



TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JUHANA JAAKKOLA
PIKAVIESTINTÄ JA VIESTINNÄN ANALYSOINTI VALTIONHAL-
LINNON TIETO- JA KYBERTURVALLISUUDEN JOHTAMISESSA
Diplomityö

Tarkastaja: professori Samuli Pekkola
Tarkastaja ja aihe hyväksytty Talouden
ja Rakentamisen tiedekunnan tiede-
kuntaneuvostossa 13.1.2016

TIIVISTELMÄ

JUHANA JAAKKOLA: Pikaviestintä ja pikaviestinnän analysointitoiminta valti-onhallinnon tieto- ja kyberturvallisuuden johtamisessa
Tampereen teknillinen yliopisto
Diplomityö, 80 sivua, 3 liitesivua
Lokakuu 2016
Tietojohdamisen diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tietohallinto- ja järjestelmät
Tarkastaja: professori Samuli Pekkola

Avainsanat: Pikaviestintä, Viestinnän analysointi, tietoturvaluisuus, kyberturvaluisuus, valtionhallinto, tietojohdaminen

Valtionhallinnon tason tieto- ja kyberturvaluisuus ja sen menestyksekkäs johtaminen ovat avainasemassa turvallisten digitaalisten palveluiden tuottamisessa kansalaisille. Palveluiden siirtyessä digitaalisiksi tietoturvariskien mahdolliset vaikutukset kasvavat, jolloin tarvitaan parempaa varautumista ja reagoitakyvykkyyttä riskien aiheuttamiin poikkeustilanteisiin. Nykyisen verkottuneen ja jaettujen tietojärjestelmien tilanne muodostaa monitoimijaympäristön, jossa poikkeustilanteet voivat koskettaa monia organisaatioita. Jotta tietoturvariskit ja niiden mahdolliset vaikutukset voidaan tällaisessa tilanteessa minimoida, tarvitaan tietoa ja tiedonvaihtoa eri toimijoiden välillä jaetun tilannekuvan muodostamiseksi.

Tässä diplomityössä tarkastellaan valtionhallinnon tieto- ja kyberturvaluisuuden strategista johtamista ja siihen liittyviä haasteita tietoriskien hallintamallien sekä tietojohdamisen näkökulmasta. Työ liittyy valtionhallinnon tietoturva-asiantuntijoille suunniteltuun pikaviestinjärjestelmään ja sen yhteyteen kehitettäviin pikaviestinnän analysointityökaluihin, jolloin työssä tarkastellaan erityisesti näiden järjestelmien tarjoamia mahdollisuuksia.

Työssä toteutettujen haastattelujen ja havainnoinnin perusteella pikaviestinjärjestelmä mahdollistaisi paremman tiedon jakamisen organisaatorajojen ylittävästi tietoturva-asiantuntijoiden välillä. Tämä voisi tehostaa ja helpottaa asiantuntijoiden työtehtäviä ja parantaa eri toimijoiden välistä yhteistyötä. Pikaviestinnän analysoinnilla ja sen tuloksilla voitaisiin nopeasti tuottaa yleisen tason tilannekuvaa valtionhallinnon yleistä tieto- ja kyberturvaluisuutta seuraaville tahoille sekä hyödyntää näitä tietoja raportoinnissa päätöksentekijöille.

ABSTRACT

JUHANA JAAKKOLA: Instant Messaging and Message Analysis in Information Security Management

Tampere University of Technology

Master of Science Thesis, 80 pages, 3 Appendix pages

Lokakuu 2016

Master's Degree Programme in Information and Knowledge Management

Major: Information Management and Systems

Examiner: Professor Samuli Pekkola

Keywords: Instant Messaging, Instant Messaging analysis, Information Security, Cyber Security

As Finland's public services are becoming more and more digitalized, consequences of risks related to information security are becoming more severe. Thus successful information security management in the Government, from preparation to response and recovery, is becoming more and more important activity. Information systems and services they provide are in current state heavily interconnected, which ties separate organizations together if an information security incident were to occur. This requires active co-operation and information exchange between the parties involved.

In this thesis, the current state and challenges of the strategic information security management of Finnish Government were examined. Especially interest was placed on information transfer and exchange in the context of information security management. Thesis was related to an instant messaging system (IM) under development, which was planned to be implemented for information security experts working in the Finnish Government and its agencies. In addition, a system for analyzing messages transferred through the IM system was prototyped.

The main finding, derived from interviews and observations conducted in the thesis, is that an inter-organizational instant messaging system could improve working efficiency and co-operation between information security experts due to enhanced capabilities for information sharing. Additionally, by analyzing and extracting information from discussion held in the IM system, experts gathering information on the general information security situation could achieve better situational awareness and produce information to decision makers.

ALKUSANAT

Tämä diplomityö on tehty osana Valtiovarainministeriön SecICT –hanketta, joka on ollut keskeisessä osassa valtionhallinnon tieto- ja kyberturvallisuuden kehittämisessä. Uusia ideoita tarvitaan haastavassa ja nopeasti kehittyvässä tieto- ja kyberturvallisuuden maailmassa ja diplomityöni myötä sain olla mukana tutkimassa uuden tyyppistä ja hieman erilaista lähestymistapaa sen kehittämiseen.

Haluan kiittää Kirsi Janhusta diplomityömahdollisuudesta sekä ohjauksesta työn suunnittelun ja toteutuksen aikana. Kiitos Kirsille sekä Markus Haposelle mahdollisuudesta päästä mukaan valtionhallinnon tieto- ja kyberturvallisuuden näköalapaikalle. Kiitän myös professori Samuli Pekkola ohjauksesta ja arvokkaasta palautteesta. Lisäksi haluan kiittää kaikkia työkavereita sekä muita henkilöitä Valtorissa ja Valtiovarainministeriössä, jotka ovat antaneet työstä palautetta ja olleet työn valmistumisessa mukana.

Helsingissä 21.10.2016

Juhana Jaakkola

SISÄLLYSLUETTELO

1.	JOHDANTO	1
1.1	Tutkimuksen kohde ja metodologia.....	3
1.2	Tutkimusongelma ja tutkimuskysymykset.....	4
1.3	Rajaukset.....	5
1.4	Tutkimusasetelma ja -ote	6
2.	TIETO- JA KYBERTURVALLISUUS	8
2.1	Tieto- ja kyberturvallisuuden aihealue ja käsite.....	8
2.2	Strategisen tason johtaminen.....	13
2.3	Operatiiviset prosessimallit	17
2.4	Tilannetietoisuus poikkeustilanteiden johtamisessa	19
2.4.1	Tilannetietoisuus ja tilannekuva	21
2.5	Tieto- ja kyberturvallisuuden operatiivinen toiminta valtionhallinnossa	24
2.6	Tieto- ja kyberturvallisuuden tietojohtaminen	26
2.6.1	Tiedon jakaminen valtionhallinnon TKT-johtamisessa	29
3.	PIKAVIESTINTÄ	35
3.1	Pikaviestinnän ominaispiirteet	35
3.2	Pikaviestinnän käyttö.....	38
3.3	Pikaviestinnän analysointi ja tiedonlouhinta.....	40
4.	TUTKIMUKSEN KOHDE	43
4.1	Pikaviestinjärjestelmän toiminta	43
4.2	Analysointitoiminta	44
5.	TUTKIMUSPROSESSI	46
5.1	Tutkimusprosessi.....	46
5.2	Haastattelumenetelmien valinta ja hyödyntäminen	47
5.3	Haastateltavat henkilöt.....	48
5.4	Havainnointi	49
5.4.1	Havainnoinnin tavoitteet ja kohteet tutkimuksessa	50
5.4.2	Havainnoinnin toteutus	51
6.	TUTKIMUKSEN TULOKSET	52
6.1	Käyttäjä- ja tiimitaso.....	52
6.2	Organisaatiotaso	55
6.3	Valtionhallinnon taso.....	59
7.	POHDINTA.....	63
7.1	Vaikutukset tietojohtamisen näkökulmasta.....	63
7.2	Poikkeustilanteisiin liittyvät haasteet ja vaikutukset niihin	67
8.	YHTEENVETO.....	70
8.1	Keskeiset havainnot ja päätelmät	70
8.2	Tutkimuksen arviointi ja jatkotutkimusehdotukset	71
	LÄHTEET	73

LIITE 1. PIKAVIESTINJÄRJESTELMÄN JA ANALYSOINTITOIMINNAN TIETOVIRTAKAAVIO	78
LIITE 2. HAASTATTELUIDEN KYSYMYSRUNKO	79
LIITE 3 HAASTATTELUISSA ESIINTYNEET TEEMAT	81

LYHENTEET JA MERKINNÄT

SOC	Security Operations Centre, tietoturva- ja tietoturvavalmu
TKT	Tieto- ja kyberturvallisuus
VAHTI	Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
KYHA	Kansallinen Kyberharjoitus
NIST	National Institute of Standards and Technology, Yhdysvallat
SecICT -hanke	Valtiovarainministeriön ympärivuorokautisen tietoturvatoininnan kehittämishanke
CNSS	Committee on National Security Systems
MACCSA	Multinational Alliance for Collaborative Cyber Situational Awareness
ENISA	European Union Agency for Network and Information Security
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ICT	Information and Communication Technologies

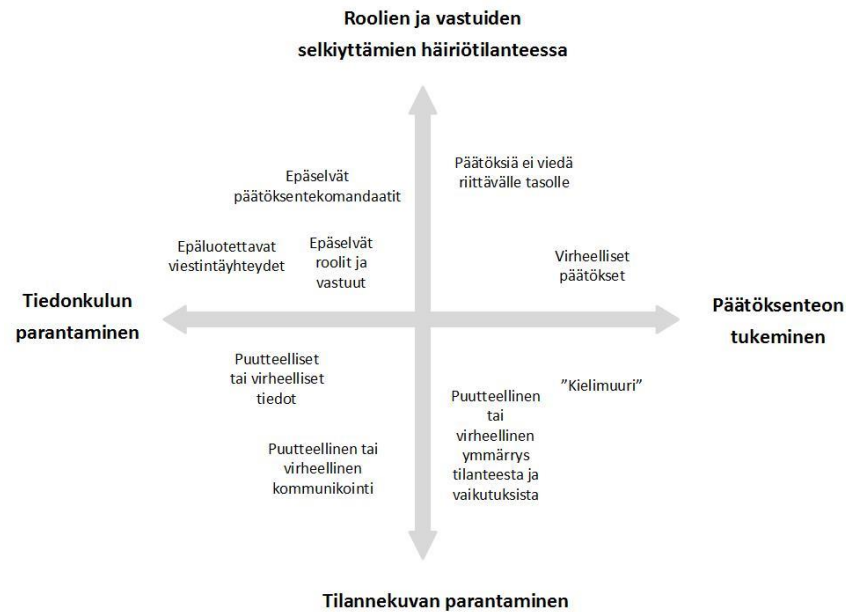
1. JOHDANTO

Tieto- ja kyberturvallisuus on nousemassa yhä vahvemmin osaksi turvallisuutta myös kansallisen tasolla palveluiden ja yhteiskunnan toimintojen digitalisaation seurauksena. Yhtenä Valtion keskeisenä tehtävänä on yhteiskunnan ja sen palveluiden toimivuuden ja saatavuuden turvaaminen, joten Yhteiskunnan turvallisuusstrategian toimeenpanoa on laadittu Kansallinen Kyberturvallisuusstrategia (Kyberturvallisuusstrategia, 2013). Palveluita ja niiden tietoturvaluutta uhkaavat tilanteet ovat nousseet esiin mediassa ja voivat olla vaikutuksiltaan laaja-alaisia, kuten valtion virastojen verkkopalveluiden tuottajaan kohdistunut palvelunestohyökkäys 19.11.2015 (Kaleva, 2015).

Näiden tapahtumien seurauksena on havaittu, että valtionhallinnon tarjoamien digitaalisten palveluiden tietoturvaluuden vaarantumisen vaikutukset voivat ulottua moneen eri organisaatioon. Nykyisessä tilanteessa palveluiden ja niiden vaatiman infrastruktuurin tuottamiseen voi osallistua useita eri organisaatioita joten toiminta ja toimintaa tukevat järjestelmät ovat yhä enemmän kytköksissä toisiinsa. Tästä johtuen tilanteiden selvittämien ja vaikutusten hallinta *yhteistyössä eri organisaatioiden kesken* onkin nousemassa yhä tärkeämmäksi osaksi valtionhallinnon tieto- ja kyberturvallisuuden toteuttamista. Yhteistyö tuo kuitenkin valtionhallinnon tieto- ja kyberturvallisuuden johtamiseen monia eri osa-alueita haasteineen, kuten esimerkiksi eri toimijoiden roolit ja vastuut sekä päätöksentekoon liittyvät seikat.

Haasteet eivät kuitenkaan rajoitu toimintaan tai prosesseihin. Yhteistyöhön perustuvassa toiminnassa tiedonvaihdolla on suuri merkitys, jotta monimutkaisissa tapahtumista voidaan pyrkiä muodostamaan kokonaiskuva ja ymmärrystä tilanteesta (Leppänen et al. 2016. s. 16-19). Täten myös tiedon johtamisen kehittäminen on keskeinen osa valtionhallinnon tieto- ja kyberturvallisuuden kehittämistä. Tätä korostavat havainnot Kansallisissa kyberharjoituksista, joista esimerkiksi yhtenä keskeisenä havaintona todettiin, että johtajilla ei ole kaikissa tilanteissa riittävää ja oikeaa tietoa päätöksenteon tueksi (Janhunen, 2015). Tähän diplomityöhön liittyvässä laajemmassa kokonaisuudessa, eli valtionhallinnon tieto- ja kyberturvallisuuden johtamisessa kehityskohteenä on siis sekä toiminta että tieto ja sen johtaminen.

Yleisesti edellä mainittuja haasteita ja kehityskohteita, eli diplomityön ongelmakenttää, on hahmoteltuna seuraavalla sivulla kuvassa 1. Kuvassa on myös esiteltynä yleisellä tasolla hankkeen tavoitteita, eli tiedonkulun ja tilannekuvan parantaminen, sekä päätöksenteon tukeminen ja roolien ja vastuiden selkiyttäminen. Näillä kehityskohteilla ja -toimilla pyritään vaikuttamaan esitettyihin haasteisiin ja puutteisiin.



Kuva 1. Tunnistettuja haasteita ja puutteita valtionhallinnon tietoturvallisuuden johtamisessa. (Janhunen 2015)

Valtionhallinnossa tietoturvallisuuden tieto- ja kyberturvallisuuden kehittämiseksi on perustettu SecICT –hanke, joka käynnistäminen pohjautuu Valtioneuvoston periaatepäätökseen 7/2009 (Valtioneuvosto, 2009, s. 32) SecICT -hankkeen tavoitteena on ollut parantaa valtionhallinnon tieto- ja kyberturvallisuutta, sekä osaltaan vastata kuvassa 1 tunnistettuihin haasteisiin ja puutteisiin.

Osana SecICT -hanketta on kehitetty ja pilotoitu pikaviestintäjärjestelmää tiedonkulun parantamiseksi valtionhallinnon tietoturva-asiantuntijoiden välillä sekä yleisesti valtionhallinnon tieto- ja kyberturvallisuuden johtamisen tukemiseen. Alustavan suunnitelman mukaan järjestelmän avulla Valtionhallinnon eri ministeriöissä, virastoissa, palveluntuottajissa sekä muissa elimissä toimivat tietoturvallisuudesta vastaavat henkilöt ja asiantuntijat voivat keskustella tieto- ja kyberturvallisuuteen liittyen. Tulevaisuudessa järjestelmää voidaan tarjota mahdollisesti myös Valtionhallinnon ulkopuolisille yksityisille toimijoille.

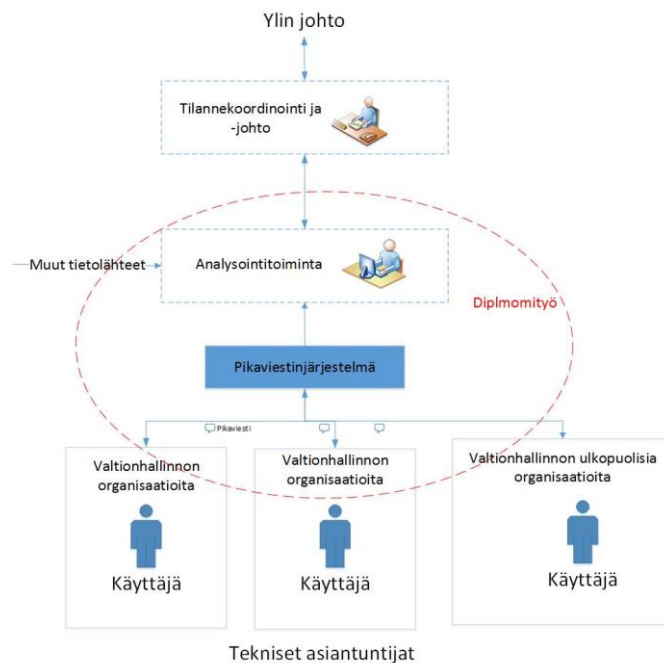
Diplomityön tutkimuskohteena on kyseinen pikaviestinjärjestelmä. Yksinkertaistettuna kyseessä on keskustelu- ja tiedonvaihtokanava eri valtionhallinnon organisaatioissa toimiville teknisille asiantuntijoille. Pelkkä asiantuntijoiden välinen yhteistyö ja tiedonvaihto eivät kuitenkaan riitä, koska laajemmissa poikkeustilanteissa kyseiset asiantuntijat eivät ole päätöksiä tekevä taho. Täten tarvitaan tiedon tuottamista organisaatiohierarkiassa ylempänä oleville tahoilla päätöksenteon tueksi. Tiedon tulisi myös olla myös hyödynnettävissä olevaa eli sen pohjalta tulisi pystyä muodostamaan ymmärrys poikkeustilanteesta ja siihen liittyvästä päätöksenteosta. Tästä johtuen pikaviestinjärjestelmän yhteyteen on suunniteltu myös pikaviestintään perustuvaa analysointikyvykkyyttä, millä pyri-

tään tuottamaan keskusteluista ja niihin osallistuviin organisaatioiden tietoturvallisuudesta yleistason tietoa päätöksenteon tueksi. Tarkempi kuvaus tutkimuskohteesta eli pikaviestinjärjestelmästä ja analysointitoiminnasta on luvussa 4.

Johdanto diplomityöhön, sen tutkimuskohteeseen ja –kysymyksiin sekä näihin liittyviin rajauksiin on myöhemmin tässä luvussa. Luvussa 2 tarkastellaan tutkimuskohteen laajempaa teoreettista viitekehystä, jonka näkökulmista tutkimuskohdetta ja tutkimuskysymyksiä lähestytään. Luvussa 5 esitellään tutkimuksen metodologiset valinnat sekä kuvataan, kuinka tutkimus toteutettiin. Luvussa 6 esitellään empiriisen tutkimuksen tulokset. Luvussa 7 pohditaan tutkimuksen empiriisiä tuloksia kirjallisuuskatsauksen pohjalta tehtyjä havaintojen vasten. Viimeisessä luvussa tehdään yhteenveto, arvioidaan tutkimusta sekä tarkastellaan mahdollisia jatkotutkimuskohteita.

1.1 Tutkimuksen kohde ja metodologia

Tutkimuksen päätutkimuskohteena on pikaviestintäjärjestelmä sekä tähän järjestelmään liittyvä analysointitoiminta, jotka ovat tarkemmin esiteltynä luvussa 4. Tutkimusprojektin aikana pikaviestinjärjestelmää kehitettiin ja se implementointiin, mutta sitä ei vielä otettu laajempaan käyttöön. Tutkimuskohteeseen liittyvä käyttäjä- ja prosessikokonaisuus on yleisellä tasolla hahmoteltuna kuvassa 2. Kuvassa on kokonaisuuteen liittyviä toimijoita, niiden rooleja ja niiden välisistä vuorovaikutussuhteista.



Kuva 2. Diplomityössä tarkasteltava kokonaisuus

Kuvassa alhaalla on järjestelmän käyttäjät, joiden väliseen viestintään pikaviestinjärjestelmä on suunniteltu. Pikaviestinjärjestelmän avustuksella käytävistä keskusteluista on

analysoinnin avustuksella tarkoituksena tuottaa tietoa ja hyödyntää sitä häiriö- ja poikkeamatilanteiden käsittelyyn liittyvässä yhteistyön tukemisessa. Tarkemmin järjestelmäkokonaisuus, sen toimintaperiaatteet ja tavoitteet ovat esiteltynä luvussa 4. Nämä kaksi kokonaisuutta, ovat toiminnallisesti ja tutkimuksen näkökulmasta tiiviissä yhteydessä toisiinsa. Tästä syystä tutkimuskohteesta puhuttaessa ei ole järkevää erottaa pikaviestinjärjestelmää ja siihen liittyvää analysointitoimintaa toisistaan. Täten tutkimuskohteen viitataessa tarkoitetaan sekä pikaviestinjärjestelmää että siihen liittyvää analysointitoimintaa.

1.2 Tutkimusongelma ja tutkimuskysymykset

Diplomityössä tutkimuskohdetta haluttiin tarkastella teknistä tarkastelua laajemmasta näkökulmasta, joten tutkimusongelmaksi määriteltiin pikaviestinjärjestelmän ja analysointitoiminnan mahdollisten vaikutusten tutkiminen valtionhallinnon tieto- ja kyberturvallisuuden johtamiseen. Diplomityössä olisi ollut mahdollista myös tehdä laajempaa ja yksityiskohtaisempaa tarkastelua siitä, mitä kyseinen järjestelmä teknisesti mahdollistaa, sillä pikaviestinjärjestelmän kehitystyötä ja implementointia sekä siihen liittyvä dokumentaatiota suoritettiin diplomityöhön liittyvässä SecICT –hankkeessa. Tässä tutkimuksessa pyrittiin kuitenkin ymmärtämään pikaviestinjärjestelmän teknistä ja toiminnallista kokonaisuutta, sillä järjestelmän implementointia alustavasti suunniteltaessa yhtenä oletuksena on ollut, että pikaviestinjärjestelmä voisi mahdollistaa esimerkiksi mutta uusia toimintamalleja. Tavoitteena on, että ymmärtämällä näitä uusia toimintamalleja ja ilmiöitä voidaan niitä pyrkiä hyödyntämään paremmin.

Tutkimuksen ensisijainen päätutkimuskysymys on:

Millaisia ovat pikaviestinjärjestelmän ja analysointitoiminnan mahdolliset vaikutukset valtionhallinnon tieto- ja kyberturvallisuuden johtamiseen?

Alatutkimuskysymyksinä ovat:

Millaisilla johtamismalleilla voidaan kuvata valtionhallinnon tieto- ja kyberturvallisuuden johtamista?

Mitä haasteita valtionhallinnon tieto- ja kyberturvallisuudenjohtamiseen liittyy tietojohtamisen näkökulmasta?

Mitä ovat pikaviestinjärjestelmät ja viestinnän analysointi ja miten niitä voidaan hyödyntää valtionhallinnon tieto- ja kyberturvallisuuden johtamisen kontekstissa?

Miten pikaviestinjärjestelmä ja analysointitoiminta vaikuttavat ja mitä ne mahdollistavat tieto- ja kyberturvallisuuden johtamisessa tietojohtamisen näkökulmasta?

Tutkimuskysymysten avulla on tarkoituksena tehdä tarkastelu pikaviestinnästä ja pikaviestinnän analysoinnista ja niiden tarjoamista mahdollisuuksista valtionhallinnon tieto-

ja kyberturvallisuuden kontekstissa. Tähän kontekstiin liittyviä ominaispiirteitä esitellään luvussa 2. Kontekstiin liittyy esimerkiksi organisaatorajat ylittävää toimintaa, koska valtionhallinnon tapauksessa tieto- ja kyberturvallisuuteen liittyvää päätöksentekoa tekeviä tahoja on useita, riippuen tilanteesta. Näitä erityispiirteitä tutkitaan alatutkimuskysymyksillä, jolloin niitä voidaan pyrkiä päätutkimuskysymykseen vastattaessa ottamaan huomioon.

Tutkimuksessa tarkastellaan myös tieto- ja kyberturvallisuuden johtamista tietojohdamisen näkökulmasta, koska tunnistetut haasteet ja osaltaan niiden ratkaisemiseen suunniteltu pikaviestinjärjestelmä liittyvät esimerkiksi tiedon jakamiseen ja siihen liittyviin haasteisiin. Vaikka tutkimuksen pääasiallisena tarkoituksena on kehittää valtionhallinnon TKT-johtamista, tietojohdamisen lähestymistavan avulla tarkasteltuna voidaan ymmärtää ja hahmottaa mahdollisia tiedon ja sen jakamisen haasteita TKT-johtamisen haasteiden taustalla. Tutkimuksessa tarkastellaan myös pikaviestinnän ominaispiirteitä sekä niiden tarkoitusta ja käyttötapoja, jotta pikaviestinjärjestelmän ja analysointitoiminnan vaikutuksia voidaan ymmärtää.

1.3 Rajaukset

Valtionhallinnon tieto- ja kyberturvallisuuden johtamiseen liittyviä päätöksentekorakenteita ja –prosesseja ei tutkimuksessa tarkastella yksityiskohtaisesti, vaan niitä käsitellään yksinkertaistetulla mallilla, joka on esiteltyä myöhemmin luvussa 2.2. Tutkimuksessa valittiin tarkastelutasoksi pääosin valtionhallinnon tieto- ja kyberturvallisuuden johtaminen, eli organisaatioiden välinen taso, koska sekä tilaaja että tutkimuskohde ovat osa tätä kokonaisuutta. Tutkimuskohdetta tarkasteltiin osana TKT-johtamista tietojohdamisen ja tilannejohtamisen näkökulmista

Teknisellä tasolla pikaviestinnän analysointia tutkitaan ja siihen liittyviä sovelluksia kehitetään Maanpuolustuskorkeakoulun toteuttamassa projektissa (Puuska et al. 2016), joten tämä osa-alueen sisältö ei tarkemmalla tarkastelutasolla sisälly tämän tutkimuksen alueeseen. Pikaviestinjärjestelmän osalta ei tarkastella toteutettavia teknologiavalintoja, vaan tutkimuksessa keskitytään pikaviestinjärjestelmän ja analysointitoiminnan mahdollistamiin tiedon jakamisen ja tuottamisen toimintamalleihin ja näiden mukanaan tuomiin hyötyihin teknisen tarkastelutason sijaan, koska tässä yhteydessä ei kehitetä teknologisesti uusia ratkaisuja.

Tutkimuksen päätarkoituksena ei ole tarkastella pikaviestinjärjestelmän käyttäjien tasolla tapahtuvaa toimintaa, vaan näkökulmana tutkimuksessa on tilaajan näkökulma, joka on toimintaa ohjaavana strategisella tasolla. Tilaaja toimii valtionhallinnon TKT-johtamisen viitekehyksessä ohjaavana toimijana, ei aktiivisena johtamiselimenä. Tutkimuksessa ei täten oteta kantaa operatiivisen päätöksentekotason tai ylimmän aktiivisen johdon toimintamalleihin tai tavoitteisiin. Täten tutkimuksessa painopiste ei ole kuinka tai miten johdon

ja päätöksenteon tulisi aktiivisena toimijana hyödyntää pikaviestinjärjestelmästä tai analysointitoiminnasta saatavia tietoja, vaan miten se hyödyntää valtionhallinnon TKT-johdantamista kokonaisuutena ohjaavan toimijan näkökulmasta.

1.4 Tutkimusasetelma ja -ote

Asetetut tutkimuskysymykset viittaavat ymmärtämiseen ja ymmärryksen muodostamiseen tutkimuskohteesta. Tutkimuksen tuloksista odotettiin pääosin deskriptiivisiä eli tutkimuskohdetta ja sen merkityksiä ja vaikutuksia kuvailevia. Taulukossa 1 on yhteenveto tutkimuksen tutkimusasetelmasta.

Taulukko 1. Tutkimusasetelmaan liittyvät valinnat

Näkökulma	Valinta	Merkitys ja vaikutukset
Tieteenfilosofia	Pragmaattinen Tulkin-nallinen	Kaikki hyödynnettävissä oleva tieto on arvokasta; Tutkijan olettamukset ja subjektiivisuus huomioidaan
Tutkimusstrategia	Laadullinen moni-metodinen tapaustutkimus	Valittiin kaksi laadullista menetelmää, joilla kerätään tietoa yhdestä kohteesta
Aineistonhankintamenetelmät	Laadulliset menetelmät	Valittiin menetelmiksi haastattelu ja havainnointi. Hylättiin muut mahdolliset vaihtoehdot
Tutkimusmenetelmä	Laadullinen	Sisällön luokittelu ja sisällönanalyysi
Päätelyn logiikka	Pääosin induktiivinen/Aineistolähtöinen	Olemassa olevan teorian todentaminen
Ajallinen kesto	Läpileikkaava	Tutkimuskohteen tutkiminen yhtenä ajankohtana

Tutkimuksessa ei pyritty muodostamaan normatiivisia suosituksia, kehotuksia tai järjestelmämäärittelyitä. Deskriptiivisiä tuloksia tavoiteltaessa ei tehty lähtökohtaisia ontologisia rajoituksia, koska tutkimuskohdetta haluttiin ymmärtää mahdollisimman kokonaisvaltaisesti muodostetussa viitekehyksessä. Näkökulmat, jotka käsittelevät tutkimuskohdetta esimerkiksi tiedonhallinnan sosiaalisesta näkökulmasta, sisältävät interpretivismiin viittaavia olettamuksia todellisuuden olemuksesta ja hyväksyttävästä tiedosta. Eli tutkimusta suunniteltaessa arvioitiin, että myös esimerkiksi haastattelujen ja niiden analysoinnin avulla voidaan saavuttaa validia tutkimusaineistoa ja –tuloksia. Tutkimuksen taustaoletuksena on täten, että kaikki saatavilla olevat tiedot tutkimuskohteesta ovat epistemologisesti yhtä valideja ja kaikki tiedot ovat lähtökohtaisesti yhtä arvokkaita. Tieteenfilosofisesti tutkimusta lähestyttiin siis pragmaattisesti, koska tutkimus sisältää monia, mutta oletettavasti yhtä päteviä, näkökulmia tutkimuskohteeseen. Tutkimuskohdetta lähestyt-

tiin osittain esimerkiksi sosiaalitieteiden näkökulmasta, mutta pääosin tutkimuksessa päädyttiin kuitenkin hyödyntämään tietoturvallisuuden ja tietojohdamisen tutkimusalueiden kautta muodostettuja näkökulmia, koska ne olivat alustavan analyysin mukaan tutkimusongelmankentän keskiössä.

Pragmaattisen tieteenfilosofian ja lähestymiskulman pohjalta tutkimusstrategiaksi valittiin laadullinen moni-metodinen tutkimus. Tutkimuskohteen vaikutuksia ei ollut alustavan arvion mukaan järkevää mitata määrällisillä mittareilla, joten lähtökohdaksi valittiin laadullinen tutkimus. Moni-metodinen lähestymistapa valittiin, koska tutkimuskohteesta pyrittiin saamaan laaja-alaisesti tietoa johtopäätösten tekemiseksi. Aaltolan & Vallin (2010) mukaan laadullisessa tutkimuksessa kaikkea mitä tutkimuksessa tapahtuu, voidaan hyödyntää tutkimusaineistona. Aineiston keräämisen menetelmän tutkimuksessa hyödynnettiin haastatteluita ja havainnointia. Haastattelu on monipuolinen aineistonkeruumenetelmä, jonka avulla voidaan kerätä laadullista tutkimusaineistoa ihmisistä ja heidän toiminnastaan. Havainnointi eli observointi sopii mm. vuorovaikutusten tutkimiseen, mikä on yksi tutkimuskohteen keskeisimpiä ominaisuuksia. Havainnointia sovellettiin tutkimuksessa haastatteluiden tuottaman aineiston laajentamiseen ja osittain haastattelussa esille tulleiden asioiden todentamiseen. Tarkempi kuvaus empiirisen osion toteutuksesta tutkimuksessa on luvussa 5. (Saaranen-Kauppinen & Puusniekka, 2006).

Tutkimusmenetelmänä käytettiin aineiston sisällönluokittelua ja -analyysiä. Luokittelu tehtiin haastattelussa esiintyneiden teemojen mukaan. Sisällönanalyysi perustui pääosin teoreettiseen viitekehykseen. Päättelyn logiikka siis tutkimuksen tapauksessa sisältää pääosin induktiivista, eli aineistolähtöistä, havaintojoukosta yleistävää päättelyä. Havaintojoukkona ovat empiirisen tutkimuksen tulokset joista pyritään päättelemään tutkimuskohteen vaikutukset tieto- ja kyberturvallisuuden johtamiseen. (Saunders et al. 2009)

Kuvailevana tutkimuksena, ja aineiston menetelmävalintojen seurauksena tutkimukseen liittyy subjektiivisuutta tulkintojen, eli tulosten ja niiden merkitysten analyysien osalta. Tutkija on sekä haastattelussa että havainnoinnissa osallisena aineiston hankintaan, mikä voi vaikuttaa tutkimusaineistoon ja sen pohjalta tehtäviin päätelmiin (Saaranen-Kauppinen & Puusniekka 2006). Työn teoreettinen viitekehys kuitenkin pyrittiin muodostamaan validoitujen tutkimusten sekä yleisesti tunnettujen mallien avulla, millä voidaan vähentää subjektiivista validointia viitekehyksen osalta. (Saunders et al. 2009)

Laadullinen tutkimus sisältää tutkijan tekemiä tulkintoja aineistosta, joita tutkimuksessa kerätään. Täten tutkimuksessa pyrittiin kiinnittämään huomiota tulkintojen oikeellisuuteen ja tiedostamaan, miten tutkijan asennoituminen vaikuttaa tuloksiin. Vaikutuksia pyrittiin minimoimaan keräämällä tutkimusaineistoa eri lähteistä, jotka edustivat eri näkökulmia tutkimuskohteeseen, jotta tutkijan näkökulma muodostuisi mahdollisimman laajaksi. Ajallisesti tarkasteltuna tutkimus on poikkileikkaava eli se kuvaa yhtenä ajanjaksona tutkittavaa kohdetta ja sen vaikutuksia yhtenä ajanhetkenä. Valinnan taustalla on tutkimusprojektiin käytettävissä oleva aika ja resurssit.

2. TIETO- JA KYBERTURVALLISUUS

Tutkimus toteutettiin osana johdannossa kuvattua hanketta, jonka yhtenä tavoitteena on ollut kehittää valtionhallinnon tietoturvaluutta. Tutkimuksen lähtökohdiksi muodostuivat täten valtionhallinnon tietoturvaluus ja sen johtaminen. Tutkimuksen kohteena olevan pikaviestinjärjestelmän tulevilla käyttäjillä on ainakin yleisellä vastuualueellaan järjestelmiä, joiden kautta voidaan uhata ihmisten ja asioiden fyysistä turvallisuutta, tutkimuksen viitekehukseen otettiin sekä tieto- että kyberturvallisuuden asiakokonaisuudet.

Tutkimuskohdetta tarkastellaan täten osana valtionhallinnon tieto- ja kyberturvallisuuden johtamista (TKT- johtaminen). Aiheanalyysin perusteella pikaviestinjärjestelmän tarkoituksena on tukea toisaalta tiedonhallinnallisiin haasteisiin vastaamista, mutta myös tukea tieto- ja kyberturvallisuuden johtamisen sisältämää häiriö- ja poikkeustilannejohtamista. Tästä syystä teoreettisessa tarkastelussa esitellään yleisellä tasolla valtionhallinnon TKT –johtamista riskienhallinnan mallien avulla sekä tarkastellaan mallia tietojohtamisen ja tilannejohtamisen näkökulmista.

2.1 Tieto- ja kyberturvallisuuden aihealue ja käsite

Tutkimuksen keskeisenä aihealueena on tieto- ja kyberturvallisuus sekä näihin liittyvät ilmiöt. Termit ja niihin liittyvät käsitteet ovat vähitellen vakiintumassa, mutta niitä käytetään edelleen epä johdonmukaisesti (Holmgren, 2016. s. 68). Tieto- ja kyberturvallisuus liittyy tietojärjestelmien, laitteiden ja tietoverkkojen muodostamaan kokonaisuuteen, jossa tietoja käsitellään sähköisessä muodossa. Tästä ympäristöstä voidaan käyttää myös nimitystä ”kyberavaruus” (Cyberspace), joka on Yhdysvaltalaisen Committee on National Security System (CNSS, 2010) määritelmän mukaan

Globaali tietoympäristö, joka koostuu keskinäisen verkoston muodostavista viestintä- ja tietoverkoista, kuten Internet, sekä sen toteuttavasta infrastruktuurista.

