Tuomas Herranen

KEVYTTÄ KESKUSTELUA VAI TIIVISTÄ TIETOJEN VAIHTOA?

TIETOVERKKORIKOLLISUUDEN TILANNETIETOISUUDEN JAKAMINEN LUOTTAMUSVERKOSTOSSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2018

TIIVISTELMÄ

Herranen, Tuomas
Kevyttä keskustelua vai tiivistä tietojen vaihtoa? Tietoverkkorikollisuuden tilannetietoisuuden jakaminen luottamusverkostossa
Jyväskylä: Jyväskylän yliopisto, 2018, 76 s.
Tietojenkäsittelytiede, pro gradu - tutkielma
Ohjaaja(t): Lehto, Martti

Räjähdysmäisesti lisääntyneiden kyberrikosten taloudellisten vaikutusten arvioidaan olevan merkittäviä, mutta silti ilmoituskynnys rikoksista on korkea. Viranomaiset pystyvät puuttumaan tapauksiin vain rajallisesti, koska suuri osa teoista ei näy rikostilastoissa. Tästä syystä julkisen ja yksityisen sektorin yhteistyö onkin elintärkeää kyberrikollisuuden torjumisessa. Yksi rakenne yhteistyöhön on luotettu foorumi, jossa elinkeinoelämän harjoittajat ja viranomaiset voivat kokoontua keskustelemaan asioista epävirallisesti. Tässä tutkimuksessa tunnistettiin seikat, jotka vaikuttavat tietoverkkorikollisuuden tilannetietoisuuden jakamiseen tietoturvayritysten ja viranomaisten välisessä luottamusverkostossa. Puolistrukturoitujen asiantuntijahaastatteluiden avulla selvitettiin, millaista tietojenvaihtoa luottamusverkoston toimijat toivovat sekä mitä haasteita he tunnistavat tietojen jakamiseen liittyen. Pehmeää systeemimetodologian avulla vastauksista muodostettiin määrämuotoinen kehitysprosessi siten, että luottamusverkoston toiminnan kehittämiseen voidaan ryhtyä järjestelmällisesti. Tutkimustulosten perusteella tietoverkkorikollisuuden tilannetietoisuuden jakamisen tulisi palvella niin viranomaisten tarvetta kehittää konkreettista tilannetietoisuusnäkymää tapahtuviin rikoksiin, kuin myös lisätä yritysten edustajien ymmärrystä tietoverkkorikoksista sekä niiden taustalla vaikuttavista ilmiöistä. Jaettavan tiedon tulisi olla sellaista, minkä tietäminen olisi tarpeellista kaikille luottamusverkoston toimijoille ja sen avulla saavutettavan ymmärryksen tulisi mahdollistaa tilannetietoisuuden käyttäminen päätöksenteon apuna. Edellytyksenä tietoisuuden jakamiselle koettiin, että yhteistyön tulisi olla salassapitovelvollisuuksien puitteissa mahdollisimman avointa, vastavuoroista, noudattaa ryhmässä vallitsevia normeja ja perustua muuhun kuin pelkkiin fyysisiin tapaamisiin. Tietoisuuden jakamista edesauttaisi, mikäli luottamusverkostolla olisi yhteiset tavoitteet, taloudellisia kannustimia tehdä yhteistyötä sekä tehokkaat kommunikointikanavat tai jaettu tilannetietoisuusnäkymä. Tilannetietoisuuden jakamista puolestaan haittaisivat vapaamatkustajailmiö, luottamuksen puute ryhmän jäsenten kesken sekä saavutetun tilannetietoisuuden tulkintaan käytettävän yhtenevän sisäisen mallin puuttuminen. Kyberturvallisuuskeskus koettiin luontevimmaksi tahoksi koordinoimaan tällaista yhteistyötä, koska verkoston toimijoilla on jo ennestään toimiviksi koetut suhteet keskuksen kanssa.

Asiasanat: kyberrikollisuus, tietoverkkorikollisuus, tilannetietoisuus, tiedon jakaminen, luottamusverkosto

ABSTRACT

Herranen, Tuomas
Casual Conversations or Intensive Information Sharing? Sharing Situational Awareness on Network Crime within Organizational Trust Relationships
Jyväskylä: University of Jyväskylä, 2018, 76 p.
Computer Science, Master's Thesis
Supervisor(s): Lehto, Martti

The cost of cybercrime to societies has risen as cybercrime activity has grown explosively. Despite significant economic impacts, the police-recorded cybercrime rates do not represent a sound basis for statistics. Often the activity is not reported to the police altogether resulting in an inadequate situational awareness and limited capability to act against the criminals. Thus, public-private partnerships and information sharing is vital in the fight against cybercrime. One potential structure to facilitate this sharing is a trusted forum or platform where private sector entities and authorities can meet face-to-face at regular intervals and hold informal, un-attributable discussions. This study identified the issues that affect information sharing on network crime in a trusted forum consisting of Finnish information security companies and authorities. Members of the forum were given an opportunity to express their wishes for the cooperation in semi-structured interviews as well as to call out identified challenges in the information sharing. Based on the interview results, a formal development process for the cooperation was formed by leveraging soft system methodology. The study results show that the information sharing should contribute to building tangible situational awareness of network crime for the authorities but also serve private sector members by revealing potential actors behind the activity and shedding light on their attack patterns. The shared information should serve all members of the forum while the gained situational awareness should enable better dynamic decision making. A precondition for any kind of information sharing is that the sharing complies with group norms, is reciprocal and as overt as possible considering the non-disclosure obligations of the members. In addition, the sharing would benefit from jointly defined goals and from economic incentives to participate. To gain the most out of cooperation, sharing should not be based only on face-to-face meetings. Effective communication methods or a shared situational awareness display would promote the cooperation. The cooperation would suffer if members attempt to free ride in the forum, do not trust each other or lack shared mental models to interpret the results of the shared situational awareness. The National Cyber Security Centre Finland (NCSC-FI) at the Finnish Communications Regulatory Authority was seen as the suitable owner and coordinator for this information sharing since the members have working relations with the centre.

Keywords: Cyber Crime, Network Crime, Situational Awareness, Information Sharing, Organizational Trust Relationships

KUVIOT

TAULUKOT

SISÄLLYS

1 Johdanto

Tieto- ja viestintäteknologian kehittyminen ja yhteiskuntien verkottuminen on avannut lukuisia uusia mahdollisuuksia kaupankäynnille, palveluiden välittämiselle sekä ihmisten väliseen kanssakäymiseen. Monet sellaiset transaktiot, jotka olivat aikaisemmin sidottuja tiettyyn maantieteelliseen paikkaan tai tiettyyn aikaan, on nykyään mahdollista toteuttaa vuorokauden ympäri lähes mistä päin maailmaa tahansa. Tämä on kuitenkin avannut uusia tilaisuuksia myös rikollisille, jotka ovat nopeasti oppineet hyödyntämään verkottuneen yhteiskunnan tarjoamia uusia toimintamahdollisuuksia. Nopeasti kehittyvä ja muotoaan muuttava kyberrikollisuus asettaa valtavia paineita niin rikollisia tietoverkoissa jäljittäville viranomaisille kuin yhteiskunnan muille toimijoille, jotka yrittävät parhaansa mukaan suojautua erilaisia rikollisia hyökkäyksiä vastaan.

Kyberrikollisuus on ylittänyt joidenkin arvioiden mukaan tietyissä EU-maissa perinteisen rikollisuuden määrän tapahtuneiden rikosten osalta (National Crime Agency, 2016) ja ilmiön taloudellisten vaikutusten arvioidaan olevan merkittäviä (Europol, 2105; Europol, 2016). Kyberrikollisuuden todellisten vaikutusten arvioiminen on kuitenkin haastavaa rikosten korkean ilmoituskynnyksen takia. Yhdistyneiden kansakuntien huumeiden ja rikollisuuden torjunnasta vastaavan toimiston (UNODC) mukaan viranomaisten kyky puuttua muuhun kuin ilmoitettuun kyberrikollisuuteen on hyvin rajallinen ja valtaosan kyberrikollisuudesta arvioidaan siksi jäävän piilorikollisuudeksi (UNODC, 2013). Ilmoitusten vähäisyyden on arvioitu johtuvan muun muassa tietoisuuden ja oikeiden raportointikanavien puutteesta, uhrin häpeän tunteesta tai tarpeesta varjella yksilön tai yhteisön mainetta sekä yleisestä epäluottamuksesta poliisiviranomaisten kyberrikosten selvittämiskykyä kohtaan. Rikosilmoitusten kautta viranomaisten tietoon tulleiden kyberrikosten arvioidaankin näin ollen muodostavan kansainvälisesti vain häviävän pienen osan todellisista tapahtumamääristä (UNODC, 2103).

Pelkonen ym. (2016) ovat tekemänsä kyselytutkimuksen perusteella esittäneet, että uhrien syyllistäminen ja epäonnistumisen pelko haittaavat kyberhyökkäyksistä ja tietoturvaloukkauksista kertomista myös Suomessa,

jolloin suuri osa rikoksen tunnusmerkistön täyttävistä teoista pysyy viranomaisten näkymättömissä. Tässä tutkimuksessa selvitetään keinoja kehittää kansallisesti kyberrikollisuuteen liittyvää tilannetietoisuutta tiivistämällä viranomaisten ja tietoturvayritysten välistä tietojenvaihtoa. UNODC:n (2013) mukaan julkisen ja yksityisen sektorin yhteistyö on elintärkeää kyberrikollisuuden torjumisessa, sillä kyberrikoksiin liittyvä todistusaineisto on lähes poikkeuksetta elektronisessa muodossa ja tarvittavan näytön kokoaminen edellyttää perinteisten esitutkintakeinojen lisäksi erialisten sähköisten tallennusvälineiden tutkimista ja reaaliaikaisten tietovirtojen analysointia. Rikosten tutkiminen vaatii myös oikea-aikaista reagointia sekä pitkälle erikoistuneita tutkintamenetelmiä elektronisen todistusaineiston muuttuvan luonteen takia. Uusia kyberrikollisuuden tekomuotoja paljastuu jatkuvasti, mikä asettaa jatkuvia paineita niin poliisiorganisaatioiden kuin yritystenkin osaamisen kehittämiselle. Lisäksi merkittävään osaan kyberrikollisuudesta liittyy kansainvälinen ulottuvuus, mikä tuo mukanaan ylikansallisten tutkimusten suorittamiseen, valtioiden itsemääräämisoikeuteen, lainsäädäntöön ja kansainväliseen oikeuteen liittyviä haasteita (UNODC, 2013).

De Muynck & Portesi (2015) mukaan yleisin rakenne verkkoihin ja tietoturvaan liittyvien tietojen vaihtamiseen on luotettu foorumi, jossa elinkeinoelämän harjoittajat ja viranomaiset voivat kokoontua säännöllisesti keskustelemaan asioista epävirallisesti. Tässä tutkimuksessa foorumin muodostaa luottamusverkosto, joka koostuu viranomaisista sekä tietoturvayritysten edustajista.

Tutkimusaihe perustuu valtioneuvoston kanslian ja poliisiammattikorkeakoulun tutkijoiden kehitysehdotukseen julkaisussa ”Tietoverkkorikollisuuden tilannekuva” (Leppänen, Lindeborg & Saarimäki, 2016), jossa esitetään, että tilannetietoisuutta tietoverkkorikollisuuden tilasta voisi rakentaa osallistamalla tietoturvayritykset tilannetietoisuuden tuottamiseen suljetun luottamusverkoston kesken. Tutkimuksen tarkoituksena on tarkastella, miten tietoverkkorikollisuuteen liittyvää tilannetietoisuutta kannattaisi muodostaa ja miten sen jakaminen kannattaisi toteuttaa tietoturvayritysten ja viranomaisten kesken tutkimuksen kohteena olevassa luottamusverkostossa. Tutkimusaihe syntyi keväällä 2016 tutkijan ja Keskusrikospoliisin kyberrikostorjuntakeskuksen päällikön keskusteluiden pohjalta. Tutkimusaiheen määrittelyyn ja rajaamiseen on osallistunut niin Keskusrikospoliisin kyberrikostorjuntakeskuksen kuin Viestintäviraston kyberturvallisuuskeskuksen henkilöstöä. Tutkimus keskittyy ainoastaan sähköisissä tietoverkoissa esiintyviin rikoksiin, eli tietoverkkorikoksiin, eikä ota kantaa muihin kyberrikollisuuden osa-alueisiin.

Kansainvälinen kybertilannetietoisuuteen liittyvä tutkimus on pääasiassa hyvin teoreettista ja empiiriset tutkimustulokset loistavat poissaolollaan. Lisäksi kybertilannetietoisuuden jakamiseen liittyvä tutkimus on jäänyt akateemisissa piireissä vähälle huomiolle (Franke & Brynielsson, 2014). Tietoturvayritysten ja viranomaisten yhteistyön tiivistäminen mahdollistaa ymmärryksen lisäämisen piilorikollisuudeksi jäävästä ilmiöstä ja rikastaa kansallista

kybertilannetietoisuutta. Parhaassa tapauksessa kehittyvän tilannetietoisuuden pohjalta on mahdollista tunnistaa kyberilmiöitä, jotka uhkaavat Suomalaista yrityskenttää sekä muodostaa ennakointi- ja reagointikyky niiden torjumiseksi.

Tutkimus rakentuu siten, että luvussa 2 analysoidaan kirjallisuuskatsauksen perusteella kyberrikollisuutta ilmiönä sekä luodaan määritelmä tietoverkkorikollisuudelle. Lisäksi luvussa tarkastellaan aikaisemman tutkimuksen pohjalta tilannetietoisuuden käsitettä sekä sen muodostamiseen ja jakamiseen liittyviä seikkoja. Lopuksi näiden perusteella rakennetaan malli, joka kuvaa, miten tietoverkkorikollisuuden tilannetietoisuus muodostuu luottamusverkostossa. Työn tutkimusasetelma sekä metodologia esitellään luvussa 3 ja tutkimuksen empiirisen osion tulokset luvussa 4. Tutkimuksen empiiristä osaa varten haastateltiin tietoturvayritysten, keskusrikospoliisin kyberrikostorjuntakeskuksen sekä viestintäviraston kyberturvallisuuskeskuksen henkilöstöä. Tutkimuksen tarkoituksena on selvittää millaista tietojenvaihtoa luottamusverkoston toimijat toivovat sekä, mitä haasteita he tunnistavat sekä mitkä asiat pitää ratkaista ennen kuin tietoja voidaan ryhtyä jakamaan tehokkaasti. Luvussa 5 esitellään tutkimustulokset sekä konkreettiset kehitystoimenpiteet, joita suositellaan tietoturvayritysten ja viranomaisten yhteistyön tiivistämiseksi. Pohdinta on esitetty luvussa 6.

2 Tietoverkkorikollisuuden tilannetietoisuuden jakaminen

Tässä luvussa määritellään tutkimuksen teoreettinen viitekehys ja kuvataan tutkimuksen keskeiset käsitteet. Luvussa avataan tutkimusaiheeseen liittyviä vaikeasti käsitettäviä ja moniulotteisia kokonaisuuksia yhtenäisen käsitteistön luomiseksi.

Alaluvuissa 2.1 ja 2.2 käsitellään kyberrikollisuutta ilmiönä ja luodaan tutkimuksen tarpeisiin soveltuva määritelmä tietoverkkorikollisuudelle. Lisäksi luvuissa käsitellään niitä tunnuspiirteitä, jotka ovat tyypillisiä tälle kyberrikollisuuden muodolle. Alaluvussa 2.3 analysoidaan tilannetietoisuuden käsitettä, tilannetietoisuuden merkitystä päätöksenteossa sekä havainnollistetaan, miten tilannetietoisuutta tietoverkkorikollisuudesta voidaan rakentaa sen tunnuspiirteitä havainnoimalla. Lopuksi alaluvussa 2.4 pohditaan tilannetietoisuuden jakamisen edellytyksiä luottamusverkostossa aikaisempien tutkimusten valossa.

2.1 Kyberrikollisuus ilmiönä

Termi kyberrikollisuus (engl. c*ybercrime*) esiintyi ensi kerran 1990-luvun puolessa välissä kuvaten rikoksia, joissa digitaalinen laite tai tietojärjestelmä oli joko rikoksen suorittajan työkalu, kohde tai mahdollisesti molempia (Sabillion, Cavaller, Cano & Serra-Ruiz 2016). Kahtakymmentä vuotta myöhemmin kyberrikollisuuden määritelmä Euroopassa on jakautunut karkeasti kolmeen eri alamuotoon, joita ovat: tietotekniikkaa hyväksikäyttäen tehdyt perinteiset rikollisuuden muodot, laittoman sisällön julkaiseminen sekä ainoastaan tietoliikenneverkoissa esiintyvä rikollisuus (Euroopan komissio, 2007). Nämä alamuodot ovat keskenään hyvinkin erilaisia, mutta niissä kaikissa tietotekniikkaa hyväksikäytetään henkilökohtaisen tai taloudellisen hyödyn tavoittelemiseksi tai haitan aiheuttamiseksi toiselle osapuolelle.

Tietokoneisiin liittyvät rikokset ovat siis jo pitkään olleet vakiintunut ilmiö, mutta nopea maailman laajuinen verkottuminen on vaikuttanut vahvasti ilmiön kehitykseen. UNODC:n (2013) kattavan kyselytutkimuksen mukaan rikolliset ovat nopeasti oppineet hyödyntämään verkottuneen yhteiskunnan tarjoamia uusia mahdollisuuksia. Kyberrikollisuudelle onkin tyypillistä, että ylikansallista rikoshyötyä tavoitellaan globaalien tietoverkkojen avulla. Verrattain lyhyessä ajassa ilmiö on muuttunut teknisesti lahjakkaiden ihmisten suorittamista yksittäistä teoista massarikollisuudeksi, jonka suorittamiseen ei välttämättä tarvita erikoistaitoja. Laajassa mittakaavassa teot edellyttävät kuitenkin lähes poikkeuksetta korkeaa järjestäytymisastetta ja järjestäytyneen rikollisuuden arvioidaan kytkeytyvän jopa 80% kyberrikoksista. Vaikka rikollisorganisaatiot

eivät ole jokaisen yksittäisen teon taustalla, on rikoksen suorittamiseen käytetty työkalu tai ohjelmisto useimmiten rikollista alkuperää (UNODC, 2013).

Valtaväestöllä on merkittävästi suurempi riski joutua kyberrikollisuuden kuin perinteisen rikollisuuden uhriksi. Esimerkiksi erilaiset käyttäjän identiteettiin kohdistuvat loukkaukset ovat tyypillisiä suoraan väestöön kohdistuvia kyberrikosten tekomuotoja. Valtaosa kyberrikollisuudesta on tietotekniikan avulla suoritettuja perinteisiä rikoksia kuten kiristyksiä, petoksia sekä laittoman sisällön julkaisemista ja jakelua. Tästä huolimatta yrityksiin ja yhteisöihin kohdistuvat teot keskittyvät vahvasti tietoliikenneverkoissa esiintyviin rikoksiin kuten tietomurtoihin, palvelunestohyökkäyksiin sekä haittaohjelmien levittämiseen. Vaikka näiden rikosten osuus on viranomaisarvioiden mukaan vain 10 - 30 % kaikesta kyberrikollisuudesta, kohdistuvat ne muita tekomuotoja selkeämmin yrityksiin ja yhteisöihin muodostaen niille muuta kyberrikollisuutta huomattavasti suuremman uhan (UNODC, 2013).

Yritykset ja yhteisöt ovat pyrkineet suojautumaan erilaisilta hyökkäyksiltä kääntymällä tietoturvapalveluita tarjoavien kaupallisten yritysten puoleen. Tietoturvayritysten kyky havaita tai puuttua tietotekniikan avulla tehtyihin perinteisiin rikoksiin on melko rajattu, mutta sähköisissä tietoverkoissa esiintyvän rikollisuuden, eli tietoverkkorikollisuuden torjunnasta on sen sijaan syntynyt lukuisia liiketoimintamahdollisuuksia. Seuraavissa alaluvuissa on esitetty tutkimuksen tarpeisiin soveltuva tietoverkkorikollisuuden määritelmä ja kuvattu millaisista tunnuspiirteistä, eli elementeistä, kyseinen rikollisuuden muoto rakentuu.

2.2 Tietoverkkorikollisuus kyberrikollisuuden muotona

Tietoverkkorikollisuudella (engl. *Network Crime*) tarkoitetaan tässä tutkimuksessa ainoastaan tietoliikenneverkoissa esiintyviä rikoksia, jotka loukkaavat tietoverkoissa tai niihin liitetyissä järjestelmissä käsiteltävän tiedon luottamuksellisuutta, eheyttä tai saatavuutta. Tällaisiin tekoihin liittyvät Euroopan komission (2007) sekä UNOCD:n (2013) määritelmien mukaan seuraavat kuviossa 1 esitetyt tunnuspiirteet, joihin viitataan tässä tutkimuksessa tietoverkkorikollisuuden elementteinä.

- Luvaton pääsy tietojärjestelmään tai -verkkoon
- Luvaton pääsy dataan (sis. tietoliikenteen sieppaamisen)
- Järjestelmän tai datan luvaton häiritseminen
- Haittaohjelmien ja muiden väärinkäyttöön tarkoitettujen työkalujen tuotanto, jakelu ja ylläpito

KUVIO 1 Tietoverkkorikollisuuden elementit

Kuviossa 1 mainittujen tunnuspiirteiden lisäksi UNOCD:n määritelmässä on erotettu omaksi tunnuspiirteeksi tietoturvakontrollien tai yksityisyydensuoja-mekanismien rikkominen. Tässä tutkimuksessa vastaavaa erottelua ei ole tehty, sillä kyseisen tunnuspiirteen katsotaan sisältyvän teon luvattomaan luonteeseen. Rajaus on yhtenevä Suomen lainsäädännön kanssa, jossa kontrollien tai suojamekanismien rikkomista ei ole säädetty erilliseksi rikokseksi, vaan ne ovat raskauttavia tekomuotoja, jotka saattavat tehdä muutoin tavanomaisesta tieto- tai viestintärikoksesta törkeän rikoksen (Rikoslaki 39/1889, luku 38).

Lisäksi kaikissa edellä mainituissa määritelmissä, on kuvattu myös joukko tietotekniikkaa hyväksikäyttäen tehtyjä, sekä laittoman sisällön julkaisemiseen liittyviä rikoksia, joihin tässä tutkimuksessa on viitattu yleisesti kyberrikollisuutena. Tutkimuksessa tehdäänkin ero tietotekniikkaa tai -verkkoa hyväksikäyttäen tehdyn rikosten (kuten erilaisten petokset tai kiristykset) ja tietoverkkorikosten välille, joista ensin mainitun katsotaan olevan osa yleisempää kyberrikollisuutta ja jälkimmäisen muodostavan tunnuspiirteiltään yhtenäisen osajoukon. Tässä tutkimuksessa tietoverkkorikollisuudella tarkoitetaankin vain niitä rikoksia, jotka muodostuvat yhdestä tai useammasta tietoverkkorikollisuuden elementistä (ks. taulukko 1).

TAULUKKO 1 Tieto- ja viestintärikokset Suomen lainsäädännössä

Rikoslaki (39/1889) luku 38	**Tietoverkkorikollisuuden elementti**
1 § Salassapitorikos	-
2 § Salassapitorikkomus	-
3 § Viestintäsalaisuuden loukkaus	Luvaton pääsy dataan
4 § Törkeä viestintäsalaisuuden loukkaus	Luvaton pääsy dataan
5 § Tietoliikenteen häirintä	Järjestelmän tai datan luvaton häiritseminen
6 § Törkeä tietoliikenteen häirintä	Järjestelmän tai datan luvaton häiritseminen
7 § Lievä tietoliikenteen häirintä	Järjestelmän tai datan luvaton häiritseminen
7a § Tietojärjestelmän häirintä	Järjestelmän tai datan luvaton häiritseminen
7b § Törkeä tietojärjestelmän häirintä	Järjestelmän tai datan luvaton häiritseminen
8 § Tietomurto	Luvaton pääsy tietojärjestelmään tai -verkkoon ja/tai luvaton pääsy dataan
8a § Törkeä tietomurto	Luvaton pääsy tietojärjestelmään tai -verkkoon ja/tai luvaton pääsy dataan
8b § Suojauksen purkujärjestelmärikos	Haittaohjelmien ja muiden väärinkäyttöön tarkoitettujen työkalujen tuotanto, jakelu ja ylläpito.
9 § Henkilörekisteririkos	-
9a § Identiteettivarkaus	-

Huomionarvoista yleisen kyberrikollisuuden ja tietoverkkorikollisuuden välistä rajaa määritettäessä on, etteivät ne ole toisiaan poissulkevia. Esimerkiksi petos voi vaatia ensin luvattoman pääsyn tietojärjestelmään ja uhrin kiristäminen voidaan toteuttaa siihen erityisesti tarkoitetun haittaohjelman avulla.

Varsinaisiksi tietoverkkorikoksiksi lasketaan kuitenkin tässä tutkimuksessa vain tekojen ne osuudet, joista on selkeästi tunnistettavissa tietoverkkorikollisuuden elementit.

Ymmärtääkseen tietoverkkorikollisuuden luonnetta paremmin, tulisi voida havainnoida sellaisia tekoja, joista on tunnistettavissa edellä mainitut tietoverkkorikollisuuden elementit. Koska niin tietoverkko- kuin kyberrikollisuus jäävät usein piilorikollisuudeksi, tulisi näkyvyys tapahtuviin rikoksiin rakentaa muuten kuin rikostilastojen avulla. Näin muodostuvan tilannetietoisuuden avulla saattaisi olla mahdollista kytkeä rikostilastoissa yksittäisiltä näyttävät teot osaksi isompia kampanjoita ja toteuttaa rikoksia torjuvia ja ennaltaehkäiseviä toimenpiteitä.

2.3 Tilannetietoisuuden tutkimuksesta

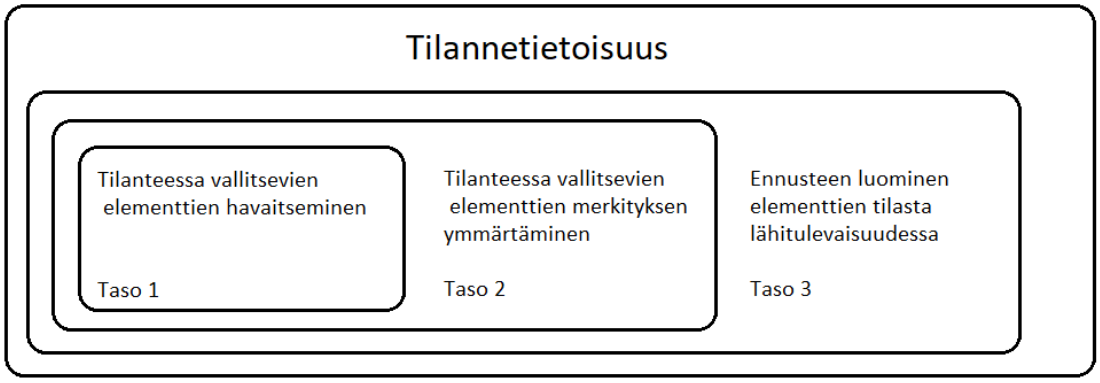
Kybertilannetietoisuutta käsittelevää kirjallisuutta tutkineiden Ulirk Franke ja Joel Brynielsson (2014) mukaan kybertilannetietoisuutta ja sen muodostamista voidaan lähestyä joko teknologisena tai kognitiivisena ilmiönä. Teknologinen lähestymistapa voi keskittyä esimerkiksi siihen, miten tietyssä järjestelmässä kootaan data, prosessoidaan se ja yhdistellään siten, että teknologian avulla pystytään luomaan oikeellista tietoa tilannetietoisuuden muodostamisen tueksi. Kognitiivinen lähestymistapa puolestaan tutkii yksilöiden kykyä ymmärtää saatavilla olevaa tietoa ja taitoa hyödyntää sitä päätöksenteon tukena (Franke & Brynielsson, 2014). Tässä tutkimuksessa tilannetietoisuuden muodostamista käsitellään pääasiassa kognitiivisena ilmiönä, jolloin merkitykselliseksi muodostuu itse tilannetietoisuuden käsite. Tilannetietoisuutta jakavan verkoston toiminnan kannalta on keskeistä ymmärtää mitä termillä tarkoitetaan, mistä se muodostuu sekä miten ja mihin tilannetietoisuutta on tarkoitus käyttää.

2.3.1 Tilannetietoisuus käsitteenä

Tilannetietoisuuden (engl. *Situational / Situation Awareness*) muodostamista on tutkittu käyttäytymistieteellisestä ja kognitiivisesta näkökulmasta tiivisti 1980 luvulta lähtien. Yhdysvaltalainen Mica R. Endsley on toiminut yhtenä alan pioneereista kirjoittaen yli 200 tieteellistä artikkelia ja julkaisua tilannetietoisuuden muodostamisesta, mallintamisesta sekä soveltamisesta. Endsley on esittänyt laajasti hyväksytyn (Franke & Brynielsson, 2014; Wickens, 2008) tilannetietoisuuden käsitteellisen määritelmän jonka mukaan tilannekuvalla tai tilannetietoisuudella tarkoitetaan: ”ympäristössä olevien elementtien havaitsemista ajassa ja paikassa, niiden merkityksen ymmärtämistä sekä ennusteen luomista elementtien tilasta lähitulevaisuudessa” (Endsley, 1988, 792).

Endsley on myöhemmin jalostanut määritelmäänsä ja luonut sen pohjalta teoreettisen mallin, jonka mukaan tilannetietoisuus voidaan jakaa kolmelle eri

tasolle. Taso 1 ”havaitseminen” tarkoittaa havaintojen tekemistä saatavilla olevista datasta, taso 2 ”ymmärtäminen” tarkoittaa datan tulkitsemista sekä sen merkityksen oivaltamista ja taso 3 ”ennustaminen” tarkoittaa kykyä hahmottaa, mitä todennäköisesti tapahtuu seuraavaksi (Endsley, 1995). Tilannetietoisuuden voi ymmärtää eri tietoisuuden tasoille sijoittuvaksi portaittain rakentuvaksi ymmärrykseksi siitä, mitä havainnot ympäröivästä todellisuudesta tarkoittavat tietyllä ajan hetkellä ja mitä niiden perusteella voidaan päätellä tilanteen kehittymisestä lähitulevaisuudessa (ks. kuvio 2).



KUVIO 2 Tilannetietoisuuden käsitteellinen määritelmä (Endsley, 1995, 35, muokattu)

Endsleyn teoreettista mallia on arvosteltu esimerkiksi tieteellisyyden puutteesta ja liiallisesta yleistämisestä (Dekker & Hollnagel, 2004) sekä siitä, että se keskittyy liiaksi tilannetietoisuuden tarkastelemiseen ympäröivästä todellisuudesta irrallisena mallina (Salmon, Stanton, Walker, Jenkins & Rafferty, 2010). Nämä väitteet on kuitenkin joko pääosin kumottu, tai perustuvat pitkälti väärinymmärryksiin ja virheellisiin olettamuksiin (Endsley, 2015). Vaikka tilannetietoisuuden muodostamiseen liittyviä tuoreempia teoreettisia malleja on kehitetty (ks. esim. Salmon ym. 2008; Endsley, 2015), on Endsleyn esittämää mallia kuitenkin pystytty onnistuneesti puolustamaan yli kaksikymmentä vuotta sen julkaisusta, tehden siitä verrattain luotettavan lähtökohdan tilannetietoisuuden käsitteelliselle mallintamiselle.

