Nils Willberg

# KYBEROSAAMISEN NYKYISET JA TULEVAT TARPEET JULKISEN SEKTORIN ORGANISAATIOISSA

## PRO GRADU

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2017

# TIIVISTELMÄ

Willberg, Nils
Kyberosaamisen nykyiset ja tulevat tarpeet julkisen sektorin organisaatioissa
Jyväskylä Jyväskylän yliopisto, 2017, 51 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Tutkimuksessa arvioidaan kahden julkisen sektorin organisaation kyberammatillisen osaamisen nykyisiä ja lähitulevaisuuden tarpeita. Tutkimuksen kohdeorganisaatioissa kyberammatillinen osaaminen liittyy vahvasti niiden ydintoimintoihin. Kyberammatillista osaamista tarkastellaan NCWF -viitekehyksen kategorioiden ja eritysalueiden kautta. Viitekehyksen luokittelujen perusteella laaditaan organisaatiokohtainen ydinkompetenssiesitys organisaatio-osaamisen näkökulmasta. Tutkimus edustaa laadullisen tutkimuksen case -lähestymistapaa, jossa aineistonkeruumuotona on teemahaastattelu ja aineiston analyysimenetelmänä teorialähtöinen sisällönanalyysi. Tulosten perusteella ydinkompetenssiesitysten painopistealueet vaihtelevat merkittävästi organisaatioiden välillä. Toisaalta riittävän kyberosaamisen saavuttaminen lähitulevaisuuden taktisen ja operationaalisen tason ydintoimintojen alueella on selkeästi keskeinen haaste molemmissa organisaatioissa. Jatkotutkimusten kannalta olennaista olisi keskittyä syvällisen, kyberammatilliseen osaamiseen liittyvän tiedon hankintaan eri tyyppisistä organisaatioista. Tältä pohjalta mahdollistuisi relevanttien hypoteesien muodostaminen, mikä palvelisi myös kvantitatiivisia tutkimusasetelmia ja sitä kautta tutkimustulosten yleistettävyyttä.

Asiasanat: julkinen sektori, kyberammatillinen osaaminen, ydinkompetenssi, case -tutkimus

# ABSTRACT

Willberg, Nils
Current and future needs of the cyber expertise in public sector organizations
Jyväskylä: University of Jyväskylä, 2017, 51 p.
Information Systems, Master's Thesis
Supervisor: Lehto, Martti

The investigation will assess the need of the cyberprofessional expertise in two public sector organizations. In the target organizations cyberprofessional expertise is related to their core activities. Cyberprofessional expertise is examined on the basis of NCWF -framework and its categories and specialty areas. A frame of reference on the basis of an organization-wide core competency ratings shall be drawn up in the presentation from the perspective of the organizational knowledge. The study represents a qualitative research and its case study -approach, in which the material collection takes the form of a theme interview and the material analysis a theory based content analysis. On the basis of the results the priorities of the core competence presentations vary significantly between organizations. On the other hand, the achievement of a sufficient level of the cyber expertise in the area of the tactical and operational core activities is clearly a key challenge in both organizations. Essential for further research would be to focus to obtain on an in-depth knowledge of the cyberprofessional expertise in different types of organizations. On this basis, it would be possible to form relevant hypotheses which would also serve quantitative studies and through this generalization of the research results.

Keywords: public sector, cyberprofessional expertise, core competence, case -study

## KUVIOT



## TAULUKOT

# SISÄLLYS

# 1. JOHDANTO

## 1.1. Kyberuhat organisaatiotason erityishaasteena

Työvoiman kyberosaaminen ja sen kehittäminen on noussut keskeisten strategisten haasteiden joukkoon yhä useammissa valtioissa. Taustalla voidaan nähdä erityisesti yhteiskunnan kriittiseen infrastruktuuriin kohdistuvien kyberuhkien lisääntyminen. (Cybersecurity Competence Building Trends, 2016). Kyberalan tutkimusten mukaan ongelmatilanteiden riski kohdistuu useimmiten suoraan organisaatiotasolle, sillä organisaatioiden toiminta on lähes poikkeuksetta vahvasti informaatioteknologiasta riippuvaista (Goodman, 2014).

Tyypillisesti kyberuhat nähdään teknologiakeskeisinä ulkoisina uhkina kuten hakkerointeina ja haittaohjelmina (Doherty & Fulford, 2005). Toisaalta sisäiset väärinkäytökset organisaatioissa ovat myös kasvussa, mikä vaatii suurempaa panostusta sisäisten uhkien torjuntaan (Spears & Barki, 2010). Onnistuneen tietoturvapolitiikan omaksumisessa ja toteuttamisessa organisaatiorakenteella on suuri merkitys. Tietoturvapolitiikan käytännön menestyksen kannalta tämä tarkoittaa organisatorista joustavuutta, johon liittyy valmius uudistaa ja sopeuttaa työntekijöiden yksilöllisiä rooleja organisaation sisällä (Karyda, Kiountouzis & Kokolakis, 2004). Tietoturvapolitiikka vaatii kuitenkin taustalleen myös vakiintunutta hallintoa, jotta sen onnistunut kehittäminen ja toteutus olisivat mahdollisia (Knapp, Morris, Marshall & Byrd, 2009).

Kansalliset rajat ylittävä yhteistyö voi olla yksi keino vahvistaa yleistä kyberosaamisen tasoa (Hoffman, Burley & Toregas, 2012). Valtioiden välinen yhteistyö kyberalueella onkin välttämätöntä ja lisääntyy kaiken aikaa. Tästä huolimatta riittävän valtiollisen autonomian saavuttaminen ja ylläpito ovat kuitenkin tärkein väline kyberuhkien torjunnassa. Yhä arkaluonteisempien tehtävien lisääntyessä pätevä paikallinen työvoima on nähtävä kansallista turvallisuutta edistävänä tekijänä (Cybersecurity Competence Building Trends, 2016).

## 1.2. Kyberalan koulutus ja osaamisen kehittäminen

Erityisluonteensa, so. jatkuvan muutoksen hallitsevuuden, vuoksi kyberalan osaaminen ja kehittäminen vaatii riittävän laajan näkökulman omaksumista kaikessa toiminnassa (Cybersecurity Competence Building Trends, 2016). Käytännössä kyse on holistisesta lähestymistavasta työvoiman kehittämiseen, mikä tarkoittaa eri alojen näkökulmien ja toimijoiden mukanaoloa kehittämisprosessissa. Työvoiman kehittämissuunnitteluun voi siten osallistua kouluttajia, ura-

ammattilaisia, työnantajia ja vaikuttajia sekä julkiselta että yksityiseltä sektorilta. Ydintekijä on kuitenkin yksilöllisen asiantuntijuuden kehittäminen toimintakentän kokonaisuuteen istuvaksi (Hoffman ym., 2012).

Kyberosaamisesta onkin tullut korostetusti ihmisten ongelma: se edellyttää erikoistunutta työvoimaa, joka omaa riittävän kompetenssin hyödyntää tehokkaasti ja vaikuttavasti olemassaolevaa kyberturvallisuusteknologiaa (Professionalizing Cybersecurity: A path to universal standards and status, 2014).

Monitieteisenä ja nopeasti teknologisesti kehittyvänä alueena myös kyberalan koulutukselta vaaditaan traditionaalisista näkökannoista poikkeamista. Käytännössä tämä tarkoittaa julkisen ja yksityisen sektorin aiempaa tiiviimpää ja laajempaa yhteistyötä alan koulutuksen organisoinnissa (Cybersecurity Competence Building Trends, 2016; National Initiative for Cybersecurity Education, 2013). Kyse on samalla erityisesti pitkän aikavälin yhteisötason vaikutuksista työvoiman suunnittelun ja sen käytännön toteutuksen alueilla (Fourie, Hettema & Watters, 2014).

Varsinkin Suomen kaltaisessa pienessä maassa julkisen sektorin tiivis yhteydenpito tutkimus- ja yrityssektorin kanssa on molemminpuolisen tiedonvälityksen kannalta olennainen tekijä (Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, 2016). Koulutusta voidaan pitää avaintekijänä tuleviin kyberhaasteisiin vastaamaan kykenevien ammattilaisten kehittämisessä (Professionalizing Cybersecurity: A path to universal standards and status, 2014). Vallitseva työvoiman osaamisvaje tarjoaisikin juuri tällä hetkellä ainutlaatuisen mahdollisuuden kouluttaa taitavia IT -alan ammattilaisia kyberturvallisuuden tehtäviin (Vogel, 2016).

## 1.3. Kybertyövoiman määrittelemättömyys ja sen tarjonnan puute

Tässä tutkimuksessa kyberosaamisella viitataan kyberammatilliseen osaamiseen, mikä tarkoittaa kyberasiantuntijuuteen ja sitä edellyttäviin tehtäväsisältöihin liitettävää professionalismia. Tutkimuksen osaamisnäkökulma on organisaatiotason osaamisessa, jolloin myös kyberammatillista osaamista lähestytään sitä edellyttävien toimintojen tasolla. Yksityiskohtaisiin tehtäväsisältöihin ja varsinkaan niihin liittyviin ammattinimikkeisiin tutkimuksessa ei suoranaisesti paneuduta, sillä niissä on kyse tällä hetkellä voimakkaasti kehittyvistä ja muuttuvista sisällöistä.

Kyberturvallisuuden tai ylipäätään informaatioturvallisuuden professionalismia on hankala määritellä kovin yksiselitteisesti. Erityisesti kyberturvallisuudessa on edelleen kyse suhteellisen uudesta professiosta, mikä tarkoittaa samalla professionalismin tasosta käytävää debattia alan sisällä. Epämääräisyys näkyy myös siinä, että organisaatiot eivät välttämättä tunnista alan tehtävissä

vaadittavia taitoja. Toisaalta niillä voi olla myös ongelmia rekrytoida vaadittavan kompetenssin omaavia työntekijöitä (Furnell, Fischer & Finch, 2017).

Yksi kyberuhkien torjunnan suurimpia haasteita onkin juuri pätevän työvoiman löytäminen ja kehittäminen alan asiantuntijatehtäviin. Alan selkiintymättömät pätevyysvaatimukset ovat seurausta jatkuvasta tehtävä- ja tietovaatimusten kehittymisestä ja laajenemisesta. (Cybersecurity Competence Building Trends, 2016; Professionalizing Cybersecurity: A path to universal standards and status, 2014). Epätarkoituksenmukaista tilannetta monimutkaistavat entisestään alati vaihtelevat käsitykset siitä, mitä kyberammattilaisuus ylipäätään tarkoittaa. Organisaatioiden kyky tunnistaa itse tarvitsemansa osaamisen laatu nouseekin tällaisessa tilanteessa erityisen tärkeäksi (Furnell ym., 2017).

Tässä tutkimuksessa kyberammatillista osaamista kartoitetaan julkisen sektorin kontekstissa. Tutkimuksen kohteeksi on valittu julkisia organisaatioita, joissa kyberammatillinen osaaminen edustaa tai liittyy niiden keskeisiin ydintoimintoihin. Tutkimuskohteiden toiminnan edellyttämää kyberammatillisen osaamisen sisältöä arvioidaan sekä nykyhetken että lähitulevaisuuden vaatimusten näkökulmasta. Tutkimuksessa otetaan siten kantaa myös mahdollisiin näköpiirissä siintäviin kehitystarpeisiin. Pelkkä nykytilan selvittäminen antaisi osaamisvaatimuksista varsin rajoittuneen kuvan, sillä nopeasti kehittyvät ja muuttuvat tarpeet luovat väistämättä osaamiselle uusia haasteita vallitsevassa todellisuudessa.

Kyberammatilliseen osaamiseen ja siihen liittyviin tarpeisiin kohdistunutta tutkimusta on toistaiseksi olemassa varsin vähän. Erityisen niukasti osaamista ja tarpeita on kartoitettu julkisen sektorin kontekstissa. Osaamisen ja osaamistarpeiden selvittämisen lähtökohdan muodostavat tässä tutkimuksessa organisaatioiden itsensä ilmaisemat, kyberturvallisuuteen liittyvät sisällöt. Tätä lähestymistapaa voidaan perustella sekä tutkimusalueen yleisellä vähäisyydellä että kyberturvallisuuden professionalismiin ja sen tehtäväsisältöihin liitetyllä epämääräisyydellä. Tällaisessa lähtötilanteessa tarkoituksenmukaisin ja luotettavin keino saada selville kyberammatilliseen osaamiseen liittyvät organisaatiotason vaatimukset onkin selvittää organisaatioiden omia näkemyksiä tilanteestaan ja siihen liittyvistä kehitysnäkymistä.

Tutkimus noudattelee laadulliseen lähestymistapaan perustuvaa case -tutkimuksen menetelmää. Tutkimusaineisto muodostuu kohdeorganisaatioiden edustajien haastatteluista, joiden runko rakentuu National Cybersecurity Workforce Framework (NCWF) -viitekehyksen (National Initiative for Cybersecurity Education, 2013) sisältöalueille. Viitekehys on kyberammatillisia toimintoja ja tehtäväalueita laajasti kattava ja määrittelevä esitys, jonka avulla voidaan toteuttaa ja havainnollistaa myös kyberosaamiseen liittyvää profilointia. Tässä tutkimuksessa NCWF -viitekehystä sovelletaan aineistonkeruu- ja analyysivaiheissa organisaatiokohtaisesti esiin nousevien sisältöjen ilmentämien tarpeiden pohjalta.

Ammatillisten standardien määrittäminen edesauttaisi rekrytoinnin ohella myös kyberalan koulutusta sekä laajemminkin tarvittavan työvoiman kehittämistä (Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals, 2014). Professionalismi houkuttelisi pätevää työvoimaa ja ehkäisisi samalla ei-kompetentin työvoiman hakeutumista alalle, minkä lisäksi se toimisi seulana yksilöiden sijoittamisessa tarkoituksenmukaisempiin tehtävänkuviin (Burley, Eisenberg & Goodman, 2014). Kyberammattilaisuuden kehittäminen onkin noussut prioriteetiksi sekä kansallisen puolustuksen että kyberalan taloudellisen merkityksen vuoksi. Jälkimmäisessä on kyse kyberalan kasvavasta taloudellisesta potentiaalista, mikä lisää alan työvoiman kysyntää ja luo mahdollisuuksia tuotteistaa kyberalan osaamista (Cybersecurity Competence Building Trends, 2016).

Tällä hetkellä saatavilla olevan ja todellisuudessa tarvittavan työvoiman välillä vallitsee osaamisvaje, joka tunnustetaan maailmanlaajuisesti. Osaamisvaje vaikuttaa kansalliseen turvallisuuteen niin yksityisellä kuin julkisellakin sektorilla (Vogel, 2016; Fourie ym., 2014). Fundamentaalisinta vaje on varsinkin teknisissä tehtävissä, mutta sitä ilmenee yhtä lailla johtamisen, erityisesti tulevaisuuden työvoiman johtamisen haasteissa (Cybersecurity Forum Initiative, 2013). Erityisesti julkisella sektorilla näyttää olevan vakavia ongelmia sopivan ja pätevän työvoiman löytämisessä, palkkaamisessa ja säilyttämisessä. Julkisen sektorin näkökulmasta vahvat suhteet yliopistoihin olisi yksi keino parantaa osaavan työvoiman saatavuutta. Tämä tarkoittaisi käytännössä työvoiman pakollista siirtymistä ainakin määräajaksi julkisen sektorin käyttöön, jotta yhteiskunnan kriittisen infrastruktuurin toiminta voitaisiin turvata (Goodman, 2014).

Kyberalan ammattilaisten ja sidosryhmien keskuudessa vallitseva tilanne nähdään jatkumona aina koulutuksen organisoinnista työelämään siirtymiseen saakka. Nämä intressiryhmät ovat tunnistaneet kolme aukkoa, jotka ehkäisevät organisaatioita vastaamasta kyberturvallisuustarpeisiinsa. Kompetenssiaukosta on kyse silloin kun työnhakijalla ei ole organisaatioiden edellyttämää professiotasoa. Monelta hakijalta puuttuu myös riittävä ammatillinen kokemus, jolloin voidaan puhua kokemusaukosta. Näiden lisäksi voi syntyä aukko korkeakoulutetun työvoiman liian pitkästä viiveestä siirtymisessä koulutuksesta työmarkkinoille (Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals, 2014).

Edellisen näkemyksen mukaan syy vallitsevaan tilanteeseen olisi siis lähinnä koulutuksessa ja työntekijöiden kompetenssissa, ei niinkään organisaatioiden omassa valmiudessa tunnistaa vaadittavaa osaamista. Tämä käsitys puoltaisi osaamistarpeiden selvittämisen yleistä merkityksellisyyttä organisaatiotasolla, sillä siitä voisi potentiaalisesti seurata koulutuksen vaikuttavuuden ja sitä kautta myös työntekijöiden professionismin paranemista. Ammatillisen kokemuksen edistäminen sitä vastoin näyttäisi selvästi velvoittavan myös organisaatioita aktiivisemman roolin omaksumiseen.

Tässä tutkimuksessa kyberammatillista osaamista tarkastellaan ydinkompetenssin käsitteen kautta. Tutkimuksen tavoitteena on hahmottaa kyberammatillisen osaamisen nykytilan ja tulevien kehitystarpeiden pohjalta kyberammatillisen osaamisen ydinkompetenssi kussakin tutkimuksen kohdeorganisaatiossa. Ydinkompetenssi ymmärretään tavallisimmin sellaiseksi osaamiseksi, joka tulee esiin organisaation toimiessa kokonaisuutena. Tällainen ydinosaavaa organisaatiota luonnehtiva ydinkompetenssi on pysyväisluonteinen ominaisuus, vaikka se vaatiikin ylläpitoa ja tarvittaessa myös ydinkompetenssin kehittymistä (Pralahad & Hamel, 1990).

