LAUREA AMMATTIKORKEAKOULU Uuden edellä

Turvallisuusluokitellun tiedon suojaaminen palveluhankintojen tarjouslaskentavaiheessa

Case: Puolustushallinnon rakennuslaitos, Etelä-Suomen alueyksikkö

Herranen, Tuomas

2013 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Turvallisuusluokitellun tiedon suojaaminen palveluhankintojen tarjouslaskentavaiheessa

Case: Puolustushallinnon rakennuslaitos, Etelä-Suomen alueyksikkö

Tuomas Herranen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Lokakuu, 2013

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Tuomas Herranen

Turvallisuusluokitellun tiedon suojaaminen palveluhankintojen tarjouslaskentavaiheessa

Case: Puolustushallinnon rakennuslaitos, Etelä-Suomen alueyksikkö

Vuosi 2013 Sivumäärä 66

Puolustushallinnon rakennuslaitos vastaa puolustushallinnon kiinteistötoimen asiantuntija- ja hanketehtävistä sekä palvelutuotannon järjestämisestä. Laitoksen Etelä-Suomen alueyksikkö on vastuussa puolustushallinnon kiinteistöpalveluista Etelä-Suomen Sotilaslääänin alueella ja sen edustalla Suomenlahden Meripuolustusalueen saarissa. Alueyksikkö joutuu luovuttamaan turvallisuusluokiteltua tietoa sidosryhmilleen palveluhankintojen tarjouslaskentavaiheessa. Tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa maanpuolustukselle. Kun turvallisuusluokiteltu asiakirja luovutetaan vastaanottajalle, se siirtyy tietosisältöineen vastaanottajan hallintaan kaikkine siihen liittyvine velvollisuuksineen. Alueyksikön on pyrittävä varmistumaan, että sen sidosryhmät suojaavat niille luovutetun tiedon asianmukaisesti.

Tämän tapaustutkimuksen päätavoitteena on tuottaa informaatiota, jota käytäntöön soveltamalla Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikkö pystyy luomaan tarkoituksenmukaiset ja tehokkaat tiedon suojausvaatimukset palveluhankintojen tarjouslaskentavaiheeseen. Samalla tutkimuksessa tarkastellaan Kansallisen turvallisuusauditointikriteeristön (KATAKRI) kriteerien käytettävyyttä palveluhankintojen tarjouslaskentavaiheen turvallisuusjärjestelyissä.

Ei ole yksiselitteisesti määritelty, miten puolustusvoimien turvallisuusluokiteltua tietoa tulisi suojata sidosryhmien kanssa tehtävässä yhteistyössä. Absoluuttista totuutta siitä, milloin turvallisuusluokiteltu tieto on riittävästi suojattu, on hankala määritellä ja vielä hankalampi mitata. Kun etsitään riittäviä, mutta mahdollisimman kustannustehokkaita tiedon suojauskeinoja, on tärkeää selvittää tarjousprosessien parissa työskentelevien asiantuntijoiden omia kokemuksia siitä, miten turvallisuusluokitellun tiedon suojausvaatimukset vaikuttavat hankintaprosessiin.

Tutkimusongelmaa lähestytään fenomenologis-hermeneuttisesta näkökulmasta. Fenomenologiassa ollaan kiinnostuneita ihmisten kokemusmaailmoista. Tutkimuksessa selvitetäänkin haastatteluaineistoa laadullisesti analysoimalla, palveluhankintojen parissa työskentelevien asiantuntijoiden omaa suhtautumista tutkittavaan ilmiöön. Lisäksi tutkija pyrkii aktiivisesti tekemään tulkintoja käsiteltävästä haastatteluaineistosta oman esiymmärryksensä pohjalta ja siten kuljettamaan lukijaa hermeneuttisella kehällä kohti ymmärtämiseen sekä merkityksenantoon tähtäävää ulottuvuutta.

Tämän tutkimuksen perusteella voidaan todeta, ettei KATAKRI:n täysmääräinen käyttäminen ole järkevää puolustusvoimien turvallisuusluokiteltua tietoa sisältävien palveluhankintojen tarjouslaskentavaiheessa. KATAKRI:n kriteerien käyttäminen sovelletusti, yhteistyön laatu ja syvyys huomioon ottaen, on kuitenkin perusteltua. KATAKRI:n kriteerit ovat nimittäin helposti ennakoitavissa ja yhtenäistävät viranomaisten vaihtelevia käytäntöjä. Ehdotus turvallisuusluokitellun tiedon suojausvaatimuksiksi palveluhankintojen tarjouslaskentavaiheeseen on esitetty liitteessä 6.

Asiasanat: Puolustushallinnon rakennuslaitos, puolustusvoimat, palveluhankinta, tarjouslaskenta, turvallisuusluokiteltu tieto, suojausvaatimukset, Kansallinen turvallisuusauditointikriteeristö

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Security Management

Herranen, Tuomas

Protecting Classified Information in the RFQ Phase of Service Procurement: a Case Study of Construction Establishment of Defense Administration

Year 2013 Pages 66

The Construction Establishment of Defense Administration is in charge of expert and procurement tasks of the Finnish Defense Forces' real estate administration, as well as of the organization of service production. The Southern Regional Unit (SRU) is responsible for property maintenance in the area of Southern Military Command including the isles in the Gulf of Finland. SRU is compelled to hand over classified information (CI) to different stakeholders during the Request for Quotation (RFQ) phase of service procurement. Unauthorized disclosure of CI can damage the Defense Forces. If a classified document is handed over to a stakeholder, the responsibility to protect the document lies upon its shoulders. Nevertheless, the SRU must ensure that the stakeholders are able to provide sufficient safeguards to protect the CI.

The main objective of this case study is to provide such knowledge that the SRU can apply into practice when building sufficient and effective safeguards during the RFQ phase of public service procurement. The usability of the National Security Audit criteria as the foundation of security measures during the RFQ phase is examined in the process.

It is not unambiguously determined how the CI should be protected when working with stakeholders. It is hard to define the absolute truth when the protective safeguards are strong enough and it is even harder to measure it. In the search for sufficient yet cost-effective safeguards, it is important to analyze the opinions of the experts in the field of service procurement. It is also important to investigate how the safeguards affect the procurement process as a whole.

In this study, the research problem is examined in the light of phenomenological and hermeneutic traditions. Phenomenology is the study of structures of consciousness as experienced from the first-person point of view. The interview data is analyzed with qualitative methods, in order to shed light on the attitudes of the experts concerning safeguarding CI. The researcher interprets the interview data based on his pre-reflective assumptions. Such an approach is often used in hermeneutic tradition in order to move downwards along the hermeneutic circle towards understanding and relevance.

This study shows that it is not practical to follow National Security Audit criteria letter by letter during the RFQ phase of service procurement. Instead, it is rational to use certain requirements in National Security Audit criteria considering the level and depth of co-operation with the stakeholders. The requirements in National Security Audit criteria are easy to anticipate and they unify the varying practices of different Finnish authorities. In appendix 6 there is a proposal (in Finnish) for what requirements should be put in place in order to set up sufficient safeguards for CI during the RFQ phase of service procurement.

Keywords: Construction Establishment of Defense Administration, Finnish Defense Forces, service procurement, RFQ-phase, classified information, safeguards, National Security Audit criteria

Sisällys

1 Johdanto

Tämä tapaustutkimus käsittelee puolustusvoimien turvallisuusluokitellun tiedon suojaamista Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikön kilpailuttamien palveluhankintojen tarjouslaskentavaiheessa. Alueyksikön on pystyttävä takaamaan hallinnoimansa tiedon luottamuksellisuus silloin, kun se luovuttaa tietoa sidosryhmilleen palveluhankintojen yhteydessä. Käytännössä tietoja luovutetaan organisaation ulkopuolelle ensimmäisen kerran hankintojen tarjouslaskentavaiheessa. Vaiheeseen osallistuville ehdokkaille luovutetaan tarjouslaskenta-aineisto, jonka suojausvaatimuksiin tämä tutkimus keskittyy.

Ylimitoitetuista suojausvaatimuksista johtuvat liialliset turvallisuusjärjestelyt palveluhankintojen tarjouslaskentavaiheessa voivat aiheuttaa lisäkustannuksia ja -töitä palvelun tarjoajille. Tilaaja, puolustusvoimat, saattaa joutua maksamaan niistä aiheutuvan kokonaiskustannusten nousun lopulta palvelun hinnassa. Lisäksi potentiaalisia palvelun tarjoajia saattaa jättäytyä ulos kilpailutuksesta, jolloin markkinoilla olevaa kilpailua ei välttämättä pystytä hyödyntämään täysmääräisesti.

Tutkimus rakentuu seuraavasti. Ensimmäisessä luvussa kuvataan tutkimuksen rakenne. Luku kaksi valottaa tutkimuksen taustaa ja aihepiiristä aikaisemmin tehtyä tutkimusta. Luvut kolme ja neljä käsittelevät puolestaan tutkimuksen tietoteoreettisia perusteita ja niitä metodologisia valintoja, joiden kautta tutkimusongelmaa lähestytään. Tutkimuksen luvuissa viisi kuvataan palveluhankintaprosessi ja luvussa kuusi kartoitetaan asiantuntijahaastatteluin sen turvallisuusjärjestelyiden kanssa töitä tekevien henkilöiden kokemuksia siitä, miten turvallisuusluokitellun tarjouslaskenta-aineiston suojausvaatimukset vaikuttavat koko prosessin etenemiseen.

Haastatteluaineistoa laadullisesti analysoimalla pohditaan Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikön julkisten palveluhankintojen tarjouslaskentavaiheen turvallisuusjärjestelyjen tarkoituksenmukaisuutta sekä Kansallisen turvallisuusauditointikriteeristön (KATAKRI) kriteerien käytettävyyttä tarjouslaskenta-aineiston suojausvaatimusten perustana. Johtopäätökset esitellään luvussa seitsemän ja ehdotus turvallisuusluokitellun tiedon suojausvaatimuksiksi palveluhankintojen tarjouslaskentavaiheeseen on esitetty liitteessä 6.

Tämä opinnäytetyö on tapaustutkimus, joten sen tuloksista ei tulisi tehdä yleistyksiä. Tapauksen valintaa ohjaa kuitenkin kiinnostus niin tietoturvallisuutta kuin turvallisuusluokitellun tiedon suojausvaatimuksia kohtaan monimutkaisissa hankintaketjuissa. Teoreettisena ilmiönä tapaus edustaa hyvin molempia aihealueita. Tutkimuksessa käytetyt tärkeimmät käsitteet on määritelty liitteessä 1 ja aihepiiriin olennaisesti liittyvä lainsäädäntö on kuvattu liitteessä 2.

2 Tutkimuksen tausta

Hallituksen esityksen yleisperusteluissa laiksi viranomaisten toiminnan julkisuudesta todetaan, että oikeutta saada tietoja viranomaisten toiminnasta voidaan pitää keskeisenä yksilöiden perusoikeutena. Julkisuusperiaate ei kuitenkaan Suomessa, kuten ei muissakaan maissa, merkitse yksilöiden ehdotonta oikeutta tiedon saantiin. Silloin tällöin julkisuuden on väistyttävä muiden yhteiskunnallisesti tärkeiden syiden vuoksi. (HE 30/1998 luku 3.1.)

Monet Puolustushallinnon rakennuslaitoksen hallinnoimat asiakirjat on määritelty salassa pidettäviksi ja turvallisuusluokiteltu viranomaisten toiminnan julkisuudesta annetun lain (621/1999, julkisuuslaki) perusteella. Palveluhankinnan sisältäessä turvallisuusluokiteltua tietoa, julkisuusperiaatteen ja yhteiskunnallisesti tärkeiden syiden nojalla salassa pidettäväksi määritellyn tiedon välille muodostuu jännite. Turvallisuusluokiteltu tieto kuuluu puolustusvoimille, sitä hallinnoi Puolustushallinnon rakennuslaitos ja palvelun toteuttamiseen sitä tarvitsee palvelua tarjoava yritys. Onnistunut hankinta on vuorovaikutteinen prosessi, joka edellyttää selkeätä vastuunjakoa tilaajan, hankkijan ja palvelun tuottajan kesken.

Kuva 1 Onnistunut hankinta

Puolustushallinnon rakennuslaitoksen hallinnoimien turvallisuusluokiteltujen asiakirjojen salassapitointressi, eli syy miksi asiakirjassa olevaa tietoa halutaan suojata, perustuu suoraan Suomen lainsäädäntöön ja julkisuuslakiin. Asiakirjojen salassapitotahto ilmaistaan viranomaisympäristössä asiakirjojen luokitteluna. Salassa pidettävät viranomaisen asiakirjat on määritelty pääosin julkisuuslain 24 §:ssä ja niiden luokittelusta säädetään tietoturvallisuudesta valtiohallinnossa annetun valtioneuvoston asetuksen (681/2010¸ tietoturva-asetus) 3 luvussa.

Salassa pidettävien viranomaisten asiakirjojen salassapitointressi ja -tahto on siis kohtuullisen helppo osoittaa, mikäli viranomainen vain osaa tunnistaa salassa pidettävän tiedon ja luokitella sen oikein. Tiedon tosiasiallinen salassapito, jolla tässä tutkimuksessa tarkoitetaan kaikkia salassa pidettävään tietoon kohdistettavia suojaustoimenpiteitä, joilla yritetään estää sen oikeudeton paljastuminen, ei kuitenkaan ole yhtä mutkatonta. Usein tiedon luottamuksellisuutta ja eheyttä suojattaessa tiedon saatavuus voi kärsiä. Tiedon suojaaminen myös maksaa, sillä riittävät turvallisuusjärjestelyt vaativat investointeja. Ongelmiin törmää helposti myös sidosryhmäyhteistyössä, kun tietoa joudutaan luovuttamaan organisaation ulkopuolelle. Yhteistyökumppaneihin luottaminen saattaa osoittautua hankalaksi, jos niiden valmiudesta käsitellä ja suojata salassa pidettävää tietoa ei pystytä varmistumaan.

2.1 Puolustushallinnon rakennuslaitos

1990-luvulla valtiohallinnossa yhtiöitettiin tai ”laitostettiin” parikymmentä virastoa, eikä valtion kiinteistösektorikaan selvinnyt tästä toimintojen tehostamiseen tähdänneestä ajanjaksosta muutoksitta. Vuonna 1992 tehdyssä valtion rakennustoiminnan tehokkuuden parantamista tarkastelleessa selvityksessä päädyttiin esittämään tuolloisen rakennushallituksen lopettamista. Valtion kiinteistöomaisuus hajautettiin 15 kiinteistöyksikölle, joista suurin oli Valtion kiinteistölaitos. Vuodesta 2001 se on tunnettu nimellä Senaatti-kiinteistöt. Puolustushallinnon kiinteistöt jäivät vielä tuolloin puolustusministeriön hallintaan. Niiden rakentamisesta, omistamisesta ja ylläpidosta vastasi puolustusministeriön kaksi erillistä osastoa: kiinteistö- ja rakennusosasto. (Helin 2002, 17.)

Vuonna 1994 puolustusministeriön rakennusosastosta ja puolustusvoimien alueellisesta kiinteistöorganisaatiosta muodostettiin puolustusministeriön alainen nettobudjetoitu virasto, Puolustushallinnon rakennuslaitos. Laitoksen oman palvelutuotannon toimintamalleja lähdettiin tuolloin kehittämään ja markkinoilta hankittavien palvelujen kilpailuttamismenettelyjä lisättiin. Keskeisin muutos tapahtui rakennuttamisen toimialalla vuonna 1998 laitoksen luopuessa kokonaan omasta rakentamisesta. Rakennuslaitoksen henkilöstömäärä väheni 10 ensimmäisen vuoden aikana 2 500:sta 1 300:aan palvelujen ulkoistamisen, toimintojen rationalisoimisen sekä varuskuntien lakkauttamisten takia. (Helin 2002, 19; Helin 2004, 16.)

Puolustushallinnon rakennuslaitoksen toiminta-ajatuksena on järjestää puolustushallinnolle parhaat kiinteistöpalvelut niin rauhan aikana kuin poikkeusoloissakin. Laitoksen asiakkaita ovat esimerkiksi puolustusvoimat, puolustusministeriö, Kruunuasunnot ja Senaatti-kiinteistöt. Laitoksen toimialoihin kuuluvat kiinteistö-, siivous-, energia-, rakennuttamis-, ympäristö- ja hallintopalvelut sekä tekniset palvelut. Rakennuslaitos toimii puolustushallinnon kiinteistö- ja ympäristöalan osaamiskeskuksena vastaten alan asiantuntija-, ja hankintatehtävistä sekä palvelutuotannon järjestämisestä. Vuonna 2012 laitoksen kokonaisliikevaihto oli 162,6 miljoonaa euroa ja sen palveluksessa oli 889 henkilöä. (Puolustushallinnon rakennuslaitos 2013a, 6-7.)

Rakennuslaitoksen keskusyksikön alaisuudessa toimivissa seitsemässä alueyksikössä hankitaan tai tuotetaan puolustusvoimille esimerkiksi asiantuntijatehtäviin, hankesuunnitteluun, varuskuntien kehittämis- ja alueidenkäyttösuunnitteluun, kiinteistönhoitoon, kunnossapitoon, energiahuoltoon, ympäristönsuojeluun ja tietohallintaan liittyviä palveluita. Lisäksi laitos tuottaa puolustusvoimille asukasisännöintipalveluja sekä puolustusvoimien käytössä olevien tilojen kiinteistövarallisuuden haltijoille rakennuttamis-, omistaja- ja asiantuntijapalveluita. Näissä palveluissa on otettu huomioon myös poikkeusolojen valmiusnäkökohdat. (Puolustushallinnon rakennuslaitos 2013b, 6.)

Puolustushallinnon rakennuslaitoksen Etelä-Suomen alue (myöhemmin PHRAKLE-S) vastaa puolustushallinnon kiinteistöpalveluista Etelä-Suomen Sotilaslääninalueella ja sen edustalla Suomenlahden Meripuolustusalueen saarissa. PHRAKLE-S:llä on noin 30 puolustushallinnon asiakasta, kuten: Puolustusministeriö, Pääesikunta, Etelä-Suomen Sotilaslääninin Esikunta, Suomenlahden Meripuolustusalueen Esikunta sekä näiden alaisia joukko-osastoja ja laitoksia. PHRAKLE-S:n toimipisteet sijaitsevat varuskunnissa Helsingissä, Kirkkonummella, Tammisaaressa ja Tuusulassa. (Puolustushallinnon rakennuslaitos 2012.)

2.2 Tietoturvallisuuden merkitys Puolustushallinnon rakennuslaitoksessa

Puolustushallinnon rakennuslaitoksen tärkein suojattava omaisuus on sen hallinnassa oleva tieto. Johtuen roolistaan puolustushallinnon ja ennen kaikkea puolustusvoimien kiinteistönhoidon, kunnossapidon ja alueidenkäytön suunnitellussa, sen käyttöön luovutetaan maanpuolustuksen kannalta merkittävää tietoa, joka on usein turvallisuusluokiteltu. Tiedon turvallisuusluokittelun perusteisiin pureudutaan tarkemmin kappaleessa 2.3.

Puolustushallinnon rakennuslaitoksen tulee pitää huolta niin omasta tietoturvallisuudestaan kuin sidosryhmäturvallisuuden toteutuksesta myös sen hallinnoimissa hankkeissa ja -hankinnoissa (Puolustusministeriö 2007, 19). Laitoksen on siis pystyttävä takaamaan hallinnoimansa tiedon luottamuksellisuus myös silloin, kun se luovuttaa tietoa sidosryhmilleen palveluhankintojen yhteydessä.

Puolustusministeriön osastrategiassa Puolustushallinnon turvallisuus (2009, 11) ennustetaan, että tietojärjestelmiin kohdistuvat uhkat yleistyvät ja voimistuvat tulevaisuudessa. Lisäksi strategiassa todetaan informaatioyhteiskunnan kehityksen ja informaatioteknologian sovellusten laaja-alaisen käyttöönoton lisäävän riippuvuutta herkästi haavoittuvista järjestelmistä. Yhteiskunnan turvallisuusstrategiassa (2010, 14) yhdeksi koko yhteiskunnan elintärkeitä toimintoja uhkaavaksi uhkamalliksi onkin mainittu tietoliikenteen ja tietojärjestelmien vakavat häiriöt eli kyberuhkat, jotka vaikutuksiltaan voivat olla hyvinkin laaja-alaisia. Kolme vuotta myöhemmin julkaistussa Suomen kyberturvallisuusstrategiassa (2013,18) todetaan, että Suomi on jo joutunut sellaisten kyberoperaatioiden kohteeksi, joiden painopiste on ollut kyberaktivismissa, -rikollisuudessa ja -vakoilussa. Kybertoimintaympäristö on muuttanut perinteisiä valta-asetelmia siten, että sekä pienten valtiollisten että ei valtiollisten toimijoiden mahdollisuudet toimia tehokkaasti ovat parantuneet. Kybermaailmassa suuruus ja massa eivät enää ole hallitsevia, vaan osaaminen (Suomen kyberturvallisuusstrategia 2013, 17.)

Kyberoperaation tai muun vahingonteon suorittaminen vaatii osaamisen lisäksi tietoa. Tietoa siitä, mistä tiloista käsin hallitaan mitäkin järjestelmiä ja mihin niillä pystytään vaikuttamaan. Perinteinen vakoilu ei ole menettänyt merkitystään tällaisten tietojen hankkimisessa (Puolustusministeriö 2009, 3). Tiedot voivat paljastua myös silkasta huolimattomuudesta, mikäli niitä ei ole tunnistettu salassa pidettäväksi, eikä niille ole osattu määrittää tarvittavia suojaustoimenpiteitä. Teknologian kehittyessä tiedon oikeanlaisen luokittelun, suojaamisen ja jakelun merkitys korostunee entisestään verkottuneissa yhteiskunnissa.

Jos turvallisuusluokiteltu tieto joutuu hankintaprosessin yhteydessä sellaisen henkilön haltuun, jolle se ei kuulu, voivat niin hankinnasta vastaava taho kuin palveluntuottajakin, syyllistyä rikoslaissa rangaistavaksi säädettyihin tekoihin. Rikoslain (39/1889) 40 luvun 5 §:ssä nimittäin säädetään että, mikäli viranomaisen palveluksessa oleva oikeudettomasti paljastaa palvelussuhteensa perusteella tietoonsa saaman salassa pidettävän asiakirjan tai tiedon tai käyttää tietoa hyväkseen tai toisen vahingoksi, voi teko täyttää virkasalaisuuden rikkomisen tunnusmerkistön. Teon ei tarvitse olla tahallinen, vaan huolimattomuudesta tapahtuvasta teosta voidaan rangaista tuottamuksellisena virkasalaisuuden rikkomisena. (Vapaavuori 2005, 136.)

Jos sidosryhmän edustaja puolestaan paljastaa oikeudettomasti palveluhankintaprosessin yhteydessä hänelle luovutettua turvallisuusluokiteltua tietoa, saattaa teko täyttää rikoslain 38 luvun 1§:n mukaisen salassapitorikoksen tunnusmerkistön. Tämä edellyttää, että ensinnäkin laissa tai asetuksessa on säädetty salassapitovelvollisuus tai viranomainen on lain nojalla määrännyt tällaisen. Lisäksi tekijä on asemassaan, toimessaan tai tehtävää suorittaessaan saanut tiedon salassa pidettävästä seikasta ja paljastaa sen tai käyttää sitä omaksi tai toisen hyödyksi. (Vapaavuori 2005, 109.)

Mikäli salassapitorikos olisi kokonaisuutena arvioiden vähäinen, voitaisiin teosta rangaista puolestaan rikoslain 38 luvun 2 §:n mukaisena salassapitorikkomuksena (Vapaavuori 2005, 111–113). Teon vaarantaessa valtion turvallisuutta tai jos tiedon hankkimisen taustalla voitaisiin katsoa olleen organisoitua tiedustelutoimintaa, myös teon rangaistavuusaste luonnollisesti kovenisi. Ankarimmillaan PHRAKLE-S:n hallinnoiman tiedon oikeudettomasta hankkimisesta, välittämisestä, luovuttamisesta, ilmaisemisesta tai julkistamisesta, käyttämisestä tai paljastamisesta olisi mahdollista joutua syytetyksi jopa rikoslain 12. luvun mukaisesta maanpetosrikoksesta. Maanpetosrikoksiin lukeutuvat esimerkiksi vakoilu, törkeä vakoilu, turvallisuussalaisuuden paljastaminen ja luvaton tiedustelutoiminta (Rikoslaki 12 luku, 5-9§).

Jotta tiedon oikeudettomasta paljastumisesta aiheutuvat vahingot voidaan minimoida, tulee tieto suojata. Tietoa suojaavien turvallisuusjärjestelyiden tulisi olla suhteessa tiedon paljastumisesta aiheutuvaan vahinkoon. Mitä suuremman vahingon tiedon paljastuminen aiheuttaa yksityiselle tai yleiselle edulle, sitä tiukemmin sitä pitää myös pyrkiä suojelemaan. Tiedon suojaustaso ja -tarve osoitetaan viranomaisympäristössä luokittelemalla tieto.

