HANKKEIDEN TURVALLISUUDEN KEHITTÄMINEN PUOLUSTUSVOIMISSA

Timo Tolkki

2020 Laurea

Laurea-ammattikorkeakoulu

Hankkeiden turvallisuuden kehittäminen Puolustusvoimissa

Timo Tolkki

Turvallisuusjohtamisen YAMK

Opinnäytetyö

Joulukuu 2020

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusjohtamisen koulutusohjelma

Tradenomi (YAMK)

Timo Tolkki

Hankkeiden turvallisuuden kehittäminen Puolustusvoimissa

Vuosi 2020 Sivumäärä 66

Tämän opinnäytetyön tavoitteena on kehittää Puolustusvoimien hankkeiden turvallisuutta. Hankkeiden turvallisuuden kehittämistä tarkastellaan sidosryhmäturvallisuuden näkökulmasta. Työn tarkoituksena on selvittää, miten Puolustusvoimien hankkeiden turvallisuutta voidaan kehittää ja luoda ehdotuksia hankkeiden turvallisuuden kehittämiseksi. Opinnäytetyön toimeksiantajana toimi Pääesikunnan turvallisuussektori.

Opinnäytetyön kehittämistehtävänä on tutkia, miten Puolustusvoimien hankkeiden turvallisuutta voidaan kehittää sidosryhmäturvallisuuden näkökulmasta. Alakehittämistehtäviä ovat: selvittää mitkä ovat onnistumisen avaintekijät hankkeissa, ja selvittää minkälaisia kehittämiskohteita hankkeiden turvallisuudessa on tunnistettavissa sidosryhmäturvallisuuden osalta.

Työn tietoperustana on kirjallinen lähdeaineisto, joka muodostuu aiheeseen liittyvistä säädöksistä sekä Puolustusvoimien sisäisistä normeista ja ohjeista. Tätä tietoperustaa on tuettu osin työn haastatteluaineistolla sekä Puolustusvoimien hankealan neuvottelupäivien materiaalilla. Viitekehys rakentuu uutta materiaalista suorituskykyratkaisua kehittävän hankkeen ja siihen liittyvän sidosryhmäturvallisuuden osatekijöistä.

Opinnäytetyö toteutettiin laadullisena kehittämistyönä. Kehittämistehtävään pyrittiin vastamaan asiantuntijoiden tutkimushaastatteluista kerätyn aineiston avulla. Tutkimushaastattelut olivat luonteeltaan puolistrukturoituja teemahaastatteluita. Aineiston analysointiin käytettiin aineistolähtöisen sisällönanalyysin tekniikkaa. Päättelyn logiikka oli induktiivinen eli aineistosta löytyneiden yhteneväisyyksien perusteella pyrittiin muodostamaan yleistyksiä.

Keskeisenä tuloksena aineistosta nousi esiin neljä asiakokonaisuutta, joihin tulisi kiinnittää huomiota hankkeiden turvallisuuden kehittämiseksi sidosryhmäturvallisuuden näkökulmasta. Nämä neljä kokonaisuutta ovat: hankkeen turvallisuusvaatimusten huolellinen määrittely hanketta valmisteltaessa, turvallisuuden asiantuntijaresurssien käyttö, henkilöstön osaamisen säännöllinen ylläpito ja kasvattaminen sekä käytännön toimenpideohjeiden laadinta ja saatavuus.

Hankkeisiin liittyy hyvin paljon erilaisia huomioon otettavia asioita ja näiden huomioiminen vaatii laajaa asiantuntijuutta. Hankepäällikön merkitys hankkeen laadukkaalle ja sujuvalle toteutukselle on erittäin suuri. Sidosryhmäturvallisuuteen liittyvät asiat toteutuvat hankkeissa yleisesti ottaen hyvin, johtuen henkilöstön ammattitaidosta ja huolellisuudesta sekä eri viranomaisten välisen ja puolustushallinnon sisäisen yhteistyön laadukkuudesta. Toisaalta, vaikka hankkeiden turvallisuus toteutuukin hyvin, niin sen toteuttaminen ei aina tapahdu optimaalisella tavalla vaan asioiden selvittämiseen kuluu usein henkilöstöllä paljon aikaa ja työskentelyä oman varsinaisen vastuualueen ulkopuolella. Hankkeiden turvallisuutta voitaisiin kokonaisvaltaisesti parhaiten kehittää integroimalla turvallisuus tehokkaammin hanketoimintaan, sen prosesseihin, henkilöstön koulutukseen sekä ohjeisiin.

Asiasanat: Puolustusvoimat, hanke, turvallisuus, sidosryhmäturvallisuus

Laurea University of Applied Sciences **Abstract**

Degree Programme in Security Management

Master of Business Administration

Timo Tolkki

Developing Program Security in Finnish Defence Forces

Year 2020 Pages 66

The aim of this master's thesis is to develop project security in Finnish Defence Forces. The project security is examined from the perspective of industrial security. The purpose of this work is to find out how the project security of Finnish Defence Forces could be developed and to create proposals for improvement. The thesis was commissioned by the security sector of Finnish Defence Forces.

The development task is to study how the security of Finnish Defence Forces' projects can be developed from the perspective of industrial security. Sub tasks are: to find out the key factors for success and to identify areas of development in project security in terms of industrial security.

The theory is based on literature that consists of subject related to statute and Finnish Defence Forces' internal directives and instructions. The theory is supported in part with the material from interviews and with material from the seminar of Finnish Defence Forces' project sector. The framework is constructed by elements of material project and project related industrial security.

The thesis was implemented as a qualitative development work. The aim was to take on the development task with the help of the material collected from the experts' research interviews. Research interviews were semi-structured thematic interviews in nature. Data-based content analysis techniques were used to analyze the data. The logic of reasoning was inductive, thus within the similarities found in the data, attempts were made to form generalizations.

As a key result, four issues emerged from the material that should be addressed in order to develop project security from an industrial security perspective. These four components are: the thorough definition of project security requirements during project preparation, the use of security experts, the regular maintenance and development of staff skills, and the development and availability of practical operational guides.

There are many different issues involved in projects and these require extensive expertise. The importance of the project manager for the high-quality and smooth implementation of the project is prominent. Issues concerning industrial security in projects are generally well implemented, due to the professionalism and diligence of the staff and the quality of co-operation between different authorities and within the defense administration. On the other hand, even if the security of projects is well implemented, its implementation is not always done in an optimal way. Staff often spend a lot of time and work outside their own area of responsibility. Project safety could be holistically developed by integrating security more effectively into project activities, its processes, staff training and guidelines.

Keywords: Finnish Defence Forces, project, security, industrial security

Sisällys

1 Johdanto

Puolustusvoimien (PV) lailla säädettyjä tehtäviä ovat: Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen, osallistuminen kansainvälisen avun antamiseen sekä osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan. (Laki Puolustusvoimista 55/2007, 2§). Näiden tehtävien suorittamiseksi Puolustusvoimat tarvitsee määrällisesti ja laadullisesti riittävän suorituskyvyn arvioituja uhkia vastaan. Maanpuolustuksen uskottavuutta kehitetään toimintaympäristön asettamien vaatimusten mukaan. Tällä hetkellä Suomen turvallisuusympäristö on muutoksen kourissa ja sen muutoksen arvioidaan olevan pitkäkestoinen. Suomen ratkaisu sotilaallisten uhkien torjumiseksi on ammattitaitoinen henkilöstö, nykyaikaisten ja suorituskykyisten asejärjestelmien käyttö sekä laaja asevelvollisista koottu reservi. Puolustuskykyyn liittyy sotilaallisen suorituskyvyn lisäksi myös vahvasti kansallinen viranomaisyhteistyö sekä kansainvälinen puolustusyhteistyö. (Puolustusministeriö 2018, 1).

Yhteistyö on tärkeä osa Suomen turvallisuutta ja maanpuolustusta. Suomen ulko- ja turvallisuuspoliittisen selonteon (2020) mukaan Suomen turvallisuuden avaintekijöitä ovat yhteiskunnan kriisinsietokyvyn, huoltovarmuuden ja yhtenäisen Euroopan Unionin lisäksi vahva kansallinen puolustuskyky sekä tiivis kansainvälinen ulko-, turvallisuus- ja puolustuspoliittinen yhteistyö (Valtioneuvosto 2020, 24). Myös viimeisimmässä puolustusselonteossa (2017) painotetaan puolustusyhteistyön kehittämistä osana Suomen puolustuskykyä. Maanpuolustuksen materiaalista suorituskykyä kehitetään luomalla valmiuksia kansainväliselle materiaaliyhteistyölle. (Valtioneuvosto 2017, 15-17).

Toimintaympäristön ja uhkakuvien muutokset sekä teknologian kehittyminen asettavat vaatimuksia puolustusjärjestelmän suorituskyvylle. Suorituskykyä voidaan tarkastella Puolustusvoimien sotilaallisen suorituskyvyn käsitemallin (2018) mukaan vaikuttavuuden, kyvykkyyden ja ratkaisuiden sekä elinjakson näkökulmasta. Puolustusvoimissa suorituskykyvajeisiin vastataan usein erilaisilla hankkeilla. (Pääesikunta 2018, 5). Esimerkkeinä merkittävistä strategisista hankkeista voidaan mainita tällä hetkellä ajankohtaiset ilmavoimien HX- ja merivoimien Laivue 2020 -hanke (Puolustusvoimat 2020a). Näiden lisäksi Puolustusvoimissa on käynnissä useita pienempiä hankkeita osana Puolustusvoimien kehittämisohjelmia.

Hankkeisiin liittyen Puolustusvoimat tekee paljon yhteistyötä erilaisten sidosryhmien kanssa. Yhteistyötä tehdään niin kansallisesti kuin kansainvälisestikin. Koska hankkeet liittyvät Suomen puolustuskyvyn ylläpitoon ja kehittämiseen on hankkeiden turvallisuusnäkökulmat otettava tarkasti huomioon. Hanketurvallisuuden kehittämisen tarpeeseen on kiinnitetty

huomiota puolustushallinnossa. Puolustusministerin ja Puolustusvoimien komentajan välisessä vuoden 2019 tulossopimuksessa on yhdeksi puolustushallinnon vaikuttavuuden ja toiminnan tuloksellisuuden kannalta keskeiseksi toimenpiteeksi määritetty toimenpiteiden käynnistäminen strategisten hankkeiden hanketurvallisuuden kokonaisuuden ohjaamiseksi (Puolustusministeriö 2018, 7). Puolustusministeriön näkökulmasta hanketurvallisuudessa korostuu kansainvälisten tietoturvallisuusvelvoitteiden tunnistaminen ja toteutus turvallisuusluokiteltua tietoa sisältävissä hankkeissa. Puolustusvoimien sisällä hankkeiden turvallisuuden kehittäminen on otettu Puolustusvoimien logistiikkatoimialan johdolla yhdeksi kehittämisalueeksi kaikkiin Puolustusvoimien hankkeisiin liittyen. (Haastatteluaineisto 2020).

1.1 Kehittämistehtävä ja rajaukset

Tämän opinnäytetyön tavoitteena on kehittää Puolustusvoimien hankkeiden turvallisuutta. Työn tarkoituksena on selvittää, miten Puolustusvoimien hankkeiden turvallisuutta voidaan kehittää ja luoda ehdotuksia hankkeiden turvallisuuden kehittämiseksi. Hankkeiden turvallisuutta tarkastellaan sidosryhmäturvallisuuden näkökulmasta.

Hankkeiden turvallisuus kattaa hyvin monia ja ajallisesti laajoja asiakokonaisuuksia, joten asian käsittely opinnäytetyön muodossa vaatii rajausten tekemistä. Työssä noudatetaan seuraavia rajauksia: Hankkeen turvallisuutta tarkastellaan sidosryhmäturvallisuuden näkökulmasta eli toisin sanoen hankkeeseen liittyy salassa pidettävän tiedon vaihtoa Puolustusvoimien ja sidosryhmien välillä. Hankeen toteutusta tarkastellaan hankkeen hallinnan näkökulmasta. Turvallisuusluokitellun tiedon osalta työ käsittelee TLIV-TLII -tasojen tietojen käsittelyä. Sidosryhmäturvallisuuden osalta huomioidaan sekä kansallinen että kansainvälinen näkökulma.

Opinnäytetyön kehittämistehtävänä on tutkia, miten Puolustusvoimien hankkeiden turvallisuutta voidaan kehittää sidosryhmäturvallisuuden näkökulmasta. Alakehittämistehtäviä ovat: selvittää mitkä ovat onnistumisen avaintekijät hankkeissa, ja selvittää minkälaisia kehittämiskohteita hankkeiden turvallisuudessa on tunnistettavissa sidosryhmäturvallisuuden osalta.

Hankkeiden turvallisuuden kehittämistä tarkastellaan laadullisesta näkökulmasta. Opinnäytetyössä käytetään kehittämismenetelmänä aineistolähtöistä sisällönanalyysiä. Analysoitava lähdeaineisto on kerätty asiantuntijoiden teemahaastatteluilla. Toisena menetelmänä työssä sovelletaan tapaustutkimuksen periaatteita. Tapaustutkimuksen avulla vahvistetaan työn tietoperustaa käyttämällä esimerkkitapausta konkreettisena esimerkkinä sidosryhmäturvallisuuden toimenpiteistä hankkeessa.

1.2 Teoreettiset lähtökohdat

Työn tietoperusta on rakennettu kirjalliseen lähdeaineistoon, organisaation sisäisiin normeihin ja ohjeisiin sekä organisaation sisäisillä hankealan neuvottelupäivillä käsiteltyihin esityksiin perustuen. Suoraan tämän työn tietoperustaksi soveltuvia, kotimaisia tai ulkomaisia väitöskirjoja tai lisensiaattitöitä ei löytynyt.

Tärkeimmät kirjalliset lähteet ovat aiheeseen liittyvät säädökset sekä Puolustusvoimien sisäiset normit ja aiheeseen liittyvä kirjallisuus. Aiheeseen liittyy myös jonkin verran Puolustusvoimien turvallisuusluokiteltuja normeja, joiden avulla julkisten asiakirjojen antamaa ohjausta on tarkennettu. Turvallisuusluokiteltua tietoa ei ole käytetty tässä työssä lähteenä.

Tiedon käsittelyä Puolustusvoimien hankkeissa ohjaavat tärkeimpinä säädöksinä: laki viranomaisten toiminnan julkisuudesta (621/1999), laki julkisen hallinnon tiedonhallinnasta (906/2019), laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), turvallisuusselvityslaki (726/2014), valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) sekä kansainväliset tietoturvallissuusopimukset.

Puolustusvoimien käytännön hanketoimintaa ohjaavana asiakirjana toimii Pääesikunnan normi: Hankeohje (2017b). Hankeohje antaa yleiset periaatteet siitä millaisia asioita hankkeen hallinnassa ja hankesuunnitelman laadinnassa tulisi ottaa huomioon ja se tarjoaa myös mallin hankesuunnitelmasta. Ohje on tarkoitettu erityisesti hankepäälliköiden avuksi. (Pääesikunta 2017b, 5). Puolustusvoimien suorituskykyjen elinjaksonhallinta on kuvattu Pääesikunnan normissa: Joukon ja järjestelmän elinjaksonhallinta (2017c). Hankintatoimintaa Puolustusvoimissa ohjaa Pääesikunnan määräys: Puolustusvoimien hankintamääräys (2015a), joka luo kehyksen Puolustusvoimien hankintayksiköiden hankintojen toteuttamiselle (Pääesikunta 2015a, 7). Yleisenä projektitoiminnan lähteenä käytetään Jyri Kosolan kirjaa Puolustusvoimien projektiohje (2012), jossa on kuvattuna ISO-21500 standardin mukainen projektitoiminta Puolustusvoimien viitekehyksessä (Kosola 2012, 3).

Puolustusvoimien turvallisuutta ohjaa ylimpänä asiakirjana Pääesikunnan operatiivisen osaston normi: Puolustusvoimien turvallisuus (2015b). Hankintojen sidosryhmäturvallisuuteen liittyvät oleellisesti Pääesikunnan asiakirjat Puolustusvoimien sidosryhmäturvallisuus (2017a), Turvallisuusjärjestelyiden varmistaminen Puolustusvoimien ja sidosryhmien välisessä yhteistyössä (2017d) sekä Puolustusvoimien tietoturvallisuusohje (2020).

Kehittämistyön tekijä osallistui Puolustusvoimien sisäisille hankealan neuvottelupäiville keväällä 2020. Neuvottelupäivien teemana oli hanketurvallisuus ja neuvottelupäivillä käsiteltiin hanketurvallisuuden elementtejä turvallisuustoimialan näkökulmasta. Osa

neuvottelupäivillä käsitellystä aineistosta oli turvallisuusluokiteltua ja osa julkista. Neuvottelupäivillä käsiteltiin hankealan ajankohtaisten tietoiskujen lisäksi hanketurvallisuuteen liittyen esimerkiksi seuraavia aiheita: hanketurvallisuus puolustusministeriön näkökulmasta, sidosryhmä-, tila-, sähkö- ja kyberturvallisuuden näkökulmat Puolustusvoimien hankkeissa.

Hanketurvallisuuden neuvottelupäivät osoittivat sen, että hanketurvallisuus on Puolustusvoimille aiheena erittäin ajankohtainen ja tärkeä sekä toisaalta myös sen, että hanketurvallisuus on käsitteenä haastava ja hyvin monialainen. Neuvottelupäivät toimivat erinomaisena välineenä aiheeseen liittyvän tietopohjan rakentamisessa ja asiantuntijoiden kanssa verkostoitumisessa.

Hankkeita ja erilaisia projekteja käsittelevää kirjallisuutta ja tutkimusraportteja sekä -artikkeleita on runsaasti saatavilla mutta viranomaisten ja yritysten välistä salassa pidettävän tiedon käsittelevää aineistoa ei löytynyt. Aihetta ei ole tutkittu aikaisemmin Suomessa tästä näkökulmasta mutta työn aihetta sivuavia tutkielmia löytyi jonkin verran. Aineiston hakuun käytettiin erilaisia tietokantoja kuten Google Scholar, Laurea Finna, MPKK Finna, Ebsco Host sekä ProQuest. Hakusanoina käytettiin yhdessä ja erikseen kirjoitettuna esimerkiksi: hanke, turvallisuus, sidosryhmä, turvaluokiteltu, tieto sekä englanniksi military program security, project, program, security, industrial security ja stakeholder security.

Anssi Aaltonen (2014) on laatinut Maanpuolustuskorkeakoulun esiupseerikurssilla tutkielman *Puolustusvoimien turvaluokiteltujen hankkeiden hanketurvallisuus.* Tutkielma on turvallisuusluokiteltu TLIV-tasolle. Työssä Aaltonen tarkastelee tuolloin ajankohtaisena aiheena olleen turvallisuusselvityslain uudistuksen vaikutuksia Puolustusvoimien hankkeiden turvallisuuden toteuttamiseen. Työn keskeisenä tuloksena havaittiin, että lakiuudistus tuo muutoksia kaikkiin hankkeen vaiheisiin turvallisuuden osalta ja näin ollen vaikuttaa hankkeen kokonaissuunnitteluun. Työn kirjoittamisen jälkeen lainsäädäntö sekä PV:n turvallisuusorganisaatio on uudistunut.

Toinen aihetta käsittelevä tutkielma on Jarno Simin (2010) Teknillisen korkeakoulun turvallisuusjohdon koulutusohjelmassa laatima työ *Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus.* Työssä selvitetään mitä vaatimuksia PV:n kaupallisen ja turvallisuusalan normit asettava hankintaprosessin turvallisuudelle ja miten turvallisuusasiat tulee huomioida hankintaprosessin eri vaiheissa. Työn yhteenvedossa todetaan, että tärkein asia hankintojen turvallisuudelle on turvallisuusluokitellun tiedon tunnistaminen ja että turvallisuuden kannalta tärkein henkilö hankintaprosessissa on hankinnasta kokonaisvastuussa oleva henkilö.

Tuomas Herranen (2013) tarkastelee Laurea ammattikorkeakoulun opinnäytetyössään turvallisuusluokitellun tiedon suojaamista palveluhankintojen tarjouslaskentavaiheessa. Työ

käsittelee kansallisen turvallisuusauditointikriteeristön (KATAKRI) soveltamista Puolustushallinnon rakennuslaitoksen turvallisuusluokiteltua tietoa sisältävien hankkeiden tarjouslaskentavaiheessa.

Turvallisuusluokiteltujen rakennushankkeiden toteuttamista oli tutkittu jonkin verran, näistä mainittakoon Lauri Sailion (2012) laatima esiupseerikurssin tutkielma *Turvallisuus Puolustusvoimien turvaluokiteltua tietoa sisältävissä rakennushankkeissa* sekä Toni Lahden (2017) Aalto Yliopiston turvallisuusjohdon koulutusohjelmassa laatima tutkielma *Rakennushankkeiden turvallisuus Puolustusvoimien hallinnoimilla alueilla.* Näissä töissä käsiteltiin rakennushankkeiden turvallisuutta monelta kantilta mutta yhtenä johtopäätöksenä molemmissa töissä todettiin, että PV:n turvallisuustoimialan tulisi olla mukana hankkeiden suunnittelussa heti hankkeen alusta alkaen.

1.3 Työn rakenne

Tässä opinnäytetyössä on pyritty noudattamaan yleistä tutkimusraportin perusrakennetta. Työn runko-osa koostuu johdannosta, menetelmäosasta, tuloksista sekä pohdinnasta (Hirsjärvi, Remes & Sajavaara 2009, 250). Opinnäytetyön johdanto muodostuu 1. ja 2. luvusta. Työn toisessa luvussa on esitelty aiheen kannalta oleellinen tietoperusta. Tietoperusta koostuu Puolustusvoimien turvallisuus- ja hanketoiminnasta sekä hankkeisiin liittyvän sidosryhmäturvallisuuden osatekijöistä. Toisen luvun lopussa on esitelty tapaustutkimuksen menetelmiä soveltaen tapausesimerkki hankkeesta ja siihen liittyneistä sidosryhmäturvallisuuden elementeistä. Tämän tavoitteena on konkretisoida tietoperustassa käsitellyt asiat esimerkin avulla. Kolmannessa luvussa on esitelty työn kehittämismenetelmä. Neljännessä luvussa on esitelty kehittämismenetelmän avulla työssä esiin nousseet tulokset. Viidennessä ja viimeisessä luvussa on kehittämistyön tuloksien perusteella muodostetut johtopäätökset sekä työn tutkimuseettinen tarkastelu ja jatkotutkimustarpeiden pohdinta.

2 Hankkeiden turvallisuus

Puolustusvoimien turvallisuustoiminnan tavoitteena on ennaltaehkäistä operatiivista suorituskykyä ja päätehtävien toteuttamista uhkaavat turvallisuusriskit. Turvallisuustoiminnalla pyritään varmistamaan organisaation toiminnan jatkuvuus kaikissa tilanteissa ja se sisältää kaikki ne keinot, joilla turvataan Puolustusvoimien henkilöstö, tiedot, materiaali, tekninen infrastruktuuri sekä ympäristö kaikilta tahallisilta ja tahattomilta uhkilta. Tavoitetilassa turvallisuustoiminta on luonnollinen osa linjaorganisaation normaalia toimintaa. Organisaation turvallisuuskulttuurin avaintekijöiksi on määritetty ihmisten arvot ja asenteet, esimiesten esimerkki sekä organisaation toimintatavat. (Pääesikunta 2015b, 5-7).

Puolustusvoimien turvallisuusohje määrittää PV:n turvallisuustoiminnan tavoitteet, johtamisen sekä sen toimeenpanon. Puolustusvoimat täyttää valtion viranomaisena kaikki sitä koskevat lakisääteiset vaatimukset kaikessa toiminnassa. Organisaation johto on myös sitoutunut turvallisuuden toteuttamiseen. Turvallisuustoiminnan laadukas toimeenpano vaatii priorisointia ja priorisoinnin on perustuttava riskianalyyseihin. Vastuu riskianalyysien laadinnasta on Puolustusvoimien hallintoyksiköillä. Normien edellyttämien resurssien puuttuessa on siitä tehtävä ilmoitus virkatietä määräyksen antajalle. Vastuu turvallisuudesta kuuluu linjaorganisaation mukaiselle johdolle ja turvallisuustoiminta tulee integroida mukaan kaikkeen toimintaan tarvittavilta osin. Puolustusvoimien erityispiirteenä voidaan nähdä turvallisuustoiminnan liittyvän jatkumona sekä normaali- että mahdollisten poikkeusolojen toimintaan. (Pääesikunta 2015b, 3-7).