Holmgren (2016, s. 68) tarkastelee kyber -etuliitettä ”digitaalisena tilana, jossa yhdistyy informaatioteknologia ja jossa toimitaan tietoverkkojen välityksellä.” Kyber –termiin siis liittyy vahvasti käsitystä tilasta, jossa toimitaan fyysisen maailman verrattavasti.

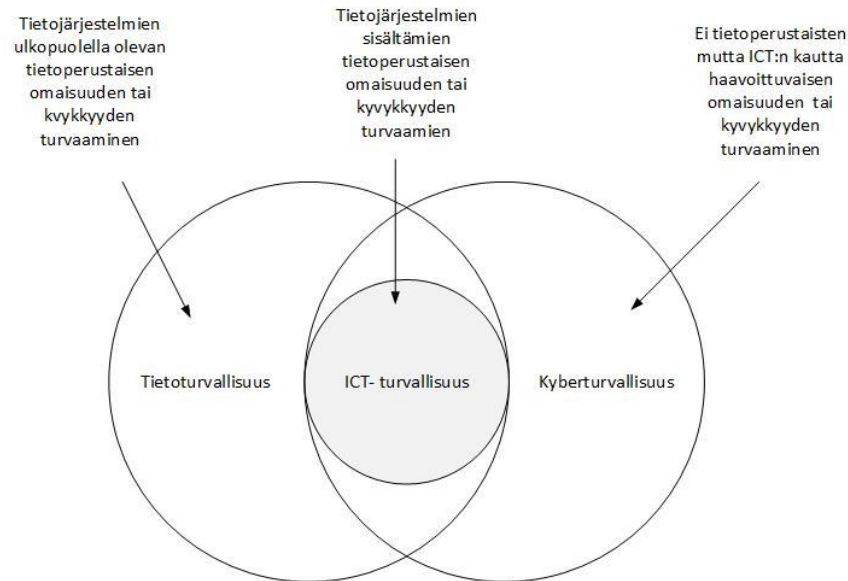
Tietoturvaluus, eli tiedon turvallisuus on toinen osa tieto- ja kyberturvallisuuden aihealuetta, jonka lähtökohdat ovat hieman erilaiset. Tietoturvaluus nimensä mukaisesti keskittyy tietoon ja sen turvaamiseen, erona kyberturvallisuuden toimintalähtöiseen ajattelutapaan. Kansainvälinen ISO/IEC 27000:2009 standardi määrittelee tietoturvaluuden tavoitteeksi tiedon, eli datan, informaation tai tietämyksen, luottamuksellisuuden, eheyden ja saatavuuden säilyttämisen (ISO/IEC 2009). Luottamuksellisuudella tarkoite-

taan, että tietoa ei ole saatavilla tai sitä ei paljasteta luvattomille tahoille. Eheydellä viitataan tiedon muuttumattomuuteen ja saatavuudella tiedon olemista saatavilla halutulla ajanhetkellä.

Kyberturvallisuus käsite lähestyy digitaalista ympäristöä ja turvallisuutta vahvemmin toiminnan ja toimenpiteiden näkökulmasta, mikä on perusteltua, sillä kyber -kokonaisuudella on merkittävä rooli ja se tuo merkittävää hyötyä niin yksittäisten ihmisten, organisaatioiden kuin valtioidenkin toimintaan, jolloin sen luotettava ja häiriötön toiminta on tärkeää (Williams, 2014). Whittaker (2004) huomauttaakin että kyberavaruus ei ole pelkästään sähköinen infrastruktuuri, vaan paikka tai tila, jossa toimitaan ja vaikutetaan. Kyberavaruudessa tapahtuvan toiminnan turvaaminen, eli tieto- ja kyberturvallisuus on siten tärkeä osa sähköisessä tietojenkäsittely ja –siirtoympäristössä toimimista. Tieto- ja kyberturvallisuus pohjautuu turvallisuuskäsitykseen (safety, security), joka Merriam-Websterin (2016) sanakirjan mukaan tähtää kohteen fyysisen turvallisuuden eli koskemattomuuden ja vahingoittumattomuuden turvaamiseen.

Vaikka edellä tieto- ja kyberturvallisuus liitetään vahvasti digitaaliseen ympäristöön, on molemmilla termeillä yhtymäkohdat fyysiseen maailmaan ja siinä tapahtuvaan toimintaan. Jos tietoturvallisuus on perinteisesti yhdistetty tietokoneisiin ja sähköisessä muodossa olevaan tietoon, termi kyberturvallisuus laajentaa Von Solms & Van Nierek (2013) mukaan tietoturvallisuuden kohdealuetta osa-alueille, joita ei ole perinteisesti katsottu kuuluvan tietoturvallisuuden osa-alueeseen. Heidän mukaansa tietoturvallisuus koostuu eri osa-alueista, joilla pyritään tiedon ja tietoon perustuvan toiminnan sekä alla olevan teknologisen infrastruktuurin turvaamiseen. Kyberturvallisuus puolestaan on ulottuvuus tietoturvallisuudesta fyysiseen turvallisuuteen, jolloin siihen käsitetään osa-alueet, joilla turvataan kohteet, jotka ovat haavoittuvia teknologisen infrastruktuurin kautta. Tällaisia kohteita voivat olla esimerkiksi energiantuotantolaitokset, joita ohjataan tietojärjestelmien avulla. Turvaamisella käsitetään tässä yhteydessä täten myös mahdolliset fyysiset vahingot eli pyritään estämään tietotekniikan kautta tai sen avulla toteutuvat fyysisetkin turvallisuusuhat. (Von Solms & Van Nierek, 2013)

Kuvassa 3 on esiteltyä tieto- ja kyberturvallisuuden tavoitteita suhteessa toisiinsa. Tavoitteet menevät osittain päällekkäin. Molemmista voidaan erottaa digitaalinen ja fyysinen kohde ja tavoite, jolloin sähköisessä ympäristössä tapahtuvan toiminnan ja sen sisältämän tiedon turvaaminen, eli ICT-turvallisuus, on vain yksi osa-alue kokonaistavoitetta. (Von Solms & Van Nierek, 2013)



Kuva 3. Tieto- ja kyberturvallisuus, mukailten Von Solms & Van Nieriek (2013)

Von Solmsin & Van Nierikin (2013) lähestymistavan avulla tarkasteltuna tieto- ja kyberturvallisuus ja siihen liittyvä toiminta on tietoturvallisuuden näkökulmasta sekä tietojärjestelmien sisältämän, että niiden ulkopuolella olevan tiedon turvaaminen. Kyberturvallisuuden näkökulmasta tavoite ja siihen liittyvä toiminta on välillisesti ICT:n kautta haavoittuvan tiedon, omaisuuden, kyvykkyyden ja toiminnan turvaamista.

Turvallisuuteen, turvallisuuden tilanteen ja uhkakuvien arviointiin liittyy vahvasti riskin käsite ja riskien hallinta. Riskit ovat myös vahvasti osa tieto- ja kyberturvallisuuden johtamisen aihealuetta. Valtionneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (Vahti 7/2009) asettaa tietoturvatoininnan ja tietoturvallisuuden johtamisen keskeiseksi osa-alueeksi ja kehittämiskohteeksi tietoturvallisuuteen liittyvän riskienhallinnan, joka on osa ennaltaehkäisyä ja varautumista.

Riski on perinteisen turvallisuusnäkökulman määritelmän mukaan onnettomuuden todennäköisyys ja sen seurausten vakavuuden yhdistelmä, jolloin riskienhallinnassa pyritään sekä pienentämään todennäköisyyttä negatiiviselle tapahtumalle, että pienentämään tai rajoittamaan tapahtuman seurauksia. Tietoturvallisuuden kontekstissa riskit ovat ISO/IEC 27000 –standardin määritelmän mukaan mahdollisuus, että uhka, eli ulkopuolinen toimija, hyödyntää turvattavan kohteen haavoittuvuutta ja siten aiheuttaa organisaatiolle haittaa. Turvattava kohde on jotain, mikä on organisaatiolle tai henkilölle arvokas. Tietoriskin kontekstissa kohde voi olla esimerkiksi toiminnan mahdollistaja, kuten tietojärjestelmä tai tietoverkko, tai kilpailuetua tuottava tieto tai osaaminen (ISO/IEC 2009). Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän VAHTI:n määritelmän mukaan tietoriski on tapahtuma, ”jolloin tieto tai tietojärjestelmä ei ole käytettävissä, tieto on muuttunut jonkin tapahtuman kautta tai päätenyt ulkopuolisten haltuun” (VAHTI, 2003). Tässä määritelmässä esiintyvät kolme tietoturvallisuuden tavoitetta: saatavuus, eheys ja luottamuksellisuus. Näiden kahden määritelmän erona on, että ensimmäisessä

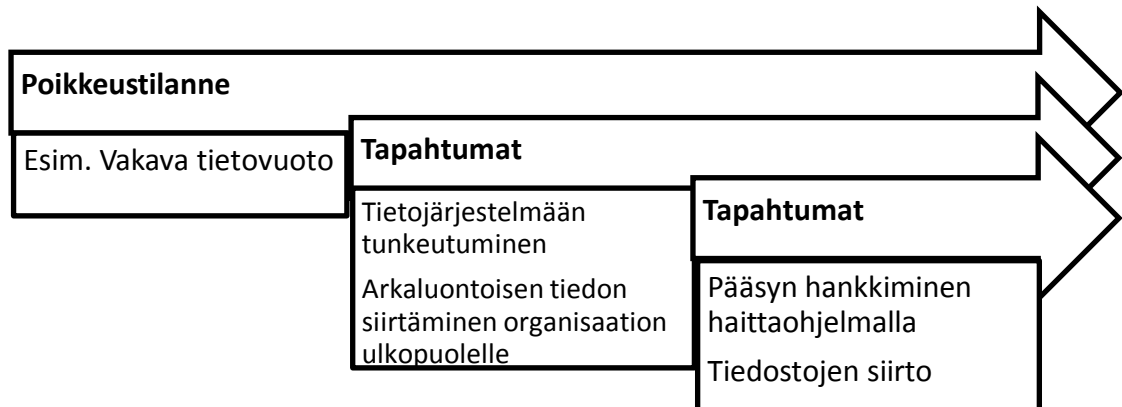
tapahtuman negatiiviset vaikutukset ei ole välttämättä realisoituneet, mutta uhkan realisoitumisen todennäköisyys on olemassa.

Kyberriski on Von Solmsin & Van Nierikin (2013) erottelun ja edellä esitettyjä määritelmiä hyödyntämällä määritettävissä riskiksi, joka uhkaa tietoverkkojen ja –järjestelmien kautta kohdetta, joka toimii fyysisessä maailmassa tai sen toimenpiteet vaikuttavat fyysiseen maailmaan. Kuten jo kyber –termin määrittelyssä, kyberriski voidaan siis liittää toimintaan tietoturvallisuuden tiedon sijaan. Valtionhallinnon kontekstissa toiminta voi olla yhteiskunnallisesti merkittävää ja Haller et al. (2010, s.6) liittävätkin kyberriskin erityisesti ns. kriittiseen infrastruktuuriin ja siihen liittyviin järjestelmiin. Kriittistä infrastruktuuria on valtion ja sen kansalaisten yleisen toiminnan ja turvallisuuden liittyvää infrastruktuuria, kuten energiantuotanto ja sähkönsiirtoverkosto. Riskinä on näiden palveluiden tuottamisen vaarantuminen. Kyberriskin realisoituminen voisi täten suoraan vaikuttaa fyysisen maailman kohteisiin, joten se eroaa tietoriskistä lähinnä vaikutuksiltaan. Tietoriskit vaikuttavat tietoon tai tietojärjestelmiin ja niiden kautta mahdollisesti toimintaan. Tutkimuksen kontekstissa kyberriskiä tarkastellaan tietoriskin synonyymina eli tietoon sekä tietojärjestelmiin ja –verkkoihin kohdistuvana riskinä.

Vakavien ja laajavaikutteisten riskien realisoituminen johtaa poikkeustilanteeseen (Major Incident), joka voidaan rinnastaa kriisitilanteisiin sen vaatiman laajemman reagoinnin kautta; poikkeustilanteen selvittäminen vaatii erillisiä, normaalien prosessien ”ulkopuolella” olevia toimenpiteitä. Rosenthal & Kouzmin (1997, s. 279) toteavat, että yleisesti kriisitilanteen ominaispiirteitä ovat tarve ja välttämättömyys isoille päätöksille normaalitilannetta lyhyemmässä aikaikkunassa. Kriisitilanteita ja niihin liittyvää päätöksentekoa leimaa myös usein niiden tuleminen yllätyksenä päätöksentekijöille. Organisaatiossa poikkeustilanne, tai sen synonyymi vakava häiriötilanne, ovat lähtökohtaisesti jokaisen organisaation itsensä määriteltävissä. Yleisesti sen voidaan kuitenkin katsoa olevan tilanne, joka on toimijan toiminnan tai turvallisuuden kannalta sietämätön, eli se uhkaa merkittävästi esimerkiksi organisaation toimintaa tai sen olemassaoloa. Tällöin tarvitaan päätöksentekoa ja toimenpiteitä vahinkojen välttämiseksi tai minimoimiseksi sekä poikkeustilanteesta toipumiseen eli palaamiseen normaalitilanteeseen. Yleensä poikkeustilanteen käsite liitetään ajanjaksoon, jossa häiriöt ja niihin liittyvät tapahtumat ovat alkaneet tai jatkuvat, eli poikkeustilanne käsitetään ajanjaksona jolloin jotain haitallista parhaillaan tapahtuu. Baskerville et al. (2013) kuitenkin huomauttaa että poikkeustilanne voi olla myös pelkkä uhka, että siirryttäisiin normaalitilanteesta sietämättömään tilanteeseen. Eli myös laajempi ja välitön riski ja sen realisoitumisen uhka voivat myös muodostaa nopeaa reagointia vaativan poikkeustilanteen.

Tieto- ja kyberturvallisuuden kontekstissa poikkeustilanne on usein tapahtumien ketju, joka sisältää tapahtuman tai tapahtumien sarjan, jotka johtavat toimijan kannalta vakavasti haitalliseen lopputulokseen (ENISA, 2014). Yksittäinen tapahtuma sisältää joukon toimenpiteitä, jotka johtavat tapahtuman toteutumiseen ja lopulta poikkeustilanteen rea-

lisoitumiseen. Eli yksittäinen tapahtuma ei välttämättä itsessään aiheuta haittaa organisaatiolla, vaan ne ovat osa tapahtumien ketjua, joka johtaa organisaation kannalta haitalliseen tapahtumaan tai ilmiöön. Toisaalta jokin yksittäinen tapahtuma voi lopulta johtaa vakavasti haitalliseen tilanteeseen, jolloin on tarpeen reagoida tähän yksittäisenä tapahtumana harmittomaan tapahtumaan. Alla olevassa kuvassa 4 havainnollistetaan poikkeustilanteen muodostumista sen osakokonaisuuksista kuvitteellisessa poikkeustilanteessa.



Kuva 4 Poikkeustilanne TKT-kontekstissa, mukailen ENISA (2010, s. 60)

Poikkeustilanne koostuu siis tapahtumista, jotka johtavat vakavasti toimijan kuten organisaation kannalta haitalliseen lopputulokseen. Kuvan 4 esimerkissä organisaation tietojärjestelmään tunkeutuminen, johtaa tietojen vuotamiseen organisaation ulkopuolelle. Tunkeutuminen voi sisältää monia eri vaiheita, kuten haittaohjelman siirtäminen järjestelmään, jossa tiedot sijaitsevat. Kyseessä on yksinkertaistettu malli, joten reaali maailmassa tapahtumat ja niiden ketjut voivat olla huomattavasti monimutkaisempia.

Poikkeustilanne jakaa organisaation TKT-johtamisen ajallisesti kahteen osaan: tilanteeseen, jossa poikkeustilanteeseen varaudutaan, ja tilanteeseen, jossa poikkeustilanteeseen reagoidaan. Tieto- ja kyberturvallisuuden johtaminen voidaan täten jakaa yleisellä tasolla estämiseen (prevention) ja reagoimiseen (response) tähtääviin elementteihin, jotka sovitetaan ympäristöön ja tilanteeseen sopiviksi. Vaikka poikkeustilanteiden hallinta alkaa jo ennen poikkeustilanteen realisoitumista, eksklusiivisesti riskien eliminoimiseen tähtäävät tieto- tai kyberturvallisuusstrategiat eivät ole riittäviä takaamaan riittävää turvallisuutta nykyisessä dynaamisten, eli nopeasti muuttuvien tieto- ja kyberriskien tilanteessa. Poikkeustilanteisiin reagoiminen ja siihen vaikuttavien tekijöiden hallinta (Incident response) on tärkeä osa organisaation TKT –riskien hallintaa. Organisaatioiden tulee riittävästi resursoida ja toteuttaa reagoimiseen tarvittavat prosessit ja toimijat. (Siegel et al, 2002, Baskerville et al. (2014, s. 139), Ambiola, 2007, Alberts et al. 2004)

TKT –kontekstissa tilanteen kriittisyyteen tai vakavuuteen eli tilanteen sietämättömyyteen vaikuttaa esimerkiksi toiminnan tai prosessien riippuvuus riskin kohteena olevasta tietojärjestelmästä. Mikäli organisaation toimintaa on hyvin riippuvainen tietojärjestelmästä johon riski kohdistuu, on sen toiminnan palauttaminen normaalitilaan tärkeää, jotta liiketoiminnan prosessit voivat jatkua. Muita tilanteen vakavuuteen vaikuttavia tekijöitä ovat haitalliset seuraukset ja niiden suuruus, kuten esimerkiksi raha- tai mainetappiot. Toisaalta kriittisyyden tietojärjestelmälle tai sen tukemalle toiminnalle voivat määritellä asetetut velvoitteet ja vaatimukset, jotka tulevat esimerkiksi fyysisen turvallisuuden kautta, kuten esimerkiksi tuotantolaitosten turvajärjestelmät, joiden häiriö voisi vaarantaa työntekijöiden turvallisuuden. Valtiollisella tasolla Suomessa Yhteiskunnan Turvallisuusstrategia, YTS, (Valtioneuvosto, 2010), määrittelee erilaisia yhteiskunnan kannalta elintärkeitä toimintoja, kuten valtion johtaminen, jotka tulee turvata myös poikkeustilanteissa. Kohonnut riski, esimerkiksi edellä mainittua toimintoa tukevissa järjestelmissä, saattaisi aiheuttaa tilanteen jossa tarvittaisiin aktiivista, normaalista poikkeavaa toimintaa ja toiminnan johtamista tilanteen estämiseksi ja mahdollisten korjaavien toimenpiteiden ja prosessien nopeuttamiseksi.

2.2 Strategisen tason johtaminen

Tieto- ja kyberturvallisuuden strateginen johtaminen on oleellinen osa tietoriskien ja mahdollisten poikkeustilanteiden järjestelmällistä ja kattavaa hallintaa. Yleisesti strategisella tasolla ohjataan toimintaa ja sen pääsuuntia sekä määrittellään toiminnan painopistealueita eli toimintoja ja riskejä joihin kiinnitetään erityisesti huomiota ja resursseja. Painopistealueita voidaan määritellä esimerkiksi yrityksen liiketoimintastrategian ja riskien arvoinnin avulla tarkastelemalla kriittisiä liiketoiminta-alueita ja –prosesseja sekä niitä tukevia tietojärjestelmiä. Valtionhallinnon organisaatioiden tapauksessa painopistealueita tehdään myös lainsäädäntöön pohjautuen, joka määrittelee esimerkiksi eri ministeriöiden ja virastojen lakisääteisiä tehtäviä ja niiden tuottamia palveluita.

Tieto- ja kyberturvallisuuden strategisella tasolla siis tarkastellaan ja arvioidaan sekä ehkäistään ja pienennetään organisaatiotasolla tietopääomaan ja tietojärjestelmiin kohdistuvia riskejä eli hallitaan organisaation laajuisesti tietoriskejä, jotta organisaatio voisi välttää mahdolliset poikkeustilanteet ja niiden haitalliset seuraukset. Strategisella tasolla riskienhallinta koostuu neljästä osakokonaisuudesta:

Yleinen riskienhallinta-strategian suunnittelu, jonka tarkoituksena määritellä kuinka riskejä arvioidaan, niihin reagoidaan ja valvotaan.

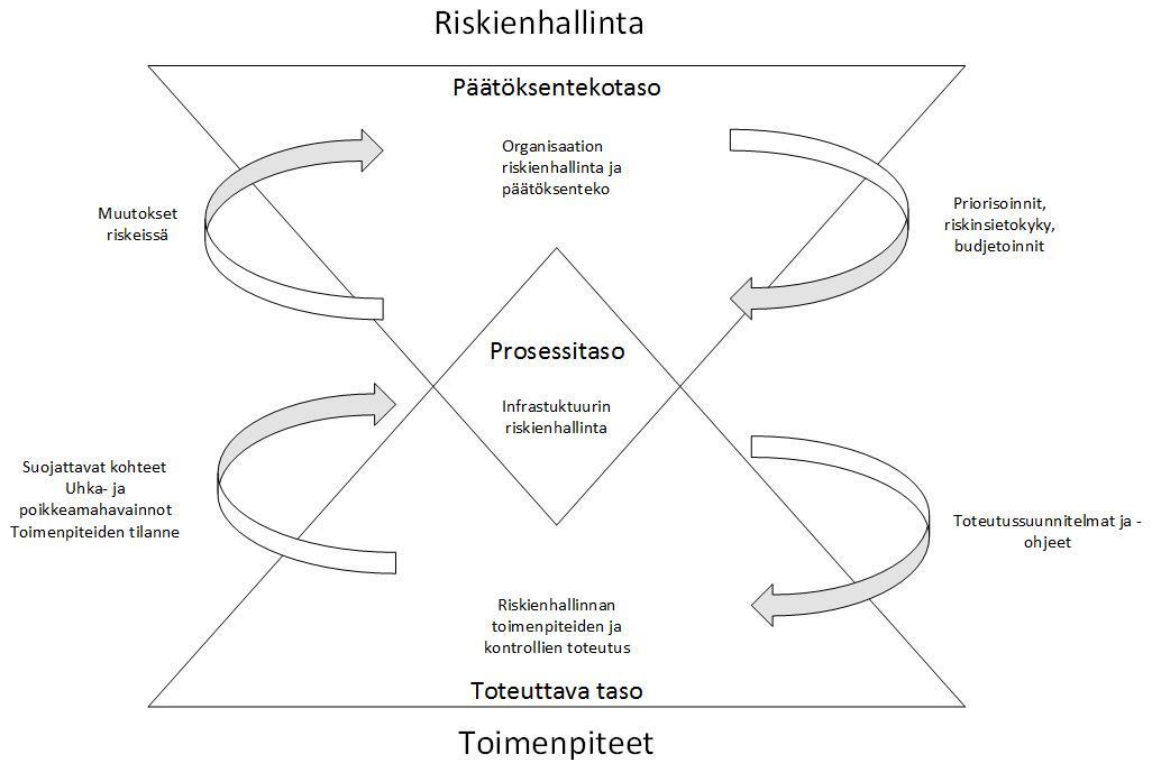
Riskin ja sen muotoutumisen määrittely, eli uhkien, todennäköisyyksien ja niiden vaikutusten ja seurausten arviointi

Strategisten, organisaation laajuisten toimenpiteiden suunnittelu riskien vaikutusten estämiseksi

Riskien valvonta ja riskienhallinnan jatkuvuuden suunnittelu sekä strategisella että operatiivisella tasolla

Tässä National Institute of Standards and Technologyn (NIST, 2012) julkaisun SP 800-30:n esittelemässä lähestymistavassa riskienhallintaa lähestytään siis prosessina tai metodologiana, jonka pääkohdat ovat riskienhallintaprosessin suunnittelu, riskien määrittely, riskien käsittelyn ja ehkäisemisen suunnittelu ja riskienhallinnan jatkuvuuden varmistaminen. Strategisella tasolla TKT-toiminta on sekä operatiiviseen että strategisen tason toiminnan kehittämistä ja suunnittelua sekä molempien tasojen TKT-toiminnan jatkuvuuden ja järjestelmällisyyden varmistaminen.

Edellä mainittu lähestymistapa kuvaa riskienhallinnan strategisen tason tavoitteet ja prosessit, mutta se ei kuvaa eri toimijoita tai niiden rooleja suhteessa riskienhallinnan kokonaisuuteen. Strategisella tasolla tapahtuvan suunnittelun tulisi ohjata ja vaikuttaa myös operatiivisen tason toimintaa. NIST:llä (2014) on myös toinen malli, jonka avulla strategisen riskienhallinnan roolia ja merkitystä organisaation operatiivisen toiminnan kannalta voidaan tarkastella ja hahmottaa. National Institute of Technologyn (NIST, 2014, s.12) ohjeessa kuvataan organisaation tietoriskienhallintaa ja siihen liittyviä tietovirtoja kolmiportaisella mallilla: Ylimpänä ovat organisaation kokonaisriskienhallintaa ja siihen liittyvää päätöksentekoa harjoittava päätöksentekotaso. Seuraavassa tasossa on prosessitaso, jossa toteutetaan infrastruktuuritason riskienhallintaa, ja alimpana on toteuttava taso, joka implementoi ja toteuttaa riskienhallintakontrollit –ja toimenpiteet. Kuvassa 6 on havainnollistettuna NIST:n malli.



Kuva 5. Tietoriskien hallintaa kuvaava yleinen prosessi- ja toimintamalli. (mukaillen NIST, 2014)

Kuvassa 6 on nähtävissä TKT- johtamiseen liittyvien eri toimintotyyppien jatkumo operatiivisista toiminnoista hallinnollisiin. Mallin jaottelu voitaisiin toteuttaa myös operatiivisiin, taktisiin ja strategisiin toimintoihin, kuten Santos Moreira et al. (2008) esittävät. Päätöksentekotason toiminnot, eli strategiset toiminnot voidaan katsoa olevan luonteeltaan operatiivista toimintaa ohjaavia tai organisaation kokonaisriskienhallinnan johtamista. Alemmalla tasolla toiminnot ovat operatiivisia, kuten esimerkiksi verkkoliikenteen valvonta eli käytännön toimenpiteitä suorittavia. Hallinnollisia toimintoja ovat esimerkiksi tietoturvallisuuden hallintajärjestelmä. Hallinnollista toimintaa ohjaavat usein ulkopuolelta tai organisaation strategian asettamat vaatimukset, kuten lait tai standardit. (Von Solms, 2005). Yleistason mallina kuvassa 6 ei oteta kantaa siihen millainen prosessi riskienhallinnan toteuttamisesta muodostuu, mutta se tarjoaa viitekehysten, jonka avulla riskienhallinnan eri toimintoja voidaan jäsentää. Käytettävä malli ei kuvaa täydellisesti tätä kokonaisuutta, mutta periaatetasolla se havainnollistaa tilannetta, jossa nykyisin NIST:in mukaan organisaatioiden riskienhallinta etenkin tietoriskien osalta toimivat: Riskien arviointia ja toimenpiteiden priorisointia ja suunnittelua toteuttava tasot eivät ole toteuttamassa konkreettisia toimintoja, kuten kontrolleja tai korjaavia toimenpiteitä.

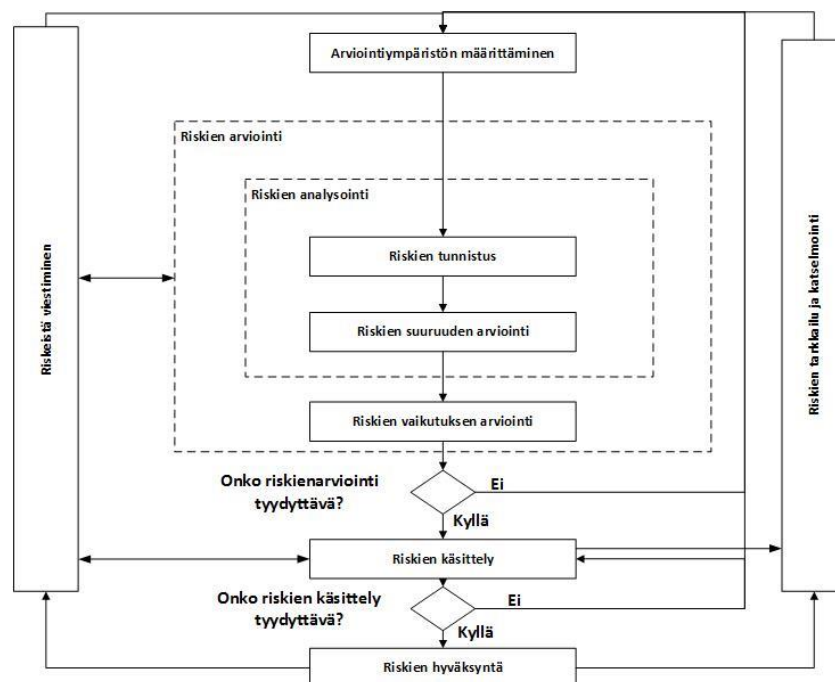
Malli havainnollistaa myös valtionhallinnon tietoturvallisuuden johtamiseen keskeisesti liittyvää problematiikkaa, jossa päätöksentekijöiden ja toimenpiteitä suorittavien tahot ovat erillään toisistaan ja niiden välille tarvitaan tietovirtoja. Käytännössä tilanne on valtionhallinnon TKT-johtamisen osalta monimutkaisempi ja sisältää muitakin kuin mallissa

esitettyjä rooleja omaavia toimijoita Valtionhallinnon TKT –johtaminen sekä siihen liittyvä yhteistyö ja koordinointi ovat laajoja kokonaisuuksia, joihin liittyy esimerkiksi Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän VAHTI:n toiminta sekä useita muita toimijoita eri rooleissa (VAHTI, 2016, Janhunen, 2015).

Tieto- ja kyberturvallisuuden johtamiseen on olemassa useita menetelmiä ja viitekehyksiä, joista useimmat lähestyvät aihetta riskienhallinnan näkökulmasta eli ennaltaehkäisyn ja varautumisen kautta. Malleja voidaan hyödyntää kehitettäessä ja toteutettaessa organisaatioon riskienhallinnan käytäntöjä ja prosesseja. Niitä voidaan käyttää apuna jäsentelämään ja systematisoimaan riskienhallintaa ja siten parantamaan sen kattavuutta.

Tunnetuimpia lähestymistapoja tieto- ja kyberturvallisuuden riskienhallintaan ja johtamiseen ovat ISO/IEC 27000 –standardisarjassa määriteltävä tietoturvallisuuden johtamisen hallintajärjestelmä, sekä National Institute of Standards and Technology:n SP 800-30. Muita johtamismalleja ovat esimerkiksi DCSSI:n EBIOS, Albertsin et al. (2003) OCTAVE ja Iso-Britannian Central Computer and Telecommunications Agency:n CRAMM (Feinz et. al. 2013). Ennakointiin ja riskien minimoimiseen pyrkivät mallit ovat olleet hallitsevia lähestymistapoja tietoturvallisuuden johtamisessa, jolloin reaktiivinen kyvykkyys ja sen kehittäminen ovat jääneet vähemmälle huomiolle. (Baskerville et al. (2013).

ISO/IEC 27000 –standardiperhe lienee tunnetuin tietoturvallisuuden johtamisen ja hallinnan viitekehys. Näistä ISO/IEC 27005 kuvaa riskienhallintametodologian, joka jakaantuu riskien arviointiin, riskien käsittelyyn ja riskien hyväksymiseen. Standardissa kuvattu riskienhallintamalli on kuvassa 5



Kuva 6. ISO 27005 tietoriskien hallintamalli, mukailen lähteestä ISO / IEC (2008).

Riskien arviointi ja jakaantuu riskien tunnistamiseen, suojattavien kohteiden tunnistamiseen, uhkien tunnistamiseen, käytössä olevien hallintakeinojen tunnistamiseen, haavoittuvuuksien tunnistamiseen ja seurausten tunnistamiseen. Riskien arviointi käsittelee riskianalyysimenetelmiä, seurausten arviointia, häiriön todennäköisyyden arviointia sekä riskitason, eli hyväksyttävän riskitason määrittelyä. Riskien käsittelyvaihtoehtoina standardissa ovat riskin muokkaaminen, säilyttäminen, välttäminen ja jakaminen. Riskien hyväksymisessä määritellään kriteerit, joiden perusteella riskin voidaan katsoa olevan hyväksyttävällä tasolla. Näiden lisäksi standardissa käsitellään myös tietoturvariskejä koskevaa viestintää ja tiedonvaihtoa.

2.3 Operatiiviset prosessimallit

Tieto- ja kyberturvallisuuden operatiivinen toiminta on organisaation toimintaan liittyvän kyberympäristön aktiivista riskien etsimistä, arviointia ja Eri lähteet muodostavat operatiiviseen riskienhallintaan liittyvän kokonaisprosessin eri osa-alueista ja askeleista tarkastelutasosta ja tarkoituksesta riippuen. Malleissa on kuitenkin paljon yhteistä, koska ne hyödyntävät yleensä tunnettuja ja hyväksytyjä parhaita käytäntöjä. Yhtenäistä niille on valvonta ja havainnointi, tilannetietoisuuden muodostaminen, palautumis- tai toipumistoimenpiteet sekä raportointi tilanteesta ja sen käsittelystä sekä tilanteesta oppiminen. (Alberts et al. 2000)

NIST:n (2014, s.8) ohjeessa oleva kyberriskien hallinnan viitekehys sisältää yleisellä tasolla funktiot, jotka riskienhallinnassa tulisi toteuttaa tai ainakin huomioida. Vastaavat funktiot löytyvät myös MACCSA:n (2013, s. 11) viitekehuksesta, joskin siinä funktiot nähdään puhtaasti organisaation suojautumiskeinoina eikä niinkään riskienhallinnan lähtökohtina. Funktiot kuitenkin organisoivat ylätasolla sitä toimintaa, jotka tulisi huomioida ja toteuttaa tietoriskien hallinnan mahdollistamiseksi. Funktiot ovat täten ylätason käsitteitä, jotka sisältävät yksittäisiä toimintoja tai toimenpiteitä. Yksittäiset toiminnot tai toimenpiteet vaihtelevat organisaatiosta ja tarkasteltavasta kohteesta riippuen. Ohjeissa esiteltävät funktiot ovat seuraavat:

Suojattavien kohteiden tunnistaminen: Riskien systemaattinen minimointi ja käsittely ovat mahdollista vain, jos kohteet ja niihin kohdistuvat riskit ovat tunnistettu, ja tieto niistä on oikealla taholla. Suojattavia kohteita ovat tieto- ja kyberturvallisuuden kontekstissa järjestelmät, laitteet, tietoverkot sekä näihin tallennetut tiedot. Suojattavien kohteiden tunnistaminen ja kohteiden merkityksellisyyden arviointi mahdollistaa riskiarvioinnin tekemisen.

Suojautuminen: Riskien minimoimiseen tai niiden estämiseen tähtäävät hallinnolliset ja tekniset toimenpiteet ja ratkaisut, joista voidaan käyttää myös nimitystä

suojamekanismit. Suojamekanismit voivat sisältää myös uhka- ja poikkeustilanteiden havaitsemista tukevia mekanismeja.

Uhka- ja poikkeustilanteiden havaitseminen ja tunnistaminen: toimenpiteet, menetelmät ja prosessit, joilla uudet uhkatilanteet ja mahdolliset poikkeustilanteet sekä niiden muodostamat riskit havaitaan. Uhkat ja poikkeustilanteet on lähtökohdaisesti tunnistettava, jotta niihin voitaisiin reagoida.

