Markus Ketonen

KYBERSIETOISUUDEN HUOMIOIMINEN HANKKEISSA

Opinnäytetyö

Kyberturvallisuus

Insinööri YAMK

2022

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (ylempi AMK)
Tekijä/Tekijät	Markus Ketonen
Työn nimi	Kybersietoisuuden huomioiminen hankkeissa
Toimeksiantaja	Puolustusvoimat
Vuosi	2022
Sivut	61 sivua, liitteitä 7 sivua
Työn ohjaaja	Marko Oras

TIIVISTELMÄ

Tutkittavana oleva käsite oli kybersietoisuus. Opinnäytetyön tarkoituksena oli tuottaa uutta ja luotettavaa tietoa kehittämään kybersietoisuuden huomioimista hankkeen toiminnassa. Tutkimustehtävänä oli selvittää Puolustusvoimien hankkeen elinkaariprosessi ja määritellä, miten ohjeet ja normit ohjaavat hanketta. Opinnäytetyön tutkimus toteutettiin puolistrukturoidun teemahaastattelun ja Webropol-kyselyn avulla, joiden tavoitteena oli selvittää hankkeen asiantuntijoiden hankkeen aikana kehittämät parhaat toimenpiteet ja tunnistaa kehitettävät osa-alueet hankkeen ja järjestelmän elinkaaressa.

Tässä opinnäytetyössä käytettiin lähestymistapana kvalitatiivista tutkimusotetta, jossa konstruktiivista tutkimusta käytettiin tarkentavana tutkimusmenetelmänä. Opinnäytetyön tutkimuksessa keskityttiin teemahaastatteluiden ja Webropol-kyselyssä havaittuihin tuloksiin, joita verrattiin teoriaosuuden sisältöön.

Opinnäytetyön tutkimus jaettiin kahteen vaiheeseen, jossa ensimmäisessä vaiheessa kerättiin lähdemateriaali ja muodostettiin opinnäytetyön teoriaosuus. Lähdekirjallisuutta ja materiaalia hankittiin erilaisista sähköisistä lähteistä, Maanpuolustuskorkeakoulun (MPKK) kirjastosta sekä Puolustusvoimien sisäisistä ohjeista ja normeista. Tutkimuksen toisessa vaiheessa toteutettiin tutkimuksen käytännön osuus, joka koostui asiantuntijahaastatteluista ja Webropol-kyselystä. Toinen vaihe sisälsi myös haastatteluiden ja Webropol-kyselystä saatujen vastausten analysoinnin.

Haastattelujen, Webropol-kyselyn sekä teoriaosiossa käytettyjen normien ja ohjeiden perusteella oli mahdollista todeta, että Puolustusvoimien ja Suomen kansallisen lainsäädännön ohjeistukset ja normit ovat hyvin laajoja kokonaisuuksia. Haastatteluissa korostettiin, että järjestelmien hyväksymisprosessi on raskas dokumenttikeskeinen prosessi. Tätä prosessia tulee kehittää niin, että pitkän aikavälin hankkeet voisivat reagoida tekniikan kehitykseen riittävällä nopeudella. Kybertoimintaympäristö on jatkuvasti ja nopeasti kehittyvä kokonaisuus, joten tämä tulee huomioida hankkeen elinkaaressa. Tärkeintä opinnäytetyön lopputuotoksen perusteella oli, että pystyttiin muodostamaan opetussisältöä Kybersietoisuuden huomioiminen hankkeessa -opetustilaisuuteen.

Asiasanat: Kybersietoisuuden kehittäminen, resilienssisuunnittelu, tietoturvallisuus, kyberturvallisuus, käytettävyys

South-Eastern Finland University of Applied Sciences

Degree title	Master of Engineering
Author (authors)	Markus Ketonen
Thesis title	Cyber resilience in a project
Commissioned by	Puolustusvoimat
Time	2022
Pages	61 pages, 7 pages of appendices
Supervisor	Marko Oras

ABSTRACT

The concept under study was cyber resilience. The purpose of this master's thesis was to produce new and reliable information to develop the attention of cyber resilience in project management. The task of this master's thesis research mission was to find out the life cycle process in Finnish Defense Forces project and to define how the guidelines and norms guide the project(s). The study was conducted through a semi-structured themed interview and a Webropol survey aimed at finding out the best measures developed by the project experts during the project and to identify possible areas of the project's expertise.

In this master's thesis a qualitative study approach was used and a constructive research method was used as a refining and more detailed research method. The focus of this master's thesis was in the content gathered from the semi-structured themed interviews and the theory content of this thesis were used as a secondary source material.

The research process of this master's thesis was divided into two phases. The first phase consisted of collecting the source literature and writing the theory section of this master's thesis. The source literature and material were retrieved from various electronic sources, The National Defence University (NDU) library and Finnish Defence Forces internal directives and norms. The second, practical phase of the study consisted of as expert interviews and the Webropol survey. The second phase also included analyzing the responses received from the interviews and Webropol survey.

Based on the interviews, Webropol survey and the norms and guidelines used in the theory section, it was possible to establish that the guidelines and standards of the Finnish Defence Forces and Finnish national legislation are very broad. It was emphasized in the interviews that the systems approval process is a heavy, document-oriented process. This process should be developed to enable long-term projects to respond to technological progress at a sufficient rate. The cyber environment is a constantly and rapidly evolving entity, so this should be considered in the life cycle of the project. Based on the thesis, it was possible to produce source material and educational content for the Cyber Resilience in Project seminar.

Keywords: Cyber resilience development, cyber resilience engineering, information security, cyber security, usability

SISÄLLYS

1 JOHDANTO

Valtionneuvoston julkaiseman puolustusselonteon (2021) mukaan kyberpuolustusta tulee kehittää niin, että sen avulla voidaan turvata paremmin Puolustusvoimien omat sekä muut puolustuskykyyn suoraan vaikuttavat järjestelmät. Digitalisaation yleistymisen vaikutukset näkyvät myös puolustuksen toimintaympäristön kasvuna, jolloin puolustuksen toimintakyvyt ja järjestelmät ovat yhä enemmän riippuvaisia kybertoimintaympäristöstä (Valtionneuvosto 2021 8–9, 32). Kybertoimintaympäristö on jatkuvasti muuttuva, joten järjestelmän selviytymisen vaatimukset ovat lisääntyneet. Tähän pyritään yleisimmin vastamaan tietoturvallisuudella, jonka tarkoituksena on varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Tietoturvallisuus määritellään Kyberturvallisuussanaston (2018) mukaan seuraavasti: -- "S*aatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa*" (Turvallisuuskomitea 2018, 15). Tietoturvallisuus ei itsessään ole riittävä, kun kybertoimintaympäristön kautta muodostuvat kyberuhat koostuvat jatkuvista, kehittyneistä ja muuntautumiskykyisistä turvallisuusuhista. Näihin kyberuhkiin pyritään vastaamaan kybersietoisuudella, jolloin järjestelmällä on kyky ennakoida kyberuhkia vastaan kyberresursseja, jotka ovat kestäviä ja sopeutuvia epäsuotuisissa olosuhteissa. (Bodeau ym. 2017, 1.)

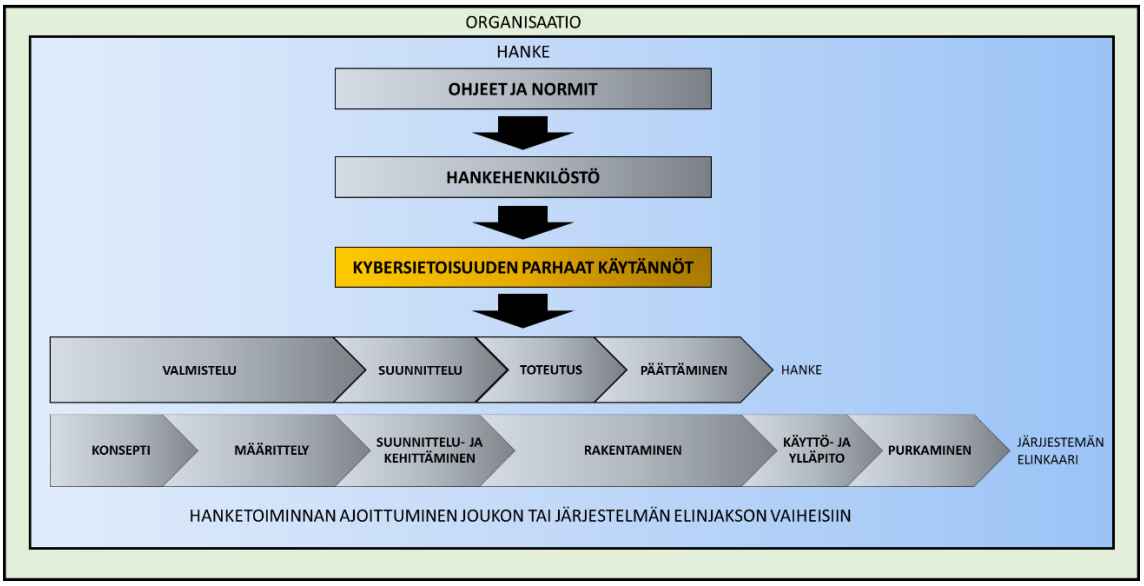
Puolustusvoimien kehittämisohjelmat voivat olla kymmenien tai jopa satojen miljoonien eurojen suuruisia laajoja suorituskyvyn kokonaiskehittämiseen tähtääviä tehtäväkokonaisuuksia. Nämä kehittämisohjelmat toteutetaan hankkeina, projekteina ja hankintoina, joissa suorituskykykokonaisuus koostuu toimintakokonaisuuksista. Nämä kehittämisohjelmat muodostavat Puolustusvoimissa määritetyn suorituskyvyn osan, kuten toimintakykyisen joukon tai järjestelmän. Hanke on Puolustusvoimien kehittämisen peruselementti, jolla kehitetään yhden suorituskyvyn kaikkia osatekijöitä: henkilöstöä, materiaalia, käyttö- ja toimintaperiaatetta, organisaatiota sekä toiminnan tarvitsemaa informaatiota. (Kosola 2012, 9.) Esimerkkinä voidaan käyttää Puolustusvoimien strategisina hankkeina toteutettavia HX-hanke sekä hanketta Laivue 2020 (Puolustusvoimat 2021).

Kybersietoisuus käsitteenä on vielä toistaiseksi vähän käytetty käsite ja termi, jolle ei löydy suoraa määritelmää suomenkielellä. Ulkomaalaisissa lähdeteksteissä kybersietoisuutta tarkoittava termi on *Cyber Resilience* tai *Cyber Resiliency* (Bodeau ym. 2011). Kybersietoisuuden lähimpänä suomenkielisenä vastineena voidaan pitää resilienssi-sanaa (sietoisuus), joka määritellään kyberturvallisuuden sanastossa (2018) seuraavasti: -- "*yksilöiden ja yhteisöjen kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja kriisejä ja palautua niistä"* (Turvallisuuskomitea 2018, 14).

1.1 Tutkimustehtävänä kybersietoisuus hankkeen elinkaaressa

Tutkittavana ilmiönä ja käsitteenä on kybersietokyky. Opinnäytetyön tavoitteena on tuottaa uutta ja luotettavaa tietoa kehittämään kybersietoisuuden huomioimisesta hankkeen toiminnassa. Tutkimustehtävänä on selvittää Puolustusvoimien hankkeen elinjaksojen hallintaprosessin toiminta sekä hanketta ohjaavien ohjeiden ja normien merkitys. Haastattelemalla hankkeen asiantuntijoita pyritään selvittämään parhaat toimenpiteet, joita he ovat kehittäneet hankkeen aikana sekä tunnistaa mahdollisesti kehitettävät osa-alueet hankkeen asiantuntijoiden osaamisesta. Opinnäytetyön lopputuotoksen tavoitteena on, että voidaan tehdä opetusehdotuksia Kybersietoisuuden huomioinen hankkeessa -opetustilaisuuteen.

Kuvassa yksi (1) esitetään opinnäytetyön viitekehys, jolla havainnollistetaan Puolustusvoimien hankeprosessi vaiheittaisena mallina suhteutettuna järjestelmän elinkaareen. Ohjeet ja normit ovat niitä, jotka ohjaavat hankehenkilöstöä ja keskiössä on korostettuna kybersietoisuuden parhaat käytännöt. Tällöin havainnoinnin kohteena on ihminen ja tämän toiminnan suhde tutkittavaan ilmiöön (Kananen 2015 78). Tässä opinnäytetyössä ei keskitytä Puolustusvoimien kybersietoisuuden toteutuksen konseptiin tai tekniikkaan. Kybersietoisuutta tarkastellaan hankkeen prosessin ja parhaiden käytänteiden näkökulmasta.



Kuva 1. Opinnäytetyön viitekehys mukailtuna (Pääesikunta 2017)

Hankkeen onnistunut toteuttaminen edellyttää Puolustusvoimien normien ja ohjeiden sekä parhaiden käytänteiden tasapuolista huomioimista hankkeen elinkaaren kaikissa vaiheissa sekä on osattava sovittaa ne osaksi hanketta. Tutkimusongelmana on ymmärtää kybersietoisuuden merkitys ja tämän merkitys hankkeen ja järjestelmän elinkaaressa, joten tästä voitiin muodostaa seuraava tutkimuskysymys: Miten kybersietoisuuden huomioimista hankkeen elinkaaressa voidaan kehittää?

Apukysymyksinä ovat:

1. Vastaavatko Puolustusvoimien normit ja ohjeet akateemista tutkimusaineistoa?
2. Mitä ovat ne käytännöt, joita hankkeessa työskentelevät henkilöt ovat kehittäneet?
3. Vastaako Puolustusvoimien hanketoiminnassa toteutettava käytäntö tutkimusaineiston teoriaa?

Tutkimushypoteesiksi voidaan muodostaa, että hankehenkilöstö käsittää hankkeen prosessit ja järjestelmän elinkaarivaiheet normiohjauksen perusteella sekä osaa soveltaa käytännössä kybersietoisuuden merkitystä hankkeen ja järjestelmän elinkaareen.

1.2 Aikaisempi tutkimus ja tärkeimmät lähteet opinnäytetyölle

Kybertoimintaympäristöä ja -turvallisuutta käsitteleviä tutkimuksia löytyi tietokantahaun hetkellä runsaasti, mutta käsitteenä ”kybersietoisuus”, esiintyi suomenkielisessä tutkimuksessa, julkaisussa tai blogikirjoituksessa 39 kertaa. Haettaessa sanalla "resilienssi" haun tulos tuottaa tulokseksi tutkimuksia psykologiassa, jossa resilienssillä tarkoitetaan henkistä kapasiteettia, jonka avulla ihminen pystyy, usein tiedostamattomasti, hyödyntämään niitä voimavaroja ja vahvuuksia, jotka ylläpitävät hänen hyvinvointiaan erilaisissa tilanteissa. (Helsingin yliopisto 2020.)

Tehtäessä tietokantahakua sanoilla ”resilienssi kyberturvallisuus” lähimpänä tämän opinnäytetyön tutkimusta voidaan pitää valtionneuvoston selvitys- ja tutkimustoiminnan julkaisusarjan raporttia 17/2019: Kokonaisresilienssi ja turvallisuus: tasot, prosessit ja arviointi. Raportissa tarkennetaan resilienssin merkitystä sekä esitetään keinoja edistää resilienssiä suomalaisessa yhteiskunnassa. Resilienssi määritellään raportissa kolmivaiheisesti vastustuskyvyksi, toimintakyvyn säilyttämiseksi ja oppivaksi mukautumiseksi. (Hyvönen ym. 2019.)

Puolustusvoimien hankintoja, hanketta, projektia tai sen turvallisuutta koskevia tutkimuksia löytyi tietokantahakujen perusteella useampia, mutta nämä käsittelevät kuitenkin pääsääntöisesti hankkeiden turvallisuutta tai osaamisvaatimuksia eri näkökohdista. Alla on listattuna aihealuetta käsittelevät tutkimukset.

Jarkko Simin (2010) tekemä tutkielma Teknillisessä korkeakoulussa Koulutuskeskus Dipolin turvallisuusjohdon koulutusohjelmassa: Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus. Tutkimuksen tavoitteena oli luoda esimerkki, miten hankintaprosessin eri vaiheissa tulee huomioida turvallisuusasiat ja miten turvallisuusvastuut jakautuvat hankintaprosessin eri toimijoille. Tutkimuksessa selvitettiin, mitä vaatimuksia normit asettavat hankintaprosessin turvallisuudelle.

Lauri Saulion Esiupseerikurssilla 64 (2012) tekemä tutkimus, jossa selvitettiin mitä turvallisuus tarkoittaa Puolustusvoimien turvaluokiteltua tietoa sisältä-

vissä rakennushankkeissa. Tutkimuksen mukaan rakennushankkeen tärkeimmät turvallisuustoimenpiteet kohdistuvat palvelunhankintaan, jossa tulee turvallisuus huomioida jo tarveselvitysvaiheessa sekä projektin kulun ja turvallisuuden kannalta tärkeimmät päätökset tehdään hankesuunnitteluvaiheessa. Saulion tekemä tutkimus sopii tämän opinnäytetyön aihealueeseen hyvin, koska Saulio käsitteli työssään Puolustusvoimien normeja sekä ohjeita, jotka viittaavat hanketurvallisuuteen.

Tätä opinnäytetyötä tukevana työnä voidaan pitää Timo Tolkin (2020) Laurean ylemmän ammattikorkeakoulun turvallisuusjohtamisen koulutusohjelmassa tekemää opinnäytetyötä. Tutkimuksen aiheena ja tavoitteena oli hankkeiden turvallisuuden kehittäminen Puolustusvoimissa. Tolkki tarkasteli hanketurvallisuutta sidosryhmien näkökulmasta ja työn keskeisimpänä tuloksena hän piti neljää asiakokonaisuutta: hankkeen turvallisuusvaatimusten huolellinen määrittely hanketta valmisteltaessa, turvallisuuden asiantuntijaresurssien käyttö, henkilöstön osaamisen säännöllinen ylläpito ja kasvattaminen sekä käytännön toimenpideohjeiden laadinta ja saatavuus. Tolkin tekemä opinnäytetyö sopii tämän työn aihealueeseen hyvin, koska työ on varsin tuore ja käsittelee myös Puolustusvoimien normeja sekä ohjeita. Huomioina pitää muistaa, että Tolkin työssä näkökulma on sidosryhmien turvallisuudessa, mutta kokonaisuutena on varsin kattava.

Kybersietoisuus kytketään ulkomaisessa tutkimuskirjallisuudessa systeemisuunnitteluun (System Engineering) ja systeemien turvallisuussuunnitteluun (Systems Security Engineering). Systeemiajattelu on jo pitkään Puolustusvoimissakin käytetty käsite ja järjestelmien suunnittelua ohjaava toimintamalli. Ulkomaisessa kybersietoisuutta (Cyber Resilience) käsittelevässä kirjallisuudessa ja tutkimusasiakirjoissa kybersietoisuus on ollut jo hetken aikaa käytetty termi ja käsite. Erityisesti Yhdysvalloissa toimivien valtiohallinnon tutkimusorganisaatioiden toimesta on käsitteestä ja aiheesta tehty tutkimuksia ja artikkeleita noin vuodesta 2010 alkaen. (Bodeau ym. 2011.)

Mitre-organisaatio julkaisi vuonna 2011 tutkimusasiakirjan Cyber Resiliency Engineering Framework, jossa kuvataan kybersietoisuuden suunnittelun viitekehys ja miten kybersietoisuus asemoidaan systeemisuunnittelun ala-alojen

joukkoon. Mitre on ulkomaalainen voittoa tavoittelematon organisaatio, jonka tarkoituksena on antaa suunnitteluapua sekä tuottaa teknisiä ohjeita.

Mitre-organisaatio julkaisi vuonna 2017 tutkimusasiakirjan Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines. Tutkimusasiakirja on tarkoitettu järjestelmien suunnittelijoille, joilla on käytännöntietoa kybersietoisuuden käsitteistä ja tekniikoista, kuten miten kybersietoisuuden suunnitteluperiaatteet tunnistetaan ja sovitetaan järjestelmään. Tutkimusasiakirjassa kybersietoisuutta käsitellään siten, että analysoidaan, kuinka hyvin tietty suunnittelu-, toteutus- tai käyttöönottoprosessi soveltuu järjestelmän suunnitteluperiaatteisiin. Tämä tutkimusasiakirja perustuu jo olemassa olevaan Mitre-organisaation vuonna 2011 julkaisemaan Cyber Resiliency Engineering Framework (CREF) kybersietoisuutta koskevaan tutkimusasiakirjaan.

Alexander Kott ja Igor Linkov julkaisivat vuonna 2018 kirjan Cyber Resilience of Systems and Networks. Kirjassa käsitellään kybersietoisuuden peruskäsitteitä, joiden lähteinä on käytetty akateemisia, teollisia sekä valtiollisia tutkimusaineistoja.

NIST-instituutti (National Institute of Standards and Technology) julkaisi vuonna 2021 tutkimusasiakirjan Developing Cyber Resilient Systems: A Systems Security Engineering Approach. Tutkimusasiakirjan tarkoituksena on ohjata, miten kybersietoisuuden käsitteitä, rakenteita ja teknisiä käytäntöjä voidaan soveltaa osaksi järjestelmän systeemisuunnittelua ja riskienhallintaa. Tutkimusasiakirja on tarkoitettu käytettäväksi yhdessä ISO / IEC / IEEE 15288: 2015, Järjestelmäsuunnittelu ja ohjelmistotuotanto -standardin kanssa.

1.3 Opinnäytetyön rakenne

Tässä opinnäytetyössä käytettiin IMRAD-mallin (Introduction, Methods, Research/Results and Discussion) mukautettua rakennetta, joka koostuu johdannosta, tutkimusasetelmasta, teoriaosuudesta, tutkimustuloksista, johtopäätöksistä, lähteistä sekä liitteistä. IMRAD-mallin käytön tarkoituksena on, että tämä antaa opinnäytetyön tieteelliselle kirjoittamiselle pelisäännöt, joita noudattamalla kirjoittaminen, lukeminen ja arviointi helpottuvat. IMRAD-mallissa tietyt

tutkimukseen liittyvät perusasiat löytyvät vakiopaikoiltaan, joka perinteisessä rakennemallissa noudattaa mallia: johdanto, teoriaosuus, tutkimusasetelma, tutkimustulokset, johtopäätökset, pohdinta, lähteet ja liitteet. Rakennemallin valinnalla opinnäytetyön kirjoittaja osoittaa, että aihealue on aukoton ja tutkija aikoo ratkaista esittämänsä ongelman. (Kananen 2015, 14–19.)

