelytapoja (Pugh, Hickson, Hinings & Turner, 1968). Tietoturvaorganisaation rakennekaaviosta on vaikuttaa sekä formalisoinnin, että standardoinnin kautta, sillä eri rakennekaavion osat kuvaavat, sekä ohjaavat henkilöiden toimintaa organisaatiossa ainakin jossain määrin. Rakennekaavion eri osien formalisoinnin ja standardoinnin merkitystä on kuitenkin vaikea pohtia tämän tutkimuksen tulosten avulla.

6 Huomioita tuloksista

Tässä luvussa tavoitteena on verrata tutkimuskysymyksiä edellisen luvun tuloksiin. Lisäksi tarkastellaan, miten löytöjä voidaan hyödyntää toiminnan kehittämiseen tutkittavassa organisaatiossa ja mahdollisesti muissa organisaatioissa.

Tutkimuksen pääkysymys oli ”**Miten tietoturvan hallintorakenne vaikuttaa kyberturvallisuuden hallintaan?**” Tuloksista löytyi tähän kysymykseen monia vastauksia. Daltonin ym. (1980) mukaan organisaatiorakenne ohjaa ihmisten toimintaa organisaation sisällä. Tässä vaiheessa on hyvä pohtia sitä, onko rakenne vaikuttava tekijä kyberturvallisuuden hallintaan vai onko kyberturvallisuuden hallinnan tarpeista ja kontekstista muodostunut tämä rakenne. Pughin, Hicksonin, Hiningsin ja Turnerin (1969) tutkimuksessa havaittiin, että organisaation rakenne liittyy läheisesti kontekstiin, jossa se toimii ja suuri osa rakenteen vaihtelusta on selitettävissä kontekstiin liittyvistä tekijöistä. Tämän tutkimuksen tavoitteena ei ole kuitenkaan selvittää ohjaako rakenne vai konteksti kehitystä rakenteen ja hallinnan osalta. Sen sijaan tutkitaan, kuinka nykytilan rakenne vaikuttaa toimintaan.

Kuten aikaisemmin kirjallisuuskatsauksessa todettiin, että ”Jokaisen organisaation tehtävänä on omaksua itselleen sellainen rakenne, joka palvelee parhaiten ja tehokkaimmin sen perimmäisiä tavoitteita” (Harisalo, 2008 s. 76). Tämän tutkimuksen aineiston perusteella voidaan olettaa, että tutkittavan organisaation kyberturvallisuuden hallintorakenne on onnistunut tässä. Ensinnäkin osallistamalla on otettu henkilöitä mukaan eri organisaatioyksiköistä, joiden tehtävät eivät pääosin liity tietoturvaan. Rakenteen avulla on muodostettu eri yhteistyöryhmiä, joilla on eri tehtävät kyberturvallisuuden hallinnassa, kuten tietoturvatiimi ja tekninen tietoturvaryhmä.

Rakenteesta liittyvä havainto oli myös se, että organisaatiossa on valmiit toimintaroolit tietoturvatapahtumia varten. Tämä voidaan nähdä rakenteesta johtuvana tekijänä, sillä tietyt vastuualueet tehtävissä toimivat luonnollisesti myös hyvin rooleina tietoturvatapahtumissa. Roolien lisäksi organisaatiossa oli määritelty myös toimintamalleja tällaisiin tapahtumiin.

Osa hallintorakenteessa esiintyvistä rooleista ja tiimeistä asettui kahden organisaation päätöksentekotason rajapintaa. Esimerkiksi tietohallinto- ja tietoturvapäällikkö toimivat strategisen ja operatiivisen kerroksen rajapinnassa. Tätä voidaan käytännöllisesti tulkita niin, että osa henkilön työtehtävistä on strategisia ja osa operatiivisia. Sama havainto tehtiin myös tietoturvatiimistä.

Rakenteessa oli havaittavissa myös jako hallinnollisen ja teknisen tietoturvan välillä. Kirjallisuuskatsauksessa ei löydetty tutkimusta siitä, että onko tämä tehokas tapa tuottaa kyberturvallisuutta, mutta tässä kontekstissa tämä jakautuminen näyttäisi toimivan.