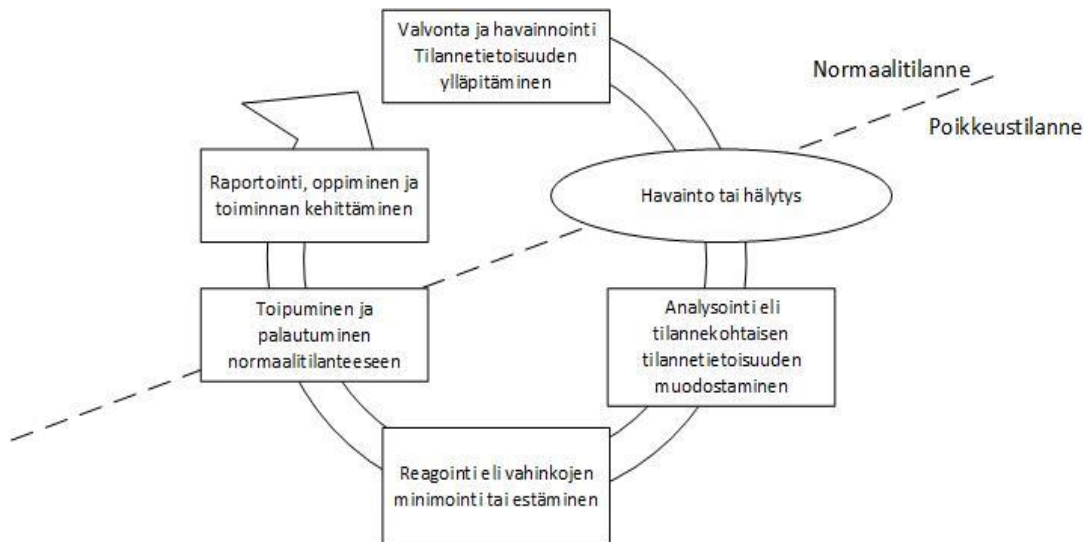
Reagoiminen: Havaittuihin uhka- tai poikkeamatilanteen hallitsemiseksi käynnistettävät prosessit ja niihin liittyvät hallinnolliset tai tekniset toimenpiteet, jotka tähtäävät mahdollisten haittavaikutusten todennäköisyyden pienentämiseen tai tapahtuneiden haittavaikutusten rajoittamiseen.

Palautuminen: Strategioiden, prosessien ja toimenpiteiden suunnittelu, joilla siirrytään poikkeustilanteesta normaalitilanteen toimintaan, sekä häiriötilanteissa suunnitelmien toteuttaminen.

Näitä funktioita toteutetaan kaikilla kuvan 6 kolmella tasolla, joskin nämä toiminnot eroavat toisistaan tasosta riippuen: päätöksentekotasolla funktioita tarkastellaan kokonaisvaltaisesti riskienhallinnan strategisesta näkökulmasta. Tällä tasolla tehdään strategiset päätökset siitä, mitkä ovat priorisoitavat riskit ja millaisilla toimenpiteillä ja resursseilla riskejä käsitellään. Prosessitasolla tarkastellaan prosessien sekä niihin liittyvien tietojärjestelmien ja palveluiden riskienhallintaa ja allokoidaan osoitetut resurssit konkreettisille toimenpiteille. Funktioita tarkastellaan prosessitasolla operatiivisen suunnittelun ja ohjauksen näkökulmasta. Toteuttavalla tasolla pääosin toteutetaan suunniteltuja toimenpiteitä, jotka edellä esitettyihin funktioihin liittyy eli esimerkiksi implementoidaan ja valvotaan uhkien havaitsemiseen tarkoitettuja prosesseja ja menetelmiä. (NIST, 2014)

Vastaavia osakokonaisuuksia on myös Fenzin et al. (2014, s. 418) muodostamassa tietoturvariskien hallintametodologiassa. Tämä yleisen tason kuvaus on muodostettu kirjallisuudessa esitettyjen tietoturvariskienhallinnan malleista (COBIT, ISO 27000), jotka heidän havaintojensa mukaan sisältävät vain vähän eroavaisuuksia eli ne sisältävät samoja elementtejä. Fenzin et al. (2004, s. 418) yhdistelemällä muodostettu metodologia sisältää tietojärjestelmäkokonaisuuksien määrittelyn, uhka- ja haavoittuvuusarvioinnin, riskienarvioinnin sekä tarvittavien suojamekanismien tunnistamisen, arvioinnin ja implementoinnin. Kyseinen malli painottaa enemmän ennakoivia riskien minimoinnilla ja arvioinnilla, kun taas NIST:n (2014) malli on lähtökohdiltaan toiminnallinen ja reaktiivinen.

Kuvassa 7 oleva prosessimalli kuvaa tieto- ja lyberturvallisuuden operatiivista toimintaa normaali- ja poikkeustilanteessa. Siinä esiintyvät yleisimmin kirjallisuudessa esitetyt vaiheet ja toimenpiteet joita operatiiviset toimijat tekevät. Kyseessä on jatkuva prosessimalli, jossa normaalitilanteesta siirrytään poikkeustilanteeseen ja poikkeustilanteesta takaisin normaalitilanteeseen. (Fenz et al. 2004, Alberts et al. 2004, NIST 2014)



Kuva 7. Poikkeustilanteiden käsittelyn prosessimalli

Normaalitilanteessa toimenpiteet keskittyvät tilanteen valvontaan ja havainnointiin. Poikkeustilanteen käsittely aloitetaan, kun organisaatio on havainnut tapahtumia, jotka sen määrittelyn mukaan tarvitsevat poikkeustilanneprosessin käynnistämistä eli laajempaa tilannekuvan keräämistä ja tarkempaa analysointia. Kun ymmärrys tilanteesta on muodostettu, voidaan arvioida tarvittavat toimenpiteet ja päätökset toipumisesta eli palautumisesta normaaliin tilanteeseen. Ideaalitapauksessa poikkeustilanteen käsittelystä opitaan ja toimintatapoja kehitetään, jotta organisaatio olisi paremmin varautunut mahdollisiin tuleviin poikkeustilanteisiin. Realisoitumisella on syy, jonka selvittämällä voidaan varautua mahdollisiin tulevaisuuden tilanteisiin ja seurauksiin jotka vaarantavat tieto- ja kyber turvallisuuden ja siten mahdollisesti aiheuttavat muuta vahinkoa.

2.4 Tilannetietoisuus poikkeustilanteiden johtamisessa

Poikkeustilanteisiin ja niiden johtamiseen liittyy oleellisesti tietoisuus ja ymmärrys tilanteesta, koska näissä tilanteissa tarvitaan usein merkittäviä päätöksiä suhteellisen lyhyessä ajassa. Jo lähtökohtaisesti edellä kuvattu prosessimallin mukainen reagointi poikkeustilanteeseen on mahdollista vain, jos poikkeustilanne on tunnistettu ja sen laajuus ja mahdolliset vaikutukset ymmärretty. Tämä korostuu valtionhallinnon tapauksessa, koska tehokas laajoihin, monia toimijoita ja organisaatioita koskettavaan tilanteeseen reagointi hallitusti ja johdetusti vaatii tietoa ja ymmärrystä tilanteeseen liittyvistä tekijöistä ja sen mahdollisista kehityssuunnista.

Perinteisen ja usein käytetyn, Endsleyn (1995) muodostaman mallin mukaan ratkaisevan tekijän erityisesti kompleksisiin ja dynaamisiin tilanteisiin liittyvässä aikakriittisessä päätöksenteossa muodostaa kognitiivinen tiedon kerääminen ja käsittelyn prosessi, jota hän kuvaa termillä *tilannetietoisuus* (eng. Situational awareness). Tilannetietoisuus kolmiosainen kokonaisuus, joka kuvaa toimijan ymmärrystä sen käsittelemästä tilanteesta. Toi-

mijan tulisi pyrkiä hyvään tilannetietoisuuteen, jotta epävarmuus tai epätietoisuus esimerkiksi päätöksentekovaihtoehtoista ja niiden seurauksista vähenisi. Tilannetietoisuus käsittelee havainnot tilanteesta, ymmärryksen havaintojen merkityksestä sekä projektion havaintojen vaikutuksesta tulevaisuuteen. (Endsley 1995) Tilannetietoisuus on havainnointia ja tiedon prosessointia tilasta, eli (toiminta)ympäristöstä, jossa tilanne tapahtuu sekä tietoisuutta tapahtumien ajallisesta ulottuvuudesta eli tilanteen muutoksista tulevaisuudessa (Kuusisto, 2014). Hyvän tilannetietoisuuden vastakohtana voidaan pitää tilannetta, jossa toimijalla on puutteelliset tai epävarmat tiedot ja käsitys tilanteesta ja siihen liittyvistä tekijöistä, johtaen epävarmuuteen, hitaaseen päätöksentekoon ja mahdollisesti väärin päätöksiin (Zimmermann, 2014, s.25). Tilannetietoisuus ja sen muodostuminen voidaan yksinkertaisemmillaan ajatella olevan tiedon keräämisen ja analysoinnin prosessi, jonka avulla toimija saavuttaa ymmärryksen ympäristöstään ja sen muutoksista, ja osaa siten tehdä oikeat päätökset.

Tilannetietoisuuden ja sen muodostumisen tutkimista ja tilannetietoisuuden merkityksellisyyttä Endsley (1995) perustelee sillä että kompleksisissa ja dynaamisissa ympäristöissä jo yksilötasolla ihmisen kyvyt tilannetietoisuuteen ja siten tehokkaaseen ja oikea-aikaiseen päätöksentekoon ovat rajoittuneet. Täten tilannetietoisuuden muodostumiseen vaikuttavat tekijät ovat hyvä tunnistaa, jotta tilannetietoisuuden muodostamista voidaan tukea. Tilannetietoisuus ei käsitteenä ole suoraan sidottu pelkästään normaalista poikkeaviin tilanteisiin, mutta riittävä tilannetietoisuuden haasteet korostuvat niissä. Näissä tilanteissa tarve tilanteen ymmärtämiseen kasvaa nopeiden muutosten seurauksena.

Huomioitavaa on myös, että vaikka teoreettisesti riittävä ja faktoihin perustuva tilannetietoisuus mahdollistaa tehokkaan ja oikean päätöksenteon, tilannetietoisuuden muodostumiseen vaikuttaa monia tekijöitä. Yksilötasolla tilannetietoisuus on riippuvainen toimijasta ja yksilöllinen, koska se on sidottu käytettävissä olevaan informaatioon sekä aikaisempien kokemusten tai koulutuksen ansiosta muodostuneeseen ymmärrykseen. Eri näkökulmista ja eri informaatiolähteiden avulla tarkasteltuna tilanteet näyttäytyvät erilaisena. Endsley (1995) lisäksi huomauttaa, että vaikka tilannetietoisuus, eli ymmärrys tilanteesta vaikuttaa päätöksentekoon, se ei suoraan johda päätöksenteon oikeellisuuteen. Oikea tieto ei välttämättä johda oikeaan päätökseen tai tilannetietoisuus voi pohjautua tietoon joka johtaa väärin tulkintoihin ja johtopäätöksiin. Myös Kuusisto (2005) toteaa, että tilannetietoisuus on aina jossain määrin rajoittunut, eli yksilöt eivät kykene muodostamaan täydellistä kuvaa tilanteesta ja sen kehittymisestä tulevaisuudessa, johtuen havaintojen puutteellisuudesta ja rajoittuneesta kyvykkyydestä tilanteen tulkintaan. Täten päätöksentekijällä tulisi olla käytettävissään tieto, joka on tilanteen vaatiman päätöksenteon kannalta oleellista.

Yksilöistä koostuvan kokonaisuuden, kuten tiimin tai organisaation, tilannetietoisuuden (Endsley 1995) näkee koostuvan sen jäsenten tilannetietoisuuden yhdistelmästä. Endsley (1995) tarkastelee ryhmän jäsenten tilannetietoisuutta suhteessa jäsenen tehtävien vaati-

muksiin. Eli ryhmän tilannetietoisuus ei ole riittävä, mikäli jokainen jäsen ei pysty suoriutumaan hänelle osoitetuista tehtävistä, vaikka muiden jäsenten tilannetietoisuus olisi-kin riittävä. (Endsley 1995). Teoreettisesti tästä näkökulmasta ajateltuna laajemmalla eli organisaatioiden välisellä tasolla tilannetietoisuus vaatii, että jokaisella organisaatiolla on riittävä tilannetietoisuus omista tehtävistä suoriutumiseen. Kuten todettua, tieto- ja kyberturvallisuuteen liittyvät tehtävät eivät kuitenkaan välttämättä rajoitu yhden organisaation sisälle vaan voidaan tarvita organisaatioiden välistä yhteistyötä, jolloin tarvitaan yhteinen käsitys tilanteesta (Kuusisto et al. 2007).

2.4.1 Tilannetietoisuus ja tilannekuva

Eri konteksteissa ja eri tarkoitukseen muodostettavan tilannetietoisuuden asettavat erilaisia tietotarpeita. Tällöin luonnollisesti myös tietolähteet ja esimerkiksi tiedon laadulle asetettavat kriteerit ovat vaihtelevat. Seuraavassa tarkastellaan mitä tilannetietoisuutta muodostetaan tieto- ja kyberturvallisuuden kontekstissa sekä mitä ominaispiirteitä ja haasteita sen muodostamiseen liittyy. Tilannetietoisuutta lähestytään tilannekuva –käsitteen avulla: *tilannetietoisuus muodostetaan tilanteesta saatavan tilannekuvan perusteella*. Endsleyn (1995) määritelmässä tilannekuva sisältyy tilannetietoisuuteen, koska hän näkee yhtenä tilannetietoisuuden osa-alueena havainnot tilanteesta. Endsley (1995) asettaa tiedon keräämisen ehkä enemmän toimijan omaksi tehtäväksi, kun tilannekuva käsitteessä lähdetään mallista, jossa tietoa tuotetaan päätöksenteon tueksi.

Tutkimuksessa tarkastellaan erityisesti *tieto- ja kyberturvallisuuden tilannekuva* (TKT-tilannekuva), koska tutkimuksen kontekstissa tutkimuskohteella luodaan tilannetietoisuutta, jota tarvitaan toimintaa ja päätöksentekoon tieto- ja kyberturvallisuutta vaarantavassa poikkeustilanteessa. Tilannekuvan voidaan katsoa sisältävän kaiken sen tilanteesta saatavan datan ja informaation, jonka perusteella toimija muodostaa ymmärryksen tilanteesta nykyhetkessä sekä luo projektioita tulevaisuuteen (Barford et al. 2010). Tilannekuva määritellään tässä tutkimuksessa siten tiedoksi, jonka perusteella toimija muodostaa tilannetietoisuutta, eli muodostaa ymmärrystä tilanteesta toimintansa ja päätöksentekonsa tueksi.

Turvallisuuslähtöisesti tarkasteltuna tilannetietoisuus on tilannetietoisuutta organisaation uhka- ja riskitilanteesta, ymmärrystä niiden vaikutuksista ja tilanteen kehittymisestä. Tästä lähtökohdasta Yhdysvaltalainen komitea, Committee on National Security Systems (CNSS 2015, s.115), määrittelee omassa sanastossaan tilannetietoisuudeksi

Paikkaan ja aikaan sidottu havainto, käsitys tai ymmärrys (perception) organisaation turvallisuus- ja uhkatilanteesta; ymmärrys turvallisuustilanteen ja uhkatilanteen perusteella organisaatioon kohdistuvasta riskistä sekä näiden kokonaisuuk- sien muutoksesta tulevaisuudessa.

Kuten voidaan havaita, tämä käsite sisältää Endsleyn (1995) mallin peruselementit, tiedon nykyhetkestä, ymmärryksen ympäristön vuorovaikutussuhteista ja ymmärryksen tulevaisuuden kehityssuunnista. Kuten yleisesti tiedon hyödyntämisessä, pelkkä datan kerääminen ei riitä, vaan tarvitaan kyvykkyyttä datan jalostamiseen tiedoksi ja ymmärrykseksi (Kuusisto, 2014, s. 44), eli tilannekuvan jalostamista tilannetietoisuudeksi. Tieto- ja kyberturvallisuuden kontekstissa tilannetietoisuus on siis ymmärrys suojattavan kohteen, kuten tietojärjestelmän ja sen suojauskeinojen muodostamasta kokonaisuudesta, sekä ymmärrystä sen tilanteesta ja siihen liittyvistä tapahtumista tarkasteltavalla ajanhetkellä sekä tulevaisuudessa.

Tilannetietoisuutta TKT-kontekstissa on myös ymmärrys siitä, onko kyseessä poikkeustilanne, joka vaatii erillisten toimenpiteiden tai prosessien käynnistämistä. Tilannekuva toimii siis organisaatioiden tai valtionhallinnon tason tietoturvatiminoille merkkeinä ulkopuolisesta ja haitallisesta toiminnasta tietojärjestelmäympäristössä (Indicator of Compromise, IOC). Eli tilannekuvan perusteella tietoturvaluutta valvovat tahot pyrkivät päättämään onko kyseessä mahdollisesti organisaation tietoturvaluuden kannalta haitallisesta toiminnasta ja siten mahdollisesta poikkeustilanteesta (Gragido, 2012).

Tieto- ja kyberturvallisuuden kontekstissa tilannekuva voi muodostua laajasta skaalasta hyvin erilaisia tietolähteitä uutisista tietojärjestelmien lokitietoihin. Tilannekuva voi koostua sekä järjestelmistä kerätyistä tiedosta, että ihmisten välittämästä tiedosta. Tilannekuva voidaan jakaa strategisen ja operatiivisen tason tilannekuvaan sen käyttötarkoituksen perusteella, kuten esimerkiksi Leppänen et al. 2016 tekevät. Strategisella tasolla tilannekuvaa tarvitaan organisaatiotason strategisen päätöksenteon tueksi, operatiivisella tasolla puolestaan esimerkiksi yksittäiseen järjestelmään liittyvän päätöksenteon tueksi. Toisaalta tilannekuvaa voidaan tarkastella myös Endsleyn (1995) tilannetietoisuuden määritelmän avulla, jolloin tilannekuvan tarkoituksena on tuottaa joko ymmärrystä nykytilanteesta ja siihen liittyvistä tekijöistä ja niiden vuorovaikutussuhteista, tai tuottaa tietoa tilanteen kehittymisestä tulevaisuudesta. Tällöin voidaan arvioida, millaista tilannekuvaa tarvitaan tietyn tyyppisen tilannetietoisuuden muodostamiseen, kuten esimerkiksi tulevaisuuden ennakkointiin (Rummukainen et al. 2015).

Hyödyntämällä Franken & Brynielssonin (2014) sekä Barfordin et al. (2010) näkemyksiä, tilannekuvan käsite voidaan jakaa kolmeen osaan kuvan 8 mukaisesti. Jaottelu tehdään tässä tapauksessa tiedon kuvaaman kohteen perusteella. Vaihtoehtoinen, tarkempi jaottelumalli voisi olla esimerkiksi jaottelu tietolähteiden perusteella, kuten tilannekuvajärjestelmistä saata tieto tai julkisista lähteistä saatava tieto. Tässä yhteydessä käytetään yleis-tason jaottelua, koska tutkimuksen tarkoituksena ei ole keskittyä tarkemmin tilannekuvan muodostamiseen ja sen sisältöön. Käytetyn tilannekuvan jaottelumallin osat ovat toimintaympäristöön liittyvä tieto, tietojärjestelmiin liittyvä tieto sekä uhkatieto. Kuten yleisesti, myös tilannekuvatieto voidaan jakaa kolmeen perustasoon, dataan, informaation ja tietämykseen.



Kuva 8. Tilannekuvan kategoriat (Franke & Bryenilsson, 2014; Barford et al, 2010)

Eri kategoriat ovat kiinteässä yhteydessä toisiinsa, ja tilannekuvan tulkitsemisen ja ymmärryksen muodostamisen yhteydessä tietoja yhdistellään tilannetietoisuudeksi. Voidaan myös argumentoida, että yksittäinen tieto ei ole itsessään hyödyllistä ilman laajempaa kontekstia. Esimerkiksi tietojärjestelmän tilanteesta ilman siihen liittyvää toimintaympäristöä ja uhkatieta ei ole hyödyllistä. Toisaalta pelkkä uhkatieta esimerkiksi uudesta uhkasta, kuten uudesta haittaohjelmasta, ei ole itsessään hyödyllistä, vaan tarvitaan tietoa siitä, mihin järjestelmiin ja palveluihin uhka kohdistuu, jotta tarvittavat toimenpiteet ja resurssit voidaan kohdistaa oikein (Janhunen, 2015).

Tietojärjestelmäympäristöön liittyvä tieto koostuu tietojärjestelmäinfrastruktuurista ja niiden tuottamista palveluista sekä näiden sen hetkisestä toiminnasta ja tilanteesta. Kattavaan ympäristötietoon tarvitaan tietoa järjestelmien vuorovaikutus- ja riippuvuussuhteista, jotta yksittäisten tapahtumien väliset vaikutukset ja vaikutusketjut voidaan hallita. Tämän määrittelyn avulla luodaan käsitys järjestelmien ja palveluiden keskinäisistä vaikutus- ja riippuvuussuhteista, minkä avulla voidaan tehdä riski- ja vaikuttavuusarvioita, esimerkiksi taloudellisista menetyksistä. Ympäristötiedon kerääminen mahdollistaa NIST:n riskienhallintamallin funktion suojattavien kohteiden tunnistamisen sekä turvamekanismien toteuttamisen. Ympäristötiedon kerääminen on täten tärkeä osa myös jatkuvaa normaaliolojen riskienhallintaa.

Uhkatieta koostuu havainnoista menetelmistä ja tekotavoista tai tietojärjestelmäinfrastruktuurin kohdista, joita voitaisiin hyödyntää haitalliseen toimintaan. Uhkatieta sisältää siis tietoa tekijöistä, jotka voivat lisätä tietoriskien todennäköisyyttä ja vaikutuksia, kuten esimerkiksi haavoittuvuudet eli väärinkäyttömahdollisuudet tietojärjestelmissä. Uhkatieta sisältää myös tietoa toimijoista ja yleisesti toiminnasta, joka voi uhata organisaation

tietoturvallisuutta. Havainnot voivat sisältää havaintoja sekä menneisyydessä tapahtuneista, että parhaillaan käynnissä olevasta tieto- ja kyberturvallisuutta uhkaavasta toiminnasta. Uhkatietoa voidaan käyttää riskien todennäköisyyksien ja realisoitumisen vaikutusten arviointiin. Havainnot haitallisesta toiminnasta mahdollistavat reagoinnin, eli uhan aiheuttaman tietoriskin minimoimiseen tähtäävien toimenpiteiden käynnistämisen, sekä palautumisen normaalitilanteeseen.

Muu päätöksentekoon liittyvästä tieto, eli toimintaympäristötieto, koostuu tiedosta, jota tarvitaan TKT-johtamisen tueksi. TKT-johtamisen näkökulmasta toimintaympäristöä ovat myös organisaation asettamat tai sen ulkopuolelta tulevat tavoitteet tai vaatimukset joita se pyrkii tieto- ja kyberturvallisuuteen liittyvässä toiminnassaan noudattamaan. Toimintaympäristöön liittyvää tietoa on valtionhallinnon tapauksessa tieto esimerkiksi toimintamahdollisuuksista häiriötilanteissa tai niitä rajoittavista tekijöistä, kuten mahdollisista lainsäädännöllisistä tekijöistä.

Reaaliaikaisen tilannetietoisuuden saavuttamisen tarvitaan luonnollisesti tilannekuvaa, joka kuvaa todellista tilannetta kyseisellä ajanhetkellä. Tilannekuvassa ja sen tuottamisessa huomioonotettavia seikkoja ovat käytettävän tiedon laatu ja sen kattavuus, jotka voivat vaikuttaa tilannetietoisuuden ajantasaisuuteen ja oikeellisuuteen. Toisaalta TKT-tilannekuvan perusteella tulisi kyetä ennakoimaan tilanteen mahdollisia kehityssuuntia ja arvioimaan todennäköisintä tulevaisuuden tilannetta, sekä normaali- että häiriötilanteissa. Tilannekuvaa tulisi myös laajentaa tietojärjestelmätiedon ulkopuolelle, fyysiseen maailmaan ja toimintaan. Yhdistämällä tilanteeseen vaikuttavat muut tiedot, kuten esimerkiksi sopimustiedot, ympäristö- ja uhkatietoon, voidaan muodostaa ymmärrys tilanteesta ja sen kehittymisestä sekä siihen liittyvistä riskeistä ja niiden seurauksista myös fyysisessä toiminnassa. Tämä mahdollistaa reagoinnin ja tulevaisuuden tilanteeseen ja tietoriskeihin varautumisen siten, että se yhdistetään organisaation kokonaisriskienhallintaan (Barford et al. 2010)

2.5 Tieto- ja kyberturvallisuuden operatiivinen toiminta valtionhallinnossa

Yksi tapa, etenkin isojen organisaatioiden tapauksessa, operatiivisen tason TKT-tilannekuvan tuottamiseen ja tilannetietoisuuden ylläpitämiseen on perustaa organisaation TKT-tilannetta aktiivisesti seuraava ja havaittuihin poikkeamiin reagoiva organisaatioyksikkö. Toimintaa tehdään esimerkiksi Valtion tieto- ja viestintätekniikkakeskus Valtorissa, joka keskittyy asiakasorganisaatioidensa käyttämän tietoliikenneverkon valvontaan ja poikkeamien analysointiin (Valtori, 2016).

Vakiintunutta suomenkielistä käsitettä tälle toiminnalle ei ole, vaan kaupallisia ja organisaatioiden sisäisiä palveluita tuotetaan vaihtelevilla termeillä. Kaupallisia palveluita tuotetaan nimikkeillä kuten tietoturvanhallintakeskus tai ympärivuorokautinen kyberturval-

lisuuskeskus (Cygate, 2016, CGI, 2016), kun valtionhallinnossa käytetään termiä tietoturvaluovomo tai englanninkielistä termiä Security Operations Centre ja sen lyhennettä SOC. Yhteistä näille on organisaation tietojärjestelmien ja tietoverkkojen tieto- ja kyberturvallisuuden tilanteen ympärivuorokautinen valvonta sekä poikkeaviin tilanteisiin reagointi. Valtori, 2016) Myös jotkin kirjallisuuslähteet kuten Onwubiko (2015) ja Zimmermann ((2014), käyttävät termiä SOC. Tutkimuksessa käytetään täten termiä Security Operations Centre ja sen lyhennettä SOC siitä toiminasta ja toimintayksiköstä, joka aktiivisesti seuraa sen vastuualueena olevan kokonaisuuden, kuten yksittäisen organisaation, tieto- ja kyberturvallisuuden tilannetta.

Onwubikon, (2015) näkemyksen mukaan SOC muodostuu ihmisistä, prosesseista, tehtävistä ja teknologiasta, jotka tuottavat tieto- ja kyberturvallisuutta uhkaavien riskitekijöiden havainnointia ja analysointia sekä reagointia toteuttavia palveluita. SOC voidaan määritellä myös sen toiminnan kautta: SOC on ryhmä asiantuntijoita, jotka havaitsevat, analysoivat, raportoivat ja estävät tieto- ja kyberturvallisuuteen liittyviä uhka-, häiriö- ja poikkeustilanteita eli reagoivat tilanteisiin organisaatiossa (Zimmermann, 2014). SOC –toiminnan fokus on tietoverkkojen ja –järjestelmien tietoturvaluudessa ja siihen liittyvissä hallinnollisissa ja teknisissä toimenpiteissä ja toiminnan kehittämisessä, ei organisaation tietoturvaluuden hallinnassa eli esimerkiksi tietoturvaluuden prosessien ja politiikkojen muodostamisessa. Nimensä mukaisesti tietoturvaluomon tehtävät koostuvat pääosin valvonnasta ja tilannetietoisuuden ylläpitämiseen valvottavaan ympäristöön liittyen. Rummukaisen et al. (2015) tutkiman tietoturvaluomon tehtäviin kuuluivat ympäristön valvonta, poikkeustilanteiden tunnistaminen ja analysointi sekä sisäinen ja ulkoinen viestintä.

Tilanteessa, jossa monen organisaation strategisesta TKT-johtamisesta ja ohjauksesta vastaa yksi taho, SOC –toiminta organisoidaan hierarkkisesti, jossa pienempien, hajautettujen SOC ryhmien tai organisaatioiden yläpuolella toimii koordinoiva ja hallinnoiva keskus. Ylemmän tason SOC voi olla monen eri yksittäisen organisaation SOC-toimintaa hallinnollisella tasolla koordinoiva, mutta se ei suoraan osallistu alempien SOC toimintojen käytännön toimintaan. Valtionhallinnon strategisen tason TKT-johtamisen näkökulmasta toiminta mahdollistaisi tilannekuvan saamisen myös organisaatioiden sisältä, jolloin järjestelyllä mahdollistettaisiin laajan ja hajautetun tilannekuvan kokoaminen ja tuottaminen keskitetysti valtionhallinnon TKT-johtamisen tueksi. (Janhunen, 2015; Zimmermann, 2014)

NIST:n (2014) riskien hallintamallia soveltamalla organisaatiokohtaiset SOC:t edustavat pääosin prosessitasoa tai toimenpiteitä toteuttavaa tasoa riippuen prosessista tai tehtävästä. Ne toteuttavat pääasiassa tietoturvaluokien havainnointia ja niihin reagointia, jotka ovat osa NIST:n mallin funktioita. Yksittäisellä alemman tason SOC-yksiköllä ei kuitenkaan ole ”toiminta-alueenaan” koko valtionhallinnon TKT-tilanteen valvonta.

2.6 Tieto- ja kyberturvallisuuden tietojohdaminen

Tietojohdamisen näkökulmat ja työkalut voivat tarjota uusia mahdollisuuksia tieto- ja kyberturvallisuuden johtamiseen, kuten riskienarviointiin, liittyvien haasteiden tunnistamiseen ja ratkaisemiseen. Tieto ja sen hyödyntäminen ovat keskeinen osa organisaation toimintaa kaikilla tasoilla sekä operatiivisessa toiminnassa että liiketoimintaa tukevissa toiminnossa kuten tieto- ja kyberturvallisuuden johtamisessa. Stonen (2016) näkemyksen mukaan tieto on osa organisaation strategista kyvykkyyttä, ja tiedon jakaminen vaikuttaa organisaation valmiuteen ja kyvykkyteen ratkaista sen kohtaamia haasteita.

Yleisesti menestyvät organisaatiot ovat Choon (1998) mukaan toimijoita jotka etsivät, keräävät ja tallentavat sekä hyödyntävät tietoa. Ne pyrkivät ymmärtämään ympäristöönsä keräämällä ja prosessoimalla tietoa. Tarvittaessa ne mukautuvat ympäristöönsä ja muuttavat toimintaansa keräämänsä tiedon ja sen avulla muodostetun ymmärryksen mukaisesti. Tilanteen, organisaation ja sen ympäristön muuttuminen muuttaa vaatii uutta tietoa eli tietotarpeet muuttuvat. Tietoon liittyvä toiminta on oltava jatkuvaa, koska muutoksen jälkeen tiedon tarve muuttuu ja sen etsimisen ja hyödyntämisen prosessi alkaa alusta. Tieto- ja kyberturvallisuudessa pyritään hyödyntämään tietoa ja luomaan turvallisuutta varautumalla ja ennakoimalla sekä vastaamalla mahdollisiin häiriötilanteisiin. Keskeistä on ymmärtää ympäristöä, sen toimijoita ja siinä tapahtuvia muutoksia. Choon (1998) mukaan merkittävä organisaation tiedon hyödyntämiseen vaikuttava tekijä on ymmärrys ja ymmärryksen tavoittelu (sense making). Ymmärtämällä tietoa ja sen merkitystä pyritään vähentämään kerättyyn dataan tai informaatioon sekä toimintaan ja ympäristöön liittyvää epävarmuutta ja epätietoisuutta, jotka vaikeuttavat päätöksentekoa. Myös Kuusiston (2007) muodostamassa päätöksentekoa kuvaavassa mallissa on keskeistä informaation hyödyntäminen ja jalostaminen ymmärrykseksi, jolla voidaan luoda käsitys ongelmaan liittyvistä rajoitteista, mahdollisuuksista, todennäköisyyksistä sekä mahdollisista ratkaisuista.

Tilannetietoisuuden muodostamiseen ja päätöksentekoon liittyy täten monia eri tietoelementtejä, jotka tulisi tuottaa tai olla saatavissa. Tietoa ja tilannekuvaa tarvitaan tukemaan riskienhallintaa ja esimerkiksi lisäämään näkyvyyttä toimintaympäristöön ja muihin toimijoihin, sekä yhteistyötahoihin että tieto- ja kyberturvallisuutta vaarantaviin toimijoihin, niiden tavoitteisiin, toimintaan ja kyvykkyysiin. (Borum et al. 2015, s. 329) TKT-riskienhallinnan ja siihen liittyvien haasteiden arviointi ja ratkaiseminen voidaan siis katsoa olevan osittain tietojohdamisen tutkimusalueella eli tieto- ja kyberturvallisuutta voidaan myös ”tietojohdtaa” sen kehittämiseksi. Tietojohdamisen työkalujen avulla voidaan pyrkiä vastaamaan näihin haasteisiin tunnistamalla esimerkiksi tietojärjestelmien kehityksen kautta tai esimerkiksi hyödyntämällä tiedon laadun arvioimisessa käytettäviä menetelmiä. Tietojohdamisen tarpeellisuus TKT-kontekstissa perustuu tiedon merkityksellisyyteen päätöksenteossa. Tämä korostuu erityisesti poikkeustilanteissa, joissa tarvitaan nopeasti päätöksiä. Tietojohdamisen tarjoamat näkökulmat voidaan siis pitää TKT –johtamisen haasteiden ja mahdollisesti ratkaisujen ymmärtämiseen käytettävissä olevina työkaluina.

Yleillä tasolla tietojohdaminen on Lönnqvistin (2007, s. 114) määritelmän mukaan tutkimusalue, joka tarkastelee muiden johtamistieteiden tavoin ”erilaisten organisaatioiden toimintaa, johtamiseen ja kehittämiseen liittyviä ilmiöitä”. Tietojohdaminen tuo lisäarvoa ”informaatioon ja tietoon liittyvien resurssien, prosessien ja teknologioiden roolien ymmärtämisessä organisaation toiminnassa.” Tietojohdamista voidaan tarkastella Laihosen et al. (2013) mukaan kolmesta eri näkökulmasta: ilmiön ymmärtäminen, johtamisen käytännöt sekä johtamisen työkalut. Ensimmäinen näkökulma tarkastelee tietoa ja kuinka tieto luo lisäarvoa organisaation liiketoiminnassa. Toinen näkökulma tarkastelee, kuinka tärkeät tietoresurssit tunnistetaan ja miten niitä tulisi johtaa ja kehittää, jotta ne tuottaisivat lisäarvoa liiketoiminnassa. Kolmas näkökulma tarkastelee tiedon johtamisen käytännön työkaluja, joiden avulla organisaation tietoon liittyviä prosesseja voidaan hallita ja päätöksentekoa tukea. Näitä näkökulmia ja lähestymistapoja voidaan hyödyntää sekä haasteiden tunnistamisessa että niiden ratkaisemisessa. Tietojohdamisesta ja sen tarjoamista mahdollisista ratkaisuista voidaan Laihosen et al. (2013, s. 8) mukaan tunnistaa kaksi pääsuuntausta: liikkeenjohdollinen ja tietotekninen. Ensimmäinen tarkastelee tietoa organisaatioita tiedon käyttäjinä sekä tietoa niiden menestystekijänä, jälkimmäinen korostaa tietojärjestelmien roolia tiedon hallinnassa ja hyödyntämisessä. Tiedon johtaminen on siis toisaalta tiedon ja siihen liittyvien prosessien johtamisen haaste, mutta toisaalta myös tietotekninen haaste.

