Haaga-Helia
ammattikorkeakoulu Oy

Kyberturvallisuuden mittaaminen

Jani Iiskola

Opinnäytetyö
Tietojenkäsittelyn
koulutusohjelma
2019

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Jani Iiskola

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Kyberturvallisuuden mittaaminen

Sivu- ja liitesivumäärä
50 + 1

Yhteiskunnasta on tullut enenemissä määrin riippuvainen sähkönjakelusta sekä tieto- ja viestintäverkoista. Yhteiskunnan kriittinen infrastruktuuri on usein yksityisten yritysten ja organisaatioiden hallinnassa. Tätä keskinäisriippuvuutta on alettu kutsumaan kybertoimintaympäristöksi. Kybertoimintaympäristö tuo mahdollisuuksia yhteiskunnalle ja liiketoiminnalle, mutta mahdollisuuksien mukana tulee aina myös riskit. Kyberturvallisuuden tarkoitus on mahdollistaa kybertoimintaympäristön tehokas hyödyntäminen. Kyberturvallisuuteen käytetään maailmanlaajuisesti mittavia resursseja. Näin ollen resurssien oikea kohdentaminen on yrityksille kriittistä.

Tässä tutkimuksessa tutkittiin, miten kyberturvallisuudesta voidaan saada tietoa ja miten kyberturvallisuutta voidaan arvioida ja mitata. Tutkimuksen tavoitteena oli tuottaa mahdollisimman käytännönläheistä ja aikaa kestävää tietoa kyberturvallisuudesta, joka ymmärretään muuttuvana ja abstraktina käsitteenä. Lisäksi tavoitteena oli arvioida mahdollisuuksia kyberturvallisuuden mittaamiselle yritysten ja organisaatioiden näkökulmasta. Kyberturvallisuutta tarkasteltiin Kööpenhaminan koulukunnan turvallistamisteorian näkökulmasta. Tutkimus toteutettiin kuvailevalla kirjallisuuskatsauksella sekä laadullisella sisällönanalyysillä keväällä 2019.

Lähdeaineiston perusteella kyberturvallisuutta voi arvioida ja mitata organisaation tai yrityksen näkökulmasta strategisella, toiminnallisella sekä teknis-taktisella tasolla. Strategisella tasolla kyberturvallisuuden mittaaminen on yrityksen kypsyyden arviointia. Kypsyyttä voidaan arvioida eri käytössä olevien viitekehysten ja mallien avulla. Strategisella tasolla voidaan arvioida myös kyberturvallisuuden tavoitteiden saavuttamista. Strategiselta tasolta asetetaan myös vaatimuksen kyberturvallisuuden toiminnalliselle tasolle. Toiminnallisella tasolla kyberturvallisuuden mittaaminen on riskienhallintaa ja -analysointia. Kyberriskienhallintaa voidaan toteuttaa perinteisillä riskimatriiseilla tai tilastotieteellisillä menetelmillä. Tilastotieteellisissä menetelmissä etuna on se, että kriittisen päätöksenteon tueksi on saatavilla tieteellistä tietoa täysin subjektiivisen tiedon sijaan. Lähdeaineistossa ei kyetty kuitenkaan osoittamaan tieteellistä tietoa siitä, mikä riskienhallinnan menetelmä tukee päätöksentekoa ja vähentää epävarmuutta parhaiten. Teknisellä ja taktisella tasolla kyberturvallisuuden mittaaminen on esimerkiksi työntekijöiden tietoturvallisuustaitojen arviointia ja kehittämistä, haavoittuvuuksien korjaamista ja tietoliikenteen monitorointia. Tekniseltä ja taktiselta tasolta saadun tiedon perusteella kyetään toiminnallisella tasolla arvioiman riskejä paremmin. Näin ollen eri tasot tukevat toisiaan ja kattava kyberturvallisuus vaatii kaikkien tasojen huomioimista.

Asiasanat
Kyberturvallisuus, turvallisuus, mittaaminen, riskienhallinta

SISÄLLYS

1 JOHDANTO

1.1 Aiheen esittely

Vuonna 2013 FBI:n johtaja James Comey totesi, että tulevaisuudessa kyberturvallisuuteen tullaan käyttämään vähintään yhtä paljon resursseja kuin perinteiseen tuvallisuuteen. (Hubbard & Seieser, 2016, 7). Syyskuun 11. terrori-iskujen aikaan vuonna 2001 USA:n kyberturvallisuus markkinat olivat noin 4 miljardia dollaria, kun vuonna 2015 USA:n Puolustusministeriön kyberturvallisuusbudjetti oli noin 36 miljardia dollaria (Hubbart & Seiersen, 2016, 30). Resurssien käytön kasvaessa niiden tehokkuuden ja merkittävyyden arviointi korostuu. Päätöksenteon tueksi tarvitaan luotettavaa tietoa. Suurin osa kyberhyökkäyksistä kohdistuu pieniin ja keskikokoisiin yrityksiin, joilla on vain rajalliset kyberturvallisuusresurssit. (Fielder 2016, 13.)

Kyberturvallisuuden tutkimus on nuori tieteenala. Digitaalinen tiedonkäsittely on ollut olemassa noin 100 vuotta ja verkostoinunut tiedonkäsittely noin 50 vuotta. Kyberturvallisuus on noussut puheenaiheeksi vastan 1980- ja 1990-luvulla internetin yleistyessä. (Edgar & Manz, 2017, 33). Kybertoimintaympäristö on jatkuvasti muuttuva ja kompleksinen käsite. Se yhdistää fyysisen ja digitaalisen maailman. Sen myötä on avautunut lukemattomia mahdollisuuksia ja uusia keksitään jatkuvasti. Mahdollisuuksien mukana on tullut kuitenkin myös uhkia. Uhkan vastakohtana on turvallisuus. (Limnéll ym. 2014, 14.) Kyberturvallisuudella pyritään minimoimaan, hallitsemaan, poistomaan ja tunnistamaan kybertoimintaympäristön uhkia, jotta mahdollisuuksia voitaisiin hyödyntää mahdollisimman tehokkaasti ja toimivasti.

Suomi on tietoyhteiskuntana riippuvainen sähköisistä tietoverkoista sekä -järjestelmistä ja näin ollen haavoittuvainen siihen kohdistuvista uhkista. Tätä keskinäisriippuvuutta on alettu kutsumaan *kybertoimintaympäristöksi* (VNp 24.1.2013). Valtion, yritysten, organisaatioiden ja ihmisten lisääntyvä riippuvuus sähköstä, tietoliikenteestä, verkoista ja näistä muodostuvista palveluista, asettaa vaatimuksia kybertoimintaympäristön turvallisuudelle. Riippuvuuksien lisääntyessä uhkien vaikutukset kasvavat. Yhteiskunnan kriittinen infrastruktuuri on usein yksityisten yritysten ja organisaatioiden omistamaa ja ylläpitämää. Näin ollen juuri yritysten ja organisaatioiden kyky turvata kybertoimintaympäristö on yhteiskunnan toimivuuden kannalta kriittistä. Tietojärjestelmien ja automatiikan lisääntyvä hyödyntäminen kasvattaa hyökkäyspinta-alaa. Puolustus on usein hyökkääjää jäljessä ja se on vain niin vahva kuin sen heikoin lenkki. (Fielder 2016, 14.)

Kyberturvallisuuden kehittäminen vaatii kyberturvallisuuden arviointia. Kyberturvallisuuden arviointi on kuitenkin haastavaa, mikäli turvallisuus ymmärretään subjektiivisena ja muuttuvana ilmiönä. Kyberturvallisuuden mittaamista on pyritty standardisoimaan erilaisilla parhailla

käytännöillä, viitekehyksillä ja menetelmillä. Tässä ei laajasti ole kuitenkaan onnistuttu. (Wang ym. 2017, 2.) Ongelmana on myös se, etteivät yritykset ole halukkaita käyttämään resursseja turvallisuuteen, elleivät ne liity suoraan liiketoimintaprosesseihin (Kurittu 2019). Tässä tutkimuksessa tarkastellaan miten kyberturvallisuudesta voidaan saada tietoa. Lisäksi tarkastellaan menetelmiä kyberturvallisuuden arviointiin ja mittaamiseen yritysten sekä organisaatioiden näkökulmasta.

1.2 Aikaisempi tutkimus

Kybertoimintaympäristöä ja -turvallisuutta käsitteleviä tutkimuksia löytyi tietokantahaussa runsaasti. Kyberturvallisuuden mittaamisesta on tehty joitakin aihetta käsitteleviä teoksia ja artikkeleita, mutta ei tieteellisiä tutkimuksia. Tietokantahaun perusteella lähimpänä tätä tutkimusta voidaan pitää Pendleton (2016) tutkimusta: *A Survey on Systems Security Metrics*. Pendleton (2016) käsittelee järjestelmäturvallisuuden mittareita ja mittaamista. Lisäksi merkittävänä aikaisempana tutkimuksena voidaan pitää Lehto ym. (2018) *Kyberturvallisuuden strateginen johtaminen Suomessa*. Lehto ym. (2018) selvittää mahdollisuuksia arvioida Suomen kansallisen tason kyberturvallisuuden valmiuksia eri kypsyysmallien avulla.

Suomen kyberturvallisuusstrategian (VNp 2013) jälkeen julkaistuja kyberturvallisuutta käsitteleviä suomalaisia opinnäytetöitä on tehty noin kymmenen. Tämän tutkimuksen kannalta lähimpänä on Tomi Turusen työ: *Kyberturvallisuuden hallintamallin kehittäminen* (Kaakkois-Suomen ammattikorkeakoulu, 2018). Turunen käsittelee opinnäytetyössään miten kyberturvallisuutta hallinnoidaan, mallinnetaan ja dokumentoidaan.

1.3 Tutkimustehtävä

Tutkittavana ilmiönä on kyberturvallisuus. Tutkimustehtävä on jaettu kahteen vaiheeseen. Ensimmäisessä vaiheessa tutkimusongelmana on selvittää, mitä on kyberturvallisuus ja miten siitä voidaan saada tietoa. Tässä vaiheessa luodaan ymmärrys ilmiöstä vastaamalla ensimmäiseen tutkimuskysymykseen:

1. Mitä on kyberturvallisuus ja miten siitä voidaan saada tietoa?

Toisessa vaiheessa ensimmäisen tutkimuskysymyksen tuloksien perusteella vastataan seuraaviin tutkimuskysymyksiin:

2. Miten kyberturvallisuutta voi mitata?
3. Minkälaisia olemassa olevia menetelmiä kyberturvallisuuden arviointiin on käytössä?