Puolustusvoimien turvallisuutta johtaa PV:n turvallisuusjohtaja. Tämä tehtävä on kytketty osaksi organisaation valmiuspäällikön tehtäviä. Pääesikunnan operatiivisen osaston turvallisuussektorin johtaja johtaa turvallisuustoimialan suunnittelua. (Pääesikunta 2015b, 6). Puolustusvoimien sidosryhmäturvallisuutta johtaa sidosryhmäturvallisuuspäällikkö.

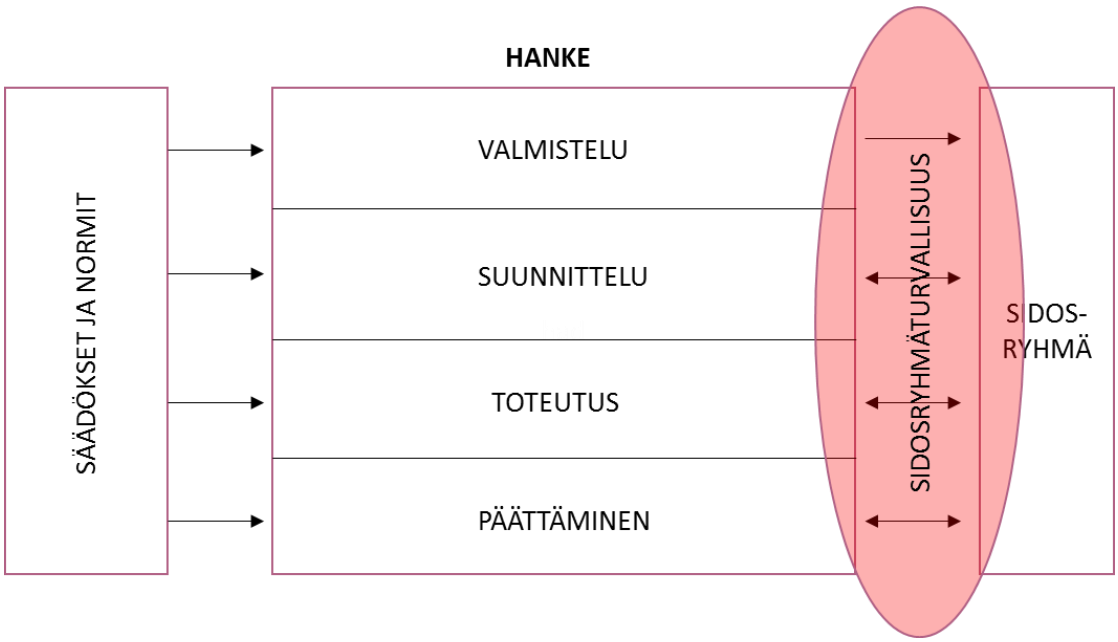
Puolustusvoimien turvallisuuden eri alat (14 kpl) ovat Puolustusvoimien toiminta (2017e, 30) -normin mukaan seuraavat:

- työ- ja palvelusturvallisuus
- turvallisuusvalvonta
- tilaturvallisuus
- pelastustoimi
- tietoturvallisuus
- sidosryhmäturvallisuus
- turvallisuus- ja lupahallinto
- räjähdeturvallisuus
- kemikaaliturvallisuus
- sähköturvallisuus

- ympäristöturvallisuus
- kuljetusten turvallisuus ja liikenneturvallisuus
- sotilasilmailun lentoturvallisuus
- sotilasmerenkulun turvallisuus.

Puolustusvoimien hankeohjeen (2017b) mukaan hanketurvallisuus voidaan jakaa kolmeen osaan hankkeen eri osa-alueisiin liittyen: hankeen toteuttamiseen liittyvää turvallisuuteen, hankkeen lopputuotteen turvallisuuteen sekä lopputuotteen käyttöperiaatteisiin liittyvään turvallisuuteen. Ohjeen mukaan hanketurvallisuutta tulee tarkastella kaikkien Puolustusvoimien turvallisuuden alojen kautta ja huomioida ne tarvittavilta osin. (Pääesikunta 2017b, 16-17). Näin ollen termi ”hanketurvallisuus” on erittäin laaja ja se voidaan ymmärtää sekä hankkeen että turvallisuuden näkökulmasta monilla eri tavoilla, riippuen hankkeen luonteesta ja asiaa tarkastelevan henkilön taustasta, tehtävästä ja organisaatiotasosta.

Tämän opinnäytetyön viitekehys (kuvio 1) muodostuu hankkeen toteuttamiseen liittyvästä sidosryhmäturvallisuudesta. Työn tietoperustassa tätä kokonaisuutta tarkastellaan hanketoiminnan ja sidosryhmäturvallisuuden näkökulmasta. Tärkeimmät työssä käytettävät käsitteet ovat liitteenä (liite 1).



Kuvio 1: Opinnäytetyön viitekehys

2.1 Hanke

Puolustusvoimien ja maanpuolustuksen kehittämistarpeet sekä suorituskykyvajeet tunnistetaan Puolustusvoimien kehittämisohjelmissa. Kehittämisohjelmat ovat erittäin laajoja kokonaisuuksia, joiden tavoitteena on kehittää laajoja suorituskykyalueita kuten esimerkiksi meri- tai ilmapuolustusta kokonaisuutena. (Kosola 2012, 9).

Tunnistettuihin kehittämistarpeisiin ja suorituskykyvajeisiin vastataan erilaisilla hankkeilla. Hanke on siis suorituskyvyn kehittämisen ”työkalu” ja osa suorituskyvyn elinjaksoa. Hanke on luonteeltaan projektimainen ja sitä varten perustetaan erillinen hankeorganisaatio. Hankkeet sijoittuvat Puolustusvoimien suorituskyvyn elinjaksomallissa pääasiassa suunnittelu ja kehittämis- sekä suorituskyvyn rakentamisvaiheeseen. Hanketta valmistellaan yleensä normaalin linjaorganisaation työnä jo suorituskyvyn elinjakson aikaisemmissa konsepti- ja määrittelyvaiheissa, ennen varsinaisen hankkeen käynnistämistä. (Pääesikunta 2017b, 6-9).

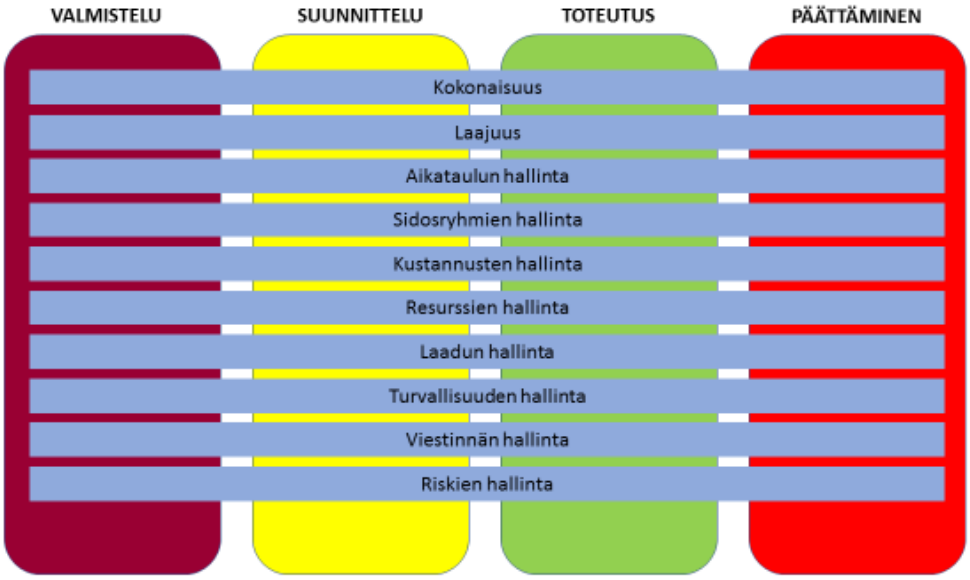
Puolustusvoimien sotilaallisen suorituskyvyn käsitemallin mukaisesti suorituskyky on ”kyky suorittaa tietty toiminta tai saavuttaa tietty vaikutus”. Tätä voidaan tarkastella neljästä näkökulmasta, joista yksi on ratkaisu. Suorituskykyratkaisu on usein materiaalin (esimerkiksi laivan tai panssarivaunun) hankkiminen, mutta se voi olla myös menetelmällinen eli esimerkiksi toimintavan tai konseptin muuttaminen. Suorituskykyratkaisua voidaan tarkastella seuraavien osatekijöiden kautta: doktriini, organisaatio, koulutus, materiaali, johtajuus, henkilöstö, infrastruktuuri ja yhteistoimintakyky. (Pääesikunta 2018, 5-10). Tämä on siinä mielessä oleellista, että hankkeessa tehdyillä turvallisuusratkaisulla on vaikutusta suorituskyvyn koko elinjaksolle, vaikka itse hanke olisikin jo päättynyt. Tässä työssä tarkastellaan hankkeen sidosryhmäturvallisuutta pääasiassa materiaalisen osatekijän kannalta, mutta hankkeessa toteutetut sidosryhmäturvallisuuden ratkaisut voivat vaikuttaa esimerkiksi myös infrastruktuuriin tai yhteistoimintakykyyn.

Hanke koostuu toiminnallisesti hankkeen hallinnasta ja hankkeen tuotteesta eli tavoitellusta suorituskykyratkaisusta. Hanketta johtaa hankepäällikkö, joka käyttää hankkeen hallinnan keinoja (kuvio 2) hankkeen johtamiseen. Hankkeen tavoitteena on suunnitella ja rakentaa puuttuvaan suorituskykyyn liittyvät osatekijät sekä integroida nämä toimivaksi kokonaisuudeksi. Lopputuloksena syntyvä tuote voi olla esimerkiksi materiaalia, tietojärjestelmä tai näistä muodostuva järjestelmäkokonaisuus. (Pääesikunta 2017b, 5-7).

Hanke jakautuu ajallisesti neljään vaiheeseen, jotka ovat: valmistelu-, suunnittelu-, toteutus- ja päättämisvaihe. Hankkeen etenemistä ja hankesuunnitelmaa sekä hankkeeseen liittyviä asiakirjoja tarkastellaan säännöllisissä hankekatselmoinneissa. Hankkeen valmisteluvaiheessa luodaan hankkeelle aikataulu ja arvioidaan sen vaatimat resurssit sekä varmistetaan, että hankkeen tavoitteet ovat oikeat suhteessa tunnistettuun suorituskykyvajeeseen. Valmisteluvaiheessa vertaillaan erilaisia konsepteja vaatimusten täyttämiseksi ja tehdään

lopullinen päätös hankkeen toteuttamisesta. Kun hanke on asetettu, sille nimetään hankepäällikkö, joka vastaa siitä, että hanke täyttää sille asetetut tavoitteet määräajassa ja annetuilla resursseilla. Usein hankkeen valmistelijana toiminut henkilö jatkaa hankepäällikön tehtävässä. Hankkeen valmisteluvaiheessa aloitetaan myös hankkeen turvallisuusvaatimusten määrittely. Tähän kuuluu sidosryhmäturvallisuuden näkökulmasta oleellinen vaihe eli sidosryhmäanalyysin laadinta, jonka tavoitteena on tunnistaa hankkeeseen liittyvät sisäiset ja ulkoiset sidosryhmät. Suunnitteluvaiheessa hankkeen ohjeistukset viimeistellään ja hankkeen jälkeisen ylläpitovaiheen järjestelyt valmistellaan ennen siirtymistä hankkeen toteutusvaiheeseen. Hankkeen toteutusvaiheessa tuotetaan ne osatekijät (kuten materiaalihankinnat), joilla suorituskykyvajeeseen halutaan vastata ja yhdistetään ne toimivaksi kokonaisuudeksi. Hankkeen päättämisvaiheessa hankkeen tuote eli suorituskykyratkaisu tarkastetaan ja siirretään linjaorganisaation käyttöön. (Pääesikunta 2017b, 10)

Hankkeen hallinta muodostuu kuvion 2 mukaisista kokonaisuuksista. Hankeen hallinnan perusteet määritetään hankesuunnitelmassa. Hankesuunnitelma on hankepäällikön työkalu joka määrittää henkilöstön vastuut ja tehtävät hankkeessa. Hanke pyritään jakamaan pienempiin kokonaisuuksiin, jolloin sen hallinta on helpompaa. Hankesuunnitelmassa sidosryhmäturvallisuuteen otetaan kantaa erityisesti suunnitelman kohdissa sidosryhmäanalyysi sekä hanketurvallisuus. Sidosryhmäanalyysin tarkoituksena on tunnistaa hankkeeseen liittyvät sidosryhmät eli ne henkilöt ja organisaatiot, jotka vaikuttavat jollain tapaa hankkeeseen tai joihin hankkeella on vaikutusta. Tämä vaatii hyvin tarkkaa sisäisen ja ulkoisen toimintaympäristön tarkastelua ja tätä analyysia päivitetään hankkeen edetessä. Tärkeää on tunnistaa myös sidosryhmiin liittyvät turvallisuusvaatimukset. Hankesuunnitelman turvallisuusliitteessä pitäisi olla hankkeen vaatimukset tarvittaville turvallisuuden aloille sekä mahdollisuuksien mukaan myös toimenpiteet niiden vaatimusten täyttämiseksi. (Pääesikunta 2017b, 11-17).



Kuvio 2: Hankkeen hallinnan osatekijät ja hankkeen vaiheet

Hankkeen hallinnan osatekijöistä tärkeitä hankkeen sidosryhmäturvallisuuden kannalta ovat erityisesti sidosryhmien hallinta, riskien hallinta ja turvallisuuden hallinta. Sidosryhmäanalyysi yhdessä hankkeelle laadittavan tiedonluokittelumatriisin kanssa antavat perusteita turvallisuusvaatimusten määrittelylle sekä riskienhallinnalle. Riskienhallinnalla pyritään tunnistamaan hankkeen henkilöstöön, omaisuuteen, tietoon, toimintaan, ympäristöön ja maineeseen kohdistuvat negatiiviset tapahtumat ja niihin varautuminen. Turvallisuuden hallinnalla tarkoitetaan käytännön toimenpiteitä, joilla hankkeen turvallisuusvaatimuksiin vastataan. (Pääesikunta 2017b, 7-17).

Mikäli suorituskykyvajeen paikkaaminen päätetään toteuttaa hankkimalla uutta materiaalia, voidaan hankkeen sisään perustaa hankintaprojekti. Hankintaprojektin käynnistämisestä päätetään yleensä hankkeen toteutusvaiheessa. Termiä hankinta käytetään silloin kuin Puolustusvoimat hankkii materiaalin, palvelun tai työn organisaation ulkopuolelta kaupallisin menetelmin. (Pääesikunta 2017b, 5-8). Hankkeen sidosryhmäturvallisuuden toimenpiteet painottuvat usein juuri hankintaprojekteihin siihen sisältyvästä kaupallisesta yhteistyöstä johtuen.

Kuten hanke niin myös hankintaprojekti jakaantuu neljään vaiheeseen: valmistelu-, suunnittelu-, toteutus- ja päättämisvaiheisiin. Hankkeisiin sisältyvän projektin valmistelu nivoutuu osin hankkeen suunnitteluvaiheeseen, jossa määritetään hankinnan tavoitteet ja valmistellaan toimeksianto hankinnasta sekä annetaan käsky projektin käynnistämiseksi. Tämän jälkeen käynnistyy hankinnan suunnitteluprosessi, jonka lopputuloksena syntyy projektisuunnitelma hankinnan toteuttamiseksi. Projektin toteuttaminen tarkoittaa hankinnan

toimeenpanoa projektisuunnitelman mukaisesti. Hankintaprojekti päättyy, kun hankinta on saatu toteutettua. (Kosola 2012, 25-26).

Hankintaprojektit toteutetaan pääasiassa Puolustusvoimien logistiikkalaitoksen järjestelmäkeskuksen toimenpitein. Logistiikkalaitoksen projektiohjeen (2017) mukaisesti projektinhallinnan osa-alueet noudattavat pääpiirteittäin kuviossa 2 esitettyjä hankkeen hallinnan osa-alueita sekä yleisiä projektinhallinnan standardeja. Kuten hankkeessa niin myös hankintaprojektissa laaditaan ja ylläpidetään sidosryhmäanalyysiä ja toteutetaan turvallisuuden- ja riskien hallintaa. Turvallisuuden hallinnalla pyritään varmistamaan projektin toteuttamiseen ja projektin tuotteeseen liittyvien turvallisuusnäkökulmien huomioon ottaminen hankinnan kaikissa vaiheissa. (Logistiikkalaitos 2017, 1-6). Projektin riskienhallinnan tavoitteena on tunnistaa ja analysoida projektiin sekä hankinnan henkilöstöön, materiaaliin ja tietoon kohdistuvat riskit sekä käsitellä niitä tarpeen mukaan (Pääesikunta 2015a, 40-41). Hankintaprojekti toteuttaa yleensä hankkeeseen liittyvät tietopyynnöt (RFI, Request for Information) ja tarjouspyynnöt (RFQ, Request for Quotation) mahdollisille materiaalin toimittajille sekä vastaanottaa vastaukset näihin. Nämä saattavat usein sisältää turvallisuusluokiteltua tietoa, jolloin sidosryhmäturvallisuuden toimenpiteitä tulee olla käytännössä huomioituna jo tässä vaiheessa hanketta. (Logistiikkalaitos 2017, 2-4).

2.2 Henkilöstö ja vastuut

Puolustusvoimissa hanketoimintaa ohjataan Pääesikunnan logistiikkaosaston toimesta. Hankkeet valmistellaan joko Pääesikunnan tai puolustushaaraesikuntien toimesta ja hankepäällikkö tulee yleensä samasta organisaatioista. Hankepäällikkö vastaa siitä, että hanke saavuttaa sille tehtäväksi annetun suorituskyvyn sen käyttöön myönnetyillä resursseilla. Hankepäällikkö vastaa oman toimivaltansa puitteissa hankkeen johtamisesta ja osatekijöiden yhteensovittamisesta. Hänen tehtäviin kuuluu hankkeen hallinta ja vastuu hankkeen kokonaisuudesta ja hänellä on määritetyt valtuudet päätösten sekä muutosten tekemiseen. Hankepäällikkö vastaa myös hankkeen turvallisuudesta. Hankepäällikön tehtäviin kuuluu hankesuunnitelman mukainen hankkeen toiminnan ohjaaminen, koordinointi ja valvonta. Hankepäällikkö jakaa tehtävät ja vastuualueet hankkeen henkilöstölle sekä laatii toimeksiantoja hankkeen toteuttamiseen liittyen. Hankepäällikön on tärkeää olla aktiivisesti yhteydessä hankeorganisaatioonsa ja hankkeen sidosryhmiin tilannekuvan ylläpitämiseksi. (Pääesikunta 2017b, 7,18).

Hankeorganisaatio muodostetaan henkilöistä, jotka osallistuvat hankkeeseen normaalien työtehtäviensä ohessa. Hankkeelle perustetaan yleensä ohjausryhmä sekä hankeryhmä. Ohjausryhmä huolehtii siitä, että hanke etenee kohti sille asetettuja tavoitteita ja hankeryhmän tehtävänä on hankkeen toimeenpano hankesuunnitelman mukaisesti. Hankeryhmää johtaa hankepäällikkö ja siihen osallistuvat muut hankkeen avainhenkilöt kuten

projektipäälliköt, tarvittavat edustajat puolustushaaroista sekä järjestelmävastuullisesta organisaatiosta ja tarpeen mukaan eri alojen, kuten turvallisuuden, asiantuntijoita. Hankepäällikkö suunnittelee ja osittaa hankkeen tarpeen mukaan alaprojekteihin, joita johtavat projektipäälliköt. Näitä ovat yleensä esimerkiksi hankintaprojekti ja käyttöönottoprojekti. (Pääesikunta 2017b, 6-8).

Projektipäällikkö vastaa projektin tavoitteiden saavuttamisesta hänelle annettujen resurssien puitteissa. Hankepäällikkö on toimeksiannossaan määrittänyt valtuudet minkä perustella projektipäällikkö voi tehdä päätöksiä ja muutoksia omaan projektiinsa liittyen. Esimerkiksi hankintaprojektin osalta projektipäällikkö on hänelle annettujen valtuuksien mukaisesti vastuussa hankinnan turvallisuudesta. Projektipäällikön vastuu on yleensä määritelty tarkemmin hankesuunnitelmassa. Projektipäällikkö vastaa suoraan hankepäällikölle ja raportoi hänelle säännöllisesti. (Pääesikunta 2017b, 18). Logistiikkalaitokseen kuuluva Järjestelmäkeskus vastaa hankintatoiminnan käytännön valmisteluista ja toteutuksesta ja se asettaa usein juuri hankintaprojektin päällikön projektin johtoon (Puolustusvoimat 2020b).

Hankkeeseen nimetään usein turvallisuusvastaava hankeorganisaatioon kuuluvien henkilöiden joukosta. Hankkeen turvallisuusvastaava johtaa hankkeen turvallisuusvaatimusten määrittämistä. Hänen tehtäviinsä voi kuulua esimerkiksi hankkeeseen liittyvien turvallisuusasioiden selvittäminen, hankintakohtaisten turvallisuusdokumenttien valmistelu sekä projektiryhmän, erityisesti hankepäällikön ja kaupallisen asianhoitajan, pitäminen ajan tasalla olemassa olevista sidosryhmäturvallisuuden järjestelyistä. (Pääesikunta 2015a, 44-45; Haastatteluaineisto 2020).

Puolustusvoimien turvallisuustarkastajat ovat sidosryhmäturvallisuuden asiantuntijoita. Kaikista puolustushaaraesikunnista sekä Logistiikkalaitoksesta löytyvät päätoimiset turvallisuustarkastajat, joiden tehtävänä on toimia yhteistyöstä vastuussa olevien henkilöiden turvallisuusasiantuntijoina. Turvallisuustarkastajan olisi hyvä olla mukana hankesuunnitelman turvallisuutta käsittelevien osien laadinnassa sekä hankepäällikön ja hankkeen turvallisuusvastaavan tukena turvallisuusasioiden selvittämisessä ja turvallisuusvaatimusten, kuten tarvittavien turvallisuusselvitysten ja turvallisuussopimusten, määrittelyssä ja valmistelussa. (Pääesikunta 2015a, 28; Haastatteluaineisto 2020).

Kaupallisen asianhoitajan tehtäviä turvallisuuden näkökulmasta on hankinta-asiakirjojen laatiminen turvallisuusnäkökohdat huomioiden. Tästä syystä hänen on tunnettava mahdollisen turvallisuussopimuksen sisältö ja sen mahdolliset vaikutukset kaupalliseen sopimukseen. Kaupallisissa sopimuksissa on huomioitava turvallisuus- ja salassapitolausekkeet sekä määritettävä kaupan purkuehdoksi myös turvallisuussopimuksissa ja -liitteissä mainitut ehdot. (Pääesikunta 2015a, 45).

2.3 Sidosryhmäturvallisuus

Sidosryhmäturvallisuuden vaatimukset tulevat lainsäädännöstä. Sidosryhmäturvallisuudella tarkoitetaan kaikkia menetelmiä ja toimenpiteitä, joilla suojataan julkisuuslain tai muun säädöksen perusteella salassa pidettäväksi tai turvallisuusluokitelluksi määrätty tieto tehtäessä yhteistyötä sidosryhmien kanssa. Julkisuuslain 26§:n mukaan viranomaisen on ennakolta varmistuttava tiedon asianmukaisesta suojaamisesta, jos viranomainen antaa salassa pidettävää tietoa organisaation ulkopuolelle, esimerkiksi yritykselle yhteistyön toteuttamista varten (Julkisuuslaki 621/1999). Myös hankintalain 64 § edellyttää hankintayksikön määrittävän riittävän tietoturvallisuuden tason hankintaan kohdistuvat riskit huomioiden (Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1397/2016). Lain julkisista puolustus- ja turvallisuushankinnoista 41 § antaa hankintayksikölle oikeuden asettaa hankinnalle tietoturvallisuutta koskevia vaatimuksia ja pyytää sitoumuksia sekä tietoja tietoturvallisuusvaatimuksien täyttämisestä. Näistä, kuten myös mahdollisista turvallisuusselvityksistä, on ilmoitettava tarjoajille etukäteen hankintailmoituksessa tai tarjouspyynnössä. (Laki julkisista puolustus- ja turvallisuushankinnoista 1531/2011; turvallisuusselvityslaki 726/2014).

