Opinnäytetyö (YAMK)

Teknologiaosaamisen johtaminen

2021

Juha Porkka

# KYBEROSAAMISEN KARTOITTAMINEN KUNNOSSAPITO-ORGANISAATIOSSA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (YAMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Teknologiaosaamisen johtaminen

2021 | 61 sivua, 3 liitesivua

Juha Porkka

# KYBEROSAAMISEN KARTOITTAMINEN KUNNOSSAPITO-ORGANISAATIOSSA

Digitalisaatio ja erilaisten tietoteknisten järjestelmien huima kehittyminen pakottaa yritykset ja julkisen hallinnon organisaatot tilanteeseen, jossa niiden on pakko ottaa kyberturvallisuus ja kybersietoisuus huomioon oman toiminnan suunnittelussa niin henkilöstön kuin tietoteknisten järjestelmien osalta. Tämän opinnäytetyön tavoitteena oli kartoittaa suomalaisen elinjakson hallinnan palveluita tuottavan yrityksen kunnossapitoinsinöörien kyberosaaminen kolmella eri toimipisteellä, jotka sijaitsivat eri puolilla Suomea. Osaamiskartoituksen keskeisin teema oli keskittyä järjestelmien kunnossapitoinsinööreillä olevaan osaamiseen kybersietoisuuden näkökulmasta.

Opinnäytetyön teoreettinen viitekehys pohjautui yhteiskunnan kriittisten toimintojen ja toimialojen kyberturvallisuuden sekä kybersietoisuuden kehittämiselle. Lisäksi mukaan otettiin ihmisten ammatillisen ja muun osaamisen kehittymistä ja keinoja osaamisen kehittämiseksi. Toimeksiannon osaamisvaatimusten pohjana toimiva kansallinen auditointikriteeristö (Katakri) ja sieltä valitut kunnossapidon osaamisvaatimukset olivat myös tärkeä osa tämän opinnäytetyön teoreettista viitekehystä.

Opinnäytetyön tutkimusosuus suoritettiin käyttäen puolistrukturoitua haastattelua, joka tutkimusmenetelmänä kuuluu kvalitatiivisiin menetelmiin. Kolmelta paikkakunnalta haastateltiin yhteensä kuuttatoista erilaisten teknisten järjestelmien kunnossapidosta vastaavaa järjestelmäinsinööriä. Työn tuloksena saatiin kartoitettua ja dokumentoitua kaikkien kolmen toimipisteen kyberosaaminen osaamismatriisiin. Lisäksi onnistuttiin paikantamaan ydinosaamisen sijainti ja saamaan selkeä kuva henkilöstön koulutustarpeista ja tarpeellisen koulutuksen sisällöstä. Osaamiskartoituksen lisäksi tutkimuksen tuloksena kirjattiin organisaatiota koskevia kybersietoisuuden kehitysehdotuksia.

ASIASANAT:

kunnossapito, kyberturvallisuus, kybertoimintaympäristö, osaaminen

MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Technology Competence Management

2021 | 61 pages, 3 pages in appendices

Juha Porkka

# CYBER COMPETECE ANALYSIS IN A MAINTENANCE ORGANIZATION

The digitalization and dramatic technological development of information technology systems are forcing companies and the public sector to the situation where they must take cybersecurity and cyber resilience into account in general as well as when developing technical systems and human resources. The present Master´s thesis discusses the cybersecurity competences of maintenance engineers working for a Finnish company that offers life cycle management services for its clients. These engineers were working in three different locations around Finland. The main theme of this competence study was to focus on cyber resilience competences of system maintenance engineers.

The theoretical framework of the study is based on the development of cyber security and cyber resilience in the critical functions and industries of the society. In addition, the development of people's professional and other skills is discussed. The national audit criteria (Katakri), which serve as the basis for the competence requirements of the study and the maintenance competence requirements selected therefrom, are also an important part of the theoretical framework of this Master´s thesis.

A semi-structured interview, which is a research method belonging to the qualitative methods, was used in the research part of the study. In total, sixteen system engineers responsible for the maintenance of various technical systems from three different locations were interviewed. The cyber competence of all three locations was mapped and documented on the competence matrix as a result of the study. The core competences and a clear picture of the training needs and necessary content were analysed according to the location and documented. The development proposals for the cyber resilience actions of a maintenance organization were also recorded.

KEYWORDS:

maintenance, cybersecurity, cyberspace, competence

# SISÄLTÖ

# LIITTEET



# KUVAT



# KUVIOT



# TAULUKOT

# KÄYTETYT LYHENTEET

| | |
|---|---|
| WEF | World Economic Forum, Maailman talousfoorumi |
| IT | Information Technology, Informaatioteknologia |
| CIS | The Center for Internet Security, Tietoturvallisuuskeskus |
| OSINT | Open Source Intelligence, Avoimien lähteiden tiedustelu |
| POC | Point Of Contact, Yhteyshenkilö |

# 1 JOHDANTO

Tämän opinnäytetyön toimeksiantaja on suomalainen teknisen elinjakson hallintapalveluita tuottava yritys. Yrityksen liiketoiminnan pohjana ovat pitkäaikaiset kumppanuussuhteet erilaisilla toimialoilta toimivien yritysten ja organisaatioiden kanssa. Yritys toimii yhteiskunnallisesti merkittävässä tehtävässä niin normaali- kuin poikkeusoloissa, tuottaen teknisen kaluston ja erilaisten järjestelmien kokonaisvaltaisia huolto- ja kunnossapitotoimia niin Suomessa kuin asiakkaiden kansainvälisissä operaatioissa ja harjoituksissa.

Yritys on panostanut voimakkaasti kehittyäkseen entistä monipuolisemmaksi huolto- ja kunnossapidon kokonaisosaajaksi nyt ja tulevaisuudessa. Digitalisaatio, kyberturvallisuus, ilmastoriskit, kuljetuslogistiikan suurhäiriöt ja esimerkiksi pandemiat ovat ottaneet entistä suurempaa roolia tulevaisuuden visioissa. Myös globaalin turvallisuustilanteen epävarmuus ja muutokset tuovat mukanaan tarpeen kehittää yrityksen toimintaa. Lisäksi suurimman kumppanin yhteiskunnallisestikin merkittävät hankkeet tuovat yritykselle töitä hankintavaiheiden tuen ja hankkeiden elinjaksosuunnittelun muodossa. Osana yrityksen strategiaa on myös kasvaa jatkuvasti ja luoda uusia kumppanuussuhteita uusien asiakkaiden kanssa. Samalla yritys panostaa osaamisen monipuolistamiseen erilaisilta toimialoilta, joka tukee sen itselleen asettamaa kasvustrategiaa.

## 1.1 Työn taustaa

Asiakkaan uudet mittavat hankkeet tuovat yritykselle monia uusia liiketoimintamahdollisuuksia ja haasteita. Uudet järjestelmät ja niiden korkea integraatio- ja teknologiataso tuovat tarpeen luoda uusia palveluita asiakastarpeiden tyydyttämiseksi. Uusien palveluiden, sekä palvelutuotteiden suunnittelu ja tulevaisuuden toteuttaminen, tulevat olemaan iso osa yrityksen toimintaa tulevaisuudessa.

Järjestelmien ja toimialojen integroituessa enemmän yhdeksi kokonaisuudeksi, tulee palveluita, kompetensseja, prosesseja ja toimintamalleja miettiä aivan uudella tavalla. Nykyisten toimintamallien sovittaminen uusien palveluiden vaatimuksiin tuottaa haasteita, koska ne ovat rakentuneet vanhempien järjestelmien tarpeisiin. Nykyiset toimintamallit ja -tavat eivät välttämättä tue uusien palveluiden tehokasta tuotantoa.

Vanhassa mallissa toiminta on keskitetty pääosin yhden toimialan alle linjaorganisaatiomallin mukaisesti. Järjestelmien digitalisoituminen mahdollistaa uudenlaiset tavat toteuttaa palvelutoimintaa riippumatta toimipaikan sijainnista. Näin ollen eri toimipaikoilla olevien kompetenssien hyödyntäminen tulee vieläkin tärkeämmäksi kuin ennen, jotta uudet palvelut saadaan tuotettua asiakkaalle mahdollisimman järkevästi ja tehokkaasti turvallisuusaspektit huomioiden.

Digitalisoituminen, etäyhteyksien lisääntyminen ja näihin kohdistuvat uhat tuovat myös kyberturvallisuuden ja kybersietoisuuden aspektit entistä suuremassa määrin huolto- ja kunnossapitotoiminnan keskiöön kaikilla yrityksen toimialoilla ja toimipaikoilla. Globalisaatio sekä järjestelmien digitalisoituminen muuttavat toimintaympäristöä jatkuvasti. Turvallisuus- ja toimintaympäristön muuttuessa kansallisen turvallisuuden uhkatekijät, kuten vakoilu ja terrorismiin liittyvät hankkeet ja ilmiöt siirtyvät enenemissä määrin tietoverkkoihin. (Nadja Nevaste, Rauli Paananen, Pentti Olin, Tuija Kuusisto, Kimmo Rousku 2017, 6.)

Toimeksiantajan maanttieteellisesti hajautetun organisaation kannalta on tärkeää suunnitella ja ymmärtää, mikä tulee olemaan minkäkin toimipisteen rooli tulevaisuuden digitaalisessa palvelutuotannossa, jotta esimerkiksi matriisiorganisaatiomallia pystyttäisiin hyödyntämään mahdollisimman tehokkaasti. Tulevien palveluiden kannalta toiminnan tulee olla yhdenmukaista toimialasta ja toimipaikasta riippumatta. Tähän tavoitteeseen päästään, kun tiedostetaan yrityksen osaaminen kokonaisvaltaisesti. Kun kunkin toimipaikan osaaminen tunnetaan, voidaan toimintamallit, prosessit ja käytännön työ suunnitella tehokkaasti tuotettaviksi.

## 1.2 Tutkimusmenetelmät

Opinnäytetyön tutkimusotteeksi valikoitui laadullinen tutkimusote sen monikäyttöisyyden takia. Kvalitatiivinen tutkimusote sisältää monenlaisia tapoja hankkia, analysoida ja tulkita erilaisia aineistoja. Opinnäytetyön tutkimus tehtiin aineistolähtöisesti, sillä teorialähtöinen tutkimus olisi vaatinut pohjakseen teorian tai mallin. (Anita Saarinen-Kauppinen & Anna Puusniekka 2009, 6-7.)

Sopivimmaksi aineistonkeruumenetelmäksi tähän opinnäytetyöhön valikoitui haastattelu. Haastattelu on yleisimpiä tiedonkeruutapoja, joita näemme esimerkiksi jokapäiväi-

sessä journalismissa lehtien sivuilla erilaisien haastattelututkimuksien muodossa. Haastattelussa osapuolet keskustelevat enemmän tai vähemmän järjestelmällisesti tutkimusaiheesta. Haastattelulla on sen mahdollisesta avoimuudesta riippumatta kuitenkin selkeä päämäärä, jolla pyritään saamaan vastaus tutkimustehtävään. (Hirsjärvi & Hurme 2001, 34,42)

Erilaisia haastattelutapoja- ja tyyppejä on useita. Yksi yleisemmistä tavoista luokitella haastattelu perustuu sen jäsentelyyn ja kiinteyteen. Käytännössä tämä tarkoittaa haastateltavan liikkumatilaa haastattelun aikana ja kuinka tarkkoja esitetyt kysymykset ovat. Haastattelutavoista puolistrukturoitu haastattelu antoi parhaat lähtökohdat tämän opinnäytetyön tutkimusosan toteuttamiselle. Puolistrukturoitu haastattelu toteutetaan ennalta suunniteltujen kysymysten pohjalta siten, että kaikille haastateltaville esitetään samat kysymykset. Kysymysten esittämisjärjestyksellä ei puolistrukturoidussa haastattelussa ole merkitystä. Puolistrukturoidussa haastattelussa on kuitenkin selkeä rakenne sekä aihepiirit ja teemat ovat kaikille haastateltaville samoja. (Hirsjärvi & Hurme 2001, 47-48, 66; Eskola & Suoranta 2000, 86-87.)

Puolistrukturiotu haastattelu perustuu keskustelunomaiseen tilanteeseen, jossa kysymykset ja teemat ovat ennalta suunniteltuja. Puhumis- ja kysymysjärjestys sekä käsiteltävien asioiden laajuus ovat kysymysten osalta vapaita. Haastattelija tekee haastatteluista lyhyitä muistiinpanoja, jotta voi keskittyä haastatteluun sen dokumentoinnin sijaan. Haastattelussa läpi käytävät teemat voidaan listata. Haastatteluun voidaan myös tarpeen mukaan lisätä täydennykseksi alateemoja ja avainsanoja. Puolistrukturoitu haastattelu muistuttaa teemahaastattelua ja edellyttää syvällistä perehtymistä tutkittavaan aihepiiriin. Haastateltavien tilanne on myös tunnettava hyvin, jotta haastattelu voidaan kohdentaa oikeisiin teemoihin. Kysymysten sekä haastateltavien valinta on tärkeää, jotta tutkittavasta asiasta saadaan paras mahdollinen aineisto. Tutkimukseen ei siis kannata valita henkilöitä sattumanvaraisesti. (Anita Saarinen-Kauppinen & Anna Puusniekka 2009, 55-57.)

## 1.3 Tutkimuksen tavoitteet ja rajaukset

Opinnäytetyön tavoitteina oli kartoittaa yrityksen toimipisteillä työskentelevien kunnossapitoinsinöörien kyberosaaminen kokonaisvaltaisesti, osaamisen dokumentointi kybersietoisuuden näkökulmasta sekä kunnossapidon kybersietoisuuden toteutuminen käytännössä. Työn tuloksien analysoinnilla tavoiteltiin myös kokonaisnäkemystä siitä,

millaista osaamista yrityksen tulee mahdollisesti hankkia tulevaisuudessa, jotta loppuasiakkaalle voidaan toteuttaa ja tuottaa uusia palveluita turvallisesti ja suunnitellusti.

Osaamista tavoiteltiin tarkasteltavan eritoten kunnossapidon kybersietoisuuden näkökulmasta yrityksen toimipaikkojen välillä. Kun yrityksen osaaminen suhteessa vaatimuksiin saatiin selvitettyä kokonaisvaltaisesti, pystytään tulevaisuudessa toteuttamaan kustannustehokkaat ja yhdenmukaiset toimintamallit kunnossapidon kybersietoisuuden osalta.

Tutkimuksen päätavoite oli löytää vastaus tutkimuskysymykseen, joka vastaa opinnäytetyön tutkimusongelmaan:

- Mikä on kunnossapito-organisaatiossa työskentelevien järjestelmien kunnossapitoinsinöörien kyberosaamisen nykytila kybersietoisuuden näkökulmasta?

Tarkentavilla alakysymyksillä selvitettiin osaamista tarkemmin sekä saatiin kuva, miten osaaminen jakautui eri toimialojen ja toimipaikkojen kesken. Alakysymysten avulla saatiin laajennettua osaamiskartoitus koskemaan myös toimintamalleja. Tuloksia voidaan hyödyntää toimintamallien yhtenäistämisessä toimipaikoittain.

- Miten kyberosaaminen jakautuu toimipaikkojen välillä?
- Miten osaamiskartoitusta pystytään hyödyntämään tulevaisuudessa?
- Mitä osaamista tarvitaan tulevaisuudessa, jotta asiakasvaatimukset täyttyvät?

**Rajaukset**

Tämän opinnäytetyön tavoitteena oli tutkia ja tuottaa tulevaisuuden johtamisjärjestelmien ja kyberpalveluiden palvelutuotteiden suunnittelua ja käytännön toteuttamista. Uusien toimintamallien suunnittelu, sekä prosessien kuvaaminen siten, että koko organisaation osaaminen saataisiin hyödynnettyä mahdollisimman tehokkaasti rajattiin kuitenkin kokonaisuudesta pois. Tämä olisi ollut liian laaja kokonaisuus.

Toimeksianto rajattiin koskemaan kunnossapito-organisaatiossa työskentelevien järjestelmäinsinöörien kyberosaamisen kartoitusta kybersietoisuuden osalta. Osaamista tarkasteltiin toimialoittain ja toimipaikoittain, jotta osaamisen kokonaiskuvasta saatiin mahdollisimman selkeä.

Osaamiskartoitus antoi itsessään hyvän pohjan toteuttaa toimeksiannon alkuperäistä agendaa, koska sen pohjalta voitiin suunnitella osaamisen kehittämistä ja aloittaa koulutukset suunnitelman mukaisesti. Kun toimipaikkojen osaaminen saatiin selvitettyä, auttaa se osaltaan luomaan toimintamallit ja prosessit parhaan osaamisen ympärille. Näin ollen tulevaisuudessa toteutettavia palvelutuotteita pystytään todennäköisesti tuottamaan helpommin, kun organisaatiolla on selkeät toimintamallit ja tekemistä ohjaavat prosessit.

# 2 KYBERTURVALLISUUS

Suomen kyberturvallisuusstrategiassa mainitaan kyberturvallisuuden olevan tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuudesta huolehtiminen yhteiskunnan elintärkeiden toimintojen osalta on pystyttävä turvaamaan sekä normaali-, että poikkeusoloissa. Yhteiskunta on hyvin riippuvainen tietoverkkojen ja -järjestelmien toiminnasta. Esimerkiksi huhtikuussa 2020 teleoperaattori Telian verkossa havaittiin valtakunnallinen vika, joka lueteltiin A-luokan häiriöksi. A-luokan häiriöksi luetaan sellainen häiriö, joka vaikuttaa esimerkiksi vähintään 200 000 henkilön internetyhteyksien toimintaan. Operaattorin kiinteät sekä langattomat datayhteydet olivat poikki tai pätkivät osalla asiakkaista ympäri Suomea. Telian laiteviasta johtunut verkko-ongelma oli hyvä osoitus siitä, miten haavoittuvaisia olemme yhteyksiin kohdistuville häiriöille ja häirinnälle. (Suomen kyberturvallisuusstrategia 2013, 1-2., Härkönen HS,STT)

Koska tietoverkot, järjestelmät ja niissä liikkuva sähköinen tieto elävät vahvassa keskinäisriippuvuussuhteessa, on tätä moninaista sähköisen tiedon käsittelyyn tarkoitettua ympäristöä alettu kutsumaan kybertoimintaympäristöksi niin kotimaassa kuin kansainvälisestikin. Lisääntyvä tietointensiivisyys, kasvava ulkomainen omistus ja palveluiden ulkoistaminen, laitteistojen- ja järjestelmien keskinäinen integraatio, täysin avointen tietoverkkojen käyttö sekä sähköriippuvuus ovat tuoneet uusia vaatimuksia yhteiskunnan elintärkeiden toimintojen turvaamiseksi niin normaali, kuin poikkeusoloissa. Uhkien vaikutukset kybertoimintaympäristöön ovat muuttuneet ihmisten, yritysten sekä yhteiskunnan kannalta aiempaa vaarallisimmiksi. Nykyään kyberuhkia muodostavat toimijat ovat entistä ammattimaisempia ja joukkoon voidaan laskea myös valtiolliset toimijat. Kybertoimintaympäristöön voidaan toteuttaa perinteisiä hyökkäyksiä sotilaallisten voimakeinojen ohella vakavissa kriiseissä, mutta niitä voidaan käyttää myös taloudellisen ja poliittisen vaikuttamisen välineinä. (Suomen kyberturvallisuusstrategia 2013, 1-2.)

Kybertoimintaympäristöä ei tulisi nähdä pelkästään uhkana ja hyökkäyskohteena. Kybertoimintaympäristön kasvaessa, se luo myös uusia mahdollisuuksia ja voimavaroja sekä liiketoimintamahdollisuuksia yrityksille. Kun toimintaympäristön turvallisuuteen kiinnitetään erityistä huomiota, on yritysten toiminta ja toiminnan suunnittelu helpompaa. Turvallinen kybertoimintaympäristö on yrityksille myös erityisen hyvää mainosta kansallisilla ja kansainvälisilläkin kentillä. (Suomen kyberturvallisuusstrategia 2013, 1-2)


Kuvio 1. Suomen kyberturvallisuuden visio (Suomen kyberturvallisuusstrategia 2013, 3.)