Tutkimuksen tavoitteena on arvioida mahdollisuuksia kyberturvallisuuden mittaamiselle yritysten ja organisaatioiden näkökulmasta. Tutkimuksen tavoitteena ei ole luoda täysin valmista mallia tai sapluunaa, jolla organisaatio voisi arvioida omaa kyberturvallisuuttaan. Valmiita viitekehyksiä arviointiin on olemassa ja tässä tutkimuksessa tarkastellaan niiden ominaisuuksia ja kykyä vähentää epävarmuutta kyberturvallisuudesta. Tässä tutkimuksessa kyberturvallisuus ymmärretään muuttuvana ilmiönä, jolloin tieto voi olla jo huomenna vanhaa. Näin ollen perusteltuna tavoitteena on löytää aikaa kestäviä ja dynaamisia malleja, joita voidaan soveltaa organisaation erityispiirteiden ja tarkoitusten mukaan. Tavoitteena on myös kuvata problematiikkaa kybertuvallisuuden mittaamiseen liittyen ja tutkia, onko aineistosta löydettävissä hyviä käytäntöjä tai näkökulmaeroja ilmiön mittaamiseen. Tavoitteena on myös lisätä tieteellisyyttä, tietoa ja ymmärrystä ilmiöstä, jota voidaan pitää suhteellisen nuorena. Henkilökohtaisena tavoitteena on lisätä ymmärrystä ilmiöstä ja sen analysoinnista, arvioinnista ja mittaamisesta, jotta voin hyödyntää kertynyttä osaamista kyberturvallisuudesta tulevaisuudessa.

1.4 Tutkimuksen tarpeellisuus

Yritysten liiketoimintaprosessien riippuvuus tietoliikenteestä ja -verkoista lisääntyy jatkuvasti. Kyberilmiöstä on viime vuosina julkaistu paljon tutkimuksia, kirjoja ja artikkeleita. Ilmiö on kuitenkin suhteellisen uusi eikä kaikkia sen tuomia mahdollisuuksia ja uhkia tiedosteta riittävän laajasti. Kyberturvallisuuden parantaminen edellyttää ennen kaikkea perustietojen ja -taitojen kehittämistä (Limnéll ym. 2014, 107). Tämä tutkimuksen tarkoituksena on lisätä perustietoja kyberilmiöstä.

Kyberturvallisuuteen panostetaan mittavia resursseja. Resurssien oikea kohdentaminen edellyttää tietoa kyberturvallisuuden tilasta sekä siihen kohdistuvista uhkista ja riskeistä. Lisäksi se vaatii onnistunutta päätöksentekoa. Tässä tutkimuksessa tarkastellaan eri tapoja saada tietoa kyberturvallisuudesta. Lisäksi tarkastellaan eri menetelmiä arvioida organisaation kyberturvallisuuden tasoa ja valmiuksia.

Vaikka kyberilmiötä voidaan pitää trendi-ilmiönä, niin kyberturvallisuuden mittaamisesta on julkaistu vain vähän tieteellisiä tutkimuksia tai artikkeleita. Aikaisempia opinnäytetöitä kyberturvallisuuden mittaamisesta ei ole julkaistu, joten tutkimukselle on tarvetta. Tieteellisyyden lisääminen vaati ilmiön monipuolista tutkimista.

2 TUTKIMUSTEORIA JA -MENETELMÄT

2.1 Teoreettinen viitekehys

Teoreettinen viitekehys tai teoriatausta osoittaa tutkimuksen paikan suhteessa muuhun tutkimukseen. Sen tarkoitus on myös ohjata tutkimuksen tekemistä ja se sisältää keskeiset aiheeseen liittyvät teoriat. Teorian tulee myös kytkeytyä tutkimusongelmaan, jolloin teorian ja empirian välille syntyy looginen jatkumo. (KvaliMOTV 2019). Teoreettinen viitekehys on ikään kuin kieli, jolla tutkimus kirjoitetaan. (Sipilä & Koivula 2014, 21).

2.1.1 Teoreettinen paradigma

Ontologia on oppi olevaisesta tai oppi olemassa olon luoteesta. (Tieteen termipankki, 2019a). Ontologia voidaan jakaa kahteen ääripäähän: realistinen ja nominaalinen. Realistinen käsitys ontologiasta on objektiivinen, kun taas nominaalinen käsitys on subjektiivinen. Objektiivisuus tarkoittaa sitä, että maailma nähdään samanlaisena riippumatta katsojasta. Subjektiivisuus puolestaan tarkoittaa sitä, että jokainen kokee maailman omanlaisenaan.

Epistemologialla tarkoitetaan tietoteoriaa, joka kysyy mitä tieto on ja miten tietoa voi saada. Se tarkastelee myös totuuden ongelmaa sekä tiedon ja tietämisen ehtoja. (Tieteen termipankki, 2019b). Ontologinen näkemys ohjaa myös epistemologisia näkemyksiä. Jos maailma nähdään subjektiivisena, miten siitä voidaan saada tietoa? Laajan turvallisuuskäsityksen myötä turvallisuus mielletään usein subjektiiviseksi. Jokainen ihminen kokee turvallisuutta tai turvattomuutta omalla tavallaan. Kybertoimintaympäristö ja -turvallisuus on ihmisen luoma abstraktinen alati muuttuva käsite. Kyberturvallisuudesta voidaan saada tietoa esimerkiksi tutkimalla, keskustelemalla ja mittaamalla. Ilmiön dynaamisuutta voidaan perustella sillä, että sen tuomat mahdollisuudet ja uhkat muuttuvat jatkuvasti. Tutkimisen ja mittaamisen haasteena on pysyä ilmiön muutoksen mukana. Ilmiön muuttuessa, myös mittarit ja näin ollen tutkimustulokset muuttuvat. Tämä on oleellista ymmärtää tarkasteltaessa tutkimuksen tuloksia.

Metodologia eli menetelmäoppi on oppi siitä, millä tiedonhankinta menetelmillä tietoteorian näkemyksistä ja valinnoista voidaan hankkia tarvittava ja saatavilla oleva tieto sekä miten sitä voidaan tutkia. (Tieteen termipankki 2019c). Näin ollen voidaan kysyä, millä tiedonhankintamenetelmillä voidaan kyberturvallisuudesta hankkia tietoa, kun se on jatkuvasti muutoksessa. Kyberturvallisuudessa yhdistyy fyysinen maailma ja bittien maailma, jolloin tietoa voidaan saada sen eri osa-aluista laadullisilla ja määrällisillä menetelmillä.

Metodologisena haasteena kyberturvallisuudessa on, että se mielletään usein tekniikaksi ja teknologisiksi ratkaisuiksi. Tällöin saattaa muodostua mielikuva, että kyberturvallisuuden tutkiminen on vain teknisten tieteenalojen tehtävä, jota tutkitaan määrällisillä menetelmillä. Kyberturvallisuus on kuitenkin kaksi kolmasosaa muuta kuin tekniikka. (Limnéll ym. 2014, 47). Tällä periaatteella suurin vastuu kyberturvallisuuden tutkimisesta olisi muilla kuin tekniikan aloilla. Poikkitieteellinen tutkimus lisää ja edistää tiedettä.

Teoreettinen paradigma tarkoittaa teoreettista malliratkaisua sekä tutkijayhteisössä vallitsevien periaatteiden, uskomusten, arvostusten ja tieteellisten normien kokonaisuutta. Paradigmat ovat siis tapa tulkita maailmankuvaa, jota ei kuitenkaan voida osoittaa aukottomasti todeksi, mutta on yleisesti hyväksytty. (Tieteen termipankki, 2019d). Ongelmana kyberturvallisuuden tutkimuksessa on, että se on niin nuori tieteenala, ettei ilmiöstä ole muodostunut tiedeyhteisössä yleisesti hyväksyttyä paradigmaa. (Edgar & Manz, 2017, 33). Tästä syystä tässä tutkimuksessa sovelletaan turvallisuuden tutkimuksessa käytettyä tietoteoriaa. Paradigman puuttuminen luo haasteita, mutta toisaalta myös mahdollisuuksia. Tutkijalle jää mahdollisuus tieteenrajoissa soveltaa, kokeilla ja luoda uutta. Ilmiöitä voidaan ymmärtää ja tutkia monesta eri näkökulmasta, eikä absoluuttista totuutta siitä, mikä on oikea tai väärä tulkinta voida välttämättä osoittaa.

2.1.2 Turvallisuus

Turvallisuus tarkoittaa vapautta uhkista (Eskola 2008, 1). Kylmän sodan jälkeen yhdeksi kriittiseksi turvallisuusteoriaksi kehittyi niin sanotun *Kööpenhaminan koulukunnan* piirissä *turvallistamisteoria* (eng. securitization theory). Teoria tarkastelee turvallisuutta puheiden ja kirjoitusten kautta, jolloin sitä voidaan pitää hyvin samankaltaisena konstruktivismin kanssa. Konstruktivismin mukaan ihminen voi kehittää maailmaa haluamaansa suuntaan. Näin ollen yhteiskuntaan kohdistuvia riskejä voidaan välttää tai minimoida. (Harisalo 2005, 58.) Sosiaalisessa konstruktivismissa turvallisuus muodostuu siitä, miten ilmiöstä puhutaan. (Sipilä & Koivula, 2014, 28–30).

Turvallistamisteorian referenssiteoksena voidaan pitää Buzanin, Weaverin ja de Wilden teosta *Security–A New Framework for Analysis* (1998). Kylmän sodan aikainen turvallisuuskäsitys voidaan nähdä kapeana turvallisuutena. Kylmän sodan jälkeen yleistyi käsitys laajasta turvallisuudesta. Ongelmaksi muodostui se, että Neuvostoliiton uhka oli poissa, jolloin valtioiden tuli kyetä perustelemaan turvallisuuden ylläpitoon käytettäviä resursseja. Näin ollen valtiot löysivät uusia uhkia, jotka eivät enää olleet vain toisia valtioita. Turvallisuuskäsitys laajeni sotilaallisesta turvallisuudesta koskemaan myös taloudellista, sosiaalista, ympäristöllistä ja poliittista turvallisuutta. Enää valtiot eivät yksin omistaneet turvallisuuden käsitettä vaan se ulottui aina yksilöihin asti. (Eskola 2008, 1.) Turvallistamista voidaan pitää politisoinnin seu-

raavana askeleena. Asioiden politisoinnilla tarkoitetaan sitä, että valtio ottaa niihin poliittisesti jollain tavalla kantaa. Näin ollen turvallistamisella tarkoitetaan sitä, että valtio näkee asian uhkana ja ryhtyy toimenpiteisiin uhkan poistamiseksi. (Buzan ym. 1998, 20–23.) Valtio on korostanut kybertoimintaympäristöön liittyviä uhkia *Kansallisissa riskiarvioissa* (2015 ja 2018) sekä *Yhteiskunnan turvallisuusstrategiassa* (2017). Kybertoimintaympäristön turvallistaminen on johtanut muun muassa *Kyberturvallisuusstrategian* luomiseen. Kyberturvallisuus ei niinkään ole uusi osa-alue Buzan ym. (1998) esittämiin osa-alueisiin, vaan se liittyy olennaisesti jokaiseen. Kybertoimintaympäristöä turvallistamisteorian näkökulmasta on tutkinut muun muassa Hansen & Nissenbaum julkaisussa *Digital Disaster, Cyber Security and the Copenhagen School* (2009).