Ensimmäisessä luvussa esitetään johdanto opinnäytetyöhön, jossa lukijalle esitetään tutkimustehtävän aihe, aikaisempi tutkimus, tutkimustehtävä ja viitekehys sekä opinnäytetyön rakenne.

Toisessa luvussa käsitellään tutkimusteoriaa ja -menetelmiä sekä kerrotaan, mistä tutkimusaineisto hankkeen ja kybersietoisuuden teoriaosuudelle hankittiin. Luvussa myös kuvaillaan opinnäytetyön tutkimuksen luokittelu sekä tutkimusprosessi.

Kolmannessa luvussa käsitellään kybersietoisuuden periaatteita ulkomaalaisen tutkimuskirjallisuuden mukaan.

Neljännessä luvussa esitetään Puolustusvoimien hanke sekä käsitellään sotilaallisen suorituskyvyn käsitemallia, jonka näkökulmat voidaan rinnastaa kybersietoisuuden resilienssisuunnitteluun. Tässä luvussa esitetään myös Puolustusvoimien turvallisuustoiminta normiohjauksen perusteella sekä käsitellään vaatimustenhallinnan ja riskienhallinnan periaatteita.

Viidennessä luvussa kuvataan käytännön näkökohtia kybersietoisuuden soveltamisesta järjestelmän elinkaaressa, joka pohjautuu ulkomaalaiseen tutkimusasiakirja lähdeaineistoon. Tämä osa opinnäytetyössä on käytännön osuus, joka toteutettiin teemahaastatteluna. Luvussa kerrotaan myös teemahaastatteluiden analyysimenetelmä sekä sisältöanalyysin toteutus.

Kuudennessa luvussa esitetään opinnäytetyön tutkimusprosessin mukaisesti johtopäätökset, joiden tarkoituksena on tutkimustulosten yleistäminen.

Seitsemännessä luvussa pohditaan opinnäytetyön tutkimuksen ja tutkimustuloksien suhdetta teoreettiseen viitekehykseen. Luvussa esitetään myös mah-

dolliset jatkotutkimusaiheet sekä tarkastellaan tutkimuksen luotettavuutta. Luvun tarkoituksena on vastata kysymykseen: Miten kybersietoisuuden huomioimista hankkeen elinkaaressa voidaan kehittää?

2 TUTKIMUSTEORIA JA -MENETELMÄT

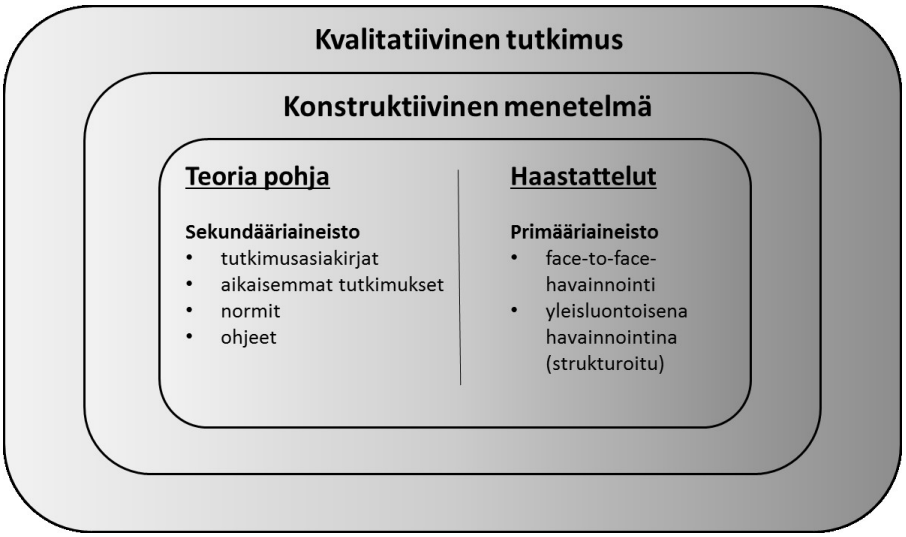
Tässä luvussa käsitellään tutkimusteoriaa ja -menetelmiä sekä kerrotaan, mistä tutkimusaineisto hankkeen ja kybersietoisuuden teoriaosuudelle hankittiin. Luvussa myös kuvaillaan opinnäytetyön tutkimuksen luokittelu sekä tutkimusprosessi.

Tutkimusotteeksi valittiin konstruktiivinen tutkimus, koska opinnäytetyön tavoitteena oli selvittää parhaat toimenpiteet, joita hankehenkilöstö on kehittänyt hankkeen aikana sekä tunnistaa mahdollisesti kehitettävät ja painotettavat osa-alueet hankehenkilöstön osaamisessa (reaalimaailman ongelma). Konstruktiivinen tutkimusote on kehitetty liiketaloustieteen alueelle, mutta sen potentiaalinen soveltamisala on laaja ja varsin suosittu liiketalouden ja tekniikan tutkimuksissa. (Lukka 2001.)

Lukan mukaan konstruktiivinen tutkimusote on innovatiivisia konstruktioita tuottava metodologia, jolla pyritään ratkaisemaan reaalimaailman ongelmia ja tällä tavoin tuottamaan kontribuutioita sille tieteenalalle, jossa sitä sovelletaan (Lukka 2001).

Jorma Kanasen (2017) mukaan tutkimusotteet voidaan luokitella monella tavalla. Tässä opinnäytetyössä käytettiin lähestymistapana kvalitatiivista tutkimusotetta, jota voidaan pitää yläkäsitteenä opinnäytetyön tutkimusluokittelussa. Konstruktiivista tutkimusta käytettiin tarkentavana tutkimusmenetelmänä, joka on enemmän kuin perinteinen kvalitatiivinen tutkimus. Kvalitatiivisessa tutkimuksessa pyritään ymmärtämään ja selittämään tutkittavaa ilmiötä. Konstruktiivinen menetelmä jakaantuu aineistonkeruumenetelmiin ja analyysimenetelmiin, jonka pohjalta muodostettiin tämän opinnäytetyön teoreettinen viitekehys (kuva 2). Opinnäytetyön tutkimuksen keskiössä olivat primääriaineistona teemahaastattelun sisältö induktiivisena sekä abduktiivisena päättelynä. Opinnäytetyön teoriapohja toimi tutkimuksen sekundäärisenä aineistona,

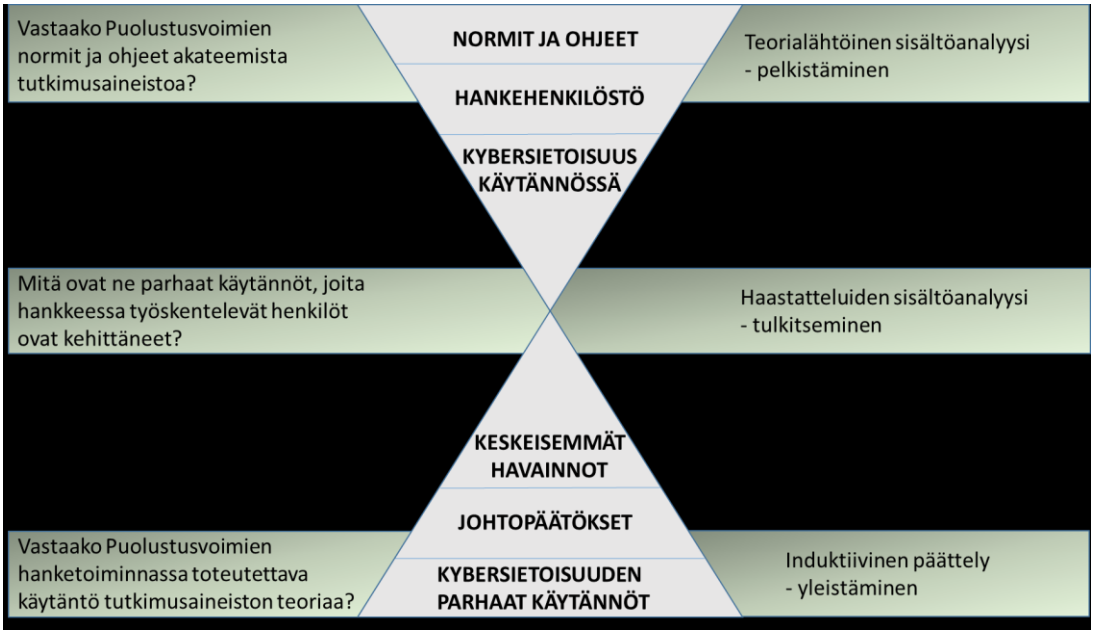
josta muodostettiin sisältöanalyysi. (Kananen 2017, 13; Hirsjärvi & Hurme 2017, 136.)



Kuva 2. Opinnäytetyön teoreettinen viitekehys mukailtuna (Kananen 2017, 13)

2.1 Opinnäytetyön tutkimusprosessi

Opinnäytetyön tutkimusprosessista muodostettiin ensin tiimalasimallin mukainen vaiheittainen etenemismuoto (kuva 3), jonka tarkoituksena on havainnollistaa ja selventää tutkimuksen etenemistapa. Tiimalasimallin sisältö ja vaiheet muodostuivat opinnäytetyön viitekehyksestä (kuva 1) ja tutkimuskysymyksistä, jotka esitettiin luvussa 1.1 Tutkimustehtävänä kybersietoisuus hankkeen elinkaaressa.



Kuva 3. Tutkimusasetelma (Nupponen 2017, 7)

Opinnäytetyön tutkimus jaettiin kahteen vaiheeseen, jossa ensimmäisessä vaiheessa kerättiin lähdemateriaali sekä muodostettiin opinnäytetyön teoriaosuus. Lähdekirjallisuutta ja materiaalia hankittiin erilaisista sähköisistä lähteistä, Maanpuolustuskorkeakoulun (MPKK) kirjastosta sekä Puolustusvoimien sisäisistä ohjeista ja normeista.

Lähteinä käytettävät opinnäytetyöt ja tutkielmat olivat tämän opinnäytetyön tavoitteiden mukaisesti vähintään ylemmän ammattikorkeakoulun tasoisia opinnäytetöitä tai tutkielmia. Puolustusvoimien hankkeita ja projekteja käsitteleviä lähteitä löytyi tietokantahakujen perusteella runsaasti. Opinnäytetyön sekundaarinen viiteaineisto koostui hankkeita ja projekteja käsittelevistä oppaista sekä Puolustusvoimien sisäisistä ohjeista. Sekundaarisen lähdeaineiston tukena käytettiin myös ulkomaalaisia tutkimusasiakirjoja, kybersietoisuutta käsitteleviä kirjoja sekä standardeja.

Kyberturvallisuudesta ja kybertoimintaympäristöstä liittyvää materiaalia on olemassa paljon, mutta itse kybersietoisuudesta ja sen merkityksestä löytyi suhteessa rajoitetusti. Esimerkiksi sanalle "kybersietoisuus" ei ole suomenkielelle selvää määritystä tehtynä, mutta kybersietoisuutta parhaiten kuvaava määritelmä on resilienssi. Englanninkielellä "kybersietoisuutta" käsitellään sanoilla Cyber Resilience tai Cyber Resiliency. Nämä asiat huomioiden pyrittiin keskittymään siihen, että lähdemateriaali oli laadukasta ja hankittu varmennetuista lähteistä.

Tutkimuksen toisessa vaiheessa toteutettiin tutkimuksen käytännön osuus asiantuntijahaastatteluina sekä analysoitiin saatuja vastauksia, joista muodostuivat opinnäytetyön johtopäätökset ja pohdintaosuus. Haastattelut toteutettiin puolistrukturoituna teemahaastatteluina, jonka kysymykset pohjautuivat opinnäytetyön ensimmäisestä vaiheesta. Asiantuntijahaastatteluilla selvitettiin käytännön kokemuksia, kuten: Miten asiantuntijat ymmärtävät kybersietoisuuden? Miten he ovat huomioineet kybersietoisuuden vaatimuksia hankkeen eri vaiheissa? sekä miten asiantuntijat kehittäisivät kybersietoisuuden huomioimista hankkeessa? Asiantuntijahaastatteluiden tavoitteena oli etsiä kokemuksien kautta muodostuneita hyviä menettelytapoja ja verrata niitä tutkimusasiakirjojen ja Puolustusvoimien ohjeiden sekä normien vaatimuksiin. Haastateltavaksi

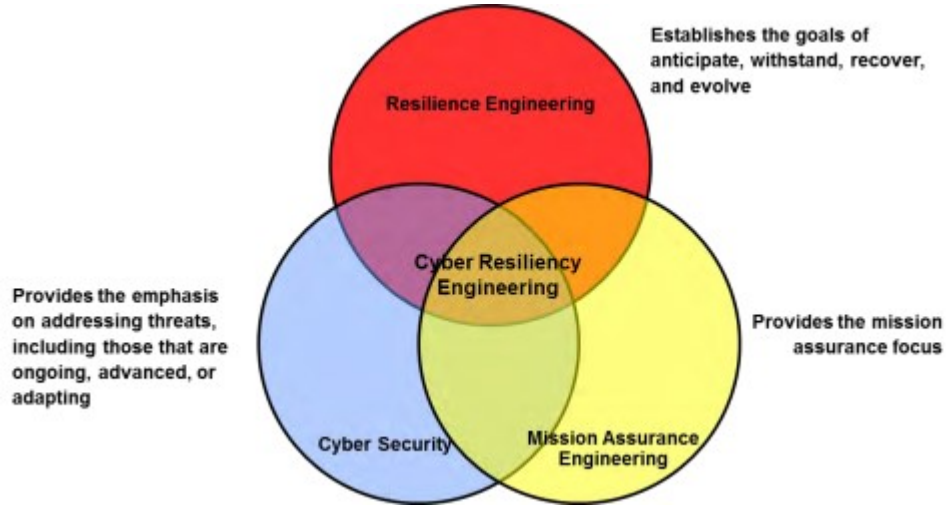
tutkija pyrki saamaan mahdollisimman laajan vastaajajoukon hankkeiden asiantuntijoita, jotta pystyttiin muodostamaan mahdollisimman hyvä vertailupohja käytännön eroavaisuuksista.

3 KYBERSIETOISUUS

Tässä luvussa käsitellään kybersietoisuuden periaatteita Mitre-organisaation vuoden 2011 tutkimusasiakirjan Cyber Resiliency Engineering Framework, Kott & Linkovin vuoden 2018 kirjan Cyber Resilience of Systems and Networks sekä NIST-instituutin vuoden 2021 tutkimusasiakirjan Developing Cyber Resilient Systems: A Systems Security Engineering Approach mukaan.

3.1 Kybersietoisuuden suunnittelun viitekehys

Kybersietoisuuden viitekehys (Cyber Resiliency Engineering Framework, kuva 4) kuvataan Mitre-organisaation (2011) julkaisemassa tutkimusasiakirjassa Cyber Resiliency Engineering Framework siten, että kybersietoisuuden suunnittelu (Cyber Resilience Engineering) muodostuu resilienssisuunnittelusta (Resilience Engineering), kyberturvallisuudesta (Cybersecurity) ja operaatioturvallisuudesta (Mission Assurance Engineering). (Bodeau ym. 2011, 13.)



Kuva 4. Kybersietoisuuden suunnittelun viitekehys Mitre-organisaation mukaan (Bodeau ym. 2011, 13)

Resilienssisuunnittelun tavoitteena on ennakoida, kestää, toipua ja kehittää kyberresursseja, jossa ennakoinnin tarkoituksena on tunnistaa riskienhallin-

nan kautta kyberresurssien sidonnaisuus kybertoimintaympäristöön. Ennakoinnin oleellisena tarkoituksena on taata toiminnan jatkuvuus, joka voidaan mieltää jatkuvuudenhallintana. Jatkuvuudenhallintaa voidaan pitää resilienssisuunnittelun osa-alueena, jolla organisaatio varautuu hallitsemaan häiriötilanteet (esim. sähkönsyötön varmentaminen) ja jatkamaan toimintaansa hyväksyttävällä tasolla. (Turvallisuuskomitea 2018, 14; Ross ym. 2021, 9–10.)

Kestämisen tavoitteena on, että toiminta jatkuu heikentyneessä tai vaihtoehtoisessa tilassa kunnes hyökkäys on käsitelty riittävän hyvin ja toipuminen on mahdollista. Kestämisen ensisijaisena painopisteenä on, että organisaation ja järjestelmän olennaiset toiminnot on tunnistettu ja pyritään estämään kyberhyökkääjän toiminta. (Bodeau ym. 2011, 16; Ross ym. 2021, 10.)

Toipumisen tavoitteena on vahinkojen määrittäminen, palauttaa toiminnallisuudet ja arvioida järjestelmän luotettavuus. Vahinkojen määrittäminen sisältää hyökkäyksessä käytetyn haittaohjelman analysoinnin, joka voidaan toteuttaa esimerkiksi monitoroinnin ja tallenteiden kautta. Analysoinnin perusteella voidaan selvittää esimerkiksi haittaohjelman alkuperä sekä tarvittaessa jakaa tästä tietoa muille organisaatioille. Toipuminen voi olla vaiheittaista, mutta haasteena tässä on palautettujen tietojen ja toimintojen luotettavuus. (Bodeau ym. 2011, 16; Ross ym. 2021, 10.)

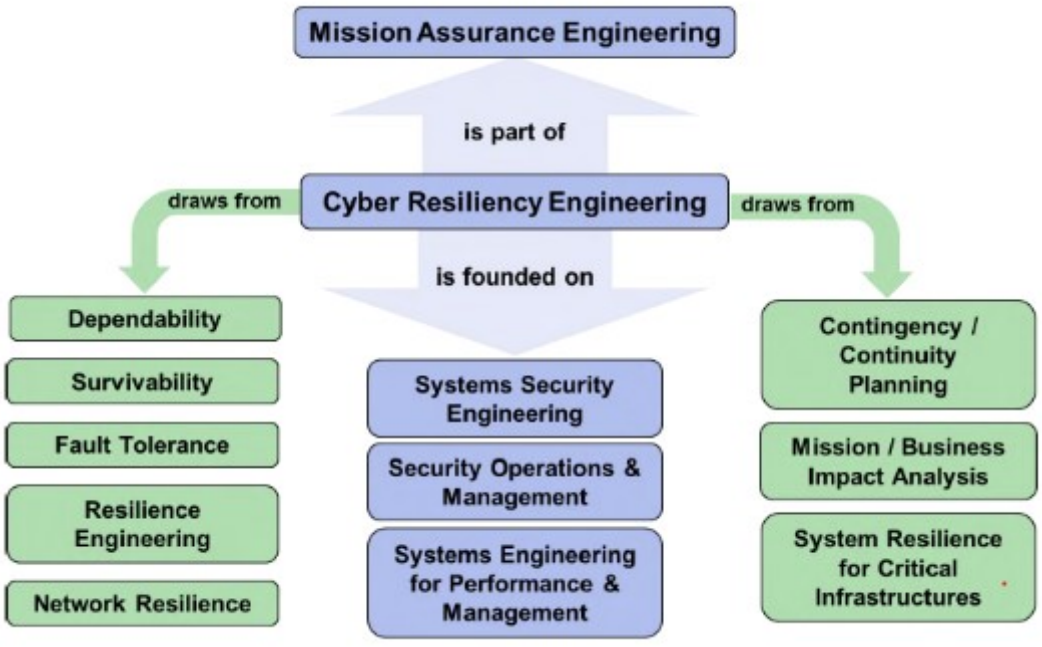
Kehittämisen tavoitteena on muuttaa organisaation prosesseja ja toimintatapamalleja, joissa pyritään minimoimaan todellisia ja suunniteltuja haittavaikutuksia. Ensisijaisesti kehittämisen tavoitteena on kehittää organisaation henkilöstön osaamista, joita voidaan esimerkiksi tarkastella osaamisen kehittämisen kautta. Vasta toisena tulee järjestelmien kehittäminen, jossa järjestelmän haavoittuvuuksia parannellaan kybersietoisuuden näkökulmasta. (Bodeau ym. 2011, 17; Ross ym. 2021, 10.)

Kyberturvallisuus on tiedon, laitteistojen, verkostojen, ohjelmistojen ja käyttäjien luottamuksellisuuden, eheydyn ja saatavuuden turvaamista koko elinjakson ajan. Kyberturvallisuus muodostuu ylläpitäjien ja käyttäjien välisestä yhteistoiminnasta ja siinä huomioidaan kybertoimintaympäristön vaikutukset fyysiseen maailmaan. Kybersietoisuuden suunnitteluun näkökannalta kybertur-

vallisuuden tarkoituksena on tuoda kybertoimintaympäristön kautta muodostamat kyberuhat, jotka muodostuvat jatkuvista, kehittyneistä ja muuntautumiskykyisistä kyberuhista. Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. (Bodeau ym. 2011, 13–14; Laari ym. 2019, 9.)

3.2 Kybersietoisuus systeemisuunnittelun näkökulmasta

Kuten aikaisemmassa luvussa todettiin, kybersietoisuuden suunnittelu (Cyber Resilience Engineering) on operaatioturvallisuuden (Mission Assurance Engineering) osa, joka koostuu systeemin turvallisuussuunnittelusta (System Security Engineering, kuva 5). Systeemin turvallisuussuunnittelun tavoitteena on suojata ihmisiä ja omaisuutta kehittyneitä uhkia vastaan. (Bodeau ym. 2011, 9–10.) Systeemin turvallisuussuunnittelu perustuu systeemisuunnittelun periaatteisiin, joka muodostuu joukosta teknisiä ja toiminnallisia menetelmiä, joiden tarkoituksena on kuvata järjestelmän toimivuutta. Tällöin systeemisuunnittelun avulla järjestelmästä voidaan luoda konsepti, kehittää järjestelmän teknistä suunnittelua sekä ohjata ja valvoa järjestelmän testaus-, mittaus-, ja hyväksyntäprosesseja. (Kosola 2013, 3.)