Sidosryhmäturvallisuutta Puolustusvoimissa johtaa ja ohjaa Pääesikunta. Pääesikunta määrittää yleiset periaatteet sidosryhmäturvallisuuden toimenpiteiden toteuttamiselle ja kouluttaa turvallisuustarkastajat Puolustusvoimien tarpeisiin. Puolustusministeriö ohjaa sidosryhmäturvallisuuden järjestelyjä erityisesti kansainvälisen yhteistyön osalta. Puolustusministeriö ohjaa ja valvoo kansainvälisten tietoturvallisuusvelvoitteiden toteutumista puolustushallinnossa ja hyväksyy kansainvälisten hankkeiden turvallisuusdokumentaation. (Pääesikunta 2017a, 2-3).

Sidosryhmäturvallisuutta toteutetaan varmistamalla yhteistyöhön liittyvät turvallisuusjärjestelyt. Tähän sisältyy esimerkiksi yrityskohtaiset turvallisuussopimukset sisältäen turvallisuusauditoinnit, hankkeiden turvallisuusohjeet, yritys- ja henkilöturvallisuusselvitykset, turvallisuusjärjestelyiden valvonnan, turvallisuuden tilannekuvan ylläpidon sekä Puolustusvoimien ja yhteistyökumppaneiden henkilöstön kouluttamisen. (Pääesikunta 2017a, 3).

2.3.1 Salassa pidettävän tiedon käsittely

Tiedon salassa pidettävyys perustuu lakeihin. Puolustusvoimien hankkeiden osalta salassa pidettävän tiedon käsittelyä ohjaa erityisesti laki viranomaisen toiminnan julkisuudesta (621/1999), tiedonhallintalaki (906/2019) ja asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Näiden lisäksi kansainvälisissä hankkeissa on huomioitava kansainvälisen tietoturvallisuuslain (588/2004) sekä valtioiden välisten tietoturvallisuussopimusten (GSA, General Security Agreement) asettamat vaatimukset erityissuojattavalle tietoaineistolle.

Julkisuuslain 2 §:n mukaan Suomen viranomaisten asiakirjat ovat julkisia, ellei niitä ole julkisuuslain 24 §:n tai jonkin muun lain perusteella erikseen määritetty salassa pidettäväksi. Lain mukaan jokaisella kansalaisella on oikeus saada tietoa julkisesta asiakirjasta. Salassa pidettävästä viranomaisen asiakirjasta ei saa antaa tietoa muuten kuin julkisuuslain 26 §:n määrittämissä tapauksissa. (Laki viranomaisen toiminnan julkisuudesta, 621/1999).

Julkisuuslaki määrittää mitkä ovat viranomaisen salassa pidettäviä asiakirjoja ja laki julkisen hallinnan tiedonhallinnasta sekä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa määrittävät ohjeet valtionhallinnon asiakirjojen turvallisuusluokittelulle. Turvallisuusluokittelua käytetään kansallisesti vain julkisuuslain määrittämissä tapauksissa ja laki kansainvälisistä tietoturvallisuusvelvoitteista määrittää viranomaisten toimenpiteet kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Valtionhallinnon asiakirjojen turvallisuusluokittelua voidaan soveltaa myös toisen maan viranomaiselta tai kansainväliseltä toimielimeltä saatuun asiakirjaan, mikäli kansainvälisissä tietoturvallisuusvelvoitteissa asiaa ei ole ohjeistettu. (Laki julkisen hallinnon tiedonhallinnasta 906/2019; Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019).

Viranomaisten asiakirja on turvallisuusluokiteltava ja turvallisuusluokka on merkittävä asiakirjaan, mikäli asiakirja tai siihen sisältyvä tieto on julkisuuslain 24 §:n 1 momentin 2, 5 tai 7-11 kohdan perusteella salassa pidettävä ja asiakirjaan sisältyvän tiedon väärinkäyttö tai oikeudeton paljastuminen voi aiheuttaa vahinkoa esimerkiksi yleiselle turvallisuudelle, maanpuolustukselle tai kansainvälisille suhteille. Merkintää turvallisuusluokituksesta ei saa tehdä muissa tapauksissa, ellei sen tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai se liittyy muuten kansainväliseen yhteistyöhön. (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

Erityissuojattavalla tietoaineistolla tarkoitetaan salassa pidettäviä asiakirjoja ja materiaalia, joka on turvallisuusluokiteltu kansainvälisen tietoturvallisuusvelvoitteen mukaisesti. Käytännössä se tarkoittaa toisen valtion viranomaisten turvallisuusluokittelemaa tietoa, jota käsitellään Suomen viranomaisten tai elinkeinonharjoittajien toimesta esimerkiksi kaupallisen yhteistyön seurauksena. Erityissuojattava tietoaineisto on pidettävä salassa

turvallisuusluokituksensa mukaisesti. Näitä sääntöjä sovelletaan sekä viranomaisiin että yrityksiin ja heidän henkilöstöönsä silloin, kun nämä ottavat osaa turvallisuusluokiteltuun hankkeeseen. (Ulkoministeriö 2016, 4-6).

Kansainvälisten tietoturvallisuusvelvoitteiden toteutumista Suomessa ohjaa ja valvoo ulkoministeriön kansallinen turvallisuusviranomainen (National Security Authority, NSA). Kansallisen turvallisuusviranomaisen tehtävänä on valvoa, että erityissuojattavia tietoaineistoja käsitellään ja ne suojataan asianmukaisesti. Puolustusministeriö, Pääesikunta, Suojelupoliisi sekä liikenne- ja viestintävirasto Traficom toimivat oman toimialueensa osalta määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA). Määrätyillä turvallisuusviranomaisilla on lailla säädettyjä tehtäviä. Puolustusministeriö, Pääesikunta ja Suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa. Liikenne- ja viestintävirasto Traficom toimii kansallisen turvallisuusviranomaisen asiantuntijana (National Communication Security Authority, NCSA) tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. (Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004).

Erityissuojattavaa tietoaineistoa käsittelevän viranomaisen ja elinkeinonharjoittajan on huolehdittava siitä, että henkilöt, jotka tarvitsevat tietoa tehtäviensä hoitamiseen ovat nimetty etukäteen ja vain heillä on pääsy tietoaineistoon. Laki velvoittaa kansallisen turvallisuusviranomaisen ilmoittamaan toiselle sopimusosapuolelle, mikäli turvallisuusluokitellun tiedon suoja on vaarantunut tai tietoturvallisuuttaa koskevia määräyksiä on loukattu. Kansallinen turvallisuusviranomainen on myös lain mukaan velvoitettu selvittämään asian ja saattamaan syyllisen syytteenalaiseksi. (Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004).

Kansainväliset tietoturvallisuussopimukset ovat valtiosopimuksia, joissa Suomi sitoutuu suojamaan sopimuksissa määritetyin tietoturvallisuuden toimenpitein suomeen sopimuksella luovutetun turvaluokitellun materiaalin. Sopimus voi olla kahden valtion tai suomen ja monikansallisen yhteisön kuten EU:n tai NATO:n kanssa tehty. Näitä tietoturvallisuusvelvoitteita ohjaa laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Turvallisuusluokitellun tiedon suojaamisesta sopiminen kahden tai monen valtion välillä edellyttää aina valtiosopimusta, jossa sopimusosapuolet velvoitetaan huolehtimaan toisen sopimusosapuolen turvallisuusluokitellusta materiaalista asianmukaisesti. (Ulkoministeriö 2016, 4-5).

Esimerkiksi Suomen ja Yhdysvaltojen välinen tietoturvallisuussopimus, joka on ratifioitu valtioneuvoston asetuksella 42/2013, velvoittaa sopijaosapuolet suojaamaan toiselta osapuolelta välillisesti tai suoraan saadut turvallisuusluokitellut tiedot sopimuksessa määritetyin tavoin. Sopimuksessa määritetään, miten turvallisuusluokitellut tiedot merkitään

materiaaleihin ja mitkä ovat turvallisuusluokkien vastaavuudet. Sopimuksessa määritetään myös se, miten turvallisuusluokiteltu tieto suojataan, mistä tulee varmistua ennen tiedon luovuttamista toiselle osapuolelle ja miten tietoa voidaan välittää. Sekä viranomais- että yksityisiin organisaatioihin tulee määrittää pätevä vastuuhenkilö, jolla on vastuu ja valtuudet tiedon suojaamiseen sekä valvontaan. Lisäksi tietoturvallisuussopimuksessa määritetään ohjeet muun muassa vierailuista, turvallisuusstandardeista, tiedon kopioinnista, tiedon hävittämisestä, turvallisuusluokituksen alentamisesta tai poistamisesta sekä tiedon katoamisesta tai vaarantumisesta. (Valtioneuvoston asetus 42/2013).

Valtioiden väliset tietoturvallisuussopimukset muodostavat näin ollen perustan luottamukselle kahden tai useamman valtion välisessä tiedonvaihdossa. Aseteknologian tekniset yksityiskohdat ja valtioiden sotilaallinen suorituskyky halutaan yleensä pitää salassa turvallisuuden tai yrityssalaisuuden näkökulmasta. Ilman luottamusta ei näitä tietoja voitaisi vaihtaa, eikä näin ollen hankintoja kyettäisi suorittamaan. Suomella on tällä hetkellä 19 voimassa olevaa tietoturvallisuussopimusta toisen valtion, ja viisi tietoturvallisuusopimusta eri yhteisöjen: Euroopan avaruusjärjestön (ESA), Organisation for Joint Armament Cooperation (OCCAR), Pohjois-Atlantin liiton (NATO), Pohjoismaiden sekä Euroopan unionin jäsenvaltioiden kesken (Ulkoministeriö 2020).

Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) säädetään asiakirjojen turvallisuusluokittelusta, turvallisuusluokkien merkitsemisestä sekä turvallisuusluokiteltujen asiakirjojen käsittelystä. Suomen kansallisia turvallisuusluokkia (TL) on tiedonhallintalaissa määritetty neljä. Turvallisuusluokkien jako perustuu tiedon paljastumisen tai väärinkäytön mahdollisten seuraamusten vakavuudelle TLIV-luokan lievästä vahingosta aina TLI-luokan erityisen suureen vahinkoon asti.

TURVALLISUUSLUOKKA	SUOMEKSI	RUOTSIKSI	ENGLANNIKSI
TLI	ERITTÄIN SALAINEN	YTTERST HEMLIG	TOP SECRET
TLII	SALAINEN	HEMLIG	SECRET
TLIII	LUOTTAMUKSELLINEN	KONFIDENTIELL	CONFIDENTIAL
TLIV	KÄYTTÖ RAJOITETTU	BEGRÄNSAD TILLGÅNG	RESTRICTED

Taulukko 1: Turvallisuusluokitukset ja niiden ruotsin- ja englanninkieliset vastineet. (Valtioneuvoston asetus 1101/2019).

Oikeus turvallisuusluokitellun materiaalin käsittelyyn voidaan antaa vain henkilölle, jolla on tehtäviensä puolesta tarve käsitellä turvallisuusluokiteltua tietoa ja kenelle on selvitetty turvallisuusluokiteltujen tietojen käsittelyä koskevat ohjeet. Viranomaisen on dokumentoitava henkilöt, joille käsittelyoikeus on myönnetty, kun kyseessä on oikeus käsitellä turvallisuusluokkien I, II ja III tietoaineistoja. (Valtioneuvoston asetus 1101/2019).

Salassa pidettäviä tietoja voidaan tiedonhallintalain 14§:n mukaisesti siirtää yleisessä tietoverkossa turvallisuusalueiden ulkopuolelle vain salattua tai muuten suojattua menetelmää käyttäen. Tiedon turvallisuusluokitus on huomioitava käytettävien tietojärjestelmien ja tiedonsiirtomenetelmien salauksen turvallisuudessa. (Valtioneuvoston asetus 1101/2019).

Puolustusvoimien sisäinen tietoturvaohje on asiakirja, joka ohjeistaa miten julkisuuslain, tiedonhallintalain sekä turvallisuusluokitteluasetuksen ja kansainvälisen tietoturvallisuusvelvoitelain asettamiin vaatimuksiin vastataan Puolustusvoimissa. Puolustusvoimien tietoturvaohje määrittää ne asiat, jotka tulee huomioida eri turvallisuusluokituksen omaavien tietoaineistojen käsittelyssä. Seuraavassa on nostettu esiin erityisesti Puolustusvoimien ja sen ulkopuolisten sidosryhmien väliseen tiedon käsittelyyn liittyviä asioita.

Mikäli salassa pidettävän ja turvallisuusluokitellun tietoaineiston siirtäminen julkisessa verkossa on turvallisuusluokituksensa puolesta mahdollista (TLIV-TLIII), on siirtäminen organisaatiosta ulos tehtävä hyväksytyllä salaustuotteella salattuna ja turvasähköpostia käyttäen. TLIV-tason materiaali voidaan siirtää myös salaamattomana turvasähköpostilla, mikäli vastaanottavan sidosryhmän tietojärjestelmä ja tietoliikennejärjestelmä on auditoitu ja hyväksytty TLIV-tasolle. Tietojensiirrossa on huomioitava se, että tietojen vastaanottaja on kyettävä varmistamaan ennen kuin hän pääsee käsittelemään tietoja. Vaihdettaessa salassa pidettävää tietoa sidosryhmien kanssa tulee varmistua turvallisuussopimuksen voimassaolosta sekä palveluympäristön tarkastuksista. Salassa pidettävän materiaalin osalta tulee myös varmistua siitä, että sidosryhmällä on hyväksytyt menettelytavat heidän käyttöön luovutetun materiaalin asianmukaisesta käsittelystä. Tämä varmistuminen perustuu yritysturvallisuusselvityksen ja riittävien turvallisuussopimusten laatimiseen tai voimassaolon tarkistamiseen. Turvallisuusluokiteltuja asiakirjoja tulee säilyttää Puolustusvoimien turva-alueilla tai sidosryhmän hyväksytyssä tilassa ja pääsy niihin pitää olla suojattu sivullisilta. (Pääesikunta 2020, 18-24).

TLIV (KÄYTTÖ RAJOITETTU) -tason asiakirjojen käsittelyssä tulee huomioida samat asiat kuin mitkä koskevat kaikkia turvallisuusluokiteltuja asiakirjoja. Tämän lisäksi pitää huomioida,

että TLIV-tason paperiasiakirjoja tulee säilyttää turvallisuusalueilla ja mikäli niitä säilytetään sähköisessä muodossa esimerkiksi tietokoneella tai ulkoisessa muistissa, pitää siinä olla riittävä salausratkaisu eikä sitä saa jättää valvomatta. TLIV asiakirjojen siirtäminen yleisessä verkossa on mahdollista salattuna tai turvasähköpostilla. TLIV paperiasiakirjojen lähettäminen on mahdollista myös postin välityksellä. (Pääesikunta 2020, 24-25)

TLIII (LUOTTAMUKSELLINEN) -tason asiakirjojen käsittelyssä tulee huomioida samat asiat kuin TLIV -tason asiakirjoissa. TLIV-tasoa koskevien vaatimusten lisäksi TLIII tietoa käsitteleville henkilöille tulee olla myönnetty käsittelyoikeus TLIII-tason tietoon, heillä tulee olla tehtävään perustuva tarve tiedon käsittelyyn ja henkilöt on dokumentoitava. TLIII-tason tietojen käsittely turva-alueen ulkopuolella tapahtuu sähköisesti vaatimukset täyttävän päätelaitteen ja tietoliikennejärjestelyn avulla. Tästä voidaan poiketa vain erillisellä luvalla poikkeustapauksissa. Tämän lisäksi pitää huomioida, että TLIII tason paperiasiakirjat on säilytettävä turva-alueella erikseen hyväksytyssä säilytysyksikössä. Kun käsitellään TLIII-tason asiakirjoja sähköisessä muodossa, tulee hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä pienentää tarpeen mukaisilla turvallisuustoimenpiteillä. TLIII-tason paperiasiakirjojen siirtäminen on mahdollista kuriiria käyttäen. (Pääesikunta 2020, 26-28).

TLII (SALAINEN) -tason asiakirjojen käsittelyssä tulee huomioida samat asiat kuin TLIII-tason asiakirjoissa. TLIII-tasoa koskevien vaatimusten lisäksi tulee huomioida, että TLII-tason asiakirjojen sähköinen käsittely tapahtuu ainoastaan Puolustusvoimien sisäisessä erillisessä ympäristössä. TLII-tason asiakirjoja ei saa siirtää yleisessä verkossa. TLII-tason paperiasiakirjojen siirtäminen on mahdollista kuriiria käyttäen. (Pääesikunta 2020, 29-31).

2.3.2 Turvallisuusselvitykset

Hankkeiden turvallisuuden yhtenä elementtinä ovat turvallisuusselvitykset. Turvallisuusselvitysten tarkoituksena on pyrkiä ennaltaehkäisemään vahingollista toimintaa, joka kohdistuu valtion turvallisuuteen tai kansainvälisiä suhteisiin, maanpuolustukseen tai merkittävään yksityiseen taloudelliseen etuun. Turvallisuusselvityksiä voidaan laatia henkilöistä tai yrityksistä ja näin ollen niitä kutsutaan joko henkilöturvallisuusselvityksiksi tai yritysturvallisuusselvityksiksi. Henkilöturvallisuusselvitysten perusteena voi olla useita erilaisia työhön tai toimeksiantoon liittyviä tehtäviä joissa vaaditaan erityistä luotettavuutta kuten oikeus turvallisuusluokitellun tiedon käsittelyyn. Yritysturvallisuusselvitys laaditaan hankkeiden yhteydessä yleensä silloin, jos hankkeessa ollaan laatimassa yrityksen kanssa yhteistyösopimusta, johon sisältyy TLI-TLIII tasoa olevan turvallisuusluokitellun tai muuten salassa pidettävän tiedon luovuttamista yritykselle. Yritysturvallisuusselvityksellä arvioidaan yrityksen luotettavuutta ja sitoumustenhoitokykyä sekä sen tietoturvallisuuden tasoa. (Turvallisuusselvityslaki 2014).

Turvallisuusselvityksien laatimisesta päättää yleensä Suojelupoliisi mutta Puolustusvoimien toimintaan ja hankkeisiin liittyen päätöksen tekee Pääesikunta (Turvallisuusselvityslaki 2014). Pääesikunnassa toimiva määrätty turvallisuusviranomainen (PE DSA) tekee PV:n henkilö- ja yritysturvallisuusselvitykset ja osallistuu kansainvälisten turvallisuusselvitystodistusten laadintaan. Pääesikunnan operatiivisen osaston turvallisuussektori toimii linkkinä kansallisen turvallisuusviranomaisen suuntaan selvitettäessä ulkomaisten yritysten yritys- ja henkilöturvallisuustodistusten voimassaoloa. (Pääesikunta 2017a, 5).

Yritysturvallisuusselvityksen laadinnassa käytetään hyväksi laadittua hakemusta, määritettyjä tietolähteitä sekä yritykselle tehtävää tarkastusta. Tarkastus kohdistuu yrityksen tiloihin ja tietoliikennejärjestelyihin. Näillä pyritään tarkastamaan tietojen suojaamisen taso, yrityksen tilavalvonta sekä henkilöstön koulutustaso. (Turvallisuusselvityslaki 2014). Yritysten tietoturvallisuuden auditointiin voidaan käyttää KATAKRI-auditointityökalua, joka on määritetty myös kansainvälisen tietoturvallisuusvelvoitteen mukaiseksi auditointityökaluksi. Yritysturvallisselvityksen päätteeksi yritys allekirjoittaa sitoumuksen vaaditun turvallisuustason ylläpitämiseksi. (Ulkoministeriö 2015, 17-18).

Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyy henkilö- ja yritysturvallisuusselvitykset ja niiden perusteella myönnettävät turvallisuusselvitystodistukset. Henkilöturvallisuusselvitystodistus on englannin kielellä personnel security clearance (PSC) ja yritysturvallisuusselvitystodistus on facility security clearance (FSC). Yritysturvallisuusselvitys toimii pohjana kansainväliselle yritysturvallisuustodistukselle, minkä yritys tarvitsee osallistuakseen kansainväliseen tarjouskilpailuun tai hankintaan. Mikäli yrityksellä on yritysturvallisuusselvitystodistus niin sen henkilöistä ei vaadita erillisiä henkilöturvallisuusselvitystodistuksia vaan ne sisältyvät yritysturvallisuusselvitystodistukseen. Kansainvälistä yritysturvallisuustodistusta voi hakea Suomen tai ulkomaan viranomainen tai kohdeyritys itse. Yritys- ja henkilöturvallisuusselvitystodistuksen myöntää kansallinen turvallisuusviranomainen ja se edellyttää Suomessa turvallisuusselvityslain mukaisen perusmuotoisen tai laajan turvallisuusselvityksen laadintaa. Puolustusvoimat voi hakea kansallisen turvallisuusviranomaisen kautta kansainvälistä yritysturvallisuusselvitystodistusta ulkomaisesta yrityksestä, jonka kanssa Puolustusvoimat on laatimassa turvallisuusluokiteltua sopimusta. Tällöin kyseisen yrityksen kotimaan kanssa tulee olla voimassa oleva tietoturvallisuussopimus. Tietoturvallisuussopimukset määrittävät yleensä, että yritysturvallisuustodistus tarvitaan vasta TLIII (CONFIDENTIAL) -tasolta ylöspäin. (Ulkoministeriö 2015, 16-17). Vain ne yritykset, joille on myönnetty yritysturvallisuusselvitystodistus, voivat käsitellä kansainvälisen tietoturvallisuusvelvoitteen määrittämää erityissuojattavaa tietoaineistoa. Turvallisuusselvitys ja kansainvälinen turvallisuusselvitystodistus ovat voimassa viisi vuotta ja ne voidaan tarvittaessa uusia viranomaisen, hakijan tai selvityksen kohteen toimesta, mikäli voimassaolon jatkaminen on tarpeellista. (Laki kansainvälisistä tietoturvallisuusvelvoitteista 2004).

2.3.3 Sidosryhmäturvallisuus hankkeissa

Sidosryhmäturvallisuuden toimenpiteet hankkeessa määräytyvät hankekohtaisista turvallisuusvaatimuksista. Tarve sidosryhmäturvallisuuden toimenpiteille muodostuu hankkeessa yleensä kaupallisen yhteistyön seurauksena, kun sidosryhmälle luovutetaan, siltä vastaanotetaan tai yhteistyön myötä syntyy salassa pidettävää tietoa. Hankkeen sidosryhmä voi olla kotimainen tai kansainvälinen kumppani, esimerkiksi aseteknologiaa valmistava yritys tai toinen valtio. Usein kansainvälisten yritysten tuotteisiin saattaa sisältyä myös erityissuojattavaa tietoa eli toisen valtion turvaluokittelemaa tietoa. Koska esimerkiksi asejärjestelmien tekniset yksityiskohdat, maanpuolustuksen suorituskyky ja käyttöperiaatteet sekä yritysten tuotekehitys ovat usein sensitiivistä tietoa, liittyy tämänkaltaisen tiedon vaihtoon paljon uhkia ja riskejä. Jotta nämä uhat ja riskit olisivat hankkeen hallittavissa, on hankkeessa huomioitava erilaisia toimenpiteitä salassa pidettävän tiedon suojaamiseksi. Tämän tunnistaminen on yhteistyöstä vastuussa olevan henkilön eli hankepäällikön vastuulla. Turvallisuusvaatimukset tulee huomioida jo hanketta valmisteltaessa. Turvallisuusvaatimusten määrittelyssä hankepäällikön tukena toimivat Puolustusvoimien turvallisuustarkastajat. Turvallisuusvaatimukset määräytyvät tapauskohtaisesti salassa pidettävän tiedon turvallisuusluokan ja siihen kohdistuvan uhan, yhteistyön laadun, sekä asiaan vaikuttavien muiden säädösten ja sopimusten perusteella. Sidosryhmäturvallisuutta toteutetaan turvallisuusjärjestelyiden todentamisella ja valvonnalla, sidosryhmien ja niiden henkilöstön luotettavuuden arvioinnilla, koulutuksella sekä tilannekuvan ja uhka-arvion ylläpitämisellä. (Pääesikunta 2017a, 2-3).