Suomalainen näkökulma laajasta turvallisuudesta on kokonaisturvallisuuden malli. Yhteiskunnan turvallisuuden rakentamiseen ja kehittämiseen osallistuvat kaikki hallinnonalat. Kriittinen infrastruktuuri on pääasiassa yksityisten yritysten hallinnassa. *Yhteiskunnan turvallisuus strategia 2017* (YTS 2017, 7) määrittelee kokonaisturvallisuuden seuraavasti: ”Kokonaisturvallisuus on suomalaisen varautumisen yhteistoimintamalli, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä.” Kyberturvallisuuden merkitys on korostunut uusimmissa valtion riskiarvioissa ja YTS 2017 kyberturvallisuus nähdään merkittävänä osana kokonaisturvallisuutta.

Puheissa ja kirjoituksissa korostuu usein ilmiön uhkalähtöisyys. Kyberturvallisuus on trendiaihe ja siihen liitetään usein esimerkiksi kybersodankäynti, -vaikuttaminen, -rikollisuus ja -terrorismi. Puhuttaessa mahdollisuuksista harvemmin käytetään ”kyber” etuliitettä. Usein puhutaan *e*-urheilusta, *e*-kirjasta, *e*-busineksesta tai verkkokaupasta. Näin ollen voidaan perustellusti tulkita, että *kyber*ilmiöön liittyy *turvallistaminen*.

Kyberturvallisuuden tutkimuksessa yhdistyy fysiikan lakien, ihmisen käyttäytymisen sekä tietotekniikan tutkiminen, mikä tekee sen tutkimisesta uniikin ja haastavan. Ilmiötä voidaan tutkia esimerkiksi sovellusten ja käyttöliittymien, tietokoneiden ja tietoliikenneyhteyksien kautta tai ihmisen käyttäytymisen kautta. Fyysisen ja kybertoimintaympäristön tutkiminen eroavat toisistaan siinä, ettei kybermaailmaa voida täysin tutkia samojen fysiikan lakien perusteella. Kybertoimintaympäristössä ei esimerkiksi ole pituutta tai massaa, joita voitaisiin mitata. Näin ollen myös turvallisuuden tutkiminen näissä kahdessa toimintaympäristössä on erilaista. Esimerkiksi fyysisessä maailmassa kyetään mittaamaan, kuinka paljon voimaa tarvitaan jonkun esteen rikkomiseen tai kuinka kauan käytössä olevalla voimalla siihen kestää. Kybermaailmassa tämä ei onnistu, jolloin hyökkääjät pyrkivät hyödyntämään haavoittuvuuksia, joita puolustaja ei ole osannut huomioida, sen sijaan, että hyökkäisi suoraan puolustusta vastaan. (Edgar & Manz 2017, 55–56.) Lähimmäs näitä fyysisen maailman lainalaisuuksia voidaan päästään arvioitaessa palvelunestohyökkäykseen tarvittavaa tietoliikennemäärää

suhteessa kohteen palvelinten suorituskykyyn tai aikaa tietyn mittaisen salasanan murtamiseen käytössä olevalla laskentateholla.

Kyberturvallisuuden tutkimuksessa merkittävän haasteen asettavat dynaamiset ja muuttuvat uhkat (Black ym. 2008, 4). Kybertoimintaympäristössä, jossa fyysiset lait eivät päde, uhkan muodostaa kuitenkin ihmiset, jotka oppivat, jakavat tietojaan ja muuttavat toimintatapojaan. Näin ollen kyberturvallisuuden tutkimus vaatii ymmärrystä fyysisen- ja kybertoimintaympäristön muodostavasta maailmasta ja sen lainalaisuuksista. (Edgar & Manz 2017, 56–57.) Kyberturvallisuuden tutkimuksen tunnettuja suuntauksia ovat hyökkäyksen havaitseminen, turvallisuusmekanismien suunnittelu, sovellusturvallisuus, virus- ja uhka-analyysi, riskienhallinta ja kryptografia (Edgar & Manz 2017, 57–58.)

2.1.3 Näkökulma ja rajaukset

Turvallisuutta voidaan tutkia monesta näkökulmasta. Tässä tutkimuksessa kyberturvallisuus ymmärretään osana laajaa turvallisuuskäsitystä ja Suomen kokonaisturvallisuuden mallia. Kehittyneen informaatio- ja viestintäteknologian mahdollistama toimintaympäristö on *turvallistettu*. Tämä kriittinen infrastruktuuri on lähtökohtaisesti yksityisten yritysten omistuksessa. Näin ollen tutkimus keskittyy tarkastelemaan turvallisuutta yritysten ja organisaatioiden näkökulmasta, jolloin korostuu ilmiön käytännönläheinen tarkastelu.

Tutkimuksessa ei keskitytä tarkastelemaan turvallisuutta valtion näkökulmasta. Näin ollen ilmiöön olennaisesti liittyvät uhkat, kuten kybersodankäynti tai kyberterrorismi, on rajattu pois. Koska valtion turvallisuuden kannalta kriittinen infrastruktuuri on usein yksityisten yritysten ja organisaatioiden omistuksessa, niin valtiollista näkökulmaa ei kuitenkaan voida täysin sivuuttaa. Tässä tutkimuksessa ei kuitenkaan tarkastella kyberturvallisuuden mittaamista kansallisten mittareiden näkökulmasta (kts. esim. Lehto ym. 2018).

Tutkimuksessa ei myöskään keskitytä teknisten ratkaisujen yksityiskohtiin tai ominaisuuksiin. Teknisellä tasolla tarkastellaan menetelmiä, joiden avulla voidaan saada tietoa kyberturvallisuuden tasosta, mutta niiden toimivuutta, käyttökelpoisuutta tai luotettavuutta ei arvioida.

Koska ilmiön ymmärretään muuttuvan jatkuvasti, on ajallinen rajaus lähdeaineistossa perusteltua. Ensisijaiseksi lähdeaineistoksi on ajallisen rajauksen perusteella valkoitu *Suomen kyberturvallisuusstrategian* (VNp 2013) jälkeen julkaistut lähteet. Tätä ajallista rajausta tukee myös se, että samana vuonna Yhdysvalloissa annetun asetuksen perusteellä on luotu organisaatioiden käyttöön kyberturvallisuuden kypsyysmalli. Turvallisuuden sekä mittaamisen teorian osalta on hyödynnetty myös vanhempaa lähdeaineistoa.

2.1.4 Keskeiset käsitteet

Tässä tutkimuksessa mittaamisella tarkoitetaan toimenpidettä, joka suoritetaan epävarmuuden vähentämiseksi (Hubbard & Seiersen 2016, 21; Pendleton 2016; 62:3; Hayden 2010, xxiv). Mittarilla puolestaan tarkoitetaan yksittäistä menetelmää, joka tuottaa dataa tai tietoa (Pendleton 2016; 62:3; Hayden 2010, 4). Kybertoimintaympäristöllä tarkoitetaan fyysisen ja digitaalisen maailman yhdistymistä ja keskinäisriippuvuutta (VNp 24.1.2013). Kyberturvallisuudella tarkoitetaan kybertoimintaympäristön tekemistä turvalliseksi (Edgar & Manz, 2017, 34). Kyberturvallisuus ymmärretään muuttavana, abstraktina ja osittain subjektiivisena käsitteenä.

2.2 Tutkimusmenetelmät

Metodi eli tutkimusmenetelmät ovat keino vastata epistemologian asettamiin vaatimuksiin. Se miten tutkija ymmärtää maailmaa ja siitä saatavaa tietoa, ohjaa metodivalintoja: miten voidaan parhaiten saada tietoa tutkittavasta ilmiöstä. Tässä tutkimuksessa kyberturvallisuus nähdään olevan subjektiivinen ja dynaaminen ilmiö. Näin ollen siitä on hankala saada täysin objektiivista ja aikaa kestävää tietoa.

Tutkimusmenetelmien tarkoituksena on tuottaa tutkimusongelmaan ratkaisu, joka on uskottava, luotettava ja totuudenmukainen. Menetelmien avulla kerätään aineisto, josta ratkaisu etsitään. (Kananen, 2017, 84.) Kyberturvallisuutta voidaan tutkia hyödyntämällä teoreettisia, havainnoinnin, kokeellisia tai sovellettuja tutkimusmenetelmiä (Edgar & Manz 2017, 56–57). Tämä tutkimus on toteutettu teoreettisena, mutta sen tavoitteena on tuottaa käytännönläheistä tietoa.

2.2.1 Kuvaileva kirjallisuuskatsaus ja laadullinen sisällönanalyysi

Kuvaileva kirjallisuuskatsaus on aineiston tarkastelua ilman tiukkoja rajoja sekä sääntöjä. Tässä tutkimuksessa kuvailevan kirjallisuuskatsauksen tarkoituksena oli parantaa kokonaiskäsitystä ja tunnistaa olemassa olevia ongelmia aiheesta. (Salminen, 2011.)

Laadullinen sisällönanalyysi on yksi yhteiskuntatieteissä eniten käytetty tutkimusmenetelmä. Laadullinen sisällönanalyysi voidaan toteuttaa joko aineistolähtöisenä, teoriasidonnaisena tai teorialähtöisenä. Aineistolähtöisessä sisällönanalyysissä mukaillaan induktiivisen päättelyn logiikkaa. Tällä tarkoitetaan sitä, että aineistolle ei esitetä kysymyksiä vaan tarkastellaan millaisia asioita ja ilmiöitä aineistosta nousee esille. Induktiivinen tutkimusote tähtää täysin objektiiviseen tutkimukseen. Tämän tavoitteleminen saattaa kuitenkin olla jopa mahdotonta (Salo, 2015.) Teorialähtöinen sisällönanalyysi mukailee puolestaan deduktiivisen päättelyn

logiikkaa. Teorialähtöisessä sisällönanalyysissä aineistolta kysytään tutkijan valitsemaan teoriaa ja pyritään saamaan aineistosta tulos, joka tukee tai ei tue käytettyä teoriaa tutkittavasta ilmiöstä.

