Kati Ilomäki

PRO GRADU -TUTKIELMA

TIETOVIRRAT JA NIIDEN HALLINTA KYBERTILANNEKUVAN MUODOSTAMISEN KONTEKSTISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Ilomäki, Kati
Tietovirrat ja niiden hallinta kybertilannekuvan muodostamisen kontekstissa
Jyväskylä: Jyväskylän yliopisto, 2023, 99 s.
Turvallisuus ja strateginen analyysi, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Tietoisuus kyber- ja tietoturvallisuusriskeistä sekä näiden vaikutuksista kansalliseen ja kansainväliseen turvallisuuteen on kasvanut viimeisen vuosikymmenen aikana. Tiedosta muodostuva arvopotentiaali on keskeinen osa kybertoimintaympäristön turvaamista, eikä se ole mahdollista ilman eri toimijoiden välistä yhteistyötä. Tietovirtojen avulla voidaan tarkastella organisaatioiden kykyä muuntaa tietoresursseja arvoksi, joka tässä tutkimuksessa sidottiin kybertilannekuvan muodostamiseen. Yleisesti tietojohtamisen tehtävä on parantaa organisaatioissa ja sen sidosryhmissä tapahtuvaa arvonluomiskykyä. Tämän tutkimuksen tavoitteena oli pyrkiä tunnistamaan parhaat käytänteet tietovirtojen hallintaan kybertilannekuvan muodostamisen kontekstissa. Parhaiden käytänteiden tunnistamiseksi tutkimuksessa selvitettiin tietovirtojen muodostumisen ja niiden hallinnan yleisiä periaatteita sekä lisäksi pyrittiin tunnistamaan, millaisia käytännön haasteita näihin mahdollisesti liittyy. Havaintojen pohjalta pyrittiin selvittämään, onko tietovirtojen hallintaan kybertilannekuvan muodostamisen kontekstissa esitettävissä jonkinlainen ideaalimalli. Tutkimus toteutettiin monimenetelmäisenä kvalitatiivisena tutkimuksena. Tutkimusaineisto kerättiin havainnoimalla erästä kotimaista kyberturvallisuusharjoitusta sekä haastattelemalla yhteensä kahdeksaa asiantuntijaa neljästä eri organisaatiosta. Tietovirtoja pyrittiin hahmottamaan kybertilannekuvan muodostamisen kontekstissa hakien näkemyksiä niin organisaation, verkoston kuin myös laajemmin yhteiskunnan näkökulmasta. Monipuolisen ja laajahkon tulokulman valinta perustui siihen, että aihetta on tutkittu Suomessa aiemmin jokseenkin vähän. Tietoon ja siihen liittyvät ilmiöt mielletään usein monimutkaisiksi ja abstrakteiksi, mikä teki myös tästä tutkimuksesta osaltaan haastavan kokonaisuuden. Saadut tulokset kuvaavat ilmiötä ylätasolla, eikä kovinkaan yksityiskohtaisia käytänteitä tietovirtojen hallintaan ole mahdollista tutkimuksen pohjalta esittää. Tutkimuksessa kuitenkin tunnistettiin melko laajasti yleisiä periaatteita ja haasteita, joita tietovirtoihin ja niiden hallintaan kybertilannekuvan muodostamisen kontekstissa liittyy. Tietovirrat ja niiden hallinta kybertilannekuvan muodostamisen kontekstissa on moniulotteinen ja laaja kokonaisuus, jota ei voida pitää itsestäänselvyytenä. Tutkimusaihe on merkittävä, sillä ilman ymmärrystä organisaatioiden tietoprosesseista ei pystytä hyödyntämään tietoresurssien todellista arvoa kybertilannekuvan muodostamisessa.

Asiasanat: tietovirrat, kybertilannekuva, kyberturvallisuus, tietojohtaminen

ABSTRACT

Ilomäki, Kati
Knowledge flows and their management in the context of maintaining cyber situational picture
Jyväskylä: University of Jyväskylä, 2023, 99 pp.
Security and Strategic Analysis, Master's Thesis
Supervisor: Lehto, Martti

Overall awareness of cyber and information security risks and their potential impact on national and international security has grown over the past decade. The value potential created by knowledge is a crucial element of securing cyber operational environment, and furthermore, which is not succeeded without co-operation between different organisations and other actors. Knowledge flows can be used to examine the ability of how organisations transform their knowledge resources into value, which in this study is related to maintaining cyber situational picture. In general, knowledge management aims at improving the value creating capability of organisations and their stakeholders. The objective of this study was to identify best practices for managing knowledge flows in the context of maintaining cyber situational picture. To identify best practices, the research explored the general principles of knowledge flows and their management, as well as challenges associated with the research topic. Based on the findings of this study, it was sought to identify whether some kind of ideal model for managing knowledge flows could be formed. The study was carried out as a multimethod qualitative study. The research material was collected by observing a Finnish cybersecurity exercise and by interviewing a total of eight specialists from four different organisations, seeking perspective from organisations, networks as well as from wider society point of view. The versatile and wide-ranging approach was partly explained by as not much of previous research in Finland had been made within the same context. Knowledge and related phenomena are often considered as complex and abstract, which also made this study challenging to conduct. The obtained results describe the phenomenon at a high level, and thus, it is not possible to present very detailed practices for managing the knowledge flows based on this study. However, the study identified rather broadly general principles and challenges associated with knowledge flows and their management in the context of maintaining cyber situational picture. The knowledge flows and their management in this context are multidimensional and extensive, which cannot be taken for granted. The research topic is significant since without understanding of organisations' knowledge processes, we are unable to utilize the true value of knowledge resources on maintaining cyber situational picture.

Keywords: knowledge flows, cyber situational picture, cybersecurity, knowledge management

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tietoisuus kyber- ja tietoturvallisuusriskeistä sekä näiden vaikutuksista kansalliseen ja kansainväliseen turvallisuuteen on kasvanut viimeisen vuosikymmenen aikana. Erityisesti keväällä 2022 Venäjän Ukrainaa vastaan aloittaman hyökkäyssodan myötä kyberulottuvuuden merkitys osana sodankäynnin strategiaa ja yhteiskunnan kriittisiin toimintoihin vaikuttamista on korostunut uudella tavalla myös suojautumisen näkökulmasta. Kyse on pitkälti kyberturvallisuuden tietojohtamisesta ja tarkemmin tiedon arvopotentiaalin tunnistamisesta ja hyödyntämisestä toiminnan eri tasoilla.

Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa toimintaympäristöön voidaan luottaa ja se on turvattu (Sanastokeskus, 2018). Kybertoimintaympäristön turvaaminen ei kuitenkaan ole mahdollista ilman yhteistyötä (Laari, Flyktman, Härmä, Timonen & Tuovinen, 2019), mikä vahvistaa oletuksena tarvetta toimivalle vuoropuhelulle ja tiedon virtaamiselle eri toimijoiden välillä.

> Kyberturvallisuus on laaja kokonaisuus, joka koskettaa koko yhteiskuntaa kriittisestä infrastruktuurista aina kuluttajiin asti. Kybertoimintaympäristön laajuus ja levinneisyys tarkoittavat kuitenkin sitä, että sen turvallisuutta ei ole mahdollista hoitaa yhden tahon toimenpitein vaan se vaatii yhteistyötä eri toimijoiden välillä. (Laari ym., 2019, s. 8.)

Kyberturvallisuuden osalta Suomessa tehdään tiivistä yhteistyötä niin yksityisen kuin julkisen sektorin välillä. Kansallisella tasolla Liikenne- ja viestintävirasto Traficomin alaisen Kyberturvallisuuskeskuksen rooli on keskeinen Suomen kyberturvallisuuden poikkeamahallinnassa sekä tilannekuvan muodostamisessa ja analysoinnissa. Kyberturvallisuuskeskus toimii kansallisena yhteyspisteenä tietoturvapoikkeamien ja -uhkien hallinnassa sekä tarvittaessa tutkii ja auttaa tapauksiin liittyviä tahoja selvittämään niitä. Lisäksi Kyberturvallisuuskeskuksen CERT-toiminto (Computer Emergency Response Team) tuottaa ja ylläpitää kybertilannekuvaa yhdessä kansallisten ja kansainvälisten kumppanien ja kollegoiden kanssa. Tärkeä osa kyberturvallisuuden ylläpitämistä on myös turvallisuusviranomaisten operatiivisen tason tiedonvaihtoverkosto VIRT (Virtual Incident Response Team), joka varautuu yhteistoiminnassa laajavaikut-

teisiin tietoturvahäiriötilanteisiin. Lisäksi on olemassa toimialakohtaisia kybertiedonvaihtoryhmiä, joista käytetään nimitystä ISAC (Information Sharing and Analysis Centre). ISAC:it ovat yhteistyöelimiä, jotka muodostuvat usein eri toimialoilla, kuten kemian ja metsäteollisuuden, pankki, energiateollisuuden, ruokatuotannon, terveydenhuollon aloilla toimivista organisaatioista. (Pöyhönen, Nuojua, Lehto & Rajamäki, 2019).

Koska kyberuhat ovat luonteeltaan globaaleja, on kybertoimintaympäristön kehittyviin uhkiin pyrittävä yhtä lailla vastaamaan usein valtioiden rajat ylittävällä yhteistyöllä, jotta uhkia vastaan kehitetyt lieventävät toimenpiteet ja tekniset keinot olisivat mahdollisimman tehokkaita (Skopik, Setanni & Fiedler, 2016). Skopik ym. (2016) painottavatkin kansainvälistä yhteistyötä äärimmäisen tärkeänä tehokkaiden vastekeinojen kannalta, sillä kybermaailma ei noudata reaalimaailmassa hahmotettavia valtioiden rajoja tai oikeusjärjestelmää täysimääräisesti. Esimerkiksi Euroopan Unionin kyberturvallisuusstrategian ja NIS-direktiivin tavoitteina on edistää kyberturvallisuutta EU:ssa velvoittaen jäsenmaita keskinäiseen tiedonvaihtoon, kansallisten kybersuorituskykyjen kehittämiseen sekä valvontaan kriittisten toimialojen, kuten energiasektorin ja digitaalisen infrastruktuurin osalta (European Commission, 2022; EU 2016/1148), mitkä ovat tärkeä osa kyberturvallisuuden tietojohtamisen poliittista ohjausta.

Strategista johtamista tarvitaan kyberturvallisuuden yhteensovittamiseen ja koordinoimiseen sekä eri toimijoiden välisten yhteistoimintarakenteiden varmistamiseen (Lehto & Limnéll, 2021). Suomen kokonaisturvallisuuden yhteistoimintamalli luo perusteet viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyölle osana varautumista ja toimimista häiriötilanteissa (Valtioneuvoston periaatepäätös, 2017). Vuonna 2019 julkaistussa *Kyberpuolustuksen kehittämisen strategiset linjaukset* -julkaisussa korostuu nimenomaan eri tahojen välisen yhteistyön merkitys kansallisessa kyberpuolustuksessa ja kyberturvallisuuden ylläpitämisessä (Puolustusministeriö, 2019). Kyberturvallisuus tulee ennen kaikkea nähdä laajana yhteiskunnallisena ilmiönä, joka tuo monet eri toimijat yhteen (Lehto & Limnéll, 2021).

Yleisesti tiedon ympärille muodostuvat verkostot voivat olla suljettuja tai avoimia, hajautettu maantieteellisen sijainnin ja koon mukaan, tai toisaalta rakentua joko kasvokkain tai tietojärjestelmien välityksellä tapahtuvan tiedonvaihdon ympärille. Ne voivat yhtä lailla olla myös yhden organisaation sisäisiä tai usean organisaation välisiä verkostoja. Vuori, Helander ja Mäenpää (2019) viittaavat Magnussoniin ja Nilssoniin (2003), joiden mukaan tiedon (tai tietämyksen) jakamisen ympärille rakentuvan verkoston strategisena motivaattorina voi olla liiketoimintalähtöiset (engl. business-oriented) tai oppimiseen (engl. learning-oriented) liittyvät taustatekijät. Liiketoimintalähtöiset organisaatiot hakevat verkostoista rahallista hyötyä, kun taas oppimiseen keskittyvät organisaatiot pyrkivät tiedon jakamisella luomaan uutta tietoa ja suorituskykyjä. (Vuori ym., 2019.) Muun muassa kyberpuolustuksen osa-alueella yritystoiminnan tarjoaman potentiaalin hyödyntämiseksi on tunnistettu mahdollisuus muodostaa strategisia kumppanuuksia (Puolustusministeriö, 2019), jolloin verkoston strateginen motivaattori muodostuu kenties laajemman hyöty- ja arvo-

käsityksen ympärille kuin pelkästään taloudelliseen voittoon tai oppimiseen tähtäävässä toiminnassa.

Yhteistyö- ja tietoa tuottavien tahojen tunnistaminen luo edellytykset tiedon jakamiselle ja sitä kautta tilannetietoisuuden kehittymiselle (Pöyhönen ym., 2019). Toimijoiden välinen tiedonvaihto perustuu pitkälti luottamukseen. Luottamus kehittyy ajan myötä ja usein se rakentuu yksilötasolla asiantuntijoiden välillä (Vázquez, Acosta, Spirito, Brown & Reid, 2012). Luottamuksen syntyyn vaikuttaa lisäksi saadun tiedon merkityksellisyys ja sen koettu arvo omassa toiminnassa (Vázquez ym., 2012), mikä tulee myös huomioida rakennettaessa organisaation toimintakulttuuria tiedonvaihdon osalta. Verkostoissa tiedon jakamisen hallitseminen voi kuitenkin olla haastavaa useista syistä, kuten esimerkiksi tasapainottelusta tiedon jakamisen riski- ja hyötynäkökulman välillä, tietojärjestelmiin liittyvistä ongelmista, henkilöiden motivoimisesta tai tiedon monipuolisuudesta johtuen (Vuori ym., 2019).

Tämän tutkielman tarkoituksena on pyrkiä tunnistamaan parhaat käytänteet tietovirtojen hallintaan kybertilannekuvan muodostamisen kontekstissa. Tutkielma etenee siten, että seuraavissa alaluvuissa esitellään tutkimustehtävä sekä aiempaa aihepiiriin liittyvää tutkimusta. Tutkielman toisessa ja kolmannessa pääluvuissa käsitellään tutkimuksen kannalta keskeistä teoriakehystä lähtien liikkeelle organisaatioiden yleisestä tietojohtamisesta syventyen kybertoimintaympäristöön liittyviin tunnuspiirteisiin ja ominaisuuksiin, jotka heijastavat organisaatioiden kyberturvallisuuden tietojohtamiseen. Neljännessä pääluvussa esitellään tutkimuksessa käytetyt tutkimusmenetelmät sekä tutkimuksen eri vaiheet. Pääluvussa viisi esitetään tutkimuksen keskeisimmät tulokset, jonka jälkeen seuraavassa pääluvussa tutkimustuloksia käsitellään vastaamalla tarkemmin tutkimustehtävään ja pohditaan tutkimuksen merkitystä, luotettavuutta sekä esitetään tutkimusprosessin aikana heränneet jatkotutkimusaiheet. Viimeinen pääluku muodostuu tutkielman yhteenveto-osuudesta.

1.1 Tutkimustehtävä

Tutkimuksen tavoitteena on pyrkiä tunnistamaan parhaat käytänteet tietovirtojen hallintaan kybertilannekuvan muodostamisen kontekstissa. Tutkimuksen lähtöasetelmana on oletus, että tietovirrat muodostuvat useista eri lähteistä niin organisaation sisältä kuin ulkoisilta sidosryhmiltä. Yhtenä tutkimuksen näkökulmana on hahmottaa tiedonvaihdon aikakäsitystä ja sen vaikutusta toimintaan kybertilannekuvan muodostamisen kautta. Parhaiden käytänteiden tunnistamiseksi tulee selvittää tietovirtojen muodostumisen ja niiden hallinnan yleiset periaatteet sekä lisäksi pyrkiä tunnistamaan millaisia käytännön haasteita näihin mahdollisesti liittyy. Havaintojen pohjalta pyritään selvittämään, onko mahdollista esittää jonkinlainen ideaalimalli tietovirtojen hallintaan kybertilannekuvan muodostamisen kontekstissa. Tutkimuksen pääkysymyksenä on:

- Onko tietovirroista ja niiden hallinnasta esitettävissä jonkinlaista ideaalimallia kybertilannekuvan muodostamisen kontekstissa?

Tutkimuksen pääkysymyksen tueksi laadittiin kaksi aihetta tarkentavaa ja ymmärrystä laajentavaa alakysymystä:

- Millaisia tietovirtojen muodostumiseen ja niiden hallintaan liittyviä yleisiä periaatteita on tunnistettavissa kybertilannekuvan muodostamisen kontekstissa?
- Mitä haasteita tietovirtojen muodostumiseen ja niiden hallintaan liittyy?

Tieteenfilosofisena lähtökohtana tässä tutkimuksessa on interpretivistinen eli tulkinnallinen näkemys ontologiasta ja epistemologiasta. Ontologia viittaa olettamuksiin todellisuuden luonteesta ja tunnuspiirteistä, kun taas epistemologia keskittyy olettamuksiin tiedosta ja kuinka sitä on mahdollista hankkia (Creswell & Poth, 2018, s. 20–21; Saunders, Lewis & Thornhill, 2019, s. 133; Puusa & Juuti, 2020, s. 34). Ontologista näkemystä tässä tutkimuksessa kuvastavat organisaatioiden tietoon ja sen käsittelyyn liittyvät rakenteet ja toimintamallit, jotka kytkeytyvät kybertilannekuvan muodostamiseen. Epistemologia puolestaan liittyy ihmisten mahdollisiin erilaisiin näkemyksiin ja kokemuksiin tiedon eri ilmenemismuodoista tietovirtojen ja niiden hallinnan näkökulmasta kybertilannekuvan muodostamisen kontekstissa. Epistemologiaksi Puusan ja Juutin (2020, s. 34) mukaan kutsutaan niin tiedon käsitettä kuin tiedon saavuttamisen menetelmiä, joka tässä tutkimuksessa on kyberturvallisuuden tietojohtamista käsittelevien tietosisältöjen ja merkitysten tunnistamista organisaatioiden toiminnassa. Todellisuutta ei toisin sanoen voida puhtaasti määrittää organisaatiorakenteilla ja toimintamalleilla, vaan osa tutkimuksen kannalta merkityksellisestä tiedosta syntyy ihmisten erilaisista näkemyksistä ja tulkinnoista.

Tutkimuksen tavoitteena on pyrkiä tunnistamaan kybertilannekuvan muodostamiseen liittyviin tietovirtoihin ja niiden hallintaan vaikuttavia tekijöitä laaja-alaisesti, minkä vuoksi tutkimusta päätettiin lähestyä hermeneuttisesti. Hermeneuttisessa tutkimuksessa tutkijalla on tyypillisesti joko omakohtaisen kokemuksen tai niin sanotusti toisen kautta saatuna tietona muodostunut ennakkokäsitys tutkittavasta aihepiiristä (Puusa & Juuti, 2020, s. 73). Tämän tutkielman osalta tutkijan ennakkokäsitys tutkimuksen aihealueesta on muodostunut hänen työkokemuksensa kautta. Hermeneuttisen näkemyksen mukaan yksityiskohtien tulkinta vaikuttaa kokonaisuuden tulkintaan, ja toisaalta tutkimuskohteesta tehty uudelleen tulkinta tuottaa edelleen laajempaa ymmärrystä tutkittavasta aiheesta (Jyväskylän yliopisto, 2015a). Hermeneuttinen lähestymistapa on luonteeltaan kehämäistä, mikä mahdollistaa palaamisen edeltäviin vaiheisiin tutkimusprosessin edetessä ja aiemmin kirjattujen näkemysten korjaamisen. Lähtökohtana on, että tutkija pyrkii niin sanottuun ilmeisyyteen eli siihen, että tulkinta lisää ymmärrettävyyttä aiheesta eikä sen ja tutkimusaineiston välillä ole ristiriitaa. Tähän tutkimuksen kehämäiseen lähestymistapaan viitataan hermeneuttisen kehän käsitteenä. (Puusa & Juuti, 2020, s. 73–74.)

Toisaalta määritettyä tutkimustehtävää on mahdollista tarkastella myös konstruktionismin avulla. Suuntauksen mukaan ilmiöiden ja maailman merkitykset ovat sosiaalisesti ja kulttuurisesti tuotettuja rakenteita, joissa ihminen tuottaa omassa toiminnassaan erilaisia totuuksia ja tietoja (Jyväskylän yliopisto, 2015b). Tällöin organisaatioiden kybertilannekuvaa muodostavat toiminteet ja siihen kytkeytyvät organisatoriset prosessit ja toimintatavat voidaan nähdä merkityksiä muodostavina rakenteina, joista ihmiset muodostavat oman toimintansa ja tehtävänsä kautta erilaisia totuuksia, kuten esimerkiksi tässä tutkimuksessa tarkasteltavista tietovirroista ja niiden hallinnasta kybertilannekuvan muodostamisen kontekstissa.

Tutkimuksen aihealue on moniulotteinen, eikä kaikkia mahdollisia näkökulmia voida kuitenkaan ottaa huomioon. Tässä tutkimuksessa käsitellään tietovirtoja ja niiden hallintaa ainoastaan kyberturvallisuuden tilannetietoisuuden ja tilannekuvan näkökulmista melko abstraktilla tasolla. Tutkimuksen ulkopuolelle rajataan yleisesti kybertilannekuvatoiminteisiin liitetyt tekninen kybervalvonta, poikkeamanhallinnan sekä kybersietoisuuden prosessit ja niiden käytännöt toteutukset, vaikka ne sivuavat myös tämän tutkimuksen aihepiiriä. Tutkimuksen tavoitteena ei myöskään ole arvioida aihepiiriin liittyviä teknisiä menetelmiä ja ratkaisuja, joiden avulla tietoa esimerkiksi jaetaan eri toimijoiden välillä, tai myöskään toteuttaa niiden välistä vertailua.

1.2 Aiempi tutkimus

Tietovirroista ja niiden hallinnasta kybertilannekuvan muodostamisen kontekstissa löytyy melko vähän aiempaa tutkimusta. Toisaalta tutkimuksen vähäisyyttä voi jokseenkin selittää se, että kyberturvallisuus on itsessään aihealueena vieläkin verrattain tuore. Suomen ensimmäinen kyberturvallisuusstrategia hyväksyttiin vuonna 2013 (Valtioneuvoston periaatepäätös, 2013) ja sitä päivitettiin vuonna 2019 (Valtioneuvoston periaatepäätös, 2019), mikä voinee erityisesti vaikuttaa kyberturvallisuuden tietojohtamiseen liittyvän tutkimuksen vähäisyyteen nimenomaan Suomen viitekehyksessä. Kyberturvallisuuden tutkimusta teknisestä näkökulmasta on toteutettu jossain määrin enemmän kuin kokonaisvaltaisemmassa kyberturvallisuuden tietojohtamisen viitekehyksessä, pois lukien valtioneuvoston tutkimushankkeet kuten *Kriittisen infrastruktuurin tilannetietoisuus* (Horsmanheimo ym., 2017) sekä *Kyberturvallisuuden strateginen johtaminen Suomessa* (Lehto ym., 2018), joissa on pyritty selvittämään kyberturvallisuuden laajempaa yhteiskunnallista vaikutusta, yhteistoiminnan edellytyksiä sekä myös kyberturvallisuuden johtamista Suomessa.

Muun muassa Eldardiry ja Caldwell (2015) ovat tutkineet verkkovalvomoiden (engl. network operations center, NOC) ja tietoturvavalvomoiden (engl. security operations center, SOC) toimintaa informaatiohallinnan ja tehtävien yhteensovittamisen sekä tilannekuvan tuottamisen näkökulmasta. He toteavat, ettei aihepiiristä juurikaan löydy akateemista tutkimusta, jossa käsiteltäisiin inhimillisten tekijöiden, mukaan lukien kognitiivisen kyvykkyyden, merkityk-

sellistämisen ja organisatoristen prosessien vaikutusta mainittujen valvomoiden toimintaan (Eldardiry & Caldwell, 2015). Skopik ym. (2016) näkevät, että tiedonvaihdon mahdollistavien systeemien järjestäminen ei pelkästään vaadi teknisten ja teknologisten näkökulmien huomioimista, vaan yhtä lailla lainsäädännön ja erilaisten standardien, sekä sosiaalisten ja taloudellisten rakenteiden tutkimista. Myös Vázquez ym. (2012) näkevät tarpeellisena tehdä tutkimusta sosiaalisen näkökulman esiintuomiseksi tiedonjakamisessa. Tutkielman kannalta olennainen kyberturvallisuuteen liittyvä lähdekirjallisuus näyttäytyy siten osin pirstaleisena.

Sen sijaan yleisesti tietojohtamista käsittelevää kirjallisuutta on saatavilla runsaasti (mm. Nonaka & Takeuchi, 1995; Choo, 1998 & 2006; Huotari, Hurme & Valkonen, 2005; Laihonen ym., 2013; jne.). Nonakan ja Takeuchin (1995) teosta *The Knowledge-Creating Company* voidaan pitää klassikkona ja yhtenä keskeisimmistä tietojohtamisen teorialähteistä myös tässä tutkimuksessa. Nonakan ja Takeuchin (1995) SECI-malli uuden tiedon luomiseen toimii pohjana monille muille malleille, kuten heidän jatkojalostamalleen monitasoisen tiedonluomisen mallille, jota voidaan soveltaa organisaation eri tasoilla ja laajemmin myös yhteistyöverkostoissa. Uuden tiedon luomisen malli (Nonaka & Takeuchi, 1995) ja tiedon hallinnan prosessimalli (Choo, 1998 & 2006) liittyvät myös tässä tutkimuksessa käsiteltäviin tietovirtoihin. Mica Endsley on tutkinut yleistä tilannetietoisuuden muodostumista ja päätöksenteonmalleja (Endsley, 1995). Hänen julkaisujaan voidaan pitää tilannekuvan muodostumisen osalta perusteorialähteenä myös tämän tutkimuksen kannalta.

Esimerkiksi Norri-Sederholm, Joensuu ja Huhtinen (2017) ovat tutkineet turvallisuustoimijoiden tiedonkulkua ja tilannekuvan muodostumista muun muassa poliisi- ja pelastuspalvelutoiminnassa. Heidän mukaansa tilannekeskustoiminta (eng. situation centre), erityisesti tiedonkulun ja tilannekuvan näkökulmasta, ovat vähän tutkittuja ja kirjallisuutta on yleisesti niukasti. Toisaalta muun muassa Pöyhönen ym. (2019), Parish ja Madahar (2016) sekä Kuusisto, Kuusisto ja Wolfgang (2015) ovat tutkineet tilannetietoisuuden muodostumista kyberturvallisuuden viitekehyksessä, mutta kuten todettu, kokonaisvaltaista aiempaa tietovirtatutkimusta kyberturvallisuuden osalta ei tätä tutkimusta tehdessä kuitenkaan tunnistettu. Tilannekuvatutkimuksen vähäisyyttä voinee myös selittää aihepiirin operatiivinen luonne, mikä tekee siitä ja siihen liittyvistä yksityiskohdista usein luottamuksellisuuskysymysten alaisia. Yleisesti julkisen tutkimuksen tekeminen näyttäytyy haastavana tämän tyyppisessä aihepiirissä, vaikka sen tarpeellisuus onkin tunnistettu (mm. Norri-Sederholm, Joensuu & Huhtinen, 2017).

Tietoperustaiseen arvonluontiin ja organisaation tietoprosesseihin liittyy monia ongelmia ja haasteita, mitä pidetään lähdekirjallisuudessa yhtenä soveltuvana tulokulmana tietojohtamiseen ja siihen liittyvään tutkimukseen (mm. Jalonen, 2015). Lisäksi lähdekirjallisuudessa esitetty kritiikki toisaalta peräänkuuluttaa tarvetta empiiriselle tutkimukselle ja käytännön kehittämistyötä tukeville sovelluksille kyberturvallisuustutkimuksessa. Muun muassa Laihonen esittää (2011, s. 81), että erityisesti ”tietovirtatutkimus -- kaipaa konkreettisia

lähestymistapoja, jotka lisäisivät ymmärrystä tiedon virtaamiseen liittyvistä käytännön ilmiöistä ja näihin vaikuttavista tekijöistä.” Jalosen (2015) mukaan tietojohtamisen kääntöpuoleen liittyvää tutkimusta, kuten informaation aktiiviseen välttämiseen, tiedonkulun pullonkauloihin, liialliseen informaatioon, ja niin edelleen, on huomattavasti vähemmän kuin tietojohtamista edistäviin tekijöihin liittyvää tutkimusta. Hän näkee kehityssuunnan huolestuttavana, sillä ilman ”kulisseihin” pureutuvaa tutkimusta ei voida myöskään täysin päästä käsiksi nykyorganisaatioiden keskeiseen haasteeseen, ”joka ei niinkään ole informaation puute, vaan merkityksellisen ja relevantin tiedon löytämisen vaikeus” (Jalonen, 2015).

Aiempi tutkimus tunnistaa kybertoimintaympäristössä yhteistyön merkityksen eri tahojen toiminnassa kyberuhkia vastaan. Muun muassa Rizov (2018) sekä Goodwin ja Nicholas (2015) käsittelevät kyberuhkatiedon jakamisen merkitystä ja sen tuomaa hyötyä organisaatioiden suojautumisen kannalta. Kirjallisuuden pohjalta havaittiin, ettei kyberturvallisuuden kontekstissa käytetä juurikaan käsitettä tietovirrat, vaan samaan ilmiöön liittyviin asioihin viitataan ’tiedonjakamisen’ ja ’tiedonvaihdon’ käsitteillä (mm. Rizov, 2018; Skopik ym., 2016; Tounsi & Rais, 2017). Tässä tutkimuksessa käytetään sovelletusti molempia käsitteitä.

Toisaalta aiemmassa tutkimuksessa nousee esiin myös monia haasteita niin yleisen tietojohtamisen kuin kyberturvallisuuden näkökulmista. Muun muassa Riege (2005) sekä Vuori ym. (2019) ovat tutkineet tiedon jakamisen esteitä, joita organisaatioiden tietoperustaisessa toiminnassa tyypillisesti esiintyy. Parish ja Madahar (2016) ovat puolestaan kuvanneet kybertilannetietoisuuden muodostumiseen liittyviä haasteita sosioteknisen kybertoimintaympäristön kompleksisuudesta käsin. Skopik ym. (2016) uskovat, että kybertilannekuvatoiminteiden jalkauttamiseen liittyvät haasteet johtuvat siitä, että kyberturvallisuutta koskeva tiedonvaihto edellyttää monialaista tutkimusta, mitä oletetusti ei ole toiminnan kehittämisen kannalta kyetty riittävällä syvyydellä toistaiseksi toteuttamaan. Myös Lehdon ja Limnéllin (2021) tutkimus osoittaa, että kyberturvallisuuden ylläpidon kannalta erityistä huomiota tulisi kiinnittää koordinoinnista huolehtivaan toiminteeseen, mikä osaltaan liittyy tilannetietoisuuden muodostamiseen, jotta sen rooli palvelee organisaatioiden todellista tarkoitusta. Tiedonkeruu ja siihen perustuva päätöksenteko tapahtuu kuitenkin usein liian hitaasti suhteessa kybertoimintaympäristön muutosnopeuteen (Lehto & Limnéll, 2021), mikä osaltaan tekee kybertilannekuvan muodostamisesta mielenkiintoisen tutkimuskohteen.

Kirjallisuuskatsauksessa on pyritty ottamaan huomioon aihepiiriin keskeisesti vaikuttavat osatekijät niin tietojohtamisen kuin kybertoimintaympäristön osalta. Katsauksessa ei syvennytä yksityiskohtaisesti esimerkiksi tiettyihin teknisiin valvontaratkaisuihin, joista karkeasti ajateltuna muodostuu yksi tietovirta kybertilannetilannekuvan muodostamisen kannalta. Tarkoituksena on ennemmin hahmottaa kokonaiskuva, jolloin yleisluonteisessa katsauksessa korostuu tutkimuksen avoin suhtautuminen tietovirtojen ja niiden hallinnan lähtökohdista kybertilannekuvan muodostamisen kontekstissa. Vaikka aihetta lähestytään

yleisluonteisena katsauksena, pyritään haasteita tunnistamalla löytämään mahdollisia laajasti huomioitavia ja organisaatioiden toimintaa kehittäviä näkökulmia kybertilannekuvan muodostamisen kontekstissa niin organisaatioiden sisäisten toimintojen kuin verkostotoiminnan kannalta.

2 TIETO ORGANISAATIOIDEN TOIMINNASSA

Tässä luvussa käsitellään tietojohtamisen teoriaa, jota vasten tietovirtoja ja niiden hallintaa kybertilannekuvan muodostamisen kontekstissa peilataan tutkielman myöhemmässä vaiheessa. Tarkoituksena on luoda kokonaisvaltainen käsitys tiedon merkityksestä organisaatioiden toiminnassa ja siitä, miten organisaatiot voivat parhaiten hyödyntää tietoa ja luoda sillä arvoa omassa toiminnassaan.

Luvun ensimmäisessä osiossa käsitellään tietojohtamista, sekä lisäksi avataan tiedon määritelmää ja sen eri tasoja ja tiedon merkitystä organisaatioiden toiminnalle erilaisten tietoon liittyvien prosessien näkökulmista. Luvun lopussa käydään läpi tiedon organisaatioille synnyttämää arvoa, joka sidotaan tietovirtojen, tilannekuvan ja tilannetietoisuuden käsitteisiin, sekä lisäksi avataan lähdekirjallisuudessa esiin nousseita yleisimpiä haasteita liittyen organisaatioiden tietoperustaiseen toimintaan.

2.1 Tietojohtaminen

> [-] tieto ei ole nykyisin pelkästään kriittinen resurssi, vaan yhä useammin myös organisaatioiden tuottama lopputuote (Jalonen, 2015).

Viimeisiä vuosikymmeniä kuvastaa saatavilla olevan informaation määrän kasvu, mikä on edellyttänyt tiedon merkityksen tunnistamista laaja-alaisesti organisaatioiden toiminnassa. 1990-luvun puolivälissä syntyi näkemys, joka korostaa viestinnän, vuorovaikutuksen ja oppimisen keinojen hyödyntämistä ihmisiin sitoutuneen tiedon ja osaamisen valjastamiseksi organisaatioiden käyttöön. (Huotari ym., 2005, s. 49.) Tästä näkemyksestä syntyi tietojohtamisen teoria (engl. knowledge management), jonka taustalla on ajatus siitä, että organisaatioiden menestys on riippuvainen tiedon merkityksen ymmärtämisestä ja sen oikeanlaisesta hyödyntämisestä organisaatioiden toiminnassa (Laihonen ym., 2013).

Tietojohtaminen ulottuu moniin johtamisen osa-alueisiin, eikä sille ole olemassa yksiselitteistä määritelmää. Sen synonyymeinä on pidetty 'tietämyksen hallintaa', 'osaamisen johtamista' ja 'tietämyksen johtamista'. Tietojohtaminen eroaa tietohallinnosta (engl. information management), jolla viitataan tiedon alempaan abstraktiotasoon liittyvään toimintaan. Käytännössä tietohallinnolla tarkoitetaan siis *informaation* hallintaa, kun tietojohtamisessa on kyse laajemman kokonaisuuden strategisesta johtamisesta. (Huotari ym., 2005, s. 134–135.)

Tietojohtamisen teoreettisena lähtökohtana voidaan pitää muun muassa resurssi- ja tietoperustaisia käsityksiä organisaatioista. Tietoperustaisissa organisaatioissa informaatio- ja tietoresurssit ovat yhtä lailla toiminnan tuotoksia ja panoksia. Tietojohtaminen kytkeytyy tietopääoman (engl. intellectual capital) sekä osaamispääoman (engl. knowledge capital) hallintaan, jotka mielletään tietojohtamista laajemmiksi käsitteiksi. Tietojohtaminen voidaan nähdä toisaalta teoreettisena lähestymistapana, mutta samalla käytännön johtamismenetelmänä, jonka avulla voidaan hahmottaa tietopääomaan ja sen kehittämiseen liittyviä ilmiöitä ja hallita sen muodostumiseen vaikuttavia tekijöitä. Huotarin ym. (2005, s. 49) mukaan tietojohtamisen tavoitteena on hyödyntää yksilöllistä tietoa ja muuntaa se "koko työyhteisön, organisaation tai yhteistyöverkoston toiminnaksi". Pyrkimyksenä toisin sanoen on hyödyntää tätä organisaatioon ja yhteisöön sitoutunutta tietoa muun muassa organisaation suorituskyvyn ja strategisen osaamisen lisäämiseksi ja uuden tiedon luomiseksi sekä kehittää sellaisia toiminta- ja informaatioympäristöjä, jotka edistävät näiden toteutumista. Tietojohtamisen tehtävä on parantaa organisaatioissa ja sen sidosryhmissä tapahtuvaa arvonluomiskykyä. (Huotari ym., 2005, s. 49–50, 134–135 & 140.)

Laihonen ym., (2013) jakavat tietojohtamisen kahteen pääsuuntaukseen, joita ovat liikkeenjohdollinen ja tietotekninen suuntaus. Liikkeenjohdollisessa suuntauksena tieto nähdään organisaation menestystekijänä, ja sen keskeinen tehtävä on pyrkiä kehittämään erilaisia välineitä tietoon liittyvien johtamistehtävien suorittamiseksi. Tietoteknisessä suuntauksessa keskiöön puolestaan nousevat tietojärjestelmät, joiden avulla tietoa pyritään hallitsemaan. Laihonen ym. (2013) pitävät tätä jaottelua kuitenkin jokseenkin keinotekoisena. (Laihonen ym., 2013.)

Organisaatiot voivat toisaalta toteuttaa tiedolla johtamisen käytäntöjä eri tavoin, jotka voivat perustua esimerkiksi kodifiointi- tai personointistrategioihin. Strategiat eivät ole toisiaan poissulkevia, vaan niitä voidaan myös toteuttaa samanaikaisesti. Kodifiointistrategian mukaisesti toimivat organisaatiot tyypillisesti tukeutuvat eksplisiittiseen tietoon, joka on koodattu ja tallennettu erilaisiin tietojärjestelmiin tai dokumentteihin. Tällaista strategiaa noudattavissa organisaatioissa toiminta perustuu tiedon systemaattiselle uudelleenkäytölle ja tiedon organisointi, jakaminen ja soveltaminen tapahtuu tietojärjestelmien avulla. Personointistrategioissa painopiste on puolestaan ihmisten välisessä hiljaiseen tietoon ja kokemuksiin perustuvassa toiminnassa. Tietojärjestelmien rooli personointistrategiassa on toimia ihmisten välisen kommunikoinnin ja verkostoitumisen mahdollistajana. (Jalonen, 2015.)

Tietojohtamisessa tieto voidaan ymmärtää joko staattisena objektina (engl. static knowledge) tai tietämisen (engl. knowing) dynaamisena prosessina. Tieto on luonteeltaan eksplisiittistä silloin, kun se mielletään objektiksi eli erilaisten informaatioresurssien kaltaisiksi, kuten kirjallisiksi raporteiksi. Kun tiedosta puhutaan puolestaan dynaamisena prosessina, käsitetään tieto tällöin luonteeltaan sosiaalisena, jossa korostuu myös hiljaisen ja implisiittisen tiedon merkitys. Huotari ym. (2005, s. 50) puolestaan määrittävät tietojohtamisen kolmen ulottuvuutta, joita ovat (1) ihmisten johtaminen tiedon luojina ja tuottajina, (2) informaation hallinta tiedon luomisessa ja tuottamisessa sekä (3) näihin liittyvien prosessien tuloksellisuutta edistävien asioiden hallinta. Tietojohtamisessa tieto käsitetään sosiaalisena ja dynaamisena prosessina. (Huotari ym., 2005, s. 49–50.) Tiedon erilaisia määritelmiä käsitellään tarkemmin seuraavassa alaluvussa.

2.1.1 Tiedon määrittely

Tieto nähdään monimutkaisena määrittää ja siihen sisältyy monenlaisia elementtejä. Voidaan puhua datasta (engl. data), informaatiosta (engl. information) ja tiedosta tai tietämyksestä (engl. knowledge). Arkikielessä käsitteitä tieto ja informaatio käytetään usein toisilleen synonyymeinä, mutta teoreettisessa tarkastelussa niiden välillä tunnistetaan eroavaisuus. Datan voidaan ajatella olevan raaka-ainetta, josta informaatio syntyy. Data ei kuitenkaan itsessään pidä sisällään merkityksiä vaan se on irrallista tietoa, kuten merkkejä tai numeroita. Informaatio on puolestaan datasta johdettua tietoa, joka sisältää jonkin merkityksen. (Huotari ym., 2005, s. 38; Sydänmaanlakka, 2012, s. 187.)

Sydänmaanlakka (2012) viittaa kirjassaan *Älykäs organisaatio* Davenportin ja Prusakin (1998) näkemykseen datan muuttumisesta informaatioksi; näin tapahtuu, kun se on:

- kytketty kokonaisuuteen
- analysoitu
- korjattu
- tiivistetty (Sydänmaanlakka, 2012, s. 188).