2.3 Tiedon salassapito ja turvallisuusluokittelu

Viranomaisen asiakirja on pidettävä salassa, jos se julkisuuslain tai muun lain perusteella on säädetty salassa pidettäväksi tai jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus (julkisuuslaki 6 luku, 22§). Salassa pidettävät asiakirjat tai niihin sisältyvät tiedot voidaan luokitella osoittamaan, minkälaisia tietoturvallisuutta koskevia vaatimuksia niiden käsittelyssä on tarpeen noudattaa. Luokiteltujen asiakirjojen käsittelyä ohjataan suojaustasojen avulla, jotka määritellään tietoturva-asetuksen 9 §:ssä. Sellaisiin salassa pidettäviin asiakirjoihin, joiden oikeudeton paljastuminen voi aiheuttaa joko vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle julkisuuslain 24 §:n 1 momentin 2 ja 7 – 10 kohdissa tarkoitetulla tavalla, voidaan tehdä erillinen turvallisuusluokitusmerkintä (tietoturva-asetus 3 luku, 11 §). Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004, kansainvälinen tietoturvallisuusvelvoite) 8§:n mukaan erityissuojattavaan tietoaineistoon on tehtävä turvallisuusluokittelumerkintä siitä riippumatta, mitä julkisuuslaissa tai sen nojalla säädetään.

Turvallisuusluokitusmerkintä voidaan tehdä esimerkiksi silloin kun asiakirja sisältää henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevia ja niiden toteuttamiseen vaikuttavia tietoja. Myös asiakirjat, jotka koskevat sotilastiedustelua, puolustusvoimien varustamista, kokoonpanoa, sijoitusta tai käyttöä voidaan turvallisuusluokitella. Lisäksi sotilaallista maanpuolustusta palvelevia keksintöjä, rakenteita, laitteita tai järjestelmiä taikka maanpuolustuksen kannalta muutoin merkityksellisiä kohteita

taikka puolustusvalmiuteen varautumista koskevat asiakirjat, voidaan varustaa turvallisuusluokitusmerkinnällä. (Julkisuuslaki 24 § 7-10k.). Turvallisuusluokitusmerkintää koskevista erityissäännöksistä säädetään tietoturva-asetuksen 11§:ssä. Tiedon suojaustasot ja turvallisuusluokkamerkinnät on kuvattu tarkemmin tämän opinnäytetyön liitteessä 3.

Turvallisuusluokiteltujen asiakirjojen asianmukainen suojaus tulisi pystyä takaamaan myös silloin, kun tietoa joudutaan luovuttamaan organisaation ulkopuolelle. Luokitellut asiakirjat tulee toimittaa vastaanottajalle suojaustason asettamien vaatimusten mukaisesti. Luokiteltu asiakirja tulee jakaa siten, etteivät sivulliset pääse käsiksi suojattavaan tietoon. Kun asiakirja luovutetaan vastaanottajalle, se siirtyy tietosisältöineen vastaanottajan hallintaan kaikkine siihen liittyvine oikeuksineen sekä velvollisuuksineen, jollei erityissäännöksistä muuta johdu (VAHTI 2/ 2010, 69–70). Hankintayksiköille onkin taattu julkisista hankinnoista annetun lain (348/2007, hankintalaki) 8 luvun 54 §:ssä mahdollisuus esittää ehdokkaiden tai tarjoajien rahoituksellista ja taloudellista tilannetta, teknistä suorituskykyä ja ammatillista pätevyyttä sekä laatua koskevia vaatimuksia sekä vaatia ehdokkaita ja tarjoajia esittämään niihin liittyviä selvityksiä.

Erilaisten selvitysten tekeminen vie aikaa ja saattaa pitkittää palveluhankinnan tarjouslaskentavaihetta. Selvitykset tarjoavat kuitenkin mahdollisuuden karsia ne ehdokkaat pois, joiden ei katsota soveltuvan palveluntuottajaksi. Edellyttämällä sellaista laadukasta turvallisuustoimintaa, jossa turvallisuusluokiteltu tieto on suojattu esitettyjen suojausvaatimusten mukaisesti, luodaan pohja tiedon tosiasialliselle salassapidolle myös palveluhankintojen tarjouslaskentavaiheessa.

2.4 Aikaisempi tutkimus

Puolustusvoimien turvallisuusluokitellun tiedon suojaamisesta palveluhankintojen yhteydessä ei ole Suomessa tehty julkista tieteellistä tutkimusta. Aihetta on käsitelty aikaisemmin majuri Jarmo Simin Teknillisen korkeakoulun turvallisuusjohdon koulutusohjemaan vuonna 2010 tekemässä tutkielmassa ”Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus” sekä kapteeni Lauri Saulion maasotalinjan esiupseerikurssille vuonna 2012 tekemässä tutkielmassa ”Turvallisuus puolustusvoimien turvaluokiteltua tietoa sisältävissä rakennushankkeissa”. Nämä työelämälähtöiset tutkielmat käsittelevät turvallisuusluokiteltua tietoa sisältävien hankintojen ja rakennushankkeiden turvallisuutta ohjaavaa lainsäädäntöä, normistoa ja niiden pohjalta laadittuja ohjeistuksia sekä eri toimijoiden turvallisuusvastuita ja -velvollisuuksia hankintaprosessien ja hankkeiden eri vaiheissa. Simi ei ota tutkielmassaan lainkaan kantaa hankintojen sidosryhmille aiheuttamiin turvallisuusvaatimuksiin. Saulio puolestaan tutkii eri osapuolten tehtäviä hyvin yleisellä tasolla sellaisissa rakennushankkeissa, joissa hankitaan ulkopuoliselta palveluntuottajalta tarvittava työsuoritus.

Simi etsii tutkielmassaan vastausta kysymykseen: ”mitkä ovat hankintaprosessin turvallisuustehtävät ja miten ne jakautuvat hankintaprosessin eri vaiheissa?”. Hänen tavoitteenaan on ollut määrittää turvallisuustehtävät ja vastuut hankintaprosessin eri vaiheissa. Simin (2010, 33) mielestä turvallisuuden tulee näkyä kaikissa hankintoihin liittyvässä toiminnassa, mutta sen ei tule olla itseisarvo vaan yksi osa hankintaprosessia. Turvallinen hankintaprosessi syntyy vain kaikkien toimijoiden jatkuvan ja oikea-aikaisen yhteistoiminnan tuloksena.

Saulio puolestaan selvittää omassa tutkielmassaan: ”Mitä turvallisuus tarkoittaa puolustusvoimien turvallisuusluokiteltua tietoa sisältävissä rakennushankkeissa?”. Tutkielman viitekehyksenä toimii sidosryhmän kanssa toteutettava rakennushanke, jonka turvallisuus koostuu Saulion (2012, 36) johtopäätösten perusteella monesta eri osatekijästä, kuten projektiorganisaation ammattitaidosta, eri osapuolten tunnistetuista vastuista, oikeilla perusteilla valituista palveluntuottajista, tehtävistä työsuorituksista, oikea-aikaisista päätöksistä, sopimuksista ja sopimusten valvomisesta.

Puolustushallinnon rakennuslaitosta on sen perustamisesta lähtien kehitetty puolustusvoimien tarpeita vastaavaksi asiantuntija- ja palvelujenhankintaorganisaatioksi, jolla omaa palvelutuotantoa on lähinnä kriisiajan puolustuskiinteistöissä, sekä tapauksissa, joissa palveluja ei ole voitu sijaintipaikkakunnalla järjestää vapaan kilpailun perusteella (Helin 2004, 16). Oman tuotannon ulkoistaminen ja siirtyminen markkinoilta hankittavien palvelujen kilpailuttamismenettelyihin ovat aiheuttaneet haasteita tietojen suojaamiselle. Puolustusvoimien turvallisuusluokiteltua tietoa on väistämättä jouduttu luovuttamaan rakennuslaitoksen sidosryhmille entistä enemmän. Tämä tapaustutkimus syventää edellä mainittujen aihepiiriin liittyvien tutkielmien tasoa. Tutkimus siirtyy koko ilmiötä kuvailevalta yleiseltä tasolta, palveluhankintojen tarjouslaskentavaihetta syvällisesti kuvaavalle eli deskriptiiviselle tasolle.

3 Tutkimusongelman asettelu

Tutkija suoritti korkeakouluharjoittelun Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikössä keväällä 2013. Yhtenä tehtävänä harjoittelujakson aikana oli perehtyä yksikön palveluhankintojen turvallisuusjärjestelyiden perusteisiin puolustusvoimien turvallisuusluokiteltua tietoa sisältävissä hankinnoissa.

PHRAKLE-S:ssä pyrittään takaamaan hankintakohtaisen turvallisuustason toteutuminen, mutta haluttaan välttää tilanne, jossa ylimitoitetuista turvallisuusjärjestelyistä saattaisi aiheutua varteenotettavien tarjoajien vähyyttä, kilpailun toimimattomuutta, tai kilpailutus- ja toimitusaikataulujen viivästymistä. Kehittääkseen palveluhankintojen turvallisuusjärjestelyjensä tehokkuutta ja palvelunsa laatua, PHRAKLE-S päätyi tämän opinnäytetyön avulla selvittämään

hankintojensa tarjouslaskentavaiheen turvallisuusjärjestelyjen tarkoituksenmukaisuutta puolustusvoimien turvallisuusluokiteltua tietoa sisältävissä hankinnoissa.

3.1 Tutkimuksen tavoite ja tutkimuskysymykset

Tämän opinnäytetyön päätavoitteena on tuottaa informaatiota, jota käytäntöön soveltamalla Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikkö pystyy luomaan tarkoituksenmukaiset tiedon suojausvaatimukset julkisten palveluhankintojen tarjouslaskentavaiheeseen. Kehittämällä PHRAKLE-S:n hankintojen turvallisuusjärjestelyitä opinnäytetyön tulosten perusteella, alueyksikkö pystyy varmistumaan hankintakohtaisen turvallisuustason toteutumisesta. Lisäksi sidosryhmien tasapuoliset mahdollisuudet hinnoitella ja tarjota palveluita paranevat, kun niiden on mahdollista arvioida palveluhankintojen tarjouslaskentavaiheen turvallisuusjärjestelyistä aiheutuvat kustannukset. Tutkimus tukee myös osaltaan ehdokkaiden ja tarjoajien syrjimätöntä kohtelua, kun turvallisuusluokitellun tiedon suojausvaatimukset ovat kaikkien osapuolien tiedossa heti hankintaprosessin alkuvaiheessa.

Tutkimuksen toisena päätavoitteena on tarkastella Kansallisen turvallisuusauditointikriteeristön kriteerien käytettävyyttä palveluhankintojen tarjouslaskentavaiheen turvallisuusjärjestelyissä. Tutkimuksen pääkysymys on: ”Mitkä ovat turvallisuusluokitellun tiedon suojausvaatimukset Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikön palveluhankintojen tarjouslaskentavaiheessa?”. Kysymykseen etsitään vastausta tarkastelemalla viiden asiantuntijan kokemuksia turvallisuusluokitellun tiedon suojaamisesta ja KATAKRI:n käytettävyydestä tarjouslaskentavaiheen suojausvaatimusten perustana.

Vastaamalla alakysymyksiin ”Mitkä ovat turvallisuusluokitellun tiedon suojausvaatimusten perusteet?” ja ”Mitkä ovat mahdollisia turvallisuusluokitellun tiedon oikeudettomasta paljastumisesta aiheutuvia seurauksia?” lukijaa pyritään kuljettamaan kohti ymmärtämiseen sekä merkityksenantoon tähtäävää ulottuvuutta. Koska tutkimuksen konteksti on kuvattu seikkaperäisesti, on lukijan mahdollista ymmärtää, miten turvallisuusluokitellun tiedon suojaaminen kytkeytyy laajempaan teknologian kehitykseen liittyvään ilmiöön.

3.2 Tutkimusaiheen rajaukset

Tässä tapaustutkimuksessa tutkitaan rajattua suppeaa kohdetta rajatulla haastatteluaineistolla. Tutkimus keskittyy yhteen yhteisöön (PHRAKLE-S) ja sen kilpailuttamiin julkisiin palveluhankintoihin. Tutkimusaiheena on puolustusvoimien turvallisuusluokitellun tiedon suojaaminen palveluhankintojen tarjouslaskentavaiheessa. Tutkimuksen aihe on saatu tutkimuksen kohteena olevalta yhteisöltä.

Laeissa ja asetuksissa on lukuisia määräyksiä erilaisten henkilöiden salassapitovelvollisuudesta. Lisäksi viranomaisille on lain perusteella annettu oikeus eri yhteyksissä määrätä tiettyjen tietojen salassapitovelvollisuudesta. Tässä tutkimuksessa keskitytään vain julkisuuslain 24 §:n 2 & 7-10 kohdan sekä kansainvälisen tietoturvallisuusvelvoitteen mukaan turvallisuusluokitellun ja salassa pidettäväksi määrätyn tiedon suojaamiseen.

Tutkimuksessa tarkastellaan KATAKRI:n kriteerien käytettävyyttä suojausvaatimusten perustana. Tutkimuksessa keskitytään suojaustasojen IV, III ja II tietoihin (ks. liite 3), sillä KATAKRI ei ota kantaa suojaustason I tiedon suojausvaatimuksiin.

Puolustus- ja turvallisuushankintalain tarkoittamat hankinnat on rajattu tutkimuksen ulkopuolelle, koska sellaisten tekeminen PHRAKLE-S:ssä on harvinaista. Lisäksi kyseisen lain tarkoittamat hankinnat ovat luonteeltaan salassa pidettäviä ja siksi niiden käsitteleminen julkisessa opinnäytetyössä olisi ongelmallista.

Tutkimuksen aineistona toimii viideltä asiantuntijalta sähköpostitse kerätty haastatteluaineisto, jota tutkija täydentää omalla tulkinnallaan. Haastatellut asiantuntijat on valittu sekä palveluhankintoja tekevästä Puolustushallinnon rakennuslaitoksesta että puolustusvoimista, jonka turvallisuusluokittelemaa tietoa hankinnan tarjouslaskenta-aineisto saattaa sisältää. Asiantuntijahaastattelut on kuvattu tarkemmin kappaleessa 4.2.2.

4 Metodologisia valintoja

Tämän tutkimuksen tietoteoreettisia, eli ontologisia perusteita pohdittaessa voi törmätä moniin ristiriitaisuuksiin tiedon luonteen ymmärtämisessä. Kysymykset siitä *”mitä tieto on?”*, *”onko salassa pidettävä tieto salaista?”*, *”jos tieto on salaista, kuka siitä tietää?”* ja *”jos tiedosta ei tiedä kukaan, onko sitä olemassa?”* voisivat innoittaa kiivaaseen filosofiseen väittelyyn kaikesta olemassa olevasta, maailman luonteesta ja todellisuuden rakenteesta. Tämän välttämiseksi tulee salassa pidettävä tieto tässä tutkimuksessa ymmärtää yleisesti informaatioksi, joka on tarkoitettu vain tiettyjen henkilöiden käyttöön ja sen perusteella määrätty lain nojalla salassa pidettäväksi. Tieto olemukseltaan ei siis ole salaista, vaan salassa pidettävää. Myöskään tutkimuksen kannalta keskeinen termi *”turvallisuus”* ei ole yksiselitteinen, vaan jokaisella lukijalla on oma subjektiivinen käsityksensä siitä, mitä se tarkoittaa.

Tämä tutkimus on ontologialtaan intersubjektiivinen. Sen todellisuuskuva muodostuu kulttuurisena ihmisten välisessä vuorovaikutuksessa ja todellisuus perustuu enemmän ihmisten kokemuksiin ja elämyksiin, kuin luonnontieteessä vaikuttaviin lainalaisuuksiin. Absoluuttista totuutta siitä, milloin turvallisuusluokiteltu tieto on riittävästi suojattu, on hankala määritellä ja vielä hankalampi mitata. Turvallisuusluokiteltu tieto voi pysyä salassa lukitussa pöytälaati-

kossa ja toisaalta järeäänkin kassakaappiin on mahdollista murtautua. Kiivasta tahtia kehittyvä teknologia tarjoaa yhä uusia keinoja päästä käsiksi oikeudettomasti salassa pidettäviksi luokiteltuihin tietoihin. Toisaalta tarjousprosessiin osallistuvan henkilön huolimaton lipsautus voi saattaa tiedon pahantahtoisiin korviin kovista suojaustoimenpiteistä huolimatta.

Tutkimusongelmaa lähestytään fenomenologis-hermeneuttisesta näkökulmasta, sillä fenomenologisen tieteenfilosofian keskiössä on ajatus siitä, että maailma on subjektiivinen ilmiö, joka rakentuu oman mielemme sisällä. Maailman ajatellaan koostuvan kaikkien ihmisten minä-maailmoista ja niitä ympäröivistä sieluttomista objekteista. Fenomenologiassa maailmaan keskitytään siis sellaisena, kuin ihminen sen kokee. (Anttila 2006, 329–334.)

Tässä tutkimuksessa tarkastellaan haastatteluaineistoa, jossa palveluhankintojen parissa työskentelevät asiantuntijat kuvaavat omaa suhtautumistaan tutkittavaan ilmiöön, eli turvallisuusluokitellun tiedon suojaamiseen sekä avaavat omaa käsitystään sen merkityksestä hankintaprosessin tarjouslaskentavaiheen etenemiselle. Asiantuntijoiden oma kokemus ilmiön vaikutuksesta hankintaprosessiin on äärimäisen arvokas, kun etsitään riittäviä tiedon suojauskeinoja, jotka kuitenkin haittaisivat hankintaprosessia mahdollisimman vähän. Asiantuntijoiden kokemusmaailmaa kuvailemalla ja sitä kriittisesti arvioimalla pyritään löytämään sellainen todellisuuskuva, jossa tiedot olisi suojattu asianmukaisesti siten, että suojaustoimenpiteistä aiheutuisi kuitenkin mahdollisimman vähän haittaa tarjousprosessin etenemiselle.

Tutkija ei itse pysy objektiivisena kertojana tyytyen kuvailemaan muiden kokemuksia käsiteltävästä aiheesta, vaan pyrkii myös aktiivisesti tekemään tulkintoja käsiteltävästä haastatteluaineistosta oman esiymmärryksensä pohjalta. Tämä puolestaan on tyypillistä hermeneutiikalle. Hermeneutiikka on filosofiassa ymmärtämistä ja tulkintaa korostava suuntaus. Hermeneutiikassa pyritään rakentamaan konkretisoitu kuva, kokonaisuus, tutkittavasta ilmiöstä. Tutkijan työskentely on eräänlaista vuoropuhelua, jossa tutkija suhteuttaa aineistoon omat merkitysehdotuksensa ja korjaa niitä, mikäli kohteen tulkinta ja ymmärretyksi tuleminen niin vaatii. (Anttila 2006, 305 & 548.)

4.1 Tutkimusstrategia

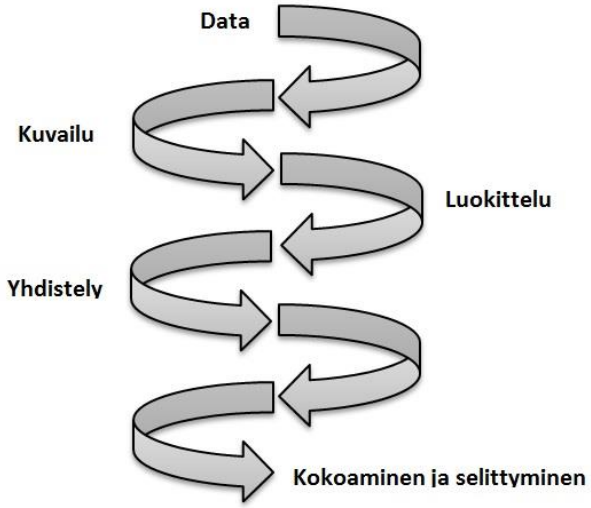
Tämä opinnäytetyö on laadullinen, deskriptiivinen tapaustutkimus. Laadullisen tutkimuksen lähtökohtana on todellisen elämän kuvaaminen ja tavoitteena on usein ilmiön ymmärtäminen, selittäminen, tulkinta sekä usein myös sitä kautta saadun tiedon soveltaminen (Anttila 2006, 275; Hirsjärvi, Remes & Sajavaara 2012, 161). Koska turvallisuusluokitellun tiedon tosiasiallista salassapitoa on vaikeaa mitata määrällisesti, tiedon luokittelu perustuu vahvasti lainsäädäntöön ja tiedon suojaamisen tarve on sidoksissa julkisuuslain 7 luvun 31 §:ssä määritettyyn aikaan, on aihetta hedelmällistä lähestyä juuri laadullisesta näkökulmasta.

Kuvailevat, deskriptiiviset tutkimukset vastaavat tavallisesti kysymyksiin: *”Mikä ilmiö on?”* tai *”Millainen ilmiö on?”*. Niiden tarkoituksena on kuvata systemaattisesti tutkittavaan ilmiöön liittyvät tosiasiat ja tunnuspiirteet tarkasti ja todellisuuden mukaisesti. Syvälliseen kuvaukseen tähtäävät tutkimukset ovat usein luonteeltaan tapaustutkimuksia. Tapaus- eli case-tutkimus on sellainen empiirinen tutkimus, jonka tarkoituksena on tavallisesti kuvailla intensiivisesti jotain tiettyä, tavallisesti sosiaalista kohdetta kuten yksilöitä, ryhmiä, laitoksia tai yhteisöjä. Kiinnostuksen kohteena ovat usein prosessit, joissa yksittäistapausta tutkitaan yhteydessä ympäristöönsä luonnollisissa tilanteissa. Fokuksena voivat olla esimerkiksi kohteiden taustatekijät, ajankohtainen asema ja tilanne, ympäristötekijät, sisäiset tai ulkoiset vaikuttavat tekijät. Nämä seikat vaikuttavat harvoin yksinään ja siksi niistä pyritään tapaustutkimuksissa saamaan mahdollisimman seikkaperäinen, kokonaisvaltainen ja tarkka kuvaus. (Anttila 2006, 285–286; Hirsjärvi, ym. 2012, 134–135.)

Monet edellä mainitut tapaustutkimuksen piirteet täyttyvät tämän tutkimuksen osalta, sillä tutkimuksen kohteena on yksi yhteisö (PHRAKLE-S) j tutkimus keskittyy hankintaprosessiin. Lisäksi tutkimusaihetta tarkastellaan prosessin tarjouslaskentavaiheessa. Anttila (2006, 287) huomauttaa kuitenkin, että tapaustutkimukset keskittyvät yleensä enemmän selitykseen kuin tulkintaan ja, ettei hyvä case-tutkija pyrikään tulkitsemaan vaan ainoastaan kuvaamaan tarkasti kohdettaan. Myös Hirsjärvi ym. (2012, 135) toteavat, että tapaustutkimuksen tavoitteena on tyypillisimmin ilmiön kuvailu.

Tämän opinnäytetyön tulkintaan nojaava lähestymistapa ja aktiivinen pyrkimys vuoropuheluun tekstin ja tutkijan välillä erottaa tutkimuksen perinteisestä tapaustutkimuksesta. Ilmiön luonnetta kuvaavat luvut kaksi ja viisi ovat luonteeltaan vahvasti deskriptiivisiä ja pyrkivät lisäämään lukijan ymmärrystä käsiteltävästä ilmiöstä. Kyseisissä luvuissa vastataan myös tutkimuksen alakysymyksiin. Luvut kuusi ja seitsemän ovat puolestaan tyyliltään enemmän hermeneuttisia ja niissä on nähtävissä vahvasti tutkijan oma tulkinta ja kädenjälki. Näistä luvuista löytyvät perusteet tutkimuksen pääkysymyksen vastaukselle.

Laadullisessa tutkimuksessa analyysi kuvataan usein spiraalin omaisesti kierroksina eteneväksi prosessiksi, jolle on annettu nimeksi hermeneuttinen kehä (ks. kuva 2). Kehällä edetään aineistossa (data) vaihe vaiheelta eteenpäin, jolloin ensin saavutetaan aineiston edustaman ilmiön kuvailun taso, sen jälkeen luokittelun taso ja siitä sisältöelementtien yhdistelyn tason kautta lopulta ilmiön kokoamisen ja selittymisen taso. (Anttila 2006, 280.)



Kuva 2 Hermeneuttinen kehä (Anttila 2006, 280)

Anttila (2006, 280–281) toteaa, että laadullinen tutkimus voidaan sovittaa hermeneuttisen tulkinnan eri syvyystasoille tutkimustavoitteen mukaisesti. Jotkut menetelmistä toteuttavat laadullisen kuvailun tavoitteen, toiset tavoittavat ilmiössä olevien piirteiden luokitteluun pyrkiviä tavoitteita. Joidenkin menetelmien avulla tulkitaan ja yhdistellään ilmiön piirteitä ja joidenkin menetelmien avulla pystytään syvällisesti ymmärtämään ilmiön olemusta. Tämä opinnäytetyö pyrkii saavuttamaan ns. kolmannen syvyystason, joka tähtää ilmiön tulkintaan, ymmärtämiseen ja merkityksenantoon (Vrt. Anttila 2006, 281).