Hankkeen vaatimukset sidosryhmäturvallisuudelle määräytyvät pitkälti sidosryhmän sekä yhteistyön aikana käsiteltävän tiedon turvallisuusluokan perusteella. Sidosryhmät määritellään hankkeen sidosryhmäanalyysissä ja luovutettava tieto tulee analysoida tiedonluokittelumatriisin avulla. Tiedonluokittelumatriisilla kuvataan mitä ja minkä turvaluokituksen tasoista tietoa joudutaan missäkin hankkeen vaiheessa luovuttamaan tai vastaanottamaan. Tiedonluokittelumatriisissa tulisi huomioida myös hankkeen aikana mahdollisesti syntyvä uusi tieto ja sen turvallisuusluokitus. Tämän seurauksena on tärkeää tunnistaa mihin säädöspohjaan hankkeeseen liittyvän tiedon suojaamisvaatimukset perustuvat, sillä lainsäädäntö asettaa erilaisia vaatimuksia salassa pidettävän tiedon suojaamiselle sen alkuperästä riippuen. (Logistiikkalaitos 2020).

Kansallisen yhteistyön osalta pohjan sidosryhmäturvallisuuden toteuttamisperiaatteille muodostaa Puolustusvoimien ja sidosryhmän välinen turvallisuussopimus. Turvallisuussopimuksella sovitaan turvallisuusjärjestelyistä ja -menettelyistä yhteistyöhön liittyen ja tämä sopimus mahdollistaa turvallisuusluokkien TLIV-TLII materiaalin luovuttamisen suomalaisen yrityksen käsiteltäväksi. Turvallisuussopimus on aina yrityskohtainen ja määräaikainen tai se voi olla yhteistyö- tai hankekohtainen eli se kattaa vain kyseessä olevaan

yhteistyöhön liittyvän tiedon vaihdon. TLIV-tasoisen tiedon käsittelyyn riittää myös ns. turvallisuussitoumus. Turvallisuussitoumusta käytetään usein silloin kun yhteistyö saattaa jäädä lyhytaikaiseksi käsittäen esimerkiksi yksittäisen hankkeen tarjouspyyntövaiheen. Turvallisuussitoumuksella sidosryhmä sitoutuu hankkeen eli Puolustusvoimien asettamiin turvallisuusjärjestelyihin. Salassa pidettävää tietoa käsitteleviltä henkilöiltä otetaan myös vaitiolovakuutus. Vaitiolovakuutus otetaan sen jälkeen, kun henkilöt ovat osallistuneet heille annettuun, lain velvoittamaan koulutukseen. Vaitiolovakuutus toimii varmenteena sille, että henkilö on ymmärtänyt salassapitovelvoitteen merkityksen ja tietää miten salassa pidettävää tietoa tulee käsitellä. TLIII- ja TLII tason tietoja käsitteleviltä henkilöiltä edellytetään myös voimassa olevia henkilöturvallisuusselvityksiä. Usein turvallisuusselvitykset tehdään myös TLIV-tason tietojen käsittelyä varten. Puolustusvoimien turvallisuussopimus toimii myös hyvänä lähtökohtana yritysturvallisuusselvitykselle sekä yrityksen kansainväliselle yritysturvallisuusselvitystodistukselle, mikäli yrityksellä on sille tarve. (Logistiikkalaitos 2020).

Kansainvälisten hankkeiden turvallisuuskäytänteet ja turvallisuusdokumentit ovat Pihlajamäen (2020) mukaan kehittyneet kansainvälisten toimijoiden yhteistyönä. Tässä kehitystyössä NATO:n ja EU:n turvallisuusregulaatioilla on merkittävä rooli. EU-maista suurin osa eli 24 on myös NATO:n jäsenmaita. Näin ollen on luonnollista, että NATO:n ja EU:n käyttämät turvallisuuden prosessit ja menetelmät siirtyvät myös suomen viranomaisia koskeviin menettelytapoihin. Kansainvälisessä yhteistyössä selkeänä erona on se, että Puolustusvoimilla ei ole viranomaisen toimivaltaa ulkomaisia yrityksiä kohtaan. Pohja kansainväliselle sidosryhmäturvallisuudelle muodostuu valtioiden välisistä tietoturvallisuussopimuksista (GSA). Niissä määritetään perusteet myös hankkeiden turvallisuustoiminnalle. Yhtenä keskeisenä elementtinä tässä on kansainväliset yritys- ja henkilöturvallisuusselvitystodistukset jotka myöntää kunkin maan oma kansallinen turvallisuusviranomainen. Yritysturvallisuusselvitystodistukset vaaditaan, mikäli on tarpeen luovuttaa yritykselle TLIII- tai TLII-tason tietoa. TLIV- tason tietoa voidaan luovuttaa, mikäli yritys sitoutuu hankkeen määrittämiin turvallisuusvaatimuksiin esimerkiksi kirjallisella turvallisuussitoumuksella. Tätä voidaan käyttää esimerkiksi tilanteessa, missä tarjouspyyntöihin sisältyy TLIV-tason tietoa. Myös tiedon siirrossa on huomioitava valtiosopimusten edellyttämät toimenpiteet. Tasojen TLII-TLIII tiedon siirtäminen fyysisesti rahtina tai kuriirilla tulee perustua molempien valtioiden DSA viranomaisten toimesta hyväksyttyihin suunnitelmiin. Sähköinen tiedonsiirto tulee olla salattua ja salausohjelman tulee olla Traficomin hyväksymä. Mikäli hankkeessa käsitellään sähköisesti kansainvälistä erityissuojattavaa tietoa, tulee varmistaa, että tietojärjestelmät ja verkot täyttävät edellytykset ja tarvittaessa niille tulee hankkia NCSA:n akkreditointi. Kaikki tämä vaatii huolellista suunnittelua ja näillä toimenpiteillä on vaikutusta hankkeen kustannuksiin ja aikatauluihin. Kansainvälisessä yhteistoiminnassa onkin erityisen tarkkaan harkittava, milloin ja minkä tasoista turvallisuusluokiteltua tietoa on todella tarpeen luovuttaa. Kansainvälisessä toiminnassa yrityksiä ohjaa ja valvoo kyseisen maan oma

kansallinen turvallisuusviranomainen. Tieto- ja tarjouspyyntövaiheissa kannattaa välttää turvaluokitellun tiedon luovuttamista, ellei se ole täysin välttämätöntä, jo pelkästään yhteistyön käytännön toteutuksen kannalta. (Pihlajamäki 2020).

Käytännön turvallisuustoimenpiteet kansainvälisissä hankkeissa määrätään ja yhteen sovitetaan turvallisuusasiakirjoilla, joita ovat kansainvälisen käytännön mukaan Security Aspects Letter (SAL) ja Program Security Instructions (PSI) asiakirjat. PSI asiakirjaan osaksi liittyy myös Security Classification Guide (SCG) eli tiedonluokittelumatriisi. (Logistiikkalaitos 2020). Puolustusministeriö tukee hanketta kansainvälisten hanketurvallisuusdokumenttien laadinnassa ja hyväksyy PSI asiakirjat. PSI on hanketurvallisuusohje, joka laaditaan yleensä isoihin ja monimutkaisiin hankkeisiin tai hankkeeseen, johon osallistuu useiden maiden edustajia. PSI-dokumentti tai muu vastaava turvallisuusohje on välttämätön osa laajempia hankkeita, joissa käsitellään turvallisuusluokiteltua tietoa. Dokumentin tarkoituksena on kerätä yhteen kyseistä hanketta koskevat turvallisuusohjeet ja muodostaa ne periaatteet, joilla hankkeen turvallisuusvaatimuksiin vastataan. PSI-dokumentti voi olla varsinaisen hankintasopimuksen liitteenä ja sitä tulee päivittää tarvittaessa. Mikäli hankkeeseen tai hankintaan liittyy osahankintoja, voidaan niihin laatia SAL-dokumentti PSI:n pohjalta. SAL-dokumentti on PSI-dokumenttia suppeampi asiakirja. Siinä tuodaan esiin hankkeen turvallisuusvaatimukset ja ne hankkeen elementit mitkä vaativat suojaustoimenpiteitä. SCG-dokumentti on tiedonluokittelumatriisi eli ohje tiedon turvallisuusluokittelusta. SCG tuotetaan PSI-asiakirjan liitteeksi. SCG määrittää hankeen eri elementtien sisältämän tiedon turvallisuusluokitukset ja tällä varmistetaan, että kaikilla hankkeen osapuolilla on sama tieto hankkeen eri prosessien tai komponenttien luokituksesta. Kaikkia hankkeen turvallisuusdokumentteja tulee päivittää tarpeen mukaan hankkeen edetessä. Perusteet hankkeiden turvallisuusasiakirjoihin tulevat kansainvälisestä turvallisuussäännöstöstä sekä kansainvälisistä tietoturvallisuussopimuksista ja esimerkiksi NATO on luonut mallin PSI- ja SAL-asiakirjoista omiin hankkeisiinsa liittyen. Hanketurvallisuusasiakirjat määräävät turvallisuustoiminnan minimitason ja niissä on määriteltävä turvallisuuden vastuut ja johtaminen, hankkeen elementtien turvallisuusluokitukset ja niiden merkinnät sekä rinnastettavuudet. Lisäksi ohjeella määritetään vaatimukset ja perusteet esimerkiksi pääsy- ja kulkuoikeuksille sekä vierailukäytänteille, turvallisuusselvitystodistuksille, tilaturvallisuudelle, käytettäville tietojärjestelmille ja tiedonsiirrolle, turvallisuuskoulutukselle, viestinnälle sekä turvallisuuspoikkeamien hallinnalle. (Pihlajamäki 2020).

Sidosryhmäturvallisuuden näkökulmasta hankkeen tulee siis tuottaa sidosryhmäanalyysi ja tiedonluokittelumatriisi jo hankkeen valmisteluvaiheessa. Näiden avulla sidosryhmäturvallisuuteen liittyvät prosessit, kuten turvallisuusselvitys- ja turvallisuussopimusprosessit, saadaan suunniteltua ja valmisteltua riittävän aikaisessa vaiheessa. Mikäli hankkeeseen liittyy kansainvälistä yhteistoimintaa, tulee ottaa huomioon,

että kansainvälisen yritysturvallisuustodistuksen saaminen saattaa kestää hyvinkin pitkään. Hankkeen suunnitteluvaiheessa tulee käynnistää tarvittavat turvallisuussopimus- ja asiakirjavalmistelut sekä turvallisuusselvitysprosessit, hankkeen turvallisuustaso huomioiden. Myös turvallisuussopimusten valmistelu, erityisesti kansainvälisissä hankkeissa, vaatii hyvin paljon aikaa. Ennen kuin varsinaista hanketta päästään toteuttamaan valittujen yhteistyökumppaneiden kanssa, tulee turvallisuusasiakirjat ja -sopimukset valmistella ja ne tulee allekirjoittaa osana kaupallisia sopimuksia.

2.4 Tapaustutkimus: hankkeen sidosryhmäturvallisuuden elementit

Tapaustutkimuksella tarkoitetaan yleisesti erilaisia ja monipuolisia menetelmiä tiedon hankkimiseksi jostain yksittäisestä tapahtumasta, yksilöstä tai muuten rajatusta kokonaisuudesta (Saaranen-Kauppinen & Puusniekka, 2006). Tapaustutkimuksen tavoitteena on tutkittavan yksittäisen kohteen tai ilmiön erilaisten ominaisuuksien mahdollisimman tarkka ja totuudenmukainen kuvaaminen (Hirsjärvi, Remes & Sajavaara 2009, 134-135). Tapaustutkimukselle on tunnusomaista, että se muodostaa itsessään selkeän kokonaisuuden. Tiedonkeruu voi tapahtua lukuisilla eri tavoilla ja tiedon analysointi voidaan toteuttaa niin määrällisin kuin laadullisinkin menetelmin. Tapaustutkimukset ovatkin melko yleisiä työelämässä, sillä sen periaatteet ovat sovellettavissa moniin projekteihin sekä kehittämis- tai arviointitöihin. Tapaustutkimuksen tutkimuksellisena heikkoutena voidaan nähdä tulosten yleistettävyys. Kun tutkittava asia on tarkkaan rajattu yksittäinen tapahtuma, on siitä hankala tehdä yleistettäviä ja kaikkialla päteviä yhteenvetoja. Kuitenkin siitä saadut tulokset voivat olla hyödynnettävissä muuallakin, vaikka yleispäteviä johtopäätöksiä ei voitaisikaan tehdä. (Saaranen-Kauppinen & Puusniekka, 2006).

Tapausesimerkkinä on geneerinen hanke, johon sisältyy yhteistoimintaa kansainvälisten sidosryhmien kanssa ja turvallisuusluokitellun tiedon vaihtoa. Esimerkki perustuu Puolustusvoimissa 2010-luvun aikana toteutettuun hankkeeseen, jossa päädyttiin hankkimaan asejärjestelmä ja siihen liittyvää materiaalia ulkomailta. Hanke oli julkinen ja siitä löytyy julkista tietoa Internetistä mutta se käsitellään tässä anonyymisti, sillä hankkeeseen liittyvät asiakirjat ovat osin turvallisuusluokiteltuja. Tapaustutkimuksen materiaali on kerätty hankkeen projektipäällikön haastattelusta ja sitä on osin tuettu hankkeeseen liittyvillä dokumenteilla.

Hanke perustui valtioneuvoston puolustusselontekoon sekä Puolustusvoimien kehittämisohjelmaan. Hankkeen omisti Maavoimat ja se kesti kokonaisuudessaan noin kymmenen vuotta. Hankkeen avulla Suomelle hankittiin uusi asejärjestelmä puuttuvan suorituskyvyn tuottamiseksi. Kyseistä asejärjestelmätyyppiä ei Suomessa valmisteta, joten ainakin hankkeen päähankinta eli varsinaisen asejärjestelmän osto oli tehtävä ulkomailta. Hankkeen valmisteluvaiheessa lähetettiin turvallisuusluokitellut, TLIV-tasoa olevat

tietopyynnöt (RFI, Request for information) yhdeksälle yritykselle heidän mahdollisista järjestelmäratkaisuistaan. Tietopyynnöissä edellytettiin, että yritys käsittelee tietopyyntöä luottamuksellisesti ja että, yritys sitoutuu erilliseen turvallisuussopimukseen myöhemmin hankkeen edetessä. Hankkeen suunnitteluvaihe kesti kolme vuotta ja tietopyyntöjen vastausten perusteella hanke lähetti TLIV-tasoa olevat tarjouspyynnöt (RFQ, Request for quotation) kolmelle yritykselle varsinaista tarjouskilpailua varten. Tarjouskilpailun jälkeen tärkein päähankinta päätettiin toteuttaa Yhdysvaltojen kanssa FMS-kauppana (Foreign Military Sales), jossa myyjä osapuolena toimi Yhdysvaltojen liittovaltio. Tämän päähankinnan lisäksi tehtiin useita muita hankintoja. Päähankinnan lisäksi hankkeeseen liittyi toinen hankinta, joka sisälsi turvallisuusluokitellun tiedon vaihtoa ja myös se suuntautui ulkomaille. Myös kotimaisilta toimittajilta ostettiin järjestelmän käyttöön liittyvää materiaalia mutta näihin ei liittynyt turvallisuusluokitellun tiedon vaihtoa. Hanke ositettiin kahteen projektiin eli hankinta- ja ylläpito sekä suorituskyvyn käyttöönottoprojektiin. Hankintaprojektista vastasi Puolustusvoimien logistiikkalaitoksen järjestelmäkeskus, joka toteutti hankinnat. Hankintojen toteuttaminen tapahtui neljän vuoden aikana. (Haastatteluaineisto 2020).

Hankesuunnitelman mukaisesti kyseisen hankkeen turvallisuustoimenpiteiden tavoitteena oli suojata hankkeeseen liittyvät, maanpuolustuksen kannalta tärkeät tiedot sekä ehkäistä ja estää tahalliset vahingon- tai väkivallanteot, onnettomuudet ja varkaudet sekä toteutuessaan pienentää näiden vaikutusta hankkeelle. Hankkeen turvallisuustoiminnan keskiössä oli anastusherkän materiaalin suojaaminen. Hankkeen turvallisuusasioista vastasi hankepäällikkö. Hänen apunaan turvallisuusasioissa työskenteli hankeupseeri, joka oli nimetty hankkeen turvallisuusvastaavaksi. Myös hankkeen sidosryhmiä velvoitettiin asettamaan turvallisuusvastaava omaan organisaatioonsa, jotta yhteistyö turvallisuusasioissa saatiin tehtyä sujuvaksi. Tämä myös velvoitetaan Suomen ja Yhdysvaltain välisessä tietoturvallisuussopimuksessa. Toimivaltaista turvallisuustarkastajaa ei hankkeeseen ollut nimetty mutta hankeupseerilla oli mahdollisuus konsultoida oman organisaationsa turvallisuustarkastajia tarvittaessa. Hankeupseeri avusti myös hankintaprojektin päällikköä, joka vastasi varsinaisen hankinnan turvallisuudesta. Tämän hankkeen osalta hankinta on siinä mielessä merkittävä sidosryhmäturvallisuuden näkökulmasta, että sen puitteissa tapahtui suurin osa tiedonvaihdosta ulkomaisten sidosryhmien kanssa. Hankeupseeri vastasi hankkeeseen liittyvien turvallisuusasioiden kouluttamisesta hankehenkilöstölle painopisteen ollessa tietoturvallisuuteen liittyvissä asioissa. (Haastatteluaineisto 2020).

Turvallisuusvaatimusten osalta hankkeessa tunnistettiin tarve turvaluokitellun tiedon käsittelylle sidosryhmien kanssa jo hyvin aikaisessa vaiheessa. Hankkeelle laadittiin sidosryhmäanalyysi jo hyvin aikaisessa vaiheessa sen painopisteen ollessa organisaation sisäisten sidosryhmien tunnistamisessa. Hankkeen valmisteluvaiheessa tehtiin tarkempi sidosryhmäanalyysi, jossa oli mukana myös ulkoiset sidosryhmät ml. mahdolliset ulkomaiset materiaalintoimittajat. Hankkeessa käsiteltävää, luovutettavaa ja vastaanotettavaa tietoa

selvitettiin ja analysoitiin tiedonluokittelumatriisin avulla. Sidosryhmäanalyysiä ja tiedonluokittelumatriisi päivitettiin hankkeen edetessä. Hankkeen alusta asti oli selvää, että hankkeessa joudutaan luovuttamaan turvallisuusluokiteltua tietoa ja vastaanotetaan erityissuojattavaa tietoa. (Haastatteluaineisto 2020).

Hankkeessa luovutettiin TLIV-luokan tietoa jo hankkeen valmisteluvaiheessa. Tämä vaikutti esimerkiksi käytettävissä oleviin tiedonvälitysmenetelmiin. TLIV-tietoa välitettiin salattuna sähköpostina ja CD-levyillä kirjatun kirjeen sisällä. Hankkeessa vastaanotettiin erityissuojattua CONFIDENTIAL ja SECRET -tasojen tietoa ja tämä aiheutti vaatimuksia mm. tilaturvallisuusratkaisuille materiaalin säilyttämisen osalta. Erityissuojattava tieto kuljetettiin kuriirilla tai rahtina. Ennen tietopyyntöjen lähettämistä hankeupseeri varmisti, onko kohdeyrityksillä voimassa oleva yritysturvallisuustodistus ja mille tasolle mahdollinen selvitys on tehty, jotta TLIV-tasoa olevat tietopyynnöt voitiin lähettää yrityksille. (Haastatteluaineisto 2020).

Päähankintaan liittyvät turvallisuusasiat sovittiin hankinnan toimitussopimuksessa eikä varsinaisesti erillistä hanketurvallisuusohjelmaa laadittu. Sopimuksessa sovittiin mm. tiedon välittämisen, kuljetusten turvallisuuden ja tilaturvallisuuden vaatimuksista sekä menetelmistä. Hankintaprojekti järjesti muutamia palavereita Suomessa, joissa käsiteltiin TLIII-tasoista tietoa. Tämän vuoksi hankeupseeri käsitteli vierailupyynnöt normaaleiden käytäntöjen mukaisesti. Haasteena tässä havaittiin riittävän turvallisuusluokitustason tilojen saatavuus. (Haastatteluaineisto 2020).

Kaiken kaikkiaan esimerkkihankkeen vaatimukset sidosryhmäturvallisuudelle etenkin erityissuojavan tiedon suojaamiseen liittyen olivat merkittävät esimerkiksi turvallisuusrakentamisen ja turvallisuusauditointien osalta. Rakentaminen on hyvin aikaa vievää toimintaa, joten tästä olisi voinut aiheutua merkittäviä viivästyksiä, mikäli turvallisuusnäkökulmia ei olisi huomioitu ajoissa. Turvallisuusauditoinnit sisälsivät myös ns. turvallisuusvierailuja (VNA 42/2013). Tässä hankkeessa turvallisuus otettiin heti hankkeen alusta alkaen huomioon ja hankkeen turvallisuusvaatimuksiin reagoitiin tarpeen mukaan hankkeen edetessä. Näin ollen turvallisuuteen liittyvät asiat eivät aiheuttaneet viivästyksiä tai muita ongelmia hankkeelle.

3 Hankkeiden turvallisuuden kehittäminen

Tämä opinnäytetyö on luonteeltaan laadullinen eli kvalitatiivinen kehittämistyö. Laadullisuus kehittämis- tai tutkimustyössä tarkoittaa, että työssä pyritään kuvailemaan käsiteltävää ilmiötä mahdollisimman kokonaisvaltaisesti siihen liittyvien käsitteiden, sanojen ja ihmisten henkilökohtaisten kokemusten kautta. Laadulliselle tutkimukselle on tunnusomaista, että ihmiset ovat tutkimuksen keskiössä ja heidän henkilökohtaiset näkökulmansa nousevat vahvasti esiin. (Hirsjärvi, Remes & Sajavaara 2009, 161-164). Laadullinen tutkimusote ei kuitenkaan sulje kokonaan pois määrällistä tarkastelua, mitä on käytetty tässä työssä tulosten keskinäisen merkittävyyden arviointiin (Alasuutari 2011, 26).

Laadullisessa tutkimuksessa aineisto kerätään usein haastatteluiden, kyselyiden, erilaisten dokumenttien tai havainnoinnin menetelmin. Näitä menetelmiä voidaan myös yhdistellä. (Sarajärvi & Tuomi 2009, 71). Tässä opinnäytetyössä varsinainen tutkimusaineisto koostuu asiantuntijoiden teemahaastatteluiden aineistosta. Asiantuntijoista koostuva kohdejoukko on valittu tarkoituksenmukaisesti mikä on myös yksi laadulliselle tutkimukselle tyypillinen piirre (Hirsjärvi, Remes & Sajavaara 2009, 164).

Tässä työssä käytetty kehittämismenetelmä on aineistolähtöinen sisällönanalyysi. Sisällönanalyysin avulla pyritään tutkimusaineiston sanalliseen kuvailuun. Sisällönanalyysi on tyypillinen laadullisen tutkimuksen menetelmä, sillä sen avulla kyetään löytämään aineistosta merkityksiä ja niiden suhteita sekä muodostamaan näistä kokonaisuuksia. Sisällönanalyysia käytetään, kun aineistosta pyritään löytämään yhteneväisyyksiä tai erilaisuuksia, toiminnan logiikkaa tai tiettyjä toistuvia teemoja. Tutkimusaineisto voi kuvata esimerkiksi haastateltavien kokemuksia tai ajattelutapoja tutkittavasta asiasta. Jos tutkimusaineistosta lasketaan havaintoyksiköitä esimerkiksi toistuvia sanoja tai ajatuskokonaisuuksia puhutaan sisällön erittelystä eli kvantifioimisesta. (Vilkka 2005, 139-140).