Kyberosaamisen tarkastelua ydinkompetenssiin liitettynä voidaan perustella sekä ydinkompetenssin organisaatiotasoisuuden että sen sisältämän kehityksellisen ulottuvuuden kautta. Turbulentissa kybermaailmassa tehtävänkuvat ja tilanteet voivat muuttua hyvinkin nopeasti, jolloin katsantokanta on perusteltua suunnata vakaampiin kokonaisuuksiin ja tuleviin kehityskulkuihin. Tästä näkökulmasta ydinkompetenssia voidaan pitää havainnollisena käsitteenä pyrittäessä hahmottamaan organisaatioiden kyberosaamisen ydintoimintoja ja niihin liittyviä olennaisia kehitystekijöitä. Kyse on samalla yhdestä konkreettisesta välineestä, jolla voidaan selkeyttää organisaatioiden käsityksiä ja ymmärrystä omasta kyberosaamisestaan ja sen tulevista haasteista. Ymmärryksen lisääntyminen mahdollistaa myös organisaatioiden tarkoituksenmukaisemman yhteistyön koulutussektorin kanssa, mikä voi potentiaalisesti parantaa kyberalan koulutuksen vaikuttavuutta. Tämä taas poistaa osaltaan työvoiman osaamisvajetta, mikä voi lopulta johtaa edellä mainittujen kyberturvallisuustarpeiden aukkojen pienentymiseen.

## 1.4. Suomen erityispiirteet

Suomessa valtaosa kyberosaamisesta on keskittynyt yksityiselle sektorille ja tutkimuslaitoksiin. Toisaalta myös julkisella sektorilla on oma merkittävä roolinsa varsinkin kyberosaamisen kehittämisen alueella. Tämä näkyy erityisesti yleisenä resurssien allokointina, alan kehitystä ohjaavan lainsäädännön ja suuntaviivojen määrityksenä sekä myös merkittävänä julkisten organisaatioiden asiakkuutena alan yrityksille. Merkittävää kyberalan osaamista julkisella sektorilla edustavat muun muassa Viestintäviraston Kyberturvallisuuskeskus, Keskusrikospoliisin Kyberrikostorjuntakeskus sekä Puolustusvoimat (Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, 2016). Edellä mainitut organisaatiot edustavatkin kyberalan asiantuntijayhteisöjä, joiden toiminnassa kyberturvallisuus kuuluu niiden keskeisiin ydinalueisiin.

# 2. KIRJALLISUUS

## 2.1. Ydinkompetenssi organisaatiotason käsitteenä

Yksityisellä sektorilla kehittynyt kompetenssipohjainen henkilöstöresurssien johtaminen on muodostunut yhä keskeisemmäksi teemaksi myös julkisen sektorin palvelujen kehittämisessä. Kehityksen taustalla voidaan nähdä julkisten resurssien strategisen johtamisen tarve, jonka nopeasti muuttuva ympäristö on saanut aikaan. Ydinkompetenssi voidaan erottaa henkilöstöresurssien johtamiseen liittyvän kompetenssitarkastelun kolmanneksi vaiheeksi. Tässä jatkumossa kompetenssi on ennen ydinkompetenssia liitetty joko yksilöllisiin kompetensseihin tai organisatoristen kompetenssimallien luomiseen ja johtamiseen (Skorkova, 2016).

Ydinkompetenssin käsite on tunnettu kasvatus- ja liiketaloustieteissä, joiden piirissä sen sisältöä kuitenkin tulkitaan hyvin eri tavoin. Kasvatustieteellisen näkemyksen mukaan käsite tarkoittaa sellaisia oppimistuloksia, so. taitoja ja pätevyyksiä, jotka yksilö joko hankkii tietyn oppimisjakson aikana tai osoittaa saavuttaneensa tällaisen oppimisjakson lopussa (Holmes & Hooper, 2000). Kasvatustieteessä ydinkompetenssin käsitteellä on siten kuvattu puhtaasti yksilöön liittyviä ominaisuuksia.

Liiketaloustieteissä ydinkompetenssi taas on tyypillisesti yhdistetty joko erinomaiseen inhimilliseen suorituskykyyn yksilötasolla tai organisaatiotason kompetensseihin kilpailuedun saavuttamisessa. Chenin & Changin (2011) mukaan nämä tulkinnat voidaan pelkistää strategiseksi inhimillisten resurssien johtamiseksi, jolloin puhutaan toisiaan täydentävistä mikro- ja makrotason kompetensseista. Tällöin makrotason ydinkompetenssi johtaa strategisesti mikrotason inhimillistä kompetenssia, joka taas täydentää ydinkompetenssin kokonaiseksi. Keskeistä tässä prosessissa on näiden kahden tason välinen vuorovaikutus organisatorisen kontekstin sisällä (Chen & Chang, 2011).

Käytännössä edellisessä on kyse siitä, että organisaation kulttuuri, visio, missio, strategia ja arvot moderoivat kumpaakin ydinkompetenssin tasoa (Chen & Chang, 2011). Tämä edistää lopulta myös organisaation jäsenten jaettua ymmärrystä organisaation tavoitteista ja niiden saavuttamisesta. (Ulrich, 1991). Tällöin kompetenssi on luonteeltaan kontekstisidonnaista, so. heikosti organisaation ulkopuolelle siirrettävää ja kopioitavaa. Kompetenssi myös kehittyy vasta pitkän aikavälin kuluessa työntekijän ja organisaation välisessä, satunnaisesti toteutuvassa vuorovaikutussuhteessa (Chen & Chang, 2010). Työntekijöiden keskuudessa kehittynyttä yleistä ymmärrystä ja jaettuja tarkoituksia voidaan pitää myös menestyksellisen tietoturvapolitiikan omaksumisen edellytyksenä (Karyda ym., 2004).

Pralahad ja Hamel (1990) ovat hahmotelleet ydinkompetenssin käsitettä yritysmaailman kontekstissa. Sisällöllisesti käsite kattaa organisaation koko ulottuvuuden ja soveltuu modifioituna myös julkisen sektorin tarkasteluun. Lähtökohtana on holistinen näkökulma ydinkompetenssiin, jonka perusta lepää organisaation kollektiivisessa oppimisessa. Tällaisella oppimisella voidaan potentiaalisesti parantaa kaikkia niitä reaaliprosessin osia, joilla yritys saa aikaan (taloudellista) arvonlisäystä (Pralahad & Hamel, 1990).

Pralahadin ja Hamelin (1990) mukaan kyse on pohjimmiltaan eri osa-alueiden harmonisoinnista, joka liittyy niin työn organisointiin kuin itse arvon aikaansaamiseen. Tämä edellyttää kuitenkin kommunikointia, osallistumista ja syvää sitoutumista työskentelyyn yli organisatoristen rajojen (Pralahad & Hamel, 1990). Julkisen sektorin näkökulmasta tämä tarkoittaa riittävän tiiviitä yhteyksiä tutkimus- ja yritysmaailmaan molemminpuolisen, ajankohtaisen tiedon välittämiseksi. Ainakin julkisen sektorin ja tutkimusmaailman välinen yhteydenpito vaikuttaisi kuitenkin vielä olevan osin puutteellista. Toisaalta näyttäisi siltä, että julkiset organisaatiot vaikuttavat asiakkaan roolissaan vahvasti yritysten innovaatiotoimintaan (Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, 2016.).

Konventionaalisesti ydinkompetenssi käsitetään ilmiöksi, joka tulee esiin organisaation toimiessa kokonaisuutena. Pralahadin & Hamelin mukaan ydinkompetenssi pyrkii kuvaamaan organisaation ydinosaavana kokonaisuutena, jolloin voi olla perusteltua puhua myös ydinosaamisen portfoliosta (Pralahad & Hamel, 1990). Ydinkompetenssista on loogisesti erotettavissa yksilötason (työntekijän) kompetenssi 'väliaikaisena voimavarana', joka muodostuu aina organisatorisen vuorovaikutuksen kontekstissa. Tässäkin kompetenssi voi kuitenkin syntyä vain organisaation sisällä, jolloin se on kontekstisidonnaista ja organisaation pysyvän kilpailuedun ylläpitoon liittyvää (Chen & Chang, 2010). Goddard on määritellyt metakompetenssiksi organisaation kyvyn rakentaa ja ylläpitää ydinkompetenssiaan (Goddard 1997).

Goddard (1997) tarjoaa ydinkompetenssille useita erilaisia määritelmiä, jotka on luotu yksityisen sektorin arvontuottoprosessien näkökulmasta. Näistä osa on kuitenkin sovellettavissa myös julkiselle sektorille. Yhden määritelmän mukaan ydinkompetenssissa on kyse muun muassa organisaation toimintaan upotetusta, yksilöistä riippumattomasta ominaisuudesta, joka saa ilmaisunsa organisaation jäsenten päivittäisessä toiminnassa. Ydinkompetenssi voi toisaalta liittyä myös joihinkin organisaation tulevaisuuden kannalta kriittisiin toimintoihin sen arvoketjussa. Se on myös olennaisesti luonteeltaan joustavaa ja siten uusiin olosuhteisiin ja toimintatapoihin mukautuvaa. Goddard nimeää ydinkompetenssin myös organisaation sisäisen differentiaation 'geneettiseksi' raaka-aineeksi, jolla hän viittaa ydinkompetenssin kolmeen, sen piirteiksi nimeämäänsä alueeseen: organisaation uskomusjärjestelmään, käyttäytymistyyliin ja infrastrukturaaliseen suunnitteluun (Goddard, 1997).

Ydinkompetenssin tunnistamisessa organisaation johdolla on ratkaiseva rooli. Sen on kyettävä näkemään organisaatio kokonaisuutena, jotta ydinkompetenssiin liittyvät komponentit voidaan tunnistaa. Tämä edellyttää näkökulman siirtämistä serialistisesta holistisemmaksi, mikä on usein haastava tehtävä. Tilannetta voi edesauttaa sellaisen strategisen kaavan tai arkkitehtuurin kehittäminen, joka helpottaa ydinkompetenssin tavoitteiden laadintaa. Ydinkompetenssissa on aina kyse jostain pysyväisluonteisesta: se ei vanhene vaan pikemminkin paranee käytettäessä ja jaettaessa sitä organisaation sisällä. Toisaalta ydinkompetenssin käytön laiminlyönti voi myös heikentää sitä ja vaikeuttaa siten organisaation toiminnan suuntaamista tulevaisuudessa (Pralahad & Hamel, 1990).

## 2.2. Kyberammattilaisuuden kompetenssi

Tutkimuskirjallisuudessa yleisesti tunnustettu käsitys on se, että informaatioturvallisuuteen liittyy teknologisen aspektin ohella myös sosio-organisatorinen ulottuvuus (Reece & Stahl, 2014; Kayworth & Whitten, 2010). Näiden kahden välinen tasapaino on olennaista, sillä toimiakseen konkreettinen teknologia vaatii organisaatiolta tietoturvapolitiikkaa ja samalla myös sen ilmenemistä organisaation jäsenten käyttäytymisessä. Kyse on siten tietoturvapolitiikan kommunikointi- ja hyväksymisprosessien samanarvoisuudesta varsinaisen teknologian täytäntöönpanon kanssa. (Reece & Stahl, 2014). Tällaista asetelmaa voidaan tarkastella holistisesti sellaisena kokonaisuutena, jossa sosio-organisatoriset mekanismit ja teknologinen kompetenssi yhdistyvät osaksi informaatioturvallisuuteen keskittynyttä sosio-teknistä strategiaa (Kayworth & Whitten, 2010).

Kyberturvallisuus osana informaatioturvallisuutta kattaa laajan joukon ammatteja teknologiasta ja johtamisesta aina erilaisiin poliittisiin tehtäviin saakka. Osa näistä ammateista on peräisin kyberalueen ulkopuolelta, jolloin voidaan puhua hybrideistä ja tilanteen mukaan muuttuvista tehtävänkuvista. Professionalismin näkökulmasta tämä tarkoittaa sitä, että kyberalueella voidaan tunnistaa sekä professionaalisia että sitä kohti pyrkiviä tehtäviä. Nopeasti vaihtuvat tehtävät jäävät kuitenkin näiden ulkopuolelle, sillä ne katoavat tyypillisesti jo ennen professionaalistumisvaihetta. (Burley ym., 2014).

Professionalismin saavuttamiselle voidaan asettaa sellaisia yleisiä kriteereitä kuten vakaat tieto- ja taitovaatimukset, pysyvät työroolit, ammatilliset rajat, uralla etenemisen mahdollisuudet ja ammattietiikan muodostuminen. Toistaiseksi kyberturvallisuuden toimintakenttä ei kuitenkaan kokonaisuutena täytä näitä kriteereitä. Yleisesti professionaalistamisstrategia tulisi aina kohdistaa työvoiman erityishaasteisiin, jotta puutteisiin voidaan vaikuttaa. Kyberturvallisuudessa työvoimaan liittyvät haasteet ovat selkeästi kapasiteetin ja kykyjen

alueilla. Yleisen professionalismin tavoittelun sijaan tulisikin vaikuttaa näihin tunnistettuihin ja spesifeihin työvoiman puutteisiin. (Burley ym., 2014).

Wilsonin & Wilsonin (2011) mukaan kyberprofessionalismilla voidaan viitata sellaisiin ammattilaisiin, joiden päätehtävät liittyvät informaatioturvallisuuteen, ja jotka tunnistavat itsensä kyber- tai turvallisuusasiantuntijoiksi. Lisäksi nämä asiantuntijat rakentavat ja ylläpitävät tietokonejärjestelmien kriittistä infrastruktuuria, johon julkinen ja yksityinen sektori ovat oppineet luottamaan. (Wilson & Wilson, 2011). Kyse on tässä selvästi yleisen tason kyberprofessionalismin määritelmästä, jossa ei oteta tarkemmin kantaa eri tehtäväalueiden edellyttämiin kompetensseihin.

Kyberturvallisuuden työtehtäville on tunnusomaista se, että niissä kohdattava todellisuus on jatkuvan muutoksen tilassa. Tämä pätee niin eteen tuleviin uhkiin kuin niiden vastatoimiinkin, mutta myös toiminnan perustana olevaan teknologiaan. Uutena alana kyberturvallisuus on myös voimakkaassa ammatillisessa kehitysvaiheessa, mikä peräänkuuluttaa osaamista useilta toimialoilta ja samalla aivan uudenlaisia lähestymistapoja. Kaiken kaikkiaan kyberturvallisuuden kompleksinen ongelmakenttä ja dynaaminen luonne tekevät alan työvoimarakenteen hahmottamisesta haasteellista. (Hoffman ym, 2012). Kyberalalla voidaan kuitenkin tunnistaa toimintoja ja ammatillisia tai tehtäväkohtaisia kriteereitä ja ominaisuuksia, jotka esiintyvät toistuvasti myös tutkimuskirjallisuudessa. Tutkimukset on tyypillisesti toteutettu yksityisen sektorin kontekstissa, mutta niissä esiintyviä ammatillisia kompetensseja voidaan yhdistää myös julkisen sektorin kontekstiin.

Klimoski (2016) pitää kyberalueen johtajan ja hänen tukiorganisaationsa keskeisenä ominaisuutena uskottavuuden saavuttamista organisaation kaikkien sidosryhmien silmissä. Informaatioturvallisuuden johtajan uskottavuus rakentuu hänen mukaansa luotettavuuden, itseluottamuksen, henkilön aiempien menestysten aktiivisen esilletuonnin sekä tarkoituksenmukaisesti rakentuneen sosiaalisen verkoston varaan (Klimoski, 2016). Itseluottamus edellä viittaa erityisesti alakohtaiseen tietämykseen, mikä on myös tämän tutkimuksen näkökulmasta yksi keskeinen kompetenssialue. Tutkimusten mukaan vaikuttaisi kuitenkin siltä, että tietämys on usein liian spesifioitunutta, vaikka tarvetta olisi nimenomaan laajemmalle näkökulmalle. Kyse on tässä organisaation toiminnan kokonaisvaltaisen ymmärryksen puutteesta (Klimoski, 2016). Kuvattu tilanne näyttäisi joka tapauksessa viittaavan osittaiseen epätasapainotilaan, jossa teknologinen aspekti korostuu sosiaalisten tekijöiden kustannuksella.

Tärkeimmiksi tekijöiksi edellisistä Klimoski (2016) nostaa aiempien saavutusten rekisteröinnin ja sosiaalisen pääoman rakentamisen. Aiemman urakulun kyberturvallisuustietämyksen ja kokemuksen omasta kehittymisestä tulisi hänen mukaansa proaktiivisesti kehittää johtajan portfoliota (Klimoski, 2016). Todellisuudessa pätevän työvoiman alitarjontatilanne luonee omat rajoitteensa sille, miten laajasti tällaisia portfolioita on mahdollista koota. Sosiaalinen pää-

oma puolestaan on tunnetusti parhaita keinoja uskottavuuden hankkimiseksi. Siinä voidaan puhua henkilökohtaisesta suhdeverkostosta, joka mahdollistaa niin tavoitteiden saavuttamisen kuin henkilökohtaisen ja ammatillisen kehittymisen (Klimoski, 2016). Jatkuvien uusien uhkien leimaamalla kyberalalla vahva verkostoituneisuus onkin varsin ilmeinen etu. Yleisesti uskottavuus on kuitenkin Klimoskin (2016) mukaan johtajan ja henkilöstön yhteisen vastuunoton tulosta, mikä mahdollistaa 'strategisen kyvyn' kehittymisen uskottavuuden edellytyksenä.