4.2 Tutkimusmenetelmät

Hyvän tutkimuksen kannalta on tärkeää, että lukijalle on selkeää, mistä ja miten tutkija hankkii tietonsa ja miten pätevää se on. Lisäksi lähestymistavan on oltava menetelmällisesti mahdollinen ja se on pystyttävä toteuttamaan käytännössä. (Anttila 2006, 59–60.)

Tässä tutkimuksessa käytetyillä menetelmillä luodaan tutkimusaiheesta syvällinen kuvaus tarkastelemalla ilmiötä ja sen kontekstia kirjallisuuden avulla. Lisäksi ilmiön parissa työskentelevien henkilöiden kokemusmaailmoihin pureudutaan analysoimalla haastatteluaineistoa laadullisesti. Kohdeorganisaation toivomuksesta tulkinnalla on ollut vahva painotus tutkimusmenetelmiä valittaessa.

4.2.1 Tiedonhankintaprosessi ja kirjallisuuskatsaus

Aikaisempaa tutkimusta etsittiin internetistä suorittamalla yleinen vapaa sanahaku Google hakukonepalvelulla, koska se on hakupalvelimista käytetyin ja sillä on laajin tietokanta (Hirsjärvi ym. 2012, 90). Lisäksi tehtiin tarkennettu haku sähköisiin Doria, Helda, Melinda ja Theseus -julkaisukokoelmiin, jotka sisältävät suomalaisten korkeakoulujen julkaisuja. Tavoitteena oli löytää etenkin Maanpuolustuskorkeakoulussa, Laurea-ammattikorkeakoulussa sekä Aalto Yliopistossa tehtyjä pro gradu -tasoisia tutkimuksia. Näiden korkeakoulujen tutkimus- ja kehitystyön hedelmien odotettiin vastaavan parhaiten tutkimuksen aihepiiriä. Tiedonhaussa keskityttiin Suomen kielellä tehtyihin aineistoihin, koska tiedon suojaaminen on vahvasti sidoksissa kohdemaansa lainsäädäntöön.

Aineistohaku suoritettiin hakusanoilla ”puolustusvoimat”, ”puolustushallinnon rakennuslaitos”, ”palveluhankinta”, ”salassa pidettävä tieto”, ”tarjouslaskenta”, ”tarjouspyyntö”, ”tiedon käsittely”, ”turvallisuus”, ”turvallisuusluokittelu”, ”turvallisuusluokiteltu tieto” sekä näiden termien eri variaatioilla. Tarkennetuissa hauissa keskityttiin 2000-luvulla julkaistuihin vähintään pro gradu -tasoisiin tutkimuksiin. Aihepiiriä ympäröivä lainsäädäntö on muuttunut radikaalisti 2000-luvulla teknologisen kehityksen myötä, joten tätä vanhemmat tutkimukset eivät olisi huomioineet nykypäivän lainsäädäntöä tarvittavissa määrin.

Aihepiiristä ei löytynyt tieteellistä tutkimusta, joka toisaalta vahvisti tutkimusaukon olemassaolon. Tästä syystä päädyttiin tutkimuksen taustaa kuvailtaessa käyttämään alemman tason tutkielmia, joita täydennettiin tekemällä aihealueesta suppea traditionaalinen kirjallisuuskatsaus. Traditionaalinen, eli kuvaileva kirjallisuuskatsaus keskittyi aihepiiriä ympäröivään lainsäädäntöön (ks. liite 2) sekä soveltuvin osin Tom Vapaavuoren teokseen ”Yrityssalaisuudet ja salassapitosopimukset”, johon edellä mainittu lainsäädäntö on selkeästi tiivistetty. Lisäksi tutustuttiin Puolustushallinnon ministeriötason ohjeistuksiin sekä Valtion hankintakäsikirjaan. Tutkimuksen metodologia pohjaa puolestaan Pirkko Anttilan kirjaan Tutkiva toiminta ja teos, ilmaisu ja tekeminen sekä Hirsjärven, Remeksen ja Sajavaaran teokseen Tutki ja Kirjoita.

Valtion hankintakäsikirja 2010:n tarkoituksena on toimia valtion virastojen ja laitosten hankintaohjeiden sisältöä, hankinnan menettelyitä ja toimintatapoja yhtenäistävänä ja kehittämistä tukevana mallina sekä valtionhallinnon hankintatoimen konserniohjauksen välineenä (Hytönen & Lehtomäki 2010, 29). Valtion hankintakäsikirja 2010 muodostaa hankintaprosessin kuvauksen selkärangan. Organisaation kuvaus puolestaan perustuu PHRAKL:n vuoden 2012 henkilötilinpäätökseen, toimintakertomukseen ja tilinpäätöslaskelmiin sekä laitoksen sidosryhmälehden artikkeleihin sekä internet-sivujen organisaatiorakennetta kuvaavaan osioon.

Syvällisen esiymmärryksen saavuttamiseksi, tutkija on tutustunut myös Puolustushallinnon rakennuslaitoksen julkaisemattomiin lähteisiin kuten hankintaohjeeseen sekä hankintojen turvallisuustoiminnan ohjeistuksiin. Näihin dokumentteihin ei kuitenkaan viitata suoraan tutkimuksessa.

4.2.2 Asiantuntijahaastattelut

Tiedonhankintaprosessin yhteydessä kävi selväksi, että yltääkseen tutkimustavoitteen mukaiseen ymmärtämiseen ja merkityksenantoon tähtäävään ulottuvuuteen, ei pelkkä tukeutuminen kirjallisiin lähteisiin ollut riittävää. Edetäkseen hermeneuttisella kehällä alemmas kohti syvempiä tasoja, oli päästävä käsiksi myös ilmiön parissa työskentelevien ihmisten kokemusmaailmoihin.

Aineiston keruumenetelmäksi valikoitui asiantuntijahaastattelu (elite interviewing), jossa haastateltavat ovat erityisesti valittuja tutkittavaa ilmiötä silmällä pitäen. Asiantuntijahaastatteluissa haastateltavien tulee olla koulutettuja alansa asiantuntijoita, joilla on asemansa perusteella mahdollisuus antaa tietoa tutkittavaan ilmiöön liittyvistä laajoista kysymyksistä, ilmiön historiallisesta kehityksestä ja esimerkiksi tulevaisuuden suuntaviivoista. Haastattelun tarkoituksena on koota heidän hallussaan oleva erikoistietämys. (Anttila 2006, 189–199.)

Asiantuntijahaastattelu toteutettiin sähköpostitse strukturoituna haastatteluna. Haastattelulomakkeessa (ks. liite 4) oli sekä avoimia että suljettuja kysymyksiä. Suljettujen kysymyssarjojen lopussa annettiin valittavaksi myös vapaa vaihtoehto, jos etukäteen määritellyistä vastausvaihtoehdoista ei sopivaa vastausta löytynyt. Suljetut kysymykset laadittiin nominaaliasteikolle, mikä tarkoittaa, että vastausvaihtoehdot eivät asetu millekään arvoasteikolle, eikä niistä mitään voida pitää toisen edellä olevana (Anttila 2006, 262). Tähän päädyttiin, koska jokaisen vastaajan kokemusmaailma itsessään on tutkimusaiheen kannalta mielenkiintoinen, eikä yksittäinen mielipide ole toista huonompi.

Kysymyslomake sisälsi 16 kysymystä, joiden tarkoituksena oli hahmottaa vastaajien kokemusmaailmaa ja arvioida KATAKRI:n käytettävyyttä tarjouslaskentavaiheen turvallisuusjärjestelyissä. Haastattelu lähetettiin vastaanottajille 25.5.2013 ja vastausaikaa oli kesäkuun 2013 loppuun. Myöhemmin vastausaikaa pidennettiin 31.7.2013 asti. Haastateltaviksi valittiin yhteistyössä kohdeorganisaation edustajan kanssa palveluhankintojen turvallisuusjärjestelyiden kanssa työskenteleviä ihmisiä Puolustushallinnon rakennuslaitoksesta sekä puolustusvoimista.

Haastattelu lähetettiin sähköpostitse kolmelle puolustusvoimissa työskentelevälle turvallisuuspäällikölle, yhdelle hallinnollisen tietoturvallisuuden päällikölle ja yhdelle kaupallisjuridiselle asiantuntijalle sekä kahdelle Puolustushallinnon rakennuslaitokselle työskentelevälle turvallisuuspäällikölle, yhdelle hankkijalle ja yhdelle projektipäällikölle. Jottei pelkkä turvallisuusnäkökulma dominoisi vastauksia, pyrittiin haastatteluilla tavoittamaan myös puhtaasti kaupallisen alan ammattilaisia, jotka kuitenkin törmäävät turvallisuusluokitellun tiedon suojausvaatimuksiin työtehtävissään. Haastatteluun vastasi viisi tavoitellusta yhdeksästä asiantuntijasta. Heistä yksi edustaa puolustusvoimia ja neljä Puolustushallinnon rakennuslaitosta.

Koska turvallisuusluokitellun tiedon suojausvaatimukset koskettavat ennen kaikkea PHRAKLE-S:n sidosryhmiä, haluttiin opinnäytetyössä ottaa huomioon myös sidosryhmien edustajien mielipiteet suojausvaatimusten merkityksestä palveluhankintaprosessille. Tästä syystä erillinen kysymyslomake (ks. liite 5) lähetettiin myös sellaisiin yrityksiin, jotka olivat harkinneet osallistumista erään PHRAKLE-S:n kilpailuttaman palveluhankinnan tarjouslaskentavaiheeseen.

Kyselyn vastaajiksi valittiin edellä mainitun hankinnan tarjouslaskentavaiheen sopimusyhteyshenkilöksi ja turvallisuusvastaavaksi ilmoitettuja henkilöitä. Osassa tapauksista molempiin tehtäviin oli merkitty yksi ja sama henkilö. Kysymyslomake lähetettiin 17 henkilölle, jotka edustivat 12 eri yritystä. Kysymyslomakkeet lähetettiin 17.6.2013 ja vastausaikaa oli elokuun loppuun asti. Vastauksia saatiin vain kaksi, joten niiden perusteella ei voi tehdä yleistyksiä sidosryhmien suhtautumisesta asiaan. Lisäksi vastausten validiutta arvioitaessa, tulee ottaa huomioon, että sidosryhmien edustajien vastausten laatuun on saattanut vaikuttaa halu näyttäytyä mahdollisimman positiivisessa valossa palveluhankintoja teettävän organisaation silmissä.

Yksittäisen henkilön kokemusmaailmoina nämä kaksi vastausta ovat kuitenkin huomionarvoisia, koska tutkimusaihetta pystytään niiden ansiosta käsittelemään useammasta kuin yhdestä näkökulmasta. Lisäksi ne tarjoavat myös mahdollisuuden tarkastella pinnallisesti KATAKRI:n vaatimusten parissa painivien yritysten näkemyksiä kyseisen kriteeristön käytettävyydestä, joka laajemmalla otannalla voisi olla kokonaan oman tutkimuksen aihe. Kappaleessa 6.7 on lyhyt yhteenveto näistä kahdesta vastauksesta.

Asiantuntijahaastattelujen vastauksia käsitellään tässä opinnäytetyössä siten, etteivät vastaajien henkilöllisyys, toimenkuva tai organisaatio ole yksilöitävissä tai pääteltävissä yksittäisen mielipiteen osalta. Tällä ratkaisulla taataan se, että haastateltavat pystyvät vastaamaan kysymyksiin rehellisesti. Näin menettelemällä oli mahdollista tulkita haastateltavien mielipiteitä ilman, että esimerkiksi henkilön asema puolustusvoimissa vaikuttaisi vastauksiin. Haastatteluaineistot ovat tutkijan hallussa.

4.2.3 Sisällönanalyysi

Sisällönanalyysi on tutkimusmenetelmä, jonka avulla voidaan tehdä toistettavia ja päteviä päätelmiä tutkimusaineiston suhteesta sen asia- ja sisältöyhteyteen. Sisällönanalyysin luokitusrunko on luettelo tutkimuksen kaikista sisältöluokista, jotka sisältävät osioita, eli pienempiä luokiteltavissa olevia tekijöitä. (Anttila, 2006 292–293.)

Haastatteluaineisto on pilkottu ja järjestetty kuvassa 3 esitetyn luokitusrungon mukaisesti eri aihepiirejä kuvaaviin havaintoyksiköihin. Tarkoituksena on nostaa esiin tutkimusongelmaa valaisevia näkemyksiä. Luvussa 6 tarkastellaan vastauksien jakaantumista havaintoyksiköiden sisältöluokkien sisällä ja luodaan kokonaisvaltainen kuvaus vastaajien kokemusmaailmoista. Analyysiä täydennetään tutkijan omalla tulkinnalla.

Kuva 3 Haastatteluaineiston luokitusrunko

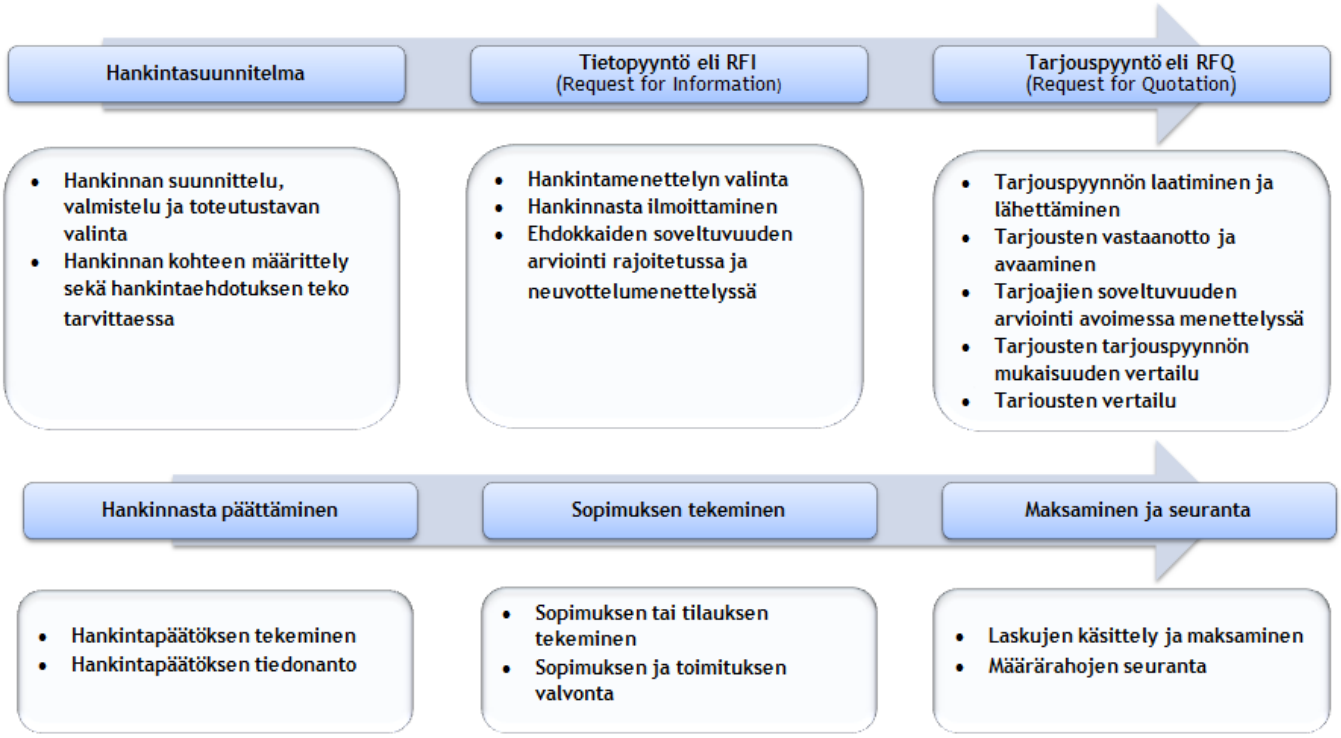
5 Hankintaprosessi

Suomessa on luotu koko valtiohallinnon yhteinen hankintastrategia (ks. VM julkaisuja 35/2009), jonka tarkoituksena on edistää valtiontalouden kannalta avointa ja taloudellista hankintaa ja siihen liittyvää logistiikkaa sekä pyrkiä nostamaan hankintatoimen toteutuksen tehokkuutta kaikissa valtionhallinnon yksiköissä. Kukin ministeriö vastaa oman hallinnonalansa hankintatoimen ohjauksesta ja toteutuslinjoista. (Hytönen & Lehtomäki 2010, 20.) Hankinnan toteutusta käynnistettäessä on valittava hankintaan soveltuva hankintamenettely. Hankintalain soveltamisalan piirissä olevat hankintamenettelyt on lueteltu alla taulukossa 1.

Menettely	Huomattavaa
Avoin menettely	Yksivaiheinen, selkeä, käynnistetään hankintailmoituksella, ei neuvottelumahdollisuutta, sopii perushankintoihin.
Rajoitettu menettely	Kaksivaiheinen, käynnistetään hankintailmoituksella, ei neuvottelumahdollisuutta, sopii hankintoihin, joissa on tarve rajoittaa osallistujien määrää ja rajaamiseen löytyy selkeitä perusteita, yleensä pitkäkestoinen tavara- tai palveluhankinta.
Neuvottelumenettely	Kaksivaiheinen, käynnistetään hankintailmoituksella, neuvottelumahdollisuus, edellyttää aina laissa määriteltyjen neuvottelumenettelyn edellytysten täyttymistä, monimutkainen hankinta.
Suorahankinta	Yksivaiheinen, ei hankintailmoitusta, neuvottelumahdollisuus yhden tai useamman toimittajan kanssa, edellyttää aina laissa määriteltyjen suorahankinnan edellytysten täyttymistä. EU kynnysarvot ylittävässä suorahankinnassa uusi vapaaehtoinen ilmoitus ja 14 päivän odotusaika.
Kilpailullinen neuvottelumenettely	Monivaiheinen, käynnistetään hankintailmoituksella, tarkoitettu erityisen monimutkaisiin hankintoihin, joiden valintaperusteena on kokonaistaloudellinen edullisuus, joissa hankintayksikkö ei pysty objektiivisesti ennakolta määrittelemään hankinnan oikeudellisia tai taloudellisia ehtoja tai teknisiä keinoja ja joissa lisäksi hankintayksikkö haluaa neuvotella hankinnan toteuttamisvaihtoehdoista.
Suunnittelukilpailu	Menettely, jonka tarkoituksena on hankkia suunnitelma, jonka tuomaristo valitsee kilpailulla ja jossa voidaan antaa palkintoja.
Puitejärjestely	Yhden tai usean hankintayksikön ja yhden tai usean toimittajan välinen sopimus, jossa sovitaan joko kaikista hankintaan sovellettavista ehdoista tai osa ehdoista jätetään auki. Käynnistetään yleensä avoimella, rajoitetulla tai neuvottelumenettelyllä.

Taulukko 1 Hankintamenettelyt (Hytönen & Lehtomäki 2010, 55)

Ministeriöiden vastuulla on tarpeellisten hankintatoimen yhteistoimintamenettelyjen aikaansaaminen hallinnonalallaan sekä hallinnonalan keskitetyistä menettelyistä sopiminen. Yksittäisen hankinnan toteutuksen ohjaamisesta ja toteutuksen asianmukaisuudesta vastaa kukin hankintayksikkö eli virasto tai laitos. (Hytönen & Lehtomäki 2010, 22.) Hankintaprosessiin kuuluvat Valtion hankintakäsikirjan (2010, 31) mukaan pääsääntöisesti kuvan 3 mukaiset vaiheet.



Kuva 4 Hankintaprosessin eteneminen (Hytönen & Lehtomäki 2010, 31, muokattu)

Hankintoihin liittyy ostohinnan lisäksi myös muita kustannustekijöitä. Erilaiset työaikaa vaativat toimenpiteet, kuten tarjouspyynnön suunnitteluun, tarjousten vertailuun ja hankinnasta sopimiseen käytettävä työaika ja erilaiset muut hallinnolliset toimenpiteet, muodostavat hankintatoimessa jopa 70 % kustannustekijöistä (Hytönen & Lehtomäki 2010, 25). Optimoimalla hankintojen turvallisuusjärjestelyt ja minimoimalla niistä aiheutuvat lisätyöt PHRAKLE-S voi siis parhaassa tapauksessa paitsi parantaa turvallisuusluokitellun tiedon suojausta, myös karsia hankintojen parissa käytettyä työaikaa ja sitä kautta hankintojen kokonaiskustannuksia.

5.1 Palveluhankintojen turvallisuus

Palveluhankintojen turvallisuus on otettava huomioon niiden suunnittelun käynnistämisestä alkaen ja jo hankintasuunnitelmassa tulee olla määriteltynä hankkeen turvaluokitus ja sen vaatimat turvallisuusjärjestelyt. Hankintalaissa taataan hankkijalle mahdollisuus asettaa tarjoajan soveltuvuutta koskevia ennakkoehtoja tarjouspyyntöprosessiin osallistumiselle rajoitetussa menettelyssä, neuvottelumenettelyssä tai kilpailullisessa neuvottelumenettelyssä.

Ehdokkaiden joukosta valitaan tällöin ne, jotka hyväksytään tarjoajiksi ja joille lähetetään tarjouspyyntö tai jotka kutsutaan neuvotteluun. Ne ehdokkaat tai tarjoajat, joita koskee jokin poissulkuperuste tai, jotka eivät täytä tarjouspyynnössä tai hankintailmoituksessa asetettuja tarjoajan soveltuvuutta koskevia vähimmäisvaatimuksia, suljettaan tarjouskilpailusta. (Hytönen & Lehtomäki 2010, 103.)

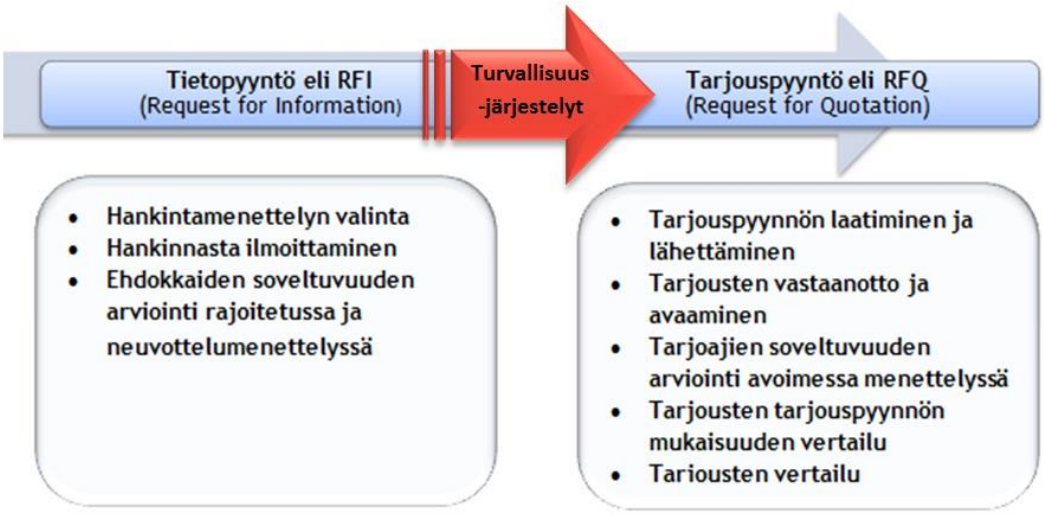
Puolustushallinnon rakennuslaitos on sitoutunut pitämään salassa kaikki puolustusvoimien sille luovuttamat salassa pidettäviksi säädetyt tai sellaisiksi lain nojalla määrätyt tiedot. Sidosryhmät pyritään sitouttamaan tiedon salassapitoon ja turvallisuuslähtöiseen toimintaan sopimuksin, joissa määritellään osapuolten vastuut ja velvollisuudet hankintaprosessin eri vaiheissa. PHRAKLE-S edellyttääkin sidosryhmiltään kirjallista sitoutumista määrättyihin turvallisuusjärjestelyihin ennen kuin se luovuttaa turvallisuusluokiteltua tarjouslaskenta-aineistoa potentiaalisille palvelun tarjoajille. Mikäli palvelun tarjoaja rikkoo tätä tarjouslaskentavaiheen turvallisuutta koskevaa sopimusta, voi se johtaa ennalta määriteltyyn sopimussakkoon, sopimuksen purkamiseen tai viranomaisen tutkintaan ja vakavimmillaan jopa rikossyytteeseen.