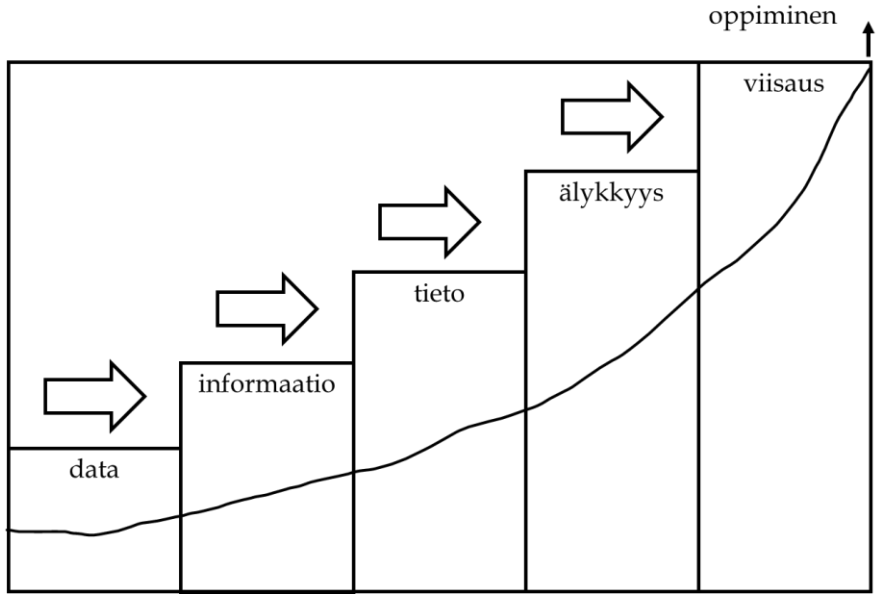
Tällöin informaatio nähdään osana laajempaa kokonaisuutta, sen merkitys ymmärretään sekä dataan liittyvät virheet on korjattu ja se on esitetty selkeämmässä muodossa. Informaatio kuvataan tyypillisesti *viestiksi*, jolla on lähettäjä ja vastaanottaja. Informaation eli viestin on tarkoitus muuttaa vastaanottajan tulkintaa jostain asiasta sekä vaikuttaa tämän harkintaan ja käyttäytymiseen (Davenport & Prusak, 1998). Informaatio voi muuttua tiedoksi, kun joku henkilö on ottanut sen vastaan. Huotari ym. (2005, s. 39) mukaan ”tieto (engl. knowledge) syntyy, kun informaation vastaanottaja tulkitsee informaation ja hyväksyy tulkintansa, jolloin se yhdistyy osaksi hänen tietorakennettaan ja muuttaa sitä.” (Huotari ym., 2005, s. 38–39; Sydänmaanlakka, 2012, s. 187–189.)

Sydänmaanlakka (2012, s. 189) viittaa Davenportin ja Prusakin (1998) määritelmään tiedosta, joka avaa käsitteen moniulotteisuutta:

> Tieto on jäsentyneiden kokemusten, arvojen, informaation ja oivalluksien sekoitus, joka tarjoaa viitekehyksen arvioida uusia kokemuksia ja informaatiota. Tieto syntyy ja sitä sovelletaan tietäjän mielikuvissa. Organisaatiossa tieto on usein sidottu dokumentteihin, rutiineihin, prosesseihin, toimintatapoihin ja normeihin. (Sydänmaanlakka, 2012, s. 189.)

Huotari ym. (2005, s. 39) ja Sydänmaanlakka (2012, s. 189) ovat yhtä mieltä siitä, että tietoon liittyy olennaisesti ihmisen ymmärrys itsestään ja ympäröivästä maailmasta sekä myös yksilön henkilökohtaiset kokemukset. Tämän näkemyksen mukaan tieto sijaitsee ihmisissä, ja siten ilman ihmisen tulkintaa ja merkityksellistämistä tietoa ei itsessään olisi. Tästä yksilöllisestä tiedosta tulee informaatiota, kun se viestitään toiselle, jolloin informaation lähettäjälle kyseessä on ”viestitty tieto” ja käänteisesti vastaanottajalle se on tulkittua informaatiota. (Huotari ym., 2005, s. 39; Sydänmaanlakka, 2012, s. 187–189.)

Tiedon tasot ja ymmärryksen rakentuminen luovat pohjan tietojohtamisen peruskäsitteistölle (Laihonen ym., 2013). Yksi tapa määrittää näiden käsitteiden suhdetta on tiedon arvoketju (engl. value chain of information), jossa datan ajatellaan jalostuvan informaatioksi ja informaation edelleen tiedoksi ihmisten käyttöön. Sydänmaanlakka (2012) puolestaan viittaa tiedon hierarkiaan (kuvio 1) mallintaessaan datan, informaation ja tiedon suhdetta, josta saattaa muodostua oppimisen ja kokemusten kautta älykkyyttä sekä lopulta viisautta. (Huotari ym., 2005, s. 38; Sydänmaanlakka, 2012, s. 187–192.)



KUVIO 1 Tiedon hierarkia (mukaillen Sydänmaanlakka, 2012, s. 118).

Tiedon määrä kasvaa mitä ylemmäs portaikossa siirrytään (kuvio 1). Myös oppiminen kasvaa mitä syvemmästä tiedon tasosta puhutaan. Älykkyydellä (engl. intelligence) tarkoitetaan tiedon hyödyntämistä oikeaan aikaan, oikeisiin ratkaisuihin, valintoihin ja päätöksiin. Viisauteen (engl. wisdom) liittyvät tiiviisti yksilön arvot, moraalikäsitys sekä kokemukset. Viisaus on siten jotain

syvällisesti sisäistettyä, itse sovellettua ja testattua tietoa. Älykkyyttä ja viisautta käsitellään toimintaa ohjaavina tiedon lajeina, jotka heijastavat yksilöiden ominaisuuksia, kuten arvoja ja henkilökohtaisia kokemuksia. (Sydänmaanlakka, 2012, s. 190–191.)

Tiedon arvoketjun ja hierarkian lisäksi tietoa voidaan mallintaa ulottuvuuksina. Nonaka ja Takeuchi (1995) perustavat tietoa ja tiedon luomista käsittelevät teoriansa episteemisen ja ontologisen tiedon ulottuvuuksiin. Ontologinen lähestymistapa käsittää, että tieto syntyy vain ja ainoastaan ihmisissä yksilöinä, eivätkä organisaatiot voi luoda tietoa ilman heitä. Nonakan ja Takeuchin (1995) episteeminen lähestymistapa perustuu Polanyin (1966) erotteluun hiljaisesta (engl. tacit) ja eksplisiittisestä (engl. explicit) tiedosta, mikä toimii tyypillisenä tiedon jaottelumallina. Hiljainen tieto on henkilöön sitoutunutta ja tiettyyn kontekstiin liittyvää tietoa, ja siten se on hankala muuttaa formaaliin muotoon tai viestiä. Nonaka ja Konno (1998) edelleen jakavat hiljaisen tiedon kahteen ulottuvuuteen – tekniseen ja kognitiiviseen. Teknisellä ulottuvuudella viitaan usein yksilön epämuodolliseen tietotaitoon (engl. know-how), kun taas kognitiivinen ulottuvuus muodostuu meihin sisäänrakennetuista uskomuksista, ajatuksista, arvoista ja mentaalimalleista (Nonaka & Konno, 1998). Eksplisiittinen tieto puolestaan tarkoittaa tietoa, joka on siirrettävissä formaaliin, systeemiseen muotoon. Nonaka & Takeuchi (1995, s. 61) eivät näe näitä toisistaan erillään olevina, vaan toisiaan täydentävinä kokonaisuuksina. (Sydänmaanlakka, 2015, s. 192; Nonaka & Takeuchi, 1995, s. 59–61.)

Hiljaisen ja eksplisiittisen tiedon lisäksi Choo (2001, s. 198) esittää kulttuurisen tiedon käsitteen (engl. cultural knowledge). Sillä tarkoitetaan tiettyyn joukkoon, kuten työyhteisöön, kuuluvien jäsenten olettamuksia, uskomuksia ja käytäntöjä, joilla annetaan arvo ja merkitys uudelle tiedolle tai tietämykselle ja joiden varassa yhteisön jäsenet selittävät ja ymmärtävät yhteisönsä todellisuutta. Kulttuurinen tieto luo yhteistä tulkintapohjaa ja samalla edistää informaation välittymistä ja tiedon jakamista yhteisössä. (Choo, 2001, s. 198; Huotari ym., 2005, s. 69.) Eksplisiittisen ja hiljaisen tiedon väliin usein sijoitetaan myös implisiittinen tieto (engl. implicit knowledge), jota joidenkin käsitysten mukaan voidaan ilmaista kielellisesti, mutta tällöin hiljaista tietoa ei (Huotari ym., 2005, s. 67).

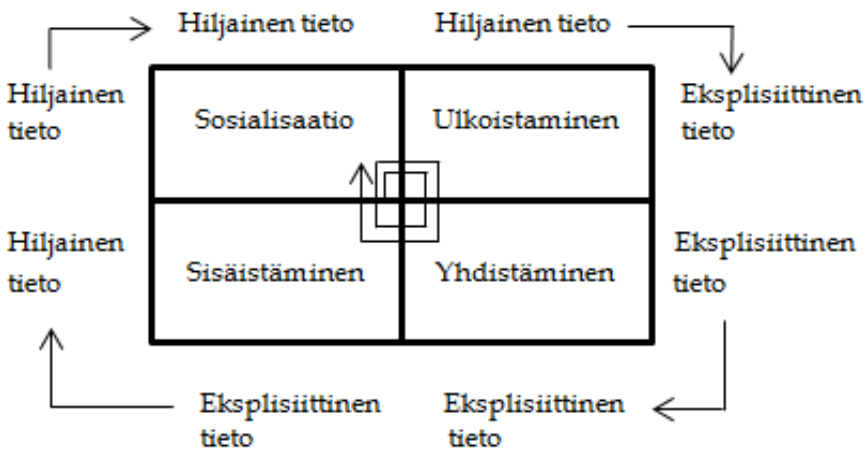
2.1.2 Tiedon muuttumisprosessi

Nonaka ja Takeuchi (1995, s. 62) esittävät, että organisaatiossa tietoa syntyy hiljaisen ja havaittavissa olevan tiedon vuorovaikutuksessa. Tästä ajatuksesta he loivat tiedon nelikenttä mallin eli SECI-mallin, joka kuvastaa uuden tiedon syntymistä tai muuntumista (engl. knowledge conversion). Mallin neljä vaihetta ovat:

- sosialisaatio (engl. socialization)
- ulkoistaminen (engl. externalization)
- yhdistäminen (engl. combination)

- sisäistäminen (engl. internalization). (Nonaka & Takeuchi, 1995, s. 62.)

Nonakan ja Takeuchin (1995, s. 61) näkemys painottaa tiedon muuntumista yksilöiden välisenä sosiaalisena prosessina sen sijaan, että se rajoittuisi pelkästään yksilöön itseensä. Malli voidaan siten nähdä tiedon luomisen dynaamisena prosessina, jossa hiljaisen ja eksplisiittisen tiedon välinen jatkuva dialogi synnyttää uutta tietoa ja vahvistaa sitä ontologian eri tasoilla (yksilö, organisaatio ja organisaatioiden välinen) (Farnese, Barbieri, Chirumbolo & Patriotta, 2019). Kuviossa 2 esitetään nämä SECI-mallin neljä vaihetta.

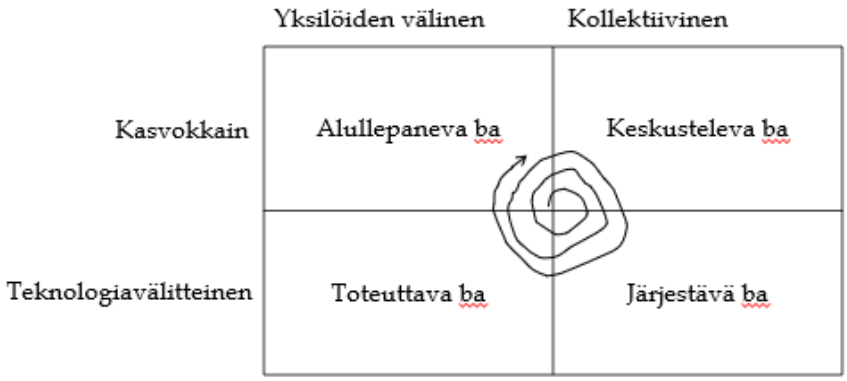


KUVIO 2 SECI-malli Pullin (2018) pro-gradu -tutkielmassa *Tiedolla johtamisen kehittäminen* (mukaillen Nonaka & Takeuchi, 1995, s. 62 & 71).

Sosialisaatiossa on kyse tyypillisestä mestari-oppipoika-asetelmasta, jossa oppiminen tapahtuu seuraamalla, matkimalla ja tekemällä. Sosialisaatiossa hiljainen tieto muuttuu toisen yksilön hiljaiseksi tiedoksi kokemuksia jakamalla ja tehdessä oppimalla. Sydänmaanlakan (2012, s. 193) mukaan "sosialisaatiossa ei siirretä vain tietoja ja taitoja, vaan myös alalle liittyviä toimintamalleja, normeja ja arvoja." Hiljainen tieto voi välittyä yksilöltä toiselle vain, jos heidän välillään vallitsee yhteinen kokemus. Nonakan ja Takeuchin (1995, s. 63) mukaan ilman tätä yhteistä kokemusta henkilön on äärimmäisen vaikeaa heijastaa itsensä toisen ihmisen ajatteluprosessiin. Ulkoistaminen puolestaan tarkoittaa hiljaisen tiedon muuttumista eksplisiittiseen muotoon eli toisin sanoen siinä yksilöiden hiljainen tieto muuttuu konkreettisesti käsiteltävään muotoon, kuten erilaisiksi dokumenteiksi tai asiakirjoiksi. Ulkoistaminen nähdään organisaatioille erityisen arvokkaana, sillä se mahdollistaa tiedon tehokkaamman jakamisen. Yhdistämisellä tarkoitetaan prosessia, jossa eri eksplisiittiset tiedot liitetään laajemmiksi kokonaisuuksiksi, kuten osaksi tietojärjestelmiä. Yhdistelyllä tarkoitetaan Sydänmaanlakan (2012, s. 194.) mukaan myös tiedon jalostumista. SECI-mallin viimeinen vaihe pitää sisällään eksplisiittisen tiedon sisäistämisen siten, että se muuttuu jälleen yksilön

hiljaiseksi tiedoksi. Sisäistämisen vaiheessa yksilö ikään kuin määrittää tiedon uudelleen, mikä alkaa ohjata yksilön toimintaa myös tiedostamatta. (Sydänmaanlakka, 2015, s. 193; Nonaka & Takeuchi, 1995, s. 62–63.)

Uuden tiedon luomiseen liittyy myös vuorovaikutuksen mahdollistavat olosuhteet, josta Nonaka ja Konno (1998) puhuvat ba-käsitteenä. Kuviossa 3 on kuvattu käsitteen eri tyypit. Ba tarjoaa ikään kuin alustan yksilöllisen ja jaetun tietämyksen edistämiseen, ja se voi olla henkinen (jaettu kokemus), virtuaalinen (erilaiset tietojärjestelmät) tai fyysinen (kokoustila) konteksti, tila tai myös niiden yhdistelmä. Ba mukailee SECI-mallin neljää vaihetta. (Nonaka & Konno, 1998.)



KUVIO 3 Ba-käsitteen tyypit (mukailtu Nonaka & Konno, 1998; Huotari ym., 2005, s. 141).

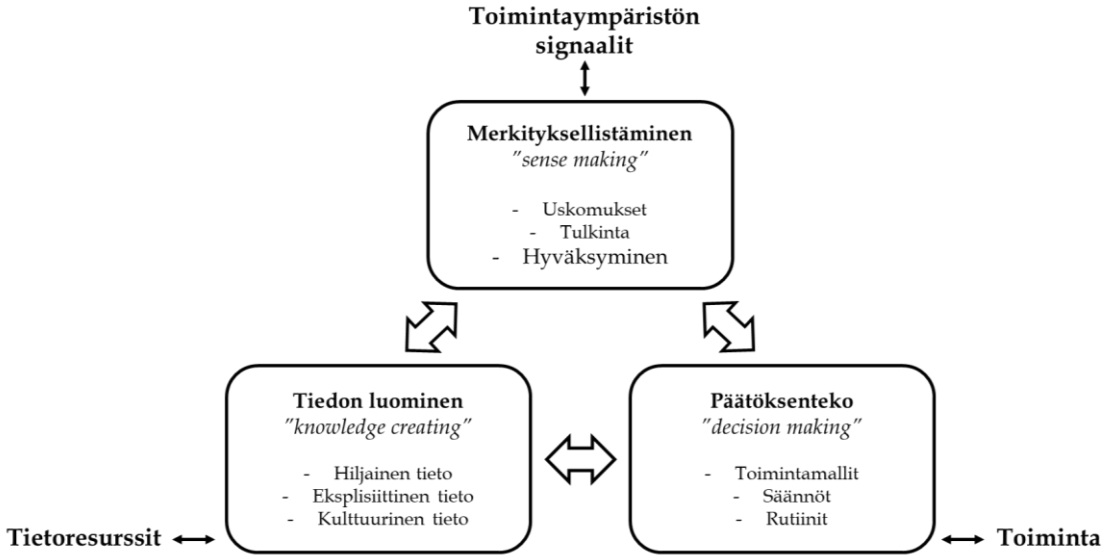
Ba on siis yhteinen konteksti, jossa toiminnan osapuolet ovat keskenään vuorovaikutuksessa. Alullepanevassa ba:ssa organisaation tai jonkin muun joukon jäsenet sosiaalistuvat tiedon luomiseen jakamalla yksilöllisiä ajatuksiaan ja kokemuksiaan. Alullepaneva ba vaatii kasvokkain viestintää, sillä siinä syntyy muun muassa luottamuksen ja sitoutumisen tunteet, ja sitä voidaan pitää perustana esimerkiksi tiedon jakamiselle. Keskustelevassa ba:ssa yksilöt jakavat hiljaista tietoaan ja pyrkivät muuttamaan sen yhteiseksi ymmärrykseksi. Keskusteleva ba on usein tietoisemmin muodostettu kuin alullepaneva ba. Keskusteleva ba liittyy SECI-mallin ulkoistamisvaiheeseen. Järjestävä ba puolestaan mahdollistaa tiedon yhdistämisen. Se on virtuaalinen vuorovaikutuksen tila, joka yhdistää uuden eksplisiittisen tiedon olemassa olevaan tietovarantoon, kuten erilaisiin tietokantoihin. Toteuttava ba puolestaan tukee luodun tiedon sisäistämistä tekemällä oppimisen -periaatteen kautta. (Huotari ym., 2005, s. 140–142; Nonaka & Konno, 1998.)

2.1.3 Organisaation tietoprosessit

Nonaka ja Takeuchi (1995, s. 59) näkevät tiedon luomisen organisaatioissa prosessina, jossa organisaatio pyrkii vahvistamaan yksilöissä syntyvää tietoa ja kiteyttämään sen osaksi organisaation tietoverkostoa (engl. knowledge network of the organization). Prosessi tapahtuu ikään kuin laajenevassa vuorovaikutus-

yhteisössä, joka ylittää niin organisaation sisäiset kuin organisaatioiden välisetkin tasot ja rajat. (Choo, 1998, s. 1–2; Nonaka & Takeuchi, 1995, s. 59.)

Choo (2006) jaottelee organisaation tietoprosessit kolmeksi toisiinsa linkittyväksi kokonaisuudeksi, jotka on havainnollistettu kuviossa 4. Nämä prosessit voivat toisaalta tukea toisiaan, mutta samalla toimia hidasteena tai esteenä organisaation tietoperustaiselle toiminnalle. (Choo, 2006, s. 249.)



KUVIO 4 Organisaation tietoprosessit (mukailtu Choo, 2006, s. 250).

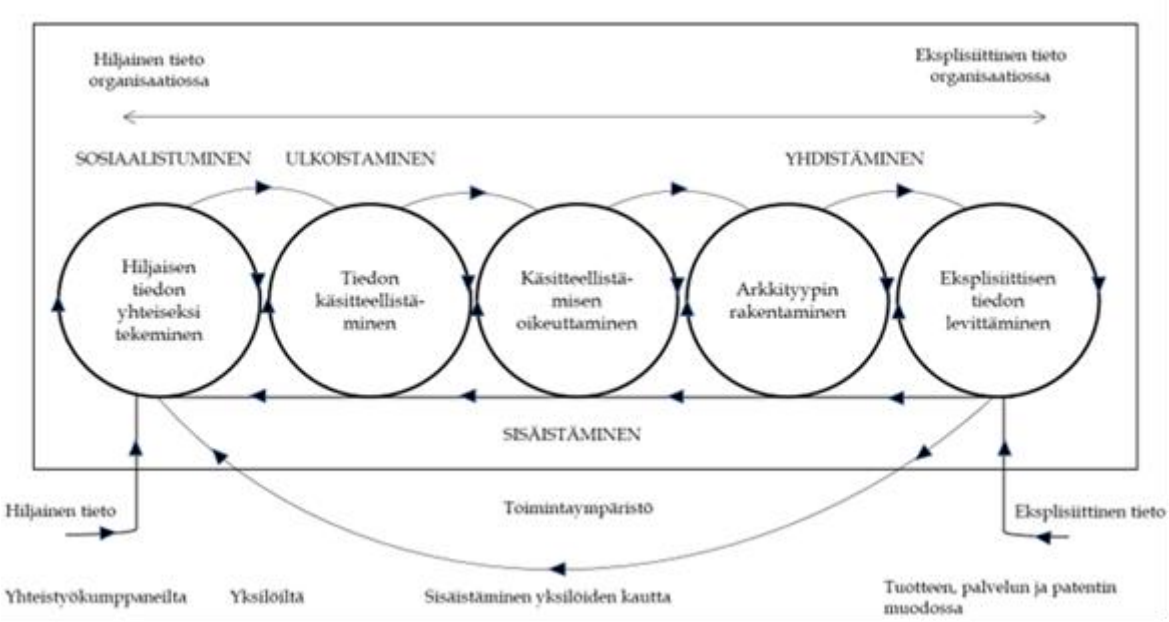
Merkityksellistämisellä tarkoitetaan toimintaympäristössä havaittujen muutosten tai uusien signaalien tunnistamista ja tulkintaa organisaatioon liittyvien uskomusten ja aiemman tietämyksen ja kokemusten kautta. Tuotoksena on käsitys havaitusta ongelmasta tai mahdollisuudesta. Tiedon luomisen prosessi puolestaan käynnistyy, kun organisaatio tunnistaa toiminnassaan merkittävän tietoaukon (engl. knowledge gap), joka halutaan täyttää, tai se kohtaa uudenlaisen ongelman, jonka ratkaisemiseksi tarvitaan uutta tietoa. Tiedon luomiseen hyödynnetään kaikkia mahdollisia tietoresursseja. Prosessin tavoite on kehittää uudenlaisia näkemyksiä tai kyvykkyyksiä, joilla organisaatio pystyy vastaamaan tunnistettuun ongelmaan tai haasteeseen. Tiedon luomisen prosessi toimii yhtenä päätöksentekoprosessin mahdollistajana. Päätöksenteko pohjautuu aiempien sääntöjen ja normien kunnioittamiseen, mutta toisaalta siihen liittyy keskeisesti myös kyky tunnistaa milloin vanhat olettamukset eivät enää sovellu tarvittavien toimenpiteiden toteuttamiseen ja on tarve luoda uusia toimintatapamalleja ja ohjeita. (Choo, 2006, s. 249–250.)

Tiedon luominen ja sen hyödyntäminen ovat Choon (1998, s. 2) mukaan erityinen organisatorinen haaste. Tieto ja asiantuntemus ovat yleensä hajautettu ympäri organisaatiota ja ovat usein tiiviisti sidottu yksittäisiin henkilöihin. Ilman selkeää ymmärrystä organisaation tietoprosesseista, joiden kautta tieto muuttuu oivallukseksi, tietämykseksi ja edelleen toiminnaksi, ei organisaatio

pysty hyödyntämään tietoresurssiensa ja -teknologioidensa todellista arvoa (Choo, 1998, s. 1–2).

Nonaka ja Takeuchi (1995) ovat jalostaneet tiedon luomisen prosessimallia siten, että se huomioisi myös yksilöä ja ryhmää laajemmin useampia toimintatasoja työyhteisöissä, organisaatioissa tai yhteistyöverkostoissa. He viittaavat monitasoisella tiedon luomisella työyhteisön kykyyn luoda uutta tietoa ja levittää sitä organisaation eri toiminnan tasoille. (Huotari ym., 2005, s. 125). Tämä monitasoinen tiedon luomisen malli on kuvattu kuviossa 5. Malli perustuu tiedon muuntumiseen SECI-prosessissa ja se muodostuu viidestä vaiheesta:

1. hiljaisen tiedon yhteiseksi tekeminen
2. hiljaisen tiedon käsitteellistäminen
3. käsitteellistämisen oikeuttaminen
4. arkkityypin rakentaminen
5. uuden eksplisiittisen tiedon levittäminen (Huotari ym., 2005, s. 126–217).



KUVIO 5 Monitasoinen tiedon luomisen malli (mukailtu Huotari ym., 2005, s. 125; Nonaka & Takeuchi, 1995, s. 84).

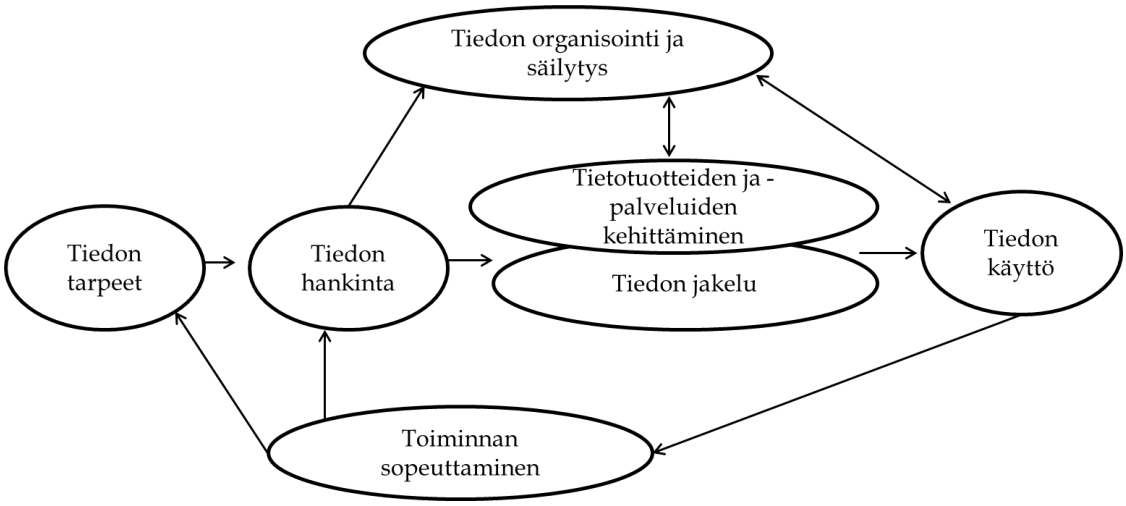
Monitasoisen tiedon luomisen mallissa tieto ikään kuin kumuloituu tasolta toiselle, ja työyhteisön on myös kyettävä sitomaan uusi tieto organisaation toiminnan rakenteisiin, käytänteisiin ja järjestelmiin, sekä niissä tuottaviin palveluihin ja tuotteisiin (Huotari ym, 2005, s. 125).

2.1.4 Tiedonhallintaprosessi

Englanninkielisellä termillä 'information management' voidaan viitata suomeksi joko tietohallintoon tai tiedonhallintaan. Tietohallinnon käsitteellä Huotarin ym. (2005) mukaan "kuvataan informaatioon kytkeytyvää toimintaa

organisaatioympäristössä ja siihen liittyvien ilmiöiden monitieteellistä tutkimusta" (Huotari ym., 2005, s. 47). Informaatiotutkimuksessa tietohallinnolla viitataan laajempaan näkökulmaan organisaation käytössä olevista informaatioresursseista, joihin kuuluu myös ihmisiltä saatava tieto joko organisaation sisältä tai ulkopuolisista lähteistä. Tämä näkemys pitää sisällään myös informaatioresurssien hallinnan. Tiedonhallinnassa (myös tiedon hallinta) Huotarin ym. (2005) mukaan on puolestaan kyse informaation hallinnasta "eri yhteyksissä osana yksilöiden, ryhmien, organisaatioiden ja yhteisöjen toimintaa". (Huotari ym., 2005, s. 47–48).

Organisaatioiden tiedonhallintaa voidaan kuvata vaiheittaisella mallilla (engl. process model of information management), joka on esitetty kuviossa 6. Tässä Choon (1998) kehittämässä mallissa huomioidaan tiedonhallinnan (engl. information management) monivivahteisuus, jossa yhdistyvät niin tietoresurssien, teknologioiden kuin toimintatapojen ja normien hallinta. Choon (1998, s. 260) mukaan näistä rakentuu tiedon hallinnan muodollinen infrastruktuuri; eli toisin sanoen se, miten tietoa tuotetaan ja miten se muuntuu organisaatiossa, tapahtuu tämän infrastruktuurin kautta. Tiedon tuottaminen ja muuntuminen heijastaa organisaatiokulttuuria ja sen määritelmiä sisäisistä rooleista, rutiineista ja säännöistä. Choo (1998, s. 260) kuitenkin painottaa, että muodollisesta infrastruktuurista huolimatta viime kädessä tiedon ja sen merkitys on sidottu yksilön ajatuksiin, tunteisiin ja toimintaan. (Choo, 1998, s. 260–261.)



KUVIO 6 Tiedonhallinnan prosessi (mukailtu Choo, 1998, s. 261; Huotari ym. 2005, s. 56).

Tiedonhallinta voidaan nähdä useista aliprosesseista koostuvien prosessien kokonaisuutena tai verkostona, joiden tehtävä on omaksua (engl. acquire), luoda (engl. create), jäsentää (engl. organize), jakaa (engl. distribute) ja käyttää tai hyödyntää (engl. use) tietoa. Tiedonhallinnan prosessi kytkeytyy aiemmin kuvattuihin organisaation tietoprosesseihin (kuvio 4). Tiedonhallinnan prosessi käynnistyy, kun jokin tietotarve nousee esille esimerkiksi ratkaistavan ongelman tai päätöksentekotarpeen seurauksena. Prosessin lähtökohtana on

tietotarpeiden tunnistaminen. Toinen vaihe liittyy tiedon hankintaan, joka on joko säännöllistä tai kertaluonteista sidottuna johonkin tiettyyn tarpeeseen (Laihonen ym., 2013). Tiedonhankinnassa keskeistä on, että käytössä on riittävän laaja tietolähteiden joukko, mutta toisaalta näistä on kyettävä valitsemaan oman toiminnan ja tietotarpeiden kannalta tärkeimmät tietolähteet, joiden kautta hankitaan säännöllisesti tietoa. Hankittu tieto organisoidaan ja taltioidaan sisäisiin tietojärjestelmiin tarkoituksenmukaisesti, jotta se on tarvitsijoidensa saatavilla. Samalla se muodostaa niin sanotun organisaatiomuistin, joka tarkoittaa organisaation järjestettyä tietämystä.

Huotarin ym. (2005, s. 58) mukaan organisaatiomuisti on ”yksilökeskeinen ja toisaalta yhteisesti jaettu menneisyyttä tallentava prosessi, joka vaikuttaa organisaation oppimiseen ja päätöksentekoon”. Organisointi mahdollistaa tiedonhaun sekä tiedon käytön ja jakelun. Tietotuotteiden ja -palveluiden tarkoituksena on tuottaa lisäarvoa, joka edistää tiedon käyttöä. Periaatteena on, että informaatiota ja tietoa yhdistellään ja jalostetaan sen käyttötarkoituksen ja -tarpeen mukaan. Tietotuotteet ja -palvelut nähdään välttämättöminä päätöksenteon kannalta, sillä päätöksenteko edellyttää prosessoitua tietoa. Tiedon jakelun kannalta oleellista on, että tietotuotteet on toteutettu ja kohdennettu siten, että ne vastaavat käyttäjien tietotarpeita. Tietoa käytetään ja sovelletaan muun muassa ongelmatilanteissa ratkaisun löytämiseen ja päätöksentekoon sekä hyödynnetään myös uuden tiedon luomiseen. Toiminnan sopeuttamisella viitataan toimintaympäristössä tunnistettuihin muutoksiin sopeutumiseen. (Huotari ym. 2005, s. 57–60; Choo, 1998, s. 261–270.)

Tavoitetilassa tiedon tehokkaan hyödyntämisen lopputuloksena on mukautuva toiminta, jolla tarkoitetaan sellaisten toimintamallien valintaa ja toteuttamista, jotka perustuvat organisaation tavoitteisiin, mutta vastaavat myös senhetkisiin ympäristön vaatimuksiin. Organisaation vaste on vuorovaikutuksessa toisten samassa ympäristössä toimivien organisaatioiden kanssa luoden uusia osallistavia signaaleja ja viestejä, joista voi muodostua uusia tiedon hyödyntämisen kehiä ja näin tiedonhallinnan prosessi käynnistyy uudelleen. (Choo, 1998, s. 261; Huotari ym., 2005, s. 60.)

2.2 Tietovirrat

Tietovirroilla tarkoitetaan yleisesti prosessia, jossa erilaisista tapahtumista syntyvää informaatiota välitetään lähettäjältä vastaanottajalle. Ahlavuon, Hyypän ja Haggrenin (2011) mukaan tietovirrat (tai kommunikaatiovirrat) ovat erilaisten prosessien avulla siirrettyä tietoa yksilöiden, ryhmien, eri organisaatioiden tai tietovarantojen välillä. Prosessi kytkeytyy vahvasti tiedon käsitteeseen ja sen muuntumisprosessiin datasta informaatioksi ja edelleen tiedoksi ja tietämykseksi. Laihosen (2011) mukaan ”tiedonkulku tai tarkemmin tietovirrat nähdään keskeisenä tekijänä muutettaessa organisaation tietoresursseja arvoksi”. Tietovirtoja on erilaisia ja ne edellyttävät erilaisia organisatorisia työkaluja ja tiedon siirtämisen käytäntöjä. Lähtökohtana on, että hiljaisesta aineettomasta

tiedosta saadaan tehtyä näkyvää, eksplisiittistä tietoa. Tämä on mahdollista vain, jos yksilöiden ja organisaation tiedolla on konkreettinen kanava tai ilmentymä, jossa tieto muuntuu kommunikoitavaan muotoon. (Jalonen, 2015; Laihonen, 2011.) Tässä muun muassa Choo (1998, s. 264) korostaa ihmisresursseja koko tietovirtaprosessien mahdollistajana.

Tietovirtojen ensisijainen tehtävä on mahdollistaa suorituskyvyn ja asiantuntemuksen siirtyminen ajassa, paikassa ja tarvittaessa myös organisaatioiden välillä sinne, missä sitä tarvitaan (Nissen, 2002). Tietovirtoihin liittyy monia osatekijöitä, joita voidaan tarkastella organisaation eri tasoilla. Ahlavuo ym. (2011) yhdistävät tietovirtoihin muun muassa tiedon jalostamiseen ja jakamiseen, tietämyksen visualisointiin, esittämiseen ja analysointiin sekä lisäksi toimintatapoihin, tietovarantoihin, tiedonkulkuun ja tiedon lajeihin liittyviä osatekijöitä. Lisäksi yhtenä keskeisenä osatekijänä vaikuttaa toimijoiden välinen luottamus (Laihonen, 2011). Koska tietovirtoihin liittyy niin monia eri osatekijöitä, on tietovirtojen tarkastelu nähtävä hyvin moninaisena kokonaisuutena. Yleisesti ongelmana on, ettei tieto tai tietämys ole jakautunut organisaatiossa tasaisesti (Nissen, 2002). Vaikka tietovirtojen ja niiden hallinnan merkitys organisaation menestyksen kannalta on kiistämätön, on tietovirtoja itsessään kuitenkin tutkittu varsin vähän (Ahlavuo ym., 2011).

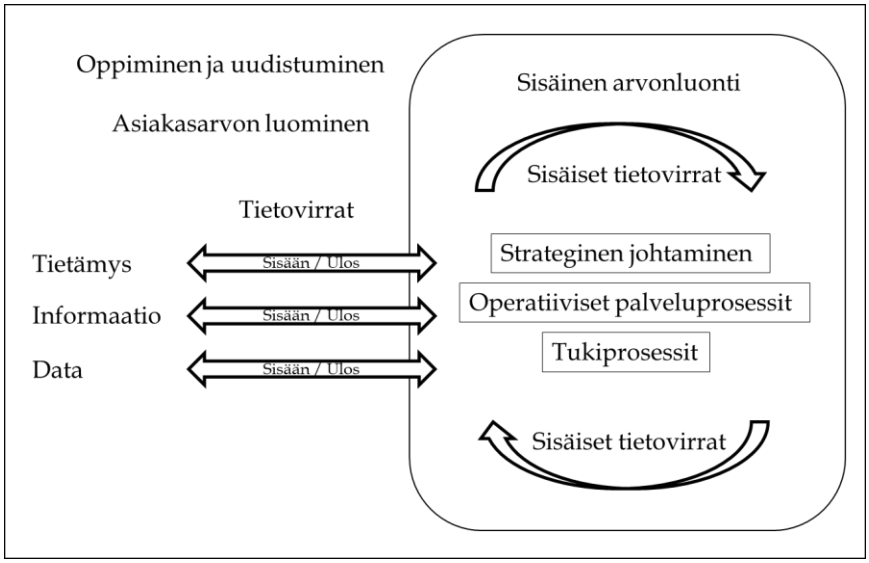
Laihosen (2011) mukaan tietovirrat voidaan mieltää itsessään organisaation työkaluksi, jonka avulla arvoverkon kompleksista toimintaympäristöä voidaan pyrkiä jäsentämään. Arvoverkolla voidaan tarkoittaa esimerkiksi viranomaisten muodostamaa verkostoa jollakin tietyllä toimialalla tai yritysmaailmassa asiakkaista, alihankkijoista ja muista eri sidosryhmistä muodostuvaa liiketoiminnan kannalta keskeistä verkostoa. Keskittymällä toimijoiden välisiin vuorovaikutussuhteisiin, voidaan arvoverkon kompleksista rakennetta ymmärtää paremmin. Laihosen (2011) mukaan vuorovaikutussuhteissa on nimenomaan kyse tietovirroista, ja niiden johtaminen tulisi nähdä keskeisenä tekijänä suoristuskykyistä ja tuloksellista arvoverkkoa rakennettaessa. Ajatus on ymmärrettävissä maalaisjärjellä: tehokas tiedonkulku parantaa organisaation tuottavuutta ja on siten nähtävissä keskeisenä arvonluonnin lähtökohtana. Tietovirtoja voidaan myös tarkastella organisaation toimintakokonaisuuden alisysteeminä, jossa johtamisessa tarvittavien ja tuotettavien tietojen rakennetta kuvataan usein tietomalleina tai tiedonhallintaprosesseina (Kuusisto & Kuusisto, 2006). Kuusiston ja Kuusiston (2006) mukaan tällöin ”tietovirrat muodostuvat tietomallien sekä tiedonhallintaprosessien tuottamista ja tarvitsemista tietosisällöistä”.

Kuusisto ja Kuusisto (2006) korostavat tarvetta kiinnittää huomiota tiedon lähettäjän ja vastaanottajan mahdollisuuksiin ymmärtää toisiaan mitä monipuolisemmaksi johtamisessa tarvittavien ja tuotettavien tietovirtojen rakenne kehittyy. Ymmärtämisen edellytyksenä on, että tietoa lähettävän ja vastaanottavan yksilön tai yhteisön välillä vallitsee yhteinen ja jaettu käsitys siitä, mitä tieto yksilön tai yhteisön välisessä toiminnallisessa kulttuurissa merkitsee. Kuusisto ja Kuusisto (2006) viittaavat tähän *tietoalkion* käsitteellä. Tietomallia, tiedonhallintaprosessia tai koko tietosisältöä ei tarvitse jakaa, vaan se riittää, että yhtei-

nen tietoalkio on olemassa yhteistoimintaa varten. (Kuusisto & Kuusisto, 2006.) Jos yhteinen tietoalkio kuitenkin puuttuu, voi sillä olla moninkertaisia vaikutuksia yhteistoiminnan kannalta, kun tiedon todellista arvoa tai merkitystä ei tunneta.

Tietovirtoja voidaan myös tarkastella joko yksittäisinä tiedonsiirtotapahtumina tai osana kompleksisempaa vuorovaikutustilannetta, jolloin ne ovat joko yksi- tai kaksisuuntaisia. Peruslähtökohtana on aina, että tietovirta on vuorovaikutuksen konkreettinen ilmentymä ja sen avulla – ikään kuin kuljettimena – tieto siirtyy lähettäjältä vastaanottajalle. Tällöin yksinkertaisimmillaan tietovirta voi olla yksisuuntainen. Saatuun tietoon (tietovirtaan) kuitenkin usein vastataan (palaute), jolloin syntyy vastakkaissuuntainen tietovirta. Vuorovaikutustilanteissa on siten tunnistettavissa yksinkertaisimmillaan kaksisuuntaisia tietovirtoja. Laihosen (2011) mukaan ”tietovirta voi toimia joko vuorovaikutuksen käynnistävänä impulssina tai palautteena johonkin aikaisempaan tietovirtaan”. Mitä moniulotteisemmasta vuorovaikutustilanteesta on kyse, sitä vaikeammaksi ymmärtää ja ennustaa kokonaisuus muuttuu. (Laihonen, 2011; Ahlavuo ym. 2011.)