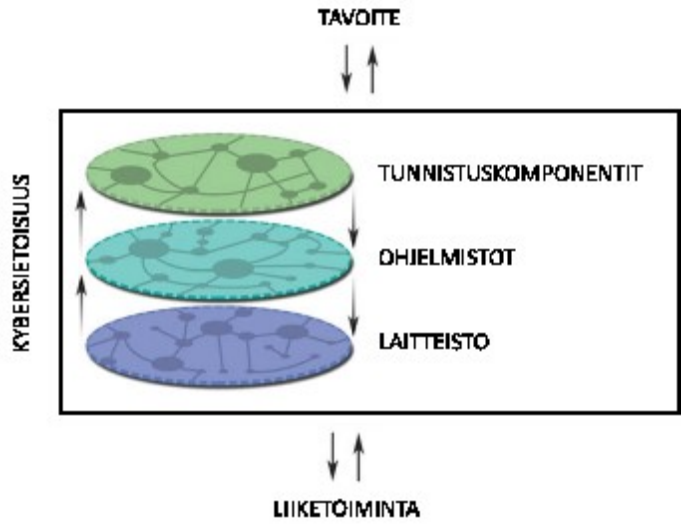
Kuva 5. Mitre-organisaation esitys kybersietoisuuden suunnittelusta (Bodeau ym. 2011, 9)

Systeemisuunnittelu on Puolustusvoimissa jo pitkään käytetty käsite ja toimintatapamalli, mutta systeemin turvallisuussuunnittelun näkökannalta keskiössä on tietoturvallisuus. Tietoturvallisuuden tarkoituksena on turvata tiedon luottamuksellisuus, eheys ja saatavuus, josta käytetään käsitettä tietoturvan CIA-malli (Confidentiality, Integrity, Availability). Luottamuksellisuudella tarkoitetaan sitä, että kukaan muu sivullinen ei saa tietoa käsiinsä ja eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Käytännössä tietoturvallisuudella tarkoitetaan esimerkiksi kulunvalvontaa, tilojen lukitusta, asiakirjojen turvallisena säilyttämisenä ja hävittämisenä, tietojen salaamisena ja varmuuskopiointina sekä palomuurien, virustorjuntaohjelmien ja varmenteiden käyttönä. (Bodeau ym. 2011, 10; Kosola 2013, 3; Laari ym. 2019, 15.)

Keskeinen käsitys CIA-mallista on ymmärtää, että yhden tai useamman periaatteen priorisointi voi tarkoittaa toisten kompromisseja. Esimerkiksi järjestelmä, joka vaatii suurta luottamuksellisuutta ja eheyttä, voi uhrata saatavuuden merkitystä. Tämä kompromissi ei ole välttämättä huono asia, kun tämä on tietoinen valinta. Meidän tulee yksinkertaisesti päättää, että kuinka näitä periaatteita sovelletaan järjestelmän vaatimuksia luotaessa. Loppujen lopuksi hyvin suunnitellun järjestelmän tarkoituksena on tarjota saumatonta ja turvallista käytettävyyttä. (Walkowski 2019.)

3.3 Kybersietoisuus ja järjestelmät

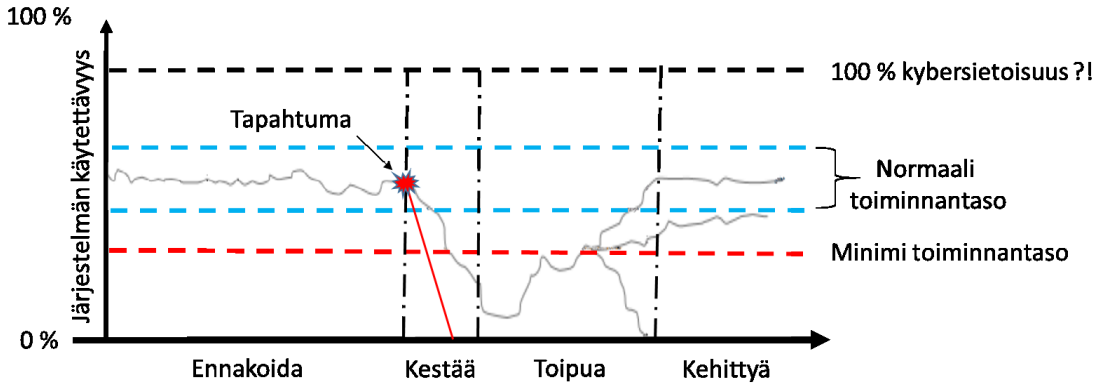
Kottin ja Linkovin (2019) mukaan kybersietoisuus on ja se tulee ajatella monimutkaisena kokonaisuutena, joka käsitteenä on hyvinkin laaja ja käsittää monia tieteenaloja. Kybersietoinen järjestelmä koostuu toisiinsa kytketyistä laitteistoista, ohjelmistoista ja tunnistuskomponenteista, joiden tarkoituksena on toimia synkronisesti yhdessä. Kybersietoisuuden tavoitteena (kuva 6) on kokonaisuutena varmistaa toiminnan jatkuvuus, vaikka järjestelmään on kybertoimintaympäristön kautta tapahtunut haitallista vaikuttamista. (Kott & Linkov 2019, 3.)



Kuva 6. Kybersietoisuuden tarkoitus mukailtuna (Kott & Linkov 2019, 3)

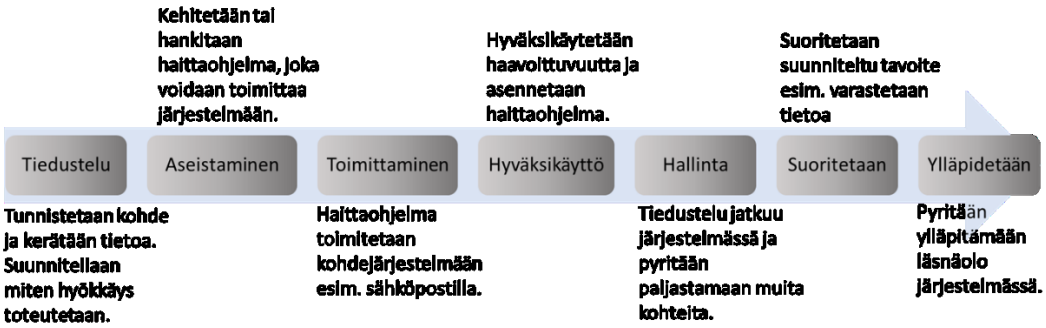
Tutkijan näkemyksenä on, että kybersietoisuuden määrittelyyn voidaan käyttää käsitettä käytettävyys (Usability), jonka Jyri Kosola (2007) määrittelee julkaisussaan Suorituskyvyn elinjaksohallinta: -- "*Käytettävyydellä kuvataan missä määrin järjestelmä kykenee täyttämään tehtävänsä. Operatiivinen käytettävyys kuvaa missä määrin järjestelmä on teknisesti toimiva ja kykenee täyttämään operatiivisen tehtävätarpeen vallitsevissa olosuhteissa*." (Kosola 2007, 404).

Järjestelmän käytettävyyttä voidaan tällöin käyttää, kun halutaan kuvata järjestelmän kybersietoisuutta (kuva 7). Kybersietoisen järjestelmän tarkoituksena on, että järjestelmä kykenee kestämään kyberhyökkäyksen ja voidaan palauttaa vähintään minimi toimintatasolle tai palauttaa kokonaan takaisin normaalille toiminnantasolle. Pahin mahdollinen skenaario palautumisessa on, että kyberhyökkäyksestä palautuminen ei onnistu ja järjestelmä joudutaan kokonaan sammuttamaan (punainen viiva kuvassa). Tällöin kyberhyökkääjät ovat saavuttaneet mahdollisen tavoitteensa ja estäneet järjestelmän käytettävyyden. Tästä voidaan johtaa ajatusmalli kybersietoisuuden suunnittelulle, että hyvin toteutettu järjestelmä on kybersietoinen ja takaa toimintavarmuuden vaikeissakin kyberolosuhteissa, vaikka kyberhyökkäys on heikentänyt järjestelmää. (Bodeau ym. 2017, 55; Kott & Linkov 2018, 6.)



Kuva 7. Kuvio perustuu Mitre-organisaation kybertappoketjun prosessiin (Cyber Kill Chain) ja Kottin ja Linkovin esittämään malliin, kun järjestelmä joutuu kyberhyökkäyksen kohteeksi (Bodeau ym. 2017, 56; Kott & Linkov, 2018, 6.)

Kuvassa seitsemän (7) esitetty malli perustuu Mitre-organisaation kybertappoketjun prosessiin (Cyber Kill Chain), jonka tarkoituksena on antaa kybersietoisuuden suunnittelulle uhkamallipohjainen lähestyminen. Kybertappoketju (kuva 8) perustuu Yhdysvaltojen armeijalle kehitettyyn F2T2EA-tähtäysdoktriiniin (Find, Fix, Track, Target, Engage, Assess), jota kyberhyökkääjät käyttävät mallina kybertoimintaympäristössä. Kybertappoketju on systemaattinen prosessi, jonka tarkoituksena on löytää kohde ja kohdistaa tähän haluttu vaikutus. Puolustautujan näkökannalta tämä merkitsee sitä, että pyritään tunnistamaan ja estämään mahdollisimman monta näistä vaiheista ja takaamaan paremmat mahdollisuudet selviytyä kyberhyökkäyksistä. (Hutchins ym. 2011, 4–5; Bodeau ym. 2017, 55.)



Kuva 8. Kybertappoketjun elinkaari mukailtuna (Bodeau ym. 2017, 55)

Kuten luvun alussa todetaan, että kybersietoisuus on osa erittäin suurta tieteenalaa ja kokonaisuutta. Järjestelmän käytettävyyden osana on myös ihminen, jotka käyttävät näitä järjestelmiä. TEPA-termipankki (2021) määrittelee järjestelmän seuraavasti: -- " *tietyllä tavalla toimiva yhtenäinen kokonaisuus,*

jonka osien väliset suhteet on määritelty". Tämän määritelmän mukaan voidaan ajatella, että ihminen ja kone muodostavat järjestelmäkokonaisuuden toiminnallaan. Lähtökohtaisesti ihminen on yleensä se heikon lenkki, joka aiheuttaa tiedostomattaan tai tiedostaen suurimman tietoturvariskin. Tällöin tarvitsemme jatkuvaa osaamisen kehittämistä, jonka tavoitteena on lisätä ihmisen ymmärrystä ja osaamista kybertoimintaympäristöstä ja turvallisuudesta.

4 HANKE PUOLUSTUSVOIMISSA

Tässä luvussa esitetään Puolustusvoimien hanke sekä käsitellään sotilaallisen suorituskyvyn käsitemallia, jonka näkökulmat voidaan rinnastaa kybersietoisuuden resilienssisuunnitteluun. Tässä luvussa esitetään Puolustusvoimien turvallisuustoiminta annetun normiohjauksen perusteella, jolla ohjataan hankkeessa huomioitavia turvallisuustekijöitä. Vaatimustenhallinta on yksi keskisin menetelmä, kun järjestelmää suunnitellaan, rakennetaan ja ylläpidetään. Vaatimustenhallinnan lähteinä käytettiin Jyri Kosolan vaatimustenhallinta opasta (2013) sekä Puolustusvoimien vaatimustenhallintaohjetta. Riskienhallinta kuuluu oleellisena osana hankkeeseen, jossa kybersietoisuuden riskienarviointi kohdistuu kybertoimintaympäristöön ja tätä kautta tuleviin riskeihin. Riskienhallinnan lähteinä käytettiin Mitre-organisaation tutkimusasiakirjoja sekä Puolustusvoimien ohjetta riskienarviointiin, joka pohjautuu kansainvälisiin standardeihin sekä kansallisiin ohjeistuksiin.

4.1 Hanke ja sotilaallinen suorituskyky

Puolustusvoimien hankkeet ja projektit toteutetaan kehittämisohjelmien kautta, joiden tarkoituksena on hankkia Puolustusvoimille sotilaallisesti suorituskykyinen joukko tai järjestelmä. Näiden kehitysohjelmien tarkoituksena on kehittää suorituskyvyn kaikkia osatekijöitä, kuten henkilöstöä, materiaalia, käyttö- ja toimintaperiaatteita sekä organisaatiota ja toiminnan tarvitsemaa informaatiota. Hanke jaetaan neljään yksittäiseen aikaan sidottuun elinjakson vaiheeseen: valmistelu, suunnittelu, toteutus ja päättäminen (kuva 9). Nämä hankkeen elinjakson vaiheet voidaan jakaa toteutettavaksi pienempinä projekteina. (Kosola 2012, 9; Puolustusvoimat 2017b, 26; Puolustusvoimat 2018a, 5.)

Kuva 9. Hankkeen elinkaari jaksottaisina vaiheina (Pääesikunta 2017b, 9)

Timo Tolkki (2020) määrittelee suorituskyvyn käsitteen opinnäytetyössään Hankkeiden turvallisuuden kehittäminen Puolustusvoimissa seuraavasti: -- "*Puolustusvoimien sotilaallisen suorituskyvyn käsitemallin mukaisesti suorituskyky on kyky suorittaa tietty toiminta tai saavuttaa tietty vaikutus. Tätä voidaan tarkastella neljästä näkökulmasta, joista yksi on ratkaisu.*" (Tolkki 2020, 13.)

Tolkki on käyttänyt lähteenään Puolustusvoimien ohjetta (HO46) Sotilaallisen suorituskyvyn käsitemalli, jossa määritetään sotilaallisen suorituskyvyn näkökulmat. Todettakoon, että Tolkilta puuttuu tarkempi selite suorituskyvyn käsitteelle. Suorituskyvyn selite avaa enemmän kontekstia suorituskyvyn määritteelle: -- "*Sotilaallisen suorituskyvyn käsitemallin tarkoitus on muodostaa yhtenäinen käsitteistö, jolla varmistetaan, että kaikki suorituskyvyn määrittämiseen ja kehittämiseen osallistuvat tahot käyttävät yhdenmukaisia termejä. Tämä mahdollistaa yhdenmukaiset menettelyt esimerkiksi strategisessa suunnittelussa sekä kehittämisohjelmien, hankkeiden ja hankintojen valmistelussa, toteuttamisessa ja ohjaamisessa sekä näihin liittyvässä vaatimustenhallinnassa.*" (Pääesikunta 2018a, 5-6.)

Sotilaallisen suorituskyvyn käsitemallia tarkastellaan neljästä näkökulmasta:

- Vaikuttavuus
- kyvykkyys
- ratkaisu
- elinjakso.

Vaikuttavuusnäkökulma on toteutusriippumatonta toimintaa ja sillä kuvataan käsitteellisellä tasolla, mitä vaikuttavuutta halutaan saada aikaan, kuten haluttua lopputulosta, tavoitetta tai päämäärää. Tällöin suorituskyvyn käyttö on riippuvaista toimintaympäristötekijöistä, jonka yhtenä käsitteenä on informaatiotekijät. Sotilaallisen suorituskyvyn käsitemallin ohjeen liitteessä A Vaikuttavuusnäkökulman käsitteet, informaatiotekijät määritellään seuraavasti: -- *"Informaatiotekijöitä ovat kansallinen tiedustelu, viestintä- ja tiedotusvälineet, eri toimijoiden ja sosiaaliryhmien tiedotustoimet sekä niiden vastaanottavuus,*

herkkyys ja haavoittuvuus viestiä; tietoverkkoihin, johtamisjärjestelmiin (CIS) sekä johtamiseen ja valvontaan (C2S) kohdistuvat tietoverkkohyökkäykset. (COPD)" (Pääesikunta 2018b, A-4.)

Kyvykkyysnäkökulma on myös toteutusriippumatonta ja kuvataan käsitteellisellä tasolla, esimerkiksi mitä kyvykkyyksiä vaikuttavuuden aikaansaamiseksi tarvitaan. Kyvykkyysnäkökulma ei ota kantaa ratkaisuun, kuten tekniseen ratkaisuun. Kyvykkyysnäkökulmat muodostuvat seitsemästä pääkyvykkyysalueesta, josta yksi on suojaus ja jonka alakyvykkyytenä on puolustus. Tämän alakäsitteen alakäsitteenä on kyberuhat, joka määrittelee kyvyn mitätöidä tai vähentää vihamielisen toiminnan vaikuttavuutta kyberuhkien osalta. Kyvykkyysalueet rakentuvat moniportaisesta hierarkiasta, jonka tarkoituksena on määrittää haluttu vaikutus kyvykkyytenä. Useimmiten vaikuttavuuden aikaansaamiseksi tarvitaan useita tai kaikkia kyvykkyyksiä. (Pääesikunta 2018a, 8.)

Ratkaisunäkökulmassa korostetaan käsitettä järjestelmä, joka määritellään seuraavalla tavalla: -- "*Toistensa kanssa vuorovaikutteisten osien yhdistelmä, joka on koottu yhtä tai useampaa asetettua tarkoitusta varten. Kokonainen järjestelmä sisältää kaikki tarpeelliset laitteet, ympäristöt, materiaalit, tietokoneohjelmistot, yrityskohtaisen räätälöinnin, teknisen dokumentaation, tarvittavat palvelut ja käyttöhenkilöstön. Järjestelmä on riittävä siihen toiminnan tasoon ja tarkoitukseen, jota sen käyttämisessä vaaditaan."* Ratkaisunäkökulma on toteutusriippuvainen, jota kuvataan kahdeksalla ratkaisunäkökulman osatekijällä (DOTMLPFI): doktriini, organisaatio, koulutus, materiaali, johtajuus, henkilöstö, infrastruktuuri ja yhteistoimintakyky. Näiden osatekijöiden välisellä suhteella ja yhdistelmillä muodostetaan tavoiteltavat kyvykkyydet ja vaikuttavuudet. (Pääesikunta 2018a, 9.)

Elinjaksonäkökulmalla kuvataan järjestelmän elinjaksoja, jonka määritelmänä kuvataan: -- "*Elinjakso kuvaa järjestelmän, tuotteen tai palvelun kehittymistä konseptista luopumiseen saakka*." Elinjaksonäkökulmalla pyritään esimerkiksi vastaamaan kysymykseen, milloin järjestelmä on käytettävissä. (Pääesikunta 2018a, 10.)

Järjestelmän kybersietoisuutta ei ole tarkoitus mieltää sotilaalliseksi suorituskyvyksi, mutta kybersietoisuuden resilienssisuunnittelun periaatteet vastaavat

hyvin sotilaallisen suorituskyvyn käsitemallin neljää näkökulmaa: vaikuttavuus, kyvykkyys, ratkaisu ja elinkaari. Tämän vuoksi on oleellista ymmärtää resilienssisuunnittelun periaatteet, jota käsiteltiin luvussa 3.1 Kybersietoisuuden suunnittelun viitekehys. Kuten luvussa 1.2 Aikaisempi tutkimus ja tärkeimmät lähteet todettiin, kybersietoisuus on vielä käsitteenä toistaiseksi vähän käytetty käsite ja termi. Ulkomaalaisessa tutkimuskirjallisuudessa kybersietoisuus on jo kauan käytetty käsite, jossa kybersietoisuudesta käytetään englanninkielisiä sanoja Cyber Resilience tai Cyber Resiliency. Puolustusvoimien määräyksessä Kybersietoisuuden varmistaminen järjestelmissä (2020) määritetään, että kybersietoisuudella (KYSI) tarkoitetaan: -- "*joukon ja järjestelmän kykynä sietää kybertoimintaympäristön kautta tulevia uhkia sekä tukea puolustusjärjestelmien operaatiovarmuus suorituskykyjen suunnittelussa, rakentamisessa ja käytön aikana*". (Pääesikunta 2020b, 4.) Yhdistämällä kybersietoisuuden resilienssisuunnittelun periaatteet sekä sotilaallisen suorituskyvyn periaatteet yhdeksi kokonaisuudeksi voidaan kehittää kybersietoinen järjestelmä, joka pystyy kestämään kybertoimintaympäristön kautta tulevia jatkuvia ja kehittyviä kyberuhkia vastaan.

4.2 Turvallisuustoiminta

Puolustusvoimien turvallisuusohje (2015) määrittelee turvallisuustoiminnan sekä turvallisuustoimialan johtamisen sekä tavoitetilan, jonka tarkoituksena on turvata Puolustusvoimien päätehtävien toteutus. Operatiivisten suorituskykyjen osalta turvallisuusohjeen tarkoitus on turvata Puolustusvoimien henkilöstöä, tietoja, materiaalia, teknistä infrastruktuuria sekä ympäristöä kaikilta tahallisilta ja tahattomilta uhilta kaikissa tilanteissa. Turvallisuusohjeen mukaan parasta turvallisuustoimintaa on ennaltaehkäisy, jossa riskienhallinta on työkaluna avainasemassa. (Pääesikunta 2015b, 5.)

Puolustusvoimien turvallisuusohjeessa (2015) määritetään Puolustusvoimien turvallisuustoimialat, jotka oleellisesti vaikuttavat hankkeessa toteutettavaan turvallisuuteen. Nämä turvallisuustoimialat jaetaan 15 eri toimialaan ja näistä alakohdista on luotava oma turvallisuussuunnitelmansa, jonka tarkoituksena kuvata miten turvallisuutta toteutetaan hankkeessa. (Pääesikunta 2015b, 5; Pääesikunta 2017a, 16.)

Puolustusvoimien hankeohjeen (2017) mukaan hanketurvallisuus toimialoineen listattuna:

- Työ- ja palvelusturvallisuustoiminta
- turvallisuusvalvonta ja sotilaspoliisitoiminta
- tilaturvallisuus
- pelastustoimi
- tietoturvallisuus
- tekninen tietoturvallisuus
- sidosryhmäturvallisuus
- henkilöstön turvallisuushallinto ja lupahallinto
- räjähdeturvallisuus
- kemikaaliturvallisuus
- sähköturvallisuus
- ympäristöturvallisuus
- kuljetusten turvallisuus ja liikenneturvallisuus
- sotilasilmailun lentoturvallisuus
- sotilasmerenkulun turvallisuus.

4.3 Vaatimustenhallinta

Vaatimustenhallinta on yksi keskeisin menetelmä, kun järjestelmää suunnitellaan, rakennetaan ja ylläpidetään. Vaatimustenhallinta on yleisluonteinen työkalu, jolla voidaan analysoida järjestelmän sille asetetut perusteet, mittarin mitata todellista tasoa sekä kehittää järjestelmää koko elinkaarensa aikana. Vaatimustenhallinta on systemaattista työskentelyä, jonka tarkoituksena on kustannustehokkaasti mahdollistaa järjestelmän tarpeet ja tavoitteet, luoda yhtenäinen näkemys ja ymmärretään mitä ollaan oikeasti tekemässä. (Pääesikunta 2017b, 4.)