Jos palvelua tarjoavissa yrityksissä ei sisäistetä turvallisuusluokitellusta tarjouslaskenta-aineistosta aiheutuvia velvoitteita, ajaudutaankin helposti ongelmiin jo hankintaprosessin alkumetreillä. Turvallisuusjärjestelyiden yllättäessä tarjouslaskentaan osallistuvat yritykset, saattaa seurauksena olla kilpailutusaikataulujen viivästymistä ja sekaannuksia. Turvallisuusluokitellun tiedon suojausvaatimukset saattavat aiheuttaa sidosryhmille lisäkustannuksia ja -töitä, jotka on huomioitava tarjouslaskentavaiheeseen varatun ajan puitteissa tai muuten tarjouslaskenta-aineisto jää kokonaan saamatta. Uhkana on, että saadakseen tarjouslaskenta-aineiston haltuunsa, yritykset väittävät täyttävänsä suojausvaatimukset, vaikka näin ei välttämättä olisikaan.

5.2 Sidosryhmäturvallisuuden ohjaus

Hankinnan suunnitteluvaiheessa määritellään hankintakohtaiset turvallisuusjärjestelyt sidosryhmille luovutettavan tiedon suojaustason perusteella. Ennen turvallisuusluokitellun aineiston luovuttamista, palvelua tarjoava yritys toimittaa PHRAKLE-S:lle tarjouslaskentaan osallistuvan henkilöstön turvallisuusselvityshakemukset, vaitiolovakuutukset sekä selvityksen oman yritysturvallisuutensa tilasta. Jos yrityksellä on voimassa oleva turvallisuussopimus Puolustusvoimien kanssa, voidaan sille luovuttaa sopimuksessa määriteltyä suojaustasoa vastaavat asiakirjat. Jos yritys ei täytä asetettuja vaatimuksia, se voi tutustua aineistoon PHRAKLE-S:n osoittamassa tilassa. Turvallisuusluokitellun tarjouslaskenta-aineiston saadakseen, tulee yrityksen kyetä osoittamaan, että se pystyy suojaamaan aineiston vaiheen aikana. Mikäli yritys ei täytä PHRAKLE-S:n asettamia vaatimuksia, ei sille aineistoa lähetetä.

Sidosryhmien soveltuvuutta tarkasteltaessa PHRAKLE-S pyrkii varmistumaan riittävistä turvallisuusjärjestelyistä ja suojausvaatimusten täyttymisestä sidosryhmien keskuudessa tehtävillä turvallisuuskartoituksilla. Turvallisuuskartoituksissa käytetään apuna soveltuvin osin Kansallista turvallisuusauditointikriteeristöä eli KATAKRI:a sekä puolustusvoimien pääesikunnan pysyväisasiakirjoihin pohjautuvia vaatimuksia.



Kuva 5 Turvallisuusjärjestelyt tarjouslaskentavaiheessa
(Hytönen & Lehtomäki 2010, 31, muokattu)

KATAKRI valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Sen tarkoituksena oli luoda viranomaisille ja yrityksille yhteinen turvallisuuskriteeristö yhteisöturvallisuusmenettelyn yhtenäistämiseksi ja yritysten omavalvonnan sekä viranomaisen tekemien turvallisuustarkastusten eli auditointien parantamiseksi. Turvallisuuskriteeristön valmisteluun osallistui lukuisia viranomaisia, elinkeinoelämän edustajia ja turvallisuusalan toimijoita. Yhteistyön tulos – KATAKRI – toimii kansallisesti velvoittavana asiakirjana silloin, kun suomalaisen yrityksen turvallisuustaso varmennetaan kansallisen turvallisuusviranomaisen toimesta kansainväliseen viranomaispyyntöön pohjautuen ja yhteisöturvallisuustodistuksen myöntämiseen tähdäten. (Puolustusministeriö 2011, 2-3.)

KATAKRI sisältää 167 kysymystä, jotka kaikki sisältävät velvoitteita turvallisuusvaatimusten täyttymisestä kolmella tasolla, jotka ovat perus-, korotettu ja korkea taso. Mikäli vain yritykset, joille olisi myönnetty yhteisöturvallisuustodistus, olisivat kelpoisia osallistumaan tarjouskilpailuihin, putoaisi potentiaalisten palvelun tarjoajien määrä todennäköisesti murto-osaan nykyisestä. Tämä saataisi vääristää kilpailua ja nostaa hankintojen hintaa. KATAKRI:n kriteerit ovat kuitenkin käyttökelpoisia suunniteltaessa puolustusvoimien turvallisuusluokitellun tiedon suojausvaatimuksia. KATAKRI:n luomisprosessin johtovastuu oli nimittäin osoitettu puolustusministeriölle, joten on perusteltua olettaa, että KATAKRI:n kriteerejä luodessa on kuunneltu myös puolustusvoimien edustajien mielipiteitä turvallisuusluokitellun tiedon suojaamisesta.

Mutta tulisiko KATAKRI:a soveltaa sidosryhmäturvallisuuden ohjauksessa täysimääräisesti vai tulisiko kriteeristöstä soveltaa suojausvaatimuksia sidosryhmäyhteistyön laajuus huomioon ottaen? Onko perusteltua käyttää raskasta yhteisöturvallisuusselvityksiin tarkoitettua kriteeristöä tarkasteltaessa sidosryhmien soveltuvuutta palvelun tuottajaksi puolustusvoimille? Mitkä lopulta ovat turvalllisuusluokitellun tiedon suojausvaatimukset Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikön hankintojen tarjouslaskentavaiheessa?

6 Turvallisuusluokitellun tiedon suojaaminen palveluhankintojen tarjouslaskentavaiheessa

Turvallisuus on vain yksi osa hankintaprosessia (Simi 2010, 33), joten sen eteen tehtävät järjestelyt eivät saa haitata kohtuuttomasti prosessin etenemistä. Tässä tiivistyy tutkimusta ohjaava esiymmärrys, joka toimii asiantuntijahaastatteluun valitun kysymysrungon (ks. liite 4) tukirankana.

Esioletuksena on, että asiantuntijoiden mielestä KATAKRI:n täysmääräinen käyttäminen tarjouslaskentavaiheen turvallisuusjärjestelyissä haittaisi liiaksi palveluhankintaprosessin etenemistä ja aiheuttaisi kilpailun toimimattomuutta. Tämä on ristiriidassa hankintalain 1§:ssä kuvatun lain tarkoituksen kanssa. Liian kovat turvallisuusjärjestelyt eivät nimittäin tehostane julkisten varojen käyttöä, tai edistä laadukkaiden hankintojen tekemistä lain tavoitteiden mukaisesti, eivätkä turvaa yritysten ja muiden yhteisöjen tasapuolisia mahdollisuuksia tarjota tavaroita, palveluita ja rakennusurakointia julkisten hankintojen tarjouskilpailuissa.

Kappaleissa 6.1–6.7 on analysoitu sähköpostitse tehdyn asiantuntijahaastattelun vastauksia. Vastaukset tarjoavat mahdollisuuden sekä hahmottaa aihepiirin parissa työskentelevän viiden asiantuntijan kokemusmaailmaa että arvioida KATAKRI:n käytettävyyttä tarjouslaskentavaiheen turvallisuusjärjestelyissä.

6.1 Pääsy puolustusvoimien turvallisuusvyöhykkeille

Puolustusvoimat on määritellyt tilansa kuuluvaksi neljälle eri turvallisuusvyöhykkeelle. Näiden vyöhykkeiden tarkoituksena on muun muassa estää pääsy salassa pidettäviin tai muutoin arkaluontoisiin aineistoihin mahdollisimman varhaisessa vaiheessa. Turvallisuusjärjestelyt tiukentuvat sitä mukaa, mitä lähemmäs fyysisesti tietoon päästään.

Ensimmäisellä kolmella kysymyksellä (kysymykset 1.1 - 1.3) selvitettiin millaisia turvallisuusjärjestelyitä tulisi olla voimassa tarjouslaskentavaiheessa, jos kilpailutuksen voittavalle palvelun tuottajalle myönnetään toimeksiannon yhteydessä pääsy puolustusvoimien 4 - 2.turvallisuusvyöhykkeen tiloihin. Kysymyksessä ei käsitelty ollenkaan kovimpien turvallisuusjärjestelyiden eli 1. turvallisuusvyöhykkeen tiloja. Kysymykset turvallisuusvyöhykkeistä lisättiin haastatteluun kohdeorganisaation edustajan pyynnöstä, vaikka niistä ei voikaan etsiä vastausta itse tutkimuksen pääkysymykseen. Ne toimivat kuitenkin hyvänä johdantona asiantuntijahaastatteluun ja kuvaavat osaltaan myös problematiikkaa, joka Puolustushallinnon rakennuslaitoksen hankinnoissa täytyy ottaa huomioon.

Mikäli esimerkiksi yrityksen henkilöstöturvallisuusasioihin ei ole kiinnitetty huomiota tarpeeksi aikaisessa vaiheessa, törmätään viimeistään sopimusvaiheessa ongelmiin. Miten varmistua sii-

tä, ovatko palveluntuottajan työntekijät tarpeeksi luotettavia, jotta heidät voidaan päästää työskentelemään puolustusvoimien eri turvallisuusvyöhykkeille?

Kysymysten asettelussa turvallisuusjärjestelyiksi ehdotettiin KATAKRI:n tasojen soveltamista siten, että palvelun suorittamisen edellyttäessä pääsyä 4.turvallisuusvyöhykkeelle, olisi voimassa perustason vaatimukset (kysymys 1.1). Mikäli palvelua suoritettaisiin 3. turvallisuusvyöhykkeellä, voimassa olisivat korotetun tason vaatimukset (kysymys 1.2) ja 2. turvallisuusvyöhykkeellä korkean tason vaatimukset (kysymys 1.3). Asiantuntijoilta kysyttiin tulisiko turvallisuusvyöhykkeellä työskentelyä edellytettäessä käyttää tarjouslaskentavaiheessa vastaavan KATAKRI-tason vaatimuksia:

A. Ei ollenkaan
B. Sovelletusti (miten?)
C. Täysmääräisesti
D. Jotenkin muuten (miten?).

Vastauksista pystytään tarkastelemaan esimerkiksi tulisiko haastateltujen asiantuntijoiden mielestä KATKAKRI:n perustason vaatimukset jättää kokonaan huomioitta silloin, kun pääsy myönnetään 4.turvallisuusvyöhykkeelle (kysymys 1.1, vastausvaihtoehto A), mutta korkean tason vaatimukset taas ottaa täysmääräisesti huomioon silloin, kun pääsy myönnetään 2.turvallisuusvyöhykkeelle (kysymys 1.3, vastausvaihtoehto C). Vastausten jakaantuminen näkyy kuviossa 1.

Kuvio 1 Vastaukset kysymyksiin 1.1 - 1.3

Kolmen vastaajan mielestä KATAKRI:n vaatimuksia tulisi käyttää soveltaen turvallisuusjärjestelyihin tai niihin tulisi kiinnittää huomiota jollain muulla perusteella (vaihtoehdot B ja D) silloin, kun palvelun tuottajalle myönnetään toimeksiannon yhteydessä pääsy puolustusvoimien 4 - 2. turvallisuusvyöhykkeen tiloihin. Kaksi vastaajaa koki, ettei turvallisuusjärjestelyihin tarvitse vielä tarjouslaskentavaiheessa kiinnittää huomiota (vaihtoehto A). Yksikään vastaaja ei kokenut, että KATAKRI:a tulisi soveltaa tarjouslaskentavaiheessa täysmääräisesti (vastausvaihtoehto C) silloin, kun kysymys on palvelun tuottajan pääsyoikeuksista puolustusvoimien turvallisuusvyöhykkeille.

Eräs vastaaja ehdotti, että yrityksen omistajuus tulisi selvittää edellä kuvatuissa tapauksissa jo tarjouslaskentavaiheessa, vaikka varsinaisiin turvallisuusasioihin ei muutoin vielä kiinnitettäisikään huomiota. Ehdokkaiden omistajuuden selvittäminen tarjouslaskentavaiheessa ennaltaehkäisisi mahdollisia omistajuudesta aiheutuvia epäselvyyksiä palveluhankintaprosessin myöhemmissä vaiheissa. Vaatimus ehdokkaiden omistajuuden selvittämisestä olisikin viisasta liittää jo hankintailmoituksen yhteyteen ja asettaa ehdoksi tarjouslaskentavaiheeseen osallistumiselle.

Toinen vastaaja koki, että jos palvelun toteuttaminen edellyttää sidosryhmän työntekijöiden liikkumista puolustusvoimien 4. turvallisuusvyöhykkeellä, tulisi heiltä vaatia vaitiolovakuutus. Jos työntekijöiden täytyisi päästä 3. turvallisuusvyöhykkeelle, tulisi heistä vaitiolovakuutuksen lisäksi tehdä suppea turvallisuusselvitys. Puolustusvoimien 2. turvallisuusvyöhykkeelle pääsyä edellytettäessä, tulisi sidosryhmän työntekijöistä vaitiolovakuutuksen lisäksi tehdä perusmuotoinen turvallisuusselvitys.

Edellä kuvattu järjestely liittyy kuitenkin vasta itse palvelusuoritukseen, eikä siten turvallisuusjärjestelynä ole kovinkaan käytännöllinen vielä tarjouslaskentavaiheessa. Useiden sidosryhmien (joista vain yksi valitaan palvelun tuottajaksi) henkilöstön turvallisuusselvittäminen vaatisi kohtuuttomasti resursseja ja pitkittäisi palveluhankintaprosessia. Perustellumpaa olisikin tarjouslaskentavaiheessa kiinnittää huomiota esimerkiksi sidosryhmän tapaan rekrytoida ja irtisanoa työntekijöitään. KATAKRI:n kriteereistä voisi soveltaa esimerkiksi niitä, jotka keskittyvät sellaisiin toimenpiteisiin, joilla sidosryhmä pyrkii varmistamaan, ettei sen työntekijöille jää työsuhteen päättymisen jälkeen kulkulupia tai avaimia puolustusvoimien turvallisuusluokiteltuihin tiloihin.

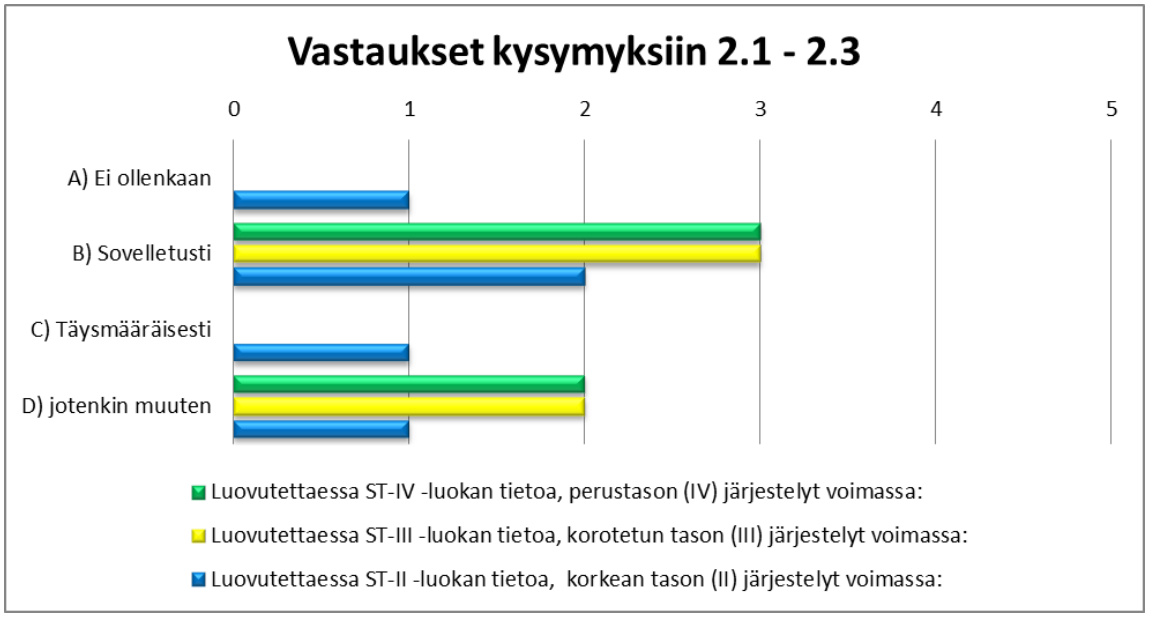
Tosin näidenkään prosessien edellyttäminen tarjouslaskentavaiheessa ei ole välttämätöntä. Riittää kunhan valittu palveluntuottaja sitoutuu toimimaan annettujen menettelyohjeiden mukaisesti palvelusopimuksen allekirjoittamiseen mennessä. Lisäksi varsinaista palvelusuoritusta tehdessä tulisi vaitiolovakuutukset ja turvallisuusselvitykset tehdä aikaisemmin kuvatulla tavalla.

6.2 Turvallisuusluokitellun tiedon luovuttaminen

Seuraavassa kolmessa kysymyksessä (kysymykset 2.1 - 2.3) pyrittiin selvittämään asiantuntijoiden mielipiteitä siitä, millaisia turvallisuusjärjestelyitä tulisi olla voimassa, jos sidosryhmälle luovutetaan tarjouslaskentavaiheessa suojaustasojen (myöhemmin ST) IV-II tietoja. Kysymyksen asettelussa turvallisuusjärjestelyiksi ehdotettiin KATAKRI:n tasojen soveltamista siten, että ST-IV luokan tietoa luovutettaessa olisi voimassa perustason vaatimukset, ST-III luokan tietoa luovutettaessa korotetun tason vaatimukset ja ST-II luokan tietoa luovutettaessa korkean tason vaatimukset. Vastausvaihtoehtoja oli neljä. KATAKRI:n vastaavan tason vaatimukset tulisi huomioida suojaustasojen IV-II tietoja luovutettaessa:

A. Ei ollenkaan
B. Sovelletusti (miten?)
C. Täysmääräisesti
D. Jotenkin muuten (miten?).

Vastauksista pystytään tarkastelemaan esimerkiksi tulisiko haastateltujen asiantuntijoiden mielestä KATKAKRI:n vaatimukset jättää kokonaan huomioitta silloin, kun tarjouslaskentavaiheessa sidosryhmälle luovutetaan ST-IV luokan tietoa (kysymys 2.1, vastausvaihtoehto A), mutta ottaa täysmääräisesti huomioon silloin, kun sidosryhmälle luovutetaan ST-II luokan tietoa (kysymys 2.3, vastausvaihtoehto C). Vastausten jakaantuminen näkyy kuviossa 2.



Kuvio 2 Vastaukset kysymyksiin 2.1 - 2.3

Kun tietoa joudutaan luovuttamaan tarjouslaskentavaiheessa sidosryhmille, vaihtelevat tähän haastatteluun vastanneiden asiantuntijoiden mielipiteet siitä, miten KATAKRI:a tulisi käyttää. Vastausten perusteella selkeää on vain se, ettei ST-IV tai ST-III luokkien tietoa luovutettaessa KATAKRI:n vaatimuksia tarvitse ottaa huomioon täysmääräisesti. Yksi vaihtoehdon B molemmille tasoille vastannut asiantuntija piti tarkoituksenmukaisena henkilö- ja fyysisen turvallisuuden osa-alueiden täysmääräistä soveltamista, sallien kuitenkin lievennykset hallinnollisessa turvallisuudessa. Tietoturvallisuuden vaatimukset hän olisi pitänyt voimassa fyysisten asiakirjojen säilytyksen osalta ja kieltänyt asiakirjojen sähköisen käsittelyn kokonaan. Toinen vaihtoehdon B valinnut vastaaja oli puolestaan valmis soveltamaan kaikkia osa-alueita kevennetysti ja kolmannen ehdotus sovellutuksi järjestelyksi oli:

”Henkilöiden hyväksyntä, vaitiolovakuutus, käsittely- ja säilytysjärjestelyt (aineiston mukaisesti) ja turvallisuuskoulutus oikeista toimintatavoista. Kevennetty menettely ja turvallisuuskartoitus (yrityksen itse tekemä)”.

Vastausvaihtoehdon D valinneet asiantuntijat eivät tarkentaneet, millaisia turvallisuusjärjestelyitä he olisivat asettaneet voimaan ST-IV luokan tietoa luovutettaessa. ST-III luokan tietoa luovutettaessa, olisi toinen heistä käyttänyt henkilöturvallisuuden ja fyysisen turvallisuuden osa-alueita täysmääräisesti ja soveltanut hallinnollisen turvallisuuden ja tietoturvallisuuden osa-alueiden vaatimuksia. Toinen taas kannatti, että ST-III tason tietoihin tutustuttaisiin valvotusti hankkijaorganisaation tiloissa.

ST-II -luokan tiedon luovuttamisesta on vaikea tehdä päätelmiä näiden asiantuntijoiden vastausten perusteella. Yksi vastaaja oli sitä mieltä, että mikäli ST-II -luokan tietoa joudutaan sidosryhmälle luovuttamaan, tällöin myös KATAKRI:n Korkean tason vaatimusten tulee olla täysmääräisesti voimassa. Eräs asiantuntija koki puolestaan, ettei turvallisuusjärjestelyitä tarvita ollenkaan. Vastaajaa tarkensi sanallisesti tarkoittavansa, että turvallisuusjärjestelyitä ei tarvita, koska ST-II -luokan tietoa ei tule luovuttaa sidosryhmälle. Samaa mieltä oli myös vastaaja, joka vastasi vaihtoehdon D. Nämä molemmat ehdottivat, että ST-II -luokan tietoihin tulisi tutustua valvotusti joko Puolustushallinnon rakennuslaitoksen tai puolustusvoimien tiloissa. Kaksi asiantuntijaa oli kuitenkin valmis luovuttamaan sidosryhmälle ST-II tason tietoa siinä määrin, kuin se on tarjouslaskentavaiheen kannalta tarpeellista. Tällöin turvallisuusjärjestelyissä tulisi ottaa huomioon KATAKRI:n korkean tason vaatimukset soveltaen.

Kysymyssarjojen 2.1 - 2.3 yhteenvedoksi tarkoitetussa kysymyksessä 3 kysyttiin vielä: *”Tulisiko KATAKRI:a voida käyttää mielestäsi hankinta- / hankekohtaisesti soveltaen vai pitäisikö sitä käyttää täysmääräisesti kun puolustusvoimien turvallisuusluokiteltua tietoa luovutetaan sidosryhmien käyttöön hankintojen / hankkeiden tarjouslaskentavaiheessa?”*. Vastausvaihtoehtoja oli kolme:

A. Täysmääräisesti
B. Hankinta- / hankekohtaisesti soveltaen
C. Jotenkin muuten (miten?).

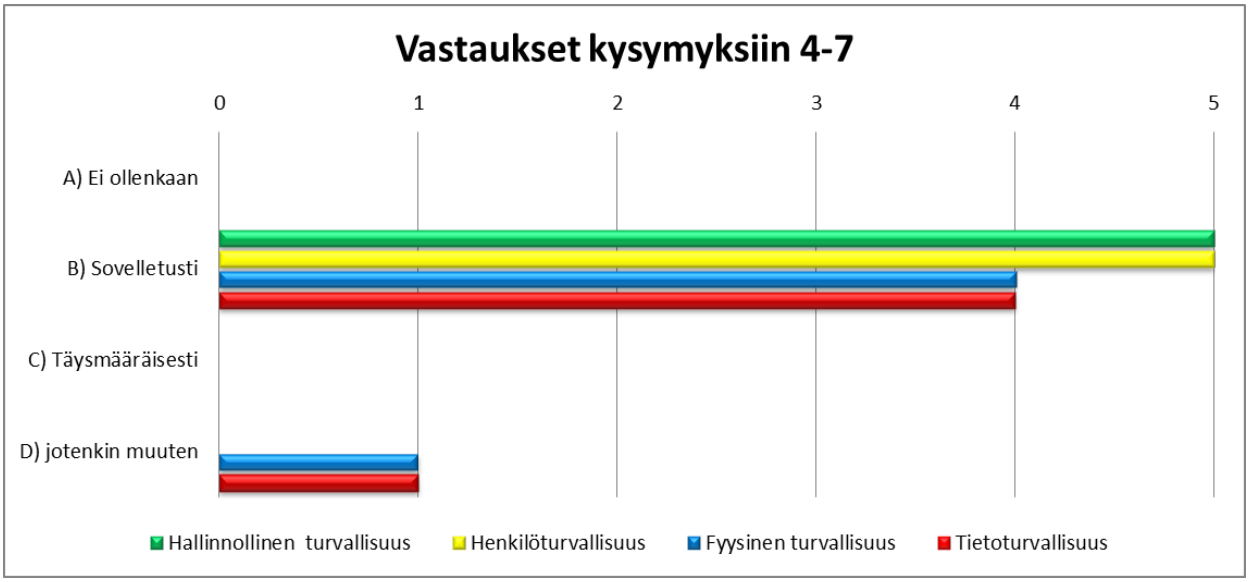
Vastaukset olivat linjassa aikaisempien vastausten kanssa, eikä KATAKRI:n täysmääräinen käyttäminen hankintojen tai hankkeiden tarjouslaskentavaiheessa saanut kannatusta. Kolme vastaajaa olisi ollut valmis soveltamaan KATAKRI:n vaatimuksia aina hankintakohtaisesti (vastausvaihtoehto B). Vaihtoehdon C valinneet kahden vastaajan mielestä organisaation sisäisesti tulisi sopia yksi kevennetty menettely KATAKRI:n vaatimuksista jokaista tiedon luokkaa (ST-IV, ST-III ja ST-II) kohden.