Seuraavaksi vastataan tutkimuksen alakysymykseen, **miten tietoturvan hallintorakenne vaikuttaa tietoturvainformaation kulkuun?** Hallintorakenteen vaikutus tietoturvainformaation kulkuun oli tuloksissa merkittävä. Erityinen painoarvo tässä on yhteistyöryhmillä. Tekninen tietoturvaryhmä ja

tietoturvatiimi olivat viestinnällisesti keskeisiä tekijöitä organisaatiossa. Yhteistyöryhmien avulla organisaatio kokosi tietoa eri organisaatioyksiköistä yhteen ja pystyi näin tuottamaan tilannekuvaa tehokkaasti kybertoimintaympäristöstä. Tiedon tulkinnan jakaminen on keskeinen tekijä monitieteisessä kokonaisuudessa, jota tarvitaan organisaation kyberturvallisuustoimien tukemiseksi (Sallos, Garcia-Perez, Bedford & Orlando, 2019). Näihin yhteistyöryhmiin kuului henkilöitä eri kyberturvallisuuden ja organisaation osa-alueilta, joten näiden ryhmien avulla organisaatiossa kyettiin yhdistämään osaamista monen eri henkilön osalta, joka mahdollisti sen, että analyysissä oli mukana kyberosaamisen lisäksi myös organisaatioyksiköiden osaamista.

Kaikki haastatteluihin osallistuneista mainitsivat jossain vaiheessa, että kokevat viestinnän toimivana. Haastatteluissa tuli myös ilmi, että tähän on organisaatiossa panostettu viime aikana ja tulokset näyttäisivät positiivisilta.

Informaation kulusta johtoryhmään ja sieltä poispäin huomattiin, että tietoturvapäällikkö ja osittain myös tietoturva-asiantuntija toimivat viestinnällisenä solmuna johtoryhmän ja muun organisaation välillä. Johtoryhmälle viestittäessä tapahtuu myös tiedon suodatusta heille sopivampaan, eli korkeatasoisempaa muotoon.

Alakysymyksestä ”**Miten tiedonhallinnalla voidaan tehostaa informaation kulkua hallintorakenteessa?”** havaittiin, että tiedonhallinnallisia työkaluja organisaatiolla oli käytössä useampia. Tiketöintijärjestelmä, joka liittyi vahvasti kyberturvallisuuteen, dokumenttienhallintajärjestelmä ja intranet. Organisaatiossa on siis jo pyritty löytämään tiedonhallinnallisia keinoja, joilla pystytään viestimään tehokkaammin. Nämä keinot vastaavat tähän tutkimuskysymykseen ainakin osittain.

Tiketöintijärjestelmä koettiin toimivana monella tavalla. Esimerkiksi se vähensi sähköpostien määrää, jota haastateltavat saivat tietoturva-asioihin liittyen. Lisäksi tiketöintijärjestelmä toimi kanavana, johon tietoturvatapahtumat keskittyvät, josta niiden tarkastelu jälkikäteen on helpompaa. Tiketöintijärjestelmän käyttöä toivottiin vielä enemmän etenkin henkilöiden osalta, jotka eivät kuuluneet tietoturvaorganisaatioon. Tiketöinti vaikuttasi olevan tehokas tapa pitää kirjaa tietoturvatapahtumista ja sillä voidaan myös tehostaa tilannekuvan tuottamista, sillä kokonaisuus on helpompi hahmottaa, kun useat yksittäiset tapahtumat ovat tarkasteltavissa yhdessä paikassa.

Dokumenttienhallintajärjestelmä oli toinen keskeinen tiedonhallinnan työkalu. Tällä jaettiin esimerkiksi ohjeistuksia ja kokouksissa käytettyjä materiaaleja koko organisaatiolle. Dokumenttienhallintajärjestelmän avulla saadaan myös vähennettyä sähköpostiliikennettä, mikä yleensä koetaan hyvänä asiana organisaatioissa. Dokumenttienhallintajärjestelmän aktiivisempi käyttö voisi olla tiedonhallinnan kannalta hyvä ratkaisu, sillä dokumenttien keskitetty käyttö lähtökohtaisesti nostaa työntekijöiden tehokkuutta. Informaation hallinnan efektiivisyys selittää 41 prosenttia tietotyöntekijän tehokkuudesta (Hwang, Kettinger, & Yi, 2015). Dokumenttienhallintajärjestelmän käytön koulutuksella ja käyttöönottoon rohkaisulla voitaisiin nostaa työntekijöiden informaationhallinnallista efektiivisyyttä.