Jyri Kosola ihmettelee Vaatimustenhallinta oppaassaan: --"*Miksi vaatimusten laadintaa ei aina hallita systemaattisesti. Vastaus tähän on yksinkertainen: vaatimusten laadinta on vaativaa ja työlästä"*. Tätä vastausta voidaan tulkita hankkeen onnistumisen kannalta, että hankkeeseen osallistuvien on tunnettava kriittiset vaatimukset ja nämä ovat asetettu oikein. Vaatimustenhallinta on erinomainen työkalu juuri kybersietoisuuden suunnittelun käyttöön, kun halutaan saavuttaa järjestelmälle haluttu toimintataso. Vaatimuskriteerien luominen, merkitys ja asettaminen vaativat kybersietoisuuden kannalta ensisijaisesti osaamista sekä asian ymmärtämistä. Ymmärtääkseen vaatimustenhallinnan perusteita on osattava ja ymmärrettävä vaatimuskriteerien luokittelu ja näiden perustelu, joten näiden kriteerien mallina voidaan käyttää Jyri Kosolan

Vaatimustenhallintaoppaassa (2013) käyttämää kolmiportaista mallia. Malli voidaan luoda seuraavasti: 1. ehdottomat tai kriittiset 2. tärkeät tai ensisijaiset 3. tarpeelliset tai toissijaiset. Useampiportaisempaa mallia hän ei suosittele, koska malli lisää virheen mahdollisuutta. (Kosola 2013, 5, 15–16.)

Hankkeen elinkaaren näkökulmasta vaatimustenhallinnan kriittisyys on konsepti-, suunnittelu- ja rakentamisvaiheissa. Kybersietoisuuden näkökannalta edellä mainitut vaiheet ovat kriittisiä, kun kybersietoisuutta suunnitellaan ja toteutetaan. Vaatimuskriteerit toimivat niin sanottuina mittareina, kun siirrytään hankkeen elinjakson vaiheesta seuraavaan ja käyttää näitä kriteereitä seuraavan vaiheen suunnittelun perustana. Huomioitavana yksityiskohtana vaatimuskriteereitä luotaessa Kosola pitää, että yksittäisillä vaatimuksilla ei voi muodostaa toimivaa ratkaisua. (Kosola 2013, 4–5.)

4.4 Riskienhallinta

Sanalle riski voi olla monenlaista määritelmää ja tarkoitusta, joka riippuu käsitteen esittäjästä tai asiayhteydestä. Valtionvarainministeriön julkaisussa 22/2017 liitteessä 1 määritellään, että riskillä tarkoitetaan: -- "*Epävarmuuden vaikutus tavoitteisiin. Vaikutus on poikkeama odotetusta. Vaikutus voi olla myönteinen tai kielteinen suhteessa odotusarvoon. Riski kuvataan useimmiten viittaamalla tapahtumaan ja/tai seurauksiin ja ilmaistaan todennäköisyyden ja vaikutuksen yhdistelmänä."* (Rousku 201, 1). Yleisemmin riskillä tarkoitetaan vaaraa tai uhkaa, jonka todennäköisyyttä pyritään välttämään. Riskin todennäköisyyttä voidaan arvioida matemaattisin menetelmin, joka esitetään kaavalla: Riski (riskiluku) = Todennäköisyys x riskin vaikutus. (Lagerblom 2014, 16.)

Kuten Valtionvarainministeriön julkaisussa todetaan, riski voidaan mieltää myös positiivisessa mielessä, kun riski koetaan pienenä. Riskejä käsitellään yleensä tapahtumien kautta, joiden todennäköisyyttä ja vaikutusta pyritään arvioimaan. Oli riski huomioitu tai jätetty huomioimatta, voidaan myös tämä kokea riskinä. Se mikä ei ole nyt huomioitu riskienarvioinnissa, ei ole myöhemminkään mukana. (Ilvo 2018, 10.)

Puolustusvoimien riskienhallinta perustuu Suomen lainsäädäntöön, normeihin, kansalliseen ja kansainväliseen riskienhallinnan ohjeistukseen. Valtionvarainministeriön julkaisun 22/2017 liite 1 määritee riskienhallinnan seuraavasti: -- "*Koordinoitu toiminta, jolla johdetaan ja ohjataan, hallitaan organisaation riskejä*" (Rousku 2017, 1). Puolustusvoimat määrittelee ohjeessaan Sisäinen valvonta ja riskienhallinta (2021) että, riskienhallinta on osa Puolustusvoimien jokapäiväistä rutiinia ja ajattelutapaa. Riskienhallinnan tavoitteena on turvata Puolustusvoimien lakisääteisten tehtävien edellyttämän toiminnan jatkuvuus sekä varmistaa, että toiminnan lain- ja vaatimustenmukaisuuden tavoitteet täyttyvät. Puolustusvoimien toiminnalle asetetut tavoitteet ovat turvallisuus, laatu, maine ja hyvä hallinto. (Pääesikunta 2021a,12.)

4.5 Riskienhallinnan standardeista

Suomen standardisoimisliiton (2022) mukaan standardien käytön tarkoituksena on parantaa ja helpottaa ihmisten arkea. Tuotteiden ja palveluiden osalta standardien tarkoituksena on lisätä näiden turvallisuutta, laatua sekä yhteensopivuutta. Standardit ovat julkisia julkaisuja, joihin on kirjattu yhteisesti sovittuja vaatimuksia, suosituksia ja ominaisuuksia tuotteille, palveluille sekä järjestelmille. (Suomen standardisoimisliitto 2022.)

”Standardi”-sanaa käytetään yleisesti puhekielessä. Standardi voi esimerkiksi tarkoittaa, että hotellissa on standardihuoneet tai saamasi palvelu ei miellytä sinun laatustandardeja. Puolustusvoimissa standardeja käytetään jatkuvasti, jolla pyritään kustannustehokkuuteen ja yhtenäisten toimintatapojen mahdollistamiseen. Standardit ovat toisin sanoen yleiseen ja toistuvaan käyttöön tarkoitettuja, tunnetun tahon julkaisemia asiakirjoja, joiden käyttöä voidaan erikseen vaatia käytettävän. (Puolustusvoimat 2022; Suomen standardisoimisliitto 2022.)

Puolustusvoimien riskienhallinta perustuu SFS-ISO 31000:2018 -standardiin, josta on tehty ohje riskienarviointiin prosessina (Pääesikunta 2021b, 12). Riskienarviointi ohje (2021) perustuu SFS-ISO 31010:2019 -standardiin, joka tarjoaa useita ohjeita, miten valita, soveltaa ja käyttää erilaisia riskien tunnistamismenetelmiä. Standardin lähtökohtana on käytetty tekniikkaan pohjautuvia

menetelmiä, joita voidaan edelleen kehittää sopimaan käytettäväksi erilaisissa tilanteissa ja toimintaympäristöissä. (SFS-ISO 31010:2019, 6.)

Kansainvälinen ISO/IEC 27032:2012 -standardin tarkoitus on antaa ohjeita kyberturvallisuuden ja tietoturvallisuuden välisestä suhteesta sekä miten ratkaista kyberturvallisuuteen liittyviä ongelmia. Standardin ISO/IEC 27032 (2012) mukaan standardeja ISO-31000 ja ISO/IEC 27005 voidaan käyttää, kun pyritään toteuttamaan standardin ISO/IEC 27001 mukaisia tietoturvallisuuden hallintajärjestelmiä koskevia vaatimuksia. (ISO/IEC 27032:2012, 22.)

Standardissa ISO/IEC 27001 (2017) esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Tietoturvallisuuden hallintajärjestelmän tarkoitus on suojata tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskienhallintaprosessin avulla sekä vahvistaa sidosryhmien luottamusta siihen, että riskejä hallitaan asianmukaisesti. (SFS-EN ISO/IEC 27001:2017, 5)

SFS-ISO 31000 -standardin (2018) tarkoitus on antaa perusteita ja yleisiä ohjeita riskienhallintaan sekä hallitsemaan riskejä (SFS-ISO 31000:2018, 5). SFS-ISO/IEC 27005:2018 -standardissa esitetään ohjeistusta tietoturvariskien hallintaan organisaatioissa, mutta ei kuitenkaan esitetä mitään tiettyä tietoturvariskien hallinnan menetelmää (SFS-ISO/IEC 27005:2018, 5). Kaikkien näiden standardien yhdistävänä tekijänä on, että kukin organisaatio muokkaa, kehittää ja määrittelee itse riskienhallintaan liittyvät tehokkaan toimintamallinsa kybertoimintaympäristössä.

4.6 Riskienhallinta hankkeessa

Riskienhallinta sisältyy Puolustusvoimien prosesseihin sekä hankkeisiin, projektitoimintaan ja kaikkiin merkittäviin muutoksiin, esimerkiksi organisaatio- ja prosessimuutoksiin. Hyvänä riskienhallintatapana pidetään, että tämä on aktiivista ja säännöllisesti suoritettavaa toimintaa. Riskienhallinnalla vastataan toimintaympäristössä tapahtuviin muutoksiin sekä edistetään Puolustusvoimien asemaa Suomen kansalaisten luottamusta nauttivana organisaationa ja työnantajana. Riskit ovat jatkuvasti muuttuvia tai niiden tärkeys voi ajansaatossa

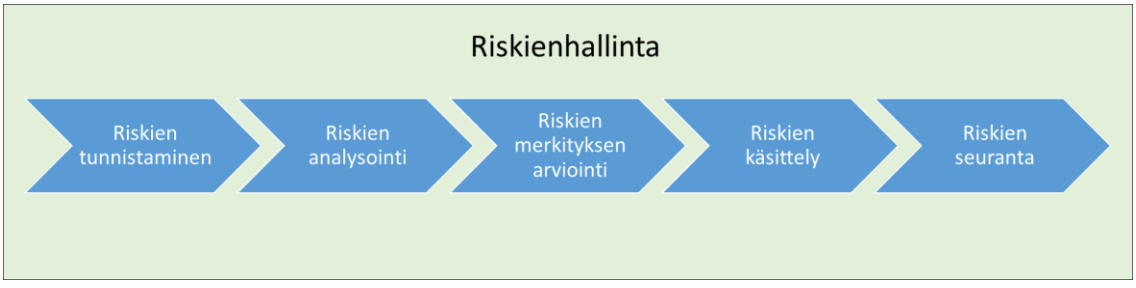
muuttua, tällöin riskienarviointi pitää tehdä uudelleen. Riskienhallinnan perimmäisenä tarkoituksena on estää negatiivinen vaikutus Puolustusvoimien maineeseen. (Pääesikunta 2021a, 5; Pääesikunta 2021b, 12–14.)

Kuten luvun alussa todettiin, että riskienhallinta kuuluu oleellisena osana Puolustusvoimien hankkeeseen. Hankkeen riskienhallinnan toteutuksen näkökannalta on, että hanke havaitsee ja kuvaa riskit, jotka ovat seuraamuksiltaan huomattavia ja varautuu niin niiltä osin mihin pystyy. (Pääesikunta 2017a, 14.)

Hankkeessa riskienhallinta jakautuu riskien tunnistamiseen, arviointiin, käsittelyyn ja ohjaukseen. Riskien tunnistamisen tavoitteena on määrittää mahdollisesti riskejä aiheuttavat tapahtumat ja niiden ominaisuudet, jotka riskin toteutuessa voivat vaikuttaa myönteisesti tai kielteisesti hankkeen tavoitteisiin. Riskien arvioinnin tarkoitus on mitata riskejä ja asettaa ne merkittävyysjärjestykseen jatkotoimenpiteitä varten. Riskien käsittelyn tarkoitus on kehittää vaihtoehtoja ja määrittää toimenpiteet, joilla parannetaan mahdollisuuksia ja vähennetään hankkeen tavoitteisiin liittyviä uhkia. Riskin ohjauksen tarkoitus on rajata hankkeelle koituvien häiriöiden määrä mahdollisimman vähäiseksi seuraamalla, suoritetaanko riskejä koskevia toimenpiteitä ja onko niillä haluttu vaikutus. (Pääesikunta 2017a, 14.)

4.7 Kybersietoisuuden huomioiminen riskienarvioinnissa

Riskien arviointiprosessia kuvataan Puolustusvoimien riskienhallintaohjeiden mukaan yksittäisinä vaiheina, jota voidaan käyttää riskienhallinnan tukena (kuva 10).



Kuva 10. Riskienhallinnan prosessi (Pääesikunta 2021b,1)

Kuvassa 10 esitetään Puolustusvoimissa yleisesti käytetty riskienarviointiprosessin malli, joka pitää sisältää seuraavat vaiheet (Pääesikunta 2021b,1):

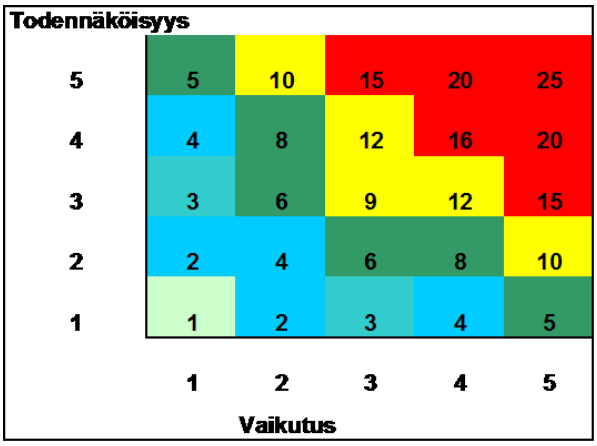
- Tunnistaminen
- analysointi
- arviointi
- käsittely
- seuranta.

Riskien tunnistamisen tavoitteena on havaita ja kuvata kaikki merkittävät riskit ja mahdollisuudet, riskilähteet, vaikutusalueet, tapahtumat, mukaan lukien olosuhteiden muutokset ja näiden syitä sekä mahdollisia seurauksia. Riskien tunnistamisessa merkittävänä osana on tunnistaa osaaminen riskienhallintaan sekä ulkopuolisten tekijöiden mahdollinen vaikutus riskeihin. (Valtionvarainministeriö 2017, 21.)

Riskien tunnistamisen kybersietoisuuden näkökannalta on ymmärtää riskien vaikutus ja kybertoimintaympäristö, jossa järjestelmä tulee toimimaan tai jo toimii. Kybersietoisuuden riskien tunnistamiseen ja määrittelemiseen voidaan käyttää oletusta, että kysymme itseltämme "miten kyberhyökkääjä käyttäisi järjestelmän ominaisuuksia saavuttaakseen jalansijan järjestelmässä?" sekä "mitä kyberhyökkääjä saavuttaa tällä hyökkäyksellä?" Vastaamalla näihin kysymyksiin pystymme luomaan listauksen riskeistä ja tunnistaa riskit, jotka ovat avainasemassa. Riski, jota ei ole tunnistettu tässä vaiheessa, ei myöskään ole myöhemminkään mukana. (Bodeau ym. 2017, 5, 8; Pääesikunta 2021b, 1.)

Riskien analysoinnin tarkoitus on antaa perusteet, kuinka analysoidaan riskien syitä, lähteitä, seuraamuksia ja seuraamuksien todennäköisyyttä. Riskien analysoiminen voi olla yllättävän vaikeata muodostaa selvää kuvaa, koska riskin todennäköisyyttä voi olla vaikeata muodostaa. Riskin todennäköisyyttä arvioidaan yleensä tapahtuman luonteen mukaan, joka luokitellaan riskin toistuvuuden tai kertaluonteisuuden mukaan. Tällöin riskianalyysin yksityiskohtaisuus tulee riippumaan riskistä ja analyysin tarkoituksesta sekä saatavilla olevasta tiedosta. Kuten aikaisemmin olemme todenneet, kybertoimintaympäristö on jatkuvassa muutoksessa ja selkeän kuvan muodostaminen voi olla todella haasteellista. Tällöin voimme muodostaa kysymyksen, "miten voimme luokitella riskien todennäköisyydet ja vaikuttavuudet kybertoimintaympäristössä?". (Valtionvarainministeriö 2017, 22; Pääesikunta 2021b, 2.)

Riskien merkityksen arvioinnin tarkoitus on auttaa tekemään päätöksiä riskianalyysin tulosten perusteella siitä, että mitä riskejä on tarpeen käsitellä ja mikä on niiden käsittelyn toteuttamisen tärkeysjärjestys. Riskien merkityksen arviointi tehdään yleisesti antamalla riskin todennäköisyydelle ja vaikutukselle numeerinen arvo, josta muodostetaan riskiluku (kuva 11). (Pääesikunta 2021b, 3–4)



Kuva 11. Kuvassa esitetään riskimatriisi, jota käytetään Puolustusvoimien riskien merkityksen arvioinnissa (Pääesikunta 2021b, 3)

Riskiluvun muodostamisen tarkoituksena on kertoa, että pitääkö riskiluvun pienentämiseksi tehdä toimenpiteitä (kuva 12). (Pääesikunta 2021b, 3–4.)

Riskin suuruus	Tarvittavat toimenpiteet riksin pienentämiseksi
Merkityksetön riski (Riskiluku 1)	Riski on niin pieni, että toimenpiteitä ei tarvita.
Vähäinen riski (Riskiluku 2-4)	Toimenpiteitä ei välttämättä tarvita. Tilannetta tulee seurata, jotta riski pysyy hallinnassa
Kohtalainen riski (Riskiluku 5-8)	On ryhdyttävä toimenpiteisiin riskin pienentämiseksi. Toimenpiteet tulee mitoittaa ja aikatauluttaa järkevästi. Jos riskiin liittyy erittäin vakavia seurauksia, on tarpeen selvittää tapahtuman todennäköisyys tarkemmin.
Merkittävä riski (Riskiluku 9-14)	Riskin pienentäminen on välttämätöntä. Toimenpiteet tulee aloittaa nopeasti. Riskialtis toiminta pitää saada loppumaan nopeasti eikä sitä saa aloittaa ennen kuin riskiä on pienennetty.
Sietämätön riski (Riskiluku 15-)	Riskin poistaminen on välttämätöntä. Toimenpiteet tulee aloittaa välittömästi. Riskialtis toiminta tulee keskeyttää eikä sitä saa aloittaa ennen kuin riski on poistettu.

Kuva 12. Kuvassa esitetään, että millaisilla toimenpiteillä Puolustusvoimissa riskejä pienennetään (Pääesikunta 2021b, 4)

Riskiluvun pienentämiseksi toimenpiteet voivat olla lisäanalyysin tekeminen tai lopputuloksena voi olla, että päätetään olla käsittelemättä riskiä millään muilla tavoin kuin ylläpitämällä jo olemassa olevin hallintakeinoin. (Pääesikunta 2021b, 3–4.)

Riskien käsittely on yhden tai useamman riskienkäsittelytoimenpiteen valitsemista ja toteuttamista, joista Puolustusvoimien riskienhallintaohjeen mukaan noudatetaan seuraavia yleisiä periaatteita (Pääesikunta 2021b, 5):

- Ensisijaisesti estetään uhkatekijän syntyminen tai poistetaan syntynyt uhkatekijä muuttamalla toimintaa.
- Jos tämä ei ole mahdollista, pienennetään riskiä. Tämä tapahtuu useimmiten pienentämällä uhan toteutumisen todennäköisyyttä ja pyritään vaikuttamaan seurausten vakavuuteen. Parhaiten riskejä voidaan pienentää valvomalla, sopimalla, ohjeistamalla ja kouluttamalla riskien pienennyskeinoja.
- Jos riskin pienentäminen ei ole mahdollista, pyritään parantamaan kykyä sietää sen laukeamisesta aiheutuvia vaikutuksia.
- Jäljelle jäävän niin sanottu jäännösriskin hyväksyminen on toimenpide, joka edellyttää tietoista päätöstä.

Kybersietoisuuden näkökannalta riskien käsittely on juuri ennakointia, joka on osa resilienssisuunnittelun tavoitteita. Riskien käsittelyn hyötynä on, että pyritään lähtökohtaisesti pienentämään kyberhyökkäyksen vaikutuksen vakavuutta vähentämällä hyökkäyksen intensiteettiä, laajuutta ja kestoa. (Graubart 2016, 9.)

Riskien seurannan tarkoituksena on katselmoinnin avulla varmistaa riskienhallintakeinojen tehokkuutta ja vaikuttavuutta. Riskejä käsitellään Puolustusvoimien johtamisen foorumeissa, kuten hanke-, projekti-, ja harjoituskokouksissa. Näissä kokouksissa käsitellään riskien kehittymistä sekä riskienhallinnan toimenpiteitä, jotka dokumentoidaan kokouspöytäkirjoihin ja harjoitusasiakirjoihin. Kokouksen esittäjän vastuulla on kirjata sekä koostaa tarvittavat selvitykset ja lausunnot riskeistä, jonka jälkeen laatii ratkaisuesityksen päätettäväksi. Kokouksen esittäjän vastuulla on myös kirjata ratkaisu kokouspöytäkirjoihin. (Pääesikunta 2021b, 6.)

Kybersietoisuuden näkökulmasta riskien seurannalla tarkoitetaan enemmänkin järjestelmän teknisiä ominaisuuksia, joita voidaan arvioida riskienhallintakeinojen avulla. Näitä järjestelmän teknisiä ominaisuuksia voidaan arvioida

esimerkiksi hankkeessa vaatimustenhallinnan kautta sekä käyttö ja ylläpitovaiheessa, kun järjestelmään tehdään päivityksiä tai muutoksia. Nämä ovat hyvin yleisluontoisia ja laajoja asiakokonaisuuksia, mutta kulminoituvat kybersietoisuuden tehokkuuden seurantaan, jonka perimmäisenä tarkoituksena on varmistaa ja maksimoida järjestelmän toiminnan jatkuvuus.