Myös valtionhallinnon TKT-johtamisen tarkastelussa hyödynnettyä NIST:n (2014) riskienhallintamallia voidaan lähestyä tietojohdamisen paradigmana, vaikka malli ei itsessään otakaan kantaa tiedonkulun prosesseihin tai tiedonsiirtoväyliin. Mallia voidaan hyödyntää ajattelumallina, jonka avulla voidaan tarkastella esimerkiksi mitä tietoa eri toimijat tarvitsevat riskienhallinnan eri funktioiden toteuttamiseen eri tilanteissa ja miten tietoa voidaan eri toimijoiden välillä siirtää. Jos päätöksentekoa ja toimenpiteitä toteuttavat taho ovat eri entiteettejä, tarvitaan tilannetietoa (luku 2.2) sisältävä tietovirta alatasolta ylöspäin, jotta riskienhallintaa ja päätöksentekoa siihen liittyen voisivat tehdä faktapohjaisia päätöksiä. Vastaavasti alemman tason toimijat tarvitsevat tietoa näistä päätöksistä ja toimenpiteisiin käytettävissä olevista resursseista. Kaikki tilanteet eivät vaadi asian käsittelyä päätöksentekotasolla, vaan toteuttavan tason asiantuntijat voivat tehdä itsenäisesti, mutta laajemmat, enemmän resursseja ja johtamista vaativat toimenpiteet yleensä käsitellään organisaatioiden päätöksentekotasolla. Oleellista kuitenkin on, että tietoriskin todennäköisyys ja mahdolliset negatiiviset vaikutukset minimoidaan riskiarvioinnin ja suunnitelmien mukaisesti. NIST:n riskienhallintamallia alhaalta ylöspäin sovellettaessa voidaan havaita myös samankaltaisuuksia liiketoimintatiedon hallintaan ja siihen liittyviin haasteisiin. Liiketoimintatiedon hallinta viittaa prosessiin, jossa tuotetaan tietoa yrityksen toiminnasta ja tilanteesta johdon päätöksenteon tueksi. Prosessi sisältää tietotarpeiden tunnistaminen, tiedon keräämisen ja arvioinnin sekä jalostamisen ja jakamisen sitä tarvitseville tahoille. (Pirttimäki 2007).

Kuten voidaan havaita, myös Franken & Brynälssonin (2014) tilannetietoisuuden käsite sisältää tietojohdamiseen tyypillisesti liittyviä haasteita, joita ovat tiedon tuottaminen, kokoaminen, jalostaminen ja hyödyntäminen (Laihonen et al 2013). Tietojohdaminen voidaan siis nähdä TKT-johtamisen yhtenä paradigmana tai työkaluna sekä operatiivisella että strategisella tasolla. TKT-johtamiseen Franke & Brynälsson (2014) muodostavat omassa tutkimuksessaan kaksiulotteisen TKT - tilannetietoisuuden määritelmän, joka yhdistää tilannetietoisuuden tietojohdamisen aihepiiriin kuuluviin asioihin eli teknologian hyödyntämisen tiedon tuottamiseen ja siirtämiseen tilanteen analysoinnin ja päätöksen tueksi. He näkevät että TKT –tilannetietoisuuden haasteiden koostuvan kahdesta ulottuvuudesta: teknisestä tai teknologisesta osasta ja kognitiivisesta elementistä. Teknisen elementin haasteet liittyvät tiedon keräämiseen, siirtämiseen ja yhdistelemiseen eli tilannekuvan tuottamiseen. Kognitiiviset haasteet liittyvät tiedon tulkitsemiseen ja ymmärtämiseen eli tilanteen hahmottamiseen ja sitä kautta tilannetietoisuuden muodostamiseen. Kuten Franken & Brynälssonin (2014) tilannetietoisuuden käsitteestä voidaan havaita, se sisältää tietojohdamiseen tyypillisesti liittyviä haasteita, joita ovat tiedon tuottaminen, kokoaminen, jalostaminen ja hyödyntäminen (Laihonen et al 2013). Toisaalta edellä mainittuja aktiviteetteja tarvitaan myös TKT – johtamisen kannalta normaalitilanteissa tilannetietoisuuden ylläpitämiseksi ja poikkeustilanteiden havaitsemiseksi. Toiminnoissa on myös pohdittava tiedon olemusta ja sisältöä sekä sen hyödynnettävyyttä tietämyksen ja ymmärryksen lisäämiseksi. Kuten Barford et al. (2010, s. 4) toteavat, tilannetietoisuutta tavoitellaan tiedon eri tasoilla, raakadatasta pitkälle jalostettuun tietoon. Raakadata voi olla esimerkiksi järjestelmäluetteloita, kun taas tilannetiedon perusteella voitisiin tehdä tulkintoja tästä luettelosta.

Huomioitavaa kuitenkin on, että toisaalta, riippuen ratkaistavasta ongelmasta, Laihoson et al. (2014) mukaan tietoturvaluus voidaan nähdä osana tietojohdamista, mikä mahdollistaisi hieman erilaisen lähestymistavan organisaation tietojohdamiseen ja siihen liittyvien toimintojen kehittämiseen. Yksi organisaation resursseista on tietopääoma, joka voi aiheuttaa esimerkiksi taloudellisia tappiota tai mainehaittoja, mikäli tiedot menetetään tai ne päätyvät väärin käsiin. Digitaalisessa muodossa olevaan tietoon kohdistuu tietoriski, joka tulee ottaa huomioon tiedonhallintaa suunniteltaessa ja toteutettaessa. Tiedon tai tietoon perustuvan palvelun turvaamiseen tarvitaan tietoturvaluus, sen johtamista ja siihen liittyviä prosesseja, isommissa organisaatioissa ja laajemmissa poikkeustilanteissa yhteistyötä ja tiedonvaihtoa eri toimijoiden kesken. Tieto- ja kyberturvaluus ja tietojohdaminen ovat siis näkökulmia ja aihealueita joita voidaan hyödyntää lähestymistapoina toistensa haasteiden ratkaisemiseen. TKT-johtamisen malleja voidaan hyödyntää tietojohdamisen kehittämiseen tietoturvaluuden näkökulmasta ja tietojohdamisen erityyppisiä malleja TKT-toiminnan kehittämiseen.

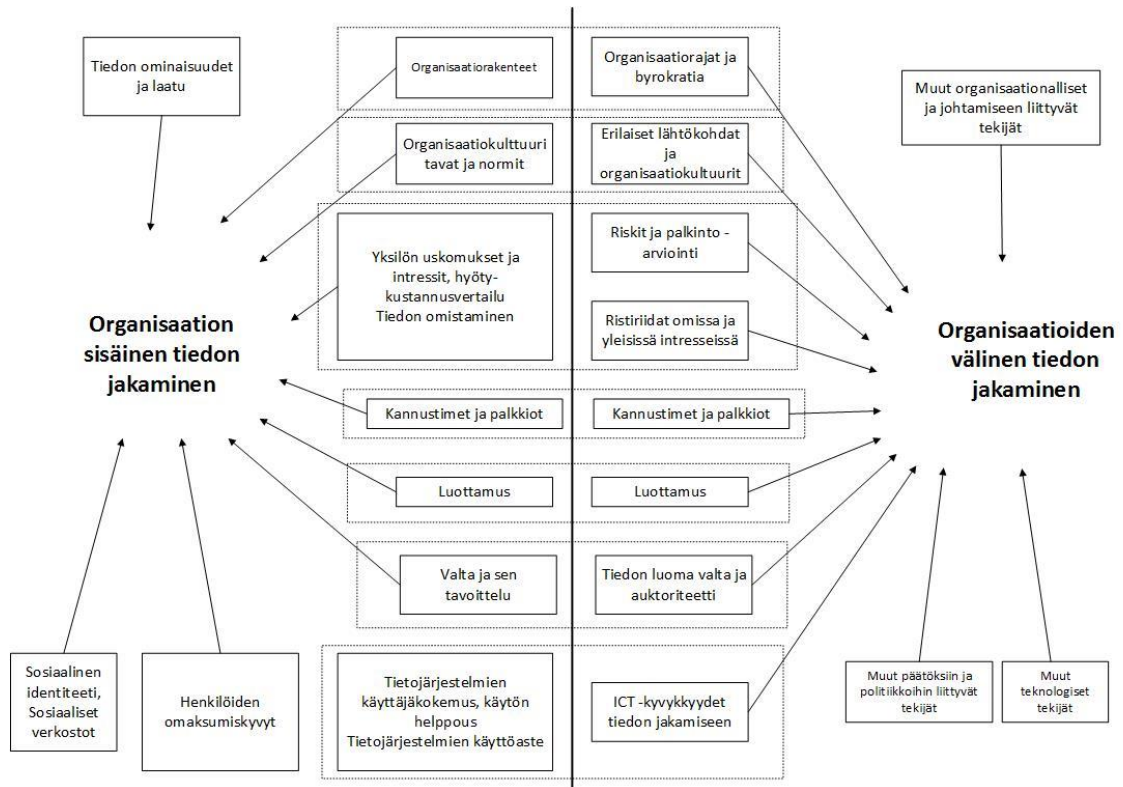
2.6.1 Tiedon jakaminen valtionhallinnon TKT-johtamisessa

Tietojohtamisen, ja erityisesti tiedon jakamisen, tarpeellisuutta valtionhallinnon tieto- ja kyberturvallisuuden johtamisessa korostaa se, että siinä tehdään päätöksiä ja toimenpiteitä ympäristössä, joka on kompleksinen ja siihen liittyy useita toimijoita. Operatiivisella tasolla toiminta-, eli palveluiden tuotantoympäristöinä on Janhusen (2015) mukaan pääosin organisaatorajat ylittävä yhteinen tietojärjestelmien ja tietoverkkojen muodostama kompleksien infrastruktuuri- ja palvelukokonaisuus, ”kyberympäristö” tai ”kyberavaruus”. Kompleksisille systeemeille, kuten kyberympäristöille, on Kuusiston (2014, s. 48) mukaan tunnusomaista, että ne ovat jatkuvan muutoksen alaisia, jolloin kaikkien yksityiskohtien tietäminen on haastavaa tai jopa mahdotonta. Kompleksisten systeemien osat ovat toisistaan riippuvaisia, jolloin pelkästään yhteen kohteeseen rajoittuvat toimenpiteet ovat tehottomia, tarvitaan poikkeustilanteissa yhteistoimintaa, tiedon jakamista ja päätöksentekoa (Hernandez-Ardieta et al. 2013).

Leppäsen et al. (2016, s.17) tekemän selvityksen mukaan valtion hallinnon tason TKT-toiminnassa oleellista on eri organisaatioiden välinen tiedonvaihto, jotta poikkeustilanteissa saadaan kattava kokonaiskuva. TKT –tilannekuvaa tarvitaan valtionhallinnon tapauksessa sekä organisaatioiden sisäisistä että organisaatorajat ylittävistä tietojärjestelmäympäristöistä. Tilanteesta tekee haastavan se, että vaikka päätöksentekoon ja toimintaan vaikuttavia lainsäädännöllisiä organisaatorajoja on olemassa, tietojärjestelmät ja tietoverkot voivat olla jaettuja. Tällöin myös niihin liittyvät riskit eli uhat ja niiden seuraukset voivat koskettaa jaettuun ympäristöön liittyviä organisaatioita). Tästä syystä on tärkeää että, organisaatioilla on yhteinen käsitys tilanteesta, jotta voidaan tehdä päätöksiä riskien ja poikkeustilanteiden käsittelemiseksi (MASSCA, 2014). Tutkimuksen kontekstissa, eli organisaatioiden kesken jaetun ICT-ympäristön tilanteesta tiedon jakaminen voi siis osaltaan määrittää organisaation kyvykkyyden ymmärryksen muodostamiseen tästä ympäristöstä, TKT-näkökulmasta siis tilannetietoisuuden muodostamiseen. Jaetun ymmärryksen tavoittelu luo siis tarpeen tiedon jakamiselle. Tiedon jakamisesta ja sen hyödyntämisestä mahdollisesti saatavat hyödyt ulottuvat siis myös organisaatioiden tieto- ja kyberturvallisuuden johtamiseen. Hyödyt tiedon jakamisesta tulevat esiin etenkin poikkeustilanteissa, joissa eri osapuolten tulisi pyrkiä yhteisen tilannetietoisuuden muodostamiseen, koska usean toimijan tilanteessa tulisi pyrkiä jaettuun tai yhteiseen tilannetietoisuuteen (collective awareness) (Stone, 2016, Pitt et al. 2013). Yksittäisten toimijoiden tulisi ymmärtää miten yksittäiset teot ja päätökset vaikuttavat kokonaisuuteen. Koska tilannetietoisuuden muodostuminen on tulkintaa, johon vaikuttavat myös yksilön arvomaailma, Pitt. et al (2013) esittävät, eri toimijoilla tulisi olla jaettu ”konteksti” eli yhteiset arvot sekä muut tilanteen tulkintaan vaikuttavat tekijät, jotta he päätyisivät yhteiseen tilannetietoisuuteen. Yhteinen tilannetietoisuus on merkittävä osa-alue yhteistoiminnassa, erityisesti yhteistyössä, joka tapahtuu pääosin tietokoneiden ja muiden viestintävälineiden avustuksella.

TKT-johtamisessa ja tilannetietoisuuden muodostamisessa tulee ottaa huomioon myös tiedon jalostamisen prosessit ja menetelmät, koska pelkkä tilannekuvan jakaminen ei riitä, mikäli tietoa ei osata jalostaa tilannetietoisuudeksi eli yhteiseksi ymmärrykseksi tilanteesta. Voidaan tarvita myös yhteistyössä toteutettua kerätyn tiedon analysointia, jotta tiedon merkitys kokonaisuutena ymmärretään ja sen pohjalta voidaan arvioida päätöksentekoa ja siihen liittyviä tekijöitä. Kuusiston (2014, s. 44) ja Barford et al. (2010, s. 4) mukaan tilannetietoisuutta ei voida tavoitella pelkästään tuottamalla dataa, koska pelkästään datan avulla päätöksiä ei voida tehdä tehokkaasti, vaan sitä tulee myös osata tulkita. Pelkkä data ja sen tuottamien eivät näin ollen välttämättä vähennä työkuormitusta, joka päätöksentekoon liittyy. Tiedon jakamisella voidaan osittain ratkaista näitä ongelmia, jotka liittyvät jalostetun tiedon saamiseen, mikäli hyödyntäjä ei kykene itse tuottamaan tarvittavaa jalostettua tietoa. (Leppänen et al. 2016, s. 17, Kuusisto (2014, s. 44) ja Barford et al. (2010, s. 4)

Valtionhallinnon tapauksessa tiedonvaihtoa tarvitaan myös eri organisaatioiden välillä. Yleisesti tiedonvaihto organisaatioiden välillä on kompleksinen kokonaisuus, johon vaikuttaa monia eri tekijöitä henkilöiden välisellä tasolla, organisaatioyksiköiden välisellä tasolla sekä organisaatioiden välisellä tasolla (Yang & Maxwell, 2011). Eri tasoilla havaittavat tekijät vaikuttavat toisiin, sekä samoilla että eri tasoilla oleviin tekijöihin. Henkilöiden väliseen tiedonvaihtoon vaikuttavat tekijät, kuten keskinäinen luottamus, vaikuttavat täten myös organisaatioiden väliseen tiedonvaihtoon. Tekijät voidaan jaotella organisaationallisiin, teknologisiin sekä poliittisiin ja lainsäädännöllisiin tekijöihin. Organisaationalliset tekijät liittyvät organisaatiokulttuureihin, toimintatapoihin ja organisaationallisiin kyvykkyyksiin, teknologiset tiedon siirron työkaluihin ja poliittiset ja lainsäädännölliset tekijät päätöksiin ja linjauksiin tietojen jakamisesta. Alla olevassa kuvassa 9 on Yangin & Maxwellin (2011) tutkimuksessaan löytämiä tekijöitä.



Kuva 9. Organisaatioiden sisäiseen sekä niiden väliseen tiedonvaihtoon vaikuttavat tekijät, mukailen Yang & Maxwell (2011).

Kyseisessä kuvassa ei eritellä tekijöiden välisiä riippuvuussuhteita. Osa tekijöistä voivat vaikuttaa toisiinsa ja siten epäsuorasti tiedon jakamiseen. Esimerkiksi kannustimet ja palkkiot voivat vaikuttaa organisaatiokulttuuriin. Kuvasta voidaan nähdä, että monet tiedon jakamiseen vaikuttavat tekijät ovat organisaatiotasolla ja yksilötasolla samankaltaisia. Esimerkiksi ICT -kyvykkyuden vaikutusta tiedon tuottamiseen, siirtämiseen ja hyödyntämiseen voidaan painottaa sekä yksilö- että organisaatiotasolla.

Myös European Union Agency for Network and Information Security (ENISA, 2010) on toteuttanut Delphi-menetelmällä tutkimuksen, jossa se kartoitti taulukossa 3 tiedon jakamiseen vaikuttavia tekijöitä tieto- ja kyberturvallisuuden kontekstissa. Tekijät jaoteltiin niiden vaikuttavuuden mukaan tärkeisiin, keskimääräisen ja matalan tärkeysasteen tekijöihin.

Taulukko 2. Tiedonvaihtoon kannustavia tekijöitä, ENISA (2010).

Tärkeä	Keskimääräinen	Matala
1. Taloudellisten resurssien säästäminen	3. Osallistujien välinen luottamus	7. Osallistumisaktiivisuudesta saatavat taloudelliset hyödyt

2. Laadukas ja arvokas tieto	4. Etuoikeutetun tiedon saaminen viranomaisilta	8. Osallistumisen mahdollistama näkyvyys ja vaikutusmahdollisuudet
	5. Olemassa olevat prosessit ja toimintamallit tiedon jakamiseen	9. Osallistumisella saatavat mainehyödyt
	6. Osallistujien päätöksenteollisen autonomian säilyminen	10. Osallistumisen mahdollistamien analysointi- ja neuvontapalveluiden käyttö
		11. Yksilötason asenteet ja preferenssit

Tekijöistä osa on vastaavia kuin Yang & Maxwellin (2011) kartoittamat, mutta myös eri tekijöitä on huomioituna. Tähän tutkimukseen osallistuvat asiantuntijat edustivat pääosin yksityistä sektoria, joten eroavaisuudet selittyvät mahdollisesta näkökulmaerosta. Enisan (2010) vastauksissa painotettiin erityisesti tiedon jakamisesta saatavia taloudellisia säästöjä sekä arvokkaan ja laadukkaan tiedon saamista. Taloudelliset säästöt syntyvät kun käytäntöjä ja menetelmiä voidaan jakaa jolloin niitä ei tarvitse kehittää jokaisessa organisaatiossa erikseen. Tiedon vaihtoon osallistuvien välinen luottamus on merkittävä tiedonvaihdon edellytyksenä ja siihen kannustavana psykologisena tekijänä. Kuten ENISA:N tutkimuksessa, jossa se nostettiin kolmanneksi tärkeimmäksi tekijäksi, myös Leppäsen et al. (2016, s.18-19) Suomessa tehdyn selvityksen mukaan luottamus on selkeästi yksi tärkeimpiä edellytyksiä tiedon vaihtoon. Luottamus kannustaa tiedonvaihtoon, koska tällöin henkilö olettaa ja uskoo vastapuolen haluavan auttaa ja omaavan sellaista tietoa joka voisi auttaa häntä (Abrams et al 2003, s. 65). Muita Leppäsen et. al (2016) selvityksessä esiin nousseita edellytyksiä ovat molemminpuolinen hyöty ja vastavuoroisuus sekä sovittujen rajojen noudattaminen, mikä osaltaan liittyy luottamuksen rakentamiseen.

ENISA:n (2010) tutkimuksessa kartoitettiin myös taulukossa 3 olevia haasteita ja esteitä tiedon jakamisessa.

Taulukko 3. Haasteita ja esteitä tiedonvaihdossa, ENISA (2010)

Tärkeä	Keskimääräinen	Matala
1. Puutteellinen tiedon laatu	4. Väärän tyyppiset osallistujat	11. Tiedon jakamisen hallittavuus
2. Mainehaittoihin liittyvät riskit	5. Lainsäädännölliset tekijät	12. Osallistumisen kustannukset
3. Huono hallinnointi	6. Tietovuotojen riski	13. Mahdolliset muut haitat
	7. Ryhmäkoko	14. Kilpailulainsäädäntöön liittyvät tekijät
	8. Viranomaistoimijoiden tiedon salailu	

-
9. Riittämättömät tai väärin kohdistetut investoinnit tietoturvallisuuteen
 10. Kilpailu
-

ENISA:n (2010) tiedon jakamiseen ja haasteisiin liittyvät tekijät painottuivat vastauksissa erityisesti tiedon laatuun, organisaation puutteellisen tai virheellisen toiminnan paljastumisesta johtuviin mainehaittariskeihin, sekä tiedonjakoon liittyvien työkalujen ja ympäristön huonoon hallintaan. Vastaajat eivät nähneet kilpailullisten tekijöiden vaikuttavan tiedon jakamiseen, pääosin koska tieto- ja kyberturvallisuuteen liittyvät tekijät ovat harvoin osa organisaation ydinosaa ja eivät siten ole merkittäviä kilpailu-etua tuottavia tekijöitä. Monissa tapauksissa tilanne onkin päinvastainen, tiedon jakaminen voikin olla edellytys turvallisuuden kehittymiseksi ja sen varmistamiseksi. Positiivisesti tiedonvaihtoon suhtautuvat organisaatiokulttuuri ja tiedonvaihtokulttuuri voivat vähentää kynnystä tiedonvaihtoon organisaatioiden välillä, kuten Yang & Maxwell (2011) esittävät tutkimuksessaan. Tietoa jakamalla organisaatiot voisivat tehostaa resurssien käyttöä vähentämällä samojen turvallisuusjärjestelmien kehittämistä eri organisaatioissa. Toisaalta tiedon jakaminen voisi johtaa esimerkiksi parempien turvallisuuskäytäntöjen kehittymiseen ja leviämiseen organisaatioiden välillä, jos kehitystä tehdään yhteistyössä.

Kuten todettua, tietojärjestelmäympäristöjen jatkuva muutos aiheuttaa haasteita tilanteen ymmärtämiseen ja tilannetietoisuuden muodostamiseen. Vastaavat haasteet liittyvät myös yleisemmin TKT-johtamiseen kuten Fenzin et al. (2014) tunnistivat tutkimuksessaan. He tukevat näkemystä, jonka mukaan tieto- ja kyberturvallisuuden johtamisessa suuren haasteen on organisaation tietojärjestelmäkokonaisuuden inventaarion hallinta. Heidän mukaansa organisaatioilla on haasteita kerätä ja ylläpitää kattavaa tietoa ohjelmistoista ja laitteista, eli IT-ympäristöstä, joka organisaation hallinnassa on. Tällöin kyseessä on pääosin tiedon keräämisen ja tuottamisen haasteet, jota lisäävät IT-ympäristön dynaamisuus. Puutteelliset tiedot vaikeuttavat häiriöiden vaikutusten arviointia ja voivat siten vääristää riskien arviointia ja toimenpiteiden suunnittelua.

Meissner et al. (2002) mukaan merkittäviä tiedonhallinnallisia puutteita ja haasteita, jotka poikkeustilanteessa toimintaa tukevissa tietojärjestelmissä tulisi ratkaista, ovat informaatiolähteiden integrointi ja linkitys toisiinsa, kommunikaatiovälineiden saatavuus, nopea yhteys dataan, informaation ajantasaisuus ja standardimuotoinen informaatio. Informaatiolähteiden integroinnilla pyritään eri tietojen yhdistämiseen tilannetietoisuuden muodostamiseksi tilanteen muodostamasta kokonaisuudesta, joihin yleensä liittyy useita ympäristöjä. Kommunikaatiovälineiden saatavuus mm. redundanttisten järjestelmien avulla, mahdollistaa yhteistyön ja tiedon jakamisen eri toimijoiden välillä vakavissakin häiriötilanteissa. Aikakriittisissä tilanteissa nopeasti saatavissa oleva ja ajantasainen informaatio

ovat edellytyksiä onnistuneelle ja tehokkaalle päätöksenteolle. Standardimuotoisella informaatiolla pyritään helpompaan integrointiin ja siten laajempaan tiedon hyödynnettävyyteen.

Tiedon välittämisen mahdollistaminen voi siis kontekstista riippuen olla sekä johtamisen haaste että tietotekninen haaste. Eli haasteet voivat liittyä joko riskienhallinnan prosesseihin, johtamiskäytäntöihin tai toimintatapoihin ja näihin liittyvään tiedonkulkuun, tai haasteet voivat liittyä teknisiin haasteisiin riskienhallinnan käytännön toteuttamisessa sekä siihen liittyvässä tiedon tuottamisessa ja siirtämisessä. Edellä esitetyt tieto- ja kyberturvallisuuden johtaminen ja siihen liittyvä päätöksenteko, yhteisen tilannetietoisuuden muodostaminen sekä tilannekuvan hankkiminen ja jakaminen voidaan siis nähdä tietojohdamisen haasteina, jolloin tieto- ja kyberturvallisuuden johtaminen asettaa tietotarpeita sekä tiedon jakamisen ja siirtämisen tarpeita. Tässä tapauksessa sitä tarkastellaan tiedon siirtämisen ja jakamisen haasteena. Tiedon jakamiseen voi liittyä sekä sisäisiä että ulkoisia sidosryhmiä, kun kyseessä on montaa organisaatiota koskettava tilanne ja monia aktiivisia toimijoita sisältävä tilanne. (MACCSA, 2013, Laihonon et al, 2013, s. 21-22).

3. PIKAVIESTINTÄ

Tietokoneavusteinen viestintä on yleistynyt tapa kommunikoida ja välittää tietoa. Sähköisillä viestintävälineillä, kuten sähköpostilla, voi olla alempi ”käyttökynnys” kuin esimerkiksi puhelimella, koska sähköiset viestintävälineet ovat kasvokkain tapahtuvaa kommunikointia ajallisesti joustavampia niiden mahdollistaman virtuaalisen toiminnan ansiosta. Viestintäkanavalla, tutkimuksen kontekstissa tietokoneavusteisuudella, on kuitenkin vaikutuksia viestinnän kontekstiin, kuten viestin tulkintaan vaikuttaviin tekijöihin. Wainfanin & Davisin (2004) huomioiden mukaan esimerkiksi ihmisten hierarkkiset suhteet tulevat enemmän esille ja vaikuttavat viestiin reagointiin kasvokkain tapahtuvassa kommunikoinnissa sähköistä viestintää enemmän, koska tietokoneavusteisesta kommunikaatiosta puuttuvat nonverbaaliset viestinnän elementit kuten eleet ja ilmeet, jotka vaikuttavat viestin tulkintaan ja siten mahdollisesti toimintaan. (Wainfan & Davis, 2004).

Tiedonvaihdoisesta ja tiedonvaihtoon vaikuttavan kontekstin näkökulmasta on siten merkitystä, miten viestintä tapahtuu. Välineet tulisi mahdollistaa ja tukea tiedonvaihtoa siirrettävän tiedon ominaispiirteet huomioon ottaen. Data on lähtökohtaisesti helposti siirrettävissä tietojärjestelmien ja siten ihmisten välillä, mutta tietämyksen tai osaamisen eli ns. hiljaisen tiedon siirtämien on haastavampaa, koska se on kontekstiin ja yksilöihin sitoutunutta (Choo 1998). Tutkimuksen kontekstissa siirrettävää osaamista voi olla esimerkiksi tilannekuvan analysointiin ja sen tulkintaan liittyvä osaaminen. Osaaminen on tärkeää, jotta tilannekuvan sisältämästä tiedosta osataan tulkita ja tunnistaa esimerkiksi eri tapahtumat ja niiden väliset suhteet. Pelkän jalostamattoman datan siirrossakin voidaan tarvita tietämyksen siirtoa, jotta data osataan tulkita ja hyödyntää oikein (Roberts, 2000). Yleisen näkemyksen mukaan hiljaisen tiedon tai kontekstiin tai henkilöihin sitoutuneen tietämyksen ja osaamisen siirrossa tarvitaan toimijoiden välistä vuorovaikutusta ja kommunikointia, joissakin tapauksissa jopa läsnäoloa eli sosiaalista vuorovaikutusta (Choo, 1998, Nonaka & Takeuchi, 1995). Sosiaalisen vuorovaikutuksen mahdollistavia viestintävälineitä voidaan täten pitää merkittävänä tekijänä jalostetumman tiedon tai osaamisen sähköisessä siirtämisessä eri toimijoiden välillä. Yksi tätä tukeva mahdollinen teknologinen ratkaisu voisi olla organisaatioissa yleistyneet pikaviestinjärjestelmät, kuten seuraavassa luvussa esitellään.

3.1 Pikaviestinnän ominaispiirteet

Pikaviestin on tietokoneavusteinen kommunikointimenetelmä eli järjestelmä, joka mahdollistaa tietokoneen tai muun päätelaitteen ohjelman avulla reaaliaikaisen kommuni-

koinnin kahden tai useamman osapuolen välillä. Reaaliaikaisuus on pikaviestimien leimallisina ominaisuuksina, jotka vaikuttavat mm. sen käyttötapoihin ja –tilanteisiin. Reaaliaikaisuus vaikuttaa jo lähtökohtaisesti käyttäjien odotuksiin ja olettamuksiin järjestelmästä: pikaviestintään kohdistuu sähköpostiin verrattuna erilainen vaatimus viestinnän vastaajasta. Sähköpostiin ei odoteta välitöntä vastausta kuten pikaviestiin. Sähköposti on siten pääosin asynkronista pikaviestinnän ollessa synkronista eli pääosin keskustelun kaltaista vuorovaikutteista kommunikointia (Handel & Hersleb, 2002).

Reaaliaikaisuuden lisäksi Renneckerin & Godwinin (2003, s. 141 - 142) mukaan yksittäisen käyttäjän näkökulmasta pikaviestintäjärjestelmillä on viisi lisäarvoa tuottavaa ominaisuutta:

Pikaviestinjärjestelmä mahdollistaa tavoitettavuustietojen välittämisen, jolloin käyttäjät voivat olla tietoisia muiden käyttäjien saavutettavuudesta (Presence awareness). Läsnaolotiedon välittämällä käyttäjä voi tietää, voiko vastaanottaja vastaanottaa viestejä ja siten arvioida vastaukseen kuluva aika. Usein käyttäjällä on mahdollisuus oman tavoitettavuutensa hallitsemiseen tavoitettavuusilmoituksilla ja sallimalla viestit vain tietyiltä käyttäjiltä tai käyttäjäryhmiltä (Myös Cameron & Webster, 2004).

Vastaanottajan hälyttäminen saapuvasta viestistä, (“Pop-up” Recipient Notification). Pikaviestintä muistuttaa tällä ominaisuudellaan puhelinta, jolla on mahdollisuus tuoda ilmoitus saapuvasta viestistä tai yhteyspyynnöstä vastaanottajan tietoisuuteen. Joissakin järjestelmissä myös viestin sisältö tai osia siitä näytetään suoraan käyttäjän ruudulla. Pikaviestintä on puhelimen tavoin ”tunkeutuva” (intrusive) eli se lähtökohtaisesti vaatii vastaanottajan reagointia.

Mahdollisuus useaan yhtäaikaiseen keskusteluun samalla viestintävälineellä (Within-medium Polychronic Communication.) Pikaviestinjärjestelmät tyypillisesti tarjoavat mahdollisuuden kommunikoida usean henkilön kanssa samalla päätelaitteella ja –ohjelmalla, toisin kuin perinteisesti puhelimet. Vastaavasti pikaviestinjärjestelmät mahdollistavat henkilön kutsumisen keskusteluun nopeammin kuin kasvokkain tapahtuvissa keskusteluissa.

Mahdollisuus viestintään ilman puhetta (Silent Interactivity). Pikaviestinjärjestelmä mahdollistaa viestinnän häiritsemättä muita, jolloin viestintä pikaviestinjärjestelmällä ei ole riippuvainen työympäristöstä, kuten mahdollisesti puhelimen avointen toimistoympäristöjen tapauksessa.

Järjestelmästä riippuen, keskustelujen tallennus tai poisto keskustelujen jälkeen (Ephemeral Transcripts). Pikaviestinjärjestelmät voivat tilanteesta ja käyttötarkoituksesta riippuen tarjota mahdollisuuden keskusteluiden käymiseen siten, että keskusteluja ei tallenneta.

Tilanteesta, tehtävästä ja työympäristöstä riippuen jotkin ominaisuudet voivat olla hyödyllisempiä kuin toiset. Pikaviestimet voivat esimerkiksi mahdollistaa viestinnän tilanteissa, joissa puhuminen ei ole toivottavaa, kuten hiljaisissa työtiloissa tai avokontto-reissa. Ryhmäkeskusteluominaisuus voi mahdollistaa virtuaalisen työskentelyn, jossa tarvitaan yhteistyötä mutta osallistujat sijaitsevat maantieteellisesti erillään.

Samoja ominaisuuksia ja ominaispiirteitä on myös muissa viestintävälineissä, kuten alla olevassa taulukossa 4 on esitettyä, joskin pikaviestinnällä muodostuu erilaisesta yhdistelmästä kuin muut viestintävälineet

Taulukko 4. Pikaviestinjärjestelmän ominaispiirteet muihin kommunikaatiomenetelmiin verrattuna, mukailten Rennecker & Godwin, 2003, s.143).

		Teknologian ominaisuudet ja ominaispiirteet					
Teknologia		Teksti-pohjainen	Synkroninen / Interaktiivinen	Tavoitet-tavuuden ilmai-seminen	Tunkeutuva	Yhtäaikai-nen vies-tintä mo-nen henki-lön kanssa	Keskustelujen tallennus
	Pikaviestintä	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä	Ei / Kyllä
	Sähköposti	Kyllä	Ei	Ei	Ei	Ei	Kyllä
	Faksi	Kyllä	Ei	Ei	Ei	Ei	Kyllä
	Puhelin	Ei	Kyllä	Ei	Kyllä	Kyllä	Yleisesti ei
	Kasvokkain keskustelu	Ei	Kyllä	Kyllä	Kyllä	Kyllä	Ei

Kuten taulukosta voidaan havaita, pikaviestinnällä on eniten yhtäläisyyksiä kasvokkain tai puhelimitse tapahtuvaan viestintään. Kyseessä on siis viestintäväline, jolla pyritään jäljittelemään kasvokkain tapahtuvaa keskustelua, mutta pohjautuen kuitenkin kirjoitettuun viestintään. Pikaviestinnän suosio perustuu siten osittain sen mahdollistamaan viestintämuotoon, jolla epämuodollisen, eli puhelimitse tai kasvokkain tapahtuvan viestinnän ja kommunikoinnin ominaispiirteitä. Pikaviestintä onkin käytössä osittain korvannut muut, edellä mainitut viestintävälineet (Raven et al. 2002)

3.2 Pikaviestinnän käyttö

Havaintojen mukaan pikaviestintäjärjestelmien avulla käydyt keskustelut ovat usein lyhyitä ja niillä on vain yksi tarkoitus ja päämäärää, tosin pikaviestinnällä on myös muita mahdollisia käyttötapoja. Keskustelut ovat usein nopeita kysymyksiä ja vastauksia ja keskustelun aikana voidaan käyttää myös muita tiedonvaihdonvälineitä. Ryhmäkeskusteluna tapahtuvalle pikaviestinkommunikoinnille on havaittu olevan tunnusomaista keskustelujen alkaminen jonkin tapahtuman seurauksena ja sen jälkeinen intensiivinen kommunikointi, jonka jälkeen keskustelu päättyy usein nopeasti. Pikaviestintään motivoivana tekijänä on siis usein jokin tapahtuma, joka halutaan käsitellä välittömästi ja nopeasti. Tällaisia välitöntä käsittelyä edellyttäviä tapahtumia voivat olla myös tieto- ja kyberturvallisuuden liittyvät tapahtumat ja operatiivinen reagointi niihin.

Muita viestintätehtäviä, joihin pikaviestintää usein käytetään, ovat työtehtävien koordinointi ja aikataulutus, valmistelemattomien, impromptu tapaamisten koordinointi. Vapaaajalla käyttötapoja on esimerkiksi yhteyksien pitäminen ystäviin ja sukulaisiin. Pikaviestinnälle on ominaista että, sen aikana käyttäjät tekevät myös usein useita tehtäviä samanaikaisesti eli pikaviestinnän avulla tapahtuvat yhteydenotot eivät keskeytä muita työtehtäviä. Pikaviestinjärjestelmillä käyttäjät voivat myös osittain hallita muiden henkilöiden aiheuttamia häiriöitä, koska se mahdollistaa tavoitettavuudesta ilmoittamisen. Käyttäjö voi siis ilmaista olevansa tilanteestaan riippuen joko tavoitettavissa tai ei-tavoitettavissa ja ohjata muiden henkilöiden yhteydenotot sopivampaan ajankohtaan. (Handel & Herb-
sleb, 2002, Isaacs et al. 2002, Nardi et al. 2000, Cameron & Webster, 2004)

Ou et al. (2010) tutkimuksen mukaan pikaviestinnällä voidaan tehostaa tiimien työskentelyä ja tuloksia, koska se tarjoaa välineen sosiaalisen verkostoitumiseen, jolla on positiivinen vaikutus tiedonjakoa tukevan ilmapiirin syntymiseen. Sosiaaliset verkostot ovat heidän mukaansa merkittävä tekijä tiedonvaihdon ja yhteistyön kannalta, sillä positiiviset suhteet vähentävät kynnystä tiedonvaihdolle ja tiimityöskentelylle. Li et al. (2005) näkevät ainakin kaupallisten pikaviestimien olevankin pääosin sosiaaliseen verkostoitumiseen käytettävä väline, jota hyödynnetään ”yhteydessä pysymiseen”, eli tavoitettavuuden ylläpitämiseen.