Informaation kulun tehostaminen tämän tutkimusten tulosten perusteella tässä kontekstissa tapahtuu lisäämällä tiketöintijärjestelmän ja dokumenttienhallintajärjestelmän käyttöä. Potentiaali tiedonhallinnalliseen tehokkuuteen on organisaatiossa luotu näiden järjestelmien avulla, mutta ne eivät ole vielä täysin käytössä kaikkien henkilöiden osalta. Organisaation tulisi siis ohjata henkilöstöä käyttämään näitä järjestelmiä enemmän ja tarvittaessa kouluttaa heitä siihen, jotta saavutetaan maksimaalinen tehokkuus näiden järjestelmien osalta.

Yksi mahdollisuus, mikä organisaatiolla olisi tiedonhallinnan järjestelmien osalta on Nonakan (1994) mallin mukainen hiljaisen tiedon muuttaminen eksplisiittiseksi tiedoksi. Tässä voitaisiin hyödyntää tiketöintijärjestelmässä tuotettuja tikettejä ja dokumenttienhallintajärjestelmää. Tietoturvatapahtuman jälkeen voitaisiin kirjata tapahtuma ja miten se ratkaistiin ylös dokumenttienhallintajärjestelmään, jonka kautta organisaatio pystyisi systemaattisesti tuottamaan hiljaisesti tiedosta eksplisiittistä, mitä Nonaka (1994) kutsuu ulkoistamiseksi. Näin yksittäisten henkilöiden ongelmanratkaisukeinot, jotka ovat monesti hiljaiseen tietoon perustuvia, saataisiin kirjattua ylös muotoon, jota muut voisivat käyttää vastaavanlaisissa tilanteissa. Organisaatioilla on yleinen ongelma, että työntekijöiden poistuessa hiljainen tieto lähtee heidän matkassansa. Tämä olisi yksi keino minimoida tätä tiedon hävikkiä.

7 Yhteenveto

Tämän tutkimuksen tavoitteena oli selvittää, miten kyberturvallisuuden hallintorakenne vaikuttaa kyberturvallisuuden hallintaan. Tapaustutkimuksen avulla saatiin tulokseksi useita eri huomioita rakenteen vaikutuksista. Tutkimuksen tuloksissa nousi esiin kolme keskeistä huomiota. Ensimmäinen huomio oli, että rakenteesta havaittiin jako kolmen organisaation päätöksentekotason osalta, sekä jakautuminen tekniseen ja hallinnolliseen tietoturvaan. Toinen keskeinen huomio oli eri yhteistyöryhmien käyttäminen kyberturvallisuuden hallinnassa. Kolmas huomio oli henkilöstön osallistaminen kyberturvallisuuden tuottamiseen eri puolita organisaatiota.

Organisaation kyberturvallisuuden hallintorakenteen rakennekaaviota analysoitiin organisaation kolmen päätöksentekotason ja haastatteluaineiston avulla. Tästä havaittiin, että kyberturvallisuuden hallintorakenne jakautuu organisaation kolmelle päätöksentekotasolle, kun hallintorakennetta tarkastellaan alhaalta ylöspäin. Horisontaalisesti katsottuna organisaatiokaaviosta löytyi jako hallinnollisen- ja teknisen kyberturvallisuuden välillä. Lisäksi analyysissä havaittiin, että yhteistyöryhmät ja henkilöt voivat asettua tasojen rajapintaan ja tämä voi olla tehokas tapa informaation kulun tehostamiseksi etenkin tasojen välillä.

Toinen tutkimuksen keskeinen huomio oli yhteistyöryhmät, joissa on edustusta kaikilta eri tasoilta ja hallinnolliselta ja tekniseltä puolelta. Kaikkien päätöksentekotasojen ja hallinnollisen, että teknisen puolen edustus minimoi viestinnällisiä haasteita, joita hallintorakenteen jakaminen saattaa aiheuttaa. Yhteistyöryhmien muodostaminen tehokkaan tiedonhallinnan kanssa auttaa organisaatiota pitämään tilannekuvaa yllä kybertoimintaympäristöstään. Informaation kokoaminen yhteistyöryhmien ja tiedonhallinnan avulla mahdollistaa tilannekuvan hahmottamisen helpommin ja tehokkaammin.

Kolmas keskeinen huomio tutkimuksen tuloksissa oli osallistaminen. Osallistamalla henkilöitä eri puolilta organisaatiota, kyberturvallisuuden toteutukseen on mahdollista tuoda spesifiä tietoa organisaation eri osista kyberturvallisuuden suunnitteluun ja toteutukseen. Osallistaminen auttaa myös turvallisuuskulttuurin toteuttamisessa organisaatiossa.