Kybertoimintaympäristö on jatkuvassa muutoksessa, joten tunnetut riskienhallinnan mallit ja menetelmät eivät aina ole suoraan sopivia riskienarviointiin. Tätä voidaan esimerkiksi tarkastella liiketoiminnan kautta, jossa riskienarviointimenetelmät pohjautuvat rahallisen omaisuuden yksityiskohtaiseen ja tarkkaan määritykseen. Lähtökohtana tälle perinteiselle riskienarvioinnille on, että rahalliset tappiot minimoidaan tai kokonaisuudessaan vältetään. Tämän vuoksi on oleellista, että riskienhallintaa ja riskienarviointia kehitetään organisaation käyttöön sopivaksi. Kehittääksemme riskienarviointi prosessia kybersietoisuuden näkökulmasta on oleellista määritellä, onko järjestelmä osa kybertoimintaympäristöä. Tällöin järjestelmän kybersietoisuuden riskienarviointi kohdistuu kybertoimintaympäristöön ja tätä kautta tuleviin riskeihin. Oleellisinta on tehdä selkeät rajaukset kybersietoisuudesta, jonka tarkoituksena on kartoittaa, mikä kuuluu riskienarviointiin ja mikä jää tämän ulkopuolelle sekä tunnistaa merkittävät riippuvuudet järjestelmien välillä. (Bodeau ym. 2017, 8; SFS-ISO 31010: 2019, 11; ISO-IEC 27032, 22–23.)

5 KYBERSIETOISUUDEN KÄYTÄNTEET

Tässä luvussa kuvataan käytännön näkökohtia kybersietoisuuden soveltamisesta järjestelmän elinkaaressa, joka pohjautuu National Institute of Standards and Technology vuonna 2021 julkaisemaan Developing Cyber Resilient Systems: A Systems Security Engineering Approach -tutkimusasiakirjaan, Puolustusvoimien normiohjeeseen ja opinnäytetyön haastatteluaineistoon. On kuitenkin korostettava, että NIST-instituutin tutkimusasiakirjan mukaan kybersietoisuus ei edellytä mitään erityistä elinkaarta tai järjestelmän kehittämisprosessia. Tällöin kybersietoisuuden arviointi voidaan suorittaa missä tahansa vaiheessa ja iteratiivisesti koko järjestelmän elinkaaren ajan. (Ross ym. 2021, 5.)

5.1 Tutkimuksen toteutus

Haastattelut toteutettiin verkkohaastatteluna marraskuussa 2021 hyödyntäen Skypeä sekä Webropol-kyselyä. Haastatteluiden toteuttaminen COVID-19-pandemian aikana johti siihen, että henkilökohtaisia tapaamisia (face-to-face) pyrittiin välttämään. Teemahaastattelun runko (liite 3) muodostettiin opinnäytetyön tekijän induktiivisesta päättelystä, jonka teoreettisena pohjana toimi tutkimusasiakirjat, alan kirjallisuus sekä Puolustusvoimien normit ja ohjeet. Haastateltavat henkilöt muodostuivat hankkeiden johtoon kuuluvista esimiehistä, projektipäälliköistä sekä asiantuntijoista, joilla on kokemusta hankkeista ja projekteista. Haastatteluun valitulle henkilöille lähetettiin ensimmäiseksi kutsu haastatteluun sähköpostilla (liite 1), jonka jälkeen heille soitettiin haastatteluajan sopimista varten. Ensimmäisten haastatteluiden aikana haasteltavat ohjasivat ottamaan yhteyttä tiettyihin henkilöihin, koska heillä saattaa olla parempi ymmärrys kybersietoisuuden käytännön toteuttamisesta hankkeessa. Henkilömäärä täten laajeni hieman alkuperäisestä suunnitelmasta, mutta tutkittavan ilmiön kannalta saatiin paremmin vastauksia. Haastattelupyyntöjä lähetettiin yhteensä 20 kappaletta, joista kahdeksan (8) nauhoitettiin ja viisi (5) vastasi Webropol-kyselyyn. Haastattelut kestivät noin 45 minuuttia, jonka aikana haastattelija teki omia muistiinpanojaan.

5.2 Tutkimusaineiston keruumenetelmät

Puolistrukturoidun teemahaastattelun avulla pyrittiin ymmärtämään paremmin opinnäytetyön kohteena olevaa ilmiötä, jossa selvitettiin haasteltavien ymmärrystä sekä toiminnan suhdetta kybersietoisuuteen. (Kananen 2017, 90.)

Tutkittavana ilmiönä ja käsitteenä oli kybersietoisuus, koska opinnäytetyön tavoitteena oli selvittää Puolustusvoimien hankkeen elinjaksojen hallintaprosessin toiminta ja tuottaa uutta, luotettavaa tietoa kehittämään kybersietoisuuden huomioimista hankkeen toiminnassa.

Haastatteluiden tarkoituksena oli keskittyä tiettyihin teemoihin, joista keskusteltiin avoimesti ja joita tarkennettiin muutamalla täydentävällä kysymyksellä. Teemahaastattelun etuna oli tämän monipuolisuus, koska haastattelumenetelmää ei sidottu tiettyyn formaattiin. Teemahaastattelu ei myös ota kantaa siihen montako kertaa haastatteluita tehdään, koska keskustelu etenee tiettyjen

keskeisten teemojen varassa. (Hirsjärvi & Hurme 2017, 48.) Kysymyksien teemat muodostuivat opinnäytetyön teoriapohjasta ja täydentävät kysymykset muodostuivat haastattelun aikana. Näin varmistettiin, että teemat olivat kaikille haasteltaville samat. Teemat olivat kybersietoisuuden ymmärtäminen määritelmänä, kybersietoisuuden merkitys normiohjauksen perusteella ja kybersietoisuuden kehittäminen hankkeessa.

Teemahaastattelu opinnäytetyön tutkimustiedon keruumenetelmänä oli erittäin toimiva toteutusmenetelmä, koska teemahaastattelut voitiin tallentaa ja näihin tallennuksiin voitiin myöhemmin palata. Tallenteiden hyötynä oli, että haastateltavien kertomuksia pystyttiin paremmin vertaamaan haastattelun aikana tehtyihin muistiinpanoihin. Vaihtoehtoisena vastausmahdollisuutena käytettiin Webropol-kyselyä, koska osa haastateltavista pyysi lähettämään kysymykset vaihtoehtoisesti kirjallisena. Vaihtoehtona olisi voitu käyttää sähköpostikyselyä, mutta tutkija halusi testata Webropol-kyselyn toimivuutta vapaamuotoisina vastauksina. Webropol-kysely toimi hyvin sähköpostikyselyn omaisesti, jossa vastaajat saivat kirjoittaa omia näkemyksiään tutkittavasta ilmiöstä ilman, että heidän kanssaan olisi sovittu erillistä aikaa osallistua haastateltavaksi.

5.3 Kerätyn aineiston analysointi

Kerätyn aineiston sisältöanalyysinä käytettiin induktiivista sekä abduktiivista päättelyä, jossa induktiivisessa päättelyssä keskeisenä oli teoria-aineiston läheisyys. Abduktiivinen päättely tarkoittaa, että tutkijalla on jonkinlainen teoreettinen johtoidea tutkittavasta ilmiöstä, jonka tutkija pyrki todentamaan aineistonsa avulla. (Hirsjärvi & Hurme 2017, 136.) Näkemys abduktiivisesta päättelystä muodostui opinnäytetyötä tehdessä, joka piti sisällään osallistumisen Puolustusvoimien kybersietoisuus hankkeissa opetustilaisuuteen ensin opiskelijana ja seuraavilla kursseilla luennoitsijana. Itse haastatteluiden teemat ja analyysi muodostuivat niin sanottuna jatkumona opinnäytetyön teoriaosuudesta, opetustilaisuuden aineistoista ja luennoista, joten näistä voitiin muodostaa oma näkemys ja tulkinta kybersietoisuudesta hankkeen elinkaaressa.

Analyysi tehtiin merkityksen tiivistämisenä ja tulkintana, jossa tiivistämisen tarkoituksena oli huomioida haastateltavien ja kyselyyn osallistuneiden henkilöiden näkemyksiä lyhyesti. Tulkitseminen on usein kvalitatiivissa analyyseissa läsnä, mutta ei pohjautunut niin sanottuun "näkyvissä" olevaan tarkasteluun, vaan pyrittiin löytämään piirteitä, jotka eivät ole suoranaisesti tekstissä näkyvissä. (Hirsjärvi & Hurme 2017, 137.) Tulkinta näille haastatteluille muodostui tutkijan näkökulmasta, jonka pyrkimyksenä oli laajentaa haastatteluiden ja kyselyn sisältöä. Tulkinnat pohjautuivat tutkijan näkemyksiin, jotka pohjautuvat opinnäytetyön teoreettiseen lähdeaineistoon, kuten Puolustusvoimien ohjeisiin ja normeihin, ulkomaalaisiin tutkimusasiakirjoihin, kansainvälisiin ja kansallisiin säädöksiin sekä standardeihin. Kuitenkin Puolustusvoimien ohjeet ja normit ovat määräämiä, joita tulee noudattaa, joten "liikkumavaraa" jäi todella vähän sovellettavaksi.

Haastattelu- ja kyselyaineiston käsittelyssä on valittavana kaksi tapaa, jotka ovat puhtaaksi kirjoittaminen sanasta sanaan tai aineistoa ei kirjoiteta tekstiksi, vaan päätelmät tehdään suoraan tallennetusta materiaalista. (Hirsjärvi & Hurme 2017, 138, 141.) Tallennettuna materiaalina pääosassa olivat haastattelun aikana tehdyt muistiinpanot, joista pyrittiin poimimaan avainsanoja käytännön toteutustavoista. Avainsanat pohjautuivat opinnäytetyön teoriaosuudesta, jotka olivat kybersietoisuuden ymmärtäminen, riskienhallinta, käytettävyys, vaatimusten määrittely, jatkuvuudenhallinta ja kybersietoisuuden kehittäminen hankkeen elinkaaressa. Lainaukset Puolustusvoimien normeista ja ohjeista, haastatteluista ja kyselyistä tehtiin suoraan teemahaastattelun aineiston pohjalta, joten tarkalle litteroinnille ei koettu syytä.

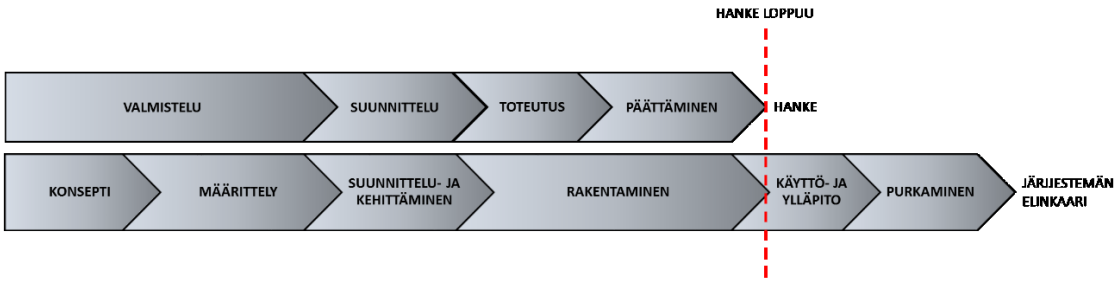
5.4 Kybersietoisuus osana järjestelmän elinkaarta

Kaikilla järjestelmillä on elinkaarensa, jota yleisesti kuvataan toiminnallisella mallilla (kuva 13). Järjestelmän elinkaarihallintaprosessin tarkoituksena on määritellä, ylläpitää sekä varmistaa, että elinkaarta koskevat menettelyt ja toimintatavat ovat yhdenmukaisia (Suomen Standardisointiliitto 2020).

Kuva 13. Järjestelmän elinkaari kuvattuna (Pääesikunta 2014, 3)

Toiminnallisessa mallissa järjestelmän elinkaari on jaettu vaiheisiin, jolla kuvataan toimintaa ja tarkoituksena on luoda yhtenäinen kuva siitä, mitä ja missä vaiheessa sekä millaisella aikataululla järjestelmän elinkaarta johdetaan alusta lopetukseen. (Pääesikunta 2014, 3.)

National Institute of Standards and Technology -tutkimusasiakirjassa (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach järjestelmän elinkaarta kuvataan konseptilla, kehittämisellä, rakentamisella, käytöllä, ylläpidolla ja purkamisella. NIST-instituutin järjestelmän elinkaari eroaa Puolustusvoimien järjestelmän elinkaarimallista siinä määrin, että määrittelyvaiheen lopussa hanke vasta asetetaan. Lisäksi Puolustusvoimien mallissa (kuva 14) käyttö- ja ylläpitovaihe on yhdistetty samaksi. (Ross ym. 2021, 17; Pääesikunta 2020a, 11.)



Kuva 14. Hankkeen vaiheiden sijoittuminen suhteessa järjestelmän eri elinvaiheisiin (Pääesikunta 2017a, 9)

5.4.1 Konsepti

Puolustusvoimien joukon ja järjestelmän elinjaksohallintaohjeessa (HQ496) konseptivaihe kuvaillaan seuraavasti: -- *"Laaditaan perusteet hankkeen asettamiselle, jossa kartoitetaan eri ratkaisuja sekä arvioidaan niiden toteuttamismahdollisuuksia annettujen suorituskykyvaatimusten ja reunaehtojen puitteissa. Vaiheen lopussa valitaan toteutettava käyttökonsepti (ratkaisu). "* sekä -- *"Konseptivaiheessa laaditaan kuvaus siitä, millä aikataululla suorituskyky luodaan, kuinka pitkään sitä pidetään yllä ja missä vaiheessa siitä tullaan luopumaan. Tämä edesauttaa erilaisten konseptivaihtoehtojen vertailua, teknologiaratkaisujen vaihtoehtovertailussa ja hankintastrategioiden valinnassa sekä ohjaa käyttö- ja ylläpitovaiheen resurssien suunnittelua sekä tätä tukevaa tutkimus- ja kehittämistoimintaa."* (Pääesikunta 2020a, 9.)

Hankkeen asiantuntijat korostivat järjestelmän käyttöperiaatetta ja vaatimusmäärittelyn tärkeyttä. Ensimmäisenä tulee määrittää järjestelmän käyttöperiaatteen tavoitteet, joita tarkennetaan vaatimustenmäärittelyllä. Saadaksemme vastaukset kybersietoisuuden tavoitteista, voimme käyttää seuraavia kysymyksiä: -- "*Mihin hankittava tuote liittyy? Mitä sillä on tarkoitus tehdä? Minkälaiseen tietoturvaluokkaan tuote liitetään? Mitä sillä on tarkoitus tuottaa ja kuinka kauan järjestelmää käytetään? Näistä lähtökohdista saadaan ensimmäiset määrittelyt vaatimuksille."* (Haastatteluaineisto 2021.)

NIST-instituutin tutkimusasiakirjassa (2021) kybersietoisuuden tavoitteet saavutetaan "räätälöinnin" (tailoring) avulla. Räätälöintiä käytetään prioriteettien luomisessa kybersietoisuuden tavoitteiden saavuttamiseksi. Prioriteettien saavuttamiseksi käytetään organisaation riskienhallintastrategiaa, joka määrittää mitkä strategisen suunnittelun ja räätälöinnin periaatteet ovat tärkeimpiä. Konseptivaiheessa strategisen suunnittelun ja järjestelmän käyttökonseptin periaatteet tulee olla yhdenmukaisia suunniteltaessa käytettävää järjestelmää tai suorituskykyä. Räätälöinti ja riskienhallinta yhdistettynä on tehokas mittari, kun halutaan tunnistaa ja määrittää ehdotettu kybersietoisuudenratkaisu. (Ross ym. 2021, 17-18.) Kuten hankeohjeen määrittelyssä konseptivaiheen tarkoituksena on ohjata (räätälöidä) käyttö- ja ylläpitovaiheen resursseja, esimerkiksi hankkeen tavoitteena on tunnistaa kunnossapidolliset vaatimukset varaosien ja tarvikkeiden osalta.

Vastauksista merkille nostettavin käsite oli tietoturvaluokka, josta voitiin päätellä tämän tarkoittavan tiedon luokittelua. Tiedon luokittelun tavoitteena on varmistaa, että suojattavan tiedon suojaustaso on riittävä. Suojaustason määrittely toimii tässä tapauksessa ohjaavana menettelynä, joka määräytyy sen perusteella miten merkittävä tieto tai suojattava järjestelmä on. (SFS-ISO/IEC 27001:2017, 18.)

5.4.2 Määrittely

Puolustusvoimien joukon ja järjestelmän elinjaksohallintaohjeessa (HQ496) määrittelyvaihe kuvaillaan seuraavasti: -- *"Tarkennetaan konseptivaiheen tuotteita, tunnistetaan suorituskyvyn ratkaisunäkökulman eri osatekijöiden liitynnät ja muiden suorituskykyjen sekä hankkeiden väliset rajapinnat mukaan lukien*

kansainvälisen yhteistoiminnan tarpeet ja mahdollisuudet. Lisäksi valmistelussa tarkennetaan hankkeen riskejä, riskienhallintamenettelyjä ja turvallisuusvaatimuksia sekä -tarpeita. Tarvittavat tietopyynnöt (RFI, Request For Information) ja/tai markkinakartoitus toteutetaan pääsääntöisesti määrittelyvaiheessa teknisten ja taloudellisten perusteiden suunnittelua varten " (Pääesikunta 2020a, 10.)

Hankkeen asiantuntijat korostivat, että RFI-vaiheessa kybersietoisuuden vaatimukset tulee olla tiedossa niin pitkälle kuin mahdollista. Kybersietoisuuden vaatimukset luodaan järjestelmän vaatimustenmäärittelyllä, jolla asetetaan perusteet järjestelmän käyttöperiaatteet. Esimerkiksi järjestelmästä tulee varustaa sähkönsyötön varmennuksella, joka takaa järjestelmän käytettävyyden 24 tunnin ajan. Hankkeen asiantuntijat erityisesti korostivat, että vaatimustenmäärittely tulee harkita tarkkaan. Liian tiukat vaatimukset voivat aiheuttaa sen, että tarjouksia ei tule. Liian löyhästi määritellyt vaatimukset eivät taas tuota haluttua tulosta, jonka tuloksena kybersietoisuuden rakentaminen voi muodostua kohtuuttoman raskaaksi omalle organisaatiolle." (Haastatteluaineisto 2021.)

Jyri Kosolan (2007) mukaan määrittelyvaiheessa tarkennetaan konseptivaiheen vaatimuksia, jotka ollaan saatu markkina- ja teknologiakartoituksen kautta. Tämä on oleellisin ero NIST-instituutin tutkimusasiakirjassa (2021) esitettyyn järjestelmän elinkaarimalliin, jossa ei käsitellä markkina- ja teknologiakartoitusta. Tutkimusasiakirjassa keskitytään enemmänkin systeemisuunnittelun näkökulmiin. (Ross ym. 2021, 17.) Markkina- ja teknologiakartoitus kuuluu oleellisena osan Puolustusvoimien määrittelyvaiheeseen, jossa luodaan tietopyyntö (RFI). Tietopyynnön tarkoituksena on selvittää millä yrityksellä on valmius vastata tarjouspyyntöön, joka muodostaa käsityksen siitä minkälaisella järjestelmäkonseptilla tai järjestelmillä voidaan kyseinen suorituskyky luoda. Tietopyyntö auttaa tässä tapauksessa, kun järjestelmävaatimukset voivat olla eri konsepteilla hyvinkin erilaisia. (Kosola 2007, 222.)

5.4.3 Suunnittelu ja kehittäminen

Puolustusvoimien joukon ja järjestelmän elinjaksohallintaohjeessa (HQ496) suunnittelu- ja kehittämisvaihe kuvaillaan seuraavasti: -- *"Tarkennetaan määrittelyvaiheen tuotteita sekä varmistetaan, että suorituskyvyn rakentamisen ja ylläpidon kustannukset ja niiden seurannaisvaikutukset eivät ylitä annettuja resursseja. Tarvittavat tarjouspyynnöt (RFQ, Request For Quotation) ja tarjouksien vertailu/valinta toteutetaan pääsääntöisesti suunnittelu ja kehittäminen -vaiheessa teknisten ja taloudellisten perusteiden tarkastamista varten."* (Pääesikunta 2020a, 11.)

Hankkeen asiantuntijoiden mukaan suunnittelu- ja kehittämisvaiheessa tulee olla järjestelmätoimittajien tiedot käytettävissä. Järjestelmätoimittajien tietojen perusteella voidaan luoda ensimmäinen uhka- ja riskianalyysi, jolla on todellista merkitystä. Analyysin perusteella pystytään määrittelemään jatkotoimenpiteet, mahdolliset lisäkysymykset toimittajille sekä pystytään selvittämään omat mahdollisuudet rakentaa haluttu järjestelmä tai järjestelmäkokonaisuus. (Haastatteluaineisto 2021.)

Oleellisena osana suunnittelu- ja kehittämisvaihetta on hankinnan valmistelu ja hankinnan toteutus. Hankinnan valmistelulla tarkoitetaan hankintaan liittyviä suunnittelu- ja hallinnollisia toimenpiteitä, jotka voivat olla pienhankintoja tai kokonaan uuden järjestelmäkokonaisuuden hankintaa (suorituskyky). (Kosola 2007, 243.) Tässä kohtaa voidaan vain todeta, että hankintatoiminta ja tähän liittyvä kaupallishallinnolliset asiat menevät tämän opinnäytetyön ulkopuolelle, joten näitä ei käsitelty tässä opinnäytetyössä. Kuitenkin hankinnan valmistelu ja hankinnan toteutus ovat oleellisessa osassa hankkeen kokonaisuutta, jossa kybersietoisuus tulee ottaa myös huomioon.

Hankinnan valmisteluun kuuluu tietopyyntöjen (RFI) valmistelu ja lähettäminen, johon järjestelmätoimittajat vastaavat tarjoamalla tuotteitaan. Tietopyyntöjen vastausten perusteella voidaan tehdä tarkennuksia vaatimustenmäärittelyyn, jonka perusteella voidaan luoda tarjouspyyntö (RFQ) varteenotettaville järjestelmätoimittajille. Tarjouspyynnön liitteenä esitetään tarkennettu vaati-

mustenmäärittely teknisistä spesifikaatioista (kuten kybersietoisuus/ICT-varautuminen), joilla määritellään konkreettiset ratkaisut tavoiteltavasta järjestelmävaatimuksista. (Kosola 2007, 222, 314.)