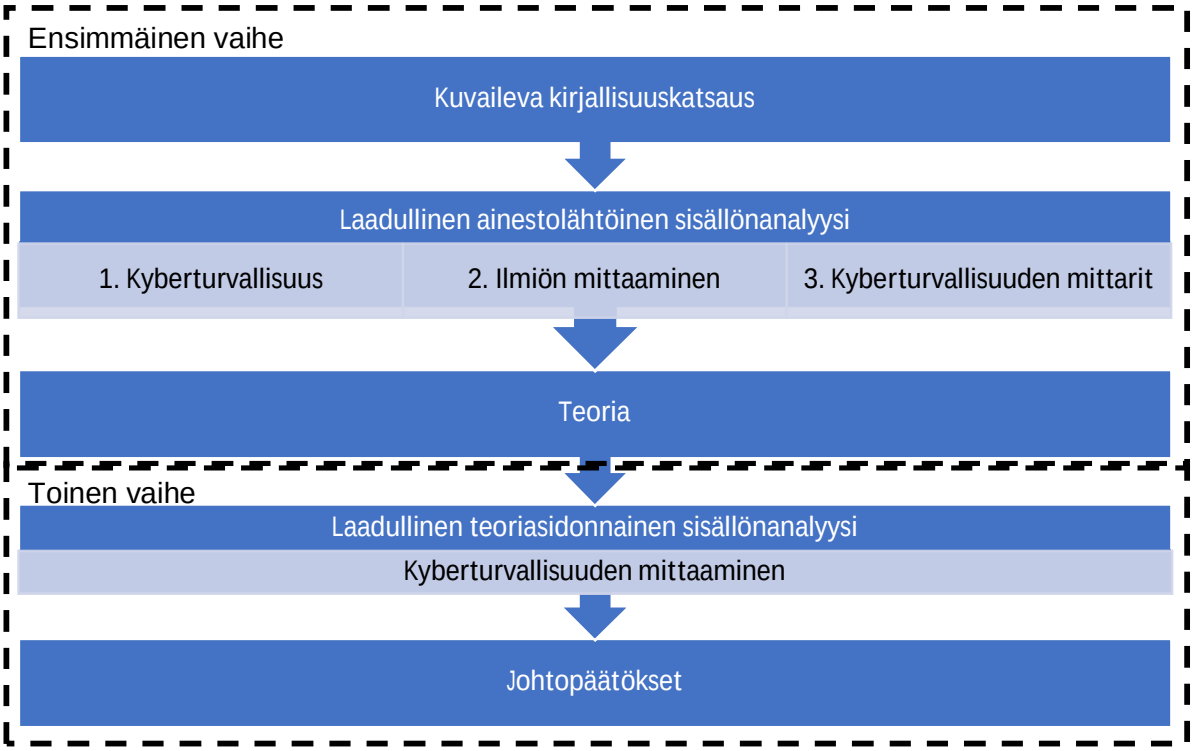
Tämä tutkimus on toteutettu ensimmäisessä vaiheessa aineistolähtöisenä sisällönanalyysinä ja toisessa vaiheessa teoriasidonnaisena sisällönanalyysinä. Teoriasidonnainen sisällönanalyysi on aineistolähtöisen ja teorialähtöisen välimuoto, joka mukailee abduktiivisen päättelyn logiikkaa. Tämä tarkoittaa sitä, että tutkimista ohjaa jokin valittu teoria, mutta se ei ole hallitsevassa asemassa. Teorian osuus ja merkitys eri tutkimusvaiheissa saattaa vaihdella. (Tuomi & Sarajärvi 2009, 104.) Tutkimuksen toteutus muodostui neljästä vaiheista (Kananen 2017, 131–133):

1. Aineiston keruu
2. Aineiston yhteismitallistaminen
3. Aineiston koodaaminen ja segmentointi
4. Uusi aineiston keruu

Aikaisemmat kokemukset ja tiedot aiheesta ohjaavat jonkin verran aineiston hakua ja tulkintaa. Näin ollen absoluuttiseen objektiivisuuteen on hankala päästä. Tutkimuksen tavoitteet ohjaavat menetelmävalintaa. Tavoitteena on tutkia miten subjektiivista ilmiötä voidaan mitata ja arvioida mahdollisimman objektiivisesti. Näin ollen aiemmat mittaamisesta esitetyt teoriat, käsitteet ja määritelmät ohjaavat kyberturvallisuuden mittaamisen analysointia.

2.2.2 Tutkimusprosessi

Tämä tutkimus muodostui kahdesta vaiheesta. Ensimmäisessä vaiheessa kuvailevalla kirjallisuuskatsauksella luotiin riittävä kuva kyberilmiöstä. Tämän jälkeen perehdyttiin olemassa oleviin kyberturvallisuuden kypsyysmalleihin. Näiden perusteella luotiin teoriapohja tutkimuksen toiseen vaiheeseen, jonka tavoitteena oli selvittää, miten kyberturvallisuutta voidaan mitata. Toisen vaiheen tutkimustulokset ovat tämän tutkimuksen johtopäätökset.



Kuva 1. Tutkimusprosessi

2.3 Tietohaku ja lähdeaineisto

Tietokantahaut toteutettiin 19.3.2019 Theseukseen, Finnaan ja Google Scholariin. Theseukseen on koottuna suomalaisten ammattikorkeakoulujen opinnäytetöitä ja julkaisuja 27:stä kokoelmasta (Theseus 2019). Finnaan on koottuna suomalaisten museoiden (58), kirjastojen (66) ja arkistojen (11) julkaisuja saataville. Finnasta löytyy myös organisaatiokohtaiset hakupalvelut (Finna.fi 2019). Google Scholar on yhdysvaltalaisen Googlen tarjoama hakupalvelu, josta voi hakea tieteellisiä julkaisuja. Joissakin tapauksissa palvelu näyttää aineistoon kohdistuneiden viittausten määrän ja lukijoiden vertaisarvion aineistosta, jolloin aineiston merkittävyyttä voidaan arvioida. Palvelu on maksuton, mutta sen sisällöstä ja kattavuudesta ei ole saatavilla tarkkaa tietoa. (Oulun yliopisto 2019.)

Tietokantahaku Theseus-tietokantaan tuotti hakusanalla ”kyberturvallisuus” 140 amk-tasoista opinnäytetyötä ja 33 ymak-tason työtä. Kun hakusana rajattiin koskemaan nimikettä, tuloksena oli kolme amk-tason opinnäytetyötä.

Finna-tietokannassa hakusana ”kyberturvallisuus” tuotti yhteensä 977 tulosta, joissa hakusana esiintyy. Näistä 417 oli kirjoja, 283 lehtiä tai artikkeleita ja 184 opinnäytetöitä. Tarkennetulla haulla nimikkeisiin tuloksena oli yhteensä 125 osumaa, joista 58 oli lehtiä tai artikkeleita, 29 opinnäytetöitä ja 22 kirjoja. Hakusana ”turvallisuuden mittaaminen” tuotti neljä eri julkaisua. Kahdessa julkaisussa käsiteltiin työturvallisuutta (engl. safety).

Google Scholarista hakusana ”kyberturvallisuus” tuotti yhteensä 686 tulosta. Nimikkeisiin kohdistettu haku tuotti 17 tulosta. Hakuehdoilla ”kyberturvallisuus” AND ”mittaaminen” tuloksena oli 9 tulosta. Tarkkahaku ”kyberturvallisuuden mittaaminen” tai ”kyberturvallisuuden mittaus” ei tuottanut tuloksia. Nimikkeisiin kohdistettu hakusana ”cybersecurity” tuotti 7 580 tulosta. Tarkennettuhaku ”cybersecurity measurement” tuotti kaksi tulosta. Scopus-tietokantaan ei ole Haaga-Helian kautta pääsyä.

Tietokantahaussa selvisi kaksi asiaa. Ensiksi kyberturvallisuutta on käsitelty runsaasti osana muuta tutkimusta. Kuitenkin kyberturvallisuuden mittaamisesta löytyi hyvin vähän julkaisuja, eikä niitäkään voida pitää tieteellisinä julkaisuina. Toiseksi ilmiöön perehtyminen kuvailevalla kirjallisuuskatsauksella vaatii huomattavaa lähdeaineiston rajausta käytössä olevien resurssien ja opinnäytetyön luonteen vuoksi.

Ongelmana lähdeaineistossa on, että ilmiöstä on saatavilla paljon eri tasoisia ja tyylisiä julkaisuja. Julkaisujen pätevyyttä ja toistettavuutta on vaikea arvioida. Tieteellisiä julkaisuja aiheesta on jonkin verran. Theseus ja Finna eivät tarjoa tiedeyhteisölle mahdollisuutta vertaisarvioida julkaisuja, joten myös niiden laadun arviointi on hankalaa.

Tutkimuksen teorian ja menetelmien osalta ensisijaisina lähteinä on käytetty *Security – A New Framework for Analysis* (Buzan ym. 1998), *Research methods for cyber security* (Edgar & Manz 2017), *Tutki ja Kirjoita* (Hirsjärvi ym. 2002) sekä *Laadullinen tutkimus pro graduna ja opinnäytetyönä* (Kananen 2017).

Ilmiöön perehtymiseen ensisijaisena lähteenä on käytetty teosta *Kyberturvallisuus* (Limnéll, Majewski & Salminen, Docendo 2014) sekä *Suomen kyberturvallisuusstrategia* (Valtioneuvoston periaatepäätös 23.1.2014). *Kyberturvallisuus* ei ole tieteellinen julkaisu vaan kirja, joka ilmentää kirjoittajiensa mielipiteitä ja näkökulmia. Kirjoittajat ovat kuitenkin aihealueen kansallisia kärkiosaajia, joten teos sopii hyvin ymmärryksen lisäämiseen ilmiöstä.

Tämän tutkimuksen kannalta merkittävimmät kyberturvallisuuden mittaamista käsittelevät aikaisemmat teokset ovat: *How to Measure Anything in Cybersecurity* (Hubbard & Seiersen 2016), *IT-Security Metrics – Practical Framework for Measuring Security and Protecting Data* (Hayden 2010) sekä *A Survey on Systems Security Metrics* (Pendleton 2016). Teokset eivät ole tieteellisiä, mutta niissä esitetyt menetelmät perustuvat tilastotieteeseen. Lisäksi kirjoittajat hyödyntävät laajasti aikaisempaa tieteellistä tutkimusta näkemyksiensä tueksi. Pendleton ym. (2016) tutkimus tuottaa paljon tietoa järjestelmäturvallisuuden (engl. system security) mittaamisesta. Tutkimuksessa tuodaan esille käytännönläheisiä menetelmiä saada tietoa turvallisuuden tasosta. Tämän tutkimuksen tarkoituksena ei kuitenkaan ole syventyä näihin yksityiskohtiin.

3 KYBERTOIMINTAYMPÄRISTÖ

Suomi on tietoyhteiskuntana riippuvainen sähköisistä tietoverkoista sekä -järjestelmistä, mikä tekee yhteiskunnasta haavoittuvaisen. Digitalisaatio on kuitenkin mahdollistanut toimintojen tehostamisen monilla eri toimialoilla ja tasoilla. Fyysisen ja digitaalisen maailman keskinäisriippuvuutta on alettu kutsumaan *kybertoimintaympäristöksi* (VNp 24.1.2013). Lisääntyvä riippuvuus sähköstä, tietoliikenteestä, verkoista ja näistä muodostuvista palveluista, asettaa vaatimuksia kybertoimintaympäristön turvallisuudelle. Riippuvuuksien lisääntyessä uhkien vaikutukset kasvavat.