Seuraavassa taulukossa 5 on koottuna eri kirjallisuuslähteiden tekemiä havaintoja pikaviestinnän ominaisuuksista ja sen käyttötavoista. Hieman tutkimusnäkökulmasta riippuen eri tutkimukset painottavat eri ominaisuuksia ja käyttötapoja.

Taulukko 5. Pikaviestinjärjestelmien ja pikaviestinnän ominaispiirteitä.

	<i>Handel & Hersleb (2002)</i>	<i>Nardi et al.(2000)</i>	<i>Garrett & Danzinger (2007)</i>	<i>Ou et al. (2010)</i>	<i>Ou & Davison (2010)</i>
<i>Läsnäolo- ja tavoitettavuustietojen välittäminen</i>	x	x	x		
<i>Reaaliaikainen, synkronoitu viestintä</i>		x	x	x	
<i>Epämuodollinen viestintä</i>		x		x	
<i>Työnteon- ja viestinnän koordinoituväline</i>	x	x			
<i>Tapahtuman käynnistämä intensiivinen viestintä</i>	x				
<i>Sosiaalisenverkostoitumisen väline</i>				x	x

Useimmissa tutkimuksissa havainnot ovat kiinnittyneet pikaviestinjärjestelmien mahdollistaman läsnäolotietojen lähettämiseen ja vastaanottamiseen. Lisäksi havaittiin että pikaviestintää käytettiin usein myös viestinnän koordinointiin, kuten aikataulujen sopimiseen. Toisaalta esimerkiksi Handel & Herbsleb (2002) havaitsivat että pikaviestintää käytettiin myös varsinaisten ongelmien ratkaisuun. Eli tutkimusten mukaan pikaviestintään käytetään useimmiten suhteellisen yksinkertaisiin tilanteisiin, mutta sitä voidaan käyttää myös kompleksisten ongelmien ratkaisussa ja ratkaisuprosessin tukena yhteistyö- ja koordinoituvälineenä.

Pikaviestinnän mahdollistamalla interaktiivisuudella voi olla käyttäjien näkökulmasta myös huonoja puolia: Pikaviestintäjärjestelmille ominainen käyttäjän jatkuva tavoitettavuus ja sen aiheuttamat keskeytykset voivat tuoda mukanaan mahdollisesti negatiivisia vaikutuksista työntekoon (Ou & Davison, 2011). Pikaviestintämahdollisuus voi johtaa työntekijän tehtäväkuorman lisääntymiseen ja lisätä yhden tekijän muiden ”häiriölähteiden”, kuten sähköpostin ja puhelimen, rinnalle ja haitata työntekoa tuomalla jatkuvia keskeytyksiä työntekoon.

Häiriövaikutukset eivät kuitenkaan ole yksiselitteisiä ja vastakkaisia tutkimustuloksia ovat julkaisseet ainakin Garrett ja Danzider (2007) sekä Nardi et al. (2000). Edellä mainittujen mukaan pikaviestinjärjestelmä voitaisiin ajatella tuovan lisäkuormaa työntekijöille ja olevan yksi työnteon keskeytyksiä lisäävä tekijä, mutta he havaitsivat että pikaviestintä sekä kannustaa tiheämpään kommunikointiin että vähentää työntekijöiden kokemaa työnteon keskeytyksiä. Pikaviestinjärjestelmä mahdollistaa yhteydenottojen aiheuttaman keskeytysten minimoinnin mahdollistamalla keskustelusta neuvottelun ja siirtämisen parempaan ajankohtaan. Lisäksi pikaviestintäjärjestelmän läsnäolotiedon välittämisellä käyttäjät voivat paremmin hallita yhteydenotoista aiheutuvia keskeytyksiä työssään viestimällä tavoitettavuudestaan ja siten vähentää turhia yhteydenottoja muilta käyttäjiltä. Nardi et al. (2000) havaitsivat tutkimuksessaan tapauksia joissa pikaviestintä oli jopa suositumpaa kuin kasvokkain tapahtuvan kommunikointi, koska pikaviestintä koettiin vähemmän häiritseväksi ja se mahdollisti usean tehtävän tekemisen yhtäaikaaisesti tietokoneella työskennellessä. Myös Ou & Davison (2011) väittävät tutkimustulostensa perusteella että, pikaviestinnän työntekijöille aiheuttamat häiriöt ovat pieniä suhteessa paremman viestinnän ja tiedonvaihdon paranemisen tuottamiin hyötyihin. Toisaalta Mansi & Levy (2013) havaitsivat omassa tutkimuksessaan että pikaviestinnällä on yleensä negatiivisia vaikutuksia tehtävien suorittamiseen käytettyyn aikaan ja siten työnteon tehokkuuteen.

Pikaviestinnän käytölle luonteenomaisella epämuodollisuudella voi myös joissakin tapauksissa olla negatiivinen vaikutus: mikäli viestintä ei esimerkiksi noudata formaaleja prosesseja viestillä ei välttämättä ole sitovuutta (Cameron & Webster 2005). Muiden edellä mainittujen riskitekijöiden ohella pikaviestinjärjestelmä voi muodostaa organisaatiolle myös tietoturvallisuutta uhkaavan riskitekijän. Pikaviestinjärjestelmää voidaan mahdollisesti käyttää teknisenä välineenä tai alustana organisaation tietojärjestelmiin tunkeutumiseen tai sen avulla voidaan mahdollisesti levittää esimerkiksi viruksia tai muita haittaohjelmia. Toisaalta pikaviestinjärjestelmä voi lisätä esimerkiksi tietovuodon riskiä, sillä sen mahdollistama epämuodollinen viestintä ja sosiaalinen verkostoituminen voi saada työntekijän helpommin luovuttamaan tietoja ulkopuolisille tai oikeudettomille henkilöille. (Leavitt, 2005) Toisaalta pikaviestinjärjestelmä voi mahdollistaa myös oikeudettoman pääsyn keskusteluihin, mikäli pääsynvalvontaa ei suoriteta riittävän hyvin.

3.3 Pikaviestinnän analysointi ja tiedonlouhinta

Pikaviestinnän analysointi ja tiedonlouhinta on toimintaa, jossa keskustelujen ja niissä lähetettyjen viestien muodostamasta tietomassasta pyritään löytämään hyödyllistä informaatiota. Viestinnän sisällön tapauksessa tietomassa on sanat, erityisesti niiden semanttiset merkitykset ja linkitykset muihin sanoihin. Suomenkielisten sanojen tapauksessa kiinnostavaa ovat myös sanojen taivutukset ja niiden analysointi, koska taivutuksilla erotetaan eri sijamuodot toisistaan joten eri taivutusmuodot muuttavat sanojen ja lauseiden merkityksiä (Huovelin et al, 2013, s.144).

Klusterointi, eli luokittelu ja ryhmittely, on yksi yleinen lähestymistapa viestinnän analysointiin. Yksittäisten luokiteltujen sanojen avulla voidaan klusterointia tehdä viesteille ja siten myös keskusteluille. Tietokoneella tehtävä klusterointi viestien tapauksessa perustuu usein matemaattisiin algoritmeihin, joka edellyttää viestien sisällön esittämistä numeerisesti. Sanojen esittämiseen numeerisesti käytetään yleisesti vektoreita tai matriiseja, joilla kuvataan sanan ominaisuuksia, kuten sen liittymistä johonkin laajempaan termiin. Lähtökohtaisesti luokittelun mahdollistamiseksi tarvitaan jokin ominaisuus, joka erottaa kaksi kohdetta toisistaan. Luokittelua ei siis tehdä sanoille sellaisenaan, vaan niiden numeerisille vastineille. (Salton et al. 1975, Yang & Chute, 1992,)

Myös viestejä, tai jopa kokonaisia dokumentteja, voidaan kuvata vektoreilla. Tässä tapauksessa sanoista muodostetaan viestin ”ominaisuusvektori”, eli viestin ominaisuuksien matemaattinen esitys, jonka perusteella viesti luokitellaan ennalta määriteltyyn kategoriaan. Viesti ei joko kuulu yhteenkään kategoriaan, kuuluu yhteen kategoriaan tai kuuluu useaan eri kategoriaan. Yksikertaisimmillaan vektori voidaan muodostaa binäärisesti, eli esiintyykö jokin sana viestissä vai ei (Adams & Martell, 2008, s. 581-582, lähteestä Salton et al. 1975). Monimutkaisemmissa tarkasteluissa voidaan sanoille antaa esimerkiksi painoarvoja, jolloin painoarvoltaan suurempia sanoja sisältävät viestit luokitellaan todennäköisemmin tiettyihin kategorioihin. Viesteistä voidaan tarkastella myös sanojen välisiä relaatioita, lauserakenteita tai muita kieliopillisia tekijöitä, mutta esimerkiksi Puuska et al. (2016) lähestyvät tutkimuksessaan viestejä vain kokoelmana sanoja, eli ns. ”Bag-of-Words” lähestymistavalla.

Yksi analysointitavoite on keskustelujen aihe-alueen selvittäminen keskustelun sisältämän viestinnän sisällön perusteella, kuten esimerkiksi Puuskan et al. (2016) tutkimuksessa (Topic extraction, Topic identification). Tällöin pyritään selvittämään se aihekokonaisuus jota keskustelussa käsitellään. Aihe-alueen selvittäminen perustuu usein luokitteluun, mutta selvitystä voidaan tehdä myös esimerkiksi avainsanojen avulla tai viesteissä esiintyvillä muilla viittauksilla, kuten Internet –osoitteilla, kuten Dong et al. (2006) ovat tutkimuksessaan tehneet.

Useampien yhtäaikaisten keskustelujen seuraamista ja valvontaa voidaan myös helpottaa ”keskustelu ympäristön” eli pikaviestinjärjestelmässä käytyjen keskustelutapahtumien analysoinnilla. Tällöin pyritään löytämään paitsi kiinnostavaa tietoa sisältäviä viestejä, myös löytämään keskustelut joissa nämä viestit ovat esiintyneet. Eli tässä tapauksessa analysoinnilla pyritään löytämään kiinnostava keskustelu useiden keskustelujen joukosta. Analysoinnilla voidaan myös pyrkiä löytämään kiinnostavan tiedon koko konteksti eli kaikki siihen liittyvät viestit, mikäli nämä viestit ovat hajaantuneet eri keskusteluihin (Thread extraction). Eli pyritään rakentamaan tiedolle konteksti poimimalla viestejä useiden keskustelujen joukosta. (Adams & Martell, 2008)

Yksi mahdollisuus pikaviestinnän analysoinnissa on myös keskustelijoiden käyttäytymisen analysointi, ja mahdollisesti profilointi, käyttäjien aktiivisuuden ja lähetettyjen viestien perusteella. Tiedonlouhinnan kohde voi tässä tapauksessa olla myös viestien ja käyttäjien tuottamien metatietojen analysointi, kuten esimerkiksi viestien lähettämisaikankohdat ja viestien vastaanottajat. Pikaviestinnästä, kuten muustakin viestinnästä voidaan etsiä kirjoittajalle ominaisia tunnuspiirteitä ja siten pyrkiä selvittämään käyttäjän identiteettiä mikäli viestintä on anonyymiä. Tällaisia tunnuspiirteitä ovat esimerkiksi pienten ja isojen kirjaimien käyttö ja sanojen määrä lauseissa. (Orebaugh & Allnutt, 2009, Bengel et al. 2004)

Turvallisuusnäkökulmasta pikaviestinnän analysointia voidaan hyödyntää tapahtumien kulun selvittämiseen ja todisteiden hankintaa eli forensiikkaan. Keräämällä päätelaitteesta tai tallentamalla järjestelmässä lähetetyt viestit ja niiden lähetyksajankohdat, voidaan muodostaa käsitys tapahtumien järjestyksestä ja mahdollisesti eri henkilöiden rooleista siinä. (Husain & Sridhar, 2010,)

4. TUTKIMUKSEN KOHDE

Tutkimuksen kohteena olevien pikaviestinjärjestelmän ja analysointitoiminnan tavoitteena on parantaa poikkihallinnollisten, eli useita eri hallinnonaloja koskettavien, tietoturvariskien havaitsemista ja käsittelyä yhteistyössä eri valtionhallinnon organisaatioiden kesken. Strategisella tasolla pikaviestinjärjestelmän tavoitteena on parantaa valtionhallinnon tietoturvariskien hallintaa ja siten kokonaisriskienhallintaa ja varautumista. Tarkasteltava kokonaisuus koostuu kahdesta pääosasta, pikaviestinjärjestelmästä ja siihen liittyvästä analysointitoiminnasta.

4.1 Pikaviestinjärjestelmän toiminta

Pikaviestimen toiminnallinen päämäärä on tarjota kommunikointiväline käyttäjien, eli valtionhallinnon tietoturva-asiantuntijoiden, väliseen TKT –toimintaan liittyvään viestintään. Teknisenä järjestelmänä pikaviestinjärjestelmä ei ole tietojärjestelmien väliseen, eli M2M- viestintään (Machine-to-Machine), suunniteltu väline, mutta sillä voidaan käyttäjien avulla välillisesti siirtää tietoa kahden eri järjestelmien välillä.

Tarkasteltava pikaviestinjärjestelmä on pääominaisuuksiltaan tyypillinen, joskaan se ei mahdollista suunnitelmien perusteella muun kuin tekstimuotoisen tiedon lähettämisen. Pikaviestimessä on keskustelukanavia, joissa keskustelut käydään. Kanavia voidaan muodostaa sekä yleiseen keskusteluun että tilanne- tai käyttäjäryhmäkohtaisesti. Lisäksi järjestelmä mahdollistaa ”läsnäolotiedon” välittämisen, jolloin käyttäjät voivat nähdä ketkä muut henkilöt ovat järjestelmän avulla kyseisellä kanavalla tavoitettavissa. Järjestelmällä pyritään lisäämään yhteistyö- ja viestintämahdollisuuksia eri organisaatioiden asiantuntijoiden kesken, jolloin voidaan paremmin toipua myös laajemmista häiriötilanteista.

Pikaviestinjärjestelmän ja analysointitoiminnan muodostaman kokonaisuuden tuottamat tietovirrat ja toiminta prosessinäkökulmasta ovat esiteltynä liitteessä 1 olevassa kuvassa. Tietovirtoja muodostuu sekä käyttäjien välillä että käyttäjien ja analysointitoiminnan välillä. Tietovirtojen näkökulmasta pikaviestinjärjestelmä ja analysointitoiminta sisältävät sekä ihmiseltä ihmiselle, tietojärjestelmien välisiä, että tietojärjestelmästä ihmiselle tapahtuvia tietovirtoja. Tieto on pikaviestinjärjestelmässä eksplisiittistä eli kirjoitetussa muodossa tai kuvallisessa muodossa olevaa tietoa. Viestintä sisältää täten tietoalkioita – tai tuotteita, jotka muodostuvat käyttäjien tuottamina. Tietosisältö on alustavasti pääosin tieto- ja kyberturvallisuuteen liittyvää, joskin vasta muodostumassa olevat käytännöt ja toimintatavat voivat vaikuttaa tietosisältöihin ja tietovirtoihin.

Loogisella tasolla järjestelmä on verrattain yksinkertainen: se muodostuu käyttäjien pääteohjelmistoista, pikaviestinpalvelimesta sekä sen yhteydessä toimivista analysointityökaluista. Järjestelmä toteutetaan siten, että se toimii muista viestintä- ja tietojärjestelmistä erillisenä, jolloin järjestelmä tarjoaa mahdollisuuden viestintään myös tilanteissa, joissa pääasialliset käytössä olevat viestintävälineet, kuten sähköposti eivät ole käytettävissä.

4.2 Analysointitoiminta

Pikaviestinnän, eli viestisisältöjen ja viestien metatietojen, analysointityökalujen on suunniteltu tukevan valtionhallinnon TKT- toimintaa osana poikkihallinnollista analysointipalveluita. Nämä analysointipalvelut on valtionhallinnon TKT- asiantuntijoiden muodostama verkosto, josta eri organisaatiot saavat tukea sekä normaaliin toimintaan että poikkeustilanteissa toimimiseen (Janhunen, 2015). Pikaviestinnän analysointi perustuu olettamukseen, että viestinnän sisällössä, eli sanoissa, on hyödynnettävää ja lisäarvoa tuottavaa informaatiota eli tieto- ja kyberturvallisuuden johtamisessa ja tilannekuvan tuottamiseen käytettävissä olevaa tietoa.

Analysointipalvelut ovat eri organisaatioissa toimivien asiantuntijoiden muodostama kokonaisuus, jotka tutkivat ja analysoivat havaittuja tieto- ja kyberturvallisuuden poikkeamia. Tämän analysointitoiminnan yksi tärkeimmistä päämääristä on poikkeamaan liittyvän kokonaisuuden hahmottaminen. Analysointipalvelut yhdistävät pikaviestinnän analysoinnin tuottaman tiedon muuhun valtionhallinnon tieto- ja kyberturvatoimijoiden sekä järjestelmien tuottamaan tietoon, ja tuottavat siten laajempaa TKT-tilannekuvaa johtamisen tueksi. Pikaviestinjärjestelmä tai pikaviestinnän analysointitoiminta ei täten suoraan tuota tietoa päätöksentekijöille, vaan vahvistaa analysointipalveluiden toimintaa ja sen mahdollisuuksia tuottaa tietoa päätöksenteon tueksi. Pikaviestinnän analysointitoiminta muodostaa täten osan analysointipalveluiden käytettävissä olevista tiedonkeruumenetelmistä.

Tutkimuksen kohteena olevan pikaviestinnän analysointia ovat tutkineet ja kehittäneet Puuska et al. (2016) Analysointityökalu tunnistaa viesteissä esiintyvät sanat ja luokittelee viestin aiheen ennalta määriteltuihin uhka-kategorioihin. Kategoriat perustuvat MACCSA:n (Multinational Alliance for Collaborative Cyber Situational Awareness) luokitteluun, jolloin tällä hetkellä määriteltäviä uhkakategorioita ovat:

Taulukko 6. Puuskan et al. (2016) analysointityökalun käyttämät uhkakategoriat

Kategoria	Kuvaus
Oikeudeton pääsy; tunkeutuminen	Oikeudeton fyysinen tai sähköinen pääsy tietojärjestelmään tai –verkkoon
Palvelunesto	Toiminta, tarkoituksellinen tai tahaton, joka johtaa tietojärjestelmien tai –verkkojen saatavuuden menettämiseen

Haitallinen ohjelma –tai koodi	Haittaohjelman asentaminen ja sen suorittaminen tietojärjestelmässä
Sääntöjen vastainen käyttö	Laillisten käyttäjien käyttöohjeiden ja –määräysten vastainen käyttö
Skannaus, tiedustelu tai tunkeutumisen yritys	Oikeudeton tietojärjestelmän tai –verkon skannaus tai muu tiedustelu; tunkeutumisen yritys
Tutkinta	Tilanteen tai toiminnan tutkinta, jonka riikollisuutta epäillään

Analysointityökalu on siis ohjelma, joka siihen asetetun luokittelualgoritmin perusteella luokittelee viestin johonkin ylläolevista kategorioista. Algoritmit ”opetetaan” opetusaineiston, eli viestitietokannan avulla. Ohjelmassa sovelletaan siis koneoppimista. Luokittelualgoritmit eivät kuitenkaan ole täydellisiä, vaan ne luokittelevat oikeisiin kategorioihin noin 70-80 prosenttia sanoista. Kategoriat eivät ole lukittuja, vaan niitä voidaan muuttaa tarvittaessa. Oleellista on kuitenkin että kategoria eroavat selkeästi toisistaan, etteivät algoritmit luokittele sanoja väärin kategorioihin. Haasteena tässäkin on, että jotkin sanat ja viestit voitaisiin luokitella useampaan eri kategoriaan, kuten yleisesti tilannekuvan osalta luvussa 2.3.2 todetaan. (Puuska et al. 2016)

Alla olevassa kuvassa 10 on ruutukaappaus prototyypistä, jossa pikaviestinjärjestelmän yhteydessä on analysointityökalu, joka luokittelee lähetetyt viestit yllä oleviin kategorioihin. (Puuska et al 2016). Kuvassa on kuvitteellinen keskustelu, johon asiantuntija osallistuu, tässä tapauksessa havainnolla palvelunestohyökkäyksestä.

```

SCAN - Security Chat ANalyser
08:37 [Users #kyber]
08:37 [@redox] [ bot]
08:37 -!- Irssi: #kyber: Total of 2 nicks [1 ops, 0 halfops, 0 voices, 1 normal]
08:39 <@redox> Palvelunestohyökkäys osoitteesta 127.0.0.1 havaittu palomuurin lokeista #fw-1
08:39 < bot> Threat class: Denial of Service
08:39 < bot> IP(s) detected: 127.0.0.1
08:39 < bot> HT(s) detected: #fw-1
08:40 <@redox> Työasemilla havaittu haittaohjelmaperäistä liikennettä ulos sisäverkosta #apt-uhka
08:40 < bot> Threat class: Malicious Code
08:40 < bot> HT(s) detected: #apt-uhka
08:40 <@redox> Palvelinsaliin on murtauduttu, Poliisi tutkii asiaa #apt-uhka
08:40 < bot> Threat class: Investigation
08:40 < bot> HT(s) detected: #apt-uhka

```

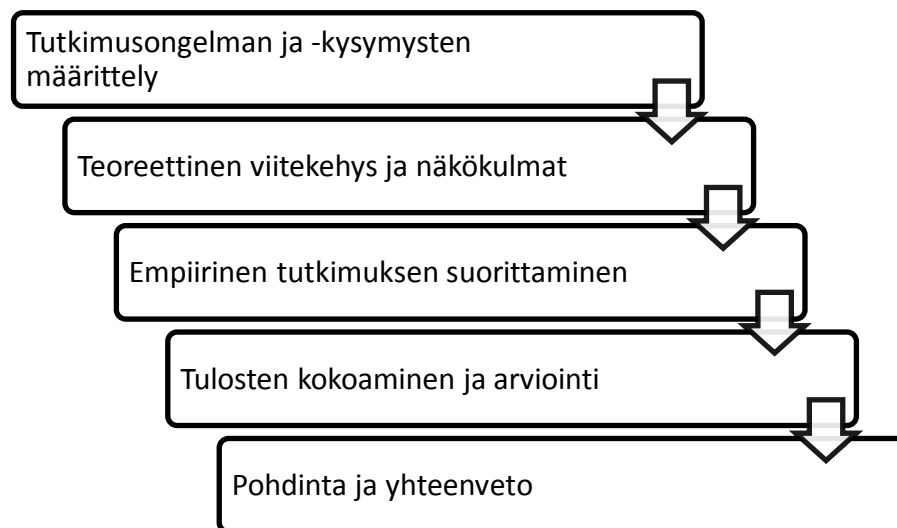
Kuva 10. Prototyyppi pikaviestinnän analysointityökalusta, lähteestä Puuska et al. (2016, s 19)

Tämänhetkinen analysointityökalujen kyvykyys liittyy täten keskustelujen aiheen tai aihealueen tunnistamiseen. Lisäksi ohjelma tunnistaa määriteltäviä avainsanoja tai määritellyssä syntaksissa esitettyjä sanoja, tässä tapauksessa laitteiden verkko- eli IP-osoitteita sekä # -merkillä aloitettuja sanoja.

5. TUTKIMUSPROSESSI

5.1 Tutkimusprosessi

Tutkimusprosessista, joka on esiteltynä kuvassa 11, muodostui yleistä tutkimusprosessia noudattava (TTY, 2015, s. 3). Tutkimusprosessi käynnistettiin tutkimusongelman ja aiheanalyysin kautta. Aiheanalyysissä selvennettiin työn ongelmakenttää eli valtionhallinnon TKT-johtamisen kokonaisuutta sekä tutkimuskohdetta ja sen roolia siinä. Tilaajan kanssa yhteistyössä tarkennettiin ja määriteltiin tutkimuksen tarkoitusta eli etsittiin tilaajan kannalta sekä tutkimuksellisesti hyödyllistä tutkimusfokusta. Aiheanalyysin perusteella tutkimuksen ongelmakentäksi rajattiin tieto- ja kyberturvallisuus sekä sen osana tietojohdaminen. Tutkimusongelman määrittelyn jälkeen tehtiin näkökulmien rajaukseksi ja tarkastelukohteiksi yleinen TKT-johtaminen strategisella tasolla normaali- ja häiriötilanteissa, sekä tilannetietoisuuden käsitteen ja tietojohdamisen tarjoamat näkökulma aiheeseen. Tämän jälkeen muodostettiin alustavat tutkimuskysymykset ja tutkimuksen tavoitteet, joita rajattiin yhteistyössä tilaajan kanssa lopulliseen muotoonsa. Tämä vaihe oli useille projekteille tyypillisesti iteratiivinen. Näistä lähtökohdista muodostettiin tutkimuskohteen teoreettista viitekehystä valitusta näkökulmista. Tämän perusteella etsittiin kirjallisuuskatsauksen avulla asioita joihin tutkimuskohde voisi valtionhallinnon TKT-johtamisessa vaikuttaa.



Kuva 11. Diplomityön tutkimusprosessi.

Empiirisessä tutkimusosiossa tavoitteena oli kerätä tietoa tutkimuskohteesta ja etsiä tukea kirjallisuuden perusteella esitetyille väitteille ja lisäksi osaltaan laajentaa vastauksia tutkimuskysymyksiin. Empiirisellä osiolla tutkimuksessa pyrittiin kartoittamaan pikaviestintijärjestelmään ja analysointitoimintaan liittyvien sidosryhmien arvioita vaikutuksista tieto- ja kyberturvallisuuden johtamiseen valtionhallinnossa. Empiirisessä tutkimuksessa

tehtiin haastatteluita sekä lisäksi havainnointia. Tutkimuksia pikaviestinjärjestelmästä tai pikaviestinnän analysoinnista TKT –johtamisen kontekstissa ei kirjallisuuskatsauksessa löydetty, jolloin sitä haluttiin tukea muilla tietolähteillä. Tutkimuksen aikana tutkimuskohde ei kuitenkaan ollut operatiivisessa käytössä, jolloin ei ole mahdollista havainnoida tai kerätä tietoa konkreettisista vaikutuksista. Tämä rajoittaa suoria tietolähteitä, koska ei ole käytettävissä vaikutuksia kuvaavaa dataa.

Empiirisessä tutkimuksessa kerättyä aineistoa jäseneltiin ja analysoitiin luvun 6 mukaisesti. Jäseneltyä aineistoa tarkasteltiin ja sen merkityksiä pohdittiin kirjallisuuskatsauksen avulla luvussa 7. Tutkimusaineistosta myös nostettiin esille asioita, joita kirjallisuuskatsauksessa ei tullut esille. Lopuksi muodostettiin yhteenveto, johon koottiin keskeiset havainnot ja päätelmät. Yhteenvedossa myös arvoitiin tukimusta ja mahdollisia jatkotutkimuskohteita.

5.2 Haastattelumenetelmien valinta ja hyödyntäminen

Haastattelut ovat Hirsjärven ja Hurmeen (2011) mukaan luonnollinen keino henkilöiden mielipiteiden ja näkemysten kartoittamiseen. Haastatteluissa tutkija voi vuorovaikutuksen avulla välittää kuvaa haastateltavan ajatuksista. Haastattelu sopii moniin erilaisiin tutkimuksiin sen joustavuuden ansiosta Hirsjärven & Hurmeen (2011). Toisaalta haastattelut sopivat tilanteeseen, jossa tutkimusalue on vähän kartoitettu tai tuntematon, koska se antaa mahdollisuuden sekä haastateltavalle että haastattelijalle mahdollisuuden tarkentaviin kysymyksiin. Lisäksi tutkimuksen tarkoituksena on *ymmärtää* vaikutuksia, jolloin arvoitiin, että on tarpeen selventää ja syventää näkemyksiä. Pikaviestintäjärjestelmä ja siihen liittyvä analysointitoiminta sekä näiden vaikutukset olivat tutkimuksen aikana haastateltaville uusi aihealue.

Haastatteluille mahdollisena vaihtoehtona tarkasteltiin kyselyitä, joka on toinen yleinen ihmistutkimuksen tutkimusmenetelmä. Kyselyn suurin etu olisi ollut aineiston käsittelyn helppous ja esimerkiksi mahdolliset kvalitatiiviset aineistoa kuvaavat luvut. (Hirsjärvi & Hurme, 2011). Tutkimuksessa laajan aineiston kerääminen ei kuitenkaan ollut mahdollista, koska pikaviestinjärjestelmän käyttäjäkunta oli rajoitettu tutkimusta tehtäessä. Mahdollisten vastaajien rajallinen määrä ei mahdollistanut järkevää kyselyn toteuttamista. Näistä syistä päädyttiin haastatteluun empiirisenä menetelmänä kyselylomakkeen sijaan.

Haastattelumenetelmäksi valittiin (Hirsjärvi & Hurme 2011) teemahaastatteluksi kuvaama puoli-strukturoitu haastattelumenetelmä, Teemahaastattelussa keskitytään valittuihin aihepiireihin ja keskustelu etenee näiden keskeisten teemojen varassa. Puoli-strukturoimattomassa haastattelussa jokin osa-kokonaisuus pidetään samana kaikissa haastatteluissa, mutta muutoin haastattelua ei ole rajoitettu, esimerkiksi vastausvaihtoehdoilla. Teemahaastattelussa teemat ovat kaikissa haastatteluissa samat mutta siitä puuttuu strukturoidulle haastattelulle tunnusomainen kysymysten tarkka esitysjärjestys.

Haastatteluissa keskityttiin etsimään sidosryhmien näkemyksiä pikaviestinjärjestelmän mahdollisista vaikutuksista haastateltavien toimintaan ja työnkuvaan. Kysymykset laadittiin tietojohtamisen ja tilannejohtamisen näkökulmista. Tällä tavoin saatiin tietoa eri sidosryhmiltä siitä, mitkä heidän näkemyksen mukaansa olisivat pikaviestinjärjestelmän vaikutukset heidän näkökulmastaan. Haastattelut olivat suhteellisen vapaamuotoisia, jolloin saatiin monipuolisemmin eri näkemyksiä, mikä oli tutkimuksen tarkoitus. Haastattelut tehtiin haastateltavien organisaation tiloissa kasvokkain, lukuun ottamatta ensimmäistä haastattelua joka toteutettiin puhelimitse. Haastattelut suoritettiin yksilöhaastatteluina. Haastattelut tehtiin haastattelua 1 lukuun ottamatta kasvokkain, joko haastateltavan organisaation tai tilaajaorganisaation tiloissa. Haastattelut kestivät noin 25-50 minuuttia.

Haastattelujen kysymysrunko on liitteessä 2. Haastatteluiden teemat muodostettiin tutkimuksen aihepiiriin, valtionhallinnon tieto- ja kyberturvallisuuden johtamisen näkökulmasta. Lisäksi hyödynnettiin tutkimusprosessin aikana SecICT -hankepäällikön kanssa tehtyjä vapaamuotoisia haastatteluita (Janhunen, 2015) sekä näiden muistiinpanoja.

5.3 Haastateltavat henkilöt

Haastateltavat ovat valtionhallinnon eri organisaatioissa työskenteleviä henkilöitä, joiden tehtäväkuvaan kuuluvat sekä tekniseen että hallinnolliseen tietoturvaluuteen liittyvät tehtävät. Osa heistä on pikaviestinjärjestelmän käyttäjiä, muiden haastateltavien osalta pikaviestinjärjestelmä vaikuttaa heidän tehtäviinsä tai he ovat muutoin sen sidosryhmiä. Osa haastateltavista valittiin diplomityön tilaajan suosituksesta.

Haastatteluissa aluksi kysyttiin haastateltavan tehtävistä ja heidän työssään kohtaamista haasteista, jotta oli paremmin mahdollista ymmärtää haastateltavien lähtötilanne osana valtionhallinnon TKT-toimintaa sekä haastateltavan suhde tutkimuskohteeseen. Tämän jälkeen edettiin kysymysrunгон avulla eri aihepiirien käsittelyyn ja lopuksi tiedusteltiin vapaamuotoisesti haastateltavien kommentteja pikaviestinjärjestelmään liittyen. Haastattelut nauhoitettiin ja litteroitiin haastatteluaineistoksi. Litterointi toteutettiin tiivistäen, jolloin haastatteluviesteistä tallennettiin vain oleelliset osat.

Haastateltava 1 toimii keskeisen valtionhallinnon IT-palveluntuottajan Valtorin SOC –operaattorina, joten hänen tehtäviinsä kuuluu esimerkiksi verkkoliikenteen valvonta ja tietoturvapoikkeamiin reagointi sekä niiden selvittämisen koordinointi ja hallinta. SOC –operaattori on operatiivisella tasolla yhteydessä muihin viranomaisiin ja sidosryhmiin.

Haastateltava 2 toimii SOC –toiminnon projektipäällikkönä, jonka tehtäviin kuuluu SOC-toiminnan hallinnointi ja kehittäminen. Kehittämiseen kuuluu SOC –toiminnan työkalujen ja prosessien kehittämistä, jonka seurauksena haastateltava on ollut mukana pikaviestinjärjestelmän kehittämisessä. Lisäksi projektipäällikkö toimii yhteistyössä muiden valtionhallinnon organisaatioiden kanssa hallinnollisella tasolla ja kehittää organisaatioiden välistä yhteistyötä.

Haastateltava 3 oli haastatteluissa Viestintäviraston Kyberturvallisuuskeskuksen tilannekeskuksen edustajana. Tilannekeskuksen tehtäviin sisältyvät esimerkiksi kansallisen TKT-tilannekuvan kerääminen ja ylläpitämien sekä koordinoivana tahona toimiminen laajemmissa poikkeamatilanteissa. Kyberturvallisuuskeskuksen toimii myös Suomen kansallisena yhteistyötahona kansainvälisten sidosryhmien kuten muiden valtiollisten tietoturvatuimijoiden kanssa.

Haastateltava 4 toimii Valtioneuvoston kansliassa (VNK), tietoturvallisuuspäällikkönä. Valtioneuvoston kanslian tehtävät valtionhallinnon tieto- ja kyberturvallisuuden kokonaisuudessa liittyvät esimerkiksi ministeriöiden käyttämien tietojärjestelmäpalveluiden valvontaan. Lisäksi kansliassa toimii Valtioneuvoston tilannekeskus, jonka tehtävänä on koostaa valtioneuvostolle yhteiskunnan turvallisuutta koskevaa tilannekuvaa. Tilannekuvaan liittyy myös kyberturvallisuus yhtenä osa-alueena. VNK ei ole pikaviestinjärjestelmän käyttäjä, mutta mahdollinen analysointitulosten hyödyntäjä.

Haastateltava 5 toimii Maanpuolustuskorkeakoulussa Sotatekniikan laitoksella tutkijana, ja on ollut kehittämässä pikaviestinnän analysointitoimintaa (Puuska et al. 2016). Lisäksi haastateltava on ollut mukana Kansallisissa Kyberturvallisuusharjoituksissa, joissa analysointityökalujen prototyyppejä alustavasti kehitettiin ja jonka pohjalta tutkimus käynnistettiin. Haastateltava ei edusta pikaviestinjärjestelmän käyttäjiä tai sen hyödyntäjiä. Haastattelusta pyrittiin keräämään tietoa tieto- ja kyberturvallisuuteen liittyvän pikaviestinnän analysoinnista ja sen mahdollisista vaikutuksista ja hyödyntämismahdollisuuksista TKT-johtamiseen liittyen.