Hankinnan toteuttamisella tarkoitetaan tarjouspyynnön (RFQ) laadintaa, joka on ensimmäinen hankintaprosessin kaupalliseen toteuttamisvaiheeseen liittyvä pakollinen toimenpide. Tarjouspyynnön yhtenä perusteasiakirjoina ovat operatiivinen konsepti ja järjestelmäsuunnitelma. Operatiivisen konseptin tarkoituksena on vastata järjestelmän yleisestä käytettävyydestä, järjestelmän erityispiirteistä ja järjestelmän sidonnaisuudesta muihin osajärjestelmiin. Järjestelmäsuunnitelman tarkoituksena on vastata järjestelmävaatimuksiin, joilla kuvataan toiminnallisia vaatimuksia, sidonnaisuuksia muihin järjestelmiin, ympäristövaatimuksiin, infrastruktuurivaatimuksiin, laatuvaatimuksiin ja turvallisuusvaatimuksiin. Oleellisena osana tarjouspyynnöstä on tunnistaa, että järjestelmää tarjoava yritys kykenee täyttämään asetetut vaatimukset. (Kosola 2007, 312, 318.)

NIST-instituutin tutkimusasiakirjan (2021) mukaan kehittämisvaiheessa on selvitetty ja priorisoitu kybersietoisuuden vaatimukset, jotka asetetaan vaatimuksina tulevalle järjestelmälle. NIST-instituutin tutkimusasiakirjassa korostetaan suunnitteluvaiheessa tapahtuvaa käytännön testaamista, jolla voidaan analysoida ja evaluoida järjestelmän kybersietoisuutta. Käytännön testaaminen tapahtuu esimerkiksi rasittamalla järjestelmää riittävästi, jonka tarkoituksena on testata järjestelmän vikasietoisuutta sekä kybersietoisuutta. (Ross ym. 2021, 17; Kosola 2007, 307, 319.) NIST-instituutin ja ISO-15288 standardin mukaisesti järjestelmätestaukset tulisi tehdä ennen kuin päätetään hankkia kyseistä järjestelmää, mutta käytännössä toteutus on aivan muuta. Käytännössä järjestelmätestit tulevat vasta rakentamisvaiheessa, kun ensimmäinen prototyyppi sarjavalmisteisesta järjestelmästä konkreettisesti rakennetaan. Tämä sinällään on jo merkittävä huomio, kun ja jos halutaan toteuttaa järjestelmävaatimukset täyttävä järjestelmä.

5.4.4 Rakentaminen

Puolustusvoimien joukon ja järjestelmän elinjaksohallintaohjeessa (HQ496) rakentamisvaihe määritellään seuraavasti: -- *"Rakennetaan suunniteltu suorituskyky, otetaan vastaan hankittu materiaali/palvelu, varustellaan ja integroidaan järjestelmät sekä luodaan valmiudet joukkojen tuottamiselle. Rakentamisvaiheessa tulee huomioida suorituskyvyn todentaminen ja kelpuuttaminen (verifiointi ja validointi) sekä järjestelmän käyttöön hyväksyntään ja käyttöönottoon liittyen ohjeistuksen ja koulutuksen varmistaminen, viranomaistarkastukset, hanketurvallisuus ja sidosryhmäturvallisuussopimukset sekä elinjaksosuunnitelman ajantasaisuus ml. elinjaksokustannuslaskelma."* (Pääesikunta 2020a, 12.)

Hankkeen asiantuntijat korostivat, että järjestelmä tulee rakentaa vaatimusmäärittelyn mukaisesti sekä järjestelmän toimittaja tulee sitouttaa kybersuojautumisen rakentamiseen. Rakentamisvaiheessa on ensisijaisen tärkeätä, että järjestelmälle haetaan tarvittavat hyväksynnät. Nämä hyväksynnät koostuvat SAA-lausunnosta sekä teknisestä hyväksynnästä, joilla järjestelmä voidaan hyväksyä käyttöön. (Haastatteluaineisto 2021.)

Kybersietoisuus tulee ajatella osana isompaa kokonaisturvallisuutta, jota käsiteltiin luvussa 4.2 Turvallisuustoiminta. Kuitenkaan kybersietoisuutta ja kyberturvallisuutta ei ole listattuna kokonaisturvallisuuden listaukseen, vaikka tietoturvallisuus ja tekninen tietoturvallisuus löytyvät listauksesta. Kybersietoisuus määrätään erillisellä asiakirjalla osaksi järjestelmän turvallisuutta, jolla varmistetaan järjestelmän kybersietoisuus rakennettavien ja hankittavien järjestelmien, palveluiden ja kehitettävien uusien joukkojen osalta. Käytännössä kybersietoisuuden toteuttaminen vastuu norminmukaisuudesta jää kuitenkin hankkeelle, projektille tai hankinnalle itselleen. Tästä syystä hankkeiden, projektien ja hankinnoista vastaavien tulee nimetä kybersietoisuuden suunnittelusta vastaava henkilö tai tiimi, joiden tehtävänä on järjestelmän kybersietoisuuden toteutus ja kehittäminen. (Haastatteluaineisto 2021.)

NIST-instituutin tutkimusasiakirjan (2021) mukaan kybersietoisuus voidaan liittää osaksi hankkeen toteuttamiseen liittyvää turvallisuutta ja hankkeen kautta

toteutettavan järjestelmän turvallisuutta, vaikka tätä ei suoraan tutkimusasiakirjassa mainita. Tutkimusasiakirja määrittelee, että kybersietoisuuden suunnittelu voidaan liittää osaksi muita suunnitteluperiaatteita, kuten turvallisuus. (Ross ym. 2021, 13.) Tästä voidaan johtaa hankkeen toteuttamiseen liittyvään turvallisuuteen, joka huomioidaan turvallisuussopimuksella. Turvallisuussopimus on osa hankintasopimusta, joka on rakentamisvaiheessa viimeisteltävä asiakirja. Turvallisuussopimus on molempia osapuolia sitova asiakirja, jolla osapuolet sitoutetaan pitämään salassa kaikki salassa pidettävät tiedot. (Kosola 2007, 343.)

Järjestelmässä toteutettava turvallisuuteen sitouttaminen tarkoittaa käytännössä vaatimustenmukaisuusvakuutusta (COC, Certificate of Conformity), jolla järjestelmän toimittaja velvoitetaan antamaan vakuus siitä, että toimitettu järjestelmä täyttää sopimuksessa kirjatut vaatimukset. Hankintasopimus on tällöin tärkeässä roolissa, jolla järjestelmän toimittaja sitoutetaan kybersuojautumisen (kybersietoisuuden) rakentamiseen ja varsinkin ylläpitämiseen operointi- ja purkamisvaiheiden aikana. Tästä käytetään nimitystä huolto-, kunnossapito- tai tukisopimus. (Pääesikunta 2015a, 2; Kosola, 2007, 356.)

Tekninen hyväksyntä on osa järjestelmän suunnittelu ja rakentamisprosessia, jonka tarkoituksena on varmistaa, että järjestelmä täyttää sille asetetut tekniset ja toiminnalliset vaatimukset sekä turvallisuusvaatimukset. (Pääesikunta 2015a, 5; Kosola, 2007, 356–359.) NIST-instituutin tutkimusasiakirjan (2021) mukaan rakentamisvaiheessa järjestelmän testaus ja validointi ovat oleellisessa osassa. Kybersietoisuuden testauksen osalta rakentamisvaiheen aikana tulee suorittaa suunnittelu- ja määrittelyvaiheen aikana suunnitellut testit sekä korjattava testeissä havaitut puutteet. Rakentamisvaiheen aikana tehtävä testaus on tärkein, koska rakentamisvaiheen jälkeen järjestelmä siirtyy käyttö- ja ylläpitovaiheeseen. (Ross ym. 2021, 17.)

SAA-lausunto (Security Accreditation Authority) on osa järjestelmän teknistä hyväksyntää, jonka suorittaa Liikenne- ja viestintävirasto Traficom. SAA-lausunto on tietojärjestelmien arviointi- ja hyväksyntäprosessi, jossa turvallisuusviranomainen antaa virallisen lausunnon turvallisuusjärjestellyistä. Traficomin suorittamalla hyväksynnällä tarkoitetaan prosessia, jonka päätteeksi: -- *"järjes-*

telmä on hyväksytty käytettäväksi määritellyssä turvaluokassa, tiettyä turvallisuuden takaavaa toimintatapaa noudattaen käyttöympäristössään ja hyväksyttävällä riskitasolla, sen pohjalta, että hyväksytyt tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet on toteutettu". Oleellisinta SAA –lausunnon hyväksynnästä on huomioida, että SAA -lausunto on voimassa 3 vuotta myöntämispäivästä. SAA -lausunto voi raueta, jos järjestelmän turvallisuudessa tapahtuu jokin merkittävä muutos. (Traficom 2021, 1, 6.) Teknisen hyväksynnän merkitys korostuu järjestelmän käyttö ja ylläpitovaiheeseen, kun järjestelmän käytössä tapahtuu merkittävä muutos. Järjestelmäpäivitykset tai tavanomaiset ylläpidosta aiheutuvat muutokset eivät vaikuta voimassaolevan hyväksynnän raukeamiseen, kuitenkin järjestelmävastuullinen organisaatio on vastuussa hyväksyntäkriteerien ylläpitämisestä. (Pääesikunta 2015a, 13.)

5.4.5 Käyttö, ylläpito ja purkaminen

Hankkeet ovat määräaikaisia, jotka päättyvät rakentamisvaiheen lopussa. Puolustusvoimien joukon ja järjestelmän elinjaksohallintaohjeessa (HQ496) käyttö- ja ylläpitovaihe on yhdistetty yhdeksi vaiheeksi, jossa: --" *Käyttö ja ylläpito -vaiheen vastuu on joukko- ja järjestelmäkokonaisuuden osalta suorituskykyvastuullisella. Suorituskyvyn materiaalisen osatekijän osalta vastuu on järjestelmävastuullisella*." sekä -- "*Käyttö- ja ylläpitovaiheessa seurataan saavutettua suorituskykytasoa arvioimalla suorituskyvyn ylläpidettävyyttä ja riittävyyttä operatiivisiin suunnitelmiin sekä käytön volyymiin nähden. Lisäksi seurataan materiaalin teknistä elinjaksoa ja arvioidaan edellytykset ylläpitää sitä tulevaisuudessa elinjaksosuunnitelman mukaisesti. Näiden tietojen perusteella päätetään suorituskyvyn käytön ja ylläpidon jatkamisesta, päivittämisestä tai luopumisesta. Mikäli suorituskyky päätetään päivittää ja päivitys toteutetaan hankkeena, elinjakson vaiheet tehdään uudestaan tarvittavassa laajuudessa."* (Pääesikunta 2020a, 13.)

Hankkeen asiantuntijoiden ja järjestelmävastuullisten mukaan, käyttö- ja operointivaiheessa on ylläpidettävä määräajoin kybersuojautumisen tilannetta ja riskianalyysiä. Kuten aikaisemmassa luvussa todettiin, SAA-lausunto on voimassa vain kolme vuotta kerrallaan ja on uusittava määräajoin. Asiantuntijat korostivat, että uuden SAA -lausunnon saamisen prosessi on aloitettava

ajoissa, jotta SAA-lausunto ei vanhene ja järjestelmä ei mene käyttökieltoon. (Haastatteluaineisto 2021.)

Kybertoimintaympäristö on jatkuvassa muutoksessa, joten järjestelmän kybersietoisuutta tulee seurata. Käyttö- ja ylläpitovaiheessa oleellisena osana on seurata kybersietoisuuden tehokkuutta ja toteutumista, joka voi joissain tapauksissa heikentyä toimintaympäristön muutosten vuoksi. Tehokkuuden ja toteutumisen heikentymän esimerkkinä voidaan käyttää, kun käyttäjämäärä lisääntyy radikaalisesti tai järjestelmä otetaan käyttöön uusissa toimintaympäristöissä. (Ross ym. 2021, 17.) Käyttö- ja ylläpitovaihe on järjestelmän elinkaaren näkökannalta kaikkein pisin. Järjestelmän elinkaari voi olla useita vuosia tai vuosikymmeniä pitkä ajanjakso, jonka aikana järjestelmään lisätään tai poistetaan komponentteja. Merkittävintä käyttö- ja ylläpitovaiheessa on tunnistaa järjestelmän sidonnaisuus toisiin järjestelmiin, joka voi pahimmassa tapauksessa heikentää järjestelmän kybersietoisuutta. Käytännössä tämä voi esimerkiksi tarkoittaa, että seurataan järjestelmän suorituskykytasoa arvioimalla päivityksien, kunnossapidon ja operatiivisen käytettävyyden kustannuksia. Seuraamalla näitä tunnusmerkkejä voidaan arvioida, täyttyykö kriteerit järjestelmän päivittämisestä vai luovutaanko järjestelmästä kokonaisuudessaan. (Pääesikunta 2020a, 13; Haastatteluaineisto 2021.)

Purkamisvaihe aloitetaan jo käyttö- ja ylläpitovaiheessa, kun järjestelmästä on päätetty luopua ja tämä tapahtuu hallitusti vaiheittain. Kuten käyttö- ja ylläpitovaiheessa järjestelmän purkaminen voi vaikuttaa muiden osajärjestelmien kybersietoisuuteen, tällöin kybersietoisuuden toteutuminen tulee analysoida ja varmentaa. Purkamisvaiheessa tulee varmistaa, että järjestelmässä käytetyt komponentit tai järjestelmän osat tuhotaan asianmukaisesti. Komponenttien tuhoaminen tulee toteuttaa niin, ettei tuhottavasta komponentista pystytä palauttamaan tai keräämään arkaluontoistatietoa. (Pääesikunta 2020a, 13–14; Ross ym. 2021, 18.)

6 JOHTOPÄÄTÖKSET

Tässä luvussa esitetään opinnäytetyön tutkimusprosessin mukaisesti johtopäätökset, joiden tarkoituksena on tutkimustulosten yleistäminen. Luvussa kä-

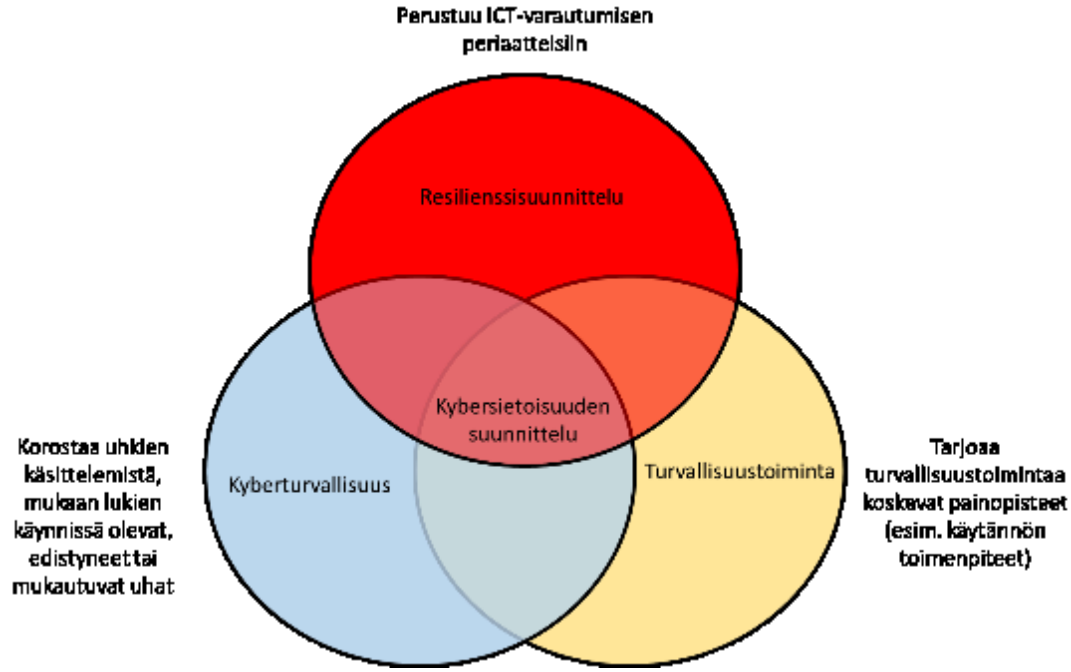
sitellään ja mallinnetaan kybersietoisuuden suunnittelun viitekehys sekä kybersietoisuuden mallintaminen systeemisuunnittelun näkökannalta. Viitekehys sekä systeemisuunnittelun malli muodostettiin opinnäytetyön teoriaosuudesta sekä haastatteluiden ja Webropol-kyselyn pohjalta.

Vastaako Puolustusvoimien normit ja ohjeet akateemista tutkimusaineistoa?

Kuten luvussa 3.1 Kybersietoisuuden suunnittelun viitekehys esitetään, kybersietoisuuden suunnittelu muodostuu resilienssisuunnittelusta, kyberturvallisuudesta ja operaatioturvallisuudesta. Resilienssisuunnittelun perusteet muodostuvat ennakoinnista, kestävyydestä, toipumisesta ja kyberresurssien kehittämisestä. Kyberturvallisuus on tiedon, laitteistojen, verkostojen, ohjelmistojen ja käyttäjien luottamuksellisuuden, eheydyn ja saatavuuden turvaamista koko elinjakson ajan. Operaatioturvallisuus muodostuu systeemin turvallisuussuunnittelusta, jonka keskiössä on tietoturvallisuus. Tällöin voidaan yleistää, että kybersietoisuuden tavoitteena on turvata tiedon luottamuksellisuus, eheys ja saatavuus.

Puolustusvoimien resilienssisuunnittelu perustuu ICT-varautumisen periaatteisiin (Information and Communications Technology), joka on riskienhallintaan pohjautuvaa ICT-toimintaan. ICT-varautuminen perustuu jatkuvuudenhallintaan ja tiedon turvaamisesta kaikissa olosuhteissa, joka pitää sisällään hallinnolliset, toiminnalliset, tekniset toimenpiteet sekä ratkaisut, joilla varmistetaan tiedon saatavuus ja toiminnollisuuksien häiriötön toiminta kaikissa olosuhteissa. Kybersietoisuuden suunnitteluun näkökannalta kyberturvallisuuden tarkoituksena on tuoda kybertoimintaympäristön kautta muodostamat kyberuhat, jotka muodostuvat jatkuvista, kehittyneistä ja muuntautumiskykyisistä kyberuhista. (Pääesikunta 2020c, 1; Bodeau ym. 2011, 13)

Kybersietoisuuden suunnittelun viitekehys voidaan ulkomaalaisten tutkimusasiakirjojen, Puolustusvoiminen normien ja ohjeiden sekä haastatteluiden mukaan mallintaa (kuva 15), joten Puolustusvoimien normit ja ohjeet pohjautuvat kyllä akateemiseen tutkimusaineistoon.



Kuva 15. Tutkijan näkemys johdettuna Mitre-organisaation kybersietoisuuden suunnittelusta (Bodeau ym. 2011, 13)

Kuvassa 15 esitetty turvallisuustoiminta perustuu Mitre-organisaation operaatioturvallisuuteen, mutta Puolustusvoimien näkökannalta turvallisuustoiminnan tarkoituksena on tarjonta huomioitavat painopisteet ohjeiden ja normien mukaan. Huomiona turvallisuustoiminnan 15 toimialasta on se, että kyberturvallisuutta ja kybersietoisuutta ei ole listattuna kokonaisturvallisuuden listaukseen. Tietoturvallisuus ja tekninen tietoturvallisuus löytyvät listauksesta, mutta kyberturvallisuutta ja kybersietoisuutta ei listauksesta löydy. Kuten luvussa 4.1 Hanke ja sotilaallinen suorituskyky todettiin, kyberuhilta suojautumista ja puolustautumista vastaan käsitellään kyvykkyysnäkökulmasta. Kybersietoisuus kuitenkin määrätään erillisellä asiakirjalla (HQ928, Kybersietoisuuden varmentaminen järjestelmässä) osaksi järjestelmän turvallisuutta, jolla varmistetaan järjestelmän kybersietoisuus rakennettavien ja hankittavien järjestelmien, palveluiden ja kehitettävien joukkojen osalta. Tästä johtuen kybersietoisuutta ohjaava normi ja kyberuhilta suojautuminen tuntuvat irrallisilta ja päälle liimatuilta kokonaisuuksilta, jotka aiheuttavat hämmennystä hankkeita toteuttavien ja järjestelmistä vastaavien keskuudessa. (Haastatteluaineisto 2021.) Päätelmä perustuu lukuihin 4.1 Hanke ja sotilaallinen suorituskyky, 4.2 Turvallisuustoiminta ja 5.4.4 Rakentaminen, joissa käsiteltiin Puolustusvoimien kokonaisturvallisuutta sekä kybersietoisuuden käytäntöjä hankkeen elinkaaressa.

Mitä ovat ne käytännöt, joita hankkeessa työskentelevät henkilöt ovat kehittäneet?

Kuten opinnäytetyön tutkimuksen tavoitteena oli haastatella hankkeen asiantuntijoita ja pyrkiä selvittämään parhaat toimenpiteet, joita he ovat hankkeen aikana kehittäneet. Kuten luvussa 5.2 Tutkimusaineiston keruumenetelmät todettiin, teemahaastattelu ja Webropol-kysely toimivat hyvin opinnäytetyön tutkimustiedon toteutusmenetelmänä. Vastauksiksi saatiin kerättyä enemmänkin huomioita, joita tulee huomioida hankkeen elinkaaren eri vaiheissa. Vastauksien ja esimerkkien puutteellisuus johtui varmaankin siitä, että opinnäytetyön toteutustapa on julkinen. Nämä konkreettiset etsittävät käytänteet ovat mahdollisesti tietoturvaluokiteltua materiaalia ja tietoa, joten tämän vuoksi tähän alakysymykseen ei saatu toivottuja käytännön esimerkkejä.