Kybertoimintaympäristölle on useita eri määritelmiä, mutta määritelmissä usein yhdistyy kolme asiaa: data, teknologia ja ihmiset. (Edgar & Manz 2017, 34.) Limnéll ym. (2014, 14) määrittelee kybertoimintaympäristön olevan fyysisen ja bittien maailman yhdistelmä, sillä molemmat vaikuttavat toisiinsa. Kybertoimintaympäristönä voidaan pitää kaikkea, mikä liittyy tuotannon toteuttamiseen ja ylläpitämiseen. Ulkoministeriö (2019) määrittelee kybertoimintaympäristön seuraavasti:

> Kybertoimintaympäristöllä tarkoitetaan ihmisten luomaa digitaalista rinnakkaistodellisuutta, joka maailmanlaajuisesti yhdistää informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta toisiinsa ihmisiä ja laitteita valtioiden rajojen yli.

Liiketoiminnassa mahdollisuudet voidaan jakaa liiketoiminnan kasvattamiseen ja kannattavuuden kehittämiseen (Juvonen 2014, 15). Kybertoimintaympäristö mahdollistaa eri hallinnonaloille uusia tapoja suorittaa ydinprosesseja sekä tarjota palveluita asiakkailleen. Esimerkiksi tuotannon kannalta kybertoimintaympäristö mahdollistaa tuotantolinjojen ja -laitosten automatisoinnin. Pilvipalvelut mahdollistavat pääsyn tietoon sekä työkaluihin mistä päin maailmaa tahansa ja milloin tahansa, sillä kybertoimintaympäristössä fyysinen aika ja tila katoavat. Esineiden internet (engl. Internet of Things, IoT) ja laitteiden välinen viestintä mahdollistavat uusia innovatiivisia tapoja hyödyntää teknologiaa. Yritykset kehittävät viestintäteknologiaansa ja -järjestelmiään nopeasti ymmärtämättä välttämättä sen mukana tulevia uusia riskejä. Tämä vaatii organisaatioilta uudenlaista riskienhallintaa. (Keskuskauppakamari 2016, 4.) Kyberturvallisuudesta itsestään on muodostunut liiketoimintaetu.

3.1 Uhka, riski ja haavoittuvuus

Kybertoimintaympäristössä korostuu uhkalähtöisyys. Tällä tarkoitetaan sitä, että ilman uhkia ja riskejä ei ole turvallisuutta. *Uhka* muodostuu vakavuudesta ja uskottavuudesta. Näihin vaikuttaa puolestaan kyvykkyydet, jotka voidaan jakaa materiaalisiin ja taidollisiin. Kybertoimintaympäristössä kaikkia uhkia ei voida ennakoida tai ottaa huomioon. Tämän kaltaisia uhkia on alettu kutsumaan *mustiksi joutseniksi*. (Limnéll ym. 2014, 106.) Kyberuhka on mahdol-

lisuus haitalliselle teolle, jonka tarkoitus on vahingoittaa tai häiritä tietoverkkojärjestelmää (Oxford dictionaries 2019). Uhkia voidaan tarkastella eri tasoilla (kansainvälinen, kansallinen, yritykset ja yksilöt) ja niiden merkittävyys vaihtelee tasoittain.

Mahdollisuuksien mukana tulevat myös *riskit* (Juvonen 2014, 9–10). *Riskillä* tarkoitetaan epävarmuutta ilmiöön liittyvistä menetyksistä, katastrofeista tai muista ei-toivotuista lopputuloksista ja tapahtumista (Hubbard 2014, 84; Kuusela & Reijonen 2005, 28; Juvonen 2014, 8). Riski voidaan toisaalta ymmärtää päätöksenteon uskalluksena sekä valinnan vapautena eri vaihtoehtojen välillä. Riskit koetaan pelottavina, kun niitä ei voida hallita. (Kuusela & Reijonen 2005, 16–17.) Riskit voidaan jakaa *dynaamisiin* ja *staattisiin riskeihin*. Dynaamisista riskeistä voi seurata menetyksiä tai voittoja, kuten esimerkiksi vedonlyönti. Staattisia riskejä voi seurata ainoastaan menetykset, kuten esimerkiksi sairaudet. Staattisten riskien todennäköisyyksiä voidaan arvioida helpommin kuin dynaamisia. Staattisia riskejä vastaan on kehitetty esimerkiksi vakuutukset. (Kuusela & Reijonen 2005, 33–34.) Riskit pitävät sisällään ilmentymisen todennäköisyyden ja vakavuuden. Riskin todennäköisyydellä tarkoitetaan riskin sattumistiheyttä. Vakavuudella tarkoitetaan riskin toteutumisesta aiheutuvaa todennäköistä menetystä. Riskin suuruudella tai vaikuttavuudella tarkoitetaan todennäköisyyden ja vakavuuden yhteisvaikutusta. (Juvonen 2014, 10–13.)

Kyberriski on informaatioteknologian toimimattomuudesta johtuva riski taloudellisesta tai maineellisesta menetyksestä (Institute of Risk Management 2019). Riskit sisältyvät kaikkeen toimintaan eikä niitä voi täysin poistaa tai torjua toisin kuin uhkia. Riski on olemassa olon ehto ja negatiivisen tapahtuman mahdollisuus tulevaisuudessa. Riskien kanssa voi kuitenkin oppia elämään ja niitä voidaan hallita. Riskienhallinnan päämääränä on riskien todennäköisyyksien ja vaikutusten minimoiminen. Se on metodi, jolla pyritään tunnistamaan ja arvioimaan riskejä sekä valitsemaan, kehittämään ja toteuttamaan vaihtoehtoja. Riskienhallinnan voidaan myös katsoa kertovan organisaation luotettavuudesta ja vastuullisuudesta. Onnistuneen riskienhallinnan seurauksena resursseja riskien vähentämiseen saadaan kohdistettua tehokkaasti. (Limnéll ym. 2014, 109.) Teknologia lisää myös riskienhallinnan mahdollisuuksia. Riippuvuuksien lisääntyessä riskien vakavuus ja vaikuttavuus saattavat kuitenkin kasvaa (Kuusela & Reijonen 2005, 36.)

Haavoittuvuus on ominaisuus, joka heikentää järjestelmän toimintavarmuutta. Se voidaan ajatella olevan järjestelmän sisäinen ominaisuus, joka johtuu viasta tai heikkoudesta. Haavoittuvuuksien hallinta on niiden systemaattista tunnistamista, luokittelemista, korjaamista ja lieventämistä. Haavoittuvuus on uhkasta jäljelle jäävä osa, kun siitä on poistettu sietokyky ja palautumiskyky. (Limnéll ym. 2014, 106.)

Yksi kybertoimintaympäristön merkittävimmistä haavoittuvuuksista ovat käyttäjät. Tätä haavoittuvuutta pyritään usein paikkaamaan koulutuksella. Nielsen (2017) tutki organisaation kybervalmiuksia mittaamalla organisaation tietojärjestelmien käyttäjien tietoja, taitoja ja ominaisuuksia. Nielsenin tutkimuksen kirjallisuuskatsauksessa selvisi muun muassa puutteita kybertuvallisuuden mittaamisen määrittelyssä ja saatavilla olevassa kirjallisuudessa. (Nielsen 2017, 4.)

Valtion näkökulmasta vakavimmat kyberuhkat kohdistuvat kriittiseen infrastruktuuriin. Uhkan taustalla saattaa olla terrorismi, rikollisuus, valtiollinen toimija tai valtion tukema toimija. Valtiot saattavat käyttää esimerkiksi rikollisjärjestöjä omien tavoitteidensa saavuttamiseksi, jolloin teot ja valtion osallisuus ovat myös kiistettävissä. (Sisäministeriön julkaisuja 2019:5, 49–50.) Suomen kansallinen riskiarvio 2018 luokittelee kybertoimintaympäristön mahdollistamat uhkat osaksi hybridivaikuttamista (Sisäministeriön julkaisuja 2019:5, 17). Hybridivaikuttaminen on valtiollisen toimijan ei-sotilaallisia keinoja vaikuttaa toisen valtion poliittiseen ja taloudelliseen päätöksen tekoon. Esimerkiksi poliittiseen mielipiteeseen saatetaan vaikuttaa sosiaalisen median välityksellä. Yhteiskunnan toimivuuden kannalta merkittäviä kyberuhkia ovat viestintäpalveluihin ja -verkkoihin kohdistuvat uhkat, sillä muun muassa sähköverkkojen ja maksuliikenteen toiminta ovat riippuvaisia viestintäpalveluiden toimivuudesta. Yleisimmät viestintäpalveluiden häiriöt johtuvat sähkönsaannin häiriintymisestä. Vakavin kyberuhka on hyökkäykset energiantuotantoa ja terveyspalveluita vastaan, sillä silloin saatetaan menettää ihmishenkiä. Muita vakavia uhkia on satelliittipaikannuksen ja fi-verkkotunnuksen nimipalvelujen häiriintyminen. (Sisäministeriön julkaisuja 2019:5, 48–49.) Kriittiseen infrastruktuuriin kohdistuvat hyökkäykset saattavat olla houkuttelevia niiden vaikuttavuuden takia. Suurin osa kriittisestä infrastruktuurista on yksityisten yritysten ja organisaatioiden hallussa. Näin ollen kansallisen tason kyberturvallisuutta ei voida täysin erottaa yritysten ja organisaatioiden kyberturvallisuudesta.

Organisaatiolle uhkat muodostuvat sisäisitä ja ulkoisista uhkista. Ulkoiset uhkat voidaan ajatella olevan organisaation ulkopuolisen tahon tekemä tahallinen ja tarkoitusperäinen hyökkäys. Sisäiset uhkat voidaan jakaa tahallisiin ja tahattomiin uhkiin. Tahattomat uhkat saattavat johtua esimerkiksi tietämättömyydestä, hajamielisyydestä tai piittaamattomuudesta. Ne voivat myös olla tiedostettuja tai tiedostamattomia. (Limnéll ym. 2014, 106.) Tahalliset sisäiset uhkat muodostuvat sisäpiiririkoksista. Sisäpiiririkoksella tarkoitetaan sellaisen henkilön tekemää rikosta, joka kykenee hyödyntämään organisaatiosta saatuja tietoja ja taitoja, joihin muilla ei välttämättä olisi ollut pääsyä. Sisäpiirin tekemät kyberhyökkäykset olivat vuonna 2013 noin 14 % kaikista kyberhyökkäyksistä. Näistä hyökkäyksistä puolissa tapauksista entinen työntekijä hyödynsi vanhoja tunnuksiaan tai takaportteja, joita ei ollut suljettu (Verizone 2013, 5). Vuonna 2018 sisäpiiriläinen oli osallisena 28 % hyökkäyksistä (Verizone 2018, 2).

Sisäpiiriläisen tekemältä hyökkäykseltä saattaa olla hankalampi suojautua. Uhka on kuitenkin todellinen ja sen merkittävyys näyttää kasvavan.