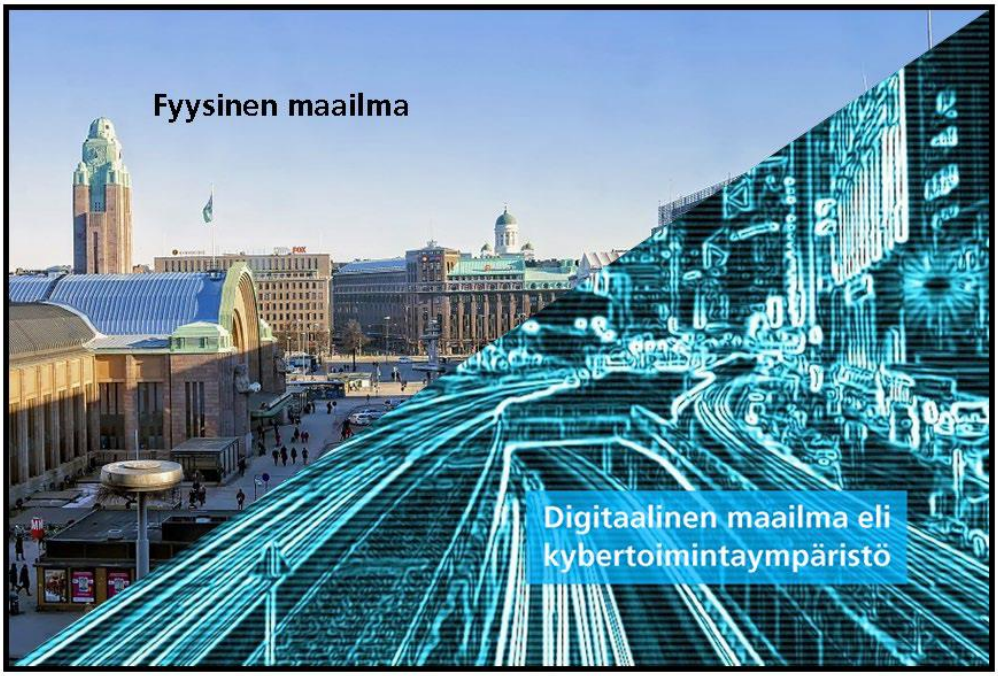
Keskeinen kyberturvallisuuden visioiden sisältö on kyberuhkilta suojautuminen kaikissa mahdollisissa tilanteissa osaavan henkilöstön ja kansainvälisen yhteistyön avulla. Kyberturvallisuusvisioissa määritellään myös tulevaisuuden kehityssuunnat ja tavoitteet, joiden mukaan organisaatio etenee kohti asetettuja tavoitteita. Monet yhteisöt, yritykset ja maat ovat alkaneet laatia omia kyberturvallisuuden visioita ja ekosysteemejä kybertoimintaympäristöjensä ympärille, josta esimerkkinä kuvio 1 Suomen kyberturvallisuuden visiosta. (Suomen kyberturvallisuusstrategia 2013, 3.; Allied ICT Finland 2019)

Maailman talousfoorumi on kartoittanut vuonna 2018 digitalisaation kehityskulun muokkaavan työmarkkinoita huomattavasti. WEF julkaisi myös 2019 Global Risks Report raportin, jossa listattiin vaikuttavuuden ja todennäköisyyksien osalta 10 suurinta uhkaa. Listalla viidenneksi todennäköisimmäksi sijoittui laaja-alainen kyberhyökkäys, sama uhka oli vaikuttavuuden listalla seitsemäs. Tämä kuvaa hyvin, miten digitalisoituva maailma tuo uutena suuntauksena myös kyberriskien lisääntymisen, joka johtaa myös riskien merkityksen kasvuun. Forbes on arvioinut kyberturvallisuuteen liittyvien tuotteiden ja pal-

veluiden arvon olleen vuonna 2018 yli 114 miljardia dollaria, jossa kasvua edellisvuodesta oli 12,4%. Vuonna 2020 arvon ennustettiin olevan jopa 170 miljardia dollaria. (Allied ICT Finland 2019)

## 2.1 Kybertoimintaympäristö

Kybertoimintaympäristö, jota havainnollistetaan kuvassa 1, rakentuu maailmanlaajuisesta informaatioverkostosta. Tähän monimutkaiseen ja -kerrokselliseen verkkoon kuuluvat turvallisuusviranomaisen, yritysmaailman ja julkishallinnon kommunikaatioverkkoja sekä erilaisia valvonta- ja ohjausjärjestelmiä, jotka ovat osa kriittistä infrastruktuuria ja teollisuutta. Kybertoimintaympäristön tunnusomaisia piirteitä ovat elektroniikan sekä radiotaajuuksien käyttö, kun digitaalista informaatiota varastoidaan, siirretään tai muokataan tietoverkkoja käyttäen.

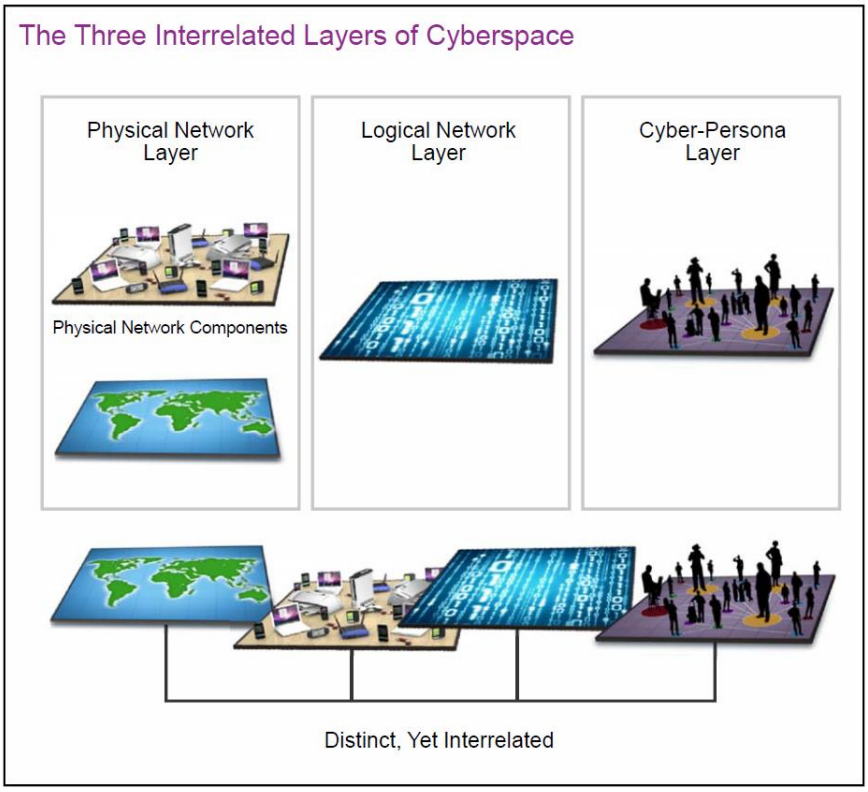



Kuva 1. Havainnekuva kybertoimintaympäristöstä (Laari ym. 2019, 11.)

Puolustusvoimien kyberpuolustuskäsikirja käsittelee käytännöllisinä esimerkkeinä kybertoimintaympäristöiksi esimerkiksi tietojärjestelmiin perustuvia ydinvoimaloiden ohjausjärjestelmiä, pankki- ja maksujärjestelmiä, elintarvikkeiden kuljetus- ja logistiikkajärjestelmiä sekä liikenteen ohjausjärjestelmiä. Kybertoimintaympäristö ei myöskään rajoitu

pelkästään valtiollisiin toimijoihin, vaan mukaan sulautuu myös kaikki ihmisten käyttämä sähköinen asiointi. Sähköiseksi asioinniksi lukeutuvat esimerkiksi sosiaalinen media, sähköiset varaus- ja musiikkipalvelut sekä puhelut. (Laari ym. 2019, 9-10.)

Yksittäiselle ihmiselle kybertoimintaympäristö näyttäytyy yleisesti vain internet-yhteytenä tai sosiaalisen median kanavana riippuen henkilön omasta osaamisesta. Kybertoimintaympäristö ulottuu kuitenkin lähes kaikkialle käsittäen internetin, tietoverkot, erilaiset järjestelmät ja niihin liittyvät oheislaitteet sekä datan ja tietoympäristön käyttäjät. Ilman edellä mainittua infrastruktuuria ja käyttäjiä, kybertoimintaympäristöllä ei ole toiminta-edellytyksiä. Toimiva kybertoimintaympäristö mahdollistaa maailmanlaajuisen tiedonvaihdon, joka vaikuttaa kaikkiin elämän osa-alueisiin maailmanlaajuisesti. Kybertoimintaympäristöä voidaan kuvata käyttämällä kolmea toisiinsa liittyvää kerrosta. Kybertoimintaympäristö koostuu fyysisestä-, loogisesta sekä käyttäjäkerroksesta kuvion 3 mukaisesti. (Cyberspace Operations, Joint Publication 3-12 2018, 22)




Kuvio 2. Kybertoimintaympäristön kerrokset (Cyberspace Operations, Joint Publication 3-12 2018, 23)

Kybertoimintaympäristön fyysinen kerros koostuu laitteista ja infrastruktuurista, joihin säilötään dataa ja jotka kuljettavat sekä prosessoivat tätä dataa verkon fyysisten komponenttien välillä. Fyysinen kerros sisältää nimensä mukaisesti fyysisiä laitteita kuten verkkoon liitetyt tietokoneet, tallennusmediat, verkkokaapelit, sekä -kytkimet ja langattomat linkit. (Cyberspace Operations, Joint Publication 3-12 2018, 22)

Looginen kerros koostuu niistä kybertoimintaympäristön osista, jotka eivät ole fyysisiä laitteita. Tällaisia osia ovat esimerkiksi erilaiset ohjelmistot ja ohjelmakoodit, jotka ohjaavat fyysisen verkon komponentteja. Nämä loogisen kerroksen osat eivät ole riippuvaisia linkin tai solmun fyysisestä sijainnista, vaan niitä voidaan suorittaa hajautetusti monessa paikassa. Uudenlaiset pilvipalvelut ovat hyvä esimerkki loogisen kerroksen toiminnasta, sillä käyttäjä ei välttämättä tiedä missä fyysisen kerroksen laitteet sijaitsevat. Solmu puolestaan edustaa verkkoon kytkettyä fyysistä laitetta, joka voi olla esimerkiksi kannettava tietokone tai muu mobiililaite. Erilaiset verkkoasetukset, tietoliikenneprotokollat sekä tietoturvaan liittyvät asetukset ohjaavat solmun toimintaa fyysisen kerroksen kanssa. (Cyberspace Operations, Joint Publication 3-12 2018, 23)

Kybertoimintaympäristön käyttäjäkerroksessa toimivat sitä käyttävät ihmiset ja persoonat. Käyttäjäkerrosta hallitaan verkon- ja IT-ohjelmistojen käyttäjätunnuksien välityksellä joko manuaalisesti tai automatisoiduin prosessein. Yksi fyysinen henkilö voi luoda ja ylläpitää useita persoonia kybertoimintaympäristössä. Henkilöllä voi olla esimerkiksi erillinen työ- ja henkilökohtainen sähköpostitili. Lisäksi henkilö voi omata erilaisia identiteettejä eri web-foorumeilla, chat-huoneissa ja sosiaalisen median palveluissa. Sama malli toimii myös kääntäen, jolloin monella fyysisellä henkilöllä voi olla pääsy yksittäiseen sähköpostiin tai sosiaalisen median palveluun. Kybertoimintaympäristön kannalta käyttäjäkerros ja fyysinen henkilö muodostavat edelleen suurimman uhan. (Cyberspace Operations, Joint Publication 3-12 2018, 24)

## 2.2 Kyberuhka

Uusinta teknologiaa otetaan jatkuvasti käyttöön yhteiskunnan eri osa-alueiden toiminnoissa. Samalla digitalisoitumisen nouseva trendi luo siitä riippuvaisille toimijoille uusia uhkia, sillä suuri osa käyttämistämme digitaalisista laitteista ja palveluista sisältää haavoittuvuuksia kyberturvallisuuden näkökulmasta (Laari ym. 2019, 28.). Vuonna 2017 merkittävimmiksi kyberuhiksi luetellaan Suomen kyberturvallisuusselvityksen mukaan

erilaisten kiristyshaittaohjelmien määrän kasvu, ohjelmistojen ja laitteistojen haavoittuvuuksien hyödyntäminen, sekä liiketoiminnan tuhoamiseen tai henkilötietojen varastamiseen liittyvät uhat. Myös erilaiset tietojen kalasteluyritykset ja huijaukset, kohdennetut hyökkäykset sekä palvelunestohyökkäykset ovat ajankohtaisia uhkia. Kyberturvallisuusselvitys kertoo myös, että yhteiskunnalle kriittisimmät toimialat ovat yleisimmin kyberhyökkäyksen kohteena. Tällaisia toimialoja ovat esimerkiksi logistiikka, julkishallinto, pankki- ja rahoitusalat, terveydenhuoltotoimiala sekä valmistus ja tuotanto. Edellisen perusteella kyberuhka voidaan siis määritellä uhaksi, joka kohdistuu teknologian tai käyttäjien kautta järjestelmiin tai ihmisiin. Kyberuhkien kohteeksi arvellaan joutuvan tulevaisuudessa entistä enemmän niin yrityksiä, organisaatioita kuin yksityishenkilöitäkin ja uhan arvellaan kasvavan käsi kädessä teknologian käytön lisääntymisen sekä digitalisoitumisen myötä. (Nevaste ym.  2017, 4)

Kyberuhan toteutuessa, voidaan sillä tuottaa merkittäviä häiriöitä tai mahdollisesti jopa lamauttaa kriittistä infrastruktuuria tai sen osia ja yhteiskunnan toiminnan kannalta elintärkeitä toimintoja. Kyberhyökkäyksen vakavuusastetta voidaan pitää merkittävänä, sillä esimerkiksi suurvallat pitävät kyberhyökkäystä sotilaallisena toimena, johon voidaan vastata kaikin mahdollisin keinoin. Suurvallat ovat toistaiseksi kuitenkin pidättäytyneet voimankäytöstä, sillä niitä vastaan kohdennetut kybertoimet on tulkittu pehmeiksi toimiksi. Tämän vuoksi sotilaallisen voiman käyttökynnyksen on arveltu olevan matalampi kuin jos kyseessä olisi ollut perinteinen sotilasoperaatio. Kyberaktivismin, -vakoilun ja -rikollisuuden lisääntyminen osoittaa, että valtiollisten ja ei-valtiollisten kybertoimijoiden määrä on kasvussa. Globalisoituva kybertoimintaympäristö muuttaa perinteisiä kansainvälisiä valta-asetelmia, jolloin esimerkiksi yksittäisille ei-valtiollisille toimioille sekä pienillekin valtioille avautuu mahdollisuus toimia tehokkaasti isossa mittakaavassa. (Suomen kyberturvallisuusstrategia 2013, 19)

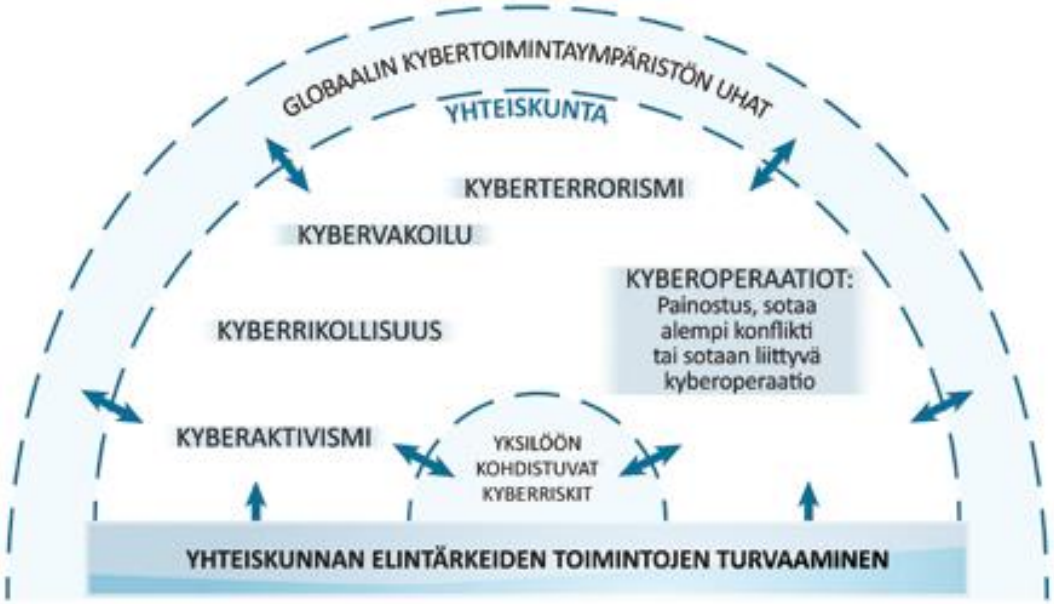
Mitä enemmän tietoyhteiskunta on riippuvainen erilaisista digitaalisista palveluista ja sähköisistä järjestelmistä, sitä alttiimpi se on kybertoimintaympäristön kautta tapahtuvalle vaikuttamiselle. Suomi on tietoyhteiskuntana suhteellisen kehittynyt ja onkin jo joutunut kyberoperaatioiden avulla tehtävän vaikuttamisen kohteeksi. Suomen julkishallintoa ja elinkeinoelämää kohtaan on pääasiassa kohdennettu kyberaktivismia, -rikollisuutta ja -vakoilua, jotka on pyritty tekemään hyödyntämällä järjestelmähaavoittuvuuksia. Hyökkäyskohteiden tarkka valinta, hyökkäyskohteiden tiedustelu, kehittyneet hyökkäystekniikat sekä edistykselliset haittaohjelmat kertovat toiminnan ammattimaisuudesta ja tavoitteellisuudesta. Digitalisaatio sekä sähköisten järjestelmien levittäytyminen yhä

laajemmalle yhteiskunnan erilaisiin ohajusfunktioihin sekä teollisuustuotantoon, ovat avanneet uusia mahdollisuuksia hyödyntää ihmisten toiminnan, organisaatioiden prosessien ja laitteiden haavoittuvuuksien kautta tapahtuvaan kybervaikuttamiseen. (Suomen kyberturvallisuusstrategia, 18)

Kehityksen aiheuttama kybervaikuttamisen keinojen monipuolistuminen onkin mahdollistanut fyysisten vaikutusten aikaansaamisen tällä vuosituhannella. Vuonna 2010 astuttiin uudelle aikakaudelle kyberturvallisuuden näkökulmasta, kun Stuxnet-verkkomato löydettiin. Kyseinen mato oli osa Yhdysvaltain ja Israelin tiedusteluoperaatiota, joka tunnettiin nimellä Olympic games. Operaation tarkoituksena oli häiritä ja vahingoittaa fyysisesti Iranissa sijaitsevan Natanzin ydinlaitoksen uraanin rikastamiseen käyttämiä tietojärjestelmiä kybertoimintaympäristöä hyödyntämällä. Stuxnet-verkkomato saatiin vietyä ydinlaitoksen järjestelmiin mahdollisesti muistitikulla, koska laitoksen tietokoneet ja järjestelmät eivät olleet yhteydessä internettiin turvallisuussyistä. Stuxnet käytti hyväkseen Windows käyttöjärjestelmän neljää tunnettua haavoittuvuutta. Näistä haavoittuvuuksista kaksi olivat nollapäivähaavoittuvuuksia. Nämä kaksi haavoittuvuutta tulivat julki operaation yhteydessä, joten ne olivat julkisesti tuntemattomia ennen operaatiota. Kyberoperaatio onnistui ja sen toteutuksen seurauksena onnistuttiin tuhoamaan uraanin rikastamiseen tarkoitettuja sentrifugeja noin 1000 kappaletta. Lisäksi operaatio viivästytti Iranin uraanin rikastushanketta jopa vuosilla. (Laari ym. 2019, 30-31)

Stuxnet-verkkomadon lähdekoodin kirjoittaminen on ollut mittava projekti ja vaatinut huomattavia kehitysresursseja. Samalla mato osoitti, että kybertoimintaympäristöön vaikuttaminen huolellisesti valmistelluilla kybertyökaluilla mahdollistaa myös fyysisen vahingon aiheuttamisen sähköisissä järjestelmissä ja laitteissa. Yhteiskunnan toiminnan kannalta tärkeisiin teollisuusautomaatiolaitteisiin ja ohjelmoitaviin logiikkoihin kohdistuukin tällä vuosituhannella entistä suurempi kyberuhka, sillä ne ovat entistä useammin kyberhyökkäyksen kohteena. Kuviossa 3 on esitetty suomen kyberuhkamalli, jonka tarkoitus on kuvata kyberuhkien vaikutusmekanismeja, häiriöitä, lähteitä, kohteita ja vaikutuksia kohteeseen. Suomen kyberturvallisuusstrategian muistion mukaan uhat kohdistuvat mahdollisesti suoraan tai välillisesti kansallisesti kriittiseen infrastruktuuriin, yhteiskunnan kannalta elintärkeisiin toimintoihin ja kansalaisiin maan sisä- tai ulkopuolella. Yhteiskunnan kannalta elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat uhkatekijät esiintyvät mahdollisesti samanaikaisina, itsenäisesti tai toisiaan jatkaen. Kyberuhkien vaikuttavuus toteutuu usein nopeasti, mutta niiden ajallinen kesto sekä eskaloitumisnopeus vaihtelevat. Kybertoimintaympäristön levittäytyminen maailmanlaajuiseksi

vaikeuttaa uhkien syiden, taustalla olevien toimijoiden, hyökkäyskohteiden ja tavoitteiden sekä ilmenemisen vaikutuksien ja laajuuden ennustamista. (Suomen kyberturvallisuusstrategia, 18-19)




Kuvio 3. Suomen kyberuhkamalli (Suomen kyberturvallisuusstrategia 2013, 19)

Kyberuhkatoimijat voidaan jakaa eri kategorioihin toiminnan tavoitteellisuuden ja kybertoimintaan käytettyjen resurssien osalta. Kuviossa 3 esitetään neljä kybertoimintaympäristössä vaikuttavaa uhkatoimijaa:

- Kyberaktivismi
- Kyberrikollisuus
- Kybervakoilu
- Kyberterrorismi

Kyberaktivistit pyrkivät välittämään ja levittämään omaa ideologiaansa kybertoimintaympäristössä. Internet ja sosiaalinen media ovat mahdollistaneet laajojen sosiaalisten verkostojen luomisen ihmisten kesken, joilla on samoja intressejä. Kybertoimintaympäristö on tehnyt perinteisestä aktivismista huomattavasti nopeatempoisempaa, tavoittavampaa, vakuuttavampaa ja lähdekritiikitöntä (McCaughey & Ayers 2003, 25-26). Kyberaktivistit pyrkivät saamaan toiminnalleen mahdollisimman laaja huomio, jotta heidän osaamisensa vakuuttaisi laajemmat massat. Kyberaktivismiin voi myös sisältyä vandalismia, jonka tavoitteena on kohteen toiminnan häirintä tai tuhoaminen. (Laari ym. 2019, 32)

Kyberrikollisuus voidaan määritellä laajasti luottamuksellisen tiedon luvattomaksi tai laittomaksi käytöksi, varkaudeksi, tuhoamiseksi, muokkaamiseksi sekä palveluiden, ohjelmistojen, tiedon, välineiden tai tietoverkkojen kopioimiseksi. Kyberrikollisuudeksi voidaan luokitella kaikki rikollinen ja laiton toiminta, joka tapahtuu tietokoneen, älypuhelimen tai muun vastaavan teknologiaa sisältävän laitteen välityksellä. Teknologian ja kybertoimintaympäristön kehittyessä myös kyberrikollisuus saa uusia muotoja. Kyberrikolliset pyrkivät tavoittelemaan esimerkiksi taloudellista hyötyä monin erilaisin keinoin (Marcum 2019, 3-4). Tyypillisesti kyberrikolliset tavoittelevat taloudellisia hyötyjä käyttäen erilaisia tiedonkalastelumenetelmiä, joilla pyritään saamaan esimerkiksi yksityisen henkilön verkkopankkitunnukset käyttöön sähköpostin avulla. Muita vastaavia menetelmiä ovat myös erilaiset kiristyshaittaohjelmat, jotka voivat lukita hyökkäyskohteen pääsyn omaan tietokoneeseensa, jos kohde ei maksa vaadittua rahasummaa. Vastaavia huijauksia voidaan toteuttaa myös sähköpostin välityksellä, joiden avulla pyritään saamaan kohde lähettämään rahaa kyberrikolliselle. (Laari ym. 2019, 32)

Kybertoimintaympäristössä toteutettavaa kybervakoilua suorittavat muun muassa valtiolliset toimijat osana tiedusteluoperaatioitaan. Kybervakoilua voivat suorittaa myös suurilla resursseilla ja osaavalla henkilöstöllä varustautuneet toimijat, jotka eivät toimi suoraan valtiojohtoisesti, mutta niillä voidaan myös katsoa olevan suoria yhteyksiä virallisiin toimijoihin. Kybertoimintaympäristö on mahdollistanut kybervakoilun ulottamisen laajalle ja tehnyt siitä myös kustannustehokkaan tavan harjoittaa erimuotoista vakoilutoimintaa. Kybertoimintaympäristön kasvu ja monipuolistuminen sekä kiinni jäämisen pieni riski ovat avanneet erilaisille tiedustelutoimijoille uusia tapoja harjoittaa kybertiedustelua ja -vakoilua. Kybervakoilulla pyritään saamaan tietoa kohteessa olevista järjestelmistä, niitä käyttävistä henkilöistä sekä digitaalisesta materiaalista, kuten sähköposteista ja ohjelmistoista. Vakoilun kohteena voivat olla myös erilaiset älylaitteet ja tietokoneet joiden kameroita ja mikrofooneja on mahdollista tarkkailla sekä kuunnella käyttäjän tietämättä. Kybervakoilua pyritään kohdistamaan organisaatioiden sisäisten ja virallisten järjestelmien lisäksi siellä työskentelevien henkilöiden omiin yksityislaitteisiin. Lisäksi henkilöihin voidaan kohdistaa henkilötiedustelua, kerätä tietoa erilaisista avoimista lähteistä OSINT menetelmillä ja tiedustelemalla kohdehenkilön sosiaalisen median profiileja. (Laari ym. 2019, 33-34)

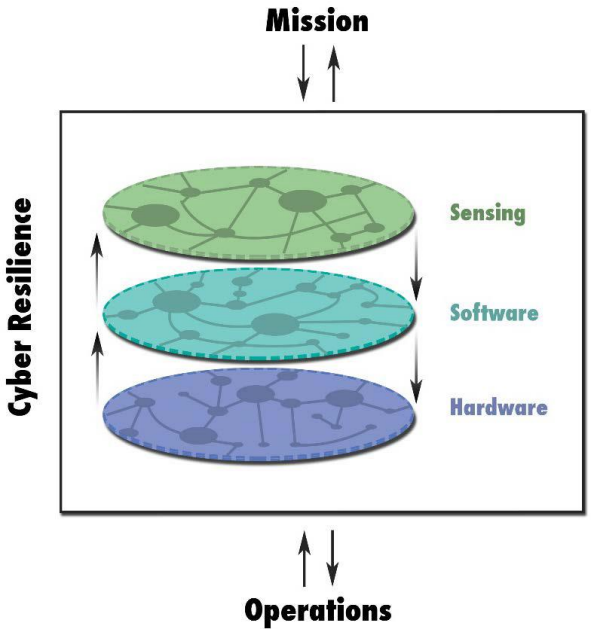
Kyberterrorismi luokitellaan oppikirjamaisesti terrorismiksi, joka pyritään kohdistamaan suoraan kybertoimintaympäristöön liitettyihin järjestelmiin, jotka hoitavat esimerkiksi kriit-

tisen infrastruktuurin toimintoja. Internetin maailmanlaajuinen leviäminen on mahdollistanut myös muunlaisen terroritoiminnan, kuten terrori-iskulla uhkaamisen verkon välityksellä, erilaiset vaikuttamisyritykset sekä terroristisen ideologian levittämisen maailmanlaajuisesti. Lisäksi kyberterroristit voivat vaihtaa tietoja esimerkiksi terrorikohteista salaamalla datansa erilaisilla menetelmillä, vaikka paikalliset valtiot valvoisivat tai sensuroisivat kybertoimintaympäristössä liikkuvaa dataa. Vaikka kybertoimintaympäristö onkin viime vuosina laajentunut nopeasti, toistaiseksi kyberterrorismi ei ole yleistynyt eikä merkittäviä terroritekoja ole toteutettu. (NATO Advanced Research Workshop on Response to Cyber Terrorism, 34-35)

# 3 KYBERSIETOISUUS

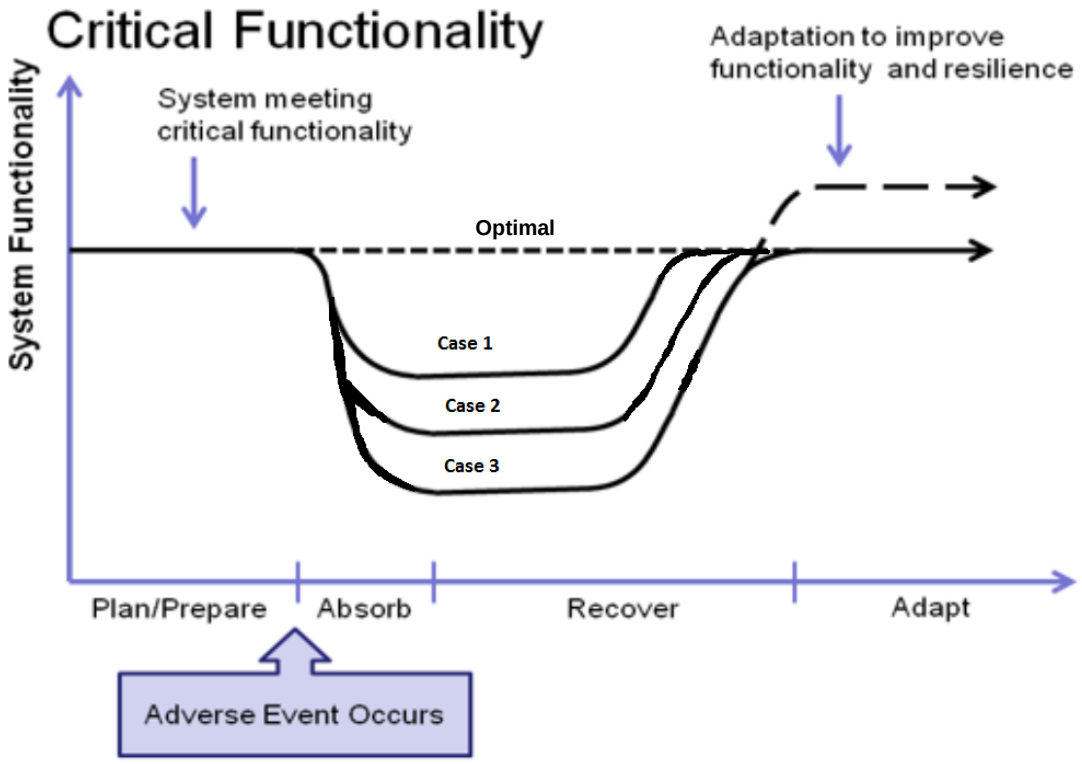
Sietoisuus on terminä moniulotteinen ja juontaa juurensa monilta eri tieteenaloilta. Sietoisuuden määritelmä integroi ekologiset, sosiaaliset, psykologiset, organisatoriset sekä tekniset määritelmät ja näkökulmat yhdeksi kokonaisuudeksi. Teknisestä näkökulmasta sietoisuus on määritelty järjestelmien kyvyksi ennakoida ja sopeutua yllätyksen sekä epäonnistumisen mahdollisuuteen. Siihen liittyy myös uhkaava muutos turvallisuusympäristössä, jolloin järjestelmän toiminta ja selviäminen on tärkeää, kun tilanteen ehkäiseminen on mahdotonta. (Kott & Linkov 2018, 2-3)

Järjestelmien kybersietoisuus kuvaa erityisesti tietojärjestelmän kykyä kohdata, absorboida, palautua ja mukautua kybertoimintaympäristön kautta tapahtuvaan haitalliseen vaikuttamiseen. Monimutkaisten tietojärjestelmien fyysisten komponenttien ja niiden sisältävän informaation kybersietoisuus pitää sisällään myös sosiaaliset ja kognitiiviset alueet inhimillisen tekijän mukanaolon vuoksi. Kokonaisvaltainen järjestelmän kybersietoisuus, joka esitetään kuviossa 4, varmistaa fyysisten järjestelmien ja laitteiden (Hardware), ohjelmistojen (Software) ja aistivien komponenttien (Sensing) saumattoman toiminnan ja järjestelmän palauttamisen kybertoimintaympäristön kautta tapahtuvan vaikuttamisen aikana. (Kott & Linkov 2018, 2-3)




Kuvio 4. Kybersietoisuuden tasot (Kott & Linkov 2018, 3)

Järjestelmien kybersietoisuussuorituskykyä voidaan mitata käyttäen järjestelmien toiminnallisuusastetta (System Functionally) ja kybervaikuttamisen kohtaamiseen (Plan/Prepare), absorboimiseen (Absorb), toipumiseen (Recover) ja tilanteeseen sopeutumiseen (Adapt) käytettyä aikaa kuvion 5 mukaisesti.




Kuvio 5. Kybersietoisuuden mittaaminen (Kott & Linkov 2018, 6, muokattu)

Järjestelmän kriittiseksi toimintapisteeksi (Critical Functionality) voidaan määritellä se piste, jolloin järjestelmä täyttää sille asetetut perustoimintavaatimukset. Kybertoimintaympäristön tai muuta kautta tapahtuvan vaikuttamisen alkaessa, alkaa järjestelmän käytettävyys laskea, jolloin se ei enää täytä asetettuja toimintavaatimuksia. Optimaalisessa tilanteessa tai vähäisen kybervaikuttamisen aikana järjestelmä on täysin kybersietoinen, jolloin sen käytettävyys ei laske. Todellisessa tilanteessa, kun järjestelmä on suunniteltu ja toteutettu sietämään hyvin kybervaikuttamista, kykenee se absorboimaan (Absorb) osan kybervaikuttamisesta, jolloin sen vaikutus järjestelmän käytettävyyteen jää vähäisemmäksi. Kuviossa 5 on havainnollistettu case 1 - 3 esimerkein miten kybersietoisuus vaikuttaa järjestelmän toipumisaikaan ja käytettävyyden tasoon. Kybersietoinen järjestelmä toipuu (Recover) nopeammin kybervaikuttamisen jälkeen ja sen aikana, jolloin sen käytettävyys nousee tasaisesti pisteeseen ennen vaikuttamisen alkamista.

Järjestelmän sopeutumiskyky (Adapt) on ominaisuus, jolla käytettävyys voi jopa parantua, koska järjestelmä osaa torjua sitä vastaan kohdistettua kybervaikuttamista. Järjestelmien kybersietoisuudella onkin suuri merkitys niiden käytettävyyteen ja palautumisnopeuteen. Hyvin toteutettu järjestelmä on kybersietoinen ja takaa toimintavarmuuden vaikeissakin kyberolosuhteissa. (Kott & Linkov 2018, 5-8)

## 3.1 Kybersietoisuuden toteuttaminen

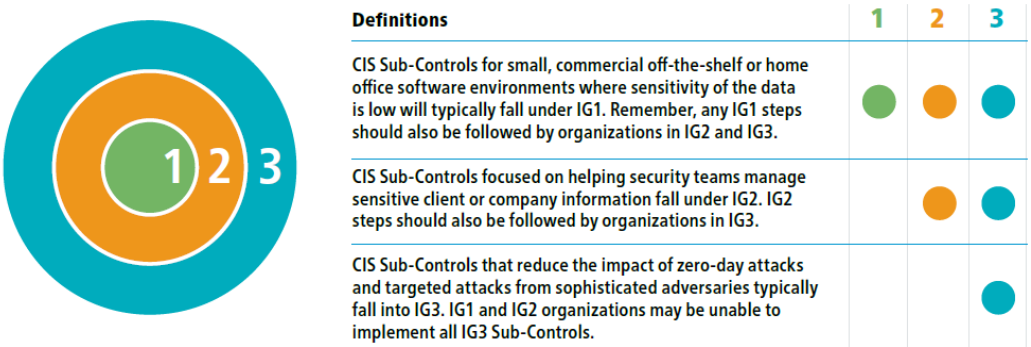
CIS on organisaatio, joka missio on tunnistaa, kehittää, validoida, suositella ja ylläpitää kyberturvallisuuden parhaita ja hyväksi todettuja käytäntöjä. CIS:n mukaan olemme nyt tietoteknisesti siinä kehityspisteessä, että voimme alkaa kutsua tietoturvauhkiin varautumista kyberpuolustukseksi. Kybertoimintaympäristö saa jatkuvasti uusia ulottuvuuksia, kun järjestelmät sekä liiketoimintamallit monimutkaistuvat. Myös erilaiset fyysisten järjestelmien riippuvuussuhteet laajenevat ja niiden käyttäjät siirtyvät enenemissä määrin mobiiliympäristöön. Tämän vuoksi myös yksityishenkilöihin, yrityksiin sekä valtiollisiin toimijoihin kohdistuu entistä enemmän erilaisia uhkia kybertoimintaympäristön kautta. (CIS Inc. 2019, 5-6)

CIS on luonut mallin, joka ottaa huomioon monta kyberturvallisuuden riskitekijää sekä erilaista hyökkäysvektoria. CIS:n mallissa toimintaohjeet jaetaan kolmeen rinnakkaiseen kategoriaan taulukon 1 mukaisesti. Toimintaohjeet jakautuvat tasaisesti, ottaen huomioon koko organisaation toiminnan, sen koon sekä erilaiset toimintaprosessit, laitteet ja ohjelmistot. Yrityksen tai organisaation koko toiminnan läpileikkaava ohjeistus, joka sisältää laite- ja ohjelmistoturvallisuuteen liittyvät asiat, sekä henkilöstön osuuden turvallisuuteen on CIS:n mukaan paras tapa parantaa organisaation kybersietoisuutta. (CIS Inc. 2019, 5-6)

| Aloitustaso | Perustaso | Organisaatiotaso |
|---|---|---|
| • 1.Laitteistojen keskitetty hallinta ja kirjanpito<br>• 2.Ohjelmistojen keskitetty hallinta ja kirjanpito<br>• 3.Tietoturvahaavoittuvuuksien seuranta ja hallinnointi<br>• 4.Käyttöoikeuksien hallinta<br>• 5.Turvalliset laite- ja ohjelmistokonfiguraatiot työasemille, mobiililaitteille sekä palvelimille<br>• 6.Järjestelmälogien auditointi, monitorointi ja huolto | • 7.Internetselain- ja sähköpostiturva<br>• 8.Malmware:n torjunta<br>• 9.Verkon rajoitukset ja kontrollointi (portit, protokollat ja palvelut)<br>• 10.Datan palautettavuus<br>• 11.Palomuurien, kytkimien ja routtereiden turvallinen konfiguraatio<br>• 12.Rajapintapuolustus<br>• 13.Datan suojaus<br>• 14.Pääsynhallinta dataan ja tietoon<br>• 15.Langattomien verkkojen hallinta<br>• 16.Käyttötilien hallinta ja monitorointi | • 17.Kybertietoisuuden lisääminen ja koulutusohjelmat<br>• 18.Ohjelmistoturvallisuus<br>• 19.Tietoturvapoikkeamiin reagointi ja raportointi<br>• 20.Tunkeutumisharjoitukset ja testaus |

Taulukko 1. Rinnakkaiset toimintamallikategoriat (CIS Inc. 2019. 4, muokattu)

Nämä kolme kategoriaa sisältävät toimintaohjeita, jotka jaotellaan yrityksen tai muun organisaation koon mukaan kolmeen eri implementointiryhmään kuvion 6 mukaisesti. Yrityksen tai organisaation ottaessa mallia käyttöön, tulee sen lähteä liikkeelle aloitustasolla luetelluista kohdista. Aloitustasolla luodaan CIS:n mukaan perusteet toiminnan kokonaisvaltaiselle kyberhygienialle, jolla saavutetaan kybersietoisuuden perusteet. (CIS Inc. 2019, 6-7)




Kuvio 6. CIS implementointiryhmät (CIS Inc. 2019, 9)

Suosituksen mukaan noin 10 henkeä työllistävän organisaation tulee aloittaa kybersietoisuuden kehittäminen implementointiryhmän 1 kohdista. Sieltä valikoidaan ne kehittämisalueet ja toimintamallit, jotka palvelevat parhaiten organisaation liiketoimintaa tai tehtäviä. Pienten organisaatioiden on toimittava omien resurssien puitteissa ja keskityttävä niihin kohtiin, jotka palvelevat parhaiten sen oman toiminnan ja asiakkaiden kyberturvallisuutta. Jos organisaatio toimii kriittisen infrastruktuurin tai vastaavan toimintavarmuutta vaativan kriittisen palvelun tuottajana, tulee uusia turvallisuusmalleja ottaa käyttöön enemmän kuin niissä, jotka toimivat ei kriittisillä aloilla. (CIS Inc. 2019, 9)

Kuviossa 7 havainnollistetaan aloitustason kohdan 1 laitteiston keskitetyn hallinnan ja kirjanpidon ohjetta numero 4, joka on implementointiryhmän 1 ohjeistus. Kohdassa ohjeistetaan pitämään ajantasaista seurantaa kaikesta tietotekniikasta, joilla voidaan tallentaa tai prosessoida tietoa. Ryhmän 1 ohjeet implementoidaan myös suurempiin organisaatioihin. Seurannan piiriin kuuluvat kaikki tietotekniset laitteet kytkettiinpä niitä yrityksen tai organisaation tietoverkkoihin tai ei. Ryhmän 1 ohjeet implementoidaan myös suurempien ryhmissä 2 ja 3 olevien organisaatioiden toimintamalleihin. (CIS Inc. 2019, 13)

| Sub-Control | Asset Type | Security Function | Control Title | Control Descriptions | Implementation Groups | | |
|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 |
| 1.4 | Devices | Identify | Maintain Detailed Asset Inventory | Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not. | ● | ● | ● |

Kuvio 7. Aloitustason Implementointiryhmän 1 ohje 1.4 (CIS Inc. 2019, 13)

Implementointiryhmän 2 kohtia suositellaan, jos organisaatio toimii kansallisesti ja työllistää satoja henkilöitä. Organisaatiossa työskentelee yleensä henkilö tai henkilöitä, jotka vastaavat tietotekniikan hallinnasta ja infrastruktuurin yleisestä suojaamisesta sekä turvallisuudesta. Suuremmissa organisaatiossa voi myös olla toimintoja tai osastoja, joiden riskiprofiilit ovat kyberturvallisuuden näkökulmasta erilaisia. Tämän vuoksi turvallisuutta parantavia toimintamalleja tulee implementoida käyttöön enemmän ja valikoidummin. Jotkut toimintamallit ovat kuitenkin hyvin riippuvaisia yritystason tekniikasta sekä organisaation osaamisesta, joten organisaation asiantuntemus tulee olla hyvällä tasolla, että toimintamalleja voidaan ottaa käyttöön. Isommissa organisaatioyksiköissä kestetään

yleisesti lyhyitä palvelunkeskeytyksiä kohtuullisen hyvin, koska riskeihin ollaan varauduttu, kun niitä osataan tunnistaa. Yleisesti suurin huolenaihe implementointiryhmän 2 organisaatioille on organisaation sidosryhmien luottamuksen menettäminen, jos tietoturvallisuus vaarantuu tai rikkomus tapahtuu. Tällöin yritys tai organisaatio voi mainehaitan takia menettää asiakkaitaan tai kumppaneitaan. (CIS Inc. 2019, 8)