Merkittävimpänä huomiona voidaan pitää, että kybersietoisuus tulee huomioida järjestelmän koko elinkaaren ajan ja tätä tulee seurata järjestelmällisesti. Järjestelmien teknologinen kehitys on todella nopeaa, joten taistelu haavoittuvuuksia vastaan on jokapäiväistä ja kestää järjestelmän koko elinkaaren ajan. Tällöin järjestelmän haavoittuvuuksia tulee järjestelmällisesti etsiä sekä analysoida niiden mahdollinen vaikutus järjestelmään. Analyysin perusteella tulee tehdä tarvittavat päätökset sekä toteuttaa tarvittavat toimenpiteet järjestelmän suojaamiseksi. Mitä kauemmin järjestelmää käytetään, sitä suurempi riski on kybervaikuttamiselle järjestelmän vanhetessa. (Haastatteluaineisto 2021)

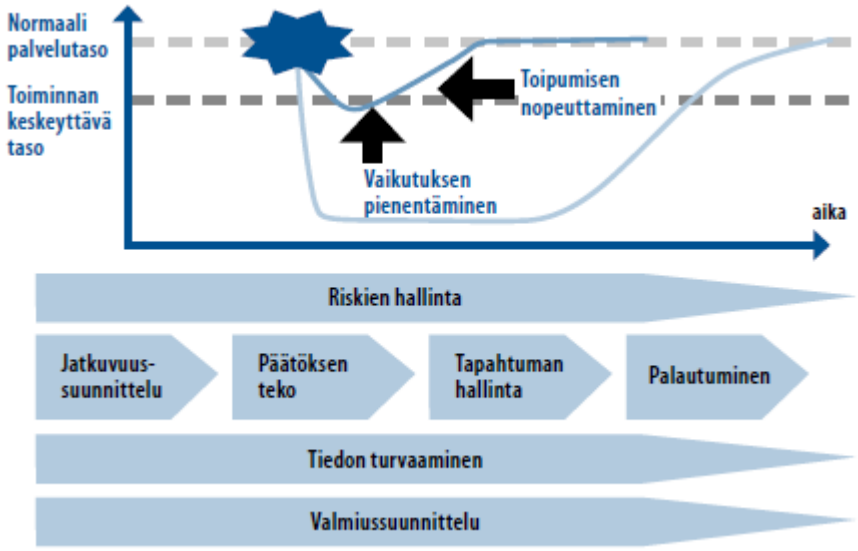
Kuten luvussa 5.4.1 Konsepti todettaan, ensimmäisenä tulee määrittää järjestelmän käyttöperiaatteet, joita tarkennetaan vaatimustenmäärittelyllä. Hyvänä käytännön esimerkkinä voidaan pitää, että vastataan kysymykseen, "minkälaiseen tietoturvaluokkaan tuote tullaan liittämään?"

Vastauksena kysymykseen voidaan pitää seuraavaa. Avainasemassa on tunnistaa järjestelmässä käytettävä tietoturvallisuusluokka. Tietoturvallisuusluokka saadaan tiedon luokittelulla, jonka tavoitteena on varmistaa suojattavan tiedon suojaustason riittävyys sekä toteutusmenetelmät. Tällöin kybersietoisuuden suunnittelun lähtökohdat perustuvat riittävään kyberuhilta suojautumiseen sekä taataan järjestelmän toiminnan käytettävyys myös poikkeusoloissa.

Vastaako Puolustusvoimien hanketoiminnassa toteutettava käytäntö tutkimusaineiston teoriaa?

Haastatteluiden perusteella kybersietoisuuden ja kyberuhilta suojautumisen ymmärtäminen ja tavoitteiden saavuttaminen riippuvat hyvinkin paljon hankehenkilöiden taustoista ja kokemuksesta. Hankeisiin osallistuvilla henkilöillä on hyvinkin erilaisia käytännön toimintatapoja toteutuksen suhteen, mutta käytännön toimintatavat eivät poikkea turvallisuus- ja hankeohjeessa määritellyistä asiakohdista. Kriittisesti ajatellen normit, ohjeet ja määräykset ovat niitä mitä tulee noudattaa, mutta ovat hyvin vaikeasti löydettävissä sekä kybersietoisuuden rakentaminen normiohjauksen mukaisesti vaati jopa enemmän työtä kuin muu hankkeeseen liittyvä työ. Puolustusvoimissa normia, ohjeita ja määräyksiä on todella paljon, mikä osaltaan vaikuttaa toteutuksien kirjoon, mutta kokonaisuutena turvallisuustoiminta on kiinteä osa kaikkea Puolustusvoimien toimintaa ja ainakin pyritään huomioimaan kaikessa toiminnassa. Haasteina erityisesti koettiin hankkeen kybersietoisuudesta vastaavan henkilön saaminen / löytäminen, koska haastateltavien mukaan Puolustusvoimien henkilöstörakenteessa ei kyseistä tehtävää ole luotuna. Puolustusvoimissa hankkeita on todella paljon ja jokainen hanke on erilainen, tällöin kybersietoisuudesta vastaavan henkilön on omattava riittävät tiedot ja taidot kybersietoisuudesta sekä hankkeista. (Haastatteluaineisto 2021.)

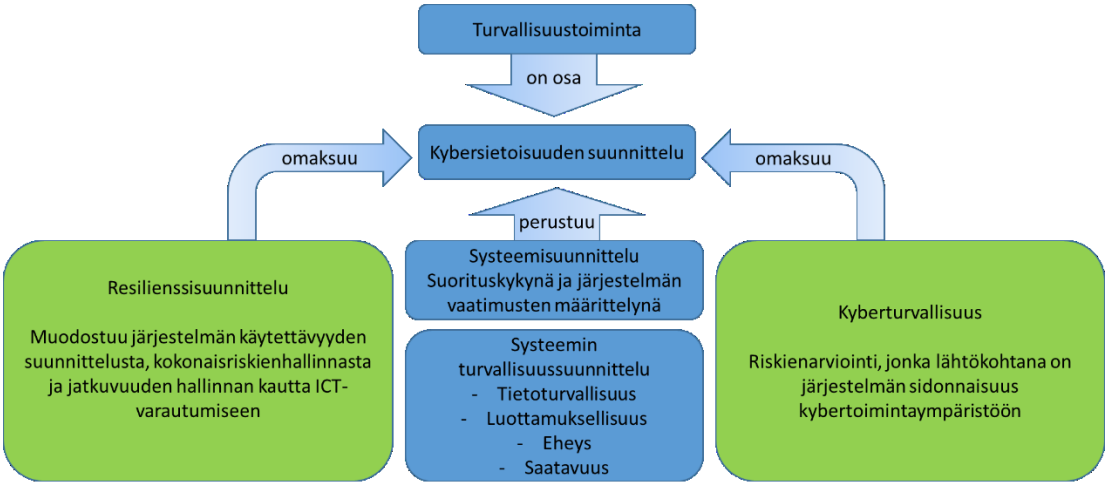
Haastatteluiden perusteella haavoittuvuuksien hallinta on osa kokonaisriskienhallintaa, johon oleellisena osana lopulta liittyy jatkuvuuden hallinnan kautta ICT-varautuminen (kuva 16). Kokonaisriskienhallinnassa keskeisintä ICT-varautumisessa on systemaattinen tapa arvioida uhkia, vaatimuksia sekä käytettävissä olevia resursseja. Riskienarvioinnissa oleellisinta on tunnistaa jäännösriski, joka johdetaan toimintavaikutusarvion määrittämän kokonaisriskin ja kontrollikohtaisen suojausvaikutuksen erotuksena. Jäännösriskin käsittelyssä on oleellista tiedostaa riskin suuruus, josta voidaan tietoisesti tehdä hallinnollinen päätös ja hyväksyä jäännösriskin suuruus. (Haastatteluaineisto 2021; Valtionvarainministeriö 2012, 33–35.)



Kuva 16. Jatkuvuuden hallinta on osa ICT-varautumista toteuttava prosessi (Valtionvarainministeriö 2012, 33)

Kuten luvussa 3.2 Kybersietoisuus systeemisuunnittelun näkökulmasta todettiin, kybersietoisuuden suunnittelu on operaatioturvallisuuden osa, joka koostuu systeemin turvallisuussuunnittelusta. Systeemin turvallisuussuunnittelun perustuu systeemisuunnittelun periaatteisiin, jossa systeemin turvallisuussuunnittelun tavoitteena on suojata ihmisiä ja omaisuutta kehittyneitä uhkia vastaan.

Kybersietoisuuden suunnittelu voidaan ulkomaalaisten tutkimusasiakirjojen, Puolustusvoiminen normien ja ohjeiden sekä haastatteluiden mukaan mallintaa (kuva 17) siten, että kybersietoisuuden suunnittelu perustuu Puolustusvoimien turvallisuustoimintaan. Järjestelmän kybersietoisuuden suunnittelu perustuu systeemisuunnittelun periaatteisiin, jonka keskiössä on suorituskyvyn ja järjestelmän vaatimusten määrittely. Käytännössä systeemisuunnittelun periaatteet voivat olla eriäviä käytännön toteutuksien osalta suunniteltaessa järjestelmää, mutta noudattavat lopulta samaa lopputulosta. (Haastatteluaineisto 2021.)



Kuva 17. Tutkijan näkemys johdettuna Mitre-organisaation tutkimusasiakirjan mukaan, miten kybersietoisuutta huomioidaan osana järjestelmän systeemisuunnittelua (Bodeau ym. 2011, 10)

Systeemin turvallisuussuunnittelu perustuu tietoturvallisuuteen, jonka keskiössä on turvata järjestelmän luottamuksellisuus, eheys ja saatavuus. Hankkeet tuottavat suorituskykyä, joilla on aina jonkinlaista operatiivista merkitystä ja vaikutusta kokonaisuuteen. Suojaamattomat tai huonosti suojatut kohteet muodostavat uhan toiminnalle, jolloin esimerkiksi tärkeät tiedot päätyvät oikeudettomien haltuun. Tällöin tietoon ei voida enää luottaa tai pahimmillaan estävät järjestelmän toiminnan kokonaan. Tietoturvallisuus ei voi jäädä siihen, että pelkästään suojataan kohteet. Ilman valvontaa ollaan pelkän luulon tai luottamuksen varassa, että mitään ei tapahdu tai tapahtuessa kaikki on kunnossa. Ilman järjestelmä- ja kybervalvontaa suojautuminen jää vajaaksi. Uhkaan ei voi reagoida, ellei sitä havaitse. Tietoturvallisuuden merkitys katoaa, jos esimerkiksi tietojärjestelmiä käyttävät henkilöt eivät tiedosta sen merkitystä tai toimivat huolimattomasti joko tahallaan tai tahattomasti. Tähän vaikuttaa olennaisesti se, että käyttövaltuushallinnan prosessit, riittävä koulutus ja ohjeistukset ovat kunnossa. (Haastatteluaineisto 2021.)

7 POHDINTA

Tässä luvussa pohditaan opinnäytetyön tutkimusta ja tutkimustuloksien suhdetta teoreettiseen viitekehykseen sekä esitetään mahdolliset jatkotutkimus mahdollisuudet. Luvussa tarkastellaan myös tutkimuksen luotettavuutta ja pyritään vastamaan kysymykseen, miten kybersietoisuuden huomioimista hankkeen elinkaaressa voidaan kehittää.

Tutkimuksen luotettavuus ja hyödynnettävyys

Tutkittavana ilmiönä ja käsitteenä oli kybersietoisuus. Opinnäytetyöni tavoitteena oli tuottaa uutta ja luotettavaa tietoa kehittämään kybersietoisuuden huomioimisesta hankkeen toiminnassa. Tutkimustehtävän tarkoitus oli selvittää Puolustusvoimien hankkeen elinjaksojen hallintaprosessin toiminta ja hanketta ohjaavien ohjeiden ja normien merkitys. Haastattelut toteutettiin puolistrukturoidun teemahaastattelun sekä Webropol-kyselyn avulla, joiden tavoitteena oli selvittää parhaat toimenpiteet, joita hankeen asiantuntijat ovat kehittäneet hankkeen aikana sekä tunnistaa mahdollisesti kehitettävät osa-alueet hankkeen asiantuntijoiden osaamisesta.

Teemahaastatteluiden pitäminen oli alussa haastavaa, koska oikeitten henkilöiden löytäminen oli vaikeaa. Halusin löytää sellaisia henkilöitä, joilla on paras käytännön osaaminen ja ymmärrys hankkeiden sekä projektien toimintatavoista. Lopulta teemahaastatteluun ja Webropol-kyselyyn osallistui yhteensä 20 henkilöä, joista kahdeksan (8) nauhoitettiin ja viisi (5) vastasi Webropol-kyselyyn. Haastattelut kestivät noin 45 minuuttia, jonka aikana tein omia muistiinpanoja. Puolustusvoimien hankintoja, hankkeita, projekteja tai sen turvallisuutta koskevia tutkimuksia löytyi tietokantahakujen perusteella useampia, mutta nämä käsittelevät pääsääntöisesti hankkeiden turvallisuutta tai osaamisvaatimuksia eri näkökohdista. Tämä osaltaan vaikeutti itse tutkimuksen tekemistä, koska kybersietoisuudesta ei ole aikaisempia suomalaisia tutkimuksia tehty. Puolustusvoimissa normeja, ohjeita ja määräyksiä on todella paljon, jotka osaltaan vaikeuttivat teoriaosuuden konkreettisen tiedon etsimisessä sekä kirjoittamisessa.

Välitarkastelun ja haastatteluiden jälkeen huomasin, että opinnäytetyöni rakenne ja teoriasisältö kybersietoisuudesta on väärin. Tästä johtuen muutin opinnäytetyöni teoriaosuuden kybersietoisuudesta uudelleen, mutta tutkimusmenetelmää en vaihtanut alkuperäisestä tutkimussuunnitelmasta. Lähteiden aikaleimoista voi todeta sen, että opinnäytetyön tekemisessä meni kokonaisuudessaan yli vuosi. Lopullisen version tästä opinnäytetyöstä tein kevään 2022 aikana, jonka johdosta opinnäytetyön rakenne ja sisältö noudattaa paremmin kehittämistutkimuksen raportointimallia. Opinnäytetyön kirjoittaminen

ja tekeminen venyivät alkuperäisestä tutkimussuunnitelmasta, koska tutkimussuunnitelmani oli liian optimistinen. Ajankäytön sovittaminen töitten ja vapaa-ajan kanssa oli todella haasteellista, jonka vuoksi opinnäytetyön sisältö muuttui aina, kun aloitin tekemään opinnäytetyötä pitkän tauon jälkeen.

Tärkeintä opinnäytetyöni lopputuotoksen perusteella oli, että pystyin muodostamaan koulutussisältöä Kybersietoisuuden huomioiminen hankkeessa -opetustilaisuuteen. Perehtyneisyyteni kybersietoisuuteen alkoi siten, että osallistuin Kybersietoisuuden huomioinen hankkeessa -opetustilaisuuteen ensin opiskelijana ja myöhemmissä opetustilaisuuksissa luennoitsijana. Tutkimusmenetelmäkseni valitsin konstruktiivisen tutkimuksen, mutta tutkimukseni pohjautui enemmänkin etnografiseen tutkimukseen. Etnografisen tutkimuksen tarkoituksena on mahdollistaa syvällinen ja tiheä kuvaus tutkittavasta ilmiöstä, joka edellyttää elämistä itse ilmiön kanssa. Tämä vaatimus taas täyttyi siten, että työskentelen Puolustusvoimissa ja osallistun teknisenä asiantuntijana eri projekteihin sekä hankkeisiin. Jorma Kanasen (2017) mukaan etnografista tutkimusta ei pidä sekoittaa omalla työpaikallaan tehtyyn kehittämistyöhön, koska tutkija elää ja ymmärtää ilmiötä ulkopuolista paremmin. Tästä johtuen kehitystutkimuksen tekeminen omalle työpaikalleen voi aiheuttaa sen, että tutkimustuloset pohjautuvat tutkijan ”muisteluihin”, mikä ei täytä tieteellisen aineistonkeruuvaatimuksia. Opinnäytetyöni luotettavuuden nimissä voin todeta, että tutkimuksessa oli tutkimusjakso, aineiston keruuvälineet, tutkimusongelma sekä -kysymykset, joihin tuotettiin aineistoa. Opinnäytetyöni tutkimuksen luotettavuuden näkökannalta tutkimuspäätelmiä varmennettiin luetuttamalla niitä teemahaastatteluun vastanneilla asiantuntijoilla, jotka vahvistivat päätelmieni oikeellisuuden (validius). (Kananen 2017, 87–88.)

Opinnäytetyön tutkimushypoteesiksi muodostettiin, että hankehenkilöstö käsittää hankkeen prosessit ja järjestelmän elinkaarivaiheet normiohjauksen perusteella sekä osaavat soveltaa käytännössä kybersietoisuuden merkityksen hankkeen ja järjestelmän elinkaaressa. Testatakseni tutkimushypoteesin paikkaansa pitävyyden voidaan todeta, että tutkimushypoteesi kyllä osittain pitää paikkansa. Tutkimushypoteesia testasin teemahaastattelun sekä Webropol-kyselyn perusteella. Testauksen tulokseksi osoittautui, että kybersietoisuuden ja kyberuhilta suojautumisen ymmärtäminen ja tavoitteiden saavuttaminen riippuvat hyvinkin paljon hankehenkilöiden taustoista ja kokemuksesta.

Hankeisiin osallistuvilla henkilöillä on hyvinkin erilaisia käytännön toimintatapoja toteutuksen suhteen, mutta käytännön toimintatavat eivät poikkea turvallisuus- ja hankeohjeessa määritellyistä asiakohdista. Kriittisesti ajatellen normit, ohjeet ja määräykset ovat niitä mitä tulee noudattaa, mutta ovat hyvin vaikeasti löydettävissä. Kybersietoisuuden rakentaminen normiohjauksen mukaisesti vaati jopa enemmän työtä kuin muu hankkeeseen liittyvä työ. Puolustusvoimissa normeja, ohjeita ja määräyksiä on todella paljon, joka osaltaan vaikuttaa toteutuksien kirjoon, mutta kokonaisuutena turvallisuustoiminta on kiinteä osa kaikkea Puolustusvoimien toimintaa ja ainakin pyritään huomioimaan kaikessa toiminnassa.

Jatkotutkimus mahdollisuudet

Haastatteluiden perusteella kybersietoisuuden kokonaisvastuun kohdentaminen koettiin haastavaksi, koska Puolustusvoimien termistöllä järjestelmän elinkaarimallin mukaisesti voidaan olettaa, että vastuu järjestelmän kybersietoisuudesta jakaantuu järjestelmävastuulliselle sekä suorituskyvyn omistajalle. Hankkeen aikana toteuttava kybersietoisuuden vastuu voidaan päätellä kuuluvan hankepäällikölle. Päätelmä perustuu Timo Tolkin (2020) tekemään kehittämistutkimukseen: -- "*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*". (Tolkki 2020, 45.)

Hankkeet ja projektit ovat aikaan sidottuja kokonaisuuksia, jotka alkavat konseptivaiheesta ja loppuvat hankkeen päätösvaiheessa. Hankkeen loputtua järjestelmän ylläpitovastuu siirtyy järjestelmävastuulliselle ja suorituskykyvastuullisuus suorituskyvyn omistajalle. Suorituskyvyn omistajana toimii Puolustusvoimien puolustushaara Maa-, Meri- tai Ilmavoimat ja suorituskyvyn materiaalivastuu on puolustushaarojen järjestelmävastuullisella, joten kybersietoisuuden vastuunjako tulee olla määritettynä. Esimerkiksi järjestelmän ylläpitovaihe voi olla järjestelmästä riippuen jopa kymmeniä vuosia, joten kybersietoisuuden varmistaminen ylläpitovaiheessa vaatii enemmän ymmärrystä sekä tutkimista. Ylläpitovaiheessa järjestelmälle tehdään päivityksiä, järjestelmästä vaihdetaan

komponentteja tai järjestelmä liitetään osaksi muita osajärjestelmiä. Jatkotutkimukseksi ehdotan, miten kybersietoisuuden huomioimista voidaan kehittää järjestelmän elinkaaren ylläpitovaiheessa, tai miten voidaan ylläpitää järjestelmän kybersietoisuutta.

Miten kybersietoisuuden huomioimista hankkeen elinkaaressa voidaan kehittää?

Tässä opinnäytetyössä esitettyjen normien ja ohjeiden sekä kybersietoisuuden viitekehyksien käytön tarkoituksena on mahdollistaa järjestelmällinen ja pitkäjänteinen kybersietoisuuden kehittäminen organisaatiossa. Opinnäytetyön sisältöä voidaan esimerkiksi käyttää Kybersietoisuuden huomioiminen hankkeessa -opetustilaisuudessa tai sitten ihan yleisesti koulutusmateriaalin lähteenä. Toivon, että opinnäytetyön sisältö auttaa paremmin ymmärtämään kybersietoisuutta sekä resilienssisuunnittelun periaatteita, joita voidaan kehittää paremmaksi. Opinnäytetyöni on hieman ”maailmaa syleilevä” tutkimus ja kybersietoisuutta käsiteltiin hyvinkin käsitteellisellä tasolla. Jos tutkimuksen sisällössä olisi menty teknisiin toteutustapoihin ja käytänteisiin, ei tutkimusta olisi voitu tehdä julkisena versiona, joten tähän toteutustapaan en halunnut lähteä ja tehdä pahimmassa tapauksessa kaksi erillistä opinnäytetyötä.

Haastatteluiden, Webropol-kyselyn sekä teoreettisena lähdeaineistona käytettyjen normien ja ohjeiden perusteella voidaan todeta, että Puolustusvoimien ohjeet ja normit sekä Suomen kansallinen lainsäädäntö on hyvinkin laaja kokonaisuus. Haastatteluissa korostettiin, että järjestelmän hyväksyttäminen on hyvinkin raskas dokumenttiorientoitunut prosessi. Tätä prosessia tulisi kehittää niin, että kyetään pitkäaikaisissa hankkeissa vastamaan riittävällä nopeudella teknologian kehitykseen. Tämän hetkinen hankkeen prosessimalli on jäykkä ja aiheuttaa sen, että järjestelmä valmistuessaan on kybersietoisuuden ja tekniikan näkökannalta vanhentunut. Normeja ja ohjeita tulee kehittää yhtenäisemmäksi siten, että kybersietoisuutta viedään paremmin normaaliksi osaksi järjestelmän kehittämistä sekä tuotettavia dokumentteja.

Uhkakuvia ajateltaessa kybertoimintaympäristö on jatkuvasti laajeneva kokonaisuus, joka ulottuu ihmisen joka päiväiseen toimintaan jollakin lailla. Lisäämällä turvallisuustietosuutta, joka saavutetaan lisäämällä kyberturvallisuuden

koulutusta. Lisäämällä kyberturvallisuuden koulutusta nostetaan myös kybersietoisuuden tiedostamista. Ensisijaisesti kysymys ei ole siitä, että pystytäänkö vihollisen pääsy järjestelmään perinteisen turvallisuusajattelun ja toimenpiteiden kautta estämään vaan siitä, että miten sen vähäisemmän tai laajemman vaikutuksen alla pystytään säilyttämään järjestelmän käytettävyys.

LÄHTEET

Bodeau, D., Graubart, R. & Bedford, M. 2011. Cyber Resiliency Engineering Framework. PDF-dokumentti. Saatavissa: https://www.mitre.org/sites/default/files/pdf/11_4436.pdf [Viitattu 3.1.2020].