Rikollisuus on siellä missä on arvoa (rahaa). Arvon siirtyessä kybertoimintaympäristöön, rikollisuus siirtyy mukana. Kyberrikollisuudella tarkoitetaan kybertoimintaympäristössä tapahtuvaa rikosta. Merkittävä ongelma käsitteen määrittelyssä on se, että rikollisuus ja rikos on yleisesti sidottuna kansallisiin ja kansainvälisiin lakeihin ja säädöksiin. Kybertoimintaympäristössä on hankala määrittää kansalliset rajat. Rikos saattaa tapahtua Suomessa, mutta hyökkäys saattaa tulla mistä päin maailmaa tahansa. Kybertoimintaympäristössä ei ole kansainvälisesti yhteneväistä lainsäädäntöä, valvontaa tai tutkintaa. Näin ollen tekijän saattaminen edesvastuuseen on hankalaa. Esimerkiksi 2/3 valtioista ei erittele kyberrikollisuutta perinteisestä rikollisuudesta. (Limnéll ym. 2014, 120.) Tämä tekee kyberrikollisuudesta houkuttelevaa. Aika ja tila katoavat näin ollen myös rikollisuudesta, jolloin sen tulisi kyetä katoavan myös torjunnasta ja tutkinnasta. Aina rikosta ei myöskään huomata, jolloin sitä ei raportoida tai tutkita. Kybertoimintaympäristö on myös luonut ennennäkemättömät määrät aineetonta pääomaa, johon kohdistunutta rikollisuutta voi olla vaikea arvottaa. (Limnéll ym. 2014, 119–123.)

Kyberrikollisuuden taustalla saattaa olla yksilö, ryhmä, organisaatio tai valtio. Tekijää on usein vaikea näyttää toteen. Ihmisten moraalikäsitys ei myöskään ole täysin pysynyt muutoksen vauhdissa. Monelle saattaa olla hyväksyttävämpää ladata elokuva internetistä tai kirjautua toisen sosiaaliseen mediaan kuin esimerkiksi varastaa elokuva kaupasta tai käyttää varastettua henkilöllisuustodistusta. (Limnéll ym. 2014, 121.)

Kyberrikollisuus on globaalisti kasvava ongelma. Se käy yhä aggressiivisemmaksi ja kehittyneemmäksi. EU:ssa ongelmaa vastaan perustettiin Europolin yhteyteen *European Cybercrime Center* vuonna 2013 (Europol 2019). Keskusrikospoliisiin perustettiin vuonna 2015 kyberrikostorjuntakeskus (Poliisi 2019).

MIT Technology Review mukaan vuoden 2018 merkittävimmät kyberuhkat olivat (MIT 2019):

- suurten tietomurtojen lisääntyminen
- pilvipalveluihin kohdistuvat kiristysohjelmat (ransomware)
- tekoälyn aseellistaminen
- fyysisten ja kyberhyökkäysten yhdistäminen (esim. sähkönjakelu)
- tietokoneiden kaappaukset kryptovaluutan louhintaan
- vaalien hakkerointi

Kyberturvallisuuskeskuksen julkaisu *Tietoturvan vuosi 2018* listaa ”TOP-5” organisaatioihin kohdistuvat tietoturvauhkat (Kyberturvallisuuskeskus 2018, 5):

- rikolliset pyrkivät rikastumaan tiedoillasi
- ulkoistetut palvelut hyökkääjän lisäväylinä

- näkyvyyden puute
- arvokas tieto aktivoi vakoilijoita
- palvelunestohyökkäykset ovat arkipäivää

Vuonna 2018 Kyberturvallisuuskeskuksen saamista haittaohjelmahavainnoista 57 % koski IoT (Internet of Things) laitteita. Haittaohjelmista on vaikea päästä eroon, sillä suurta osaa haavoittuneista laitteista ei päivitetä. (Kyberturvallisuuskeskus 2018, 12.)

Avoimuus tutkimuksessa ja tiedon jakamisessa vähentää uhkia. Ongelmana on ollut, että organisaatiot pyrkivät peittelemään altistumistaan hyökkäykselle säilyttääkseen maineensa. Maineen menettäminen saattaa vaikuttaa suoraan asiakaskäyttäytymiseen ja näin ollen yrityksen tulokseen. Kybertoimintaympäristöön liittyy paljon tietämättömyyttä, joka lisää ilmiön uhkakeskeisyyttä.

3.2 Kyberturvallisuus

Kyberturvallisuudelle on myös olemassa useita määritelmiä. Yksinkertaisesti kyberturvallisuus on toimenpiteitä, joilla kybertoimintaympäristöstä tehdään turvallinen (Edgar & Manz, 2017, 34.) Kyberturvallisuudella varmistetaan, että kybertoimintaympäristöön voi luottaa ja sen tarkoituksenmukaisesta toiminnasta voidaan huolehtia (Rousku 2014 ,56). Kyberturvallisuus on oleellinen osa organisaatioiden riskienhallintaa (NIST 2018, v). Kyberturvallisuuden varmistaminen on organisaation tulevaisuuden varmistamista (Limnéll ym. 2014, 58).

Tietoturvallisuuden voidaan katsoa olevan tiedon luotettavuuden, eheyden ja saatavuuden turvaamista. Kyberturvallisuus puolestaan pitää sisällään kaiken mikä liittyy tuotannon turvaamiseen (Rousku 2014, 55). Tämä tarkoittaa esimerkiksi sähkön saatavuuden varmistamista, tuotantolinjaston ja automaatiotekniikan toiminnan varmistamista tai tieto- ja maksuliikenteen turvaamista. Turvallisella kybertoimintaympäristöllä pyritään helpottamaan yksilöiden, yritysten ja organisaatioiden toiminnan suunnittelua ja toimintamahdollisuuksia. Sen nähdään myös lisäävän liiketoiminta-aktiivisuutta sekä investointihalukkuutta.

Kyberturvallisuudesta on tullut kymmenessä vuodessa oleellinen osa kokonaisturvallisuutta ja yhteiskunnan elintärkeiden toimintojen turvaamista. Suomen kansallinen riskiarvio 2015 (2016, 18) luokittelee kybertoimintaympäristön riskit yhteiskuntaan laaja-alaisesti vaikuttaviksi riskeiksi. Esimerkiksi rahoitusmarkkinat ovat täysin riippuvaisia sähkönsaannista ja tietojärjestelmien toimivuudesta. (YTS 2017, 57.) Yhteiskunnan turvallisuusstrategiassa 2017 (2017, 57) kyberuhkiin varautuminen nostetaan yhdeksi kehittämisen kohteeksi. Julkisen hallinnon ICT-infrastruktuurin ja digitaalisten palvelujen käyttö on välttämätöntä yhteiskunnan elintärkeiden toimintojen kannalta ja niiden turvallisuus sekä käytettävyys on varmistettava kaikissa tilanteissa. Tämän tavoitteen saavuttamiseksi valtiovarainministeriö on ohjeistanut julkisen

hallinnon ICT-infrastruktuurin, digitaalisten palvelujen ja tietojen turvallisuuden vähimmäisvaatimukset (YTS 2017, 60).

Turvallisuuden luomisessa merkittävää on myös sen keskitetty johtaminen ja johdon sitouttaminen. Prosessien ja tuotteiden suunnittelussa kyberturvallisuus pitäisi ymmärtää sisään rakennettuna (Limnéll ym. 2014, 14, 191–193.) Ihminen ei lähtökohtaisesti halua maksaa turvallisuudesta ylimääräistä, vaan haluaa turvallisuuden sisäänrakennettuna. IoT:n yleistymisen myötä turvallisuusvaatimukset lisääntyvät. Tulevaisuudessa voi joutua hankkimaan palomuurin esimerkiksi jääkaappiin, televisioon tai keittiön lamppuun.

Puolustuskyvyn luomisessa keskeistä on kerroksittainen suojaus. Tämä pitää sisällään esimerkiksi palomuurit, virustorjunnan, tunkeutumiseneston ja -havaitsemisen. Näiden kerroksien on kyettävä myös keskustelemaan keskenään, jolloin puolustukseen saadaan dynaamisuutta (esim. IP:n asettaminen mustalle listalle tai CA-maineen tunnistus) (Limnéll ym. 2014, 195, myös Kurittu 2019). Lisäksi tulee olla sietokykyä ja palautumiskykyä. Kommunikaatiota tarvitaan myös toimijoiden välillä. Useat kybertoimintaympäristön palvelut, kuten esimerkiksi pilvipalvelut, ostetaan ulkopuoliselta taholta. Tietoliikenneverkkojen käyttöoikeudet ostetaan esimerkiksi teleoperaattoreilta. Tällöin kommunikaatio näiden toimijoiden välillä korostuu. Esimerkiksi palvelunestohyökkäyksen sattuessa teleoperaattori kykenee ohjaamaan sisään tuleva hyökkäyksen ”mustaan aukkoon” tai ”pesuripalvelimen” läpi (passiivinen puolustus). Yhteistyötä tarvitaan myös valtion ja sen alla toimivien organisaatioiden välillä. Valtion ensisijainen tehtävä on luoda turvallisuutta (kts. esim. Buzan ym. 1998). Sen tehtävä on luoda turvallinen ympäristö, jossa organisaatiot voivat toimia. Passiivisten puolustusmenetelmien lisäksi on kehitetty aktiivisia puolustusmenetelmiä, joiden tarkoituksena on hyökätä hyökkääjää vastaan. Ongelmana on, ettei todellista tekijää välttämättä tiedetä tai ettei puolustavalla hyökkäyksellä rikota lakia. Keskeistä on luoda uskottava puolustus, jolloin vaikutus on ennaltaehkäisevä. (Limnéll ym. 2014, 193–196.) Loppupeleissä kyberpuolustus on kuitenkin vain niin vahva kuin sen heikoin lenkki. Tätä korostaa jatkuvasti kasvava hyökkäyspinta-ala ja *nolla-päivä*-haavoittuvuudet. Näin ollen rajallisten resurssien kohdentaminen oikeisiin puolustusmenetelmiin korostuu. Puolustaja joutuu puolustautumaan kaikkialla, kun taas hyökkääjä voi valita minne hyökätä. (Fielder 2016, 13–14.)

Yhä useampi toiminnallisuus kybertoimintaympäristössä ulkoistetaan, mukaan lukien turvallisuus. Tämä tuo mahdollisuuksia, mutta myös haasteita. Yrityksen kannalta ulkoistaminen saattaa tuoda säästöjä ja tehostaa toimintaa. Harhaluulona saattaa olla, että ulkoistamisen mukana myös uhkat ja riskit ulkoistetaan. Ongelmana on kuitenkin se, että vaikka esimerkiksi pilvipalvelu on toisen yrityksen palvelimella, niin varastetut tiedot ovat palvelunottajan. Näin ollen epätietoisuus lisääntyy siitä, miten palveluntarjoaja on hoitanut kyber- ja tietoturvansa tai kuka vastaa mahdollisista tappioista. Hyökkäyspinta-alan pienentäminen on yksi keino

vähentää uhkia. Uhkien ja riskien kasvaessa kaikessa toiminnassa korostuu jatkuvuuden hallintasuunnitelma.