Suomalaisessa kontekstissa tilannekuvan käsitettä ja tilannetietoisuuden muodostumista on tutkinut muun muassa filosofian tohtori Rauno Kuusisto. Kuusisto teki vuonna 2005 Liikenne- ja viestintäministeriön toimeksiannosta haastattelututkimuksen, jossa selvitettiin keskeisten turvallisuusviranomaisten tilannekuvan ja tilannetietoisuuden luonnetta. Tutkimus oli osa kehitystyötä, jonka tavoitteena oli muodostaa yhteensopiva kokonaisuus turvallisuusviranomaisten toimintaa tukevista erilaisista viestintä- ja järjestelmärakenteista sekä -palveluista. Vaikka haastatteluaineisto oli suppeahko (11 vastaajaa) eikä sen perusteella voi tehdä yleistettäviä päätelmiä, osoittaa tutkimus hyvin sen, miten tilannekuvan liittyvän suomenkielisen

käsitteistön ympärillä voidaan jo pienessäkin vastaajajoukossa havaita eri näkökulmista johtuvaa käsitteiden tulkinnan erilaisuutta.

Kuusisto (2005) määrittelee käsitteellisessä analyysissään termit: *tilanne, tilannetietoisuus, tilanneymmärrys ja tilannekuva,* joita kaikkia turvallisuusviranomaisten edustajat käyttivät haastatteluissa osittain päällekkäin. Yleisimpänä terminä käytössä oli tilannekuva, joka joissain tapauksissa kuvasi kaikkia muita edellä mainittuja käsitteitä. Kuusiston määritelmän mukaan tilannekuva on tietystä tilanteesta saatu kuva tai käsitys. Määritelmän käyttö on kuitenkin hänen mukaansa eksaktissa yleisessä tekstissä hankalaa, koska käsite on monimerkityksinen sekä tulkinnanvarainen (Kuusisto 2005).

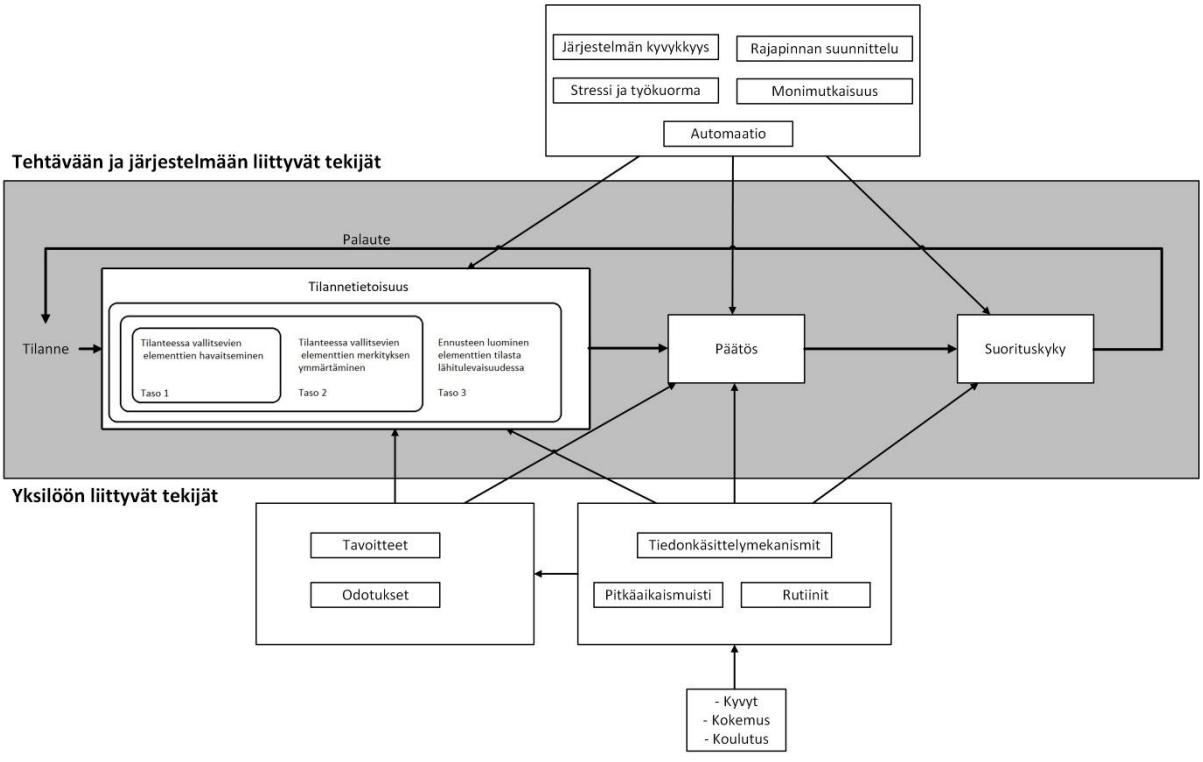
Kuusiston tutkimuksen teoreettinen perusta perustuu hänen aikaisempaan työhönsä (Kuusisto, 2004), jonka pohjalta hän päätyy käyttämään käsitteitä tilanne, tilanteen malli, tilannetietoisuus ja tilanneymmärrys. Tilanne on Kuusistolle käsite, joka kuvaa ajallisilla määreillä rajattavissa olevia toimijan omia, tai sen ulkopuolella olevien toimijoiden aikaansaamia tapahtumia. Tilanteen malli on kuvallisesti, sanallisesti tai kirjallisesti ilmaistu kuvaus noista tapahtumista, jonka perusteella todellinen tilanteen olemus voidaan hahmottaa (vrt. Endsleyn malli, taso 1 – havaitseminen). Tilannetietoisuus tarkoittaa Kuusistolle tilanteen tulkintaa, systeemin vuorovaikutusten ymmärtämistä ja tietoisuuden luomista tilanteen vaatimista toimenpiteistä, mikä edellyttää ulkoa tulevan datan ja oman suorituskyvyn tietämistä (vrt. Endsleyn malli, taso 2 – ymmärtäminen). Tilanneymmärrys on puolestaan Kuusistolle tilanteen ja tilannetietoisuuden tulkitsemista kokonaisympäristö huomioiden siten, että tulkitsija ymmärtää mitkä tekijät itseen ja muuhun maailmaan vaikuttavat ja miten tilanne voi kehittyä. Tilanteen ymmärtävä tietää tällöin myös, miten tilanteessa tulee toimia. Tilanneymmärrys edellyttääkin kykyä ennakoida ja nähdä välittömän ajallisen ja paikallisen toiminnan ulkopuolelle (vrt. Endsleyn malli taso 3, – ennustaminen).

Kuusiston määrittelemä käsite ”tilanteen malli” voidaan rinnastaa Endsleyn mallin tasoon 1, jolloin tilanne kuvaamalla pyritään saamaan havaintoja ympäröivästä todellisuudesta. Kuusiston käsitys ”tilannetietoisuudesta” voidaan tulkita yhteneväksi Endsleyn mallin tason kaksi kanssa, jossa muodostetaan tarvittava ymmärrys vallitsevasta tilanteesta. Endsleyn tason kolme voidaan puolestaan katsoa pitävän sisällään Kuusiston määritelmän tilanneymmärryksestä, joka luo tulkitsijalle mahdollisuuden ymmärtää, mitkä tekijät itseen ja muuhun maailmaan vaikuttavat, miten tilanne voi kehittyä ja miten siihen tulisi reagoida. Näiden kolmen tason katsotaan tässä tutkimuksessa muodostavan tilannetietoisuuden tietystä ajan hetkestä. Jotta termi ei jäisi tulkinnanvaraiseksi yläkäsiteeksi, tulee se hahmottaa eri tietoisuuden tasoille sijoittuvaksi portaittain rakentuvaksi ymmärrykseksi siitä, mitä havainnot ympäröivästä todellisuudesta tietyllä ajan hetkellä tarkoittavat ja mitä niiden perusteella voidaan päätellä tilanteen kehittymisestä lähitulevaisuudessa. Pelkkä saavutettu ymmärrys tietystä tilanteesta ja sen todennäköisistä kehityskuluista ei ole itseisarvo, vaan sen avulla

tulisi myös pystyä muodostamana käsitys parhaasta mahdollisesta toimintatavasta ja tehdä päätös tarvittaviin toimiin ryhtymisestä. Tilannetietoisuuden merkitystä päätöksenteossa käsitellään seuraavassa alaluvussa.

2.3.2 Tilannetietoisuuden merkitys päätöksenteossa

Endsleyn (Endsley 1988; 1995; 2015) mukaan tilannetietoisuutta muodostavalle henkilölle ei riitä, että hän havaitsee ympärillään vallitsevan tilanteen. Henkilön täytyy myös ymmärtää havaintojensa syvällisempi merkitys omien (tai hänelle asetettujen) tavoitteiden valossa, jotta syntynyttä tietoisuutta voi käyttää päätöksenteon tukena. Henkilön roolin kannalta oleelliset tavoitteet määrittelevät sen mitkä havainnot ovat tärkeitä ja hyödyllisiä kulloisenkin tehtävän suorittamiseksi. Endsleyn (1995) teoreettinen malli (ks. kuvio 3) kuvaa tilannetietoisuuden saavuttamisen merkityksen dynaamisessa päätöksentekoprosessissa.



KUVIO 3 Tilannetietoisuuden merkitys dynaamisessa päätöksenteossa (Endsley, 1995, 35, muokattu)

Endsleyn (1995) esittämän mallin mukaan päätöksenteko rakentuu yksilön käsitykseen vallitsevasta tilanteesta. Päätökset tehdään hänen mukaansa tilannetietoisuuden perusteella ja suorituskyky perustuu pitkälti yksilön taitoon muodostaa mahdollisimman totuudenmukainen tietoisuus ympäröivästä

todellisuudesta ja tehdä sen perusteella mahdollisimman hyviä päätöksiä. Tilannetietoisuuden muodostumiseen vaikuttavat sekä yksilön käsitys ympäröivästä todellisuudesta, että ennakko-odotukset siitä, mitä muodostettavalla tietoisuudella yritetään saavuttaa. Mallissa havaintoja tulkitseva yksilö pyrkii omien tiedonkäsittely-mekanismiensa, pitkäaikaisen säilömuistinsa sekä opittujen sisäisten malliensa avulla muodostamaan käsityksen siitä, mitä havainnot tarkoittavat ja mitä niiden perusteella voi päätellä. Tämän ymmärryksen muodostumiseen vaikuttavat niin yksilön henkilökohtaiset ominaisuudet, kokemus ja koulutus kuin yksilön kanssa vuorovaikutuksessa olevan systeemin kyvykkyydet sekä tietoa välittävien rajapintojen toimivuus, havainnoitavan tiedon monimutkaisuus ja sen prosessoinnin automaation aste. Tilannetietoisuus muodostuu portaittain kasvavasta tietoisuuden tilasta, jossa aluksi tehdään havaintoja saatavilla olevasta datasta, tulkitaan niitä omien kykyjen ja systeemin kyvykkyyksien rajoissa muodostaen tietoa ja ymmärrystä siitä, mitä tietyllä hetkellä tapahtuu. Tämän perusteella muodostetaan ennuste siitä, mitä seuraavaksi tulee tapahtumaan ja miten siihen tulisi reagoida (Endsley, 1995).

Kuviossa 3 tilannetietoisuus ja päätöksenteko on kuvattu selkeästi erillisiksi prosesseiksi, sillä päätös tietynlaisesta toiminnasta ei ole välttämättä riippuvainen tietoisuuden laadusta tai sen syvyydestä. Huonollakin tilannetietoisuudella voi tehdä oikeita päätöksiä ja toisaalta erinomainenkaan ymmärrys vallitsevasta tilanteesta ei takaa suorituksen laatua, jos toimijalla ei ole kykyä, koulutusta tai tarvittavaa kokemusta tehdä päätöstä tilanteen vaatimista toimenpiteistä. Tilannetietoisuus voi kuitenkin vaikuttaa positiivisesti päätöksentekoon, jos sen muodostajalla on muut tarvittavat edellytykset oikean päätöksen tekemiseksi (Endsley, 1995; 2000).

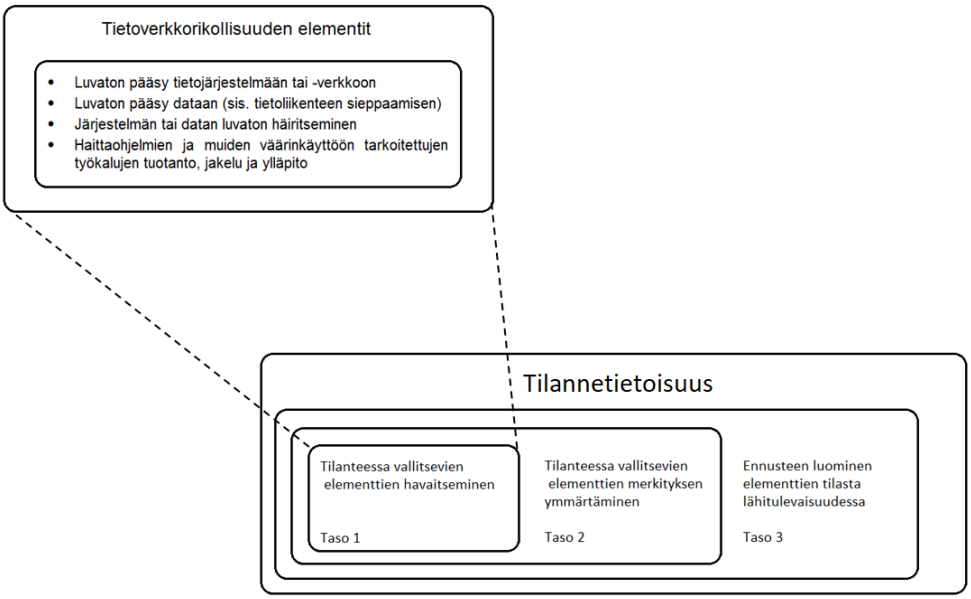
Myös tietoverkkorikollisuuden tilannetietoisuuden muodostamista suunniteltaessa tulisi ottaa huomioon, että tietoisuuden tulisi palvella päätöksentekoa ja tukea tilanteen edellyttämien toimenpiteiden hahmottamista. Luottamusverkostossa tilanteen tekee haasteelliseksi se, että tilannetietoisuuden hahmottamiselle on erilaisia tarpeita. Jokaisella verkoston toimijalla on omat tavoitteensa sidosryhmiensä odotusten täyttämiseksi sekä henkilöstön työrooleja palvelevan tilannetietoisuuden saavuttamiseksi. Lisäksi myös kuviossa 3 kuvatut järjestelmäkohtaiset edellytykset sekä henkilöstön henkilökohtaisiin ominaisuuksiin liittyvät muuttujat vaikuttavat organisaatioittain muodostettavan tilannetietoisuuden laatuun. Erilaisista tarpeista ja kyvykkyyksistä huolimatta tietoverkkorikollisuuden tilannetietoisuuden tulisi pystyä palvelemaan kaikkia luottamusverkoston toimintaan osallistuvia osapuolia. Etenkin sen tulisi tarjota tilannetta tulkitsevalle taholle mahdollisuus muodostaa ymmärrys siitä, mitkä tietoverkkorikollisuuteen liittyvät tekijät tarkkailtavaan ympäristöön vaikuttavat tietyllä ajanhetkellä ja miten tilanne voi kehittyä. Tilanteen ymmärtävä tietää tällöin myös, miten tulee toimia niin omien kuin edustamansa organisaation tavoitteiden saavuttamiseksi. Ilman kykyä hahmottaa sitä, mitä todennäköisesti tapahtuu seuraavaksi, tietoverkkorikollisuuden tilannetietoisuus jää vain pinnallisemmille

tietoisuuden tasoille sijoittuvaksi nykytilanteen kuvaukseksi, jonka perusteella voi olla haasteellista saavuttaa konkreettista hyötyä luottamusverkoston toimijoille.

2.3.3 Tilannetietoisuus tietoverkkorikollisuuden kontekstissa

Tilannetietoisuuden tutkiminen on viimevuosina ulottunut myös kyberympäristöön. Franken ja Brynielssonin (2014) mukaan kiinnostus kybertilannetietoisuuden muodostamiseen on kasvanut viime vuosina jatkuvasti. Heille kybertilannetietoisuus tarkoittaa yleisemmän tilannetietoisuus -käsitteen alaryhmää, joka voidaan muodostaa mistä tahansa epäilyttävistä tai kiinnostavista kyberympäristön tapahtumista. Tässä tutkimuksessa huomio kyberympäristössä kiinnitetään tietoverkkorikoksiin, joiden määritelmä esitettiin alaluvussa 2.2. Tietoverkkorikollisuuden tilannetietoisuuden katsotaan muodostavan siis yhden osa-alueen laajemmasta kybertilannetietoisuudesta.

Tietoverkkorikollisuuden tilannetietoisuuden muodostamisen kannalta on tärkeää ymmärtää, mistä elementeistä tietoisuus koostuu, sillä ne määrittävät, mitä havaintoja yksilön tulisi tehdä ja mitkä tapahtumat ovat tilannetietoisuuden kannalta oleellisia. Oleellisia havaintoja tekemällä yksilöllä on mahdollisuus muodostaa ymmärrys tilanteessa vallitsevista seikoista niiden rajoitteiden valossa, mitä käsiteltiin edellisessä alaluvussa. Näin saavutettua tietoisuuden voidaan käyttää päätöksenteon apuna, minkä tulisi olla tietoisuuden muodostamisen perimmäinen tarkoitus. Tietoverkkorikollisuuden tilannetietoisuus muodostuu tietoisuuden eri tasoille sijoittuvasta portaittaisesta ymmärryksestä, jonka perusteella on mahdollista käsittää, mitä tietoverkkorikkorikollisuuteen viittaavat havainnot tarkoittavat tietyllä ajan hetkellä ja mitä niiden perusteella voidaan päätellä tilanteen kehittymisestä lähitulevaisuudessa. Luvussa 2.2 tunnistetut tietoverkkorikollisuuden elementit ovat niitä havainnoitavia tapahtumia, joiden perusteella tietoverkkorikollisuuden tilannetietoisuus tulisi muodostaa, kuten kuviossa 4 on kuvattu.



KUVIO 4 Tietoverkkorikollisuuden tilannetietoisuuden muodostaminen

Endsley (2012) alleviivaa, että tilannetietoisuuden muodostamisella on kyberympäristössä väistämättä teknologinen ulottuvuus, mutta myös vahva linkki ihmisten väliseen sosiaaliseen kanssakäymiseen. Teknologisten tuotteiden avulla voidaan tuottaa tilannetietoisuutta, mutta ilman kognitiivista analyysiä on mahdotonta muodostaa sellaista tietoisuutta, joka auttaisi ymmärtämään ja ennakoimaan kehittyviä uhkia. Yksittäinen tilannetietoisuutta muodostava toimija voi tehdä analyysin vain tekemiensä havaintojen perusteella, mikä ei ole riittävää esimerkiksi kansallista tilannetietoisuutta muodostettaessa. Franke ja Brynielsson (2014) ovat tunnistaneet 11 eri valtion kyberturvallisuusstrategioissa tahtotilan kehittää kansallista kybertilannetietoisuutta ja niistä useissa painotetaan myös kybertilannetietoisuuden jakamisen tärkeyttä. Seuraavassa alaluvussa pohditaan, miten tietoverkkorikollisuuden tilannetietoisuus olisi mahdollista jakaa eri toimijoiden välillä siten, että se kattaisi kaikkien toimijoiden oleelliset havainnot ja siten, että sen perusteella olisi mahdollista muodostaa yhteinen ymmärrys siitä, mitä havainnot tarkoittavat ja mitä niiden perusteella voidaan päätellä tietoverkkorikollisuuden kehittymisestä lähitulevaisuudessa.

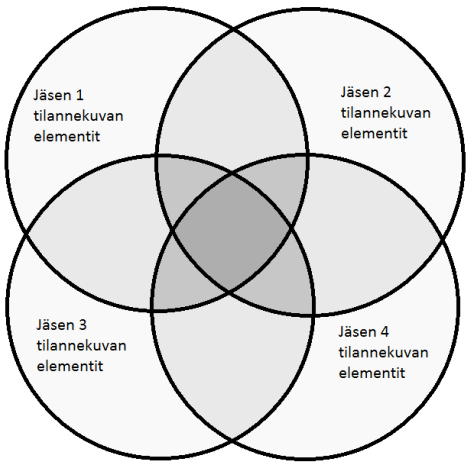
2.4 Tilannetietoisuuden jakaminen

Vaikka tilannetietoisuuden tutkimus on viimeisen 25 vuoden aikana vakiinnuttanut paikkansa tutkimusaiheena ja myös kybertilannetietoisuuden muodostamista on viime vuosina tutkittu laajasti (Franke & Brynielsson, 2014; Endsley, 2015), verrattain harvassa tutkimuksessa on kuitenkaan keskitytty

siihen, miten kybertilannetietoisuutta voidaan muodostaa vaihtamalla tietoja eri organisaatioiden kesken (Franke & Brynielsson, 2014). Jotta voidaan saavuttaa käsitys kybertilannetietoisuuden jakamiseen vaikuttavista seikoista, luodaan seuraavissa alaluvuissa katsaus yleisempään yhteisen tilannetietoisuuden muodostamiseen ja tilannetietoisuuden jakamiseen liittyvään tutkimukseen, josta on huomattavan paljon enemmän lähdeaineistoa saatavilla. Tämän jälkeen esitetään synteesi siitä, miten yhteinen tietoverkkorikollisuuden tilannetietoisuus voidaan muodostaa luottamusverkostossa jaettavien havaintojen perusteella ja mitkä seikat sen jakamiseen vaikuttavat.

2.4.1 Yhteisen tilannetietoisuuden muodostaminen

Endsley (1995) sivuaa tilannetietoisuuden teoreettista mallia koskevassa artikkelissaan lyhyesti myös yhteisen tilannetietoisuuden muodostamista ryhmän jäsenten kesken. Hän esittää artikkelissa ajatuksen, että ryhmässä voidaan muodostaa yhteinen tilannetietoisuus ryhmän jäsenten henkilökohtaiset tilannetietoisuudet yhdistämällä. Jokaisella ryhmän jäsenellä on oma tilannetietoisuutensa, jonka hän on luonut omien tavoitteidensa ja työroolinsa liittyvien tehtävien suorittamiseksi. Jäsenten henkilökohtaisten tilannetietoisuuden elementit (havainnot, joista tietoisuus muodostuu) asettuvat kuitenkin limittäin kuten kuviossa 5 on esitetty. Kuvioon on alkuperäiseen nähden korostettu harmaan eri sävyillä ne tilannetietoisuuden elementit, jotka ovat yhteisiä tiimin eri jäsenille. Näin ollen kuvion keskelle muodostuu tumman harmaa alue, joka kuvaa sitä tietoisuutta, jonka ymmärtäminen on kaikille ryhmän jäsenille oleellista. Vaalealla on kuvattu taas ne tietoisuuden elementit, jotka ovat tarpeellisia vain ryhmän tietyn jäsenen tavoitteiden ja tehtävien kannalta.



KUVIO 5 Ryhmän tilannetietoisuus (Endsley 1995, 39, muokattu)

Endsley (1995) huomauttaa, ettei koko ryhmän suoriutumisen kannalta ole edullista, jos vain yksi ryhmän jäsen tietää sellaiset tilannetietoisuuden elementit, joiden tulisi olla ryhmän suoriutumisen kannalta kaikkien tiedossa. Jos ryhmän tietty jäsen ei jaa muille jäsenille sellaista tietoisuutta, mitä he tarvitsisivat tavoitteidensa täyttämiseksi tai tehtäviensä suorittamiseksi, on ryhmällä heikommat lähtökodat päätöksenteolle. Toisin sanoen, jos ryhmän yhteinen tilannetietoisuus on heikko, voi ryhmän suoriutuminen kokonaisuudessaan kärsiä.

Endsley on myöhemmin (ks. esim. Endsley & Jones, 1997; Endsley & Robertson, 2000) laventanut määritelmäänsä ryhmän tilannetietoisuudesta käyttäen termiä jaettu tilannetilannetietoisuus. Endsley ja Robertson (2000) määrittelevät termin jaettu tilannetietoisuus (*shared situational awareness)* tarkoittavan sellaista tietoisuutta, joka on tarpeellista koko ryhmän toiminnalle. Heidän mukaansa jaetun tilannetietoisuuden tulee olla mahdollisimman yhtenevä ryhmän jäsenten kesken, jotta ryhmän toiminta olisi mahdollisimman tehokasta. Ilman jaettua ja yhtenäistä tilannetietoisuutta on mahdollista, että tarpeellisia havaintoja jää kommunikoimatta (ei ymmärretä mitä tietoa muut tarvitsevat), asioita jää tekemättä (ei tiedetä, kenen vastuulla tehtävä on), tai toiminta ei ole oikea-aikaista (asioita tehdään väärään aikaan). Kirjoittajat esittävät myös, että yksittäisen ryhmän jäsenten tulisi kunkin tahollaan pystyä luomaan kokonaiskuva (sisäinen malli) myös siitä, mitä tietoa muut yhteisen tavoitteen eteen vuoksi työskentelevät ryhmät tarvitsevat onnistuakseen omista tehtävistään.

Yhteisen tilannetietoisuuden muodostaminen mutkistuu kuitenkin, jos tietoisuus tulee pystyä rakentamaan yhden ryhmän jäsenten sijasta useiden eri ryhmien välille. Endsley ja Jones (1997) mukaan yhteistä tilannetietoisuutta muodostavien itsenäisten ryhmien jäsenet työskentelevät lähes poikkeuksetta erossa toisistaan, mutta niillä on yhteinen tavoite (syy miksi tilannetietoisuutta muodostetaan), keskinäinen riippuvuussuhde (toisten ryhmien panoksen ymmärtäminen on tärkeää yhteisten tavoitteiden saavuttamiselle) ja nimetyt roolit (kaikkien ei tarvitse tehdä samoja asioita). Näin ne muodostavat yhteenliittymän, jolla on yhteinen missio. Vaatimukset yhteisen tilannetietoisuuden sisällölle perustuvat eri ryhmien yhteneviin tilannetietoisuuden tarpeisiin samoin, kuin ryhmän sisäisesti eri jäsenten kesken (ks. kuvio **5**). Mitä tehokkaampaa näihin osa-alueisiin perustuva tiedonvaihto on, sitä paremmat edellytykset kullakin ryhmällä on tahollaan reagoida dynaamisesti muuttuvaan tilanteeseen. Koska kukin ryhmä työskentelee erossa toisistaan, ovat ne riippuvaisia tehokkaista kommunikointikanavista sekä mahdollisesti jaetuista tilannekuvanäkymistä. Eri ryhmien tulisi myös pystyä tulkitsemaan jaettavaa havaintoja yhtenevän sisäisen mallin pohjalta, jotta ne voivat ymmärtää, mitkä seikat vaikuttavat kaikkiin toimijoihin ja mitä toimenpiteitä niiden takia vaaditaan. Yhteinen sisäinen malli on tärkeä korkeamman tason tilannetietoisuuden (tasot 2 ja 3) jakamisen kannalta, jonka avulla on mahdollista muodostaa kuva siitä, mikä tilanteen vaikutus on kaikkien ryhmien yhteiseen missioon (Endsley & Jones, 1997).

Endsleyn teoreettiseen malliin pohjautuva käsitys tilannetietoisuudesta ei arvostelijoiden mukaan kuitenkaan sovellu yhteisen tilannetietoisuuden muodostamiseen. Esimerkiksi Salmon ym. (2010) esittävät, että ongelmia syntyy, kun yksinomaan yksilön tilannetietoisuuden muodostumisen kuvaamiseen tarkoitettua sisäistä mallia aletaan soveltaa yhteistyöhön perustuviin järjestelmiin. Oleelliseksi eriävissä näkemyksissä nousee englannin kielisten käsitteiden *Shared Situational Awareness* (Endsley & Jones, 1997; Endsley & Robertson, 2000) sekä *Distributed Situational Awareness* (Salmon ym. 2008; Salmon ym. 2010) merkityserot.

Kriitikot kuten Salmon ym. (2010) arvostelevat esimerkiksi, ettei termi *Shared Situational Awareness* kerro tarkoitetaanko sanalla jaettu (*shared*) sitä, että jokainen henkilö ymmärtää tarkasteltavan tilanteen samalla tavalla (ns. yhteinen ymmärrys) vai, että jokaisella henkilöllä on hallussaan tietty osa tilannetietoisuudesta (ns. loogisesti jaettu tilannetietoisuus). Määrittelemättä on heidän mukaansa jäänyt myös se, voivatko eri henkilöt muodostaa samasta aineistosta keskenään yhtenevän tilannetilannetietoisuuden. Vaikka tietty tilannetietoisuus voi olla siinä mielessä jaettu, että useampi henkilö tarvitsee sitä työssään, ei se heidän mielestään voi kuitenkaan muodostaa yhtenäistä ymmärrystä tilanteesta, joka olisi sama kaikilla ryhmän jäsenillä, koska jokainen tulkitsee sitä omien kykyjensä pohjalta. Salmon ym. (2010) puhuvatkin yhteensopivista tilannetietoisuuksista, joita kaikkia tarvitaan yhteisen tehtävän suorittamiseksi. He käyttävätkin aikaisemmin, vuonna 2008 lanseeraamaansa termiä *Distributed Situational Awareness,* jolla tarkoitetaan hajautettua yhteensopivien tilannetietoisuuksien muodostamaa kokonaisuutta.

Endsley (2015) kuitenkin torjuu kritiikin huomauttaen, ettei ole esittänyt jaetun tilannetietoisuuden tarkoittavan yhtenäistä ymmärrystä tilanteesta, joka olisi kaikille täysin sama. Päinvastoin jo 1995 teoreettisessa mallissaan hän alleviivaa yksilön kykyjen vaikuttavan yhtenä tekijänä tilannetietoisuuden muodostamiseen. Hän myös muistuttaa, että ryhmän jäsenten ei tarvitse jakaa kaikkea tietoaan, vaan pelkästään se osa, jonka tietäminen on tarpeellista koko ryhmän toiminnalle (Endsley, 2015). Tämä määritelmä on myös hyvin lähellä Kuusiston (2005) käyttämää määritelmää *Yhteinen tilannetietoisuus*. Yhteisellä tilannetietoisuudella hän tarkoittaa yhteisesti ymmärrettävä mallia ja kuvausta tilanteen tulkintaan vaikuttavista tiedoista, jotka ovat yhden tai useamman käyttäjän yhteisesti käytettävissä.