# 3. TUTKIMUKSEN TAVOITTEET

## 3.1. Tutkimuksen tavoitteet ja rajaus

Tässä tutkimuksessa kyberosaamista tarkastellaan julkisen sektorin organisaatioiden tietoturvan kontekstissa. Kyberosaamisen taloudellinen merkitys jää siten tutkimuksen aihepiirin ulkopuolelle. Tutkimuksessa kyberosaamisen tarkastelu rajataan lisäksi organisaation professionaaliseen kyberosaamiseen, jolloin siihen ei sisälly kaikilta organisaation jäseniltä vaadittava tavanomaiseksi luonnehdittava kyberosaaminen. Tutkimuksen tavoitteena on hahmottaa kohdeorganisaatioiden kyberammatillisen osaamisen ydinkompetenssi. Tavoitteeseen pyritään kyberosaamisen nykytilan määrittämisen ja lähitulevaisuuden asettamien osaamisvaatimusten arvioinnin kautta.

Ydinkompetenssin hahmottamisessa ei oteta kantaa yksilöllisiin kompetensseihin, vaan kyse on organisaatioiden tarkastelusta yksinomaan niiden toiminnan kokonaistasolla. Tutkimuksessa noudatetaan siten tavanomaisinta tapaa tulkita ydinkompetenssin muodostumista. Organisaatiotason tarkastelussa pidättäytymistä voidaan perustella myös kybermaailman turbulentilla luonteella, mikä luo heikot edellytykset yksilöllisen tiukoille tehtäväkohtaisille rajauksille. Staattisiin, pysyviin ja hierarkkisiin olettamuksiin perustuva käsitys yksilöllisestä kompetenssista jäisi siten tässä kontekstissa kompetenssin kuvauksena rajoittuneeksi (Chen & Chang, 2010).

Tutkimuksessa pyritään vastaamaan kysymykseen, millainen ydinkompetenssi kohdeorganisaatioille muodostuu nykytilan ja lähitulevaisuuden kehityskulun huomioivassa kokonaisesityksessä. Organisaatioiden toiminnan tarkoitus ja sen toteuttamiseen liittyvät kyberalueen toiminnot nousevat tässä tarkastelun keskiöön. Kyberosaamisen eri alueiden ja toimintojen hahmottamisessa hyödynnetään soveltuvin osin jäljempänä esiteltyä National Cybersecurity Workforce Framework (NCWF) -viitekehystä. Viitekehyksen avulla voidaan tunnistaa tietoturva-alueittain vaihtelevat kompetenssit, joiden pohjalta myös organisaatiotason ydinkompetenssi muodostetaan. Näin ollen NCWF -viitekehyksestä muodostuu samalla tutkimuksen kyberammatillisen osaamisen tarpeiden määrittelyn pääasiallinen väline. Tarkoituksena on hahmottaa sen avulla muotoutuvan arviointikehyksen kautta kunkin kohdeorganisaation kyberammatillinen ydinkompetenssiesitys.

## 3.2. Ydinkompetenssi viitekehyksessä

Kyberalan työvoiman kysynnän kautta ilmaistaan samalla myös kybertyövoimaan liitettävät kompetenssitekijät (Goodman, 2014). National Initiative for Cybersecurity Education (NICE) on luonut kompetenssien jäljittämiseen yleisen tason systemaattisemman välineen. NICE on kansallisesti koordinoitu pyrkimys kehittää kyberturvallisuustietoisuutta sekä kyberturvallisuuden opetusta, koulutusta ja asiantuntijuutta. Pyrkimystä edesauttamaan on luotu NCWF-viitekehys (kuvio 1), jonka avulla voidaan määritellä täsmällisemmin kyberturvallisuuteen liittyviä työtehtäviä ja niiden ammatillisia profiileja. Viitekehys on syntynyt tarpeesta luoda organisatorisista ja ammatillisista rakenteista riippumaton menetelmä joustavan ja korkealaatuisen kybertyövoiman rekrytoinnin tueksi. Viitekehystä voidaan pitää ydintekijänä kyberuhkien ehkäisy- ja puolustuskyvyn kannalta juuri sen johdonmukaisten, tarkkojen ja laadukkaiden ammatillisten sisältöerittelyjen vuoksi (National Initiative for Cybersecurity Education, 2013).

Viitekehyksen luokittelu ja sanasto ovat sovellettavissa yhtä lailla niin julkiselle, yksityiselle kuin akateemiselle sektorille. Sen kattavuus ulottuu myös yli toimialojen, organisaatioiden ja eri työtehtävien. Kehyksen yleisrakenteen muodostavat seitsemän eri aihealueen kategoriaa, joiden sisällä on yhteensä kolmekymmentäkaksi kategorioiden mukaan ryhmiteltyä, toisiinsa liittyvää erityisaluetta. Vaikka kehys perustuukin olennaisesti täsmällisiin nimikkeisiin ja määritelmiin, on sen tarkoitus mukautua olemassa oleviin organisaatiorakenteisiin. Keskeistä onkin hyödyntää kehyksen tarjoamaa taksonomiaa kuvattaessa samankaltaisia työn sisältöjä, vaatimuksia ja niihin liittyviä taitoja (National Initiative for Cybersecurity Education, 2013).

Tässä tutkimuksessa NCWF-viitekehystä sovelletaan sekä ydinkompetenssin sisältöjen että lopullisten ydinkompetenssiesitysten hahmottamisen taustarakenteena. Kohdeorganisaatioiden ydinkompetenssin sisältö muodostetaan viitekehyksen kyberturvallisuuden osa-alueita erittelevän kategoriajaon mukaisesti. Organisaatioissa tunnistetut kyberturvallisuuteen liittyvät toiminnot sijoitetaan viitekehyksessä niihin kategorioihin ja erityisalueisiin, joihin toiminnot todennäköisimmin liittyvät. Viitekehyksen taksonomiaa sovelletaan kuitenkin jokaisen tutkimusentiteetin osalta tilannekohtaisesti, mikä käytännössä tarkoittaa tarpeettomien viitekehyksen sisältöjen sivuuttamista.

## 3.3. NCWF -viitekehys

Oheisessa kuviossa on esitetty tiivistetysti NCWF-viitekehyksen seitsemän kategoriaa. Turvallisuuden tarjoaminen -kategoria kattaa laajasti turvallisen in-

formaatioteknologisen järjestelmän luonnin ja toteutuksen erityisalueet. Niihin sisältyy informaation ja ohjelmistojen laadunvarmistuksen arviointia sekä ohjelmistoturvallisuuden ja vaatimusmäärittelyn suunnittelua. Tarkastelussa ovat muun muassa IT-järjestelmien kyky vastata organisaation laadunvarmistuksen ja turvallisuuden vaatimuksiin ja se, kehitetäänkö uusia ohjelmistoja ja sovelluksia vai parannetaanko olemassa olevia. Muita erityisalueita ovat teknologinen tutkimus ja teknologian kehittäminen sekä turvallisuusjärjestelmien arkkitehtuurin elinkaaripohjainen kehittäminen, testaus ja arviointi. Niissä otetaan kantaa siihen, kehitetäänkö turvallisuusarkkitehtuuria elinkaaren aikana tai miten ja millä kriteereillä toiminnallisia vaatimuksia arvioidaan ja miten ne voidaan muuttaa teknisiksi vaatimuksiksi. Lisäksi arvioidaan järjestelmän testaus- ja arviointikriteereitä ja niitä valmiuksia, joita järjestelmän kehittäminen eri vaiheissa edellyttää.

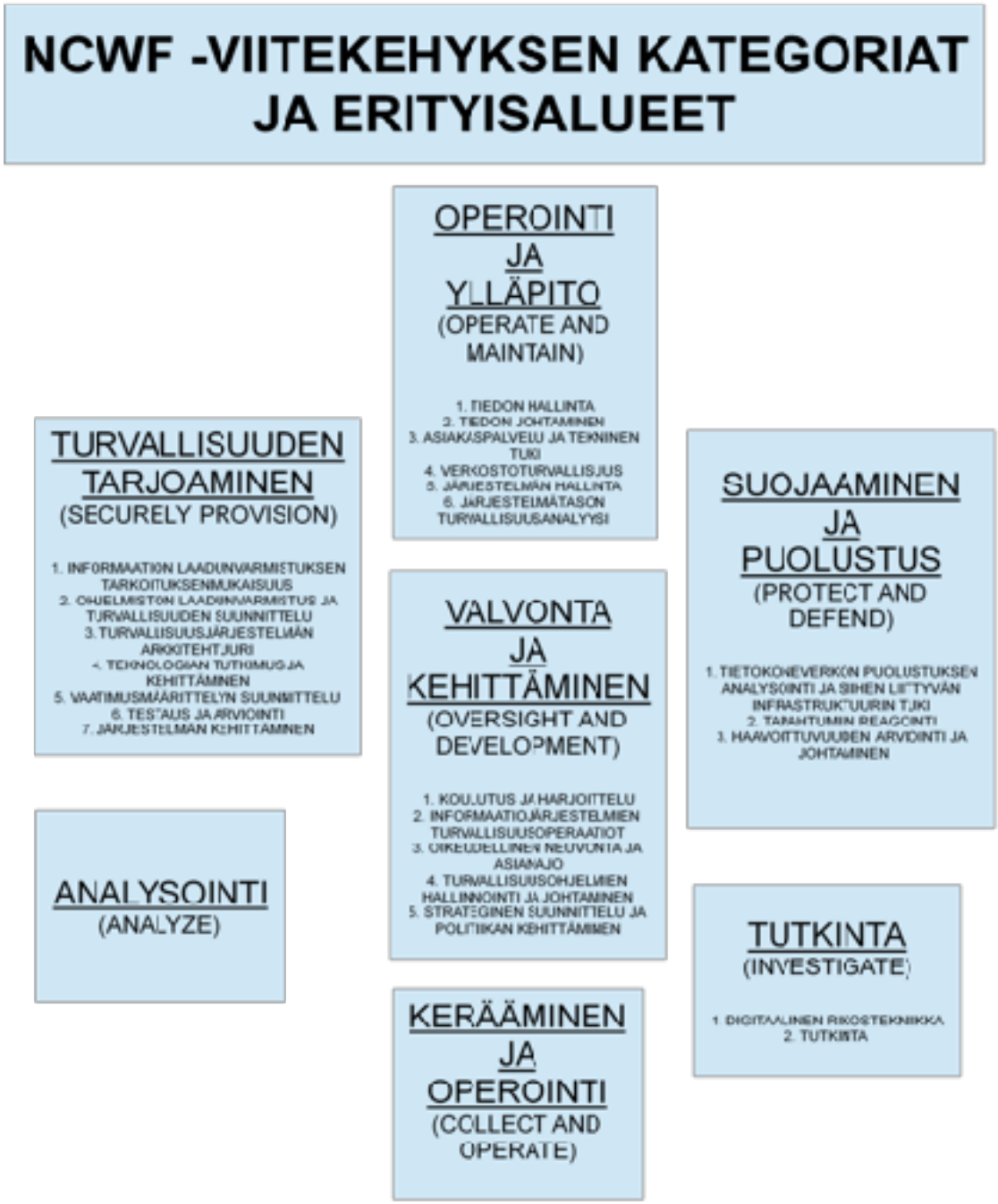
Operointi ja ylläpito -kategoriassa on kyse järjestelmän tuki-, hallinnointi- ja ylläpitotoiminnoista järjestelmän suorituskykyä ja turvallisuutta silmällä pitäen. Tiedonhallinnan erityisalue sisältää tietokantojen ja tiedon johtamisjärjestelmän hallinnoinnin. Tiedon johtamisen toimintoja taas ovat tärkeiden tietopääomien ja informaatiosisältöjen tunnistaminen, dokumentointi ja näihin tietovarantoihin pääsyn kontrollointi. Asiakaspalvelu ja tekninen tuki -erityisalue liittyy organisaation sisäiseen asiakaspalveluun sekä ylläpito- ja koulutuspalvelujen tarjoamiseen. Muita erityisalueita ovat verkostoturvallisuus, järjestelmän hallinta ja järjestelmätason turvallisuusanalyysi. Niiden kuuluvia toimintoja ovat muun muassa järjestelmäturvallisuuden integrointi, testaus, operointi ja ylläpito sekä verkostoturvallisuudesta huolehtiminen mahdollisen erillisen toimintamallin avulla.

Suojaaminen ja puolustus -kategorian tarkoituksena on tunnistaa, analysoida ja lievittää uhkia sisäisessä järjestelmässä ja verkossa. Tietokoneverkon puolustuksen analysointi ja siihen liittyvän infrastruktuurin tuki -erityisalueella arvioidaan sitä, millaisia puolustustoimia käytetään ja millaista informaatiota kerätään kybertapahtumien tunnistamiseksi, analysoimiseksi ja raportoimiseksi, jotta voidaan edesauttaa informaation, järjestelmien ja verkostojen suojelua. Lisäksi otetaan kantaa siihen, miten näitä toimenpiteitä tuetaan laitteiden ja ohjelmistojen toteutuksella, testauksella, käyttöönotolla, ylläpidolla, arvioinnilla ja hallinnoinnilla. Tapahtumiin reagoinnin erityisalueella on kyse haitallisten vaikutusten lieventämisestä reagoimalla tarkoituksenmukaisesti kiireellisissä tilanteissa. Haavoittuvuuden arviointi ja johtaminen -erityisalueella otetaan kantaa riskien hallinnan, so. uhkien ja haavoittuvuuden arviointi, sietokyvyn määrittely ja tarkoituksenmukaisten toimenpiteiden suunnittelu, osa-alueisiin.

Tutkinta -kategorian toiminnot liittyvät järjestelmään ja verkostoihin kohdistuneiden kybertapahtumien tutkintaan ja evidenssin tuottamiseen niistä. Digitaalinen rikostekniikka -erityisalueella toteutuneista kybertapahtumista kerätään, prosessoidaan, taltioidaan, analysoidaan ja esitetään digitaalista näyttöä.

Tutkinta -erityisalue kattaa taktiikan, tekniikan, menettelytavat ja välineet, joita varsinaisessa tutkinnassa hyödynnetään. Kerääminen ja operointi -kategorian tarkoitus on havainnoida kiellettyjä operaatioita ja kerätä todistusaineistoa kehittävää kyberturvallisuusinformaatiota. Analysointi -kategoriassa sisään tulevaa kyberinformaatiota arvioidaan ja arvotetaan tiedon merkityksellisyyden näkökulmasta.

Valvonta ja kehittäminen -kategoria liittyy laajemmin kyberturvallisuustyön johtamiseen, suuntaamiseen ja ohjaamiseen organisaation sisällä. Koulutus ja harjoittelu -erityisalueella arvioidaan, suunnitellaan ja toteutetaan erilaisia henkilöstön kehittämiseen liittyviä toimintoja. Informaatiojärjestelmien turvallisuusoperaatiot -erityisalueen tarkoituksena on valvoa sisäisten ja ulkoisten informaatiojärjestelmien verkoston informaatiovarmuutta. Oikeudellinen neuvonta ja asianajo -erityisalue liittyy järkevän laillisuusneuvonnan ja -suositusten järjestämiseen organisaation jäsenille. Turvallisuusohjelmien hallinnointi ja johtaminen -erityisalueen tarkoituksena on ottaa kantaa siihen, miten ja millä alueilla informaatioturvallisuutta organisaatiossa toteutetaan. Strateginen suunnittelu ja politiikan kehittäminen -erityisalueella priorisoidaan toiminnan suuntaaminen, resurssien allokointi, eri toimintaohjelmat ja infrastruktuurit intressialueittain




KUVIO 1 NCWF -viitekehyksen kategoriat ja erityisalueet

# 4. TUTKIMUSMENETELMÄT

## 4.1. Tutkimuksen sijoittuminen laadullisen tutkimuksen perinteeseen

Tutkimus voidaan sijoittaa laadullisen tutkimuksen fenomenologi-hermeneuttiseen perinteeseen. Fenomenologiassa tutkitaan yksilöiden kokemuksia ilmiöistä, joihin on ladattu yhteisöllisen tason kautta muotoutuneita merkityksiä (Tuomi & Sarajärvi, 2009). Tässä tutkimuksessa pyritään selvittämään organisaation jäsenten kokemia kyberosaamisen tarpeita, joiden merkitys ja relevanssi olisi perusteltavissa koko organisaation tasolla. Tutkimukseen valikoitujen informanttien ammattiaseman perusteella voidaan olettaa, että esille nousevat tarpeet ovat merkityksellisiä myös organisaatiotasolla.

Heikkisen ja Laineen (1997) ja Laineen (2001) mukaan hermeneutiikan kautta tutkittavan ilmiön tulkinnalle ja ymmärtämiselle etsitään sääntöjä oikean ja väärän tulkinnan erottamiseksi (ks. Tuomi & Sarajärvi, 2009, 35). Laineen (2001) mukaan tämä voidaan erottaa kaksitasoiseksi rakenteeksi, jossa perustasolla on tutkittavan esiymmärrys ilmiöstä ja toisella tasolla siihen pohjautuva varsinainen tutkimus. (ks. Tuomi & Sarajärvi, 2009, 35). Tässä tutkimuksessa perustasolla selvitetään yksilöiden näkemykset organisaation kyberammatillisen osaamisen tarpeista, joista muodostetaan viitekehykseen pohjautuva organisaation kyberammatillinen ydinkompetenssi. Fenomenologis-hermeneuttisen tutkimuksen tavoitteena on merkityksillä ladatun kokemuksen käsitteellistäminen (Tuomi & Sarajärvi, 2009). Tässä tutkimuksessa pyritään muodostamaan ja havainnollistamaan sellaisen ilmiön kokonaisrakennetta, joka on jo yksilöiden kokema, mutta ei välttämättä vielä tietoisesti ajateltu.