Kyberturvallisuus on mahdollisuuksien ja uhkien välistä tasapainottelua. Usein ilmiössä korostuvat uhkat, kun pitäisi korostaa mahdollisuuksia. (Limnéll ym. 2014, 15.) Täydellistä kyberturvallisuutta ei ole, kuten ei ole täydellistä fyysistä turvallisuuttakaan. Kyberturvallisuusprofessori Jarno Limnéllin mukaan parhaiten uhkiin varaudutaan laittamalla perusasiat kuntoon (Limnéll ym. 2014, 107). Mitä enemmän kybermahdollisuuksia hyödynnetään, sitä enemmän uhkia ja riskejä kohdataan (Limenll ym. 2014, 158). Tietoverkko on joko turvallinen tai turvaton (Wang ym. 2017, 3).

3.2.1 Kyberturvallisuusstrategia

Yritysten kannalta strategiaa voidaan pitää keinona ja menetelmänä saavuttaa päämäärä eli tavoite, joka on usein liitettynä liiketoiminnan tuottavuuteen (Hammarsten, 2017). Strategia kertoo kuinka yritys luo arvoa omistajille ja asiakkaille (Juvonen 2014, 34). Strategia voidaan ymmärtää myös suunnitelmakokonaisuutena, jossa tunnistetaan yrityksen nykytila, toimintaympäristön muutokset ja asiakkaiden tarpeet. Tavoitteena on saavuttaa kilpailuetu suhteessa muihin. (Hiltunen, 2017). Näiden tavoitteiden saavuttamista pitää kyetä arvioimaan, jonka tueksi on kehitetty erilaisia mittareita (Hammarsten, 2017).

Kybertoimintaympäristön mukana tulleet haasteet ovat johtaneet eritasoisten suositusten julkaisuihin, joilla pyritään parantamaan kybertoimintaympäristön turvallisuutta. Tämän kaltaisia julkaisuja voivat olla esimerkiksi (Kauppakamari 2016, 6):

- ylätason visioita sisältävät suositukset
- suosituksiin perustuvat kansalliset strategiat, jotka sidotaan esimerkiksi toimintaympäristön lainsäädäntöön (esim. *Suomen kyberturvallisuusstrategia)*
- strategioista johdetut viitekehykset, joiden avulla organisaatiot voivat arvioida ja kehittää omaa toimintaansa (esim. NIST CSF)
- standardit, jotka ohjaavat organisaation prosesseja tietoturvallisempaan suuntaan ”parhaiden käytäntöjen” avulla (esim. ISO 27001)
- tekniset standardit, jotka ohjaavat rajapintojen yhteensovittamista (esim. HTTPS)

Vuonna 2011 päätettiin käynnistää kansallisen kyberturvallisuusstrategian laatiminen osana yhteiskunnan turvallisuusstrategian toimeenpanoa. Suomen kyberturvallisuusstrategiassa (2013) määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus. (VNp 24.1.2013)

> Kyberturvallisuusstrategialla luodaan yhteinen ymmärrys kyberturvallisuudesta ja vahvistetaan yhteiskunnan kokonaisturvallisuutta. Strategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. Kyberturvallisuusstrategian linjausten ja niiden toteuttamiseksi tarvittavien toimenpiteiden avulla Suomi kykenee kansallisesti hallitsemaan kybertoimintaympäristön tahallisia tai tahattomia haittavaikutuksia sekä vastaamaan ja toipumaan niistä. (Turvallisuuskomitea, 2013)

Suomen kyberturvallisuuden visiona on muun muassa suojata elintärkeät toiminnot kaikissa tilanteissa. Lisäksi visiona on varmistaa mahdollisuus hyödyntää kybertoimintaympäristöä tehokkaasti kaikilla tasoilla. (VNp 24.1.2013, 3.) Strategian yhdeksännessä linjauksessa otetaan kantaa vaatimusten hallintaan, jonka voidaan katsoa pitävän sisällään kyvykkyyksien analysoinnin ja mittaamisen (VNp 24.1.2013, 10):

> Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle. Kyberturvallisuuden kehittäminen vaatii selkeää vastuiden määrittelyä ja tehtävien jakoa strategisten linjausten mukaisesti. Käytännössä tämä edellyttää, että kukin hallinnonala tekee riskiarvioinnin ja kypsyysanalyysin, joiden avulla tunnistetaan kyberturvallisuuden kannalta merkittävät haavoittuvuudet ja riskit sekä niiden hallinnan taso. Saatujen tulosten perusteella laaditaan kunkin hallinnonalan toimeenpano-ohjelmat sekä tuetaan elinkeinoelämän toimeenpano-ohjelmien tekemistä yhteistoiminnassa huoltovarmuusorganisaation kanssa.

Osana kyberturvallisuusstrategian toimeenpano-ohjelmaa on kehitteillä kyberturvallisuuden kypsyysmalli, jolla voidaan mitata toiminnan tasoa ja kehittymistä (VNp 24.1.2013, 38). Valtiovarainministeriön julkaiseman toiminnan jatkuvuuden hallinnan ohjeen (VAHTI 2/2016) tarkoituksena on antaa suosituksia organisaation toiminnan turvaamiseksi kehittämällä varautumis-, jatkuvuus-, toipumis- ja valmiussuunnittelua. Suunnitelmien avulla organisaatio voi varautua erilaisiin normaaliolojen häiriötilanteisiin sekä poikkeusoloihin. VAHTI-ohjeita on annettu 2000-luvun alusta alkaen. Vuonna 2014 julkaistiin VAHTI tietoturvallisuuden arviointi -ohje. Viranomaisten osalta tietoturvallisuuden arviointi perustuu *lakiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista* 1406/*2011* (VAHTI 2/2014, 27).

Yritysten kyberstrategia voidaan jakaa kolmeen tasoon: strateginen, operatiivinen ja kyvykkyyksien taso. Strategisella tasolla määritellään mitä kybermahdollisuuksia käytetään tulevaisuudessa sekä mitä tunnettuja mahdollisuuksia ja uhkia ne pitävät sisällään. Lisäksi määritellään kyberalttiit prosessit. Operatiivisella tasolla määritetään millaisia turvallisuusprosesseja, -käytäntöjä ja -malleja tarvitaan sekä miten ne toimeenpannaan. Strategiasta luodaan mahdollistamissuunnitelma ja turvallisuussuunnitelma. (Limnéll ym. 2014, 179.) Mahdollistamissuunnitelmassa määritellään, mitä pitää tehdä, jotta strategisella tasolla valitut mahdollisuudet voidaan toteuttaa. Turvallisuussuunnitelmassa määritellään, mitä pitää tehdä, jotta voidaan minimoida tunnetut uhkat, hallita riskejä ja mitata turvallisuuden tasoa. (Limnéll ym. 2014, 180.) Kyvykkyyksien tasolla määritellään, miten mahdollistamissuunnitelma ja turvallisuussuunnitelma saadaan toteutettua. Määrittelyn tukena voidaan käyttää arvioita neljästä osa-alueesta: ihmiset (ml. säännöt ja ohjeistukset), prosessit, teknologia ja palvelut. Näiden osalta voidaan arvioida, tarvitaanko uusia osaajia, prosesseja tai palveluita. Lisäksi voidaan tarkastella mikä teknologia sopii parhaiten. (Limnéll ym. 2014, 180.)

3.3 Yhteenveto

Tutkimuksen ensimmäisen vaiheen johtopäätöksenä on, että kyberturvallisuus on monimutkainen sekä muuttuva ilmiö ja siitä voidaan saada tietoa eri tasoilla. Mahdollisuudet tuovat mukanaan riskejä. Lisääntyvä riippuvuus teknologiaan korostaa uhkia ja lisää riskien vakavuutta. Turvallisuuden tilasta voidaan saada tietoa arvioimalla toimintaympäristön uhkia, riskejä ja haavoittuvuuksia. Kyberturvallisuus on tuottamatonta toimintaa, joten siihen ei haluta panostaa, elleivät riskit liity suoraan liiketoimintaprosesseihin (Kurittu 2019).

Tutkimuksen toisessa vaiheessa sovelletaan kyberturvallisuuden mittaamiseen teoriaa Limnéll ym. (2014) mukaisesta kyberturvallisuusstrategian taso-jaottelusta (strateginen, operatiivinen, kyvykkyydet). Yrityksen kybervalmiuksia voidaan arvioida kypsyysmallien avulla, jotka kertovat laajemmin siitä, mitkä valmiudet yrityksellä on kohdata kyberuhkia ja -riskejä. Tähän liittyy olennaisesti muun muassa kyberturvallisuusstrategia. Toiminnallisella tasolla kyberturvallisuudesta voidaan saada tietoa muun muassa tunnistamalla hyökkäyksiä, turvallisuusmekanismien suunnittelulla, sovellusturvallisuudella, virus- ja uhka-analyysillä, riskienhallinnalla ja kryptografialla. Tutkimusaineiston perusteella yritysten ja organisaatioiden näkökulmasta kyberturvallisuutta voidaankin kuitenkin parhaiten mitata riskienhallinnalla ja -analyysillä.

Tässä tutkimuksessa ei kyetä kattavasti tarkastelemaan kaikkia ylläkuvattuja menetelmiä ja näkökulmia. Tutkimuksen toinen vaihe keskittyy käsittelemään kyberturvallisuuden riskienhallintaa. Näin ollen tutkimuksen toisen vaiheen teoriasidonnaiseen sisällönanalyysiin johdetaan teoriaa myös riskienhallinnan periaatteista ja sen soveltamisesta kyberturvallisuuden mittaamiseen. Mittaamisen tulisia aina perustua jonkin tavoitteen saavuttamiseen. Näitä tavoitteita tulisi asettaa yritysten ja organisaatioiden strategioissa. Näin ollen onnistunut kyberturvallisuuden mittaaminen tulisi perustua kyberturvallisuusstrategian asettamiin tavoitteisiin.

4 KYBERTURVALLISUUDEN MITTAAMINEN

4.1 Mittaaminen

Strategisten mittareiden onnistunut asettaminen vaatii, että yrityksen johto tietää mitä pitää saavuttaa ja miten siihen päästään. Strategian mukaiset mitattavat tavoitteet ja vastuu niiden saavuttamisesta merkitsee tulosvastuuta, joka voi tarkoittaa muutakin kuin rahamäärää. Mittarit kertovat mitkä asiat ovat tärkeitä: ”*Kun kaikki on tärkeää, mikään ei ole tärkeää*”. Tavoitteiden, toiminnan ja lopputuloksen linkittäminen muodostaa syy-seuraus -ketjuja. Toimintavarmuus puolestaan synnyttää asiakasuskollisuutta, mikä saattaa näkyä kannattavuudessa. Liiketoiminnassa mitattavia asioita voivat olla esimerkiksi asiakastyytyväisyys tai -käyttäytyminen. (Hammarsten, 2017.)