Kaikki nämä kolme huomiota ovat nousseet esiin konkreettisesti tutkittavan organisaation kyberturvallisuus hallintorakenteen rakennekaaviossa. Etenkin yhteistyöryhmien virallistaminen rakennekaavion avulla voi olla keskeinen tekijä näiden ryhmien toimivuuden onnistumisessa. Osallistamista ja yhteistyötä tapahtuu varmasti kaikissa organisaatioissa, mutta tämä kannattaa tuoda esiin myös rakennekaaviossa, jotta toiminta virallistuu ja vakiintuu.

Tutkimuksen tulokset tukevat organisaation laajan yhteistyön ja henkilöstön osallistumisen merkitystä kyberturvallisuuden hallinnassa ja siten tutkimuksessa esiin nousseita keskeisiä löytöjä voidaan suositella yleisesti käytettäväksi eri organisaatioissa.

Tulevien tutkimusten kannalta organisaation päätöksentekotasojen rajapinnassa työskentelevien henkilöiden tehokkuutta kyberturvallisuuden tuottamiseksi kannattaisi jatkossa tutkia tarkemmin. Tämän tutkimuksen tulosten perusteella ei voi tehdä päätelmiä onko tämä hyvä tapa kyberturvallisuuden tuottamiseksi, mutta alustavasti se vaikuttaisi toimivalta keinolta organisoida kyberturvallisuuden hallintorakennetta.

Toinen jatkotutkimusten kohde on kyberturvallisuuden hallintorakenteen jakaminen hallinnolliseen ja tekniseen tietoturvaan. Tähänkään kysymykseen tämän tutkimus ei pysty suoraan vastaamaan, mutta tässä kontekstissa tämä ratkaisu ainakin toimii. Yhteistyöryhmillä, jotka yhdistävät molemmat puolet voi olla vaikutusta tämän jaon toimivuuteen.

LÄHTEET

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

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

Ashby, W. R. (1961). *An introduction to cybernetics*. Chapman & Hall Ltd.

Bennet, D., & Bennet, A. (2004). The rise of the knowledge organization. In *Handbook on Knowledge Management 1* (pp. 5-20). Springer, Berlin, Heidelberg.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.

Chase, R. L. (1997). The knowledge - based organization: an international survey. *Journal of Knowledge Management*.

Conklin, W. A., & Dietrich, G. (2008). Systems theory model for information security. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (pp. 265-265). IEEE.

Dalton, D. R., Todor, W. D., Spendolini, M. J., Fielding, G. J., & Porter, L. W. (1980). Organization structure and performance: A critical review. *Academy of management review*, *5*(1), 49-64.

Dandurand, L., & Serrano, O. S. (2013). Towards improved cyber security information sharing. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)* (pp. 1-16). IEEE.

Drucker, P. F. (1988). The coming of the new organization.

Drucker, P. F. (1999). Knowledge-worker productivity: The biggest challenge. *California management review*, *41*(2), 79-94.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors Society annual meeting* (Vol. 32, No. 2, pp. 97-101). Sage CA: Los Angeles, CA: SAGE Publications.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, *37*(1), 32-64.

Euroopan unioni, (2016). Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen

korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

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

Hirsijärvi, S., Remes, P., & Sajavaara, P. (2009). Tutki ja kirjoita, Kustannusosakeyhtiö Tammi, 15.

Hwang, Y., Kettinger, W. J., & Yi, M. Y. (2015). Personal information management effectiveness of knowledge workers: conceptual development and empirical validation. *European Journal of Information Systems*, *24*(6), 588-606.

Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, *57*(10), 2206-2211.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & security*, *24*(3), 246-260.

Kelloway, E. K., & Barling, J. (2000). Knowledge work as organizational behavior. *International journal of management reviews*, *2*(3), 287-304.

Kim, J. (2017). Cyber-security in government: reducing the risk. *Computer Fraud & Security*, *2017*(7), 8-11.

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

Lehto, M. & Kähkönen, A. (2015). Kyberturvallisuuden kansallinen osaaminen. Jyväskylä: Jyväskylän yliopisto.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M., 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, helmikuu 2017.

Libicki, M. C., 2007. Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New York 2007.