## 4.2. Tutkimusmenetelmä

Tapaustutkimusta voidaan pitää yhtenä keskeisenä tiedonhankinnan strategiana kvalitatiivisen metodologian alueella, jolla sitä käytetään lähestymistapana lähes kaikissa strategioissa (Metsämuuronen, 2011). Informaatioteknologian nopeasti muuttuvan kentän tutkimisessa tapaustutkimuksen strategia toimii myös luontevasti. Tämä tulee esiin niin käytännön toimijoilta tavoitetussa tiedossa kuin sen pohjalta kehitetyissä teorioissa. Toisaalta tutkimusintressit ovat siirtyneet teknologisista kysymyksistä kohti johtamisen ja organisaation kenttää sekä sitä kautta myös kontekstin ja teknologisten innovaatioiden vuorovaikutuksen alueille. Vallitseva kehitys palvelee hyvin tapaustutkimuksen strategiaa,

jolla voidaan tutkia monimutkaisia prosesseja niiden luonnollisessa kontekstissa ja luoda sitä kautta nopeasti uutta ymmärrystä alati muuttuvasta ympäristöstä (Benbasat Goldstein & Mead, 1987). Edellä kuvattu kehityskulku näyttäisi pätevän erityisen hyvin juuri kyberturvallisuuden nopeasti kehittyvällä ja muuttuvalla alueella.

Tämän tutkimuksen asetelma täyttää pitkälti tapaustutkimuksen tunnuspiirteet, minkä vuoksi tapaustutkimus valikoituu luontevasti tutkimuksen toteuttamisen menetelmäksi. Tutkimuskohteeksi on rajattu yksittäisten organisaatioiden kyberammatillinen osaaminen, johon liittyviä tarpeita pyritään selvittämään kokonaisvaltaisesti ja syvällisesti. Tapaustutkimukselle on tyypillistä juuri kohteen syvällinen ymmärtäminen huomioimalla samalla sen taustat monipuolisesti (Saaranen-Kauppinen & Puusniekka, 2006).

Tutkimuksessa ei suoranaisesti pyritä yleistämään saatuja tuloksia, vaikka tarkoitus onkin arvioida niiden merkitystä laajemmassa kontekstissa. Yleisesti tapaustutkimuksen tulosten hyödynnettävyyttä kannattaa pohtia esimerkiksi laajempien lisätutkimusten suunnittelun apuna. Tutkimuksen huolellinen toteuttaminen erityisesti pätevän aineiston kuvauksen ja sen analyysin kautta voi edesauttaa tätä prosessia vahvistamalla tulosten merkitystä ja oikeellisuutta (Saaranen-Kauppinen & Puusniekka, 2006).

## 4.3. Tutkimuksen kohdejoukko

Tutkimuksen kohdejoukko muodostuu sellaisista julkisista organisaatioista, joiden toiminnassa kyberammatillinen osaaminen on olennaisessa roolissa. Olennaisuus tulee esiin sekä organisaatioiden toiminnan tarkoituksen että niiden ydintoimintojen kautta, jolloin ne soveltuvat myös hyvin tutkittaviksi NCWF-viitekehyksen näkökulmasta. Viitekehyksen käyttöä aineistonkeruun lähtökohtana puoltaa se, että siihen on koottu varsin kattavasti kyberturvallisuuden toimintakentän eri osa-alueet. Näin voidaan varmistua olennaisten kyberammatillisen osaamisen sisältöjen mukanaolosta tutkimusaineistossa. Tutkimuskohteiden omien, viitekehyksen ulkopuolisten tekijöiden esiin nostamisella voidaan puolestaan välttää viitekehyksen strukturoinnin mahdollisia jäykkyyksiä.

## 4.4. Aineiston hankintamenetelmä

Aineiston keruumuotona on puolistrukturoitu teemahaastattelu, jonka sisältö noudattelee NCWF-viitekehyksen viiden kategorian rakennetta. Kaksi viitekehyksen kategoriaa, "analysointi" sekä "kerääminen ja operointi" eivät sisälly suoraan haastattelurunkoon niihin liittyvien erityisalueiden uniikin ja vahvasti

erikoistuneen työn luonteen vuoksi. Lisäksi haastattelussa annetaan haastateltaville mahdollisuus tuoda esiin kompetenssialueita, joita NCWF-viitekehyksen sisällöissä ei suoraan ilmene. Hirsjärven ja Hurmeen (2015) mukaan teemahaastattelu on menetelmä, jolla voidaan oletusarvoisesti tutkia kaikkia yksilön kokemuksia, ajatuksia, uskomuksia ja tunteita. Keskeistä siinä on haastattelun eteneminen määrättyjen teemojen varassa, jolloin yksityiskohtaiset kysymykset jäävät sivurooliin. Teemahaastattelussa korostuvat haastateltavien omat tulkinnat ja merkitykset asioista sekä se, että annetut merkitykset ovat syntyneet vuorovaikutuksen tuloksena (Hirsjärvi & Hurme, 2015).

Haastateltaville toimitetaan ennakkoon tutustumista varten NCWF-viitekehys sisältöalueineen. Tällöin haastateltavat voivat pohtia valmiiksi sisältöalueisiin liittyviä tarpeita organisaatiossaan, mikä voi lisätä haastatteluissa esiin tulevan tiedon määrää, laatua ja luotettavuutta. Tuomen ja Sarajärven (2009) mukaan haastatteluissa on tärkeintä saada mahdollisimman paljon tietoa halutusta asiasta. Tätä tavoitetta voidaan edesauttaa luovuttamalla haastateltaville jo ennalta haastattelukysymykset tai -aiheet (Tuomi & Sarajärvi, 2009).

## 4.5. Aineiston analyysimenetelmä

Aineiston analyysimenetelmänä sovelletaan teorialähtöistä sisällönanalyysia, joka on yksi laadullisen sisällönanalyysin menetelmistä. Milesin ja Hubermanin (1994), Sandelowskin (1995) ja Politin ja Hunglerin (1997) mukaan teorialähtöisessä sisällönanalyysissa tutkimusaineisto luokitellaan jonkin olemassa olevan viitekehyksen mukaan. Viitekehyksellä voidaan tässä yhteydessä tarkoittaa yhtä lailla niin teoriaa kuin jotakin käsitejärjestelmääkin (ks. Tuomi & Sarajärvi, 2009, 113). Analyysimenetelmän valintaa voidaan perustella tässä tutkimuksessa sovellettavan valmiin viitekehyksen ja sen muodostaman strukturoidun analyysirungon kautta. Pattonin (1990), Marshallin ja Rosmanin (1995) ja Latvalan ja Vanhanen-Nuutisen (2001) mukaan strukturoidulla analyysirungolla koetellaan tyypillisesti jotakin olemassa olevaa teoriaa tai käsitejärjestelmää uudenlaisessa ympäristössä (ks. Tuomi & Sarajärvi, 2009, 113).

Deduktiivisessa sisällönanalyysissa luokittelukategoriat perustuvat aiempaan tietoon, johon kuuluvia sisältöjä aineistosta etsitään; analyysia ohjaa näin ollen aiemman tiedon pohjalta muodostettu teoria tai viitekehys (Tuomi & Sarajärvi, 2009). Tässä tutkimuksessa analyysirunko rakentuu NCWF-viitekehyksen kategorioille, joihin aineistosta esiin nouseva merkityksellinen sisältö deduktiivisen sisällönanalyysin mukaisesti luokitellaan. Lisäksi analyysirungon mahdollisista ulkopuolisista sisällöistä luodaan tarpeen mukaan uusia luokituksia, jolloin kyse on induktiivisen päättelyn periaatteista.

Käytännössä sanasta sanaan litteroitu aineisto luetaan läpi niin monta kertaa, että viitekehykseen perustuvia tai muita merkityksellisiä sisältöjä ei enää nouse siitä esiin. Aineistosta nousevat sisällöt jaotellaan lisäksi kolmelle eri tasolle sen mukaan millaista autonomisuuden astetta ne kohdeorganisaatiossa edustavat. Normatiivisuus edustaa tässä jaottelussa organisaatiolle ulkoa osoitettua toimintoa, jolloin kyse on yksinomaan ulkoapäin annetun velvoitteen hoitamisesta. Tällaisia toimintoja edustavat sellaiset vakiintuneet ja lainsäädäntöön perustuvat tehtävät, joita julkisille organisaatioille voidaan osoittaa. Yhteistoiminnallisuuteen taas liittyy erilaista strukturoitua yhteistyötä organisaation ulkopuolisten toimijoiden kanssa. Yhteistyöhön perustuvat toiminnot liittyvät sekä viranomaisyhteistyöhön että sopimuspohjaiseen toimintaan kolmansien osapuolten kanssa. Itsenäisessä toiminnassa organisaatio puolestaan määrittelee ja toteuttaa itse kaikki tähän kategoriaan liittyvät toimintonsa.

Ydinkompetenssin näkökulmasta on melko selvää, että juuri itsenäiseen toimintaan liitettävä sisältö nousee tutkimuksessa tarkastelun keskiöön. Toisaalta varsinkin yhteistyöhön liittyvissä toiminnoissa on myös itsenäisempiä alueita, joilla on vaikutuksia ydinkompetenssin sisältöön. Periaatteessa myös normatiivisten toimintojen tasolla voisi olla oma merkityksensä, sillä niidenkin suorittaminen edellyttää organisaatiolta riittävää kompetenssia. Ero kahteen muuhun tasoon on kuitenkin siinä, että normatiivisissa toiminnoissa organisaatio ei voi käytännössä määritellä tai vaikuttaa merkittävästi toimintojen sisältöön.

# 5. TULOKSET

## 5.1. Puolustusvoimien johtamisjärjestelmäkeskus

Puolustusvoimien johtamisjärjestelmäkeskus (jatkossa PVJJK) on puolustusvoimien palveluntuottaja, jonka toiminnassa kyberosaaminen liittyy sekä sen oman palvelutuotannon suojaamiseen että erilaisiin puolustuksellisiin ja vaikuttamiseen liittyviin toimintoihin. PVJJK:ssa informaatioturvallisuuden kokonaiskenttä voidaan erotella tietoturvan ja kyberturvallisuuden osa-alueisiin. Ensin mainittuun ei sisälly varsinaista uhkaulottuvuutta, vaan se liittyy organisaation järjestelmien ja lakisääteisten palvelujen turvaamiseen. Jälkimmäisessä taas on kyse kansallisen kyberturvallisuuden sotilaallisesta osasta, mikä PVJJK:n osalta tarkoittaa erilaisten kyberpuolustuksellisten toimintojen, so. suojautuminen ja vaikuttaminen, toteuttamista.

Yleisesti koko puolustusvoimien henkilöstöön liittyvänä erityispiirteenä on syytä tuoda esiin potentiaalisesti käytettävissä olevan työvoiman ja sitä kautta myös kyberosaamisen laaja pohja. Kantahenkilökunnan ja asevelvollisten lisäksi potentiaaliseen henkilöstöresurssiin voidaan lukea kuuluvaksi ennen kaikkea merkittävä reserviläisten joukko. Kyberammatillisen osaamisen näkökulmasta kyse on merkityksellisestä asiasta, sillä reserviläisten joukossa on tunnistettua kyberosaamista. Tämä osaaminen huomioidaan ja sitä päivitetään myös PVJKK:ssa pohdittaessa reserviläisten sijoittamisia erityisesti poikkeusolojen tehtäviin.

PVJJK:sta haastatteluun osallistuivat keskuksen johtaja Mikko Soikkeli ja kyberyksikön päällikkö Anssi Kärkkäinen. Haastattelu toteutettiin puolustusvoimien johtamisjärjestelmäkeskuksen tiloissa 21.12.2016. Haastattelu tallennettiin samanaikaisesti kahdella eri tietokoneella ja se kesti yhteensä noin 70 minuuttia.

### 5.1.1. Turvallisuuden tarjoaminen

PVJJK:n turvallisuuden tarjoaminen -kategorian (taulukko 1) normatiiviselle tasolle voidaan sijoittaa neljän erityisalueen toimintoja. Yleisesti puolustusvoimien järjestelmien tietoturvaa hallitaan tietohallintopäätösmenettely -prosessilla, jossa pyritään huomioimaan tietoturva jo järjestelmien kehittämisvaiheessa. Toteutettavasta järjestelmä- ja ohjelmistokehityksestä, testauksesta ja päivityksestä vastaa pääosin puolustusvoimien logistiikkalaitos. Tämän lisäksi standardisoituja ja suppeampia sovelluksia voidaan hankkia tarvittaessa ulkopuolisilta toimittajilta.

Yhteistoiminnallisella tasolla PVJJK on mukana kehitettävien sovellusten vaatimusmäärittelyssä ja testaustoiminnoissa. PVJJK voi sovellusten hyödyntäjänä esittää karkean tason vaatimusmäärittelyt, jotka logistiikkalaitos tyypillisesti johtaa yhtenä osaprojektina. Kyse voi joskus olla myös jonkin suuremman hankkeen yhdestä osasta. Osa kehitettävistä sovelluksista saattaa lisäksi vaatia laboratorio- tai kenttäolosuhteissa suoritettavaa testausta. Tällöin kehitettäville sovelluksille asetetaan keskimääräistä tiukempia vaatimuksia, joiden täyttymistä logistiikkalaitos testaa erilaisissa olosuhteissa.

Itsenäisellä tasolla keskeiseksi nousee tietoturvaluokkiin perustuva tiedon suojaustason määrittäminen, mikä on yksi puolustusvoimien ja PVJJK:n erityispiirteistä. PVJJK määrittelee valtaosan käsittelemästään tiedosta joko salaiseksi tai johonkin sitä väljempään, kuitenkin suojattavaan tietoturvaluokkaan kuuluvaksi. Salattavan tiedon tietoturvaluokkaa voidaan tarvittaessa myös muuttaa nopeasti tiedon elinkaaren vaiheiden mukaan. Lisäksi itse tietoa voidaan joutua muokkaamaan tai yleistämään jollekin toiselle tietoturvatasolle sopivaan muotoon. Nämä toiminnot edellyttävät myös sen määrittelyä, millaisilla kontrolli- ja salausmekanismeilla ja tiedonsiirtoyhteyksillä tiedon suojaustaso kulloinkin pyritään varmistamaan.

TAULUKKO 1 Turvallisuuden tarjoaminen (PVJJK)

| *AUTONOMISUUSTASO* | INFORMAATION LAADUNVARMISTUKSEN VAATIMUSTENMUKAISUUS | OHJELMISTON LAADUNVARMISTUS JA TURVALLISUUDEN SUUNNITTELU | JÄRJESTELMIEN TIETOTURVA-ARKKITEHTUURI | JÄRJESTELMÄN VAATIMUSTEN SUUNNITTELU | TESTAUS JA ARVIOINTI | JÄRJESTELMIEN KEHITTÄMINEN |
|---|---|---|---|---|---|---|
| ***NORMATIIVINEN***<br><br>*(ORGANISAATION VAIKUTUSPIIRIN ULKOPUOLELLA MÄÄRITTYVÄT TOIMINNOT)* | | Logistiikkalaitos kehittää räätälöityjä ohjelmistoja<br><br>Ohjelmistoja hankitaan ulkopuolisilta toimittajilta | Tietohallintopäätös-menettelyprosessin kautta ohjautuva<br><br>Laajoja järjestelmiä päivitetään enemmän | | Yleensä logistiikka-laitoksen vastuulla | Yleensä logistiikka-laitoksen vastuulla |
| ***YHTEISTOIMINNALLINEN***<br><br>*(YHTEISTYÖSSÄ MUIDEN KANSSA MÄÄRITTYVÄT TOIMINNOT)* | | | | Loppukäyttäjä esittää yleensä karkeat vaatimukset, jotka logistiikkalaitos toteuttaa toimeksiantona sopimuskohtaisesti | Tarvittaessa asejärjestelmiin liittyvään olosuhdetestaukseen osallistumista | |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***ITSENÄINEN***<br><br>*(ORGANISAATION SISÄLLÄ MÄÄRITTYVÄT TOIMINNOT)* | Tiedon suojaustason ja tietoturva-luokkien suunnittelu ja määrittely<br><br>Tietoturva-kontrollien ja tiedonsiirto-yhteyksien määrittely<br><br>Tiedon elinkaaren kontrollointi<br><br>Tiedon muokkaaminen ja välittäminen tietoturvatasolta toiselle | | | | | |

### 5.1.2. Operointi ja ylläpito

PVJJK:lla on lainsäädäntöön perustuvat velvoitteensa tiettyjen palvelujen tuottamiseksi, mikä tulee esiin operointi- ja ylläpito -kategorian (taulukko 2) normatiivisella tasolla. Käytännössä kyse on muiden viranomaisten kanssa käytettävistä yhteisistä järjestelmistä ja verkkopalveluista. Saman lainsäädännön noudattamisesta eri viranomaistahojen välillä seuraa myös pitkälti yhdenmukainen käsitys määräysten, ohjeiden ja suojaustasojen merkityksestä. Yhteistoiminnallisuutta ilmenee tässä kategoriassa vain puolustusvoimien omien, suljettujen järjestelmien käytössä eri yksiköiden välillä.

Itsenäisellä tasolla PVJJK:n tietohallinto perustuu siihen, että tiedolla on aina määritelty omistaja. Tiedon omistaja myös määrittelee tiedon suojaustason, pääsyoikeudet ja varastointipaikan. Sensitiivinen tieto on turvaluokiteltua tai -luokittelematonta tietoa, joka vääränlaisessa kontekstissa voi vaarantaa puolustusvoimien tai sen henkilöstön toimintaa. Operaatioturvallisuudella pyritään varmistamaan, että sensitiivinen tieto ei valuisi vääriin käsiin.