5.4 Havainnointi

Toiseksi tutkimusmenetelmäksi haastattelujen tueksi valittiin havainnointi, toiselta nimeltään observointi. Havainnointi on joko systemaattista, eli strukturoitua, tai ei-systemaattista, eli strukturoimatonta, tutkittavan kohteen tai ilmiön tarkkailua. Systemaattinen tarkkailu on jäsenneiltyä ja yksityiskohtaisesti suunniteltua ja toteutettua, ei-systemaattinen puolestaan väljempää ja joustavampaa. Strukturoidussa havainnoinnissa ongelmanasettelu tulee olla jäsenneilty, jolloin voidaan päättää mitä havainnoidaan ja millä tavoin. Havainnointia suunniteltaessa voidaan esimerkiksi määritellä kerättävän tiedon luokittelu tai mitta-asteikoita, joita käytetään havainnoinnin perustana. Strukturoimattomassa havainnoinnissa pyritään saamaan mahdollisimman paljon erilaista tietoa tutkittavasta asiasta. Tällöin havainnoinnissa ei niinkään keskitytä määriteltyjen luokiteltujen tietojen keräämiseen vaan voidaan vapaamuotoisemmin kerätä erityyppisiä havaintoja. Riippumatta havainnoinnin toteutuksesta, tutkimusmielessä tehtävässä havainnossa tiedot tulee kuitenkin koota systemaattisesti ja tarkoituksenmukaisesti, jotta tiedot vastaavat ongelmanasettelua. Havainnointi voi kohdistua tapahtumiin, ihmistutkimuksessa käyttäytymiseen tai fyysisiin kohteisiin, kuten kohteen fyysiseen ympäristöön. (Saaranen-Kauppinen & Puusniekka, 2006, Anttila, 2007)

5.4.1 Havainnoinnin tavoitteet ja kohteet tutkimuksessa

Havainnointi suoritettiin Valtionvarainministeriön ja Puolustusministeriön Valtakunnallinen Kyberturvallisuusharjoitus 2016 –harjoituksessa eli vuosittaisessa KYHA-harjoituksessa (myöhemmin ”harjoitus”). Kyseinen harjoitus on viranomaistoimijoiden tieto- ja –kyberturvallisuuden häiriönhallinnan testaamiseen ja parantamiseen tähtäävä harjoitus. Harjoitus toteutettiin ns. toiminnallisena harjoituksena, jossa osallistujat olivat aktiivisesti toimivia osapuolia harjoitusympäristössä. Harjoitusympäristöön mallinnettiin osallistuvien viranomaistahojen tuottamia ja käyttämiä ICT-palveluita sekä niitä yhdistäviä tietoliikenneverkkoja. Harjoituksessa osa osallistujista toimi oikeaa tilannetta vastaten näiden palveluiden tuottajina ja osa osallistujista palveluiden käyttäjinä. Lisäksi harjoitusympäristöön oli toteutettuna Internetiä simuloiva verkko, joka sisälsi useita simuloituja julkisia palveluita. Harjoituksessa näihin palveluihin ja niiden tukemiin prosesseihin tehtiin harjoituksen johdon sekä erillisen haitallista toimintaa tekevän tiimin toimesta erityyppisiä poikkeustilanteita, kuten palveluksenestohyökkäyksiä, jotka harjoitukseen osallistuvien tuli tunnistaa ja selvittää. Harjoitus kesti yhteensä neljä päivää, josta noin kolme päivää oli varsinaisia harjoitustapahtumia.

Tutkimukseen havainnointi harjoituksessa valittiin, koska harjoituksessa osallistujilla oli käytettävissään vastaava pikaviestinjärjestelmä mitä tutkimukseen liittyen kehitetään. Lisäksi harjoituksen osallistujat ovat niitä käyttäjiä, joita tutkimuksen pikaviestinjärjestelmälle on alustavasti suunniteltu, eli valtionhallinnon tieto- ja kyberturvallisuuden asiantuntijoita. Täten harjoituksessa oli mahdollisuus päästä observeerimaan pikaviestinjärjestelmän käyttöä poikkeustilanteissa oikeata simuloivassa ympäristössä. Harjoituksessa toteutettiin myös pikaviestinnän analysointitoimintaa, jolla tuotettiin keskusteluiden luokitelua ja visualisointia harjoituksen johdon tueksi. Havainnoinnilla voitiin siten kerätä tietoa pikaviestinjärjestelmän mahdollistamista toimintamalleista ja niiden vaikutuksista valtionhallinnon TKT- johtamisen näkökulmasta.

Havainnointitekniikaksi valittiin passiivinen osallistuva havainnointi osallistumatta kuitenkaan harjoituksen varsinaisiin tapahtumiin. Harjoituksen päätavoite ei ollut pikaviestinjärjestelmän tai analysointitoiminnan testaaminen, joten havainnoinnilla ei haluttu vaikuttaa harjoituksen tapahtumien kulkuun.

Havainnointitilanne oli havainnoijan kannalta uusi, joten havainnoinnista ei pyritty tekemään strukturoitua vaan havainnointisuunnitelmasta tehtiin suhteellisen avoin ja siinä käsiteltiin vaan havainnoinnin pääkohteet. Tutkimuksen tavoitteena oli analysoida pikaviestinjärjestelmän vaikutuksia valtionhallinnon tieto- ja kyberturvallisuuden johtamiseen, jolloin kaikki tulokset ja havainnot tähän liittyen katsottiin arvokkaiksi.

5.4.2 Havainnoinnin toteutus

Ennen harjoitusta tehtiin havainnointisuunnitelma yhteistyössä harjoituksen järjestäjien kanssa. Havainnoitsija toteutti harjoituksessa osana tilannekuvaa tarkkailevaa tutkimusryhmää. Suunnitelman tehtiin tutkimuskysymysten pohjalta, jotta varmistettiin että havainnoinnilla kerätään tietoa, jota voidaan hyödyntää tutkimuskysymyksiin vastattaessa. Suunnitelmaan kirjattiin havainnoinnin kohteet ja asiat joihin pyrittiin havainnoinnin aikana kiinnittämään huomiota.

Havainnointi toteutettiin luvussa 4 kuvatun analysointitoimijan sekä päätöksentekotason näkökulmasta Havainnointia tehtiin jokaisena harjoituspäivänä ja havainnoinnin aikana oltiin läsnä harjoitustilassa, jossa osallistujat harjoituksen aikana toimivat. Lisäksi harjoituksen aikana havainnoijalla oli mahdollisuus seurata pikaviestinjärjestelmässä käytyjä keskusteluja sekä niistä tuotettuja analysointituloksia. Harjoituksessa osallistujilla oli käytössään pikaviestinjärjestelmä kommunikointiin muiden osallistujien kanssa sekä erillinen pikaviestinjärjestelmä toiminnan raportointiin ja yhteydenpitoon harjoituksen johdon kanssa. Analysoinnin tulokset olivat sekä luvussa 4 esiteltyä kielellistä analyysiä ja viestien luokittelua, että viestiliikenteen visualisointia.

Määrältään tiimien välistä pikaviestintää oli kohtalaisesti, tiimien ja harjoituksen johdon välistä kommunikointia viestintää runsaasti. Tiimien välisessä viestinnässä pikaviestintään hyödynnettiin jonkin verran. Harjoituksessa pikaviestinjärjestelmää hyödynnettiin myös eräänlaisen raportointityökaluna havaintojen ja toimenpiteiden kirjaamiseen. Järjestelmä muodosti siihen syötettyjen avainarvojen (avainsanojen) pohjalta rakenteellisen esityksen viestin sisällöstä. Eri havainnot ja tapahtumat erotettiin #-tunnisteella, joiden perusteella järjestelmä liitti samaa tapahtumaa koskevat havainnot yhteen. Havainnoinnin toteutusta vaikeutti se, että harjoituksen tiimien jäsenet sijaitsivat omissa, tiimikohtaisissa tiloissaan, jolloin tiimin sisäinen kommunikointi oli heidän kannaltaan luontevampaa tehdä suullisesti. Täten tiimien sisäistä pikaviestinjärjestelmän avulla tapahtuvaa kommunikointia ei juurikaan ollut, joten havainnointitilanne ei täysin vastaa suunniteltua pikaviestinjärjestelmän käyttöä. Tämä kuitenkin mahdollisti havainnoinnin hieman erilaisesta näkökulmasta ja toi esille uusia käyttötapoja ja –mahdollisuuksia.

6. TUTKIMUKSEN TULOKSET

Empiirisen tutkimuksen tulokset saatiin edellisessä kappaleessa esiteltyjen henkilöiden haastatteluista sekä Kansallisen Kyberharjotuksen 2016 havainnoinnista. Tulokset jaoteltiin kolmelle tasolle, joista jokainen edustaa hieman eri näkökulmaa tutkimuskohteeseen. Tutkimusaineiston jäsentelyssä ja analysoinnissa havaittiin aineiston jakaantuvan pääosin joko yksilö- tai tiimitasolle, organisaatiotasolle tai valtionhallinnon tasolle, joten päädyttiin käyttämään tätä jaottelua. Tulosten pohdinnassa luvussa 7 on tuloksia käsitelty ja hyödynnetty enemmän teemoittain.

Tutkimusaineisto koostui litteroiduista haastatteluista, haastatteluiden muistiinpanoista sekä havainnoinnin muistiinpanoista. Kerätty tutkimusaineisto, ja siitä muodostetut tulokset ovat kohtalaisen monipuolisia ja eri näkökulmia pikaviestinjärjestelmään ja analysointitoimintaan tuli esille runsaasti. Pikaviestinjärjestelmän luonteesta johtuen luonnollisesti esiin nousivat sen mahdollistama interaktiivisuus ja kaksisuuntaisuus. Haastatteluissa nousi esiin pääosin mahdollisia hyötyjä, joita pikaviestinjärjestelmä ja analysointi-toiminta voisivat TKT-toimintaan tuoda, jolloin mahdollisia haittavaikutuksia käsiteltiin verrattain vähän. Lisäksi haastatteluissa käsiteltiin pikaviestinjärjestelmän mahdollisia vaikutuksia toimintaan ja toimintatapoihin. Haastatteluiden avulla saadut tulokset painottuvat pääosin tietoon ja sen jakamiseen liittyviin tekijöihin. Tätä selittää todennäköisesti se, että järjestelmän ei ollut tulosten keräämisen aikana operatiivisessa käytössä eikä vastaavaa järjestelmää ole aikaisemmin ollut, jolloin on ehkä hieman haastavaa arvioida järjestelmään tästä näkökulmasta. Havainnoinnin tulokset painottuvat organisaatio- ja valtionhallinnon tasoille, koska harjoituksessa oli rajalliset mahdollisuudet yksittäisten käyttäjien toiminnan seuraamiseen.

Liitteen 3 taulukkoon on koottuna yhteen haastatteluissa esille tulee asiat haastateltavittain. Liitteen taulukossa on mainittu vain kertaalleen eri asiat, vaikka joistakin asioista keskusteltiin useammassa kuin yhdessä haastattelussa.

6.1 Käyttäjä- ja tiimitaso

Yksittäisen käyttäjän näkökulmasta järjestelmä tarjoisi mahdollisuuden monen erityyppisen tiedon, sekä yleisen tiedon että tilannekuvan, keräämiseen ja vaihtamiseen. Yksittäisen käyttäjän näkökulmasta pikaviestinjärjestelmä tarjoaa mahdollisuuden ”horisontaalisen”, eli riskienhallinnan operatiivisen tason kommunikoinnin tiedonvaihdon. Sen avulla voidaan kerätä tilannekuvaa sekä yleisellä tasolla että yksityiskohtaista TKT –tietoa. Pikaviestimen avulla käyttäjä voi kerätä ja vaihtaa tietoa esimerkiksi haittaohjelmahavainnoista, haavoittuvuuksista, eli yleisesti tietoa tieto- ja kyberturvallisuuteen liittyvistä tapahtumista omassa ja muissa organisaatioissa. Toisaalta, mikäli häiriötilanteen käsittely

edellyttää, pikaviestimen avulla voidaan välittää myös yksityiskohtaisempaa tietoa, esimerkiksi organisaatioiden tietojärjestelmien tilanteesta. Tiedonjaon ja –keräämisen näkökulmasta pikaviestinjärjestelmä tarjoaisi siis kahden käyttäjän välisen viestintävälineen tai ryhmäviestinnässä virtuaalisen ”tilan”, jossa on mahdollista esittää kysymyksiä useille toimijoille ja saada vastauksia näihin kysymyksiin. Järjestelmän avulla yksittäiset käyttäjät voisivat synkronisesti, eli keskustellen, jakaa ja levittää TKT -tietoa muita välineitä nopeammin muille käyttäjille ja organisaatiolle. Lisäksi järjestelmän avulla voidaan antaa esimerkiksi suosituksia toimenpiteistä tai ohjeistaa muita käyttäjiä eli vaihtaa ja jakaa osaamista sekä operatiiviseen TKT-toimintaa että tilannekuvaan liittyen. Myös mahdollisuus esimerkiksi tarkentavien kysymysten esittämiseen nousi esille yhtenä merkittävänä hyötynä. Operatiivisella tasolla eli toimenpiteitä toteuttavalla tasolla pikaviestinjärjestelmä voisi siis tuoda hyötyjä päivittäiseen toimintaan nopean ja kaksisuuntaisen tiedonvaihdon mahdollistamana viestintävälineenä.

Harjoituksessa tehtyjen havaintojen mukaan useissa tapauksissa pelkkä tilannekuva esimerkiksi teknisestä järjestelmästä ei riitä, vaan tarvitaan ymmärrystä uhkien realisoinnin ja niiden käsittelyksi tarvittavien mahdollisten toimenpiteiden vaikutuksista fyysisessä maailmassa tuotettuihin palveluihin. Pikaviestinjärjestelmä voisi mahdollistaa myös TKT-toimintaan liittyvän tiedon ulkopuolisen tiedon eli toimintaympäristötiedon välittämisen ja sen keräämisen yksilötasolla. Kaikki haastateltavat näkivätkin järjestelmän tuottamien hyötyjen muodostuvan ensisijaisesti kaksisuuntaisen tiedonvaihdon ja interaktiivisuuden perusteella.

Haastateltavien 1 ja 2 edustaman SOC –toiminnan, eli organisaatiotason operatiivisen TKT-toimijan näkökulmasta pikaviestinjärjestelmä voisi tukea toiminnon muita tietolähteitä ja tiedonhankintamenetelmiä mahdollistamalla kaksisuuntaisen tiedonvaihdon ja tuottamalla järjestelmän luomasta verkostosta tilannekuvatietoa tieto –ja kyberturvallisuuteen liittyen. Yhteistoiminta muiden viranomaisten kanssa on muilta osin toiminut hyvin, mutta sähköpostin avulla tapahtuvassa viestinnässä on ollut viivettä.

[H1] ” tietoturvatyöimijöiden [...] kanssa yhteistyö on mennyt [...] positiivisissa merkeissä, ollaan saatu aina tukea kun on pyydetty ja välitetty raportteja kun saatu tapauksia heiltä, päivystyspuhelimet ja tän tyyppiset palvelut on toiminut oikein hyvin. [...] Esimerkiksi jos CERT ilmoittaa uhkasta niin se saa heti tiedon onko meillä havaittu sitä ja me saadaan tieto missä sitä on havaittu ja missä laajuudessa ja pitääkö meidän alkaa toimenpiteisiin [...] siinä voi olla viivettä sähköpostilla hyvinkin paljon [...] [pikaviestinjärjestelmällä] voitaisiin saada tieto jo seuraavalle päivälle”

Erityisen arvokasta pikaviestinjärjestelmästä saatavaa tietoa olisi tilannekuva, joka on SOC –toiminnoilta huomattavaa tai havaitsemattaa. Tällaiseen tietoon ja siihen liittyvään tapahtumaan ei todennäköisesti ole reagoitu, jolloin sen muodostama riski käsittelemättä ja uhka riskin seurauksien realisoinnista on yhä olemassa. Pikaviestinjärjestelmä voisi

täten olla päivittäistä toimintaa tukeva työkalu lisäämällä käytettävissä olevia tietolähteitä ja laajentamalla näkyvyyttä muiden yhteisessä kyberympäristössä olevien toimijoiden tilanteeseen, mikä parantaa ainakin tietolähteiden osalta tilannetietoisuuden muodostamista. Heidän näkökulmastaan pikaviestinjärjestelmä voisi osittain vastata myös Fenzin et al. (2014) tunnistamiin haasteisiin tietojärjestelmäympäristöihin liittyvän inventaariotiedon keräämisessä ja ylläpitämisessä ainakin yleisellä tasolla, mahdollistamalla interaktiivisuuden muiden järjestelmän käyttäjäorganisaatioiden kanssa.

Käyttäjäkokemuksen ja sen teknisten ominaisuuksien merkitystä pikaviestinjärjestelmän tuoman lisäarvon muodostumisessa tuotiin esille useassa haastattelussa. Kyberturvallisuuskeskuksen asiantuntijoiden näkökulmasta pikaviestinjärjestelmällä voitaisiin ehkä korvata osittain sähköpostia tiedon levittämisessä. Sähköpostiin verrattuna mukaan pikaviestinjärjestelmän tuottamia etuja ovat sen mahdollistama viestinnän ja toimenpiteiden parempi kronologisen järjestyksen seurattavuus.

Tämän ansiosta pikaviestinjärjestelmän käyttäjäkokemus tilanteen seuraamisessa on parempi ja käyttäjät ovat hänen mukaansa paremmin tietoisia tapahtumien etenemisestä eli heidän tilannetietoisuutensa on parempi. Sähköpostiviesteihin voidaan vastata satunnaisessa järjestyksessä, jolloin poikkeamatilanteissa asioiden selvittelyssä voi esiintyä sekaannuksia. Tämä voi johtaa väärin reagointeihin tai reagoimattomuuteen, joten sähköpostin avulla tapahtuva koordinointi on hankalampaa. Pikaviestinjärjestelmillä on vastaava etu myös puhelimeen verrattuna, koska puhelusta ei yleensä jää tallennetta myöhemmin tarkasteltavaksi tai puhelun ulkopuolisten tarkasteltavaksi. Puhelimen avulla tapahtuvasta viestinnästä voi siis olla haastavampaa seurata tilanteen etenemistä.

Parempaa käyttäjäkokemusta pikaviestinjärjestelmä voisi tarjota myös luottamuksellisen tiedon käsittelyssä. Mikäli järjestelmä toteutetaan siten että se mahdollistaa tiedon käsittelyn kryptografisesti salatuttuna, voivat käyttäjät hyödyntää järjestelmää luottamuksellisen tiedon jakamiseen ja luottamuksellisten asioiden käsittelyyn. Valtioneuvoston asetus 681/2010 tietoturvallisuudesta valtionhallinnossa velvoittaa viranomaisia lähettämään luottamukselliseksi luokitellut asiakirjat salatusti tietoverkkojen ylitse. Nämä tietoturva-vaatimukset täyttävän pikaviestinjärjestelmän tapauksessa käyttäjien ei tarvitsisi käyttää nykyisiä ratkaisuja, kuten salattuja sähköposteja tai muita ratkaisuja, jotka ovat haastateltavien mukaan huonompia käytettävyydeltään. Nykyisissä ratkaisuissa salatut sähköpostit esimerkiksi poistetaan automaattisesti, yleensä 14 vuorokauden kuluttua lähettämisestä, jolloin aikaisempiin viesteihin ei ole mahdollista palata ellei niitä erikseen omalle työasemalleen tallenna.

Käyttäjäkokemukseen liittyen haastateltava 4 totesi, että järjestelmän ja analysoijien tulisi kyetä tarjoamaan tilannekuvaa myös mobiilisti, koska monessa tapauksessa poikkeusti-

lanteet eivät rajoitu normaaleihin työaikoihin eli arkipäiviin, vaan niitä esiintyy myös iltaisain ja viikonloppuisin. Järjestelmän avulla voitaisiin tässä tapauksessa myös mahdollistaa tilannekuvan saamisen kellonajasta ja paikasta riippumatta.

Pikaviestinnän analysoinnin ja siten valtionhallinnon TKT-tilannekuvan kannalta on merkityksellistä millaisia viestejä käyttäjät syöyttävät pikaviestinjärjestelmään. Käyttämällä esimerkiksi tunnisteita, jotka erottavat viesteitä avainsanoja, voidaan parantaa analysointityökalujen toimivuutta ja luokittelun onnistumista. Toisaalta haastateltava 5 oli samaa mieltä mm. Raven et al. (2002) kanssa siitä, että pikaviestinnän ”puhekielimäisyys” nopeuttaa yksilöiden viestintäprosesseja ja on yksi merkittävä edistävää tekijä pikaviestinjärjestelmän yksilötason adoptoinnissa.

[H5] ”Siitä oli puhetta että homma helpottuisi huomattavasti jos vähänkin käytettäisi etukäteen kerrottuja viestejä tai sanoja, jotain tiettyjä termejä. Tässä on tää hashtag käytössä joka on oikeasti ihan kätevä. Tällaisia jos laittaisi lisää niin se helpottaisi [analysointia], mutta se hidastaisi sitä puhekielimäisyyttä mikä tuolla chatilla on, että jos se menee melkein koodaamiseksi niin ei ihmiset sitten käytä sitä”

Hänen näkemyksensä, sekä Janhusen (2015), mukaan asiantuntijataso käyttäjät eivät kuitenkaan ole halukkaita muodolliseen, esimerkiksi määrämuotoisiin raporteihin perustuvaan tiedonvaihtoon, vaan he haluavat joustavamman viestintävälineen. Joustavuudella tarkoitetaan tässä yhteydessä viestin kieliasun ja esitystyylin vapaamuotoisuutta. Mikäli tästä mahdollisuudesta puhekieliseen viestintään luovutaan, esimerkiksi määrättyillä käytösäännöillä tai ohjeilla, voi halukkuus järjestelmän käyttöön heikentyä jolloin siitä saatavat hyödyt vähentyä.

6.2 Organisaatiotaso

Organisaatiotasolla haastateltavat näkivät että pikaviestinjärjestelmä voisi tukea sekä organisaatioiden sisäistä että niiden välistä tiedonvaihtoa. Kansallisen kyberturvallisuuden tilannekuvan ylläpitämisen vastuutahona toimiva Kyberturvallisuuskeskus voisi hyödyntää järjestelmää toimintansa tukemiseen, eli tilannetiedon keräämiseen valtionhallinnon organisaatioista keräämällä keskusteluissa mainittuja havaintoja esimerkiksi haittaohjelmista. Pikaviestinjärjestelmä mahdollistaisi siten tieto- ja kyberturvallisuuteen liittyvän toiminnan ohjaamisen ja neuvonnan sekä molemminpuolisen tilannekuvan ylläpitämisen. Pikaviestinjärjestelmä ja analysointi voisi täten parantaa edellytyksiä ja tukea TKT-poikkeamiin reagoimista koko valtionhallinnon tasolla, jos sen avulla voidaan muodostaa kokonaiskuva tilanteesta organisaatioverkoston tasolla ja jakaa se verkoston jäsenille.

[H3] ”Me tuupattaisiin sinne tietoa ja kysymyksiä jostain asiasta, onko tällaisia asioita havaittu. Vastaavasti porukka voisi tehdä kysymyksiä meidän suuntaan”

Lisäksi pikaviestintäjärjestelmää voitaisiin synkronoidun viestinnän mahdollistavana järjestelmänä hyödyntää ajantasaisemman tilannekuvan jakamiseen ja tilannetietoisuuden ylläpitämiseen organisaatioiden sisällä sekä niiden kesken. Nykyisellään yhteyttä pidetään pääosin sähköpostitse, jolloin vasteaika viestinnässä voi olla pidempi ja edellisessä luvussa mainittu tilanteen seuraaminen sähköpostiviesteistä voi olla haastavaa.

Pikaviestinjärjestelmä voisi toimia organisaatioille keskitettynä yhteyspisteenä muiden organisaatioiden tietoturvahenkilöstöön, mikä helpottaisi yhteydenpitoa organisaatioiden kesken. Yhteyden saaminen ja oikean henkilön tavoittaminen sähköpostilla on joissain tapauksissa koettu hankalaksi. Yksi kontaktipiste, josta olisi tavoitettavissa organisaatioiden tieto- ja kyberturvallisuuden kanssa työskentelevät henkilöt vähentäisi tarvittaviin henkilöihin yhteyden saamiseen tarvittavaa työmäärää. Keskitetty yhteyspiste vähentäisi eri organisaatioiden yhteyshenkilöiden etsimiseen käytettävää aikaa.

(H3) ” Se olis [...] yks paikka minne vois keskittää viestinnän [...]

Pikaviestinjärjestelmä voisi täten nopeuttaa yhteyden saamista eri henkilöihin ja organisaatioihin, ja siten tehostaa työskentelyä ja organisaatioiden välistä yhteistyötä, olettaen luonnollisesti että sen käyttäjinä tarvittavat henkilöt. Tästä ominaisuudesta hyötyisi erityisesti Kyberturvallisuuskeskus, joka toimii valtionhallinnon tietoturverkoston keskeisenä tekijänä (Janhunen, 2015). Myös havaintojen perusteella pikaviestinjärjestelmä nopeuttaisi huomattavasti tiedon saamista, sillä harjoituksessa sähköpostia käytettäessä tieto saapui usein useiden välikäsien kautta tiedon hyödyntäjälle. Melko usein välissä olevat toimijat olivat prosessimäärittysten mukaisia, mutta joissakin tapauksissa toimijat olivat mukana vain koska tiedon lähettäjä ei ollut varma, kuinka tavoittaa tiedon vastaanottaja.

Sekä haastateltavan 5, että harjoituksen havaintojen mukaan yksi oleellinen osa-alue TKT-johtamisessa on järjestelmätason tiedon yhdistäminen järjestelmillä tuotettaviin palveluihin. Jotta häiriötilanteen vakavuutta voidaan arvioida ja sen ratkaisemiseen tarvittavat optimaaliset päätökset voidaan tehdä, tulee ymmärtää järjestelmissä tapahtuvien muutosten vaikutukset reaali maailman toimintaan eli prosesseihin jotka hyödyntävät näiden järjestelmien tuottamia palveluita.

[H5] Ja täällä ylempänä [johtoportaaassa] haluttais tietää mitkä on ne vaihtoehdot ja mitä seurauksia sillä on että otetaan pois käytöstä tämä systeemi tai mitä voi seurata jos se [järjestelmä] ei ole ihan samanlainen mutta suunnilleen toimii.

Prosessi voi olla valtionhallinnon tapauksessa esimerkiksi ajoneuvojen rekisteröinti, joka hyödyntää ja tukeutuu ajoneuvorekisteriin. Tässä tarvitaan haastateltavan 5 näkemyksensä mukaan asiantuntijaa, joka osaa koostaa tarvittavan kokonaiskuvan tilanteesta siihen liittyvistä asioista eli ymmärtää tilanteen ja sen kontekstin eli järjestelmien liittymisen palveluihin. Mikäli kyseisen asiantuntija asema ei oikeuta tarvittavien päätöksen tekemiseen tilanne tulee eskaloida, eli raportoida ylemmälle taholle päätöksen tekemiseksi.

Myös harjoituksen havaintojen perusteella kontekstiedon kerääminen ja ymmärtäminen oli yksi merkittävä haaste toiminnassa. Pääosin tämän tiedon kerääminen tapahtui sähköpostilla tai muilla menettelyllä kuten kokouksilla, mutta pikaviestinjärjestelmä voisi tukea tätä toimintaa.

Strategisella tasolla johtamistyökaluna pikaviestinjärjestelmää ei ainakaan toistaiseksi nähdä, sillä tarvittavat toimintatavat ja prosessit häiriötilanteiden johtamiseen eivät ole vakiintuneet ja ovat osittain vielä kehittämiskohteita, joten ne eivät tue järjestelmän käyttöä. Operatiivisella tasolla on olemassa toiminnanohjausjärjestelmät vakavuudeltaan vähäisempien häiriöiden hallintaan, joita normaalissa toiminnassa käytetään. Pikaviestinjärjestelmä ei siis haastateltavien mukaan korvaa nykyisiä operatiivisia prosesseja ja järjestelmiä, mutta voi toimia niiden käytön tukena, kommunikointivälineenä henkilöiden välisessä yhteistyössä.

Pikaviestinjärjestelmä ja analysointityökalut voisivat mahdollistaa paitsi viestinnän analysoijien että asiantuntijoiden tilannetietoisuuden parantamisen eri organisaatioiden ja ryhmien toiminnasta. Toisaalta analysointityökalujen avulla voidaan myös tukea ymmärryksen muodostamista eri tiimien tilanteesta.

[H5] No siitä kategorisoinnista on hyötyä että sillä voidaan [erottaa asioita toisistaan]. [...] [Toinen näkökulma on että] kun kyberturvallisuusharjoituksissakin oli monta chättiä vierekkäin niin siitä oli jo hankala seurata että mitä jokainen niistä tiimeistä tekee. Että pelkästään jo siin että pystyy katsomaan lähetettyjen viestien määrästä [...] mitä näistä kanavista kannattaa seurata. Lisäksi jos tuli isompi tilanne kosketti vaikka kahta organisaatiota niin [viestien määrästä pystyi todentamaan tilanteen].

Tämän ominaisuuden merkityksellisyyttä tukevat siis havainnot sekä tutkimuksen harjoituksesta, että sitä edeltävissä harjoituksista (Janhunen, 2015). Tämän tutkimuksen harjoituksessa suurin osa harjoituksen osallistujista seurasi aktiivisesti pikaviestinjärjestelmän keskusteluita ja oli selkeästi havaittavissa, että tietoisuus muiden ryhmien toiminnasta auttoi ryhmiä tarkastelemaan omaa toimintaansa sekä ympäristöään ja arvioimaan omassa organisaatiossa tai ryhmässä tarvittavia korjaavia toimenpiteitä. Muiden ryhmien toiminnan seuraaminen saattoi siis toimia eräänlaisena ”herätteenä”, jonka perusteella omaa toimintaa lähdettiin kehittämään.

Analysointityökaluilla voitaisiin siis parantaa ja kehittää mahdollisuuksia tilannetietoisuuden ylläpitämiseen. Vaikka tutkimuksen kohteena oleva pikaviestinjärjestelmä on suunniteltu valtionhallinnon laajuiseksi, pikaviestinjärjestelmä ja viestinnän analysointi voitaisiin toteuttaa myös organisaatioiden sisäiseen TKT-johtamiseen ja tilannetietoisuuden muodostamiseen, esimerkiksi organisaation riskienhallintapäällikölle.

Harjoituksessa käytetty mallia pikaviestinjärjestelmän hyödyntämisestä eräänlaisena raportointimenetelmänä voitaisiin hyödyntää myös organisaatioiden sisäisesti. Pikaraportoinnissa joko käyttäjät tai analysointityökalut lisäävät avainsanoja eli tunnisteita viesteihin, joiden avulla eri viestit linkitetään yhdeksi dokumentiksi (raportiksi). Tämän toimintamallin tarkoituksena on ja sen tuottama lisäarvo perustuu raporttien nopeuteen, jolloin ne ovat ajantasaisia. Pikaraportit kuvaavat tilannetta nykyhetkellä tai lähimenneisyydessä eli ne tuottavat tietoa nykytilanteesta ja parantavat siten tilannetietoisuuden muodostumista. Analysointityökaluilla voitaisiin havaintojen mukaan helpottaa raportin tulkintaa, eli yhdistää raportin tietoja laajempiin asiakokonaisuuksiin, tai laajentaa raportin asiiasältöä yhdistämällä siihen tietoja pikaviestinjärjestelmän muodostamasta verkostosta.

Havaintojen mukaan pikaviestinjärjestelmää voidaan käyttää myös vastuiden ja tehtävien siirtoon organisaatioilta toiselle, mikäli havaitaan että esimerkiksi häiriöilmoituksen käsittely sitä vaatii. Tosin usein varsinainen siirto toteutettiin eri järjestelmässä, mutta pikaviestinjärjestelmää käytettiin siirrosta ja sen yksityiskohdista neuvotteluun ja sopimiseen. Harjoituksessa eri osallistujat toimivat tilanteessa, jossa organisaatiot olivat hyvin sidottuja toisiinsa tietojärjestelmien ja niiden tuottamien palveluiden kautta. Organisaatiot tuottivat toisilleen ja hyödynsivät toistensa palveluita, joiden ICT-infrastruktuuri saattoi olla kolmannen osapuolen hallinnassa. Tällöin esiin nousivat erityisesti kysymykset vastuualueista ja päätöksentekovallasta ja haasteet näiden ratkaisemisessa. Oleellista on havaintojen mukaan näissä tilanteissa tiedonvaihto eri toimijoiden kesken jotta kokonaiskuva eli yhteinen tilannetietoisuus muodostettua ja esimerkiksi vastuualueet voidaan sopia. Myös haastatteluissa mainittiin, että näihin valtionhallinnon TKT-johtamisen osaluaisiin liittyy merkittäviä haasteita. Tulevaisuudessa pikaviestinjärjestelmä voisi mahdollisesti tukea toimintaa ja johtamista, esimerkiksi vastuiden jakamiseen ja päätösten tekemiseen, mikäli johtamisen vastuut ja toimintatavat muodostetaan ja vakiinnutetaan.

Kuten todettua, yhteisen kielen ja siten yhteisen ymmärryksen puuttuminen ovat aiheuttaneet haasteita TKT – poikkeustilanteita käsittelevissä harjoituksissa. Pikaviestinnän analysointitoiminnalla on mahdollisuus vaikuttaa haasteisiin, joissa toimenpiteitä toteutettava asiantuntijataso ja päätöksiä tekevä taso eivät käyttäneet yhteistä kieltä. Asiantuntijat toimivat pääosin ”teknisellä tasolla”, jolloin he keskustelevat omilla termeillään, jotka eivät ole päätöksentekotasolle tuttuja. Tällöin päätöksentekijöille tuotettu tieto ei ole päätöksenteon kannalta hyödyllistä, eli ymmärrettävää ja oikeassa muodossa olevaa tietoa. Mikäli viestiä ei ymmärretä, vaikka se olisikin sanallisessa muodossa ja päätöksentekijän käytettävissä, on haastavaa tehdä arvioita tarvittavista päätöksistä ja niiden seurauksista. Tämä on voinut johtaa esimerkiksi ylireagoiteihin ja väärin toimenpiteisiin, kun päätöksentekijän tilanneymmärrys ja –tietoisuus viestinnän väärinymmärtämisestä johtuen ei ole ollut riittävä (Janhunen, 2015).

(H5) Se on se mitä noissa harjoituksissa on tullut esille. [...] [Johto] ei ole välttämättä enää IT-alan ihmisiä. [...] Tilanteet tapahtuvat järjestelmissä mutta ne raportit pitäisi saada [eri organisaatiotasoilla] hyödynnettävään muotoon. [Esimerkiksi]

jos menisi [Ylimmälle johdolle] sanomaan että tässä palomuurissa on nollapäivähaavoittuvuus, niin ei se välttämättä osaa siihen sanoa mitään.

Viestien analysoinnissa on tavoitteena luokitella viestejä, jolloin ne voidaan ”abstraktoida” ja yhdistää eri aihepiireihin. Viestien analysoinnista saatavan hyöty olisi siten viestien luokittelu laajempiin ja yleisemmän tason asiakokonaisuuksiin ja siten mahdollisesti ”teknisen kielen” korreloimisen päätöksentekotason käyttämän kielen kanssa. Tämä mahdollisesti auttaisi päätöksentekijää tarvittavien päätösten hahmottamisessa ja niiden mahdollisten seurausten arvioinnissa. Vaikka pikaviestinjärjestelmällä voidaan levittää myös teknistä tietoa, haastateltavien mukaan päätöksentekotaso ei välttämättä osaa hyödyntää tätä tietoa, koska eivät ole IT-asiantuntijoita. Tarvitaan siis mm. Kuusiston (2014, tiedon jalostamista).

6.3 Valtionhallinnon taso

(H1) ”Se että tieto välittyy nopeasti joka paikkaan, siinä ois se [pikaviestinjärjestelmän] etu.

Sekä haastatteluissa että harjoituksessa tuli esille, että yleisemmällä tasolla poikkeus- ja turvallisuus- ja TKT-toimintaan liittyviä haasteita on sovittujen tai vakiintuneiden käytäntöjen puuttuminen, mikä hankaloittaa tiedonkulkua. Poikkeustilanteissa käytäntöjen puuttumien hankaloittaa myös toiminnan koordinoitua, etenkin Kyberturvallisuuskeskuksen näkökulmasta, jonka tehtäviin koordinoitua kuuluu. Mikäli tarvittavat käytännöt ja toimintatavat saadaan muodostettua, pikaviestinjärjestelmä voisi toimia virtuaalisena ”koontumispaikkana”, josta poikkeustilanteen sidosryhmät ovat tavoitettavissa nopeasti, jolloin tilanteen selvittäminen koordinoitua voidaan aloittaa.