Kuviossa 8 havainnollistetaan perustason kohdan 11 palomuurien, routtereiden ja kytkimien turvallinen konfiguraatio ohjetta numero 1. Ohje kuuluu implementointiryhmään kaksi ja ohjeistaa ylläpitämään ja dokumentoimaan yrityksen tai organisaation turvallisuusstandardeja ja toimintamalleja kaikkien luotettujen verkkolaitteiden ja niiden konfiguraatioiden osalta. Implementaatioryhmän 2 ohjeet otetaan käyttöön myös implementaatioryhmän 3 organisaatioissa. (CIS Inc. 2019, 8)

| Sub-Control | Asset Type | Security Function | Control Title | Control Descriptions | Implementation Groups | | |
|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 |
| 11.1 | Network | Identify | Maintain Standard Security Configurations for Network Devices | Maintain documented security configuration standards for all authorized network devices. | | ● | ● |

Kuvio 8. Perustason Implementointiryhmän 2 ohje 11.1 (CIS Inc. 2019, 43)

Toiminnan laajentuessa globaaliksi ja työntekijöiden tai muiden toimijoiden määrän noustessa tuhansiin, CSI suosittelee kolmannen implementointiryhmän toimintaohjeiden käyttöönottoa organisaation resurssien puitteissa. Kolmannen ryhmän organisaatioissa työskentelee päätoimisesti kyberturvallisuuden huippuammattilaisia, jotka ovat perehtyneet riskienhallintaan, penetraatiotestaukseen sekä yleiseen ohjelmistoturvallisuuteen. Implementointiryhmän 3 organisaatioiksi valikoituvat yleisesti yhteiskuntien toiminnan kannalta kriittiset toimijat. Näitä organisaatioita vastaan kohdistettu ammattimainen kyberhyökkäys voi aiheuttaa merkittävää haittaa yleiselle turvallisuudelle ja hyvinvoinnille. Näiden organisaatioiden tuleekin sietää ammattisesti toteutettua kybervaikuttamista ja kyberhyökkäyksiä erityisen hyvin. (CIS Inc. 2019, 8)

Kuviossa 8 havainnollistetaan perustason kohdan 13 implementointiryhmän 3 ohjetta numero 9, jossa ohjeistetaan yritystä tai organisaatiota kryptaamaan kaikilla USB-muistityypeillä oleva tieto aina kuin muistilaite ei ole käytössä, kun sellaisia käytetään yrityksen tai organisaation operatiivisessa toiminnassa. (CIS Inc. 2019, 8)

| Sub-Control | Asset Type | Security Function | Control Title | Control Descriptions | Implementation Groups | | |
|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 |
| 13.9 | Data | Protect | Encrypt Data on USB Storage Devices | If USB storage devices are required, all data stored on such devices must be encrypted while at rest. | | | ● |

Kuvio 9. Perustason Implementointiryhmän 3 ohje 13.9 (CIS Inc. 2019, 49)

# 4 OSAAMINEN

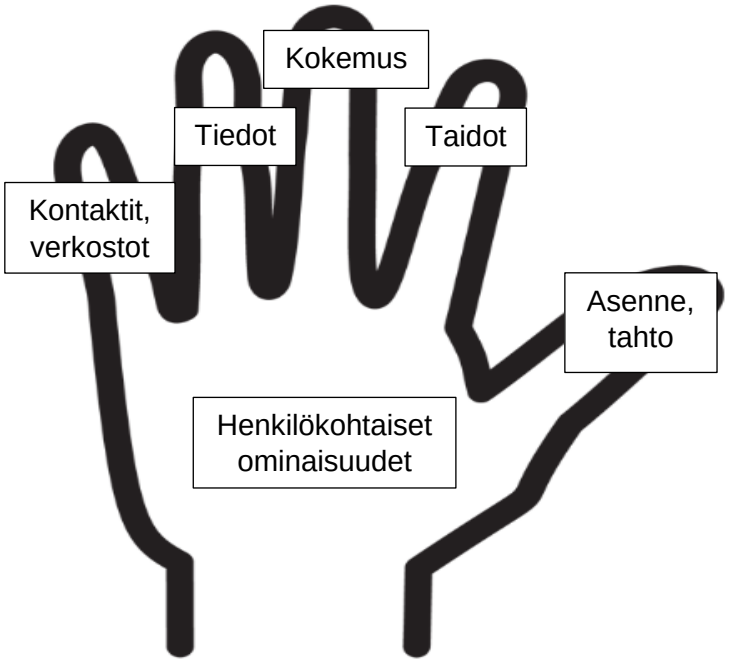
Homo sapiens, eli moderni ihmislaji on erittäin oppimiskykyinen. Toisin kuin mikään muu maapallolla elävä organismi, olemme kykeneväisiä sopeutumaan elinympäristöömme ja muokkaamaan sitä siten, että voimme maksimoida selviytymismahdollisuutemme. Yksilön ja yhteisöjen oppimisen kautta ihmiset ovat kautta aikain keksineet ratkaisuja ongelmiin, tehneet päätöksiä ja käyttäneet luovuutta, kun on ollut tarve täyttää korkeatasoiset tarpeet ruuan, lämmön ja turvallisen elintilan suhteen. 2000-luvulle tultaessa, ovat ihmiskunnan haasteet muuttaneet muotoaan. Organisaatioissa tämä näkyy vaateena työskennellä fiksummin, kykynä tehdä tärkeitä päätöksiä nopeasti etenevissä projekteissa ja kykynä oppia työskentelemään yhdessä. Myös ongelmienratkaisukyvyt korostuvat monimutkaisessa ja epävarmassa maailmassa. Samat oppimiseen ja sopeutumiseen vaikuttavat teemat ovat siis läsnä nykyajankin organisaatiossa oppimista ja osaamista ohjaavina tekijöinä. (Sadler-Smith 2006, 97)

Osaaminen voidaan määritellä monella eri tavalla riippuen itse määrittelijästä ja hänen näkemyksestään. Yleisesti osaamisesta puhutaan, kun tutkitaan erimerkiksi työntekijöiden suoriutumista työtehtävistään tai kyvystä kehittää työtään ja käytettäviä työmenetelmiä. Osaaminen näkyy konkreettisesti, kun oppimisen tukoksena on syntynyt kykyjä ratkaista työhön liittyviä ongelmia ja kykyjä soveltaa teoreettista tietoutta tehokkaasti myös käytännön tekemiseen. Osaaminen skaalautuu myös tiimitasoiseksi, koska suurien kokonaisuuksien hallinta ja eteenpäin vieminen ei välttämättä onnistu yksilötason kyvyillä. Yksilö voi tarvita tuekseen ryhmän, jotta hän pystyy suoriutumaan annetuista tehtävistä. (Otala 2008, 46-48)

Yrityksien, muiden organisaatioiden ja myös yksilön näkökulmasta osaaminen on niiden tärkein voimavara. Osaamisella luodaan edellytykset kaikelle onnistumiselle työelämässä ja muissa organisaatioissa. (Hätönen 2011, 8-9 ; Ranki 1999, 10) Viitala kuvaileekin osaamisen olevan lähtökohta organisaatioiden ja yritysten strategiselle kyvykkyydelle. Yleisesti organisaatioiden ja yritysten toimintaa ohjaavat erilaiset strategiat ja visiot, joiden tarkoituksena on kehittää näiden liiketoimintaa. Liiketoimintaan ja sen kehittämiseen liittyy vahvasti myös osaaminen, osaamisen kehittäminen ja henkilöstön kokemus. Liiketoiminnan kehittämisen kannalta on siis tärkeää, että yritys- ja organisaatiotasolla toiminta on yhtenäistä ja vallitsevien strategioiden ja visioiden mukaista, jotta toiminta kehittyy halutun mallin mukaisesti. (Viitala 2013, 48,170 ; Ranki 1990, 16)

## 4.1 Yksilöiden osaaminen

Yksilöiden osaaminen rakentuu aiemmin opituista asioista ja kokemusten tuomasta tiedosta, taidosta, kontakteista ja erilaisista verkostoista. Myös omat kyvyt yhdistää oman osaamisen komponentteja yhdeksi kokonaisuudeksi. Asenne ja tahto luetellaan Otalan mukaan osaamiseksi, jotka hän kuvaa osaamisen käden kautta kuvion 10 mukaisesti. Kämmen, joka kuvaa yksilön henkilökohtaisia taitoja, yhdistää kompetenssit yhdeksi kokonaisuudeksi, joiden perustana toimivat yksilön henkilökohtaiset ominaisuudet. (Otala 2008, 50-51)




Kuvio 10. Yksilön osaaminen (Otala 2008, 51, muokattu)

Osaaminen ilmenee eri tavoin riippuen ihmisen sosiaalisista taidoista, kuten esimerkiksi tunneälystä. Saman koulutuksen ja kokemuksen omaava henkilö voi osoittaa osaamistaan eri tavoin riippuen hänen persoonallisuudestaan, asenteestaan ja tavastaan kommunikoida muiden ihmisten kanssa. Motiivit ja erilaiset kyvyt luoda sekä tuottaa mielikuvia kuuluvat myös henkilökohtaisiin ominaisuuksiin. Niitä täydentävät myös kyky uusien mahdollisuuksien näkemiseen ja niiden hyödyntämiseen. Yksilön osaamiseen vaikuttavat osaltaan asenne ja tahto kuin myös tekemisen ja koulutuksen kautta saadut erilaiset taidot ja tiedot. Hiljainen tieto ja kokemukset liittyvät myös oleellisesti tekemiseen. Hiljai-

nen tieto määritellään Otalan mukaan ääneen lausumattomaksi tiedoksi, joka on henkilökohtaista, tiettyyn tilanteeseen ja toimintaan liittyvää toisille henkilölle vaikeasti siirrettävää tietoa. Yksilön osaamisen ilmenemisen kannalta merkittävässä osassa on kyky luoda verkostoja muiden osaajien ja sidosryhmien kanssa sekä hankkia ja ylläpitää kontakteja. (Jalava, Palonen, Keskinen & Kontkanen 1999, 17-18; Otala 2008, 50-53, 346)

Työelämäkvalifikaatio on käsite, jolla voidaan Viitalan mukaan kuvata työssä tarvittavaa osaamista. Tämä kuvaa myös valmiuksia, joita työntekijät työssään tarvitsevat. Työntekijä on voin hankkia tarvittavat valmiudet esimerkiksi kouluttautumalla, tekemällä konkreettista työtä tai verkostojensa ja sosiaalisten kontaktiensa avulla. Työntekijä voi myös omata kykyjä ja persoonallisia ominaisuuksia, joita ei ole ollut mahdollista hankkia työkokemuksen tai koulutuksen avulla. Osaamiset joita työntekijä työssään tarvitsee, voidaan jaotella tehtävä- ja ammattikohtaiseen osaamiseen sekä yleiseen osaamiseen. Työelämäkvalidikaatio, eli työelämän yleinen osaaminen on kompetenssi, joka on työtehtävästä riippumatonta osaamista. Erityisosaamiset, jotka ovat työntekijöiden osaamisen ydintä, nimitetään yleisesti substanssiosaamiseksi. Viitala on kuvannut substanssiosaamisen osaamispyramidin huipulle kuvion 11 mukaisesti. (Viitala 2013, 179)


Kuvio 11. Osaamispyramidi (Viitala 2013, 180, muokattu)

Ammattitaito rakentuu Viitalan mukaan osaamispyramidin mukaisesti. Pyramidissa kuvatut kerrokset havainnollistavat ammattitaidon erilaisia osa-alueita. Yksilön persoonallisuuden ominaisuuksia, ihmisenä kehittymistä sekä yleisiä työelämässä tarvittavia taitoja tarvitaan luomaa kvalifikaatioiden perusta pyramidin alimmalle tasolle. Suoritettavaan työtehtävään liittyvät kvalifikaatiot ovat pyramidin ylimmillä tasoilla. (Viitala 2013, 179)

Työssä menestymiseen muuttuvassa työelämässä vaikuttavat vahvimmin pyramidin alaosassa olevat valmiudet. Jatkuvan muutoksen kautta tapahtuva oman osaamisen kehittämistarve kysyy työntekijältä asennetta ja kertoo, onko hän valmis muuttumaan. Asenne kertoo myös, onko yksilö vastuuntuntoinen työyhteisönsä asioista. Työyhteisöjen tiedon tarve ja saanti on lisääntynyt merkittävästi yksilötasolla, joten asiantuntijoiden ja asiakkaiden kanssa verkostoituminen onkin tärkeä osaamisalue yksilön näkökulmasta. (Viitala 2009, 180)

Kun työntekijä hankkii työssä vaadittavia tietoja ja taitoja, syntyy osaamista, joka on oppimisprosessin tulos. Asiantuntijuus muodostuu, kun työntekijän ammatillinen osaamisen muodostava teoria ja käytäntö yhdistyvät. Oppimista tapahtuu, kun työntekijä tekee, kokee, onnistuu ja epäonnistuu. Oppimisympäristöllä, kulttuurilla ja yleisellä ilmapiirillä on myös vaikutusta oppimiseen, jota ohjaavat oppijalle tärkeät tarpeet, palaute ja odotukset. Oppimisen tärkein edellytys Otalan mukaan on kuitenkin yksilön oma motivaatio. Oppimista voidaan mallintaa hänen mukaansa kertolaskulla, jossa kertojina ovat tarjolla oleva tieto, oppijan motivaatio sekä taito kysyä. Jos joku laskun kertojista on nolla, on oppimisen tulos myöskin nolla. Koskaan ei työelämässä ole ollut tietoa tarjolla niin paljon kuin sitä on nykyaikana, joten sitä on mahdollista halutessaan kysyä. Tiedonhankintaan voi oppia, mutta motivaatiota ei voi pakkosyöttää. Motivaation muodostumiselle on kuitenkin mahdollista luoda otolliset olosuhteet, jolloin se kehittyy sisäisesti. Yksilön on siis haluttava saavuttaa oppimisella tavoitteensa. (Otala 2008, 64-67)

Oma-aloitteinen omasta osaamisesta huolehtiminen ja sen ylläpitäminen sekä kehittäminen ovat yksilön omalla vastuulla. Osaamisen tulee olla myös linjassa oman organisaation tavoitteiden ja visioiden kanssa. Oppimisen vastuu luo sitoutumista omaan kehittymiseen sekä oppimiseen. Oletuksena ei voida pitää, että osaamisen hankinta lähtee yrityksen tai organisaation johdosta, vaan siihen tulee sitouttaa myös yksilöt ja koko henkilöstö. (Otala 2008, 65; Kauhanen 2006,147)

## 4.2 Osaamisen arviointi

Osaamisvahvuuksia ja osaamispuutteiden tunnistamista pyritään etsimään organisaatiossa tai työpaikoilla suoritettavassa osaamisen arvioinnissa. Arvioinnin tarkoituksena ei yleensä ole työntekijöihin liittyvien riskien tai työtehtävissä menestymisen selvittäminen. Henkilöstön kompetenssikartoitusten ja erilaisten arvioiden käyttäminen osaamisen johtamisen välineenä on yleistynyt organisaatioissa 1990-luuvulta alkaen. Osaamisen arviointi tarkoittaa Hätösen mukaan tarkasteltavan kohteen tai toiminnan tulkinnallista analyysiä, sekä toiminnan tuottaman hyödyn ja arvon määrittämistä mahdollisimman tarkasti ja luotettavasti. Arviointi tuottaa tietoa jonka perusteella pystytään ohjaamaan organisaation kehittymistavoitteiden asettamista. Arvioinneilla luodaankin näin ollen perusta osaamisen kehittämistyölle. Nykyisten organisaatioiden ja työpaikkojen osaamisen arvioinnit toteutetaan usein työntekijän itsearviointina, jota täydentää esimiehen arvio alaisensa osaamisesta. Kehityskeskustelulla tarkennetaan yleistä osaamisen arviointia, jonka perusteella tehdään henkilön kehityssuunnitelma. (Hätönen 2011, 32-34)

Itsearvioinnin tarkoituksena on työntekijän itsenäisesti suorittama oman osaamisen, suoritusten ja saavutusten arviointi. Arviointi vaatii omaan työhönsä liittyvien osaamisten ja tavoitteiden tunnistamista sekä taitoa tulosten kriittiseen arviointiin. On kuitenkin erityisen tärkeää huomata, että itsearviointi on yksipuolinen käsitys suoriutumisesta ja osaamisesta. Kokonaisuuden kannalta paras tulos saavutetaan, kun yhdistetään eri henkilöiden antamat arviot. Yksilöiden arviot omasta osaamisestaan ja toiminnastaan perustuvat omakuvan realistisuuteen. Jos yksilö ei tiedosta puutteita, vahvuuksia ja kykyjään, saattaa arviossa esiintyä yli- ja aliarviointia. (Hätönen 2011, 32-34; Lankinen, Miettinen & Sipola 2004, 79.)

Kehityskeskusteluiden tavoitteena on pyrkiä löytämään yhteinen näkemys ja linja yrityksen tavoitteiden ja työntekijän tarpeiden välille. Kehityskeskustelu on yksi johtamisen työkalu ja se käydään esimiehen ja alaisen välillä säännöllisin väliajoin. Kehityskeskustelun tulee olla avointa kommunikaatiota ja sen tarkoituksena on parantaa työntekijän suoriutumista työtehtävistään. Sen konkreettisina tavoitteina on määritellä kehittymissuunnitelma ja kehittämistarpeet sekä arvioida saavutetut tulokset ja sopia uusista tavoitteista. Yksi tärkeimmistä kehityskeskustelun tavoitteista onkin esimiehen ja alaisen yhteistyön kehittäminen, johon liittyy myös työilmapiirin ja yleisten työskentelyolosuhteiden kehittäminen. (Hätönen 2011, 32-33; Lankinen, Miettinen & Sipola 2004, 79 ; Sydänmaanlakka 2012, 92)

Yksi tärkeä osaamiskartoituksen osa on osaamistietojen taltiointi. Dokumentoituja tuloksia voidaan hyödyntää kehityssuunnitelmien laadinnassa. On tarkoituksenmukaista varastoida osaamistietojen määrittelyt, listaukset ja luokittelut ja niistä saatava tieto, jotta niillä voidaan jatkossa helpottaa organisaation ja työpaikan käytännön työtä. Osaamistietojen tallentamiseen onkin kehitetty monenlaisia digitaalisia osaamistietojärjestelmiä. Monet toimijat ovat myös kehittäneet omia ohjelmistoja osaamistietojen tallentamiseen. Ohjelmistojen tarkoitus on helpottaa osaamis- ja muiden tietojen ylläpitämistä henkilön koulutuksen, osaamisen, pätevyyksien, taitojen kehittämissuunnitelmien ja työtehtävähistorian osalta. Ne osaltaan tukevat osaamisen johtamista, kehittämistä ja arviointia. (Hätönen 2011, 48; Sydänmaanlakka 2012, 133-135)

## 4.3 Osaamisen vaatimukset

Tähän opinnäytetyöhön ja sen tutkimusosuuteen liittyvät kunnossapitohenkilöstön osaamisen vaatimukset tullaan mallintamaan kansallisen turvallisuusauditointikriteeristön suositusten mukaan (Katakri 2015). Ensimmäinen Katakri eli kansallinen turvallisuusauditointikriteeristö valmistui osana hallituksen sisäisen turvallisuuden ohjelmaa vuonna 2009. Sitä valmisteltiin puolustusministeriön johdolla yhteistyössä viranomaisten ja elinkeinoelämän kanssa. Katakri on auditointityökalu, jota viranomaisorganisaatiot käyttävät kohdeorganisaatioiden arvioinnissa, kun kyseessä on viranomaisten salassa pidettävän tiedon suojaaminen. Katakri kokoaa yhteen kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat perusvaatimukset. Katakri itsessään ei aseta ehdottomia vaatimuksia tietoturvallisuudelle. Siihen on koottu vaatimuksia, jotka perustuvat voimassa olevaan lainsäädäntöön ja kansainvälisiin tietoturvallisuusvelvoitteisiin, jotka sitovat myös Suomea. (Katakri 2015, 2-3)

Katakria on mahdollista käyttää, kun auditoidaan yrityksen tai organisaation tietoturvallisuusjärjestelyjen toteutumista viranomaisten tietojärjestelmien turvallisuuden arvioinneissa sekä yritysturvallisuusselvityksissä. Yrityksien, organisaatioiden sekä viranomaisten turvallisuustyön ja muun kehittämisen ohjaamiseen voidaan myös soveltaa Katakrin ohjeita. Katakrin käytöllä pyritään varmistamaan kohdeorganisaatioiden riittävät turvallisuusjärjestelyt oikeudettoman paljastumisen ehkäisemiseksi niissä ympäristöissä, jossa käsitellään viranomaisen salassa pidettävää, omistamaa tai leimaamaa tietoa. Lisäksi tavoitteena on turvallisuusvaatimusten huomioonottamisen varmistaminen turvallisuuden hallinnassa. (Katakri 2015, 2-3)