PVJJK:n ja muiden kuin tiettyjen viranomaistahojen välisen yhteistoiminnan edellytyksiä PVJKK arvioi erillisellä sidosryhmäturvallisuuden menetelmällä. Kyse on pitkälti verkostojen hallintaan liittyvästä turvallisuusselvitysmenettelystä, jossa arvioidaan muun muassa yhteistyökumppaneiden toimitilojen vaatimustenmukaisuutta ja niiden henkilöstön taustoja. Nämä yhteistyökumppanit ovat useimmiten yksityisen sektorin yrityksiä. PVJKK:n järjestelmiin ja tietoihin pääsy edellyttää yhteistyökumppanilta aina erillisen turvallisuussopimuksen allekirjoittamista. Tarvittaessa PVJJK voi tehdä myös seurantatarkastuksia sopimuksiin perustuen tai tilanteiden muuttuessa. Tällöin kyse on yleensä sopimusperusteisten määräaikojen umpeutumisesta tai henkilöstömuutoksista yhteistyöorganisaatiossa.

TAULUKKO 2 Operointi ja ylläpito (PVJJK)

| ***AUTONOMISUUSTASO*** | **TIETOHALLINTO** | **VERKKOPALVELUT** | **JÄRJESTELMÄNHALLINTA** |
|---|---|---|---|
| ***NORMATIIVINEN***<br><br>*(ORGANISAATION VAIKUTUSPIIRIN ULKOPUOLELLA MÄÄRITTYVÄT TOIMINNOT)* | | Lainsäädäntöön perustuva yhteisten järjestelmien käyttö muiden viranomaisten kanssa | Lainsäädäntöön perustuva yhteisten järjestelmien käyttö muiden viranomaisten kanssa |
| ***YHTEISTOIMINNALLINEN***<br><br>*(YHTEISTYÖSSÄ MUIDEN KANSSA MÄÄRITTYVÄT TOIMINNOT)* | | | Ulkopuolisilta suljettujen omien järjestelmien käyttö |
| ***ITSENÄINEN***<br><br>*(ORGANISAATION SISÄLLÄ MÄÄRITTYVÄT TOIMINNOT)* | Tiedon omistajana pääsyoikeuksien, suojaustason ja varastointipaikan määrittely ja hallinta<br><br>Sensitiivisen tiedon hallinta operaatioturvallisuuden varmistamisen kautta | | Sidosryhmäturvallisuuden varmistaminen yleisenä menetelmänä<br><br>Turvallisuusselvitysmenettelyt muiden yhteistyökumppaneiden kuin määrättyjen viranomaistoimijoiden osalta ja niihin perustuva yhteistyöosapuolten hyväksyntä erillisen turvallisuussopimuksen kautta<br><br>Yhteistyökumppaneihin kohdistuvien auditointien toteuttaminen ja niiden pohjalta myönnettävät määräaikaiset pääsyoikeudet |

### 5.1.3. Suojaaminen ja puolustus

Suojaaminen ja puolustus -kategorian normatiiviselle tasolle liittyviä toimintoja ovat strategisen tason kyberpuolustuksen kehittäminen sekä valtionhallinnon yhteistoimintafoorumin kautta PVJJK:lle lakisääteisesti määrittyvät tehtävät. Kyberpuolustus suorituskykynä määritellään strategisella tasolla puolustusvoimien ylimmässä johdossa, joka myös ilmaisee suorituskykyyn liittyvät kehittämistarpeet ja -alueet. PVJJK:n yhteistyö muiden viranomaisten kuten poliisin ja Kyberturvallisuuskeskuksen kanssa tulee yhtä lailla esiin myös yhteistoiminnallisella tasolla. Käytännössä tämä tarkoittaa havaintojen ja tietojen vaihtoa valtionhallinnon yhteistoimintafoorumin kautta. Viranomaisten välinen yhteistyö on merkittävässä roolissa erityisesti laadittaessa erilaisia uhka-analyyseja. Toinen yhteistoiminnallisen tason alue liittyy PVJJK:n yhteistyöhön muiden puolustusvoimien yksiköiden ja myös ulkopuolisten toimijoiden kanssa. Kyse on tällöin harjoituksista ja testauksesta, joiden avulla voidaan suoraan vaikuttaa muun muassa organisaation toiminnan ja käyttöperiaatteiden jalostumiseen.

Itsenäisen toiminnan tasolla PVJJK:n toiminnalle luonteenomainen 'uhkalähtöisyys' tulee varsin havainnollisesti esiin. Toiminnan yleisenä lähtökohtana on riskien arviointi, mikä tarkoittaa jatkuvaa uhkatilanteiden seurantaa ja analysointia. Seuranta ei rajoitu yksinomaan ulkoisen ympäristön tapahtumiin, sillä myös oman toiminnan seurauksiin liittyviä mahdollisia riskejä on reflektoita-

va. Järjestelmätasolla fokus on sekä omissa että yhteistyökumppaneiden järjestelmissä. Riskien arvioinnin ensisijaisena tavoitteena on kuitenkin PVJJK :n omien järjestelmien ja niihin sisältyvän kriittisen tiedon suojaaminen.

Organisaation järjestelmät pyritään suojaamaan kybertoimintaympäristöstä jatkuvalla seurannalla omien päivystysjärjestelmien avulla. Koko tietokoneverkon puolustusinfrastruktuurin operaatiotaidollinen toimintakyky edellyttää kuitenkin yhä enemmän taktisten käyttöperiaatteiden tunnistamista ja niiden kehittämistä. PVJJK:lla on tarvittaessa kyky reagoida nopeasti toimintaympäristön muutoksiin jopa hyökkäyksellisin vaikuttamisoperaatioin. Kyberpuolustuksen liittäminen osaksi taktisen ja operationaalisen tason toimintoja nousee keskeiseksi intressiksi myös tapahtumiin reagoitaessa.

TAULUKKO 3 Suojaaminen ja puolustus (PVJJK)

| ***AUTONOMISUUSTASO*** | **TAPAHTUMIIN REAGOINTI** | **TIETOKONEVERKON PUOLUSTUSINFRASTRUKTUURIN TUKI** | **HAAVOITTUVUUDEN ARVIOINTI JA HALLINTA** |
|---|---|---|---|
| ***NORMATIIVINEN***<br><br>*(ORGANISAATION VAIKUTUSPIIRIN ULKOPUOLELLA MÄÄRITTYVÄT TOIMINNOT)* | Kyberpuolustuksen strategisen tason kehittämispäätökset | | Valtionhallinnon yhteistoiminta-foorumin (VIRT) kautta |
| ***YHTEISTOIMIN-NALLINEN***<br><br>*(YHTEISTYÖSSÄ MUIDEN KANSSA MÄÄRITTYVÄT TOIMINNOT)* | Käyttöperiaatteiden jalostuminen harjoitus- ja testaustoiminnan kautta | | Yhteistyö muiden viranomaisten kanssa muun muassa valtionhallinnon yhteistoimintafoorumin (VIRT) kautta |
| ***ITSENÄINEN***<br><br>*(ORGANISAATION SISÄLLÄ MÄÄRITTYVÄT TOIMINNOT)* | Nopea reagointi muutoksiin tarvittaessa<br><br>Kyberpuolustuksen liittäminen sotilaallisen toiminnan osaksi taktisella ja operationaalisella tasolla<br><br>Vaikuttaminen tarvittaessa hyökkäyksellisten kyberoperaatioiden kautta<br><br>Teknisen osaamisen leventäminen ja laajentaminen | Omien järjestelmien suojaaminen kybertoimintaympäristöstä<br><br>Omat päivystysjärjestelmät<br><br>Kyberpuolustuksen operaatiotaidollisten taktisten käyttöperiaatteiden tunnistaminen ja kehittäminen | Koko toiminta riskiarviointilähtöistä, jossa riskejä arvioidaan muuttuneiden uhkatilanteiden ja myös oman toiminnan seurausten kautta<br><br>Hallinnonalalle kuuluvien lakisääteisten tehtävien suorittaminen<br><br>Omien järjestelmien suojaamisen ohella yhteistyökumppaneiden järjestelmien seuranta<br><br>Jatkuva uhka-analyysien teko ja seuranta 24/7 |

### 5.1.4. Tutkinta

Tutkinta on PVJJK:ssa puhtaasti itsenäinen toiminta-alue. Haastattelussa tutkintaan liittyviä toimintatapoja – kuten esimerkiksi siihen liittyviä käytännön työkaluja – ei kuitenkaan voitu sen tarkemmin avata. Kyse on kuitenkin erilaisten tietoteknisten selvitysten tekemisestä, mihin organisaatiolla on olemassa valmiudet niin infrastruktuurin kuin sen käyttötaitojenkin osalta.

TAULUKKO 4 Tutkinta (PVJJK)

| ***AUTONOMISUUSTASO*** | **TUTKINTA** |
|---|---|
| ***NORMATIIVINEN***<br><br>*(ORGANISAATION VAIKUTUSPIIRIN ULKOPUOLELLA MÄÄRITTYVÄT TOIMINNOT)* | |
| ***YHTEISTOIMINNALLINEN***<br><br>*(YHTEISTYÖSSÄ MUIDEN KANSSA MÄÄRITTYVÄT TOIMINNOT)* | |
| ***ITSENÄINEN***<br><br>*(ORGANISAATION SISÄLLÄ MÄÄRITTYVÄT TOIMINNOT)* | Tietoteknisten selvitysten tekeminen |

### 5.1.5. Valvonta ja kehittäminen

Normatiivinen koulutus perustuu puolustusvoimien yhteiseen tietoturvapolitiikkaan ja mahdollisiin, tarpeen mukaan toteutettaviin lisäkursseihin. Yhteisessä tietoturvapolitiikassa on kyse koko henkilöstölle suunnatusta koulutuksesta, jolla ei ole käytännön merkitystä PVJJK:n kyberammatillisten osaamisprofiilien rakentumiselle. Yhteistoiminnallisen tason koulutus puolestaan toteutetaan käytännön harjoittelutoimintana, jolla on oma vuosisuunnitelmansa. Tällä koulutuksella on merkitystä myös PVJJK:n kyberammatillisen osaamisen kannalta, sillä harjoittelu kuuluu puolustusvoimien ydintoimintoihin.

PVJJK:n kyberammatillisen osaamisen profilointi perustuu vahvasti organisaation omaan näkemykseen vaadittavasta osaamisesta. Tässä yhteydessä voidaankin puhua tietynlaisesta politiikasta osaamisen kehittämisessä ja sen vuosittaisessa kartoittamisessa. Taustalla on systemaattinen kartoitus kulloisistakin osaamistarpeista, joihin pyritään vastaamaan sekä omilla ja ulkopuolisten tarjoamilla koulutuksilla että käytännön harjoittelutoiminnalla. Osaamistarvetta arvioidaan aina erikseen henkilö- ja tehtäväkohtaisilla tasoilla. Uusien henkilöiden osalta arvioidaan ensin olemassa oleva osaaminen, minkä pohjalta määritellään vaadittava lisäkoulutustarve.

TAULUKKO 5 Valvonta ja kehittäminen (PVJJK)

| ***AUTONOMISUUSTASO*** | **KOULUTUS** | **STRATEGINEN SUUNNITTELU JA POLITIIKAN KEHITTÄMINEN** |
|---|---|---|
| ***NORMATIIVINEN***<br><br>*(ORGANISAATION VAIKUTUSPIIRIN ULKOPUOLELLA MÄÄRITTYVÄT TOIMINNOT)* | Yhteiseen tietoturvapolitiikkaan liittyvä tietoturvakoulutus<br><br>Lisäkoulutustarpeeseen perustuvat kurssit | Yhteinen tietoturvapolitiikka, joka on suunnattu koko henkilöstölle ja jolla ei ole merkittävää vaikutusta organisaation kyberammatillisiin osaamisprofiileihin |

| | | |
|---|---|---|
| ***YHTEISTOIMINNALLINEN***<br><br>*(YHTEISTYÖSSÄ MUIDEN KANSSA MÄÄRITTYVÄT TOIMINNOT)* | Vuosisuunnitelmaan perustuva harjoittelutoiminta | |
| ***ITSENÄINEN***<br><br>*(ORGANISAATION SISÄLLÄ MÄÄRITTYVÄT TOIMINNOT)* | Vuosittainen osaamiskartoitukseen perustuva koulutus<br><br>Lisäksi osaamistarpeiden tunnistamiseen pohjautuva lisäkoulutus<br><br>Vuosisuunnitelmaan perustuva harjoittelutoiminta | Perustuu pitkälti omaan näkemykseen vaadittavasta kyberammatillisesta osaamisesta<br><br>Vuosittainen osaamiskartoitus tehtävä- ja henkilötasolla |

## 5.2. Kyberrikostorjuntakeskus

Keskusrikospoliisin Kyberrikostorjuntakeskus on viranomaistoimija, joka tarkastelee kybermaailman tapahtumia pitkälti ulkoapäin. Sen pääasialliset tehtävät liittyvät muiden organisaatioiden tai yksilöiden kokemien kyberrikosten tutkintaan ja selvittämiseen. Kyberrikosten tutkinnan ohella tehtäväkenttään kuuluu rikosten ennaltaehkäisyyn ja paljastamiseen liittyviä osa-alueita. Organisaation toiminnan fokus on kuitenkin selkeästi kyberrikosten tutkinnassa, jolloin myös valtaosa sen kyberosaamisesta liittyy suoraan tutkintaan sekä tätä palvelevaan tiedon ja todistusaineiston keräämiseen. Tehtäväkenttä painottaa tutkinta -kategorian keskeistä roolia organisaation kyberosaamisessa, jota tarvitaan sekä teknisen että taktisen alueen toiminnoissa.

Muut kategoriat liittyvät Kyberrikostorjuntakeskuksen toimintaan lähinnä välillisesti. Käytännössä tämä tarkoittaa organisaatiolla sellaista roolia, jossa se toteuttaa toimintaansa hyödyntämällä sille annettuja ja muiden ylläpitämiä resursseja tai toimimalla yhteistyössä ulkopuolisten tahojen kanssa. Tämä tarkoittaa samalla sitä, että näissä kategorioissa organisaatiolla ei esiinny puhtaasti itsenäiseksi luokiteltavia toimintoja, vaan ne kytkeytyvät aina muiden osapuolten valmiuksiin ja niiden tekemiin ratkaisuihin. Käytössä olevan turvallisuusvarannon osalta tämä näkyy siinä, että toiminnan edellyttämä infrastruktuuri saadaan poliisihallinnon it -osastolta valmiiksi kehitettynä kokonaisuutena. Kyberrikostorjuntakeskuksella on tässä puhtaasti tarpeiden esittäjän rooli. Toiminnallisella tasolla taas tutkinnan, ennaltaehkäisyn ja paljastamisen yleisenä edellytyksenä voidaan pitää eri osapuolten välisen yhteistoiminnan onnistumista.

Kyberrikostorjuntakeskuksesta haastateltiin keskuksen johtajaa Timo Piiroista. Haastattelu toteutettiin puhelinhaastatteluna 2.1.2017. Haastattelu tallennettiin samanaikaisesti tietokoneelle ja mobiililaitteelle. Haastattelu kesti yhteensä noin 71 minuuttia.

### 5.2.1. Tutkinta

Kyberrikostutkinta käynnistyy tyypillisesti asiakkaan rikosilmoituksen pohjalta. Alkuvaiheessa muodostetaan tilannekuva asiakkaan omien käsitysten ja käytössä olevan informaation perusteella. Asiakkaan mahdollisen alkuanalyysin lisäksi Kyberrikostorjuntakeskus pyrkii aina jäljittämään myös tapahtumiin liittyvän datan ja lokitiedostot eri lähteistä. Niiden paikantaminen voi kuitenkin olla haasteellista asiakkaan dataliikenteen seurannan puutteellisuuksien ja laiminlyöntien tai toiminnan ulkoistuksiin liittyvien alihankintaketjujen vuoksi. Datan ja lokitietojen puutteellisuus on yleinen Kyberrikostorjuntakeskuksen tutkintaa vaikeuttava ja hidastava tekijä. Mikäli dataliikennettä hallinnoi jokin kolmas osapuoli on tutkintalupa joskus haettava oikeusprosessin kautta. Tilanne voi olla tätäkin mutkikkaampi silloin, jos dataliikenteen hallinnoinnin alihankintaketju pitenee. Toisaalta koko tutkintaprosessi voi myös laueta siihen, että asiakas katsoo asian loppuun käsitellyksi eikä nosta sen tiimoilta syytettä.

Asiakkaan intressi on tavallisesti rikoksentekijän tunnistamisessa ja hyökkäyksen motiivin selvittämisessä. Tapahtumien selvittäminen edellyttää usein laajaa keinovalikoimaa, sillä tietoja on hankittava lukuisista eri lähteistä. Eri viranomaisten välisellä yhteistyöllä on suuri merkitys rikosprosessien selvittämisessä, mikä tarkoittaa yhä useammin yhteistyötä myös maan rajojen ulkopuolella. Kyberrikostorjuntakeskuksen käytössä on yhteistyön lisäksi poliisin pakkokeinovalikoima, joka tehostaa osaltaan selvitystyötä.

Teknisessä tutkinnassa organisaatio hyödyntää kaupallisia sovelluksia, joiden avulla tutkitaan päätelaitteita ja niiden sisältämiä lokitietoja. Teknistä osaamista hankitaan organisaation sisäisellä koulutuksella, mutta sitä voidaan tarvittaessa ostaa myös kaupallisista lähteistä. Teknisen tutkinnan alueella organisaatiossa toimii sekä teknisen koulutuksen saaneita poliisiviranomaisia että siviilivirkamiehiä. Siviilihenkilöstö edustaa usein sellaista teknisen osaamisen aluetta, joka on organisaatiolle välttämätöntä, ja jolla paikataan poliisiviranomaisten osaamisvajetta. Yleisesti teknisen osaamisen kehittäminen on poliisissa ollut vakiintunutta jo useita vuosia, mikä tarkoittaa sekä koulutustarpeiden tiedostamista että valmiuksia kouluttaa henkilöstöä vaadittuihin tehtäviin.