6.3 KATAKRI:n osa-alueiden painopisteet

Esioletuksena oli, etteivät asiantuntijat kannata KATAKRI:n täysmääräistä soveltamista palveluhankintojen tarjouslaskentavaiheessa. Niinpä kysymyksillä 4-7 selvitettiin asiantuntijoiden mielipiteitä siitä, millä KATAKRI:n neljästä turvallisuuden osa-alueesta (Hallinnollinen turvallisuus, Henkilöstöturvallisuus, Fyysinen turvallisuus ja Tietoturvallisuus) turvallisuusjärjestelyiden painopisteen tulisi olla. Vastausvaihtoehtoja oli neljä, tulisiko KATAKRI:n kunkin osa-alueen vaatimukset huomioida tarjouslaskentavaiheessa:

A. Ei ollenkaan
B. Sovelletusti (miten?)
C. Täysmääräisesti
D. Jotenkin muuten (miten?).

Vastauksista pystytään tarkastelemaan tulisiko haastateltujen asiantuntijoiden mielestä KATKAKRI:n vaatimukset jättää kokonaan huomioitta tarjouslaskentavaiheessa esimerkiksi Hallinnollisen turvallisuuden osa-alueelta (kysymys 4, vastausvaihtoehto A), mutta ottaa täysmääräisesti huomioon tietoturvallisuuden osalta (kysymys 7, vastausvaihtoehto C). Vastausten jakaantuminen näkyy kuviossa 3.



Kuvio 3 Vastaukset kysymyksiin 4-7

Haastatteluun vastanneet asiantuntijat eivät kannatteet yhdenkään yksittäisen KATAKRI:n osa-alueen täysmääräistä soveltamista tarjouslaskentavaiheessa. Kolme viidestä vastaajasta koki tärkeäksi, että etenkin sidosryhmien tarjouslaskenta-aineiston käsittelyyn osallistuvan henkilöstön turvallisuuskoulutukseen tulisi kuitenkin panostaa hallinnollisen turvallisuuden vaatimuksia suunniteltaessa.

Turvallisuuskoulutus korostuu etenkin silloin kun sidosryhmälle luovutetaan turvallisuusluokiteltua tietoa. Henkilöille, jotka osallistuvat tarjouslaskenta-aineiston käsittelyyn tulisi antaa tarkat ohjeet turvatoimien tarpeellisuudesta ja niiden täytäntöönpanomenettelyissä. Luokitellun tiedon käsittelystä tulisi luoda selkeä ohjeistus ja tarjouslaskentahenkilöstö tulisi ohjeistaa ja velvoittaa ilmoittamaan havaitsemistaan tietoturvapoikkeamista ja uhista. Turvallisuuskoulutus tulisi myös dokumentoida, jotta hankkija voi varmistua siitä, että koulutuksessa on käyty läpi oikeat asiat.

Henkilöturvallisuuden osa-alueelta tärkeimmiksi järjestelyiksi nousivat asiantuntijoiden vastausten perusteella vaitiolovakuutusten tekeminen sekä turvallisuusselvitykset, jotka kaikki vastanneet kokivat tärkeiksi. Täytyy muistaa, että jos tarjouslaskentaan osallistuu muita kuin Suomen kansalaisia, tulee heistä vaatia henkilöturvallisuustodistus (Personal Security Clearance, PSC). Kappaleessa 6.1 mainittu menettely yrityksen omistajuuden selvittämiseksi sekä menettely myös muiden vastuuhenkilötietojen ja yrityskytkentöjen selvittämiseksi pitäisi olla käytössä ainakin silloin kuin sidosryhmälle luovutetaan ST-III tai ST-II tason tietoja. Sidosryhmällä tulisi viimeistään sopimusvaiheessa olla myös käytössä menettelyohje toimenpiteistä työsuhteen päättyessä (ks. kappale 6.1).

Fyysisen turvallisuuden vaatimukset tulisi vastaajien mukaan ottaa huomioon tarjouslaskentaan käytettävän tilan osalta tarvittavassa laajuudessa. Mikään yksittäinen fyysisen turvallisuuden osa-alue ei noussut vastausten perusteella muita tärkeämmäksi.

Rakenteellisen turvallisuuden ja turvallisuusteknisten järjestelmien osalta KATAKRI:n fyysisen turvallisuuden osa-alueen vaatimukset perustasolla eivät ole vielä kohtuuttoman kovia. Voisi olla käytännöllistä hyväksyä ST-IV -luokan tiedon lisäksi jopa ST-III -luokan tiedon käsittely ja säilytys perustason tilassa, kunhan paperimuotoisen turvallisuusluokitellun aineiston säilytysyksikkönä olisi tarpeeksi jykevä kassakaappi. Vastaavasti jos ST-III -luokan tiedon säilytysyksikkönä toimisi esimerkiksi vain lukittava kaappi, olisi loogista vaatia KATAKRI:n korotetun tason toteutumista rakenteellisen turvallisuuden ja turvallisuusteknisten järjestelmien osalta. KATAKRI:n korkean tason vaatimuksia ei tarvitsisi ottaa ollenkaan huomioon fyysisen turvallisuuden osalta, jos ST-II -luokan tiedon luovuttamista sidosryhmille pyrittäisiin välttämään viimeiseen asti. ST-II -luokan tietoihin voisi tutustua valvotusti joko Puolustushallinnon rakennuslaitoksen tai puolustusvoimien tiloissa.

Muiden osa-alueiden tavoin myös tietoturvallisuudessa pitäisi asiantuntijoiden vastausten perusteella pystyä soveltamaan. Puolustushallinnon rakennuslaitoksen henkilöstön mielestä tärkeitä olivat etenkin paperimuotoisten asiakirjojen käsittelyyn, säilytykseen ja hävittämiseen liittyvät vaatimukset. Vastauksissa painotettiin, että sähköistä materiaalia ei tulisi luovuttaa sidosryhmille hankintojen tarjouslaskentavaiheessa. Tietojärjestelmien ja tietoliikenteen turvallisuuden varmistaminen on aikaa vievä prosessi, joka vaatii erityistä teknistä asiantuntijuutta. Se, että turvallisuusluokiteltuja asiakirjoja ei pidetä sähköisinä tiedostoina, eikä sidosryhmien tietojärjestelmiä tarvitse näin ollen auditoida, säästää siis valtavasti tarjouslaskentavaiheeseen liittyvää työaikaa.

6.4 Turvallisuusjärjestelyiden vaikutus tarjousprosessin etenemiseen

Kysymyksissä 8 ja 9 pyrittiin selvittämään mahdollisia negatiivisia kokemuksia organisaatioiden nykyisten tarjouslaskentavaiheen turvallisuusjärjestelyiden vaikutuksesta tarjousprosessin etenemiseen. Kahdeksas kysymys oli avoin kysymys, jossa pyydettiin vastaajaa kertomaan lyhyesti oman organisaationsa tarjouslaskentavaiheen turvallisuusjärjestelyistä.

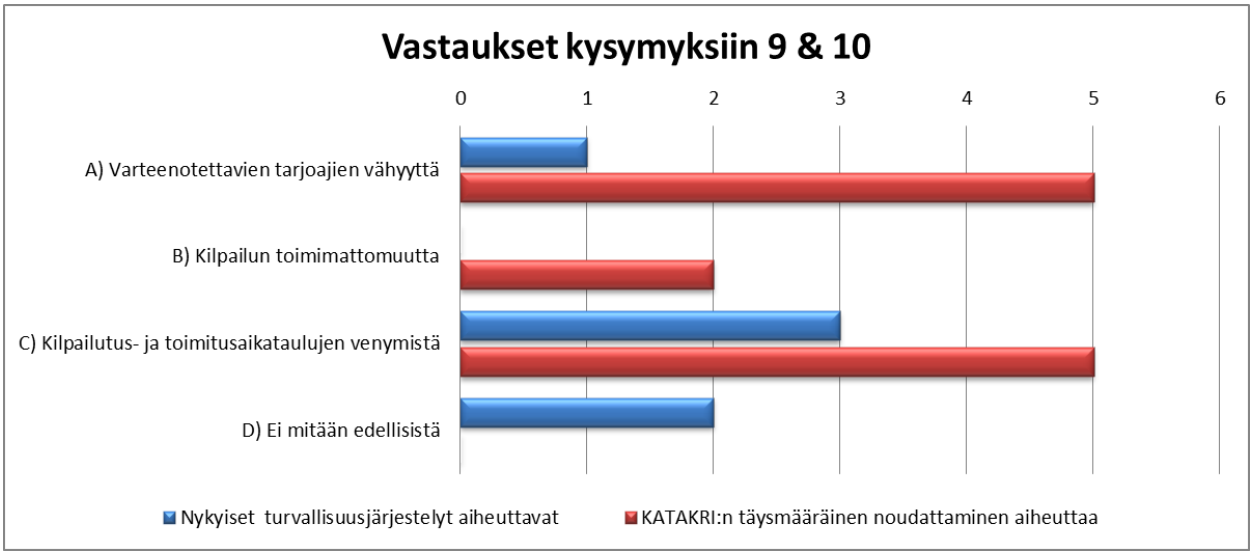
Vastaajien edustamien organisaatioiden turvallisuusjärjestelyt palveluhankintojen tarjouslaskentavaiheessa muistuttivat asiantuntijoiden kuvausten perusteella melko lailla toisiaan. Karkeana yhteenvetona voidaan todeta, että aluksi hankinnasta tehdään hankintasuunnitelma, jossa otetaan kantaa hankinnan turvallisuustasoon. Samassa yhteydessä mietitään, tuleeko tarjouspyyntöön sellaista tietoa, että hankinta vaatii tarjouslaskentavaiheen turvallisuusjärjestelyjä. Lähtökohtaisesti pyritään julkiseen aineistoon.

Tarjouslaskentaa koskevat turvallisuusvaatimukset lähetetään tarjouspyyntötietojen yhteydessä, mikäli vaihe edellyttää turvallisuusluokitellun tietoaineiston luovuttamista. Palveluntarjoaja sitoutetaan turvallisuusjärjestelyihin turvallisuussopimuksella, johon tiedon suojausvaatimukset on yksilöity. Palveluntarjoajan järjestelyt tarkistetaan ennen turvallisuusluokitellun tarjouslaskenta-aineiston luovuttamista. Puolustushallinnon rakennuslaitos tarjoaa pääsääntöisesti sidosryhmilleen myös mahdollisuuden tutustua luokiteltuun aineistoon valvotusti omissa tiloissaan. Lisäksi tarjouspyynnön saajille ilmoitetaan KATAKRI:n taso, joka heidän tulee täyttää jos heidät valitaan kyseisen palvelun tuottajaksi.

Yhdeksännellä kysymyksellä selvitettiin, millaisia negatiivisia vaikutuksia yllä kuvatun kaltaisilla järjestelyillä voisi olla tarjouspyyntöprosessin etenemiselle. Kysymys oli muodoltaan suljettu ja vastausvaihtoehtoja oli neljä. Vastaaja sai halutessaan valita useamman kuin yhden vastausvaihtoehdon. Kysymys kuului: ”Aiheuttavatko tarjouslaskentavaiheen nykyiset turvallisuusjärjestelynne kokemuksesi mukaan usein”:

A. Varteenotettavien tarjoajien vähyyttä
B. Kilpailun toimimattomuutta
C. Kilpailutus- tai toimitusaikataulun viivästymistä / venymistä
D. Ei mitään edellisistä.

Kysymyksessä 10 kysyttiin puolestaan vastaajien mielipidettä siitä, mitä kävisi jos puolustusvoimat antaisi kirjallisen määräyksen, että KATAKRI:a on käytettävä täysmääräisesti aina kun sen turvallisuusluokiteltua tietoa luovutetaan sidosryhmien käyttöön (myös tarjouslaskentavaiheessa). Vastaaja sai valita useamman kuin yhden vastausvaihtoehdon. Vaihtoehdoiksi annettiin samat neljä vaihtoehtoa kuin kysymyksessä 9. Vastaukset kysymyksiin 9 ja 10 näkyvät kuviossa 4.



Kuvio 4 Vastaukset kysymyksiin 9 & 10

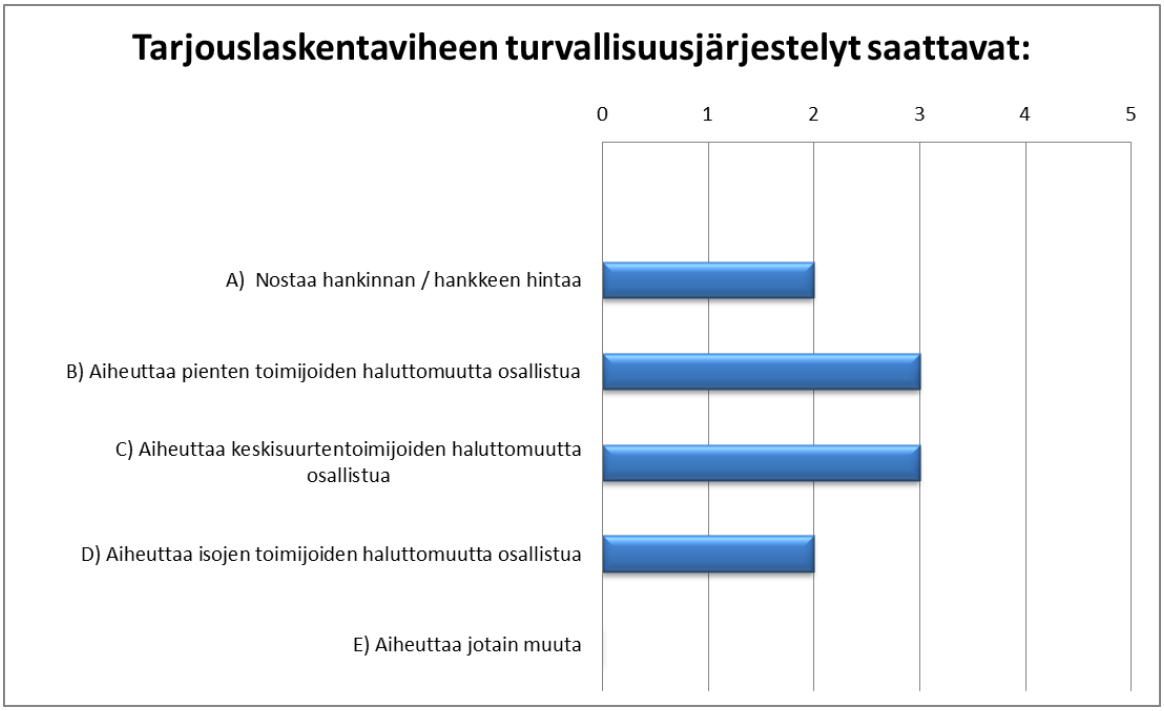
Yksi vastaajista koki, että organisaation nykyiset turvallisuusjärjestelyt sekä karsivat potentiaalisia tarjoajia (vaihtoehto A) että aiheuttavat kilpailutus- ja toimitusaikataulujen venymistä (vaihtoehto C). Kolme vastaajaa oli puolestaan sitä mieltä, että kilpailutus- ja toimitusaikataulut venyvät tarjouslaskentavaiheen turvallisuusjärjestelyiden takia, mutta järjestelyt eivät aiheuta varteenotettavien tarjoajien vähyyttä. Kaksi vastaajaa koki, etteivät turvallisuusjärjestelyt aiheuta mitään edellä kuvattuja negatiivisia vaikutuksia. Erilaiset kokemukset selittyvät paitsi erilaisilla haastateltujen subjektiivisilla kokemuksilla, myös sillä, että heidän edustamiensa organisaatioiden toimintatavat tarjouslaskentavaiheessa eroavat hienoisesti toisistaan.

Ennakko-oletuksen mukaisesti vastanneet asiantuntijat kokivat yksimielisesti, että KATAKRI:n täysmääräinen käyttö palveluhankintojen tarjouslaskentavaiheessa aiheuttaisi sekä kilpailutus- ja toimitusaikataulujen venymistä että karsisi potentiaalisia palveluntarjoajia hankintakilpailuista. Kaksi vastaajaa oli sitä mieltä, että se aiheuttaisi suoranaista kilpailun toimimattomuutta.

Kysymyksessä 11 pyydettiin vielä tarkentamaan yleisesti niitä mahdollisia negatiivisia vaikutuksia, joita tarjouslaskentavaiheen turvallisuusvaatimukset saattavat asiantuntijoiden kokemusten mukaan aiheuttaa. Vastaaja sai valita useamman kuin yhden vastausvaihtoehdon. Vaihtoehtoja oli viisi:

A. Nostaa hankinnan / hankkeen hintaa
B. Aiheuttaa pienten toimijoiden haluttomuutta osallistua kilpailutukseen
C. Aiheuttaa keskisuurten toimijoiden haluttomuutta osallistua kilpailutukseen
D. Aiheuttaa isojen toimijoiden haluttomuutta osallistua kilpailutukseen
E. Aiheuttaa jotain muuta (mitä?)

Kysymys 11 jakoi asiantuntijoiden mielipiteet ja siihen vastasi kolme viidestä haastatellusta. Vastaamatta jättäneiden kahden asiantuntijan kanta on tulkittu siten, etteivät tarjouslaskentavaiheen turvallisuusjärjestelyt heidän kokemuksensa mukaan aiheuta mitään vastausvaihtoehdoissa A-E kuvattua seurausta. Vastaukset kysymykseen 11 näkyvät kuviossa 5.



Kuvio 5 Vastaus kysymykseen 11

Kysymykseen vastanneet kolme asiantuntijaa olivat sitä mieltä, että tarjouslaskentavaiheen turvallisuusjärjestelyt saattavat vaikuttaa palveluntuottajien halukkuuteen osallistua tarjouskilpailuun. Kaikki kolme kokivat, että pienet ja keskisuuret toimijat saattavat olla haluttomia osallistumaan tarjouskilpailuun. Kaksi vastaajaa oli myös sitä mieltä, että isotkin toimijat saattavat karttaa tämän kaltaisia kilpailutuksia. Lisäksi kaksi vastaajaa koki, että turvallisuusjärjestelyt tarjouslaskentavaiheessa saattavat nostaa koko hankinnan hintaa.

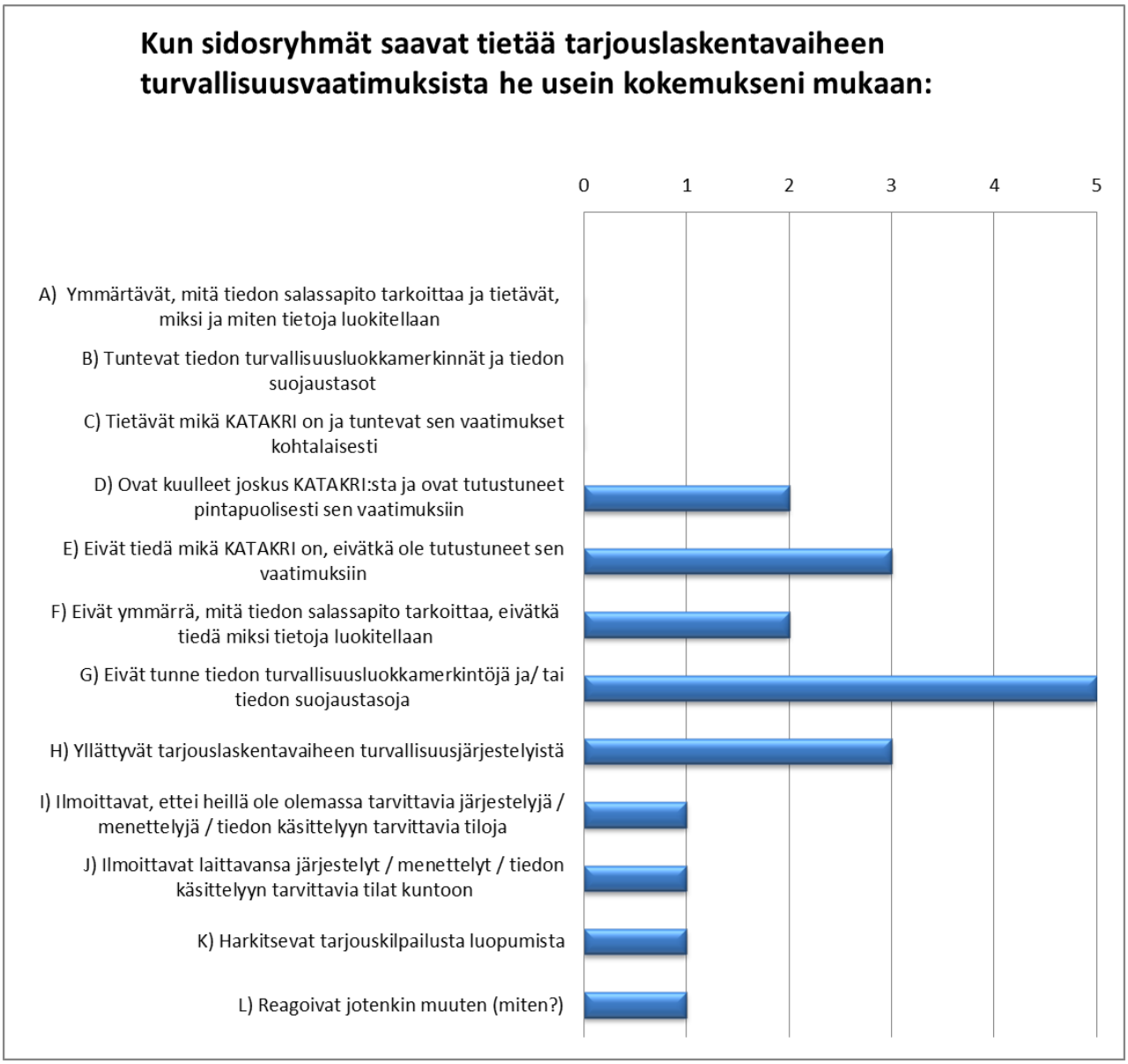
6.5 Sidosryhmien valmius osallistua turvallisuusluokiteltua tietoa sisältäviin hankintoihin

Avoimella kysymyksellä 12 selvitettiin asiantuntijoiden kokemuksia siitä, kuinka hyvin tarjouskilpailuihin osallistumista harkitsevat sidosryhmät todella tiedostavat turvallisuusluokiteltua tietoa sisältävästä hankinnasta tai hankkeesta aiheutuvat velvoitteet. Lisäksi kysymyksellä selvitettiin ymmärtävätkö sidosryhmät, että jo tarjouslaskentavaiheeseen osallistuminen saattaa aiheuttaa heille lisätyötä ja kustannuksia. Lisäksi kysymyksessä 13 tiedusteltiin miten vastaajien organisaatiot pyrkivät omia sidosryhmiään niiden turvallisuusjärjestelyissä tukemaan.

Kolme viidestä vastanneesta asiantuntijasta oli sitä mieltä, etteivät tarjouskilpailuihin osallistuvat yritykset tiedosta velvoitteita, eivätkä osaa ennakoida hankinnan turvallisuusjärjestelyistä aiheutuvia lisätöitä tai -kustannuksia. Kaksi vastaajaa puolestaan koki, että pääsääntöisesti velvoitteet ja lisäkustannukset tiedostetaan, kunhan turvallisuusvaatimuksista on ennakkokysely- ja tarjouspyyntövaiheessa tiedotettu tarpeeksi selvästi ja yksityiskohtaisesti. Ongelmia on aiheuttanut lähinnä aikaisempien turvallisuusjärjestelyiden kirjavuus.

Haastateltujen asiantuntijoiden edustamat organisaatiot pyrkivät tukemaan omia sidosryhmiään lähinnä tiedottamalla turvallisuusasioista hankintojen yhteydessä. Puolustusvoimat pitää omille sidosryhmilleen myös satunnaisesti turvallisuuskoulutusta. Eräs asiantuntija koki, että turvallisuustietoisuuden parantamiseksi olisi hedelmällistä järjestää turvallisuusasioihin painottuneita tiedotustilaisuuksia sidosryhmille.

Kysymyksellä 14 selvitettiin asiantuntijoiden mielipiteitä siitä, miten sidosryhmät, joilla ei ole ennestään yhteistyötä ja/tai turvallisuussopimusta puolustusvoimien kanssa, reagoivat saadessaan tietää tarjouslaskentavaiheen turvallisuusjärjestelyistä. Vastausvaihtoehtoja oli 12 ja niiden jakaantumisen on nähtävissä kuviossa 6.