Aineistolähtöinen sisällönanalyysi perustuu induktiiviseen päättelyyn joka tarkoittaa, että tutkimuksen tulokset pyritään luomaan puhtaasti varsinaiseen tutkimusaineistoon perustuen. Toinen sisällönanalyysin muoto on teorialähtöinen eli deduktiivinen sisällönanalyysi, jossa ensin muodostetaan teoria, johon aineiston analyysi perustuu. Näiden väliin sijoittuu teoriaohjaava sisällönanalyysi, jota kutsutaan myös abduktiiviseksi sisällönanalyysiksi. (Sarajärvi & Tuomi 2009, 95-98). Tässä kehittämistyössä on myös abduktiivisen päättelyn logiikalle tunnusomaisia piirteitä, koska työn tietoperusta on jossain määrin vaikuttanut kehittämistehtävän muodostumiseen ja ennakkokäsityksiin tutkittavasta asiasta. Täydellisen induktion logiikka on ylipäätään kiistanalaista, koska puhtaasti havaintoihin perustuva ja täysin tutkijasta tai aikaisemmasta tiedosta riippumaton päättely ei ole mahdollista (Sarajärvi & Tuomi 2009, 95). Tämän työn tulokset perustuvat haastatteluaineistosta tehtyihin havaintoihin eikä aikaisempi teoria suoraan ohjaa tulosten raportointia. Aineistosta tehtyjen

yksittäisten havaintojen perusteella on muodostettu yleistyksiä, joten analyysi noudattaa induktiivista logiikkaa.

Sisällönanalyysin tekniikoita avulla voidaan käyttää monenlaisten dokumenttien ja lähteiden tulkintaan. Sisällönanalyysin avulla järjestetystä aineistosta on kyettävä tekemään myös laadukkaita johtopäätöksiä. Tämä on paljon kiinni tutkijan ammattitaidosta, kokemuksesta ja kyvystä yhdistellä asiaan liittyvää tietoa toisiinsa. (Sarajärvi & Tuomi 2009, 103).

Sisällönanalyysi on laadullisen tutkimuksen perusanalyysimenetelmä. Sarajärvi & Tuomen (2009, 91-94) mukaan sisällönanalyysi koostuu seuraavista vaiheista:

- Kiinnostuksen kohteiden määrittäminen kehittämistehtävän mukaisesti.
- Aineiston tutkiminen, kiinnostavan materiaalin merkitseminen, kerääminen ja erottelu muusta aineistosta.
- Aineiston luokittelu ja analyysi.
- Yhteenvedon kirjoittaminen.

Aineistolähtöistä sisällönanalyysiä on käytetty tässä työssä haastatteluaineiston analysoinnissa ja työn tulosten muodostamisessa. Menetelmävalintaa on ohjannut aihepiirin luonne ja käsiteltävän tiedon saatavuus ja käytettävyys julkisessa työssä. Esimerkiksi varsinaiset hankesuunnitelmat ovat usein turvallisuusluokiteltuja, joten niitä ei ollut mahdollista käyttää työn aineistona. Tämän aihepiirin asiantuntijat ovat suhteellisen pieni joukko ihmisiä ja aiheeseen liittyy paljon toimintatapoja ja menetelmiä, jotka ovat syntyneet kokemusten ja yhteistyön kautta mutta varsinainen dokumentaatio niistä puuttuu tai se ei ole yleisesti saatavilla. Näin ollen kehittämisen kohteena olevaan ilmiöön on päästy parhaiten käsiksi asiantuntijoiden teemahaastatteluiden avulla. Haastatteluiden tulokset, työn tietoperusta ja muu lähdemateriaali sekä tekijän omat näkemykset toimivat johtopäätösten ja kehitysehdotusten perustana.

Tutkimushaastattelut muodostavat työn tärkeimmän lähdeaineiston. Haastatteluiden tarkoituksena on välittää asiantuntijoiden ajatukset ja kokemukset tutkittavasta aiheesta (Hirsjärvi & Hurme 2008, 41). Tutkimushaastattelut olivat puolistrukturoituja haastatteluita eli teemahaastatteluita. Teemahaastattelun ominaispiirteisiin kuuluu, että haastateltavat tuntevat haastattelun aihepiirin, haastattelija on selvittänyt tutkittavaa asiaa itselleen tärkeimmiltä osin ja rakentanut tämän perusteella haastattelurungon, joka keskittyy tutkimuksen aiheen kannalta tärkeisiin teemoihin. Teemahaastattelu tarkoittaa sitä, että haastatteluissa keskustellaan kehittämistehtävän kannalta tärkeistä teemoista ja haastattelun tarkoituksena on, että haastateltava antaa oman kuvauksensa haastatteluun valituista teema-alueista (Hirsjärvi & Hurme, 47-48).

3.1 Teemahaastatteluiden toteutus

Työhön haastateltiin kaikkiaan yhdeksän henkilöä. Haastateltavat henkilöt valikoituivat haastateltaviksi asiantuntijuutensa perusteella ja heidän valintaansa ohjattiin tämän opinnäytetyön toimeksiantajan taholta. Valituilla asiantuntijoilla on paras kokemus hankkeista ja niiden sidosryhmäturvallisuuden toteuttamisesta omalla vastuualueellaan (liite 4). Haastattelu sopii erittäin hyvin tämän työn aineistonkeruumenetelmäksi, koska työn aihe on hyvin laaja ja moniulotteinen.

Haastatteluiden avulla kerättiin asiantuntijoiden kokemuksia siitä, miten heidän kokemuksensa perusteella sidosryhmäturvallisuus toteutuu Puolustusvoimien hankkeissa, mitkä ovat heidän mielestään onnistumisen avaintekijöitä hankkeiden sidosryhmäturvallisuudessa, minkälaisia haasteita he ovat kohdanneet sekä miten he kehittäisivät hankkeiden sidosryhmäturvallisuutta Puolustusvoimissa. Lisäksi kävimme keskustelua hanketurvallisuuden käsitteestä ja miten sitä tulisi määritellä, mutta sitä ei ole tässä opinnäytetyössä raportoitu. Tästä on laadittu erillinen muistio organisaation sisäiseen käyttöön.

Haastattelut toteutettiin elo-syyskuun aikana syksyllä 2020. Suoritin yhteydenotot haastateltaviin ja lähetin heille lyhyen haastattelupyynnön sähköpostilla, jossa selvitin työn tarkoitusta ja tavoitteita sekä haastattelun toteutustapaa. Haastattelupyyntö löytyy tämän opinnäytetyön liitteenä (liite 2). Kaikissa haastatteluissa oli kolme yhteneväistä teemaa, joiden osalta asiantuntijat saivat tuoda näkemyksiään esiin. Haastatteluiden teemat olivat: hanketurvallisuuden käsite, hanketurvallisuuden nykytila ja hanketurvallisuuden kehittäminen. Haastatteluissa käytetty lomake löytyy työn liitteenä (liite 3).

Haastattelut suoritettiin joko henkilökohtaisen tapaamisen kautta tai Skypen välityksellä. Voimassaolleet etätyösuositukset kyseisenä ajankohtana johtivat siihen, että haastatteluista pääosa tehtiin Skypen välityksellä. Tämä ei merkittävästi haitannut haastatteluiden tekemistä koska teema oli hyvin substanssikeskeinen eikä esimerkiksi haastateltavien tunnetilojen tulkinnalle ollut tarvetta. Haastattelut tallennettiin ja ne litteroitiin pian haastatteluiden jälkeen.

3.2 Haastatteluiden analysointi

Haastatteluaineiston aineistolähtöinen sisällönanalyysi koostuu Sarajärvi & Tuomen (2009) mukaan aineiston litteroinnista, pelkistämisestä, ryhmittelystä ja abstrahoinnista. Tässä työssä sisällönanalyysi on toteutettu sitten, että litteroitu aineisto luettiin ensin läpi ja sen sisältö tutkittiin useaan kertaan. Litteroiduista aineistosta etsittiin kehittämistehtävän kannalta oleellinen ja kiinnostava tieto. Tämän jälkeen aineisto pelkistettiin eli redusoitiin siten, että vain työn kannalta oleellinen tieto jäi käsiteltäväksi. Jäljelle jäänyt aineisto on ryhmitelty niistä löydettyjen yhteneväisten ajatuskokonaisuuksien perusteella neljään osaan. Aineiston abstrahoinnin kautta on muodostettu yhteensä 15 alaluokkaa, kuusi yläluokkaa sekä neljä pääluokkaa. Nämä neljä pääluokkaa muodostavat työn tulokset. (Sarajärvi & Tuomi, 2009, 108-113). Aineiston ryhmittely toteutettiin merkitsemällä redusoitu aineisto eri väreillä niiltä osin kuin se kosketti jotain näistä neljästä ajatuskokonaisuudesta. Värikoodattu aineisto ryhmiteltiin allekkain kukin väri omaan taulukkoonsa. Värikoodattu aineisto luettiin jälleen läpi ja tästä aineistosta abstrahoitiin alaluokkia, yläluokkia ja pääluokka seuraavan esimerkin mukaisesti.

Esimerkki haastatteluaineistosta*: Sidosryhmäturvallisuuden asiat tulee miettiä jokaisessa hankkeessa tapauskohtaisesti. Nämä vaatimukset tulee määritellä heti hankkeen alussa ja niitä tulee päivittää hankkeen kuluessa, jotta niistä ei aiheudu myöhemmin viiveitä hankkeen läpiviemiselle*. Tästä muodostettiin seuraavanlaiset alaluokat: "huolellinen turvallisuusvaatimusten määrittely mahdollistaa oikeat toimintatavat" ja "turvallisuusvaatimusten määrittely on aloitettava heti hankkeen alussa". Tämän ajatuskokonaisuuden yläluokka on: "huolellinen turvallisuusvaatimusten määrittely mahdollistaa asianmukaisen tiedon käsittelyn hankkeen alusta alkaen" ja pääluokka on: "valmistelu". Pääluokkien osalta sisältö kvantifioitiin laskemalla kuinka monta kertaa kyseiseen pääluokkaan kuuluva ajatuskokonaisuus mainittiin aineistossa ja kuinka monessa haastattelussa se tuli esille. Tällä erittelyllä ole merkittävää vaikutusta työn tulosten kannalta, sillä asioiden esiintyvyys haastatteluissa ei ole eksaktisti vertailukelpoista. Tämä kuitenkin auttoi työn tekijää luomaan painotuksia tulosten raportoinnissa.

Esimerkki tästä analysointimallista on kuviossa 3.

ESIMERKKI AINEISTOSTA	ALALUOKAT	YLÄLUOKKA/PÄÄLUOKKA	Haastattelut/ Esiintyvyys
Sidosryhmäturvallisuuden asiat tulee miettiä jokaisessa hankkeessa tapauskohtaisesti. Nämä vaatimukset tulee määritellä heti hankkeen alussa ja niitä tulee päivittää hankkeen kuluessa, jotta niistä ei aiheudu myöhemmin viiveitä hankkeen läpiviemiselle.	1.) Huolellinen turvallisuusvaatimusten määrittely mahdollistaa oikeat toimintatavat. 2.) Turvallisuusvaatimusten määrittely on aloitettava heti hankkeen alussa.	Huolellinen turvallisuusvaatimusten määrittely mahdollistaa asianmukaisen tiedon käsittelyn hankkeen alusta alkaen. / VALMISTELU	7/23
Hankepäälliköt ovat avainasemassa hankkeiden läpiviemisessä. Hankepäälliköillä tulee olla riittävä turvallisuuden asiantuntemus käytössä hankkeen alusta alkaen.	1.) Hankepäällikkö tarvitsee käyttöönsä turvallisuus- ja hankealan asiantuntemusta. 2.) Asiantuntemuksen oltava hankepäällikön käytössä hankkeen alusta alkaen.	Hankepäälliköllä oltava käytettävissään turvallisuusalan asiantuntemusta hankkeen alusta alkaen. / HENKILÖSTÖ	5/12
Hankkeet vaativat laajaa ymmärrystä ja ne ovat usein luonteeltaan hyvin yksilöllisiä, joten saadut opit eivät välttämättä päde seuraavassa hankkeessa. Myös henkilöstön vaihtuvuus vaikeuttaa kokemustiedon siirtämistä.	1.) Koulutuksen oltava säännöllistä ja ajankohtaista henkilöstön vaihtuvuudesta johtuen. 2.)Turvallisuus- ja hankehenkilöstön osaamisen kasvattaminen tärkeää yhteistoiminnan sujuvuuden varmistamiseksi.	Henkilöstön osaamisen säännöllinen ylläpitäminen ja kasvattaminen. / OSAAMINEN	7/15
Turvallisuusmääräykset ja asiaan liittyvät sisäiset normit ovat selkeitä ja riittävän kattavia mutta jonkilainen virallinen "ruohonjuuritason" toimenpideohje erityisesti kansainvälisen yhteistyön näkökulmasta voisi helpottaa toimintaa.	1.) Nykyinen normitus on riittävä mutta sen ajanmukaisuudesta on huolehdittava. 2.) Kansainvälisten turvallisuuskäytänteiden toteuttamisen ohjeistusta voisi kehittää.	Ohjeet ja työkalut mahdollistavat laadukkaan käytännön toiminnan. / OHJEET JA TYÖKALUT	5/15

Kuvio 3: Teemahaastatteluiden analysointi

Työn tulokset muodostuvat näistä neljästä aineistosta esiin nousseesta pääluokasta ja niiden sisältöjen tulkinnoista. Aineiston analysoinnin ja alustavan raportoinnin jälkeen haastatteluiden tulokset lähetettiin haastateltaville vielä kommentoitavaksi mahdollisten väärinymmärrysten poissulkemiseksi.

4 Kehittämistyön tulokset

Teemahaastatteluiden sisällönanalyysin kautta aineistosta nousi esiin neljä pääluokkaa mihin tulisi kiinnittää huomiota hankkeiden turvallisuuden kehittämiseksi. Nämä neljä luokkaa ovat:

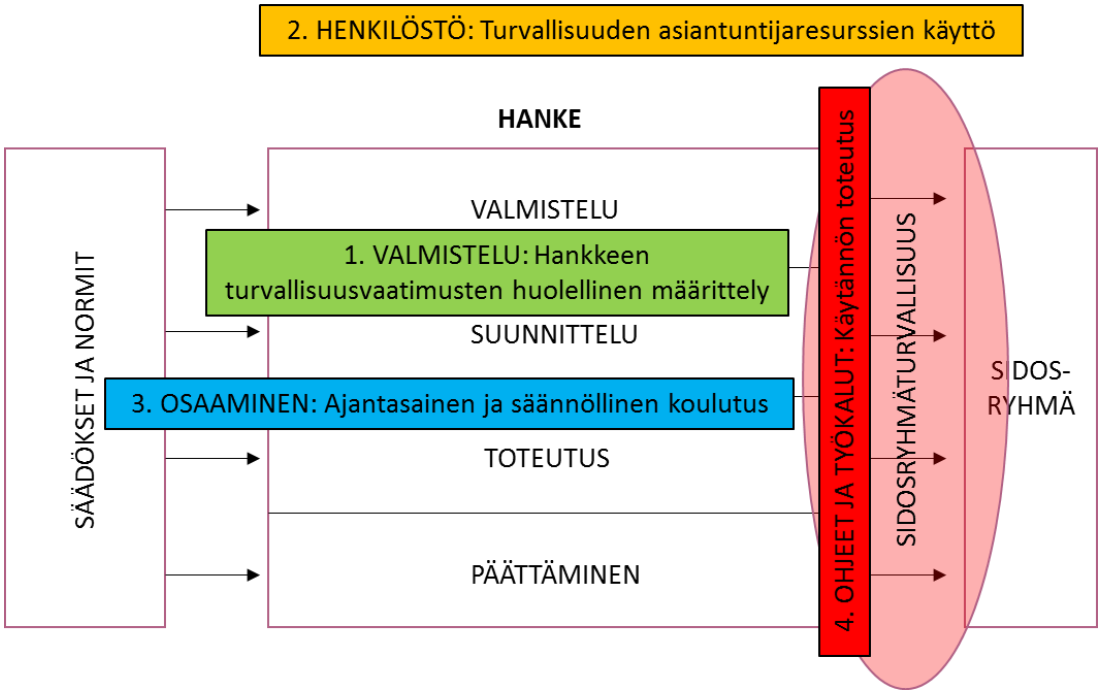
1. VALMISTELU: Hankkeen turvallisuusvaatimusten huolellinen määrittely

2. HENKILÖSTÖ: Turvallisuuden asiantuntijaresurssien käyttö

3. OSAAMINEN: Ajantasainen ja säännöllinen koulutus

4. OHJEET JA TYÖKALUT: Käytännön toteutus

Nämä neljä luokkaa ovat opinnäytetyön viitekehykseen sidottuna seuraavassa kuvassa:



Kuvio 4: Opinnäytetyön tulokset

Seuraavissa alaluvuissa esittelen haastatteluiden tulokset tarkemmin. *Kursivoidulla tekstillä* on esitetty haastatteluaineistosta kirjoitettuja yhteenvetoja, jotka kuvaavat kyseisestä pääluokkaa koskevia asioita. Yhteenvedot perustuvat kahden tai useamman henkilön haastatteluaineistoon, ellei muuta ole mainittu. Yhteenvedot eivät ole suoria lainauksia, mutta niillä kuvataan haastatteluissa esiin nousseita asioita.

4.1 Valmistelu

Aineiston perusteella tärkeimmäksi osatekijäksi hankkeiden sidosryhmäturvallisuuden onnistumisessa nousi hankkeen turvallisuusasioiden huolellinen valmistelu ja suunnittelu hankkeen alussa. Tämä asia nousi litteroidusta aineistosta esiin oman tulkintani mukaan yhteensä noin 19 kertaa.

Turvallisuusnäkökulmat tulee ottaa heti hankkeen alussa huomioon. Tämä käsittää mm. sidosryhmäanalyysin, tiedonluokittelumatriisin laadinnan, turvallisuusvaatimusten analysoinnin, säädöspohjan huomioimisen sekä tarvittavien asiantuntijaresurssien hankkimisen. (Haastatteluaineisto 2020).

Huolellisella turvallisuusnäkökulmien analysoinnilla ja toimenpiteiden valmistelulla varmistutaan siitä, että hankkeen turvallisuus rakentuu oikeille perustuksille heti hankkeen alusta alkaen. Tämä tarkoittaa muun muassa sitä, että hankkeen alussa on selvitettävä, joudutaanko hankkeessa luovuttamaan tai vastaanottamaan salassa pidettävää tietoa sekä mihin säädöspohjaan tiedon salassa pidettävyys ja käsittely perustuvat.

Hankkeen alussa tulee analysoida ne tiedot mitkä joudutaan luovuttamaan PV:n ulkopuolisille, kansainvälisille tai kotimaisille, sidosryhmille. Tämän lisäksi tulee tehdä hankkeeseen liittyvien tietojen turvallisuusluokka-analyysi eli laatia tiedonluokittelumatriisi ja analysoida mitä näistä tiedoista joudutaan käsittelemään PV:n ulkopuolisten tahojen kanssa. Jos joudutaan luovuttamaan turvallisuusluokiteltua tietoa, niin sen perusteella tulee määritellä hankkeen vaatimukset sidosryhmäturvallisuudelle. (Haastatteluaineisto 2020).

Sidosryhmäanalyysi hankkeessa tarkoittaa sidosryhmäturvallisuuden näkökulmasta erityisesti Puolustusvoimien ulkoisten sidosryhmien tunnistamista. Tiedonluokittelumatriisi on tietojen turvallisuusluokituksen analyysi hankkeessa luovutettavan, vastaanotettavan tai luotavan tiedon turvallisuusluokituksen osalta. Aineistosta nousi esiin yksittäisen vastaajan erittäin tärkeä huomio tähän liittyen.

Luovutettavien tietojen turvallisuusluokka on määritettävä tarkasti ja sen jälkeen on vielä tarkkaan mietittävä, että mitä näistä on pakko toimittaa sidosryhmälle ja mitä ei. TLIV-tason turvallisuussopimus on yritykselle merkittävästi edullisempi TLII-tason sopimus. Valmisteluiden huolellisuus on siis tärkeää myös yrityksen näkökulmasta. (Haastatteluaineisto 2020).

Turvallisuusluokituksen määrittely tulee tehdä tarkasti ja tiedon yliluokittelua "varmuuden vuoksi" tulee välttää, koska mitä korkeamman turvallisuusluokan tietoa käsitellään, niin sitä korkeammat vaatimukset sen suojaamiselle on. Tämä tarkoittaa yleensä myös korkeampia kustannuksia.

Säädöspohja, jonka perusteella tieto on salassa pidettävää, määrittää tiedon käsittelyn periaatteet. Tämän säädöspohjan tunnistaminen, osana turvallisuusvaatimusten määrittelyä, nousi aineistosta esiin useita kertoja. Mikäli tiedon salassa pidettävyys perustuu julkisuuslakiin (621/1999) tehdään sen turvallisuusluokittelu ja huomioidaan siitä johtuvat velvoitteet valtionhallinnon turvallisuusluokitteluasetuksen (VNA 1101/2019) sekä Puolustusvoimien erityisvaatimusten mukaisesti. Mikäli esimerkiksi hankkeessa vastaanotetaan kansainvälisen tietoturvallisuusvelvoitteen mukaista erityissuojattavaa tietoaineistoa kuten salaiseksi luokiteltua asejärjestelmäteknologiaa, on siitä aiheutuvat vaatimukset huomioitava kansainvälisen tietoturvallisuusvelvoitelain (588/2004) sekä valtioiden välisten tietoturvallisuussopimusten ja niissä annettujen vaatimusten mukaisesti. Seuraava huomio nousi esille yksittäisessä haastattelussa.

Avaintekijänä on tunnistaa, minkälaista tietoa hankinnassa on tarpeen käsitellä. Pitää tunnistaa ja tutustua olemassa oleviin vaatimuksiin, joihin Suomi on sitoutunut kansainvälisesti. Esimerkiksi tietoturvasopimukset on tehty eri maiden kanssa ja ne eivät kaikki ole samanlaisia. Tämän vuoksi on täysin mahdollista, että syntyy tilanteita joissa jonkun maan kanssa ei voida tehdä samoja asioita mitä tehdään jonkin toisen maan kanssa. (Haastatteluaineisto 2020).

Kuten esimerkiksi Suomen ja Yhdysvaltojen välisessä tietoturvallisuussopimuksessa (VNA 42/2013) on mainittu, tämä voi tarkoittaa hankkeen näkökulmasta esimerkiksi TLII-tason edellyttämiä tilaturvallisuuden, kulunvalvonnan ja henkilöstöturvallisuuden toimenpiteitä. Näihin toimenpiteisiin vaikuttaa myös paljon se missä muodossa tieto on. Muistitikulle todennäköisesti löytyy helposti tilaa riittävän turvallisuusluokituksen omaavasta kassakaapista mutta jos TLII-tason laite on kuorma-auton kokoinen, se saattaa tarkoittaa rakennustöiden aloittamista turvallisuusvaatimusten täyttämiseksi. Huolellisuus turvallisuustoimenpiteiden suunnittelussa on tärkeää paitsi tiedon ja suorituskyvyn suojaamisen, niin myös organisaation luotettavuuden ja maineenhallinnan näkökulmasta. Tämä on tärkeää erityisesti kansainvälisten sidosryhmien kanssa toimittaessa, jolloin turvallisuusasioissa korostuu luottamus yhteistyöosapuolen kansallisiin turvallisuusviranomaisiin. Tässä on yksittäisessä haastattelussa asiasta kuvattu esimerkki.

Yhtenä avaintekijänä suomalaisten viranomaisten kansainvälisessä toiminnassa on hankintojen yhteensovittamisen kansainvälisten toimijoiden ja kansainvälisten sopimusten kanssa. Käytännössä tämän asian huomiotta jättäminen on näkynyt esimerkiksi suomalaisen viranomaisen vaatiessa kansainvälistä yritysturvallisuustodistusta tasolle TLIV (restricted). Tämä on monessa tietoturvallisuussopimuksessa suljettu yritysturvallisuusselvitysten ulkopuolelle eli tälle tasolle ei tehdä yritysturvallisuusselvityksiä. Tämän vaatiminen esimerkiksi tarjouskilpailussa aiheuttaa ongelmia paitsi sen käytännön toteutuksen kanssa niin myös yritysten yhdenvertaisen kohtelun näkökulmasta. Lisäksi asia saattaa olla

ristiriidassa valtiosopimuksen kanssa. On hyvin tärkeää, että hankinnan valmisteluvaiheessa katsotaan vaatimusten yhteensopivuus kansainvälisten tietoturvallisuusvelvoitteiden kanssa. (Haastatteluaineisto 2020).