Haastateltavan 3 mukaan nykytilanteessa oikeiden kontaktien ja yhteys henkilöiden löytäminen on ollut ajoittain haastavaa, koska organisaatiokohtaiset yhteyspisteet eivät ole selvillä

[H3] ”meille se voisi toimia osittain semmosena paikkana mistä me saadaan sitä tietoa mitä me lähdetään hakemaan, ettei tarvis lähteä metsästä [SOC-toimijoita] tai jotain muuta vastaavaa jostain puhelimesta tai turvapostilla [...] tai riippuen paikasta muulla tällaisella”

Pikaviestinjärjestelmä voisi näissä tilanteissa nopeuttaa Kyberturvallisuuskeskuksen tilannekuvan keräämisen prosessia, eli tilanteeseen liittyvää ympäristötietoa, tapahtumia ja havaintoja, tapahtumien seurauksia sekä tarvittavia toimenpiteitä.

Pikaviestinjärjestelmä voisi myös toimia organisaatioiden välisen toiminnan koordinaatiovälineenä, ja mahdollisesti jopa yhtenä valtionhallinnon tason johtamistyökaluista, mikäli johtamiskäytännöt ja –hierarkiat saadaan sovittua kuten haastatteluissa todettiin.

(H2) ”Tästä voi tulla työkalu tietynlaiseen johtamiseen, mutta pelisäännöt pitää saada ensin selväksi.”

Toisaalta haastatteluissa todettiin myös, että vakiintuneiden tiedonvaihtokäytäntöjen puuttuminen saattaa johtaa esimerkiksi siihen, että samoja asioita tehdään uudestaan eri valtionhallinnon organisaatioissa, mikä vähentää TKT-toiminnan yleistä tehokkuutta. Tietoturvatieto ja -osaaminen ovat lokeroituneet ja hajautuneet eri henkilöille, vaikka samasta tiedosta voisivat hyötyä myös muut TKT-toimijat ja organisaatiot, jotka työskentelevät saman tavoitteen, valtionhallinnon tieto- ja kyberturvallisuuden eteen. Pikaviestinjärjestelmä saattaisi lisätä vaihtoehtoja tiedon ja osaamisen vaihtoon eri organisaatioiden kesken, olettaen että järjestelmällä on käyttäjiä, jotka käyttävät järjestelmää hyödyllisellä tavalla. Lisäksi haastatteluissa todettiin, että kynnys valtionhallinnon tasolla organisaatioiden väliseen tiedonvaihtoon häiriötilanteista ja niiden seurauksista on suuri, jolloin pikaviestinjärjestelmä saattaisi lisätä häiriötilanteista viestintää organisaatioiden kesken pienentämällä organisaation kokemia esteitä tiedon antamiseen.

(H2) ”Kun puhutaan tietoturvasta ja tieto on lokeroitunutta ja häiriötilanteessa kynnys kertoa muille saattaa olla aika iso. Mutta jos tällä päästään turvallisuusviranomaisten yhteistyöhön ja opitaan toistemme virheistä niin tämä voi olla hyvä tapa vaihtaa tietoa. Voidaan esimerkiksi jakaa tietoa asianomistajille. Keskustelurinki on aina helpompi tapa saada asiantuntijaporukka viestittelemään keskenään. [...] Jos huomataan että tiettyjen keskustelujen määrä [tai] siellä on tiettyjä avainsanoja huomattavasti enemmän niin siitä saadaan tietää trendi ja siihen pystytään reagoimaan koko valtionhallinnon tasolla.”

(H1) : Lähinnä tämä tulisi toimimaan mun käsityksen mukaan tässä vaiheessa siihen että me saadaan tietoa ja pystytään siihen tietoon välittömästi vastaamaan. [...] Esimerkiksi jos [Kyberturvallisuuskeskuksen päivystystoiminto] CERT ilmoittaa uhkasta niin se saa heti tiedon onko meillä havaittu sitä ja me saadaan tieto missä sitä on havaittu ja missä laajuudessa ja pitääkö meidän alkaa toimenpiteisiin [...] siinä voi olla viivettä sähköpostilla hyvinkin paljon [...] [pikaviestinjärjestelmällä] voitaisiin saada tieto jo seuraavalle päivälle [toimenpiteitä tekevälle henkilölle]

Pikaviestinnän analysointi voisi toimia yhtenä menetelmänä laajemman mittakaavan tilannekuvan tuottamisessa, jota voitaisiin jakaa eri organisaatioille, ja parantaa siten mm. Stonen (2016) ja Pitt el al. (2013) korostamaa jaettua tilannetietoisuutta. Laajemmalla tasolla valtionhallinnon TKT-tilannetta tarkkaileville henkilöille analysointityökaluilla voitaisiin mahdollisesti poimia näistä keskusteluista signaaleja, jotka kertovat havaituista poikkeamista, mutta jotka eivät vielä ole laajemmassa tiedossa. Eli tilanteissa joissa kaksi organisaatiota on tehnyt samoja havaintoja mutta eivät ole viestineet siitä toisille. Työkalut voisivat siis toimia tilannekuvajärjestelmänä keskusteluihin, joita eri valtiohallinnon TKT –asiantuntijoiden välillä käydään. Havainnoinnin perusteella jo keskitetty keskusteluiden seuranta voisi merkittävästi auttaa kokonaistilanteen seurannassa, mutta työkalut

voisivat seurannasta aiheutuvaa työkuormaa. Keskusteluja seuraamalla sekä analysointityökaluilla voitaisiin mahdollisesti havaita tieto – ja kyberturvallisuuteen liittyviä ”trendejä” valtionhallinnon organisaatioiden tasolla ja arvioida näiden perusteella onko kyseessä laajempi uhka, kuten esimerkiksi järjestäytynyt toiminta, joka vaatisi laajempia toimenpiteitä ja yhteistyötä.

[H1] [...] jos saadaan esimerkiksi tieto [uhkasta tai poikkeamasta] niin voitaisiin reagoida ennen kuin se tulee meille [...] se antaa etukäteismahdollisuuden reagoida tiettyihin uhkiin [kuten yhteiskunnallisella tasolla vakaviin uhkiin] ja voidaan mahdollisesti valmistautua siihen etukäteen.”

Joissain tapauksissa pikaviestinjärjestelmä voisi siis mahdollistaa jopa ennakkotiedon saamisen häiriötilanteesta, jolloin reagoimiseen tarvittavia toimenpiteitä arvioimiseen ja suunniteluun käytettävissä oleva aika olisi pidempi. Harjoituksessa pikaviestinjärjestelmää käytettiin jonkin verran myös ns. haavoittuvuuskoordinointiin eli uusista haavoittuvuudesta tiedottamiseen ja suositeltavien korjaustoimenpiteiden tai muiden riskiä ehkäisevien käytäntöjen jakamiseen eri organisaatioiden välillä. Tällöin pikaviestinjärjestelmää käytettiin sekä horisontaaliseen että vertikaaliseen, ylhäältä alaspäin suuntautuvaan tiedon vaihtoon.

Mikäli analysoinnilla voitaisiin saada ns. hiljaisia signaaleja eli indikaatiota laajemmista uhkaavista tapahtumista. Tätä tietoa voisivat hyödyttää esimerkiksi virastojen tietohallintopäälliköitä tai muuta valtionhallinnon osana TKT- johtamista toimivaa henkilöä.

(H2) ”Se että kannattaako sitä ulottaa virastojen hallintoon, tietohallintopäälliköille, niin minun mielestä ensisijaisesti ei, koska he ei siitä tiedosta hyödy, vaan se kannattaa olla työkalu josta saadaan toivottavasti kaivettua sellaista signaalitietoa tai analyysitietoa mitä voidaan viedä eteenpäin.”

Näiden hiljaisten signaalien tai trendien avulla voidaan mahdollisesti kehittää organisaatiokohtaista ja valtionhallinnon TKT-toimintaa mikäli niiden perusteella nähdään kehityskohteita tai muutoin tarpeita muutoksille.

Vastaavat haasteet ja asiat myös valtionhallinnon keskeisen toimijan, valtioneuvoston osalta. Haastateltavan 4 näkemyksen mukaan pikaviestinkeskustelun analysointi voisi auttaa Valtioneuvoston Tilannekeskusta yleisen tieto- ja kyberturvallisuuteen liittyvän tilanteen hahmottamisessa. Tilannekeskus ei suoraan hyödy järjestelmässä mahdollisesti käytävästä operatiivisen tason teknisiä yksityiskohtia käsittelevästä keskusteluista, koska heidän tehtäviinsä ei sisälly operatiivinen tieto- ja kyberturvallisuuteen liittyvä toimintaa, kuten haittaohjelmien poistamista. Valtioneuvoston yhteisen TKT-tilannekuvan koostaminen on valtioneuvoston tilannekuvan koostaminen operatiivisella on kuitenkin tilannekeskuksen vastuulla. Tilannekeskus kokoaa myös yleistä valtion turvallisuuden tilannekuvaa valtionjohdolle, mutta ajoittain myös yksityiskohtaisempia selvityksiä. Tähän sisältyvät myös tieto- ja kyberturvallisuuteen liittyvät asiat. Tilannekuvakeskus myös jakaa

tietoturvalisuuuteen liittyviä tiedotteita. Haasteltavan 4 oman työnkuvan näkökulmasta, eli valtioneuvoston käyttämien palveluiden osalta merkittävä vaikutuksia heidän toimintaansa ovat vaikutukset jotka näkyvät palveluiden tuottamisen ja näihin liittyvien työprosessien tasolla. Toisin sanoen, tilannekeskus ja Valtioneuvoston kanslia ovat kiinnostuneita tapahtumista siinä vaiheessa, kun ne vaikuttavat ministeriöiden henkilöstön käyttämien palveluiden saatavuuteen ja käytettävyyteen. Tilannekuvassa on hänen näkemyksensä mukaan kehitettävää:

[H4] [...] niin meillä ei juurikaan ole tilannekuvaa, niinkun valtioneuvoston palveluiden osalta, johtuen [palveluntuottajan] kyvykkyydestä tuottaa sitä tilannekuvatietoa. [Tilannekuva] on tällä hetkellä hyvin reaktiivista.

Haastateltavan 4 mukaan heidän tarvitsemansa tieto ja tilannekuva tulisi vastata tähän haasteeseen, eli valtioneuvoston tietoturvallisuuden johtamisen ennakointikyvykkyyden parantamiseen. Tieto tapahtuneesta poikkeustilanteesta saadaan vasta tilanteen eskaloituttua jolloin päätöksentekoprosessit voidaan aloittaa vasta tilanteen jo käynnistyttyä tai pahimmassa tapauksessa vahinkojen tapahduttua. Valtioneuvoston tilannekeskuksen käsittelemän tiedon tulee hänen mukaansa kuitenkin olla jalostettua, eli siihen tulee sisältyä arviot tilanteen vaikuttavuudesta ja mahdollisista käynnistetyistä toimenpiteistä ja tilanteen etenemisestä.

[H4] Meillehän pitäisi tulla tietoa [esimerkiksi muutoksista verkossa], eli jotain sen tyyppistä mihin pitää pystyä varautumaan [...] esimerkiksi viestinnän tai päätöksenteon kautta. Mut tavallaan sellaista että tekninen kama suodatetaan siitä tietyllä tasolla pois.

Tästä näkökulmasta pikaviestinjärjestelmä voisi parantaa välillisesti valtioneuvoston tietoturvallisuutta parantamalla sen palveluntuottajan ja sidosryhmien tieto- ja kyberturvalisuuuteen liittyvää operatiivista tiedonvaihtoa ja toimintaa. Analysointitoiminta voisi tällöin tuottaa mahdollisesti ennakointia ja varautumista tukevaa tilannetietoa valtioneuvoston tilannekeskukselle jo ennen poikkeustilanteeseen päättymistä. Vastaavasti nämä välilliset vaikutukset ulottuisivat myös palveluiden käyttäjiin, vaikka he eivät voisikaan suoraan hyötyä järjestelmästä.

7. POHDINTA

Tiedon johtaminen tilannekuvan saamiseksi ja tilannetietoisuuden muodostamiseksi on yksi keskeisiä tieto- ja kyberturvallisuuden johtamisen tavoitteita. NIST:n (2014) mallin mukainen TKT –johtaminen asettaa tieto- ja tiedonsiirtotarpeita eri toimijoiden välille, jolloin muodostuu tiedonhallinnallinen haaste, jossa tiedon tarvitsijan ja tuottajan välille tarvitaan tiedonsiirtokanava. Valtionhallinnon TKT –johtamisen tapauksessa tiedon siirtäminen ei ole pelkästään horisontaalista, vaan tarvitaan tiedon jakamista eri organisaatioiden välillä. Organisaatiot voivat sijaita eri hallinnonaloilla, jolloin ne eivät ole kiinteässä yhteistyössä keskenään ja omaavat omilla hallinnonaloillaan päätöksenteko-oikeudet. Tästä huolimatta ja tämän seurauksena tiedon jakamista tarvitaan, jotta yhteisten tietojärjestelmien tilanteessa voidaan tehokkaasti toimia. Normaalioloissa, eli tilanteessa jolloin tietoriski ei ole realisoitunut, TKT- johtaminen vaatii mallin mukaan tiedonkulkua ylhäältä alaspäin, esimerkiksi riskienhallinnan tavoitteista, painopisteistä ja resursseista. Alhaalta ylöspäin tulee tuottaa tietoa esimerkiksi tietoa tietojärjestelmistä ja niiden tilasta sekä näihin liittyvien toimenpiteiden tilanteesta. Näiden lisäksi molemmilla tasoilla tulisi olla ymmärrys fyysisestä toimintaympäristöstä ja tietojärjestelmien tuottamien palveluiden liittymisestä siihen.

7.1 Vaikutukset tietojohdamisen näkökulmasta

Kirjallisuushavaintojen perusteella pikaviestinjärjestelmillä on yleisesti moniulotteisia vaikutuksia ja hyödyntämismahdollisuuksia. Ne ovat yksinkertaisimmillaan kirjoitetun tekstin välittämiseen tarkoitettuja järjestelmiä, joilla on kuitenkin monia eri käyttömuotoja ja vaikutuksia työntekoon. Järjestelmät mahdollistavat uudenlaisia työskentelytapoja niiden tarjoaman reaaliaikaisuuden ansioista, tutkimuksen käyttökontekstissa voivat mahdollistaa jopa organisaatioiden välisiä toimintamalleja tiedonvaihtoon ja toiminnan koordinointiin. Pikaviestinjärjestelmä voi toimia myös sosiaalisen verkostoitumisen välineenä ja ylläpitää jatkuvaa tavoitettavuutta virtuaalisessa työympäristössä. Sosiaalinen verkostoituminen ja sen mukanaan tuoma luottamus voi alentaa kynnystä tiedon jakoon käyttäjien kesken, mahdollisesti jopa organisaatorajojen ylitse. Toisaalta pikaviestinjärjestelmän mahdollistama jatkuva tavoitettavuus voi tuottaa keskeytyksiä ja häiritä siten työntekoa ja laskea sen tehokkuutta. Joidenkin tutkimusten mukaan tiedonvaihdon tehostuminen ja parantuminen henkilöiden kesken ovat kuitenkin suhteessa suuremmat kuin järjestelmän aiheuttamat haitat. (Ou & Davison, 2010)

Yksilö ja tiimitasolla pikaviestintäjärjestelmät edustavat mielenkiintoista viestintämuotoja yhdistävää teknologiaa, sillä ne mahdollistava interaktiivisen ja epämuodollisen, keskustelua muistuttavan kommunikoinnin. Viestinnän epämuodollisuus ja vapaamuotoi-

suus ovat haastattelujen mukaan merkittävä käyttömukavuutta ja käyttöhalukkuutta parantava tekijä. Harjoituksessa pikaviestintä oli kieliasultaan lähempänä yleiskieltä kuin mitä haastatteluiden perusteella olisi ollut odotettavissa. Harjoituksen havaintojen perusteella viestinnän määrämuotoisuudella ja esimerkiksi avainsanojen käyttö kuitenkin parantaisi ja helpottaisi viestinnän analysointia. Tästä johtuen järjestelmän laajemmassa käyttöönnotossa on mahdollisesti tehtävä kompromisseja kieliasun vapaamuotoisuuden ja analysoinnin tehokkuuden välillä. Yleisesti kuitenkin käyttäjien halukkuus käyttää järjestelmää on DeLonen & McLeanin (2003) mukaan merkittävä tekijä järjestelmästä saatavien hyötyjen muodostumiselle. Toinen mahdollinen käyttömukavuutta lisäävä tekijä on pikaviestinjärjestelmän monipuolisuus. Pikaviestinjärjestelmät kirjoitettuun viestintään pohjautuvina ne muistuttavat myös sähköpostia, tarjoamalla mahdollisuuden vastaanottaa ja lukea viesti myöhemmin tai uudestaan jälkepäin. Haastatteluidenkin mukaan pikaviestinjärjestelmä

Kuten tutkimuksen aikaisessa havainnoinnissa sekä mm. Herslebin et al. (2002) tutkimuksessa tuli esille, pikaviestinjärjestelmä tarjoaa nopean ja helppokäyttöisen kommunikointikanavan, joka mahdollistaa opportunistiset, eli välittömät, tilanteen vaatimat keskustelut kasvokkain tapahtuvan työskentelyn tapaan. Pikaviestin loi tilanteita, joissa keskustelu ja viestintä olivat epämuodollista. Tämä tukee Krautin et al. (1990) mukaan yhteistyötä ja –toimintaa sosiaalisten suhteiden muodostumisen kautta. Lisäksi edellä mainituissa tutkimuksissa järjestelmä loi tiimiin kuulumisen tunnetta tavoitettavuuden ja epämuodollisen viestinnän kautta, mikä mahdollisesti lisää yksilöiden halukkuutta osallistua aktiivisesti ryhmän toimintaan. Tutkimuksen kontekstissa pikaviestinjärjestelmä voisi mahdollistaa virtuaalisen ”työtilan”, jonne operatiivisen tason asiantuntijat voivat virtuaalisesti kokoontua, ja tehdä esimerkiksi tiedonhankintaa kysymällä ja keräämällä tietoa muilta asiantuntijoilta. Sekä Krautin et al. (1990) että tämän tutkimuksen empiiristen tulosten mukaan pikaviestinjärjestelmä voisi myös luoda valtionhallinnon tieturva-asiantuntijoiden välistä yhteenkuuluvuuden tunnetta ja siten kannustaa tiedon jakamiseen ja sen pyytämiseen.

Toisaalta pikaviestinjärjestelmä myös nopeuttaa ryhmänlaajuista kommunikointia mahdollistamalla kyselyiden lähettämisen koko tiimille yhdellä kertaa. Vastaavia havaintoja tehtiin myös tutkimuksessa, jossa ainakin harjoitusteknisestä näkökulmasta keskitetty pikaviestinjärjestelmä tehosti ryhmien tiedonvaihtoa laajentamalla tiedon leviämisen aluetta eli mahdollistamalla viestien lähettämisen monelle henkilölle yhtä aikaa. Ominaisuus voi vaikuttaa triviaalilta, mutta tilannekuvan ja jaetun tilannetietoisuuden näkökulmasta sillä voi olla merkittävä tilannetta parantava rooli. Tietojohtamisen työkalujen näkökulmasta pikaviestintäjärjestelmä voisi siis mahdollistaa nopean kaksisuuntaisen ja synkronisen tiedonvaihdon, joko kahden tai useamman osapuolen välillä. Vaikka teknologiana tutkimuksen järjestelmä onkin suhteellisen yksinkertainen ja itsessään se mahdollistaa vain tekstimuotoisten viestien reaaliaikaisen välittämisen käyttäjien välillä, se luo konk-

reettisen ja nopean tiedonvaihtokanavan luomisen, jota vastaavaa ei kaikkien organisaatioiden tietoturvahenkilöstöjen välillä ole ollut. Nykyisellään yhteydenpito tapahtuu pääasiassa sähköpostin välityksellä, mutta pikaviestinjärjestelmän avulla käyttäjät voisivat kaksisuuntaisen kommunikointimahdollisuuden avulla pyrkiä nopeuttamaan tiedon saantia ja vaikuttamaan saamansa tiedon laatuun ja kattavuuteen esimerkiksi tarkentavilla kysymyksillä.

Järjestelmän kehityksessä ja käyttöönotossa on huomioitava, että käyttäjien halukkuuteen käyttää järjestelmää, ja jakaa sen avulla tietoa, vaikuttaa järjestelmän käyttäjien lukumäärä, kuten esimerkiksi Feledi & Fenz (2012) havaitsivat tutkimuksessaan. Siinä he havaitsivat, että web-pohjaisten yhteistyövälineiden käyttöön, myös turvallisuusteemaan keskittyvien, vaikuttaa oleellisesti nk. kriittinen massa. Vähäinen käyttäjämäärä vähentää halukkuutta tiedon jakamiseen, koska siitä saatavat hyödyt ovat vähäisemmät. Tällöin myös uusien käyttäjien halukkuus liittyä järjestelmän käyttäjäksi on vähäisempi. Tämä on erityisen tärkeää huomioida tutkimuskohteena olevan järjestelmän tapauksessa, koska sen tuottama lisäarvo on sidoksissa sen käyttöasteeseen ja käyttäjien siihen tuottamaan tietoon.

Organisaatiotasolla ja organisaatioiden välisellä tasolla pikaviestinjärjestelmä voisi mahdollisesti vaikuttaa Yang & Maxwellin (2011) kuvassa 9 ja ENISA:n (2010) taulukoissa 2 ja 3 esittämiin tiedon jakamiseen vaikuttaviin tekijöihin, lisäämällä kannustimia ja vähentämällä sosiaalisia ja organisaationallisia esteitä. Positiivisen tiedonvaihtokulttuurin syntyminen valtionhallinnon operatiivisten tietoturva-asiantuntijoiden välille voisi lisätä tieto- ja kyberturvallisuuteen liittyvän tiedon jakamista, joten tutkimuksen kohteena olevan pikaviestinjärjestelmä voi teoreettisesti lisätä henkilöiden välistä tiedon vaihtamista ja jakamista, sillä se tarjoaa mahdollisuuden sosiaalisten verkostojen luomiseen henkilöiden välillä. Järjestelmän suunnitellut käyttäjät työskentelevät eri organisaatioissa, jolloin se tarjoaa mahdollisuuden organisaatorajat ylittävään verkostoitumiseen ja siten positiivisesti tiedonvaihtoon suhtautuvan kulttuurin luomiseen organisaatioiden välillä. TKT-johtamisen näkökulmasta järjestelmä voi täten parantaa valtionhallinnon eri organisaatioissa työskentelevien tietoturva-asiantuntijoiden, eli riskienhallintamallin toteuttavan tason verkostoitumista tarjoamalla kanavan epämuodolliseen ja vapaamuotoiseen kommunikointiin ja yhteistyöhön. Epämuodollisella viestinnällä on Oun et al. (2011) mukaan merkittävä rooli verkostoitumisen edistäjänä. Verkostoitumisen ja hyvien sosiaalisten suhteiden positiivisista vaikutuksista henkilötason suhtautumiseen tiedon jakamiseen on saatu viitteitä Chowin & Chanin (2008) tutkimuksessa, jossa he havaitsivat, että sosiaalisilla verkostoilla oli vaikutuksia tiedon jakamiseen vaikuttaviin asenteisiin.

Toisaalta pikaviestin ei pelkästään luo viestintävälineenä mahdollisuutta tiedon vaihtoon, vaan tarjoaa mahdollisuuden myös tiedonvaihdosta sopimiseen ja neuvotteluun sekä tiedonvaihtoprosessien ohjaamiseen. Pikaviestimen avulla voidaan tiedustella esimerkiksi vastaanottajan saavutettavuutta ja neuvotella tiedonvaihdon yksityiskohdista, kuten tiedon formaatista ennen tiedon siirtämistä. Nämä ovat Nardin et al. (2000) mukaan tärkeitä

tiedonvaihtoprosessin vaiheita, jotka edesauttavat yhteyden muodostamista, mikä johtaa tiedonsiirtoon. Pikaviestinjärjestelmien synkroninen viestintä tarjoaa mahdollisuuden viestinnän varmistukseen ja siten parantaa kahden eri osapuolen välisestä viestinnästä riippuvaisten prosessien onnistumisen todennäköisyyttä. Harjoituksessa pikaviestinjärjestelmää käytettiin usein esimerkiksi sähköpostin välityksen onnistumisen varmistamiseen eli varmistuskinona sille, että tiedon lähetys ja vastaanotto onnistuivat. Täten pikaviestinjärjestelmä toi eräänlaista redundanssia kommunikointivälineisiin ja kommunikoinnin onnistumisen varmistukseen ryhmien välillä.

ENISA:n (2010) tutkimuksessa kolmanneksi merkittävin tekijä tiedon vaihdon halukkuudelle on luottamuksen rakentaminen. Pikaviestinjärjestelmä voisi mahdollisesti myös poistaa tai vähentää vähäisestä luottamuksesta tai sen puuttumisesta syntyviä esteitä tiedon jakamiselle. Organisaatorajat ylittävä pikaviestinjärjestelmä mahdollistaisi virtuaalisen ”kokoontumispaikan” ja tukisi mahdollisesti luottamusverkoston syntymistä. Luottamusverkoston tarpeellisuus on tunnistettu ja sitä on muodostettu myös muilla tavoin osana tutkimukseen liittyvää hanketta (Janhunen, 2015). Pikaviestintä on myös mm. Oun et al. (2010) ja Oun & Davisonin (2010) havaintojen mukaan lisännyt verkostoitumista ja siten käyttäjien välisen luottamuksen lisääntymistä. Toisaalta myös tiedon jakamisesta aiheutuvien mainehaittojen riski voi olla pienempi, mikäli järjestelmä toteutetaan suljettussa ja luotettavassa ympäristössä, koska tällöin negatiivisten asioiden päätyminen julkisuuteen on epätodennäköisempää kuin virallisten kanavien kautta toimittaessa. Näiden lisäksi tutkimuksen kontekstin pikaviestinjärjestelmä tarjoaisi ainakin asiantuntijoille pääsyn etuoikeutettuun tietoon muilta viranomaisilta luotettavassa ympäristössä, mikä ENISA:n (2010) tutkimuksessa nousut esille keskimääräisen kannustavana tekijänä tiedonvaihtoon. Tutkimuksessa mukana olleet edustivat pääosin yksityisen sektorin toimijoita, mutta tämän tyyppinen kannustin voisi toimia myös julkishallinnon organisaatiolle.

Viestiliikenteen analysointi on TKT-kontekstissa uusi tapa tuottaa toistaiseksi hyödyntämättömästä tietomassasta hyödynnettävää tietoa. Hajautetussa toimintamallissa ja –ympäristössä eri järjestelmät, niiden tuottamat palvelut ja tarvittavat muut tiedot ovat eri puolilla valtionhallintoa jolloin TKT-kontekstissa tilannekuvan kerääminen analysoitavaksi voi olla haastavaa. Viestinnän analysointi voi osittain vastata tähän tarjoamalla näkyvyyttä eri toimijoiden ja niiden järjestelmien tilanteeseen. Keskitetyllä pikaviestinjärjestelmällä ja sen analysoinnilla voitaisiin valtionhallinnon TKT-johtamisessa tuottaa eräänlaista tilannekuvaa ilman suuria ja mahdollisesti haastavia teknisiä integraatioita eri organisaatioiden välille. Lisäksi analysoitava tietomassa on jo jossain määrin jalostettua tietoa, koska se on valtionhallinnon tietoturva-asiantuntijoiden tuottamaa. Analysoinnilla voitaisiin siis tuottaa tilannekuvaa ja tukea siten tilannetietoisuuden muodostumista. Analysoinnilla tuotettava tilannekuva riippuu keskustelujen sisällöstä. Huomioitavaa on myös, että pelkän analysoitavan tiedon tuottaminen ei kuitenkaan riitä, vaan tarvitaan tiedon levittämiseen määritellyt hyödyntäjät, prosessit ja menetelmät. Lisäksi tarvitaan muut

tätä toimintaa tukevat järjestelmät, jotka soveltuvat pikaviestintää paremmin suurempien datamassojen, kuten esimerkiksi tietojärjestelmien inventaariotiedon, välittämiseen.

Kuten todettua, TKT-kontekstissa päätöksentekijöiden ja operatiivisten toimijoiden välillä voi olla ns. ”kielimuuri”. Operatiiviset toimijat käyttävät termistöä ja sanoja, joita päätöksentekotason henkilöt eivät ymmärrä. Ongelman ratkaisemiseksi tarvittaisiin joko päätöksentekijöiden ymmärryksen lisäämistä tai menetelmän jolla viestintä yhdistetään päätöksentekijöiden osaamiseen. Analysointityökalut ja sanojen luokittelu ja kategorisointi voisivat ehkä toteuttaa osittain molempia yhdistämällä viestimässään viestejä ehkä tunnetumpiin termeihin. Analysointitoiminnalla voitaisiin tuottaa jalostetumpaa tietoa, jos esimerkiksi yhdistetään havaintoon tietoja havainnon vakavuudesta. Toisaalta mikäli kyseessä on yksinkertainen tapaus, voisi esimerkiksi riittää että operatiivisten asiantuntijoiden käyttämät termit ”käännetään” yleiskielelle.

7.2 Poikkeustilanteisiin liittyvät haasteet ja vaikutukset niihin

Tutkimuskohteella on edellytyksiä tuottaa tilannekuvaa sekä yksilötasolla että valtionhallinnon TKT-johtamisen näkökulmasta. Poikkihallinnollisissa poikkeustilanteissa valtionhallinnon tieto- ja kyberturvallisuuden johtaminen eli tilannejohtaminen vaatii sen eri sidosryhmiltä riittävää tilannetietoisuutta siitä ympäristöstä ja sen tapahtumista, joista tilanne muodostuu. Pikaviestinjärjestelmä mahdollistaa tiedon jakamisen ainakin toimenpiteitä toteuttavalla tasolla, mikä voi edesauttaa yhteistä tilannetietoisuutta, sillä jaetun tilannetietoisuuden ja konsensuksen saavuttaminen useamman toimijan kesken on riippuvainen kommunikoinnista (Salas et al. 1995). Pikaviestinjärjestelmä voi mahdollisesti luoda ja parantaa yhteistä tilannekuvaa riskienhallinnan operatiivisella tasolla tarjoamalla mahdollisuuden keskusteluun ja tiedonvaihtoon toimintaan osallistuvien toimijoiden kesken. Suunnitelluilla analysointityökaluilla tilannetietoa voidaan tuottaa myös päätöksentekotasolle.

Luvussa 3 tutkituista viestintävaihtoehdoista sähköpostiliikenteen analysointi olisi myös mahdollista, ottaen huomioon sähköpostin pikaviestintää lähtökohtaisesti pidemmän viestinnän aikaikkunan. Faksit ovat verrattain vähäisessä käytössä eivätkä ole pikaviestintään verrattavissa oleva nykyaikainen ratkaisu. Puheen analysointi ja esimerkiksi luokittelu aiheen mukaan ei ole nykyisillä teknologisilla ratkaisuilla kannattavaa ja kasvokkain tapahtuvan kommunikoinnin analysointiin tarvittaisiin erillinen henkilö tai laite läsnä keskustelutilassa. Pikaviestinnän analysoinnin hyödyt voisivat siis tulla esiin etenkin aikakriittisissä, eli nopeaa päätöksentekoa vaativissa tilanteissa, joissa ei välttämättä ole aikaa formaaleihin menettelyihin tiedon saamiseksi. Haastatteluiden mukaan on usein tilanteita, joissa päätöksentekijät haluavat tietoa välittömästi tai ainakin mahdollisimman pian. Näissä tilanteissa raportin ei tarvitse olla erityisen kattava tai yksityiskohtainen, riittää että sen avulla saadaan alustava käsitys ja tilannetietoisuus poikkeustilanteesta. Eli tilanteissa joissa vaaditaan raportti hyvin nopeasti, yksi mahdollisuus olisi toteuttaa rat-

kaisu, joka tuottaa eräänlaisen ”pikaraportin” keskusteluissa esiintyneiden asioiden, kuten avainsanojen, pohjalta, ja siten tukea päätöksentekijöiden tueksi. Pikaviestinnän analysointi voisi auttaa ja nopeuttaa myös laajempien uhkien tai poikkeamatilanteiden vaatimaa ylemmälle taholle raportointia tuottamalla kontekstietoa, luokittelemalla keskusteluviestejä kategorioihin ja poimimalla keskusteluista muuta tilanteeseen liittyvää tietoa. Harjoituksen havaintojen mukaan tämä kontekstietä on usein merkittävä osa päätöksentekoa.

Pikaviestinjärjestelmä avulla voitaisiin havaintojen mukaan myös tuottaa ja muuhun tilannekuvaan liittää toimintaympäristöön liittyvää tietoa, mikä on tärkeää, jotta ymmärrettään kyberympäristön riskien ja toimenpiteiden vaikutukset fyysisessä maailmassa. Kyberturvallisuusharjoituksessa havaittiin useitakin tilanteita, joissa tulevat fyysisen maailman vaikutukset vaikuttivat toimenpidemahdollisuuksiin ja siten päätöksiin ”kybermaailmassa”. Havainnot tukevat sekä Franke & Bryenilssonin (2014) että Badford et al. (2013) argumentteja toimintaympäristötiedon merkityksellisyydestä tilannekuvassa sekä tilannetietoisuuden muodostamisessa. Tältä osin pikaviestinjärjestelmä ja analysointitoiminta voisivat parantaa yleisesti kyberavaruuden ja fyysisen toimintaympäristön tilannetietoisuuden muodostamista.

Vakavat, eli poikkihallinnolliset, normaalia nopeampaa reagointia ja tilannejohtamista vaativat vakavat tieto- tai kyberturvapoikkeamat saattaisivat vaatia aktiivisen, operatiivista päätöksentekoa tekevän ryhmän perustamista. Tällaisissa tilanteissa pikaviestinjärjestelmä voi mahdollistaa nopeasti käyttöönotettavan viestintätyökalun ja tukea yhteistyö- ja koordinointiin liittyvien prosessien käynnistämistä. Pikaviestinjärjestelmällä voisi siis olla rooli operatiivisessa johtamisessa. Pelkkä tekstimuotoinen viestintä voi kuitenkin asettaa rajoitteita viestinnän tehokkuudelle, kuten Knott et al. (2006) havaitsivat koekeskelmassa, jossa pikaviestintäjärjestelmä muodosti operatiivista ja aikakriittistä päätöksentekoa vaativassa tilanteessa ryhmätason yhteistyö- ja koordinointityökalun. Pikaviestinjärjestelmää käytettiin joko yksistään tai yhdessä puheyhteyden mahdollistavan järjestelmän kanssa. Käyttötilanteet olivat hyvin intensiivisiä skenaarioharjoituksia. Ryhmätasolla tarkasteltaessa he havaitsivat, että aikakriittisessä päätöksenteossa ja konsensuksen muodostamisessa pelkkään tekstimuotoiseen kommunikaatioon perustuva viestintä ei ollut yhtä tehokas kuin reaaliaikainen puheyhteys. Molempien yhdistelmä oli tehokkaampi yhteistyöväline kuin pelkkä teksti kuitenkaan merkittävästi eroamatta pelkästä puheeseen perustuvasta järjestelmästä. Knott et al. (2006) tutkimuksen pikaviestinjärjestelmän käyttökonteksti on erilainen kuin tässä tutkimuksessa tarkasteltavan järjestelmän, mutta mahdollisuudet vastaavaan käyttötapaukseen ovat olemassa ja pikaviestinjärjestelmä voisi tukea vastaavaa toimintaa.

Myös haastatteluiden perusteella pikaviestinjärjestelmä olisi mahdollisesti toimintaa tukeva viestintäväline, jonka suurin lisäarvo tulisi sen mahdollistamasta reaaliaikaisesta kahdensuuntaisesta viestinnästä. Järjestelmän tuottama lisäarvo on siis suhteessa sen avulla tavoitettaviin henkilöihin ja organisaatioihin. Järjestelmän käyttöönoton ei nähty

merkittävästi muuttavan TKT-toimintaan liittyviä työprosesseja, joihin on jo pääsääntöisesti olemassa muut järjestelmät. Järjestelmän tarjoamat hyödyt ovatkin pääosin operatiivisella tasolla tiedon jakamisessa, pääasiassa asiantuntijaverkoston eli riskienhallinnan toimenpiteitä suorittavan tason kesken. Levitettävää tietoa voisi olla mitä tahansa TKT-tilannekuvaan liittyvää tietoa, pääpainon ollessa haastatteluiden perusteella uhkatiedossa, kuten esimerkiksi haavoittuvuusjulkaisuista tiedottamisessa. Tämä voi strategisella tasolla parantaa valtionhallinnon tietoturvallisuuden kokonaistilannetta, jos organisaatio ja niiden asiantuntijat voivat järjestelmällä välitetyn tiedon ansiosta nopeammin reagoida TKT-poikkeustilanteisiin. Lisäksi järjestelmä mahdollistaisi asiantuntijoiden verkostoitumisen ja verkostojen ylläpitämisen, mikä voisi alentaa kynnystä tiedon vaihtoon ja tiedosta saatavan lisäarvoin jakamiseen muille käyttäjille ja organisaatioille.