Kuvio 6 Vastaukset kysymykseen 14

Tähän haastatteluun vastanneiden asiantuntijoiden kokemuksen mukaan palveluhankintojen tarjouskilpailuihin osaa ottavat yritykset eivät useinkaan tunne tiedon turvallisuusluokkamerkintöjä tai tiedon suojaustasoja. Yritykset eivät myöskään välttämättä ymmärrä mitä tiedon salassapito tarkoittaa tai tiedä miksi tietoja luokitellaan. Kolmen vastaajan mielestä yritykset yllättyvät tarjouslaskentavaiheen turvallisuusjärjestelyistä; KATAKRI:sta on ehkä kuultu, mutta se ei ole yrityksille tuttu ja sen vaatimuksiin on tutustuttu korkeintaan pintapuolisesti.

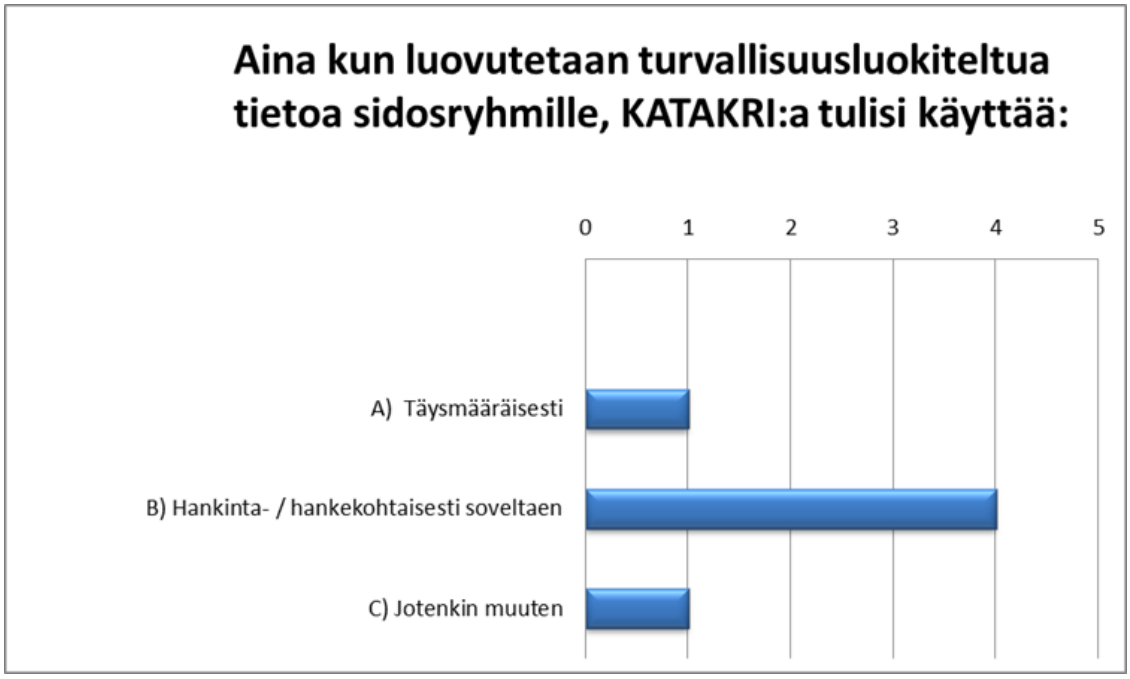
6.6 Hankintojen turvallisuusjärjestelyiden aiheuttamat haasteet

Avoimessa kysymyksessä 15 kysyttiin: ”Minkälaisia turvallisuusvaatimuksista johtuvia ongelmia tai haasteita olette havainneet hankintojen / hankkeiden tarjouslaskentavaiheiden yhteydessä?” Ongelmaksi koettiin muun muassa se, että mikäli turvallisuusluokiteltua tietoa joudutaan kilpailutukseen osallistuville yrityksille luovuttamaan, voidaan hankintamenettelyinä käyttää ainoastaan rajoitettua- tai neuvottelumenettelyä, jotka ovat aikaa vieviä. Toinen ongelmaksi mainittu seikka liittyi tilojen järjestämiseen tarjouslaskentahenkilöstölle, mikäli palveluntarjoaja haluaa tutustua tarjouslaskenta-aineistoon hankkijan tiloissa. Lisäksi henkilöt tarvitsevat tällöin niin sanotun päällystakin eli henkilön, joka valvoo tarjouslaskennan suorittamista.

Tarjouskilpailuun osallistuvat yritykset, jotka haluavat turvallisuusluokitellun tarjouslaskenta-aineiston haltuunsa, saattavat puolestaan totuudenvastaisesti tulkita omat turvallisuusjärjestelynsä riittäviksi ja puutteet paljastuvat vasta auditioinnin yhteydessä. Tilat saatetaan myös ilmoittaa aikaisemmin auditoiduksi jonkun muun hankinnan tai hankkeen yhteydessä, mutta auditoinnit tai niiden dokumentointi ovat olleet puutteellisia, eivätkä ne ole välttämättä ole perustuneet KATAKRI:n vaatimuksiin.

Tarjouslaskentaan tarkoitettujen sidosryhmien tilojen auditoinnit tai tilojen järjestäminen sidosryhmien henkilöstölle on kuitenkin sujuvan hankintaprosessin kannalta järkevää. Hankintakohtaisen turvallisuustason toteutuminen olisi erään asiantuntijan mukaan mahdollista taata myös siten, että kaikilta yrityksiltä, jotka osallistuvat tarjouslaskentaan edellytettäisiin turvallisuussopimusta Puolustushallinnon rakennuslaitoksen tai puolustusvoimien kanssa. Tällöin vastaajan mukaan hankinnat ja hankkeiden käynnistyminen venyisivät kuitenkin suhteettomasti.

Kysymyksessä 16 kysyttiinkin asiantuntijoiden suoraa kantaa siihen tulisiko KATAKRI:a käyttää täysmääräisesti **aina** kun puolustusvoimien turvallisuusluokiteltua tietoa luovutetaan sidosryhmien käyttöön. Kysymys 16 oli muodoltaan suljettu ja vastausvaihtoehtoja oli kolme. Niiden jakaantumien on nähtävissä kuviossa 7:



Kuvio 7 Vastaus kysymykseen 16

Asiantuntijat eivät kannattaneet KATAKRI:n täysmääräistä käyttämistä hankintojen tarjouslaskentavaiheessa (kysymys 3), eikä täysmääräinen käyttö saa kannatusta muissakaan tilanteissa, joissa puolustusvoimien turvallisuusluokiteltua tietoa luovutetaan sidosryhmille. Yksi henkilö vastasi sekä A että B vaihtoehdon. Vastaaja kuitenkin tarkensi sanallisesti, että KATAKRI:a on käytettävä täysmääräisesti ainoastaan, mikäli hankinta edellyttää jatkuvaa kumppanuutta juuri tietyn yrityksen kanssa. Tämä tulee kyseeseen lähinnä tietyissä erikoisosaamista vaativissa palveluissa. Muussa tapauksessa KATAKRI:a tulisi kyseisen asiantuntijan mukaan käyttää hankintakohtaisesti soveltaen. Myös vaihtoehdon C valinnut vastaaja tarkensi, että KATAKRI:a tulisi käyttää yhteistyön laajuus huomioon ottaen. Muut kolme vastaajaa kannattivat hankintakohtaista soveltamista.

6.7 Sidosryhmien edustajien kokemuksia tarjouslaskentavaiheen turvallisuusjärjestelyistä

Kahden yrityksen edustajat vastasivat sidosryhmille lähetettyyn kyselyyn. Molemmat olivat sitä mieltä, että heidän edustamillaan organisaatioilla oli hyvät valmiudet osallistua sellaisen palveluhankinnan tarjouslaskentavaiheeseen, joka sisältää puolustusvoimien turvallisuusluokiteltua tietoa. Molemmat vastanneet kokivat, että heidän edustamassaan yrityksessä ymmärrettiin mitä tiedon salassapito ja luokittelu tarkoittaa sekä tunnettiin tiedon turvallisuusluokkamerkinnät ja tiedon suojaustasot.

Toisessa yrityksessä tiedettiin entuudestaan mikä KATAKRI on ja tunnettiin sen vaatimukset kohtalaisesti. Toisessa KATAKRI vaatimuksineen ei puolestaan ollut tuttu. Molemmat vastaajat

vakuuttivat, että yrityksessä tiedostettiin palveluhankinnan tarjouskilpailuun osallistumista harkitessa, että turvallisuusluokiteltua tietoa sisältävästä hankinnasta aiheutuu tiettyjä velvoitteita palveluntuottajalle. Molemmissa yrityksissä vastaajien mukaan myös ymmärrettiin, että jo tarjouslaskentavaiheeseen osallistuminen saattaa aiheuttaa yritykselle lisätyötä ja kustannuksia.

Kummallakaan yrityksellä ei ollut osoittaa tarjouslaskentavaiheeseen omaa tilaa, joka olisi täyttänyt PHRAKLE-S:n vaatiman fyysisen turvallisuuden tason. Vastaajien mukaan se ei saanut kuitenkaan yrityksiä luopumaan tarjouskilpailuista. Toinen vastaajista kertoi yrityksensä valinneen sellaisen toimintatavan, jossa turvallisuusluokiteltuihin tietoihin tutustuttiin PHRAKLE-S:n tiloissa. Samaisesta yrityksessä myös ilmoitettiin, että PHRAKLE-S:n vaatimusten mukaisen turvatilan rakentaminen olisi ollut mahdollista, mutta se olisi aiheuttanut kuitenkin merkittäviä lisäkustannuksia. Molemmat vastaajat pitivät kyseiseen palveluhankintaan liittyneitä KATAKRI:in perustuvia turvallisuusvaatimuksia sopivina, kaikille tasapuolisina sekä oman yrityksensä turvallisuustoimintaa tukevina mahdollisina kilpailuvaltteina.

Kysyttäessä millaisena sidosryhmän edustajat näkevät KATAKRI:n vaatimukset yleisesti, molemmat vastaajat pitivät vaatimuksia sopivina ja kaikille tasapuolisina, helposti ennakoitavina sekä yrityksen omaa turvallisuustoimintaa tukevina mahdollisina kilpailuvaltteina. Molemmat olivat kuitenkin sitä mieltä, että vaatimukset myös nostavat kaikkien osapuolten kustannuksia palveluhankintojen yhteydessä. Toinen vastaajista koki myös, että vaatimukset saattavat viivästyttää kilpailutus- ja toimitusaikatauluja.

Kumpikaan vastaajista ei kokenut KATAKRI:n vaatimusten olevan kilpailua haittaava tekijä tai ylimääräinen riesa. Molemmat olivat sitä mieltä, että KATAKRI:a tulisi kuitenkin käyttää vain hankintakohtaisesti soveltaen. Tärkeää oli vastaajien mukaan etenkin se, että tilaajaorganisaatio on osannut tunnistaa tiedon suojaustarpeen ja luokitella tiedon oikein. Vain todella suojattava tieto tulisi turvallisuusluokitella ja suojausvaatimukset tulisi kohdistaa vain kyseiseen tietoon. Toinen vastaajista piti mahdollisena, että jos Puolustushallinnon rakennuslaitos edellyttäisi sidosryhmiltään KATAKRI:n Perustason täyttämistä aina luovuttaessaan puolustusvoimien turvallisuusluokiteltua tietoa sidosryhmiensä käyttöön, jo Perustason vaatimukset harventaisivat mahdollista palveluntarjoajien joukkoa, kovemmista vaatimuksista puhumattakaan.

7 Johtopäätökset

Turvallisuus on huomioitava aina kun puolustusvoimien turvalllisuusluokiteltua tietoa luovutetaan sidosryhmille. Sidosryhmien tulisi sisäistää tämä harkitessaan osallistumista puolustusvoimien turvallisuusluokiteltua tietoa sisältävän palveluhankinnan kilpailutukseen. Palvelun hankkijan tulisi tähdentää sidosryhmille jo palveluhankintojen tietopyyntö- eli RFI-vaiheessa, että turvallisuusluokitellusta tarjouslaskenta-aineistosta saattaa aiheutua ehdokkaille turvallisuusjärjestelyistä johtuvia lisätöitä ja -kustannuksia. Tärkeää on, että tilaajaorganisaatio osaa tunnistaa tiedon suojaustarpeen ja luokitella tiedon oikein. Vain todella suojattava tieto tulee turvallisuusluokitella ja suojausvaatimukset tulee kohdistaa vain kyseiseen tietoon.

Mikäli turvallisuusluokiteltu tieto paljastuu oikeudettomasti hankintaprosessin aikana, voi seurauksena olla sekä hankkijan että palvelun tarjoajan edustajien syyllistyminen rikoslaissa rangaistavaksi säädettyihin tekoihin. Lisäksi pahimmassa tapauksessa myös maanpuolustuksen etu saattaa vaarantua. Verkottuneessa yhteiskunnassa tiedon oikeanlaisen luokittelun, suojaamisen ja jakelun merkitys korostunee entisestään teknologian kehittyessä.

Kansallinen turvallisuusauditointikriteeristö on ensisijaisesti luotu viranomaisten työvälineeksi yhteisöturvallisuusmenettelyyn (Puolustusministeriö 2011, 2-3.). Tämän tutkimuksen perusteella voidaan todeta, ettei sen täysmääräinen käyttäminen ole järkevää puolustusvoimien turvallisuusluokiteltua tietoa sisältävien palveluhankintojen tarjouslaskentavaiheessa. Havainto vahvistaa tutkimuksen esioletuksen. Kun sidosryhmälle tehdään turvallisuuskartoitus ennen turvallisuusluokitellun tiedon luovuttamista, on KATAKRI:n kriteerien käyttäminen sovelletusti (yhteistyön laatu ja syvyys huomioon ottaen) kuitenkin perusteltua. KATAKRI:n kriteerit ovat nimittäin helposti ennakoitavissa ja yhtenäistävät viranomaisten vaihtelevia käytäntöjä.

Luovutettavien tietojen suojaustaso määrittää turvallisuusjärjestelyiden tason. Luomalla suojausvaatimukset KATAKRI:n kriteerien pohjalta, PHRAKLE-S pystyy tukemaan hankintaprosessiin osallistuvia ja myöhemmin mahdolliseen yhteisöturvallisuusmenettelyyn tai turvallisuussopimusjärjestelyyn hakeutuvia sidosryhmiään. Turvallisuusjärjestelyiden ollessa kaikille tasapuolisia ja helposti ennakoitavia, voivat yritykset entistä paremmin arvioida kilpailutukseen osallistumisesta aiheutuvia kustannuksia. Lisäksi yritykset pystyvät prosessin edetessä varautumaan portaittain lopullisiin turvallisuussopimuksen mukaisiin vaatimuksiin.

Turvallisuusjärjestelyiden tulee kattaa turvallisuusluokitellun tiedon koko elinkaari hankintaprosessin aikana. Suojausvaatimusten tulee olla voimassa tietojen luomisen, muokkaamisen, käytön, luovutuksen, säilyttämisen, arkistoinnin ja hävittämisen ajan. Jotta turvallisuusluokiteltu tieto on suojattu asianmukaisesti palveluhankintojen tarjouslaskentavaiheessa, tulee vähintään seuraaviin seikkoihin kiinnittää huomiota:

1. Yrityksen omistajuus ja vastuuhenkilöt on selvitettävä. ST-III ja ST-II tason tietoja luovutettaessa myös yrityskytkennät tulee selvittää.

2. Yritykseltä tulee vaatia dokumentointi siitä, että tarjouslaskentavaiheeseen osallistuvalle henkilöstölle on annettu tarvittava turvallisuuskoulutus. Koulutuksen sisältö tulee määritellä hankintakohtaisesti. PHRAKLE-S:n edustajan tulee toimia kouluttajana luovutettaessa ST-III tai ST-II tason tietoja.

3. Tarjouslaskentaan osallistuvilta henkilöiltä on vaadittava aina vaitiolovakuutus. ST-III ja ST-II tason tietoja luovutettaessa tulee henkilöistä tehdä myös turvallisuusselvitys.

4. Jos tarjouslaskentaan osallistuu muita, kuin Suomen kansalaisia, tulee heiltä vaatia henkilöturvallisuustodistus (PSC).

5. Tarjouslaskentaan käytettävän tilan tulee täyttää fyysiselle turvallisuudelle asetetut vaatimukset. Yrityksille on taattava myös jatkossa mahdollisuus tutustua tarjouslaskenta-aineistoon valvotusti PHRAKLE-S:n tiloissa.

    a. ST-IV tietoja luovutettaessa tulisi olla voimassa KATAKRI:n fyysisen turvallisuuden perustason vaatimukset

    b. ST-III tietoja luovuttaessa tulisi olla voimassa KATAKRI:n fyysisen turvallisuuden perustason vaatimukset, jos tiedon säilytysyksikkönä on korotetun tason mukainen kassakaappi tai holvi ja tila on valvottu rikosilmoitinjärjestelmällä korotetun tason mukaisesti. Mikäli säilytysyksikkö tai rikosilmoitinjärjestelmä ei täytä korotetun tason vaatimuksia, tulee muita fyysisen turvallisuuden korotetun tason vaatimuksia soveltaa täysmääräisesti.

    c. ST-II tason tietoja luovutetaan ainoastaan, jos yrityksellä on jo ennestään osoittaa tarjouslaskentaan KATAKRI:n korkean tason mukaan auditoitu tila. Muutoin ST-II tason tietoon tutustutaan valvotusti PHRAKLE-S:n tiloissa.

6. Turvallisuusluokiteltua tietoa ei tule käsitellä tietojärjestelmissä.

7. Turvallisuusluokiteltua tietoa ei tule luovuttaa muille kuin erikseen mainitulle tarjouslaskentaan osallistuvalle henkilöstölle, johon pätee kohdassa kolme esitetyt vaatimukset. Aineistosta ei tehdä kopioita.

8. Jos tarjouslaskennan yhteydessä luodaan uusia asiakirjoja, jotka sisältävät turvallisuusluokiteltua tietoa, luokitellaan ne vastaavan suojaustason mukaisesti.

9. Tarjousten välittäminen postitse ja turvallisuusluokitellun tarjouslaskenta-aineiston tuhoaminen suoritetaan erikseen PHRAKLE-S:n ohjeiden mukaan.

10. Yrityksen työntekijöiden rekrytointiin ja työsuhteen päättämiseen liittyviin toimenpiteisiin tulee kiinnittää huomiota viimeistään varsinaista palvelusopimusta tehdessä.

Se, että palvelun hankkija osaa valita tarkoituksenmukaiset suojausvaatimukset KATAKRI:sta, vaatii niin kaupallista ymmärrystä kuin turvallisuusalan tuntemustakin. Mikäli kriteerien valinnassa epäonnistutaan, voi asiantuntijoiden kokemuksen mukaan seurauksena olla niin varteen otettavien tarjoajien vähyyttä kuin kilpailutus- ja toimitusaikataulujen venymistäkin. Liitteessä 6 on ehdotus soveltuvista KATAKRI:n kriteereistä, joiden käyttöä tulisi harkita Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikön hankintojen tarjouslaskentavaiheessa.

8 Pohdinta

Tämän tutkimuksen perustana oli kohdeorganisaation tarve saada käyttöönsä sellaista informaatiota, jota se voi käyttää hyväkseen tarkastellessaan omien turvallisuusjärjestelyidensä tarkoituksenmukaisuutta palveluhankintojen tarjouslaskentavaiheessa. Tutkimuksen tarve oli aito ja työelämälähtöinen.

Tutustuttaessa aikaisempaan tutkimukseen kävi ilmi, ettei aihepiiristä ole tieteellistä tutkimusta. Tämä toisaalta vahvisti tutkimusaukon olemassaolon ja kuvaa hyvin ilmiön luonteen haasteellisuutta. Pään vaivaa aiheuttivat kysymykset siitä, miten julkisessa opinnäytetyössä olisi hedelmällistä käsitellä salassa pidettävien tietojen suojausvaatimuksia, mihin vaatimusten tulisi perustua ja miten näiden vaatimusten toimivuutta voisi mitata?

Koska absoluuttista totuutta siitä, milloin turvallisuusluokiteltu tieto on riittävästi suojattu, on hankala määritellä ja vielä hankalampi mitata, päädyttiin tutkimuksessa selvittämään asiantuntijoiden kokemuksia aihepiiristä. Laadullinen tutkimus, jossa lähtökohtana on todellisen elämän kuvaaminen ja tavoitteena ilmiön ymmärtäminen, eikä niinkään ilmiön mittaaminen, oli siis tutkimusotteena validi.

Validiteetilla eli tutkimuksen pätevyydellä ja luotettavuudella tarkoitetaan perinteisesti tutkimuksen kykyä, selvittää sitä, mitä sillä on tarkoitus selvittää. Validiteettia arvioitaessa kohdistetaan yleensä huomio kysymykseen, miten hyvin tutkimusote ja siinä käytetyt menetelmät vastaavat sitä ilmiötä, jota halutaan kuvata. (Anttila 2006, 512–513.)

Fenomenologinen lähestymistapa sopi ilmiön tutkimiseen, sillä fenomenologiassa maailmaan keskitytään sellaisena kuin ihminen sen kokee. Jotta kohdeorganisaation esittämä toivomus tutkijan omasta tulkinnasta olisi myös metodologisesti perusteltu, päädyttiin näkökulmaa täydentämään hermeneutiikalla. Hermeneuttisen tutkimuksen kohdetta kutsutaan usein tekstiksi. Tekstillä voidaan tarkoittaa kaikkia sellaisia seikkoja, joihin voi latautua merkityksiä, kuten esimerkiksi puhetta, kuvia ja tapahtumien kuvauksia (Anttila 2006, 549). Tässä tutkimuksessa tekstinä toimi haastatteluaineisto.

Hermeneuttisen lähestymistavan voi tulkita jossain määrin nakertavan tämän tutkimuksen validiteettia, sillä sitä ei valittu siksi, että se olisi ollut paras tapa lähestyä haastatteluaineistoa. Tulkintaa painotettiin kohdeorganisaation toivomuksesta ja tulkinnallisuutta on tutkimuksessa pyritty perustelemaan hermeneutiikalla. Näin hermeneutiikasta kuitenkin muodostuu tutkimuksessa vain yleiskäsite tulkinnallisuudelle. Tässä mielessä hermeneutiikka -käsitteen käyttö on kuitenkin Anttilan (2006, 549) mukaan epätarkkaa. Tutkimuksessa hermeneuttinen dialogi, tutkijan ja tekstin välinen vuoropuhelu, jää hyvin pinnalliseksi. Sen si-

jaan hermeneutiikkaan olennaisesti liittyvä tutkijan esiymmärrys ja tutkimuksen eteneminen hermeneuttisella kehällä tuodaan onnistuneesti esiin. Tämä tuo lisäarvoa lukijalle, joten hermeneuttisesta lähestymistavasta puhuminen ei johda lukijaa harhaan.

Tulkinnallisen ulottuvuuden voi myös katsoa heikentävän tutkimuksen reliabiliteettia, koska tutkija ei tyydy tutkimaan ilmiötä objektiivisesti. Reliabiliteetilla tarkoitetaan tutkimusmenetelmän ja mittareiden kykyä saavuttaa tarkoitettuja tuloksia. Onkin perusteltua kysyä, voiko mittareiden antamiin tuloksiin luottaa, jos tutkija lisää niihin omia subjektiivisia merkityssisältöjään? Tähän haasteeseen on pyritty vastaamaan kuvaamalla asiantuntijahaastatteluiden eteneminen mahdollisimman tarkasti ja liittämällä käytetyt kyselylomakkeet tutkimuksen liitteiksi (ks. liitteet 4 ja 5). Lukijalle on näin taattu mahdollisuus arvioida tutkijan päättelyä ja kritisoida sitä. Haastattelukysymykset ovat toistettavissa ja siten tutkimuksen reliabiliteetti on hyvä.

Haastatteluaineisto olisi tosin uskottavampi ja koko tutkimus luotettavampi, jos haastatellut asiantuntijat olisi mainittu tutkimuksessa nimeltä. Se olisi kuitenkin ristiriidassa tutkimusetiikan kanssa. Anttila (2006, 186) toteaakin, että joskus puuttuminen haastateltujen integriteettiin kohottaa tulosten luotettavuutta, mutta vaarantaa tutkimuksen eettiset arvot. Asiantuntijoille haluttiin taata anonymiteetti, jotta he pystyivät vastaamaan kysymyksiin rehellisesti pelkäämättä vastustensa seurauksia. Näin menettelemällä pystyttiin takaamaan, ettei mahdollisten ”väärien” mielipiteiden esittämisestä tullut haastatelluille asiantuntijoille ikäviä seurauksia omissa organisaatioissaan.

Mikäli useampi puolustusvoimien edustaja olisi vastannut asiantuntijahaastatteluun, olisi ollut mielenkiintoista verrata heidän vastauksiaan Puolustushallinnon rakennuslaitoksen henkilökunnan vastauksiin. Näin olisi ollut mahdollista verrata kahden erilaisen organisaation tapoja toimia ja opinnäytetyön heuristinen arvo, kyky löytää uusia näkökulmia, olisi ollut suurempi.