Taktinen tutkinta puolestaan tarkoittaa erilaisten hallinnollisten tehtävien ohella kuulustelujen, kotietsintöjen ja kyberrikollisten kiinniottojen suorittamista. Käytännössä on siis kyse poliisiviranomaisen tehtävistä kybertoimintaympäristössä, jolloin poliisiviranomaisella on oltava samanaikaisesti myös sekä ymmärrys kybermaailmasta että riittävästi teknistä osaamista. Laajassa mittakaavassa kaikkien osa-alueiden hallinta on ainakin toistaiseksi osoittautunut poliisille varsin haasteelliseksi tehtäväksi. Tilanne on sikäli ristiriitainen, että asia liittyy poliisin resursointipäätöksiin, joita osaltaan ohjaa sisään tulleiden rikosilmoitusten määrä. Toisaalta asiakkaiden halukkuuteen tehdä rikosilmoituksia taas vaikuttaa poliisin uskottavuus kyberrikosten selvittäjänä.

TAULUKKO 6 Tutkinta (Kyberrikostorjuntakeskus)

| ***AUTONOMISUUSTASO*** | **DIGITAALINEN RIKOSTEKNIIKKA** | **TUTKINTA** |
|---|---|---|
| ***NORMATIIVINEN***<br><br>*(ORGANISAATION VAIKUTUSPIIRIN ULKOPUOLELLA MÄÄRITTYVÄT TOIMINNOT)* | | |
| ***YHTEISTOIMINNALLINEN***<br><br>*(YHTEISTYÖSSÄ MUIDEN KANSSA MÄÄRITTYVÄT TOIMINNOT)* | Datan ja lokitietojen jäljittäminen asiakkaan kanssa<br><br>Asiakkaan omien alkujohtopäätösten pohjalta tapahtuva jatkotoimenpiteiden suunnittelu asiakkaan kanssa<br><br>Kotimainen ja kansainvälinen viranomaisyhteistyö todistusaineiston keräämisessä | Poliisin sisäinen tutkintaan liittyvä yhteistyö, jota toteutetaan sovitun tehtäväjaon mukaan |
| ***ITSENÄINEN***<br><br>*(ORGANISAATION SISÄLLÄ MÄÄRITTYVÄT TOIMINNOT)* | Analyysien teko asiakkaalta saadun datan ja lokitietojen perusteella<br><br>Datan ja lokitietojen hankkiminen kolmansilta osapuolilta tarvittaessa pakkokeinoin | Teknisen ja taktisen tutkinnan toteuttaminen |

### 5.2.2. Kerääminen ja operointi

Kerääminen ja operointi -kategoriassa merkitykselliseksi toiminnoksi nousee yhteistyöhön perustuva havainnointi. Kiellettyjen ja vilpillisten kybertoimintojen havaitseminen edellyttää käytännössä säännönmukaista yhteistyötä viranomaisten, erityisesti kyberturvallisuuteen liittyvien organisaatioiden välillä. Kyberrikostorjuntakeskuksella on yhteistyösopimus Viestintäviraston Kyberturvallisuuskeskuksen kanssa, jossa organisaatio hoitaa rikosprosesseihin liittyvän alueen.

TAULUKKO 7 Kerääminen ja operointi (Kyberrikostorjuntakeskus)

| ***AUTONOMISUUSTASO*** | **HAVAINNOINTI** |
|---|---|
| ***NORMATIIVINEN***<br><br>*(ORGANISAATION VAIKUTUSPIIRIN ULKOPUOLELLA MÄÄRITTYVÄT TOIMINNOT)* | |
| ***YHTEISTOIMINNALLINEN***<br><br>*(YHTEISTYÖSSÄ MUIDEN KANSSA MÄÄRITTYVÄT TOIMINNOT)* | Yhteistyö viranomaisten, erityisesti muiden kyberturvallisuusorganisaatioiden kanssa |

| | |
|---|---|
| *ITSENÄINEN*<br><br>*(ORGANISAATION SISÄLLÄ MÄÄRITTYVÄT TOIMINNOT)* | |

### 5.2.3. Valvonta ja kehittäminen

Kyberrikostorjuntakeskuksen poliisiviranomaisten pääasiallinen koulutus tapahtuu Poliisiammattikorkeakoulussa, joka vastaa tarvittaessa myös teknisen alan peruskoulutuksesta. Teknistä ymmärrystä tarvitaan laajasti tämän päivän rikostutkinnassa, minkä vuoksi Poliisiammattikorkeakoulussa panostetaan tähän alueeseen yhä enemmän. Kyberrikostorjuntakeskuksessa hyödynnetään myös kaupallisia koulutuspalveluita, sillä sen omat tekniset osaamisvaatimukset ovat selvästi poliisin keskimääräistä yksikköä suuremmat. Lisäksi organisaation jäsenet voivat hankkia osaamista opiskelemalla julkisissa oppilaitoksissa, tekemällä yhteistyötä näiden kanssa tai työskentelemällä eri alojen työtehtävissä. Koulutuksen ja organisaation toiminnan kehittämisen näkökulmasta yhteistyötä erityisesti eri koulutuksen tarjoajien kanssa tulisi edelleen tiivistää tulevaisuudessa.

Taktista osaamista voidaan kehittää lähinnä poliisin sisäisillä koulutuksilla, sillä taktinen toiminta on tiukasti kansallisilla ja kansainvälisillä laeilla ja sopimuksilla säädettyä toimintaa ja siten alueena ulkopuolisten koulutuksen järjestäjien ulottumattomissa. Yhteistyöstä muiden viranomaisten ja kyberalan organisaatioiden kanssa voidaan mainita aiemmin esille tuotu yhteistyösopimus Viestintäviraston Kyberturvallisuuskeskuksen kanssa. Se perustuu molemminpuoliseen toimintojen kehittämisen tarpeeseen, jonka tavoitteena on erityisesti toiminnan yleinen tehostaminen sekä yhteisen osaamisen ja koulutusmuotojen kehittäminen. Tämän tyyppinen yhteistoiminta on lisääntynyt, mutta tarve sen edelleen kehittämiselle ja kasvattamiselle on selkeästi olemassa. Tässä hidasteena on heikko liikkuvuus eri hallinnonalojen välillä: tyypillisesti työntekijät tarkastelevat asioita vain oman hallinnonalansa sisältä käsin.

Kyberrikostorjuntakeskuksessa tarvetta osaaville työntekijöille on sekä teknisellä että taktisella alueella. Viime aikojen kehityssuunta on viitannut siihen, että lähitulevaisuudessa syvällisistä teknisistä osaajista saattaa tulla pulaa. Taktisen tason osaamisesta kyberturvallisuuden alueella sen sijaan on ollut pulaa jo pitkään. Kyse on varsin yleisestä ilmiöstä poliisin koko organisaatiossa, jossa haasteeksi muodostuu kybermaailman tapahtumien merkityksen ymmärtäminen taktisen tutkinnan kannalta.

TAULUKKO 8 Kerääminen ja operointi (Kyberrikostorjuntakeskus)

| *AUTONOMISUUSTASO* | KOULUTUS JA HARJOITTELU |
|---|---|

| | |
|---|---|
| ***NORMATIIVINEN***<br><br>*(ORGANISAATION VAIKUTUSPIIRIN ULKOPUOLELLA MÄÄRITTYVÄT TOIMINNOT)* | Poliisiviranomaisten koulutus Poliisiammattikorkeakoulussa<br><br>Opiskelu yleisissä julkisissa oppilaitoksissa<br><br>Kaupallisen koulutustarjonnan käyttö |
| ***YHTEISTOIMINNALLINEN***<br><br>*(YHTEISTYÖSSÄ MUIDEN KANSSA MÄÄRITTYVÄT TOIMINNOT)* | Yhteistyö viranomaisten ja muiden kyberturvallisuusorganisaatioiden kanssa<br><br>Yhteistyö oppilaitosten kanssa<br><br>Eri alojen työtehtävissä oppiminen |
| ***ITSENÄINEN***<br><br>*(ORGANISAATION SISÄLLÄ MÄÄRITTYVÄT TOIMINNOT)* | Organisaation oma koulutus |

# 6. JOHTOPÄÄTÖKSET

## 6.1. Ydinkompetenssin muodostuminen kohdeorganisaatioissa

Tässä tutkimuksessa kohdeorganisaatioiden ydinkompetenssin sisältö muodostuu pääosin niistä NCWF -viitekehyksen kategorioiden toiminnoista, jotka toteutetaan itsenäisesti tai yhteistyössä muiden osapuolten kanssa. Kyse on siten joko täysin autonomisista tai yhteistoiminnallisen tason toiminnoista. Näissä toiminnoissa tulevat esiin sekä organisaatioiden olennaisimmat kyberosaamisen tarpeet että myös niiden todelliset mahdollisuudet vaikuttaa osaamiseensa. Kyse on juuri niistä keskeisistä toiminnoista, jotka organisaatioiden on tunnistettava kyberammatillisen työvoiman kehittämisen edellytyksenä (Furnell ym., 2017). Normatiivisen tason toimintoihin liittyy myös osaamisvaatimuksia, joita voidaan pitää edellytyksinä lähinnä lakisääteisten velvoitteiden täyttämiselle. Tämän tutkimuksen näkökulmasta niissä on kuitenkin pitkälti kyse organisaatioiden vaikutuspiirin ulkopuolella olevista toiminnoista. Näin ollen niitä ei voida pitää olennaisina ydinkompetenssin muodostumisessa, joka voi kehittyä vain organisaation sisällä (Chen & Chang, 2010).

Organisaatioiden toiminnan tarkoitus määrittää pitkälti ne kategoriat, joihin liittyvät toiminnot nousevat ydinkompetenssin sisällön kannalta keskiöön. Pääpaino ydinkompetenssin muodostumisessa on itsenäisen tason toiminnoissa, joihin myös tuloksissa on kirjattu eniten toimintoja. Tutkimusaineisto puoltaa myös vahvasti tulevaisuusnäkökulman mukanaoloa nykytilan ohella tutkimuksen toisena aikaulottuvuutena. Kybermaailmaa luonnehtivan jatkuvan muutoksen tilan vuoksi onkin olennaista tuoda esiin vielä kehittymisvaiheessa olevia toimintoja (Burley ym., 2014; Hoffman ym., 2012). Tällä on potentiaalisesti suuri merkitys, sillä kyse on käytännössä jo nyt kyberosaamisen näkökulmasta tärkeistä painopistealueista. Näistä toiminnoista muodostuukin todennäköisesti lähitulevaisuudessa osa kohdeorganisaatioiden ydinkompetenssin keskeistä sisältöä.

### 6.1.1. Puolustusvoiminen Johtamisjärjestelmäkeskus

PVJJK:ssa kyberosaamisen keskeisiksi alueiksi nousevat yhtäältä organisaation oman palvelutuotannon suojaaminen ja toisaalta kyberpuolustuksen ja -vaikuttamisen liittäminen osaksi koko puolustusvoimien sotilaallista toimintaa. Ensin mainitussa on kyse PVJJK:lle joko lakisääteisesti tai muista syistä kuuluvien tehtävien turvallisesta hoitamisesta. Tässä yhteydessä voidaan siis puhua perinteisestä palvelutuotantoympäristön tietoturvanäkökulmasta. Jälkimmäinen taas liittyy suoraan kansallisen kyberturvallisuuden sotilaalliseen osaan, jossa

PVJJK:n rooli on kyberpuolustuksen ja -vaikuttamisen toiminnoissa. PVJJK:n toiminnassa käytettävä infrastruktuuri tulee yleensä organisaatiolle valmiina, jolloin sen kyberosaamisessa itse toimintatavat sekä niihin liittyvä turvallisuus ja vaikuttavuus nousevat selkeästi hallitseviksi elementeiksi.

Puolustusvoimien informaatioteknologisen infrastruktuurin kehittämisestä vastaa pääosin logistiikkalaitos. Vaikka PVJJK ei siis itse kehitä infrastruktuuria, niin sillä on oltava selkeä näkemys niistä vaatimuksista, joita se kehitettäville järjestelmille ja sovelluksille aikoo asettaa. Sama pätee yhtä lailla kenttäolosuhteissa testattavien sovellusten käyttökelpoisuuden määrittelyyn. Edelliset liittyvät ennen kaikkea kyberpuolustukseen, jonka kehittämistyössä PVJJK:n on asetettava järjestelmille ja sovelluksille niiden suorituskykyyn liittyviä erityisvaatimuksia.

Organisaatiossa käsiteltävän informaation kannalta keskeistä on sekä tiedonlaadunvarmistus että sen hallinta. Tämä edellyttää luonnollisesti hyvin suunniteltua tietoturvakontrollia ja sen hallintaa. Tieto on osattava turvaluokitella oikein, huolehtia tiedon turvallisesta käsittelystä ja siirtämisestä sekä reagoida nopeasti tiedon statuksen muutoksiin. Informaatioon liittyviä olennaisia tekijöitä ovat myös kyky määritellä tiedon sensitiivisyysasteen mukaan pääsyoikeuksiin ja tiedon varastointiin liittyvät kriteerit.

Järjestelmänhallinnan kannalta olennaiset toiminnot liittyvät verkostoturvallisuuteen, joka PVJJK:ssa tarkoittaa sidosryhmäturvallisuuden varmistamista. Kyse on ennen kaikkea ei-viranomaistahoihin sovellettavista turvallisuusselvitysmenettelyistä, joilla kontrolloidaan yhteistyökumppaneiden pääsyoikeuksia PVJJK:n järjestelmiin ja tietovarantoihin. Käytännössä edellytyksenä on yksilöllisten selvitysten tekeminen jokaisen yhteistyökumppanin osalta. PVJJK:n on siten kyettävä tunnistamaan yhteistyöorganisaation henkilöstöön ja järjestelmiin liittyvät riskit, arvioitava niiden suhteellista merkitystä omalta kannaltaan, toteutettava määräaikaisauditointeja ja tarkkailtava jatkuvasti tilanteen mahdollisia muutoksia. Yleisen tietoturvakontrollin ohella näiden toimintojen onnistunut toteuttaminen kuuluu organisaation tietoturvan näkökulmasta olennaisiin tekijöihin.

PVJJK :n toiminnan luonteesta seuraa suojelu- ja puolustuskategorian toimintojen selkeästi muita merkittävämpi rooli sen toiminnassa: voidaan perustellusti puhua koko toiminnan rakentumisesta ympärivuorokautisen uhkaseurannan ympärille. Tämä näkyy myös kategorian yhteistoiminnallisen tason toiminnoissa, jotka nousevat selkeästi esiin suojelu- ja puolustustoimintojen kehittämisessä ja ylläpidossa. Riskien hallintaan liittyvän ympäristön havainnoinnin ja erityisesti sen perusteella laadittavien uhka-analyysien kannalta viranomaisyhteistyö nousee tässä kategoriassa kriittisen tärkeäksi. Se edellyttää PVJJK :lta niin tiedon tuottajana kuin vastaanottajana kykyä erottaa merkityksellinen informaatio kulloinkin saatavilla olevasta datan kokonaismäärästä. Toisaalta omien toimien, esimerkiksi uuden tietoliikenneyhteyden avaamisen tai

ulkopuolisten kumppanuussopimusten potentiaalisten seurannaisvaikutusten tunnistaminen on myös merkityksellinen osaamisalue.

Toiminnallisen kehittymisen kannalta keskeinen haaste on kyberpuolustuksen sulauttaminen osaksi taktisen ja operationaalisen tason toimintoja. Kyse on tässä koko puolustusvoimien laajuisesta tavoitteesta, mikä on seurausta sodankäynnin luonteessa tapahtuneista muutoksista. PVJJK:n osalta voidaan kuitenkin yhtä lailla puhua sen yleisestä kyvystä reagoida tapahtumiin tarkoituksenmukaisesti ja riittävällä nopeudella. Käyttöperiaatteiden ja toimintatapojen jatkuva kehittäminen yhteistoiminnallisissa harjoituksissa palvelee osaltaan vaadittavan osaamisen kehittämistä ja ylläpitoa. Teknisellä tasolla PVJJK:n osaaminen on jo riittävää, mutta sitä on edelleen laajennettava organisaation sisällä. Tätä voidaan pitää yhtenä seurauksena kybermaailman merkityksen kasvun aiheuttamasta muutostarpeesta organisaatiossa.

Kyberpuolustuksen yhdistäminen osaksi taktisen ja operationaalisen tason sotilaallista toimintaa on muodostumassa yhä selkeämmin PVJJK:n kyberosaamisen painopistealueeksi. Käytännössä tavoitteena on sellaisen osaamisen aikaansaaminen, jonka avulla voidaan suunnitella ja toteuttaa kybersotilaallisia toimintoja. Kyse on kuitenkin voimakkaasti kehittyvästä alueesta, minkä vuoksi kaikkia siihen liittyviä kehitystarpeita ja seurauksia - ja siten kyberosaamisen vaatimuksiakaan - ei vielä voida tunnistaa. Tämä asetelma näyttäisi noudattelevan varsin pitkälti yleistä käsitystä kybermaailman todellisuudesta (Cybersecurity Competence Building Trends, 2016; Professionalizing Cybersecurity: A path to universal standards and status, 2014; Hoffman ym., 2012). On myös syytä huomioida, että erilaisten toimintamallien ja innovaatioiden jalostuminen ja niiden vaikuttavuuden arviointi voi olla vuosien, jopa vuosikymmenen prosessi, jolloin puhutaan väistämättä pitkän aikavälin ilmiöistä tässä kontekstissa.