Uhkiin nähden hyväksyttävän turvallisuustason varmistamiseksi avaintekijänä toimii turvallisuusjärjestelyjen hallittu suunnittelu ja toteutus. Suunnittelun ja toteutuksen kohteena olevan organisaation on pystyttävä osittamaan riittävät turvallisuusjärjestelyt luotettavasti. Järjestelmällisten riskiarviointien tulee toimia pohjana turvallisuusjärjestelyiden riittävyyden arvioinnille. Hallitsemalla turvallisuusriskejä pyritään toteuttamaan turvatoimien yhdistelmä, jotka saavat aikaan tyydyttävän tasapainon kustannuksien, käyttäjien vaatimuksien sekä turvallisuuteen kohdistuvien jäännösriskien välillä. Katakrissa kuvatut erilliset osa-alueet on niputettu erillisiksi kokonaisuuksiksi, joten niitä voidaan käyttää myös erikseen. (Katakri 2015, 4)

## 4.4 Turvallisuusjohtaminen

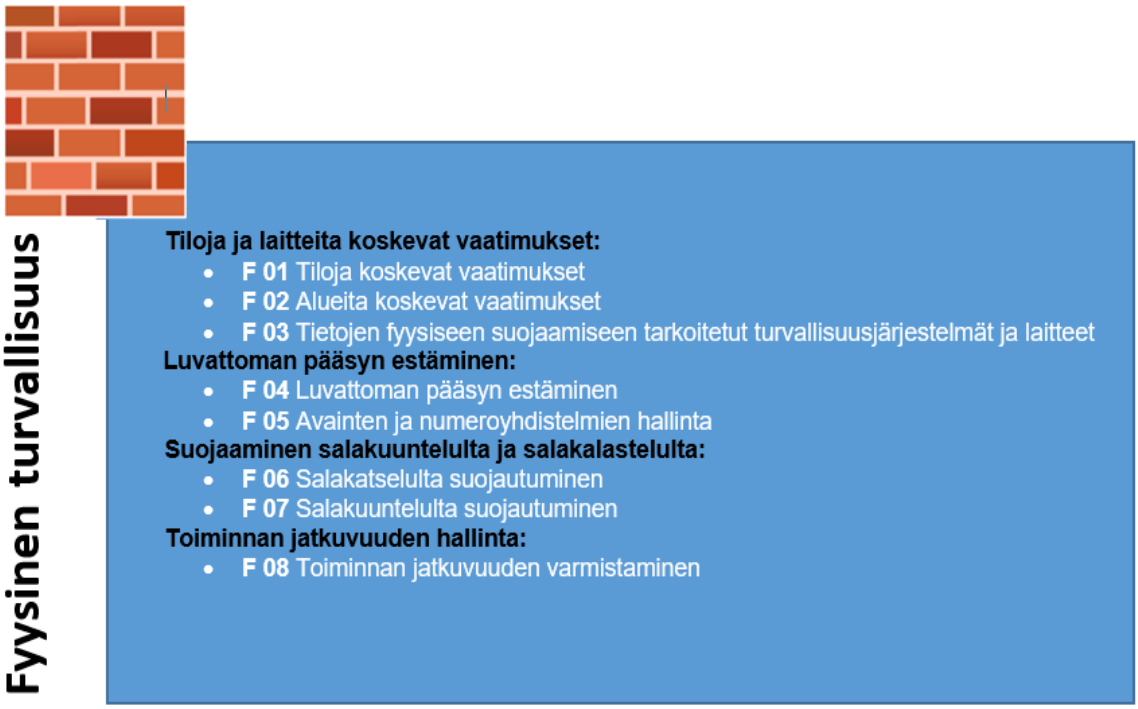
Katakrin turvallisuusjohtaminen osiossa käsitellään menetelmiä, joilla turvallisuus ja sen hallinta voidaan jalkauttaa osaksi koko työpaikan tai muun organisaation toimintaa. Turvallisuusjohtamiseen kuuluvat niin henkilö- kuin hallinnollinen turvallisuus. Turvallisuusjohtamisen vaatimukset pyrkivät varmistamaan työpaikalla tai organisaatiossa olevan turvallisuuden hallintajärjestelmän toiminnan, sekä riittävät menettelyt viranomaisen salassa pidettävän tiedon asianmukaiseen käsittelyyn henkilöstön toimesta. (Katakri 2015, 5)


Taulukko 2. Turvallisuusjohtamisen vaatimukset (Katakri 2015, 6-15)

Turvallisuusjohtamisen vaatimukset ja kategorisointi, joita havainnollistetaan taulukossa 2 ovat kokonaisuus, jotka luovat pohjan yrityksen tai organisaation turvalliselle viranomaisen salassa pidettävän tietoaineiston käsittelylle sekä operatiiviselle toiminnalle. Vaatimukset sisältävät tarkempia ohjeistuksia johdon sitouttamiseksi turvallisuustyöhön ja organisaation turvalliseen toimintaan. Lisäksi vaatimuksissa otetaan kantaa osaamisen, yleisen operatiivisen toiminnan, henkilöstön sekä liiketoiminnan turvallisuuden varmistamiseen. (Katakri 2015, 6-15)

## 4.5 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan viranomaisen salassa pidettävän tietoaineiston suojaamista oikeudettomalta paljastumiselta. Fyysiset turvatoimet pyrkivät estämään salaa- tai väkisin tunkeutumiset, ehkäistä, estää ja havaita luvattomat toimet. Lisäksi toimilla mahdollistetaan henkilöstön luokittelu perustuen heidän tiedonsaanti- ja liikkumistarpeisiinsa. Näin pystytään rajaamaan ja varmistamaan, että henkilöstö saa vain ja ainoastaan tarvitsemansa tiedon. Fyysisien turvatoimien valinta ja mitoitus perustuvat uhkakartoitukseen sekä riskien arviointiin. Vaatimuksien täyttyminen varmennetaan käyttäen erilaisia toimintamalleja. Osana organisaation riskienhallintaa, tulee yrityksessä ja organisaatiossa myös seurata fyysisten turvatoimien vaikuttavauutta. (Katakri 2015, 16)




Taulukko 3. Fyysisen turvallisuuden vaatimukset (Katakri 2015, 18-28)

Fyysinen turvallisuus perustuu kokonaisuudessaan huolelliseen suunnitteluun. Fyysisen turvallisuuden vaatimuksia ja kategorisointia havainnollistetaan edellä esitetyssä taulukossa 3. Vaatimusten tarkoituksena on ohjeistaa tilaturvallisuuteen liittyvät asiat, kuten millaisissa rakennuksissa ja tiloissa viranomaisen salassa pidettävää materiaalia säilötään ja käsitellään, millaisilla järjestelmiä tietojen käsittelyyn käytetään. Vaatimuksissa huomioidaan myös tietojen kasautumisen aiheuttaman turvallisuusluokituksen nousemisen toimenpiteet. (Katakri 2015, 16)

### 4.6 Tekninen tietoturvallisuus

Teknisen tietoturvallisuuden vaatimuksissa kuvataan tavat, joita soveltamalla voidaan varmistaa riittävät turvallisuusjärjestelyt sähköisille käyttöympäristöille, joissa hallinnoidaan tai käsitellään viranomaisen salassa pidettävää tietoa. Teknisen tietoturvallisuuden vaatimuksia ja kategorioita havainnollistetaan taulukossa 4. Tekniset tietoturvallisuusvaatimukset ohjeistavat ja lisäksi täydentävät Katakrin muiden osa-alueiden kuvauksia, kun kyseessä on paperimuotoisen aineiston suojaaminen. Ohjeistuksissa otetaan huomioon esimerkiksi hallintayhteyksiin, langattomiin verkkoihin, etäkäyttöön ja varmuuskopiointiin liittyviä asioita. (Katakri 2015, 29)

**Tekninen tietoturvallisuus**

**Tietoliikenneturvallisuus:**

- **I 01** Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen
- **I 02** Vähimpien oikeuksien periaate - Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt ko. suojaustason sisällä
- **I 03** Tietojenkäsittelyympäristön turvallisuus koko elinkaaren ajan - Suodatus- ja valvontajärjestelmien hallinnointi
- **I 04** Tietojenkäsittelyympäristöjen suojattu yhteenliittäminen -Hallintayhteydet
- **I 05** Salassa pidettävien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - Langattomat verkot

**Tietojärjestelmäturvallisuus:**

- **I 06** Vähimpien oikeuksien periaate - Pääsyoikeuksien hallinnointi
- **I 07** Monitasoinen suojaaminen - Tietojenkäsittelyympäristön toimijoiden tunnistaminen fyysisesti suojatun alueen sisällä
- **I 08** Vähimmäistoimintojen ja vähimpien oikeuksien periaate – Järjestelmäkovennus
- **I 09** Monitasoinen suojaaminen – Haittaohjelmasuojaus
- **I 10** Monitasoinen suojaaminen - Turvallisuuteen liittyvien tapahtumien jäljitettävyys
- **I 11** Monitasoinen suojaaminen - Poikkeamien havainnointikyky ja toipuminen
- **I 12** Tietoturvallisuustuotteiden arviointi ja hyväksyntä – Salausratkaisut
- **I 13** Monitasoinen suojaaminen koko elinkaaren ajan - Ohjelmistoilla toteutettavat pääsynhallintatoteutukset
- **I 14** Monitasoinen suojaaminen - Hajasäteily (TEMPEST)

**Tietoaineistoturvallisuus:**

- **I 15** Salassa pidettävien tietojen välitys fyysisesti suojattujen alueiden välillä - Aineiston sähköinen välitys
- **I 16** Salassa pidettävien tietojen välitys fyysisesti suojattujen alueiden välillä - Aineiston välitys postilla ja kuriirilla
- **I 17** Tietojenkäsittelyympäristön suojaus koko elinkaaren ajan - Salassa pidettävien tietojen jäljentäminen - Tulostus ja kopiointi
- **I 18** Tietojenkäsittelyympäristön suojaus koko elinkaaren ajan - Turvallisuustarkoituksia varten tapahtuva salassa pidettävien tietojen kirjaaminen
- **I 19** Tietojenkäsittelyympäristön suojaus koko elinkaaren ajan – Salassa pidettävää tietoa sisältävien tietoaineistojen hävittäminen
- **I 20** Salassa pidettävän tiedon käsittelyyn liittyvän tietojenkäsittelyympäristön suojaus koko elinkaaren ajan - Muutoshallintamenettelyt

**Käyttöturvallisuus:**

- **I 21** Salassa pidettävien tietojen käsittely fyysisesti suojattujen alueiden sisällä - Fyysinen turvallisuus
- **I 22** Salassa pidettävien tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä - Etäkäyttö ja etähallinta
- **I 23** Tietojenkäsittelyympäristön suojaus koko elinkaaren ajan - Ohjelmistohaavoittuvuuksien hallinta
- **I 24** Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - varmuuskopiointi

Taulukko 4. Teknisen tietoturvallisuuden vaatimukset (Katakri 2015, 30-65)

## 4.7 Kunnossapidon osaamisvaatimukset

Kunnossapito-organisaation asiantuntijoiden osaamiseen liittyvät vaatimukset ovat Katakri-vaatimusten mukaisia. Kriteeristö sisältää monia vaatimuksia eri tietoturvallisuustasoille, joita voidaan ottaa käyttöön organisaatioiden ja työpaikkojen eri toiminnoissa, jotka käsittelevät viranomaisen salassa pidettävää tietoa tai haluavat toimia muuten turvallisesti ja parantaa kybersietoisuuttaan kybervaikuttamista vastaan. Kunnossapito-organisaation kybersaamisen todentamiseksi valittiin ne vaatimukset, jotka koettiin turvallisuuden kannalta tärkeimmiksi vaatimuksiksi. Ne ovat myös lähimpänä käytännön asiantuntijatyön konkreettista tekemistä.

Opinnäytetyön toimeksiantajan kunnossapitohenkilöstö työskentelee jatkuvasti arkaluontoisten materiaalien ja laitteistojen parissa, joten fyysisen ja sähköisen materiaalin käsittelyyn sekä järjestelmien palautettavuuteen liittyvät toimintatavat on tunnettava turvallisuuden ja kybersietoisuuden säilyttämiseksi kybertoimintaympäristössä ja fyysisillä toimipisteillä. Organisaatioon liittyviä Katakri-vaatimuksia osaamisen suhteen on otettava mukaan, jotta toimipaikkakohtaisten organisaatioiden vertailu mahdollistuu.

Kunnossapito-organisaation asiantuntijan kybersietoisuuteen liittyvät osaamisvaatimukset sekä niihin liittyvät avainsanat listattuna: (Katakri 2015, 6-56)

- T 03 - Turvallisuustyön resurssit, Organisaatiolla on riittävä asiantuntemus, jotta tietoturvallisuustyön (kybersietoisuus) tarkoitus toteutuu.
    - Oma asiantuntemus
    - Organisaation asiantuntemus
    - Kontaktit

- F 03 - Tietojen fyysiseen suojaukseen tarkoitetut turvallisuusjärjestelmät ja laitteet, Tietojen säilömiseen tarkoitetut kassakaapit ovat tiedossa ja niitä osataan käyttää.
    - Kassakaappi
    - Kulkuoikeudet

- F 05 - Avainten ja numeroyhdistelmien hallinta, Avaintunnisteet ovat ainoastaan niiden henkilöiden käytössä, jotka niitä tarvitsevat. Alkuperäistunnisteet vaihdetaan poikkeuksetta.

    - Avaimet
    - Numeroyhdistelmät
    - Alkuperäisasetukset ja -salasanat/tunnukset

- F 08 - Toiminnan jatkuvuuden varmistaminen, Merkittävillä häiriötilanteilla ja poikkeustilanteilla ei saa olla vaikutusta salassa pidettävien tietojen käsittelyyn tai säilyttämiseen.
    - Tiedon palautettavuus
    - Tiedon suojaaminen poikkeustilanteessa

- I 06 - Vähempien oikeuksien periaate - Pääsyoikeuksien hallinnointi, Oikeudet ainoastaan niitä työssään tarvitseville.
    - Oikeuksien hallinnointi

- I 08 - Vähimäistoimintojen ja vähempien oikeuksien periaate - Järjestelmäkovennus, Käytössä ainoastaan työssä tarvittavat ohjelmistot.
    - Rajoitetut oikeudet
    - Rajoitetut toiminnallisuudet
    - Rajoitetut ohjelmistot

- I 09 - Monitasoinen suojaaminen - Haittaohjelmasuojaus, Työvälineissä oltava asianmukainen haittaohjelmasuojaus ennaltaehkäisyyn, estämiseen, havainnointiin, vastustuskykyyn sekä tilanteen korjaamiseen.
    - Haittaohjelmasuojaus
    - Virustorjunta
    - Oudon toiminnallisuuden havainnointi
    - Vastustuskyvyn lisääminen
    - Tilanteen korjaaminen
    - Ennaltaehkäisy

- I 11 - Monitasoinen suojaaminen - Poikkeamien havainnointikyky ja toteaminen, Pyritään havaitsemaan mahdollinen poikkeama tai hyökkäys sekä rajoittamaan ja torjumaan sen aiheuttamaa vahinkoa ja palautumaan tilanteesta lähtöpisteeseen.

- Poikkeamien tunnistaminen
- Hyökkäyksen tunnistaminen
- Haitan rajaaminen
- Palautettavuus

- I 23 - Tietojenkäsittely ympäristön suojaus koko elinkaaren ajan - Ojelmistohaavoittuvuuksien hallinta, Järjestelmien koko elinkaaren ajalle toteutettu luotettava menettely ohjelmisto-/laitehaavoittuvuuksien hallitsemiseksi.
    - Ohjelmistohaavoittuvuuksien tunnistaminen
    - Ohjelmistohaavoittuvuuksien seuranta

- I 24 - Tietojenkäsittely ympäristön suojaus koko elinkaaren ajan - Varmuuskopiointi, Salassa pidettävää tietoa sisältävät varmuuskopiot suojataan vähintään vastaavan tasoisilla menetelmillä kuin alkuperäinen tieto.
    - Varmuuskopiointi
    - Järjestelmien palautettavuus
    - Tiedon salaaminen

# 5 TUTKIMUKSEN TOTEUTTAMINEN KYSELYTUTKIMUKSENA

## 5.1 Tutkimusongelma ja kohderyhmä

Opinnäytetyön pääasiallinen tutkimusongelma oli kunnossapitotöissä työskentelevien järjestelmäinsinöörien osaaminen ja sen taso kybersietoisuuden näkökulmasta. Tutkimustehtävänä oli selvittää toimipaikkojen kunnossapito-organisaation kyberosaamisen nykytila haastattelututkimuksen avulla, jolla saatiin vastaus tutkimusongelmaan. Haastattelussa painotettiin kunnossapidon kybersietoisuuteen liittyviä asiakohtia, koska osaamisrakenne ei ollut täysin selvillä yrityksen eri toimipaikkojen välillä. Puolistrukturoitu haastattelu soveltui parhaiten tämän tyyppiseen osaamisen kartoittamiseen, sillä haastattelun alustukseksi tarkoitettu teksti ja siihen yhdistetyt kysymykset auttoivat haastateltavaa hahmottamaan, mitä osaamista kysymyksien vastauksilla pyrittiin tuomaan esille. Puolistrukturoitu haastattelu antoi myös sopivasti liikkumatilaa haastattelutilanteessa, jolloin siitä ei tullut liian kaavamainen. Haastattelussa esitettyjen kysymysten tarkoituksena oli tuoda esille turvallisuusjohtamiseen, fyysiseen- sekä tietotekniseen turvallisuuteen liittyvää osaamista, jotka liittyivät edellisessä kappaleessa 4.3 esitettyihin osaamisen vaatimuksiin.

Haastattelukysymysten vastauksien avulla pyrittiin myös selvittämään kyberosaamisen jakautuminen toimipaikkojen välillä. Kun yrityksen kokonaisvaltainen osaamisen taso ja sijainti saatiin selvitettyä, pystyttiin palveluiden tuottamisen ja ongelmatilanteiden ratkaisemisen kannalta kontaktoitua oikea organisaatio tai henkilö. Tulevaisuuden kannalta oli siis tärkeää tietää osaamisen sijoittuminen, jotta palveluiden tuottaminen asiakkaalle olisi mahdollisimman helppoa ja ongelmien ratkaisu nopeaa tulevaisuudessa. Osaamiskartoituksen perusteella pystyttiin myös selvittämään, minkälaisia palveluita pystytään tuottamaan milläkin toimipaikalla itsenäisesti. Lisäksi voitiin arvioida mahdollinen tukeutumistarve muiden paikkakuntien organisaatioihin.

**Tutkimuksen kohderyhmä**

Tutkimuksen kohderyhmäksi valikoitui kunnossapito-organisaation käytännön kunnossapitotöistä vastaavat järjestelmäinsinöörit. Insinöörit toimivat omien järjestelmiensä kunnossapidon vastuuhenkilöinä ja omaavat parhaan käytännön osaamisen järjestelmien kunnossapitoon liittyen. Järjestelmien tekninen osaaminen on avainasemassa, kun

mietitään kunnossapitoon liittyviä toimintatapoja kybersietoisuuden näkökulmasta. Kun kunnossapidosta vastaavat henkilöt tunnistavat omien järjestelmiensä liityntäpinnat turvallisuusjohtamiseen, fyysiseen- sekä tietoturvallisuuteen, saadaan kunnossapitotoiminnalle luotua mahdollisimman turvalliset toimintatavat ja prosessit. Järjestelmäinsinöörien osaaminen on myös avainasemassa uusien palveluiden suunnittelun ja niiden jalkauttamisen näkökulmasta. Kun organisaatioiden asiantuntemuksen taso on tiedossa, pystytään palvelukokonaisuudet ja suorituksen ohjaaminen toteuttamaan helpommin.

**Tutkimusaineiston keruu**

Kunnossapito-organisaatioiden kyberosaamista kartoittavaan tutkimukseen tarvittava aineisto kerättiin puolistrukturoidun haastattelun avulla. Haastattelutilaisuudessa järjestelmien kunnossapitotöistä vastaaville järjestelmäinsinööreille annettiin tutustuttavaksi liitteessä 1 oleva haastattelun alustus teksti. Tekstin tarkoituksena oli ohjata haastateltavaa ajattelemaan tietyllä tavalla, jotta liitteessä 2. esitettyihin kysymyksiin saatiin mahdollisimman laajat, sekä sisällöltään oikeansuuntaiset vastaukset liittyen kyberturvallisuuteen, kybersietoisuuteen sekä organisaation toimintaan.