Tässä tutkimuksessa on päädytty käyttämään termiä yhteinen tilannetietoisuus, jolla tarkoitetaan Endsleytä ja Kuusistoa mukaillen, sellaista tietoisuutta, joka on tarpeellista koko ryhmän toiminnalle. Tutkimuksessa katsotaan, että vastaavan yhteisen tilannetietoisuuden voi muodostaa myös useamman eri ryhmän välille, jolloin vaatimukset yhteisen tilannetietoisuuden sisällölle perustuvat eri ryhmien yhteneviin tilannetietoisuuden tarpeisiin. Kukin toimija voi tällöin hyödyntää oleellista tietoa omissa prosesseissaan, mikä auttaa kunkin toimijan oman tilannetietoisuuden syntymistä. Tällaisessa tilanteessa on oleellista, että tilannetietoisuuden kokoamiseen osallistuvilla ryhmillä olisi myös yhteiset tavoitteet ja yhtenäinen missio, jotta olisi mahdollista määrittää ne

tarpeelliset tiedot, joiden jakaminen on oleellista yhteisten tavoitteiden saavuttamiseksi. Yhteisten tavoitteiden tai siihen perustuvan tilannetietoisuuden muodostaminen eri organisaatioiden välille ei kuitenkaan ole yksinkertaista etenkään, jos tietoa jakavassa luottamusverkostossa on jäseninä sellaisia yrityksiä, jotka ovat toistensa kilpailijoita.

2.4.2 Luottamusverkosto tietoverkkorikollisuuden tilannetietoisuuden jakajana

Yleisin rakenne verkkoihin ja tietoturvaan liittyvien tietojen vaihtamiseen on luotettu foorumi, jossa jäsenet voivat kokoontua säännöllisesti keskustelemaan asioista epävirallisesti (De Muynck & Portesi 2015). Tässä tutkimuksessa foorumista käytetään termiä luottamusverkosto, koska se kuvaa osuvasti paitsi foorumin verkostomaista toteutusta, myös sen toiminnan luottamukselliseen tietojen jakamiseen perustuvaa luonnetta. Kansainvälisinä esimerkkeinä erilaisista kumppanuusohjelmista ja luottamusverkostoista tietoverkko-rikollisuuden havainnointiin liittyen ovat esimerkiksi erilaiset ISAC -yhteisöt (Information Sharing and Analysis Center) sekä FBI:n ja yritysten välinen INFRAGARD -ohjelma Yhdysvalloissa tai CiSP -toiminta (Cyber Information Sharing Partenrship) Isossa-Britanniassa (Gordon, Loeb & Lucyshyn, 2003; Davies & Patel, 2016).

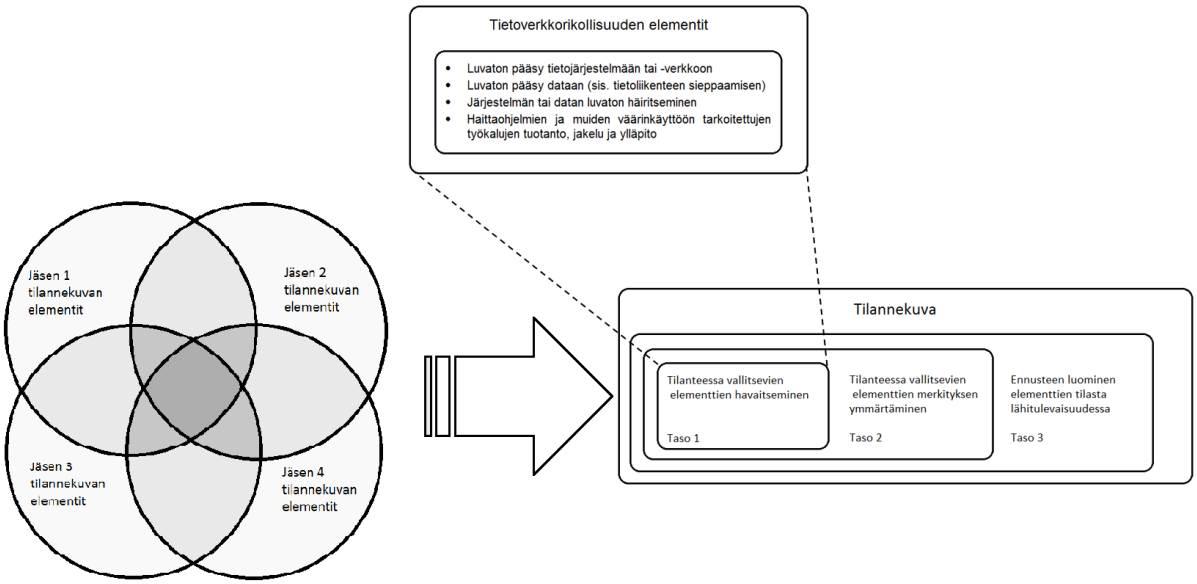
Gordon, Loeb ja Lucyshyn (2003) ovat tutkineet erilaisiin tietoturvauhkiin liittyvien tietojen jakamisen taloudellisia vaikutuksia luottamusverkostoissa. He ovat osoittaneet tutkimuksessaan, että tietojen jakaminen tarjoaa mahdollisuuden laskea kaikkien toimintaan osallistuvien tahojen kustannuksia. Kun erilaisiin hyökkäyksiin liittyviä tietoja jaetaan, on jokaisella toimijalla mahdollisuus kehittää omaa puolustuskykyään ja välttää hyökkäysten aiheuttamia vahinkoja. Yksittäisten toimijoiden puolustuskyvyn kasvaessa on todennäköistä, että yhä uusia hyökkäyksiä havaitaan ja pystytään torjumaan, mikä parhaassa tapauksessa johtaa kasvavaan tietojen vaihtoon ja kaikkien verkoston toimijoiden puolustuskyvyn kehittymiseen. Taloudelliset kannustimet yksityiskohtaisten ja totuudenmukaisten tietojen jakamiseen kiihdyttäisivät tietojenvaihtoa entisestään (Gordon, Loeb & Lucyshyn 2003; Gal-Or & Ghose 2005).

Gordon, Loeb ja Lucyshyn (2003) mukaan tietojen jakamisessa on kuitenkin myös omat haasteensa, sillä toimijat ovat usein huolissaan siitä, että antavat muille toimijoille kilpailuetua tai vahingoittavat omaa mainettaan paljastaessaan muille tietoturvauhkiin liittyviä tietoja. Lisäksi luottamusverkoston toimijoilla on taloudellinen kannustin pysyä tietojen jakajan sijasta puhtaasti vastaanottavana osapuolena hyötyen siitä, että muut verkoston toimijat ovat kehittäneet kyvyn havaita erilaisia hyökkäyksiä. Luottamusverkoston vapaamatkustajat voivat tällöin kehittää omaa toimintaansa, mutta eivät auta muita verkoston jäseniä niiden toiminnassa. Jos verkoston toimijat yrittävät vain hyötyä yhteistyöstä muiden kustannuksella, kaikki tietojen jakamisen hyödyt menetetään (Gordon, Loeb & Lucyshyn, 2003).

Myös tiedon jakamisen ja tietoturvainvestointien suhdetta tutkinut Kjell Hausken (2007) tunnistaa vapaamatkustajailmiön ja pitää sitä syynä miksi tiedonvaihto ei useinkaan onnistu. Tutkimuksessaan hän esittää, että luottamusverkoston jäsenillä tulisi olla pelkän kilpailuasetelman lisäksi myös jonkinasteinen riippuvuussuhde toisistaan. Vapaamatkustaja -ilmiön välttämiseksi ja tiedon vaihdon lisäämiseksi jäsenillä tulisikin olla kokemus samasta kohtalosta ja yhteisestä tehtävästä, jolloin luottamus toisiin jäseniin lisääntyy. Luottamuksen syvyys verkoston toisiin jäseniin puolestaan vaikuttaa siihen miten hyödyllisenä yhteistyö koetaan (Majchrzak & Järvenpää 2010). Hausken (2007) kannustaakin eri toimijoita keräämään, luokittelemaan ja jakamaan tietoa luottamusverkostoissa, mutta huomauttaa että toimijoiden välisen riippuvuussuhteiden tunnistaminen ja korostaminen ovat avaimia onnistumiseen.

Luvussa 2 on käsitelty kyberrikollisuutta ilmiönä ja luotu tutkimuksen tarpeisiin soveltuva määritelmä tietoverkkorikollisuudelle sekä käsitelty niitä tunnuspiirteitä, jotka ovat tyypillisiä nimenomaisesti tälle kyberrikollisuuden muodolle. Luvussa on lisäksi selvennetty tilannetietoisuuden käsitettä ja käsitelty sen merkitystä päätöksenteossa osoittaen, miten tilannetietoisuutta tietoverkkorikollisuudesta voidaan rakentaa sen elementtejä havainnoimalla.

Tilannetietoisuus tulisi rakentaa tietoverkkorikollisuuden elementeistä, eli tunnuspiirteistä, joita ovat luvaton pääsy tietoverkkoon, -järjestelmään tai dataan, tietoverkon tai -järjestelmän häiritseminen tai haittaohjelmien ja muiden väärinkäyttöön tarkoitettujen työkalujen tuotantoon, jakeluun ja ylläpitoon liittyvät toimet. Tilannetietoisuus muodostuu portaittain kasvavasta tietoisuuden tilasta, jossa luottamusverkoston toimijat pyrkivät kukin tahollaan havaitsemaan tietoverkkorikollisuuden elementtejä juuri heille saatavilla olevasta datasta. Havainnot jaetaan, jonka jälkeen kattavampaa tason 1 tilannetietoisuutta tulkitaan yhdessä tai erikseen systeemin kyvykkyyksien rajoissa. Näin on mahdollistaa muodostaa kattavampi ymmärrys siitä, mitä tietyllä hetkellä tapahtuu, kuin mihin yksikään toimija pystyisi itsenäisesti. Paremman ymmärryksen perusteella toimijat voivat kukin muodostaa ennusteen siitä, mitä seuraavaksi tulee tapahtumaan ja miten heidän tulisi siihen reagoida. Tilannetietoisuuden saavuttaminen ei tällöin ole itseisarvo, vaan sen avulla pystytään parempaan päätöksentekoon ja tarpeellisiin toimenpiteisiin. Kuvioon 6 on koottu oleelliset tässä luvussa esitetyt mallit tietoverkkorikollisuuden tilannetietoisuuden jakamiseen liittyen



KUVIO 6 Tietoverkkorikollisuuden tilannetietoisuuden jakaminen luottamusverkostossa

Kirjallisuuskatsauksen perusteella tietoverkkorikollisuuden tilannetietoisuuden jakamiseen luottamusverkostossa liittyy monia haasteita. Aikaisemman tutkimuksen valossa on myös esitetty, että onnistuessaan tehokkaalla tietojen vaihdolla voi olla positiivinen vaikutus tietoverkkorikosten havaitsemiseen ja torjuntaan. Ennen luottamusverkoston toiminnan syvällisempää tarkastelua, tutustutaan, miten tutkimuksen empiiristä aineistoa lähestytään. Seuraavassa luvussa esitellään tämän työn tutkimusasetelma.

3 Tutkimusasetelma

Tässä luvussa kuvataan tutkimusongelmien, -menetelmien ja aineiston muodostama kokonaisuus. Ensimmäisessä alaluvussa kuvataan mitä työssä tutkitaan, mihin kysymyksiin tutkimuksella halutaan vastata sekä mihin aineistoon tutkimus perustuu. Lisäksi alaluvussa on kerrottu tutkimuksen rajaukset. Toisessa alaluvussa on puolestaan kerrottu, millaisin metodologisin valinnoin tutkimusongelmaa lähestytään, millä tavalla tutkimuksen empiirinen aineisto on kerätty sekä millä formaalilla menetelmällä aineistoa on käsitelty.

3.1 Tutkimusongelma

Franke ja Brynielsson (2014) mukaan kybertilannetietoisuuden tutkimuksessa on keskitytty erityisesti teollisen automaation valvomojärjestelmien tilannekuvan, datafuusion sekä tilannekuvan muodostamiseen käytettävien algoritmien tarkasteluun. Tutkimus on pääasiassa ollut hyvin teoreettista ja empiiriset tutkimustulokset loistavat poissaolollaan. Sen sijaan kybertilannetietoisuuden jakamiseen liittyvä tutkimus on jäänyt akateemisissa piireissä selvästi vähemmälle huomiolle, samoin kuin kansallisen kybertilannetietoisuuden muodostaminen, vaikka jälkimmäinen on useassa valtiollisessa kyberstrategiassakin mainittu tavoite (Franke & Brynielsson, 2014).

Tilannetietoisuuden kehittäminen on mainittu tavoitteena sekä Suomen kyberturvallisuusstrategiassa (2013) että Pääministeri Juha Sipilän hallitusohjelmassa (2015), jossa sisäisen turvallisuuden tavoitteiksi mainitaan muun muassa yhteisen tilannekuvan luominen tietoverkkojen ja tietoliikenteen turvallisuudesta sekä luotettavan ja turvallisen tietojen vaihdon varmistaminen eri toimijoiden välillä. Tietoverkkorikollisuus vaikuttaa suoraan tietoverkkojen ja tietoliikenteen turvallisuuteen ja sen ehkäisyyn tarvitaan yhtenäistä tietoisuutta ongelman laajuudesta. Tietoverkkorikollisuuden tilannetietoisuus onkin yksi osa-alue yhteisen kansallisen kyberturvallisuuden tilannetietoisuuden luomisessa (Leppänen ym. 2016). Äskettäin julkaistussa Suomen kyberturvallisuusstrategian toimeenpano-ohjelmassa vuosille 2017 – 2020 on linjattu, että kyberrikostorjunnan edellytysten varmistamiseksi:

> Sisäministeriö huolehtii siitä, että poliisilla ja muilla viranomaisilla on hyvät edellytykset ennalta estää, paljastaa ja selvittää kyberrikollisuutta. Tietoverkkorikollisuuden tilannekuvaa ja tietojen vaihtoa kehitetään viranomaisten yhteisen tilannetietoisuuden parantamiseksi sekä yksityisen sektorin toimijoiden paremman varautumisen turvaamiseksi (Turvallisuuskomitea 2017, 14).

Leppänen ym. (2016) ovat esittäneet, että yksi keino muodostaa nykyistä parempaa tilannetietoisuutta tietoverkkorikollisuuden tilasta, olisi kehittää tietojenvaihtoa tietoturvayritysten ja viranomaisten kesken. Tämä pro gradu -työ

pyrkii selvittämään, mistä havainnoista tuo tilannetietoisuus tulisi rakentaa ja miten tietojen vaihto luottamusverkossa tulisi järjestää. Työn lähtökohtana on moniulotteinen ongelmalliseksi koettu tilanne, johon liittyy sosiaalisesti haastavia piirteitä eri intressiryhmien välillä. Tutkimuksen avulla pyritään selkeyttämään tilannetta ja luomaan tulevaisuuden yhteistyölle suuntaviivoja vastaamalla seuraavassa alaluvussa esitettyihin kysymyksiin.

3.1.1 Tutkimuskysymykset

Jotta tietoverkkorikollisuuden tilannetietoisuuden muodostaminen ja jakaminen luottamusverkostossa tuottaisi selkeitä hyötyjä kaikille verkoston toimijoille, pyrkii tutkimus vastaamaan kahteen pääkysymykseen:

1. **Mistä tiedoista tietoverkkorikollisuuden tilannetietoisuus kannattaa muodostaa?**

   Tutkimuksessa analysoidaan kirjallisuuskatsauksen perusteella kyberrikollisuutta ilmiönä sekä luodaan määritelmä tietoverkkorikollisuudelle. Tämän jälkeen tarkastellaan aikaisemman tutkimuksen pohjalta tilannetietoisuuden käsitettä sekä sen muodostamiseen ja jakamiseen liittyviä seikkoja. Lopuksi näiden perusteella rakennetaan malli, joka kuvaa, miten tietoverkkorikollisuuden tilannetietoisuus muodostuu luottamusverkostossa.

2. **Miten tilannetietoisuuden jakaminen kannattaa toteuttaa tutkimuksen kohteena olevassa luottamusverkostossa?**

   Tutkimuksen empiirisessä osassa haastatellaan tietoturvayritysten, keskusrikospoliisin kyberrikostorjuntakeskuksen sekä viestintäviraston kyberturvallisuuskeskuksen henkilöstöä. Tarkoituksena on selvittää millaista tietojenvaihtoa luottamusverkoston toimijat toivovat sekä, mitä haasteita he tunnistavat sekä mitkä asiat pitää ratkaista ennen kuin tietoja voidaan ryhtyä jakamaan. Lopuksi empiirisestä aineistosta koottuja havaintoja verrataan kirjallisuuskatsauksessa esille nousseisiin seikkoihin.

Vastausten odotetaan auttavan luottamusverkoston toiminnan organisoimisessa sekä toiminnan edellytysten ja siihen mahdollisesti liittyvien haasteiden tunnistamisessa. Parhaassa tapauksessa kehittyvän tilannetietoisuuden havaintojen pohjalta on mahdollista tunnistaa nykyistä tehokkaammin sellaisia rikosilmiöitä, jotka uhkaavat Suomalaista yrityskenttää ja kehittää ennakointi- ja reagointikykyä niiden torjumiseksi.

3.1.2 Tutkimusaiheen rajaukset

Tämä tutkimus koskee vain keskusrikospoliisin kyberrikostorjuntakeskuksen, viestintäviraston kyberturvallisuuskeskuksen ja tietoturvayritysten välistä luottamusverkostoa, eikä siinä käsitellä tiedon jakamista tämän verkoston ulkopuolelle tai muiden toimijoiden kesken. Tällä valinalla tutkimus on saatu kohdennettua tarkasti tutkittavaan ilmiöön sekä ongelmalliseksi koettuun tilanteeseen, joka on alun perin toiminut lähtölaukauksena tutkimukselle. Tutkimus keskittyy ainoastaan tietoverkkorikoksiin eikä ota kantaa muihin kyberrikollisuuden osa-alueisiin. Kyberrikollisuuden kenttä on laaja ja pitää sisällään keskenään niin erilaisia tekoja, ettei niitä kaikkia ole tarkoituksenmukaista tarkastella tässä tutkimuksessa. Lisäksi luottamus-verkoston toimijoiden kyky havaita tai puuttua muihin kuin tietoliikenneverkoissa ja -järjestelmissä esiintyviin rikoksiin on hyvin rajallinen. Vaikka tutkija näkee, että tutkimuksen tuloksilla voi olla positiivinen vaikutus kansallisen kybertilannetietoisuuden kehittämiseen, ei tutkimuksessa ole haluttu ottaa kantaa siihen, kenen toimesta, tai millä keinoin tietoverkkorikollisuuden tilannetietoisuus tulisi liittää osaksi laajempaa tilannetietoisuutta. Tähän ratkaisuun on päädytty, jotta kokonaisuus pysyy halittuna.

Tutkimuksessa on määritelty ne tietoverkkorikollisuuden piirteet, joita luottamusverkoston toimijoiden tulisi seurata. Tutkimuksessa ei ole kuitenkaan haluttu määritellä, miten havainnot tulisi tehdä. Verkoston toimijat hyödyntävät havaintoja tehdessään erilaisia teknologioita (ks. esim. Deylam, Muniyandi, Ardekani & Sarrafzadeh, 2016) sekä omia sosiaalisia verkostojaan. Näiden kartoittaminen tai listaaminen olisi helposti johtanut tilanteeseen, jossa tutkimuksen tuloksia ei olisi voinut raportoida osana julkista pro gradu tutkimusta. Havainnoinnin rajaaminen johonkin tiettyyn yksilöityyn tapaan olisi puolestaan turhaan sitonut tutkimuksen ajallisesti tietyn teknologian tai toimintamallin elinkaareen, jolloin siitä luovuttaessa tutkimus olisi menettänyt merkityksensä. Valittu tapa ei välttämättä olisi myöskään sopinut kaikille luottamusverkoston toimijoille. Lisäksi valitulla rajauksella tutkimus kestää paremmin aikaa, sillä vaikka uusia tietoverkkorikosten teko- kuin havainnointitapojakin keksitään jatkuvasti lisää, muodostuvat itse teot kuitenkin samoista elementeistä, jotka on määritelty tässä tutkimuksessa.

3.1.3 Tutkimusaineisto

Tutkimusongelman ja rajausten määrittelyn perusteella valittiin tutkimuksen tyypiksi laadullinen tutkimus. Tutkimuskysymykset *mistä* ja *miten* ohjasivat keräämään laadullisesti analysoitavan aineiston, joka on toiminut tutkijalle idealähteenä ja teoreettisen pohdiskelun katalysaattorina, kuten Anttila (2006, 184) määrittää. Aluksi kerättiin kirjallinen tutkimusaineisto, jonka avulla on rakennettu tutkimuksen teoreettinen viitekehys ja vastattu kysymykseen, mistä tiedoista tietoverkkorikollisuuden tilannetietoisuus kannattaa muodostaa? Tutkimus-kysymyksessä esiintyvät termit tietoverkkorikollisuus ja

tilannetietoisuus on analysoitu tarkasti aikaisemman tutkimuksen pohjalta. Aikaisempaa tutkimusta etsittiin yleisten hakukonekonepalveluiden avulla, sekä tekemällä kohdennettuja hakuja sähköisiin tieteellisiin tietokantoihin kuten Google scholar, IEEE Xplore, Science Direct sekä korkeakoulujen sähköisiin julkaisukokoelmiin kuten Doria. Sähköinen aineistohaku suoritettiin englanniksi termeillä ”situational awareness”, ”situation awareness”, ”cyber crime”, ”network crime”, ”information sharing”, ”information exchange” sekä termien eri yhdistelmillä ja käyttäen niiden suomenkielisiä vastineita. Tavoitteena oli löytää tietojenkäsittelyalan lehdissä sekä tieteellisissä konferensseissa julkaistuja tutkimusartikkeleita ja väitöskirjatasoisia tutkimuksia aineiston perustaksi.

Vaikka tieteellisissä lehdissä julkaistuja artikkeleja pidetään yleisesti konferenssijulkaisuja korkealaatuisempina, on tähän tutkimukseen hyväksytty myös konferenssijulkaisuja, sillä niiden joukosta löytyi aihepiiriä käsittelevää tutkimusta enemmän kuin alan lehdistä. Tutkimuksen lähteeksi on hyväksytty myös esimerkiksi FT, everstiluutnantti evp. Rauno Kuusiston väitöskirjatutkimus sekä sitä seurannut Liikenne- ja viestintäministeriön tilaama selvitys, sillä molemmat kuvaavat erinomaisesti tutkimuksen aihepiiriin liittyvien käsitteiden monitulkintaisuutta suomen kielessä. Tutkimusta taustoittavassa kyberrikollisuuden ilmiön sekä tietoverkkorikollisuuden piirteiden kuvailemisessa on tukeuduttu vahvasti sekä Europolin, että Yhdistyneiden kansakuntien huumeiden ja rikollisuuden torjunnasta vastaavan toimiston raportteihin, sillä niitä käytettiin useissa muissa julkaisuissa primäärilähteinä. Lisäksi tutkimuksessa on käytetty lähdeaineistona esimerkiksi Valtioneuvoston kanslian julkaisusarjan selvityksiä. Näitä selvityksiä on käytetty pääasiassa vain ohjaamaan tutkimuksessa tehtyjä valintoja tai rajauksia sekä kuvaamaan aihepiiriin liittyviä ajankohtaisia ilmiöitä suomalaisessa kontekstissa.

Kirjallisuuskatsauksen lisäksi tutkimuksessa on kerätty empiirinen haastatteluaineisto, jonka pohjalta koottuja havaintoja on verrattu kirjallisuuskatsauksessa esille nousseisiin seikkoihin. Aineisto on kerätty haastattelemalla henkilöstöä kahdesta eri tietoturva-alan yrityksestä, keskusrikospoliisin kyberrikostorjuntakeskuksesta sekä viestintäviraston kyberturvallisuuskeskuksesta. Haastatteluja tehtiin yhdeksän kappaletta ja ne suoritettiin maalis-huhtikuussa 2017. Vastaajista viisi oli virkamiehiä ja neljä edusti kahta eri yritystä. Eri intressiryhmien toiveiden ja tarpeiden kartoittamiseksi vastaajiksi valittiin henkilöitä vaihtelevalla taustalla aina liiketoiminta-alueiden johtajista, yksikön- tai tiimin vetäjistä, eri osaamisalueiden erikoisasiantuntijoihin sekä teknisiin asiantuntijoihin. Haastattelukysymykset on esitetty liitteessä 1. Haastattelukysymykset keskittyivät ryhmän työskentelyn kehittämisen sekä eri intressiryhmien tarpeiden kartoittamisen ympärille. Lisäksi haastattelun avulla pyrittiin kartoittamaan niin tietojenvaihdon nykytilaa kuin tulevaisuuden tavoitteita luottamusverkoston työskentelylle. Haastatteluaineiston avulla tutkimus saatiin kohdistettua juuri kyseiseen ryhmään sekä sen ominaispiirteisiin, mikä ei olisi

ollut mahdollista muutoin kuin keräämällä aineisto itse. Haastatteluaineisto kerättiin noudattaen tutkimusstrategiaa, joka on kuvattu seuraavassa alaluvussa.

3.2 Tutkimusstrategia

Tutkimusongelman taustalla on ongelmalliseksi koettu tilanne; tietojen vaihtoon ryhtymistä on suositeltu ja tietojen vaihtoon osallistuvat tahot ovat selvillä, mutta osapuolilla ei ole yhteistä näkemystä siitä, mihin suuntaan toimintaa tulisi kehittää. Tällaiset sosiaalisesti moniulotteiset ja vaikeasti määriteltävät ongelmalliseksi koetut tilanteet ovat tyypillisiä lähtöpisteitä tutkimukselle, jossa hyödynnetään ns. pehmeitä menetelmiä. Ongelman pehmeys viittaa sosiaalisten, monimutkaisten tilanteiden selvittämiseen, jossa ratkaisu ei ole ennalta määrätty. ”Pehmeillä menetelmillä voidaan tietojenkäsittelytieteissä etsiä vastauksia esimerkiksi kysymyksiin mitkä ovat järjestelmän ominaisuudet, voiko sitä kehittää ja jos, niin miten?” (Checkland & Poulter, 2006, 149).

Tutkimusmenetelmäksi valittiin toimintatutkimus, jossa empiirisen osuuden muodostaa puolistrukturoidun haastattelun avulla kerättävä tutkimusaineisto, joka analysoidaan pehmeän systeemimetodologian avulla. Tutkimusmenetelmän valintaa ohjasi pitkälti metodologiavalinta, joka vaikutti sopivalta tämän pro gradu -työn tutkimusasetelmaan. Alustavan valinnan jälkeen pehmeää systeemimetodologiaa, sen edellyttämää tutkimusmenetelmää sekä niitä taustoittavaa fenomenologista tieteen filosofiaa verrattiin perinteisempiin systeemiteoreettisiin suuntauksiin. Koska alustavasta katsauksessa ei löytynyt soveltuvampaa lähestymistapaa valittuun tutkimusongelmaan, valittiin tutkimusmenetelmäksi toimintatutkimus.

Toimintatutkimus (*action research*) sopii menetelmänä erinomaisesti tähän tutkimukseen, sillä se on Anttilan (2006) mukaan tutkimusmenetelmä, jonka tarkoituksena on vaikuttaa tutkimuskohteeseen, sen toimintaan tai ympäristöön sitä kehittävästi tai parantavasti. Toimintatutkimus kohdistuu tiettyyn erityistapaukseen ja sen sijaan, että menetelmän avulla etsittäisiin yleistettävää tietoa, on sen tavoitteena saada täsmällistä tietoa tiettyä tilannetta ja tarkoitusta varten. Toimintatutkimuksen tarkoituksen on kehittää uutta lähestymistapaa tiettyyn asiaan ja ratkaista niitä ongelmia, joilla on suora yhteys johonkin käytännönläheiseen toimintaan. Lähestymistapana se soveltuu parhaiten tilanteisiin, joissa ollaan kiinnostuneita jonkun käytännön hankkeen käynnistämisestä, sen sujumisesta tai siitä, miten yhteistyö eri toimijoiden välillä sujuu tai mitä seikkoja tulee ottaa huomioon (Anttila, 2006).

Toimintatutkimuksen valitsemiseen tutkimusmenetelmäksi vaikutti myös tutkijan henkilökohtainen mahdollisuus osallistua yhteistyöryhmän toiminnan kehittämiseen tämän opinnäytetyöprosessin ja sen tulosten perusteella. Tutkimusmenetelmän käyttö edellytti sellaista aineistoa, joka kuvaa tutkimuksen kohteena olevan yhteistyöryhmän toimintaa. Tällaista aineistoa ei ollut olemassa, vaan se täytyi koota tutkimusta varten. Käytännön yhteistyöhön ja sen koordinoimiseen osallistuvat ihmiset otettiin osallisiksi tutkimukseen

kartoittamalla heidän näkemyksiään ongelmalliseksi koetusta tilanteesta ja samalla tutkija pääsi itse tekemään havaintoja ryhmän toimintaan vaikuttavista poliittisista valtasuhteista ja sosiaalisista jännitteistä sekä näihin liittyvistä ennakkoasetelmista.

Toimintatutkimusta on epistemologisessa eli tieto-opillisessa tarkastelussa kritisoitu etenkin toistettavuuden puutteesta, sillä mikään sosiaalinen tilanne ei toistu kahta kertaa samanlaisena ja siksi tietyn raportoidun toimintatutkimuksen uusiminen voi osoittautua erittäin haasteelliseksi. Toimintatutkimuksen avulla kerättyjen havaintojen perusteella saavutettu tieto voidaan asettaa kyseenalaiseksi kritisoimalla tiedon alkuperää ja sen pätevyyttä (Anttila, 2006). Jos tutkimusta ei voida toistaa, tai uudella tutkimuksella ei päästä samoihin tuloksiin, miten tiedon alkuperää ja pätevyyttä sekä tutkimuksen arvoa ylipäätään voidaan arvioida? Toimintatutkimuksen tekemisessä korostuukin Checkland & Poulter (2006) mukaan sen metodologisen viitekehyksen määrittely, jonka avulla tutkimus on toteutettu. Tämän toimintatutkimuksen viitekehyksen muodostaa pehmeä systeemimetodologia, joka tarjoaa tarkasti määritellyn formaalin rakenteen, sekä yhdenmukaisen termistön, jota on käytetty puolistrukturoitujen asiantuntijahaastatteluiden avulla kerätyn aineiston käsittelyyn ja johtopäätösten tekemiseen. Tutkimus ja sen eteneminen on pyritty kuvamaan tarkasti, jotta se olisi mahdollisimman hyvin toistettavissa.