Pikaviestin järjestelmän lopulliset vaikutukset realisoituvat lopullisten käyttötapojen ja mahdollisten uusien toimintamallien vakiinnuttua. Tämä riippuu kuitenkin monesta tekijästä jotka saattavat asettaa haasteita järjestelmän hyödyntämiselle. (Herbsleb et al. 2002) tutkimuksessa havaittiin että pikaviestinjärjestelmän integroimiseen organisaatioihin liittyy esimerkiksi seuraavia haasteita: Uusille käyttäjille saattoi olla vaikeaa perustella pikajärjestelmään siirtyminen, kun heillä oli jo vakiintuneet kommunikointitavat, kuten sähköposti. Järjestelmä saatettiin tuoda tilanteeseen, jossa sille ei ollut tarkasti määriteltyä käyttötarvetta tai tehtävää. Vastaavia seikkoja on huomioitava myös pikaviestinjärjestelmän käyttöönotossa. Tärkeää on myös ns. kriittisen massan saavuttaminen eli sen varmistaminen että järjestelmällä on riittävästi käyttäjiä jotta sen käyttö nähdään kannattavana. Toisaalta myös on otettava huomioon Yang & Maxwellin (2010), ENISA:n (2010) ja Felendin & Fenzin (2012), esittämät joko kannustimina tai esteinä toimivat tekijät, jotka vaikuttavat myös pikaviestinjärjestelmän avulla tapahtuvaan tiedon jakamiseen. Osa tekijöistä, kuten järjestelmän riittävän hyvä hallinnointi, on järjestelmän tuottajan vastuulla, mutta toisaalta osa tekijöistä on riippuvainen käyttäjistä. Esimerkiksi tiedon laatu ja hyödynnettävyys riippuvat käyttäjistä, sillä tieto pääosin käyttäjien tuottamaa. Tähän on kiinnitettävä huomiota kun käyttäjiä ohjeistetaan ja järjestelmää otetaan laajempaan käyttöön.

8. YHTEENVETO

Valtionhallinnon tieto- ja kyberturvallisuuden johtaminen ja siihen liittyvä tietojohdaminen ovat olleet Valtiovarainministeriön SecICT –hankkeen myötä voimakkaassa kehityksessä. Tässä tutkimuksessa täydennettiin tätä kokonaisuutta tarkastelemalla siihen liittyviä toiminnallisia ja tiejohtamisen haasteita sekä mahdollista yhtä ratkaisuvaihtoehtoa näiden haasteiden ratkaisemiseen. Tutkimuksessa tarkasteltiin valtionhallinnon organisaatioiden tieto- ja kyberturvallisuusasiantuntijoiden, eli TKT-asiantuntijoiden väliseen viestintään suunniteltua pikaviestinjärjestelmää ja sen sisältämän viestinnän analysointia. Tutkimuksessa kerättiin ja analysoitiin eri sidosryhmien näkemyksiä pikaviestinjärjestelmän ja viestinnän analysointitoiminnan mahdollisuuksista ja hyödyistä. Tutkimuksessa päästiin myös havainnoimaan yhden, melkein vastaavassa roolissa toimivan pikaviestinjärjestelmän käyttöä valtionhallinnon TKT-toiminnassa Kansallisessa Kyberturvallisuus-harjoituksessa

8.1 Keskeiset havainnot ja päätelmät

Organisaatorajat ylittävä pikaviestinjärjestelmä ja sen tueksi toteutettavalla viestinnän analysointi tarjoavat uudenlaisen mahdollisuuden valtionhallinnon organisaatioiden väliseen yhteistyöhön ja näkyvyyteen yleiseen valtionhallinnon TKT-tilanteeseen. Pikaviestinjärjestelmä mahdollistaa eri organisaatioiden TKT-asiantuntijoiden välisen tiedonvaihdon ja tuottaen samalla tietoa poikkihallinnolliselle analysointitoiminnalle, jotka käsittelevät laajempaa häiriötilanteeseen liittyvää tietoa. Pikaviestinnän analysointitoiminta voisi siis mahdollistaa valtionhallinnon riskienhallinnan päätöksentekotasolle havainnointimenetelmän operatiivisen tason toiminnassaan käytyihin keskusteluihin ja siten sillä hetkellä valitsevaan TKT-tilanteeseen, olettaen että keskustelut käsittelevät tilannetta. Eli analysointityökalut voisivat toimia ”tilannekuvajärjestelmänä” keskusteluihin ja siten yhtenä menetelmänä kokonaistilanteeseen. Keskustelut voivat sisältää esimerkiksi laajempia tietovuotohavaintoja, jolloin ne voivat olla koordinoituja toimenpiteitä vaativia tapahtumia. Täten pikaviestinjärjestelmä ja analysointitoiminta voivat parantaa tilannetietoisuutta sekä riskienhallinnan hallinnollisella että operatiivisella tasolla. Toisaalta jo pelkkä organisaatorajat ylittävä keskitetty pikaviestinjärjestelmä toisi uusia mahdollisuuksia asiantuntijoiden väliseen yhteistyöhön ja mahdollisesti heidän väliseen verkostoitumiseen, mikä voisi kannustaa aktiivisempaan vuoropuheluun ja tiedon jakamiseen. Pikaviestinjärjestelmä voisi myös tehostaa ja tuoda parempia työvälineitä päivittäiseen yhteydenpitoon tarjoamalla valtionhallinnon TKT-toimijoille keskitetyn yhteyspisteen.

Harjoituksessa nousi esille samoja haasteita organisaatioiden välisessä yhteistoiminnassa. Organisaatorajat ylittävä pikaviestinjärjestelmä tarjosi nopeasti käytettävissä olevan

viestintävälineen eri organisaatioiden asiantuntijoille, mikä tehosti merkittävästi heidän välistä yhteistyötä. Vastaavasti pikaviestinnän analysointi tarjosi harjoituksen johdolle, joka eräällä tapaa edustaa myös päätöksentekotahoa todellisessa tilanteessa, hyvän kuvan harjoituksessa mukana olleiden ryhmien toimintaan. Tehdyt havainnot tukevat käsitystä järjestelmän hyödyllisyydestä yhtenä menetelmänä valtionhallinnon tason tilannekuvan muodostamisessa.

Pikaviestinjärjestelmää itsessään ei ole suunniteltu valtionhallinnon ja sen organisaatioiden TKT-kokonaisuuden operatiivisten haasteiden ratkaisemiseen, sillä pikaviestinjärjestelmällä tai pikaviestintään perustavalla analysointitoiminnalla ei tuota suoraan teknistä tietoa tai kontroleja yksittäisen organisaation sisäiselle TKT –toiminnolle. Pikaviestinjärjestelmä ja viestinnän analysointi eivät siis korvaa muita tietolähteitä tai toiminnassa käytettäviä järjestelmiä. Pikaviestintään osallistuvat määrittelevät lopulta, kuinka järjestelmää tullaan käyttämään. Kun kyseessä on viestintäväline, sen hyödyntämisen näkökulmasta on oleellista, millaista tietoa sen avulla jaetaan ja missä tilanteissa sitä käytetään.

8.2 Tutkimuksen arviointi ja jatkotutkimusehdotukset

Pikaviestinjärjestelmät ovat pääosin suunnattu organisaatioiden sisäiseen käyttöön, joten suoraan pikaviestinjärjestelmän vaikutuksia organisaatioiden välisellä tasolla tarkastelevaa tutkimusta ei kirjallisuudesta tutkimuksessa löydetty. Toisaalta organisaatorajat ylittävä pikaviestinjärjestelmä ja etenkin pikaviestinnän analysointi TKT- kontekstissa on verrattain uusi tutkimusalue, minkä toteavat myös Puuska et al. (2016). Täten laajempaa empiirisiä validointia esitetyille teorioille siitä, että pikaviestinjärjestelmällä olisi vaikutusta organisaatioiden väliseen tiedonvaihtoon, ei löydetty. Järjestelmä tarjoaa mahdollisuuden asiantuntijatasoisen kommunikointiin, mutta tästä ei voida tehdä suoraa johtopäätöstä tiedonvaihdon parantumisesta. Tulosten verifiointiin tarvittaisiin yksityiskohtaisempia mittareita tiedonvaihdon paranemisesta. Tutkimuksessa haastatellut henkilöt kuitenkin toivat esille pääosin samoja asioita, joita kirjallisuudessa on tutkittu organisaatioiden väliseen tiedonvaihtoon liittyen, joten mittareita voitaisiin muodostaa. Niitä ei kuitenkaan tämän tutkimuksen resurssien puitteissa voitu muodostaa. Näistä syistä johtuen tutkimus on luonteeltaan kartoittava, kuin mittaava tai asioita todentava.

Tutkimuksessa tehdyt haastattelut ja haastateltavien lukumäärä olivat verrattain suppea, joskin tilannetta paransi mahdollisuus havainnointiin suhteellisen hyvin oikeaa tilannetta vastaavassa harjoituksessa. Havainnot harjoituksesta tukevat sekä haastatteluita että kirjallisuudessa esitettyjä näkemyksiä pikaviestinjärjestelmien monista mahdollisuuksista viestintävälineenä. Tutkimuksessa yhdistettiin pikaviestimiin ja tiedonvaihtoon liittyvää tutkimusta tieto- ja kyberturvallisuuden kontekstiin. Tutkimus muodostaa yhden, kerättyyn tutkimusaineistoon pohjautuvan näkemyksen tutkimuskohteen vaikutuksista valtionhallinnon TKT-johtamiseen ja sen kehittämiseen. Mikäli tutkimuksessa olisi painotettu esimerkiksi käyttäjätasoa tai yksittäistä organisaatiota, olisivat tulokset eli arvioidut vaikutukset todennäköisesti olleet hieman erilaiset.

Aihealueeltaan, erityisesti tilannekuvan keräämisen ja tilannetietoisuuden muodostamisen osalta, tutkimus on valtionhallinnon tieto- ja kyberturvallisuuden johtamisen keskiössä. Asian tärkeydestä myös yleisesti kertoo se, että tilannekuvaa on tutkittu monessa eri yhteydessä ja sen jakamisen kehittämiseksi on perustettu organisaatioita kuten MACCSA. Toisaalta on huomioitava, että tieto- ja kyberturvallisuuteen liittyvien poikkeustilanteiden johtamisen haasteet eivät välttämättä juurikaan eroa muista poikkeustilanteista ja asiaa on jo tutkittu eri näkökulmista useiden vuosien ajan. Näitä tutkimuksia hyödyntämällä voitaisiin tieto- ja kyberturvallisuuteen liittyvää poikkeustilannetoimintaa kehittää kokonaisvaltaisemmin. Tässä tutkimuksen puitteissa tuli esille esimerkiksi verkostoitumisen, kommunikoinnin ja tiedonvaihdon merkitys ja siihen liittyvät haasteet eli pääosin tiedonvaihdon puuttuminen. Näitä samoja haasteita on tuonut esille jo 2000-luvun alkupuolella esimerkiksi Yliniemi (2004) diplomityössään, jossa tutkittiin päätöksentekoa kriisitilanteissa Puolustusvoimien näkökulmasta. Tästä voidaan päätellä, että ongelmakenttä ei sinänsä ole uusi, ja haasteet ovat ainakin pääpiirteissä tunnistettu, mutta niitä ei pystytty ainakaan kokonaisuutena ratkaisemaan. Tämä antaa viitteitä ongelmanratkaisun vaativuudesta. Tästä lähtökohdasta yhdenkin osa-alueen, kuten tässä tapauksessa asiantuntijoiden välisen tiedonvaihdon parantamisella voi olla merkitystä tilanteen parantamiseksi. Pikaviestinjärjestelmällä on tutkimuksessa haastateltujen henkilöiden mielestä teknologisenä ratkaisuna potentiaalia kehittää tiedon jakamista organisaatioiden sisällä ja niiden välillä. Toisaalta strategisen TKT-johtamisen työkaluksi suunnitelluilla pikaviestinnän analysointityökaluilla ja –toiminnalla TKT-toimintaa ohjaava ja johtava taso voi havaita signaaleja TKT-tilanteen muutoksista ja saada paremman näkyvyyden asiantuntijaverkoston ja asiantuntijoiden edustaminen organisaatioiden tilanteeseen.

Jatkokehityksen voitaisiin esimerkiksi lähteä edelleen kehittämään pikaviestinjärjestelmän käyttötapoja ja siihen liittyviä toimintatapoja siten, että ne paremmin tukisivat valtionhallinnon tieto- ja kyberturvallisuuden johtamista. Haastatteluissakin mainittuja kehityskohteista ovat järjestelmän käyttötavat ja siihen liittyvät prosessit sekä yleisesti pikaviestinjärjestelmän roolin määrittely ja vakiinnuttaminen. Lisäksi voitaisiin tutkia yhtenä vaihtoehtona pikaviestinjärjestelmän integrointia muihin järjestelmiin, jolloin kohteena voisi olla esimerkiksi Kansallisessa kyberturvallisuusharjoituksessa implementoitu ”pikaraportointijärjestelmä”, ja sen hyödyntäminen. Toisaalta mielenkiintoisia tutkimusalueita voisivat olla esimerkiksi analysointityökalujen jatkokehitys tai esimerkiksi viestiliikenteen visualisointi, joita Kyberturvallisuusharjoituksessa alustavasti pilotoitiin. Yleisellä tasolla tieto- ja kyberturvallisuuden tilannekuva ja sen visualisointi ovat kohtalaisen nuoria tutkimuskenttiä, joten niiden jatkotutkimus olisi varmasti hyödyllistä. Huomioitava on kuitenkin, että järjestelmien kehittäminen on vain osa kokonaisuutta, tarvitaan myös toimintatapojen ja prosessien tutkimista ja kehittämistä.

LÄHTEET

- Aaltola, J. & Valli, R. (2010). Ikkunoita tutkimusmetodeihin. 1, Metodien valinta ja aineiston keruu: virikkeitä aloittelevalla tutkijalla. 3rd ed. Jyväskylä, PS-kustannus, 2010 WS Bookwell. 312 s.
- Abrams, L. C., Cross, R., Lesser, E., & Levin, D. Z. (2003). Nurturing interpersonal trust in knowledge-sharing networks. *The Academy of Management Executive*, 17(4), s. 64-77.
- Adams, P.H. & Martell, C.H. (2008). Topic detection and extraction in chat, *Semantic Computing*, 2008 IEEE International Conference on, IEEE, s. 581-588.
- Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R. & Zajicek, M. (2004). Defining incident management processes for csirts: A work in progress, *Networked Systems Survivability Program*.
- Barford, P., Dacier, M., Dietterich, T.G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P. & Ning, P. (2010). Cyber SA: Situational awareness for cyber defense, in: *Cyber Situational Awareness*, Springer, s. 3-13.
- Baskerville, R., Spagnoletti, P. & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response, *Information & Management*, Vol. 51(1), s. 138-151.
- Bengel, J., Gauch, S., Mittur, E. & Vijayaraghavan, R. (2004). Chattrack: Chat room topic detection using classification, in: *Intelligence and Security Informatics*, Springer, s. 266-277.
- Borum, R., Felker, J., Kern, S., Dennesen, K. & Feyes, T. (2015). Strategic cyber intelligence, *Info and Computer Security*, Vol. 23(3), p. 317-332.
- Chow, W.S. & Chan, L.S. (2008). Social network, social trust and shared goals in organizational knowledge sharing, *Information & Management*, Vol. 45(7), s. 458-465.
- CNSS (2015). Committee on National Security Systems (CNSS) Glossary, (CNSSI No. 4009)
- Delone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. *Journal of management information systems*, 19(4), s. 9-30.
- Dong, H., Cheung Hui, S. & He, Y. (2006). Structural analysis of chat messages for topic detection, *Online Information Review*, Vol. 30(5), s. 496-516.
- Edson dos, S.M., Luciana Andréia, F.M., Antonio José dos, S.B. & Mauro César Bernardes (2008). Ontologies for information security management and governance, *Info Management & Comp Security*, Vol. 16(2), s. 150-165.
- Endsley, M.R. (2000). Theoretical underpinnings of situation awareness: A critical review, *Situation awareness analysis and measurement*, s. 3-32.
- Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems, *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 37(1), s. 32-64.
- ENISA (ed.). 2010. Good Practice Guide for Incident Management. European Union Agency for Network and Information Security. 10 s.
- ENISA (2010). Incentives for Information Sharing.

- Feledi, D. & Fenz, S. (2012). Challenges of web-based information security knowledge sharing, Availability, Reliability and Security (ARES), 2012 Seventh International Conference on, IEEE, s. 514-521.
- Fenz, S., Heurix, J., Neubauer, T. & Pechstein, F. (2014). Current challenges in information security risk management, *Information Management & Computer Security*, Vol. 22(5), s. 410-430.
- Garrett, R.K. & Danziger, J.N. (2007). IM= Interruption management? Instant messaging and disruption in the workplace, *Journal of Computer-Mediated Communication*, Vol. 13(1), s. 23-42.
- Gragido, W. (2012). Understanding Indicators of Compromise (IOC) Part 1, RSA blog, [Viitattu 25.5.2016]. Saatavilla: <http://blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i/>.
- Haller, J., Merrell, S.A., Butkovic, M.J. & Willke, B.J. (2010). Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability. Carnegie-Mellon University, Software Engineering Institute. Pittsburgh, USA.
- Handel, M. & Herbsleb, J.D. (2002). What is chat doing in the workplace? Proceedings of the 2002 ACM conference on Computer supported cooperative work, ACM, s. 1-10.
- Hernandez-Ardieta, J.L., Tapiador, J.E. & Suarez-Tangil, G. (2013). Information sharing models for cooperative cyber defence, *Cyber Conflict (CyCon)*, 2013 5th International Conference on, s. 1-28.
- Hirsjärvi, S. & Hurme, H. (2011). Tutkimushaastattelu - Teemahaastattelun teoria ja käytäntö, Gaudeamus Helsinki University Press, Oy Yliopistokustannus, HYY yhtymä, Helsinki, 213 s.
- Holmgren, P. (2016). "Pelkästä tietoturvallisuudesta ei enää seuraa kyberturvallisuutta". Käsiteanalyysi kyberturvallisuudesta. Viestintätieteiden pro gradu -tutkielma. Vaasan Yliopisto.
- Husain, M.I. & Sridhar, R. (2009). iForensics: forensic analysis of instant messaging on smart phones, in: *Digital forensics and cyber crime*, Springer, s. 9-18.
- ISO/IEC, 2008. ISO/IEC 27005:Tietoturvariskien hallinta. Suomen Standardoimisliitto SFS RY, International Standardization Organization, International Electrotechnical Commission.
- J. Pitt, A. Bourazeri, A. Nowak, M. Roszczyńska-Kurasinska, A. Rychwalska, I. Rodriguez Santiago, M. Lopez Sanchez, M. Florea & M. Sanduleac (2013). Transforming Big Data into Collective Awareness, *Computer*, Vol. 46(6), s. 40-45.
- Jajodia, S., Liu, P., Swarup, V. & Wang, C. (2010). *Cyber situational awareness, Issues and Research*, Springer, New York, USA, 249 s.
- Janhunen, K. (2015). Kirsi Janhusen haastattelut. Haastattelijana Juhana Jaakkola.
- Kaleva. (2015). Palvelunestohyökkäys haittaa valtionhallinnon verkkopalveluja. Lehtiartikkeli, Sanomalehti Kaleva, Kaleva OY. Viitattu: [8.7.2016] Saatavissa: <http://www.kaleva.fi/uutiset/kotimaa/palvelunestohyokkays-haittaa-valtionhallinnon-verkkopalveluja/712520/>
- Kraut, R.E., Fish, R.S., Root, R.W. & Chalfonte, B.L. (1990). Informal communication in organizations: Form, function, and technology, *Human reactions to technology: Claremont symposium on applied social psychology*, Citeseer, s. 145-199.

Kuusisto, R., Kuusisto, T. & Armistead, L. (2005). Common Operational Picture, Situation Awareness and Information Operations. Proc. of the 4th European Conference on Information Warfare and Security, 11. -12.7, Glamorgan, UK, s. 175-185.

Kuusisto, T., Kuusisto, R. & Nissen, M. (2007). Information Flow Aspects of Inter-organizational Crisis Management, Journal of Information Warfare, Vol. 6(2), s. 39-51.

Kyberturvallisuusstrategia (2013). Turvallisuuskomitean sihteeristö, Puolustusministeriö.

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

Leppänen, A., Linderborg, K. & Saarimäki, J. (2016). Tietoverkkorikollisuuden tilannekuva, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2016. 37 s.

Lou, H., Chau, P.Y. & Li, D. (2005). Understanding individual adoption of instant messaging: An empirical investigation, Journal of the Association for Information Systems, Vol. 6(4), s. 5.

Mansi, G., & Levy, Y. (2013). Do instant messaging interruptions help or hinder knowledge workers' task performance?. *International Journal of Information Management*, 33(3), s. 591-596.

Meissner, A., Luckenbach, T., Risse, T., Kirste, T. & Kirchner, H. (2002). Design challenges for an integrated disaster management communication and information system, The First IEEE Workshop on Disaster Recovery Networks (DIREN 2002).

Merriam-Webster, (2016). Merriam-Webster's Learner's Dictionary.

Nardi, B.A., Whittaker, S. & Bradner, E. (2000). Interaction and outeraction: instant messaging in action, Proceedings of the 2000 ACM conference on Computer supported cooperative work, ACM, s. 79-88.

NIST, (2012). National Institute of Standards and Technology, U. S Department of Commerce: Guide for Conducting Risk Assessments, Special Publication SP 800-30, Rev 1. [Viitattu 10.9.2016. Saatavissa: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial-publication800-30r1.pdf>

NIST, (2014). National Institute of Standards and Technology, U. S Department of Commerce: Framework for Improving Critical Infrastructure Cybersecurity. [Viitattu 10.9.2016]. Saatavissa: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

Onwubiko, C. (2015). Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy, Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on, London, 8-9 June 2015, s. 1-10.

Orebaugh, A. & Allnut, J. (2009). Classification of instant messaging communications for forensics analysis, The International Journal of Forensic Computer Science, Vol. 1, s. 22-28.

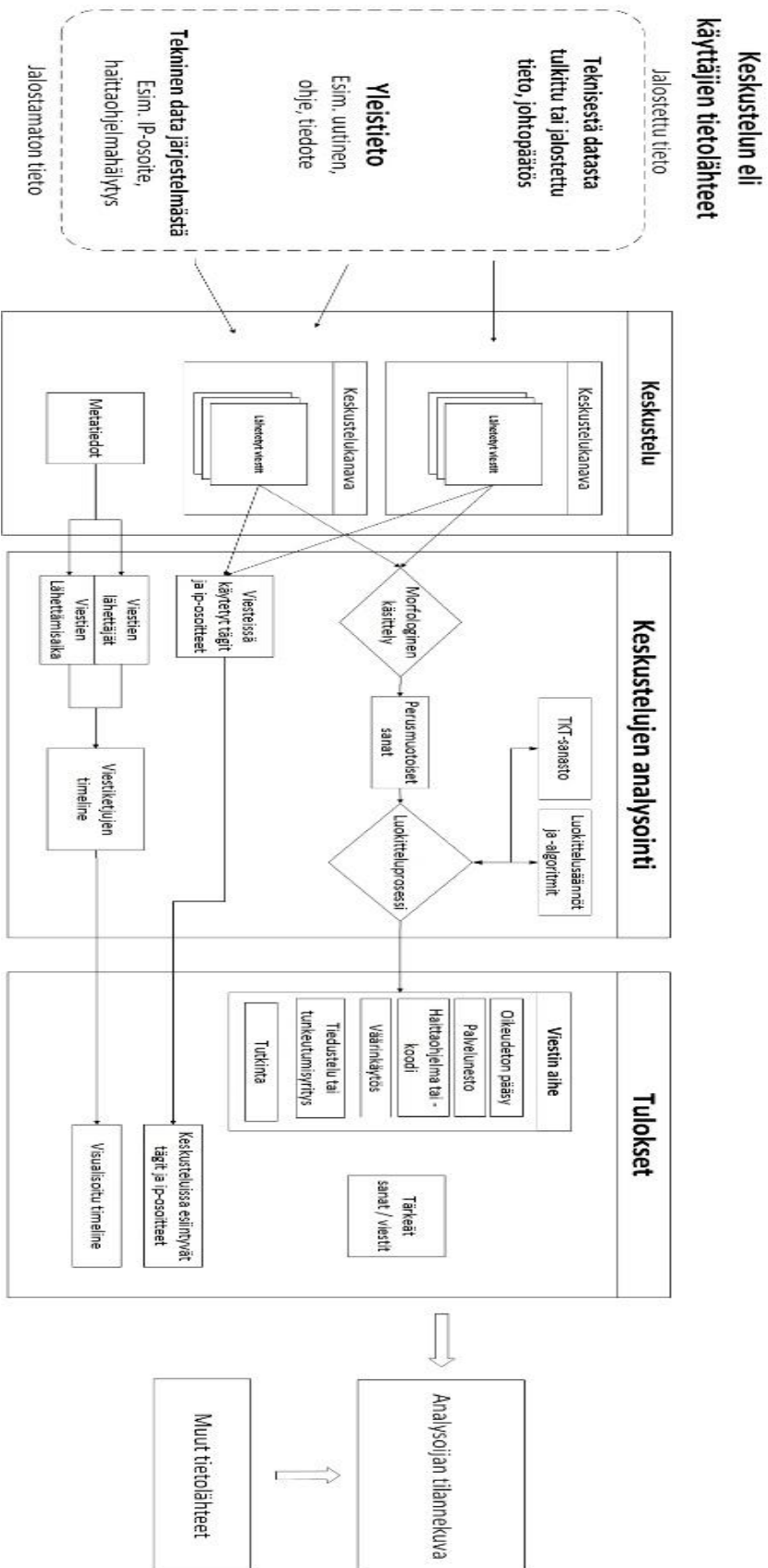
Ou, C., Davison, R.M., Zhong, X. & Liang, Y. (2010). Empowering employees through instant messaging, Information Technology & People, Vol. 23(2), s. 193-211.

Ou, C.X.J. & Davison, R.M. (2011). Interactive or interruptive? Instant messaging at work, Decision Support Systems, Vol. 52(1), s. 61-72.

- Pirttimäki, V. (2007). Business Intelligence as a Managerial Tool in Large Finnish Companies, Väitöskirja, Tampereen teknillinen yliopisto. Julkaisu 646, s. 1-148.
- Raven, M. E., Muller, M. J., Millen, D. R., Kogan, S., & Carey, K. (2002) Ease of Instant Messaging: How the Use of IBM Lotus Sametime Changes Over Time.
- Rennecker, J. & Godwin, L. (2003). Theorizing the unintended consequences of instant messaging for worker productivity, *Sprouts: Working Papers on Information Environments, Systems and Organizations*, Vol. 3(3), s. 137-168.
- Rosenthal, U., & Kouzmin, A. (1997). Crises and crisis management: Toward comprehensive government decision making. *Journal of Public Administration Research and Theory*, 7(2), s. 277-304.
- Rummukainen, L., Oksama, L., Timonen, J. & Vankka, J. (2015). Situation awareness requirements for a critical infrastructure monitoring operator, *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on*, IEEE, s. 1-6.
- Saaranen-Kauppinen, A., Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Yhteiskuntatieteellinen tietoaarkisto. Tampere. 2006. [viitattu 20.6.2016]. Saatavissa: <http://www.fsd.uta.fi/menetelmaopetus/>.
- Salas, E., Prince, C., Baker, D.P. & Shrestha, L. (1995). Situation awareness in team performance: Implications for measurement and training, *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 37(1), s. 123-136.
- Salton, G., Wong, A. & Yang, C. (1975). A vector space model for automatic indexing, *Communications of the ACM*, Vol. 18(11), s. 613-620.
- Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research methods for business students*. 5th ed. England, Pearson Education Limited. 604 s.
- Siegel, C.A., Sagalow, T.R. & Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security, *Information Systems Security*, Vol. 11(4), s. 33-49.
- Skopik, F., Wurzenberger, M., Settanni, G. & Fiedler, R. (2015). Establishing national cyber situational awareness through incident information clustering, *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on*, s. 1-8.
- Stone, S. (2015). Data to Decision for Cyberspace Operations, *Militaru Cyber Affairs*, Vol. 1(1), s. 1-12.
- TTY, (2015). *Opinnäytetyön kirjoittaminen Tampereen teknillisessä yliopistossa, Opinnäytetyön kirjoitusohje*. Tampereen Teknillinen Yliopisto. Julkaistu, 2014, päivitetty 2015.
- VAHTI, (2003). VAHTI-ohje 7/2003. Ohje riskienarvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmä.
- Valtionhallinnon ympärivuorokautisen tietoturvatoinnin kehittämishanke (2013). VM018:00/23. [Viitattu 7.7.2016] Saatavissa: <http://www.hare.vn.fi/upload/asiakirjat/19225/2448261844159695.PDF>.
- Valtioneuvosto, (2009). Valtioneuvoston periaatepäätös 7/2009 valtionhallinnon tietoturvallisuuden kehittämisestä. Valtionvarainministeriö.
- Valtioneuvosto, (2010). Yhteiskunnan Turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010, Valtioneuvosto, Puolustusministeriö, Helsinki

- Valtori, (2016). Valtorin tietoturvalvomo (SOC). [Viitattu, 7.7.2016]. Saatavissa: http://www.valtori.fi/fi-FI/Palvelut/Tulossa_olevat_palvelut/Valtorin_tietoturvalvomo_SOC
- Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security, *Computers & Security*, Vol. 38, s. 97-102.
- Wainfan, L. & Davis, P.K. (2004). Challenges in virtual collaboration: Videoconferencing, audioconferencing, and computer-mediated communications, Rand Corporation.
- Wainfan, L. & Davis, P.K. (2004). Virtual collaboration: Face-to-face versus videoconference, audioconference, and computer-mediated communications, *Defense and Security, International Society for Optics and Photonics*, s. 384-398.
- Whittaker, J. (2004). *The cyberspace handbook*, Psychology Press, Routledge, Lontoo, Iso-Britannia, 321 s.
- Yang, T. & Maxwell, T.A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors, *Government Information Quarterly*, Vol. 28(2), ss. 164-175.
- Yliniemi, T. (2004). Päätöksenteon tietotarpeet kriisitilanteissa. Diplomityö, Tampereen Teknillinen Yliopisto. Saatavilla: <http://URN.fi/URN:NBN:fi:tty-200906081070>.
- Zimmermann, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*, The MITRE Corporation, Bedford, USA, 334 s.

LIITE 1. PIKAVIESTINJÄRJESTELMÄN JA ANALYSOINTITOIMINNAN TIETOVIRTAKAAVIO



LIITE 2. HAASTATTELUIDEN KYSYMYSRUNKO

Taustatiedot

1. Millainen rooli sinulla valtionhallinnon tason tietoturvallisuuden ylläpitämisessä tai kehittämisessä?
 - a. Millaista yhteistyötä, viestintää tai tiedonvaihtoa tehtäviin liittyy?
2. Onko sinulla erikseen täsmennetty rooli mahdollisissa laajemmin valtionhallintoa koskeavissa poikkeustilanteissa?
3. Millaisia haasteita kohtaat poikkihallinnolliseen tietoturvallisuuteen liittyvässä työssäsi?

Vaikutukset ja hyödyt

4. Kenet haluaisit pikaviestimen avulla tavoittaa? Ketkä tulisi saada järjestelmän käyttäjiksi?
5. Ketkä olisivat osaltasi pikaviestinnän tärkeimmät sidosryhmät?
 - a. Normaalitilanteessa?
 - b. Poikkeustilanteissa?
6. Muuttaisiko pikaviestinjärjestelmä viestintäkäytäntöjasi tai -tapojasi? Millainen rooli pikaviestintäjärjestelmällä olisi viestinnässä?
7. Millaisia hyötyjä poikkihallinnollinen pikaviestinjärjestelmä tai nämä muutokset voisi työsi kannalta tuoda nykytilanteeseen? Voisiko järjestelmä ratkaista mainitsemiasi haasteita?
 - a. Millaisia hyötyjä voisit saada pikaviestinnän analysoinnin tuloksista?
8. Toisiko pikaviestinjärjestelmän ja/tai analysointitoiminta muutoksia työnkuvaasi tai työprosesseihin joihin osallistut?
 - i. Normaalitilanteessa?
 - ii. Poikkeustilanteissa?

9. Millaista tietoa haluaisit järjestelmästä saada?
 - a. Mihin liittyen?
 - b. Millaista / millaisessa muodossa olisi ”hyvä” tai hyödyllinen tieto?
 - c. Millaista tietoa voisit tuottaa järjestelmään/järjestelmän avulla muille käyttäjille?

10. Asettaisitko muita tarpeita / toiminnallisia vaatimuksia järjestelmälle?
 - a. Mitä muita ominaisuuksia haluaisit järjestelmällä olevan?

LIITE 3 HAASTATTELUISSA ESIINTYNEET TEE- MAT

<i>H1</i>	Nopeampi tiedon levitäminen eri toimijoiden kesken kuin nykyisillä käytävissä olevilla välineillä	Kahdensuuntainen tiedonvaihto	Tiedon saaminen tarvittavista toimipeisistä	Salaisesti luokiteltavan tiedon /tiedostojen helpompi jakaminen sähköpostin verrattuna			
<i>H2</i>	Tiedonkulun parantaminen, ”lokeroitumisen” vähentäminen	Päivittäinen operatiivisen tason viestintä sidoryhmiin kanssa	Redundanssi; vaihtoehtoinen järjestelmä häiritöiden välillä	Sosiaalisten verkostojen ylläpitäminen	Tietoturvatiedon saaminen ja kerääminen muilta asiantuntijoilta	Mikäli saadaan riittäville tietoturvatavalle, helpokäyttöisempi joissain tilanteissa kuin salattu sähköposti	
<i>H3</i>	Keskietty yhteyspiste valtionhallinnon organisaatioiden tietoturva-asiantuntijoihin, parempi tavoitettavuus	Luottamuksellisen tiedon helpompi jakaminen ja luottamuksellisten asioiden käsittely	Kaksisuuntainen tiedonvaihto eri organisaatioiden välillä	Tilanne tiedon kerääminen	Tiedon, esimerkiksi uutisten ja yleistason havaintojen jakaminen	Parempi näkyvyys organisaatioiden tilanteeseen	
<i>H4</i>	Parempi näkyvyys Valtionneuvoston järjestelmien turvallisuustilanteeseen;	Yleisen tilannekuvan /raporttien saaminen; nykyisissä raporteissa olevaa tietoa ei ole jalostettu riittävästi	Reagoitavuus ja varautuminen parantaminen; näkyvyys uhkatilanteisiin ja muutoksiin, jotka vaativat ennakoivaa päätöksenteoa	Parempi yhteys palveluntuottajan (alhankkijoilta) ja toimittajan välillä, mikä välillisesti hyödyntää palveluiden hyödyntäjiä	Tilannekuvan parantaminen saatavuus virka-ajan ulkopuolella	Mahdollinen positiivinen kulttuurin muutos tiedon jakamiseen ja poikkeamista tiedottamiseen ja raportointiin	
<i>H5</i>	Teknisen tilannekuvan abstraktiointi; asioiden erottaminen toisistaan; kontekstin luominen ja siten hyödynnettävyyden parantaminen	Pikaraportointi, tapahtumamerkinöiden kokoaminen raportointipohjaksi	Tilannekuvan, tapahtumakokoonpanon osaksi muuta tietoa;	Kyberturvallisuussanaston ”kääntäminen” eli ymmärrettävyyden parantaminen sanojen liittämällä sanat laajempaan asiantunteeseen	Näkyvyys asiantuntijoiden välisen tietojen ja kyberturvallisuuskeskustelun ”tilannekuvaajärjestelmä”	Yksittäisten keskustelujen erottaminen toisistaan analysointityökalujen avulla	