Tietovirtoja tarkasteltaessa on tärkeää selvittää kuka tietoa siirtää ja kenelle (lähettäjä ja vastaanottaja), mitä tietoa siirretään ja missä yhteydessä sekä mikä on paras keino tai kanava halutun tiedon siirtämiseen (Laihonen, 2011). Tietovirtojen kannalta tietotekniikka on lisännyt tehokkuutta, sillä se on mahdollistanut suurten tietomäärien tallentamisen digitaaliseen muotoon ja siten myös lisännyt tiedon nopeampaa saatavuutta (Ahlavuo ym., 2011). Saatavuuteen liittyy olennaisesti se, että tietotarve tulee olla määritelty ja rakenteellisesti suunniteltu (Kuusisto, 2005). Kuusiston (2005) mukaan ”saatavilla ja käytettävissä olevalla tiedolla on käyttäjille jokin tarkoitus – ja sen pitää olla käytettävissä silloin, kun sitä tarvitaan”. Riippuen tietovirrasta tarvitaan erilaisia välineitä ja tiedon siirtämisen käytänteitä. Esimerkiksi tietojärjestelmiä tarvitaan datan ja informaation välittämiseen mahdollisimman nopeasti ja häiriöttömästi, kun tietämyksen (engl. knowledge) ja kokemuksellisen tiedon siirtämiseen puolestaan tarvitaan rikkaampia menetelmiä, kuten kasvokkain pidettäviä tapaamisia. (Laihonen, 2011; Jalonen, 2015.) Kuvion 7 viitekehyksestä käy ilmi yksinkertaistetusti, miten organisaation tietovirrat muodostuvat.



KUVIO 7 Laihosen (2011) esittämä viitekehys organisaation tietovirtojen tunnistamiseksi ja analyysin tueksi.

Viitekehys kuvaa yhtä organisaatiota sen toimintaympäristössä. Siinä tietovirrat on jaoteltu organisaation sisäisiin sekä ulos- ja sisäänpäin suuntautuviin tietovirtoihin. Sisäiset tietovirrat ovat keskeinen osa organisaation sisäistä arvonluontia sen omista tietoresursseista käsin. Tietovirrat, jotka suuntautuvat organisaation ulkopuolelta sisäänpäin puolestaan ylläpitävät organisaation oppimisen ja uudistumisen prosessia. Organisaation sisältä ulospäin suuntautuvissa tietovirroissa arvoa luodaan ulkoisille sidosryhmille. Viitekehyksessä esitetyn ajattelumallin avulla on muun muassa mahdollista tunnistaa tietovirtoihin liittyviä heikkouksia ja vahvuuksia, jolloin se toimii tukena tietoprosessien analysoinnissa ja käytännön johtamisessa. (Laihonen, 2011.)

Kuusisto ja Kuusisto (2006) viittaavat artikkelissaan tiedon jakamiseen sotilaskulttuurissa, jossa se oli aiemmin perinteisesti sidottu vahvasti vallan jakamiseen organisaatiohierarkiassa. Tietovirrat organisaatioyksiköiden ja toiminnan ohella järjestyivät tyypillisesti puumaiseksi rakenteeksi, jossa tietovirrat suuntautuivat pääasiallisesti ylhäältä alaspäin käskynantoperiaatteen mukaisesti ja vain jossain määrin alhaalta ylöspäin (Kuusisto & Kuusisto, 2006). Tänä päivänä niin yritysten kuin sotilasorganisaatioidenkin toiminta on riippuvainen verkostoista, eikä puumaiseen hierarkiaan perustuvien tiedon jakamiskäytänteiden ja johtamismallin perusteella todennäköisesti päästä enää kovinkaan pitkälle. Ahlavuo ym. (2011) jakavat tietovirrat yhteensä kymmeneen erilaiseen virtausmalliin:

1. yksilöltä yksilölle organisaation sisällä
2. yksilöltä organisaatioon
3. yksilöltä asiakkaille tai kumppaneille
4. organisaation sisällä integroituna

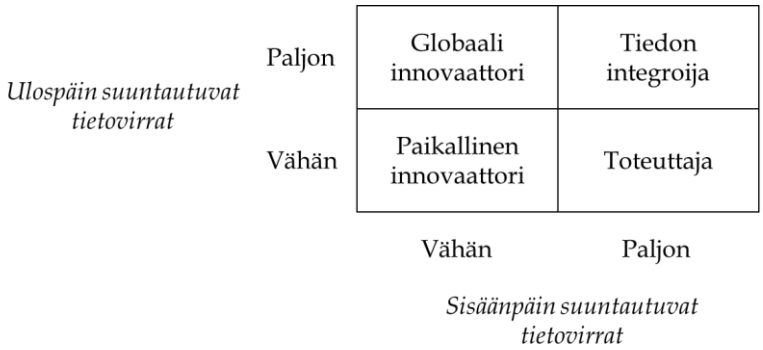
5. organisaatiolta yksilölle
6. organisaatiolta asiakkaille, kumppaneille ja/tai muille sidosryhmille
7. asiakkaiden, kumppanien ja/tai sidosryhmien välillä
8. asiakkailta, kumppaneilta ja/tai sidosryhmiltä yksilölle
9. asiakkailta, kumppaneilta ja/tai sidosryhmiltä organisaatiolle
10. tiedon tallentaminen tietovarantoihin (Ahlavuo ym., 2011).

Ahlavuon ym. (2011) tulkinnan mukaan muihin sidosryhmiin kuuluu organisaation tietovirrat, jotka muodostuvat vuoropuhelusta yhteiskunnan kanssa. Lisäksi kohdan yksi mukaista mallia tiedonvirtaamisesta organisaation sisällä yksilöltä yksilölle voidaan vielä tarkentaa siten, että tieto virtaa:

a) ryhmän sisällä,
b) yli ryhmä- tai yksikkörajojen
c) tai ryhmän sisällä ryhmän johtajalle (Ahlavuo ym., 2011).

Ahlavuon ym. (2011) näkemys tunnistaa tiedon ja sen merkityksen organisaation eri tasoilla monipuolisemmin kuin Kuusiston ja Kuusiston (2006) esimerkissä sotilasorganisaatioiden puumaisesta hierarkiasta ja tietovirtojen jakautumisesta sen mukaan. Erityisesti asiantuntijoiden välisessä vuorovaikutuksessa on perusteltua puhua korkeamman abstraktiotason mahdollistavista tietovirroista (Laihonen, 2011). Tiedon (itse tuotetun tai muualta hankitun) jakaminen oikeaan paikkaan edellyttää organisaatiolta dynaamisuutta, mutta myös toimivia organisaatiorakenteita (Ahlavuo ym., 2011), jotka tukevat tehokasta ja oikeaaikaista toimintaa tiedon arvokäsityksen kautta.

Gupta ja Govindarajan (1991 & 2000) ovat tutkineet tiedon jakamista monikansallisissa yrityksissä. Heidän mukaansa organisaation roolit on mahdollista jakaa tietovirtojen suuntausten perusteella neljään eri luokkaan, jotka on esitetty kuviossa 8. Riippuen kustakin roolista se, kuinka paljon organisaatio tuottaa tietovirtoja ulos- ja sisäänpäin, vaihtelee. Esimerkiksi tiedon integroijan roolissa olevat organisaatiot tuottavat itse paljon tietoa, mutta ottavat sitä myös paljon vastaan. Ne eivät kuitenkaan ole omavarainen tiedon suhteen, vaan niiden toiminnan edellytyksenä on ikään kuin ympäristön luotaaminen. Muita rooleja ovat globaali innovaattori, toteuttaja sekä paikallinen innovaattori. (Gupta & Govindarajan, 1991.)



KUVIO 8 Organisaatioiden roolit perustuen tietovirtojen suuntauksiin (Gupta & Govindarajan, 1991).

Gupta ja Govindarajan (2000) erottavat tieto- ja informaatiovirrat toisistaan. Informaatiovirrat ovat heidän näkemyksensä mukaan operatiivisen datan siirtämistä ja tietovirrat puolestaan asiantuntemukseen liittyvän tietämyksen tai strategisesti merkittävän ulkoisen markkinatiedon siirtämistä (Gupta & Govindarajan 1991 & 2000). Toisaalta Laihosen (2011) mukaan asiantuntijoiden välisessä vuorovaikutuksessa on perusteltua puhua korkeamman abstraktiotason mahdollistavista tiedon siirtämisen (tietovirtojen) muodoista. Tällöin tietovirta-käsitettä voidaan käyttää yleisterminä, joka viittaa eritasoisen tiedon (data, informaatio, tieto tai tietämys) siirtämiseen lähettäjältä vastaanottajalle (Laihonen, 2011).

Laihosen (2011) mukaan tietovirta-käsitettä ei itsessään ole käsitelty kirjallisuudessa kuitenkaan kovinkaan kattavasti. Yksi tunnetuimmista tietovirta-tarkasteluista perustuu aiemmin kuvattuun Nonakan ja Takeuchin (1995) SECI-malliin ja uuden tiedon luomiseen (Laihonen, 2011; Nissen, 2002). SECI-malliin pohjautuvassa teoriassa ensimmäinen mahdollinen tietovirta ilmenee sosialisaation aikana, jossa ryhmän jäsenet jakavat toisilleen merkityksellistä tietoa (Nissen, 2002). Tiedon virtaamista tapahtuu myös muissa SECI-mallin vaiheessa. Nonakan ja Takeuchin (1995) tietovirta-tarkastelua on kuitenkin kritisoitu sen käsitteellisen luonteen vuoksi, josta puuttuu käytännön sovellettavuus eli toisin sanoen menetelmät ja tavat tietovirtojen analysoimiseksi. Toisaalta usein kirjallisuudessa viitataan näkemykseen, jonka mukaan uuden tiedon luominen edellyttää aina hiljaisen tiedon ja eksplisiittisen tiedon vuorovaikutusta (mm. Ahlavuo ym., 2011; Nonaka & Takeuchi, 1995), mikä itsessään on herättänyt kritiikkiä (Laihonen, 2011). Nissen (2002) on pyrkinyt tutkimuksessaan haastamaan tätä perinteistä teoreettista tarkastelua tuomalla mukaan näkemyksen tietovirtojen käsittelyn laajuudesta muun muassa aikaulottuvuudessa, joka yhdistyy myös työnohjauksellisiin (engl. work flow) asioihin.

Laihonen (2011) näkee tietovirta-tarkasteluun liittyvän kritiikin viestinä konkreettisten lähestymistapojen tarpeesta tietovirtatutkimuksessa, joka lisäisi ymmärrystä tiedon virtaamisen käytännön ilmiöistä ja näihin vaikuttavista tekijöistä. Esimerkiksi Guptan ja Govindarajanin (2000) mukaan verkostojen tietovirtoihin liittyviä ilmiöitä on mahdollista tutkia ainakin kolmella eri tasolla: verkostojen solmukohtien (engl. nodal), kahdenvälisellä (engl. dyadic) tai koko

järjestelmän (engl. systemic) tasolla. Verkoston solmukohtien tutkimuksessa painopiste on yksiköiden toiminnassa, kahdenvälisessä yksiköiden välisessä jaetussa toiminnassa, ja koko järjestelmää koskevassa puolestaan koko verkoston toiminnan analysoinnista (Gupta & Govindarajan, 2000).

Tässä tutkimuksessa käytetään termiä 'tietovirta', sillä se mahdollistaa tutkittavan ilmiön ja siihen liittyvien tekijöiden tarkastelun laajemmin eri tietotasoilla käyttäen vain yhtä käsitettä. Jos haluttaisiin tutkia Guptan ja Govindarajanin (1991 & 2000) määritelmän mukaisesti informaatiovirtoja siten, että tieto mielletään staattiseksi objektiksi (Huotari ym., 2005, s. 59), olisi perusteltua keskittyä ilmiön määrälliseen tarkasteluun laadullisten tekijöiden sijaan. Tässä tutkimuksessa tieto kuitenkin ymmärretään sosiaalisena ilmiönä, jolloin on perusteltua ottaa huomioon tutkittavan ilmiön mahdolliset erilaiset tulkinnat.

2.3 Tilannekuva ja tilannetietoisuus

Jokainen organisaatio tarvitsee tietoa omasta toimintaympäristöstään ja sen tapahtumista sekä näiden mahdollisista vaikutuksista organisaation toimintaan, jotta se kykenee tekemään oikeita päätöksiä ja ylipäätään toimimaan. Lähtökohdaltaan tätä voidaan pitää kontingenssiteoreettisena tulkintana, jonka mukaan organisaation toiminnan täytyy sopeutua ympäristönsä vaatimuksiin (Jalonen, 2015). Pöyhönen ym. (2019) painottavat, että oikeiden päätösten tekemiseksi päättäjillä on oltava riittävät tietoperusteet, tunnettava päätöstensä mahdolliset seuraukset ja lisäksi tiedettävä mitä riskejä päätöksentekoon liittyy. Tietoperusteisessa toiminnassa päätöksenteon kannalta tärkeimpiä käsitteitä ovat tilannekuva, tilannetietoisuus sekä tilanneymmärrys.

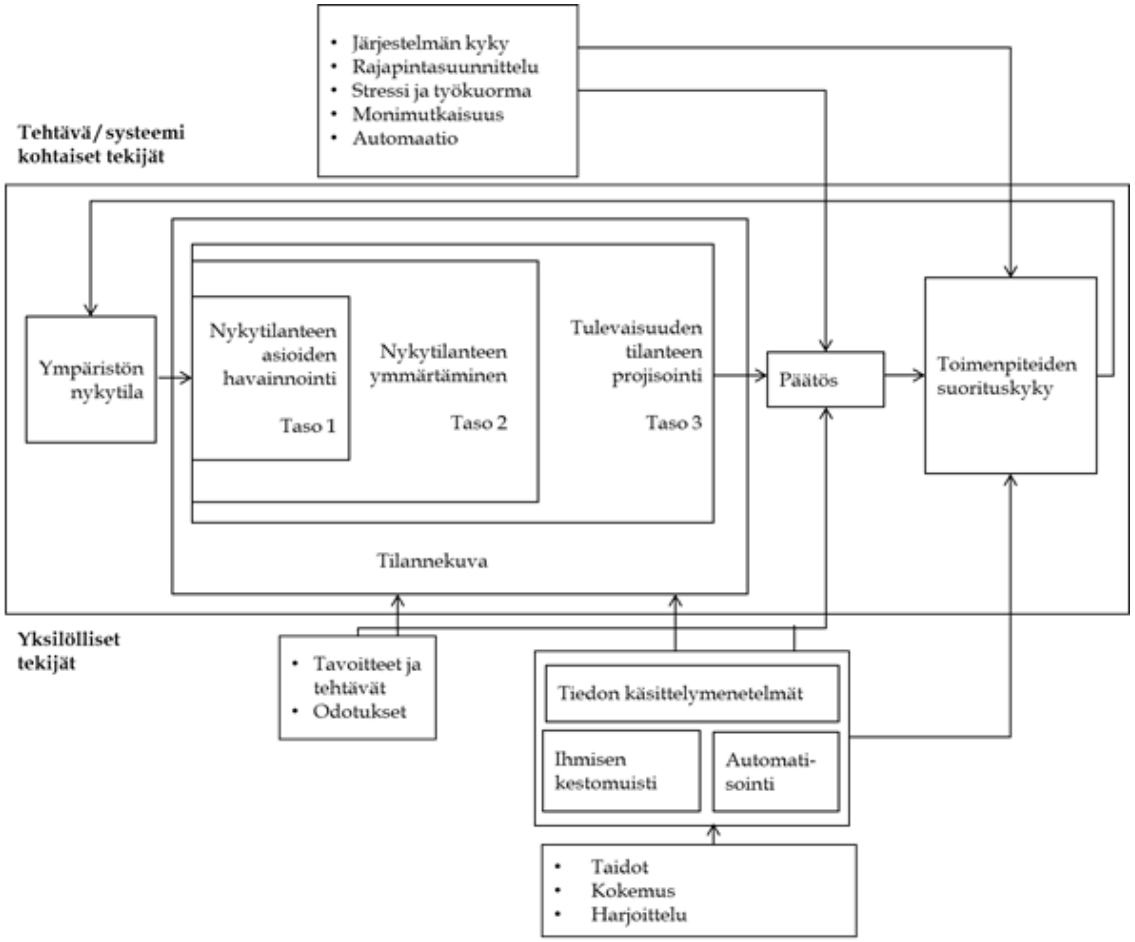
Kokonaisturvallisuuden sanaston (Sanastokeskus, 2017) määritelmän mukaan tilannekuva on "koottu kuvaus vallitsevista olosuhteista, käsillä olevan tilanteen synnyttäneistä tapahtumista, tilannetta koskevista taustatiedoista ja tilanteen kehittymistä koskevista arvioista sekä eri toimijoiden toimintavalmiuksista". Riippuen siitä, missä yhteydessä tilannekuvasta puhutaan, voidaan siitä englanniksi käyttää eri termejä. Esimerkiksi kun puhutaan tilannekuvasta konkreettisena kuvauksena johonkin tiettyyn tapahtumaan tai tilanteeseen sidottuna, käytetään englanniksi termiä 'situation picture', ja puolestaan silloin kun konkreettisen kuvauksen lisäksi viitataan tilannekuvatoimintaan tai tilaan, jossa tilanteesta on muodostettu kuva, käytetään termiä 'situation awareness'. Tilannetietoisuus (myös engl. situation awareness, SA) tarkoittaa päätöksentekoon tarvittavaa ymmärrystä tapahtuneista asioista ja niihin vaikuttaneista olosuhteista, sekä eri osapuolien tavoitteista ja mahdollisista vaihtoehdoista, joihin tilanne voi kehittyä. Tilannetietoisuus rakentuu usein muodollisesta tilanteen tai tapahtumien kuvauksesta tietyllä hetkellä eli tilannekuvasta. (Sanastokeskus, 2017.)

Tilannetietoisuuteen ja tilannekuvan muodostamiseen liittyy keskeisesti myös tilanneymmärrys. Tilanneymmärrys (engl. situational understanding) voidaan nähdä kognitiivisena tulkintana tilanteesta ja tilannetietoisuudesta

toimijan kokonaisvaltaisessa toimintaympäristössä, johon vaikuttaa olennaisesti ihmisten yksilöinä omaavat taidot, kokemus ja osaaminen (Kuusisto, Kuusisto & Wolfgang, 2015). Toisin sanoen tilanneymmärryksen tarkoitus on antaa päätöksentekijöille kattava kuvaus tilanteesta ja mahdollisesta kehityskulusta (ennakointi), jotka tukevat päätöksentekoa sekä tilanteeseen liittyvää riskien ja vaikutusten hallintaa (Parish & Madahar, 2016).

Parish ja Madahar (2016) korostavat, että terminologisesti tulisi ymmärtää ero erilaisissa päätöksentekomalleissa käytettyjen 'SA'-termien välillä ja merkitykseltään pyrkiä kohti todellista toimintaympäristön ja tapahtumien vaikutusten ymmärtämistä sen sijaan, että ympäristöstä tehdään karkeasti vain yksittäisiä havaintoja. Tilannetietoisuus vaatii kykyä kerätä tietoa ympäristöstä, keinoja ymmärtää kerättyä tietoa ja toisaalta kykyä heijastaa hankittua ymmärrystä takaisin toimintaympäristöön ja tapahtumiin sekä toteuttaa arvioita siitä, miten havaitut tapahtumat vaikuttavat omaan toimintaan. Parishin ja Madaharin (2016) mukaan tilannetietoisuus voidaan nähdä tietyn kiinnostuksen kohteen, ongelman tai tilanteen hahmottamisena tietyssä ajassa ja tilassa. Heidän mukaansa tilannetietoisuus siten antaa mahdollisuuden ymmärtää, mitä on tapahtunut ja mitä mahdollisesti tulee tapahtumaan, mutta se ei välttämättä kerro miksi se on tapahtunut. (Parish & Madahar, 2016.)

Endsley (1995) näkee tilannetietoisuuden ikään kuin tietämyksen tilana ja erottaa sen tilannetietoisuuden saavuttamiseen liittyvistä prosesseista. Endsley (1995) jakaa tilannetietoisuuden kolmeen tasoon: (1) havaitsemiseen (engl. perception), (2) ymmärtämiseen (engl. comprehension) ja (3) ennustamiseen (engl. projection). Näkemys tilannetietoisuuden syntymisestä osana päätöksentekoa on kuvattu kuviossa 9.



KUVIO 9 Tilannetietoisuuden malli päätöksentekoprosessissa (mukailtu Endsley, 1995).

Ensimmäisellä tasolla havaitaan erilaisia tilanteeseen liittyviä tekijöitä. Havainnointia voidaan ohjata esimerkiksi tukikysymyksillä, joiden avulla resursseja pystytään keskittämään ja vastaamaan paremmin ennalta tunnistettuihin tietotarpeisiin (Endsley, 1995). Tiedonhankinta (havainnointi) vaatii ihmislähtöistä toiminnan suunnittelua ja hallintaa – kuten toimintamalleja ja perusteita tiedontaltioimiseen ja jakamiseen (Choo, 1998, s. 264). Ymmärtämisessä on kyse havaittujen tekijöiden merkityksellistämisestä ja tärkeyden hahmottamisesta oman toimialan kannalta. Kolmannella tasolla pyritään luomaan tietojen perusteella tilannearvio ja ennustamaan tilanteen mahdollisia kehityskulkuja. Mallissa päätöksenteko nähdään jatkuvana kehänä, jota tilannekuva ohjaa. Omaksutun ja jäsennellyn tiedon tuloksena syntyy tilannetietoisuus. (Endsley, 1995.)

Endsley (1995) korostaa yksilöllisten ja toimintaympäristökohtaisten tekijöiden vaikutusta tilannetietoisuuden muodostumisessa. Yksilön havainnointikyky ja työmuisti ovat Endsleyn (1995) mukaan kriittisiä ja mahdollisia rajoittavia tekijöitä, kun yksilö pyrkii omaksumaan ja tulkitsemaan tietoa ympäristöstään ja muodostamaan niiden pohjalta käsityksen vallitsevasta tilanteesta. Yksilön tekemät havainnot ympäristön tilasta ovat hänen tilannetietoisuutensa (SA) pohja, ja jonka muodostumiseen vaikuttaa muun muassa henkilökohtaiset kyvyt, aiempi kokemus ja koulutus. Havainnointiin

vaikuttavat myös yksilön ennakko-olettamukset tai tavoitteet, jotka toimivat ikään kuin suodattimina ympäristön ja asiantilojen tulkitsemisessa. (Endsley, 1995.)

Tilannetietoisuudessa voidaan viitata yhtä lailla informaatioon, prosesseihin kuin myös ihmisen mentaaliseen malliin, jolla hän suoriutuu tietystä tehtävästä tai tehtäväkokonaisuudesta (Horsmanheimo ym., 2017.) Myös Choo (1998) tunnistaa yksilön havainnointikykyyn ja kognitiiviseen suorituskykyyn, sekä toisaalta organisaation laajojen tietotarpeiden asettamaan vaatimustasoon liittyvät rajoitukset ja haasteet tiedonhankinnassa (engl. information acquisition) ja hallinnassa. Kaikki saatavilla oleva tieto ei kuitenkaan ole organisaation toiminnan ja päätöksenteon kannalta olennaista. Kontekstista riippumatta on kyettävä erottamaan olennainen tieto epäolennaisesta informaatiomassasta (Jalonen, 2015). Sen vuoksi tietolähteiden valinta ja käyttö täytyy olla suunnitelmallista, ja sitä tulee mitata ja arvioida kuten mitä tahansa organisaation kriittistä resurssia. (Choo 1998, s. 263–264.)

Tilannetietoisuuden luominen ja ylläpito on sitä haastavampaa, mitä moniulotteisemmasta ja dynaamisemmasta ympäristöstä on kyse (Endsley, 1995). Siten organisaation tietojärjestelmien täytyy mahdollistaa eri tietolähteiden johdonmukainen käyttö sekä yhteistyö ja tilannetiedon jakaminen keskeisten osapuolten kanssa (Pöyhönen ym., 2019). Pöyhönen ym. (2019) kuvaavat tilannekuvaprosessin kolme vaihetta, joita ovat:

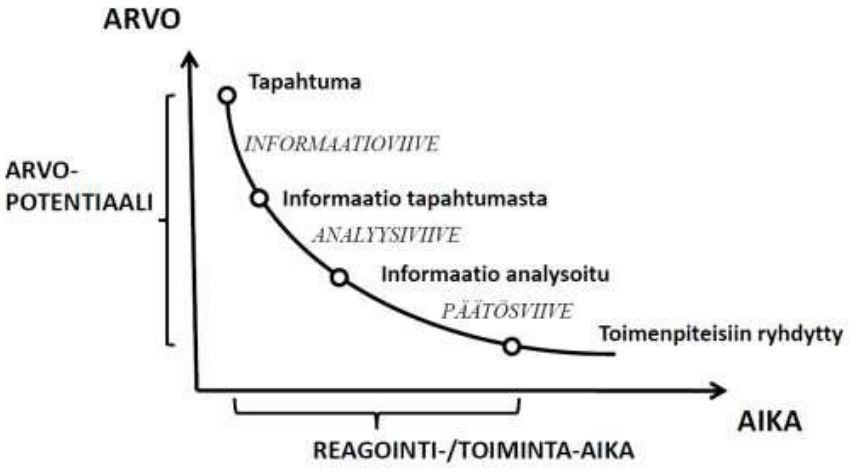
1. tiedonkeruu,
2. tiedon kokoaminen, luokitus ja analysointi, sekä
3. analysoidun tiedon oikea-aikainen ja tehokas jakaminen sitä tarvitseville (Pöyhönen ym., 2019.)

Prosessin perusajatuksesta löytyy yhteneväisyyttä edellä käsiteltyihin organisaation tietoprosesseihin sekä uuden tiedon luomiseen (Nonaka & Takeuchi, 1995; Choo, 1998). Tilannekuvaprosessissa olennaista on, että olosuhteet on järjestetty siten, että tieto ymmärretään oikein ja sitä tarvitsevilla on mahdollisuus saada toimintansa kannalta tärkeää tietoa. Esimerkiksi tietojärjestelmien täytyy mahdollistaa eri tietolähteiden johdonmukainen käyttö sekä yhteistyö ja tilannetiedon jakaminen keskeisten osapuolten kanssa (Pöyhönen ym., 2019). Pöyhönen ym. (2019) puhuvat tästä ”ympäröivänä tietoavaruutena”, joka yhtä lailla voitaisiin kuvata ba-käsitteenä, jolla tarkoitetaan uuden tiedon luomisen mahdollistavia vuorovaikutuksellisia olosuhteita (Nonaka & Konno, 1998).

Tilannekuvan muodostamista edistää, jos saatavilla on yhteinen, jaettu tietokanta tai tilannekuvajärjestelmä, johon kaikki toimijat tuottavat oman osuutensa. Tämä mahdollistaa sen, että tiedot ovat kaikkien toimijoiden saatavilla, ja sen pohjalta kukin voi valita oman toimintansa kannalta relevantit tietosisällöt ja sen avulla muodostaa tilannekuvaa ja -ymmärrystä vallitsevista olosuhteista. (Laari ym., 2019.) Horsmanheimon ym. (2017) mukaan ”tilannekuvajärjestelmän tehtävä on tuottaa informaatiota sellaisessa muodossa, että järjestelmää käyttävä henkilö pystyy saavuttamaan tai säilyttämään tilannetietoisuuden teh-

tävän vaatimalla tasolla". Tilannekuvajärjestelmän kannalta olennaista on selvittää, mitkä ovat tilannetietoisuuden vaatimukset eri päätöksenteon ja johtamisen tasoilla. Näiden pohjalta valitaan tarvittavat tietolähteet, analyysimenetelmät sekä tiedon visualisointitavat kohderyhmälle sopivalla tavalla. (Horsmanheimo ym., 2019.)

Myös aikakäsityksellä on keskeinen merkitys puhuttaessa tiedon suhteesta organisaation toimintaan ja toiminnan luomaan arvoon. Jalonen (2015) kiteyttää "mitä nopeammin organisaatio reagoi sen sisäiseen tai ulkoiseen tapahtumaan, sitä suurempi arvopotentiaali tapahtumaan liittyy". Reagointinopeuden avulla voidaan siten hahmottaa organisaation tiedolla johtamisen potentiaalia. Hackathorn (2004) toisaalta muistuttaa myös toimenpiteiden oikeaaikaisuudesta. Tällä hän tarkoittaa ei pelkästään reagointinopeutta vaan toiminnan suhteuttamista kuhunkin arvonluonnin tapahtumaan sopivalla tavalla, jolloin harkittu ajallinen viive voi olla joskus myös paikallaan ennen toimenpiteisiin ryhtymistä. (Jalonen, 2015; Hackathorn, 2004.) Arvon ja ajan suhdetta on havainnollistettu kuviossa 10.



KUVIO 10 Jalosen (2015) tulkinta tapahtumien arvopotentiaalista suhteessa aikaan (Jalonen, 2015, alkup. Hackathorn, 2004).

Toisaalta tiedon jakamisen aikakäsitys vaikuttaa myös verkostoihin. Kuusisto ja Kuusisto (2006) esittävät, että yksilön tai yhteisön olemassaolo tai halu toimia yhdessä voi muuttua epävarmaksi, jos tietoa ei välitetä toisille verkoston toimijoille tietyn ajan kuluessa. Luotettavaan tietoon ja arvioihin perustuvan asianmukaisen ja nopean tilannetietoisuuden tarve korostuu, kun täytyy tehdä nopeita ja laaja-alaisia päätöksiä (Pöyhönen ym., 2019). Pöyhösen ym., (2019) mukaan vastuuta on pahimmassa tapauksessa kyettävä delegoimaan ja toimenpiteiden käytäntöönpano toteuttamaan minuuteissa. Jos tarvittaviin toimenpiteisiin ryhtyminen vie epätarkoituksenmukaisen paljon aikaa, on se mahdollisesti merkki siitä, että jokin kohta organisaation tietoprosessista ei toimi optimaalisesti. Seuraavassa alaluvussa käsitellään keskeisimpiä haasteita, joita tietoperustaiseen toimintaan liitetään.

2.4 Tietojohtamisen haasteita

Tietojohtaminen on moninainen kokonaisuus ja organisaatioiden tietoperustaiseen toimintaan liittyy monia haasteita.

Laihonen ym. (2013) nostavat esiin tietotarpeiden määrittelyn haasteellisuuden osana asiantuntijatyötä. Tähän on useita syitä, joista keskeisimpinä ovat itse tietotarpeiden sekä organisaation ja sen toimintaympäristön muutokset, joita on vaikea ennustaa. Osiltaan tietotarpeiden määrittelyn haasteet liittyvät asiantuntijatyön luonteeseen, jonka usein ajatellaan olevan ennalta tuntemattomien ongelmien ratkaisua. Näin ollen ei myöskään ole mahdollista täsmälleen määritellä, mitkä organisaation todelliset tietotarpeet ovat, kun ratkaistavat ongelmat ovat lähtökohdiltaan tuntemattomia. (Laihonen ym., 2013).

Jalonen (2015) puhuu sen sijaan informaation välttämisestä, jolla tarkoitetaan toimimattomuuden perustelemista sillä, ettei yksilöllä ole käytössään riittävästi tietoa käsiteltävästä asiasta. Kyseessä voi myös olla informaatiosta pidättäytyminen, jolloin yksilö ikään kuin kieltäytyy tietoisesti päätöksentekoon tai toimimiseen tarvittavien tietojen ”etsimisestä”. Informaation välttämisen taustalla olevat tekijät voivat olla moninaisia, ja yhtenä jaottelutapana voidaan käyttää jakoa yksilöllisiin ja teknisluonteisiin esteisiin organisaatioympäristössä. Jalosen (2015) mukaan yksilöt ovat taipuvaisia pidättäytymään tiedonhankinnasta, jos tiedonhankinnan tunneperäiset ja teknisluonteiset esteet ovat suuremmat kuin siitä syntyvä hyöty. Tiedonhankinta puolestaan nähdään mielekkäänä, jos esteet ovat pienemmät kuin tiedon arvo. (Jalonen, 2015.)

Organisaatioiden tietoperustaista toimintaa voidaan lähestyä myös tieto-ongelmien kautta. Näitä ovat epävarmuus, joka ilmenee informaation ja varman tiedon puutteena; monimutkaisuus, joka tarkoittaa asiantilojen ja ilmiöiden toisiinsa nivoutumisesta aiheutuvaa informaation paljoutta; epäselvyys, joka ilmenee asiantilojen ja ilmiöiden tulkintavaikeutena; ja monitulkintaisuus, jolla viitataan asiantilojen ja ilmiöiden mahdollisiin erilaisiin tulkintoihin. Jalosen (2015) mukaan ”epävarmuuden ja tiedon välillä vallitsee käänteinen korrelaatio”, mikä tarkoittaa, että tiedon lisääminen vähentää epävarmuutta. Esimerkiksi organisaation sisäisten ja ulkoisten tietovirtojen systemaattinen analysointi voi vähentää organisaation epävarmuutta, jos ongelmiin liittyviä muuttujia analysoidaan huolellisesti sekä organisaation tuottamaa ja hankkimaa tietoa tallennetaan ja jaetaan tehokkaasti. Epävarmuus ja monimutkaisuus ovat luonteeltaan konvergentteja ongelmia, joihin on löydettävissä ratkaisu asiantilojen tai ilmiöiden huolellisella analysoinnilla. Epäselvyys ja monitulkintaisuus ovat puolestaan divergenttejä tieto-ongelmia, joihin ei ole yhtä ja oikeaa ratkaisua, vaan niihin liittyy olennaisesti tulkinnat. (Jalonen, 2015.)

Tiedon jakamisen esteitä voidaan jaotella lisäksi eri kategorioihin, joista kenties tunnetuin on Riegen (2005) luoma jako yksilöllisiin (engl. individual), organisatorisiin (engl. organisational) ja teknologisiin (engl. technological) tekijöihin. Kuviossa 11 esitetyt tiedon jakamisen esteet kuvastavat hyvin aihepiirin laajuutta ja moniulotteisuutta siinä, miten tietokäyttäytymiseen liittyviä ongel-

mia voi ilmetä organisaatioiden toiminnassa useilla eri tasoilla eikä näiden tarkastelu ole kovin yksiselitteistä.

KUVIO 11 Tiedon jakamisen esteet Riegen (2005) mukaan. (Riege, 2005; mukaillen Vuori ym., 2019).

Vaikka Riegen (2005) malli on monipuolinen, ei se ota kantaa organisaatioiden väliseen toimintaan mahdollisesti liittyviin haasteisiin vaan ne on liitetty osaksi organisatorisia haasteita (kuvio 11) (Vuori ym., 2019). Vuori ym. (2019) tunnistavat kaksi muuta tiedon jakamisen esteiden kategoriaa Riegen (2005) esittämien tekijöiden lisäksi. Nämä ovat verkosto- ja tietospesifit tiedonjakamisen esteet, jotka on esitetty tarkemmin taulukossa 1.

TAULUKKO 1 Verkosto- ja tietospesifit tiedon jakamisen esteet (Vuori ym., 2019).

Verkostospesifit	**Tietospesifit**
Maantieteellinen etäisyys (engl. geographical distance)	Tulkinnanvaraisuus, monimerkityksellisyys (engl. ambiguity)
Kognitiivinen läheisyys (verkoston jäsenten samankaltaisuus) (engl. cognitive proximity)	Tiedon kompleksisuus (engl. complexity)
Suhteiden vahvuus, luottamus (engl. stength of relationships, trust)	Hiljainen vai eksplisiittinen tieto (engl. tacitness/explicitness)
Tiedon välittäjän puute (engl. lack of intermediator)	Tietämyksen/tiedon suojelu (engl. knowledge protection)

Vuori ym. (2019) ovat havainneet, että verkottuneiden toimijoiden tyypillisimmät tiedon jakamisen esteet ovat lähtöisin ihmisten toiminnasta eikä niinkään teknologisista tekijöistä. Myös mitä monimutkaisempia ja erilaisempia toimintamalleja ja rakenteita toimijoilla on, sitä vaikeammaksi erityisvastuualueiden strateginen johtaminen voi muodostua (Jalonen, 2015). Laihosen (2011) palvelujärjestelmien tietovirtoja käsittelevässä tutkimuksessa yhtenä keskeisenä näkemyksenä nousee esille, että ”tiedonkulun ja tietoperustaisen arvonluonnin näkökulmasta toimijoita yhdistävien strategisen tason tietovirtojen puutee johtaa siihen, että arvoverkossa ei kyetä täysin hyödyntämään toimijoiden erikoistumiseen ja yhteistyöhön liittyvää potentiaalia.” Näin ollen on tärkeää tunnistaa liityntäpinnat keskeisiin kumppaneihin, mutta myös jäsentää organisaation sisäistä toimintaa mahdollisimman tehokkaasti. Tietojohtamisen ydin kiteytyy seuraavaan ajatukseen:

> Parhaimmillaan toimiva ja jaettu tietostrategia jäsentää tiedon luomista, organisoimista, jakamista ja soveltamista tavalla, joka edistää strategisten tavoitteiden saavuttamista ja operatiivisen toiminnan tehokkuutta. Vastaavasti pahimmillaan yhteensopimattomat tietostrategiat aikaansaavat kehitystä, jossa organisaatiot päätyvät systemaattiseen informaation ylituotantoon. (Jalonen, 2015.)

Seuraavassa luvussa taustoitetaan tutkimuskontekstia kyberturvallisuuden tietojohtamisen, kybertoimintaympäristön ja siihen liittyvien erityispiirteiden ja rakenteiden näkökulmasta.

3 KYBERTOIMINTAYMPÄRISTÖN KUVAUS

Tässä luvussa käsitellään kybertoimintaympäristön tunnuspiirteitä ja ominaisuuksia, jotka heijastavat organisaatioiden kyberturvallisuuden tietojohtamiseen. Luvun tarkoituksena on selventää tietovirtoihin ja niiden hallintaan liittyviä osatekijöitä kybertilannekuvan tuottamisen kontekstissa. Ensimmäisenä avataan kybertoimintaympäristön ja uhan määritelmää, minkä jälkeen siirrytään toiminteiden kuvauksen kautta käsittelemään kybertilannekuvan muodostamista niin tiedonjakamisen käytänteiden kuin laajemmin tiedonvaihtoverkoston näkökulmista.

3.1 Määritelmä

Kybertoimintaympäristö (engl. cyber environment, cyberspace, cyberdomain) on laaja ja moninainen käsite ja kokonaisuus, eikä sen hahmottaminen ole aina kovin yksiselitteistä. Se määritetään tyypillisesti yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaksi toimintaympäristöksi, johon kuuluvat fyysisten rakenteiden lisäksi kaikki toimintaympäristön toimijat. Kybertoimintaympäristölle on lisäksi tyypillistä elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkoja hyödyntämällä. Kybertoimintaympäristö on ihmisten, organisaatioiden ja fyysisten järjestelmien muodostama vaikutusympäristö. Sotilaallisessa kontekstissa kybertoimintaympäristö voidaan esittää myös kyberdomainina vastaavasti kuten puhuttaessa muista toimintaympäristöistä (maa, meri, ilma ja avaruus). (Sanastokeskus, 2017; Laari ym., 2019, s. 9–10; Lehto, 2019).

Parish ja Madahar (2016) puolestaan kuvaavat kybertoimintaympäristön monimutkaiseksi sosioteknisten systeemien systeemiksi (engl. socio-technical system of systems STSOS), joka mahdollistaa ja toisaalta muokkaa nykymaailmaa, sen yhteiskuntia, taloutta, teknologioita ja eri toimialoja. Se pitää sisällään fyysisiä, loogisia ja kognitiivisia osia, sekä myös digitaalisia resursseja, jotka ohjaavat niin data-, informaatio- kuin päätöksentekovirtoja, ja siten yhdistävät

erilaisia toimintoja keskenään (Parish & Madahar, 2016). Usein kybertoimintaympäristö jaetaan kuitenkin karkeasti kahteen osaan: fyysiseen maailmaan ja ihmisten luomaan keinotekoiseen digitaaliseen maailmaan (Laari ym., 2019, s. 10), jotka ovat yhteiskunnan digitalisoitumisen myötä yhä riippuvaisempia toisistaan.

Kybertoimintaympäristölle on tunnusomaista tapahtumien hektisyys, muutosnopeus ja toisaalta järjestelmien kompleksisuus. Muutosnopeus edellyttää kaikelta toiminnalta nopeaa reagointikykyä, ja myös kykyä varautua tilanteisiin, joita ei täysin kyetä ennakoimaan. Yleisesti informaatioteknologian kehityssykli näyttäytyy lyhyenä, mikä pätee myös kybertoimintaympäristössä esiintyvien uhkien ja hyökkäysmenetelmien kehittymiseen. Aika on siten yksi keskeisimmistä kybertoimintaympäristön muutosajureista. (Lehto, 2019.) Kybertoimintaympäristöä pidetään lisäksi maailmanlaajuinen, eikä sitä varsinaisesti omista kukaan (Laari ym., 2019, s. 10), mihin liittyy sekä hyviä että haastavia puolia. Esimerkiksi luonteeltaan se mielletään niin sanotusti ylikansalliseksi, ja sen vuoksi siellä tapahtuvasti toiminnasta aiheutuu valtioiden välille suvereenisuus- ja turvallisuusristiriitoja, joihin ei laillisuus- ja eettisyysnäkökulmista ole toistaiseksi löydetty yksiselitteistä ratkaisua (Lehto, 2019). Parish ja Madahar (2016) toteavatkin, että kybertoimintaympäristöä on vaikeaa tai jopa mahdotonta säännellä ja määrätä.