Bodeau, D., Graubart, R. & Bedford, M. 2017. Cyber Resiliency Design Principles Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines Approved for Public Release; Distribution Unlimited. Case Number 17-0103. PDF-dokumentti. Saatavissa: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf [Viitattu 4.1.2021].

Graubart, R. 2016. The Risk Management Framework and Cyber Resiliency. PDF-dokumentti. Saatavissa: https://www.mitre.org/sites/default/files/publications/pr-16-0776-cyber-resiliency-and-the-risk-management-framework.pdf [Viitattu 10.4.2022].

Helsingin yliopisto 2020. Mitä resilienssi on? WWW-dokumentti. Helsingin yliopisto. Saatavissa: https://www2.helsinki.fi/fi/uutiset/koulutus-kasvatus-ja-oppiminen/mita-resilienssi-on [Viitattu 7.2.2021].

Hirsjärvi, S. & Hurme, H. 2017. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Gaudeamus [Viitattu 10.11.2021].

Hutchins, E., Cloppert, M. & Amin, R. 2011. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. PDF-dokumentti. Saatavissa: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Viitattu 9.4.2022].

Hyvönen, A.-E., Juntunen, T., Mikkola, H., Käpylä, J., Gustafsberg, H., Nyman, M., Rättilä, T., Virta, S. & Liljeroos, J. 2019. Kokonaisresilienssi ja turvallisuus: tasot, prosessit ja arviointi. Opinnäytetyö. PDF-dokumentti. Saatavissa: https://www.fiia.fi/wp-content/uploads/2019/02/17-2019-kokonaisresilienssi-ja-turvallisuus.pdf [Viitattu 7.2.2021].

Ivo, N. 2018. Hankintatoimintaan liittyvät riskit puolustusvoimien logistiikkalaitoksessa. Opinnäytetyö. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:amk-2018090414861 [Viitattu 10.4.2022].

Kananen, J. 2015. Kehittämistutkimuksen kirjoittamisen käytännön opas. Miten kirjoitan kehittämistutkimuksen vaihe vaiheelta. Jyväskylän ammattikorkeakoulun julkaisusarja [Viitattu 14.2.2021].

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona - Opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylän Ammattikorkeakoulun julkaisusarja [Viitattu 14.2.2021].

Kosola, J. 2007. Suorituskyvyn elinjakson hallinta. PDF-dokumentti. Maanpuolustuskorkeakoulu. Saatavissa: https://urn.fi/URN:NBN:fi-fe2019112744474 [Viitattu 7.10.2021].

Kosola, J. 2012. Puolustusvoimien projektiohje. PDF-dokumentti. Maanpuolustuskorkeakoulu. Saatavissa: https://urn.fi/URN:ISBN:978-951-25-2327-6 [Viitattu 15.1.2021].

Kosola, J. 2013. Vaatimustenhallinnan opas. PDF-dokumentti. Maanpuolustuskorkeakoulu. Saatavissa: https://urn.fi/URN:ISBN:978-951-25-2454-9 [Viitattu 20.8.2021].

Kott, A. & Linkov, I. 2018. *Cyber Resilience of Systems and Networks*. Springer.

Laari, T., Flyktman, J., Härmä, K., Timonen, J. &Tuovinen, J. (2019). #kyberpuolustus: kyberkäsikirja Puolustusvoimien henkilöstölle. PDF-dokumentti. Maanpuolustuskorkeakoulu. Saatavissa: https://urn.fi/URN:ISBN:978-951-25-3120-2 [Viitattu 16.2.2022].

Lagerblom, V.-P. (2014). ICT-varautumisen analyysi ja kehittäminen julkisen sektorin virastossa. Opinnäytetyö. PDF-dokumentti. Saatavissa: Veli-Pekka_Lagerblom_diplomityo_040314_FINAL_digi.pdf (lut.fi) [Viitattu 10.4.2022].

Lukka, K. 2001. Kari Lukka: Konstruktiivinen tutkimusote. WWW-dokumentti. METODIX. Saatavissa: https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/ [Viitattu 21.1.2021].

Nupponen, M. 2017. Harhauttaminen Venäjän sotilasoperaatioissa. Opinnäyte. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi-fe201708108080 [Viitattu 15.3.2021].

Pääesikunta 2014. PVOHJEK-PE SUORITUSKYVYN RAKENTAMINEN JA YLLÄPITO. (HK666 Liite 2).

Pääesikunta 2015a. PVOHJEK-PE PUOLUSTUSMATERIAALIN TEKNINEN HYVÄKSYNTÄ Liite 1. (HL609).

Pääesikunta 2015b. PVOHJEK-PE PUOLUSTUSVOIMIEN TURVALLISUUS. (HL205).

Pääesikunta 2017a. PVOHJEK-PE HANKEOHJE. (HN918).

Pääesikunta 2017b. PVOHJEK-PE VAATIMUSTENHALLINTA SUORITUSKYVYN RAKENTAMISESSA JA YLLÄPIDOSSA. (HN919).

Pääesikunta 2018a. PVOHJEK-PE SOTILAALLISEN SUORITUSKYVYN KÄSITEMALLI. (HO46).

Pääesikunta 2018b. PVOHJEK-PE SOTILAALLISEN SUORITUSKYVYN KÄSITEMALLI. (HO46 LIITE A).

Pääesikunta 2020a. PVOHJEK-PE JOUKON JA JÄRJESTELMÄN ELINJAKSONHALLINTA. (HQ496).

Pääesikunta 2020b. PVHSM 4.2.3.2 TIETOHALLINTO 047 - KYBERSIETOISUUDEN VARMISTAMINEN JÄRJESTELMISSÄ. (HQ928).

Pääesikunta 2020c. PVHSM 4.2.3.2 TIETOHALLINTO 036 ICT-VARAUTUMINEN PUOLUSTUSVOIMISSA. (HQ731, Liite 1 Määritelmät).

Pääesikunta 2021a. PVOHJEK-PE PUOLUSTUSVOIMIEN SISÄINEN VALVONTA JA RISKIENHALLINTA. (HR177).

Pääesikunta 2021b. RISKIENHALLINNAN TOTEUTTAMINEN. (HR177 Liite 2).

Puolustusvoimat 2021. Strategiset suorituskykyhankkeet - Puolustusvoimat. WWW-dokumentti. Saatavissa: https://puolustusvoimat.fi/strategiset-hankkeet [Viitattu 16.1.2021].

Puolustusvoimat 2022. Sotilasalan standardisointi Puolustusvoimissa. WWW-dokumentti. Saatavissa: https://puolustusvoimat.fi/kansainvalinen-toiminta/sotilasalan-standardisointi [Viitattu 12.4.2022].

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. & McQuaid, R. 2021. Developing cyber resilient systems: *NIST Special Publication*, PDF-dokumetti. Saatavissa: https://doi.org/10.6028/NIST.SP.800-160v2r1 [Viitattu 10.4.2022].

Sanastokeskus 2021. TEPA-hakutulos erikoisalojen sanastoista ja sanakirjoista. WWW-dokumentti. Saatavissa: https://termipankki.fi/tepa/fi/ [Viitattu 20.8.2021].

Saulio, L. 2012. Turvallisuus puolustusvoimien turvaluokiteltua tietoa sisältävissä rakennushankkeissa. Opinnäyte. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi-fe201206186042 [Viitattu 10.1.2021].

Simi, L. 2010. Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus. Opinnäytetyö. PDF-dokumentti. Saatavissa: https://aaltodoc.aalto.fi/bitstream/handle/123456789/99/urn100170.pdf?sequence=1&isAllowed=y [Viitattu 11.1.2021].

Suomen standardisoimisliitto 2022. Tiedätkö mikä on standardi? WWW-dokumentti. Saatavissa: https://sfs.fi/standardeista/mika-on-standardi/ [Viitattu 12.4.2022].

ISO/IEC 27032. 2012. Information technology – Security techniques – Guidelines for cybersecurity.

SFS-ISO 27001. 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

SFS-ISO 27005. 2018. Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskienhallinta.

SFS-ISO 31000. 2018. Riskienhallinta. Ohjeet.

SFS-ISO 31010. 2019. Riskienhallinta. Riskien arviointimenetelmät.

Tolkki, T. 2020. Hankkeiden turvallisuuden kehittäminen Puolustusvoimissa. Opinnäyte. WWW-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:amk-2020123030055 [Viitattu 15.1.2021].

Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. PDF-dokumentti. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyber-turvallisuuden-sanasto.pdf [Viitattu 10.1.2021].

Valtionneuvosto 2021. Valtioneuvoston puolustusselonteko. PDF-dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163405/VN_2021_78.pdf?sequence=4&isAllowed=y [Viitattu 7.4.2022].

Valtionvarainministeriö 2012. ICT -varautumisen vaatimukset. PDF-dokumentti. Saatavissa: https://vm.fi/documents/10623/307669/ICT-varautumisen+vaatimukset/9fa21bee-efcc-485a-8677-4eb4e0a2fa1f/ICT-varautumisen+vaatimukset.pdf [Viitattu 7.3.2022].

Valtionvarainministeriö 2017. Ohje riskienhallintaan Julkisen hallinnon ICT. PDF-dokumentti. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y [Viitattu 10.3.2021].

Walkowski, D. 2019. What Is The CIA Triad? WWW-dokumentti. Saatavissa: https://www.f5.com/labs/articles/education/what-is-the-cia-triad [Viitattu 20.4.2022].

Liite 1

Saate haastatteluun osallistumisesta

Hei,

Opiskelen insinöörin ylempää ammattikorkeakoulututkintoa (YAMK) Kaakkois-Suomen ammattikorkeakoulun Master's Degree Programme in Cybersecurity ja teen opinnäytetyötä, jonka aiheena on "Kybersietoisuus hankkeen elinkaaressa. Opinnäytetyö on kehittämistutkimus, jossa kartoitetaan ulkomaalaisia tutkimusasiakirjoja sekä kirjallisia lähteitä, jotka ovat pääsääntöisesti standardeja, Puolustusvoimien normeja ja ohjeita. Tutkittavana ilmiönä ja käsitteenä on kybersietoisuus. Opinnäytetyön tavoitteena on selvittää parhaat toimenpiteet, joita hankehenkilöstö ovat kehittäneet hankkeen aikana sekä tunnistaa mahdollisesti kehitettävät ja painotettavat osa-alueet hankehenkilöstön osaamisesta. Lopputuotoksena teemahaastattelun pohjalta opinnäytetyötä voidaan käyttää kybersietoisuuden huomioiminen hankkeissa opetustilaisuudessa.

Opinnäytetyöhön on haettu ja myönnetty tutkimuslupa. Opinnäytetyön ohjaajina toimivat lehtori Marko Oras ja Kapteeni Antton Halme.

Pyytäisin teiltä mahdollisuutta päästä vastaamaan hanke ja projektien asiantuntijana?

Haastattelut tulen toteuttamaan yksilöhaastatteluna Skypen välityksellä tai voitte vastata Webropol-kyselyyn (linkki alla), miten teidän aikatauluun vain suinkin sopii. Haastattelut Skypen välityksellä tulen nauhoittamaan sekä tekemään omia muistiinpanoja. Opinnäytetyön tietoturvaluokka on julkinen, joten työssä ei tulla käsittelemään salassa pidettäviä osioita. Kybersietoisuuden parhaita käytäntöjä tarkastellaan pääasiassa käytänteiden näkökulmasta eikä niinkään teknisten ratkaisujen tai ominaisuuksien toteutuksesta. Kaikki saadut tiedot ovat luottamuksellisia ja aineistoa tullaan käsittelemään niin, että haastateltavien anonymiteetti säilyy. Työn valmistuttua kirjoitetut sähköpostivastaukset, tallenteet ja kirjoitetut muistiinpanot hävitetään asianmukaisesti.

Suunnitelmani on valmistua vielä tämän vuoden puolella, joten pyydän teiltä pikaista vastausta tähän viestiin. Aikataulussa on omalta osaltani joustovaraa Skype haastattelun pitämiseen marraskuun loppuun asti, jonka jälkeen alkaa viimeiset pääsotaharjoitukset ja joululomat.

Toivon, että aiheeni herättää kiinnostusta ja halua osallistua siihen. Osallistuminen antaa arvokasta tietoa hankkeen ja projektien kybersietoisuuden parhaista käytänteistä ja tämän avulla voidaan kehittää hanke-, ja projektihenkilöstön osaamista kybersietoisuudesta.

Linkki Webropol-kyselyyn:
https://link.webropolsurveys.com/S/CD6740FF94044E2C
Salasana: #Kysi2021
Vastausaikaa kyselyyn on 28.11.2021 klo 23:59.

Kyselyn ja haastattelun alustus

Hei ja kiitos, että osallistut tähän kyselyyn.

Opinnäytetyöni on kehittämistutkimus, jossa kartoitetaan ulkomaalaisia tutkimusasiakirjoja sekä kirjallisia lähteitä, jotka ovat pääsääntöisesti Puolustusvoimien normeja, ohjeita ja standardeja. Kyselyn tarkoituksena on selvittää parhaat toimenpiteet, joita hankehenkilöstö ovat kehittäneet hankkeen aikana sekä tunnistaa mahdollisesti kehitettävät ja painotettavat osa-alueet henkilöstön osaamisesta. Lopputuotoksena kyselyn tuloksia voidaan käyttää kybersietoisuuden huomioiminen opetustilaisuudessa.

Tutkittavana ilmiönä ja käsitteenä on kybersietoisuus, joka viittaa järjestelmän kykyyn, kuinka kohdata, absorboida, palautua ja mukautua, kun kyberhyökkäys on heikentänyt järjestelmän toimivuutta. Joten kybersietoisuuden suunnittelua voidaan toteuttaa järjestelmän käytettävyyden ja jatkuvuudenhallinnan kautta. Sotilaallisessa kontekstissa järjestelmiä tarkastellaan käytettävyyden näkökulmasta, jolloin kybersietoisuutta voidaan käyttää järjestelmän hyvyyttä mittaavana suureena ja kyvykkyytenä. Jatkuvuudenhallinnan tarkoituksena on varautua häiriötilanteita varten ja järjestelmä kykenee suorittamaan kriittiset toiminnot, vaikka sen toimivuus on heikentynyt. Lähteiden mukaan kybersietoisuuden arviointi ja suunnittelu suositellaan perustuvan aina riskienarviointiin, joka sisältyy Puolustusvoimien hankkeisiin, projektitoimintaan ja prosesseihin. Vaatimustenhallinta on osa järjestelmän elinkaarta ja täten myös osa hanketta, jonka tarkoituksena on mahdollistaa menetelmät analysoida järjestelmälle asetetuista perusteista.

Opinnäytetyön tietoturvaluokka on julkinen, joten työssä ei tulla käsittelemään salassa pidettäviä osioita. Kybersietoisuuden toteutusta tarkastellaan parhaiden käytänteiden näkökulmasta eikä niinkään teknisten ratkaisujen tai ominaisuuksien toteutuksesta. Kaikki saadut tiedot ovat luottamuksellisia ja aineistoa tullaan käsittelemään niin, että kyselyyn osallistuvien anonymiteetti halutessaan säilyy. Kyselyn lopussa on erikseen osio, jossa voit jättää yhteystietosi ja suostumuksesi osallistumisesi julkaisemisesta.

Kyselyssä keskitytään tiettyihin ennalta määritettyihin teemoihin, joita on tarkennettu muutamalla täydentävällä kysymyksellä. Teemojen etuna on se, että tämä ei sido kyselyä tiettyyn formaattiin ja kysely etenee tiettyjen keskeisten teemojen varassa. Teemat valikoituivat tutkijan käyttämästä teoriapohjasta ja näin ollen tutkija varmistaa, että teemat ovat kaikille kyselyyn osallistuville samat.

Ystävällisin terveisin!
Insltn Markus Ketonen

Teemahaastattelurunko

Haastattelut ja kyselyt toteutetaan puolistrukturoituna teemoina, jonka avulla tutkija pyrkii ymmärtämään ja saamaan käsityksen tutkimuksen kohteena olevasta ilmiöstä. Tutkittavana ilmiönä ja käsitteenä on kybersietoisuus. Opinnäytetyön tavoitteena on selvittää Puolustusvoimien hankkeen elinjaksojen hallintaprosessin toiminta ja tuottaa uutta, luotettavaa tietoa kehittämään kybersietoisuuden huomioimisesta hankkeen toiminnassa.

Haastattelun tarkoituksena on keskittyä tiettyihin teemoihin, joista keskustellaan avoimesti ja tarkennetaan muutamalla täydentävällä kysymyksellä. Teemahaastattelulla on se etu, että se ei sido sitä tiettyyn formaattiin ja keskustelu etenee tiettyjen keskeisten teemojen varassa. Teemat valikoituivat tutkijan käyttämästä teoriapohjasta ja näin ollen tutkija varmistaa, että teemat ovat kaikille haasteltaville samat.

Käsiteltävät teemat:

Esittely

- Kuvaile yleisesti oma kokemuksesi hankkeista ja projekteista?

Teema 1: Kybersietoisuuden määritelmä

Yleistä hankkeesta ja kybersietoisuudesta:

- Kuvaile miten itse ymmärrät kybersietoisuuden ja merkityksen hankkeessa?
- Mitkä ovat omasta näkökulmastasi kybersietoisuuden tärkeimmät tavoitteet?

Teema 2: Riskienhallinta, käytettävyys ja jatkuvuudenhallinta osana kybersietoisuutta

Riskienhallinnan, käytettävyyden ja jatkuvuudenhallinnan merkitys järjestelmän elinkaaressa:

- Kuvaile näkemystäsi järjestelmän elinkaaressa, missä vaiheessa ja miten kybersietoisuus tulee huomioida?
- Esimerkkeinä riskienhallinta, vaatimustenmäärittely, käytettävyys ja jatkuvuudenhallinta
- Järjestelmän elinkaarella tarkoitetaan vaiheita konseptista aina luopumiseen saakka

Teema 3: Kybersietoisuuden kehittäminen hankkeessa

Haasteet järjestelmän kybersietoisuuden toteuttamisessa:

- Kuvaile minkälaisia haasteita olet kohdannut ja miten olet ratkaissut ne?
- Kuvaile esimerkkien kautta?

Kehittämisehdotuksia:

- Kuvaile miten kybersietoisuuden huomioimista hankkeen elinkaaressa voidaan kehittää?

Tutkimuslupa

1. PESUUNNOS:n määräys HM751/18.1.2017, Tutkimusluvat puolustusvoimissa

2. RPR/SLRR hakemus DR1063/11.2.2021, Tutkimuslupahakemus (Markus Ketonen)

HALLINTOPÄÄTÖS TUTKIMUSLUPA (MARKUS KETONEN)

1 Hakemuksesta

Rannikkoprikaatissa, Suomenlinnan Rannikkorykmentissä palveleva insinööriluutnantti Markus Ketonen on toisena viiteasiakirjana olevalla hakemuksella hakenut tutkimuslupaa Merivoimien esikunnalta liittyen opinnäytetyön tekemiseen osana ylempää ammattikorkeakoulututkintoa Kotkan ammattikorkeakoulussa. (Master's Degree Programme in Cybersecurity 1910462)

Tutkimuksen aiheena on ”Kybersietoisuuden huomioiminen hankkeissa”

Tutkimuksessa etsitään vastausta siihen mitä kybersietoisuus tarkoittaa ja miten kybersietoisuus liittyy ja jakautuu hankkeen eri vaiheisiin (valmistelu, suunnittelu, toteutus ja päättäminen)

Ketosen tutkimuslupahakemuksen tarkentavat tiedot, joihin sisältyy myös tutkimussuunnitelma, on tämän asiakirjan liitetiedostona.

2 Päätös

Ensimmäisen viiteasiakirjan mukaisesti puolustushaaraesikunnat ratkaisevat puolustushaaraa ja sen alaisia hallintoyksiköitä koskevat lupahakemukset. Puolustushaaraesikunnissa lupahakemuksen käsittelystä vastaa työjärjestyksessä määrätty esikunnan osasto.

Tällä päätöksellä Merivoimien esikunta myöntää Markus Ketoselle tutkimusluvan seuraavin ehdoin:

- Tutkimuslupa koskee ainoastaan hakemuksessa esitettyä tutkimusta. Lupa on voimassa myöntämispäivämäärästä alkaen korkeintaan viisi vuotta.
- Lupa koskee tässä asiakirjassa ja siihen välittömästi liittyvässä tutkimussuunnitelmassa tarkoitetun tutkimuksen suorittamista. Puolustusvoimien aineistoa ei saa käyttää muihin tarkoituksiin.
- Kertyvää tutkimusaineistoa tulee säilyttää ja käsitellä hyvän tutkimusetiikan ja asiakirjahallintoa koskevien ohjeiden mukaisesti.

– Aineiston keräämiseen liittyvä haastattelutoiminta / tiedonkeruu tulee toteuttaa siten, ettei se häiritse kohderyhmän työtehtäviä kohtuuttomasti.

– Mahdollinen salassa pidettävä aineisto sijoitetaan erillisiin liitteisiin, joita ei luovuteta oppilaitokselle. Turvaluokiteltua aineistoa saa esitellä puolustusvoimien ulkopuolisesta henkilöstöstä vain opinnäytetyön ohjaajalle ja arvioitsijalle. Kyseinen aineisto taltioidaan ainoastaan puolustusvoimien arkistointijärjestelmään asiakirjahallintoa koskevien ohjeiden mukaisesti.

– Tämän luvan päätösnumero DR1693 on mainittava kaikissa aineistosta tehdyissä tutkimusraporteissa.

– Valmis tutkimusraportti tulee toimittaa myös Merivoimien esikuntaan operatiiviselle osastolle tutkimuksen mahdollista hyödyntämistä varten.

– Tämän luvan ehtojen rikkomisesta seuraa luvan kumoaminen ja asian oikeudellinen arviointi.

3 Muutoksenhaku ja valitusosoitus

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

4 Lisätietoja

Asiaa Merivoimien esikunnassa hoitaa yliluutnantti Petri Eronen.

Henkilöstöpäällikkö

Kommodori Patrik Lillqvist

Koulutuspäällikkö

Komentaja Mika Mäkilevo

Tämä asiakirja on sähköisesti allekirjoitettu.

LIITTEET 1. Tutkimussuunnitelma

2. Valitusosoitus