Yhteenvetona voidaan todeta, että tutkimuksen validiteetti on hyvä mutta tutkimus ei ole täysin reliaabeli. Haastateltujen asiantuntijoiden anonymiteetin takia muiden kuin tutkijan ei ole mahdollista toistaa tutkimusta täysin samanlaisena. Tämä opinnäytetyö täyttää tästä huolimatta sille asetetut tavoitteet luoden kohdeorganisaatiolle hyödyllistä taustainformaatiota vastaamalla asetettuihin tutkimuskysymyksiin.

8.1 Tutkimustulokset sidosryhmäturvallisuutta ohjaavina tekijöinä

Tietoaineiston luokittelu on viranomaisympäristössä tietoturvallisuusmenettelyn raskain vaihe. Kaikki tietoaineisto tulisi selata läpi, minkä jälkeen on päätettävä, mitkä tiedot luokitellaan salassa pidettäviksi lainsäädännön perusteella. Tietojen luokittelu on kuitenkin peruste tiedon tosiasialliselle salassapidolle. Suojausvaatimuksia mietittäessä olennaista on tieto ja tiedon merkitys — ei sen olomuoto. Tieto tulee suojata samojen periaatteiden mukaan, olipa se paperilla, sähköisessä muodossa tai puhuttuna sanana.

Tässä opinnäytetyössä esiteltiin turvallisuusjärjestelyiden perustaksi kymmenen kohtaa, jotka tulisi huomioida puolustusvoimien turvallisuusluokiteltua tietoa sisältävissä palveluhankinnoissa. Liitteessä 6 on ehdotus soveltuvista KATAKRI:n kriteereistä, joiden käyttöä tulisi harkita tarkempia suojausvaatimuksia mietittäessä. Kohdeorganisaatiota suositellaan tarkastamaan omat turvallisuusjärjestelynsä tämän opinnäytetyön tulosten pohjalta.

Lisäksi organisaatiota suositellaan kehittämään turvallisuusasioihin liittyvää sidosryhmäviestintäänsä. Sidosryhmien yleinen tiedotus olisi järkevää järjestää yhteistyössä puolustusvoimien kanssa. Esimerkiksi kerran vuodessa järjestettävät ”turvallisuuspäivät”, jossa keskityttäisiin vuosittain tietyn palvelualan turvallisuusasioihin, voisi olla toimiva konsepti. Turvallisuuspäivät tarjoaisivat puolustusvoimien sidosryhmätyöskentelystä kiinnostuneille yrityksille mahdollisuuden parantaa omaa turvallisuusosaamistaan. Sitä kautta parantuisivat myös niiden mahdollisuudet tarjota entistä parempia palveluita puolustusvoimille.

8.2 Jatkotutkimus

Tässä opinnäytetyössä tarkasteltiin viiden asiantuntijan mielipiteitä tutkimuskohteena olevasta ilmiöstä. Mikäli tutkimuksen tuloksista haluaisi tehdä yleistyksiä, tulisi haastatteluaineiston otantaa kasvattaa merkittävästi. Tämä tarjoaisi myös mahdollisuuden tarkastella henkilöiden mielipiteiden eroja määrällisesti. Määrällisen analyysin jälkeen olisi mahdollista vetää johtopäätöksiä siitä, miten henkilön tausta vaikuttaa hänen asenteeseensa ilmiön suhteen. Kvalitatiivisesta sisällön analyysistä olisi näin mahdollista siirtyä kvantitatiiviseen sisällön erittelyyn.

Opinnäytetyöprosessi herätti myös ideoita jatkotutkimukselle. KATAKRI:n tunnettavuus puolustusvoimien sidosryhmien keskuudessa olisi kokonaan oman tutkimuksensa arvoinen aihe. Samassa tutkimuksessa olisi mielenkiintoista selvittää sidosryhmien mielipiteitä KATAKRI:n kriteerien käytettävyydestä – aihealue, jota vain raapaistiin tämän työn puitteissa. Olisi myös äärimäisen mielenkiintoista, joskin kenties menetelmällisesti mahdotonta, tutkia mitkä ovat olleet aidosti tehokkaita keinoja turvallisuusluokiteltujen tietojen suojaamisessa.

Lähteet

Kirjalliset lähteet:

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

Helin, K. 2002. Puolustushallinnon rakennuslaitoksella oikea suunta. Muuriankkuri – Puolustushallinnon rakennuslaitoksen sidosryhmälehti. Joulukuu 2002. Hamina: Puolustushallinnon rakennuslaitos. 18–20.

Helin, K. 2004. Haasteellinen kiinteistöuudistus vaatii kaikkien osapuolien sitoutumista. Muuriankkuri – Puolustushallinnon rakennuslaitoksen sidosryhmälehti. Kesäkuu 2004. Hamina: Puolustushallinnon rakennuslaitos. 14–16.

Hirsjärvi, S. Remes, P. & Sajavaara, P. 2012. Tutki ja kirjoita. 15.–17. painos. Helsinki: Tammi.

Hytönen, T. & Lehtomäki, L. 2010. Valtion hankintakäsikirja 2010. Helsinki: Valtiovarainministeriö.

Puolustushallinnon rakennuslaitos 2013a. Henkilötilinpäätös 2012. Hamina: Puolustushallinnon rakennuslaitos.

Puolustushallinnon rakennuslaitos 2013b. Toimintakertomus ja tilinpäätöslaskelmat 2012. Hamina: Puolustushallinnon rakennuslaitos.

Puolustusministeriö 2007. Puolustusministeriön turvallisuustoiminnan strategia. Helsinki: Puolustusministeriö.

Puolustusministeriö 2011. Kansallinen turvallisuusauditointikriteeristö - KATAKRI, versio II. Helsinki: Puolustusministeriö.

Kyberturvallisuusstrategia 2013. Valtioneuvoston periaatepäätös 24.1.2013. Helsinki: Turvallisuuskomitean sihteeristö.

Vapaavuori, T. 2012. Yrityssalaisuudet ja salassapitosopimukset. Helsinki: Talentum.

Yhteiskunnan turvallisuusstrategia 2010. Valtioneuvoston periaatepäätös 16.12.2010. Helsinki: Puolustusministeriö.

Sähköiset lähteet:

Arkistolaki 23.9.1994/831. Viitattu 12.05.2013.
http://www.finlex.fi/fi/laki/ajantasa/1994/19940831#L6

HE 30/1998. Hallituksen esitys. Yleisperustelut. Viitattu 12.5.2013.
http://217.71.145.20/TRIPviewer/show.asp?tunniste=HE+30/1998+Yleisperustelut+2/2&base=erhe&palvelin=www.eduskunta.fi&f=WP

HE 66/2004. Hallituksen esitys. Yleisperustelut. Viitattu 12.5.2013.
http://217.71.145.20/TRIPviewer/show.asp?tunniste=HE+66/2004&base=erhe&palvelin=www.eduskunta.fi&f=WORD

Laki julkisista hankinnoista 30.3.2007/348. Viitattu 12.05.2013.
http://www.finlex.fi/fi/laki/ajantasa/2007/20070348#L8P56

Laki kansainvälisistä tietoturvavelvoitteista 24.6.2004/588. Viitattu 12.05.2013.
http://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621. Viitattu 12.05.2013.
http://www.finlex.fi/fi/laki/ajantasa/1999/19990621#L6P25

Puolustushallinnon rakennuslaitos 2012. Organisaatio: Etelä-Suomi. Viitattu 12.5.2013.
http://www.phrakl.fi/phrakl/Publish.nsf/$all/91B1B33B7244AF8CC2256FC700495C3B

Puolustusministeriö 2009. Puolustushallinnon turvallisuus – osastrategia. Viitattu 12.5.2013.
http://www.defmin.fi/files/1833/turvallisuusstrategia.pdf

Pääesikunnan tutkintaosasto 2012. DSA (Designated Security Authority) – tehtävät puolustusvoimissa. Viitattu 15.9.2012.
http://www.puolustusvoimat.fi/portal/puolustusvoimat.fi/paaesikunta/dsa

Rikoslaki 19.12.1889/39. Viitattu 12.05.2013.
http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Saulio, L. 2012. Turvallisuus puolustusvoimien turvaluokiteltua tietoa sisältävissä rakennushankkeissa. Viitattu 12.5.2013.
http://www.doria.fi/bitstream/handle/10024/77305/E4232_SaulioLP_EUK64.pdf?sequence=1

Simi, J. 2010. Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus. Viitattu 12.5.2013.
https://aaltodoc.aalto.fi/bitstream/handle/123456789/99/urn100170.pdf?sequence=1

Ulkoasiainministeriö 2013. Kansallinen turvallisuusviranomainen (National Security Authority, NSA). Viitattu 15.9.2013.
http://formin.finland.fi/Public/default.aspx?nodeid=46935&contentlan=1&culture=fi-FI

Valtioneuvoston asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta 12.11.1999/1030. Viitattu 12.05.2013.
http://www.finlex.fi/fi/laki/ajantasa/1999/19991030

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Viitattu 12.4.2013. http://www.finlex.fi/fi/laki/ajantasa/2010/20100681

VAHTI 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Viitattu 15.9.2013.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/02_Ohje_tietotuvallisuudesta_valtionhallinnossa.pdf

Julkaisemattomat lähteet:

Asiantuntijahaastattelu 25.5.2013

Sidosryhmähaastattelu 17.6.2013

Kuvat

Kuviot

Taulukot

Liitteet

Liite 1 Tutkimuksessa käytetyt keskeiset käsitteet

Erityissuojattava tietoaineisto
Erityissuojattavalla tietoaineistolla tarkoitetaan salassa pidettäviä asiakirjoja ja materiaaleja, niistä saatavissa olevia tietoja sekä niiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka on turvallisuusluokiteltu kansainvälisen tietoturvallisuusvelvoitteen mukaisesti. (Laki kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588, 2§ 2k).

Fyysinen turvallisuus
Fyysisellä turvallisuudella tarkoitetaan laitteiden, aineistojen, varastojen ja toimitilojen turvallisuutta tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää rakenteellisen turvallisuuden, kulunvalvonnan, teknisen valvonnan ja vartioinnin sekä palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan. (Puolustusministeriö 2007, 21.)

Hallinnollinen turvallisuus
Hallinnollisella turvallisuudella tarkoitetaan turvallisuustoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. (Puolustusministeriö 2007, 21.)

Hankinta
Hankinnalla tarkoitetaan palveluiden ostamista ja vuokraamista sekä urakalla teettämistä näihin liittyvine suunnittelu-, valmistelu-, päätöksenteko- ja seurantatoimintoineen. (Hytönen & Lehtomäki 2010, 29.)

Henkilöstöturvallisuus
Henkilöstöturvallisuudella tarkoitetaan henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen järjestelyihin liittyvien turvallisuustekijöiden hoitamista (Puolustusministeriö 2007, 21).

Henkilöturvallisuustodistus (Personal Security Clearance, PSC)
Henkilöturvallisuusselvityksessä toimivaltainen viranomainen tarkastaa kohteena olevan henkilön taustatiedot laissa säädetyillä menettelyllä. Turvallisuusselvitys voidaan tehdä myös suomalaisen yrityksen palveluksessa olevasta ulkomaalaisesta, mutta tällöin on otettava huomioon, että suomalaisilla viranomaisilla on rajalliset mahdollisuudet henkilön taustan selvittämiseen. (Kansallinen turvallisuusviranomainen 2011, 22.)

Kun turvallisuusselvityksen kohteena on ulkomaalainen tai ulkomailla asuva tai asunut suomalainen, ilmoitetaan turvallisuusselvityksen tuloksen yhteydessä se, miltä ajanjaksolta viranomaisilla on ollut tietoa käytössään. Kansallinen turvallisuusviranomainen on pitänyt turvallisuusselvityksen perusteella annettavan PSC-todistuksen myöntämisen edellytyksenä sitä, että henkilö on asunut Suomessa viimeiset viisi vuotta todistuksen antamista edeltävänä ajanjaksona. (Kansallinen turvallisuusviranomainen 2011, 23.)

Kansallinen turvallisuusviranomainen (National Security Authority, NSA)
Suomessa kansallisena turvallisuusviranomaisena toimii ulkoasiainministeriö. Sen tehtävänä on kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaisesti ohjata ja valvoa, että Suomelle toimitettu kansainvälinen turvallisuusluokiteltu tieto suojataan ja sitä käsitellään asianmukaisesti. Kansallinen turvallisuusviranomainen koordinoi määrättyjen kansallisten turvallisuusviranomaisten toimintaa ja työskentelee yhteistyössä niiden kanssa. Se myös myöntää kansainväliset henkilöturvallisuustodistukset (Personnel Security Clearance, PSC) ja yritysturvallisuustodistukset (Facility Security Clearance, FSC) sekä käsittelee vierailulupapyynnöt (Request for Visit, RfV). (Ulkoasiainministeriö 2013.)

Puolustusministeriö, pääesikunta ja suojelupoliisi toimivat määrättyinä turvallisuusviranomaisina (Designated Security Authority, DSA), joille on jaettu omat vastuualueet kansallisen turvallisuusviranomaisen kokonaisvastuukentästä. Viestintävirasto toimii määrättynä tietoliikenneturvallisuusviranomaisena (National Communication Security Authority, NCSA) niissä tapa-

uksissa, joissa on kyse teknisestä tietoturvallisuudesta ja tietoliikenteen turvallisuudesta. (Pääesikunnan tutkintaosasto 2012.)

KATAKRI
Kansallinen turvallisuusauditointikriteeristö.

Tarjouslaskentavaihe (Tarjouspyyntövaihe, RFQ)
Tässä opinnäytetyössä tarjouslaskentavaihetta käytetään synonyyminä tarjouspyyntövaiheelle. Vaiheeseen kuuluu Valtion hankintakäsikirjan (2011, 31) tarjouspyynnön laatiminen ja lähettäminen, jonka jälkeen vaiheeseen osallistuvat yritykset suorittavat tarjouspyynnön perusteella tarjouslaskennan ja tekevät tarjouksen. Lisäksi vaiheeseen kuuluu pääsääntöisesti tarjousten vastaanotto ja avaaminen, tarjoajien soveltuvuuden arviointi avoimessa menettelyssä, tarjousten tarjouspyynnön mukaisuuden vertailu sekä tarjousten vertailu (Hytönen & Lehtomäki 2010, 31).

Tiedon käsittely
Tiedon käsittelyllä tarkoitetaan tässä opinnäytetyössä kaikkia tietoon kohdistettuja toimenpiteitä sen koko elinkaaren aikana. Tiedon käsittelyyn sisältyy muun muassa sen säilyttäminen, siirtäminen, kopioiminen, luovuttaminen, jakelu sekä tuhoaminen.

Tiedon luokittelu / Tietoaineiston luokitus
Tiedon luokittelulla tarkoitetaan tietoaineiston jakelua ja käyttöä rajaavaa luokittelujärjestelmää, joka pohjautuu julkisuuslainsäädäntöön ja salassapitosäädöksiin. Salassa pidettävä aineisto arvioidaan ja luokitellaan tietoturvallisuus- ja tietosuojanäkökohtien perusteella. Aineisto luokitellaan sen mukaan, minkälaisia seurauksia salassa pidettävän tiedon paljastuminen ulkopuolisille tai sen mahdollinen väärinkäyttö saattaisi aiheuttaa suojattaville intresseille. (Puolustusministeriö 2007, 27.)

Tietoturvallisuus
Tietoturvallisuudella tarkoitetaan tietojen korkean käytettävyyden, hallitun eheyden sekä lain ja sopimusten mukaisen luottamuksellisuuden turvaamista hyvää tiedonhallintatapaa noudattaen. Se on niiden keinojen muodostama kokonaisuus, joiden avulla tietoriskejä minimoidaan. (Puolustusministeriö 2007, 27)

Turvallisuusjärjestelyt
Turvallisuusjärjestelyillä tarkoitetaan tässä tutkimuksessa tiedon suojausvaatimusten muodostamaa kokonaisuutta, jolla pyritään takaamaan tiedon tosiasiallinen salassapito.

Turvallisuusluokittelu
Valtioneuvoston tietoturvallisuudesta valtiohallinnossa antaman asetuksen 11–12 §:ssä pykälissä säädetään, että salassa pidettävän asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tietyissä tapauksissa tehdä erityinen turvallisuusluokitusmerkintä. Turvallisuusluokitusmerkintää (ks. liite 3) saa käyttää vain niissä asiakirjoissa, jotka ovat salassa pidettäviä julkisuuslain 24.1 §:n kohtien 2 ja 7-10 tai kansainvälisistä tietoturvallisuusvelvoitteista annetun lain perusteella. (VAHTI 2/2010, 76.)

Turvallisuusselvitys
Turvallisuusselvitys voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä. Turvallisuusselvitysmenettelyn tarkoituksena on ehkäistä rikoksia, jotka voisivat vahingoittaa vakavasti Suomen sisäistä tai ulkoista turvallisuutta, maanpuolustusta tai poikkeusoloihin varautumista, Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, julkista taloutta, yksityisen huomattavan arvokasta liike- tai ammattisalaisuutta tai muuta tähän rinnastettavaa erittäin merkittävää yksityistä taloudellista etua, taikka edellä mainittujen etujen suojaamisen kannalta erittäin merkittävää tietoturvallisuutta. Turvallisuusselvitys voidaan tehdä perusmuotoisena, laajana tai suppeana. (Laki turvallisuusselvityksistä, 1-2§.)

Turvallisuussopimus
Puolustusvoimien tai puolustushallinnon rakennuslaitoksen nimissä tehty turvallisuussopimus, jossa sovitaan sidosryhmän osalta turvallisuusjärjestelyt tilanteissa, joissa sidosryhmän kanssa tehtävän yhteistoiminnan myötä sille joudutaan luovuttamaan puolustusministeriön hallinnonalan salassa pidettävää tietoa tai materiaalia. Turvallisuussopimuksen allekirjoittaa puolustusvoimien puolesta Pääesikunnan tutkintaosaston päällikkö, puolustushallinnon rakennuslaitoksen puolesta valmiuspäällikkö ja sidosryhmän puolesta allekirjoitusvaltuuden omaava henkilö, yleensä toimitusjohtaja. (Puolustusministeriö 2007, 27.)

Turvallisuusvyöhyke
Turvallisuusvyöhykkeellä tarkoitetaan tässä opinnäytetyössä sellaisia luokiteltuja alueita, joiden tarkoituksena on muun muassa estää pääsy salassa pidettäviin tai muutoin arkaluontoisiin aineistoihin mahdollisimman varhaisessa vaiheessa. Turvallisuusvaatimukset tiukentuvat turvallisuusvyöhykkeiden vaihtuessa sitä mukaa, mitä lähemmäs fyysisesti tietoon päästään.

Palveluhankinta
Laissa julkisista hankinnoista (30.3.2007/3489) 5§:n neljännessä kohdassa on määritelty palveluhankintasopimuksen tarkoittavan: ”muuta kuin julkista rakennusurakkaa tai julkista tavarahankintaa koskevaa sopimusta, jonka kohteena on palvelujen suorittaminen”. Palveluhankinnalla tarkoitetaan tässä opinnäytetyössä siis työsuoritusta eli palvelua, joka hankitaan tilaajaorganisaation ulkopuoliselta palveluntuottajalta.

PHRAKLE-S
Puolustushallinnon rakennuslaitos, Etelä-Suomen alue

Salassa pidettävä tieto
Salassa pidettävä tieto on informaatiota, joka on tarkoitettu vain tiettyjen henkilöiden käyttöön ja määrätty lain nojalla salassa pidettäväksi joko yleisen tai yksityisen edun suojelemiseksi. Viranomaisen asiakirja on pidettävä salassa, jos se julkisuuslaissa tai muussa laissa on säädetty salassa pidettäväksi tai jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. (Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621, 6 luku 22§.)

Sidosryhmäturvallisuus
Sidosryhmäturvallisuuden päämääränä on ensi sijassa turvata maanpuolustuksen edun vuoksi salassa pidettävä tieto ja toiminta sekä torjua sidosryhmistä puolustushallinnon toimijoille aiheutuvat riskit toimittaessa yhteistyössä puolustusministeriön hallinnonalan ulkopuolisten toimijoiden kanssa. Sidosryhmäturvallisuudella suojataan myös puolustusministeriön hallinnonalan tietoon tulevia yhteistyökumppaneiden liikesalaisuuksia. (Puolustusministeriö 2007, 8.)

Suojausvaatimus
Suojausvaatimuksella tarkoitetaan tässä tutkimuksessa, yksilöityä vaatimusta tietystä toimenpiteestä, jolla pyritään ehkäisemään tiedon oikeudeton paljastuminen. Suojausvaatimukset perustuvat tässä tutkimuksessa KATAKRI:in.

Yhteisöturvallisuus (-menettely & -todistus)
Yhteisöturvallisuusmenettelyllä tarkoitetaan tässä opinnäytetyössä prosessia, joka tähtää yhteisöturvallisuustodistuksen myöntämiseen. Yhteisöturvallisuustodistus (Facility Security Clearance, FSC) voidaan myöntää yritykselle sen omasta tai ulkomaisen turvallisuusviranomaisen virallisesta pyynnöstä, jos yritys aikoo esimerkiksi osallistua kansainväliseen hankintakilpailuun, johon liittyy kansainvälisten tietoturvallisuusvelvoitteiden mukaisen salassa pidettävän tiedon tai materiaalin käsittelyä. Todistuksen myöntämiseksi yrityksen turvallisuustaso kartoitetaan ja sen tiloihin suoritetaan fyysistä turvallisuutta koskeva auditointi. Henkilöstöstä voidaan tehdä turvallisuusselvityksiä ja lisäksi yrityksen tietojärjestelmien turvallisuuden taso tarkastetaan. Tarvittaessa toimenpiteet voidaan kohdistaa myös yrityksen hyödyntämien alihankkijoiden tiloihin ja tietojärjestelmiin. Suomessa yhteisöturvallisuustodistuksen myöntää pääsääntöisesti Suojelupoliisi. (Pääesikunnan tutkintaosasto 2012.)

Liite 2 Aihepiiriin olennaisesti liittyvä lainsäädäntö

Arkistolaki (831/1994)
Arkistolaissa säädetään arkistolaitoksesta, arkistotoimesta ja sen järjestämisestä, asiakirjojen laatimisesta, säilyttämisestä ja käyttämisestä sekä lain tarkoittamista yksityisistä arkistoista. Arkistolaki koskee valtion virastoja, laitoksia sekä muita valtion viranomaisia sekä kunnallisia viranomaisia ja toimielimiä, Suomen Pankkia, Kansaneläkelaitosta sekä muita itsenäisiä julkisoikeudellisia laitoksia ja yliopistolaissa (558/2009) tarkoitettuja säätiöyliopistoja, valtion ja kunnan liikelaitoksia sekä ortodoksista kirkkokuntaa ja sen seurakuntia. Lisäksi laki koskee muita yhteisöjä, toimielimiä ja henkilöitä niiden suorittaessa julkista tehtävää lain tai asetuksen taikka lain tai asetuksen nojalla annetun säännöksen tai määräyksen perusteella siltä osin, kuin niille annetun tehtävän johdosta kertyy viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) tarkoitettuja asiakirjoja. (arkistolaki, 1 §.)

Eduskuntaan, eduskunnan oikeusasiamiehen kansliaan, valtiontalouden tarkastusvirastoon ja kansainvälisten suhteiden ja Euroopan unionin asioiden tutkimuslaitokseen sovelletaan vain lain tiettyjä osia. Tasavallan presidentin ja evankelis-luterilaisen kirkon arkistoista sekä Ahvenanmaan maakunnissa toimivien viranomaisten arkistoista säädetään erikseen muualla lainsäädännössä. (arkistolaki, 1-2 §.)

Laki julkisista hankinnoista (348/2007, hankintalaki)
Valtion ja kuntien viranomaisten sekä muiden hankintayksiköiden on kilpailutettava hankintansa siten kuin hankintalaissa säädetään. Lain tavoitteena on tehostaa julkisten varojen käyttöä, edistää laadukkaiden hankintojen tekemistä sekä turvata yritysten ja muiden yhteisöjen tasapuolisia mahdollisuuksia tarjota tavaroita, palveluita ja rakennusurakointia julkisten hankintojen tarjouskilpailuissa. (hankintalaki 1 §.)

Laki kansainvälisistä tietoturvavelvoitteista
(588/2004, kansainvälinen tietoturvallisuusvelvoite)
Kansainvälisen yhteistyön syventyessä, myös Suomessa on jouduttu miettimään, miten suojata arkaluontoisia asiakirjoja ja miten tulisi toimeenpanna kansainväliseen arkaluonteisten tietoaineistojen suojaamiseen liittyvät toimenpiteet. Tämä on edellyttänyt asiaa sääntelevän yleislain luomista. (HE 66/2004.)

Kansainvälisistä tietoturvavelvoitteista annetussa laissa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Sitä sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana. (kansainvälinen tietoturvallisuusvelvoite, 1 §.)

Laki puolustusvoimista (551/2007)
Puolustusvoimista annetussa laissa säädetään puolustusvoimien tehtävistä, toimivallasta, organisaatiosta, hallinnosta, sotilaskäskyasioiden päätöksentekojärjestelmästä ja henkilöstöstä. Lain 15 §:ssä säädetään liikkumista koskevista kielloista ja rajoituksista puolustusvoimien käytössä olevalla alueella. (Laki puolustusvoimista, 1 §.)