3.2 Kyberuhka ja keskeiset tietotyypit

Tietotekniikan ja verkottuneisuuden lisääntyminen nyky-yhteiskunnassa on edistänyt uudentyyppisten uhkien muodostumista ja mahdollistaa niiden laajemman leviämisen. Kybermaailman uhat ovat luonteeltaan globaaleja ja nopeasti kehittyviä uusien hyväksikäyttömahdollisuuksien ilmetessä, ja hyökkääjän motiivit yhä useammin ovat luonteelta yhteiskunnallisia ja poliittisia pelkän taloudellisen hyödyn tavoittelemisen sijaan (Skopik ym., 2016).

Lehto (2019) viittaa uhkaan (engl. threat) uutena tai äskettäin havaittuna tapahtumana, joka voi aiheuttaa vahinkoa organisaation tietojärjestelmissä tai organisaatiossa yleisesti. Uhkatieto (engl. threat information) on mitä tahansa tietoa, joka voi auttaa organisaatiota suojautumaan uhkaa vastaan tai havaitsemaan mahdollisen tai todellisen uhkatoimijan toiminnan (Rizov, 2018). Uhat voidaan yleisesti luokitella kolmeen kategoriaan:

1. luonnolliset uhat (esim. tulvat tai muut luonnonkatastrofit)
2. tahattomat uhat (yleisimmin käyttäjästä johtuvat virheet tai järjestelmäylläpidolliset virheet, kuten työntekijän pääsy vahingossa liian laajoihin tietovaroihin)
3. tahalliset uhat. (Lehto, 2019.)

Kyberturvallisuuden sanaston (Sanastokeskus, 2018) määritelmän mukaan kyberuhkalla (engl. cyber threat) tarkoitetaan kybertoimintaympäristöön kohdis-

tuvaa mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua, joka voi toteutuessaan vaarantaa kybertoimintaympäristöstä riippuvaisen toiminnon. Kyberuhkat voivat aiheutua niin toteutuneista tietoturvauhkista kuin myös digitaalisessa viestintäympäristössä tapahtuvista, yhteiskunnan turvallisuutta vaarantavista teoista. Ne voivat kohdistua yhteiskunnan elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin tai kansalaisiin joko suoraan tai välillisesti, ja ne voivat olla peräisin valtion sisältä tai sen rajojen ulkopuolelta. (Lehto, 2019; Sanastokeskus, 2018.) Kyberuhkatiedolla (engl. cyber threat information) tarkoitetaan mitä tahansa tietoa, joka voi auttaa organisaatiota tunnistamaan, arvioimaan, valvomaan sekä toisaalta myös hallitsemaan ja reagoimaan tunnistettuihin kyberuhkiin (Rizov, 2018).

Kybermaailman uhat näyttäytyvät haastavina määrittää, mikä osittain perustuu kybermaailman ylikansalliseen luonteeseen, mutta myös teknologian nopeaan kehitykseen ja uhkatoimijoiden kykyyn hyväksikäyttää tietojärjestelmien haavoittuvuuksia (Lehto, 2022). Tyypillisesti kyberuhkat jaetaan kuuteen tasoon sen mukaan, millaisia toimijoiden motiivit ovat:

1. kybervandalismi
2. kyberrikollisuus
3. kybervakoilu
4. kyberterrorismi
5. kybersabotaasi
6. kybersodankäynti. (Lehto, 2022.)

Tason 1 kybervandalismi pitää sisällään hakkeroinnin, haktivismin ja niin sanotun kyberparveilun, jotka tyypillisesti voivat saada julkisuudessa paljon näkyvyyttä, mutta ovat vaikutuksiltaan lyhytaikaisia ja osin vaarattomiakin. Kybervandalismista saattaa kuitenkin seurata merkittäviä taloudellisia vahinkoja yksittäiselle yritykselle tai yksilölle. Tasolla 2 puhutaan kyberrikollisuudesta, jossa tietoverkkoja ja tietojärjestelmiä hyödynnetään rikosten toteuttamiseen tai niihin kohdistetaan rikollista toimintaa. Motiivina usein on taloudellinen hyöty. Kyberrikollisuudessa tietokone tai muu laite on rikoksen objekti ja/tai sitä käytetään rikoksen toteuttamiseen. Tason 3 muodostaa kybervakoilu, joka tarkoittaa toimia, joilla hankitaan salaisia tietoja poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi käyttäen laittomia menetelmiä kyber- ja informaatioympäristössä. Kyberterrorismissa (taso 4) tietoverkkoja käytetään vihamielisiin hyökkäyksiin kriittisiä informaatiojärjestelmiä kohtaan ja toisaalta myös niiden kontrollointiin. Kyberterrorismin tavoitteena on tuottaa vahinkoa ja levittää pelkoa yhteiskunnassa sekä painostaa valtioiden poliittista johtoa. Tasolla 5 puhutaan kybersabotaasista, jossa hyökkääjä operoi sotaa alemmalla tasolla ja toiminnan taustalla on usein valtiollinen toimija tai sen tukema ryhmittymä. Kybersabotaasin tavoitteina ovat tyypillisesti epävakauden aiheuttaminen kohdemaassa, offensiivisten kyberhyökkäysten testaaminen sekä sodan tai hybridioperaatioiden valmistelu. Tasolla 6 puhutaan kyberuhan korkeimmasta muodosta eli kybersodankäynnistä, jolle Lehdon (2022) mukaan ei ole yhteisesti

hyväksyttyä määritelmää. Sillä kuitenkin useimmiten viitataan valtioiden väliseen vihamieliseen toimintaan kybertoimintaympäristössä, jossa kyberoperaatiot ovat osa muita sotilaallisia operaatioita. (Lehto, 2019; Lehto 2022.)

Kyberuhan määrittelyssä voidaan hyödyntää myös jakoa karkeasti kahteen kyberhyökkäystyyppiin, joita ovat ei-kohdistetut ja kohdistetut hyökkäykset. Ei-kohdistetuilla hyökkäyksillä uhkatoimija pyrkii saavuttamaan niin suuren joukon haavoittuvia laitteita, järjestelmiä tai käyttäjiä kuin vain mahdollista, jolloin kohteet voivat olla hyvinkin sattumanvaraisia. Tämän tyyppisiä hyökkäyksiä hyödynnetään esimerkiksi kiristyshaittaohjelmakampanjoissa. Kohdistetuissa kyberhyökkäyksissä uhkatoimija puolestaan nimensä mukaisesti valitsee kohteensa harkiten, yleensä erityisen kiinnostuksen perusteella tiettyyn toimialaan tai organisaatioon. Hyökkäyskampanjan pohjatyö vaatii resursseja niin ajallisesti kuin kyvyllisesti. Kohdistettujen kyberhyökkäysten uhka ja kohdistettuja hyökkäyksiä tekevät uhkatoimijat tunnetaan käsitteellä 'Advanced Persistent Threat' (lyh. APT). Kohdistettujen hyökkäysten taidokkuus edellyttää myös organisaatioilta jatkuvasti kehittyvää kykyä suojautua kyberuhkilta ja reagoida havaittuihin kyberhyökkäyksiin. (Lehto, 2022.)

Kyberuhkiin ja niihin varautumiseen liittyy erilaisten tietotyyppien jäsentely ja näistä muodostuvien merkityssisältöjen integroiminen osaksi organisaation varautumiseen liittyvää toimintaa. Goodwin ja Nicholas (2015) listaavat seitsemän keskeistä kyberturvallisuuden tietotyyppiä, joihin perustuvia tietoja eri toimijat vaihtavat keskenään:

- poikkeamatieto (engl. incident)
- uhkatieto (engl. threats)
- haavoittuvuustieto (engl. vulnerabilities)
- mitigointikeinot (engl. mitigations)
- tilanne-/tilannekuvatieto (engl. situational awareness)
- parhaat käytänteet (engl. best practices)
- strateginen analyysi (engl. strategic analysis). (Goodwin & Nicholas, 2015.)

Jokaisella tietotyypillä on erilainen käyttötarkoitus. Jotkut tiedoista auttavat julkisen ja yksityisen sektorin tahoja arvioimaan kyberturvallisuuteen kohdistuvia riskejä kansallisella tai organisaatiotasolla, kun puolestaan toiset auttavat analysoimaan kyberturvallisuutta pitkällä aikavälillä tai havaitsemaan käynnissä olevia hyökkäyksiä (Goodwin & Nicholas, 2015).

Uhkatiedon käyttötarkoitusta voidaan tarkastella myös organisaation toimintahierarkian eri tasoilla (strateginen, operatiivinen, taktinen ja tekninen). Tounsi ja Rais (2017) tarkastelevat näitä tasoja kyberuhkatiedustelun (engl. cyber threat intelligence) näkökulmasta. Strategisen tason tarkastelulla viitataan ylemmän tason tietoon, joka tukee päätöksentekoa ja toimintaan liittyvää riskiarviointia. Operatiivinen tieto käsittää organisaatioon kohdistuvan tietyn hyökkäyksen ilmentymää ja sen kohdeyleisönä on ensisijaisesti johtava turvalli-

suushenkilöstö. Taktisella tasolla puolestaan käsitellään tietoa uhkatoimijan käyttämistä tekniikoista ja toimintamalleista. Taktista tietoa hyödynnetään uhkatoimijan havaitsemisessa ja oman puolustuksen vahvistamisessa tunnettuja taktiikoita, tekniikoita ja menetelmiä vastaan. Teknisen tason tietoa sen sijaan käytetään teknisten resurssien, kuten valvonnan, rikastamiseen tai havaitun poikkeaman tekniseen analyysiin. (Tounsi & Rais, 2017.)

Tiedon ja sen käsittelyn merkitys on keskeinen kyberturvallisuuden toteuttamisen kannalta. Tähän liittyy olennaisesti Huotarin ym. (2015, s. 140) näkemys siitä, että tietoperustaisessa organisaatiossa tai yhteistyöverkostossa informaatio- ja tietoresurssit voidaan nähdä sekä toiminnan panoksena että sen tuotoksena. Kyberturvallisuuden ylläpitäminen perustuu pitkälti relevantin tiedon saatavuuteen ja kykyyn jäsentää sitä oman toiminnan kannalta tarvittaviin merkityssisältöihin. Päätöksenteon kannalta huomionarvoista on, että oikean tiedon saaminen oikeaan aikaan voi auttaa päättäjiä vähentämään riskejä, estämään mahdolliset kyberhyökkäykset ja myös lisäämään organisaation kriisinsietokykyä eli resilienssiä käytössä olevaan tietoperustaan peilaten (Goodwin & Nicholas, 2015).

3.3 Toiminteiden määrittely

Tässä alaluvussa avataan, minkä tyyppisestä toiminnasta on yleisesti ottaen kyse puhuttaessa kybertilannekuvaa muodostavista organisaatioiden toiminteista. Terminologisesti toiminteiden määrittely on haastavaa, sillä niistä käytetään vaihtelevasti erilaisia nimityksiä ja lyhenteitä, kuten:

- Security Operations Center (SOC)
- Cyber Security Operations Center (CSOC)
- Computer Emergency Response Team (CERT)
- Computer Incident Response Team (CIRT)
- Computer Incident Reponse Center (CIRC)
- Computer Security Incident Response Center (CSIRC) (Zimmerman, 2014, s. 8–9.)

Kybertilannekuvatoiminteille ei toisin sanoen ole yhtä yksiselitteistä määritelmää. Ne voivat vaihdella pienistä, muutaman hengen tehtäväkokonaisuuksista kansallisiin koordinointikeskuksiin (Zimmerman, 2014, s. 10). Erilaisista nimityksistä huolimatta yhteistä näille kaikille on niiden tehtävä, joka Zimmermanin (2014, s. 8) määritelmän mukaan voidaan sitoa ’Computer Network Defence’ (lyh. CND) käsitteen ja merkityksen ympärille. Karkeasti suomennettuna voitaisiin puhua *tietoverkkopuolustuksesta* tai *kyberpuolustuksesta*. CND:llä tarkoitetaan:

> The practice of defense against unauthorized activity within computer networks, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities (Zimmerman, 2014, s. 8).

Toisin sanoen tällaisten toiminteiden tärkein tehtävä on niin yksityisissä yrityksissä kuin julkishallinnon organisaatioissa havainnoida ja suojata niitä tietoturvapoikkeamilta ja mahdollisilta kyberhyökkäyksiltä. Koska kybertoimintaympäristö yhdistää kaikki tietoliikenneverkot, tietokannat ja informaatiolähteet globaaliksi systeemiksi, on näiden rakenteiden turvaaminen – eli kyberpuolustus – yhteiskunnille välttämätöntä (Lehto, 2019). Kokulun ym. (2019) näkemyksen mukaan tietoturvavalvomot tulee nähdä yhtenä nykyaikaisten organisaatioiden kriittisimmistä suojautumiskeinoista.

Kyberturvallisuuden sanaston (Sanastokeskus, 2018) määritelmän mukaan tietoturvavalvomolla tarkoitetaan organisaatiota tai sen osaa, joka muodostaa, seuraa ja analysoi tietoturvan tilannekuvaa ja toisaalta ennaltaehkäisee, tunnistaa ja analysoi tietoturvahäiriöitä. Tietoturvavalvomoiden tekninen toteutus voi olla organisaation omassa hallussa tai hankittu palveluna ulkoiselta toimittajalta (Pöyhönen ym., 2019). Tyypillisesti tietoturvavalvomo vastaa organisaation tietoturvapoikkeamien hallinnasta, mikä tarkoittaa toimenpiteitä, joilla organisaatio varautuu ja reagoi mahdollisten tietoturvahäiriöistä aiheutuneiden vahinkojen rajoittamiseen ja myös niistä toipumiseen. (Kokulu ym., 2019; Sanastokeskus, 2018.)

Zimmerman (2014, s. 24) korostaa, että iso osa tietoturvavalvomoiden työstä liittyy edunsaajien pitämiseen ajan tasalla järjestelmien tilasta. Siten tietoturvavalvomoiden tulee ymmärtää, mitä kybertoimintaympäristössä tapahtuu mikro- ja makrotasoilla. Tilannetietoisena pysyminen voi olla haastavaa, sillä tyypillisesti tietoturvavalvomot tulkitsevat tietoa useista erilaisista organisaation sisäisistä ja ulkoisista lähteistä ja kokonaisvaltaisen ymmärryksen luominen vaatii siten tietoturvavalvomoissa työskenteleviltä kykyä hahmottaa tapahtuminen vaikutussuhteita laajemmin. (Zimmerman, 2014, s. 24 & 26.) Organisaation kyky hyödyntää kansainvälisistä ja kansallisista verkostoista saatua tietoa näin ollen liittyy olennaisesti analysointikykyyn. Henkilöstön kyvyllä tulkita käytettävissä olevia tietolähteitä oikein on siten myös suuri merkitys tilannekohtaisten analyysien tekemisessä. (Pöyhönen ym., 2019).

3.4 Kybertilannekuva

Tässä osiossa tuodaan esille tilannekuvan muodostamiseen liittyviä erityispiirteitä kyberturvallisuuden näkökulmasta. Kyberturvallisuuden sanaston (Sanastokeskus, 2018) määritelmän mukaan kybertilannekuvalla tai kyberturvallisuuden tilannekuvalla (engl. cyber security situational picture, cyber security situation awareness) tarkoitetaan koottua kuvausta tietyllä hetkellä vallitsevasta tietojärjestelmien käytettävyys- ja turvallisuustilanteesta sekä kybertoimintaympäristön yleisestä tilanteesta, jota toteutetaan muun muassa mediaseuran-

nan kautta. Tunnusomaista kyberturvallisuuden tilannekuvan tuottamiselle on, että sitä tuotetaan usein yhteistyössä eri toimijoiden kesken. (Sanastokeskus, 2018.)

Zimmerman (2014, s. 26) jakaa kybertilannetietoisuuden saavuttamisen kolmeen komponenttiin:

1. informaatio
2. analytiikka
3. visualisointi (Zimmerman, 2014, s. 26).

Informaatiolla Zimmerman (2014, s. 26) viittaa erilaisiin tietolähteisiin, joita voi olla muun muassa sensoreilta saatava data, kyberuhkatiedustelun kautta saatava tieto, uutistapahtumat, laite- ja järjestelmätoimittajien julkaisemat haavoittuvuustiedot ja niin edelleen. Analytiikan avulla kerättyä tietoa tulkitaan ja jalostetaan (vrt. uuden tiedonluomisen prosessi ja merkityksellistäminen). Kolmannessa vaiheessa kerätty ja jalostettu tieto koostetaan esitettävään muotoon. (Zimmerman, 2014, s. 26.)

Tilannetietoisuuden pohjana teknisellä ja taktisella tasolla toimii erilaiset kyberturvallisuuden teknologiset ratkaisut, joiden avulla havainnointia toteutetaan ja järjestelmien tilaa arvioidaan. SIEM (engl. Security Information and Event Management) on esimerkki tällaisesta ratkaisusta, joka näyttäytyy myös yhtenä tietovirtana muodostettaessa kybertilannekuvaa. SIEM:in perusajatus on, että se kerää eri tapahtumalähteet yhteen ja tutkii tietomassaa reaaliaikaisesti. SIEM:iin voidaan tuoda syötteitä myös sensorijärjestelmän ulkopuolelta, kuten ajankohtaista haavoittuvuustietoa. Mikäli SIEM havaitsee mahdollisen poikkeaman, tekee se hälytyksen tapahtuman tarkempaa analyysia varten. Myös muun muassa tunkeilijan havaitsemisjärjestelmät (engl. Intrusion Detection System, IDS), palomuurit ja virustorjuntaohjelmat tuottavat merkityksellistä tietoa kyberturvallisuuden tilannetietoisuuden kannalta. (Lehto, 2019.)

Kybertilannekuva ei kuitenkaan muodostu pelkästään teknisestä syötteestä, vaan parhaimmillaan siihen on yhdistetty myös uhkatietoa ja yleistä tilannetietoa eri lähteistä (Laari ym., 2019). Laari ym. (2019) korostavat tässä tärkeimpänä elementtinä edelleen ihmistä, ”joka kykenee koostamaan tiedoista selkeän kokonaisuuden sekä tekemään siitä järkeviä johtopäätöksiä”. Ihmisen osaaminen ja kokemus nousevat näin ollen keskiöön (Laari ym., 2019).

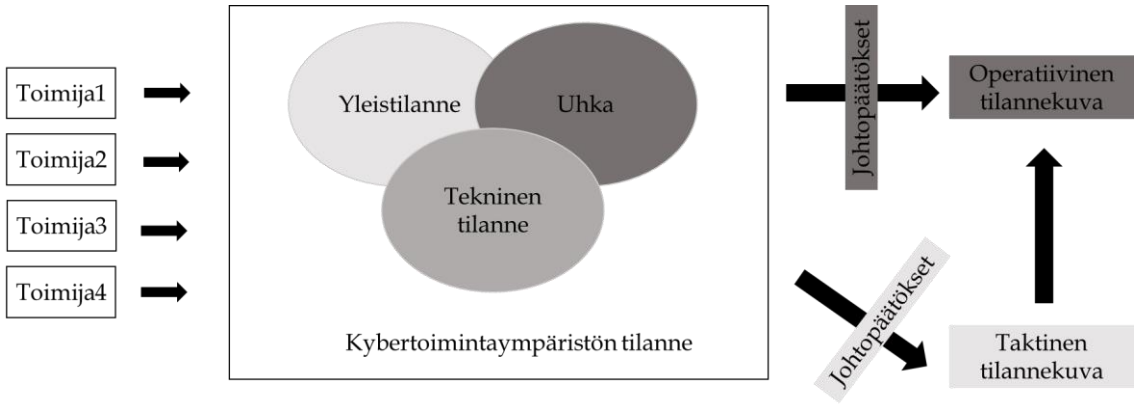
Yksi tapa jäsentää kybertilannetietoisuuden muodostumista on mallintaa sitä yhdysvaltalaisen John Boydin (1927–1997) alun perin sotilasoperaatioihin kehittämän OODA-kehyksen (engl. OODA-loop) avulla. Kybertilannetietoisuuden muodostuminen perustuu jatkuvasti tehtäviin havaintoihin (engl. observe), tilanteenarviointiin (engl. orient) yhdistettynä aiemmin koottuun tietoon ja kokemukseen, päätöksentekoon (engl. decide) tehdyn arvioinnin perusteella ja viimeisenä itse toimintaan (engl. act), jonka jälkeen kehä alkaa alusta. Perusajatuksena on, että ympäristöä tulee tarkastella useista eri näkökulmista ja pyrkiä tekemään päätöksiä tarvittavista toimenpisteistä ja toteuttamaan ne vastustajaa nopeammissa sykleissä. (Zimmerman, 2014, s. 26; Lehto, 2016.) Pöyhösen ym. (2019) mukaan tilannetietoisuuden prosessi rakentuu puolestaan tiedonke-

ruusta, tiedon kokoamisesta, luokituksesta ja analysoinnista, sekä analysoidun tiedon tehokkaasta ja oikea-aikaisesta jakamisesta sitä tarvitseville.

Tounsi ja Rais (2017) pohtivat kybertilannetietoisuuden 'oikea-aikaisuutta' eri tasoilla tarkasteltuna. Heidän näkemyksensä mukaan operatiivisella ja teknisellä tasolla tapahtuva toiminta ja tiedon hyödynnettävyys on mahdollista yleisesti lyhyemmän ajan tai vain lähes välittömästi, kun taas strategisella ja taktisella tasolla tiedon käyttöikä on jokseenkin pidempi (Tounsi & Rais, 2017). Toisaalta vaikka tiedon ajallinen hyödynnettävyys vaihtelee eri toiminnan tasoilla, korostuu kybertoiminnassa yleisesti toiminnan nopeus ja kyky reagoida sen mukaisesti. Lehto (2016) toteaakin sodankäynnin yhteydessä havaittavasta muutoksesta, että mikä aiemmin on käsittänyt toimintaa päivä-/tuntiasteikolla on muuttunut kyberulottuvuuden myötä minuutti-, ellei jopa sekuntiasteikolla tapahtuvaksi toiminnaksi. (Lehto, 2016.)

Kybertilannekuvan muodostamisen perusajatus on, ettei sitä voida tuottaa samanlaisin sisällöin kaikille tarvitsijoille, vaan sen sisältö ja tarvevaatimukset vaihtelevat eri päätöksenteko- ja johtamistasojen sekä toimijoiden välillä (Laari ym., 2019), mistä toisaalta muodostuvat eri toimijoiden uniikit vaatimukset tilannekuvatiedolle (Evesti, Kanstrén & Frantti, 2017). Kuusisto (2005) kuvaakin, ettei "tieto itsessään ei ole merkityksellistä, mikäli sitä ei ole sidottu johonkin päämäärään tähtäävään toimintaan", ja tällöin organisaation prosessit tulee nähdä tapana, jolla tietoa pyritään hyödyntämään. Yhtä lailla toimijoiden tulee jakaa ikään kuin samat lähtökohdat, jotta tilannetietoisuus on mahdollista saavuttaa. Käytännössä ympäröivän tietoavaruuden tulee mahdollistaa, että tieto ymmärretään oikein ja eri toimijoilla on myös pääsy heille tärkeään tietoon. (Pöyhönen ym., 2019.) Kuusisto ja Kuusisto (2006) viittaavat tähän yhteisen tietoalkion käsitteenä.

Laari ym. (2019) kuvaavat tilannekuvan muodostumisen taktisella ja operatiivisella tasolla yhdistelemällä ja analysoimalla toimijoiden tuottamaa sisältöä seuraavasti (kuvio 12):



KUVIO 12 Pelkistetty malli kybertilannekuvan muodostumisesta kyberpuolustuksen näkökulmasta (mukailtu Laari ym., 2019).

Kybertoimintaympäristöä kuvastaa sen nopeatempoisuus, mikä näkyy edellytyksenä hyvän tilannetietoisuuden ja nopean tiedonjaon osalta erilaisiin tapahtumiin varautuessa ja niiden hallinnassa. Luotettava ja reaaliaikainen tilannetietoisuus korostuu erityisesti tilanteissa, joissa on tehtävä nopeita ja laaja-alaisia päätöksiä, ja tällöin päätöksenteon perustana on nimenomaan oltava oikeat tiedot ja arviot meneillään olevista tapahtumista (Pöyhönen ym., 2019; Lehto, 2019). Tilannetietoisuus tukee lisäksi organisaation strategista johtamista muun muassa kyberriskienhallinnan ja laajemmin koko organisaation kyberturvallisuuden suorituskyvyn arvioinnin kautta (Pöyhönen ym., 2019). Kyberturvallisuusalalla oikean tiedon saaminen oikeaan aikaan voi auttaa päättäjiä vähentämään riskejä, sekä toisaalta kartoittamaan omia järjestelmiä hyökkääjien varalta ja myös edistämään kriisinsietokykyä eli resilienssiä (Goodwin & Nicholas, 2015). Tilannekuvan luominen on siten keskeinen osa organisaation kyberriskienhallintaa (Lehto, 2019).

Parishin ja Madaharin (2016) mukaan kybertilannetietoisuuteen liittyy monia haasteita, jotka heijastavat sosioteknisen kybertoimintaympäristön kompleksisuutta. Näitä ovat:

- monimutkainen arkkitehtuuri
- persistenssi ja laaja-alaisuus
- ’big data’
- paikka ja aika
- vaikutuksen nopeus
- attribuutio
- operatiivinen vaikutus (Parish & Madahar, 2016).

Parish ja Madahar (2016) viittaavat muun muassa persistenssillä ja laaja-alaisuudella siihen, kuinka teknologiset ratkaisut ovat monesti suoraan tai epäsuorasti yhteydessä jatkuvasti tai ajoittain verkottuneeseen maailmaan, minkä tuloksena on muodostunut osin tuntematon tai huonosti ymmärretty kokonaisuus, jota erilaiset uhkatoimijat pyrkivät jatkuvasti hyödyntämään. Toisaalta tilannetietoisuuden muodostamisen haasteisiin liittyvät kybertoimintaympäristössä merkittävästi paikan ja ajan näkökulmat. Kybertoiminta ei ole sidottu valtioiden rajoihin, mikä mahdollistaa samanaikaisesti globaalin ja paikallisen toiminnan ja sen vaikutukset. Kybertoimintaympäristössä vaikutusten nopeuteen liittyy kyky tarvittaessa myös nopeaan päätöksentekoon, jolloin edellytyksenä on reagointikykyinen organisaatio ja kyky tuottaa reaaliaikaista tilannekuvaa. Operatiivisten vaikutusten näkökulmasta kybertilannetietoisuus haastaa perinteisen strategisen, operatiivisen ja taktisen toimintahierarkian, sillä sen luominen edellyttää laajaa tilannetietoisuuden integrointia kaikilla sosioteknisen systeemin tasoilla. (Parish & Madahar, 2016.)

Tilannekuvan tuottamisen kannalta dynaamisen ja monimuotoisen kybertoimintaympäristön ajatellaan olevan yksilön kyvykkyyksien saavuttamattomissa, ja siten edellytyksenä nähdään tiimityöskentely (Eldardiry & Caldwell,

2015). Tilannetietoisuus ei toisin sanoen kehity yksilön tai pienen piirin sisällä, vaan se vaatii tiedon jakamista eri sidosryhmien välillä (Pöyhönen ym., 2019). Tiedonjakamista ja sen merkitystä käsitellään tarkemmin seuraavassa alaluvussa.

3.5 Tiedonjakaminen

> The approach, where one organization's detection becomes another's prevention, is a modern sophisticated concept that strengthens the organizations' security in advance. (Rizov, 2018.)

Tiedonjakaminen näyttäytyy kriittisenä tekijänä omaksuttaessa tietoa kyberhyökkäyksistä, ja on siten edellytys, kun varoitetaan toisia organisaatioita mahdollisista kehittyneistä uhkista (Skopik ym., 2016). Hyökkäyksen kohteeksi joutunut organisaatio omistaa arvokasta tietoa toteutuneista hyökkäystoimista, joiden jakaminen muiden kanssa on tärkeää. Tietojen jakaminen niin yksityisen kuin julkisen puolen sidosryhmien välillä on tehokas mekanismi jatkuvasti muuttuvan ympäristön parempaan hahmottamiseen ja ymmärtämiseen, sekä toisaalta kokonaisvaltaiseen oppimiseen mitä tulee riskeihin, haavoittuvuuksiin ja uhkiin, sekä näihin liittyviin ratkaisuihin. Jakamalla kyberuhkatietoa organisaatiot voivat tunnistaa kohteena olevat järjestelmät ja tietovarat, sekä saavat myös oleellista tietoa hyökkääjän pääsyyn käytättämistä tekniikoista ja mahdollisista muista tunnistetiedoista (Rizov, 2018.) Rizov (2018) listaa viisi hyötyä, jotka kyberuhkatiedon jakaminen luo:

- jaettu tilannetietoisuus (engl. shared situational awareness)
- parempi käsitys uhkasta (engl. enhanced threat understanding)
- tietämyksen kypsyminen (engl. knowledge maturation)
- laumasuoja (engl. herd immunity)
- sekä ketterämpi puolustus (engl. greater defensive agility). (Rizov, 2018.)

Kyberturvallisuutta käsittelevässä tutkimuksessa puhutaan usein termeillä 'tiedonvaihto' tai 'tiedonjakaminen' (mm. Skopik ym., 2016), mikä käytännössä viittaa samaan ilmiöön kuin tässä tutkimuksessa tarkasteltavat tietovirrat - eli tieto liikkuu lähettäjältä vastaanottajalle, mikä puolestaan liittyy laajemmin erilaisiin organisaation tietoprosesseihin. Tiedonjakamisen (engl. knowledge sharing) ja tiedonsiirtämisen (engl. knowledge tranfer) termejä käytetään Vuoren ym. (2018) mukaan yleisesti kuitenkin usein ristiin. Vuori ym. (2019) viittaavat Kingin (2006) näkemykseen, jonka mukaan tiedonsiirto on enemmän keskitettyä toimintaa, jossa on selvä tavoite ja vastaanottaja, kun taas tiedonjakamista voi tapahtua myös tiedostamatta useisiin suuntiin eikä sillä välttämättä ole selvää tavoitetta.

Tiedonjakamisen kannalta Skopik ym. (2016) listaavat viisi ulottuvuutta, jotka tulee ottaa huomioon perustettaessa laaja-alaista organisaatiokohtaista tai kansallista kyberturvallisuuskeskusta:

1. tehokas yhteistyö ja koordinointi
2. oikeudellinen ja sääntely-ympäristö
3. standardointipyrkimykset
4. alueelliset ja kansainväliset toteutukset
5. teknologian integrointi organisaatioiden välillä (Skopik ym., 2016.)

Ensimmäiseen ulottuvuuteen kuuluvat erilaiset tietoluokat, jotka ovat yhtä lailla merkityksellisiä eri sidosryhmille. Näihin lukeutuvat muun muassa tunnistetiedot (engl. indicators of compromise), tekniset haavoittuvuudet (engl. technical vulnerabilites) ja nollapäivähaavoittuvuuksien hyväksikäytöt (engl. zero day exploit) ja kriittiset palvelukatkokset (engl. critical service outage). Oikeudellisella ja sääntely-ympäristöllä Skopik ym. (2016) viittaavat tiedon jakamisen lainsäädännölliseen perustaan, jolla varmistetaan kriittisten sidosryhmien keskinäinen tiedonsaanti. Lainsäädäntöperustan lisäksi tiedonvaihto tulee sitoa jaettuihin standardeihin ja teknisiin lähtökohtiin. Edellä mainittujen ohella organisaatioilta edellytetään tiedonvaihtoa edistävien organisatoristen rakenteiden ja teknologisten valmiuksien kehittämistä niin alueellisella kuin kansainväliselläkin tasolla. Teknologisten valmiuksien osalta on keskeistä, että ne yhteensovitetaan organisaation muihin prosesseihin. (Skopik ym., 2016.) Pöyhönen ym. (2019) tuovat esille tietojärjestelmien tärkeyden tietolähteiden systemaattisen käytön ja yhteistyön mahdollistajana.

Tiedon jakaminen voi vaihdella satunnaisesta tiedonvaihdosta pitkäaikaisiin, muodollisesti perusteltuun organisaatioiden väliseen tiedonvaihtoon. (Goodwin & Nicholas, 2015). Goodwin ja Nicholas (2015) esittävät kaksi tiedonvaihdon mallia, joita ovat vapaaehtoisuuteen perustuva malli sekä pakollinen ilmoitusvelvollisuus. Ilmoitusvelvollisuuteen (engl. duty to notify) liittyy myös viranomaisten välinen tiedonvaihto, ja myös jossain määrin tiedonvaihto viranomaisten ja yksityisen sektorin toimijoiden välillä. (Pöyhönen ym., 2019.)

Tiedonjakamisen tärkeys kybertilannekuvan ja -turvallisuuden ylläpidossa on tunnistettu myös kansallisella ja kansainvälisillä tasoilla, mutta käytännöt ja toimintaperiaatteet eivät ole täysin vakiintuneet. Lähdekirjallisuuden perusteella kuitenkin ollaan yleisesti yhtä mieltä siitä, että tiedon jakaminen ja yhteistyön tekeminen vähentävät kyberturvallisuusriskiä. (mm. Tounsi & Rais, 2017; Skopik ym., 2016; Goodwin & Nicholas, 2015.) Käytännössä näkemyseroja ilmenee usein siinä:

- mitkä tahot jakavat tietoa
- mitä tietoa tulisi jakaa
- milloin tietoa tulisi jakaa
- mikä on tiedon luonne ja käyttöarvo, jota jaetaan
- miten tietoa jaetaan

- miksi tietoa jaetaan
- mitä tiedolla on mahdollista tehdä (Goodwin & Nicholas, 2015).

Vaikka tiedonvaihdon hyödyt ovat yleisesti tunnistettuja, nähdään kyberuhkatiedon jakaminen toisaalta monilta osin myös haasteellisena. Rizov (2018) näkee keskeisimpinä muun muassa luottamukseen, yhteistoimintaan sekä tiedon sensitiivisyyteen ja turvaluokitteluun liittyvät haasteet. Toisaalta myös juridiset lähtökohdat voivat asettaa tiettyjä haasteita tiedonvaihtoon eri toimijoiden välillä. Sen vuoksi onkin tärkeää laatia oikeudellinen kehys kyberturvallisuuteen liittyvän tiedon jakamiselle, joka pitää sisällään mitä tietoa, kenen kanssa ja mihin tarkoituksiin tietoja voidaan jakaa. (Rizov, 2018.)

3.5.1 Tiedonjakamisen käytännöt

Toimivan yhteistyön ja verkostotoiminnan edellytyksenä on tiedon oikeanlainen jakaminen ja käsittely. Kyberturvallisuuteen liittyvälle tiedonvaihdolle ja käsittelylle on tietyiltä osin velvoittavan lainsäädännön ohelle kehittynyt useita vapaaehtoisuuteen perustuvia säännöstöjä ja reunaehtoja, joiden avulla tiedon omistaja pystyy osoittamaan toiveensa tiedon käsittelylle ja edelleen jakamiselle luovuttaessaan tietoa eteenpäin omille sidosryhmille. Vapaaehtoisten tiedonvaihtokäytäntöjen kehityksen taustalla on ollut myös halu rohkaista erilaisia tiedonvaihtoryhmiä avoimeen tiedonvaihtoon. Luokitukset eivät kuitenkaan ole oikeudellisesti sitovia. (Kyberturvallisuuskeskus, 2022.)

Kenties yksi käytetyimmistä vapaaehtoisuuteen perustuvista säännöstöistä on muun muassa *Forum of Incident Response and Security Teams* -yhteisön (FIRST) standardoima TLP-käsittelyluokitus (engl. Traffic Light Protocol) (Kyberturvallisuuskeskus, 2022; FIRST, 2015–2022.) TLP-käsittelyluokitus on yleisesti vakiintunut kyberturvallisuuden kansallisissa ja kansainvälisissä yhteistyöryhmissä. Määritelmän mukaan varsinaisia käsittelyluokkia on neljä:

1. TLP:RED – henkilökohtainen jakelu
2. TLP:AMBER – tarveperustainen jakelu organisaation sisällä ja sen asiakkaille
    a. TLP:AMPER+STRICT – vain organisaation sisäinen jakelu
3. TLP:GREEN – yhteisön sisäinen jakelu
4. TLP:CLEAR – rajoittamaton jakelu (FIRST, 2015-2022).

Elokuussa 2022 uudistetussa protokollassa (TLP 2.0) TLP:AMBER:in alle on lisätty erillinen tarkenne (STRICT), jonka tarkoituksena on vähentää AMBER-luokittelun aiemmin herättänyttä tulkinnanvaraisuutta ja ennen kaikkea selkiyttää toimintatapaa (Gatlan, 2022). Alun perin TLP-protokolla kehitettiin, jotta tiedonvaihto eri toimijoiden ja tahojen välillä olisi helpompaa (FIRST, 2015–2022).

TLP-protokollan lisäksi yleisesti tunnettuja kyberturvallisuuteen liittyviä tiedonvaihto- ja yhteistyökäytäntöjä ovat Chatham House -sääntö sekä PAP-

luokittelu (engl. Permissible Actions Protocol). PAP-luokittelun avulla määritetään, mitä toimia vastaanotetulla tiedolla on mahdollista tehdä. Esimerkiksi PAP:RED, jolloin voidaan tehdä ainoastaan passiivisia toimia, jotka eivät ole hyökkääjän havaittavissa, kun taas PAP:GREEN mahdollistaa tiedon aktiivisen käytön puolustustoimissa, kuten liikenteen estämisessä (MISP Threat Sharing, 2022). Chatham House -sääntö puolestaan viittaa enemmän kokouskäytäntöihin, jolloin kokoukseen osallistujat voivat hyödyntää saamiaan tietoja edelleen, mutta eivät saa paljastaa myöhemmissä yhteyksissä tiedon alkulähdettä (Kyberturvallisuuskeskus, 2022).

Vapaaehtoisuuteen perustuvista säännöstöistä on hyvä erottaa, että viranomaiset noudattavat omassa toiminnassaan aina ensisijaisesti Suomessa julkisuuslakia (Kyberturvallisuuskeskus, 2022.) Laki viranomaisten toiminnan julkisuudesta ei pelkästään sääntele viranomaisten asiakirjojen ja muiden tietoaineistojen julkisuutta ja salassapitoa tai niihin liittyviä menettelyjä, vaan se pitää sisällään myös säännökset viranomaisten velvollisuuksista omassa tehtävässään edistää tiedonsaantia (L 906/2019; L 21.5.1999/621).

Useissa lähteissä toiminnan keskiöön nousee toimijoiden välisen keskinäisen luottamuksen merkitys (mm. Goodwin & Nicholas, 2015; Vázquez ym., 2012; Tounsi & Rais, 2017). Vázquez ym. (2012) mukaan tiedonjakaminen usein epäonnistuu käytännössä, koska osapuolet eivät välttämättä luota siihen, että jaettua tietoa hyödynnetään asianmukaisesti. Tätä ongelmaa lieventää erilaiset tietohallinnolliset prosessit, joiden avulla tietoa suojataan ja hallitaan koko sen elinkaaren ajan (Vázquez ym., 2012). Luottamussuhteet itsessään lisäävät luottamusta siihen, että annettuja tietoja edelleen käsitellään asianmukaisesti. Luottamuksen osalta on myös tunnistettava, ettei sitä voida säännellä esimerkiksi lainsäädännöllä, vaan se perustuu toimijoiden käytännön näyttöihin. Lainsäädännöllä toimijoita voidaan velvoittaa raportoimaan poikkeamista, mutta itsessään se ei lisää luottamusta tai yhteistyötä toimijoiden välillä tai vähennä tiedonvaihtoon liittyviä riskejä. Luottamuksen rikkoutuessa seuraukset voivat olla merkittäviä kaikille osapuolille. (Goodwin & Nicholas, 2015.)

3.5.2 Uhkatiedon jakomallit ja alustat

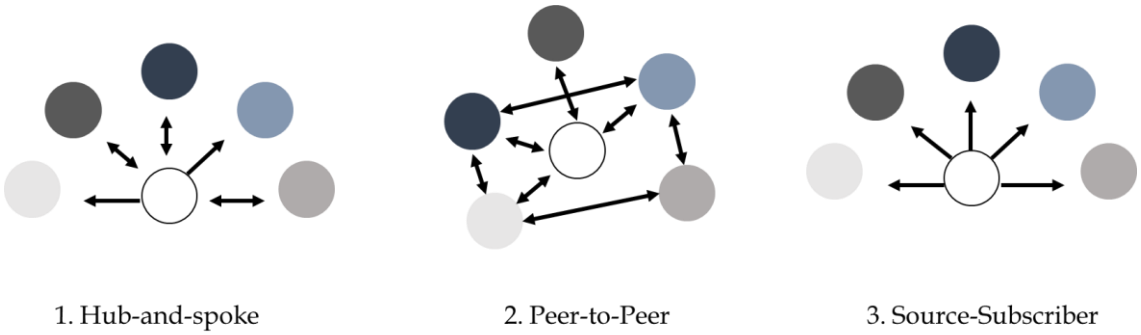
Tiedonjakamisen sovitut käytännöt tarjoavat pääsyn sellaisiin uhkatietoihin, jotka eivät monesti muuten olisi organisaation saatavilla. Keskeistä on, että jaettujen resurssien avulla organisaatiot voivat parantaa kyberturvallisuuden tasoaan hyödyntämällä kumppaniensa tietämystä, kokemusta ja kykyjä kyberuhkiin liittyen ennakoivalla tavalla. (Rizov, 2018.) Uhkatiedon jakamisella viitataan yleisesti luotettujen kumppanien väliseen tiedonvaihtoon. Taustalla on ajatus siitä, että yhden organisaation havainnoista voi tulla toisen organisaation mahdollisuus ennaltaehkäistä kyberhyökkäyksiä omia tietojärjestelmiään vastaan. (Connolly, Davidson & Schmidt, 2014.)