3.2.1 Puolistrukturoitu asiantuntijahaastattelu

Anttilan (2006) mukaan asiantuntijahaastatteluissa haastateltavat ovat koulutettuja alansa asiantuntijoita, joilla on asemansa perusteella mahdollisuus antaa tietoa esimerkiksi tutkittavaan ilmiöön liittyvistä laajoista kysymyksistä, ilmiön historiallisesta kehityksestä sekä tulevaisuuden suuntaviivoista. Haastateltavat valitaan erityisesti tutkittavaa ilmiötä silmällä pitäen ja haastattelun avulla on tarkoitus koota heidän hallussaan oleva erikoistietämys. Kuten teemahaastattelu, myös puolistrukturoitu haastattelu etenee siten, että kaikille haastateltaville esitetään samat tai likipitäen samat kysymykset samassa järjestyksessä. Puolistrukturoitu haastattelu sopii erityisesti tilanteisiin, joissa on päätetty haluttavan tietoa juuri tutkittavasta kohteesta, eikä haastateltaville haluta antaa kovin suuria vapauksia haastattelutilanteessa (Anttila, 2006; Hirsjärvi, Remes, & Sajavaara, 2009).

Puolistrukturoituun haastattelumalliin päädyttiin, jotta haastattelun kulkua pystyttiin ohjaamaan systemaattisesti ja jotta kaikki oleelliset aihepiirit saatiin kartoitettua. Puolistrukturoitu haastattelu mahdollisti vastausten vertailemisen keskenään tehokkaammin kuin mitä olisi ollut mahdollista täysin avoimessa haastattelussa. Vastaukset haluttiin kuitenkin pitää avoimina, jotta tutkija ei johdattaisi vastauksia tiettyyn suuntaan ennalta määritetyillä vastausvaihtoehdoilla. Tästä syystä strukturoitu haastattelu suljettiin pois mahdollisena aineistonkeruumenetelmänä. Puolistrukturoidut haastattelut suoritettiin kasvotusten, nauhoitettiin ja litteroitiin. Puhtaaksi kirjoitettua haastatteluaineistoa on lähestytty systeemimetodologian näkökulmasta, jolle on

tyypillistä, että muutostoimintaan osallistuvat, tai sen kohteena olevat henkilöt työskentelevät yhdessä ongelmanratkaisutilanteessa. Tällainen tilanne haluttiin kuitenkin välttää asiantuntijahaastatteluissa, jotta muiden henkilöiden, esimerkiksi oman esimiehen, viranomaisen tai kilpailijan edustajan läsnäolo ei vaikuttanut haastateltavien vastauksiin. Asiantuntijoille haluttiin lisäksi taata anonymiteetti, jotta he pystyivät vastaamaan kysymyksiin rehellisesti pelkäämättä vastustensa seurauksia. Haastatteluaineiston käsittelyyn sekä siihen valitun lähestymistavan ominaispiirteisiin paneudutaan tarkemmin seuraavassa alaluvussa**.**

3.2.2 Pehmeän systeemimetodologian perusteet

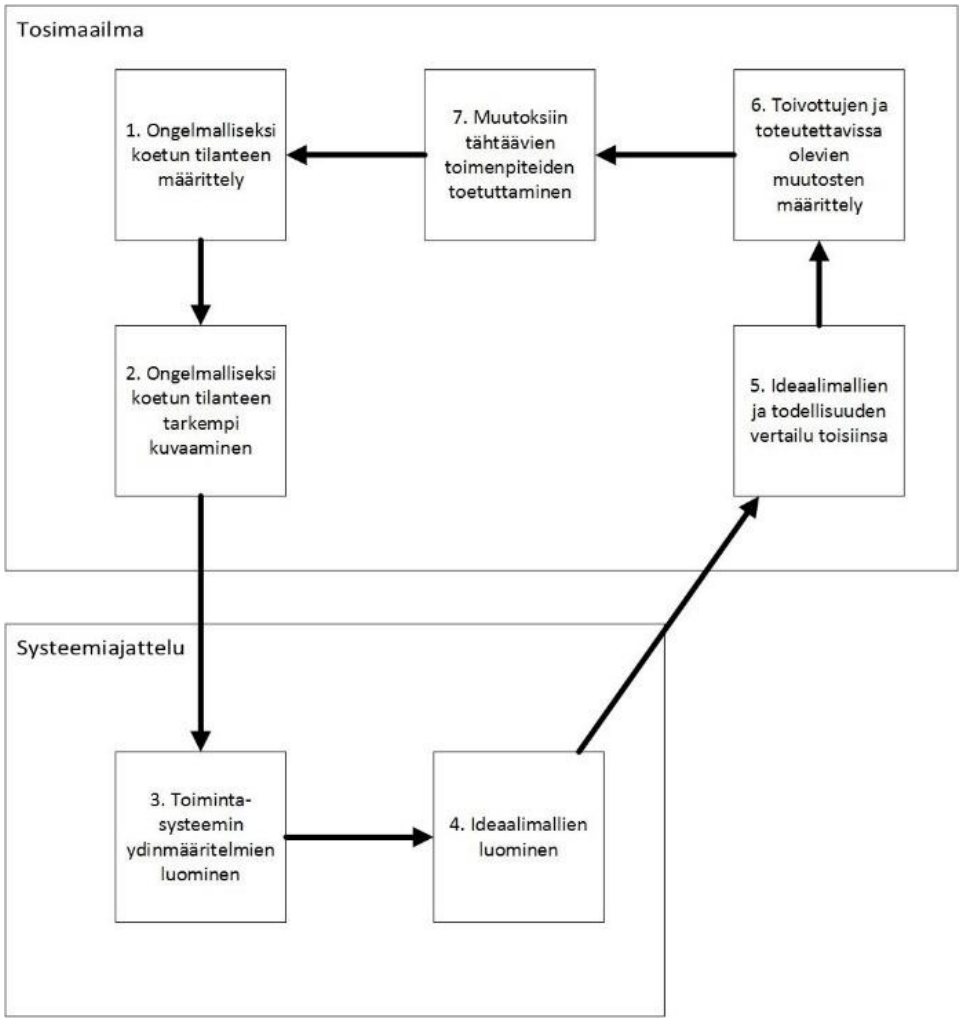
Pehmeä systeemimetodologia (*Soft Systems Methodology*) on Peter Checklandin kehittämä järjestelmällinen, toimintasuuntautunut tapa kohdata monimutkaisia ongelmalliseksi koettuja sosiaalisia tilanteita. Sen avulla voidaan muodostaa määrämuotoinen ajatteluprosessi siten, että kehitystoimintaan voidaan ryhtyä järjestelmällisesti. Metodologian ensimmäinen versio syntyi vuonna 1972 ja se julkaistiin vaihtoehtona silloisille systeemiteoreettisille suuntauksille, joiden Checkland ei kokenut olevan tarpeeksi joustavia vastaamaan tosielämän monimutkaisia ongelmanratkaisutilanteisiin. Systeemisuunnittelulle tyypillistä oli määritellä tarkka tarve ja suunnitella siihen tekninen ratkaisu. Tämä ”kova” lähestymistapa ei Checklandin mielestä kuitenkaan taipunut erilaisiin menettelytapoihin liittyviin ongelmatilanteisiin, joissa piti määritellä *mitä* tulisi tehdä tai *miten* jokin asia tulisi ratkaista (Checkland & Poulter, 2006).

Kovat systeemiteoreettiset suuntaukset pohjautuvat positivistiseen ontologiaan ja niiden mukaan maailma paljastuu tarkkailijalle sellaisena kuin se on, sisältäen erilaisia tosimaailman ilmiöitä. Pehmeä systeemimetodologia tukeutuu puolestaan fenomenologiseen suuntaukseen, jossa hyväksytään tosimaailman ilmiöiden lisäksi myös kokemusmaailman ilmiöt todellisiksi. Checklandin (1981) mukaan pehmeässä systeemimetodologiassa tarkasteltava kohde ymmärretään ja kuvataan systeeminä eli kokonaisuutena, jolle voi määritellä tunnistettavat rajat, tekijät ja toimijat sekä niiden väliset vuorovaikutussuhteet. Ihmisten tai ihmisryhmien ei ajatella olevan todelliselta olemukseltaan systeemejä, vaan niiden katsotaan muodostavan ihmisten kehittämiä toimintasysteemejä, joihin tieteellistä päättelyä ja systeemiajattelua voidaan soveltaa. Nämä toimintasysteemit ovat luonteeltaan aineettomia, mutta niiden voidaan katsoa muodostavan selkeästi havaittavan sarjan erilaisia toimintoja, jotka pyrkivät jonkun tiedostetun tai tiedostamattoman mission tai tehtävän suorittamiseen. Ihmisten kokemusmaailmoista riippuen myös erilaiset kokemukset toiminnan tarkoituksesta tai odotukset sen toivotuista tuloksista hyväksytään tosiksi, eikä systeemillä välttämättä katsota olevan yhtä selkeää tehtävää (Checkland 1981; Checkland & Scholes 1990).

Käsitys systeemeistä kokemusmaailman ilmiöinä erottaa pehmeän systeemimetodologian kovista systeemiteoreettisista suuntauksista, joissa systeemit ymmärretään tosimaailman olioiksi. Pehmeän systeemiajattelun

suurena etuna voidaan pitää sitä, että ongelmallisiksi koettuja tilanteita sekä niissä vaikeasti määriteltäviä osa-alueita voidaan jäsentää osakokonaisuuksiksi ja käsitellä organisoidulla tavalla. Tällöin voidaan Checklandin (1981) mukaan parhaassa tapauksessa saavuttaa sellainen ratkaisu, joka on sisällöllisesti enemmän kuin pelkkä tekninen, toimintaa kuvaava malli. Tämän eron ansiosta pehmeä systeemimetodologia onkin parhaimmillaan kaoottisissa ja komplekseissa ongelmatilanteissa, joissa tutkitaan ja analysoidaan esimerkiksi tietyn inhimillisen toimintasysteemin toimintaa. Kun toimintasysteemiä tarkastellaan pehmeän systeemiajattelun näkökulmasta, voidaan vuorovaikutuksesta niin systeemin sisällä kuin sen ulkopuolellakin saada uudenlaista tietoa, joka ei pelkästään auta ymmärtämään toimintaa, vaan myös muuttamaan ja kehittämään sitä (Checkland 1981).

Checklandin (1981) mukaan pehmeä systeemimetodologia rakentuu seitsemästä eri vaiheesta, joista ensimmäisessä (interventioanalyysi) määritellään ongelmalliseksi koettu tilanne, kuvataan tutkittava ilmiö ja tunnistetaan tarve tai halu kehittää tilannetta. Toisessa vaiheessa tilanne kuvataan tarkemmin ja siihen vaikkutavat sosiaaliset jännitteet (analyysi kaksi) sekä poliittiset valtasuhteet (analyysi kolme) pyritään määrittämään. Tämän perusteella tehdään kolmannessa vaiheessa toimintasysteemin analyysi CATWOE-prosessin avulla ja luodaan ydinmääritelmä siitä, mitä tutkittava systeemi voisi tulevaisuudessa olla. Tässä vaiheessa pureudutaan ihmisten kokemusmaailmoihin ja maailmankuvaan siitä, millaisena he tarkasteltavan systeemin näkevät. Ydinmääritelmän perusteella luodaan neljännessä vaiheessa ideaalimalli, joka kuvaa sen millaisista toiminnoista ja toimintaprosesseista toimintasysteemi voisi koostua. Viidennessä vaiheessa ideaalimallia ja todellisuutta verrataan toisiinsa, minkä jälkeen kuudennessa vaiheessa määritellään toivotut ja toteutettavissa olevat muutokset olemassa olevaan systeemiin. Seitsemäs vaihe pitää sisällään muutokseen tähtäävien toimenpiteiden toteuttamisen. Pehmeän systeemimetodologian perusmalli on esitetty kuviossa 7 (Checkland, 1981; Checkland & Scholes, 1990; Checkland & Poulter, 2006).



KUVIO 7 Pehmeän systeemimetodologian perusmalli (Checkland 1981, 163, muokattu)

Anita Rubinin (2005) mukaan tutkijat ovat kritisoineet pehmeää systeemimetodologiaa mm. siitä, ettei sen avulla voi varsinaisesti rakentaa systeemiä. Lisäksi kritiikkiä on suunnattu metodologian peruslähtökohtaan, jonka mukaan kaikilla toimintasysteemin jäsenillä on samanlainen mahdollisuus valita ja vaikuttaa toiminnan kehittämiseen ja systeemin muutokseen. Tämä ei useinkaan pidä paikkaansa esimerkiksi organisaatoissa, sillä yleensä kehityksen avaimet ovat tiukasti tiettyjen henkilöiden käsissä. Pehmeä systeemimetodologia soveltuukin suunnittelua paremmin systeemien ymmärtämiseen, analysoimiseen ja kehittämiseen. Pehmeän systeemimetodologian lopputulos onkin Checklandin (1981, 17) mukaan hyvin erilainen kovan systeemisuunnittelun lopputuloksista. Kyseessä on oppimisprosessi, joka johtaa päätökseen ryhtyä tiettyihin toimenpiteisiin, joiden ymmärretään ongelmallisen tilanteen ratkaisemisen sijasta johtavan tilanteen kehittymiseen sekä uuden oppimiseen. Tälle oppimisprosessille tyypillistä on syklisyys ja pehmeä systeemimetodologia tuottaakin lopputuotoksia paremmin prosessituloksia

auttamalla toimijoita jäsentämään suunnittelun, toiminnan ja merkityksenannon vaiheita.

3.2.3 Pehmeän systeemimetodologian soveltaminen tutkimuksessa

Tässä tutkimuksessa on yritetty eliminoida osa pehmeään systeemimetodologiaan kohdistuvasta kritiikistä haastattelemalla asiantuntijoita henkilökohtaisesti ulkopuolisen tutkijan toimesta, jolloin muiden henkilöiden läsnäolo ei voi vaikuttaa haitallisesti haastateltavien vastauksiin. Jokaiselle haastatteluun suostuneelle henkilölle on taattu yhtäläiset mahdollisuudet osallistua kehitystoimintaan ja annettu mahdollisuus vastata kysymyksiin rehellisesti ilman, että heidän tarvitsee pelätä vastustensa seurauksia kilpailijoiden ja/tai omien esimiestensä läsnä ollessa. Tällaisessa lähestymistavassa voi Rubinin (2005) mukaan olla riskinä, että tutkijalla itsellään on valmiina ideaalimalli, jonka hän prosessin aikana pala kerrallaan syöttää osanottajille jättäen heille kuvan, että he itse ovat tuottaneet uusia ideoita ja muutosehdotuksia. Samanaikaisesti riskinä on hänen mukaansa myös se, että prosessin myötä toimintasysteemiin yritetään tuoda sen ulkopuolelta sen toimintaan kuulumattomia arvoja ja toimintatapoja. Näihin riskeihin on otettu kantaa tutkimuksen pohdinta -osiossa (ks. luku 6).

Tutkimuksen lähtötilanteessa on tietoverkkorikollisuuden tilannetietoisuuden jakaminen määritelty ongelmalliseksi tilanteeksi, jota halutaan kehittää osallistamalla tietoturvayritykset tietojenvaihtoon viranomaisten kanssa suljetussa luottamusverkostossa. Haasteena tilanteessa on ollut, että eri intressiryhmillä on erilaisia tarpeita tilannetietoisuuden kokoamiseen ja sen jakamiseen liittyen sekä yhteistyön tulevaisuuden suuntaviivoihin nähden. Lähtötilanne on tyypillinen monimutkaiseksi ja ongelmalliseksi koettu kokonaisuus, jota voidaan lähestyä pehmeän systeemimetodologian tarjoaman syklisen oppimisprosessin avulla. Tutkimuksessa luottamusverkoston toimijoiden katsotaan muodostavan toimintasysteemin ja olevan vuorovaikutuksessa keskenään. Kirjallisuuskatsauksen perusteella esioletuksena on, että yhteistyö ja tietojenvaihto verkoston sisällä koetaan ongelmalliseksi. Lisäksi tutkija olettaa, että yhteistyötä tiivistämällä on saatavissa sellaisia etuja, jotka hyödyttävät kaikkia luottamusverkoston eri toimijoita.

Päätös ryhtyä tutkimusprojektiin muodostaa pehmeän systeemimetodologian ensimmäisen vaiheen (interventioanalyysi), jossa pyritään kartoittamaan lähtötilannetta ja tunnistamaan toimintasysteemin omistaja, asiakkaat sekä itse toimintaan osallistuvat tahot. Tämä kokonaisuus on kuvattu alaluvussa 4.1. Metodologian toisessa vaiheessa ongelmalliseksi koettu tilanne kuvataan ja määritellään tarkemmin. Metodologian toista vaihetta edustaa tässä tutkimuksessa kokonaisuudessaan luku 2, jossa on muodostettu teoreettinen viitekehys tutkimukselle ja kuvattu niitä seikkoja, jotka vaikuttavat tietojen vaihtoon luottamusverkoston kesken. Analyysit 1, 2 ja 3 (interventioanalyysi sekä sosiaalisten ja poliittisten suhteiden analyysi)

perustuvat kerätyn haastatteluaineiston lisäksi tutkijan havaintoihin haastattelutilanteissa (ks. alaluku 4.1). Toimintasysteemin analyysi on suoritettu haastatteluaineistosta CATWOE-prosessin avulla, jonka jälkeen on luotu ydinmääritelmät siitä, mitä haastateltavan maailmankuvan mukaan tutkittava systeemi voisi tulevaisuudessa olla (ks. alaluku 4.3). Tämän jälkeen luvussa 4.4 on luotu systeemin toiminnalle ideaalimalli, joita on verrattu todellisuuteen luvussa.

Tutkimuksessa muodostetut ydinmääritelmät sekä ideaalimalli perustuvat tutkijan omiin tulkintoihin haastatteluaineistosta sekä kerätyn aineiston reflektointiin. Alaluvussa 4.4 nojaudutaan kirjallisuuskatsauksessa esille nousseiden huomioiden ja ideaalimallien vertailuun, sillä tämän hetken yhteistyömallien kuvaaminen yksityiskohtaisesti ei olisi mahdollista osana julkista opinnäytetyöprosessia. Toivotut ja toteutettavissa olevat muutosehdotukset on esitetty tutkimuksen johtopäätöksissä luvussa 5. Tutkimuksen perusteella mahdollisesti käynnistyvät toimenpiteet muodostavat metodologian viimeisen vaiheen, jonka avulla toimintaa on mahdollista kehittää.

Tässä luvussa on käsitelty tutkimusongelmaa, sen rajauksia, sekä valittua tutkimusstrategiaa. Tietoverkkorikollisuuden tilannetietoisuuden jakaminen luottamusverkostossa muodostaa niin monimutkaisen kokonaisuuden, että tutkimuskysymyksiin: *Mistä tiedoista tietoverkkorikollisuuden tilannetietoisuus kannattaa rakentaa?* ja *Miten tilannetietoisuuden jakaminen kannattaa toteuttaa?* vastaaminen kovan systeemiajattelun keinoin, olisi ollut erityisen haastavaa. Tämä olisi edellyttänyt myös sitä, että ennen tutkimusprosessiin ryhtymistä olisi ollut selvää, mitä tilannetietoisuudella tarkoitetaan ja miten yhteistyö halutaan käynnistää. Tällöin olisi ollut mahdollista suunnitella systeemi, jonka avulla tilannetietoisuuden jakaminen olisi voitu toteuttaa. Koska nämä ennakkoasetelmat eivät kuitenkaan toteutuneet, tarvittiin joustava lähestymistapa, jonka avulla on mahdollista muodostaa määrämuotoinen ajatteluprosessi siten, että kehitystoimintaan oli mahdollista ryhtyä järjestelmällisesti. Tähän tarkoitukseen valittiin pehmeä systeemimetodologia, jota tutkimuksessa on sovellettu tässä luvussa kuvatulla tavalla. Tutkimuksen empiirinen aineisto on kerätty haastattelemalla asiantuntijoita. Haastatteluaineiston käsittely ja analysointi pehmeän systeemimetodologian avulla on kuvattu tarkemmin seuraavassa luvussa.

4 Luottamusverkoston toiminnan mahdollisia suuntaviivoja

Tässä luvussa käsitellään kerättyä haastatteluaineistoa määrämuotoisesti pehmeän systeemimetodologian avulla. Alaluku 4.1 kuvaa, miten ongelmallista tilannetta lähestytään valitun metodologian mukaan. Alaluvussa 4.1.1 on kuvattu niin sanottu interventioanalyysi eli tutkimuksen lähtötilanne. Alaluvuissa 4.1.2 ja 4.1.3 on suoritettu tarkastelun kohteena olevaan toimintasysteemiin vaikuttavien sosiaalisten jännitteiden sekä poliittisten valtasuhteiden analyysi. Tämän jälkeen alaluvussa 4.2 on esitelty toimintasysteemin analyysi CATWOE-prosessin avulla sekä luotu ydinmääritelmä siitä, mitä tutkittava systeemi voisi tulevaisuudessa olla. Tämän perusteella on alaluvussa 4.3. luotu ideaalimallit, joita on viimeisessä alaluvussa verrattu todellisuuteen, jota tässä tutkimuksessa edustaa luvussa 2 kuvattu teoreettinen viitekehys.

4.1 Perusanalyysi

Checkland ja Poulter (2006) mukaan pehmeän systeemimetodologiassa ongelmallista tilannetta tulee alussa lähestyä neljän vaiheen kautta. Metodologian vakiintuneen terminologian mukaan vaiheet tunnetaan nimillä: käsiteltävän ongelmallisen tilanteen visuaalinen kuvaaminen *(Rich Pictures)*, analyysi 1: interventioanalyysi, analyysi 2: sosiaalisen systeemin analyysi sekä analyysi 3: poliittisen systeemin analyysi. Usein käsiteltävää ongelmallista tilannetta sekä siinä vallitsevia suhteita voi olla vaikea kuvata kirjallisen tekstin muodossa ja lähtötilanne saattaakin olla helpompi hahmottaa visuaalisesti. Ongelmallisen tilanteen visuaalisen kuvaamisen tarkoituksena on hahmotella vapaamuotoisesti samaan kuvaan tilanteen toimijat, rakenteet sekä vallalla olevat näkemykset ja potentiaaliset sekä tunnistetut haasteet. Kuvalla pyritään selkiyttämään monimutkainen tilanne ja sitä voidaan käyttää keskustelun välineenä tutkimusprosessin alussa (Checkland & Poulter, 2006). Tämän tutkimuksen aikana luotu visuaalinen kuvaus ongelmallisesta tilanteesta on esitetty liitteessä 2.

Pehmeässä systeemimetodologiassa ongelmallisen tilanteen visuaalinen kuvaus ei välttämättä koskaan tule kokonaan valmiiksi, vaan se elää ja kehittyy ymmärryksen kasvaessa ja tilanteiden, käsitysten sekä suhteiden muuttuessa. Liitteen 2 kuva esittää niitä ennakko-oletuksia, joita tutkijalle on muodostunut epävirallisissa keskusteluissa sekä kirjallisuuskatsauksen myötä ennen haastatteluaineiston keräämistä. Kuvassa ei pyritä esittämään tarkasti ongelmallisen tilanteen kaikkia yksityiskohtia, mutta sen avulla on mahdollista hahmottaa nopeasti luottamusverkoston toimintaan vaikuttavia jännitteitä ja tekijöitä, joita on kuvattu tarkemmin seuraavissa alaluvuissa.

4.1.1 Analyysi 1 (interventioanalyysi)

Checkland ja Poulter (2006) mukaan ongelmanratkaisutilanteissa, joissa sovelletaan pehmeää systeemimetodologiaa, on aina tunnistettavissa sama lähtöasetelma. Asetelmassa henkilö tekee päätöksen lähestyä ongelmalliseksi koettua tilannetta valitun metodologian avulla kehittääkseen tai parantaakseen tilannetta. Lähtöasetelman taustalla on yleensä tunnistettavissa kolme tahoa: kehitysprosessin **asiakkaat**, jotka ovat huolissaan nykytilanteesta tai toivovat siihen parannusta, **ongelman käsittelijät tai ratkaisijat**, jotka ryhtyvät tutkimaan, miten kehitysprosessi tulisi organisoida, sekä **ongelman omistajat**, jotka ovat kiinnostuneita kehitysprosessin lopputuloksista. Näiden tahojen tunnistaminen muodostaa interventioanalyysin, joka on ensimmäinen pehmeään systeemimetodologiaan kuluvista analyyseistä. Interventioanalyysin avulla voidaan ymmärtää ongelmatilanteen monimutkaisuus ja käsitellä useamman kuin yhden tahon näkemyksiä tilanteesta (Checkland & Poulter, 2006).

Keskusrikospoliisin kyberrikostorjuntakeskus on ollut erityisen kiinnostunut tietoverkkorikollisuuden tilannetietoisuuden kehittämisestä tämän tutkimuksen puitteissa. Leppänen ym. (2016, 2) ovat selvityksessään todenneet, että: ”Tietoverkkorikollisuuden tilannekuvatyön organisointi kuuluu poliisin kyberrikostorjuntakeskukselle ja sen tärkein kehittämistarve on poliisin sisäinen”. Kyberrikostorjuntakeskus voidaan nähdä tutkimuksen asiakkaana, joka odottaa tutkimuksesta apua sidosryhmäyhteistyön määrittämiseen. Tutkimuksen avulla keskustelut tietoverkkorikollisuuden tilannetietoisuuden jakamisesta voidaan viedä riittävän tarkalle tasolle yhteistyökumppaneiden kanssa ja rakentaa sidosryhmäyhteistyöstä nykyistä systemaattisempi kokonaisuus. Keskuksen sisällä tarve kehittää tilannetietoisuutta on toisaalta koko henkilöstön yhteinen (saadaan parempi kuva siitä, millaisia tietoverkkorikoksia Suomessa tapahtuu), mutta erityisesti tietoverkkorikostorjunnan tilannekuvayksikön sekä keskuksen johdon asialistalla. Tilannekuvayksikön tehtäviin kuuluu kerätä tietoa tietoverkkorikosten tekotavoista, sekä muodostaa analyysia erilaisista trendeistä sekä rikollisryhmistä. Keskuksen johto taas tarvitsee tätä tietoa tietoverkkorikollisuuden kokonaisuuden haltuunottoon sekä tarvittavan resursoinnin suunnitteluun ja varmistamiseen.

Tässä tutkimuksessa tutkija on selkeästi ongelman käsittelijä, joka selvittää, miten kehitysprosessi tulisi organisoida ja on päättänyt lähestyä ongelmalliseksi koettua tilannetta pehmeän systeemimetodologian avulla. Tutkimuksen tulokset on päätetty raportoida osana tätä pro gradu työtä. Lähestymistavan on hyväksynyt niin työn ohjaaja kuin kehitysprosessin asiakaskin. Vastuu tilannetietoisuustyön kehittämisestä jää kuitenkin kehitysprosessin asiakkaalle, sekä toisaalta ongelman omistajille, joita tässä tapauksessa edustavat luottamus-verkoston toimintaan osallistuvat organisaatiot. Koska organisaatiot ovat päättäneet lähteä mukaan luottamusverkoston toimintaan, oletetaan niiden

olevan kiinnostuneita tilannetietoisuuden vaihtamisesta. Parhaassa tapauksessa ne pystyvät palvelemaan loppuasiakkaitaan entistä paremmin ja kehittämään mahdollisesti uusia tuotteita tai tulonlähteitä hyödyntämällä kehittynyttä tilannetietoisuutta. Toisaalta, jos yhteistyö ei palvele ongelman omistajia riittävän hyvin, saattavat ne romuttaa ryhmän toiminnan vetäytymällä tilannetietoisuuden jakamisesta. Tämä huomio alleviivaa vallan jakautumista luottamusverkostossa, jota käsitellään tarkemmin alaluvussa 4.2.2. Aluksi paneudutaan kuitenkin niihin sosiaalisiin jännitteisiin, jotka luottamusverkoston toiminnassa on tunnistettavissa.

4.1.2 Analyysi 2 (sosiaalisen systeemin analyysi)

Kehitysprosessiin ryhdyttäessä tulee ymmärtää paitsi tarkastelun kohteena olevan toimintasysteemin luonne, myös se millainen sosiaalinen todellisuus sitä ympäröi. Jotta muutos voi onnistua, tulee sen olla kulttuurillisesti toteutettavissa kyseisessä systeemissä sekä yhteensopiva systeemin arvojen ja toimintatapojen kanssa. Checkland ja Poulter (2006) mukaan pehmeässä systeemimetodologiassa tätä yhteensopivuutta arvioidaan sosiaalisen systeemin analyysissä roolien, normien sekä arvojen avulla. Rooleilla tarkoitetaan tässä yhteydessä niin muodollisia kuin epämuodollisia rooleja, joita ihmisillä muodostuu ryhmässä. Ne voivat perustua joko henkilön asemaan organisaatiossa, tai hänen asenteeseensa tai toimintatapoihinsa. Normit ovat puolestaan kirjoittamattomia sääntöjä, joita tiettyyn rooliin yhdistetään ja jonka mukaista toimintaa tietyltä roolilta odotetaan. Arvot taas muodostavat sen viitekehyksen, minkä mukaisesti tietyssä roolissa toimimista arvostetaan ja toisaalta myös arvostellaan (Checkland & Poulter 2006).

Luottamusverkoston toimijoiden roolit voidaan ylätasolla jakaa kahteen eri ryhmään: virkamiehiin ja yksityisten yritysten edustajiin, jotka kumpikin voidaan karkeasti jakaa edelleen esimiehiin, eritysasiantuntijoihin sekä teknisiin asiantuntijoihin. Lähtökohtaisesti tutkimuksessa haastateltujen henkilöiden roolista riippumatta, kaikkien voidaan katsoa suhtautuvan avoimesti mahdollisuuteen syventää tietojenvaihtoa yritysten ja viranomaisten kesken. Joukosta on kuitenkin tunnistettavissa selkeitä skeptikkoja yhteistyön syventämisen onnistumismahdollisuuksien suhteen. Luottamusverkoston kokoonpanoon, sen toiminnan syvyyteen sekä kykyyn tuottaa juuri omaa intressiryhmää palvelevaa lisäarvoa suhtaudutaan etenkin tietoturvayritysten edustajien keskuudessa epäillen. Virkamiesrooliin sidoksissa olevien henkilöiden vastauksista on puolestaan mahdollista tunnistaa oman toiminnan kehittämisen lisäksi halu kehittää koko yhteiskunnan kyberturvallisuutta sekä erilaisiin kyberuhkatilanteisiin varautumista. Vaikka osa yritysmaailman edustajista tunnisti myös tilannetietoisuustyön yhteiskunnallisen merkityksen, korostuu tässä vastaajaryhmässä kuitenkin ennen kaikkea tahto tuottaa lisäarvoa yritysten omille loppuasiakkaille ja kehittää joko olemassa olevia tai uusia palveluita vaihdetun tietoverkkorikollisuuden tilannetietoisuuden pohjalta, kuten seuraavasta vastauksesta käy ilmi:

> Kyllä mä tietysti haluaisin nähdä oman yrityksen siinä asiakkaana, että kun tietoa tuupataan johonkin suuntaan, niin sitä saadaan kymmenkertaisesti takaisinpäin, kun se taas sitten hyödyttää meidän loppuasiakkaita tuomalla lisäarvoa meidän palveluun (Vastaaja 1 / Yritys A).