Ohjaamisen tarkoituksena ei ollut antaa haastateltavalle valmiita vastauksia, vaan kertoa minkälaista osaamista haastattelulla kartoitettiin. Haastattelutilaisuuden aikana haastattelija kirjasi lyhyitä muistiinpanoja haastateltavan vastauksista liittyen kuhunkin kysymykseen. Muistiinpanoja tehdessä tuli keskittyä tuottamaan oleellista sisältöä. Tärkeintä oli kirjata ne vastaukset muistiin, kun haastateltava mainitsi asian, joka liittyi johonkin kymmenestä osaamisvaatimuksesta. Näin muistiinpanot olivat sisällöltään oikeita ja niistä saatiin myös jälkikäteen dokumentoitua osaamiseen liittyvää tietoa. Muistiinpanoja tehtäessä ja tulosten raportoinnissa tuli myös ottaa huomioon, että kenenkään yksityisyyttä tai ammattisalaisuuksia vaarannettu. (Anita Saarinen-Kauppinen & Anna Puusniekka 2009, 65-68 ; Heikkilä 2008, 32)

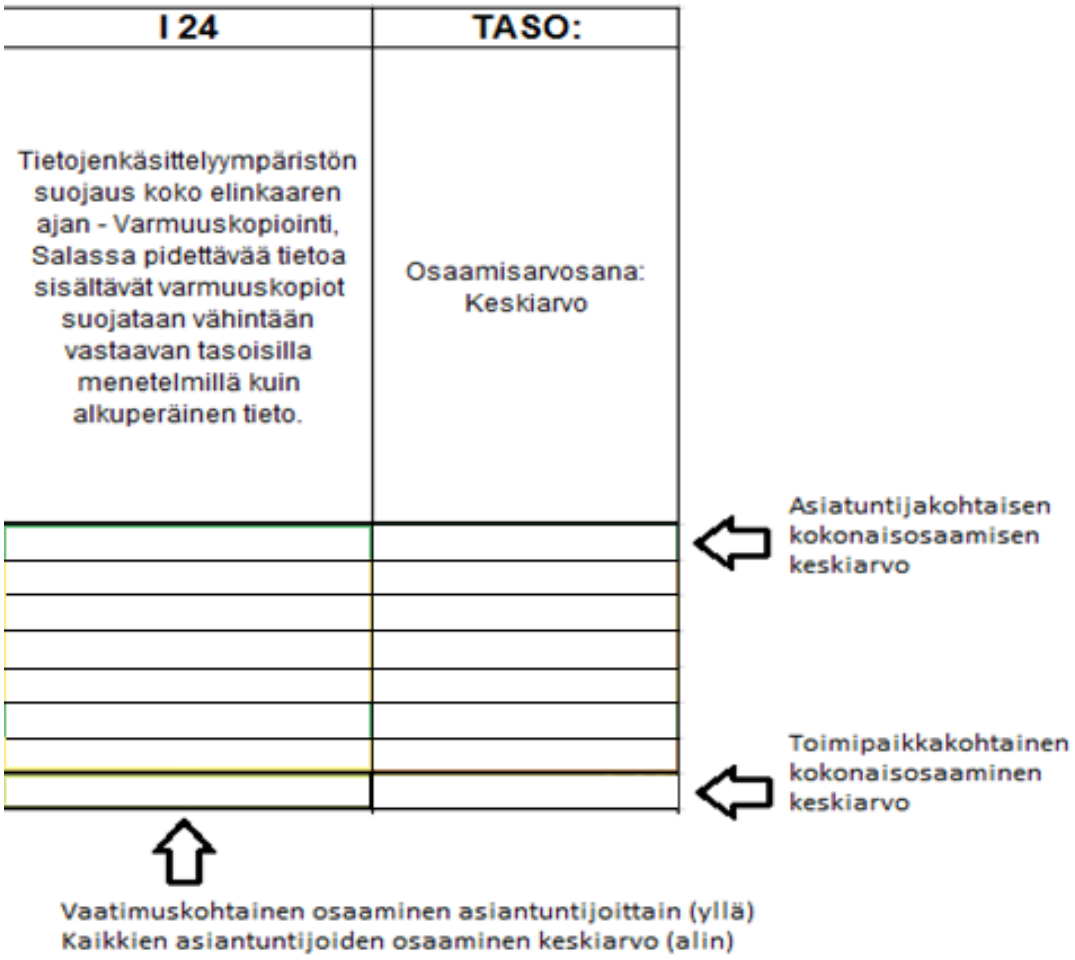
## 5.2 Osaamismatriisin laadinta

Haastatteluiden jälkeen muistiinpanot dokumentoitiin sekä analysoitiin ja niistä saatu tieto siirrettiin osaamismatriisiin, joka helpottaa ja visualisoi osaamistasoja paikkakuntakohtaisesti. Kyberosaamista koskeva osaamismatriisi, joka esitetään liitteessä 3, rakentuu kymmenen osaamisvaatimuksen ympärille siten, että kunnossapidon järjestelmäin-

sinööreiltä kerätty tieto kybersietoisuuden substanssiosaamisesta omalta ja organisaatiotasolta pisteytetään kunkin vaatimuksen kohdalle numeraalisin arvosanoin 0-3 seuraavasti:

0. Ei osaamista
1. Vähäinen osaaminen (ymmärtää mistä kyberturvallisuudessa on kysymys)
2. Perusosaaminen (tuntee kyberturvallisuuden termistön ja toimintamallit)
3. Hyvä osaaminen (pystyy ohjeistamaan muita ja kehittämään toimintaa)

Kuviossa 12 havainnollistetaan vaatimusmatriisin kohtaa I 24 ensimmäisen toimipaikan osalta. Kuvassa esitetään myös yksittäisten solujen kuvaukset mitä solussa olevalla numeraalisella arvolla tarkoitetaan.




Kuvio 12. Vaatimuksen I 24 osaaminen ja solujen kuvaukset

Vaatimuksen hyvän osaamisen (3) omaava henkilö pystyy ohjeistamaan muita ja kehittämään kunnossapito-organisaation toimintaa kybersietoisuuden näkökulmasta. Henkilö

ymmärtää avainkohdat ja kyberturvallisuuteen vaikuttavat tekijät turvallisuusjohtamisen, fyysisen- sekä tietoteknisen turvallisuuden näkökulmista ja osaa soveltaa näitä käytännön työhönsä. Henkilön osaaminen näkyy hänen turvaluokitellun materiaalin käsittelyssä, laitteiden sekä järjestelmäkokonaisuuksien käyttämisessä ja päivittämisessä, jatkuvuuden hallinnassa sekä vanhentuneen tiedon sekä kaluston hävittämisessä. Tällaiset henkilöt ovat organisaatiolle tärkeitä, koska heidän avullaan kunnossapitotoiminnan kehittäminen onnistuu sisäisien toimenpiteiden avulla.

Vaatimuksen perustason osaamisella (2) henkilö tunnistaa osan kyberturvallisuuteen ja kybersietoisuuteen liittyvistä termeistä ja ymmärtää niiden liityntäpisteet työhönsä. Perustasolla henkilö pystyy toimimaan turvallisesti kaikilla vaatimusten osa-alueilla selkeiden ohjeiden ja toimintamallien avulla, sekä kehittämään osaamistaan muiden tuella. Osaamisessa saattaa olla pieniä puutteita, jotka liittyvät fyysiseen turvallisuuteen, järjestelmien palautettavuuteen, järjestelmien turvalliseen hallintaan, järjestelmäkovennuksiin sekä pääsyoikeuksien hallintaan. Perustason osaamisen omaava henkilö on koulutettavissa hyvän osaamisen tasolle yrityksen sisäisten koulutusten ja kybersietoisuutta käsittelevien materiaalien avulla.

Vaatimuksen vähäisen osaamisen (1) omaava henkilö ymmärtää mistä kyberturvallisuudessa on kysymys, mutta ei hahmota kaikkia rajapintoja joihin se liittyy. Varsinkin kybersietoisuudesta puhuttaessa, henkilöllä on vaikeuksia hahmottaa mistä on kysymys. Henkilöllä voi olla osaamispuutteita myös tietoteknisten taitojen perusteissa, jolloin järjestelmäteknisen kokonaiskuvan hahmottaminen voi olla hankalaa. Henkilö tarvitsee jatkuvasti tukea toimiakseen turvallisesti lähes kaikilla osaamisvaatimusten osa-alueilla.

Jos henkilöllä ei ole lainkaan osaamista (0) vaatimuksesta, hän ei ymmärrä mistä on kysymys, kun puhutaan kyberturvallisuudesta, jatkuvuudenhallinnasta, palautettavuudesta, pääsyoikeuksien hallinnasta tai tiedon turvallisesta hävittämisestä. Kybersietoisuuden määritelmä ja sana ovat hänelle vieraita. Henkilöllä on myös suuria puutteita tietoteknisten laitteiden peruskäytössä ja yleisessä teknisessä osaamisessa.

# 6 TUTKIMUKSEN TULOKSET

Toimipaikkojen haastattelukierrokset suoritettiin marraskuun 2020 ja tammikuun 2021 välisenä aikana. Haastattelut toteutettiin kahdenkeskisinä tilaisuuksina, jotka alustettiin liitteessä 1 olevalla haastattelun alustuksella, jonka järjestelmäinsinöörit saivat luettavaksi ennen haastattelutilaisuutta. Haastateltujen järjestelmäinsinöörien kunnossapitovastuulla oli teknisiltä ominaisuuksiltaan erilaisia järjestelmiä ja laitteita kolmella eri toimipaikalla. Haastatteluihin valikoiduille järjestelmäinsinööreille esitettiin liitteessä 2 olevat kysymykset vaihtelevassa järjestyksessä haastattelutilanteen mukaisesti. Haastattelutilanteet kestivät ajallisesti noin 10-30 minuuttia. Haastattelun kestoon vaikutti pääsääntöisesti järjestelmäinsinöörin osaaminen kyberturvallisuuden ja kybersietoisuuden osa-alueilta, vastuujärjetelmän teknisyys sekä kyky hahmottaa organisaatio laajempana kokonaisuutena, joka ylittää toimialat ja toimipaikat.

Haastattelun kybersietoisuuteen keskittyvässä osuudessa järjestelmäinsinööreiltä kysyttiin yleisiä asioita huoltojärjestelmien kybersietoisuudesta, sen toteuttamisesta, parantamisesta sekä oman kyberosaamisensa tasosta. Vastauksien joukosta poimittiin avainsanoja eri osaamisalueista, jotka liittyivät kappaleessa 4.3 esitettyihin kunnossapidon osaamisvaatimuksiin turvallisuusjohtamisen, fyysisten- sekä tietoteknisen turvallisuuden osalta. Organisaatiota koskevien kysymysten osalta haettiin tietoa ja näkemyksiä organisaation osaamisen tasosta, sen kehittämisestä asiakaslähtöisesti sekä mahdollisten tulevan koulutusten sisällöstä.

## 6.1 Haastattelun tulkinta toimipaikka 1

Toimipaikalla 1 haastateltiin yhteensä seitsemää järjestelmäinsinööriä. Haastateltavien organisaatiotason kyberosaaminen turvallisuusjohtamiseen liittyvän vaatimuksen T 03 osalta oli haastattelun perusteella hyvällä tasolla. Hyvä taso saavutettiin, kun suurin osa järjestelmäinsinööreistä tunnisti oman kompetenssivajeensa ja osasi kontaktoida omassa organisaatiossa tai toisella toimipaikalla työskentelevän paremman kyberosaamisen omaavan asiantuntijan. Korkeamman osaamistason omaavalta henkilöltä voidaan varmistaa, onko oma toimintamalli ja -tapa oikea, jos kohdataan mahdollinen kyberturvallisuuteen vaikuttava tekijä tai uhka.

Fyysisen turvallisuuden vaatimusten F 03, F 05 ja F 08 osalta osaamisessa oli hieman enemmän hajontaa verrattuna turvallisuusjohtamisen vaatimukseen. Fyysisen turvallisuuden vaatimukset keskittyvät enemmän käytännön työhön ja proseduureihin, joten oman osaamisen taso korostui kysymysten vastauksissa. Tietojen fyysiseen suojaamiseen tarkoitetut turvajärjestelmät ja laitteet tunnettiin ja niitä osattiin käyttää kiitettävästi. Haasteita osaamisen näkökulmasta oli pääsyoikeuksien hallinnalla, sillä fyysisen pääsyoikeuden ja sen rajaamisen tärkeyttä ei osattu tuoda esille. Organisaation ollessa suhteellisen pieni, oli kuitenkin tärkeää, että tarvittava tieto oli saatavilla ja järjestelmään pääsy mahdollista, jos sitä töiden suorittamiseksi tarvittiin. Näin ollen muiden toimintamallien ollessa kunnossa, osaamisvajeesta ei aiheutunut riskejä suojattavan tiedon osalta, koska tiedettiin missä tieto sijaitsee ja kuka siihen pääsi käsiksi. Osaaminen, joka liittyi toiminnan ja töiden jatkuvuuteen suojattavan materiaalin osalta poikkeustilanteessa oli organisaatiossa kohtalaisella tasolla. Infraan liittyvät fyysiset poikkeustilanteet kuten sähkökatkot ja palohälytykset sekä toiminta niiden aikana oli hyvin ohjeistettu ja järjestelmäinsinöörien tiedossa.

Teknisten tietoturvallisuusvaatimusten I 06, I 08, I 09, I 11, I 23 ja I 24 osalta osaaminen jakautui enemmän kuin fyysisten turvallisuusvaatimusten osaaminen. Tietotekninen osaaminen oli sitä parempaa, mitä teknisemmän järjestelmän kunnossapidosta vastaavaa insinööriä haastateltiin. Vähempien oikeuksien periaate, joka liittyi työssä käytössä olevien tietokoneiden käyttäjienhallintaan ja käyttöoikeuksiin, oli organisaatiossa hyvin tiedossa. Suurin osa järjestelmäinsinööreistä osasi ja tiedosti työssä käytössä olevien tietokoneiden ja erilaisten siirrettävien medioiden, kuten muistitikkujen ja kiintolevyjen aiheuttamat tietoturvallisuusriskit. Tietoverkkoihin liittyvät proseduurit tunnistettiin myös kohtuullisen hyvin. Useampi haastateltava mainitsi, että huoltotyössä käytettäviä tietokoneita ei tulisi liittää osaksi julkista verkkoa tietoturvariskien vuoksi. Moni mainitsi myös, että ulkoisen vaikuttamisen mahdollisuudet tulee minimoida omien toimintamallien avulla, kun käytännön työtä tehdään.

Laitetasolle mentäessä osaamisessa oli hajontaa huomattavasti enemmän. Laitetason avainosaamiset liittyvät järjestelmäkovennuksiin huoltokäytössä olevien tietokoneiden ja niiden ohjelmistojen osalta. Jotkin haastateltavat tunnistivat ongelman, joka liittyy kaupallisten laitteiden kovennuspuutteisiin ohjelmistojen ja laitteiden elektroniikan osalta. Esimerkiksi kaikissa kaupallisissa tietokonemalleissa ei ole fyysistä kytkintä, jolla langattomat verkkosovittimet saa kytkettyä pois päältä. Harva järjestelmäinsinööri osasi mainita asioita, jotka liittyvät haittaohjelmasuojaukseen (virustorjunta), ennaltaehkäisyyn,

estämiseen, havainnointiin, vastustuskykyyn (sietoisuus), poikkeamiin järjestelmien toiminnassa tai tilanteiden ja poikkeamien korjaamiseen. Myös ohjelmistohaavoittuvuuksiin ja niiden aiheuttamiin riskeihin liittyviä asioita ei tuotu haastattelutilanteessa juurikaan esiin. Ohjelmistohaavoittuvuus terminä tiedostettiin, mutta sen vaatimat toimenpiteet jäävät usealta mainitsematta. Huoltojärjestelmien redundanttisuuteen, palautettavuuteen sekä järjestelmissä olevan tiedon suojaamiseen osattiin ottaa kantaa kohtuullisen hyvin. Tilaisuuden yhteydessä esitettiin myös joitain kehitysehdotuksia huoltotoimintojen palautettavuuden varmistamisen parantamiseksi.

## 6.2 Haastattelun tulkinta toimipaikka 2

Toimipaikalla 2 haastattelutilaisuuksiin saatiin osallistettua kolme järjestelmäinsinööriä. Toimipaikka 2 oli haastatteluun osallistuvista toimipaikoista pienin ja siellä työskenteli toimipaikoista vähiten ihmisiä. Kokonaisuuteen nähden pienelläkin haastatteluotoksella saatiin hyvä kuva toimipaikan kokoanisosaamisesta.

Turvallisuusjohtamiseen liittyvän T 03 vaatimuksen osalta toimipaikan osaamistaso oli hyvä. Toimipaikalla työskentelevillä järjestelmäinsinööreillä oli selkeä kuva, kenellä organisaatiossa oli tarvittava kyberosaaminen, jos oma osaamistaso ei riittänyt tilanteen tai poikkeaman selvittämiseen. Toimipaikan 2 osalta etuna oli myös järjestelmäinsinöörien lyhyt fyysinen etäisyys toisistaan, joka madalsi kynnystä kontaktoida toinen henkilö.

Fyysisen turvallisuuden vaatimusten F 03, F 05 ja F 08 osalta osaamisen taso ei poikennut toimipaikkaan 1 verrattuna. Fyysiseen turvallisuuteen liittyvät tiedon turvalliseen säilyttämiseen liittyvät toimenpiteet ja menetelmät tunnettiin pääsääntöisesti hyvin. Järjestelmäinsinöörit joiden kunnossapitovastuulla oli enemmän tietotekniikkaa ja tiedon turvallista käsittelyä vaativia järjestelmiä ja materiaaleja, tunnistivat kyberturvallisuuteen ja -sietoisuuteen liittyvät asiat paremmin kuin ne, joiden järjestelmät eivät sisältäneet teknisiä laitteita. Yleisesti toimipaikan organisaation ollessa hyvin pieni, fyysiseen turvallisuuteen liittyvät seikat ovat helpommin hallittavissa ja näin ollen mahdolliset poikkeamat oli helpompi tunnistaa.

Tietoteknisiin vaatimuksiin pureuduttaessa, oli vastauksista huomattavissa selvästi järjestelmäinsinöörien kunnossapitovastuulla olevien laitteiden teknisyys. Pääsyoikeuksien hallinnointi, järjestelmien kovennukset, haittaohjelmasuojaukset ja poikkeamien havainnointi sekä tunnistaminen olivat hallussa niillä järjestelmäinsinööreillä, joiden vastuulla

oli teknisiä laitteita ja sähköistä materiaalia. Sama kuvio toistui laitehaavoittuvuuksien ja laitteiden elinkaaren hallinnan osalta. Teknisten tietoturvallisuusvaatimusten I 06, I 08, I 09, I 11, I 23 ja I 24 osalta osaaminen toimipaikan 2 osalta oli kokonaisuudessaan hyvällä tasolla.

### 6.3 Haastattelun tulkinta toimipaikka 3

Toimipaikalla 3 haastateltiin kaikkiaan kuutta järjestelmäinsinööriä. Toimipaikka 3 oli haastatteluun osallistuneista toimipaikoista eniten kyberorjentoitunut. Tämä näkyi selvästi tutkimuskysymyksiin vastaamisessa, sillä vastauksia ja mielipiteitä kyberturvallisuuteen ja kybersietoisuuteen tuli todella nopeasti ja kattavasti kysymyksen esittämisen jälkeen. Toimipaikka 3 oli myös osallistuvista toimipaikoista suurin. Tämän vuoksi haastatteluun valikoitiin ainoastaan ne järjestelmäinsinöörit, joiden kunnossapitovastuulla olevat järjestelmät sisälsivät kyberturvallisuuden ja -sietoisuuden kannalta oleellista tietotekniikkaa ja elektroniikkaa.

Turvallisuusjohtamisen vaatimuksen T 03 osalta toimipaikan osaaminen oli erinomaisella tasolla. Toimipaikan organisaatiosta löytyi monia kyberturvallisuuteen perehtyneitä asiantuntijoita, jotka olivat perillä mitä organisaation kunnossapidon kybersietoisuus tarkoittaa ja miten sen toteutumiselle luotiin parhaat edellytykset. Kolmesta toimipaikasta paras turvallisuusjohtamisen vaatimuksiin liittyvä osaaminen löytyi toimipaikalta 3.

Fyysisen turvallisuuden vaatimusten F03, F05 ja F08 osalta toimipaikan osaaminen oli myös erinomaisella tasolla. Lähes jokainen otti haastattelutilanteessa kantaa tietojen turvalliseen säilyttämiseen sekä suojaamiseen ja fyysisten pääsyoikeuksien hallintaan. Fyysiseen tilaturvallisuuteen otettiin kantaa myös prosessien ja toimintamalien osalta. Ilman oikeita toimintamalleja ei fyysinenkään turvallisuus toteudu, jos alkuperäisasetuksia ei muuteta eikä pääsyoikeuksia eri turvallisuustasoille hallita. Toimipaikalla oli kiinnitetty myös erityistä huomiota tilaturvallisuuteen.