Kyberuhkatiedon jakamiskäytännöt näyttäytyvät usein joko aikaa vievinä manuaalisina prosesseina tai joukkona erillisiä, yhteisökohtaisia automaatioratkaisuja (Connolly ym., 2014). Käytäntöjen yhtenäistämiseksi on aiemmin mai-

nittujen tiedonkäsittelyluokitusten (mm. TLP) lisäksi kehitetty erilaisia malleja, teknisiä standardeja ja protokollia, joiden avulla on tarkoitus mahdollistaa niin sanotusti yhteisen kielen ja ymmärryksen saavuttaminen sekä siten edistää tiedonvaihtoa. Näitä mekanismeja voidaan pitää tietojohtamisen teoriasta johdettuina käytännön toteutustapoina kyberturvallisuuden kontekstissa – arvoverkossa, joka pyrkii ylläpitämään kyberturvallisuutta.

Näistä kenties yleisimpiä esimerkkejä ovat MITRE Corporationin kehittämät standardit uhkatiedon esittämiseen (Structured Threat Information eXpression, STIX), uhkatiedon välittämiseen (Trusted Automation eXchange of Indicator Information, TAXII) sekä havaintojen kuvaamiseen (Cyber Observable Expression, CyBOX) (Vertainen ym., 2021). TAXII:n perusajatus piilee siinä, että se mahdollistaa monimutkaisten tiedonvaihtorakenteiden muodostamisen eri toimijoiden kesken. STIX-datarakenteiden avulla puolestaan kyberuhkatietojen jakaminen on formalisoitua ja tehokasta. (Kokkonen, Hautamäki, Siltanen & Hämäläinen, 2016.)

Kuviossa 13 on kuvattu kolme yleisintä uhkatiedon jakomallia. Uhkatiedon jakomalleista ensimmäisessä (engl. hub-and-spoke) tiedonvaihdon koordinointikeskuksena toimii yksi organisaatio, joka vastaanottaa ja ohjaa tietoa muille tiedonvaihtoyhteisön jäsenille. Tässä mallissa tieto voi virrata miltä tahansa yhteisön jäseneltä tiedonvaihdon koordinointikeskukseen eli ”hubiin” ja päinvastoin. Tiedonvaihdon koordinointikeskus voi omalta osaltaan analysoida ja suodattaa tietoa ennen sen edelleen jakelua. Hautamäen ja Kokkosen (2020) mukaan tämä malli toimii parhaiten pienissä toimintaverkostoissa, joissa tiedon jakaminen ei näyttäydy liian aikakriittisenä tekijänä. Toisessa mallissa (engl. peer-to-peer) organisaatiot voivat toimia sekä tiedon tuottajina että kuluttajina, jolloin tietovirrat muodostuvat kumppanien välisestä vapaammasta tiedonvaihdosta. Kolmannessa mallissa (engl. source-subscriber) yksi organisaatio toimii ainoana tietolähteenä kaikille tilaajille. Tässä mallissa tieto virtaa yksisuuntaisesti. (Connolly ym., 2014.)



KUVIO 13 Uhkatiedon jakomallit (Connolly ym., 2014).

Kyberhyökkäysten yleistyessä erilaiset julkisesti saatavilla olevat tietoturvallisuusalustat ja tietolähteet ovat yleistyneet, joista kuka tahansa voi etsiä tietoa tunnistetuista uhkista, uusista haittaohjelmista ja tietokoneviruksista, sekä kuinka suojautua näiltä. Julkisesti saatavilla oleva tieto on kuitenkin yleensä geneeristä, eikä siten tarjoa toimialakohtaista ja perusteellista tietoa havaituista

kyberuhkista. (Skopik ym., 2016). Jotta tiedolla on enemmän arvoa kyberturvallisuuden ammattilaiselle, vaaditaan alustoilta toimialakohtaista niin sanotusti kovan tiedon ja myös kokemuksellisen tiedon saatavuutta. Toisaalta keskeinen vaatimus tiedonvaihdolle on, miten tietoa on mahdollista jakaa ilman että organisaation oma toiminta vaarantuu (Hautamäki & Kokkonen, 2020). Korkean riskin tiedoista, kuten sisäiset tietoturvakonfiguraatiot tai jonkin tietyn uhkatoimijan hyökkäysmenetelmistä, ollaan yleisesti tarkempia ja näiden osalta automatisoitua tiedonvaihtoa ei suosita. Matalamman riskin tietojen, kuten tietoturvaohjeiden tai yleisen uhkatiedon jakaminen automatisoidusti ei edellytä yhtä korkeaa luottamuksen tasoa kuin korkean riskin tiedonvaihto (Vázquez ym., 2012).

Kybermaailmassa uhkatiedon jakamisalustat toimivat niin ikään kuin tietovarantoina ja tiedonhallintaa edistävinä työkaluina. Kenties yksi käytetyimmistä tiedon jakamistyökaluista on alun perin Belgian ja Naton yhdessä kehittämä, nykyisin avoimen lähdekoodin ohjelmisto *Malware Information Sharing Platform* eli MISP. Se tarjoaa keskitetyn tunnistetietokannan, johon on mahdollista yhdistää niin teknistä kuin ei-teknistä informaatiota haittaohjelmista tai hyökkäyksistä. MISP luo automaattisesti relaatioita eri tapahtumien välille perustuen tapahtumissa havaittuihin yhtäläisiin teknisiin tunnisteisiin. Se mahdollistaa lisäksi teknisten luottamusverkostojen muodostamisen organisaatioiden erillisten MISP-järjestelmien välille, mikä mahdollistaa informaation jakamisen luottamusverkostoille automaattisesti, sekä erikseen luotujen alayhteisöjen välisen tiedonvaihdon erillisten erikseen määritettyjen parametrien mukaan. (Skopik ym., 2016.)

Yhtenä keskeisenä haasteena tiedonjakoalustojen osalta Dandurand ja Serrano (2013) mukaan on kuitenkin ollut tarvittavien mekanismien puuttuminen isojen tietomassojen jakamiseen. Toisaalta myös eri datalähteissä saatetaan käyttää erilaisia termejä tarkoittamaan samaa sisältöä, jolloin datalähteiden yhteensovittaminen ja lisäksi niistä tehtävät tulkinnat ovat haastavia. Tiedonvaihdon taustalla on oltava jaettu kyberturvallisuudensanasto ja taksonomia (Vázquez ym., 2012), mikä siten muodostaa yhteisen ymmärryksen ja toimintamahdollisuuksien perustan sekä lisää luottamusta toimijoiden välillä. Skopikin ym. (2016) mukaan merkittävimmät tiedonvaihtoa hidastavat tekijät liittyvät kuitenkin nimenomaan teknisiin valmiuksiin, kuten käytössä oleviin alustoihin ja työkaluihin, joiden avulla tietoa vaihdetaan ja hallitaan.

4 TUTKIMUSMENETELMÄT

Tässä luvussa käsitellään tutkielman tutkimusmenetelmiä ja sen eri vaiheita. Ensimmäisenä esitetään tutkimusstrategia, minkä jälkeen käsitellään tähän tutkimukseen valittuja aineistonkeruu- ja analyysimenetelmiä.

4.1 Tutkimusstrategia

> Yhtä turvallisuutta ja turvallisuuden tutkimusta ei -- voi olla, mutta aidosti monitieteistä turvallisuuksien eri puolien, ulottuvuuksien, ilmiöiden ja keskinäisriippuvuuksien tutkimusta voi ja sitä tarvitaan -- (Virta, 2011, s. 112–113).

Tutkimusstrategialla tarkoitetaan tutkimuksen menetelmällisten ratkaisujen kokonaisuutta (Hirsjärvi, Remes & Sajavaara, 2009, s. 132). Tutkimusstrategian valintaa ohjaa valittu tutkimustehtävä tai tutkimukselle annettu tarkoitus, jota yleensä luonnehditaan neljän piirteen perusteella:

- kartoittava
- selittävä
- kuvaileva
- ennustava. (Hirsjärvi ym., 2009, s. 132 & 137–138.)

Yhdellä tutkimuksella voi olla useampi tarkoitus ja se voi myös muuttua tutkimuksen edetessä (Hirsjärvi ym., 2009, s. 138.). Tämä tutkimus näyttäytyy kartoittavana, mutta myös osiltaan aihealuetta selittävänä ja kuvailevana tutkimuksena. Tutkimuksen tavoitteena on pyrkiä tunnistamaan parhaat käytänteet tietovirtojen hallintaan organisaatioiden kybertilannekuvaa muodostavissa toiminteissa. Parhaiden käytänteiden tunnistamiseksi tutkimuksessa selvitetään tietovirtojen muodostumisen ja niiden hallinnan yleisiä periaatteita, sekä lisäksi pyritään tunnistamaan, millaisia käytännön haasteita näihin mahdollisesti liittyy.

Tutkimusasetelman perusteella lähestymistavaksi valikoitui kvalitatiivinen eli laadullinen tutkimustapa. Hirsjärven ym. (2009, s. 81) mukaan laadullinen tutkimustapa valitaan tyypillisesti silloin, kun aihealue on entuudestaan jokseenkin tuntematon eikä sitä kyetä ennakoimaan. Kirjallisuuskatsauksen perusteella tutkimuksen aihealue on vielä jokseenkin tutkimaton, eikä kybertilannekuvan muodostumisen kontekstissa tehtyä selkeää tietovirtatutkimusta tunnistettu tämän tutkimusprosessin aikana, mikä osaltaan puoltaa laadullista lähestymistapaa tälle tutkimukselle. Tutkimuksessa keskitytään tarkasteltavan kokonaisuuden laadullisiin ominaisuuksiin ja sen ulkopuolelle rajataan määrällisten ominaisuuksien, kuten tiettyjen tietovirtojen vahvuuksien tarkastelu määritetyn ajanjakson sisällä.

Tutkittavasta aihealueesta löytyy piirteitä niin etnografisesta kuin myös tapaustutkimuksesta (engl. case study), joten tutkimus päätettiin toteuttaa monimenetelmäisenä kvalitatiivisena tutkimuksena. Tyypillisesti laadullisella tapaustutkimuksella tarkoitetaan jonkin aiheen tai ilmiön kokonaisvaltaista ymmärtämistä sen luontaisessa ympäristössä tai kontekstissa (Saunders ym., 2019, s. 196–197), joka tässä tapauksessa on tietovirtoihin ja niiden hallintaan liittyvät tunnuspiirteet kybertilannekuvan muodostamisen kontekstissa. Tapaustutkimus keskittyy tarkasteltavan aiheen tai ilmiön ja sen kontekstin vuorovaikutussuhteen hahmottamiseen. Lisäksi tapaustutkimusta käytetään usein silloin, kun tutkittavan ilmiön tai kontekstin väliset rajat eivät ole ilmeisiä. (Saunders ym., 2019, s. 196–197.) Saunders ym. (2019, s. 197) korostavat kontekstin ymmärtämisen merkitystä perusteena tapaustutkimukselle, minkä vuoksi tätä tutkimusta tehdessä kirjallisuuskatsauksessa on pyritty kuvaamaan yleisen tietojohtamisen teoriakehyksen lisäksi kybertoimintaympäristöä ja siihen sidoksissa olevia, tunnistettuja tietovirtoihin ja niiden hallintaan liittyviä elementtejä mahdollisimman kattavasti.

Etnografinen tutkimus puolestaan keskittyy ihmisiin ryhmissä, joissa he ovat vuorovaikutuksessa toistensa kanssa ja jakavat saman tilan tai paikan käsitteen, joka voi olla esimerkiksi työyhteisö, organisaatio tai yhteiskunta (Saunders ym., 2019, s. & 200). Tässä tutkimuksessa tilan käsite muodostuu kybertilannekuvaa muodostavien organisaatioiden tai niiden osien, sekä toisaalta myös laajemmin tiedonvaihtoverkoston käsitteen ympärille. Tutkimusta lähestytään tulkitsevan etnografian (engl. interpretive ethnography) lähtökohdasta, jonka mukaan on mahdollista, että asialle löytyy useita selittäviä merkityksiä yhden, todellisen merkityksen sijaan. Tämän näkemyksen mukaan monimerkityksellisyys muodostuu eri osallistujien sosiaalisesti rakentamissa tulkinnoissa, mikä mahdollistaa moniarvoisen perustan merkitysten ymmärtämiseen (Saunders ym., 2019, s. & 200.) Kybertilannekuvan muodostamisen taustalla voi olla erilaisia organisaatioiden tietotarpeita sekä toisaalta lakisääteisiä tehtäviä, jotka määrittävät esimerkiksi organisaation toimivaltuuksia ja roolia tiedonvaihtoverkostossa. Lisäksi tutkimuksen lähtöoletuksena on, että ihmisten osaaminen, kokemus ja tulkinnat vaikuttavat tietovirtoihin ja niiden hallintaan kybertilannekuvan muodostamisen kontekstissa, jolloin tutkittavasta ilmiöstä voi nousta esiin monenlaisia selittäviä merkityksiä perustuen yksilöiden tekemiin tulkin-

toihin ja käsityksiin. Olennaista etnografisessa tutkimuksessa on, että ilmiön tai asian havainnoinnin nähdään kohdistuvan osallistujiin (engl. participants) kohteiden (engl. subjects) sijaan, jolloin tulokulma on osallistavampi ja sisältää vuorovaikutussuhteen myös tutkittavan ja tutkijan välillä (Saunders ym., 2019, s. & 200).

Hirsjärvi ym. (2009, s. 81) painottavat joustavaa ongelmanasettelua edellytyksenä kvalitatiiviselle tutkimukselle. Jo pelkästään kontekstina kybertoimintaympäristö pitää sisällään mahdollisuuden nopeisiinkin muutoksiin, joten tutkimusasetelman muuttuminen nähdään mahdollisena tutkimuksen edetessä. Laadullisessa tutkimuksessa joustavuus toisin sanoen tarkoittaa sitä, että aihetta voidaan mahdollisesti joutua tarkentamaan tai jopa suuntaamaan uudelleen aineistonkeruun edetessä. Laadullisessa tutkimuksessa ei yleensä myöskään puhuta tutkimusongelmasta vaan nimenomaan tutkimustehtävästä, joka asetetaan yleisellä tasolla. (Hirsjärvi ym., 2009, s. 81 & 126).

4.2 Aineistonkeruumenetelmä

Aineistonkeruun perusajatus on, että siinä tulee hyödyntää metodia, joka parhaiten soveltuu tutkimustehtävän ratkaisemiseen (Hirsjärvi ym., 2009, s. 185). Tässä tutkimuksessa tutkimuskysymyksiin vastaamiseksi tarvitaan laaja-alaisesti tietoa tietovirtojen ja niiden hallinnan käytännön sovelluksista kybertilannekuvan muodostumisen kontekstissa yhdistettynä ihmisten kokemusperäiseen tietoon, joten aineisto päätettiin kerätä kahdella menetelmällä – havainnoimalla sekä haastatteluilla. Seuraavissa alaluvuissa on avattu ja perusteltu tarkemmin aineistonkeruumenetelmien valintaa tämän tutkimuksen kannalta.

4.2.1 Havainnointi

Tässä tutkimuksessa yhdeksi aineistonkeruumenetelmäksi valittiin havainnointi. Sen avulla voidaan saada ”välitöntä, suoraa tietoa yksilöiden, ryhmien tai organisaatioiden toiminnasta ja käyttäytymisestä”, jolloin aineistonkeruumenetelmänä siinä korostuu mahdollisuus tarkastella asioita tai ilmiöitä juuri niiden luontaisessa ympäristössä (Hirsjärvi ym., 2009, s. 213). Tässä tutkimuksessa havainnointi toteutettiin osana erästä kotimaista kyberturvallisuusharjoitusta syksyllä 2021, johon osallistui useita eri toimijoita. Havainnointi painottui yhden organisaation kybertilannekuvatoiminteen tarkkailuun. Havainnointiin pyydettiin erillinen lupa harjoituksen järjestäjältä sekä lisäksi harjoitukseen osallistuvilta organisaatiolta suullisesti.

Havainnoinnin on todettu olevan sopiva muun muassa vuorovaikutuksen sekä nopeasti muuttuvien ja ennakoimattomien tilanteiden tutkimuksessa (Hirsjärvi ym., 2009, s. 213) sekä silloin, kun tutkittavasta ilmiöstä ei juurikaan tiedetä tai siitä on vaikea saada tietoa (Tuomi & Sarajärvi, 2018, s. 94). Kybertoimintaympäristö tyypillisesti kuvataan nopeasti muuttavaksi ja vahvasti en-

nakoimattomaksi. Tässä tutkimuksessa havainnoinnin avulla pyritään muodostamaan käsitys tietovirtojen ja niiden hallinnan periaatteista kybertilannekuvan muodostamisen kontekstissa yhden organisaatiotoiminteen näkökulmasta.

Tarkkailtava toiminne muodostui yhteensä seitsemän henkilön kokoonpanosta, joilla kullakin oli hieman oma vastuualueensa kybertilannekuvan muodostamisen osalta; yhtenä asiantuntijavastuualueensa oli organisaation sisäiset tietovirrat, toisena ulkoiset sidosryhmät ja kolmantena uhkatiedustelun osakokonaisuus. Neljäs asiantuntijapositio muodostui CERT-roolista, joka toimi organisaation poikkeamatilanteissa ensivasteena. Näiden asiantuntijaroolien lisäksi mukana oli tilannekuvatoiminteen ns. tiimivetäjä sekä koko yksikön päällikkö. Näiden kahden position erona oli, että tiimivetäjä vastasi tilannekuvan muodostamisesta ja tiimin sisäisestä tehtävien koordinoimisesta, kun taas päällikköroolissa toimivan henkilön vastuulle kuului ylemmällä tasolla tehtävien koordinointi ja raportointi ylemmille tahoille koskien muun muassa lisäresursointitarpeita tai tehtävien priorisointia. Hirsjärven ym. (2009, s. 212) mukaan havainnoinnin avulla on lisäksi mahdollista selvittää toimivatko ihmiset kuten he sanovat toimivansa, mikä sen vuoksi täydentää sopivasti tässä tutkimuksessa haastatteluista muodostuvaa pääaineistoa.

Havainnoinnin lajeja on useita, mutta laadullisessa tutkimuksessa tyypillisemmin hyödynnetään osallistuvaa havainnoinnin lähestymistapaa (Hirsjärvi ym., s. 214–216). Osallistuvassa havainnoinnissa tutkija toimii aktiivisessa vuorovaikutuksessa tarkkailtaviensa kanssa. Sitä voidaan tarkastella eri asteisena, jolloin havainnoinnin kohteena olevaan toimintaan osallistuminen nähdään joko ryhmän täydellisenä jäsenenä tai osallistujan roolissa. Osallistujan roolissa havainnoijan asema tarkkailtavaan kohteeseen nähden on tuotu selvästi esille ryhmän jäsenille, kun taas täydellisen osallistumisen näkökulmasta havainnoija ei välttämättä ”paljasta” omaa tutkijan asemaansa ryhmälle, mikä nähdään tutkimuseettisesti hieman ongelmallisena. (Tuomi & Sarajärvi, 2018, s. 94–95; Hirsjärvi ym., 2009, s. 217.) Tässä tutkimuksessa havainnointi toteutettiin osallistujan roolissa, jolloin tarkkailun kohteena oleva joukko oli tietoinen tutkijan läsnäolosta ja toiminnan havainnoinnista. Havainnoinnin aikana esitettiin myös tarkentavia kysymyksiä toimintaan osallistuneille henkilöille. Havainnointia aineistonkeruumenetelmänä on kuitenkin kritisoitu siitä, että se saattaa häiritä tutkimustilannetta ja jopa muuttaa sen kulkua tai havainnoija saattaa sitoutua tilanteeseen liian tunneperäisesti, jolloin tutkimuksen objektiivisuus kärsii (Hirsjärvi ym., 2009, s. 213).

Havainnoinnin haasteena on tyypillisesti myös tiedon tallentaminen havainnointitilanteessa, ja tutkijan täytyy monesti luottaa vain omaan muistiinsa (Hirsjärvi ym., 2009, s. 213–214). Tässä tutkimuksessa havainnoinnin tukena harjoituksen järjestävän organisaation puolesta oli mahdollista hyödyntää muutamia tarkkailuun suunniteltuja työkaluja, jotka mahdollistivat muun muassa pelaajien käyttämien tiedonjakamis- ja vaihtokanavien seurannan. Havainnoinnin aikana hyödynnettiin lisäksi organisaatiolle ennalta laadittua tarkkailusuunnitelmaa, jonka pohjalta tarkkailua kohdennettiin tutkimuksen kannalta keskeisiin osa-alueisiin. Tarkkailun aikana havaintoja kirjattiin muistiin kynä ja

paperi -periaatteella. Harjoituksen päätteeksi keskeisimmistä havainnoista laadittiin erillinen tarkkailuraportti tarkkailtavalle organisaatiolle, jota hyödynnetään myös tämän tutkimuksen aineistona osin peitetysti.

4.2.2 Teemahaastattelut

Tutkimuksen pääaineisto muodostuu haastatteluista. Hirsjärven ym. (2009, s. 205) mukaan haastattelun merkittävin etu muihin aineistonkeruumenetelmiin nähden on, että se sallii joustavuuden niin haastattelutilanteessa kuin myös tulosten tulkinnassa. Haastattelijan on esimerkiksi mahdollista selventää esittämiään kysymyksiä, oikaista mahdollisia väärinymmärryksiä sekä käydä keskustelua, mikä edesauttaa mahdollisimman laajan ja kattavan aineiston saavuttamista (Tuomi & Sarajärvi, 2018, s. 85).

Haastattelut päätettiin toteuttaa tutkimuksen viitekehykseen sidottuina teemahaastatteluina. Teemahaastattelun perusidea on, että se etenee etukäteen valittujen teemojen mukaisesti, joihin liittyen on mahdollista esittää tarkentavia ja syventäviä kysymyksiä haastateltavan vastausten perusteella (Tuomi & Sarajärvi, 2018, s. 87–88). Teemahaastatteluissa korostuvat ihmisten tulkinnat asioista sekä niille antamat merkitykset (Tuomi & Sarajärvi, 2018, s. 88). Ihmisten ja inhimillisten tekijöiden liittyessä oleellisesti tämän tutkimuksen aihepiiriin, haastatteluilla voidaan saada havainnoinnin tueksi yksilöiden kokemusperäistä, asioita ja toimintatapoja selittävää tietoa muun muassa haasteista, joita tietovirtojen hallintaan mahdollisesti liittyy. Hirsjärven ym. (2009, s. 206) mukaan haastattelun heikkous aineistonkeruumenetelmänä kuitenkin on, että se vie tyypillisesti paljon aikaa eikä sen perusteella voida lähtökohtaisesti johtaa kovin yleistäviä johtopäätöksiä. Haastatteluaineisto nähdään lisäksi aina konteksti- ja tilannesidonnaisena (Hirsjärvi ym., 2009, s. 207).

Koska laadullisessa tutkimuksessa pyritään tyypillisesti ymmärtämään tiettyä toimintaa, kuvaamaan tai tekemään tulkintoja jostain ilmiöstä tai asiasta, on perusteltua, että haastatteluihin valitaan henkilöitä, joilla on entuudestaan mahdollisimman paljon tuntemusta tutkittavasta aiheesta tai ilmiöstä (Tuomi & Sarajärvi, 2018, s. 87 & 98). Tässä tutkimuksessa haastateltavia haettiin useammasta eri organisaatiosta, profiililtaan sekä kyberturvallisuuden tietojohtamisesta sekä kybertilannekuvan muodostamisen periaatteita tuntevia henkilöitä.

Haastateltavien valinnassa sovellettiin osittain niin sanottua lumipallootantaa. Tuomen ja Sarajärven (2018, s. 99) määritelmän mukaan lumipallootannalla tarkoitetaan haastattelujen toteutusta siten, että alkutilanteessa tiedetään tutkittavan ilmiön kannalta yksi tai useampi avainhenkilö, jotka ohjaavat tutkijan edelleen seuraavien sopivien tiedonantajien luo. Avainhenkilöiden valinnassa noudatettiin harkinnanvaraisuutta perustuen alustavaan suunnitelmaan potentiaalisista haastateltavista. Avainhenkilöiltä saatujen suositusten pohjalta lähestyttiin muutamia henkilöitä lisää, minkä myötä näkökulmaa saatiin laajennettua alkuperäisestä suunnitelmasta poiketen yhdellä organisaatiolla lisää. Yhteensä haastatteluja toteutettiin kahdeksan ja ne kattoivat neljän eri organisaation näkemyksiä tutkittavasta aihepiiristä. Aineiston riittävyyden osalta

pyrittiin tilanteeseen, jossa esiin ei nouse enää uusia, toisistaan merkittävästi poikkeavia vastauksia vaan aineistossa alkavat toistua samat teemat eli puhutaan aineiston kyllääntymisestä (Tuomi & Sarajärvi, 2018, s. 99).

Haastatteluja varten muodostettiin teemahaastattelurunko, joka koostui viidestä osakokonaisuudesta ja yhteensä kahdeksastatoista niiden käsittelyä tukevasta kysymyksestä. Käsiteltävät osakokonaisuudet olivat seuraavat:

1. kybertilannekuvan muodostaminen ja siihen liittyvät erityispiirteet
2. tietovirtojen hahmottaminen
3. kyberturvallisuuden yhteistoimintaverkosto
4. yksilön asiantuntijuuden merkitys
5. haasteet ja kehittämiskohteet.

Teemahaastatteluille on tyypillistä, että käsiteltävät teemat ovat etukäteen tiedossa, mutta kysymysten muotoilu ja esitysjärjestys voi vaihdella (Hirsjärvi ym., 2009, s. 208). Haastateltavien pohdinnan tueksi annettiin lisäksi valmiina kolmijako, joka ohjasi heitä pohtimaan tarkasteltavia teemoja niin organisaation, verkoston kuin laajemmin yhteiskunnallisesta näkökulmastakin.

Haastattelut toteutettiin loka-marraskuussa 2022 äänitallentamisen mahdollistavalla kokoussovelluksella verkon yli yksilöhaastatteluina. Haastatteluiden toteutuksessa ja aineiston taltioinnissa hyödynnettiin turvallisuusluokitellun aineiston (TL IV) käsittelyn mahdollistavaa verkkoympäristöä. Tutkija oli valmistautunut haastatteluiden yhteydessä kiinnittämään erityistä huomiota siihen, että vastaukset pysyivät ympäristön salliman turvaluokan puitteissa, jotta aineiston jatkokäsittely olisi mahdollista julkisen tutkimuksen puitteissa. Haastateltaville kerrottiin käsiteltävät teemat ja työn julkisuusperiaate etukäteen kirjallisesti sovittaessa haastatteluajankohtia. Haastateltavien erillistä valmistautumista ei tämän tutkimuksen kannalta katsottu tarpeelliseksi, sillä tarkoitus oli selvittää haastateltavien aitoja näkemyksiä tutkimuksen aiheesta. Kestoltaan haastattelut vaihtelivat noin 50 minuutin ja 1,5 tunnin välillä. Kysymysten asettelu oli rakennettu mahdollisimman avoimeksi, mikä näkyi myös haastateltavien vastausten polveiluna sekä taipumuksena vastata kysymyksiin melko laajasti. Tutkijan vastuulla oli huolehtia keskustelun sujumisesta, teemojen taustoittamisesta sekä kysymysten mahdollisesta tarkentamisesta, mikäli haastateltava ei meinannut saada niistä kiinni. Äänitallenteet litteroitiin tarkempaa aineiston analyysia varten manuaalisesti ja samalla anonymisoitiin tutkimuksen kannalta epäolennaiset organisaatio- ja henkilöviittaukset pois litteroidusta aineistosta, jolla pyrittiin osin varmistamaan tutkimuksen julkisuus. Haastateltaville annettiin lisäksi mahdollisuus kommentoida ja täydentää tutkimuksessa esiin nousseita asioita ennen työn lopullista julkaisua.

4.3 Aineistonanalyysi

Laadullinen analyysi jaotellaan usein induktiiviseen, deduktiiviseen tai abduktiiviseen päättelyn logiikkaan. Induktiivisella päättelyllä tarkoitetaan sitä, että yksittäisistä havainnoista pyritään luomaan yleistettäviä päätelmiä, kun taas deduktiivisessa yleisestä päätelmää peilataan yksittäisiin havaintoihin. Abduktiiviseen päättelyyn puolestaan liittyy jokin johtoajatus, jonka kautta tutkimuksessa pyritään tekemään havaintoja. Analyysiä on mahdollista tarkastella myös laadullisen tutkimuksen teorian tai teoreettisen merkityksen avulla, jolloin puhutaan usein aineistolähtöisestä, teoriaohjaavasta (myös teoriasidonnainen) tai teorialähtöisestä analyysistä. (Tuomi & Sarajärvi, 2018, s. 107–108.)

Tässä tutkimuksessa analyysimenetelmäksi valittiin teoriaohjaava sisällönanalyysi. Sisällönanalyysiä pidetään yleisesti soveltuvana monenlaiseen tutkimukseen tarjoten väljän teoreettisen kehyksen kuultujen, kirjoitettujen ja nähtyjen aineistojen analyysiin, ja sitä pidetään myös eräänlaisena perusanalyysimenetelmänä kaikissa laadullisen tutkimuksen perinteissä (Tuomi & Sarajärvi, 2018, s. 103). Teoriaohjaavalla analyysillä tarkoitetaan menetelmää, jossa tutkimuksessa käsitelty teoria voi toimia analyysin apuna, mutta se ei ole täysin sidottu esitettyyn teoriaan. Teoriaohjaavasta analyysistä on mahdollista tunnistaa aiemman tiedon vaikutus tehtyyn analyysiin, mutta sen ei kuitenkaan ole tarkoitus olla niin sanotusti teoriaa testaava vaan enemmänkin uusia ajatuksia ja näkökulmia avaava (Tuomi & Sarajärvi, 2018, s. 109).

Haastatteluaineiston analyysissä sovellettiin teemoittelua sekä tyypittelyä. Tuomen ja Sarajärven (2018, s. 105) mukaan teemoittelussa on kyse aineiston jäsentämisestä tai ryhmittelystä erilaisten aihepiirien mukaisesti. Tyypittely puolestaan viittaa siihen, että tiettyjen teemojen sisältä etsitään yhteisiä näkemyksiä, joista voidaan muodostaa eräänlainen yleistys eli tyyppiesimerkki. Usein teemoittelu lähtee liikkeelle alustavasta ryhmittelystä, minkä jälkeen aineistosta etsitään varsinaisia teemoja eli aiheita sekä näitä kuvaavia näkemyksiä. (Tuomi & Sarajärvi, 2018, s. 105–107.) Haastatteluaineiston käsittely aloitettiin alustavalla ryhmittelyllä värikoodein seuraavien tekijöiden mukaan:

- inhimilliset /yksilöön liittyvät tekijät
- organisatoriset tekijät
- teknologiset tekijät
- verkostotekijät
- tietoon liittyvät tekijät
- aikaulottuvuuteen liittyvät tekijät.

Haastateltavien vastaukset polveilivat jokseenkin paljon, minkä vuoksi alustava ryhmittely päätettiin rakentaa mukaillen Riegen (2005) ja Vuoren ym. (2019) esittämiä kategorioita tiedon jakamiseen liittyvistä tekijöistä esteiden näkökulmasta. Tässä kategorioiden avulla pyrittiin tunnistamaan tietovirtoihin ja niiden hallintaan liittyviä yleisiä periaatteita ja tekijöitä aineistoista. Tuomen ja Sara-

järven (2018, s. 110) mukaan teoriaohjaavassa päättelyssä on usein kyse abduktiivisesta päättelyn logiikasta, jolloin tutkijan ajatteluprosessi kulkee aineistolähtöisyyden ja valmiiden mallien välillä vaihtelevasti. Tällöin aineiston hankinta ja analyysi ovat joustavampia, ja tutkijan on mahdollista vapaammin valita missä määrin ja missä vaiheessa hän tuo teoriaa ohjaamaan päättelyään aineiston analyysissä (Tuomi & Sarajärvi, 2018, s. 110–111 & 113). Koska tutkimuksen yhtenä näkökulmana on hahmottaa myös aikaulottuvuuden vaikutusta kybertilannekuvan muodostamisen kontekstissa, Riegen (2005) ja Vuoren ym. (2019) esittämien tekijöiden lisäksi alustavassa aineiston ryhmittelyssä päätettiin ottaa erikseen huomioon myös aikaulottuvuuteen liittyvät tekijät. Tämän vaiheen jälkeen aineistosta etsittiin vielä tarkemmin teemoja kuvaavia näkemyksiä tyypittelyn pohjaksi. Tavoitteena oli pyrkiä löytämään aineistosta tyyppiesimerkkejä, joiden avulla tietovirtojen hallinnan ideaalimallia olisi mahdollista hahmottaa. Ideana oli lisäksi pyrkiä löytämään aineistosta sekä samankaltaisuuksia että eroavaisuuksia tietovirtojen muodostumisen ja niiden hallinnan yleisistä periaatteista kybertilannekuvan muodostamisen kontekstissa, sekä tunnistamaan näkemyksiä tähän liittyvistä haasteista. Aineisto ryhmiteltiin alustavan ryhmittelyn jälkeen vielä teemahaastattelurungon mukaan omiin osioihinsa aineiston analyysin helpottamiseksi.

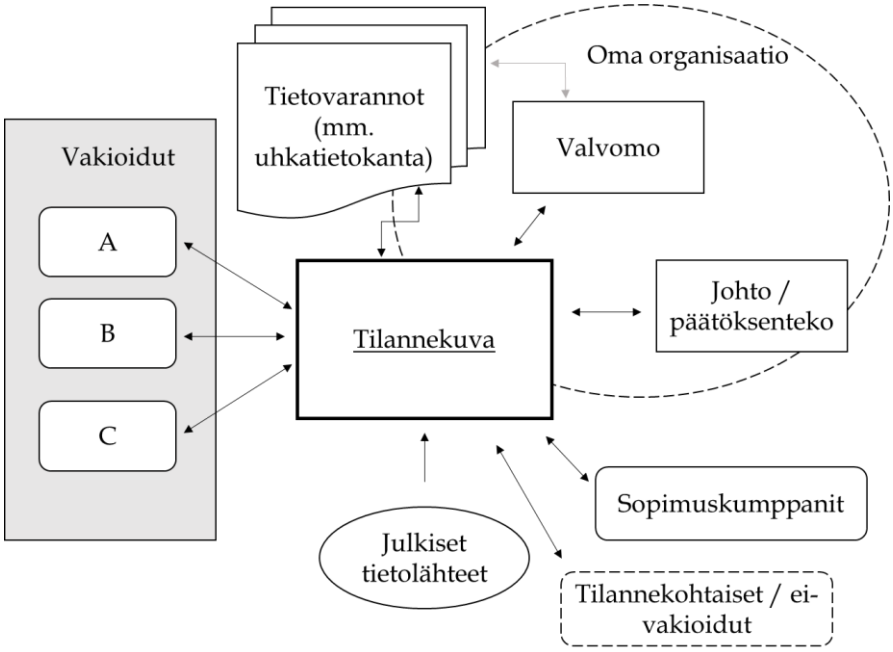
5 TULOKSET

Tässä luvussa esitetään tutkimuksen tulokset. Havainnoinnin tuloksia käsitellään ensimmäisessä alaluvussa ja toisessa alaluvussa puolestaan esitetään haastatteluaineiston tulokset. Tulosten havainnollistamiseksi alaluvussa on esitetty suoria lainauksia haastatteluista.

5.1 Havainnointi

Havainnointi toteutettiin osana viiden päivän kestoista kyberharjoitusta syksyllä 2021. Varsinaiset peliskenaariot ja -syötteet toteutettiin kolmen päivän aikana, jolloin viikon ensimmäinen päivä käytettiin työkaluihin ja harjoitusympäristöön tutustumiseen ja viimeinen päivä harjoituksen yhteenvetoon. Havainnoinnin avulla pyrittiin muodostamaan käsitys tietovirroista ja niiden hallinnan periaatteista kybertilannekuvan muodostamisen käytäntöä kuvaavassa ympäristössä.

Havainnoinnin kohteena olleen organisaation kybertilannekuvatoiminnetta on mahdollista kuvailla tiedonkäsittely ja jakamisperiaatteiltaan ”hub-and-spoke” -tyyppisen mallin mukaisesti (kts. kuvio 13). Toisin sanoen sen tarkoituksena oli ikään kuin toimia tiedon vastaanottajana ja koordinaattorina niin organisaation sisältä kuin sen ulkopuolelta tulevien tietovirtojen osalta ja ohjata ne eteenpäin tarvittaviin suuntiin. Kuviossa 14 on avattu havainnoinnin perusteella muodostunutta käsitystä tietovirtojen muodostumisesta havainnoinnin kohteena olleen toiminteen näkökulmasta.



KUVIO 14 Tietovirtojen muodostuminen havainnoinnin perusteella.

Kaikki kuviossa 14 esitetyt rakenteet eivät olleet mukana varsinaisessa peliorganisaatiossa, vaan osa pelattiin niin sanotun white teamin (lyh. WT) toimesta. WT paikkasivat niitä osapuolia, jotka eivät olleet harjoituksessa fyysisesti mukana, mutta olivat kuitenkin olennaisia pelin etenemisen kannalta ja antoivat myös toiminnallisia syötteitä pelaajatoiminteille.

Ensimmäisenä päivänä harjoitukseen osallistuneet organisaatiot vaihtoivat keskenään yhteystiedot, miten heihin tulisi olla yhteydessä minkäkin tyyppisessä tilanteessa. Harjoituksessa eri organisaatioiden välisessä kommunikoinnissa hyödynnettyjä tiedonvaihtokanavia olivat pääosin sähköposti sekä puhelinyhteys. Harjoituksen aikana kuitenkin havaittiin, ettei näitä vaihdettuja yhteystietoja ja esitettyjä kommunikointikanavia täysin noudatettu, vaan yhteydenottoja saatettiin tehdä organisaation kybertilannekuvatoiminteen ohi joko suoraan harjoituksessa mukana olleisiin muihin organisaation sisäisiin toiminteisiin, kuten valvomoihin tai ylemmän tason toimijoihin (WT), mikä hankaloitti pintatilanteen seuraamista ja tilannekuvan muodostamista keskitetyssä kybertilannekuvatoiminteessa.

Kybertilannekuvatoiminteen ohittaminen näkyi myös toiseen suuntaan havainnoinnin kohteena olleen organisaatiokokoonpanon muiden toiminteiden osalta. Keskeinen havainto oli, etteivät tarkkailtavan organisaation muut sisäiset toiminteet, kuten valvomot, täysin tunnistaneet kybertilannekuvatoiminteen roolia niin koko organisaation laajuisena kybertilannekuvan muodostajana kuin toisaalta myös yhteyspisteenä organisaation sisäisten ja ulkoisten sidosryhmien välillä. Valvomotoiminteet muodostivat valvomokohtaista tilannekuvaa havaitsemistaan tapahtumista oman fyysisen tilansa valkotaululle, mutta raportointi käytössä olevia tietojärjestelmiä, kuten tiketöintityökalua hyödyntäen oli ajallisesti viiveistä ja myös sisällöltään jokseenkin puutteellista. Tämä näkyi siinä,

ettei tilannekuvatoiminteen ollut tehtyjen kirjausten perusteella mahdollista pysyä tilannetietoisena ja muodostaa tilanneymmärrystä tapahtumien todellisista vaikutuksista, ja siten tukea päätöksentekoa tarvittavilta osin peliskenaarion mukaisessa laajavaikutteisessa poikkeamatilanteessa. Organisaation sisäisten toiminteiden välinen, tilannetta tarkemmin avaava tiedontasaus pidettiin vasta harjoituksen viimeisenä päivänä, jolloin peliskenaario oli käytännössä edennyt jo siihen pisteeseen, että uhkatoimija oli onnistunut saamaan jalansijan organisaation verkkoympäristöön ja anastamaan sieltä tietoa. Tietoa merkittävistä poikkeamista jaettiin toisin sanoen liian hitaasti, jolloin tilannekuvalla ei kyetty tukemaan päätöksentekoa tilanteen edellyttämällä tavalla.

Harjoituksen aikana järjestettiin kaksi toimijoiden välistä yhteistyökokousta, joissa toimijoilla oli mahdollista vaihtaa tietoa keskenään. Pidetyt kokoukset avasivat harjoitukseen liittyvää yleistilannetta sekä siten laajensi tilanneymmärrystä myös siltä osin, millaisia tapahtumia muut toimijat olivat havainneet. Keskeisenä havaintona lisäksi tunnistettiin, että kokoukset mahdollistivat harjoitustapahtumien yksityiskohtaisemman käsittelyn keskeisten toimijoiden kanssa ja edistivät siten tilanteen selvittelyä ja laajemmin tapahtumien vaikutusten arviointia.