Konkreettisena vielä kehitysvaiheessa oleva todellisuus näyttäytyy tietoliikenteeseen perustuvissa sotilaallisissa johtamissovelluksissa, joiden käytön edellyttämä kyberosaaminen vaikuttaa vielä osin olevan tunnistamisvaiheessa. Tavoitteena on joka tapauksessa sellaisen osaamisen saavuttaminen, joka mahdollistaa sekä taktisten ja operationaalisten käyttöperiaatteiden tunnistamisen ja kehittämisen että niihin perustuvan teknisen osaamisen liittämisen käytännön puolustus- ja vaikuttamistoimintoihin. Tässä hyökkäyksellisten kyberoperaatioiden suorituskyvyn kehittäminen näyttäisi nousevan ehkä nykyistä suurempaan rooliin tulevaisuudessa.

PVJJK:lla on laaja henkilöstöresurssi; erityisesti potentiaalisesti käytettävissä oleva työvoima on poikkeuksellisen suuri. Työvoiman osaamiskartoitukseen ja koulutukseen on myös panostettu merkittävästi, minkä tarkoituksena on reagoida kehittyvän kybermaailman jatkuviin muutostilanteisiin. Henkilöstöresurssien johtamisen alueella PVJJK:n toiminta näyttäytyykin hyvin tarkoituksenmukaisena (Cybersecurity Competence Building Trends, 2016). Lähitulevai-

suudessa keskeiseksi nousee kuitenkin PVJJK :n kyky tunnistaa uusia osaamisvaatimuksia, joita voi tulla eteen hyvinkin nopeasti (Furnell ym., 2017).

Kybermaailma nivoutuu yhä vahvemmin sotilaallisen suorituskyvyn yhdeksi elementiksi. Tämä kehityskulku kasvattaa todennäköisesti myös reserviläisten ja asevelvollisten osaamispotentiaalin kysyntää poikkeusoloissa merkittävästi. Kybermaailman ongelmien monimutkaistuminen edellyttääkin yhä laajempaa ja syvempää osaamista, jolloin siviiliryhmien osaamispääomasta voi muodostua jopa olennainen lisäresurssi kyberosaamisen kokonaisuudessa. Tämän potentiaalin tehokas hyödyntäminen vaatii kykyä kartoittaa, seurata ja päivittää systemaattisesti potentiaalisten henkilöiden osaamisprofiilia. (Cybersecurity Competence Building Trends, 2016).

Säännöllisesti toteutettavat yhteistoimintaharjoitukset ovat yksi keskeinen osaamistarpeiden tunnistamisen väylä, sillä niissä omaa ja yhteistyökumppaneiden osaamista voidaan verrata välittömästi käytännön tilanteissa. PVJJK määrittelee organisaatiossaan vaaditun kyberosaamisen autonomisesti, mikä edellyttää jatkuvaa oman osaamisen kriittistä arviointia suhteessa ulkoisen ympäristön muutoksiin. Kulloinkin vaaditun osaamisprofiilin muodostamisen ohella myös mahdollinen lisäkoulutus on organisoitava tarkoituksenmukaisesti. Tämä tarkoittaa vuosittaiseen osaamiskartoitukseen perustuvan koulutuksen ohella valmiutta tarjota myös yksilöllistä koulutusta tilanteen vaatiessa.

PVJJK:n ydinkompetenssin (Taulukko 9) toiminnoista valtaosan voidaan katsoa edustavan vakiintuneita toimintatapoja. Todellisuudessa useimmat näistäkin toiminnoista kehittyvät tai vähintään jalostuvat kaiken aikaa. Tämä on erityisen oletettavaa ainakin suojaaminen ja puolustus- sekä valvonta- ja kehittäminen -kategorioissa. Riskien hallinnan menetelmät, tekninen kehittäminen ja osaamisen päivittäminen vaativat myös uudenlaisten toimintamallien omaksumista. Suojelu- ja puolustus -kategorian toiminnot muodostavat selkeästi laajimman osan PVJJK :n ydinkompetenssissa. Siinä tulevat esiin myös koko organisaation toiminnan kannalta keskeiset tulevaisuuteen luotaavat toiminnot. Toimintojen kehittymisen lähtökohtana tässä on kuitenkin vielä osittain tuntemattoman osaamisen tunnistaminen, mitä voidaan pitää PVJJK :n keskeisenä lähitulevaisuuden haasteena (Furnell ym., 2017).

TAULUKKO 9 Ydinkompetenssi (PVJJK)

| | TURVALLISUUDEN TARJOAMINEN | OPEROINTI JA YLLÄPITO | SUOJELU JA PUOLUSTUS | VALVONTA JA KEHITTÄMINEN |
|---|---|---|---|---|
| VAKIINTUNUT | Tietoturvakontrollien suunnittelu ja hallinta<br><br>Tiedon elinkaaren määrittely | Sidosryhmä-turvallisuuden varmistaminen<br><br>Tietoturvakontrollien toteuttaminen erityisesti operaatioturvallisuuden kautta | Riskien hallinta jatkuvan seurannan ja viranomaisyhteistyön kautta sekä niihin perustuva uhka-analyysien tuottaminen<br><br>Käyttöperiaatteiden ja toimintojen kehittäminen harjoitusten ja testauksen kautta<br><br>Teknisen osaamisen ja suorituskyvyn ylläpito, laajentaminen ja kehittäminen<br><br>Koko potentiaalisen henkilöstöresurssin osaamispääoman tunteminen | Nopea ja joustava reagointikyky tehtävä- ja henkilötason osaamiseen liittyvissä vaatimuksissa |
| KEHITTYVÄ | | | Kyberpuolustuksen sekä taktisen ja operationaalisen tason sotilaallisten käyttöperiaatteiden ja toimintojen yhteensovittaminen<br><br>Yhteensovittamisen edellyttämän uuden osaamisen tunnistaminen | |

### 6.1.2. Kyberrikostorjuntakeskus

Kyberrikostorjuntakeskuksen toiminta painottuu jo toteutuneiden, epäilyttävien tai rikollisiksi luokiteltavien kybertapahtumien tutkinnan alueille. Tehtäväkenttä koostuu lisäksi erilaisista ennaltaehkäisevistä toimenpiteistä ja kybertapahtumien paljastamisista. Kaikki nämä alueet edellyttävät yhteistyötä organisaation ulkopuolisten toimijoiden kanssa, jolloin lopputulokseen vaikuttaa aina merkittävästi myös muiden osapuolten kapasiteetti. Kyse on yhtä lailla niin asiakkaiden tai toimeksiantajien valmiuksista kuin yhteistyön toimivuu-

desta organisaation varsinaisten yhteistyökumppaneiden kanssa. Kybertapahtumien kasvun ja monimutkaistumisen myötä organisaation kyky kehittää yhteistyöverkostoaan toimivien yhteistyösopimusten avulla nousee yhä tärkeämmäksi. Samalla tiivistyvän kansainvälisen yhteistyön merkitys tulee kasvamaan entisestään (Hoffman, Burley & Toregas, 2012).

Kyberrikosten selvittämisen kannalta kriittiseksi tekijäksi nousee asiakkailta saatava informaatio ja sen laatu. Todellisuudessa organisaation käyttöön saatavissa oleva informaatio on enemmän tai vähemmän puutteellista, sillä asiakkailla ei yleensä ole kykyä valvoa omia järjestelmiään riittävällä tasolla. Ilmiö liittyy siten suoraan asiakkaiden operointi- ja ylläpito, suojelu- ja puolustus, kerääminen ja operointi sekä analysointi -kategorioiden toimintojen laatuun. Taustalla voi olla asiakkaiden osaamattomuus, resurssien puute tai jopa suoranainen välinpitämättömyys. Tavallisesti kyse on kuitenkin dataliikenteen seurantatoimintojen ulkoistuksesta alihankkijalle tai jopa usealle toimijalle joskus pitkässäkin alihankintaketjussa. Alihankintaketjun pidentyminen onkin muodostunut yhdeksi keskeiseksi Kyberrikostorjuntakeskuksen tutkintaa hidastavaksi ja vaikeuttavaksi tekijäksi.

Informaation jäljitettävyyttä ja laatua on kuitenkin mahdollista parantaa ennaltaehkäisevin toimin, mikä käytännössä tarkoittaa asiakkaiden valistamista ja motivointia kohti tarkoituksenmukaisempaa tietoturvakulttuuria. Tässä Kyberrikostorjuntakeskuksella on oma roolinsa asiakkaiden tiedottajana, herättelijänä ja motivoijana - joko ennaltaehkäisevästi tai tätäkin useammin tapahtumien analysoijana. Potentiaalisesti suurempi vaikuttavuus tiedottamisessa saavutetaan kuitenkin kyberalan organisaatioiden yhteistyön kautta. Edellytykset varsinkin maan sisäiselle yhteistyölle ovat suotuisat, sillä alan toimijoiden keskinäinen tunnettuus on hyvällä tasolla. (Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, 2016). Erityisesti hallinnonalojen 'siiloutumistaipumus' on kuitenkin toistaiseksi luonut rationaaliselle yhteistyölle haasteellisuutta.

Edellisestä huolimatta keskeisessä roolissa rikosten selvittämisen kannalta on kuitenkin asiakkaiden oma valveutuneisuus. Olennaisen ja epäolennaisen erottaminen toisistaan vaatii aina analysointia, jota pelkän teknologian avulla ei voida vaikuttavasti toteuttaa. Tavoitteena onkin oltava sellaisen asiakkaan havaintokyvyn saavuttaminen, joka mahdollistaa realistisen ja ajantasaisen tilannekuvan muodostamisen kulloisestakin tilanteesta. Tämä edellyttää loogista kokonaisnäkemystä tapahtumien merkityksestä, jonka muodostaminen voi olla asiakkaan itsensä tai jonkin dataliikenteen seurannasta vastaavan ulkopuolisen toimijan vastuulla. Riskien hallinnan näkökulmasta yksi ratkaisu olisi myös toimialakohtaisten yhteisöjen muodostaminen tapahtumien havainnointia ja niistä tiedottamista varten. Tällainen organisatoristen rajojen ylittävä tilanneseuranta selkiinnyttäisi tilannekuvan muodostamista erityisesti kampanjamuotoisesti toteutettavasta haitallisesta toiminnasta. Asiakkaiden hahmottunutta

tilannekuvaa voidaan pitää myös yhtenä Kyberrikostorjuntakeskuksen selvitys- ja tutkimustyön vaikuttavuuden perusedellytyksenä.

Kyberrikostorjuntakeskuksen tehtävien edellyttämä tekninen osaaminen näyttäisi toistaiseksi olevan organisaatiossa riittävällä tasolla. Tiettyjen tehtävien hoitaminen edellyttää kuitenkin ulkopuolisen osaamisen hankkimista. Ulkoisten palvelujen käytön voi ennustaa lisääntyvän, mikäli organisaatiossa havaitut signaalit uusien käytännön osaajien vähenevästä tarjonnasta osoittautuvat pysyvämmäksi ilmiöksi (Furnell, Fischer & Finch, 2017). Tällöin kyse on samalla yhteiskunnallisen tason koulutuspoliittisesta ongelmasta, jota Kyberrikostorjuntakeskus voi kuitenkin pyrkiä lieventämään omalla sisäisellä koulutuksellaan. Tähän saakka organisaatio on paikannut osaamisvajettaan rekrytoimalla työvoimaa enenevästi myös siviilimarkkinoilta. Tulevaisuudessa myös organisaation ulkopuolelta hankittu työssäoppiminen voi nousta entistä suurempaan rooliin kyberammatillisen osaamisen kehittämisessä. Uudenlaiset osaamisen kehittämisen keinot kasvattavatkin edelleen merkitystään, mikäli kybermaailman ilmiöiden laajentumisesta aiheutuu organisaatiolle merkittävää osaamisvajetta. (Vogel, 2016; Cybersecurity Competence Building Trends, 2016; National Initiative for Cybersecurity Education, 2013).

Kyberrikosten taktisen tutkinnan osaamisvaje on edellistäkin mittavampi haaste, sillä se ulottuu poliisin koko organisaatioon. Pohjimmiltaan siinä on kyse poliisin yleisestä uskottavuudesta kyberrikosten ratkaisijana. Kyberrikostorjuntakeskuksen toimintaan vallitseva tilanne vaikuttaa ainakin niin, että välttämättä kaikki tutkinnan arvoiset kyberrikokset eivät tule poliisin eri yksiköistä edes sen tietoon. Käytännössä ainoa keino tässä on pyrkiä lisäämään poliisin yksiköiden taktisten tutkijoiden ymmärrystä kyberrikosten merkityksestä ja niiden teknisestä ulottuvuudesta.

Tilanteen edistämisessä Kyberrikostorjuntakeskuksella on keskeinen rooli, sillä kyse on taktisesta ja siten puhtaasti poliisin sisäisen toiminnan alueesta. Organisaation on kyettävä kehittämään monipuolisesti poliisihallinnon ja poliisi eri yksiköiden kyberalueen ymmärrystä ja kyberosaamista. Tämä tehtäväalue lisää todennäköisesti osaltaan myös uuden siviilityövoiman rekrytointitarvetta tulevaisuudessa. Lopullisena tavoitteena voi kuitenkin olla vain tilanne, jossa poliisin kykyyn ratkaista kyberrikoksia luotetaan ja sille annetaan tiedot potentiaalisista ja epäilyttävistä kybertapahtumista.

Kyberrikostorjuntakeskuksen ydinkompetenssin sisällössä korostuvat lähitulevaisuuteen suuntautuvat ja yhteistyötä edellyttävät toiminnot (Taulukko 10). Varsinkin organisaation päätehtävään, kyberrikosten selvittämiseen vaikuttavat merkittävästi vielä kehitysvaiheessa olevat - ja erityisesti muista osapuolista riippuvat - toiminnot. Asiakkaalta saatava alkuinformaatio on vakiintunut toiminnan lähtökohdaksi, mutta toisaalta senkin saatavuuteen ja laatuun liittyy voimakkaita kehityspaineita. Organisaation on hankittava informaatiota myös suuntautumalla yhä enemmän tiedonvaihtoon eri yhteistyöosapuolten välillä.

Tämä voi liittyä niin ennaltaehkäisevään havainnointiin kuin tietojen saantiin jo toteutuneista tapahtumista.

Organisaation sisällä taas käytännön tutkintavalmiudet edellyttävät sekä teknisen että taktisen tutkinnan kehittämistä, joista jälkimmäiseen panostamista voidaan kehittymisen näkökulmasta luonnehtia kriittiseksi tekijäksi (Cybersecurity Forum Initiative, 2013). Kyse on laajasta kokonaisuudesta poliisissa, jonka kehittämisessä Kyberrikostorjuntakeskuksella on merkittävä vastuu. Yleisesti osaamisen kehittäminen vaatiikin todennäköisesti sekä kasvavaa siviilityövoiman rekrytointia että henkilöstön lisäpätevöitymistä myös organisaation ulkopuolisissa työtehtävissä.

TAULUKKO 10 Ydinkompetenssi (Kyberrikostorjuntakeskus)

| | **TUTKINTA** | **KERÄÄMINEN JA OPEROINTI** | **VALVONTA JA KEHITTÄMINEN** |
|---|---|---|---|
| **VAKIINTUNUT** | Asiakkaan informaatioon perustuvat tutkintatoimet ja analyysit | | |
| **KEHITTYVÄ** | Kotimaisen ja kansainvälisen yhteistyön kehittäminen ja laajentaminen<br><br>Teknisen ja erityisesti taktisen tutkinnan operationaalisten toimintavalmiuksien kehittäminen | Kotimainen ja kansainvälinen yhteistyö kybertapahtumien havainnoinnissa | Yhteistyö viranomaisten ja muiden kyberturvallisuus-organisaatioiden kanssa<br><br>Organisaation ulkopuolelta hankittava osaaminen työtehtävissä |

# 7. POHDINTA

Tässä tutkimuksessa on pyritty hahmottamaan kyberosaamisen ydinkompetenssin sisältöä kahdessa erityyppisessä julkisen sektorin organisaatiossa. Vaikka tutkimusentiteetit ovat keskenään melko erilaisia, on kyberammatillinen osaaminen niiden toiminnassa kuitenkin hyvin keskeisessä roolissa. Ydinkompetenssissa on kyse organisaatiotason ominaisuudesta, joka on samalla aina uniikkia ja siten organisaatiokohtaista. Näin ollen on luonnollista ja odotettavaa, että ydinkompetenssin sisältö vaihtelee organisaatioiden välillä myös kyberosaamisen kontekstissa. Erityisesti kybermaailman voimakkaan kehittymisen vuoksi ydinkompetenssiin on tässä tutkimuksessa liitetty vakiintuneiden toimintojen ohella myös merkitystään kasvattaneita ja potentiaalisesti kasvattavia kyberosaamisen toiminta-alueita.

Ydinkompetenssin hahmottamiseksi tutkimuksessa on sovellettu valikoidusti ja organisaatiokohtaisesti National Cybersecurity Workforce Framework (NCWF) -viitekehystä. Käytännössä tämä tarkoittaa viitekehyksen niiden kategorioiden mukanaoloa, joihin liittyviä toimintoja kohdeorganisaatioissa voidaan tunnistaa. Lisäksi vain osa huomioiduista kategorioista ja niiden toiminnoista voidaan perustellusti liittää osaksi lopullista ydinkompetenssin sisältöä. Organisaatioilla voi olla sellaisia ulkopuolelta säädeltyjä, usein rutiiniluonteisia tehtäviä, joihin liittyvä kyberosaaminen on pitkälti sen oman vaikutuspiirin ulkopuolella tai jotka eivät muuten edusta sen välittömiä ydintoimintoja. Tässä tutkimuksessa ydinkompetenssi muodostuukin lähinnä toiminnoista, joiden kehittyminen voi tapahtua organisaation sisällä tai aktiivisessa yhteistoiminnassa ulkoisen ympäristön kanssa. Toisaalta kummankin kohdeorganisaation toimintaan voi silti liittyä myös ulkoapäin annettuja, organisaatiolta kyberosaamista edellyttäviä toimintoja, jotka ovat osa niiden ydinkompetenssia.