Tietoteknisten vaatimusten osalta toimipaikan 3 osaaminen erottui huomattavasti muista. Toimipaikan 3 osalta käyttöoikeuksien hallintaan kantaa otti jokainen haastateltava. Käyttöoikeuksien oikeanlainen hallinta varmisti, että huoltojärjestelmien käyttö oli turvallista kaikkialla organisaatiossa. Järjestelmäkovennuksiin ohjelmistojen osalta osattiin myös kertoa oikeanlaisia toimenpiteitä. Haastateltavat mainitsivat toimenpiteitä, joi-

den avulla huoltojärjestelmäkovennuksia voitiin tehdä niin -ohjelmisto, kuin laitepuolellakin. Tärkeimpinä asioina pidettiin, että huoltojärjestelmiin ei kyetty asentamaan kuin ainoastaan työssä tarvittavia ohjelmistoja. Ohjelmistojen asentaminen ja hallinnointi tuli myös olla keskitettyä. Huoltojärjestelmien haittaohjelmasuojaukseen, virustorjuntaan, oudon toiminnan havainnointiin, toiminnan jatkuvaan kehitykseen, tilanteiden korjaamiseen ja ennaltaehkäisyyn osattiin myös kertoa oikeita toimenpiteitä ja kehitysmalleja. Huoltojärjestelmien palautettavuutta ja varmuuskopiointia myös korostettiin monen haastateltavan toimesta. Järjestelmäinsinöörit kertoivat myös, että maailman muuttuessa jatkuvasti tietoteknisesti eteenpäin, on tämä myös huomioitava järjestelmien kunnossapidossa ja organisaation prosesseissa. Järjestelmäinsinöörit ottivat myös kantaa erilaisiin haavoittuvuuksiin, sekä niiden kanssa elämiseen, luomalla oikeanlaiset toimintamallit niiden ympärille.

Toimipaikan 3 osaaminen liittyen vaatimuksiin I 06, I 08, I 09, I 11, I 23 ja I 24 oli kaikista kolmesta toimipaikoista paras. Järjestelmien kunnossapitoon liittyvä kyberosaaminen oli myös parhaalla tasolla, kun osaamista tarkastellaan kokonaisuutena kaikkien vaatimusten osalta.

### 6.4 Haastattelun tulkinta organisaation osalta

Kaikkien kolmen toimipaikan osalta järjestelmäinsinöörit kertoivat toimipaikkansa järjestelmien kunnossapidon kybersietoisuuden toteutuvan riittävällä tasolla, kun puhuttiin kunkin järjestelmäinsinöörin vastuulla olevasta järjestelmistä. Organisaation tasolla jotkin haastateltavat näkivät ongelmaksi sen, että toimintamallit eivät olleet kaikilla puolin organisaatiota samanlaiset ja toimintamallit saattoivat vaihdella, koska ohjeistukset olivat puutteelliset. Haastateltavat mainitsivat myös lähes yhtenäisesti erilaisista kehittämiskohteista, jotka koskivat organisaation henkilöstön kouluttamista, kunnossapidon toimintamalleja, johdon sitoutumista sekä huoltotoimenpiteissä käytettävien laitteiden ja medioiden tietoturvallisuutta ja yleistä hallintaa.

Haastateltavat totesivat myös, että uudistamalla ja kehittämällä kunnossapidon kybersietoisuutta koskevat toimintamallit ja prosessit entistä paremmiksi ja yhdenmukaiseksi yrityksen sisällä, palvelevat ne myös kaikenlaisia asiakkaita ja asiakastarpeita, kun liiketoimintaa laajennetaan uusille toimialoille. Organisaation koulutuksiin liittyvään kysymykseen vastattiin vaihtelevasti riippuen haastateltavan omasta taustasta. Pääosin järjestelmäinsinöörit toivoivat mahdollisimman käytännönläheistä koulutusta, jotta se palvelisi

mahdollisimman suurta osaa organisaation työntekijöistä. Koulutuksen ollessa mahdollisimman käytännönläheinen ja helposti ymmärrettävä, ei tekninen osaaminen korostu sisällön ymmärtämisessä. Koulutussisältö tulisi valita siten, että se olisi mahdollisimman lähellä sitä toimialaa, jossa yrityksen henkilöstö toimii. Esimerkkeinä sisällöstä haastateltavat kertoivat kybersotatyyppistä aihepiiriä ja sen teknistä puolta, miten kybervaikuttaminen voidaan välttää omalla toiminnalla ja varautumalla siihen, mitkä ovat kybervaikuttamisen uhkatekijät, yleinen katsaus laiteturvallisuudesta, medioiden käyttämisestä, haavoittuvuuksista ja niiden seuraamisesta.

### 6.5 Täytetyn osaamismatriisin tulkinta

Kvalitatiivisessa tutkimusosuudessa toteutettujen haastattelujen ja osaamisvaatimusten pohjalle rakentuneen ja täytetyn osaamismatriisin perusteella voitiin päätellä, että kaikkien kolmen toimipaikan kunnossapidon kyberosaaminen kybersietoisuuden näkökulmasta oli riittävällä tasolla. Riittävä taso ylittyy, kun kunnossapidon kybersietoisuus toteutuu ja toimintaa voidaan kehittää uusia liiketoimintoja sekä järjestelmiä silmälläpitäen. Jokaisesta organisaatiosta löytyy yksi tai useampi järjestelmäinsinööri, jonka kybersietoisuuteen liittyvä osaaminen on sillä tasolla, jotta hän kykenee ohjeistamaan organisaation muita jäseniä, joilla kyberosaaminen on alemmalla tasolla.

Kartoitetun toimipaikkakohtaisen osaamisen perusteella sekä haastatteluista kertyneen aineiston perusteella pystyttiin kirjoittamaan alustava henkilöstön osaamisen kehityssuunnitelma, joka sisälsi kybersietoisuutta koskevaa teoriaa sekä käytännön toimenpiteitä sen parantamiseksi. Organisaation osalta sen toimintamalleja sekä prosesseja tulisi myös kehittää haastattelujen perusteella suuntaan, joka palvelee organisaation kybersietoisuuden kehittymistä jatkuvasti paremmaksi. Organisaatioiden johtoa tulisi myös sitouttaa ja informoida organisaation kybersietoisten toimintamallien jalkauttamisen tärkeydestä niiden toiminnassa.

### 6.6 Tutkimuksen luotettavuus

Kaikessa tutkimustyössä ja tutkimuksissa yleisesti on syytä arvioida tutkimuksen luotettavuutta. Tutkimustyötä tehdessä pyritään välttämään virheitä, mutta se ei takaa tutkimuksen luotettavuutta ja luotettavuus voi siten vaihdella. Luotattavuustarkastelulla pyri-

tään tarkastelemaan tutkimusvaiheiden suorittamisen oikeellisuutta. Luotettavuustarkasteluun voidaan sisällyttää pohdintaa tutkimusasetannan sekä tutkimusongelman oikeellisuudesta. Lisäksi tarkastelun kohteeksi voidaan ottaa tiedonkeruuvaihe ja keinot, joilla kerättyä tietoa on analysoitu. Tutkimuksen luotettavuusarvioinnin loppuvaiheessa tulisi tarkastella tutkimuksen kokonaisuuden onnistumisastetta sisältäen osoituksen aineiston analysoinnin luotettavuudesta. Lisäksi tutkijan on syytä pohtia tutkimustuloksen ratkaisua ja sen oikeellisuutta sekä luotettavuutta. (Hirsjärvi ym. 2010, 231; Heikkilä 2008, 28—30)

Luotettavuuden mittareina käytetään tutkimuksen validiteettia ja reliabiliteettia. Luotettavuuden arvioinnit tulee suorittaa käytettävissä olevien materiaalien pojalta, joita voivat olla esimerkiksi haastattelumuistiinpanot tai sähköisesti mitattu data, joka voi olla esimerkiksi sähköinen suure kuten jännite. Tutkimuksen luotettavuuteen vaikuttavat esimerkiksi otoksen suuri koko ja edustavuus. Esimerkiksi haastattelutilanteissa otoksen koko tarkoittaa haastateltavien määrää sekä edustus erilista taustaa, ikää tai ammattiryhmää. (Kananen 2014, 256-260)

Tutkimuksen validiteetilla tarkoitetaan tutkimuksen kykyä mitata sitä, mitä oli tarkoitus mitata. Käytännössä tämä tarkoittaa tutkimuksen oikeellisuutta, valittujen mittarien ja menetelmien sopivuutta ja sitä antavatko ne oikeat tulokset sekä luotettavat vastaukset tutkimusongelmaan. Reliabiliteetti taas vastaa tulosten pysyvyyttä. Tulosten pysyvyydellä tarkoitetaan toistettavuutta, eli olisiko tutkimuksen lopputulos sama, jos se uusittaisiin. (Hirsjärvi ym. 2010 231; Kananen 2014, 258)

Tutkimuksen päätavoite oli vastata tutkimuskysymykseen: "Mikä on kunnossapito-organisaatiossa työskentelevien järjestelmien kunnossapitoinsinöörien kyberosaamisen nykytila kybersietoisuuden näkökulmasta?". Lisäksi tarkentavilla alakysymyksillä pyrittiin saamaan vastauksia liittyen osaamisen jakautumiseen toimipaikoittain ja kuinka organisaatioiden osaamista voidaan hyödyntää tulevaisuudessa. Tutkimuksen aineistonkeruumenetelmäksi pyrittiin löytämään menetelmä, joka sopii parhaiten organisaation osaamisen kartoittamiseen. Opinnäytetyön tutkimusosuuden suunnitteluvaiheessa kävi ilmi, että organisaatioiden osaamiskartoituksia on tehty ajan saatossa monia, joissa aineistonkeruumenetelmänä on käytetty ennalta suunniteltua haastattelutilaisuutta tai lomaketyyppistä kyselyä. Tämä antoi hyvät lähtökohdat tutkimusvaiheen aineistonkeruumenetelmän valinnalle, sillä menetelmien avulla oli saatu muissa organisaatioissa hyviä tulok-

sia. Opinnäytetyön tutkimusosuudessa kartoitettava osaaminen koettiin liian moniulotteiseksi ja kompleksiseksi tehtäväksi lomakketyyppisellä kyselyllä, joten aineistonkeruumenetelmänä päädyttiin käyttämään haastattelua.

Tutkimuksen empiirinen vaihe toteutettiin lopulta puolistrukturoidun haastattelun avulla. Puolistrukturoitu haastattelu kuuluu kvalitatiivisiin tutkimusmenetelmiin. Haastatteluun osallistutettiin kuusitoista järjestelmien kunnossapidosta vastaavaa järjestelmäinsinööriä kolmelta eri paikkakunnalta. Kohderyhmäksi valikoituivat ne henkilöt, joilla oli paras osaaminen järjestelmien kunnossapitoon ja tekniikkaan liittyen. Kaikilla haastatteluun osallistuneilla henkilöillä oli myös vähintään AMK-tasoinen insinöörin tutkinto ja vuosien työkokemus alaltaan. Näin ollen haastatteluihin osallistuneiden henkilöiden osaamisen voitiin olettaa olevan parhaalla tasolla yrityksen laajuisesti. Haastattelutilaisuuksiin kysyttiin alun perin yhdeksäätoista henkilöä. Haastattelujen lopulliseksi osallistumisprosentiksi saatiin 84%. Tutkimuksen validiteettia tarkastellessa voidaan päätellä, että tutkimusongelmaan löydettiin ratkaisu käytetyillä tutkimusmenetelmillä. Työn alussa esitettyihin tutkimuskysymyksiin saatiin myös kauttaaltaan kattavat vastaukset, jotka ovat tulkittavissa täytetystä osaamismatriisista. Tutkimuksesta saatujen tulosten valossa voidaan kokonaisuudessaan päätellä, että asetetut tavoitteet täyttyivät. Tutkimustavoitteiden täyttyminen vahvistaa, että tutkimusasetanta oli asetettu oikein sekä tutkimusmenetelmät, sisältäen tiedonkeruu- sekä analysointimenettelyt suoritettiin oikein ja tavoitteiden mukaisesti.

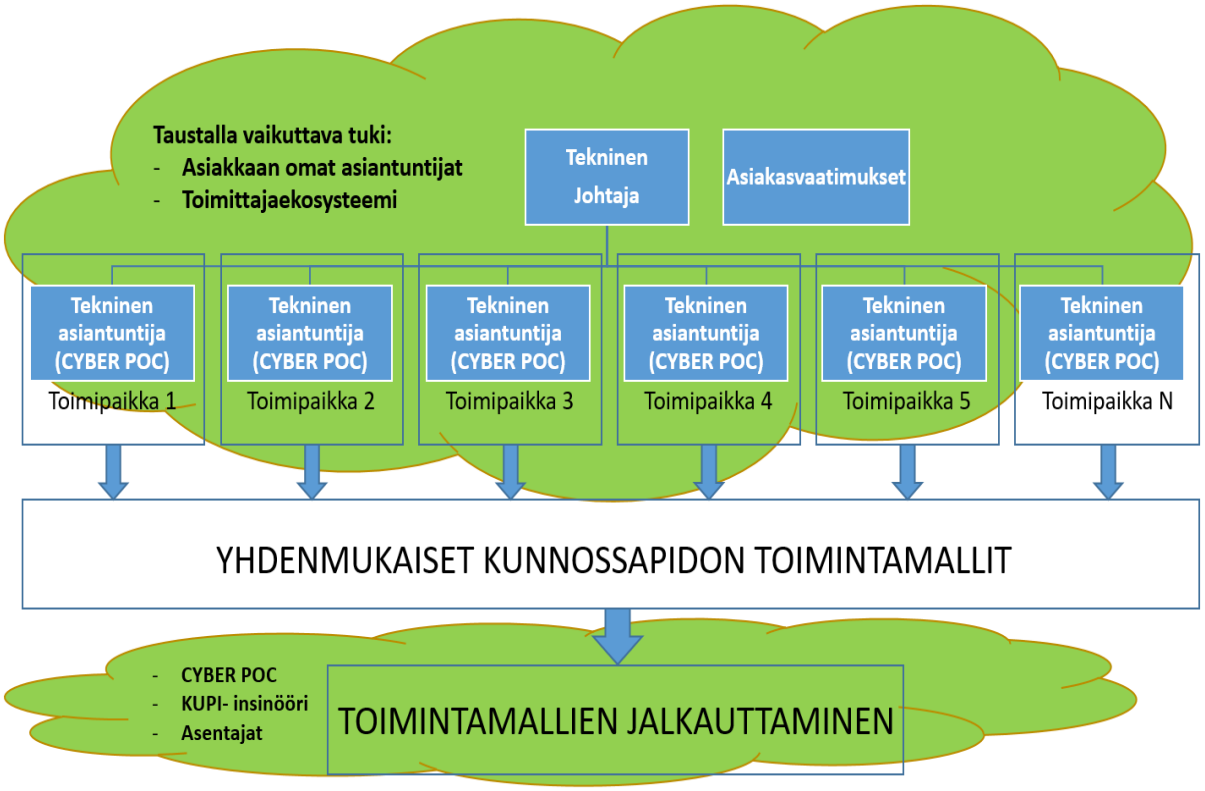
Tutkimus toteutettiin kokonaisuudessaan onnistuneesti ja tutkimuksessa kertynyt aineisto saatiin analysoitua hyvin. Tutkimuksen luotettavuuteen vaikuttavia tekijöitä löytyi haastattelukysymysten asettelusta, avainsanojen asetannasta sekä itse haastattelutilanteesta. Haastattelukysymykset pyrittiin asettamaan siten, että ne kattaisivat kokonaisuudessaan asiat, jotka liittyivät tässä opinnäytetyössä esitettyihin kyberosaamisen vaatimuksiin henkilöstön ja organisaation osalta. Kysymysten ollessa laajoja ja kyselyyn osallistuvien asiantuntijoiden tekninen osaamistaso keskivertoa korkeampi, oletettiin avainsanojen ja haastattelumuistiinpanojen välillä vallitsevan suoraviivainen yhteys. Tutkimuksen edetessä oli huomattavissa, että korkeamman osaamistason omaava ja teknisesti edistyneestä järjestelmästä vastaava henkilö mainitsi useampia avainsanoja kuin henkilö, jolla osaaminen sekä vastuujärjestelmän teknisyys olivat matalammalla tasolla. Edellä mainitun perusteella voidaan todeta kysymysten asettelun olleen oikea suhteessa asetettuihin vaatimusten avainsanoihin.

Haastattelutilanteiden osalta tutkimuksen luotettavuuteen saattoi vaikuttaa itse tilanne ja haastateltavan sen hetkinen mielentila. Haastattelutilanteessa kybersietoisuuteen liittyviä asioita saattoi jäädä tarkoituksettomasti sanomatta ja täten kysymyksen vastaus jäi haastateltavan osalta vajaaksi. Näin ollen joitain avainsanoja jäi mahdollisesti puuttumaan haastattelumuistiinpanoista. Avainsanojen puuttuminen taas vaikutti suoraan osaamisen arviointiin. Näin ollen tahaton unohdus vaikutti arviointiin alentavasti. Kokonaisuuden kannalta yksittäiset unohdukset eivät kuitenkaan vaikuttaneet lopputuotokseen merkittävästi. Vaikka tutkimuksen lopussa tehty osaamisen taulukointi olisikin tehty liian kriittisesti, ei sillä ollut lopputulokseen huonontavaa vaikutusta, koska osaamiskartoituksen pohjalta tuotettiin organisaatiolle kyberosaamista ja kybersietoisuutta koskeva koulutussuunnitelma. Jos osaaminen oli haastattelujen perusteella arvioitu liian vähäiseksi, tuli koulutussuunnitelmasta mahdollisten vajaiden vastausten perusteella sisällöltään kattavampi, koska osaaminen arvioitiin alemmalle tasolle, kuin se todellisuudessa oli.

Tutkimuksen reliabiliteetin osalta tutkimus olisi todennäköisimmin suurimmilta osin toistettava, jos haastatteluun osallistutetaan samat henkilöt ja osaamisen vaatimukset, sekä avainsanat pidetään muuttumattomina. Toistettavuuteen mahdollisesti vaikuttavia tekijöitä olisivat haastattelutilanteen muutokset sekä haastateltavan sen hetkinen vireystila.

# 7 OSAAMISEN KEHITTÄMINEN

Osaamisen kehittämisen lähtökohtana oli luoda suunnitelma, jolla pyritään kehittämään henkilöstön kyberosaamista etenkin kunnossapidon kybersietoisuuden näkökulmasta. Järjestelmäinsinöörien haastatteluista kertyneen materiaalin perusteella osaamisen kehittäminen on syytä aloittaa siitä, että huolto-organisaation toimintamallit ja ohjeistukset ovat kauttaaltaan samanlaiset, kun työskennellään teknisten järjestelmien tai salassa pidettävien materiaalien parissa. Organisaation yhdenmukaisen toiminnan kannalta on tärkeää, että järjestelmien ja organisaatioiden kyberturvallisuuteen liittyviä asioita hallittaisiin ja johdettaisiin kuvion 13 mukaisesti. Kuvion 13 matriisimallinen kyberorganisaatio on pyritty kuvaamaan mahdollisimman matalaksi, jotta tiedon kulku ja kommunikointi olisi yksilöille helpompaa, kun sitä verrataan nykyiseen toimintaympäristöön, joka on kehittynyt pitkälti linjaorganisaation mukaisesti. Keskitetty ja matriisiorganisaatiomallin mukaisesti toimiva kyberorganisaatio olisi kyvykäs tuottamaan yhdenmukaiset toimintamallit koko yrityksen laajuisesti.




Kuvio 13. Kyberorganisaatio toiminnan kehittäjänä

Käytännössä toimintamallin raamit tulisivat joko mahdollisista asiakasvaatimuksista tai ne määriteltäisiin tapauskohtaisesti teknisen johtajan sekä taustalla toimivien asiantuntijoiden ja asiakkaiden toimesta. Toimintamallin raamittamisen jälkeen toimipaikoilla työskentelevät kyber POC:t sovittavat erilaiset järjestelmät raamiin ja määrittelevät huoltotoimintaan liittyvät kyberturvallisuuteen vaikuttavat tekijät yhteistyössä asiakkaiden ja muun tukiverkoston kanssa. Toimintamallien jalkauttaminen tehtäisiin yhdessä järjestelmän kunnossapidosta vastaavan järjestelmäinsinöörin kanssa. Mahdollisuuksien mukaan jalkauttamiseen voidaan osallistuttaa myös organisaatiossa työskenteleviä käytännön töitä tekeviä asentajia. Tässä vaiheessa määriteltäisiin ne huoltotoimenpiteet ja toimintamallit, jotka liittyvät järjestelmän määräaikaishuoltoihin ja yleiseen kunnossapitoon.