Tietojärjestelmien osalta tarvittavat työkalut oli suunniteltu harjoitukseen etukäteen organisaation tarpeet ja toimintamallit edellä pelkistetysti. Työkalupaletti muodostui muun muassa pikaviestin- ja sähköpostipalveluista, uhkatietokannasta sekä tiketöinti- ja raportointityökaluista, ja niin edelleen. Harjoituksen edetessä kuitenkin huomattiin, etteivät suunnitellut organisaation yhteiskäyttöiset järjestelmät integroituneet tarkoituksenmukaisella tavalla, mikä hankaloitti kommunikointia ja tiedonvaihtoa sisäisten toimijoiden välillä sekä myös kokonaisuudessaan tilanneymmärryksen muodostumista, kun tietoa ei voitu jakaa kovinkaan ketterästi. Esimerkiksi uhkatietokanta oli rakennettu siten, että jokaisella organisaation sisäisellä toimijalla oli oma instanssinsa eivätkä ne integroituneet keskenään. Siten kerätyt uhkatiedot eivät olleet tarkoitetulla tavalla kaikkien organisaation sisäisten toimijoiden saatavilla, eikä esimerkiksi valvontaa kyetty evästämään näiden tietojen pohjalta kovinkaan ketterästi. Tiedon jakaminen vaati siten jokseenkin paljon manuaalista työtä, mikä näyttäytyi aikaa ja henkilöresursseja vievänä prosessina.

Tietojärjestelmät toimivat myös epävakaasti, mikä johtui peliympäristön kapasiteettivajeesta eikä varsinaisesti ollut peliin liittyvää toimintaa. Toisaalta järjestelmäinfrastruktuurin häiriöt voisivat myös olla todellinen tilanne, mitä toiminteet eivät tässä raportoineet osaksi tilannekuvaa. Harjoituksen intensiivisen luonteen vuoksi valvomohenkilöstön on mielekästä ratkoa itsekseen teknisiä poikkeamia mahdollisimman pitkälle, jolloin eteenpäin raportointi pelin keskellä herkästi unohtuu. Taustalla kuitenkin voi myös olla, ettei organisaation eri tasoilla työskentelevät henkilöt täysin tunnista mihin heidän oma toimintansa integroituu. Joka tapauksessa, jotta tilannekuva palvelee tarkoitustaan, on oleellista, että havaitut poikkeamat päätyvät osaksi tilannekuvaa, jotta sitä voidaan pitää oikeana.

5.2 Haastattelut

Haastatteluun osallistui yhteensä kahdeksan haastateltavaa neljästä eri organisaatiosta. Tuloksissa näkyy yleisesti haastateltavien ongelmalähtöinen suhtautuminen, mikä kertonee osin siitä, että tietovirrat ja niiden hallinta kybertilannekuvan muodostamisen kontekstissa on vielä merkittävästi kehitysasteen alla.

Taulukossa 2 on esitetty tiivistetysti millaisia tekijöitä aineiston perusteella tietovirtoihin ja niiden hallintaan on liitettävissä kybertilannekuvan muodostamisen kontekstissa. Seuraavissa alaluvuissa käsitellään haastatteluaineiston tuloksia yksityiskohtaisemmin mukaillen teemahaastattelurungon otsikointeja.

TAULUKKO 2 Tietovirtojen muodostumiseen ja hallintaan liittyviä tekijöitä haastatteluaineiston perusteella.

Inhimilliset / yksilöön liittyvät tekijät	• Luottamus • Halu jakaa tietoa • Tiedon mustasukkaisuus / henkilöityminen • Ammattitaito • Jatkuva uuden oppiminen / toimintaympäristön muutokseen mukautuminen
Organisatoriset tekijät	• Tietotarpeiden tunnistaminen • Sisäinen toimintakulttuuri • Toimivat ja tarkoituksenmukaiset prosessit, rakenteet ja roolivastuut • Toimivaltuudet ja lainsäädäntö • Käyttöoikeudet ja pääsy tietoon • Joustavuus
Teknologiset tekijät	• Tarkoituksenmukaiset tietojärjestelmät ja työkalut, jotka mahdollistavat tiedon keräämisen, käsittelyn, taltioinnin ja esittämisen. • Soveltuvat tiedonvaihtokanavat • Turvaluokitellun aineiston käsittelyyn soveltuvat tietojärjestelmät ja kommunikointikanavat • Tiedon hyödynnettävyys eri järjestelmistä (vrt. tiedon pirstaloituminen)
Verkostoihin liittyvät tekijät	• Luottamus • Henkilökohtaiset suhteet • Aktiivisuus • Yhteistoimintaa tukevat, jaetut tietojärjestelmät ja työkalut • Soveltuvat tiedonvaihtokanavat • Eri toimijoiden ja tietotarpeiden tunteminen • Toimivaltuuksien ja lainsäädännön yhtenevä tulkinta • Joustavuus • Yhdenmukainen tapa käsitellä ja jakaa tietoa
Tietoon liittyvät tekijät	• Tiedon suuri määrä • Merkityksellisyys vaihtelee toimijoittain / eri kontekstissa • Tiedon /tietolähteiden luotettavuus • Tiedon sensitiivinen luonne / luottamuksellisuus • Yhteiset tiedonkäsittelyn käytännöt • Yhteinen tulkintapohja, ml. terminologia

	• Ymmärrettävyys • Tiedon strukturoitu analysointi
Aikaulottuvuuteen liittyvät tekijät	• Toimintaympäristön muutosnopeus • Tapahtumien nopea kehittyminen • Tiedon saatavuus riittävän nopeasti (tekniset ja toimintakulttuuriin liittyvät valmiudet)

5.2.1 Kybertilannekuva ja siihen liittyvät erityispiirteet

Haastattelun ensimmäisessä osiossa pyrittiin selvittämään, millaisia näkemyksiä haastateltavilla on kybertilannekuvan muodostamisen edellytyksistä ja siihen liittyvistä erityispiirteistä esimerkiksi verrattuna muuhun tilannekuvatoimintaan. Tilannekuvaprosessi nähtiin pitkälti samanlaisena kuin minkä tahansa muun toimintaympäristön tilannekuvassa. Haastateltavat tunnistivat kuitenkin kenties isoimpana eroavaisuutena fyysisen maailman tilannekuvatoimintaan nähden käytettävissä olevat tietolähteet ja niiden suuren määrän, sekä toisaalta myös tiedon jakamiseen liittyvät rajoitteet, joita muissa toimintaympäristöissä ei jouduta samalla tavalla huomioimaan ja käsittelemään.

> Mutta se onko se kyberiä vai onko se joku muu, niin se prosessihan on tavallaan sama, siellä vaan seurataan erilaisia asioita. (Haastateltava 7)

> Siinä on sellaisia tiedonosia mitkä ei tule ilmi noissa muissa toimintaympäristöissä, eli nimenomaan lainsäädännöllä säädeltyyn tietoon vaikka nyt tietosuojaan tai erilaisiin sopimuksiin perustuen vaikkapa yrityksessä luottamukselliseen tietoon, kun se on ihmisen luoma toimintaympäristö, niin sitä on myös enemmän säädelty niin siksi siellä tapahtuva tiedonvaihto -- ei toimi yhtä tehokkaasti kuin se voisi toimia, koska sitä on myös tarkoituksenmukaisesti -- rajoitettu sitä siellä jaettavaa tietoa. (Haastateltava 3)

> Mun mielestä se eroaa siinä, että nyt ainakin tällä hetkellä kybertilannekuvan lähteitä on huomattavasti enemmän, -- kybertilannekuvaa taas rakennetaan huomattavasti, siinä on nämä elementit [organisaation itsensä tuottamat, sisäiset tietolähteet], mutta sitä tietoa tulee myös muualta… sitä tulee ehkä vielä enemmän verkostojen kautta, [oman organisaation] ulkopuolelta ja sanoisin jopa, että suhteessa tulee enemmin tietoa sinne tilannekuvaan kuin [organisaation] itsensä tuottamana. (Haastateltava 8)

Lisäksi selkeinä eroina perinteisempään tilannekuvaan nähtiin myös tarve kiinnittää erityistä huomioita raportointitapaan ja kielelliseen ilmaisuun, jotta kybertilannekuvassa esiin tuodut asiat tulevat ymmärretyksi oikein. Kybermaailman ilmiöt ovat monelle vieraita ja kybertoimintaympäristö jokseenkin hankalasti ymmärrettävä kokonaisuus. Esiin nousi myös muusta tilannekuvasta jokseenkin poikkeavana kiinnostus yksittäisiin teknisiin tapahtumiin ylemmilläkin toiminnan tasoilla.

> Se minkä mä nään tässä erilaisena, että tätä pitää sanoittaa eri tavalla. Eli tavallaan just se, millä tavalla tästä kerrotaan, niin siinä voi tulla eroja, koska tämä on kuitenkin monelle ei-ymmärrettävä tai ei-tuttu aihe. (Haastateltava 6)

> Se yks tekninen tapahtuma tai ilmiö voi kiinnostaa tai silloin sitä pystyy tarkastelemaan monesta eri [organisaation] hierarkiatasosta ja sitä ehkä halutaankin tarkastella… että se voi olla sille teknistä valvontaa tekevälle ihmiselle mielenkiintoinen, mutta sitten se voi olla ihan siellä, jopa sinne -- päätöksentekijä tasallekin mielenkiintoinen. (Haastateltava 1)

Haastatteluiden perusteella keskeisenä kybertilannekuvan muodostamisen edellytyksenä nähtiin, ettei kybertilannekuvaa voida pitää arvona itsessään vaan se tulee nähdä päätöksenteon ja toiminnan mahdollistavana välineenä tai sitä ohjaavana elementtinä. Edellytyksinä korostui lisäksi näkemys siitä, ettei voi olla kaikille toimijoille yhteistä kybertilannekuvaa, joka olisi sellaisenaan riittävä. Siten ensiarvoisen tärkeänä nähtiin tunnistaa, kenelle kybertilannekuvaa tehdään ja millaisia tietotarpeita heillä on. Vastauksissa nousi myös esille tarve ikään kuin asiakas-palveluntarjoaja-asetelmassa yhteisesti määrittää, mitä kybertilannekuvalla keskinäisesti tarkoitetaan.

> Kybertilannekuva ei ole arvo itsessään vaan se on aina väline jonkun isomman tilanneymmärryksen muodostamiseksi, jotta me voidaan tehdä jotakin. -- Hyvä kybertilannekuva on jokaiselle toimijalle tietyllä tavalla erilainen, koska he tarvitsevat sitä voidakseen tehdä sitä päätehtäväänsä, ja sen takia ne tarvitsevat siitä kaikesta tiedosta tietyt osat, josta he muodostavat omaan käyttöönsä sen tarvittavan tilannekuvan ja näin ollen ei voi olla sellaista yleistä kybertilannekuvaa, joka antaa kaikille riittävän tiedon. (Haastateltava 3)

> Tunnetaan se yleisö, jolle sitä tilannekuvaa tuotetaan, että osataan vastata niihin kysymyksiin ja tietotarpeisiin, joita sillä spesifillä kohdeyleisöllä on, jolle sitä tilannekuvaa tuotetaan… ja osataan myös antaa sellaisia asioita, mitkä tuottaa heille lisäarvoa. (Haastateltava 2)

> -- olennaisena osana, että kenelle sitä tilannekuvaa kerätään tai muodostetaan. että se ehkä ei semmoinen universaali käsite, joka pätee aina samalla tavalla vaan eri asiakasta voi kiinnostaa erilaiset seikat tai tarkastelunäkökulmat siinä tilannekuvassa. (Haastateltava 1)

> Mun mielestä ylipäätään edellytyksenä on, että ymmärretään mitä se organisaatio tarkoittaa, kun puhutaan kyberturvallisuuden tilannekuvasta, et meillä on se sama käsitys. Mä ymmärrän sen, meillä voi olla useita eri kyberin tilannekuvia, mutta me kuitenkin puhutaan samasta asiasta, kun sitä lähdetään muodostamaan ja että se on meille yhteisesti määritelty, että mitä se kyberturvallisuus tarkoittaa. Mä näen myös sen, että ei ole yhtä yksittäistä kyberturvallisuuden tilannekuvaa vaan se riippuu siitä organisaatioista ja myös niistä tarpeista – niin niistä organisaation omista kuin myös sitten niiden mahdollisten asiakkaiden tarpeista, kelle se organisaatio sitä tilannekuvaa tuottaa. (Haastateltava 6)

Kybertilannekuvan muodostamisen edellytyksinä mainittiin myös tarvittavat tekniset ratkaisut, jotka mahdollistavat tiedon keräämisen, käsittelyn ja esittämisen, sekä toisaalta myös riittävät käyttöoikeudet ja muu pääsy tarvittavaan tietoon. Lisäksi kybertilannekuvan muodostamiseen liittyvien prosessien ja eri-

laisten roolivastuiden määrittäminen ja tunteminen, sekä tavoite miksi tilannekuvaa tehdään, nousivat keskeisinä edellytyksinä esiin.

> -- tarvittavat tekniset työkalut ensinnäkin, jolla pystytään keräämään ja monitoroimaan. (Haastateltava 1)

> -- on oikeus saada aineistoja ja tilannekuvan muodostamisen pohjaksi käyttöönsä ja oikeus käsitellä niitä ja taltioida niitä. -- Sen lisäksi pitää olla tilannekuvan muodostamiseen olemassa olevat prosessit ja tietysti se tavoite, minkä vuoksi sitä tilannekuvaa muodostetaan. -- No sitten tietysti viimeisenä on rakenteet oleellisena, että pitää olla sen tilannekuvan muodostamisen, alkaen tiedonhankinnasta päättyen sitten siihen raportointiin ja esityksien tekoon siinä toimeenpanijoille, niin olemassa olevat rakenteet niin hallinnonalan sisällä kuin sitten myös poikkihallinnollisesti. -- Ja kullekin tasolle on myös sitten selvää, että mikä se heidän roolinsa on siinä kybertilannekuvan tuottamisessa ja miten he rikastavat alemmalta tasolta saamaansa tilannekuvaa, siten että he kykenevät muodostamaan omalle tasolleen sopivan tilannekuvan. (Haastateltava 4)

> Ja nyt sitten tullaan siihen, että powerpointeilla se ei synny eikä sillä, että joku kirjoittaa muistiinpanoja vaan isossa mittakaavassa se tekninen tieto on tärkeetä ja se vaatii tilannekuvan järjestelmiä, kykyä aggregoida tietoa ja muodostaa siitä automaattistakin analyysiä, muodostaa siitä aina isompaa kuvaa, mutta siellä pitää olla mahdollisuus zoomata koska kybertilannekuvalle on myös ominaista myös se, että hyvin pieni yksityiskohta vaikuttaa. (Haastateltava 3)

Haastateltavilta kysyttiin lisäksi, miten he kokevat, että kybertoimintaympäristön perusluonne vaikuttaa kybertilannekuvan muodostamiseen. Koska kybertoimintaympäristössä maantieteelliset etäisyydet tai aika eivät päde samalla tavalla kuin kenties muissa toimintaympäristöissä, merkityksellisenä nousi esiin asioiden nopea kehitys, mihin kaiken toiminnan täytyy kyetä myös adaptoitumaan.

> -- tilannekuvaa on tuotettava ehkä tavanomaista tilannekuvaa nopeammalla syklillä koska se vanhenee hyvin äkkiä. Jos ajatellaan, että tehdään jotain neljännes vuosiraportteja, niin se kertoo kyllä sen kehityksen sinä aikana, mutta ei se on jo hyvin vanhaa tietoa siinä vaiheessa. Se kertoo kyllä hyvin taaksepäin mitä on tapahtunut, mutta jos halutaan puuttua nopeasti tämmöisiin ilmiöihin niin kyllähän se edellyttää tässä nimenomaan sen, että sen pitää olla hyvinkin syklistä se tilannekuvan tuottaminen tai jäädään jälkeen. – [T]uolla perinteisellä puolella ne ilmiöt nousee huomattavasti hitaammin ja kehityskulku on paljon hitaampaa siellä ja uusien ilmiöiden muodostuminen kun sitten taas kyberissä saattaa tulla se uusi tekotapa tai uusi hyökkäystapa päälle yhden päivän tai viikonlopun aikana. Silloin se edellyttää, että tilannekuvan pitää olla käytännössä melkein reaaliaikaista. (Haastateltava 8)

> Koska nää maantieteelliset etäisyydet tai aika ei päde samassa mielessä kuin perinteisissä ulottuvuuksissa niin se haastaa tätä [kyber]tilannekuvan muodostamista… jos joku uhka saattaa kehittyä aivan äärimmäisen nopeasti ja alkaa vaikuttaa täällä meilläkin ja tietenkin se haastaa, miten ne tietovirrat siellä voi kulkea ja miten sä pystyt seulomaan siitä valtavasta tietomassasta ne relevantit asiat ja siinä tullaan näh-

> däkseni tähän verkostoon, että kukaan ei pysty itse muodostamaan sitä kokonaiskuvaa. (Haastateltava 3)

> Ehkä se on vähän niinku nopeammin kehittyvä, et… tavallaan jos tänä iltana saadaan jotain, niin se voi yön aikana vanhentua jo ihan täysin… että se tilanne elää ja jotenkin hirveen paljon tulee tietoa monista eri lähteistä, et jos esimerkiksi on joku haavoittuvuus kyseessä ja me yritetään siihen muodostaa tavallaan käsitystä siitä, että kuinka laajalle se vaikuttaa… niin sitten se saattaa olla niin, että alkuarvio on, että tämä on täysin vaaraton, mutta se on muodostunut todella kriittiseksi, kun joku on keksinyt siihen jonkun hyväksikäyttömenetelmän muutamaa tuntia myöhemmin ja sitten se koko tilannekuva on kääntynyt täysin päälaelleen. (Haastateltava 2)

5.2.2 Tietovirtojen muodostuminen

Haastattelun toisessa osiossa pyrittiin selvittämään tarkemmin haastateltavien käsityksiä tietovirroista ja niiden hallinnasta kybertilannekuvan muodostamisen kontekstissa. Haastateltavilta muun muassa kysyttiin, millainen mielikuva heillä on tietovirroista, jotka liittyvät kybertilannekuvan muodostamiseen, sekä millaiset asiat, ilmiöt tai osatekijät heidän mielestään niihin vaikuttavat. Lisäksi kysyttiin, millaisia keinoja he tunnistavat tietovirtojen hallitsemiseen ja kenen tehtävä heidän mielestään on hallita tätä kokonaisuutta.

Tietovirtojen hallinta kybertilannekuvan muodostamisen kontekstissa näyttäytyy aineiston pohjalta moniulotteiselta ja jokseenkin vaikeasti hahmotettavalta ja hallittavalta kokonaisuudelta. Yhtenä merkittävänä tekijänä haastatteluaineiston pohjalta nousee edelleen tietolähteiden valtava määrä, mikä osaltaan haastaa kokonaisuuden hallintaa.

> Se on hyvin moniulotteista, monitahoista ja monipuolista se tietovirta mitä tulee, ja se asettaa oman haasteensa siihen, miten nämä sitten suhteutetaan keskenään ja tietysti vaikeuttaa sen tilannekuvan luomista, että mikä arvo annetaan millekin, tai on vähän erilaisia tuotteita muutenkin ja näkökulmat saattaa olla vähän erilaisia ja se on taas, jos mä vertaan siihen mitä tehdään muuta [perinteisempää] tilannekuvaa [jonkun tietyn ilmoituksiin perustuvan formaatin mukaan] – mutta sitten kun joudutaan hyvin eri muotoisia ja näköisiä lähteitä käymään läpi [kyberissä], ja ottamaan se olennainen sieltä, niin siinä tulee ne omat haasteensa. (Haastateltava 8)

> Varmasti voitaisiin hallita paremminkin… se on kaikissa organisaatioissa sellainen mitä varmasti aina voitaisiin kehittää. -- Kyberissähän niitä tietolähteitä on aivan valtavasti, et pelkästään meidän kumppanuusorganisaatiot tuottaa -- varmaan kymmenittäin julkaisuja kuukausitasolla ellei jopa sitten satoja, että sitä tietoa on niin paljon kuin vaan jaksaisi lukea… -- kyberissä on mun mielestä ennen kaikkea jotenkin tosi hankala pysyä niiden tietovirtojen tasalla ja sitä tietojohtamista tehdä oikealla tavalla. (Haastateltava 2)

Tietovirtoja on hyvin erilaisia ja lähtökohtaisesti ne edellyttävät erilaisia organisatorisia mekanismeja ja prosessien hahmottamista. Haastateltavista yksi hahmotti kybertilannekuvan muodostamiseen liittyviä tietovirtoja esimerkiksi määrittelemällä ensin tietotarpeet muutamiin ylätason osa-alueisiin. Jotta näi-

hin tietovirtoja ohjaaviin tietotarpeisiin kyetään vastamaan, haastatteluiden perusteella nähtiin edellytyksenä myös laaja ymmärrys siitä, mikä tieto on milloinkin hyödyllistä ja että osataan myös välittää tietoa eri kanavia pitkin eri toimijoille. Edellytyksenä laajan ymmärryksen lisäksi tunnistettiin tarve mukautua tilanteisiin joustavasti. Haastatteluiden pohjalta kybertilannekuvan muodostamisessa ja siihen liittyvien tietovirtojen hahmottamisessa korostuu erilaisista verkostoista muodostuvat tietovirrat.

> -- miten se kybertilannekuva muodostuu, niin mun mielestä sen pitäisi muodostua -- kolmesta osa-alueesta eli tekninen tilannekuva, jossa kerrotaan, että mitä teknisiä asioita ja tapahtumia on meneillään eli tämä on meillä usein se vahvuusosa-alue, ja tätä me ollaan hyviä tekemään ja muodostamaan. Mutta sitten pitäisi kyetä tähän kokonaisuuteen liittämään myös se vastustajan toiminta, ja näkemään, että siellä pitäisi olla ne uhkat olemassa ja ehkä vertaamaan, että on näitä teknisiä tapahtumia, että liittyykö ne niihin uhkiin tai muodostuuko näistä jotain sinne. Ja sitten se viimeinen, mikä on kanssa tosi tärkeä eli oma tilanne, mitä ollaan itse tekemässä ja miten tämä liittyy meihin ja meidän toimintaan tämä kokonaisuus eli tällainen kolmikanta on minun mielestä se kybertilannekuva, mikä pitäisi muodostua ja tästä pitäisi tulla sille päätöksentekijälle ne edellytykset tehdä oikeanlaisia päätöksiä. (Haastateltava 5)

> -- Ja tietysti sitten valtionhallinnosta niin meillähän on sitten omia kanavia ja tuotteita ja tilannekuvaraportteja, jotka sitten jaetaan valinnaiselta osalta niille ihmiselle jotka niitä tarvitsee… niin kyllähän ne on myös hyvinkin keskeisessä osassa, että ymmärretään minkälaisessa tilanteessa yhteiskunnassa nyt tällä hetkellä eletään ja minkälaiset asiat nyt tällä hetkellä on pinnalla ja tietysti sitten myös kyllähän me saadaan päivittäin erilaisia kansainvälisiltä kumppaneilta tulevia koosteita, oli ne sitten uhkatietoja, haavoittuvuustietoja, uutisia, raportteja, analyyseja ja muuta niin kyllä niilläkin on sitten keskeinen paikka… et ne tulee sieltä meidän verkostoista ja tota kyberissä se on isossa asemassa, että muistetaan että ei olla yksin. (Haastateltava 2)

> Organisaatiotasolla tää on hallittavissa, mutta se edellyttää nimenomaan nyt sitten näiden prosessien luomista ja ylläpitämistä -- voidakseen muodostaa kybertilannekuvaa, tulee hyvin tarkkaan määritellä ja rajata mikä se on niiltä osin kuin sitä itse tarvitsee -- se lähteistö ja toisaalta se informaation osatekijät, mitä siihen tilannekuvaansa se organisaatio tulee tarvitsemaan. No sitten sen pitää suunnitella, miten se aikoo sen kokonaisuuden tehdä… että siinä mielessä tää on niinku varsin relevantti kysymys, että se ei synny itsestään. -- periaatteessahan se kyseisen liiketoimintayksikön tai organisaation johdon, joka viime kädessä tekee niitä päätöksiä, jonka ymmärryksen tuki tämä kybertilannekuvakin on, tulisi pystyä määrittelemään mitä se siitä tarvitsee. Käytännössähän se ei sitä pysty tekemään, riippuen toki organisaatiosta, mutta etenkin jos sen organisaation päätehtävä ei ole muodostaa kybertilannekuvaa, jolloin se jollain tavalla tulee siirtymään siellä organisaatiossa muualle ja ikään kuin jonkun pitää palvella palveluperiaatteella sitä tarvitsijaa sillä, että se pystyy muodostamaan sen tapaista tilannekuvaa mikä tukee… ja näin ollen se lopullinen kybertilannekuvamuoto ja niiden tietovirtojenkin synty… niin näen että syntyy siellä organisaation sisälläkin niiden verkostojen ja tällaisen iteratiivisen prosessin myötä. Ja miten sitä määritellään, niin se määrittelykin on minun mielestä nimenomaan tällainen jatkumo, parantamisen prosessi elikkä me emme voi päivänä x sanoa että tässä on meidän kybertilannekuva ja näitä asioita me siihen tarvitaan ja se tilannekuva on valmis, ja sitten lähdetään tekemään, vaan se tietotarve vaihtelee ja sille on mun mielestä vielä ominaista se, että niillä prosesseilla saadaan tietyllä tapaa se perus kuva

> syntymään, mutta johtuen sitten toimintaympäristön luonteesta niin sieltä jatkuvasti nousee asioita, jotka vaatii sitten tarkempaa huomiointia ja näin ollen sen mallin tulee mahdollistaa tämmöinen tarkentaminen ja zoomaaminen johonkin kohtaan. (Haastateltava 3)

Erilaiset tiedonvaihtokanavat ja tietojärjestelmät liittyvät myös oleellisesti tietovirtoihin. Haastatteluissa nousi esiin, ettei verkostotoiminnassa oikein ole sellaisia teknisiä ratkaisuja tai työkaluja, jotka mahdollistaisivat esimerkiksi turvaluokitellun aineiston käsittelyn. Tieto on usein myös pirstaloitunut useisiin eri tietojärjestelmiin, jotka eivät ole integroitu keskenään siten, että tietoa olisi haettavissa useasta järjestelmästä samanaikaisesti tehden toiminnasta ketterämpää. Yksi haastateltavista nosti esiin myös sen, että erilaisten organisaatiorakenteiden ja tietojärjestelmien tulisi olla toteutukseltaan jokseenkin yksinkertaisia, että tietoa on helppo jakaa ja käsitellä vaatimusten mukaisesti.

> -- tulee olla ne tiedonvaihtokanavat olemassa ja niiden tulee olla sekä ihmisten välisiä, joissa voidaan muodostaa sitä tilanneymmärrystä ja tarkentaa, niin jatkuvalla kommunikaatiolla, ja sitten tulee olla myös tekniset keinot, joilla tätä teknistä kuvaa tai teknisiä tiedon elementtejä voidaan välittää mahdollisimman automatisoidusti. (Haastateltava 3)

> Tietysti se haaste mikä tietovirroissa on, koska niitä on paljon, niitä tulee hyvin eri kanavia pitkin niin esimerkiksi työkalut on sellaisia, että ne eivät aina tue sitä tiedon käsittelyä ja sitä, että sulla on yksi tieto järjestelmässä A, ja toinen B:ssä ja kolmas tulee D:hen ja mitä ikinä, ja sitten se että tarvittaisiin se joku mylly mihin sen kaiken saa ja sieltä myllystä voisi aina yhdistää ja ammentaa sitä tietoa, ja musta tuntuu että se on myös yksi sellainen haaste mikä tietovirtoihin liittyy. (Haastateltava 6)

> -- on olennaista, kun puhutaan mistä tahansa käyttöliittymistä tai jutuista, niin niiden pitää olla aika yksinkertaisia. Kyse on siitä, että niiden pitää olla helppoja, yksinkertaisia juttuja miten sä voit jakaa ja täyttää ne vaatimukset, että se tieto liikkuu. (Haastateltava 7)

Yhtenä tietovirtojen hallinnan edellytyksenä nähtiin myös mahdollisimman yhdenmukainen tapa käsitellä ja jakaa tietoa, perustuen muun muassa erilaisiin kansainvälisessä kyberyhteisössä hyväksyttyihin tiedonvaihtokäytänteisiin ja -protokolliin, jotka sittemmin ovat yleistyneet myös kansallisessa tiedonvaihdossa. Nämä vapaaehtoisuuteen perustuvat käytännöt herättivät haastateltavissa kuitenkin jokseenkin ristiriitaisia näkemyksiä, sillä osa haastateltavista näkivät ne toisaalta myös siitä haasteellisena, että niihin vetoamalla mahdollisesti sivuutetaan kansallista lainsäädäntöä joiltain osin.

> -- se olisi mahdollisimman yhdenmukaista ja että kaikki ymmärtää heti mistä puhutaan niin eri protokollien avulla pyritään sitä yhdenmukaistamaan -- esimerkiksi tiedon luottamuksellisuuteen tai tiedon jakamiseen liittyvä protokolla. (Haastateltava 1)

> Ja välillä on yksinkertaisesti sellaisia tapauksia, että vaikka kaikki osapuolet haluaisi niin jakaa jotain ja siihen meillä on siihen kyvykkyys, niin laki estää sen. Että vaikka me haluttaisiin kertoa ja jakaa joku tieto niin sit meillä ei ole lainpuitteissa oikeutta

> sitä tehdä -- kanssa vaihdettua tietoa viranomaiskontekstissa vähän ketterämmin kun useimmiten on niin, että me kaikki tiedetään mistä me puhutaan mutta me ei voida sitä keskustelua virallisesti käydä koska laki ei sitä mahdollista ja sitä ei tavallaan sitä tiedonanto tai saanti velvollisuutta ole sillä toisella osapuolella, niin sitten ollaan vähän tavallaan… ei pystytä toimia sillä tavalla mitä haluttaisiin. (Haastateltava 2)

> Ja esimerkiksi TLP-luokka on sellainen yksi, jos sitä käytettäisiin oikein niin se olisi mahdollisuus, mutta tällä hetkellä se on enemmänkin syöpä. -- Kansallinen lainsäädäntö ei sitä tunne ja sillä ei ole mitään oikeudessa pitävää merkitystä, mutta silti siihen vedotaan ei mahdollistavasta näkökulmasta vaan rajoittavasta näkökulmasta, mikä ei sen TLP-luokituksen alkuperäinen tarkoitus ole. (Haastateltava 4)

Yksi haastateltavista tarkasteli tietovirtojen hallintaa osittain organisaation sisäisen yksikkö- ja tiimirakenteiden mukaisesti. Osaksi tietovirtojen hallintaa liitettiin myös määräajoin tehtävä tarkastelu, jossa kartoitetaan organisaation tietolähteet ja miten niitä hyödynnetään vai hyödynnetäänkö ollenkaan. Toisaalta haastatteluissa tunnistettiin myös tarve sellaisille rooleille ja vastuille organisaatiossa, jotka miettisivät aktiivisesti mitä tietoa organisaatiolla on, miten sitä tulisi hyödyntää ja tukevatko organisaation ja verkostojen rakenteet ja työkalut tavoiteltua toimintaa. Yhtä lailla tiedon tarvitsijan rooli nähtiin merkityksellisenä siinä, millaiseksi tietovirrat muodostuvat, mihin liitettiin myös suhteiden ylläpito henkilökohtaisella tasolla. Tarkoituksenmukaiset työkalut nousivat lisäksi esiin yhtenä keskeisimpänä edellytyksenä tietovirtojen hallinnalle, vaikka näitä ei kovin yksityiskohtaisesti haastatteluissa perustellusti avattukaan.

> -- meillä on erilaisia toimintoja, erilaisia yksiköitä joiden vastuualuein on seurata erilaisia informaatiolähteitä eli meillä on ihan määritelty että informaatiolähteet x, y ja z kuuluu vaikka tiimille g ja sitten a, b ja c informaatiolähteet kuuluu tiimille y ja niin edelleen, että sitä on tavallaan yritetty jotenkin tiimien avulla hallita sitä… ja sitten jos tulee joku uusi, niin sitten se yhteisesti neuvotellaan kuka siitä parhaiten olisi vastuussa ja kenen työtehtäviä se koskettaa, kenen työtehtävässä siitä eniten hyötyisi… ja sitten tietenkin pyritään ottamaan se jonkun yhden tietyn henkilön omistukseen ja sitten ottamaan sille henkilölle vielä varahenkilöt, että se ei missään vaiheessa unohdu tai päädy sellaiseen tilanteeseen, ettei sillä olisi ketään hyödyntäjää sillä tiedolla… ja kyllähän meillä sitten, meillä on tällaisia määräajoin tehtäviä tarkasteluja siihen, että minkälaisia tietoja me saadaan ja minne ne laitetaan, onko niitä hyödynnetty koska meille tulee sitten myös sellaisia vuosimaksullisia tai kvartaaleittain tai puolivuosittain maksettavia, maksullisia tietovarantoja mitä me saadaan, et niissä on tavallaan sitten myös taloudellinen intensiivi tarkastella niitä, että ollaanko me hyödynnetty sitä tietoa. (Haastateltava 2)

> -- kyllä sen tarvitsijan pitää niistä tietovirroista pyrkiä pitämään huoli. Ja kuten aiemmin mainitsin, niin sillä toimijalla ei välttämättä ole kykyä vaikuttaa kaikkiin niihin tietovirtoihin, mutta valitettavan usein meilläkin se on kuitenkin niin, että kun olet verkostoitunut oikein ja oikeassa tilaisuuksissa, tunnet oikeat ihmiset niin sitä kautta pääset niihin tietovirtoihin käsiksi ja edelleen se on kovinkin maallista ja ihmislähtöistä se toiminta. (Haastateltava 5)

> Työkalujen pitäisi tukea niitä tietovirtoja, mutta se on mun mielestä iso haaste, että monilla on paljon tietoa ja erilaisia tietovirtoja ja voi olla, että ne lähteetkin on tunnis-

> tettu, mutta ne järjestelmät eivät tue sitä, että sitä tietoa ja tietovirtoja pystyttäisiin käsittelemään. Se on mihin toivoisin itse, että tulisi ratkaisuja ja rooleja organisaatioon, jotka miettii kokoajan minkälaisia tietovirtoja meillä on, miten me voidaan niitä hyödyntää ja onko ne meidän järjestelmät sellaisia, että ne tukee meidän työtä. (Haastateltava 6)

Haastattelujen perusteella tietovirtojen muodostumista ja niiden hallintaa voi osittain hankaloittaa se, ettei toimijoilla ole riittävää tuntemusta tai tietämystä kenen kanssa tietoa tulisi vaihtaa. Yksi keskeinen osatekijä on luottamus. Toisaalta osa haastateltavista tunnistivat myös tiedon yliluokittelun kulttuuria sekä korostunutta vapaaehtoisuuteen perustuvien luottamuksellisuus luokituksiin vetoamista tietovirtoja rajoittavana tekijänä etenkin kansallisesta näkökulmasta.

> No välillä voi olla ihan sellainen tilanne, että ei välttämättä tunnisteta niitä oikeita vastinpareja ja että toimittaisiin kyllä yhdessä ja vaihdettaisiin tietoa, mutta ei välttämättä tiedetty, että se toinen osapuoli omaa sitä tietoa tai olisi lisäarvoa tuotettavana… että semmoinen ymmärrys siitä, että kuka käsittelee mitäkin ja kenen kanssa ollaan tekemisissä, niin sekin voi olla välillä vähän hankala kartoittaa. (Haastateltava 2)

> Toki paljonhan on aineistoja, joita voitaisiin jakaa, mutta meillä kulttuuri taas eri suunnista joko ylileimaa niitä, että ei voitaisi jakaa tai tehdään ainakin siitä jakamisesta ylileimaamisella hankalaa ja toinen kulma sitten on, että käperrytään erilaisiin TLP tai luottamuksellisuus luokituksiin niin että ei sitten voida mukamas jakaa tietoa edes viranomaisten kesken, jota on luottamuksella saatu ja molemmilla hankaloitetaan sitä toimintaa. (Haastateltava 4)

Tietovirtojen muodostumisessa tunnistettiin myös, että mitä kauemmas organisaation ydintoiminnasta mennään, sitä hankalampaa on tunnistaa ja myös luottaa siihen, että tieto pysyy toivotun joukon käsissä. Tietovirtoihin liitettiin toisaalta inhimillisenä tekijänä tiedon henkilöityminen eli tietoa vaihdetaan herkemmin sellaisten tahojen kanssa, jotka tunnetaan henkilökohtaisesti. Osa haastateltavista tunnisti tässä herkkyyden, ettei tiedonvaihtoa kaikilta osin voida myöskään pakottaa vaan se rakentuu pitkälti keskinäisen luottamuksen ja koetun hyödyn varaan.

> [Tietovirtojen hallinnan näkökulmasta] se saattaa tietyllä tavalla muodostaa semmoisia puroja mitä ei tunnistaisi jos mennään kovin kauas siitä organisaatiosta, niin sitä tiedon vastaanottajaa ei nähdä tai sitä ei välttämättä tunneta henkilökohtaisella tasolla siis, niin sitten semmoinen ehkä inhimillinen tekijä kun luottamus alkaa tulemaan, koska sitä -- ei ole nähnyt niin sitten on vähän semmoinen, että voiko siihen luottaa, että muodostuuko sieltä semmoisia tietopuroja mistä mä en itse tiedä. – [T]unnetaan henkilöitä niin niille on helpompi sitten jakaa niin kun yksityiskohtaisempaa ja laajempaa ja tarkempaa vaikka tilannekuvaa sen organisaation ulkokehille asti. -- No ehkä sen organisaation viralliset erilaiset säännöt mitä se organisaatio on kirjoittanut ja tehtävät, mitä se on kirjoittanut itselle niin ne osaltaan sitten [ohjaavat tietovirtojen muodostumista]. (Haastateltava 1)

> -- luotetaan siihen, että se tieto pysyy siellä ja sitä ei kukaan lähde vuotamaan saatikka sitten hyväksikäyttämään millään tavalla vaan se on semmoinen turvallinen paik-

ka missä organisaatiot saavat sitten jakaa tietoa niin se luottamus ja sen säilyttäminen. (Haastateltava 2)

Se on mun mielestä myös hyvä ymmärtää ja hyväksyä, että kyllä se vaan menee sillä, että jos se vastapuolella ihmiset ei sinua tunne tai ole halukkaita sinua auttamaan tai eivät koe saavansa mitään hyötyä työstään, niin sitten voi olla, että se tietovirta ei sinne tule, vaikka sellainen periaatteessa olisi olemassa. -- mutta pakottamalla -- ei tässä toimintaympäristössä mun mielestä järjesty. (Haastateltava 5)

5.2.3 Yhteistoimintaverkosto

Kolmannessa osiossa selvitettiin haastateltavien näkemyksiä kyberturvallisuuden yhteistoimintaverkostosta ja siitä, millaista arvoa he näkevät, että verkosto tuottaa tilannekuvan muodostamisen kannalta. Haastateltavat olivat yhtä mieltä siitä, ettei kyberturvallisuuden tilannekuvaa ole mahdollista muodostaa ilman toisten toimijoiden kanssa tehtävää aktiivista yhteistyötä. Kuitenkin se, millaista tietoa jaetaan, vaihtelee verkoston mukaan ja kuinka luotettavana sitä pidetään. Kuten muissa osiossa, niin tässäkin haastateltavat nostivat esiin toimintakulttuuriin ja lainsäädäntöön liittyviä tekijöitä, jotka koettiin tiedon virtaamisen näkökulmasta rajoittavina eri toimijoiden ja toiminteiden välillä.

Siihen on kyllä helppo vastata, että se on välttämätöntä. Kukaan ei pysty tekemään kybertilannekuvaa yksin. Ja meillä on Suomessa onneksi pyristelty niistä siiloista eroon ja toivottavasti niistä päästään kokonaisuudessaan eroon, mutta meillä on ehkä vielä sellaista kulttuuria, ettei oikein olla halukkaita jakamaan sitä tietoa. Totta kai siinä on niitä tiedon jakamisen rajoitteita, -- mitä laki ei yksinkertaisesti anna myöden [jakaa], mutta kaikki muu siinä… tämmöinen ilmiötiedon jakaminen, niin siinä on onneksi menty paljon eteenpäin. Kyllä edelleen olisi paljon tehtävää. (Haastateltava 8)

Sitä ei pysty muodostamaan itsessään pelkästään omin lähtein kukaan vaan se vaatii sen verkoston ennen kaikkea näiden uhkatiedon ja suojantiedon suuntaan, missä sitä omaa [tilanne]kuvaa täydennetään. (Haastateltava 3)

Kyberissä se on isossa asemassa, että muistetaan että ei olla yksin… kyber vielä vähemmän kuin muut ilmiöt tunnistaa mitään maarajoja tai kaikki vaikuttaa kaikkeen, niin sen tiedon jakaminen on siinä avainasemassa, että pysytään siellä rikollisten tahdissa tai yritetään ehkä päästä jopa edellekin… niin se että me jaetaan havaintoja siitä että jos vaikka Belgiassa on käynyt jotain samaa mitä Japanissa, niin Suomessa voidaan oppia siitä… niin se on tärkeää että verkostoissa ollaan mukana ja tuotetaan sinne myös lisäarvoa eli ei vaan olla kuunteluoppilaana vaan todennäköisimmin silloin myös itse saadaan jotain hyvää tietoa sieltä. (Haastateltava 2)

Se ero näissä on, että minkälainen verkosto on ja minkälaista tietoa sinne jaetaan. Mitä pienempi tai tutumpi verkosto on, tai se on arvioitu sellaiseksi luottamukselliseksi verkostoksi niin siellä myös jaetaan paljon enemmän ja sellaista tietoa mitä ei julkisuuteen haluta. Ja sitten jos on todella iso verkosto, jossa ei voi pomminvarmaksi mennä sanomaan, että ketä kaikkia siellä edes on, niin se menee hyvin sellaisella yleisellä tasolla, ja näin ollen minä näen, että nämä eroaa kyllä toisistaan. Se on mi-

> nun mielestä just se merkittävä ero, että minkä tyyppistä tietoa jaetaan ja kenelle. (Haastateltava 6)

Vaikka tiedonvaihto ja yhteistoiminta kyberturvallisuuden saralla nähdään merkityksellisenä ja arvoa tuottavana kokonaisuutena, tunnistettiin tässä myös paljon kehitettävää. Toisaalta nähtiin tarve täsmentää, mitä tietoa kukakin verkostotoimija kerää ja jakaa muille, sekä määrittää mihin tieto taltioidaan, jotta se on tarkoituksenmukaisesti sitä tarvitsevien saatavilla. Haastatteluissa nousi lisäksi esiin mahdollinen tilannekuvaa vinouttava toimintatapa, jossa tieto ikään kuin vahvistaa itse itseään, kun eri tahot poimivat verkostosta saamiaan tietoja osaksi omia raporttejaan, joita edelleen jaellaan taas verkostossa eteenpäin. Yksi haastateltavista painotti avaintekijänä kunkin verkostotoimijan omaa aktiivisuutta siinä, miten merkitykselliseksi yhteistoiminta lopulta tiedon saatavuuden ja hyödyn näkökulmasta muodostuu.