Tarkasteltavassa toimintasysteemissä vallitsevia normeja on ehdoton luottamuksellisuus sekä salassapitovelvoitteiden kunnioittaminen. Tämän voidaan nähdä toisaalta edesauttavan luottamuksellisen ilmapiirin syntymistä, mutta myös haittaavan tietojen jakamista luottamusverkostossa. Etenkin tietoturvayritysten edustajat joutuvat haasteellisiin tilanteisiin punnitessaan tilannekuvan jakamiseen liittyviä hyötyjä vasten asiakkaiden kanssa tehtyjä vaitiolositoumuksia. Myös virkamiehillä on omat haasteensa salassapitovelvoitteidensa kanssa. Mitä enemmän ja yksityiskohtaisempaa tietoa luottamusverkoston puitteissa olisi mahdollista vaihtaa, sitä konkreettisempaa hyötyä siitä voisi olla muille verkoston toimijoille.

Koska verkoston toiminta on vasta alkutekijöissään, myös kehittymättömien normien puute on havaittavissa vastauksista. Tämän hetken normit eivät esimerkiksi määritä yksityiskohtaisesti, miten tai minkälaisista asioista luottamusverkostossa tulisi ilmoittaa, mikä koetaan kuormittavaksi. Toimintamalli, jossa jokaisen toimijan tulee käydä läpi havaintojaan ja määritellä milloin ilmoittamiskynnys ylittyy, ei saa kannatusta.

> Meillä on alusta alkaen ollut sellainen linjaus, että se on ihan keinotekoista kuvitella, että me täällä kerättäisiin jotain agendaa ja purettaisiin se jossain tapaamisissa kvartaaleittain. Ei meillä ole sellaiseen järjestelmällisyyteen varaa (Vastaaja 1 / Yritys B).

Ilmoittamiskynnyksen määrittämiseen toivotaan selkeitä ohjeita ja myös tiedon vastaanottajilta odotetaan panostusta tiedon jatkojalostamiseen. Luottamusverkoston yhtenä kirjoittamattomana sääntönä voidaankin pitää sitä, että tiedon vaihdon tulee olla vastavuoroista. Jokaisen verkoston toimijan tulee antaa oma panoksensa yhteistyöhön. Vapaamatkustajia ei sallita, kuten seuraavista vastauksista ilmenee.

> Eli hyötyjähän tästä pitää saada kaikin puolin. Jos se hyöty on vaan yksisuuntaista sinne kyberturvallisuuskeskuksen ja keskusrikospoliisin suuntaan niin, että tietoturvayritykset ilmoittelevat asioita asiakkaistaan niin, ettei me saada mitään takaisin, niin sillä ei hirveästi voiteta (Vastaaja 1/ Yritys A).

> -- ja sitten osana pelisääntöjä jokaisella osallistujalla pitää olla mentaliteetti sellainen, että jotta tietoa voi vastaanottaa, niin sitä pitää myös jakaa. En siihen pakottaisi, mutta se mihin pitäisi pystyä on se, että jokainen olisi sekä ottavana että antavana osapuolena (Vastaaja 2 / Yritys A).

> -- haluaisin varmistua siitä, että meidän kilpailijoilla on panostus samanmuotoista, samanlaista ja yhtä palvelevaa, että siellä nähdään tämän yhteistoiminnan palvelevuus samalla tavalla (Vastaaja 3 / Yritys A).

> Toivoisin, että lähetään ensin siitä, että rakennetaan se keskinäinen luottamus ja ymmärrys siitä, että jos jaan tietoa, niin mitä oletuksia minulla on, että miten sitä tietoa hyödynnetään. Se joka vastaanottaa sen tiedon, niin ymmärtää myös sen, että heiltä odotetaan vastaan tietoa. -- Tämä perustuu vapaaehtoisuuteen, keskinäiseen hyötymiseen ja siihen että kokonaisuus hyödyttää (Vastaaja 1 / Yritys B).

Haastattelutilanteissa havaittuja toimintasysteemissä valitsevia arvoja ovat avoimuus, salassapitovelvoitteiden kunnioittaminen, ehdoton luottamuksellisuus omia loppuasiakkaita kohtaan, yhteiskuntavastuu sekä tekninen osaaminen. Nämä teemat toistuivat useimmissa vastauksissa. Kiinnostus alaa kohtaan, henkilökohtainen osaaminen sekä työmoraali ovat luottamusverkoston kantavia tekijöitä.

> -- voidaan lähtökohtaisesti heittää sellaisena oletuksena, että [mukana] on luotettavia tyyppejä, kun ne ovat halunneet olla tietoturvan kanssa tekemisissä ja siihen yleensä liittyy joku tällainen oikeudenmukaisuuden tunto. Se on helppo ehkä löytää joku semmoinen, että ollaan saman pöydän ääressä ja samalla aaltopituudella (Vastaaja 2 / KRP).

Vaikka erityisesti kilpailevien yritysten edustajien suhtautumisessa toisiinsa on havaittavissa selkeää epäluuloa, oli haastattelutilanteissa kuitenkin huomattavissa, että luottamusverkoston toimijat myös arvostavat toisiaan. Roolista riippumatta haastatellut tunnistivat, että toisella toimijalla saattaa olla tietyiltä osin parempi, tai ainakin erilainen näkymä tietoverkkorikollisuuteen kuin, mitä omassa organisaatiossa on. Tämän tiedon yhteen kokoaminen koetaan arvokkaaksi tavoitteeksi, jonka eteen ollaan valmiita tekemään yhteistyötä. Lisäksi haastatteluissa oli havaittavista, että keskinäinen kunnioitus viranomaisten ja yritysten kesken on korkealla. Tämä ilmenee muun muassa siitä, että yrityksissä yhteistyö viranomaisten kanssa nähdään selkeänä imagohyötynä ja tietynlaisena statuksen osoituksena. Viranomaisten osaamiseen luotetaan ja toisaalta virkamiehet ovat valmiita myöntämään, että yksityisillä yrityksillä saattaa olla viranomaisia paljon parempi näkyvyys tietoverkoissa tapahtuviin rikoksiin esimerkiksi tiettyyn rikollisuuden osa-alueeseen tai johonkin yksittäiseen asiakaskuntaan liittyen.

Sosiaalisen systeemin analyysin perusteella tietoverkkorikollisuuden tilannetietoisuuden tulisi palvella niin viranomaisten tarvetta kehittää konkreettista tilannekuvanäkymää tapahtuviin rikoksiin, kuin myös lisätä yritysten edustajien ymmärrystä tapahtuvista rikoksista sekä niiden taustalla vaikuttavista ilmiöistä. Näin pystyttäisiin palvelemaan erilaisia yhteistyöhön osallistuvia tahoja, jotka voisivat palvella entistä paremmin loppuasiakkaitaan, mikä johtaisi parhaassa tapauksessa kansallisesti kyberturvallisuuden kohenemiseen. Edellytyksenä tälle on, että tilannetietoisuustyö noudattaa ryhmässä havaittuja normeja, joita ovat ehdoton luottamuksellisuus, tiedon vaihdon vastavuoroisuus sekä (vielä määrittelemättömien) toimintaohjeiden noudattaminen. Toiminnassa arvostetaan mahdollisimman avointa, mutta salassapitovelvoitteet huomioivaa yhteistyötä, teknistä osaamista sekä yhteiskuntavastuuta. Yhteistyön ohjaamiseksi edellä kuvattuun suuntaan, tulee

ymmärtää, kenellä on valta määrittää yhteistyön suunta ja millaisia odotuksia sen mukanaan tuomaan asemaan kohdistuu.

4.1.3 Analyysi 3 (poliittisen systeemin analyysi)

Pehmeän systeemimetodologian mukaan poliittisen systeemin analyysissä pureudutaan ongelmalliseksi koetussa tilanteessa vallitseviin valtasuhteisiin. Checkland ja Poulter (2006) esittävät, että ihmisten muodostamiin toimintasysteemeihin liittyy aina vallan jakautumiseen liittyviä jännitteitä, jotka johtuvat toimintaan osallistuvien ihmisten vaihtelevista maailmankuvista, sekä erilaisista intresseistä. Heidän mukaansa systeemeissä kaikilla toimijoilla on aina jonkinlainen suhde systeemissä käytettyyn valtaan. Näihin suhteisiin voidaan pureutua kysymällä esimerkiksi: kuka on vastuussa toimintasysteemin ylläpitämisestä, kuka käyttää sen tuotoksia, kenellä on oikeus muuttaa systeemin toimintaa tai lopettaa se ja kuka päättää kuinka paljon aikaa sen toimintaan käytetään? Valtasuhteet voivat olla suoraan kytköksissä tiettyyn rooliin tai liittyä epäsuorasti esimerkiksi tietyn henkilön maineeseen tai osaamiseen. Vaikka kehitystoiminta olisikin kulttuurillisesti toteutettavissa, valtasuhteet määrittävät lopulta sen mihin toimintaan ryhdytään (Checkland & Poulter, 2006).

Luottamusverkoston toimijoiden roolit jaettiin edellisessä luvussa kahteen eri ylätason ryhmään: virkamiehiin sekä yksityisten yritysten edustajiin. Kummassakin ryhmässä organisaatiohierarkiassa ylempänä olevat henkilöt kuten yksikön johtajat tai tiimin vetäjät määrittävät resursseista, joita yhteistyöhön käytetään. He eivät kuitenkaan osallistu varsinaiseen tilannetietoisuuden vaihtamiseen liittyvään työskentelyyn eivätkä ole välttämättä edes tietoisia yhteistyön syvyydestä. Operatiiviseen tietojenvaihtoon osallistuvat erityisasiantuntijat sekä tekniset asiantuntijat voivat valita varsin vapaasti tilannetietoisuuden muodostamisen kannalta oleellisen tiedon keräämiseen sekä jakamiseen käytettävän työajan. Ajankäytöstä tiedusteltaessa yritysten edustajat korostivat yhteistyön vapaaehtoista luonnetta ja huomauttivat, ettei siihen käytettävä aika saisi juurikaan olla pois muusta ”tuottavasta” toiminnasta. Viranomaispuolella työhön oltiin puolestaan valmiita uhraamaan tarvittavissa määrin virkamiestunteja, joskin käytössä olevien resurssien rajallisuus tunnistettiin myös tässä ryhmässä:

> No ehkä se keskeisin rajoite [yhteistyön kehittämiselle] on resurssit. Että tahtotila meillä on suurempi kuin meidän kyky vastata siihen tahtotilaan ja tarpeeseen (Vastaaja 1, KRP).

Luottamusverkoston toiminnan ymmärtämisen kannalta on tärkeä ymmärtää, kenellä on valta määrittää millaista tilannetietoisuutta verkostossa tulisi jakaa. Yritysmaailman edustajien valtaa jakaa tietoa rajoittavat etenkin niiden loppuasiakkaiden kanssa tehdyt sopimukset. Yritykset eivät voi jakaa sellaista tietoja luottamusverkoston muiden toimijoiden kanssa, jonka jakamiseen ne eivät ole saaneet lupaa.

> Me ollaan aina oltu lähtökohtaisesti suopeita jakamaan viranomaisille -- sellaista tietoa, mitä meillä nyt sattuu olemaan helposti saatavilla ilman että joudutaan mitään asiakaslupausta rikkomaan. Asiakaslupaus on tietenkin se, että meidän asiakkaan yksityisyyden suojaa ja yrityssalaisuuksiin liittyviä tietoja me ei voida ulkopuolisille luovuttaa (Vastaaja 1 / Yritys B).

> Aina pitää olla asiakkaan hyväksyntä tai ennalta hyväksytty malli (Vastaaja 1 / Yritys A).

Tietoturvayritysten loppuasiakkaat omistavat tiedon tapauksista, joita luottamusverkostoissa tulisi käsitellä. Loppuasiakkaat eivät kuitenkaan voi rajoittaa tietojen jakamista, mikäli käsiteltävät tapaukset anonymisoidaan siten, ettei loppuasiakas ole yhdistettävissä tapaukseen. Tietoturvayritysten edustajat voivat myös keskustella yleisellä tasolla siitä, millaisia trendejä ne ovat asiakaskunnassaan havainneet. Tällaista tietojen vaihtoa rajoittaa kuitenkin yritysten välinen kilpailuasetelma. Jos yritykset kokevat olevansa suoraan toistensa kilpailijoita, ovat ne vastahakoisia jakamaan keskenään tietoa. Jaettavan tiedon perusteella kasvavan ymmärryksen pelätään kehittävän kilpailevan yrityksen kykyä palvella omia asiakkaita. Yrityksillä on siis olemassa myös intressi suojella omaa tilannetietoisuuttaan tietoverkkorikollisuudesta eikä kaikkea tietoa haluta jakaa. Näin toimimalla yritysten voidaan tulkita käyttävän valtaa verkostossa päättämällä, mitä tietoa kilpailijoilta pimitetään.

Useissa yritysten edustajien vastauksissa korostui, että varsinaisen tiedon jakamisen tulisi tapahtua viranomaisten kautta. Yritykset ovat lähtökohtaisesti suopeampia jakamaan tietoa viranomaisille kuin toisilleen, jolloin tiedonvaihto on huomattavasti avoimempaa. Viranomaiset voisivat koota ja jalostaa tiedon ja jakaa sen ryhmän muille toimijoille, sillä ryhmän toiminnan kehittämisen vallan ja vastuun koetaan olevan viranomaisten käsissä. Niiltä toivotaan aktiivista otetta sekä selkeitä toimintaohjeita, miten tietoa tulisi vaihtaa. Lisäksi viranomaisten toivotaan tarjoavan yhteistyöhön soveltuvat tekniset välineet ja vastaavan niiden ylläpitämisestä.

Koska yrityksillä on jo ennestään toimiviksi koetut suhteet viestintäviraston kyberturvallisuuskeskuksen kanssa, koetaan se luontevaksi tahoksi koordinoimaan yhteistyötä. Epävarmuutta keskusrikospoliisin suhteen herättää niin sanottu esitutkintavelvollisuus, joka esitutkintalain mukaan astuu voimaan, kun poliisi saa tiedon tapahtuneesta rikoksesta (Esitutkintalaki 805/2011, 3 luku, 1§). Tästä syystä yritysmaailman edustajat ovat varovaisia jakamaan tietoa poliisiviranomaisten suuntaan edes yleisellä tasolla. Toisaalta osa haastatelluista nimenomaisesti toivoi, että etenkin vakavimpien tapausten kohdalla poliisille jaettava tieto ohjaisi poliisin rikostiedustelua. Parantuneen tilannetietoisuuden toivottaisiin johtavan sellaisiin ennaltaehkäiseviin toimenpiteisiin, joiden avulla tietoverkkorikosten tekijöitä saataisiin entistä tehokkaammin kiinni.

Tässä luvussa on kuvattu pehmeän systeemimetodologian mukaisen perusanalyysivaiheen tulokset ja tunnistettu luottamusverkoston toimintaan liittyviä sosiaalisia jännitteitä sekä havaittuja valtasuhteita. Seuraavassa luvussa pureudutaan tarkemmin luottamusverkoston eri rooleihin.

4.2 CATWOE -prosessi

Checkland ja Poulter (2006) mukaan ihmiset pyrkivät vuorovaikutustilanteissa toimimaan tarkoituksenmukaisesti saavuttaakseen jonkun tiedostetun tai tiedostamattoman tavoitteen. Tarkoituksenmukaisen toiminnan mallintaminen (purposeful activity model) toimii pehmeässä systeemimetodologiassa yhtenä työkaluna, jonka avulla ongelmatilannetta voidaan lähestyä järjestelmällisesti. Tarkoituksenmukaisen toiminnan tunnistamista (mitä toiminnalla yritetään saavuttaa) ja mallintamista (mistä tekijöistä toimintasysteemi koostuu) on mahdollista käyttää reflektoinnin ja keskustelun välineenä ongelmallista tilannetta kehitettäessä. Päätavoitteena on löytää vastaukset kysymyksiin: mitä vuorovaikutustilanteessa tehdään, miten ja miksi? (Checkland & Poulter, 2006).

Ongelmatilannetta ruotivien keskustelujen ongelmana on usein kuitenkin se, että niissä keskitytään tilanteeseen vain tietyn toimijan näkökulmasta käsin. Todellisuus on tätä monimutkaisempi ja pyrittäessä hahmottamaan ongelmallista tilannetta, ei mallintamisen avulla pystytä välttämättä vangitsemaan tilanteen koko monimutkaisuutta tai kaikkia sen eri vivahteita. Tällöin tilannetta kannattaa lähestyä tietystä tarkasti määritellystä näkökulmasta, jonka muodostamiseksi tarvitaan ydinmääritelmä siitä, mitä toimintasysteemin tarkoituksena on saavuttaa. Ydinmääritelmän perusteella on puolestaan mahdollista luoda ideaalimalli, joka kuvaa millainen systeemi voisi parhaassa tapauksessa olla. Lopulta ideaalimalleja ja todellisuutta vertailtaessa voidaan tunnistaa sellaisia konkreettisia kehitysehdotuksia, jotka ovat toteutettavissa ja kulttuurillisesti sopivia toimintasysteemille, joka on tarkastelun kohteena.

Toimintasysteemin tarkempi määrittely tapahtuukin Checkland ja Poulter (2006) mukaan pehmeässä systeemimetodologiassa ydinmääritelmien (Root Definition) kautta, jotka rakennetaan tunnistamalla ja nimeämällä systeemin osatekijät sekä näiden väliset vaikutussuhteet CATWOE -prosessin avulla. Prosessin nimi CATWOE tulee englanninkielisitä sanoista Customers (asiakas), Actors (toimijat), Transformation process (muutosprosessi), World view (maailmankuva tai näkökulma), Owners (omistajat) sekä Environmental constraints (toimintaympäristön asettamat rajoitukset). Prosessin avulla on mahdollista tunnistaa kehittämisprosessiin liittyvät toimijat, prosessit ja niiden osatekijät, jotka vaikuttavat toimintasysteemiin, sekä kehittämisen näkökulma ja ympäristön sille asettamat rajoitukset (Chekland & Poulter 2006). Seuraavissa alaluvuissa on CATWOE -prosessin avulla haastatteluaineistoa reflektoiden tunnistettu tietoverkkorikollisuuden tilannetietoisuutta jakavan luottamusverkoston osatekijät ja näiden väliset vaikutussuhteet sekä muodostettu ydinmääritelmä luottamusverkoston toiminnalle.

4.2.1 Asiakas

Interventioanalyysissä kehitysprosessin asiakkaaksi tunnistettiin keskusrikospoliisin kyberrikostorjuntakeskus, joka on ollut erityisen

kiinnostunut tietoverkkorikollisuuden tilannetietoisuuden kehittämisestä tämän tutkimuksen puitteissa. Tämä ei kuitenkaan tarkoita sitä, että kyseinen taho olisi välttämättä ainut asiakas luottamusverkoston toiminnassa. Sosiaalisen systeemin analyysissä korostuivat näkemykset siitä, että ollakseen kulttuurillisesti toteutettavissa kyseisessä toimintasysteemissä sekä yhteensopiva systeemin arvojen ja toimintatapojen kanssa, tulee verkoston toiminnan hyödyttää kaikkia toimijoita. Muutoin verkoston toiminnan ei odoteta jatkuvan kovinkaan kauaa. Checkland & Poulter (2006) ymmärtävätkin asiakkuuden CATWOE –prosessin yhteydessä huomattavasti interventioanalyysissä mainittua asiakkuutta laajemmin. He määrittelevät sen tarkoittavan kaikkia sellaisia tahoja, joihin toimintasysteemissä tapahtuva muutosprosessi vaikuttaa. Näin ollen termi asiakas pitää tässä yhteydessä ymmärtää pelkkää kehitysprosessin asiakkuutta laajemmaksi kokonaisuudeksi, jolla on useita ulottuvuuksia.

Haastatteluissa yritysten edustajat halusivat nähdä itsensä luottamusverkoston asiakkaina, jotka saavat suoraan hyötyä kasvavan ymmärryksen, kehittyvien taitojen ja yhä parempien palvelukyvykkyyksien kasvamisen myötä. Erityisesti hyötyjiksi organisaation sisällä tunnistettiin organisaation tietoturvallisuudesta vastaavat henkilöt sekä kaupallisia palveluita tuottavien teknisten tietoturvavalvomoiden henkilökunta. Luottamusverkoston toiminnan kehittymisen myötä kasvavan ymmärryksen oletettiin vaikuttavan positiivisesti tietoturvayritysten kykyyn suojella sekä itseään että omia loppuasiakkaitaan, joiden oletettiin olevan valmiita maksamaan kehittyvistä kyvykkyyksistä ja yhä paremmista palveluista. Vaikka jaettavaa tietoa ei suoraan pystyttäisikään tuotteistamaan asiakkaille siten, että se olisi muutettavissa kassavirtaa generoivaksi tuotteeksi, kasvavan ymmärryksen oletettiin vaikuttavan positiivisesti kykyyn palvella asiakkaita entistä paremmin ja tuottavan siten hyötyjä kummallekin osapuolelle.

Viranomaisten edustajien keskuudessa yhteistyön koettiin hyödyttävän ennen kaikkea tilannetietoisuuden tuottamisesta vastuussa olevaa henkilöstöä, sekä toisaalta myös eri yksiköiden koordinoimisesta ja johtamisesta vastuussa olevia tahoja. Sekä kyberturvallisuuskeskuksella että kyberrikos-torjuntakeskuksella on siis olemassa organisaation sisäinen intressi osallistaa tietoturvayritykset tilannetietoisuusyhteistyöhön. Lopulta viranomaisten työn perimmäisenä tarkoituksena on kuitenkin tuottaa yhteiskunnalle sen tarvitsemia viranomaispalveluita, joiden asiakkaina ovat niin yksittäiset kansalaiset, kuin yhteisöt ja yrityksetkin. Luottamusverkoston toiminnassa onkin siis kyse jaetusta asiakkuudesta, josta voidaan katsoa hyötyvän niin luottamusverkoston toimintaan osallistuvat toimijat kuin myös niiden loppuasiakkaat. Viranomaisten osallistuminen verkoston toimintaan mahdollistaa lisäksi tiedon levittämisen koko maan laajuisesti kansalaisille, yrityksille ja yhteisöille, joiden voidaan yhtä lailla katsoa olevan tilannetietoisuustyön asiakkaita.

4.2.2 Toimijat

Pehmeässä systeemimetodologiassa ydinmääritelmää rakennettaessa on tunnistettava ne toimijat, jotka toteuttavat muutosprosessin (Checkland & Scholes 1990). Tässä tutkimuksessa toimijoita ovat tietoverkkorikollisuuden tilannetietoisuutta jakavaan luottamusverkostoon kutsutut tahot. Näitä ovat sekä viranomaisten, että yksityisten yritysten edustajat, joilla on kullakin hallussaan sellaista tietoa tai tietoisuutta, jota luottamusverkoston muilla toimijoilla ei välttämättä ole saavutettavissa.

Vaikka yksityisten yritysten edustajat haluaisivat ennen kaikkea nähdä itsensä yhteistyön hyötyjinä eli asiakkaina, on niiden rooli toimintasysteemin yhtenä keskeisenä toimijana kuitenkin merkittävä. Ilman niiden toimittamaa havaintodataa ei muutosprosessilla nimittäin ole sellaista syötettä, josta olisi mahdollista jalostaa tietoverkkorikollisuuden tilannetietoisuutta. Toisena olennaisena toimijana luottamusverkostossa ovat sen toimintaan osallistuvat viranomaiset eli viestintäviraston kyberturvallisuuskeskus ja keskusrikospoliisin kyberrikostorjuntakeskus. Näiden tahojen tulisi tunnistaa muiden toimijoiden niille asettamat odotukset. Viranomaisten roolin koetaan olevan ennen kaikkea luottamusverkostoon toimitetun syötteen jalostamisessa ja jakamisessa takaisin verkoston toimijoille.

Voisi olla perusteltua odottaa, että luottamusverkoston toimijoiden määrän kasvattaminen vaikuttaisi positiivisesti havaintodatan määrään ja toisi lisäresursseja toiminnalle. Vaikka haastatteluvastausten perustella lisäjäsenten mukaan ottamista ei vastusteta, on kuitenkin huomionarvoista, että mikäli toimijoiden määrää kasvatettaisiin, saattaisi se vaikuttaa heikentävästi ryhmän kokemukseen samasta kohtalosta ja yhteisestä missiosta ja vaikuttaa negatiivisesti ryhmän toimintaan (Endsley & Jones, 1997). Tästä syystä esimerkiksi muut viranomaistahot kuten puolustusvoimat, suojelupoliisi, paikallispoliisi, poliisihallitus sekä ministeriöt tulisi käsittää mieluummin toimintasysteemin välillisinä asiakkaina kuin aktiivisina jäseninä.

4.2.3 Muutosprosessi

Checkland (1981) määrittelee muutosprosessin CATWOE -prosessissa tarkoittavan yksinkertaisesti jonkin syötteen muuttumista tuotokseksi. Muutosprosessista puhuttaessa on tärkeä ymmärtää, ettei kyse ole pelkästään toisiaan seuraavista sarjasta toimintoja, jotka johtavat tiettyyn lopputulokseen, vaan konkreettisesta tapahtumasta, jossa prosessin syöte muuttaa muotoaan (Checkland ja Scholes 1990). Muutosprosessi rakentuu luottamusverkostossa tiedon havainnoimisesta, keräämisestä, jakamisesta ja käsittelystä siten, että lopputuloksen voidaan katsoa muodostavan sellaista ymmärrystä, jota yhdenkään toimijan ei olisi ollut mahdollista saavuttaa yksin. Ymmärryksen on oltava myös sellaista, että jokainen toimija tarvitsee sitä selviytyäkseen paremmin omista työtehtävistään. Muuten tilannetietoisuuden jakamisella ei ole yksittäiselle toimijalla merkitystä, eikä voida puhua yhteisestä

tilannetietoisuudesta, siten kun se on tämän tutkimuksen teoreettisessa viitekehyksessä määritelty.

Muutosprosessi on haastattelujen perusteella määriteltävissä ylätasolla, mutta käsitykset parhaasta mahdollisesta toteutustavasta eroavat eri osapuolien kesken. Ylätasolla kunkin toimijan oletetaan keräävän tietoverkkorikoksia koskevaa dataa ja jakavan sen muiden toimijoiden kanssa, silloin kun sen vakavuusaste ylittää vielä määrittelemättömän kynnyksen. Muiden toimijoiden oletetaan tämän jälkeen osallistuvan datan jalostamiseen ja viranomaisten oletetaan rikastavan tietoa havainnoilla maailmanlaajuisista tietoverkkorikollisuuden ilmiöistä. Yksityisellä sektorilla on näkyvyys siitä, minkälaista tietoverkkorikollisuutta niiden suomalaiseen asiakaskuntaan kohdistuu ja viranomaiset saattavat pystyä kytkemään yksittäisiltä näyttävät teot osaksi isompia maailmanlaajuisia hyökkäyskampanjoita omien tiedonhankintakanaviensa avulla. Tämän perusteella olisi mahdollista varoittaa muita tahoja, jotka olisivat potentiaalisia kohteita vastaaville rikoksille. Tiedon jakamisen tulisi tapahtua mahdollisimman vähällä vaivalla, mahdollisimman reaaliaikaisesti ja muodostaa sellainen lopputuotuotos, jota olisi mahdollista hyödyntää joko uusia palveluita kehitettäessä tai nykyisiä parantaessa. Yhteistyön myötä kasvava ymmärrys voitaisiin jakaa viranomaisten toimesta myös luottamusverkostoa laajemmalle yleisölle, jolloin se palvelisi laajemmin yhteiskunnan kyberturvallisuuden kehittymistä.

Viranomaiset olisivat valmiita etenemään yhteistyössä varovaisesti askeleittain, mutta vauhti saattaa muodostua liian hitaaksi yritysmaailman edustajille, jotka kokevat, ettei yhteistyöstä muodostu niille tarpeeksi hyötyjä ja jättäytyvät pois yhteistyöstä. Epämääräinen määrittely tiedon vaihtotavoille sekä subjektiivisesti kunkin tahon itse määrittämä ilmoituskynnys saattavat muodostua liian raskaiksi yrityksille, jolloin on olemassa iso riski, etteivät ne jatka luottamusverkoston jäseninä. Vaikka viranomaisilla olisikin mahdollisuus luoda syväluotaavia katsauksia tietoverkkorikollisuuden tilaan luottamusverkostossa jaetun tiedon perusteella, ei tällainen aikaa vievä raportointi välttämättä riitä yritysmaailman edustajille, jotka toivovat yhteistyöltä nopeita hyötyjä, jotka ovat helposti valjastettavissa käyttöön arkipäiväisessä työssä. Muutosprosessiin syötetty heräte, eli havainto oletetusta tapahtumasta, vaatii nopeaa reagointia, jotta siitä koettaisiin olevan aidosti hyötyä, kuten seuraavasta vastauksesta käy ilmi.

> Sen täytyy olla niin, että perustetaan sellainen klubi. Tunnistetaan ne henkilöt, tunnistetaan ne mekanismit, jolla tätä [havaintodataa] voidaan sitten laittaa vaivatta jakoon. Vaikka silleen, ettei tarvitse välttämättä edes kokonaista virkettä kirjoittaa. Tuossa dataa – tutkikaa. Sitten on sellainen olettama, että vastapuolella viranomainen hoitaa hommansa siitä eteenpäin. Ja se täytyy olla sellaista, että tänään aamupäivällä, kun minulle tulee jotain, niin laitan sen jakoon tänään aamupäivällä, ettei tarvitse sitä lähteä kuskaamaan tällaiseen fyysiseen tapaamiseen (Vastaaja 1 / Yritys B).

Tavasta, jolla tietojenvaihto toteutettaisiin ei ole yhtenäistä kuvaa haastateltujen keskuudessa. Siinä missä yksi vastaaja kokee pikaviestikanavien ja sähköpostin

riittävän, toivoo toinen osapuoli automaattista uhkatietojen vaihtoa ja kolmas toivoisi viranomaisten aloittavan ohjelmistoprojektin uhkatietopankin keräämiseksi. Fyysiset tapaamiset ja niissä keskustelu koetaan tärkeiksi lähinnä luottamuksen ja syvällisen ymmärryksen rakentamisen kannalta.

4.2.4 Maailmankuva

Kaikki ongelmallisesta tilanteesta käydyt keskustelut värittyvät keskustelijoiden erilaisten näkökulmien läpi. Checkland (1981) käyttää erilaisista näkökulmista termiä maailmankuva (Weltanschauungen), jotka ovat sisäisiä usein tiedostamattomia asenteita ja oletuksia, joiden perusteella ongelmallista tilannetta tulkitaan tietystä ennakkoasetelmasta käsin. Tilannetta ei pystytä, eikä tulekaan pystyä tulkitsemaan puhtaana ja irrallaan kontekstista, mutta erialiset näkemykset ja oletukset, jotka vaikuttavat toimijoiden tapaan tulkita tilannetta tulee tunnistaa osana CATWOE -prosessia. Kun tilanteessa vallitseville maailmankuvat määritetään ja kuvataan, pystytään eri tahojen pyrkimyksiä tietynlaiseen toimintaan tunnistamaan ja ymmärtämään paremmin. Tämä voi puolestaan johtaa ajattelun muuttumiseen eri osapuolien keskuudessa. Checkland ja Poulter (2006, 61) kertovatkin, että tavoitteena on mukauttaa erilaisia näkemyksiä ja löytää sellainen kompromissi, jonka eri osapuolet ovat valmiita hyväksymään.