Sidosryhmäturvallisuuden keinoin voidaan varmistaa hankeen turvallinen toteutus Suomen tai toisen valtion omistaman salassa pidettävän tiedon suojaamisen näkökulmasta. Hankkeen sujuvan ja turvallisen toteutumisen vuoksi turvallisuusvaatimuksia tulee määritellä jo hankkeen alkuvaiheessa, jotta hankkeen turvallisuus lähtee heti alusta asti rakentumaan oikein. Hankkeen valmisteluvaiheessa tapahtuvaa turvallisuusvaatimusten määrittelyä ja niiden päivittämistä tarpeen mukaan painotettiin aineistossa noin 15 kertaa.

4.2 Henkilöstö

Hankepäällikkö on erittäin tärkeässä ja vaativassa roolissa. Useissa haastatteluissa korostettiin hankepäällikön merkitystä ja vastuuta hankkeen turvallisuudesta. Erittäin tärkeää on, että hän tunnistaa tarpeen hankkeen turvallisuusvaatimusten määrittelylle ja siihen työhön tarvittavalle asiantuntemukselle. Hankepäällikkö vastaa turvallisuusvaatimusten määrittelystä ja tätä työtä varten hänellä on käytettävissään hankeorganisaationsa lisäksi sidosryhmäturvallisuuden asiantuntijoita eli Puolustusvoimien toimivaltaisia turvallisuustarkastajia. Tarve turvallisuusasiantuntemuksen käytölle hankkeen suunnittelun tukena nousi aineistosta esiin noin 10 kertaa.

Hankkeet ovat Puolustusvoimien suorituskykyjen kehittämisen työkalu. Jotta hankkeiden avulla saadaan paras mahdollinen suorituskyky rakennettua, hankkeen käytettävissä olevilla resursseilla, tulee hankepäälliköllä olla käytössään paras mahdollisen asiantuntemus. Tämän voisi yleistää koskemaan myös muita hankkeeseen liittyviä osa-alueita, ei ainoastaan turvallisuutta.

Haastatteluissa nousi jossain määrin esiin turvallisuusalan asiantuntijoiden riittävyys, mutta ensisijaisesti kehittämistarpeena nähtiin turvallisuusasiantuntijoiden kohdentaminen paremmin hankkeiden käyttöön. Haastateltavat olivat melko yksimielisiä siitä, että hankkeisiin on nimettävä turvallisuusvastaava, vähintäänkin kytkettynä johonkin muuhun hankeorganisaation tehtävään.

Jokaiseen hankkeeseen ei ole aina asettaa päätoimista turvallisuusvastaavaa, sillä jokainen hankeorganisaation henkilö on pois jostain muusta organisaation toiminnasta. Turvallisuusvastaavan tehtävät voidaan, hankkeesta riippuen, yleensä kytkeä johonkin toiseen tehtävään. Usein ainoa päätoimisesti hankkeen parissa työskentelevä henkilö on hankepäällikkö. (Haastatteluaineisto 2020).

Toisaalta osa vastaajista oli sitä mieltä, että turvallisuusvastaavien lisäksi hankkeisiin tulisi nimetä myös koulutettu turvallisuustarkastaja asiantuntijan rooliin. Turvallisuustarkastajan tehtävänä olisi tukea hankkeen turvallisuusvastaavan ja hankepäällikön työtä omalla asiantuntemuksellaan.

Hankkeen käyttöön tulee nimetä turvallisuustarkastaja ja turvallisuusvastaava, joka työskentelee yhteistyössä turvallisuustarkastajan kanssa. Turvallisuusvastaavan tulisi toimia hankkeen turvallisuuden käytännön tekijänä ja turvallisuustarkastajan asiantuntijana. (Haastatteluaineisto 2020).

Hankepäällikön sekä hankkeen turvallisuusvastaavan käytössä tulisi siis olla turvallisuustarkastajan asiantuntemus. Päätoimiset turvallisuustarkastajat työskentelevät samoissa esikunnissa kuin hankepäällikötkin mutta tämä yhteistyö ei toteudu aina optimaalisella tavalla. Turvallisuustarkastajien tehtäväkenttä on laaja, eikä heitä haastatteluaineiston perusteella kannata lähtökohtaisesti sitoa hankkeiden turvallisuusvastaavan tehtäviin, mutta nimeäminen hankkeen asiantuntijarooliin parantaisi tiedonkulkua ja turvallisuuden asiantuntemus olisi paremmin hankeorganisaation käytettävissä.

Turvallisuustarkastajan tulisi olla tukemassa hankepäällikköä heti hankkeen alkuvaiheessa. Hän pystyy auttamaan hankepäällikköä määrittämään, minkälaisia vaatimuksia turvallisuudelle hankkeesta aiheutuu. Mitä turvallisuusasioita pitää huomioida itse hankkeen johtamisessa ja miten ne vaikuttavat myöhemmin perustettaviin projekteihin tai tuotteen käyttöönottoon. Tuki tulisi olla hankepäällikön kotiesikunnasta koska suorituskyvyn omistaja tuntee parhaiten suorituskyvyn tarpeet, toimintaympäristön ja näin saadaan suorituskykyyn sisältyvät erityispiirteet parhaiten huomioitua. (Haastatteluaineisto 2020).

Useassa vastauksessa nousi esiin se, että hankkeita suorittavien organisaatioiden eli Pääesikunnan ja puolustushaaraesikuntien sisältä tulee löytyä kansainvälisen sidosryhmäturvallisuuden asiantuntemus. Kansallisen turvallisuusviranomaisorganisaation edustajat joutuvat toiminnan ohjaamisen lisäksi ajoittain tukemaan hankkeita hyvin käytännöllisissä asioissa kuten asiakirjojen laadinnassa. Myös tähän liittyvien yhteistoimintatasojen määrittely nousi yhtenä kehitettävänä kokonaisuutena esille. (Haastatteluaineisto 2020).

Puolustusvoimien organisaatioista löytyy haastatteluiden perusteella hankkeiden sidosryhmäturvallisuuden toteuttamiseen tarvittava asiantuntemus. Asiantuntemuksen määrä on kuitenkin rajallinen ja sen saatavuutta sekä kohdentamista hankkeiden käyttöön tulisi parantaa, erityisesti mittakaavaltaan pienempien hankkeiden osalta. Käytettävissä olevan asiantuntijuuden merkitys korostuu hankkeen alkuvaiheessa, kun turvallisuustoimenpiteitä

suunnitellaan. Kansainvälisten hankkeiden sidosryhmäturvallisuuden osalta resursseja ja osaamista tulisi kasvattaa.

4.3 Osaaminen

Tarve turvallisuusasiantuntijoiden ja hankkeisiin osallistuvan henkilöstön osaamisen kasvattamiselle ja osaamisen säännölliselle päivittämiselle nousi aineistosta esiin noin 15 kertaa. Selkeimpänä kehittämiskohteena tässä luokassa nousi osaaminen kansanväliseen yhteistyöhön liittyvästä sidosryhmäturvallisuudesta mutta myös tietoisuuden lisääminen sidosryhmäturvallisuudesta, hanketoiminnasta sekä hanketoimijoiden yhteistyöhön liittyvistä asioista nousi esiin haastatteluissa. Yhteisiä koulutustilaisuuksia toivottiin myös verkostoitumisen näkökulmasta.

Henkilöstö tekee joskus inhimillisiä erehdyksiä, mutta hankkeiden turvallisuus on yleisesti ottaen hyvällä tasolla. Kansainvälisten käytänteiden tuntemisessa ja hanketurvallisuusdokumenttien laadinnassa on havaittu kehittämistarpeita. Näihin voimme vastata koulutuksella ja huolellisella suunnittelulla. Henkilöstön määrää ei välttämättä tarvitse kasvattaa mutta hankkeisiin osallistuvan henkilöstön osaamista tulisi kasvattaa koulutuksen kautta. Niin hankkeiden turvallisuus- kuin kaupallisellakin puolella tulee ymmärtää yhteistyöhön vaikuttavat asiat. (Haastatteluaineisto 2020).

Kansainvälisten hankkeiden toteuttaminen vaatii erityistä asiantuntemusta sidosryhmäturvallisuuden näkökulmasta. Osaamisen näkökulmasta aineistosta nousi muutamia kertoja esiin se, että kansallisen ja kansainvälisen turvallisuusluokittelun tiedon erottamisessa toisistaan on kehittämistarpeita.

Jossain määrin on havaittu, että erityissuojattavaa ja turvallisuusluokiteltua tietoa ei aina osata erottaa toisistaan vaan niitä käsitellään yhtenä massana. Puolustushallinnossa tulisi kasvattaa osaamista ja ymmärrystä kansainväliseen tietoturvallisuuteen liittyvissä asioissa. (Haastatteluaineisto 2020).

Aineiston perusteella sidosryhmäturvallisuuden koulutusta tulisi lisätä hankehenkilöstölle erityisesti kansainvälisten turvallisuusasioiden osalta. Yhdessä haastatellussa nostettiin esiin myös esimerkkihankkeessa kuvatun FMS-kaupan erityispiirteiden tuntemus. Haastatteluissa ei juurikaan nostettu esiin puutteita osaamisessa kotimaisten hankkeiden sidosryhmäturvallisuuden osalta. Kansainvälisten turvallisuusdokumenttien laadinta on koettu haastavana, sillä dokumentit voivat olla hyvin yksityiskohtaisia ja niihin vaadittavan sisällön tuottaminen vaatii laajaa ymmärrystä turvallisuusasioista sekä sopimusjuridiikasta. Tämän lisäksi kansainväliset asiakirjat tulisi valmistella juridisen tarkastelun kestävällä englannin kielen taidolla.

Kehittämiskohteena tässä kansainvälisellä puolella on myös kielitaito. Esimerkiksi PSI asiakirja vaatii sopimusjuridista englanninkielen taitoa. Osaamisen tasoa tämän suhteen tulisi nostaa. Sopimusjuridiikka vaatii tietynlaisten termien hallintaa. (Haastatteluaineisto 2020).

Organisaation osaamista voidaan kasvattaa rekrytoimalla uusia ihmisiä tai kouluttamalla henkilöstöä. Sidosryhmäturvallisuusala sekä hankeala järjestävät vuosittain neuvottelupäiviä, joissa koulutetaan ajankohtaisia asioita. Näiden neuvottelupäivien antia ja toteutusta on pidetty erinomaisena. Koulutuksen on oltava säännöllistä henkilöstön vaihtuvuudesta johtuen. Hankkeen aikana sen henkilöstössä saattaa tapahtua muutoksia. Hankkeet saattava helposti kestää pitkälle toistakymmentä vuotta ja pitkään kestävissä hankkeissa tapahtuu henkilöstön vaihtumista. Tämä korostaa myös hankkeeseen liittyvän dokumentaation hallinnan merkitystä.

Meiltä löytyy riittävästi ohjausta mutta asiat voivat olla monimutkaisia eikä henkilöstö välttämättä tunne kaikkia hankkeessa huomioitavia yksityiskohtia ja toisaalta myös hankehenkilöstön vaihtuvuus aiheuttaa tässä myös haasteita. Tässä tulisi nostaa yleistä osaamistasoa ja tietoisuutta asioista, erityisesti kansainvälisten asioiden osalta. Usein hankkeet ovat myös hyvin yksilöllisiä, joten aiemmat kokemukset eivät välttämättä päde seuraavassa hankkeessa. (Haastatteluaineisto 2020).

Hankepäälliköistä osa on suorittanut Puolustusvoimien sotatalouden- ja tekniikan lisäopinnot ja saaneet sitä kautta koulutuksen hankkeisiin. Osa hankepäällikköistä on saanut hankekoulutuksensa siviiliopinnoissa ja osalla hankepäälliköistä ei ole aikaisempaa hankealan koulutusta. Hankepäälliköt ovat saattaneet työskennellä muissa hanketehtävissä ja saaneet sitä kautta kokemusta hankkeista. Hankeorganisaatioihin kuuluu yleensä paljon muitakin henkilöitä, jotka ovat saaneet projektiosaamista ja -koulutusta siviilipuolelta tai työkokemuksen kautta. (Haastatteluaineisto 2020).

Hankkeisiin liittyvät turvallisuusasiat muovautuvat esimerkiksi teknologian kehittymisen, kansainvälisten käytänteiden sekä lainsäädännön kehittymisen myötä. Toisaalta hankkeet voivat olla hyvinkin yksilöllisiä riippuen kehitettävästä suorituskyvystä ja hankkeeseen kytkeytyvistä sidosryhmistä. Tästä syystä kaiken kattavaa koulutusta on mahdotonta järjestää ja usein osaaminen syntyy kokemuksen kautta. Osaamisen tasoa tulee pitää yllä ja päivittää säännöllisesti.

4.4 Ohjeet ja työkalut

Lähes kaikissa haastatteluissa viraston olemassa olevaa normiohjeistusta pidettiin riittävänä eikä sen lisäämiselle nähty tarvetta. Asiaan liittyvät säädökset, normit ja turvallisuusmääräykset tulee tuntea hankkeen toimintaa suunniteltaessa. Sidosryhmien kanssa tehtävään yhteistyöhön liittyviä käytännön toimintaohjeita on olemassa, mutta tieto on hajaantunut eri asiantuntijoiden käyttöön. Käytännön kokemuksiin perustuvia toimintatapoja ei välttämättä ole dokumentoitu vaan ne elävät käytänteinä ja suullisena tietona hanketoimijoiden keskuudessa.

Lainsäädäntö, normit ja ohjeet tulee tuntea. Myös eri maiden erilaiset käytänteet tulee ottaa huomioon kansainvälisessä toiminnassa. Materiaalin toimittaminen ulkomaille vaatii aina huomattavan paljon enemmän taustatyötä ennen kuin materiaalia voidaan luovuttaa. (Haastatteluaineisto 2020).

Toimintatavoissa on eroja riippuen siitä, tehdäänkö yhteistyötä kansallisen ja kansainvälisen sidosryhmän kanssa. Tämä vaikuttaa käytännössä esimerkiksi tiedon sähköiseen välittämiseen, kuriiri- ja rahtitoimintaan ja siihen millä tasolla näistä asioista sovitaan.

Normit ovat sinänsä selkeitä ja esimerkiksi PV:n tietoturvaohje on hyvä tietolähde perusperiaatteiden ymmärtämiseksi. Käytännön toimenpiteiden osalta tiedon yleensä saa esimerkiksi turvallisuustarkastajalta mutta koottuna asiakirjana niitä ei oikein ole löydettävissä. Kansainvälisiin hankkeisiin liittyvien turvallisuusdokumenttien laadinta, turvaluokitellun tiedon luovuttamisen toimintaohjeiden ja kuriiritoiminnan ohjeistusta voisi kehittää. Myös jokin runko PSI- ja SAL-asiakirjojen laadinnalle helpottaisi toimintaa. (Haastatteluaineisto 2020).

Ohjeistuksen osalta nousi esiin se, että voisi olla tarpeellista laatia koottu toimenpideluettelo siitä, mitkä asiat pitää huomioida ennen turvallisuusluokitellun tiedon luovuttamista, jotta nämä olisi helppo tarkistaa. Työhän liittyvien haastatteluiden aikana Logistiikkalaitoksessa julkistettiin ohje hankintojen tietoturvallisuudesta, joka vastaa osin tähän tarpeeseen. Myös tiedon suojaamiseen käytettävät työkalut tulisi olla saatavilla ja helppokäyttöisiä. Esimerkiksi tällä hetkellä sähköpostin salaamiseen käytettäviä ohjelmia pidettiin jossain määrin hankalina ja hyvin paljon aikaa kuluttavina työkaluina.

Salaustyökalujen käyttö ei ole helppoa ja tiedon lähettäminen vie aikaa. Lisäksi erillisten työasemien saatavuus ja käytettävyys ovat välillä haasteena. Tämä hankaloittaa materiaalin toimittamista ulkomaille. (Haastatteluaineisto 2020).

Käytännön toimenpideohjeita tarvitaan normien lisäksi. Ohjeet tulee olla saatavilla ja niitä tulee päivittää säännöllisesti, jotta ne pysyvät ajantasaisina. Tällä hetkellä tarpeelliset

toimintaohjeet ovat turvallisuustarkastajien käytettävissä, mutta jos hankkeelle ei syystä tai toisesta ole nimettyä turvallisuustarkastajaa eivät nämä toimintaohjeet ole välttämättä hankeorganisaation käytettävissä. Myös kansainvälisten hankkeiden turvallisuusdokumenttien laadintaan toivottiin esimerkkejä sisältörungosta. Laadukkaiden ohjeiden ja käyttökelpoisten työkalujen avulla voidaan tukea oikeita toimintamalleja, sujuvoittaa työntekoa ja parantaa hankkeiden turvallisuuden tasoa.

5 Pohdinta

5.1 Johtopäätökset

Tämän opinnäytetyön tavoitteena oli kehittää Puolustusvoimien hankkeiden turvallisuutta. Työn tarkoituksena oli selvittää, miten Puolustusvoimien hankkeiden turvallisuutta voidaan kehittää sidosryhmäturvallisuuden näkökulmasta ja luoda ehdotuksia hankkeiden turvallisuuden kehittämiseksi.

Työn tuloksena nousi esiin neljä pääluokkaa, joihin tulisi kiinnittää huomiota hankkeiden turvallisuuden kehittämiseksi sidosryhmäturvallisuuden osalta. Nämä tunnistetut avaintekijät ja kehittämiskohteet liittyvät osittain toisiinsa ja ovat jossain määrin toisiaan tukevia. Toisin sanoen, kehittämällä yhtä pääluokkaa myös toinen pääluokka todennäköisesti kehittyy. Ohjeiden tuottaminen ja kouluttaminen lisäävät tietoisuutta. Osaamisen laajentaminen mahdollistaa asiantuntijuuden tehokkaamman hyödyntämisen hankkeiden valmistelussa ja suunnittelussa. Tärkein onnistumisen mahdollistava tekijä on turvallisuusvaatimusten huolellinen analysointi ja tarvittavien turvallisuustoimenpiteiden suunnittelu hankkeen alussa. Toisena onnistumisen mahdollistajana nousi esiin riittävän asiantuntemuksen käyttö toiminnan suunnitteluun eli hankkeissa käytettävät asiantuntijaresurssit. Kehittämiskohteena nähtiin osaamistason kasvattaminen ja ylläpito koulutuksen avulla sekä käytännön toimenpideohjeiden kehittäminen. Huomionarvoista on, että aineiston perusteella käytännön toimenpideohjeita ja asiantuntijaresurssien tehokkaampaa kohdentamista painotettiin niissä tehtävissä, jotka olivat lähempänä käytännön yhteistoimintaa yritysten kanssa, kun taas hanke- ja turvallisuusalan ylemmissä tehtävissä työskentelevät painottivat osaamisen kehittämistä organisaatiossa. Valmistelun merkitystä painotettiin tasaisesti lähes kaikissa haastatteluissa eikä ainakaan oman tulkintani mukaan varsinaisia ristiriitoja noussut esiin aineistosta missään pääluokassa. Nämä tunnistetut avaintekijät ja kehittämiskohteet ovat sinänsä yleispäteviä sekä kansallisen että kansainvälisen sidosryhmäturvallisuuden näkökulmasta, mutta aineistossa korostui kaikilla osa-alueilla hankkeiden kansainväliseen turvallisuuteen liittyvät kehittämistarpeet.

Hankkeet ovat usein monimutkaisia ja haastavia toimintokokonaisuuksia. Hankkeisiin liittyy hyvin paljon erilaisia huomioon otettavia asioita ja näiden huomioiminen vaatii laajaa asiantuntijuutta. Hankepäällikön merkitys hankkeen laadukkaalle ja sujuvalle toteutukselle on erittäin suuri. Hänen ei välttämättä itse tarvitse olla asiantuntija, mutta hänen tulee tiedostaa mitä asioita hankkeessa tulee ottaa huomioon. Tämän työn perusteella Puolustusvoimien hankkeiden sidosryhmäturvallisuuteen liittyvät asiat toteutuvat yleisesti ottaen hyvin. Tämä johtuu ammattitaitoisesta henkilöstöstä sekä eri viranomaisten välisen ja puolustushallinnon sisäisen yhteistyön laadukkuudesta. Toisaalta, vaikka hankkeiden turvallisuus toteutuukin hyvin, niin sen toteuttaminen ei aina tapahdu optimaalisella tavalla vaan asioiden selvittämiseen kuluu usein henkilöstöllä paljon aikaa ja työskentelyä oman varsinaisen vastuualueen ulkopuolella.

Turvallisuusvaatimusten huomioiminen heti hanketta valmisteltaessa on erittäin tärkeä tekijä. Hankepäällikkö vastaa hankkeensa turvallisuudesta. Jotta tarvittavat toimenpiteet tulevat huomioiduksi ajoissa on hankepäälliköiden tiedostettava vaadittavat toimenpiteet turvallisuuden toteuttamiseksi. Osa hankepäälliköistä on suorittanut sotatalouden ja tekniikan lisäopinnot, joissa hankkeisiin liittyvää sidosryhmäturvallisuutta on käsitelty, mutta suuri osa ei. Hankepäällikön tehtävä on vaativa ja hankkeen luonteesta riippuen hankepäällikön tulisi kyetä huomioimaan useita lainsäädännön, valtionhallinnon ohjeiden ja Puolustusvoimien normien velvoittamia asioita hankkeen hallinnassa ja omissa toimeksiannoissaan.

Tärkeä työkalu hankepäällikölle on Puolustusvoimien hankeohje (Pääesikunta 2017b), joka antaa yleiset periaatteet siitä millaisia asioita hankkeen hallinnassa ja hankesuunnitelman laadinnassa tulisi ottaa huomioon. Hankepäälliköiden tietoisuutta hankkeiden turvallisuusnäkökulmista voitaisiin tehostaa sisällyttämällä esimerkiksi Puolustusvoimien hankeohjeeseen hankepäällikölle selkeä suositus konsultoida oman esikuntansa toimivaltaista turvallisuustarkastajaa tai muuta sidosryhmäturvallisuuden asiantuntijaa jo aikaisessa vaiheessa hankkeen valmisteluun liittyen. Turvallisuustarkastaja voisi yhdessä hankepäällikön kanssa arvioida etukäteen minkälaista turvallisuuden asiantuntemusta hankkeen edetessä mahdollisesti tarvitaan. Näin ollen, mikäli esimerkiksi hankkeessa tullaan luovuttamaan, vastaanottamaan tai luomaan salassa pidettävää tietoa, nousisi sidosryhmäturvallisuus asiakokonaisuutena esiin hyvissä ajoin eikä siitä aiheutuisi suunnittelemattomia muutoksia tai viivästyksiä hankkeen myöhemmissä vaiheissa. Turvallisuusselvitykset ja turvallisuussopimusten tai muiden turvallisuusasiakirjojen laadinta ja niihin liittyvät hyväksynnät vaativat paljon aikaa, joten näihin liittyvät prosessit tulee käynnistää hyvissä ajoin.

Toinen kehittämisehdotus on hankkeen sisäisten "turvallisuuskatselmointien" liittäminen osaksi hankkeen hallintaa. Tämän voisi toteuttaa esimerkiksi tarkastuslomakkeella, mikä tarkastetaan yhdessä hankepäällikön ja hankkeen turvallisuusvastaavan sekä

turvallisuustarkastajan kanssa hankesuunnitelmassa määritettyinä ajankohtina, esimerkiksi ennen varsinaisia hankekatselmointeja. Hankkeen turvallisuusvastaava laatii lomakkeen osana hankkeen turvallisuuden hallintaa ja sen avulla tarkastellaan säännöllisesti hankkeen turvallisuusvaatimusten ajantasaisuutta sekä vaadittavien toimenpiteiden toteutumista. Turvallisuusvaatimusten määrittelyn suhteen kehittämistarpeet liittyvät hankepäälliköiden tietoisuuden lisäämiseen. Tämä on organisaatiossa tiedostettu ja sidosryhmäturvallisuutta tuodaan aktiivisesti esiin erilaisissa hanke- ja turvallisuusalan koulutustilaisuuksissa. Tätä työtä on jatkettava ja kun hankealan normeja tulevaisuudessa päivitetään, voisi turvallisuusnäkökulmat olla niissä selkeämmin hanketoimintaan ja -prosesseihin integroituna.