Tutkimusvaiheessa kertyneestä materiaalista pystyttiin erittelemään monia erilaisia lisätoimenpiteitä nykyisten huoltotoimenpiteiden tueksi ja entistä kybersietoisemman huoltotoiminnan rakentamiseksi. Jokaisella toimipaikalla vähintään yksi järjestelmäinsinööri korosti yhdenmukaisten toimintamallien tärkeyttä. Järjestelmäinsinööri toimipaikalta 3 kommentoi seuraavasti: "Prosessit ja järjestelmät kuntoon, laitteisto- ja ohjelmistopuolen kovennukset kuntoon, ei vanhoja huoltokoneita käytössä ja kaikki huollon koneet yhteen kiertopooliin yrityksen laajuisesti". Toimipaikalla 1 työskentelevä järjestelmäinsinööri kommentoi: "Yrityksellä tulisi olla yhdenmukainen malli kaikille toiminnoille, nyt sellaista ei ole saatavilla". Haastattelumateriaalista pystyttiin koostamaan edellä mainittujen esimerkkien avulla kattava lista huoltotoimien yhteydessä tehtävistä esimerkkitoimenpiteistä kyberturvallisuuden ja -sietoisuuden varmistamiseksi kaikilla toimipaikoilla:

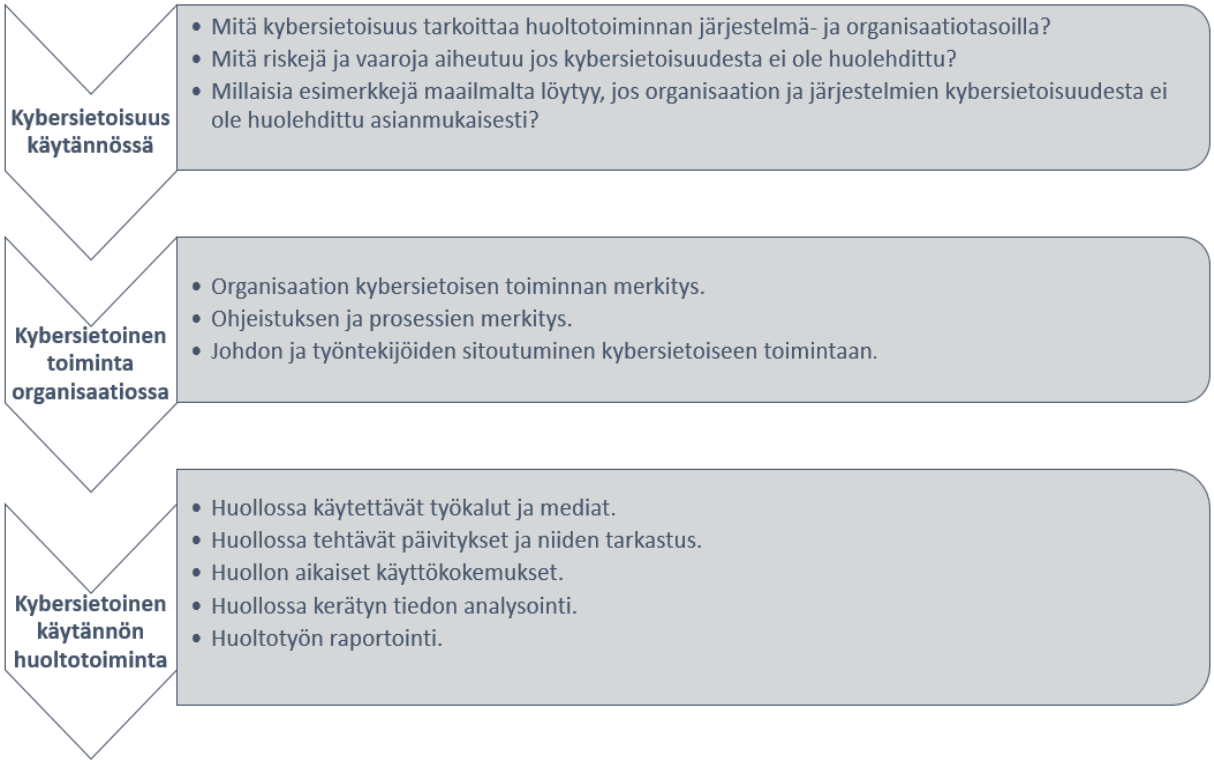
- Järjestelmän huoltoon tarkoitettujen laitteistojen kokonaisvaltainen tarkastus (kovennukset, salaukset, haittaohjelmatarkastus, siirrettävien medioiden tarkastus)
- Järjestelmäkovennusten tarkastus (käyttäjätunnukset ja salasanat)
- Järjestelmäsalauksen tarkastaminen
- Järjestelmän haittaohjelmasuojauksen tarkastaminen
- Järjestelmälokitusten päälle asettaminen
- Järjestelmän keräämän lokitiedon tarkastaminen
- Järjestelmään liitettyjen USB-laitteiden tarkastaminen
- Järjestelmäverkon palomuuriasetusten analysointi
- Järjestelmäverkon datatallenteen analysointi
- Varmuuskopioiden eheyden tarkastus
- Haavoittuvuustietojen tarkastaminen
- Langattomien verkkojen tarkastaminen

- Sähkömagneettisen spektrin tarkastaminen tuntemattomien lähettimien osalta

**Koulutuksen sisältö**

Haastattelumateriaalin pohjalta voitiin myös kirjoittaa alustava koulutussuunnitelma, jonka avulla kyetään määrittelemään kyberturvallisuuteen keskittyvän koulutustilaisuuden sisältö. Koulutustilaisuus tulisi kohdentaa niille halukkaille kunnossapitotöissä työskenteleville ja järjestelmien kunnossapidosta vastaaville järjestelmäinsinööreille, jotka vastaavat teknisesti edistyneistä tai vanhoista niin sanotuista legacy-järjestelmistä. Nämä vaativat erityishuomiota kyberturvallisuuden ja -sietoisuuden näkökulmasta. Harkinnan mukaan koulutustilaisuuteen tulisi osallistuttaa myös järjestelmien kanssa työskenteleviä ja niitä huoltavia asentajia.

Haastattelutilanteista kerätyn aineiston perusteellä koulutussisältö tulisi pitää mahdollisimman käytännönläheisenä ja keskittää tilaisuudessa läpi käytävät asiat käytännön työn tekemisen aiheisiin ja toimintamalleihin. Koulutusaiheita on havainnollistettu kuviossa 14. Koulutussuunnitelmasta voidaan eritellä kolme eri kokonaisuutta. Kybersietoisuus käytännössä-osio olisi koulutuspaketin ylätaso, jossa käytäisiin esimerkkien avulla läpi huoltotoimintojen ja -organisaation kybersietoisuutta. Esimerkkeinä voisivat toimia Suomessa ja maailmallakin tapahtuneet kyberhyökkäykset ja erilaiset kybervaikuttamisen avulla saavutetut kohdeorganisaatiolle haitalliset vaikutukset. Esimerkkien avulla havainnollistettaisiin tehtyjä asioita ja mahdollisia virheitä, jotka ovat mahdollistaneet haitallisen kynberhyökkäyksen ja -vaikuttamisen. Tähän koulutusosuuteen olisi mahdollisuuksien mukaan hyvä ottaa myös muitakin organisaatiossa työskenteleviä henkilöitä, jotta kybersietoisuuden määritelmä tulisi tutuksi muillekin kuin järjestelmien kunnossapidosta vastaaville insinööreille.




Kuvio 14. Koulutusaiheet

Kybersietoinen toiminta organisaatiossa osiossa keskityttäisiin organisaation kybersietoisiin toimintamalleihin ja prosesseihin. Koulutustilaisuudessa esille tuotavia asioita ovat esimerkiksi yhdenmukaisten toimintamallien ja prosessien merkitys, tiedon kulun ja saatavuuden merkitys, huolto-ohjeiden merkitys sekä johdon ja työntekijöiden sitoutumisen tärkeys, jotta kyberturvallisuus järjestelmien kybersietoisuuden osalta toteutuisi parhaalla mahdollisella tavalla. Organisaation jatkuva oppiminen ja osaamisen kehittämien kyberasioiden näkökulmasta tulisi myös ottaa koulutuksessa esille, sillä sen tulee olla osa organisaation jokapäiväistä toimintaa.

Kybersietoinen käytännön huoltotoiminta osio käsittelisi itse konkreettisessa huoltotyössä huomioitavia järjestelmien kyberturvallisuuteen ja -sietoisuuteen vaikuttavia asioita ja toimintamalleja. Huollossa käytettävät tietotekniset työkalut, sekä erialiset siirrettävät mediat ja niiden oikeanlainen käyttö tulisi olla yksi koulutuksen keskeisimmistä sisällöistä. Lisäksi erilaisten järjestelmäpäivitysten toteuttamiseen liittyviä turvallisuusuhkia ja -riskejä tulisi tuoda esiin konkreettisin esimerkein. Hyvänä turvallisuusuhkaesimerkkinä mainittakoon kappaleessa 2.2 esitetty Stuxnet-verkkomato. Käytännön huoltotyöhön liittyvät vahvasti myös erilaiset haavoittuvuustarkastelut, sekä laitteiston

toiminnan tarkkailu. Järjestelmiä huoltavien henkilöiden tulisi myös tunnistaa järjestelmän poikkeava käytös sekä tunnistaa ja analysoida syyt, jotka ovat järjestelmän poikkeavan käytöksen takana. Koulutustilaisuudessa tulisi siis tuoda esille esimerkkejä tietoteknisten järjestelmien poikkeavista käytöksistä ja syistä, jotka niitä voivat aiheuttaa. Huoltojen aikana voidaan myös kerätä erilaista lokitietoa tai verkkoliikennedataa. Lokiaineistojen analysoinnin ja normaalista toiminnasta poikkeavavien lokitietojen havainnointikyvyn kouluttaminen ainakin osalle järjestelmäinsinööreistä vaikuttaisi positiivisesti yrityksen liiketoiminnan kehittymiseen. Raportointi on tärkeä osa huolto-organisaation toimintaa. Raportoinnista voidaan esimerkiksi nähdä, jos järjestelmän toiminnassa on ollut poikkeamia ja mistä ne ovat mahdollisesti johtuneet. Koulutustilaisuudessa tulisi korostaa myös raportoinnin tärkeyttä.

Osaamiskartoituksen ja kehitys- ja koulutussuunnitelmien laadinnan jälkeen tulee keskittyä toimintamallien, koulutuksen ja kehittämistoimenpiteiden jalkauttamiseen. Tässä tutkimuksessa esitetyt toimenpiteet olisivat hyvä lähtökohta toiminnan kokonaisvaltaiselle kehittämiselle, jota jatkuvasti kehittyvä maailma ja teknologiat organisaatioilta vaativat. Tämä opinnäytetyö on antanut hyvät perusteet uusien palvelutuotteiden ja koulutuskokonaisuuksien suunnittelulle, sekä toimintamallien ja prosessien jalkauttamiselle.

# LÄHTEET

ALLIED ICT FINLAND STRATEGY SERIES. Kyberturvallisuus Suomessa 2019-2029. Viitattu 26.5.2020 saatavilla: https://alliedict.fi/wp-content/uploads/2019/12/Onepage_Cyber_fin.pdf

CIS (The Center for Internet Security) Inc. 2019. CIS Controls V7.1. Viitattu 20.8.2020 saatavilla: https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/

Cyberspace Operations, Joint Publication 3-12, US Joint Chiefs of Staff 2018. Viitattu 1.6.2020 saatavilla: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Eskola, Jari & Suoranta, Juha 2000: Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino

Heikkilä, T. 2008. Tilastollinen tutkimus. 7. uudistettu painos. Helsinki; Edita Prima Oy.

Hirsjärvi, Sirkka & Hurme, Helena 2001: Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Helsinki University Press.

Härkönen Anni HS, STT (2020). Telian valtakunnallinen yhteysvika oli vakavimman luokan häiriö, kertoo Kyber-turvallisuus-keskus. Viitattu 25.5.2020 saatavilla: https://www.hs.fi/kotimaa/art-2000006486885.html

Hätönen, Heljä. 2011: Osaamiskartoituksesta kehittämiseen II. Helsinki: Educa Instituutti.

Kananen, J. 2011. Kvantti: Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Katakri (kansallinen turvallisuusauditointikriteeristö). 2015. Katakri - Tietoturvallisuuden auditointityökalu viranomaisille - 2015. Viitattu 21.9.2020 saatavilla: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Kauhanen, Juhani. 2006. Henkilöstövoimavarojen johtaminen.8. uudistettu painos. Helsinki: WSOY Oppimateriaalit Oy.

Kott, Alexander & Linkov, Igor. 2019: Cyber Resilience of Systems and Networks. Cham, Switzerland: Springer International Publishing AG.

Laari Tommi, Flyktman Jouni, Härmä Katriina, Timonen Jussi, Tuovinen Jussi (2019). #kyberpuolustus : kyberkäsikirja Puolustusvoimien henkilöstölle. Viitattu 27.5.2020 saatavilla: http://urn.fi/URN:ISBN:978-951-25-3120-2

Lankinen, Paavo. Miettinen, Asko T T. & Sipola, Veikko. 2004. Kehitä osaamista – Hyödynnä kokemusta. Hämeenlinna: Talentum Media.

Marcum, Catherine D. 2019: Cyber Crime second edition. New York: Wolters Kluwer.

McCaughey, M. & Ayers, M. D. (2003). Cyberactivism: Online activism in theory and practice. New York (N.Y.) ; London: Routledge.

NATO Advanced Research Workshop on Response to Cyber Terrorism 2008: Responses to Cyber Terrorism. Ankara, Turkey: IOS press.

Nevaste Nadja, Paananen Rauli, Olin Pentti, Kuusisto Tuija, Rousku Kimmo 2017. Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 - 2020. Viitattu 22.05.2020 saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

Otala, Leenamaija. 2008: Osaamispääoman johtamisesta kilpailuetu. Porvoo: WSOY.

Palonen, Tuire., Keskinen, Soili., Kontkanen, Leila. & Jalava, Urpo. 1999. Osaaminen yrityksessä. Turku: Turun yliopisto, täydennyskoulutuskeskus.

Ranki, Anneli. 1999: Vastaako henkilöstön osaaminen yrityksen tarpeita. Jyväskylä: Gummerus kirjapaino Oy.

Saaranen-Kauppinen Anita, Puusniekka Anna et al. (2006-2009). KVALIMOTV. Kvalitatiivisten menetelmien verkko-oppikirja. Viitattu 19.5.2020 saatavilla: https://www.fsd.tuni.fi/fi/tietoarkisto/julkaisut/kvalimotv.pdf

Sadler-Smith, Eugene 2006: Learning and Development for Managers: Perspectives for Research and Practice. Malden, USA: Blackwell Publishing Ltd.

Suomen kyberturvallisuusstrategia 2013: Turvallisuuskomitean sihteeristö. Viitattu 25.5.2020 saatavilla: https://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/

Sydänmaanlakka, Pentti. 2012. Älykäs organisaatio. 8.painos. Vantaa: Talentum Media.

Viitala, Riitta. 2013: Henkilöstön johtaminen: Strateginen kilpailutekijä. 4. uudistettu painos. Porvoo: Bookwell Oy.

# Haastattelun alustus

Tämän haastattelun tarkoituksena on kerätä tietoa YAMK-opinnäytetyön kvalitatiiviseen tutkimukseen, jolla arvioidaan kunnossapidon kyberosaamista ylläpidettävien järjestelmien kybersietoisuuden osalta. Haastattelussa kertynyttä aineistoa tullaan käyttämään tulevaisuuden kyberpalveluiden ja -palvelutuotteiden suunnittelun apuna.

Sähköisten palveluiden lisääntymisen ja järjestelmien digitalisoitumisen myötä yritykset ja kriittisillä aloilla toimivat organisaatiot joutuvat uudistamaan ja miettimään toimintatapojansa kyberturvallisuuden osalta. Kyberasiat ja kybersietoisuus ovat erityisen huomion alaisena, kun työskennellään yhteiskunnan kannalta kriittisissä toiminnoissa. Kriittisiä toimintoja ovat esimerkiksi turvallisuus, logistiikka sekä tietoliikennealat.

Kunnossapito-organisaation tarkoitus on tuottaa asiakkaille erilaisia laitteiden ja järjestelmien kunnossapitopalveluita. Modernien- ja ns. legacy-järjestelmien tietyt laitteet ja ohjelmistot kuuluvat kokonaisuuksiin, joihin on mahdollista kohdistaa kybervaikuttamista monella eri tavalla. Kybervaikuttamista voidaan tehdä henkilöstön, fyysisten laitteiden ja välineiden sekä tietoverkon välityksellä. Kybervaikuttamisen motiivit voivat olla lähtöisin aktivismista, terrorismista, vakoilusta tai rikollisuudesta. Vaikuttamisen taustalla voivat olla yksittäiset ihmiset, järjestäytynyt rikollisuus tai valtiolliset toimijat.

Järjestelmien kybersietoisuus kuvaa erityisesti tietojärjestelmän kykyä kohdata, absorboida, palautua ja mukautua kybertoimintaympäristön kautta tapahtuvaan haitalliseen vaikuttamiseen. Järjestelmä on sitä kybersietoisempi, mitä nopeammin se kykenee palautumaan normaalin toiminnan tasolle kybervaikuttamisen alkamisajankohdasta. Kybersietoisuutta pystytään parantamaan yksinkertaisin keinoin, eikä se ei vaadi organisaatiolta tai yritykseltä isoja rahallisia panostuksia, kun pysytään perustasolla. Tärkeintä on huolehti tilojen turvallisuudesta, tietojärjestelmien perusturvallisuudesta sekä luoda toimintamallit, jotka huomioivat mahdolliset kyberuhat ja hyökkäyskohteet. Tärkeää on myös tunnistaa mistä kyberuhat muodostuvat, sillä se luo pohjan organisaation kyberturvalliselle toiminnalle.

# Haastattelun kysymykset

## Kybersietoisuus

1. Mitä järjestelmien kunnossapidon kybersietoisuus mielestäsi tarkoittaa?
2. Millaisia ominaisuuksia kybersietoisella huoltojärjestelmällä on?
3. Miten huoltojärjestelmien kybersietoisuutta voidaan mielestäsi parantaa?
4. Miten huolto-organisaation kybersietoisuutta voidaan mielestäsi parantaa?
5. Mikä on osaamisesi nykytila kybersietoisuuden osalta?

## Organisaation osaaminen

1. Onko kybersietoisuus huomioitu riittävän hyvin nykyisessä kunnossapito mallissa?
2. Miten kunnossapidon toimintaa voidaan mielestäsi kehittää kybersietoisuuden osalta, jotta se vastaisi paremmin asiakastarpeita?
3. Minkälaista koulutusta mielestäsi tarvitaan, jotta kunnossapidon toimintaa voidaan kehittää?

# Osaamismatriisi

| Vaatimus | | T 03 | F 03 | F 05 | F 08 | I 06 | I 08 | I 09 | I 11 | I 23 | I 24 | TASO: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Kuvaus | | Turvallisuustyön resurssit. Organisaatiolla on riittävä asiantuntemus, jotta tietoturvallisuustyön (kybersietokyky) tarkoitus toteutuu. | Tietojen fyysiseen suojaukseen tarkoitetut turvallisuusjärjestelmät ja laitteet. Tietojen säilömiseen tarkoitetut kassakaapit ovat tiedossa ja niitä osataan käyttää. | Avainten ja numerointidielmien hallinta. Avaintunnisteet ovat ainoastaan niiden henkilöiden käytössä, jotka niitä tarvitsevat. Alkuperäistunnisteet vaihdetaan poikkeuksetta. | Toiminnan jatkuvuuden varmistaminen. Merkittävillä häiriötilanteilla ja poikkeustilanteilla ei saa olla vaikutusta salassa pidettävien tietojen käsittelyyn tai säilyttämiseen. | Vähemmän oikeuksien periaate - Pääsyoikeuksien hallinnointi. Oikeudet ainoastaan niitä työssään tarvitseville. | Vähimmäistoimintojen ja vähemmän oikeuksien periaate - Käytössä ainoastaan työssä tarvittavat ohjelmistot. | Monitasoinen suojaaminen - Hälytysohjelmasuojaus, Työvälineessä oltava asianmukainen haittaohjelmasuojaus ennaltaehtäisyyn, estämiseen, haraamnontiin, vastustuskyvyn sekä tilanteen korjaamiseen. | Monitasoinen suojaaminen - Poikkeamien havainnointikyky ja toteaminen, Pyritään havaitsemaan mahdollinen poikkeama tai hyökkäys sekä rajoittamaan ja torjumaan sen aiheuttamaa vahinkoa ja palautumaan tilanteesta lähtötilanteeseen. | Tietojenkäsittelyympäristön suojaus koko elinkaaren ajan - Ohjelmistohaavoittuvuuksien hallitsemiseksi. | Tietojenkäsittelyympäristön suojaus koko elinkaaren ajan - Varmuuskopiointi. Salassa pidettävää tietoa sisältävät varmuuskopiot suojataan vähintään vastaavan tasoisilla menetelmillä kuin alkuperäinen tieto. | Osaamisarvosana: Keskiarvo |
| Toimipaikka X | Asiantuntija 1 | | | | | | | | | | | |
| | Asiantuntija 2 | | | | | | | | | | | |
| | Asiantuntija 3 | | | | | | | | | | | |
| | Asiantuntija 4 | | | | | | | | | | | |
| | Asiantuntija 5 | | | | | | | | | | | |
| | Asiantuntija 6 | | | | | | | | | | | |
| | Asiantuntija 7 | | | | | | | | | | | |
| Vaatimuksen hallinta keskiarvo: | | | | | | | | | | | | |
| Toimipaikka Y | Asiantuntija 1 | | | | | | | | | | | |
| | Asiantuntija 2 | | | | | | | | | | | |
| | Asiantuntija 3 | | | | | | | | | | | |
| Vaatimuksen hallinta keskiarvo: | | | | | | | | | | | | |
| Toimipaikka Z | Asiantuntija 1 | | | | | | | | | | | |
| | Asiantuntija 2 | | | | | | | | | | | |
| | Asiantuntija 3 | | | | | | | | | | | |
| | Asiantuntija 4 | | | | | | | | | | | |
| | Asiantuntija 5 | | | | | | | | | | | |
| | Asiantuntija 6 | | | | | | | | | | | |
| | Asiantuntija 7 | | | | | | | | | | | |
| | Asiantuntija 8 | | | | | | | | | | | |
| Vaatimuksen hallinta keskiarvo: | | | | | | | | | | | | |