Erilaisia maailmankuvia tietoverkkorikollisuuden tilannetietoisuuden kehittämiselle esiintyy niin eri toimijoiden kuin myös eri roolien välillä. Karkea jako voidaan tehdä viranomaisten ja yritysmaailman edustajien välille, mutta tarkemmassa tarkastelussa voidaan havaita myös erilaisia maailmankuvia organisaatioiden sisällä eri roolien välillä. Selkeimmät erot rakentuvat kuitenkin viranomaisten yhteiskunnallisen näkökulman ja tietoturvayritysten asiakasnäkökulman välille, jota on jo sivuttu aikaisemmissa luvuissa. Jotta tilannetietoisuuden vaihtaminen palvelee molempia osapuolia, tulee sen avulla voida sekä tuottaa lisäarvoa eli parempia tuotteita ja palveluita tietoturvayritysten asiakkaille kuin myös laajentaa viranomaisten käsitystä Suomessa havaituista tietoverkkorikollisuuden muodoista siten, että yhteistyö samalla vaikuttaa positiivisesti koko suomalaisen yhteiskunnan kyberturvallisuuden kehittymiseen.

Toinen selkeä ero maailmankuvissa on havaittavissa esimies- ja asiantuntijatason välillä. Siinä missä esimiestaso pääsääntöisesti koki erilaisten tapaamisten, keskustelujen ja ilmiö- tai trenditietojen vaihtamisen olevan riittävä tiedonvaihdon muoto, asiantuntijat puolestaan kokivat tällaisten tapaamisten arvon muodostuvan lähinnä luottamuksen rakentumisesta eri toimijoiden välille. Tietoverkkorikollisuuteen liittyvien havaintojen jakamiseen kaivattiin pääsääntöisesti paljon reaaliaikaisempaa tapaa, jolloin saavutettavat hyödyt olisivat lähes välittömästi asiantuntijoiden käytössä. Näin olisi toisaalta mahdollista nopealla syklillä rakentaa entistä tehokkaampaa palvelua yritysten asiakaskunnalle, kuin myös toisaalta kohdistaa viranomaisten rikostiedustelua ajankohtaisiin ilmiöihin. Tämä kuitenkin vaatisi yhteistyön huomattavaa

syventämistä ja jonkinasteista automatisoitua tietojenvaihtoa, sillä pelkkien kommunikointikanavien kuten sähköpostilistojen tai pikaviestintäohjelmistojen perustamisen ei uskota riittävän käynnistämään varsinaista tiedon vaihtoa.

Kolmanneksi ero maailmankuvissa voidaan nähdä niiden tahojen välillä, jotka uskovat yhteistyön kehittymiseen ja niiden välillä, jotka ovat avoimia tiedon vaihtamiselle, mutta skeptisiä sen onnistumisen suhteen. Epäilyksiä aiheuttavat etenkin yritysten edustajien keskuudessa koko asetelma, jossa tietoa jaetaan kilpaileville yrityksille sekä uskon puute siihen, että muut toimijat panostavat tietojenvaihtoon vastaavalla vaivannäöllä ja tiedon vaihdon vielä määrittelemätön luonne. Toisaalta osa toimijoista suhtautuu jo nyt tiedonvaihtoon avoimen rohkaisevasti ja näkevät sillä saavutettavan hyötyjä ennen kaikkea isossa, yhteiskunnallisessa mittakaavassa sekä avoimuuden kulttuurin edistäjänä. Isoimmat haasteet syntyvätkin näiden kahden maailmankuvan yhdistämisessä, sillä tiedonvaihtoon rohkaisevasti suhtautuvien toimijoiden voidaan olettaa alussa panostavan verkoston toimintaan muita enemmän, jolloin vaaran on niin vapaamatkustajailmiön toteutuminen kuin toisaalta saavutettavien hyötyjen vajaavaisuus, kun yhteistyö ei ole tasapuolista. Molemmat ovat jo yksinään sellaisia syitä, jotka saattavat riittää kaatamaan koko yhteistyön heti alkuunsa. Tästä syystä tietoverkkorikollisuuden tilannetietoisuuden jakamisen kynnys tulee alusta asti asettaa niin matalalle, että myös ns. skeptikot saadaan rohkaistua mukaan verkoston toimintaan.

4.2.5 Omistajat

Interventioanalyysissä ongelman omistajaksi nimettiin luottamusverkoston toimintaan osallistuvat organisaatiot, koska ne ovat kaikki tahoillaan kiinnostuneita kehitysprosessin lopputuloksista ja ne voivat myös halutessaan vaikuttaa tapaan, jolla tilannetietoisuutta vaihdetaan. Tässä mielessä kyseessä on jaettu omistajuus, jossa yksittäisellä toimijalla ei ole valtaa pakottaa muita toimijoita tiettyyn toimintamalliin. Kysyttäessä miten kukin vastaaja suhtautuu pakottavaan regulaatioon ilmoittaa havaituista tietoverkkorikoksista, pitivät vastaajat lähes yksimielisesti regulaatiota vain keinona saavuttaa minimitaso ilmoituksille. Aidon yhteistyön tulisi sen sijaan perustua vahvasti vapaaehtoisuuteen verkoston toimijoiden kesken. Isommassa mittakaavassa elinkeinoelämän toimijoiden tulevaisuudessa kiristyvä velvollisuus ilmoittaa tietoverkko- ja kyberrikoksista jakoi vahvasti mielipiteitä. Osa vastaajista koki pakottavan regulaation vaikuttavan positiivisesti entistä avoimemman ilmapiiriin syntymiseen, toiset taas kokivat sen olevan turhaa uhrien syyllistämistä. Eniten kannatusta sai toimintamalli, jossa ilmoitukset olisi mahdollista tehdä luottamuksellisesti viestintävirastolle, jolla olisi tämän jälkeen mahdollisuus auttaa uhreja ja kenties myös valta määrittää korjaavia toimenpiteitä, johon uhrin olisi ryhdyttävä.

Viestintäviraston ja etenkin sen alaisuudessa toimivan kyberturvallisuuskeskuksen rooli korostui vahvasti myös kehitystyön omistajan

roolia kysyttäessä. Vaikka siis omistajuuden voidaan katsoa olevan jaettu, niin kyberturvallisuuskeskus koettiin vastaajien keskuudessa riippumattomaksi ja luotettavaksi kumppaniksi, jonka tulisi ottaa vahva rooli luottamusverkoston toiminnan kehittämisessä. Kehitystyön koordinointi ja ohjaaminen voidaan jakaa myös keskusrikospoliisin ja viestintäviraston kesken, mutta koska valtaosalla toimijoista on jo yhteistyötä kyberturvallisuuskeskuksen kanssa ja sillä koetaan olevan vakiintunut asema tiedon jakamisen solmupisteenä, tulisi sen toimia aktiivisesti tietoa keräävänä ja sitä edelleen jakavana toimijana.

> Kyllä väittäisin, että se [omistaja] olisi tuo viestintävirasto. Se olisi luonnollinen fuusiosolu, jonne se tieto päätyy joka tapauksessa ja jonne on oletettavaa, että kotimaiset elinkeinoelämän toimijat, kotimaiset viranomaiset, ulkomaiset kollegat ja jossain määrin jopa poliisiviranomaisetkin jakavat tietoa, josta heidän on sitten olisi helppo jakaa sitä tietoa eteenpäin. En millään voi kuvitella, että se [omistajuus] olisi supossa, ei poliisissa valtakunnallisessa tai paikallisella tasolla, ei puolustusvoimissa missään nimessä, ei valtiovarainministeriössä eikä sellainen taho ole myöskään tietosuojavaltuutettu. Ei ole sellaista tahoa, jolla olisi tällainen ”name recognition” kun viestintävirastolla. Eikä ole mitään muuta sellaista luontevaa tahoa, jolla olisi sellainen uskottavuus ja luottamus (Vastaaja 1 / Yritys B).

Toimintasysteemin tulevaisuus onkin vahvasti kytköksissä siihen, millaisen otteen sen omistajaksi koettu kyberturvallisuuskeskus ottaa luottamusverkoston toiminnan kehittämiseen. Checkland ja Scholes (1990) määrittävät omistajan CATWOE prosessissa tarkoittavan ennen kaikkea tahoa, jolla on käytännön valta määrittää yhteistyön suuntaviivat tai lopettaa se kokonaan. Mikäli kyberturvallisuuskeskus ei tarjoa asiantuntijuuttaan, verkostojaan ja aktiivista tukeaan yhteistyölle, jäänee tiedonvaihdon kehittäminen tyngäksi. Sen sijaan, jos kyberturvallisuuskeskus onnistuu yhteistyössä keskusrikospoliisin kyberrikostorjuntakeskuksen kanssa määrittelemään tiedon vaihdon periaatteet ja tarjoamaan toimivat kanavat tilannetietoisuuden vaihtamiselle, voidaan tietoturvayritysten edustajien olettaa lähtevän alussa aktiivisesti mukaan tilannetietoisuuden vaihtoon. Pidemmän aikavälin onnistuminen riippuu puolestaan siitä, miten toimivaksi tuotokseksi jaetut havainnot pystytään muodostamaan.

4.2.6 Ympäristön rajoitteet

Checklandin (1981, 225) mukaan mitä tahansa toimintasysteemiä tarkasteltaessa myös ympäristön asettamat rajoitteet tulee huomioida. Ympäristön rajoitteilla hän tarkoittaa seikkoja, jotka hillitsevät toimintasysteemin kehitysmahdollisuuksia, mutta jotka toimijoiden on silti pakko hyväksyä. Esimerkkeinä toimintasysteemin ulkopuolisesta ympäristöstä johtuvista rajoitteista Checkland mainitsee esimerkiksi lainsäädännön rajoitteet sekä rajallisen budjetin asettamat raamit.

Tutkimuksen kohteena olevalle toimintasysteemin kehittämiselle ei ole asetettu erillistä budjettia, mikä tulee väistämättä asettamaan rajoitteita

yhteistyön syvyydelle. Vapaaehtoisuuteen perustuvalta yhteistyöltä, joka kuormittaa organisaation resursseja, ei voi odottaa liikoja. Tilannetietoisuuden jakaminen ei ole yhdenkään luottamusverkoston toimintaan osallistuvan organisaation ydintoimintaa, vaikka kaikki haastatellut tunnistavat, että yhteistyöstä on potentiaalisesti hyötyä osanottajille. Ollakseen osallistujille kannattavaa tulisi yhteistyöllä saavutettavan hyödyn olla toimijoiden kannalta suurempi kuin yhteistyöhön käytettävät investoinnit. Tämä tarkoittaa, että joko toiminnan lopputuotoksen tulisi olla taloudellisesti kannattava tuote tai vaihtoehtoisesti toiminnan rahoittaminen tulisi kanavoida luottamusverkoston ulkopuolelta.

Myös yhteistyöhön käytettävät henkilöresurssit tulevat väistämättä olemaan etenkin tietoturvayritysten puolesta rajalliset, joten luottamusverkoston työskentely tulisi tehdä mahdollisimman vaivattomaksi. Haastatellut eivät pääsääntöisesti kaipaa luottamusverkostosta keskustelufoorumia, vaan keinoa kehittää omaa havaintokykyään Suomessa tapahtuvaan tietoverkko-rikollisuuteen. Etenkin yritysten tekniset asiantuntijat kokevat, että yhteistyön tulisi olla enemmän teknisluonteista kuin keskustelevaa ja erilaisten tietoturvauhkien nopea kehittyminen luo paineita tietojenvaihdon saattamiseksi lähes reaaliaikaiseksi. Tämä tarkoittaisi paitsi toimivia kommunikointikanavia toimijoiden välille, myös jonkun asteista tiedonvaihdon automatisointia mikä edellyttäisi uusien toimivien työkalujen käyttöönottoa. Valtaosa vastaajista pitää tätä yhtenä edellytyksenä toiminnan kehittämiselle, eikä fyysisillä tapaamisilla uskota olevan riittävää lisäarvoa, jotta yhteistyön voisi rakentaa pelkästään niiden varaan. Vastuu toimintatapojen linjaamisesta ja työkalujen kehittämisestä tullee säilymään kehitystyön omistajien harteilla, mutta myös tietoturvayrityksistä löytynee kiinnostusta ottaa osaa jonkin asteiseen teknisten ratkaisuiden kehittämiseen.

Luottamusverkoston toimijoiden tulee hyväksyä myös se, että joko lainsäädännöstä tai asiakassopimuksista johtuvat salassapitovelvoitteet tulevat jatkossakin rajoittamaan vapaata tiedonvaihtoa. Jotta salassapitovelvoitteet eivät kuitenkaan rampauttaisi yhteistyöstä saatavia hyötyjä, tulisi toiminnassa pyrkiä siihen, että tieto anonymisoitaisiin ennen, kun se jaetaan verkostossa. Tämä muodostuisi kuitenkin haastateltujen yritysten edustajien mielestä liian kuormittavaksi vaatimuksesi ja tullee siten jäämään keskitetysti joko viranomaisten tehtäväksi tai teknologian avulla ratkaistavaksi seikaksi. Lisäksi avoimemman tiedonvaihdon kulttuurin lisääntyminen voisi vaikuttaa positiivisesti siten, etteivät yritykset yrittäisi piilotella niihin kohdistuneita tietoverkkorikoksia. Tietoturvayritykset voisivat näyttää tässä esimerkkiä yhdessä viranomaisten kanssa ja esittää tahdonilmaisun tai julkilausuman syvemmästä ja avoimemmasta tiedonvaihdosta tietoverkkorikollisuuden saralla.

4.2.7 Ydinmääritelmä

Pehmeässä systeemimetodologiassa kehitystyön kohteena oleva toimintasysteemille luodaan ydinmääritelmä (Root Definition), joka kuvaa

selkeästi mitä toimintasysteemin tulisi tehdä, miten ja minkä takia. Ydinmääritelmä pyrkii vangitsemaan toimintasysteemin syvimmän olemuksen, mutta koska se rakennetaan aina tietoisesti tietyn maailmankuvan mukaisesti, on se vain tapa tai väline tarkastella toimintasysteemiä. Checkland ja Poulter (2006) käyttävät ydinmääritelmän muodostamisessa apuna kirjainyhdistelmää PQR, jossa määritellään asia P, joka tulee tehdä tavalla Q, jotta voidaan saavuttaa R. Kun PQR –määritelmää rikastetaan CATWOE prosessissa tunnistetuilla tekijöillä, on mahdollista kuvata toimintasysteemin olemassaolon tarkoitus. Ydinmääritelmä ei siis välttämättä kuvaa toimintasysteemin tosiallista työskentelytapaa, vaan sen mitä systeemin tulisi saada aikaan. Myöhemmin ydinmääritelmän pohjalta on mahdollista visioida tosielämän rajoituksista välittämättä ideaalimalli, jonka mukaista toimintaa todellisuuteen vertaamalla on mahdollista tunnistaa toteutettavissa olevia kehitystoimenpiteitä.

Jokaisen haastateltavan antamien vastausten perusteella pyrittiin määrittelemään PQR -kaavan mukaisesti vastaukset kysymyksiin mitä (P) luottamusverkoston tulisi tehdä, miten (Q) ja miksi (R). Näitä vastauksia toisiinsa vertailemalla, oli mahdollista luoda kaksi vaihtoehtoista ydinmääritelmää tietoverkkorikollisuuden tilannetietoisuutta vaihtavalle luottamusverkostolle. Vaihtoehtoisissa ydinmääritelmissä tarkastelua ohjaavat maailmankuvat poikkeavat selkeästi toisistaan ensimmäisen korostaessa teknologiakeskeisyyttä ja toisen asiantuntijoiden välistä yhteistyötä. Teknologiakeskeisen ydinmääritelmän mukaan tietoverkkorikollisuuden tilannetietoisuutta vaihtava luottamusverkosto on:

> Viranomaisten ja yritysmaailman edustajien välinen anonyymisoitujen teknisten uhkatietojen ja muun vastaavan havaintodatan vaihtamiseen keskittyvä verkosto, jonka tarkoituksena on kerätä sellaista yhteismitallista dataa Suomessa havaitusta tietoverkkorikollisuuden elementeistä, jonka avulla voidaan muodostaa reaaliaikainen tilannetietoisuus suomalaisiin yrityksiin kohdistuvasta tietoverkkorikollisuudesta verkoston toimijoiden työn ohjaamiseksi sekä vaihtaa sellaisia tunnistetietoja, joiden avulla tietoverkkorikollisuutta pystytään torjumaan.

Kyseisessä ydinmääritelmässä muutosprosessi tapahtuu verkoston toimijoiden keräämän havaintodatan jalostuessa tilannetietoisuudeksi siitä, millaisia tietoverkkorikollisuuden elementtejä Suomessa on tietyllä ajanhetkellä havaittu. Tämä tilannetietoisuus on laajempi kuin yhdenkään yksittäisen toimijan omaan havaintokykyyn perustuva tietoisuus ja auttaa verkoston jäseniä ohjaamaan toimintaansa ajankohtaisilta uhkilta suojautumiseen. Mikäli ristiriita tietojen anonyymisoinnin (asiakastiedot) ja toisaalta riittävän tarkan datan jakamisen (uhka- ja tunnistetiedot) välillä pystytään ratkaisemaan, tarjoaa tietojen vaihto myös konkreettisen kyvyn puolustautua tietoverkkorikollisuutta vastaan. Suurin ero teknologiakeskeisen ja yhteistyötä korostavan ydinmääritelmän välillä on nimenomaan verkoston toiminnan konkreettisissa hyödyissä. Siinä missä ensiksi mainittu kehittää kykyä puolustautua entistä paremmin, tarjoaa yhteistyötä korostava ydinmääritelmä reaaliaikaisen tilannekuvan sijasta lähinnä syvällisempää ymmärrystä aikaisemmin tiettynä tarkasteluajanjaksona

havaituista ilmiöistä. Yhteistyötä korostavan ydinmääritelmän mukaan tietoverkkorikollisuuden tilannetietoisuutta vaihtava luottamusverkosto olisikin:

> Viranomaisten ja yritysmaailman edustajien välinen ilmiötason tilasto- sekä rikostiedustelutiedon vaihtamiseen keskittyvä verkosto, jonka säännöllisissä tapaamisissa käytyjen keskusteluiden perusteella olisi mahdollista muodostaa suuntaa-antavaa tilannetietoisuutta niistä suomalaisiin yrityksiin kohdistuneista tietoverkkorikollisuuden ilmiöistä, joita edeltävän tarkasteluajanjakson aikana on havaittu.

Kuvatun verkostotoiminnan hyödyt muodostuvat kasvavan ymmärryksen ja sitä kautta kehittyvän osaamisen myötä, mikä mahdollisesti edesauttaisi kutakin verkoston toimijaa palvelemaan omien intressiryhmiensä tarpeita. Verkoston toiminta olisi kuitenkin varsin reaktiivista ja tilannetietoisuus muodostuisi sen perusteella, mitä aikaisemmin on havaittu sen sijaan, että se kuvaisi mitä parhaillaan tapahtuu. Vaikka verkoston toiminta varmasti kasvattaisi toimijoiden ymmärrystä ajankohtaisista rikosilmiöistä, ei se välttämättä tarjoaisi välittömiä hyötyjä uhkilta suojautumiseen.

Jotta tietoverkkorikollisuuden tilannetietoisuutta jakavalle luottamusverkostolle pystyttiin muodostamaan vain yksi ydinmääritelmä, tehtiin päätös viedä ydinmääritelmä edellä esitettyjä määritelmiä abstraktimmalle tasolle. Tarkoituksena oli saada yhdistettyä molemmat aikaisemmat toimintamallit yhden kuvauksen alle, jolloin myöhemmin ideaalimallia määritettäessä olisi mahdollista ottaa huomioon molempien määritelmien vahvuudet. Ideaalitilanteessa anonyymisoitujen teknisten uhkatietojen ja muun vastaavan havaintodatan vaihtamista pystyttäisiin näin tukemaan toiminnalla, joka toisi mukaan kognitiivisen analyysin tason ja sitä kautta muodostuvan syvemmän ymmärryksen. Tämän ydinmääritelmän mukaan tietoverkkorikollisuuden tilannetietoisuutta vaihtava luottamusverkosto on:

> Viranomaisten ja yritysmaailman edustajien välinen anonyymisoitujen teknisten uhkatietojen ja muun vastaavan havaintodatan vaihtamiseen keskittyvä verkosto, joka pyrkii muodostamaan havaintoihin perustuvaa reaaliaikaista tilannetietoisuutta suomalaisiin yrityksiin kohdistuvasta tietoverkkorikollisuudesta ja jalostamaan sitä viranomaisten toimesta verkoston jäsenten osaamisen ja ymmärryksen kasvattamiseksi sekä tietoverkkorikollisuuden torjumiseksi.

CATWOE -analyysin perusteella ydinmääritelmän mukaisen luottamus-verkoston asiakkaita olisivat niin verkoston toimintaan osallistuvat toimijat kuin myös niiden loppuasiakkaat. Verkoston toimijoina olisivat sekä viestintäviraston kyberturvallisuuskeskus, keskusrikospoliisin kyberrikostorjuntakeskus sekä erikseen toimintaan mukaan kutsuttavat tietoturvayritykset. Muutosprosessi muodostuisi toimijoiden kerätessä kukin tahollaan tietoverkkorikoksia koskevaa dataa ja jakaessa sen muiden toimijoiden kanssa, silloin kun sen vakavuusaste ylittäisi yhdessä määritellyn kynnyksen. Tämän jälkeen viranomaiset

rikastaisivat havaintodataa maailmanlaajuista tietoverkkorikollisuutta koskevilla ilmiötiedoilla, mikäli sellaisia olisi saatavilla.

Maailmankuvassa korostuisi ehdoton luottamuksellisuus verkoston toimijoiden kesken jaetun tiedon suhteen, mutta ulospäin toiminnasta voitaisiin viestiä avoimen rohkaisevasti, jotta se kannustaisi myös muita yhteiskunnan toimijoita jakamaan tietoa niihin kohdistuneista tietoverkkorikoksista. Määritelmän mukaisen toiminnan omistajaksi koetun kyberturvallisuus-keskuksen tehtäväksi jäisi määritellä yhteistyössä KRP:n kyberrikostorjuntakeskuksen kanssa sovellettavat tiedon vaihdon periaatteet sekä tarjota toimivat kanavat havaintodatan keräämiselle ja vaihtamiselle. Ympäristön esittämistä rajoitteista hyväksyttäisiin vallitsevana olosuhteena se, että joko lainsäädännöstä tai asiakassopimuksista johtuvat salassapitovelvoitteet tulevat rajoittamaan vapaata tiedonvaihtoa. Näiden rajoitteiden aiheuttamia haittoja pyrittäisiin kuitenkin minimoimaan anonyymisoimalla dataa, joko viranomaisten toimesta tai siihen soveltuvan teknologisen ratkaisun avulla.

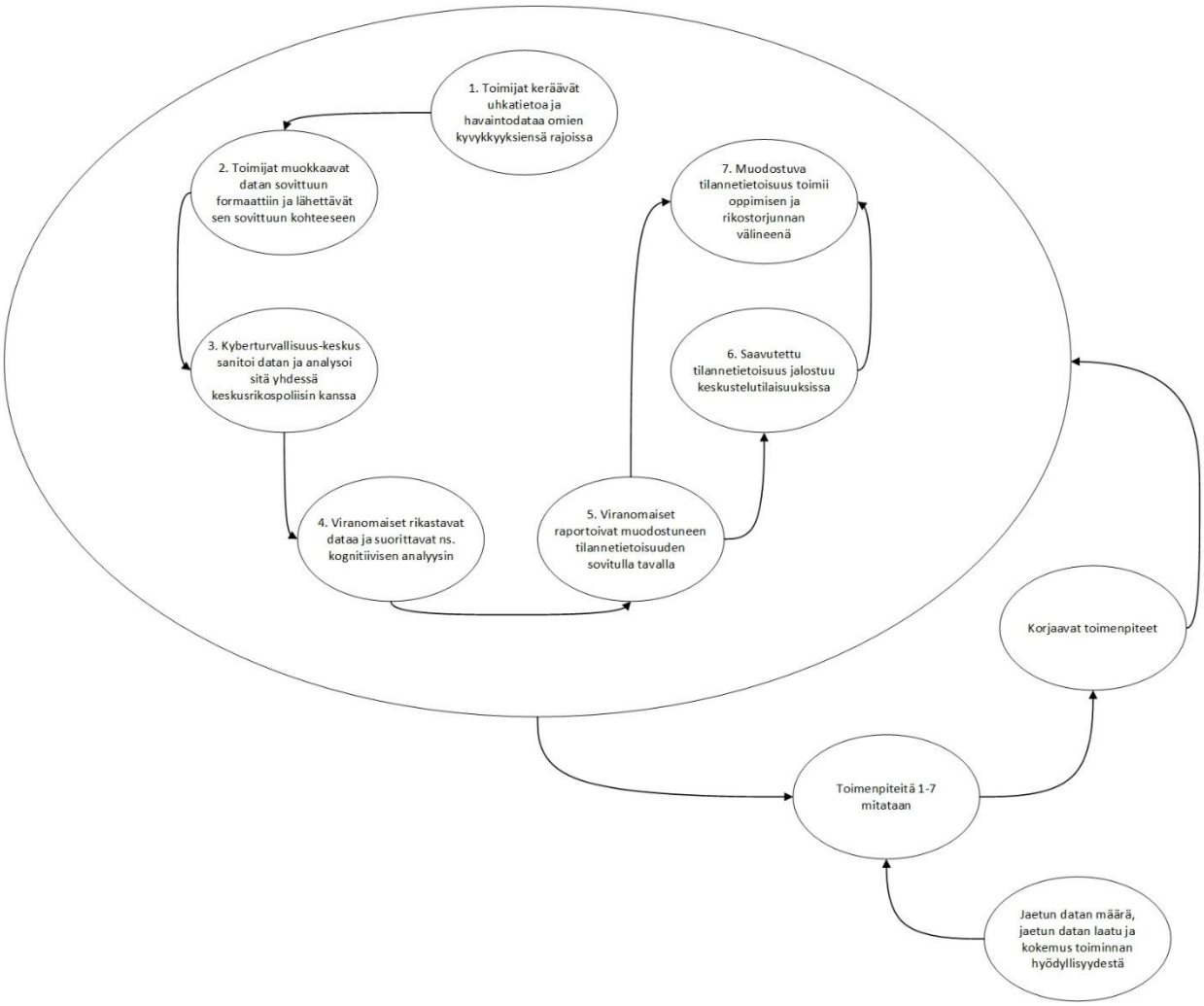
Seuraavassa alaluvussa on esitetty tarkempi ideaalimalli siitä, millä tavalla luottamusverkoston toiminta tulisi organisoida, jotta sillä olisi potentiaalia toimia esitetyn ydinmääritelmän mukaisesti. Ideaalimallin mukaista toimintaa todellisuuteen vertaamalla voidaan tämän jälkeen tunnistaa toteutettavissa olevia kehitystoimenpiteitä, joiden avulla luottamusverkoston toimintaa voidaan kehittää.

4.3 Ideaalimalli

Checkland ja Poulter (2006) mukaan ideaalimallin (*conceptual model*) luomisen tarkoituksena on koota aikaisempien analyysivaiheiden tulokset. Niiden perusteella muodostetaan ideaalimalli, jossa sarja toisiaan seuraavia toimenpiteitä esittää, miten tietystä syötteestä muodostuu muutosprosessin kautta tuotos, eli sellainen lopputulos, jota ydinmääritelmän mukaisen toimintasysteemin voi tulkita tavoittelevan. Jokaisen toimenpiteen tulee olla johdettavissa takaisin ydinmääritelmään, jotta ideaalimalli olisi puolustettavissa. Checkland ja Poulter painottavat, että malli ei ole koskaan absoluuttisesti oikeassa ja huolellisestikin rakennettu malli on korkeintaan hyvin perusteltu. Eri ihmiset voivat tulkita saman ydinmääritelmän sanoja eri tavalla ja siksi muodostaa sen pohjalta erilaisia ideaalimalleja. Ydinmääritelmän perusteella ei siis koskaan voi luoda vain yhtä oikeaa mallia. Ideaalimallin tärkein tehtävä onkin toimia keskustelun välineenä ja herättää tunteita ja mielipiteitä niissä henkilöissä, jotka osallistuvat kehittämisprosessiin (Checkland & Poulter, 2006).

Edellisessä luvussa esitetyn ydinmääritelmän mukaisessa toimintasysteemissä muutosprosessin syötteinä olisivat toimijoiden tietyllä ajan hetkellä havaitsemat tietoverkkorikollisuuden elementit. Ollakseen merkityksellistä luottamusverkoston toimijoille, tulisi jatkokäsittelyyn valittujen havaintojen ylittää vakavuusasteeltaan yhdessä sovittu kynnys. Ideaalissa tilanteessa tämä data muokattaisiin automaattisesti tai manuaalisesti yhteisesti

sovittuun formaattiin, anonymisoitaisiin ja koottaisiin yhdessä sovittuun paikkaan. Tämä mahdollistaisi muutosprosessin käynnistämisen, jossa luottamusverkoston viranomaisjäsenet voisivat yhdessä analysoida ja rikastaa tietoturvayrityksiltä saatavaa havaintodataa. Näiden eri lähteistä saattavien havaintojen perusteella muodostettua tilannetietoisuutta raportoitaisiin tämän jälkeen takaisin kaikille verkoston toimijoille. Kukin toimija voisi tulkita muodostuvaa tilannetietoisuutta tehdäkseen oman toimintansa kannalta relevantteja ennustuksia tietoverkkorikollisuuden tilasta lähitulevaisuudessa sekä käyttää tietoa oppimisen ja mahdollisesti myös suoraan rikostorjunnan välineenä. Syvällisen ymmärryksen saavuttamiseksi sekä ennen kaikkea luottamuksen rakentamiseksi ja ylläpitämiseksi luottamusverkosto voisi lisäksi kokoontua esimerkiksi puolivuosittain kasvotusten keskustelemaan tietoverkkorikollisuuden tilanteesta Suomessa. Havainnekuva ideaalimallin mukaisesta toiminnasta on esitetty kuviossa 8.