Toisena avaintekijänä nousi esiin hankepäällikön käytettävissä olevat asiantuntijaresurssit. Hankkeet ovat usein hyvin monimutkaisia ja hankepäällikkö tarvitsee tuekseen monenlaista asiantuntemusta. Hankkeiden sidosryhmäturvallisuuden osalta nämä asiantuntijat ovat Puolustusvoimien toimivaltaisia turvallisuustarkastajia, jotka löytyvät Pääesikunnan alaisista laitoksista sekä jokaisesta puolustushaaraesikunnasta. Samoista joukoista mistä hankepäällikötkin tulevat. Turvallisuuden asiantuntemus pitäisi lähtökohtaisesti olla hankepäällikön käytettävissä koko hankkeen ajan tarvittavissa määrin. Käytännössä saattaa kuitenkin olla niin, että hankepäällikkö ei tiedosta tarvitsevansa turvallisuustarkastajan palveluita eikä turvallisuustarkastaja tiedä joukossaan käynnissä olevista hankkeista tai niiden turvallisuusvaatimuksista. Yksi ratkaisu tähän on aiemmin mainittu velvoite konsultoida joukkonsa turvallisuustarkastajaa hankkeen alussa.

Toinen ratkaisu voisi olla turvallisuustarkastajan nimeäminen lähtökohtaisesti kaikkien hankkeiden organisaatioon, vähintään hankkeen valmisteluvaiheen ajaksi. Hankkeisiin tulee nimetä myös turvallisuusvastaava johtamaan turvallisuuden toteuttamista hankkeessa. Hänen turvallisuusosaamisensa ei kuitenkaan välttämättä ole kaikilta osin riittävä. Puolustusvoimien turvallisuusohjeessa (2015b, 4) sanotaan, että normien edellyttämien resurssien puuttuessa on siitä tehtävä ilmoitus virkatietä määräyksen antajalle. Tämän perusteella myös hankkeella tulisi olla tarpeelliset turvallisuuden resurssit käytössä tai ainakin niiden puute tulee tiedostaa ja ilmoittaa puutteesta virkatien mukaisesti. Mikäli toimivaltaisia turvallisuustarkastajia ei ole asettaa hankeorganisaatioon ja hankkeessa on tarve sidosryhmäturvallisuuden toimenpiteille, niin hankepäällikön käyttöön tulisi nimetä vähintään turvallisuustarkastajakurssin käynyt ja riittävän osaamisen omaava henkilö sidosryhmäturvallisuuden asiantuntijaksi. Tällä järjestelyllä voitaisiin tukea hankkeen turvallisuusvastaavaa ja toisaalta vapautetaan toimivaltaisten turvallisuustarkastajien resursseja muihin tehtäviin. On kuitenkin huomioitava, että mahdollisten turvallisuussopimusten valmistelussa vaaditaan toimivaltaisen turvallisuustarkastajan työpanosta.

Toinen tapa lisätä hankkeiden turvallisuuden asiantuntemusta voisi olla päätoimisen hanketurvallisuusvastaan tehtävän avaaminen kaikkiin puolustushaaraesikuntiin. Päätoiminen hanketurvallisuusvastaava toimisi kaikkien oman puolustushaaransa hankkeiden ”turvallisuuskonsulttina” ja näin hankkeiden turvallisuuteen liittyvä asiantuntijuus saataisiin keskitetysti hankkeiden käyttöön. Toinen mahdollisuus olisi lisätä aselajikohtaisten hankeupseereiden määrää Logistiikkalaitoksessa. Tämä menettely on käytössä osassa hankkeista ja se on koettu erittäin hyväksi. Oli hanketurvallisuusvastaava sitten puolustushaaran tai aselajin "palveluksessa" niin hän voisi erikoistua kansainvälisen sidosryhmäturvallisuuden velvoitteiden huomioimiseen ja kansainvälisten turvallisuusdokumenttien laadintaan. Hänellä tulisi olla turvallisuustoimialan perus- ja jatkokurssit suoritettuna, riittävä englannin kielen taito ja ainakin jossain määrin ymmärrystä sopimusjuridiikasta. Hän toimisi yhteyshenkilönä oman puolustushaaransa hankkeiden, muiden puolustushaarojen ja Pääesikunnan hanketurvallisuusvastaavan välillä sekä tarvittaessa myös Puolustusministeriön DSA:n suuntaan. Näin ollen hän saisi kerrytettyä kokemusta hankkeiden turvallisuudesta, toiminta pysyisi yhdenmukaisena ja sitä voitaisiin paremmin kehittää. Edelleen hänellä tulisi olla hankekohtaisesti turvallisuustarkastajien asiantuntemus tukena omassa toiminnassaan, erityisesti turvallisuuden näkökulmasta vaativimmissa hankkeissa. Tämä kehittäisi aikaa myöten koko organisaation osaamista sekä loisi selkeän yhteistoimintatason hankkeiden kansainvälisen turvallisuuden osalta.

Yhtenä kehittämiskohteena työssä nousi esiin säännöllisen ja ajantasaisen koulutuksen tarve hankkeisiin ja niiden turvallisuuteen liittyen. Koulutuksen avulla tulisi nostaa osaamistasoa erityisesti kansainvälisten turvallisuusasioiden kannalta, parantaa hankealan henkilöstön kokonaisymmärrystä hankkeisiin vaikuttavista tekijöistä sekä parantaa yhteistyötä verkostoitumalla asiantuntijoiden kesken. Konkreettisina osaamiseen liittyvinä kehittämiskohteina mainittiin kansallisesti turvallisuusluokitellun tiedon ja kansainvälisen erityissuojattavan tiedon tunnistaminen, erottaminen toisistaan ja niiden käsittelyyn liittyvien erojen tunteminen. Kansainväliseen toimintaan liittyen myös turvallisuusasiakirjojen laadintaan vaadittavaa osaamista tulisi kehittää tai hankkia, mukaan lukien tähän työhön vaadittava kielitaito.

Nykyaikainen tietotekniikka tarjoaa koulutukseen lukuisia työkaluja eikä osaamisen saavuttaminen vaadi välttämättä massiivisten koulutustapahtumien järjestämistä. Puolustusvoimissa on käytössä PVMOODLE verkko-oppimisympäristö, johon voitaisiin luoda hankealan henkilöstölle tai hankepäälliköille suunnattu ”työhönottokurssi”. Tämä voisi olla osa hankepäälliköiden perehdytystä. Tällä kurssilla voitaisiin nostaa esiin hankkeissa huomioitavia asioita mukaan lukien turvallisuusnäkökulmat. Tämä tukisi erityisesti niiden hankepäälliköiden toimintaa, ketkä eivät ole suorittaneet sotatalouden ja -tekniikan lisäopintoja tai muuta vastaavaa koulutusta. Tämä myös osaltaan tukisi turvallisuuden tehokkaampaa integroimista hanketoimintaan. Turvallisuusasioiden osalta lisäkoulutusta tulisi

suunnata hankepäälliköiden lisäksi hankkeisiin osallistuvalle turvallisuusalan henkilöstölle sekä hankkeiden turvallisuusvastaaville. Mikäli edellisessä kappaleessa esitettyjä hanketurvallisuusvastaavien tehtäviä tulevaisuudessa avattaisiin, olisi heitä mahdollista käyttää näiden asioiden kouluttajina.

Erään haastattelun aikana keskustelussa nousi esiin myös Puolustusvoimien työntekijöiden määräajoin suorittama tietoturvallisuuden peruskoulutus. Tätä voitaisiin muokata tehtäväkohtaiseksi. Asevelvollisten kouluttaja ja kansainvälisen hankkeen työntekijä tarvitsevat jossain määrin erilaista osaamista ja ymmärrystä tietoturvallisuudesta.

Viimeisenä kehittämiskohteena olivat hankkeiden turvallisuuteen liittyvät ohjeet ja työkalut. Näiden osalta esiin nousi tarve selkeille käytännön toimenpideohjeille ja toisaalta esimerkiksi salaustyökaluilta toivottiin parempaa käytettävyyttä. Nämä kehittämiskohteet koskivat pääasiassa kansainvälisten sidosryhmien kanssa tehtävää yhteistyötä. Tällä hetkellä Puolustusvoimien käyttöön on hyväksytty kaksi salausohjelmistoa. Kansainväliseen tiedon välittämiseen on kuitenkin käytettävissä useita erilaisia salaustyökaluja. Käytettävissä olevat salausohjelmat löytyvät kyberturvallisuuskeskuksen Internet sivuilta (Kyberturvallisuuskeskus 2020). Näistä saattaisi löytyä käytettävyydeltään parempia työkaluja kuin nämä kaksi nyt käytössä olevaa ohjelmistoa.

Toimenpideohjeiden osalta hankkeen turvallisuusvastaavalla tulisi olla käytössään tieto siitä, mistä asioista hänen on varmistuttava ennen kuin hän voi lähettää turvallisuusluokiteltua tietoa sidosryhmälle. Nämä asiat tulisi olla eriteltynä kansallisten ja kansainvälisten hankkeiden osalta ja jokainen turvallisuusluokka sekä tiedon välittämisen menetelmä erikseen huomioituna. Kansainvälisten hankkeiden osalta hankkeiden turvallisuusvastaavilla tulisi myös olla ohje turvallisuusasiakirjoihin sisällytettävistä asiakokonaisuuksista. Malli PSI-asiakirjaan sisällytettävistä asiakokonaisuuksista on laadittu organisaation sisäiseen käyttöön osana tätä opinnäytetyötä. Nämä ohjeet tulisivat olla kootusti hankkeen turvallisuusvastaavien saatavissa esimerkiksi projektien verkkolevyasemalla. Tähän kokonaisuuteen liittyy myös tieto tarvittavien turvallisuussopimusten ja turvallisuusselvitysten voimassaolosta.

PÄÄLUOKKA	KEHITTÄMISKOHDE	KEHITTÄMISEHDOTUKSET
VALMISTELU	- Turvallisuusvaatimusten huolellinen määrittely ja huomioiminen hankkeen valmistelussa sekä toimenpiteiden suunnittelussa	- Hankepäälliköiden koulutus ja turvallisuusnäkökulmista tiedottaminen. - Hankeohjeen päivitys: sidosryhmäturvallisuuden toimenpiteiden tarkentaminen sekä suositus konsultoida

PÄÄLUOKKA	KEHITTÄMISKOHDE	KEHITTÄMISEHDOTUKSET
		turvallisuustarkastajaa hankkeen valmistelun aikana. - Hankkeen sisäiset turvallisuuskatselmoinnit osaksi hankkeen hallintaa.
HENKILÖSTÖ	- Turvallisuuden asiantuntemuksen lisääminen ja kohdentaminen paremmin hankkeiden käyttöön. - Turvallisuustarkastajien ja hankepäälliköiden yhteistoiminnan kehittäminen. - Kansainvälisten hankkeiden sidosryhmäturvallisuuden yhteistoimintatasojen luominen.	- Turvallisuustarkastajan konsultointi hankkeen valmistelun aikana. - Hanketurvallisuusvastaavan tehtävien avaaminen puolustushaaraesikuntiin painopisteenä kansainvälinen sidosryhmäturvallisuus tai aselajikohtaisten hankeupseerien tehtävien avaaminen esimerkiksi Logistiikkalaitokselle. - Turvallisuustarkastajien nimeäminen hankeorganisaatioihin ainakin hankkeen valmisteluvaiheessa. - Turvallisuustarkastajan koulutuksen saaneiden henkilöiden käyttäminen hankkeiden sidosryhmäturvallisuuden asiantuntijoina hankkeen valmistelussa ja suunnittelussa.
OSAAMINEN	- Hankepäälliköiden yleisen tietoisuuden parantaminen sidosryhmäturvallisuuden osalta. - Salassa pidettävän tiedon alkuperän tunnistaminen ja siitä johtuvien käsittelysääntöjen tunteminen. - verkostoituminen - Kielitaidon ja juridisen osaamisen parantaminen turvallisuusasiakirjojen laadinnassa.	- Kansainvälisen sidosryhmäturvallisuuden näkökulmien huomioiminen STLO:n turvallisuuskoulutuksessa - Hankkeiden turvallisuusasioiden kouluttaminen sekä esillä pitäminen hanke- ja sidosryhmäturvallisuusalan neuvottelupäivillä. - Hankealan työhönottokurssi PVMOODLE:ssa erityisesti niille ketkä eivät ole suorittaneet STLO:a tai muuta vastaavaa hankekoulutusta.

PÄÄLUOKKA	KEHITTÄMISKOHDE	KEHITTÄMISEHDOTUKSET
		- Tehtävän mukaan kohdennettu tietoturvallisuuden peruskoulutus.
OHJEET JA TYÖKALUT	- Käytännön toimenpideohjeiden laatiminen ja saatavuuden parantaminen. - salaustyökalujen käytettävyys	- Käytännön toimenpideohjeiden luominen painopisteenä kansainvälinen sidosryhmäturvallisuus. - Käytännön toimenpideohjeiden saatavuuden parantaminen sijoittamalle ne sisäiseen verkkoon projektilevyasemalle. - PSI ja SAL asiakirjarunkojen luominen. - NCSA:n hyväksymien salaustyökalujen käytettävyyden selvittämien.

Taulukko 2: Kehittämiskohteet ja kehittämisehdotukset

Hankkeita on toteutettu pitkään ja varmasti yhtä kauan niissä on huomioitu niihin kulloinkin liittyvät turvallisuusnäkökulmat. Kokonaisuudessaan hankkeiden turvallisuutta voitaisiin parhaiten kehittää integroimalla turvallisuus ja turvallisuusjohtamisen elementit tehokkaammin hanketoimintaan ja sen prosesseihin, henkilöstön koulutukseen sekä ohjeisiin. Tarve tämänkaltaiselle kehityssuunnalle nousi esiin myös muutamissa haastatteluissa. Tätä voi perustella myös Puolustusvoimien turvallisuusohjeella (Pääesikunta 2015b, 6), missä edellytetään turvallisuustoiminnan integroimista mukaan kaikkeen toimintaan tarvittavilta osin. Ohjeessa myös todetaan johdon olevan sitoutunut turvallisuuden toteuttamiseen, joten lähtökohdat hankkeiden turvallisuusjohtamisen kehittämiselle ovat hyvät (Pääesikunta 2015b, 4). Muita turvallisuusjohtamisen elementtejä voidaan ottaa mukaan hankkeisiin esimerkiksi standardin ISO 27000:2020 mukaisista tietoturvallisuuden hallintajärjestelmistä tai kansallisesta turvallisuuden auditointikriteeristöstä. Näitä ovat johdon sitoutumisen lisäksi esimerkiksi turvallisuusvastuiden määrittäminen, asiantuntemuksen käyttö, turvallisuusriskien hallinta, jatkuvuuden hallinta, turvallisuuspoikkeamien hallinta ja tietojen luokittelu (Puolustusministeriö 2015). Näistä elementeistä korostuu erityisesti riskienhallinnan kehittäminen eli hankkeiden turvallisuusriskien tunnistaminen, analysointi ja käsittely turvallisuuspoikkeamia ennaltaehkäisevänä toimenpiteenä. Hankkeet saattavat olla erittäin monimutkaisia ja haastavia kokonaisuuksia, jolloin sisäänrakennetun turvallisuuskulttuurin ja

turvallisuuskäytänteiden merkitys turvallisuuden ylläpitäjänä korostuu. Hankkeiden sidosryhmäturvallisuuden toteuttamiseen eli salassa pidettävän tiedon suojaamiseen vaadittavat asiat yksittäisinä toimenpiteinä eivät ole kovinkaan monimutkaisia mutta niiden tekemättä jättäminen saattaa aiheuttaa merkittävää vahinkoa.

Kuten eräässä haastattelussa mainittiin, sidosryhmäturvallisuuden tavoitteena on suojata PV:n toiminnan kannalta salassa pidettävä tieto. Jos menetämme suorituskyvyn rakentamisen myötä muodostuneen tiedon, niin pahimmillaan koko työ on ollut turhaa. Eräässä toisessa haastattelussa mainittiin, että niin hankkeiden turvallisuus- kuin kaupallisellakin puolella tulee ymmärtää yhteistyöhön vaikuttavat asiat. (Haastatteluaineisto 2020). Nämä molemmat kommentit tukevat johtopäätöksiä. Hankkeiden turvallisuus ja kaupallinen puoli koetaan jossain määrin erillisiksi toimijoiksi ja tästä johtuen voisi olla hyödyllistä, että turvallisuus kulkisi paremmin integroituna mukana hankkeen hallinnassa ja hankkeen eri vaiheissa. Molempien, tai paremminkin kaikkien hankkeen ”osapuolten” tulee tuntea riittävällä tarkkuudella ydintoiminta ja sitä tukevat toiminnot. Suorituskyvyn kehittäminen hankkeen kautta on ydintoimintaa ja turvallisuus on yksi sitä tukevista toiminnoista. Tämän kokonaisuuden turvallinen toteuttaminen vaatii ennen kaikkea toimivaa yhteistyötä.

5.2 Tutkimusetiikka

Tässä opinnäytetyössä saavutettujen tulosten merkitys on organisaation toimintaa ja tavoitteita tukeva. Työn tuloksena tunnistettiin kehittämiskohteita hankkeiden turvallisuuteen liittyen ja tuotettiin kehittämisehdotuksia näihin vastaamiseksi. Tulosten perusteella on mahdollista edetä hankkeiden turvallisuuden kehittämistyössä sekä luoda konkreettisia välineitä ja menetelmiä turvallisuuden parantamiseksi ja ohjaamiseksi.

Työssä käytetyt kehittämis- ja aineistonkeruumenetelmät olivat mielestäni kehittämiskohteen suhteen oikeita. Yksityiskohtaisempaa kehitystyötä varten kohdejoukko voitaisiin valita tietystä organisaatiosta, hankkeesta tai valitun organisaatiotason edustajista. Tässä työssä kohdejoukko edusti laajasti hanke- ja turvallisuusalan toimijoita hankkeiden käytännön toteuttajista ulottuen aina sidosryhmäturvallisuus- ja hankealan johtoon sekä kansallisten turvallisuusviranomaisten edustajiin saakka.

Työn luotettavuus eli reliabiliteetti tarkoittaa tulosten toistettavuutta (Hirsjärvi, Remes & Sajavaara 2009, 231). Laadullisessa tutkimuksessa työn tuloksiin sekä johtopäätöksiin saattaa jossain määrin vaikuttaa tutkijan oma kokemus ja tulkinnat. Työn tulokset on pyritty tuottamaan tarkasti asiantuntijoiden lausuntoihin peilaten ja haastateltavilla oli mahdollisuus kommentoida työn alustavia tuloksia ennen niiden julkaisua, mahdollisten väärinymmärrysten poissulkemiseksi. Haastatteluaineisto on työssä esitetty anonyymisti eikä suoria lainauksia ole käytetty. Aineisto on kuvattu tutkijan kirjoittamina yhteenvetoina yhden tai useamman haastattelun pohjalta. Arvioisin, että työn tulokset ovat luotettavia. Tämän osalta ei voida

kuitenkaan täysin sulkea pois sitä, etteikö yksittäisen lausunnon merkitys olisi voinut muuttaa luonnettaan raportoinnin yhteydessä. Luotettavuutta puoltaa kuitenkin myös haastatteluiden saturoituminen. Haastatteluja tehtiin yhteensä yhdeksän ja aineiston selkeää saturoitumista alkoi esiintyä jo neljännen haastattelun jälkeen, joten otanta voidaan pitää tähän työhön riittävänä. Toki tärkeitä yksityiskohtia nousi esiin myöhemmissäkin haastatteluissa, mutta merkittäviä eroja tai vastakkainasetteluita ei haastatteluissa noussut esiin. Tämän perusteella arvioisin, että samanlaisella kehittämistehtävällä, rajauksilla ja kehittämismenetelmällä tutkimusta tekevä henkilö päätyisi samankaltaisiin tuloksiin pääluokkien osalta. On kuitenkin mahdollista, että aineistosta tehdyt tulkinnat, yksityiskohdat ja erityisesti työn tuloksien perusteella laaditut johtopäätökset olisivat jossain määrin erilaisia, mikäli työn olisi laatinut erilaisen koulutuksen ja kokemuksen omaava tutkija.

Työn validiteetti tarkoittaa kehittämismenetelmän sopivuutta kehittämistyöhön (Hirsjärvi, Remes & Sajavaara 2009, 231). Arvioisin, että teemahaastattelu on oikea menetelmä tämänkaltaisen kehittämistyön tekemiseen eli kehittämismenetelmä on tähän työhön validi. Kritiikkinä voidaan todeta, että aiheeseen liittyvän käsitteistön ja hankkeiden moniulotteisuus voi jossain määrin heikentää tulosten yleistettävyyttä. Työn tuloksissa ja johtopäätöksissä olisi voitu päästä vielä syvemmälle tekemällä esimerkiksi toinen haastattelukierros ryhmähaastatteluna, jossa asiantuntijat olisi kutsuttu keskustelemaan aiheesta tutkijan johdolla. Toinen tapa syventää työn validiutta olisi ollut ns. tutkijatriangulaation hyödyntäminen eli aineiston tulkinta kahden tai useamman tutkijan voimin. Tällöin tulokset olisivat olleet useamman henkilön arvioimia sekä moniulotteisempia ja virheellisten tulkintojen mahdollisuus olisi pienempi.

Työhön liittyvää tutkimusaineistoa on käsitelty TUVE-ympäristössä työskentelyn aikana. Työ ei sisällä turvallisuusluokiteltua aineistoa. Pääesikunnan operatiivinen osasto on tehnyt arvioinnin työn sisällön julkisuudesta ennen työn julkaisua. Työlle myönnetty tutkimuslupa löytyy työn liitteenä (liite 5). Kokonaisuutena arvioisin kehittämistyön tutkimuseettisesti kestäväksi.

5.3 Jatkotutkimustarpeet

Työhön liittyviä jatkotutkimustarpeita ja -mahdollisuuksia on useita. Hankkeiden turvallisuutta voidaan esimerkiksi tarkastella eri turvallisuuden alojen näkökulmasta. Valtioneuvoston uusi ulko- ja turvallisuuspoliittinen selonteko (2020) sekä edellinen puolustuselonteko (2017) painottavat sekä viranomaisten keskinäistä, että viranomaisten ja muun yhteiskunnan välistä yhteistyötä. Myös kansainvälinen yhteistyö on merkittävässä roolissa nyt ja tulevaisuudessa. Tiivistyvä yhteistyö tarkoittaa myös sidosryhmäturvallisuuden merkityksen korostumista. Nostan esille muutaman työn aikana itselleni heränneen ajatuksen, joista saattaisi olla hyötyä hankkeiden turvallisuuden kehittämiseksi tulevaisuudessa.

Tärkeimpänä jatkokehittämisen aiheena esittäisin tutkimus- tai kehittämistyötä turvallisuusjohtamisen elementtien syvemmästä integroimisesta hankkeiden prosesseihin. Olisiko hankkeiden turvallisuuden hallinnalle löydettävissä jokin turvallisuusjohtamisen tai turvallisuuden hallinnan viitekehys, mikä voitaisiin implementoida osaksi hankeprosessia? Miten esimerkiksi KATAKRI:n mukaiset turvallisuusjohtamisen elementit saataisiin kytkettyä luontevaksi ja toimintaa paremmin tukevaksi osaksi hankkeita?

Hankkeiden hallintaan liittyen jatkotutkimuksen aiheena voisivat olla hankkeiden riskienhallinnan ja tiedonluokittelumatriisin kehittäminen. Erityisesti turvallisuusriskien tunnistamista ja käsittelyä hankkeissa voitaisiin kehittää. Hankeorganisaatioiden käyttöön voisi luoda hankkeiden turvallisuuteen painottuvan riskianalyysipohjan. Näin kyettäisiin ennaltaehkäisemään esimerkiksi hankkeiden sidosryhmäturvallisuutta heikentävien riskien toteutumista. Hankkeissa käsiteltävän tiedon analysointiin käytetään tiedonluokittelumatriisia. Turvallisuusluokiteltujen tietojen analysointiin voisi kehittää työkalun, joka ohjaisi hankeorganisaatiota tiedon turvallisuusluokituksen ja tiedon alkuperän mukaisiin turvallisuustoimenpiteisiin.

Digitalisaatio, uusien teknologioiden ja viestintäverkkojen kehittyminen sekä niihin liittyvä haavoittuvuudet vaikuttavat myös sidosryhmäturvallisuuteen. Ajankohtainen jatkotutkimusaihe voisi liittyä koronapandemian aiheuttamiin muutoksiin esimerkiksi matkustamiselle ja sen myötä uudistuneille työskentelytavoille kuten etäpalavereille. Miten toteutetaan TLIII-tason etäpalaveri Puolustusvoimien ja ulkomailla toimivan yrityksen välillä turvallisesti?