PVJJK:ssa lakisääteisten palvelujen tuottaminen edustaa ulkopuolelta säädeltyä toimintaa. Kyse on kuitenkin samalla organisaation ydintoiminnoista, jolloin sen omaan osaamiseen tukeutuva palvelutuotannon turvaaminen on yksi sen ydinkompetenssin elementeistä. Organisaation hyödyntämä teknologinen infrastruktuuri on myös ulkoapäin valmiina annettua, rutiiniluonteisesti toteutettua toimintaa. Kehitettävään infrastruktuuriin voi kuitenkin liittyä toiminnan sotilaallinen ulottuvuus, jolloin organisaation on myös itsenäisesti kyettävä testaamaan sovelluksia.

Keskeisimpiä vakiintuneita ydinkompetenssin alueita PVJJK:ssa ovat kuitenkin suojaaminen ja puolustus -kategorian toiminnot. Näillä on myös selkeä yhteys toisiinsa, sillä uhka-analyysien tuottaminen onnistuu vain ajantasaisen ja tehokkaan reagoinnin, toimivan viranomaisyhteistyön sekä oikean osaamispääoman tunnistamisen ja suuntaamisen kautta. Toisaalta tietoturvakontrollien

toimivuudella on suuri merkitys verkostoturvallisuudelle ja samalla koko tietoturvalle.

Kehittyvänä kyberosaamisen alueena kyberpuolustuksen ja -vaikuttamisen liittäminen osaksi taktisen ja operationaalisen tason sotilaallista toimintaa vaikuttaisi lähitulevaisuudessa nousevan tärkeimmäksi tekijäksi PVJJK:n toiminnassa. Tätä näkemystä puoltavat sekä yleinen muutos sodankäynnin luonteessa että PVJJK:n tuleva suoriutuminen sen keskeisten, kyberpuolustukseen ja -vaikuttamiseen liittyvien tehtävien hoitamisesta. Kybermaailman muutokset voivat osoittautua jopa ennakoituakin nopeammiksi ja kokonaisvaltaisemmiksi. Samalla niihin liittyy väistämättä myös runsaasti epävarmuustekijöitä. Tällainen kehitys voi asettaa haasteita vastata nopeasti kyberosaamisen muuttuviin vaatimuksiin, koska niitä ei välttämättä aina edes tunnisteta ja tiedosteta. Toisaalta PVJJK:n käytössä oleva laaja, siviilireservin kattava henkilöstöresurssi on merkittävä vahvuustekijä osaamispääoman kasvattamisessa nopeastikin muuttuvassa tilanteessa.

Kyberrikostorjuntakeskuksen toiminnalle luonteenomaista on sen vahva kytkös ulkoiseen ympäristöön. Organisaation ulkopuolelta hankittavissa oleva informaatio ja sen laatu määrittävät pitkälti tutkintaprosessien tuloksellisuutta. Toisaalta organisaatio voi myös itse vaikuttaa tilanteeseen tarkoituksenmukaisten yhteistyöverkostojen, poliisin yksiköiden kouluttamisen ja asiakkaiden valistamisen kautta. Eritoten kahteen ensin mainittuun panostaminen onkin nähtävä toiminnan vaikuttavuuden kannalta välttämättömänä. Kyse on sekä ennaltaehkäisystä ja tietojen jäljittämisestä että poliisin yleisistä valmiuksista kohdata kybermaailman ilmiöitä. Tätä kautta voidaan lisätä myös organisaation ja koko poliisin kapasiteettia tiedottaa ja ohjeistaa asiakkaita kybermaailman alueella. Asiakkaiden omat puutteet kybertapahtumien seurannassa ja reagoinnissa ovat silti todennäköisesti jatkossakin yksi Kyberrikostorjuntakeskuksen toiminnan haasteista.

Vaikka Kyberrikostorjuntakeskus kykenee hoitamaan pääosan teknisestä tutkinnasta itsenäisesti, niin lähitulevaisuudessa asetelma voi ainakin osittain muuttua. Tämän suuntaisesta kehityskulusta antaisi viitteitä viime aikoina supistunut käytännön teknisten osaajien hakijamäärä organisaatiossa avoimena olleisiin tehtäviin. Tästä näkökulmasta arvioituna osaamisen laajentaminen ja syventäminen oppilaitosyhteistyön, organisaation ulkopuolisen työssäoppimisen ja mahdollisten uudenlaisten yhteistyömuotojen kautta nouseekin yhä tärkeämpään rooliin valmiuksien kehittämisessä ja ylläpitämisessä.

Poliisin yksiköihin liittyvä kyberrikosten taktisten tutkintavalmiuksien osaamisvaje on tällä hetkellä suurin Kyberrikostorjuntakeskuksen sisäisistä haasteista. Kyse on myös samalla ongelmasta, joka voi merkittävästi lieventyä vain pitkän aikavälin kuluessa. Tilanteen parantaminen on pitkälti Kyberrikostorjuntakeskuksen vastuulla, mikä tarkoittaa merkittävää resurssien allokointitarvetta tälle alueelle. Asetelma näyttäytyy ilmeisen kompleksisena, sillä akuut-

ti ongelma vaatisi välittömiä toimenpiteitä jatkuvasti muuttuviin kybermaailman tilanteisiin reagoimiseksi. Tilanteen vakiintuminen sellaiseksi, jossa kaikki potentiaaliset kyberrikokset eivät etene tutkintaan poliisin oman osaamisvajeen vuoksi, merkitsisi kyberrikollisten pysyvää etumatkaa suhteessa rikosten tutkintaan. Edellisen perusteella lisäresurssien suuntaaminen organisaation toimintaan näyttäisikin vääjäämättömältä tosiasialta jo lähitulevaisuudessa.

Tutkimuksen kohdeorganisaatioiden väliset erot havainnollistuvat selkeästi niiden ydinkompetenssiesitysten painottamissa kategorioissa. Erot selittyvät sekä organisaatioiden toiminnan tarkoituksen että niiden toimintaan liittyvien muiden osapuolten merkityksen kautta. PVJJK edustaa organisaatiota, jonka toiminta edellyttää itsenäistä vastuunottoa ja kyberosaamista useamman kategorian toiminnoista, vaikka toiminnan tarkoituksesta seuraakin suojelu- ja puolustus -kategorian toimintojen hallitseva rooli sen ydinkompetenssissa. Kyberrikostorjuntakeskuksen osalta taas muiden osapuolten merkitys sen toiminnalle korostuu selvästi. Tutkinta -kategorian toiminnot nousevatkin tästä syystä organisaation itsenäisenä osa-alueena melko yksiselitteisesti sen ydinkompetenssin keskiöön.

Toisaalta kohdeorganisaatioiden ydinkompetenssiesityksissä voidaan nähdä myös samansuuntaisia piirteitä. Niissä on kyse osin vielä kehittyvistä toiminnoista, jotka liittyvät suoraan kybermaailman nopeaan ja ennakoimattomaan kehitykseen. Näin ollen myös niihin liittyvä kyberammatillinen osaaminen tehtävänkuvineen on vielä selkiintymätöntä ja määrittelemätöntä. PVJJK:ssa näitä toimintoja ovat kyberpuolustuksen koordinointi taktisen ja operationaalisen sotilaallisen aktiviteetin kanssa. Kyberrikostorjuntakeskuksen ja koko poliisin organisaation osalta taas kyse on kyberosaamisen ja taktisen tutkinnan välisestä koordinoinnista. Molempien osalta voidaan siis puhua riittävän kyberosaamisen saavuttamisesta organisaatioiden taktisen ja operationaalisen tason ydintoimintojen alueella. Lisäksi kummassakin organisaatiossa nämä alueet edustavat yhä kehittyviä ja samalla erityisen haasteellisia, lähitulevaisuudessa todennäköisesti keskeisiksi nousevia toimintoja.

Edellisen perusteella on mahdollista, että kyberammatillisen osaamisen liittäminen osaksi taktisen tason toimintoja olisi yksi kyberosaamisen keskeisistä haasteista myös muissa organisaatioissa. Vaikka ilmiö ei suoraan liity tekniseen osaamiseen, niin kyse on kuitenkin kyberteknologian ja taktisen tason yhdistämisestä siten, että edellytykset vastata myös operationaalisella tasolla kybermaailman tapahtumiin ovat olemassa. Ainoastaan kaksi organisaatiota käsittävässä tapaustutkimuksessa tätä pidemmälle meneville johtopäätöksille ei kuitenkaan ole perusteita. Aineiston niukkuus onkin nähtävä tutkimuksen selkeänä puutteena siitäkin huolimatta, että sen perusteella voidaan kohtuullisen luotettavasti arvioida kohdeorganisaatioiden kyberammatillisen osaamisen tarpeita ja siihen liittyviä ydinosa-alueita. Tästä näkökulmasta tutkimuksen reliabiliteettia voidaan pitää melko hyvänä, mikä on tyypillistä tapaustutkimuksissa.

Tässä tutkimuksessa sovelletun NCWF -viitekehyksen ja ydinkompetenssin organisaatiotasoisen näkökulman välillä vallitsee ristiriitaisuuksia. Viitekehyksen tarkoituksena on ylemmän tason sisältöalueiden lisäksi määritellä tarkemmin kyberturvallisuuden tehtäväalueita ja -sisältöjä. Ydinkompetenssi taas ilmenee koko organisaation toimintojen tasolla ja on melko vaikeasti hahmotettavaa, usein näkymätöntäkin. Näin ollen se taipuu huonosti tarkempiin tehtäväerittelyihin, jotka taas liittyvät yksilötason kompetensseihin. Tässä mielessä ydinkompetenssiesityksillä ei voida suoraan tavoittaa, määritellä ja selkeyttää yksittäisiä tehtäväsisältöjä. Toisaalta ydinkompetenssin avulla voidaan kuitenkin saada kiinni olennaisia sisältöalueita ja niihin liittyviä toimintoja, joiden tunnistaminen on edellytyksenä myös tehtäväkohtaisille määrittelyille. Tässä tehtävässä se voikin toimia varsin havainnollisena välineenä myös kyberturvallisuuden alueella.

Kyberammatillista osaamista julkisen sektorin organisaatioissa on toistaiseksi tutkittu varsin niukasti. Kyberosaamista laajemmin luotaavalle tutkimukselle ajankohtaisella ja alati kehittyvällä kyberalueella löytyisikin yhä enemmän sijaa. Kyberosaamisen vaatimuksia olisi myös syytä tutkia laajemmassa joukossa eri tyyppisiä organisaatioita. Toisaalta myös syvemmän ymmärryksen saavuttamiselle yksittäisistä kohteista olisi selvästi tarvetta. Kyse olisi tällöin laajemman aineiston keräämisestä yksittäisestä tutkimusentiteetistä. Tämän tutkimuksen perusteella yksi kiinnostava tutkimusalue liittyy kyberammatillisen osaamisen ja taktisen tason toimintojen yhdistämiseen organisaation ydintoimintoja operationaalisella tasolla palvelevaksi kokonaisuudeksi.

Tapaustutkimuksen laadullinen lähestymistapa palvelisi kaikkia edellä mainittuja pyrkimyksiä todennäköisesti varsin tehokkaasti. Toisaalta sen kautta olisi myös mahdollista muodostaa perusteltuja hypoteeseja, joita voidaan testata kvantitatiivisilla menetelmillä. Tämä mahdollistaisi laajempien aineistojen käytön ja sitä kautta tutkimustulosten nostamisen yleisemmälle tasolle. Yleistäminen vaikuttaisi kiistatta positiivisesti kyberalan pitkän aikavälin koulutussuunnitteluun. Tässä yhteydessä voidaan puhua ennen kaikkea koulutuksen sisällöllisestä kehittämisestä enemmän todellisia tarpeita palvelevaksi. Lopulta tällä olisi vaikutusta myös organisaatioiden toiminnan suuntaamisen edellytyksiin, mikä tarkoittaa kyberammatillisen osaamisen liittämistä yhdeksi sen luonnolliseksi osaksi.

# LÄHTEET


Benbasat, I., Goldstein, D.K. & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly, Vol. 11, No.3 (Sep 1987),* pp. 369 - 386.

Burley, D.L., Eisenberg, J. & Goodman, S.E. (2014). Would Cybersecurity Professionalization Help Address the Cybersecurity Crisis? *Communications of the ACM, February 2014, Vol. 57, No. 2.*

Chen, H. M. & Chang, Y. C. (2010). The Essence of the Competence Concept: Adopting an Organization's Sustained Competitive Advantage Viewpoint. *Journal of Management & Organization, (2010) 16:* 677 - 699.

Chen, H. M. & Chang, W. Y. (2011). Core Competence: From a Strategic Human Resource Management Perspective. *African Journal of Business Management 5, 14,* 5738 – 5745.

Cybersecurity Workforce Competencies: *Preparing Tomorrow's Risk-Ready P r o-fessionals*. (2014). University of Phoenix. (ISC) Foundation.

Doherty, N. & Fulfor, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, Vol. 18 (4),* pp. 21 - 39.

Fourie, L., Hettema, H. & Watters, P. (2014). *The Global Cyber Security Workforce an Ongoing Human Capital Crisis.* The Global Business and Technology Association.

Furnell, S., Fischer, P. & Finch, A. (2017). Can't Get the Staff? The Growing Need for Cyber-security Skills. *Computer Fraud & Security, Vol. 2017, Issue 2,* 5 – 10.

Goddard, J. (1997). The Architecture of Core Competence. *Business Strategy Review, Vol. 8, No. 1,* 43 - 52.

Goodman, S. E. (2014). Building the Nation's Cyber Security Workforce: Contributions from the CAE Colleges and Universities. *ACM Transactions on Management Information Systems, Vol. 5, No.2, July 2014.*

Hirsjärvi, S. & Hurme, H. (2015). *Tutkimushaastattelu - Teemahaastattelun teoria ja käytäntö*: e-kirja Gaudeamus.

Hoffman, L. J., Burley, D. L. & Toregas, C. (2012). Holistically Building the Cybersecurity Workforce. *IEEE Security & Privacy, March - April 2012, Vol. 10 (2),* pp. 33 - 39.

Holmes, G & Hooper, N. (2000). Core Competence and Education. *Higher Education, Vol. 40, (3),* pp. 247 – 258.

Karyda, M., Kiountouzis, E. & Kokolakis, S. (2004). Information Systems Security Policies: a Contextual Perspective. *Computer & Security (2005) 24,* 246 - 260.

Kayworth, T & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive, Vol. 9, No. 3.*

Klimoski, R. (2016). Critical Success Factors for Cybersecurity Leaders: Not Just Technical Competence. *People and Strategy, 39.1,* 14 – 18.

Knapp, K. J., Morris Jr., R. F., Marshall, T. E. & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computer & Security (2009), Vol. 28 (7)*, pp. 493 - 508.

Metsämuuronen, J. (2011). *Tutkimuksen tekemisen perusteet ihmistieteissä: e-kirja opiskelijalaitos.* Helsinki: International Methelp, Booky.fi 2011.

NRC. 2013). *Professionalizing the Nation's Cybersecurity Workworce? Criteria for Decision-Making.* National Research Council, Computer Science and Telecommunications Board, The National Academies Press, Washington, D.C.

Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Salonen, J., Savola, R., Savolainen, P., Suominen, A., Toivanen, H., Kyheröinen, J. & Remes, J. (2015) *Kyberosaaminen Suomessa - Nykytila ja tiekartta tulevaisuuteen.* Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2015.

Prahalad, C.K. & Hamel, G. (1990). The Core Competence of the Corporation. *Harward Business Review,* May-June 1990.

Radunovic, V. & Rüfenacht, D. (2016). C*ybersecurity Competence Building Trends.* Research report. Commissioned by the Federal Department of Foreign Affairs of Switzerland. DiploFoundation.

Reece, R.P. & Stahl, B.C. (2015). The Professionalisation of Information Security: Perspectives of UK Practioners. *Computer & Security, Vol. 48, February 2015,* 182 – 195.

Saaranen-Kauppinen, A. & Puusniekka, A. (2006.) KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. Haettu 24.4.2017 osoitteesta http://www.fsd.uta.fi/menetelmaopetus/.

Senior Cyber Leadership: Why a Technically Competent Cyber Workforce Is Not Enough. (2013). The Cybersecurity Forum Initiative. Haettu 24.4.2017 osoitteesta *www.csfi.us/pubdocs/?id=39*.

Skorkova, S. (2016). Competency Models in Public Sector. *Procedia – Social and Behavioral Sciences, Vol. 230, September 2016,* pp. 226 – 234.

Spears, J.L. & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, Vol. 34, No. 3,* pp. 503 - 522.

Spidalieri, F. & Kern, S. (2014). *Professionalizing Cybersecurity: A path to universal standards and status.* Salve Regina University. Pell Center for International Relations and Public Policy, August 2014.

The National Cybersecurity Workforce Framework. (2013). *National Initiative for Cybersecurity Education.* Haettu 24.4.2017 osoitteesta http://csrc.nist.gov/nice/framework/.

Tuomi, J. & Sarajärvi, A. (2009). *Laadullisen tutkimuksen sisällönanalyysi.* Helsinki: Tammi.

Ulrich, D. (1991). Competing from the Inside Out. *Executive Excellence, Jun 1991, Vol. 8 (6),* p. 9.

Vogel, R. (2016). Closing the Cybersecurity Skills Gap. *Salus Journal, Vol.4, No. 2, 2016.*

Wilson, A. & Wilson, C. (2011). The Effects of U.S. Government Security Regulations on the Cybersecurity Professional. *Proceedings of Academy of Legal, Ethical*