> Ehkä tässä tiedonvaihdossa on kuitenkin se, että meidän pitäisi kuitenkin varoa sitä ettei me kierrätetä sitä samaa tietoa siinä myllyssä eli joku tuo siihen suppiloon tavaraa ja muut ottaa sen osaksi sitä omaa tilannekuvaa ja sitten se kiertää takaisin, eli se tieto vahvistaa itseään siellä [negatiivisessa merkityksessä], että meillä pitäisi olla sellainen tehtävänjako että kuka tuottaa mitäkin et saataisiin just ne tietovirrat, et jokainen tuottaa sen tietovirran ja sitten se siinä jossain kohtaa laitetaan yhteen. (Haastateltava 8)

> Puhuttiinpa sitten vaikka viranomaisista, niin on ihan luontevaa, että niillä kaikilla on omat palansa mistä ne kerää sitä tietoa ja niillä on omat alaverkostonsa mistä ne kerää sitä jne. Ja sillon tietenkin tullaan siihen, että se tieto alkaa kasaantua joissakin paikoissa ja sitten tullaan tähän klassiseen kysymykseen, että onko joku yksi paikka, jossa se kaikki tieto kasaantuu, ja sitten tullaan siihen mun alkuväittämään, että vaikka olisi niin meillä ei voi olla sellaista jumalkuvaa, että jaetaan se alaspäin ja se palveli kaikkia. (Haastateltava 3)

> -- tää verkostohan -- toimii ihan hyvin ja sitä tietoa vaihdetaan -- on montaa tahoa, on monenlaista seuraajaa, tietoa on saatavilla ja kun sä vaan lähdet mukaan yhteistoimintaverkostoon niin sitä tietoa on paljon saatavilla, nyt siihen vaaditaan vaan omaa aktiivisuutta. (Haastateltava 7)

Haastatteluissa tunnistettiin myös se, että tapausten selvityksessä saattaa usein olla mukana monia eri tahoja, jolloin voi olla hankala pysyä perillä siitä, kuka hoitaa mitäkin osuutta. Esimerkkinä nostettiin esille tilanne, jossa kyberhyökkäyksen kohteeksi joutunut organisaatio on ilmoittanut tapahtuneesta kansalliselle kyberturvallisuusviranomaiselle, tietosuojavaltuutetulle sekä tehnyt myös poliisille rikosilmoituksen, mutta on lisäksi palkannut kaupallisen tietoturvayhtiön selvittämään tapausta ja kieltänyt tätä jakamasta tietoa suoraan edellä mainituille viranomaisille. Tällöin myös tietovirtojen hallinta näyttäytyy haastavalta.

> No välillä voi olla ihan sellainen tilanne, että ei välttämättä tunnisteta niitä oikeita vastinpareja ja että toimittaisiin kyllä yhdessä ja vaihdettaisiin tietoa, mutta ei välttämättä tiedetty, että se toinen osapuoli omaa sitä tietoa tai olisi lisäarvoa tuotettava-

> na, että semmoinen ymmärrys siitä, että kuka käsittelee mitäkin ja kenen kanssa ollaan tekemisissä, niin sekin voi olla välillä vähän hankala kartoittaa. (Haastateltava 2)

> -- onhan siellä organisaatiopuolella varsinkin parantamisen varaa siinä, kuinka viranomaisille sitten ilmoitetaan. KTK:aan ei välttämättä saa kaikkia tietoja. (Haastateltava 8)

Tiedonvaihdosta ja verkostossa muodostetusta tilannekuvasta eri toimijoiden välillä nähtiin yhtenä hyvänä ja toimivana esimerkkinä viranomaisyhteistyö eli VIRT-toiminta esimerkiksi isojen kansallisten tapahtumien, kuten vaalien tai merkittävien valtiovierailujen yhteydessä. Lisäksi tunnistettiin, että tiettyjen toimialojen, kuten energiasektorin ympärille muodostuvat verkostot mahdollistavat kokonaisturvallisuuden viitekehyksessä toimialakohtaisesti tapahtumien ja niiden vaikutusten syvällisen seurannan, mikä tuottaa hyötyä laajemmin kansallisessa mittakaavassa eri toimijoille.

> Meillä on useita vuosia vaalien yhteydessä ollut tällainen vaali-VIRT toiminta, ja siihen tiettyyn teemaan liittyen järjestetään sitä tiedonvaihtoa niiden tahojen kesken, jotka siinä on ne keskeiset toimijat. Siinä kohdennetusti tehdään tällaista tilannekuvan vaihtoa ja sitten totta kai se tiivistyy sinne, kun se tapahtuma on päällä, jolloin tarvittaessa ollaan useita kertoja päivässä yhteydessä keskenämme. Ja silloin pystytään aika nopeasti reagoimaan, jos jotain tapahtuu ja silloin meillä on siinä keskeiset tekijät, joilla on se oma näkymä siihen esimerkiksi vaaliviranomaisilla siihen omaan tehtäväänsä. Saadaan ensikäden tietoa, jos jotain näkyy, et meillä ei ole mitään isoa, kankeaa rakennetta siinä mikä viikon jauhaa jotain asiaa ennen kuin se jalkautuu, vaan se on hyvin kohdennettua ja notkeaa se toiminta. (Haastateltava 8)

> -- niissä verkostoissa pystytään myös aina pureutumaan tiettyyn asiaan, toki tällä alalla tapahtuu ihan hirveästi kaikkea, mutta on myös tärkeää pysähtyä, vaikka energia-alan toimijoiden kyberturvallisuuteen, niin on tärkeää, että me saadaan keskeisiä toimijoita ja saadaan heiltä sitä tilannekuvaa ja mikä heidän näkemys on. Ja sitten just vaikka taas viranomaisten puolelta pystytään syöttämään sille puolelle tietoa, miten kannattaa varautua tai millaista yleishavaintoa on ollut, että pystytään vähän myös sinne jakamaan sitä tietoa ja tilannekuvaa siltä osin kuin sitä pystyy melko julkisesti kertomaan. (Haastateltava 6)

Jaetun tilannekuvan lisäksi jokainen toimija muodostaa kybertilannekuvaa ensisijaisesti kuitenkin omiin uniikkeihin tarpeisiinsa. Tähän liittyen muun muassa tunnistettiin yhtenä keskeisenä tarpeena teknisen uhkatiedon jakaminen verkostossa, jota vasten eri toimijat voivat muodostaa tarkempaa arviota heihin mahdollisesti kohdistuvista uhkista sekä myös evästää teknistä valvontaa ja niin edelleen. Myös tässä nykymuotoinen lainsäädäntö nähtiin toimintaa rajoittavana ja jopa estävänä tekijänä. Tietoa ei ole saatavilla tarpeeksi nopeasti ja spesifillä tarkkuudella, jolloin jäljet ehtivät niin sanotusti jäähtyä esimerkiksi teknisen tutkinnan näkökulmasta.

> -- niitä kybertilannekuvatarvitsijoita on ihan valtavan monessa kerroksessa ja ihan valtavan monella eriävällä tasolla, ja näin ollen se mun oma ajatus tästä nykyhetkellä on hyvin pitkälti se, että näiden perusteltujen rajoitusten… ymmärrän ne, mutta ne

> pitää olla perusteltuja ja ne minimoiden, meillä tulisi olla mahdollisimman suuri määrä tarvittaessa kontekstista irrotettua teknistä uhkatietoa ja toisaalta hyvin avoimesti jaettua käytettävissä olevaa tätä suojantietoa, jolloin tavallaan jokainen organisaatio pystyisi siitä massasta omien prosessiensa puolesta muodostamaan sen tilannekuvansa -- ja nythän nähdäkseni juurikin näiden teknisten yksityiskohtien jakaminen on se haastavin asia, mikä toisaalta olisi se mun nähdäkseni se eniten organisaatiota hyödyttävä asia. (Haastateltava 3)

> Tieto kyllä vaihtuu, mutta kyllä sitä edelleen rajoittaa, että meillä on tiettyjä tämmöisiä osin lainsäädännöstäkin johtuvia, mitkä estää sellaiset täsmällisen tiedon jakamisen. Ja se on tietenkin aikamoinen ongelma, koska sitten siinä tulee niitä tilanteita, että me tiedetään että jotain on tapahtunut, mutta me emme saa sitä täsmällistä tietoa ja sitten mennään vähän toinen silmä ummessa eteenpäin tai sitten saattaa olla, että jokin tapahtuma tulee meille jotain toista kautta tietoon viiveellä ja se olisi ollut saatavissa jo aiemmin, ja sitten jos se tulee meille sanotaan kahden viikon viiveellä tietoon niin meidän on aika vaikea enää… tottakai me otetaan se tieto vastaan ja lähdetään tekemään mitä on tehtävissä, mutta tässä skenessä se kaksi viikkoa on valitettavan pitkä aika ja voi olla, että ne jäljet on jo jäähtynyt. (Haastateltava 8)

Lisäksi tunnistettiin, että esimerkiksi valtionhallinnossa kaikki toimijat eivät ole vielä kyberturvallisuuden tietojohtamisen organisatoristen ja teknologisten valmiuksien osalta sillä maturiteettitasolla, että kaikilta osin olisi olemassa muun muassa tarkoituksenmukaiset tiedonvaihtokanavat. Yhden haastateltavista kokemuksen mukaan tämä vaikuttaa siihen, että vaikka tietoa haluttaisiin jakaa, on se järkevän tiedonvaihtokanavan puuttumisen vuoksi jopa jätetty jakamatta. Myös toimijoiden erilainen tulkintapohja tiedon hyödyntämisen ja edelleen jakelun suhteen nousi esiin haastatteluaineistosta, mikä osaltaan voi vaikuttaa tietovirtojen muodostumiseen.

> -- meillä on sellaisia tilanteita, että haluttaisiin jakaa jotain uhkatietoa, mutta ei ole varmuutta siitä, että millä tavalla ja kenelle se ois tarkoituksenmukaista jakaa, ja sen vuoksi päädytään tekemään tuota manuaalista työtä. Tai sitten on sellaisia tilanteita, että oltaisiin haluttu antaa jotain tietoa, mutta sitten on todettu, että koska ei ole mitään järkevää kanavaa jakaa sitä, niin ei lähdetäkään antamaan sitä tietoa. On niinku tunnistettu näitä ongelmia ja pyritty aktiivisesti ratkaisemaan, mutta sitten välillä kohdataan ongelmia että meillä on joku työkalu käytössä tai ollaan ottamassa sitä käyttöön, mutta meidän vaikka vastinkumppanit valtionhallinnossa eivät ole vielä sillä maturiteettitasolla, että heillä olisi se käytössä tai he eivät yksinkertaisesti ole kokeneet sille tarvetta, vaikka tekninen kyvykkyys siihen olisikin tai sitten he tulkitsee jotain tietoa sillä tavalla, että se on vain heidän käyttöönsä, että se on jotain sellaista tietoa mitä he ei just tähän alustaan halua laittaa niin sekin voi monessa tiedossa tulla sillä tavalla vastaan… (Haastateltava 2)

> -- tyypillisesti saattaa olla niin että organisaatioiden johdon tasolla, mitkä muodostavat omia verkostojaan niin siellä voidaan jakaa tätä ikään kuin ihmisten välisessä, kun ne tuntee toisensa niin siellä verkostossa voidaan jakaa kohtuullisen tarkkaakin tietoa, sellaisella klausuurilla kuin että vain teidän tietoonne, ja sitten tullaan yhteen isoon haasteeseen siinä mielessä, että siinä organisaatiossa voi olla, että sen johto tietää sellaisia asioita mitä ei taas tiedä se suorittava porras, kenen pitäisi tehdä niitä tai suosittaa tehtäväksi niitä toimenpiteitä millä suojata. (Haastateltava 3)

5.2.4 Haasteet ja kehittämiskohteet

Haastateltavilta kysyttiin lopuksi mitkä ovat heidän mielestään isoimmat tietovirtoihin liittyvät haasteet kybertilannekuvan muodostamisen kontekstissa. Kukaan haastateltavista ei todennut, että mitään haasteita tai kehitettävää ei olisi tunnistettavissa. Kenties isoimmat haasteet, jotka aineistosta nousevat esiin liittyvät joko tiedon saatavuuteen tai lainsäädännöllä sekä toimintakulttuurilla perusteltaviin rajoitteisiin.

Vastauksissa nousi esiin tarkemmin yhteistoimintaan ja sitä kautta tiedon jakamiseen sekä käsiteltävän tiedon valtavaan määrään ja sen hallintaan liittyviä haasteita. Lisäksi haasteita nostettiin esiin tiedon sensitiiviseen luonteeseen, turvaluokitteluun ja erilaisiin ympäristöihin, sekä tiedon henkilöitymiseen liittyen. Lähtökohdaltaan tunnistettiin, että yleisesti organisaatioiden toiminta on tällä hetkellä jokseenkin enemmän reaktiivista, mikä nähtiin raportoinnin ja tiedonvaihdon aikajänteen osalta myös ongelmallisena erityisesti oman toiminnan suuntaamisen kannalta. Lisäksi merkityksellistä tietoa ei välttämättä saada välitettyä eteenpäin riittävän nopeasti.

> -- se valtava määrä tietoa, että se päätyy… kun meilläkin on erilaisia, eri tasoisia, eri leimauksella hyväksyttyjä järjestelmiä, erilaisten tietojen käsittelyyn… ja sitten niitä joko saa tai ei saa tallentaa, tai ei saa käsitellä jossain tietyssä ympäristössä… ja jos toimii työssään pääsääntöisesti sellaisessa ympäristössä, mihin on vaikeampi jakaa tietoa niin tavallaan sekin voi olla sellainen, että tieto on saatavilla, mutta sun ympäristöön sitä ei ole saatavilla… niin se on välillä ongelmana. Tai sitten se, että miten joku tieto saavuttaa yksittäisen henkilön… sit pitäis aina jotenkin muistaa, että on heitäkin, jotka toimii eri ympäristössä. (Haastateltava 2)

> Ensinnäkin haasteena on -- valtava informaation määrä, eli sitä mahdollista tietoa on niin paljon. Ja toinen oli pääsy siihen tietoon. Siinä oli nämä eri syistä tulevat rajoitteet, oli ne sitten kaupallisia, lainsäädännöllisiä, viestinnällisiä, jne. eli tieto voisi olla saatavilla, mutta sitä ei kuitenkaan saa tai toinen ei jaa. (Haastateltava 3)

> Tai sitten voi olla sellaisia, että jokin tieto on hirveän henkilöitynyttä että olen saanut tämän tiedon vaikka [x] yhteyshenkilöltä ja tämä on vain minun silmilleni, niin se on myös tavallaan vaikeaa, että sä näet sen vain itse etkä sä oikein voi jakaa sitä kenellekään tai jos jaat, niin sitä ei saa jakaa siitä pisteestä eteenpäin… se tieto vois olla sellaista, mitä haluttais hyödyntää muuallakin, mutta me ei voida sitä tehdä niin se on hankalaa tai sitten voi olla sellainen, että se tieto menee jollekin tiimille ja se tiimi on työnkuvansa vuoksi, että he ei vaikka halua tai näe tarvetta jakaa sitä muille tiimeille niin… vaikka se tieto on meillä olemassa, mutta se menee jotenkin niin rajatulla porukalla että sitä tavallaan voi ajatella ikään kuin meillä ei sitä edes olisi, vaikka se on meillä ollut ja se olisi ihan käytettävissä ihan leimauksiensa puolesta… en tiedä onko se tiedon mustasukkaisuutta, että tämä on nyt minun silmilleni ja minun tiimilleni, niin en nyt anna tätä muille… (Haastateltava 2)

> Lähtökohta sen asetelman reaktiivisuudesta on väärä. Tietysti tapahtumat itsessään, kun ollaan reaktiivisessa moodissa, niin niillä voi olla hyvinkin nopea aikajänne, miten ne tapahtuu tai miten niihin pitäisi reagoivasti vastata, ja se on toki se yksi ominaispiirre, mikä siihen tilannekuvaan ja varsinkin tilannekuvan jopa yksittäisen ta-

> pahtumaan liittyvän tietojen jakamisen eri toimijoiden ja viranomaisten välillä pitäisi kiinnittää huomiota. Ei voi olla niin, että kuullaan seuraavana päivänä tai viikkotilannekuvassa tai jossain kuukausikatsauksessa jostain tapahtumasta, jolla olisi voinut olla merkitystä ja vaikka oman toiminnan suuntaamisen kannalta merkitystä, niin muillekin toimijoille kuin sille, jolle on ilmoitettu kyseinen tapahtuma. (Haastateltava 4)

Osin tiedon valtavan määrän takia, haasteena tunnistettiin myös välillä jokseenkin rajoittunut kyky havaita, mikä on oman toiminnan tai laajemmin yhteistoiminnan kannalta kulloinkin merkityksellistä tietoa. Tilannekuvan muodostamisen kannalta nähtiin tärkeänä, että toimijat puhuisivat samoilla termeillä, jolloin myös tapahtumista muodostuisi jaettu samankaltainen ymmärrys.

> Ja toisaalta valtavasta massasta on hankala ymmärtää mikä on milloinkin relevanttia, joku asia mikä tänään tapahtui minkä me mennään vaan siitä ohi, saattaisi olla, että se olisi pitänyt siinä vaiheessa huomata ja tehdä jotain toimenpiteitä. (Haastateltava 3)

> Tiedän, että sitä työtä tehdään jo. Mutta ehkä ylipäätänsä se, että kun puhutaan noista tietovirroista, että tunnistettaisiin ne omat tietovirrat ja miten sitä tietoa pystytään hyödyntämään ja käyttämään. Koska siellä on sellaisia asioita, että meille kertyy vaikka paljon tietoa mitä me ei vaan jostain syystä tunnisteta tai osata hyödyntää ja sitten toisaalta siihen tilannekuvaan ja siihen on tärkeää, että vaikka edes viranomaiset puhuisivat samaa kieltä, kun me puhutaan tilannekuvasta, niin me ymmärrettäisiin se samalla lailla. (Haastateltava 6)

Aineiston pohjalta nousi esiin myös kritiikkiä siitä, ovatko kokonaisturvallisuuden viitekehyksessä esitetyt poliittiset ja strategiset tahtotilat todellisuudessa jalkautuneet käytännön tekemiseen asti. Kritiikin taustalla esitettiin muun muassa näkemys siitä, jos todellinen tahtotila olisi olemassa, nähtäisiin nykyisessä lainsäädännössä enemmän mahdollisuuksia kuin, että etsittäisiin sitä kautta rajoitteita tiedon jakamiselle viranomaisten välillä. Yhtenä näkökulmana nostettiin esiin kyberpuolustus, jonka osalta on jokseenkin epäselvää, miten ja millä perusteilla tieto kuuluu millekin viranomaiselle. Toisaalta tiedon jakamisen rajoittumiseen liitettiin myös osin kulttuurisia syitä, kuten tiedon mustasukkaisuutta.

> -- mun mielestä se keskeinen kehittämiskohde on tän meidän kansallisen mallin aito kriittinen tarkastelu niin, että päästään tavallaan… ja sitä pitäisi nimenomaan aidosti tarkastella, eikä pitäytyä niissä olemassa olevissa kenenkään, myöskään meidän… niin miten me tehtäisiin tämä kansallisesti paremmin. Jotkut maat ovat kyenneet tähän erinäköiseen kriittiseen tarkasteluun olemassa olevan mallin osalta, ja lähteneet hakemaan uusia ratkaisuja. Ruotsilla on joitain esimerkkejä ja kansallinen kyberturvallisuuskeskus on poikkiviranomais[organisaatio], se ei ole yhden viranomaisen vaan tällainen poikkihallinnollinen [toimija]. (Haastateltava 4)

> Viranomaiset kuitenkin toimii toimivallan perusteella ja jos toimivalta ei ole kunnossa tai viranomaisten tehtävä ei ole kunnossa -- niin hyvin vaikea on nykyään tehdä yhtään mitään, kun halutaan tulkita toimivaltaa ja oikeuksia rajoittavasti eikä mah-

> dollistavasti. Esimerkiksi se, että tällä hetkellä kyberpuolustus ei ole sanatarkasti sellaisenaan säädetty puolustusvoimien tehtäväksi, vaikka se valtioneuvoston päätöksissä on näin tehty, niin rajoittaa jossain määrin jo olemassa olevan toimivallan soveltamista esimerkiksi lainsäädännöstä puolustusvoimien osalta. Sitä voidaan tietysti tulkita, että se kuuluu sotilaalliseen maanpuolustukseen niin kun se kuuluukin, mutta se on [puolustusvoimien] tulkinta ja muut viranomaiset ei välttämät tulkitse sitä samalla tavalla. Jolloin heti välittömästi on tiedonjakamisen ja tietovirtojen näkökulmasta on konflikti, millä perusteella ja miksi puolustusvoimat haluaa jotain tietoa käyttöönsä. (Haastateltava 3)

> Kyllä mä edelleen palaan siihen tiedonvaihdon rajoitusten purkamiseen, siellä on sellaisia osin lainsäädännöllisiä ja osin kulttuurillisia rajoitteita, mitkä pitäisi saada purettua, että saataisiin tiedonvaihto etenkin tässä nykyisessä tilanteessa, nyt se on kullan arvoista, että se tieto vaihtuu ja että tilannekuva olisi kaikilla mahdollisimman hyvä. Kyllä mä noita pidän aivan kärkihankkeina selvästi. (Haastateltava 8)

Haastateltavat esittivät ratkaisuja tietovirtojen hallintaan ja tiedon jakamiseen niin organisatorista lähtökohdista kuin valtionhallinnon tasolta asti. Keskeisenä nähtiin tunnistaa, mikä on oman toiminnan kannalta merkityksellistä tietoa ja miten organisaation tulisi rakentaa sisäiset toiminteensa, jotta tiedosta saadaan maksimaalinen hyöty. Merkityksellisen tiedon tunnistamisen lisäksi tärkeänä nähtiin tunnistaa oman toiminnan kannalta keskeiset sidosryhmät ja niistä muodostuva verkosto ja panostaa aktiiviseen viestimiseen. Huomiota kiinnitettiin myös lainsäädäntöön ja erilaisiin organisaatioiden ja verkostojen teknisiin valmiuksiin ja tietojärjestelmiin. Yhteistoiminnan kannalta merkityksellisenä nähtiin myös yhteneväiset toimintatavat ja yhteinen terminologinen tulkintapohja, joita tulisi edelleen kehittää.

> -- tulee tunnistaa, mikä on oman toiminnan kannalta se relevantti tieto, pitää miettiä kuka siinä organisaatiossa sitä johtaa, ketkä sitä tekee, missä sitä tehdään ja tunnistaa ne verkostot ja aktiivisesti viestiä niissä, ja tunnistaa se hiljaisen eli epäformaalin tiedon merkitys. Ja sitten on tämä tekninen ratkaisu eli paraskaan ihmisjoukko, jotka chatissa tai powerpointeilla tai fyysisessä kokouksessa sitä tietoa jalostaa ja jakaa niin, just sen [tiedon] määrän takia se ei ratkaise vaan yrityksen on investoitava, jos tämä on heille tärkeää ja haluaa tän itse tehdä, niin sen [yrityksen] on investoitava jonkunlaiseen kybertilannekuvajärjestelmään. (Haastateltava 3)

> Ja sitten varsinkin nimenomaan viranomaistyössä, että olisi se lainsäädäntö, joka tukee tätä nykyaikaa ja näitä haasteita ja uhkia, jotka meillä on. Ne on mun mielestä tosi tärkeitä, koska ne on sitten taas niitä millä pystytään takaamaan se yhteiskunnan turvallisuus laajemminkin. Ja toki lait on tehty aikana ennen kuin kyber oli edes kyberiä, että kyllähän se niissä näkyy… Ja siksi mun mielestä olisi hyvä, että saataisiin lainsäädäntö vastaamaan joiltain osin tätä tasoa, täydelliseksi se ei tule ja täällä asiat muuttuu nopeammin kuin lainsäädäntö, mutta kuitenkin niin, että ne toimintaedellytykset olisi. (Haastateltava 6)

> -- mun mielestä kaiken pitää lähteä ylhäältä, valtioneuvoston tasolta… valtion johdon tasolta, jos puhutaan vaikka varautumisvaatimuksista --, niin ne vaatimukset pitää lähteä sieltä ja sitten antaa resurssit laskea kuinka paljon, minkälaisia resursseja vaaditaan, että päästään johonkin tasoon. Ja samalla tavalla miettiä, minkälaista ti-

> lannekuvaa me siitä halutaan. -- Ja näin se pitää ollakin, että ne tulee ylhäältä ne tarpeet, että kuinka ne tietovirrat liikkuu ja mikä on se tilannekuva ja kyberin osuus siellä. -- niin tää koko kokonaisuus pitäisi uudistaa, jotta ne kokemukset näkyisi siellä ja miettiä samalla kuinka niiden kyberturvallisuuden ja kybertilannekuvan, muuhunkin tilannekuvaan liittyvien, tietovirtojen pitää tavallaan kulkea ja mitä asioita meidän pitää ottaa varautumisessa huomioon, minkälainen valmius saavuttaa. (Haastateltava 7)

> -- tietysti näkisin mielelläni sellaisen järjestelmän, että meillä olisi tällainen yksi kyberin tilannekuvajärjestelmä, johon jokainen tuottaisi tietoa ketkä siinä on mukana ja kaikki sen saman tiedon sieltä myös saisi, eli se olisi osallistujilleen hyvin tällainen läpinäkyvä järjestelmä, joka parhaimmillaan tuottaisi hyvinkin reaaliaikaista ja kattavaa tilannekuvaa. -- Vaikea ehkä järjestää ja pitäisi miettiä tarkkaan, miten sinne tietoa syötetään, mutta se vaan että tällä hetkellä jokainen puuhaa vähän siellä omillaan ja sitten tietoa jaetaan, niitä raportteja, ja niin kuin sanoin, niin se sama tieto saattaa kiertää siellä vähän niinku useammassa raportissa, että pitäisi vain kasata mahdollisimman yksiin kansiin ja yhdenmukaisesti, ja nimenomaan näistä eri tulokulmista, jokainen tuottaisi sen omansa siihen ja sitten se olisi se yhteinen kakku siellä kaikkien tarkasteltavana. (Haastateltava 8)

> -- että meidän järjestelmät tukisi meidän työtä, koska mä uskon, että tällä hetkellä monet kärsii siitä, että ne järjestelmät ei tue tai sellaisen järjestelmän tekeminen on vain niin kallista, että siihen ei ole varaa, ja sitten mennään vaan jollain powerpointeilla tai wordilla ja ollaan ihan tosi tyytyväisiä. Mut siis se, että järjestelmät olisi sellaisia, että ne tukisivat sitä tekemistä ja olisivat myös yhteneväisiä, koska sekin luo nimenomaan yhteistoimintaan, että me tehdään yhdessä samalla tavalla, meillä on yhteinen terminologia, käytetään samanlaisia järjestelmiä joissa voi olla jotain pieniä eroja sen organisaation omiin tarpeisiin nähden, mutta isossa kuvassa asioita tehtäisiin samalla tavalla että oltaisiin enemmän yhteneväisiä etenkin vaikka siellä viranomaispuolella. (Haastateltava 6)

Vastauksissa näkyi lisäksi tarve käsitellä aihetta myös laajemmassa kontekstissa, missä huomioidaan kybermaailman tapahtumien liityntäpinta myös reaalimaailman tapahtumiin ja siten myös sitä kautta muodostuviin tietovirtoihin. Yksi haastateltavista lisäksi korosti tarvetta kehittää analyysimenetelmiä, jotta saatujen tietojen perusteella tehtyihin päätelmiin on mahdollista palata, ja jotka siten tukevat tietovirtojen hallintaa kybertilannekuvan muodostamisen kontekstissa niin organisaation sisällä kuin laajemmin verkostossakin.

> Itseasiassa se täytyy muistaa, etenkin tässä nykyisessä tilanteessa, että se me pidetään kybertilannekuvaa, niin se on kybertilannekuvaa, mutta täytyy kuitenkin muistaa yhteys tuohon reaalimaailmaan eli että pitäisi koittaa siitä huolimatta katsoa myös ympärille, sen kyberin putken ulkopuolelle että mitä reaalimaailmassa tapahtuu ja onko niillä yhteyttä sinne kyberiin ja päinvastoin. Koska tässä kuitenkin eletään nyt maailmassa, jossa nää tietoverkot, niin ne on käytännössä osa kaikkea meidän elämää, niin se on väistämättä selvää, että jos kyberissä rupee tapahtumaan paljon niin ne todennäköisesti näkyy reaalimaailmassa ja päinvastoin. -- Tää on hyvä muistaa, eikä pidä vain lukittautua siihen ja katsoa sen kapean putken läpi vaan kyllä sitä on hyvä myös yhdistää tähän reaalimaailmaan ja muistaa, että ne aika tiiviisti tekemisissä keskenään. (Haastateltava 8)

-- mun mielestä se, että kun niitä tietovirtoja on todella paljon, niin sen tiedon listaamisen lisäksi me pystyttäisiin tekemään sitä analyysia vielä paremmin ja vielä jotenkin strukturoidummin, että se ei ole vain hiharavistelua vaan se perustuu menetelmiin ja siihen voidaan palata, ja miettiä miksi on tehty jollakin tavalla ja on päästy johonkin tulokseen. Sitä että organisaatiot tekee itse analyysia mutta myös sitä yhteistä ja yhdistettyä analyysia, kun ne kun saisi vielä, ne nostaisin tähän vielä sellaisiksi kehityskohteiksi. (Haastateltava 6)

6 TULKINTA JA POHDINTA

Tässä luvussa käsitellään tutkimuksen tuloksia vastaamalla tarkemmin tutkimustehtävään ja pohditaan tutkimuksen merkitystä. Lisäksi alaluvuissa arvioidaan tutkimuksen luotettavuutta ja pohditaan edelleen mahdollisia jatkotutkimusaiheita.

Tutkielman tavoitteena oli pyrkiä tunnistamaan parhaat käytänteet tietovirtojen hallintaan kybertilannekuvan muodostamisen kontekstissa. Jo pelkästään tutkielman kirjallisuuskatsausosio kuvastaa, miten moniulotteisesta aihekokonaisuudesta on kyse, kun puhutaan tietojohtamisesta, erilaisista organisaation tietoprosesseista sekä tietovirroista ja niiden hallinnasta. Tietoon ja siihen liittyvät ilmiöt mielletään lisäksi usein monimutkaisiksi ja abstrakteiksi (Laihonen ym., 2013), mikä näkyi myös tässä tutkimusprosessissa tietynlaisena haastavuutena. Tässä tutkimuksessa tietovirtoja pyrittiin hahmottamaan kybertilannekuvan muodostamisen kontekstissa hakien näkemyksiä niin organisaation, verkoston kuin myös laajemmin yhteiskunnan näkökulmista. Monipuolisen ja laajahkon tulokulman valinta perustuu siihen, että aihetta on tutkittu Suomessa aiemmin jokseenkin vähän.

Tutkimustulokset kuvaavat aihepiiriä ylätasolla eikä kovinkaan yksityiskohtaisia käytänteitä tietovirtojen hallintaan ole mahdollista kerätyn aineiston pohjalta esittää. Ylätason käsittely on perustelu osin myös aihepiirin sensitiivisellä luonteella. Siten tutkimusaineiston pohjalta ei myöskään ole mahdollista vastata tutkimuksen pääkysymykseen tietovirtojen hallinnan ideaalimallista kybertilannekuvan muodostamisen kontekstissa täysimittaisesti. Sen sijaan tutkimuksessa kuitenkin tunnistettiin melko laajasti periaatteita, joita tietovirtoihin ja niiden hallintaan kybertilannekuvan muodostamisen kontekstissa liittyy. Lisäksi tunnistettiin liuta haasteita, jotka jossain määrin enemmän ja vähemmän vaikuttavat tietovirtoihin ja niiden hallintaan tutkimuksen viitekehyksessä, mikä puolestaan kertoo siitä, ettei aihetta voida pitää itsestään selvänä.

Haastateltavien näkemykset kybertilannekuvan muodostumisesta ja siihen liitettävät erityispiirteet kertovat, että toimijoilla on lähtökohtaisesti hyvin samankaltainen käsitys kybertilannekuvan tehtävästä yleisesti organisaatio- ja kokonaisturvallisuuden konseptitasoilla. Kybertilannekuvaa ei pidetä arvona itsessään, vaan päätöksenteon ja toiminnan mahdollistavana välineenä tai sitä

ohjaavana elementtinä. Toisaalta aihe herätti myös jokseenkin eriäviä näkemyksiä siitä, miten kokonaisuus toimii kansallisella tasolla, muun muassa lainsäädännön tulkinnan ja toimivaltuuksien näkökulmasta, mikä ohjasi aiheen tarkastelua alkuperäistä ajatusta kenties hieman laajempaan, mutta sitäkin merkityksellisempään suuntaan. Tässä tutkimuksessa kokonaisturvallisuuden yhteistoimintamalli ja sen sisällä kyberturvallisuus omana toimintakenttänään muodostavat ”ba:n” eli yhteisen kontekstin (Nonaka & Konno, 1998; Huotari ym., 2005), jossa kybertoimijat ovat vuorovaikutuksessa keskenään eri tavoin.

Laihonen ym. (2013) ovat todenneet, että ”tietoon ja sen johtamiseen liittyvät asiat nivoutuvat niin luontevasti organisaation arkiseen tekemiseen, ettei tietojohtamisen käytäntöjen olemassaoloa välttämättä edes tiedosteta”, mikä on osin todettavissa myös tämän tutkimusaineiston pohjalta. Tietovirtoihin ja niiden hallintaan liittyvien keinojen nimeäminen käytännön tekemisessä voi tuntua haastavalta tai niiden merkitystä ei osata liittää osaksi omaa tehtävänkuvaa. Esimerkiksi havainnoinnin osalta näyttäytyi siltä, ettei poikkeamaraportointia kyetty toteuttamaan käytössä olevilla menetelmillä riittävän tarkasti, jotta tapahtumat olisi osattu huomioida tilannekuvassa tarvittavalla painoarvolla. Toimintaa tukeviin ja ohjaaviin prosesseihin sitoutuminen voi olla haastavaa, jos yksilöillä ei ole tarvittavaa ymmärrystä tai kokemuspohjaa tehtäväkokonaisuudesta. Tämä liittyy osittain hiljaisen tiedon välittymiseen, joka Nonakan ja Takeuchin (1995) mukaan on mahdollista vain, jos yksilöiden välillä vallitsee yhteinen kokemus. Ilman tätä yksilön on vaikea heijastaa itsensä toisen ihmisen ajatteluprosessiin ja tunnistaa, mikä tieto on merkityksellistä.

Erityisesti havainnoinnin perusteella näyttäytyi siltä, että yksilötasolta lähtevä toiminta, yksilöiden asiantuntijuus ja toimintakentän tuntemus vaikuttavat merkittävästi siihen, millaiseksi tietovirrat muodostuvat. Tämä edellyttää laajaa organisaation sidosryhmäkentän ja eri tietotarpeiden tuntemista, sekä lisäksi saumatonta ja aktiivista otetta tiedonjakamiseen eri toiminnan tasoilla. Toisaalta haastatteluaineistossa näkyi, että jokainen painotti vastauksissaan jokseenkin eri osatekijöitä, mikä selittyy varmasti osin haastateltavien eri taustoilla ja työtehtävien eri painoalueilla. Tutkimusaihe on kuitenkin merkittävä, sillä ilman ymmärrystä organisaatioiden tietoprosesseista, joiden kautta tieto muuttuu oivallukseksi, tietämykseksi ja edelleen toiminnaksi, eivät organisaatiot pysty hyödyntämään tietoresurssiensa ja -teknologioidensa todellista arvoa (Choo, 1998, s. 1–2).

Tutkimustehtävän kannalta avainroolissa näyttäytyy ennen kaikkea kyky tunnistaa, kenelle kybertilannekuvaa tehdään ja millaisia tietotarpeita heillä on. Se millaisia tietovirtoja ja niiden hallinnan mekanismeja nämä tietotarpeet lopulta muodostavat vaihtelevat eri toimijoiden välillä, eikä niitä siten voi täysin yleistää tai verrata keskenään. Osin tästä syystä tutkimustehtävän pääkysymykseen ei nähty riittävää perustaa vastata. Tietovirtoja on toki ylätasolla mahdollista määrittää erilaisten virtausmallien avulla (mm. Ahlavuo ym., 2011), joita on avattu jo kirjallisuuskatsauksessa, mutta nämä antavat vain kategorista osviittaa ja tukea toimijakohtaisten tietovirtojen hahmottamiseen. Tutkimuksen pohjalta tietovirtojen hallinta kybertilannekuvan muodostamisen kontekstissa

näyttäytyy moniulotteiselta ja jopa haastavalta kokonaisuudelta hahmottaa jo pelkästään eri tietolähteiden valtavan määrän takia. Toisaalta yksityiskohtaisten tietovirta-analyysien tekemistä julkisessa tutkielmassa ei katsottu myöskään aihepiirin sensitiivisen luonteen vuoksi mahdollisiksi.

Tietovirtojen hallinta kybertilannekuvan muodostamisen kontekstissa ei pelkästään edellytä tietolähteiden tunnistamista, mutta myös erilaisten osatekijöiden, kuten teknisten valmiuksien, toimintamallien ja prosessien luomista, jotta merkityksellinen tieto on saatavilla ja hyödynnettävissä tarkoituksenmukaisesti. Havainnoinnin tulokset osoittivat, että kaikki nämä osatekijät vaativat organisaatioilta paljon suunnittelua ja aktiivista työstämistä, jotta ne saataisiin valjastettua tukemaan tilannekuvatyöskentelyä mahdollisimman optimaalisesti. Lisäksi kiinnostavana huomiona tietovirtojen muodostumisen kannalta tutkimuksessa nousi esiin, että pienetkin tekniset yksityiskohdat koetaan kybertilannekuvan kontekstissa merkityksellisinä jopa toiminnan ylemmillä tasoilla. Toisaalta kybertoimintaympäristössä tapahtumien potentiaalinen kehitysnopeus, esimerkiksi tunnistettujen haavoittuvuuksien hyväksikäytöistä voivat eskaloitua hyvinkin nopeasti, jolloin organisaatioilla tulee olla toiminnalliset ja tekniset valmiudet tiedon prosessointiin tarvittavalla tavalla. Panostus tietovirtoihin ja niiden hallintaan on siten osa myös valmiudellista suunnittelua.

Yhtenä tietovirtojen hallinnan edellytyksenä tutkimuksen perusteella on mahdollisimman yhdenmukainen tapa käsitellä ja jakaa tietoa, mukaan lukien toimijoiden välillä yhteinen terminologinen tulkintapohja. Kuusisto ja Kuusisto (2006) viittaavat tähän 'yhteisen tietoalkion' käsitteellä, kun taas Pöyhönen ym. (2019) puhuvat 'ympäröivästä tietoavaruudesta' jotka siis periaatteiltaan molemmat tarkoittavat asioiden järjestämistä siten, että tieto ymmärretään kollektiivisesti "oikein" ja eri toimijoilla on myös pääsy heille merkitykselliseen tietoon. Toimijoiden erilainen tulkintapohja tiedon hyödyntämisen ja edelleen jakelun suhteen nousi esiin haastatteluaineistosta, mikä osaltaan tunnistettiin tietovirtojen muodostumiseen vaikuttavana tekijänä. Esimerkkinä tästä mainittiin vapaaehtoisuuteen perustuvat tiedon jakeluluokitukset, kuten Traffic Light Protocol TLP, jotka koettiin alkuperäisestä tarkoituksestaan poiketen enemmän toimintaa haittaavina ja turhan kriittisesti tiedon jakamista rajoittavina tekijöinä. Pahimmillaan näiden koettiin jopa sivuuttavan tiettyjen viranomaisten juridista tiedonsaantioikeutta.