KUVIO 8 Ideaalimalli

Kuviossa 8 esitetyn ideaalimallin mukaisessa toiminnassa kukin toimija keräisi tahollaan uhkatietoa suomalaisiin yrityksiin kohdistuvasta tietoverkkorikollisuudesta, kuten havaintodataa sekä tietoa erityisen vakavista tai merkittävistä tietoturvaloukkauksista (kohta 1). Sovitun ilmoituskynnyksen ylittävien havaintojen jakaminen tapahtuisi automatisoidun tiedonvaihdon mahdollistavassa arkkitehtuurissa viestintäviraston organisoimana ja fasilitoimana selkeästi määriteltyä yhteistä toimintamallia mukaillen, toimivilla interaktiivisilla ja reaaliaikaisen viestinnän mahdollistavilla työkaluilla toteutettuna (kohta 2). Tämän jälkeen viestintäviraston kyberturvallisuuskeskus kokoaisi ja sanitoisi havaintodatan käsitellen sen samalla siten, että se esitysmuodossaan tuottaisi lisäinformaatiota luottamusverkoston toimijoille sekä jalostaisi tietoa muiden viranomaisten avustamana niin, että mukaan pystytäisiin tuomaan kognitiivinen analyysitaso, jonka avulla pystyttäisiin hahmottamaan laajempia kokonaisuuksia ja ymmärtämään yksittäisten havaintojen konteksti (kohdat 3-4).

Kohdassa 5 viranomaiset kokoaisivat tiedon ja jakaisivat sen takaisin luottamusverkoston toimijoille sovittuja kanavia pitkin. Näin olisi mahdollista muodostaa tilannetietoisuutta Suomessa tiettynä ajanhetkenä tapahtuvasta tietoverkkorikollisuudesta ja raportoida siitä esimerkiksi yrityssegmenteittäin. Tietoturvayritykset saavuttaisivat tämän perusteella kohdassa 7 kyvyn tuottaa parempaa kohdistettua palvelua loppuasiakkailleen, jotka puolestaan pystyisivät ryhtymään ennakoiviin toimenpiteisiin välittömien uhkien torjumiseksi.

Viranomaiset pystyisivät hyödyntämään tuotettavaa tilannetietoisuutta oman tilannetietoisuutensa muodostamisessa, jolloin myös vakavien tai laaja-alaisten tietoturvaloukkausten vaikutuksia suomalaiseen yhteiskuntaan olisi helpompi arvioida. Poliisiviranomaiset pystyisivät kohdistamaan entistä paremmin omaa rikostiedusteluaan, jolloin syyllisiä voitaisiin saattaa vastuuseen. Kyberturvallisuuskeskus pystyisi puolestaan edelleen raportoimaan muodostettavaa tilannetietoisuutta kaikkia suomalaisia yrityksiä hyödyttävällä tavalla säännöllisin väliajoin sekä tarvittaessa varoittamaan yhteiskunnallisesti merkittäviä toimijoita havaituista tietoturvauhista, minkä ansiosta suomalaisyritykset voisivat kohdistaa omat resurssinsa ajankohtaisten uhkien torjuntaan. Näin suomalaisten organisaatioiden tietoturvakyvykkyydet kasvaisivat, jolloin ne pystyisivät paremmin suojaamaan omia loppuasiakkaitaan ja omalta osaltaan ylläpitämään yhteiskunnan kyberturvallisuutta.

Ideaalimallin mukaan toimivan luottamusverkoston toimintaan osallistuvien tahojen osaamisen taso, sekä kyvykkyys palvella omia intressiryhmiään kasvaisi vähitellen, kun havaittuja tietoverkkorikoksia käsiteltäisiin yhdessä viranomaisten kanssa kasvoittain järjestettävissä keskustelutilaisuuksissa. Samalla viranomaisille muodostuisi todenmukaisempi käsitys siitä, millaisia tietoverkkorikoksia Suomessa tapahtuu ja millaisia vaikutuksia rikoksilla on niiden uhreihin. Kukin voisi käyttää tietoa tahollaan parhaaksi katsomallaan tavalla ajankohtaisen tietoverkkorikollisuuden

torjumiseksi. Tiivis yhteistyö viranomaisten kanssa parantaisi mahdollisesti myös luottamusverkoston toimijoiden julkisuuskuvaa ja rohkaisisi myös muita verkoston ulkopuolisia toimijoita avoimempaan tietojenvaihtoon, minkä seurauksena kynnys ilmoittaa tietoverkkorikollisuudesta saattaisi laskea. Tällöin viranomaiset voisivat kohdistaa keinovalikoimaansa entistä tehokkaammin yrityksiä ja yhteisöjä uhkaavan tietoverkkorikollisuuden torjumiseen. Tämä vaikuttaisi positiivisesti niin yritysten, yhteisöjen ja kansalaistenkin mahdollisuuksiin suojautua erilaisia ajankohtaisia kyberuhkia vastaan, jolloin koko yhteiskunnan kyberturvallisuus kasvaisi.

Checkland ja Poulter (2006) huomauttavat, että ideaalimallia rakennettaessa tulisi aina ottaa huomioon myös, että muutosprosessin tulisi olla mitattavissa. He ehdottavat mitattaviksi määreiksi toiminnan vaikuttavuutta (*efficacy*), hyötysuhdetta (*effiency*) sekä toiminnan tehokkuutta (*effectiveness*). Toisin sanoen muutosprosessin tulisi tuottaa odotettu tuotos, eli olla vaikuttavaa. Muutos pitäisi saavuttaa mahdollisimman pienin ponnisteluin, eli sen hyötysuhteen tulisi olla positiivinen. Lisäksi muutosprosessin tulisi olla tehokasta siten, että tuotokset todella auttavat saavuttamaan myös pidemmän aikavälin tavoitteen.

Mahdollisia vaikuttavuuden, hyötysuhteen sekä toiminnan tehokuuden mittareita tiedusteltaessa haastateltavat ehdottivat esimerkiksi jaettavien havaintojen määrän sekä niiden laadun mittaamista. Lisäksi mitattavaksi ehdotettiin kokemusta toiminnalla saavutettavista hyödyistä, sekä pidemmällä aikavälillä Suomen kyberturvallisuuden tilaa, jonka objektiivisen mittaamisen todettiin kuitenkin olevan erittäin hankalaa. Eräs haastateltavista ehdotti myös, että toiminnan tehokkuutta voisi mitata seuraamalla rikostilastojen kasvua. Kasvava määrä tietoverkkorikoksia voisi haastatellun mukaan antaa vihjeitä siitä, että yhteistyö toimii ja rikoksia paljastuu entistä enemmän.

> Niin tässä vois ajatella, että on mahdollisuus nyt tähän olemassa olemaan rakenteeseen tukeutuen ja sen päälle rakentuen saamaan jotain voittoja ihan suomalaisten rikostilastojen kaunistamiseksi. Luulen, että se rikostilastojen kaunistaminen tässä kohtaa tarkoittaa, että kirjattujen rikosten määrä pomppaa kymmenen-, sata- tai tuhatkertaiseksi. Se on minulle kaunista (Vastaaja 1 / Yritys B).

Haastateltavien ehdotuksista valittiin vaikuttavuuden mittariksi jaettavan havaintodatan määrä, jota seuraamalla voitaisiin arvioida, toimiiko yhteistyö odotetulla tavalla ja saadaanko jaetulle datalle myös vastinetta. Hyötysuhteen mittaamiseen valittiin toimijoiden kokemus toiminnan hyödyllisyydestä ja toiminnan tehokkuutta voitaisiin seurata jaettavan datan laatua seuraamalla. Laadulla tarkoitetaan tässä yhteydessä sitä, että onko jaettava havaintodata siinä määrin merkityksellistä, että sen perusteella pystytään aidosti muodostamaan tilannetietoisuutta suomalaisia yrityksiä uhkaavasta tietoverkkorikollisuudesta. Myös muutosprosessin mittarit sekä niiden perusteella tehtävät korjaavat toimenpiteet on mallinnettu kuvioon 8.

4.4 Ideaalimallit ja todellisuus

Edellisessä alaluvussa kuvatun ideaalimallin tarkoitus ei ole nimestään huolimatta esittää kiistatonta määritelmää siitä, miten luottamusverkoston tulisi ideaalitilanteessa toimia. Pikemminkin sen on tarkoitus herättää lukijassa ajatuksia ja kysymyksiä, joihin vastauksia tarjoamalla pystytään mahdollisesti määrittelemään sellaisia toimenpiteitä, joiden avulla luottamusverkoston toimintaa on mahdollista kehittää. Checkland ja Poulter (2006) huomauttavatkin, ettei ideaalimallin ole tarkoituskaan kuvata todellisuutta. Ideaalimalli perustuu tiettyyn puhtaaseen maailmaankuvaan, kun taas ihmisten välisessä kanssakäymisessä erilaisia maailmankuvia on lukemattomia ja ne saattavat muuttua välillä hyvinkin nopeasti. Ideaalimalli tarjoaa mahdollisuuden jäsenneltyyn keskusteluun, jonka avulla on mahdollista luoda kehitysedotuksia järjestelmällisesti vertaamalla ideaalimallia ja todellisuutta toisiinsa.

Tyypillisesti pehmeässä systeemimetodologiassa kysytään Checkland ja Poulter (2006) mukaan ideaalimallin perusteella kysymyksiä kuten ”Toteutuuko ideaalimallin kohdassa x kuvattu toimenpide todellisuudessa, kuka sen toteuttaa, miten, miksi, miten muuten sen voisi toteuttaa?”. Kysymyksiä voidaan esittää myös eri toimenpiteiden välisiin riippuvuuksiin liittyen, kuten ”Ideaalimallissa tämä tietty toimenpide riippuu edellisessä kohdassa kuvatusta toimenpiteestä, onko näin myös todellisuudessa?”. Heidän mukaansa kysymysten muodostamisessa voi käyttää tarvittavaa luovuutta ja vastausten perusteella voidaan esimerkiksi luoda taulukko, joka kuvaa toimintasysteemin tunnistettuine kehityskohtineen verrattain tarkasti. Taulukon perusteella voidaan tarvittaessa luoda uusi ydinmääritelmä ja ideaalimalli, joiden mukaiseksi systeemin toimijat ovat valmiita muuttamaan omaa toimintaansa. Näin pehmeälle systeemimetodologialle tyypillinen syklinen oppimisprosessi jalostaa mallia eteenpäin kohti yhteisesti hyväksyttyä toimintaa (Checkland & Poulter 2006).

Checkland ja Poulter (2006) painottavat lisäksi, ettei tarkoituksena ole löytää täydellistä yhteisymmärrystä toimijoiden kesken, vaan pikemminkin muodostaa sellainen kompromissi, jonka kanssa eri toimijat pystyvät elämään. Täydellisen yhteisymmärryksen saavuttaminen on heidän mukaansa verrattain harvinaista niissä ongelmalliseksi koetuissa tilanteissa, joissa tavoitteena on muokata tietyn organisaation tai organisaatioiden toimintaa. Näissä tilanteissa jonkin asteinen kompromissi on yleensä välttämätön edellytys sille, että tilanteen kehittämiseksi pystytään ylipäätään tekemään päätöksiä (Checkland & Poulter 2006).

Tietoverkkorikollisuuden tilannetietoisuutta jakavan luottamusverkoston toiminnan nykytilan ja sen yksityiskohtien kuvaaminen yllä esitettyjen kysymysten avulla ei olisi mahdollista osana julkista opinnäytetyötä. Tästä syystä empiirisen aineiston pohjalta luotua ideaalimallia verrataan todellisuuden sijasta niihin kirjallisuuskatsauksen havaintoihin, jotka nostettiin esiin teoreettisen viitekehyksen esittelyn yhteydessä. Näiden havaintojen katsotaan

heijastavan tutkimuksen lähtökohtiin nähden riittävän tarkasti tilannetietoisuuden muodostamiseen liittyvää todellisuutta, johon ideaalimallia voidaan verrata. Tarkoituksena on reflektoida aikaisemmin tässä luvussa esitettyjä ajatuksia ja verrata niitä työn alussa esitettyyn teoriaan sekä ideaalimallin mukaiseen toimintaan. Näin pystytään määrittelemään sellaisia kehitysehdotuksia, joita luottamusverkoston toimijoille voidaan perustellusti ehdottaa toteutettavaksi. Tässä tutkimuksessa ideaalimallin ja todellisuuden herättämällä keskustelulla tarkoitetaan vuoropuhelua empiiriseen haastatteluaineistoon pohjautuvan ideaalimallin, sekä esitetyn teoreettisen viitekehyksen välillä. Vuoropuhelun avuksi luotiin taulukko 2, joka on esitetty seuraavalla sivulla.

<table>
<tr><th colspan="2">Empiirisen haastatteluaineiston perusteella luotu ideaalimalli</th><th colspan="4">Teoreettinen viitekehys</th></tr>
<tr><td colspan="2">Miten tilannekuvan jakaminen kannattaa toteuttaa?</td><td colspan="4">Mistä tiedoista tietoverkkorikollisuuden tilannetietoisuus kannattaa rakentaa?</td></tr>
<tr><td>Millaisista toimenpiteistä luottamusverkoston toiminta voisi mudostua?</td><td>Miten toiminnan vaikutusta, hyötysuhdetta ja tehokkuutta voisi mitata?</td><td>Miten syvä tilannetietoisuuden taso tulisi muodostaa?</td><td>Mistä elementeistä tietoverkkorikollisuuden tilannetietoisuus muodostuu?</td><td>Mitkä seikat edesauttavat tilannetietoisuuden jakamista?</td><td>Mitkä seikat haittaavat tilannetietoisuuden jakamista?</td></tr>
<tr><td>1. Toimijat keräävät uhkatietoa ja havaintodataa omien kyvykkyyksiensä rajoissa</td><td rowspan="3">Jaetun datan määrä (vaikutus)</td><td rowspan="3">Taso 1 tilanteessa vallitsevien elementtien havaitseminen</td><td rowspan="7">Luvaton pääsy dataan

Luvaton pääsy tietojärjestelmään tai -verkkoon

Järjestelmän tai datan luvaton häiritseminen

Haittaohjelmien ja muiden väärinkäyttöön tarkoitettujen työkalujen tuotanto, jakelu ja ylläpito</td><td>Taloudelliset kannustimet yksityiskohtaisten ja totuudenmukaisten tietojen jakamiseen</td><td rowspan="7">Vapaamatkustajailmiö.

Luottamuksen puute

Tulkintaan käytettävän yhtenevän sisäisen mallin puuttuminen</td></tr>
<tr><td>2. Toimijat muokkaavat datan sovittuun formaattiin ja lähettävät sen sovittuun kohteeseen</td><td>Tehokkaat kommunikointikanavat tai jaettu tilannekuvanäkymä</td></tr>
<tr><td>3. Kyberturvallisuuskeskus sanitoi datan ja analysoi sitä yhdessä keskusrikospoliisin kanssa</td><td>Kaikkien ei tarvitse tehdä samoja asioita</td></tr>
<tr><td>4. Viranomaiset rikastavat dataa ja suorittavat ns. kognitiivisen analyysin</td><td rowspan="2">Jaetun datan laatu (tehokkuus)</td><td rowspan="2">Taso 2 Tilanteessa vallitsevien elementtien merkityksen ymmärtäminen</td><td>Toisten ryhmien panoksen ymmärtäminen on tärkeää yhteisten tavoitteiden saavuttamiselle</td></tr>
<tr><td>5. Viranomaiset raportoivat muodostuneen tilannetietoisuuden sovitulla tavalla</td><td>Sellaista mikä on tarpeen tietää kaikille luottamusverkoston toimijoille</td></tr>
<tr><td>6. Saavutettu tilannetietoisuus jalostuu keskustelutilaisuuksissa</td><td rowspan="2">Kokemus toiminnan hyödyllisyydestä (hyötysuhde)</td><td rowspan="2">Taso 3 Ennusteen luominen elementtien tilanteesta lähitulevaisuudessa</td><td>Kokemus yhteisestä missiosta</td></tr>
<tr><td>7. Muodostuva tilannetietoisuus toimii oppimisen ja rikostorjunnanvälineenä</td><td>Voitava käyttää päätöksenteon apuna</td></tr>
</table>

Taulukosta 2 pystyy havaitsemaan ideaalimalleissa esitettyjen toisiaan seuraavien toimenpiteiden ja teoreettisen viitekehyksen suhteen toisiinsa. Ideaalimalli vastaa siihen millaisista toimenpiteistä luottamusverkoston toiminta voisi muodostua sekä siihen, miten toiminnan vaikutusta, hyötysuhdetta ja tehokkuutta voisi mitata. Teoreettisen viitekehyksen avulla on puolestaan mahdollista vastata kunkin toimenpiteen kohdalta kysymyksiin:

- Miten syvä tilannetietoisuuden taso tulisi muodostaa?
- Mistä elementeistä tietoverkkorikollisuuden tilannetietoisuus tulisi rakentaa?
- Mitkä seikat edesauttavat tilannetietoisuuden jakamista?
- Mitkä seikat haittaavat tilannetietoisuuden jakamista?

Taulukon 2 ensimmäisen loogisen kokonaisuuden muodostaa ideaalimallin kolme ensimäistä toimenpidettä, jotka ovat uhkatietojen kerääminen, datan muokkaus ja eteenpäin lähettäminen sekä datan sanitointi ja alustava analyysi. Teoreettisen viitekehyksen perusteella esitetään, että todellisuudessa tässä loogisessa kokonaisuudessa keskityttäisiin tason 1 tilannetietoisuuden muodostamiseen, jolloin tarkoituksena olisi vain havaita, kerätä ja jakaa havaintoja tietoverkkorikollisuuden elementeistä. Tämä lähestyminen vaikuttaisi haastatteluiden perusteella sopivan erityisesti teknisten asiantuntijoiden tilannetietoisuustarpeisiin, mutta tukisi toisaalta myös organisaatioiden johdon tilannetietoisuutta ympäröivästä todellisuudesta. Toiminnan käynnistymistä todellisuudessa edesauttaisivat taloudelliset kannustimet yksityiskohtaisten tietojen jakamiseen (Gordon, Loeb & Lucyshyn 2003), tehokkaat kommunikointikanavat tai jaettu tilannekuvanäkymä (Endsley, 1995; Endsley & Jones, 1997) sekä selkeä roolien jako (Endsley & Jones, 1997). Toiminnan vaikuttavuutta pystyttäisiin tässä kohtaa seuraamaan karkeasti mittaamalla jaetun datan määrää, jolloin olisi mahdollista havaita, vaihdetaanko tietoa ennakko-odotusten mukaisesti. Haastatteluiden perusteella Viestintäviraston kyberturvallisuuskeskus nähtäisiin luontevana tahona tilannetietoisuuden kokoamiseen.

Toisen loogisen kokonaisuuden muodostavat ideaalimallin toimenpiteet neljä ja viisi, jossa viranomaiset analysoisivat ja rikastaisivat tietoturvayrityksiltä kerättyä dataa, sekä raportoisivat saavutetun tilannetietoisuuden takaisin tietoturvayrityksille. Teoreettisen viitekehyksen perusteella tässä vaiheessa olisi tärkeää, että viranomaiset ymmärtäisivät nimenomaisesti muiden luottamusverkoston toimijoiden panoksen yhteisen tavoitteen saavuttamiselle (Endsley & Jones, 1997) ja raportoisivat aktiivisesti keskeisiä seikkoja saavutetusta tilannetietoisuudesta takaisin muille luottamusverkoston toimijoille. Vaikka kaikkia yksityiskohtia ei raportoitaisikaan takaisin luottamusverkoston jäsenille, tulisi viranomaisten kyetä raportoimaan toimijoille takaisin ne seikat, jotka niiden olisi oleellista tietää sekä oman toimintansa että luottamusverkoston yhteisen tavoitteen kannalta (Endsley, 1995). Tämä myös edesauttaisi jokaista toimijaa rakentamaan tahollaan tason 2 tilannetietoisuutta,

jossa vallitsevien tietoverkkorikollisuuden elementtien merkitys omaan toimintaan olisi mahdollista ymmärtää. Toiminnan tehokkuutta voitaisiin arvioida mittaamalla jaettavan datan laatua, eli sitä, että onko jaettava havaintodata siinä määrin merkityksellistä, että sen perusteella pystytään aidosti muodostamaan tason 2 tilannetietoisuutta suomalaisia yrityksiä uhkaavasta tietoverkkorikollisuudesta.

Mikäli luottamusverkoston toimijat pystyisivät todella ideaalimallissa kuvattujen toimenpiteiden avulla ymmärtämään tilanteessa vallitsevien tietoverkkorikollisuuden elementtien merkityksen, ei mikään estäisi niitä muodostamasta myös ennustetta tilanteen kehittymisestä lähitulevaisuudessa. Näin ne voisivat muodostaa tason 3 tilannetietoisuutta ympäröivästä todellisuudesta, jota kunkin olisi tahollaan mahdollista käyttää myös päätöksenteon apuna tietoverkkorikollisuuden torjumisessa. Tätä tietoisuutta olisi mahdollista edelleen jalostaa yhteisissä keskustelutilaisuuksissa. Nämä kaksi toimenpidettä yhdessä muodostaisivat viimeisen loogisen kokonaisuuden, joiden myötä kiteytyisi myös luottamusverkoston kokemus yhteisestä missiosta, joka Endsley ja Jones mukaan (1997) toimii perustana tulevaisuuden tilannetietoisuustarpeen ja yhteistyön tavoitteiden määrittämiselle. Luottamusverkoston toimijoiden kokemusta yhteistyön hyödyllisyydestä tulisi mitata säännöllisin väliajoin, jotta varmistettaisiin tavoiteltujen tulosten saavuttaminen mahdollisimman pienin ponnisteluin.

Taulukossa kolme on esitetty myös niitä tunnistettuja seikkoja, jotka saattavat haitata tilannetietoisuuden jakamista läpi koko ideaalimallin mukaisen toiminnan. Näitä ovat vapaamatkustajailmiö ja luottamuksen puute sekä toisaalta myös jaetun tiedon tulkintaan käytettävän yhtenevän sisäisen mallin puuttuminen, joka voi vaikuttaa eri toimijoiden kokemukseen koko toiminnan mielekkyydestä (Hausken 2007; Gordon, Loeb & Lucyshyn, 2003). Jaetun datan määrän mittaaminen voisi osaltaan toimia vakuutuksena kaikille toimijoille, että toiminnan osallistumisastetta mitataan ja vapaamatkustajia ei sallita. Luottamusta eri toimijoiden voisi rakentaa puolestaan kasvoittain tapaamisissa, joissa voitaisiin myös yhdessä tulkita saavutettua tilannetietoisuutta ja muodostaa yhteinen sisäinen malli siitä, miten tietoisuutta tulisi jatkossa tulkita parhaan mahdollisen lopputuloksen saavuttamiseksi.

5 Johtopäätökset

Tässä luvussa on kuvattu tutkimuksen johtopäätökset. Luku on jaettu kahteen osaan, joista ensimmäisessä on vastattu tutkimuksen luvussa 3.1.1. esitettyihin tutkimuskysymyksiin. Toisessa osassa on esitetty tehtyjen johtopäätösten perustella konkreettisia kehitystoimenpiteitä, joiden avulla luottamusverkoston toimijat voivat halutessaan ryhtyä selvittämään olisiko tutkimuksessa esitetyn ideaalimalin mukainen tietoverkkorikollisuuden tilannetietoisuuden jakaminen mahdollista käynnistää ja pohtimaan mitä se käytännössä edellyttäisi luottamusverkoston toimijoilta.

5.1 Tutkimustulokset

Tämän tutkimuksen rungon muodostivat kaksi pääkysymystä, joista ensimmäiseen vastaamalla selvitettiin, mistä tiedoista tietoverkkorikollisuuden tilannetietoisuus kannattaa rakentaa. Tutkimuksen alussa analysoitiin kirjallisuuskatsauksen perusteella kyberrikollisuutta ilmiönä sekä luotiin määritelmä tietoverkkorikollisuudelle. Tässä tutkimuksessa tietoverkkorikollisuuden katsotaan tarkoittavan ainoastaan tietoliikenneverkoissa esiintyviä rikoksia, jotka loukkaavat tietoverkoissa tai niihin liitetyissä järjestelmissä käsiteltävän tiedon luottamuksellisuutta, eheyttä tai saatavuutta. Tietoverkkorikollisuuden tunnusmerkistön täyttävissä teoissa toteutuvat aina tietyt elementit, jotka ovat:

- Luvaton pääsy dataan
- Luvaton pääsy tietojärjestelmään tai -verkkoon
- Järjestelmän tai datan luvaton häiritseminen
- Haittaohjelmien ja muiden väärinkäyttöön tarkoitettujen työkalujen tuotanto, jakelu ja ylläpito.

Tietoverkkorikollisuuden tilannetietoisuuden katsotaan muodostuvan portaittain kasvavasta tietoisuuden tilasta, jossa ensimmäisellä tasolla havaitaan tietoverkkorikollisuuden elementtejä, toisella tasolla ymmärretään niiden merkitys omalle toiminnalle ja tasolla kolme pystytään luomaan ennustus elementtien tilan kehittymisestä lähitulevaisuudessa, jolloin saavutettua tilannetietoisuutta voidaan käyttää päätöksenteon apuna.

Tutkimuksen toiseen pääkysymykseen vastaamalla tarkasteltiin, miten tietoverkollisuuden tilannetietoisuutta kannattaisi jakaa tutkimuksen kohteena olevassa luottamusverkostossa. Luvussa 2 luodun teoreettisen viitekehyksen perusteella tilannetietoisuuden jakamista luottamusverkostossa edesauttaisivat taloudelliset kannustimet sekä tehokkaat kommunikointikanavat tai jaettu tilannetietoisuusnäkymä. Lisäksi tilannetietoisuuden jakamiseen vaikuttaisi

positiivisesti selkeä roolijako, kokemus yhteisestä missiosta, sekä luottamusverkoston muiden toimijoiden panoksen ymmärtäminen. Jaettavan tiedon tulisi olla sellaista, minkä tietäminen olisi tarpeellista kaikille luottamusverkoston toimijoille ja sen avulla saavutettavan ymmärryksen tulisi mahdollistaa tilannetietoisuuden käyttäminen päätöksenteon apuna. Tilannetietoisuuden jakamista puolestaan haittaisivat vapaamatkustajailmiö, luottamuksen puute sekä tulkintaan käytettävän yhtenevän sisäisen mallin puuttuminen.

Tutkimuksen empiirisessä osiossa analysoitiin haastatteluissa saatu aineisto pehmeän systeemimetodologian mukaisesti toteuttamalla kolme perusanalyysiä (interventioanalyysi, sosiaalisen systeemin analyysi sekä poliittisen systeemin analyysi). Tämän jälkeen tehtiin CATWOE-prosessin avulla tietoverkkorikollisuuden tilannetietoisuutta jakavan luottamusverkoston ydinmääritelmä ja kuvattiin ideaalimalli, jossa sarja toisiaan seuraavia toimenpiteitä esittää, miten tietystä syötteestä muodostuu muutosprosessin kautta tuotos, jota ydinmääritelmän mukaisen toimintasysteemin voi tulkita tavoittelevan. Lopuksi tätä ideaalimallia verrattiin teoreettiseen viitekehykseen, jonka katsotaan heijastavan tutkimuksen lähtökohtiin nähden riittävän tarkasti tilannetietoisuuden muodostamiseen liittyvää todellisuutta ja mahdollistavan sen, että tutkimustuloksia voidaan käsitellä osana julkista opinnäytetyötä.

Interventioanalyysissä määritettiin kehitysprosessin asiakkaaksi keskusrikospoliisin kyberrikostorjuntakeskus, ongelman käsittelijäksi kehitysprosessin organisoimista tarkasteleva tutkija ja ongelman omistajiksi kollektiivisesti luottamusverkoston toimintaan osallistuvat organisaatiot. Sosiaalisen systeemin analyysissä tarkasteltiin, miten muutos on kulttuurisesti toteutettavissa toimintasysteemissä ja millaisten arvojen ja toimintatapojen kanssa sen on sovittava yhteen.

Tietoverkkorikollisuuden tilannetietoisuuden vaihtamisen tulisi palvella niin viranomaisten tarvetta kehittää konkreettista tilannetietoisuusnäkymää tapahtuviin rikoksiin, kuin myös lisätä yritysten edustajien ymmärrystä Suomessa tapahtuvista tietoverkkorikoksista sekä niiden taustalla vaikuttavista ilmiöistä. Edellytyksenä tietoisuuden vaihtamiselle on, että tilannetietoisuustyö noudattaa ryhmässä havaittuja normeja, joita ovat ehdoton luottamuksellisuus, tiedon vaihdon vastavuoroisuus sekä (vielä määrittelemättömien) toimintaohjeiden noudattaminen. Toiminnassa arvostetaan mahdollisimman avointa, mutta salassapitovelvoitteita kunnioittavaa yhteistyötä, teknistä osaamista sekä yhteiskuntavastuuta. Poliittisen systeemin analyysissä pureuduttiin luottamusverkostossa vallitseviin valtasuhteisiin, käsiteltiin luottamusverkoston toimintaan osallistuvien yritysten epäluuloa kilpailijoiksi koettuja tahoja kohtaan ja tunnistettiin, että viestintäviraston kyberturvallisuuskeskus koetaan luontevimmaksi tahoksi koordinoimaan yhteistyötä, koska verkoston toimijoilla on jo ennestään toimiviksi koetut suhteet keskuksen kanssa.

Tietoverkkorikollisuuden tilannetietoisuutta vaihtavan luottamus-verkoston ydinmääritelmä rakennettiin tunnistamalla ja nimeämällä

luottamusverkoston muodostaman toimintasysteemin osatekijät sekä näiden väliset vaikutussuhteet CATWOE -prosessin avulla. Ydinmääritelmän mukaisessa toimintasysteemissä tietoverkkorikollisuuden tilannetietoisuutta jakava luottamusverkosto on:

> Viranomaisten ja yritysmaailman edustajien välinen anonyymisoitujen teknisten uhkatietojen ja muun vastaavan havaintodatan vaihtamiseen keskittyvä verkosto, joka pyrkii muodostamaan havaintoihin perustuvaa reaaliaikaista tilannetietoisuutta suomalaisiin yrityksiin kohdistuvasta tietoverkkorikollisuudesta ja jalostamaan sitä viranomaisten toimesta verkoston jäsenten osaamisen ja ymmärryksen kasvattamiseksi sekä tietoverkkorikollisuuden torjumiseksi.

Luottamusverkoston toiminnan lähtökohtana on muutosprosessi, jossa yksitäisten jäsenten tietoverkkorikollisuuteen liittyviä havaintoja pyritään jakamaan paremman tilannetietoisuuden saavuttamiseksi. Luottamusverkoston tavoitteleman muutosprosessin asiakkaiksi (*customer*) tunnistettiin jaetusti niin luottamusverkoston jäsenet kuin myös niiden loppuasiakkaat. Luottamusverkoston toimijat (*actors*) toteuttavat muutoksen (*transfromation*), jossa kukin toimija kerää tahollaan tietoverkkorikoksia koskevaa dataa ja jakaa sen muiden toimijoiden kanssa, silloin kun sen vakavuusaste ylittää tietyn kynnyksen. Jotta tilannetietoisuuden jakaminen tukisi luottamusverkostossa vallitsevia erialisia maailmankuvia (*worldview*) tulee tilannetietoisuuden myötä saavutettavan ymmärryksen avulla voida sekä tuottaa lisäarvoa tietoturvayritysten asiakkaille, kuin myös laajentaa viranomaisten käsitystä Suomessa havaituista tietoverkkorikollisuuden muodoista. Muutosprosessin luontevaksi omistajaksi (*owner*) koettiin viestintäviraston kyberturvallisuus-keskus, koska valtaosalla toimijoista on jo yhteistyötä sen kanssa ja sillä koetaan olevan vakiintunut asema tiedon jakamisen solmupisteenä. Luottamusverkoston nykyisessä toimintaympäristössä on kuitenkin havaittavissa tiettyjä rajoituksia (*environmental constraints*), kuten tiedonvaihdon rahoittamiseen, resursointiin tai automatisointiin liittyvät puutteet sekä lainsäädännöstä ja asiakassopimuksista johtuvat salassapitovelvoitteet. Vaikka rahoitus, resursointi ja tiedonvaihdon automatisointi saataisiin ratkaistua, tulee toimijoiden hyväksyä, että salassapitovelvoitteet tulevat jatkossakin hillitsemään toimintasysteemin kehitysmahdollisuuksia.