Laki turvallisuusselvityksistä (177/2002)
Turvallisuusselvityksistä annetussa laissa säädetään turvallisuusselvityksestä, joka voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä. Turvallisuusselvitys voidaan tehdä perusmuotoisena, laajana tai suppeana. (Laki turvallisuusselvityksistä, 1§.)

Lain tarkoituksena on selvityksen kohteena olevan henkilön yksityiselämän suoja ja henkilötietojen suoja huomioon ottaen 1 §:ssä tarkoitettua turvallisuusselvitysmenettelyä käyttämällä parantaa mahdollisuuksia ennakolta estää rikokset, jotka vakavasti vahingoittaisivat Suomen sisäistä tai ulkoista turvallisuutta, maanpuolustusta tai poikkeusoloihin varautumista,

Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, julkista taloutta, yksityisen huomattavan arvokasta liike- tai ammattisalaisuutta tai muuta tähän rinnastettavaa erittäin merkittävää yksityistä taloudellista etua, taikka aiemmin mainittujen etujen suojaamisen kannalta erittäin merkittävää tietoturvallisuutta. (Laki turvallisuusselvityksistä, 2§.)

Laki viranomaisten toiminnan julkisuudesta (621/1999, julkisuuslaki)
Viranomaisten asiakirjat ovat julkisia, jollei viranomaisten toiminnan julkisuudesta annetussa laissa tai muussa laissa erikseen toisin säädetä. Julkisuuslaissa säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista samoin kuin viranomaisten velvollisuuksista julkisuuslain tarkoituksen toteuttamiseksi. (julkisuuslaki, 1-2§.)

Julkisuuslaissa säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan. (julkisuuslaki, 3 §.)

Rikoslaki (39/1889)
Rikoslaissa säädetään Suomen rikosoikeuden soveltamisalasta, eri rikoksista, rangaistuksista ja niiden määräämisestä, sakosta, muuntorangaistuksesta sekä rikesakosta, ehdollisesta vankeudesta, vankeudesta ja rikosoikeudellisen vastuun edellytyksistä sekä vastuuvapausperusteista, osallisuudesta rikokseen ja yrityksestä tehdä rikos. Lisäksi laissa säädetään muun muassa yhteisestä rangaistuksesta, rikoksen vanhentumisesta sekä oikeushenkilön rangaistusvastuusta ja erilaisista menettämisseuraamuksista. (rikoslaki, 1luku - 9 luku.)

Valtioneuvoston asetus julkisista hankinnoista (614/2007)
Valtioneuvoston julkisista hankinnoista antamassa asetuksessa annetaan tarkempia säännöksiä hankintalaissa ja erityisalojen hankintalaissa (349/2007) edellytetyistä hankintojen ilmoitusvelvoitteista, ilmoitusten sisällöstä, ilmoitusten lähettämisestä, julkaisemisesta ja muista viestintään sekä ilmoitusvelvollisuuteen liittyvistä seikoista sekä velvollisuudesta toimittaa hankinnoista tilastotietoja ja muita selvityksiä Suomen viranomaisille ja Euroopan unionin toimielimille. (Valtioneuvoston asetus julkisista hankinnoista, 1§.)

Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa (681/2010, tietoturva-asetus)
Valtioneuvoston antamassa asetuksessa tietoturvallisuudesta valtiohallinnossa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista. (tietoturva-asetus, 1§.)

Valtioneuvoston asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta (1030/1999)
Valtioneuvoston antaman asetuksen viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta 8-10§:ssä säädetään hyvän tiedonhallintatavan toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta ja edistämisestä sekä valtiohallinnon viestinnästä. (Valtioneuvoston asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta, 1-8 §.)

Liite 3 Tiedon suojaustasot ja turvallisuusluokkamerkinnät

Tiedon suojaustasot:

Valtioneuvoston tietoturvallisuudesta valtiohallinnossa antaman asetuksen 9 §:ssä pykälässä määrätään, että salassa pidettävien asiakirjojen luokittelussa tulee käyttää seuraavia luokkia:

1) suojaustaso I, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;

2) suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;

3) suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle;

4) suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle.

Salassapitotahto ja tiedon suojaustaso voidaan ilmaista salassapitoleimalla (ks. kuva alla). Leimaan kirjoitetaan joko käsin tai koneellisesti suojaustasoa osoittava numero. Salassa pidettävä -leimaa käytetään asiakirjoissa, jotka sisältävät joko julkisuuslain 24.1 §:n kohdissa 1, 3 - 6 sekä 11 - 32 tai muussa laissa määriteltyä salassa pidettävää tietoa. Tämän lisäksi leimaa voidaan käyttää suojaustasolla IV asiakirjoihin, jotka sisältävät viranomaisharkintaan tai käyttötarkoitussidonnan alaista luokiteltavaa tietoa. (VAHTI 2/2010, 76.)

Turvallisuusluokkamerkinnät:

Valtioneuvoston tietoturvallisuudesta valtiohallinnossa antaman asetuksen 11–12 §:ssä pykälissä säädetään, että salassa pidettävän asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tietyissä tapauksissa tehdä erityinen turvallisuusluokitusmerkintä. Turvallisuusluokitusmerkintä tehdään joko suomeksi, ruotsiksi tai englanniksi:

1) suojaustasoon I kuuluvaan asiakirjaan merkitään "ERITTÄIN SALAINEN"; tai ”YTTERST HEMLIG”; tai ”TOP SECRET”’

2) suojaustasoon II kuuluvaan asiakirjaan merkinnällä ”SALAINEN”; tai ”HEMLIG”; tai ”SECRET”

3) suojaustasoon III kuuluvaan asiakirjaan merkinnällä ”LUOTTAMUKSELLINEN”; tai ”KONFIDENTIELL”; tai ”CONFIDENTIAL”

4) suojaustasoon IV kuuluvaan asiakirjaan merkinnällä ”KÄYTTÖ RAJOITETTU”; tai ”BEGRÄNSAD TILLGÅNG”; tai ”RESTRICTED”.

Turvallisuusluokitusmerkintää (ks. kuva alla) saa käyttää vain niissä asiakirjoissa, jotka ovat salassa pidettäviä julkisuuslain 24.1 §:n kohtien 2 ja 7-10 tai kansainvälisistä tietoturvallisuus-velvoitteista annetun lain perusteella. Kansainvälisiin turvallisuusluokiteltuihin aineistoihin on tehtävä aina turvallisuusluokkaa osoittava merkintä. (VAHTI 2/2010, 76.)

Liite 4 Asiantuntijahaastattelun kyselylomake

Vastauksiani saa käyttää muun lähdemateriaalin ohella
julkisessa opinnäytetyössä siten, etteivät vastaukseni ole yksilöitävissä: **Kyllä / Ei**

Toimenkuva:
Organisaatio:

Tässä lomakkeessa pyritään selvittämään hankintojen turvallisuusjärjestelyiden parissa työskentelevien asiantuntijoiden henkilökohtaisia mielipiteitä. Vastaukset annetaan nimettömänä. Vastauksia käsitellään opinnäytetyössä siten, ettei vastaajan henkilöllisyys, toimenkuva tai organisaatio ole yksilöitävissä tai pääteltävissä yksittäisen mielipiteen osalta. Haastatteluaineisto jää vain tutkijan omaan käyttöön.

Jollei toisin mainita, tämän lomakkeen kysymykset koskevat sellaisia sidosryhmiä, joilla ei ole turvallisuussopimusta puolustusvoimien / yksikkönne kanssa.

1.1) Jos kilpailutuksen voittavalle palvelun tuottajalle / urakoitsijalle myönnetään toimeksiannon yhteydessä pääsy puolustusvoimien 4.turvallisuusvyöhykkeen tiloihin, tulisiko KATAKRI:n Perustason (IV) vaatimuksia mielestäsi käyttää hankintojen tarjouslaskentavaiheen turvallisuusjärjestelyissä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

1.2) Jos kilpailutuksen voittavalle palvelun tuottajalle / urakoitsijalle myönnetään toimeksiannon yhteydessä pääsy puolustusvoimien 3.turvallisuusvyöhykkeen tiloihin, tulisiko KATAKRI:n Korotetun tason (III) vaatimuksia mielestäsi käyttää hankintojen tarjouslaskentavaiheen turvallisuusjärjestelyissä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

1.3) Jos kilpailutuksen voittavalle palvelun tuottajalle / urakoitsijalle myönnetään toimeksiannon yhteydessä pääsy puolustusvoimien 2.turvallisuusvyöhykkeen tiloihin, tulisiko KATAKRI:n Korkean tason (II) vaatimuksia mielestäsi käyttää hankintojen tarjouslaskentavaiheen turvallisuusjärjestelyissä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

2.1) Jos sidosryhmälle luovutetaan tarjouslaskentavaiheessa ST-IV tason tietoja, tulisiko KATAKRI:n Perustason (IV) tason vaatimuksia mielestäsi käyttää hankintojen tarjouslaskentavaiheen turvallisuusjärjestelyissä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

2.2) Jos sidosryhmälle luovutetaan tarjouslaskentavaiheessa ST-III tason tietoja, tulisiko KATAKRI:n Korotetun tason (III) tason vaatimuksia mielestäsi käyttää hankintojen tarjouslaskentavaiheen turvallisuusjärjestelyissä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

2.3) Jos sidosryhmälle luovutetaan tarjouslaskentavaiheessa ST-II tason tietoja, tulisiko KATAKRI:n Korkean tason (II) vaatimuksia mielestäsi käyttää hankintojen tarjouslaskentavaiheen turvallisuusjärjestelyissä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

3. Tulisiko KATAKRI:a voida käyttää mielestäsi hankinta- / hankekohtaisesti soveltaen vai pitäisikö sitä käyttää täysmääräisesti kun puolustusvoimien turvallisuusluokiteltua tietoa luovutetaan sidosryhmien käyttöön hankintojen tarjouslaskentavaiheessa?

a) Täysmääräisesti
b) Hankekohtaisesti soveltaen
c) Jotenkin muuten [miten?]

4. Tulisiko mielestäsi KATAKRI:n Hallinnollisen turvallisuuden osa-alueen vaatimukset huomioida hankintojen tarjouslaskentavaiheen turvallisuusvaatimusten yhteydessä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

5. Tulisiko mielestäsi KATAKRI:n Henkilöstöturvallisuuden osa-alueen vaatimukset huomioida hankintojen tarjouslaskentavaiheen turvallisuusvaatimusten yhteydessä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

6. Tulisiko mielestäsi KATAKRI:n Fyysisen turvallisuuden osa-alueen vaatimukset huomioida hankintojen tarjouslaskentavaiheen turvallisuusvaatimusten yhteydessä:

a) ei ollenkaan
b) sovelletusti: [miten?]
c) täysmääräisesti
d) jotenkin muuten: [miten?]

7. Tulisiko mielestäsi KATAKRI:n Tietoturvallisuuden osa-alueen vaatimukset huomioida hankintojen tarjouslaskentavaiheen turvallisuusvaatimusten yhteydessä:

a) ei ollenkaan
b) sovelletusti: [miten?]

c) täysmääräisesti
d) jotenkin muuten: [miten?]

8. Kuvaile lyhyesti tarjouslaskentavaiheen nykyisiä turvallisuusjärjestelyjänne (jos yksikkönne ei tee hankintoja, älä vastaa tähän kysymykseen):

9. Aiheuttavatko tarjouslaskentavaiheen nykyiset turvallisuusjärjestelynne kokemuksesi mukaan usein (voit vastata useamman vaihtoehdon - mikäli ette tee hankintoja, älä vastaa tähän kysymykseen):

   a) Varteenotettavien tarjoajien vähyyttä
   b) Kilpailun toimimattomuutta
   c) Kilpailutus- tai toimitusaikataulun viivästymistä / venymistä
   d) Ei mitään edellisistä
   e) Jotain muuta: [mitä?]

10. Jos puolustusvoimat antaa kirjallisen määräyksen, että KATAKRI:a on käytettävä täysmääräisesti aina kun sen turvallisuusluokiteltua tietoa luovutetaan sidosryhmien käyttöön (myös tarjouslaskentavaiheessa), aiheuttavatko tarjouslaskentavaiheen turvallisuusjärjestelyt arviosi mukaan (voit vastata useamman vaihtoehdon):

    a) Varteenotettavien tarjoajien vähyyttä
    b) Kilpailun toimimattomuutta
    c) Kilpailutus- tai toimitusaikataulun viivästymistä / venymistä
    d) Ei mitään edellisistä
    e) Jotain muuta: [mitä?]

11. Kokemukseni mukaan tarjouslaskentavaiheen turvallisuusvaatimukset saattavat (voit vastata useamman vaihtoehdon):

    a) Nostaa hankinnan / hankkeen hintaa
    b) Aiheuttaa pienten toimijoiden haluttomuutta osallistua kilpailutukseen
    c) Aiheuttaa keskisuurten toimijoiden haluttomuutta osallistua kilpailutukseen
    d) Aiheuttaa isojen toimijoiden haluttomuutta osallistua kilpailutukseen
    e) Aiheuttaa jotain muuta: [mitä?]

12. Koetko, että tarjouskilpailuihin osallistumista harkitsevat sidosryhmänne todella tiedostavat ja ymmärtävät turvallisuusluokiteltua tietoa sisältävästä hankinnasta / hankkeesta aiheutuvat velvoitteet ja sen, että jo tarjouslaskentavaiheeseen osallistuminen saattaa aiheuttaa heille lisätyötä ja kustannuksia?

13. Miten pyritte varmistumaan siitä, että tarjouskilpailuihin osallistumista harkitsevat sidosryhmänne todella tiedostavat ja ymmärtävät turvallisuusluokitellusta palveluhankinnasta / muusta hankkeesta aiheutuvat velvoitteet ja sen, että jo tarjouslaskentavaiheeseen osallistuminen saattaa aiheuttaa heille lisätyötä ja kustannuksia?

14. Kun sidosryhmät, joilla ei ole ennestään yhteistyötä ja/tai turvallisuussopimusta puolustusvoimien / yksikkönne kanssa, saavat tietää tarjouslaskentavaiheen turvallisuusvaatimuksista he usein kokemuksesi mukaan (voit vastata useamman vaihtoehdon):

    a) Ymmärtävät, mitä tiedon salassapito tarkoittaa ja tietävät, miksi ja miten tietoja luokitellaan
    b) Tuntevat tiedon turvallisuusluokkamerkinnät ja tiedon suojaustasot
    c) Tietävät mikä KATAKRI on ja tuntevat sen vaatimukset kohtalaisesti

    d) Ovat kuulleet joskus KATAKRI:sta ja ovat tutustuneet pintapuolisesti sen vaatimuksiin
    e) Eivät tiedä mikä KATAKRI on, eivätkä ole tutustuneet sen vaatimuksiin

f) Eivät ymmärrä, mitä tiedon salassapito tarkoittaa, eivätkä tiedä miksi tietoja luokitellaan

g) Eivät tunne tiedon turvallisuusluokkamerkintöjä ja/ tai tiedon suojaustasoja
h) Yllättyvät tarjouslaskentavaiheen turvallisuusjärjestelyistä
i) Ilmoittavat, ettei heillä ole olemassa tarvittavia järjestelyjä / menettelyjä / tiedon käsittelyyn tarvittavia tiloja

j) Ilmoittavat laittavansa järjestelyt / menettelyt / tiedon käsittelyyn tarvittavia tilat kuntoon
k) Harkitsevat tarjouskilpailusta luopumista
l) Reagoivat jotenkin muuten: [miten?]

15. Minkälaisia turvallisuusvaatimuksista johtuvia ongelmia tai haasteita olette havainneet hankintojen tarjouslaskentavaiheiden yhteydessä?

16. Tulisiko KATAKRI:a voida käyttää mielestäsi varsinaisten palvelusopimusten yhteydessä (ei tarjouslaskentavaiheessa) hankinta- / hankekohtaisesti soveltaen vai pitäisikö sitä käyttää täysmääräisesti aina silloin, kun puolustusvoimien turvallisuusluokiteltua tietoa luovutetaan sidosryhmien käyttöön?

    a) Täysmääräisesti
    b) Hankekohtaisesti soveltaen
    c) Jotenkin muuten: [miten?]

17. Vapaa sana. Tähän voit halutessasi kirjata aihepiiriin liittyviä ajatuksia tai huomioita.

Kiitos vastauksistasi!

Liite 5 Sidosryhmähaastattelun kyselylomake

Vastauksiani saa käyttää muun lähdemateriaalin ohella
julkisessa opinnäytetyössä siten, etteivät vastaukseni ole yksilöitävissä: **Kyllä / Ei**

Toimenkuva:
Organisaatio:

Tässä lomakkeessa pyritään selvittämään hankintojen turvallisuusjärjestelyiden parissa työskennelleiden sidosryhmien edustajien henkilökohtaisia mielipiteitä. Vastaukset annetaan nimettömänä. Vastauksia käsitellään opinnäytetyössä siten, ettei vastaajan henkilöllisyys, toimenkuva tai organisaatio ole yksilöitävissä tai pääteltävissä yksittäisen mielipiteen osalta. Haastatteluaineisto jää vain tutkijan omaan käyttöön.

1. Ennen kuin yrityksemme osallistui Puolustushallinnon rakennuslaitoksen Etelä-Suomen alueyksikön järjestämään palveluhankinnan tarjouskilpailuprosessiin, tarjouslaskentavaiheen hankehenkilöstömme käsitykseni mukaan (voit vastata useamman vaihtoehdon):

   a) Ymmärsi, mitä tiedon salassapito tarkoittaa ja tiesi, miksi ja miten tietoja luokitellaan
   b) Tunsivat tiedon turvallisuusluokkamerkinnät ja tiedon suojaustasot
   c) Tiesivät mikä KATAKRI on ja tunsivat sen vaatimukset kohtalaisesti

   d) Olivat kuulleet joskus KATAKRI:sta ja olivat tutustuneet pintapuolisesti sen vaatimuksiin
   e) Eivät tienneet mikä KATAKRI on, eivätkä olleet tutustuneet sen vaatimuksiin
   f) Eivät ymmärtäneet, mitä tiedon salassapito tarkoittaa, eivätkä tienneet miksi tietoja luokitellaan

   g) Eivät tunteneet tiedon turvallisuusluokkamerkintöjä ja / tai tiedon suojaustasoja
   h) Yllättyivät tarjouslaskentavaiheen turvallisuusjärjestelyistä
   i) Reagoivat jotenkin muuten: [miten?]

2. Kun kuulimme tarjouslaskentavaiheen turvallisuusjärjestelyistä (voit vastata useamman vaihtoehdon):

   a) Ilmoitimme, ettei meillä ole olemassa tarvittavia järjestelyjä / menettelyjä / tiedon käsittelyyn tarvittavia tiloja
   b) Ilmoitimme laittavamme järjestelyt / menettelyt / tiedon käsittelyyn tarvittavia tilat kuntoon
   c) Harkitsimme tarjouskilpailusta luopumista
   d) Reagoimme jotenkin muuten: [miten?]

3. Tulisiko mielestäsi tilaajan hankintayksikön voida käyttää KATAKRI:n vaatimuksia hankinta- / hankekohtaisesti soveltaen vai olisiko mielestäsi parempi jos vaatimuksia käytteisiin täysmääräisesti silloin kun puolustusvoimien turvallisuusluokiteltua tietoa luovutetaan sidosryhmien käyttöön hankintojen / hankkeiden tarjouslaskentavaiheessa? Pyri perustelemaan vastauksesi.

4. Näen KATAKRI:n turvallisuusvaatimukset ensisijaisesti (voit vastata useamman vaihtoehdon):

   a) Ylimitoitettuna
   b) Alimitoitettuna
   c) Sopivina

   d) Ylimääräisenä riesana

e) Kilpailua haittaavina
f) Kilpailutus- tai toimitusaikatauluja viivästyttävinä

g) Tilaajan kustannuksia nostavina
h) Tarjoajan kustannuksia nostavina
i) Kaikkien osapuolien kustannuksia nostavina

j) Tarjoajia syrjivinä
k) Kaikille tasapuolisina
l) Helposti ennakoitavina

m) Viranomaistoimintaa yhtenäistävinä
n) Oman yrityksemme turvallisuustoimintaa tukevina
o) Mahdollisena kilpailuvalttina

p) Kertaluontoisena panostuksena
q) Jonakin muuna: [millaisena?]

5. Jos Puolustushallinnon rakennuslaitos edellyttäisi sidosryhmiltään vähintään KATAKRI:n Perustason (IV) täyttämistä täysmääräisesti aina kun luovuttaa puolustusvoimien turvallisuusluokiteltua tietoa sidosryhmiensä käyttöön (myös tarjouslaskentavaiheessa), aiheuttaisivatko laitoksen tarjouslaskentavaiheen turvallisuusjärjestelyt tässä tapauksessa arviosi mukaan (voit vastata useamman vaihtoehdon):

   a) Varteenotettavien tarjoajien vähyyttä
   b) Kilpailun toimimattomuutta
   c) Kilpailutus- tai toimitusaikataulun viivästymistä / venymistä
   d) Ei mitään edellisistä

6. Näen Puolustushallinnon rakennuslaitoksen tarjouslaskentavaiheen turvallisuusjärjestelyt, joita noudatettiin tarjoamamme palvelun hankintaprosessin yhteydessä (voit vastata useamman vaihtoehdon):

   a) Ylimitoitettuna
   b) Alimitoitettuna
   c) Sopivina

   d) Ylimääräisenä riesana
   e) Kilpailua haittaavina
   f) Kilpailutus- tai toimitusaikatauluja viivästyttävinä

   g) Tilaajan kustannuksia nostavina
   h) Tarjoajan kustannuksia nostavina
   i) Kaikkien osapuolien kustannuksia nostavina

   j) Tarjoajia syrjivinä
   k) Kaikille tasapuolisina
   l) Helposti ennakoitavina

   m) Saman suuntaisina muiden viranomaisten vaatimusten kanssa
   n) Oman yrityksemme turvallisuustoimintaa tukevina
   o) Mahdollisena kilpailuvalttina

   p) Kertaluontoisena panostuksena
   q) Jonakin muuna: [millaisena?]

7. Koetko, että palveluhankinnan tarjouskilpailuun osallistumista harkitessanne todella tiedostitte ja ymmärsitte turvallisuusluokiteltua tietoa sisältävästä hankinnasta aiheutuvat velvoitteet ja sen, että jo tarjouslaskentavaiheeseen osallistuminen saattaa aiheuttaa yritykselle lisätyötä ja kustannuksia?

8. Saitteko mielestäsi tarpeeksi opastusta turvallisuusluokitellusta palveluhankinnasta aiheutuvista velvoitteista ja siitä, että jo tarjouslaskentavaiheeseen osallistuminen saattaa aiheuttaa yritykselle lisätyötä ja kustannuksia? Mitä Puolustushallinnon rakennuslaitos voisi tehdä paremmin?

9. Minkälaisia turvallisuusvaatimuksista johtuvia ongelmia tai haasteita olette havainneet Puolustushallinnon rakennuslaitosten tilaamien palveluhankintojen tarjouslaskentavaiheiden yhteydessä?

10. Vapaa sana. Tähän voit halutessasi kirjata aihepiiriin liittyviä ajatuksia tai huomioita:

Kiitos vastauksistasi!

Liite 6 Ehdotus turvallisuusluokitellun tiedon suojausvaatimuksiksi palveluhankintojen tarjouslaskentavaiheessa

Tämän tutkimuksen johtopäätöksissä esiteltiin 10 kohdan luettelo niistä seikoista, joihin tulisi kiinnittää huomiota turvallisuusluokitellun tiedon suojausvaatimuksia suunniteltaessa. Alla on kerätty lista niistä KATAKRI:n kriteereistä, jotka ovat tutkimuksen johtopäätösten perusteella käyttökelpoisia tähän tarkoitukseen.

KATAKRI:sta tulisi soveltaa palveluhankintojen tarjouslaskentavaiheessa seuraavia kriteereitä:

Hallinnollinen turvallisuus	**Henkilöstö-turvallisuus**	**Fyysinen turvallisuus**	**Tietoturvallisuus**
A 801.0	**P 101.0**	**F 201.0**	**I 602.0**
A 805.0	**P 102.0**	**F 202.0**	**I 603.0**
	P 103.0	**F 203.0**	**I 606.0**
	P 104.0	**F 205.0**	
		F 206.0	
	P 401.0	**F 207.0**	
	P 403.0	**F 208.0**	
	P 404.0	**F 209.0**	
	P405.0	**F 210.0**	
		F 211.0	
	(P 301.0)	**F 212.0**	
	(P 302.0)	**F 213.0**	
	(P 303.0)	**F 214.0**	
		F 215.0	
	(P 605.0)	**F 217.0**	
		F 301.0	
		F 302.0	
		F 303.0	
		F 305.0	