Tutkimus osoittaa, että tarkoituksenmukaiset tietojärjestelmät ja niiden käytettävyys ovat kriittisiä tekijöitä hahmotettaessa tietovirtojen muodostumista ja niiden hallinnan edellytyksiä niin organisaatio- kuin verkostotasollakin. Tutkimuksessa tunnistettiin, etteivät esimerkiksi valtionhallinnossa kaikki toimijat ole vielä samalla kyberturvallisuuden maturiteettitasolla kyberturvallisuuden tietojohtamisen organisatoristen ja teknologisten valmiuksien osalta. Se, ettei toimijoilla ole erilaisiin tiedonvaihtotarpeisiin soveltuvia tiedonvaihtokanavia tai muita yhteistoimintaa ja tiedonvaihtoa tukevia mekanismeja käytössä, vaikuttaa luonnollisesti siihen, miten hyvin merkityksellistä tietoa on ylipäätään mahdollista saada käyttöönsä. Muodostuva arvopotentiaali on toisaalta siten toimijoiden omasta aktiivisuudesta kiinni, millaiseksi he toimintaedelly-

tyksensä rakentavat kyberturvallisuuden tietojohtamisen näkökulmasta. Tutkimuksen perusteella tietovirrat muodostuvat tällä hetkellä usein manuaalista työtä vaativien prosessien varaan, mikä vie resursseja muun muassa syvällisemmältä analyysityöltä ja tapahtumien vaikutusten arvioinnilta. Tietovirtojen, etenkin data- ja informaatiovirtojen osalta, tulisi olla automatisoidumpia.

Toisaalta tietovirrat näyttäytyvät jossain määrin perustuvan myös henkilökohtaisiin suhteisiin, jolloin voi olla, ettei tieto jakaudu ja ole käytössä niillä toiminnan tasoilla, joilla se todellisuudessa kenties kuuluisi olla. Muun muassa Laihonen (2011) sekä Vázquez ym. (2012) ovat maininneet luottamuksen yhtenä keskeisenä tietovirtoihin ja niiden hallintaan liittyvänä osatekijänä, mikä nousi esiin myös tämän tutkimuksen aineistosta. Tietoa usein vaihdetaan sellaisten henkilöiden kanssa, kenet tunnetaan henkilökohtaisesti, jolloin organisaatioiden muodolliset toiminteet tai rakenteet saatetaan sivuuttaa. Havainnoinnin perusteella tunnistettiin tällaisia tilanteita, joissa sovittuja kontaktipisteitä ei noudatettu, minkä seurauksena tietyt kybertilannekuvan kannalta olennaiset yhteydenotot ja tiedot päätyivät organisaatiossa muualle, mikä hankaloitti pintatilanteen seurantaa. Tähän toisaalta liittyy kuitenkin aineistosta esiin nousseena herkkyytenä se, ettei tiedonvaihtoa voida pakottaa vaan tietovirrat lopulta rakentuvat keskinäisen luottamuksen ja koetun hyödyn varaan.

Tiedon henkilöityminen monesti aiheuttaa myös tarpeetonta viivettä, mikä korreloi kykyyn muodostaa oikeanlaista kybertilannekuvaa. Syy tälle voi olla hyvinkin inhimillinen, eli koska toimijoilla ei ole riittävää tuntemusta tai tietämystä kenen kanssa tietoa tulisi vaihtaa, on helpompi ottaa yhteyttä henkilöön, joka tunnetaan jo entuudestaan. Kritiikkiä lieventävänä tekijänä tulee kuitenkin muistaa, että kyberturvallisuus on vielä verrattain tuore osa-alue, jolloin tarvittavien toiminteiden ja toimintamallien luominen ja integroiminen organisaatioissa ja verkostoissa pidempään olleisiin rakenteisiin on monelta osin vasta alkutekijöissään.

Tutkimuksen perusteella tieto on usein myös pirstaloitunut useisiin eri tietojärjestelmiin, mikä hankaloittaa tiedon hyödynnettävyyttä ja siitä muodostuvaa todellista arvopotentiaalia, mikä voi olla joko syy tai seuraus aiempiin esitettyihin haasteisiin nähden. Erityisen mielenkiintoisena ja kenties jatkossa kriittistä tarkastelua vaativana havaintona tutkimuksessa nousi esiin, että vaikka tietoa haluttaisiin jakaa, on se järkevän tiedonvaihtokanavan puuttumisen vuoksi joissain tilanteissa jopa jätetty jakamatta.

Parhaiden käytänteiden tunnistaminen tietovirtojen hallintaan ja niiden integroiminen toimintaan edellyttää toimijoilta kykyä aktiivisesti havainnoida omaa toimintaympäristöään ja siellä muodostuvaa tietoa, ja peilata tätä olemassa oleviin organisatorisiin prosesseihin, toimintamalleihin ja työkaluihin sekä tarvittaessa kehittää niitä. Toimintaympäristön jatkuva luotaaminen muodostaa tilannetietoisuuden perustan (Endsley, 1995). Yhtä lailla toimijoilla tulisi olla kyky jatkuvasti arvioida, mistä tiedosta on hyötyä oman toiminnan ja tehtäväkentän kannalta kybertilannekuvan muodostamisen kontekstissa, mikä näyttäytyy hyvänä käytänteenä osana tietovirtojen hallintaa. Esimerkiksi aineistosta nousi esiin tarve muodostaa organisaatioihin myös sellaisia rooleja ja tehtävän-

kuvia, jotka keskittyvät luomaan tätä tietoperustaista toimintapohjaa mukaan lukien erilaisten tietolähteiden luotaaminen hyödyn ja käytettävyyden näkökulmista. Toisaalta on tunnistettu, että tietotarpeiden määrittely asiantuntijatyössä on todella haastavaa, kun ratkaistavat ongelmat ovat lähtökohdiltaan tuntemattomia (Laihonen ym., 2013), kuten usein myös tässä tutkimuksessa kuvatussa viitekehyksessä. Siten tämä ei pelkästään edellytä organisaatioilta kykyä tunnistaa ja adaptoitua ympäristön muutoksiin, vaan se edellyttää tietynlaista avoimuutta ja joustavuutta myös yksilötasolla, ja siksi aiheen tarkastelussa on tärkeää huomioida myös organisaatioiden ja verkostojen niin sanotun muodollisen infrastruktuurin lisäksi sosiaaliset suhteet ja niiden vaikutus tietovirtojen muodostumiseen ja hallintaan.

Verkostot ja niiden kautta saatavat tiedot näyttäytyvät kritiikistä huolimatta tutkimuksen kannalta yksiselitteisen merkityksellisenä kybertilannekuvan muodostamisen kannalta. Yhteistyön merkitys on suuri, sillä kybertoimintaympäristön laajuus ja levinneisyys ei edes periaatteellisella tasolla mahdollista sitä, että turvallisuutta olisi mahdollista hoitaa yksin (Laari ym., 2019, s. 8). Tutkimuksen perusteella verkostoissa korostuu ennen kaikkea tarve tunnistaa, mitkä tiedot ovat hyödyllisiä tai jopa välttämättömiä muille verkoston jäsenille. Tähän liittyy toisaalta myös tarve tuntea eri tahojen toimivaltuudet ja vastuut riittävän tarkasti, jotta merkityksellinen tieto saadaan todellisuudessa jalkautettua sitä tarvitseville. Havainnointi lisäksi osoitti, ettei oman organisaationkaan sisällä erilaisten roolien ja tiedon saantiin perustuvien toimintaedellytysten tunnistaminen ole itsestäänselvyys vaan se vaatii aktiivista toiminnan näkyväksi tekemistä eli markkinoinnin termein ”brändäämistä”.

Lisäksi keskeinen havainto tutkimusaineiston pohjalta on, ettei tietoa saada useinkaan välitettyä eteenpäin riittävällä nopeudella. Toiminta näyttäytyy yleisesti lähtökohdiltaan jokseenkin enemmän reaktiiviselta, mikä jo itsessään luo tiedonvaihdon aikajänteen kannalta ongelmallisen asetelman arvioitaessa tiedosta muodostuvaa arvopotentiaalia. Jos verkosto ei kykene välittämään tietoa sen sisällä tietyn ajan kuluessa, voi koko sen olemassaolo ja halu toimia yhdessä muuttua epävarmaksi (Kuusisto & Kuusisto, 2006), ja sen vuoksi on tärkeää kiinnittää tietovirtojen muodostumiseen oikea-aikaisesti huomiota. Tutkimustuloksissa esiintyi juuri tämän tyyppistä kritiikkiä siitä, onko kokonaisturvallisuuden viitekehyksessä esitetyt poliittiset ja strategiset tahtotilat todellisuudessa jalkautuneet käytännön tekemiseen, sillä kokemus oli, ettei tietoa kyetä kenties täysimääräisesti jakamaan. Merkittävimmät rajoittavat tekijät tunnistettiin niin lainsäädännön tulkinnasta kuin kulttuurisista syistä, joista tutkimuksessa mainittiin esimerkiksi tiedon mustasukkaisuus ja tiedon yliluokittelun kulttuuria, jolla viitataan erilaisiin tiedon käsittelyluokituksiin ja jakelurajoitteisiin.

Tutkimuksessa nousi esiin myös muita mielenkiintoisia tietovirtojen hallintaa sivuavia näkökulmia, joita yksittäiset organisaatiot tai verkostotkaan eivät pysty itsenäisesti täysimääräisesti ratkaisemaan, mutta jotka laajuutensa vuoksi päätettiin tarkemman käsittelyn osalta jättää tämän työn ulkopuolelle. Kyberturvallisuuden tietojohtaminen on monimutkaisen kokonaisuus, joka

vaatii vielä erilaisten toimintamallien ja rakenteiden yhteensovittamista niin organisaatioissa sisäisesti kuin myös monenvälisesti kansallisella ja kansainväliselläkin tasolla. Toisaalta mitä monimutkaisempia ja erilaisempia toimintamalleja ja rakenteita toimijoilla on, sitä vaikeammaksi erityisvastuualueiden strateginen johtaminen voi muodostua (Jalonen, 2015), ja on siten ymmärrettävää, että muutos ja tarvittavien rakenteiden luominen sekä niiden integroiminen osaksi muuta toimintaa vie yksinkertaisesti vain aikaa.

6.1 Tutkimuksen luotettavuustarkastelu

Tässä alaluvussa pohditaan tutkimuksen luotettavuutta. Koska laadullinen tutkimus keskittyy tyypillisesti ihmisten subjektiivisten kokemusten ja näkemysten tarkasteluun, luo se omat haasteensa tutkimuksen uskottavuus- ja luotettavuuskysymysten tarkastelulle (Puusa & Juuti, 2020, s. 59), eikä sen arviointi perinteisesti käsitteiden ’reliabiliteetti’ ja ’validius’ avulla välttämättä ole kovin mielekästä. Tutkimuksen reliabiliteetti viittaa tulosten toistettavuuteen, mikä soveltuu yleisesti paremmin määrällisen tutkimuksen tarkasteluun kuin laadullisen, ja kun taas validius viittaa siihen, ovatko tutkijan tekemät metodologiset valinnat soveltuvia haluttujen asioiden tutkimiseen tai mittaamiseen. Laadullisen tutkimuksen luotettavuutta voidaan kuitenkin arvioida siinä, miten tutkija on onnistunut avaamaan tutkimuksen etenemistä, perustelemaan tekemiään metodologisia valintoja ja tulkintoja saatujen tulosten pohjalta. (Hirsjärvi, Remes & Sajavaara, 2009, s. 231–232.)

Puusa ja Juuti (2020, s. 175) esittävät laadullisen tutkimuksen luotettavuuspohdinnan tueksi kolme käsitettä: uskottavuus, luotettavuus ja eettisyys. Uskottavuus viittaa tutkimuksen ja sen tulosten todenmukaisuuteen ja siihen, että aineisto on kerätty asianmukaisesti. Luotettavuudella puolestaan viitataan siihen, että tutkija on onnistunut valitsemaan ja käyttämään tutkimusongelman ratkaisemiseen soveltuvia lähestymistapoja ja menetelmiä perustellusti. Tutkimuksen eettisyydellä tarkoitetaan eettisten periaatteiden huomioimista koko tutkimusprosessin läpi ja esimerkiksi sen huomioimista, ettei tutkimus vaaranna sen kohteena olevien ihmisten elämän kulkua tai yksityisyyttä sovitusta poiketen tutkimuksen missään vaiheessa. (Puusa & Juuti, 2020, s. 175.)

Tässä tutkimuksen uskottavuutta ja luotettavuutta lisää se, että tutkimusaineisto kerättiin kahdella eri menetelmällä eli havainnoimalla sekä haastattelemalla. Kun tutkimustehtävän ratkaisemiseen on käytetty useampia aineistoja, voidaan puhua aineistotriangulaatiosta, mikä osaltaan lisää tutkimuksen uskottavuutta. (Hirsjärvi, Remes & Sajavaara, 2009, s. 233). Jos tutkimusaineisto olisi muodostunut ainoastaan havainnoimalla saadusta aineistosta, olisi vaarana ollut se, että käsitys tietovirtojen liittyvistä yleisistä periaatteista olisi muodostunut melko suppeaksi katsannoksi ainoastaan yhden organisaation ja sen kybertilannekuvaa muodostavan toiminteen näkökulmasta. Harjoituksen osalta tiedonvaihtoon mahdollisesti vaikuttivat monet tekijät, joita ei täydellä varmuudella voida pitää todellisuutta kuvaavina, kuten harjoituksen aikapaine

sekä toisaalta kommunikointiin käytettävien työkalujen kankeus. Inhimillisillä tekijöillä, kuten harjoituksen mukaansatempaavuudella, halulla ratkoa tilanteita mahdollisimman pitkälle itse ja selvittää niiden teknisiä juurisyitä, saattoivat vaikuttaa siihen, miten kuvaaviksi harjoitustilanne tietovirtojen muodostumisen ja niiden hallinnan kannalta loppujen lopuksi muodostui. Havainnoinnin avulla onnistuttiin kuitenkin muodostamaan yleiskäsitys tietovirroista ja niiden hallinnasta kybertilannekuvaa tuottavan organisaation käytäntöä kuvaavassa ympäristössä. Havainnoinnin tuloksista löytyi myöhemmin yhteneväisyyksiä haastatteluaineistosta esiin nousseiden tietovirtoihin ja niiden hallintaan liittyvien periaatteiden ja tunnistettavien haasteiden kanssa, mikä toisaalta osaltaan vahvistaa, että havainnointia voidaan kuitenkin pitää jossain määrin uskottavana. Havainnointi lisäsi myös tutkijan esiymmärrystä tutkittavasta aiheesta, mikä antoi hyvän pohjan tutkimuksen pääaineiston keräämisen valmistelemiseen.

Haastatteluiden avulla saatiin laajennettua aiheeseen liittyvää aineistoa ja huomioitua kattavammin erilaisia näkemyksiä, joita tietovirtoihin ja niiden hallintaan kybertilannekuvan muodostamisen kontekstissa liittyy. Tutkimuksen luotettavuutta lisää myös se, että haastateltaville annettiin mahdollisuus täydentää ja kommentoida tuloksia ennen lopullisen tutkielman palauttamista arviointiin. Haastatteluaineiston otannassa on huomioitu eri organisaatioiden ja eri tason toimijoiden näkemyksiä aiheesta. Otantaa voidaan pitää riittävänä, sillä aineistossa alkoi ilmetä toistuvuutta, eikä merkittäviä uusia näkemyksiä enää näyttänyt nousevan esille.

Eettisyysperiaate huomioitiin tutkimuksessa lähtien aihepiirin sensitiivisyyden erityisestä huomioimisesta läpi tutkimusprosessin. Tutkimuksen toteutuksessa aineiston keruun sekä jatkokäsittelyn vaiheissa kiinnitettiin erityistä huomiota tietoturvalliseen toimintatapaan, jotta tutkimuksessa ei vahingossa paljastettaisi salassa pidettävää tai muutoin sensitiivistä tietoa, joita kuitenkin tutkimuksen aihepiiri tietyiltä osin sivuaa. Tutkimuksessa nousi lopulta esiin osin vahvaakin kritiikkiä eri toimijoiden välisestä yhteistoiminnasta, mitä ei katsottu tarpeelliseksi esittää suoraan haastateltavien nimillä tai liitettynä edes organisaatiotasolla tiettyyn toimijaan, joten tutkimuksen tulokset päätettiin esittää anonyymisti. Tutkimuksen avulla pyrittiin tunnistamaan yleisiä tietovirtoihin ja niiden hallintaan liittyviä periaatteita sekä muodostamaan käsitys merkittävimmistä aihepiiriin liittyvistä haasteista, eikä esimerkiksi tekemään tarkkaa toimijakohtaista tietovirta-analyysiä tai niiden välistä vertailua, minkä lisäsi perustetta anonyymille tarkastelulle tässä tutkimuksessa.

Hermeneuttisessa tutkimuksessa tutkijalla on tyypillisesti ennakkokäsitys tutkittavasta aiheesta, mikä ohjaa tutkimuksen etenemistä. Toisaalta myös organisaatio- ja johtamistutkimuksessa usein noudatetaan tutkimustapaa, jossa tutkijan rooli voi olla osallistava, mikä tulee huomioida reflektiivisyytenä omaan tutkimusprosessiin nähden (Puusa & Juuti, 2020, s. 179). Havainnoinnin osalta tutkijan läsnäolo on voinut vaikuttaa ja ohjata sitä, miten tarkkailtava ryhmä toimii. Samoin tutkijan näkemysten vaikutus haastatteluaineiston muodostumiseen on mahdollinen, sillä haastattelut toteutettiin melko keskustelunomaisesti teemahaastatteluina. Tulosten tulkintaan voi lisäksi vaikuttaa

myös se, missä määrin tutkija itse tuntee aihetta jo entuudestaan. Tässä tapauksessa tutkijan subjektiivinen kokemus aiheesta on muodostunut osin työelämän kautta. Esiymmärryksen voidaan kuitenkin ajatella vaikuttaneen tässä myönteisesti tutkijan kykyyn tarkastella aihekokonaisuutta sekä muun muassa haastattelun rakentamisessa ja toteuttamisessa, kun aihepiiri on entuudestaan tuttu.

6.2 Jatkotutkimusaiheet

Tutkimuksen edetessä tunnistettiin muutamia mahdollisia jatkotutkimusaiheita, joiden avulla voitaisiin laajentaa ja syventää näkemyksiä kyberturvallisuuden tietojohtamisesta organisaatio- ja verkostotasolla sekä laajemmin yhteiskunnallisesti poliittisen päätöksenteon tasolla.

Mielenkiintoisena huomiona, tässä tutkimuksessa nousi esiin osa-alueena kyberpuolustus ja siihen liittyen toimivaltuuksien epäselvyys. Nykymuotoinen lainsäädäntö ei esimerkiksi määritä selkeästi kenen vastuulle kyberpuolustus kuuluu. Toimivaltuudet, tiedonsaantioikeudet ja niin edelleen liittyvät olennaisesti kybertilannekuvan muodostamiseen ja sitä kautta myös tietovirtoihin ja niiden hallintaan. Ne tulisivat olla selkeät eikä jättää tulkinnanvaraa, jotta tietoa kyetään jakamaan eri toimijoiden välillä paremmin. Tutkimalla nykymuotoista lainsäädäntöä voitaisiin tunnistaa juridisesti tulkinnanvaraiset lainkohdat, ja sen avulla kehittää kyberturvallisuuden tietojohtamista toimivaltuuksien ja tiedonsaantioikeuksien näkökulmasta.

Tässä tutkimuksessa pyrittiin tunnistamaan parhaat käytänteet tietovirtojen hallintaan kybertilannekuvan muodostamisen kontekstissa ja saatujen havaintojen pohjalta muodostamaan ideaalimalli tietovirtojen hallintaan. Tulokset kuvasivat ilmiötä kuitenkin vain ylätasolla ja yksityiskohtaisempien käytänteiden tunnistaminen edellyttäisi syvällisempää tietovirta-analyysia yhden tai mielellään useamman organisaation näkökulmasta. Organisaatiospesifin tapaustutkimuksen toteuttaminen voi kuitenkin olla haastavaa ja aikaa vievää aihealueen kompleksisuuden vuoksi, eikä tutkimusaineisto myöskään todennäköisesti ole julkisesti käsiteltävissä. Mahdollisia lähestymistapoja tapaustutkimukselle voisi olla systeemiteoreettinen tapa, jonka avulla muodostettaisiin käsitys tietovirtoihin ja niiden hallintaan liittyvästä muodollisesta infrastruktuurista. Toisena lähestymistapana voisi olla puhtaasti ihmistieteistä haettava lähestymistapa, sillä muodollisesta infrastruktuurista huolimatta tieto ja sen merkitys on sidottu viime kädessä yksilön ajatuksiin, tunteisiin ja toimintaan (Choo, 1998). Tällä pyrittäisiin tunnistamaan erityisesti inhimillisiä tekijöitä yksityiskohtaisemmin, jotka vaikuttavat tietovirtoihin ja niiden hallintaan kybertilannekuvan muodostamisen viitekehyksessä, sekä kehittämään kyberturvallisuuden tietojohtamista siitä käsin.

7 YHTEENVETO

Tässä pääluvussa käsitellään tutkielman keskeisimpiä osa-alueita ja tiivistetään tutkimuksen tulokset. Tutkielma muodostuu teoreettisesta osiosta (luvut 1–4) sekä empiirisestä osiosta (luvut 5–7).

Tutkimuksen tavoitteena oli pyrkiä tunnistamaan parhaat käytänteet tietovirtojen hallintaan kybertilannekuvan muodostamisen kontekstissa. Tutkimuksen pääkysymyksenä oli *"Onko tietovirroista ja niiden hallinnasta esitettävissä jonkinlaista ideaalimallia kybertilannekuvan muodostamisen kontekstissa?"* sekä tarkentavina alakysymyksinä *"Millaisia tietovirtojen muodostumiseen ja niiden hallintaan liittyviä yleisiä periaatteita on tunnistettavissa kybertilannekuvan muodostamisen kontekstissa?"* ja *"Mitä haasteita tietovirtojen muodostumiseen ja niiden hallintaan liittyy?"*. Tutkimusasetelmaa muotoiltaessa kybertilannekuvan muodostumisen kontekstissa tehtyä aiempaa, selvästi tietovirtoihin liittyvää tutkimusta ei tunnistettu, minkä vuoksi tutkimuksen lähestymistavaksi valikoitui kvalitatiivinen tutkimustapa. Tutkittavasta aihealueesta löydettiin piirteitä sekä etnografisesta että tapaustutkimuksesta, joten tutkimus päätettiin toteuttaa monimenetelmäisenä kvalitatiivisena tutkimuksena.

Kirjallisuuskatsauksessa avattiin aluksi yleisestä tietojohtamiseen liittyvää teoriaa sekä tarkemmin erilaisia organisaation tietoon ja tiedon hyödyntämiseen liittyviä prosesseja, minkä avulla pyrittiin muodostamaan kokonaisvaltainen käsitys tiedon merkityksestä organisaatioiden toiminnassa. Kirjallisuuskatsauksen toisessa osiossa lisäksi käsiteltiin kybertoimintaympäristön tunnuspiirteitä ja ominaisuuksia, jotka heijastuvat tietovirtoihin ja niiden hallintaan kybertilannekuvan muodostamisen kontekstissa. Kirjallisuuskatsauksen laajuus ja siinä esiin tuodut näkökulmat kuvastavat ennen kaikkea sitä, miten moniulotteisesta aihekokonaisuudesta tutkimuksessa loppujen lopuksi oli kyse.

Tutkimusaineisto kerättiin havainnoimalla ja haastattelemalla. Havainnointi toteutettiin osana erästä kotimaista kyberturvallisuusharjoitusta, johon osallistui useita toimijoita eri organisaatioista. Havainnointi keskittyi ainoastaan yhden organisaation kybertilannekuvatoiminteen tarkkailuun. Havainnoinnin avulla muodostettiin käsitys tietovirroista ja niiden hallinnasta yleisellä tasolla käytäntöä kuvaavassa ympäristössä. Harjoitustoiminnan yhteydessä

toteutettu havainnointi ei kuitenkaan täysin kuvannut oikean maailman tilanteita muun muassa käytettävissä olevien teknisten järjestelmien osalta, mikä voinee vaikuttaa siihen, kuinka yleistettävinä tämän tutkimuksen tuloksia havainnoin osalta voidaan pitää. Tutkimuksen pääaineisto muodostui yhteensä kahdeksasta teemahaastattelusta, joista haettiin havainnoinnin tueksi yksilöiden kokemusperäistä, asioita ja toimintatapoja selittävää tietoa tutkittavasta aiheesta. Tutkimustulosten analysointi toteutettiin teoriaohjaavan sisällönanalyysin menetelmällä. Haastatteluaineiston analyysissä sovellettiin Riegen (2005) ja Vuoren ym. (2019) esittämiä kategorioita tiedon jakamiseen liittyvistä tekijöistä esteiden näkökulmasta (taulukko 2), joita olivat mukaillusti organisatoriset, teknologiset, verkosto- sekä inhimilliset ja/tai yksilöön, tietoon ja aikaulottuvuuteen liittyvät tekijät. Kokonaisuudessaan saadut tutkimustulokset kuvasivat aihepiiriä hyvin ylätasolla eikä kovinkaan syväluotaavaa tietovirta-analyysiä ollut mahdollista tehdä kummankaan aineistomuodon perusteella.

Tutkimustehtävän kannalta keskeisenä tutkimuksessa näyttäytyi kyky tunnistaa, kenelle kybertilannekuvaa tehdään ja millaisia tietotarpeita heillä on. Se millaisia tietovirtoja ja niiden hallinnan mekanismeja nämä tietotarpeet lopulta muodostavat vaihtelevat eri toimijoiden välillä, eikä niitä voi täysin yleistää tai verrata keskenään. Osittain tästä syystä tutkimuksen pääkysymykseen tietovirtojen hallinnan ideaalimallista ei nähty mahdollisena vastata.

Sen sijaan tutkimuksessa kuitenkin tunnistettiin laajasti periaatteita, joita tietovirtoihin ja niiden hallintaan kybertilannekuvan muodostamisen kontekstissa liittyy. Tämä ei pelkästään edellytä tietolähteiden tunnistamista, mutta myös erilaisten osatekijöiden, kuten teknisten valmiuksien, toimintamallien ja prosessien luomista, jotta merkityksellinen tieto on saatavilla ja hyödynnettävissä tarkoituksenmukaisesti. Tietovirtojen hallintaan yhdistettiin myös kyky tunnistaa, milloin olemassa olevat toimintamallit, säännöt ja rutiinit eivät toimi vaan on tarpeen ottaa käyttöön esimerkiksi kokonaan uusia tietolähteitä, muuttaa toiminnan painopistealueita tai toimintatapoja, jotta kyetään muodostamaan asiakkaan tietotarpeisiin paremmin vastaavaa tilannekuvaa. Teknologioiden kehittäminen näyttäytyy kenties helppona ratkaisuna. Tutkimustuloksissa kuitenkin nousi esiin yhtenä mahdollisuutena, että organisaatioihin luotaisiin rooleja, joiden vastuulle tietovirtojen muodostumisen ja niiden hallinnan mahdollistavien mekanismien jatkuva luotaaminen ja kehittäminen kuuluu.

Lisäksi tutkimuksessa tunnistettiin monia haasteita, jotka liittyvät kyberturvallisuuden tietojohtamiseen ei pelkästään organisaatiotasolla vaan myös verkostoissa ja laajemmin yhteiskunnallisen viitekehyksen tasolla. Merkittävimpinä haasteina esiin nousivat muun muassa tiedon pirstaloituminen useisiin eri tietojärjestelmiin, henkilöityminen sekä lainsäädännön ja toimintavaltuuksien tulkintaan liittyvät tekijät. Toisaalta esimerkiksi se, millaisia tiedonvaihtokanavia toimijoilla on käytössään vaikuttaa siihen, miten hyvin merkityksellistä tietoa on mahdollista saada käyttöönsä. Tiedosta muodostuva arvopotentiaali on siten pitkälti toimijoiden omasta aktiivisuudesta kiinni, millaiseksi he toimintaedellytyksensä rakentavat kyberturvallisuuden tietojohtamisen näkökulmasta.

Tutkimusta voidaan pitää merkittävänä, sillä vastaavan tyyppistä tutkimusta ei ole kotimaassa aiemmin toteutettu. Tutkimus antaa yleisellä tasolla laajahkon kuvan siitä, millaisiin asioihin organisaatioiden tulee tietovirtojen muodostumisessa ja niiden hallinnassa kybertilannekuvan muodostamisen kontekstissa kiinnittää huomiota. Kyberturvallisuuden tietojohtaminen on kuitenkin monimutkainen kokonaisuus, joka vaatii vielä laajasti erilaisten toimintamallien ja rakenteiden yhteensovittamista toiminnan eri tasoilla.

LÄHTEET

Ahlavuo, M., Hyyppä, H. & Haggren, H. (2011). Tietovirrat akateemisessa tutkimusympäristössä. *The Photogrammetric Journal of Finland, Vol 22, No. 3, 2011.*

Choo, C. W. (1998). *The Knowing Organisation. How Organisations Use Information to Construct Meaning, Create Knowledge and Make Decisions.* New York: Oxford University Press.

Choo, C. W. (2001). The knowing organization as learning organization. *Education & Training*, 2001:43, 4/5, s. 197-205.

Choo, C. W. (2006). *The Knowing Organisation. How Organisations Use Information to Construct Meaning, Create Knowledge and Make Decisions.* (2. painos). New York: Oxford University Press.

Connolly, J., Davidson, M. & Schmidt, C. (2014). *The Trusted Automated eXchange of Indicator Information (TAXII).* The MITRE Corporation.

Cresswell, J. W. & Poth, C. N. (2018). *Qualitative Inquiry and Reseach Design. Choosing Among Five Approaches.* (4. painos). SAGE Publications.

Dandurand, L. & Serrano, O. (2013). Towards Improved Cyber Security Information Sharing. *2013 5th International Conference on Cyber Conflict.*

Davenport, T. H. & Prusak, L. (1998). *Working Knowledge: How Organisations Manage What They Know.* Boston: Harvard Business School Press.

Eldardiry, O. M. & Caldwell, B. S. (2015). Improving Information and Task Coordination in Cyber Security Operation Centers. *Proceedings of the 2015 Industrial and Systems Engineering Research Conference.*

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors Journal, 37(1), 32-64.*

EU 2016/1148. *Directive of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Haettu 21.9.2022 osoitteesta https://eur-lex.europa.eu/eli/dir/2016/1148/oj

European Commission. (2022, 7. elokuuta). *The Cybersecurity Strategy*. Haettu 21.9.2022 osoitteesta https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Evesti, A., Kantrén, T. & Frantti, T. (2017). Cybersecurity situational awareness taxonomy. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 1-8.*

Farnese, M. L., Barbieri, B., Chirumbolo, A. & Patriotta, G. (2019). Managing Knowledge in Organizations: A Nonaka's SECI Model Operationalization. *Frontier in Psychology, 10:2730.*

FIRST (2015-2022). *Traffic Light Protocol (TLP). FIRST Standards Definition and Usage Guidance – version 2.0.* Haettu 6.8.2022 osoitteesta https://www.first.org/tlp/docs/tlp-a4.pdf

Gatlan, S. (2022, 4. elokuuta). *New Traffic Light Protocol standard released after five years.* Haettu 18.9. osoitteesta https://www.bleepingcomputer.com/news/security/new-traffic-light-protocol-standard-released-after-five-years/

Goodwin, C. & Nicholas, J. P. (2015). *A framework for cybersecurity information sharing and risk reduction.* Haettu 14.11.2021 osoitteesta https://www.microsoft.com/en-us/download/confirmation.aspx?id=45516

Grupta, A. & Govindarajan, V. (1991) Knowledge Flows and the Structure of control within multinational corporations. *Academy of Management Review, Vol 16, No 4, 768-792.*

Grupta, A. & Govindarajan, V. (2000) Knowledge flows within multinational corporations. *Stategic management journal, 21 (4), 473-496.*

Hackathorn, R. (2004). The BI Watch: Real-Time to Real-Value. *DM Review, 14 (1),* 24-29.

Hautamäki, J. & Kokkonen, T. (2020). Model for cyber security information sharing in healthcare sector. *Proceedings of the 2nd International Conference on Electrical, Communication and Computer Engineering* (ICECCE).

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita.* (15. uud. painos). Helsinki: Tammi.

Horsmanheimo, S., Kokkoniemi-Tarkkanen, H., Kuusela, P., Tuomimäki, L., Puuska, S. & Vankka, J. (2017). *Kriittisen infrastruktuurin tilannetietoisuus.* Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 19/2017.

Huotari, M.-L., Hurme, P. & Valkonen, T. (2005). *Viestinnästä tietoon. Tiedon luominen työyhteisössä.* (1. painos). Helsinki. WSOY.

Jalonen, H. (2015). *Tiedolla johtamisen näyttämö ja kulissit.* Teoksessa: Tiedolla johtaminen hallinnossa: teoriaa ja käytäntöjä, s. 40-68. (Toim. Virtanen, P., Stenvall, J. & Rannisto, P.-H.). Tampereen yliopistopaino Oy.

Jyväskylän yliopisto (2015a). *Hermeneutiikka.* Haettu 3.3.2022 osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tieteenfilosofiset-suuntaukset/hermeneutiikka

Jyväskylän yliopisto (2015b). *Konstruktivismi.* Haettu 3.3.2022 osoitteesta https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tieteenfilosofiset-suuntaukset/konstruktivismi

King, W. R. (2006). Knowledge transfer. In D. G. Schwartz (Ed.), *Encyclopedia of knowledge management* (pp.538–543). Hershey, PA: Idea Group Reference.

Kokkonen, T., Hautamäki, J., Siltanen, J. & Hämäläinen, T. (2016). Model for Sharing the Information of Cyber Security Situation Awareness between Organizations. *23rd International Conference on Telecommunications (ICT).*

Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A. & Ahn, G.-J. (2019). Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. *The 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS).*

Kuusisto, T. & Kuusisto, R. (2006). Verkostopuolustuksen johtaminen - tietovirtojen näkökulma itsesynkronoitumiseen. *Tiede ja Ase, Nro 64.*

Kuusisto, R. (2005). *Tilannekuvasta täsmäjohtamiseen. Johtamisen tietovirrat kriisin hallinnan verkostoissa*. Liikenne- ja viestintäministeriön julkaisuja, 81/2005.

Kuusisto, T., Kuusisto, R. & Wolfgang, R. (2015). Situation Understanding for Operational art in Cyber Operations. *The 14th European Conference on Cyber Warfare and Security ECCWS-2015.*

Kyberturvallisuuskeskus. (2022, 24. elokuuta). Yhteistyöryhmien tiedonvaihtokäytäntöjä. Haettu 3.9.2022 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/yhteistyoryhmien-tiedonvaihtokaytantoja

L 906/2019. Laki julkisen hallinnon tiedonhallinnasta. Haettu 19.9.2022 osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190906

L 21.5.1999/621. Laki viranomaisten toiminnan julkisuudesta. Haettu 19.9.2022 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Laari, T., Flyktman, J., Härmä, K., Timonen, J. & Tuovinen, J. (2019). #kyberpuolustus - Kyberkäsikirja Puolustusvoimien henkilöstölle.

Maanpuolustuskorkeakoulu, Sotataidon laitos. Julkaisusarja 3: Työpapereita nro 12.

Laihonen, H. (2011). *Tietovirrat palvelujärjestelmän tuottavuusajureina.* Teoksessa: Arvoverkkoa kokemassa – saaliina tuottavuutta ja innovaatiota (1. painos), s. 78-112. Suomen kuntaliitto. Helsinki: Kuntatalon paino.

Laihonen, H., Hannula, M., Helander, N., Ilvonen, I., Jussila, J., Kukko, M., Kärkkäinen, H., Lönnqvist, A., Myllärniemi, J., Pekkola, S., Virtanen, P., Vuori, V. & Yliniemi, T. (2013). *Tietojohtaminen.* Tampereen teknillinen yliopisto, Tiedonhallinnan ja logistiikan laitos.

Lehto, M. (2016). Theoretical examination of the cyber warfare environment. *Proceedings of the 11th International Conference on Cyber Warfare and Security ICCWS*, 223-230.

Lehto, M. (2019). Kybermaailman ilmiöitä ja määrittelyjä. Jyväskylän yliopisto, Informaatioteknologian tiedekunta.

Lehto, M. (2022). *Cyber-Attacks Against Critical Infrastructure*. Teoksessa: Cyber Security. Computational Methods in Applied Sciences, vol 56. (Toim. Lehto, M. & Neittaanmäki, P.). Springer. Haettu 18.2.2023 osoitteesta https://doi.org/10.1007/978-3-030-91293-2_1

Lehto, M. & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal, 30(3),* 139-148.

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. (2018). *Kyberturvallisuuden strateginen johtaminen Suomessa.* Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 28/2018.

Magnusson, J. & Nilsson, A. (2003). To facilitate or intervene - A study of knowledge management practice in SME networks. *Journal of Knowledge Management Practice.*

MISP Threat Sharing (2022, 18. elokuuta). *MISP taxonomies and classification as machine tags.* Haettu 18.9.2022 osoitteesta https://www.misp-project.org/taxonomies.html#_pap

Nissen, M. E. (2002). An Extended Model of Knowledge-Flow Dynamics. *Communications of the Association for Information Systems, Vol 8, 251-266.*

Nonaka, I. & Konno, N. (1998). The Concept of ”Ba”: Building a Foundation for Knowledge Creation. *California Management Review, vol 40. No 3, Spring 1998.*

Nonaka, I. & Takeuchi, H. (1995). *The Knowledge Creating Company. How Japanese Companies Create the Dynamics of Innovation.* New York: Oxford University Press.

Norri-Sederholm, T., Joensuu, M. & Huhtinen, A-M. (2017). Ensuring Information Flow and the Situation Picture in Public Safety Organisations´ Situation Centres. *Proceedings of 16th European Conference on Cyber Warfare and Security ECCWS, 267-273.*

Parish, B. R. & Madahar, B. K. (2016). *Understanding Cyberspace Through Cyber Situational Awareness.* Haettu 21.9.2022 osoitteesta https://www.semanticscholar.org/paper/Understanding-Cyberspace-Through-Cyber-Situational-Madahar/bd92f82ed048eed23107176a8740fa713e117d3b#citing-papers

Polanyi, M. (1966) *The Tacit Dimension*. London: Routledge & Kegan Paul.

Pulli, K.-M. (2018). *Tiedolla johtamisen kehittäminen: tapaustutkimus* (Pro gradu -tutkielma). Jyväskylän yliopisto. Haettu osoitteesta http://urn.fi/URN:NBN:fi:jyu-201802121471

Puolustusministeriö. (2019). Kyberpuolustuksen kehittämisen strategiset linjaukset. Haettu 21.9.2022 osoitteesta http://urn.fi/URN:ISBN:978-951-663-069-7

Puusa, A. & Juuti, P. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Tallinna: Gaudeamus Oy.

Pöyhönen, J., Nuojua, V., Lehto, M. & Rajamäki, J. (2019). Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations. *Information & Security, 43 (2),* 236-256.

Riege, A. (2005). Three-dozen knowledge-sharing barriers managers must consider. *Journal of Knowledge Management, 9 (3),* 18-35.

Rizov, V. (2018). Information Sharing for Cyber Threats. *Information & Security: An International Journal, 39(1):* 43-50.

Sanastokeskus. (2017). Kokonaisturvallisuuden sanasto. Helsinki. Haettu osoitteesta http://www.tsk.fi/tiedostot/pdf/Kokonaisturvallisuuden_sanasto_2.pdf

Sanastokeskus. (2018). Kyberturvallisuuden sanasto. Helsinki. Haettu 21.9.2022 osoitteesta http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Saunders, M. N. K., Lewis, P. & Thornhill, A. (2019). *Research Methods for Business Students.* (8. painos). Harlow: Pearson Education Limited.

Skopik, F., Setanni, G. & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security, 60,* 154-176.

Sydänmaanlakka, P. (2012). *Älykäs organisaatio.* (8. painos). Vantaa: Talentum Media Oy.

Tounsi, W. & Rais, H. (2017). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security, 72,* 212-233.

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

Valtioneuvoston periaatepäätös. (2013, 24. tammikuuta). Suomen kyberturvallisuusstrategia. Haettu 17.2.2023 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

Valtioneuvoston periaatepäätös. (2019, 3. lokakuuta). Suomen kyberturvallisuusstrategia 2019. Haettu 17.2.2023 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Valtioneuvoston periaatepäätös. (2017, 2. marraskuuta). Yhteiskunnan turvallisuusstrategia. Haettu 21.9.2022 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Vázquez, D. F., Acosta, O. P., Spirito, C., Brown, S. & Reid, E. (2012). Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships. *4th International Conference on Cyber Conflict.*

Vertainen, V., Suni, E., Vatanen, M., Hautamäki, J., Laava, T. & Piispanen, J. (2021). *Kyberhäiriöiden hallinta. Käsikirja terveydenhuollon toimijoille.* Jyväskylän ammattikorkeakoulu, IT-insituutti, JYVSECTEC.

Virta, S. (2011). Turvallisuuden tutkimus : tieteenalat ja monitieteisyyden lähtökohtia. *Tiede ja Ase : Suomen Sotatieteellisen seuran vuosijulkaisu, 69, 112-126.*

Vuori, V., Helander, N. & Mäenpää. S. (2019). Network level knowledge sharing: Leveraging Riege's model of knowledge barriers. *Knowledge Management Research & Practice, 17(3), 253-263.*

Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center.* The MITRE Corporation.