Luvussa 4.3. koottiin edellä kuvattujen analyysivaiheiden tulokset ja muodostettiin ideaalimalli, jonka mukaista toimintaa ydinmääritelmän mukaisen toimintasysteemin voi tulkita tavoittelevan. Ideaalimallin mukaisen muutosprosessin syötteinä ovat toimijoiden tietyllä ajan hetkellä havaitsemat tietoverkkorikollisuuden elementit. Ollakseen merkityksellistä luottamusverkoston toimijoille, tulisi jatkokäsittelyyn valittujen havaintojen ylittää vakavuusasteeltaan yhdessä sovittu kynnys. Ideaalissa tilanteessa tämä data muokattaisiin automaattisesti yhteisesti sovittuun formaattiin, anonymisoitaisiin ja koottaisiin keskitettyyn paikkaan. Tämä mahdollistaisi muutosprosessin käynnistämisen, jossa luottamusverkoston viranomaisjäsenet voisivat yhdessä analysoida ja rikastaa tietoturvayrityksiltä saatavaa

havaintodataa. Näiden eri lähteistä koottujen havaintojen perusteella muodostettua tilannetietoisuutta raportoitaisiin tämän jälkeen takaisin verkoston toimijoille. Kukin toimija voisi tulkita muodostuvaa tilannetietoisuutta tehdäkseen oman toimintansa kannalta relevantteja ennustuksia tietoverkkorikollisuuden tilasta lähitulevaisuudessa sekä käyttää tietoa oppimisen ja mahdollisesti myös suoraan rikostorjunnan välineenä. Syvällisen ymmärryksen saavuttamiseksi sekä ennen kaikkea luottamuksen rakentamiseksi ja ylläpitämiseksi luottamusverkosto voisi lisäksi kokoontua esimerkiksi puolivuosittain kasvotusten keskustelemaan tietoverkkorikollisuuden tilanteesta Suomessa.

Luvussa 4.4. esitetään teoreettisen viitekehyksen perusteella, että uhkatietojen keräämisen, datan muokkauksen, eteenpäin lähettämisen sekä sanitoinnin ja alustava analyysin aikana tulisi keskittyä tason 1 tilannetietoisuuden muodostamiseen, jolloin tarkoituksena olisi lähinnä havaita, kerätä ja jakaa havaintoja tietoverkkorikollisuuden elementeistä. Toiminnan käynnistymistä todellisuudessa edesauttaisivat taloudelliset kannustimet yksityiskohtaisten tietojen jakamiseen, tehokkaat kommunikointikanavat tai jaettu tilannetietoisuusnäkymä sekä selkeä roolien jako. Toiminnan vaikuttavuutta pystyttäisiin tässä kohtaa seuraamaan karkeasti mittaamalla jaetun datan määrää, jolloin olisi mahdollista havaita, vaihdetaanko tietoa ennakko-odotusten mukaisesti. Viestintäviraston kyberturvallisuuskeskus nähtäisiin luontevana tahona tilannetietoisuuden kokoamiseen.

Seuraavassa vaiheessa viranomaiset analysoisivat ja rikastaisivat luottamusverkoston toimijoilta kerättyä dataa, sekä raportoisivat saavutetun tilannetietoisuuden takaisin verkoston jäsenille. Aikaisempien tutkimushavaintojen perusteella esitetään, että viranomaisten tulisi tässä kohtaa kiinnittää erityistä huomiota muiden luottamusverkoston toimijoiden panoksen ymmärtämiseen ja raportoida aktiivisesti keskeisiä seikkoja saavutetusta tilannetietoisuudesta takaisin muille verkoston jäsenille. Mikäli muiden toimijoiden panosta yhteisten tavoitteiden saavuttamiselle ei ymmärretä ja tiedonvaihto on yksisuuntaista, ei sen jatkumiselle koeta olevan edellytyksiä. Vähintäänkin viranomaisten pitäisi pystyä raportoimaan luottamusverkoston toimijoille takaisin sellaiset seikat, jotka niiden olisi oleellista tietää sekä oman toimintansa että luottamusverkoston yhteisen tavoitteen kannalta. Näin jokainen toimija pystyisi tahollaan rakentamaan tason 2 tilannetietoisuutta, ja ymmärtämään vallitsevien tietoverkkorikollisuuden elementtien merkityksen omalle toiminnalleen. Toiminnan tehokkuutta voitaisiin arvioida mittaamalla jaettavan datan laatua, eli sitä, että onko jaettava havaintodata siinä määrin merkityksellistä, että sen perusteella pystytään aidosti muodostamaan tason 2 tilannetietoisuutta suomalaisia yrityksiä uhkaavasta tietoverkkorikollisuudesta.

Tämän jälkeen kukin luottamusverkoston toimija voisi tahollaan muodostaa tason 3 tilannetietoisuutta ja tehdä ennusteita siitä, miten tietoverkkorikollisuus tulee lähitulevaisuudessa kehittymään ja mitä se tarkoittaa yksittäisen luottamusverkoston jäsenen tai sen loppuasiakkaiden kannalta. Näin saavutettua tilannetietoisuutta oli mahdollista käyttää

päätöksenteon apuna tietoverkkorikollisuuden torjumisessa. Tilannetietoisuutta olisi mahdollista edelleen jalostaa yhteisissä keskustelutilaisuuksissa, jossa olisi myös mahdollista vahvistaa luottamusverkoston jäsenten kokemusta yhteisestä missiosta. Luottamusverkoston toimijoiden kokemusta yhteistyön hyödyllisyydestä voitaisiin mitata säännöllisin väliajoin kyselyillä, jotta varmistettaisiin tavoiteltujen tulosten saavuttaminen mahdollisimman pienin ponnisteluin.

5.2 Konkreettiset kehitystoimenpiteet

Luvuissa 4.3 ja 4.4. kuvatun ideaalimallin mukaisen toiminnan ja teoreettisen viitekehyksen eli ympäröivän todellisuuden perusteella esitettyjen suositusten mukaisen toiminnan aloittaminen vaatisi aktiivista panostusta luottamusverkoston toimijoilta. Luottamusverkoston toimintaympäristössä esiintyvät rajoitteet tulee huomioida ja hyväksyä, mutta niiden ei tulisi antaa estää yhteistyön syventämistä. Ensimmäinen askel yhteistyön kehittämiselle olisi tukea avoimemman tiedonvaihdon kulttuurin kehittymistä tietoverkkorikoksiin liittyen, jotta rikosten uhrit eivät yrittäisi piilotella tapahtunutta. Luvussa 4.2.5 esitettiin ajatus, että tietoturvayritykset voisivat näyttää tässä esimerkkiä yhdessä viranomaisten kanssa ja esittää tahdonilmaisun tai julkilausuman syvemmästä ja avoimemmasta tiedonvaihdosta tietoverkkorikollisuuden saralla. Luottamusverkoston jäsenorganisaatioiden ylimmän johdon tuki ja julkinen sitoutuminen yhteistyön kehittämiseen voisivat taata tiedonvaihdolle sen edellyttämät resurssit ja myös vaikuttaa positiivisesti luottamusverkoston toimijoiden imagoon tietoyhteiskunnan toimijoita tukevina tahoina.

Jotta pehmeän systeemimetodologian mukainen syklinen oppimisprosessi saataisiin vietyä seuraavalle asteelle, tulisi luottamusverkoston jäsenet ottaa vahvasti osallisiksi kehittämisprosessiin. Tämän tutkimuksen puitteissa on luotu tiettyjen luottamusverkoston toimijoiden edustajien haastatteluiden perusteella ideaalimalli, jonka mukaista toimintaa on verrattu teoreettisen viitekehyksen havaintoihin. Tutkimuksesta on sen sijaan jätetty pois taso, jossa ideaalimallin mukaista toimintaa vertaillaan todellisiin toimintatapoihin, koska nykyisen tiedonvaihdon syvyysasteen ja käytäntöjen raportoiminen ei olisi ollut mahdollista osana julkista opinnäytetyötä. Kun toimijoiden sitoutuminen toiminnan kehittämiseen on ensin saatu varmistettua tulisi ideaalimallissa esitettyä toimintaa tarkastellakin kriittisesti vasten verkoston todellisia toimintatapoja. Vertailun perusteella olisi mahdollista kuvata luottamusverkosto toimintasysteeminä tunnistettuine kehityskohtineen ja tarvittaessa luoda uusi ydinmääritelmä ja ideaalimalli, joiden mukaiseksi systeemin toimijat olisivat todellisuudessa valmiita muuttamaan omaa toimintaansa. Luottamusverkoston jäsenet määrittäisivät tällöin aidosti yhdessä niin toimintasysteemin tavoitteet kuin sen toimintatavatkin. Näin olisi mahdollista muodostaa aito yhteenliittymä, jolla on yhteinen missio.

Kun yhteisesti hyväksytty ydinmääritelmä ja ideaalimalli saataisiin luotua, tulisi ideaalimallissa esitettyjen toimenpiteiden toteutustavat päättää. Endsley ja Jones (1997) mukaan yhteisen tilannetietoisuuden saavuttamiseksi tulisi määrittää yhteiset tavoitteet, muodostaa yhtenevät tulkintamallit sekä yhteinen tilannetietoisuusnäkymä. Tässä tutkimuksessa esitetyn ideaalimallin tapauksessa se tarkoittaisi esimerkiksi seuraavien asioiden määrittelyä:

- Mikä on se kynnys, jonka ylittävät havainnot raportoidaan?
- Millä tavalla ja missä muodossa havaitut tietoverkkorikollisuuden elementit tulisi raportoida ja miten raportointi toteutettaisiin käytännössä?
- Miten tarvittava anonymisointi toteutettaisiin?
- Mihin kohteeseen havainnot tulisi lähettää?
- Keiden tehtävänä olisi suorittaa datan sanitointi ja analysointi?
- Millä tiedoilla kerättyä havaintodataa rikastettaisiin?
- Miten saavutettu tilannetietoisuus raportoitaisiin takaisin luottamusverkoston toimijoille?

Käytännössä luottamusverkoston jäsenten tulisi siis määritellä millaisen tietojärjestelmäarkkitehtuurin ideaalimallin mukainen toiminta vaatisi sekä mitä henkilöstöresursseja sen mukainen toiminta edellyttäisi. Myös tarkemmat toiminnan organisoimista koskevat käytännön ohjeistukset sekä mittaamisen liittyvät toimintatavat ja mittarien parametrit tulisi sopia verkoston toimijoiden kesken. Tämän jälkeen tulisi ratkaista vielä toiminnan rahoittamiseen ja organisoimiseen liittyvät seikat.

Jos yllä esitettyihin kysymyksiin ei löydettäisi vastauksia eikä yhteistyötä saataisi palvelemaan aidosti ideaalimallin mukaisesti toimivan luottamusverkoston jäseniä, olisi todennäköistä, että luottamusverkoston jäsenet luopuisivat yksi toisensa jälkeen tilannetietoisuuden jakamisesta koska yhteistyötä ei koettaisi kaikkia osapuolia hyödyttäväksi. Tutkimuksessa kehitettyä ideaalimallia ei siksi ehdoteta sellaisenaan käytäntöön sovellettavaksi. Se on tarkoitettu pehmeälle systeemimetodologialle tyypillisesti välineeksi, jonka avulla kehitykseen tähtäävä keskustelua voidaan käydä. Mallia tulisikin käyttää herättämään luottamusverkoston toimijoissa sellaisia ajatuksia ja kysymyksiä, joihin vastaamalla verkostossa pystytään yhdessä määrittelemään myös realistisesti toteutettavia kehitystoimenpiteitä. Tämän jälkeen vastuu toimintatapojen edelleen linjaamisesta ja työkalujen kehittämisestä tullee siirtymään kehitystyön omistajaksi tunnistetun viestintäviraston kyberturvallisuuskeskuksen vastuulle.

6 Pohdinta

Tämän tutkimuksen tarkoituksena oli selvittää, mistä tiedoista tietoverkkorikollisuuden tilannetietoisuus kannattaa muodostaa ja miten tilannetietoisuuden jakaminen kannattaa toteuttaa tutkimuksen kohteena olevassa luottamusverkostossa? Puolistrukturoiduissa asiantuntija-haastatteluissa kerättyä haastatteluaineistoa analysointiin pehmeän systeemimetodologian avulla. Analyysin tuloksia verrattiin teoreettisen viitekehyksen havaintoihin, joiden perusteella tehtiin johtopäätökset ja esitettiin konkreettiset kehitystoimenpiteet, joihin luottamusverkoston tulisi ryhtyä.

Tutkimuksessa tultiin siihen tulokseen, että luottamusverkoston jäsenet tulisi ottaa vahvasti osallisiksi kyberturvallisuuskeskuksen koordinoimaan kehittämisprosessiin, jossa tutkimuksessa luotua ideaalimallia verrattaisiin verkoston nykyiseen toimintamalliin, minkä avulla tulevaisuuden yhteistyön kehittämiselle voitaisiin luoda konkreettinen suunta. Näin olisi mahdollista määritellä millaisen tietojärjestelmäarkkitehtuurin verkoston toiminta vaatisi sekä mitä henkilöstöresursseja sen mukainen toiminta edellyttäisi. Tämän tiedon avulla olisi mahdollista selvittää ja ratkaista toiminnan rahoittamiseen ja organisoimiseen liittyvät seikat.

Tutkimuksen taustalla on ongelmalliseksi koettu tilanne, jossa tietoverkkorikollisuuden tilannetietoisuuden vaihtoon ryhtymistä on suositeltu (Leppänen ym. 2016) ja tietojen vaihtoon osallistuvat tahot ovat selvillä, mutta osapuolilla ei ole yhteistä näkemystä siitä, mihin suuntaan toimintaa tulisi kehittää. Tähän ongelmalliseen tilanteeseen on pyritty puuttumaan toimintatutkimuksen avulla, joka on tehty tiiviissä yhteistyössä tutkimuksen asiakkaan eli keskusrikospoliisin kyberrikostorjuntakeskuksen kanssa. Checkland ja Poulter (2006) mukaan tämänkin tutkimuksen lähtökohdan kaltaiset, sosiaalisesti moniulotteiset ja vaikeasti määriteltävät, ongelmalliseksi koetut tilanteet ovat tyypillisiä lähtöpisteitä tutkimukselle, jossa hyödynnetään ns. pehmeitä menetelmiä, kuten pehmeää systeemimetodologiaa. Pehmeillä menetelmillä voidaan tietojenkäsittelytieteissä etsiä vastauksia esimerkiksi kysymyksiin mitkä ovat tutkittavan systeemin ominaisuudet, voiko systeemiä kehittää ja jos, niin miten.

Toimintatutkimuksen ja pehmeän systeemimetodologian haasteina voidaan pitää tutkimuksen reliaabeliuutta, eli toistettavuutta, sillä ihmisten välinen sosiaalinen kanssakäyminen ei koskaan toistu kahdesti samanlaisena. Tästä syystä tällaisen tutkimusstrategian avulla toteutettuja tutkimuksia on haasteellista toteuttaa uudelleen, mikä vaikuttaa negatiivisesti niiden tulosten luotettavuuteen. Tästä huolimatta valittu tutkimusstrategia soveltui kuitenkin erinomaisesti tämän tutkimuksen tarkoituksiin, sillä tavoitteena ei ollut muodostaa yleistettävää tietoa vaan täsmällistä tietoa tiettyä tilannetta ja tarkoitusta varten. Lisäksi tutkimusmetodologiaksi valitun pehmeän systeemimetodologian avulla on mahdollista muodostaa prosessi, jonka avulla voidaan kohdata sosiaalisten tilanteiden monimutkaisuus strukturoidulla tavalla.

Pehmeä systeemimetodologia tarjoaa järjestelmällisen viitekehyksen, jonka avulla voidaan rakentaa tilanteen kehittämiseen tähtäävä ajatuskulku tavalla, joka on uudelleen toteutettavissa ja -mallinettavissa, vaikka tutkimus ei kokonaisuudessa olisikaan toistettavissa (Checkland & Poulter 2006). Tutkimuksen toistettavuutta lisää myös tutkimuskysymysten julkistaminen (ks. liite 1) sekä haastatteluaineiston nauhoittaminen ja litterointi, joten tutkimusaineiston analysoiminen on mahdollista toteuttaa myös uudestaan. Toisaalta Checkland ja Poulter (2006) toteavat, että pehmeän systeemimetodologian avulla rakennettu ideaalimalli on parhaimmillaankin vain hyvin perusteltu, sillä eri ihmiset voivat tulkita saman ydinmääritelmän sanoja eri tavalla ja siksi muodostaa sen pohjalta erilaisia ideaalimalleja.

Vaikka juuri tätä tutkimusta varten kerätty tutkimusaineisto käsittelee tarkasti tutkittavaa ilmiötä ja tutkimussuunnitelma on perusteltu, on aineiston kokoamisessa ja muokkaamisessa tiettyjä puutteita, jotka tulee ottaa huomioon tutkimuksen luotettavuutta eli validiutta arvioitaessa. Vaikka viestintäviraston kyberturvallisuuskeskuksen kautta lähetetty haastattelukutsu tavoitti arviolta kymmeniä henkilöitä, vastasi siihen vain yhdeksän henkilöä, joista kolme oli osallistunut myös tutkimuksen suunniteluun. On mahdollista, että nämä neljää eri organisaatiota edustavat tahot ovat ainoita, joilla on aito intressi kehittää luottamusverkoston yhteistyötä. Tämä tarkoittaisi sitä, että haastatteluaineisto antaa liian positiivisen kuvan luottamusverkoston toiminnan kehittämismahdollisuuksista ja aineiston perusteella rakennettu ideaalimalli on hyvin kaukana verkoston todellisista intresseistä. Toisaalta, jos ideaalimallia ja sen pohjalta esitettyjä kehitysehdotuksia sovelletaan, kuten tässä tutkimuksessa on esitetty, auttaa virheellinenkin malli yhteistyön todellisen syvyyden määrittämisessä.

Suurempi puute tutkimuksen kannalta on haastatteluaineistosta tehtyjen johtopäätösten tulkinnanvaraisuus. Vaikka pehmeä systeemimetodologia tarjoaa konkreettisen viitekehyksen, jonka avulla tutkijan ajatuksen kulkua on mahdollista seurata, nojaa johtopäätösten tekeminen hyvin vahvasti tutkijan omiin tulkintoihin. Tutkijan tekemiä päätelmiä voitaisiin pitää pätevämpinä, mikäli tutkimuskysymyksissä olisi kysytty samaa asiaa hieman eri näkökulmista ja aineisto olisi koodattu vastaamaan pehmeän systeemimetodologian eri analyysivaiheissa tarkastelun kohteina olevia seikkoja. Tällainen toteutus olisi kuitenkin joko laajentanut tutkimusaineistoa ja sen analysoimiseen tarvittavaa aikaa merkittävästi tai vaihtoehtoisesti ohjannut aineistonkeruumenetelmää enemmän strukturoidun lomakehaastattelun suuntaan. Tarkasti strukturoitu malli suljettuine vastauksineen olisi kuitenkin helposti johdattanut vastauksia ennalta määrättyyn suuntaan, eikä haastateltavien olisi ollut mahdollista tuoda omia ajatuksiaan luontevasti esiin. Valitulla lähestymistavalla pyrittiin ehkäisemään, ettei tutkija vahingossa syötä omaa valmista ideaalimallia haastateltavilla tai tuo tarkastelun kohteena olevaan toimintasysteemiin sen ulkopuolelta sen toimintaan kuulumattomia arvoja ja toimintatapoja. Tässä tutkija kokee onnistuneensa hyvin. Tulkinnanvaraisuudesta huolimatta myös tämän tutkimuksen tuloksia voidaan pitää valideina, sillä niiden perusteella on

mahdollista kehittää luottamusverkoston toimintaa. Tutkimuksen tulosten yleistämistä tulisi kuitenkin varoa. Anttilan (2006) mukaan toimintatutkimuksen tarkoituksena on kehittää uusia taitoja tai uutta lähestymistapaa johonkin tiettyyn asiaan sekä ratkaista ongelmia, joilla on yhteys johonkin käytännönläheiseen toimintaan. Tämän tutkimuksen arvon määrittää viime kädessä se, pystytäänkö sen tulosten avulla kehittämään tietoverkkorikollisuutta jakavan luottamusverkoston toimintaa. Tutkimuksen perusteella suositellaan seuraavia jatkotutkimusaiheita: toiminnan jatkokehittäminen pehmeänsysteemimetodologian avulla, tietoverkkorikollisuuden käsitteellisen määritelmän syventäminen, tietoverkkorikollisuuden tilannetietoisuuden jakamiseen vaikuttavien lainsäädännöllisten esteiden tunnistaminen sekä tilannetietoisuuden jakamiseen soveltuvan teknisen toteutuksen arkkitehtuurin määrittely.

LÄHTEET

Anttila, P. (2006). *Tutkiva toiminta ja ilmaisu, teos, tekeminen.* 2.painos. Hamina: Akatiimi.

Checkland, P. (1981). *Systems Thinking, Systems Practice.* Bath: John Wiley & Sons.

Checkland, P. & Poulter, J. (2006). *Learning for Action – A Short Definitive Account of Soft System Methodology and its use for Practitioner, Teachers and Students.* London: John Wiley & Sons.

Checkland, P & Scholes, J. (1990) *Soft Systems Methodology in Action.* Chichester: John Wiley & Sons

Davies, M. & Patel M. (2016) Are we managing the risk of sharing cyber situational awareness? *International Conference On Cyber Situational Awareness, Data Analytics And Assessment*. New York: IEEE Computer Society.

Dekker, S. & Hollnagel, E. (2004). Human factors and folk models. *Cognition, Technology and Work,* 6, s. 79-86.

De Muynck, J. & Portesi, S. 2015. Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches. The European Network And Information Security Agency. Haettu 31.03.2107 osoitteesta: https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

Deylam, H. M., Muniyandi, R.C., Ardekani, I. T., & Sarrafzadeh. A. (2016). Taxonomy of malware detection techniques: A systematic literature review. *14th Annual Conference on Privacy, Security and Trust.* Auckland: IEEE Computer Society.

Endsley, M. R. (1988). Situation awareness global assesment technique (SAGAT). *Proceedings of the National Aerospace and Electronics Conference*. (s. 789-795). New York: IEEE Computer Society.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *The Journal of Human Factors and Ergonomic Society*, Vol. 37, No. 1/1995. s. 32-64.

Endsley, M. R. (2000). Theoretical underpinnings of of situation awareness: a critical review. Teoksessa Endsley, M. R. & Garland, D. J. *Situation awareness analysis and measurement*. (s. 3-32). Mahwah, NJ: Lawrence Erlbaum Associates.

Endsley, M. R. (2015). Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making*. Vol. 9, No. 1/2015. s. 4 –32.

Endsley, M. R. & Jones, W. M. (1997). *Situation awareness, information dominance, and information warfare.* Technical Report 97–01. Belmont, MA: Endsley Consulting.

Endsley, M. R. & Robertson, M. M., (2000). Situation awareness in aircraft maintenance teams. *International Journal of Industrial Ergonomics*. Vol 26, Iss. 2. s. 301–325. Elsevier Inc.

Esitutkintalaki 22.7.2011/805. Haettu 31.03.2107 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20110805

Euroopan komissio. (2007). Convention on Cybercrime. *European Treaty Series* - No. 185. Haettu 31.03.2107 osoitteesta http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Europol. 2015. *2015 Internet Organised Crime Threat Assessment (IOCTA)*. Hague: Europol's European Cybercrime Centre (EC3). Haettu 31.03.2107 osoitteesta https://www.europol.europa.eu/iocta/2015/resources/iocta-2015.pdf

Europol. 2016. *2016 Internet Organised Crime Threat Assessment (IOCTA)*. Hague: Europol's European Cybercrime Centre (EC3). Haettu 31.03.2107 osoitteesta https://www.europol.europa.eu/iocta/2016/resources/iocta-2016.pdf

Franke, U. & Brynielsson, J. (2014). Cyber Situational awareness – a systematic review of the literature. *Computer Security* Vol. 46. s. 18-31.

Gal-Or, E. & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research* 16 (2), 186–208. Informs.

Gordon, L., A., Loeb, M., P. & Lucyshyn, W. (2003) Sharing Information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* Vol. 22, Iss 6. s 461–485. Elsevier Inc.

Hallitusohjelma (2015). *Pääministeri Juha Sipilän hallituksen ohjelma 19.5.2015*. Hallituksen julkaisusarja 10/2015. Helsinki: Valtioneuvoston kanslia.

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy.* Vol. 26, Iss. 6. s. 639–688. Elsevier Inc.

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

Kuusisto, R (2004). *Aspects on Availability. A teleological adventure of information in the lifeworld*. National Defence College Department of Tactics and Operations Art. Series 1 No. 1/2004.

Kuusisto, R. (2005). *Tilannekuvasta täsmäjohtamiseen – Johtamisen tietovirrat kriisin hallinnan verkostossa.* Liikenne- ja viestintäministeriön julkaisuja 81/2005. Helsinki: Liikenne- ja viestintäministeriö.

Kyberturvallisuusstrategia 2013. (2013). *Valtioneuvoston periaatepäätös 24.1.2013.* Helsinki: Turvallisuuskomitean sihteeristö.

Leppänen, A., Lindeborg, K. & Saarimäki, J. (2016). *Tietoverkkorikollisuuden tilannekuva.* Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2016. Helsinki: Valtioneuvoston kanslia.

National Crime Agency. 2016. *Cyber Crime Assessment 2016. Need for a stronger law enforcement and business partnership to fight cyber crime.* Viitattu 26.10.2016 http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

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

Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 9/2016. Helsinki: Valtioneuvoston kanslia.

Rikoslaki 19.12.1889/39. Haettu 31.03.2107 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Rubin, A. Pehmeä systeemimetodologia tutkimusmenetelmänä. Haettu 24.4.2017 osoitteesta https://metodix.fi/2014/05/19/rubin-pehmea-systeemimetodologia/

Sabillon, R., Cavaller, V., Cano, J. & Serra-Ruiz, J. Cybercriminals, cyberattacks and cybercrime. (2016). *International Conference on Cybercrime and Computer Forensic*. Vancouver, BC: IEEE Computer Society.

Salmon, P. M., Stanton, N. A., Walker, G. H., Jenkins, D. P., & Rafferty, L. (2010). Is it really better to share? Distributed situation awareness and its implications for collaborative system design. *Theoretical Issues in Ergonomics Science*, Vol. 11, No. 1-2/2010, s. 58-83.

Salmon, P.M., Neville, A. S., Walker, G. H., Baber, C., Jnekins, D.P., McMaster, R. & Young, M. S. (2008). What really is going on? Review of situation awareness models for individuals and teams. *Theoretical Issues in Ergonomics Science*, Vol. 9, Iss 4. s. 297–323.

Turvallisuuskomitea. (2017). *Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020*. Haettu 31.03.2107 osoitteesta. http://www.turvallisuuskomitea.fi/index.php/fi/component/k2/126-suomen-kybeturvallisuusstrategian-toimeenpano-ohjelma-2017-2020

UNODC. (2013). *Comprehensive Study on Cybercrime.* Vienna: United Nations Office on Drugs and Crime. Haettu 31.03.2107 osoitteesta. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Wickens, C. D. (2008). Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement. *Human Factors* Vol. 50, No. 3/2008, s. 397–403.

LIITE 1 HAASTATTELUKYSYMYKSET

Minkä tyyppisistä tiedoista ilmoitatte viranomaisille / tietoturvayrityksille?
Millaista yhteistyötä olette tehneet luottamusverkostoon osallistuneiden tahojen kanssa ennen?
Minkä tyyppistä tietoa olette vaihtaneet ensimmäisissä tapaamisissa?
Mitä resursseja tämän hetken yhteistyöhön kuluu?
Mihin toimintaan resursseja käytetään?
Miten resurssien käyttöä valvotaan ja kontrolloidaan?
Kuka suunnittelee yhteistyön?
Missä ympäristössä yhteistyö tehdään?
Mihin laajempaan kontekstiin tietojen vaihto mielestäsi liittyy?
Mitä rajoitteita yhteistyöllä mielestäsi on?
Miten suhtaudut tietojen vaihtoon?
Millaista tietoa olette valmiit vaihtamaan?
Mitä tietoa saat jakaa?
Miten itsenäisesti saat päättää, mitä tietoa jaetaan?
Miten tärkeänä pidät yhteistyötä?
Mikä motivoi sinua osallistumaan yhteistyöhön?
Miten hyödyllisenä pidät yhteistyötä?
Miksi tätä tietojen vaihtamista kannattaisi tehdä?
Mille roolille organisaatiossasi yhteistyöstä on eniten hyötyä?
Mitä hyötyjä sillä voidaan saavuttaa?
Mitä se edellyttää, että hyödyt voidaan saavuttaa?
Mitä tietoa tähän tarvitaan?
Minkä koet suurimmaksi esteeksi niiden saavuttamiselle?
Kenen / minkä tahon tulisi olla aloitteellinen?
Pitäisikö erityisesti kriittisen infrastruktuurin toimijoiden osalta lisätä regulaatiota ilmoitusvelvollisuuteen liittyen?
Parantaako pakottava regulaatio luottamusta?
Mitä tietoa tulisi vaihtaa?
Mitä tietoa itse toivoisit saavasi? Mihin käyttäisit ko. tietoa?
Mihin konkreettisiin toimiin voisit ryhtyä tiedon perusteella?
Millaista tiedon tulisi olla, jotta sen avulla voidaan rakentaa tilannekuvaa?
Mihin / millaisiin toimiin olet valmis ryhtymään, jotta yhteistyö toimii?
Mitä tietoa tarvitset, että voit ryhtyä toimiin?
Kuka on mielestäsi asiakas tietojenvaihdolle?
Keitä ovat toimijat jotka saavat prosessin aikaan?
Mikä on se muutosprosessi, joka saa systeemiin tulevan resurssin muuttumaan tuotteeksi? Mikä sen tulisi olla?
Kuka omistaa muutosprosessin?
Miten mittaisit yhteistyön tuloksellisuutta?
Miten mittaisit yhteistyön tehokkuutta?
Miten mittaisit, onko työllä mitään vaikutusta isommassa mittakaavassa?

LIITE 2 ONGELMATILANTEEN VISUAALINEN KUVAUS