Maier, R. (2007). *Knowledge Management Systems: Information and Communication Technologies for Knowledge Management*.

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, *104*(5), 1039-1057.

Metsämuuronen, J. (2008). Laadullisen tutkimuksen perusteet. Helsinki. *International methelp ky*.

Noor, K. B. M. (2008). Case study: A strategic research methodology. *American journal of applied sciences*, *5*(11), 1602-1604.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization science*, *5*(1), 14-37.

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health services research*, *34*(5 Pt 2), 1189.

Pugh, D. S., Hickson, D. J., Hinings, C. R., & Turner, C. (1968). Dimensions of organization structure. Administrative science quarterly, 65-105.

Pugh, D. S., Hickson, D. J., Hinings, C. R., & Turner, C. (1969). The context of organization structures. Administrative science quarterly, 91-114.

Pöyhönen, J. (2020). Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa–Systeemiajattelu. *JYU dissertations*.

Pöyhönen, J., & Lehto, M. (2020). Cyber Security: Trust Based Architecture in the Management of an Organization's Security. In *ECCWS 2020 20th European Conference on Cyber Warfare and Security* (p. 304).

Pyöriä, P. (2005). The concept of knowledge work revisited. *Journal of knowledge management*.

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

Rubenstein-Montano, B., Liebowitz, J., Buchwalter, J., McCaw, D., Newman, B., Rebeck, K., & Team, T. K. M. M. (2001). A systems thinking framework for knowledge management. *Decision support systems*, *31*(1), 5-16.

Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1-6). IEEE.

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*.

Selkälä, J. (2016). CIO decision making: issues and a process view. *Jyväskylä studies in computing*, (232).

Solms, S. V., & Solms, R. (2008). *Information security governance*. Springer Science & Business Media.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503-522.

Stanton, N. A., Chambers, P. R., & Piggott, J. (2001). Situational awareness and safety. *Safety science*, *39*(3), 189-204.

Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, *23*(4), 1836-1846.

Tiernan, S. (1993). Innovations in organisational structure. *Irish Journal of Management*, *14*(2), 57.

Tisdale, S. M. (2015). Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. *Issues in Information Systems*, *16*(3).

Turvallisuuskomitea, (2013). Suomen kyberturvallisuusstrategia 2013. Valtioneuvoston periaatepäätös 24.1.2013.

Turvallisuuskomitea, (2018). Kyberturvallisuuden sanasto.

Turvallisuuskomitea, (2019). Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös 3.10.2019.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information systems management*, *24*(4), 361-372.

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*, 1-8.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Weill, P., & Ross, J. (2005). A matrixed approach to designing IT governance. *MIT Sloan management review*, *46*(2), 26.

Whittington, R. (2006). Organizational structure. In *The Oxford handbook of strategy*.

LIITE 1 HAASTATTELUTEEMAT JA -KYSYMYKSET

Teema 1: Hallintorakenteen vaikutukset kyberturvallisuuden hallintaan

1. Mihin tietoturvaorganisaation osaan kuulut?
    a. Kuvaile lyhyesti tehtävänkuvaasi.
2. Miten tietoturvaorganisaation hallintorakenne vaikuttaa toimintaasi tehtävässäsi?
3. Minkälaista yhteistyötä teet muiden tietoturvaorganisaation osien kanssa?
4. Onko sinulla omasta mielestäsi riittävä tilannekuva konsernin muiden osien kyberturvallisuus toiminnasta?

Teema 2: Hallintorakenteen vaikutukset tietoturvainformaation kulkuun

5. Mitä tietoa välitä muille tietoturvaorganisaation osille?
6. Mitä tietoa välität kyberturvallisuuden tilannekuvan ylläpitämiseksi?
7. Mitä tietoa sinulle välitetään muilta tietoturvaorganisaation osilta?
8. Mitä tietoa vastaanotat kyberturvallisuuden tilannekuvan ylläpitämiseksi?

Teema 3: Tiedonhallinnan keinot tiedonkulun tehostamiseksi

9. Millaisella tietoturvaan liittyvällä tiedolla voisit hoitaa tehtäväsi tehokkaammin?
10. Mitä työkaluja käytät tietoturvaan liittyvän tiedon välittämiseen/vastaanottamiseen?
11. Millä tavalla toivoisit tietoturvatietoa jaettavan?
12. Minkälaista tukea tarvitset tehtäväsi toteuttamiseksi paremmin?