Tiedon merkityksen kasvu niin sodankäynnissä kuin yritysten pääomana, teknologian kehittyminen ja tiivistyvä yhteistyö niin kansallisten kuin kansainvälistenkin sidosryhmien kanssa tarkoittaa, että sidosryhmäturvallisuuden merkitys todennäköisesti kasvaa tulevaisuudessa. Tämän vuoksi Puolustusvoimien on kyettävä seuraamaan yleistä kehitystä ja oltava edelläkävijöiden joukossa turvallisuuden suhteen, jotta luottamus yhteiskunnan vankimpiin instituutioihin säilyy myös jatkossa.

Lähteet

Painetut

Alasuutari, P. 2011. Laadullinen tutkimus 2.0. 4. uudistettu painos. Tampere: Vastapaino.

Hirsjärvi, S. & Hurme, H. 2008. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. uudistettu painos. Helsinki: Tammi.

Kosola, J. 2012. Puolustusvoimien projektiohje. 3. painos. Sotatekniikan julkaisusarja 5, no 11. Maanpuolustuskorkeakoulu. Helsinki.

Sarajärvi, A., Tuomi, J. 2009. Laadullinen tutkimus ja sisällönanalyysi. 7. uudistettu laitos. Helsinki: Tammi.

Vilkka, H. 2005. Tutki ja kehitä. Helsinki: Tammi.

Sähköiset

Euroopan unioni. 2020. Euroopan unionin terminologia. Viitattu 17.10.2020. https://iate.europa.eu/entry/result/3539742/all

Herranen, T. 2013. Turvallisuusluokitellun tiedon suojaaminen palveluhankintojen tarjouslaskentavaiheessa Case: Puolustushallinnon rakennuslaitos, Etelä-Suomen alueyksikkö. Opinnäytetyö. Laurea ammattikorkeakoulu, turvallisuusalan koulutusohjelma. Espoo. Viitattu 1.11.2020. https://www.theseus.fi/bitstream/handle/10024/64705/2013_10_21_HerranenT_ONT_valmis.pdf?sequence=1

Kyberturvallisuuskeskus. 2020. Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut. Viitattu 20.11.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

Lahti, T. 2017. Rakennushankkeiden turvallisuus Puolustusvoimien hallinnoimilla alueilla. Tutkielma. Aalto yliopiston professional development, turvallisuusjohdon koulutusohjelma. Helsinki. Viitattu 1.11.2020. https://www.aaltopro.fi/media/aalto-pro-publications/tjk/lahti_toni_14_tjk_kehitysprojekti.pdf

Laki julkisen hallinnon tiedonhallinnasta 906/2019. Viitattu 19.8.2020. https://www.finlex.fi/fi/laki/ajantasa/2019/20190906

Laki julkisista hankinnoista ja käyttöoikeussopimuksista 1397/2016. Viitattu 17.10.2020. https://www.finlex.fi/fi/laki/alkup/2016/20161397

Laki julkisista puolustus- ja turvallisuushankinnoista 1531/2011. Viitattu 3.11.2020. https://www.finlex.fi/fi/laki/ajantasa/2011/20111531

Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004. Viitattu 19.8.2020. https://www.finlex.fi/fi/laki/ajantasa/2004/20040588?search%5Btype%5D=pika&search%5Bpika%5D=Laki%20kansainv%C3%A4lisist%C3%A4%20tietoturvallisuusvelvoitteista

Laki Puolustusvoimista 551/2007. Viitattu 19.8.2020. https://www.finlex.fi/fi/laki/ajantasa/2007/20070551

Laki viranomaisen toiminnan julkisuudesta 621/1999. Viitattu 19.8.2020. https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Puolustusministeriö. 2015. Kansallinen tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 22.11.2020. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Puolustusministeriö. 2018. Puolustusministeriön ja Puolustusvoimien välinen tulossopimus. Viitattu 19.8.2020. https://puolustusvoimat.fi/documents/1948673/2314399/PEVIESTOS_Vuoden-2019-tulossopimus.pdf/254ac4b3-3c81-bfb3-54c1-ad0bf9619566/PEVIESTOS_Vuoden-2019-tulossopimus.pdf

Puolustusvoimat. 2020a. HX ja Laivue 2020 - Puolustuksen strategiset hankkeet. Viitattu 6.11.2020. https://puolustusvoimat.fi/strategiset-hankkeet

Puolustusvoimat. 2020b. Puolustusvoimien logistiikkalaitos. Viitattu 22.9.2020. https://puolustusvoimat.fi/tietoa-meista/logistiikkalaitos

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere. Viitattu 2.10.2020. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L5_5.html

Saulio, L. 2012. Turvallisuus Puolustusvoimien turvaluokiteltua tietoa sisältävissä rakennushankkeissa. Esiupseerikurssin tutkielma. Maanpuolustuskorkeakoulu. Helsinki. Viitattu 1.11.2020. https://www.doria.fi/bitstream/handle/10024/77305/E4232_SaulioLP_EUK64.pdf;jsessionid=4B16B22517D159A514F3FF3C85F973C2?sequence=1

Simi, J. 2010. Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus. Tutkielma. Teknillinen korkeakoulu, turvallisuusjohdon koulutusohjelma. Helsinki. Viitattu 1.11.2020. https://aaltodoc.aalto.fi/bitstream/handle/123456789/99/urn100170.pdf?sequence=1&isAllowed=y

Turvallisuusselvityslaki 726/2014. Viitattu 28.9.2020. https://www.finlex.fi/fi/laki/ajantasa/2014/20140726

Ulkoministeriö. 2015. Turvallisuusviranomaisen käsikirja yrityksille. Viitattu 19.8.2020. https://um.fi/documents/35732/48132/turvallisuusviranomaisten_käsikirja_yrityksille/b5853259-0795-5fae-ad02-7e9eac6d5841?t=1525647184899

Ulkoministeriö. 2016. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje. Viitattu 7.9.2020. https://um.fi/turvallisuusluokitellun-tiedon-kasittelyohje

Ulkoministeriö. 2020. Voimassa olevat tietoturvallisuussopimukset. Viitattu 8.9.2020. https://um.fi/voimassa-olevat-tietoturvallisuussopimukset

Valtioneuvosto. 2017. Valtioneuvoston puolustusselonteko. Viitattu. 22.11.2020. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79274/J05_2017_VN_puolustusselonteko_Su_PLM.pdf?sequence=1&isAllowed=y

Valtioneuvosto. 2020. Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko. Viitattu 22.11.2020. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162513/VN_2020_30.pdf?sequence=1&isAllowed=y

VNA 1101/2019. Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa. Viitattu 19.8.2020. https://www.finlex.fi/fi/laki/alkup/2019/20191101

VNA 42/2013. Valtioneuvoston asetus turvallisuustoimenpiteistä turvallisuusluokitellun tiedon suojaamiseksi Yhdysvaltojen kanssa tehdyn sopimuksen voimaansaattamisesta sekä sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain voimaantulosta. Viitattu 8.9.2020. https://www.finlex.fi/fi/sopimukset/sopsteksti/2013/20130042#idp446562384

Julkaisemattomat

Aaltonen, A. 2014. Puolustusvoimien turvaluokiteltujen hankkeiden hanketurvallisuus. Esiupseerikurssin tutkielma. Maanpuolustuskorkeakoulu. Helsinki. Tutkielma ei ole julkinen.

Logistiikkalaitos. 2017. Projektin läpivientiohje. Asiakirja HN521, liite 4. Puolustusvoimat. Tampere.

Logistiikkalaitos. 2020. Ohje hankintojen tietoturvallisuusvaatimuksista. Puolustusvoimat. Tampere.

Pihlajamäki, T. 2020. Hanketurvallisuus turvaluokitellun tiedon ja kansainvälisten tietoturvallisuusvelvoitteiden näkökulmasta. Verkkoluento 24.3.2020. Puolustusministeriö.

Pääesikunta. 2015a. Puolustusvoimien hankintamääräys. Normi HK1206. 9.1.2015. Puolustusvoimat. Helsinki.

Pääesikunta. 2015b. Puolustusvoimien turvallisuus. Normi HL205. 16.2.2015. Puolustusvoimat. Helsinki.

Pääesikunta. 2017a. Puolustusvoimien sidosryhmäturvallisuus. Normi HN554. 23.10.2017. Puolustusvoimat. Helsinki.

Pääesikunta. 2017b. Hankeohje. Normi HN918. 22.12.2017. Puolustusvoimat. Helsinki.

Pääesikunta. 2017c. Joukon ja järjestelmän elinjakson hallinta. Normi HN917. 22.12.2017. Puolustusvoimat. Helsinki.

Pääesikunta. 2017d. Turvallisuusjärjestelyiden varmistaminen Puolustusvoimien ja sidosryhmien välisessä yhteistyössä. Normi HN555. 23.10.2017. Puolustusvoimat. Helsinki. Asiakirja ei ole julkinen.

Pääesikunta. 2017e. Puolustusvoimien toiminta. Normi HN707, liite 5. 23.11.2017. Puolustusvoimat. Helsinki.

Pääesikunta. 2018. Sotilaallisen suorituskyvyn käsitemalli. Normi HO46. 31.5.2018. Puolustusvoimat. Helsinki.

Pääesikunta. 2020. Puolustusvoimien tietoturvallisuusohje. Normi HP790, liite 1. 2.1.2020. Puolustusvoimat. Helsinki.

Haastatteluaineisto. 2020. Vastaajat 1-9. Elo-lokakuu 2020. Materiaali opinnäytetyön tekijän hallussa.

Kuviot

Taulukot

Liitteet

Liite 1: Käsitteet ja määritelmät

Tärkeimmät tässä työssä käytettävät käsitteet ovat määritelty seuraavasti:

Asiakirja on kirjallinen tai kuvallinen dokumentti, joka voi olla myös digitaalisessa muodossa (Laki viranomaisten toiminnan julkisuudesta 621/1999, 5 §).

Asiakirjan käsittelyllä tarkoitetaan asiakirjan vastaanottamista, laatimista, tallentamista, katselua, muuttamista, luovuttamista, kopiointia, siirtoa, välittämistä, tuhoamista, säilyttämistä ja arkistointia sekä muita asiakirjaan kohdistuvia toimenpiteitä (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019, 2 §).

Erityissuojattavaa tietoaineistoa ovat salassa pidettävät asiakirjat ja materiaalit sekä asiakirjoista ja materiaaleista saatavissa olevat tiedot sekä näiden perusteella tuotetut asiakirjat ja materiaalit, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu (Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004, 2 §).

Hanke on tässä työssä toimintokokonaisuus, jossa hankitaan Puolustusvoimien kehittämisohjelmassa määritetyn suorituskyvyn osana uusi järjestelmä Puolustusvoimien käyttöön (Pääesikunta 2017b, 5).

Hankinta on kaupallinen toiminto materiaalin, palvelun tai työn ostamisesta ulkopuoliselta toimijalta (Pääesikunta 2017b, 5).

Henkilöturvallisuusselvitys on henkilön nuhteettomuuden tai luotettavuuden varmistamiseksi laadittu selvitys (Turvallisuusselvityslaki 726/2014, 3 §).

Kansainvälinen tietoturvallisuusvelvoite on Suomea sitova kansainväliseen sopimukseen sisältyvä määräys tai muu Suomea koskeva velvoite, jota Suomen on noudatettava ja joka koskee erityissuojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä (Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004, 2 §).

Sidosryhmä tarkoittaa kaikkia niitä Puolustusvoimien ulkopuolisia tahoja (kotimaisia tai ulkomaalaisia) joiden kanssa Puolustusvoimat tekevät yhteistyötä. Yhteistyöllä tarkoitetaan kaikkea toimintaa mitä näiden sidosryhmien kanssa tehdään. (Pääesikunta 2017a, 2).

Sidosryhmäturvallisuus tarkoittaa kaikkia niitä menetelmiä ja toimenpiteitä, joita käytetään sidosryhmien kanssa toimittaessa suojaamaan julkisuuslain tai muun säädöksen perusteella salassa pidettäväksi tai turvallisuusluokitelluksi määrättyä tietoa. Sidosryhmäturvallisuuden keinoin varmistetaan sovittujen palveluiden ja velvoitteiden toteutuminen sekä laatu ja

minimoidaan riskit, jotka syntyvät yhteistoiminnasta joko Puolustusvoimille tai sidosryhmille (Pääesikunta 2017a, 2).

Salassa pidettävä tieto on julkisuuslain 24 §:n pykälän perusteella tai muun säädöksen perusteella viranomaisen salassa pidettäväksi määrittämä tieto (Laki viranomaisten toiminnan julkisuudesta 621/1999, 24 §).

Tietoaineisto tarkoittaa asiakirjoista ja muista vastaavista tiedoista muodostuvaa tietokokonaisuutta. (Laki julkisen hallinnon tiedonhallinnasta 906/2019, 2 §).

Kansainväliset tietoturvallisuussopimukset ovat valtiosopimuksia, jotka määrittävät perusperiaatteet sekä vähimmäisstandardit turvaluokittelun tiedon suojaamiseksi valtioiden tai kansainvälisten organisaatioiden välillä. (Euroopan unionin terminologia 2020).

Turvallisuusdokumentaatio on tässä työssä hankkeen aikana tarvittava ja syntyvä hankkeen turvallisuuden toteuttamiseen liittyvä asiakirja- ja tietoaineisto. (Kosola 2012, 65).

Turvallisuusluokiteltu tieto on julkisuuslain 24§:n 1 momentin 2, 5 tai 7-11 kohdan perusteella salassa pidettävä tieto, jonka oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle. (Laki julkisen hallinnon tiedonhallinnasta 906/2019, 18 §).

Viranomaisia ovat valtion hallintoviranomaiset sekä muut valtion virastot ja laitokset (Laki viranomaisten toiminnan julkisuudesta 621/1999, 4 §).

Yritysturvallisuusselvitys on yrityksen ja sen vastuuhenkilöiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi laadittava selvitys (Turvallisuusselvityslaki 726/2014, 3 §).

Liite 2: Saatekirje

Hyvä vastaanottaja,

Suoritan turvallisuusjohtamisen YAMK-opintoja Laurea ammattikorkeakoulussa, Espoossa. Olen aloittanut opintoihini kuuluvan opinnäytetyön tekemisen ja sen aiheena on "Hanketurvallisuuden kehittäminen Puolustusvoimissa." Hanketurvallisuus on rajattu tässä opinnäytetyössä turvaluokitellun tiedon käsittelyyn ja vaihtoon sekä sen aiheuttamiin vaatimuksiin Puolustusvoimien ja sidosryhmien välisessä yhteistyössä. Opinnäytetyö käsittelee sitä, minkälaisia määräyksiä turvaluokitellun tiedon vaihtoon ja käsittelyyn liittyy Puolustusvoimien ja sidosryhmien välillä, miten nuo määräykset toteutuvat Puolustusvoimien hanketoiminnassa ja miten nämä saataisiin kohtaamaan entistä paremmin.

Pyytäisin mahdollisuutta päästä haastattelemaan teitä hanketurvallisuuden asiantuntijana.

Opinnäytetyön viitekehys rakentuu Puolustusvoimien ja sidosryhmien väliseen, turvaluokitellun tiedon vaihtoon ja käsittelyyn liittyvästä lainsäädännöstä, asetuksista, normeista ja ohjeista. Haastattelun tarkoituksen on vahvistaa ja laajentaa tietopohjaa näistä sekä kuvata niitä haasteita ja uhkia mitä tähän asiaan liittyy teidän näkökulmastanne.

Haastattelun turvaluokka on julkinen eli lopullinen opinnäytetyö tulee Internetiin kaikkien saataville. Haastattelu on muodoltaan ns. teemahaastattelu (puolistrukturoitu haastattelu). Kysymykset/haastatteluteemat toimitan teille pari viikkoa ennen haastattelua ja haastattelu voidaan tarvittaessa tehdä etänä, esimerkiksi Skypen välityksellä. Haastatteluaineistoa käsitellään siten, että tuloksia purettaessa yksittäisen haastateltavan vastaukset eivät tule esiin. Mikäli teille sopii, niin julkaisen kuitenkin nimenne haastattelutaulukossa työn liitteenä.

Olisitteko käytettävissä asiantuntijana opinnäytetyöhöni elo-syyskuun aikana? Aikataulussa on omalta osaltani joustovaraa vielä lokakuun alkupuolelle mutta ehdottamani ajankohta sopisi parhaiten työskentelysuunnitelmaani.

Mikäli teille sopii, niin lähettäisin mielelläni haastatteluiden ja muun aineiston pohjalta tehdyt johtopäätökset teillä reflektoitavaksi ennen työn julkaisua. Haastatteluaineisto hävitetään opinnäytetyön valmistuttua viimeistään vuoden 2021 aikana.

Kunnioittaen,

Timo Tolkki

Liite 3: Teemahaastattelun runko

Haastattelu toteutetaan puolistrukturoituna teemahaastatteluna. Teemahaastattelu tarkoittaa sitä, että haastattelulla on ennalta määritetyt teemat ja muutamia keskustelua ohjaavia kysymyksiä mutta sinänsä keskustelu teeman alla voi kulkea kohtuullisen vapaasti. Teemat on valittu siten, että haastateltavat voivat tuoda teemoihin sisältöä omasta näkökulmastaan ja haastattelun teemat ovat kaikille haastateltaville samat.

Hankkeella tarkoitetaan tässä työssä: ”toimintakokonaisuutta, jossa tuotetaan Puolustusvoimien kehittämisohjelmassa määritetyn suorituskyvyn osa, kuten toimintakykyinen joukko tai järjestelmä.”

PV:n hankeohjeen mukaan hankeohjeen mukaan hanketurvallisuus voidaan jakaa kolmeen osaan: hankeen toteuttamiseen liittyvää turvallisuuteen, hankkeen lopputuotteen turvallisuuteen sekä lopputuotteen käyttöperiaatteisiin liittyvään turvallisuuteen

Tässä opinnäytetyössä käsittelen hanketurvallisuuden osa-alueista ***hankkeen toteuttamiseen liittyvää sidosryhmäturvallisuutta.***

Käsiteltävät teemat:

Esittely

- Kuvaile mikä on yleisesti oma kokemuksesi hankkeista ja hanketurvallisuudesta?

Teema 1: Hanketurvallisuuden määritelmä

Yleistä hanketurvallisuudesta:

- Kuvaile miten itse ymmärrät hanketurvallisuuden omaan tehtävääsi liittyen?
- Mitkä ovat omasta näkökulmastasi hanketurvallisuuden tärkeimmät/tärkein tavoitteet?

Teema 2: Hanketurvallisuuden nykytila

Hanketurvallisuuden toteutuminen Puolustusvoimissa:

- Kuvaile miten omasta näkökulmastasi Puolustusvoimien hankkeiden turvallisuus toteutuu suhteessa lainsäädäntöön, normeihin ja ohjeisiin?

Teema 3: Hanketurvallisuuden kehittäminen

Hanketurvallisuuden onnistuminen

- Mitkä ovat mielestäsi onnistuneen hanketurvallisuuden avaintekijät?
- Esimerkkien kautta kuvaileminen?

Haasteet hanketurvallisuuden toteutumisessa:

- Kuvaile minkälaisia haasteita olet kohdannut hanketurvallisuuden toteutumisessa?
- Esimerkkien kautta kuvaileminen?

Kehittämisehdotuksia

- Kuvaile, miten kehittäisit/mihin kiinnittäisit huomioita Puolustusvoimien hanketurvallisuuden kehittämistyössä.

Liite 4: Haastateltavat

HAASTATTELU NRO	TEHTÄVÄ JA ORGANISAATIO	KOKEMUS
1	Lakimies, ulkoasiainhallinto	9 vuotta kansainvälisen tietoturvallisuuden tehtävissä
2	Hankeasiantuntija, puolustushallinto	+ 10 vuotta hankealan tehtävissä
3	Turvallisuusasiantuntija, puolustushallinto	+ 20 vuotta turvallisuusalan tehtävissä
4	Hankeasiantuntija, puolustushallinto	+ 20 vuotta hankealan tehtävissä
5	Hankeasiantuntija, puolustushallinto	3 vuotta hankkeiden turvallisuustehtävissä
6	Lakimies, ulkoasiainhallinto	10 vuotta kansainvälisen tietoturvallisuuden tehtävissä
7	Hankeasiantuntija, puolustushallinto	+20 vuotta hankealan tehtävissä
8	Turvallisuusasiantuntija, puolustushallinto	+ 15 vuotta turvallisuusalan tehtävissä
9	Turvallisuusasiantuntija, puolustushallinto	+ 10 vuotta hankkeiden turvallisuustehtävissä

Liite 5: Tutkimuslupa

1. Timo Tolkin tutkimuslupa-anomus (MQ5657/06.03.2020)
2. PESUUNNOS määräys HM751/18.01.2017: Tutkimusluvat Puolustusvoimissa

HALLINTOPÄÄTÖS TIMO TOLKIN TUTKIMUSLUPAHAKEMUKSEEN

1 PERUSTEET

Kapteeni Timo Tolkki on ensimmäisellä viiteasiakirjalla hakenut tutkimuslupaa Pääesikunnasta turvallisuusjohtamisen YAMK-tutkintoon kuuluvaa opinnäytetyötä varten. Opinnäytetyön tavoitteen on kehittää Puolustusvoimien hankkeiden turvallisuutta erityisesti turvaluokitellun tiedon vaihtamiseen liittyen Puolustusvoimien ja yritysten välillä.

2 PÄÄESIKUNNAN OPERATIIVISEN OSASTON HALLINTOPÄÄTÖS LUPAEHTOINEEN

Tällä päätöksellä Pääesikunnan operatiivinen osasto myöntää Timo Tolkille tutkimusluvan ja aineistonkäyttöoikeuden.

Tutkimuksen lupaehdot ovat seuraavat:

1. Lupa koskee tässä asiakirjassa nimettyä henkilöä. Tämä tarkoittaa sitä, että tutkimusaineistoa eivät saa käsitellä muut tai aineistoa ei saa luovuttaa muille.
2. Vastuullisena tutkijana ja luvanhaltijana toimii Timo Tolkki.
3. Lupa koskee ainoastaan hakemuksessa kuvatun tutkimuksen suorittamista. Tutkimus voidaan toteuttaa tutkimussuunnitelmassa (liite 2) kuvatulla tavalla.
4. Lupa ja aineistonkäyttöoikeus on määräaikainen. Luvan voimassaolo päättyy 31.12.2021.
5. Luvanhaltija ei voi omin toimin luovuttaa aineistonkäyttöoikeutta kenellekään toiselle. Aineistonkäyttöoikeuden luovuttamiseksi katsotaan kaikki sellainen tutkimus-, ohjaus-, julkaisu tai muu toiminta, jossa Puolustusvoimien omistamien tietojen käyttöoikeus edes välillisesti siirretään jollekin toiselle.
6. Puolustusvoimien aineistoa (ml. haastattelut) on käsiteltävä turvallisuusluokkaan TLIV kuuluvana.
7. Tutkija saa toimittaa aineistosta hakemuksessaan esittämänsä julkisen opinnäytteen. Pääesikunnan operatiivinen osasto tarkastaa opinnäytteen julkisuuden ennen sen julkaisemista.

8. Tämän luvan asiakirjanumero AQ4901 on mainittava kaikissa tutkimusaineistosta tehdyissä julkaisuissa.
9. Luvanhaltija vastaa tutkimukseensa liittyen itse yhteydenotoista haastatteluiden kohteena oleviin asiantuntijoihin ja käytännön järjestelyiden sopimisesta.
10. Tämän luvan ehtojen rikkomisesta seuraa tutkimusluvan peruminen ja asian oikeudellinen arviointi.

3 MUUTOKSENHAKU JA VALITUSOSOITUS

Tähän päätökseen tyytymätön voi hakea siihen muutosta valittamalla Helsingin hallinto-oikeuteen tämän asiakirjan liitteenä olevan valitusosoituksen mukaisesti.

4 LISÄTIETOA

Tästä päätöksestä lisätietoja antaa everstiluutnantti Lauri Kajava Pääesikunnan operatiiviselta osastolta.

Apulaisosastopäällikkö

Eversti Tommi Heikkala

Sektorijohtaja

Everstiluutnantti Lauri Kajava

Tämä asiakirja on sähköisesti allekirjoitettu.

LIITTEET 1 - Valitusosoitus

2 - Tolkin tutkimussuunnitelma