Mittaamisen tarkoituksena on saada sellaista tietoa, jonka avulla voidaan tehdä johtopäätöksiä. Mittaamisen tulisi olla tieteellinen prosessi, jonka perusteella voidaan tehdä analyyseja ja hypoteeseja. Näitä voidaan testata ja testien perusteella voidaan tehdä ennusteita tulevaisuudesta. Mittaamisen perusteella halutaan saada tehtyä jotain, eikä vain tietää jotain. Päämääränä on tuottaa konkreettista totuuteen perustuvaa tietoa päätöksenteon tueksi. (Ylisirniö, 2011, 23.) Ylisirniön mukaan mittaaminen tulisi olla systemaattista ja määrällistä. Laadullinen mittaaminen tuottaa liian subjektiivisia tuloksia, jolloin liikutaan liian yleisellä tasolla. Haydenin (2010, 11) mukaan kuitenkin myös laadullisilla menetelmillä voidaan saada luotettavia tuloksia. Strategiaa ei ole ilman ihmisiä, jolloin konstruktivistista näkökulmaa ei voida tutkimuksissa täysin sivuuttaa. Strateginen analyysi pitää kuitenkin sisällään niin monta eri asiaa, että kokonaisvaltaiseen mittaamiseen tulisi käyttää matemaattistilastollisia menetelmiä ja teknologiaa hallitsemaan volyymeja. (Ylisirniö, 2011, 36.)

Kybertoimintaympäristön mahdollisuuksien mukana aineeton pääoma on kasvattanut merkitystään. Tietoa on saatavilla ja kerättävissä analysointia varten ennennäkemätön määrä. Pääasiassa yritykset mittaavat fyysisiä asioita, kuten tulosta. Näin ollen aineettoman pääoman, kuten tiedon tai turvallisuuden, hyödyntäminen jää taka-alalle. Onnistunut johtaminen vaatii onnistunutta mittaamista. (Kaplan & Norton, 2004, 11). Aineettoman pääoman merkitys muuttuvassa kybertoimintaympäristössä tulee vain korostumaan. Hyvä turvallisuuden mittari on määrällinen, objektiivinen, perustuu muodolliseen malliin, sisältää aikaulottuvuuden, on yleisesti hyväksytty, perustuu totuuteen, on kustannustehokas, saatavissa ja toistettavissa. (Abbadi, 2006, 5.)

Kyberturvallisuuden mittarit ja mittaaminen voivat auttaa organisaatiota varmistamaan, että turvallisuustoimenpiteet ovat yhteneväiset menettelytapojen, prosessien sekä ohjeistuksien kanssa. Niiden avulla voidaan arvioida myös turvallisuuden heikkouksia sekä vahvuuksia.

Lisäksi voidaan tarkastella ja tunnistaa organisaation sisäisiä ja ulkoisia turvallisuuden trendejä. Trendien avulla voidaan arvioida turvallisuuden suorituskykyä ajan kuluessa ja tilanteen muuttuessa. Organisaation tulisi ensin määrittää mitä halutaan mitata eli mistä halutaan tietoa. Tämän jälkeen tulee selvittää, että miten haluttua tietoa voidaan saada. Mittaamisen avulla voidaan selvittää jonkin asian tilaa (esim. päivitettyjen sovellusten lukumäärää) tai asetettujen tavoitteiden saavuttamista. (Black ym. 2008, 1–2.) Myös Kurittu (2019) korostaa trendien ja muutossuuntien ymmärtämisen merkitystä päätöksenteossa.

Kyberturvallisuutta voidaan auditoida ja arvioida. Näitä kahta ei tule sekoittaa toisiinsa. Auditoinnin tarkoituksena on selvittää, miten nykyiset kyberturvallisuuden konfiguraatiot vastaavat tavoitetilaa. Se ei kerro kuinka hyvä kyberturvallisuus on, vaan tarjoaa ainoastaan näkökulman turvallisuudesta. Kyberturvallisuuden arvioinnilla pyritään tunnistamaan riskejä ja haavoittuvuuksia. Haavoittuvuuksien arviointi on tekninen suoritus, jossa toimintaympäristöstä pyritään löytämään ja priorisoimaan mahdollisimman monta haavoittuvuutta. Miesslerin (2019) mukaan riskienhallinta ja -mallintaminen tulisi olla hyväksyttävän riskitason määrittämistä, nykyisen riskitason mittaamista sekä näiden kahden yhteensovittamista. Tähän toimintaan on yleisesti käytetty sekä määrällisiä että laadullisia menetelmiä. Riskienarviointi tulisi Miesslerin mukaan ymmärtää sateenvarjokäsitteenä sille, mikä on tärkeää ja miten siihen voidaan hyökätä, mitä menetät jos hyökkäys onnistuu sekä mitä voidaan tehdä hallitakseen tätä riskiä. Riskimallinnus on prosessi, jossa dokumentoidaan ja visualisoidaan miten uhkatekijät, haavoittuvuudet, hyökkäykset, vastatoimet ja vaikutukset liittyvät toimintaympäristöön. (Miessler, 2019.) Rouskun mukaan riskienhallinta on kyberturvallisuuden tärkeimpiä termejä. Hänen mukaansa kaikki tietoturvallisuuden ja jatkuvuuden hallinnan kehittämisessä tehtävä työ on riskienhallintaa. Riskienarviointi mahdollistaa resurssien kohdentamisen sinne, missä uhkan todennäköisyys ja vaikutus ovat suurimmat. (Rousku 2014, 61.)

Miesslerin mukaan mittariston tulee ennen kaikkea edistää toimintaa. Hyvä turvallisuuden mittaristo pitää sisällään yhdeksän osa-aluetta (Miessler, 2018a):

- Päätöksentekoa tukeva: mittarin tulisi johtaa toimenpiteisiin.
- Konkreettinen: mittarin tulisi perustua määrälliseen tietoon.
- Strategiaa tukeva: mittarin tulisi kertoa strategiasta, mikä on tärkeää.
- Dataan perustuva: mittari pitää pystyä selittämään ja esittelemään eri tasoisille ihmisille organisaatiossa.
- Toistettava: mittaristoon tulisi olla helppo kerätä tietoja ja se tulisi olla helposti päivitettävissä.
- Resursseihin suhteutettu: mittariston tulee olla suhteutettuna käytössä oleviin resursseihin. Sellaista ei kannata mitata, mitä ei voida muuttaa.
- Diskreetti: mittaristo tulisi jaotella tarpeen mukaisiin osiin, jolloin voidaan mitata juuri sitä dataa mitä halutaan, jolloin parannetaan läpinäkyvyyttä.
- Tarkoituksenmukainen: mittariston tulee mitata asioita, joilla on merkitystä, eikä sellaista mitä on vain helppo mitata.
- Optimaalinen: usein vähemmän mittareita on parempi kuin useita. Ennen uusien mittareiden käyttöönottoa tulee tarkastaa, että edelliset mittaristot tuottavat maksimaalista hyötyä.

Miesslerin (2018a; kts. myös Hayden 2010, 17) mukaan turvallisuudesta voidaan mitata muun muassa turvallisuuteen käytettyjä resursseja suhteessa saavutettuun hyötyyn, turvallisuushenkilöstön kokoa ja osaamista, perussuojaustoimintojen määrää (esim. virustorjunta), ohjelmistojen päivitysviivettä, turvallisuuspoikkeamien määrää henkilöstössä, organisaatiossa tapahtuneiden muutosten määrää sekä salasanojen vahvuuksia. Lisäksi erilaisten poikkeamien tarkastelu tarjoaa tietoa turvallisuuden tilasta (Kurittu 2019). Wang ym. (2017) mukaan verkkoturvallisuutta on perinteisesti mitattu haavoittuvuuksien kautta. Heidän mukaansa menetelmä on kuitenkin puutteellinen. Wang ym. esittää, että haavoittuvuuksia hyödynnettäisiin turvallisuuden analysoinnissa hyökkäyskraafien ja beyasin verkoston avulla. (Wang ym. 2017, 2–4.)

Tietoturvallisuuden johtamiseen, kehittämiseen ja hallinnointiin on olemassa useita menetelmiä. Yksi yleisesti tunnettu standardi on ISO 27001 (the International Organization for Standardization), joka tarjoaa yleisesti hyväksytyn prosessiperusteisen menetelmän tietoturvallisuuden hallintaan. ISO 27004 tarjoaa työkaluja mittaamisen ja mittareiden määrittämiseksi. (ISO 2019a.) Esimerkiksi viranomaisten tietoturvallisuuden arvioinnissa voidaan käyttää ISO 27001 perusteista arviointimenetelmää (VAHTI 2/2014, 25). Katakri on puolestaan viranomaisten käyttämä auditointimenetelmä, jolla viranomaiset voivat arvioida organisaation kykyä turvata viranomaisten salassa pidettävää materiaali (Puolustusministeriö 2019).

4.2 Kyberturvallisuuden kypsyysmalli

Lehto ym. (2018, 66) esittää, että kansallisella tasolla kyberturvallisuutta tulisi mitata vuosittain, jolloin syntyisi vuotuinen kyberturvallisuuden arvio. Arviossa tarkasteltaisiin kyberturvallisuuden eri osa-alueita ja niiden sen hetkistä tilaa. Kansallinen kyberturvallisuuden arviointimalli parantaa yritysten ja organisaation kykyä arvioida omaa kyberturvallisuuttaan. Tällä hetkellä Suomessa ei ole olemassa selkeitä kyberturvallisuuden tason mittareita, mikä hankaloittaa kehityksen kokonaisvaltaista arviointia. Lehto esittää, että vuosittainen mittaaminen tulisi pakolliseksi yhteiskunnan kriittisten toimijoiden osalta, jolloin se koskisi myös useita yrityksiä ja organisaatioita. (Lehto, ym 2018, 66.)

Yleisesti ottaen kyberturvallisuuden kypsyysmalli on keino arvioida strategisella tasolla organisaation nykytilaa ja kehittää kyberturvallisuutta. Se tarjoaa ikään kuin polun, jolla pysymistä voidaan arvioida. Saatavilla on useita erilaisia turvallisuuden ja kyberturvallisuuden kypsyysmalleja. (Christopher, 2018.) Tässä tutkimuksessa tarkastellaan *National Institute of Standards and Technology cybersecurity framework* (NIST CSF) -mallia sekä Hubbard & Seiersenin (2016) esittämää mallia, jotka ovat tarkoitettu organisaatioiden ja yritysten kyber-

turvallisuusvalmiuksien arviointiin. Näiden kahden erilaisen lähestymistavan tarkastelulla on tarkoitus luoda mahdollisimman kattava kuva valmiuksien arviointimenetelmistä.

4.2.1 NIST Cyber Security Framework (CSF)

National Institute of Standards and Technology (NIST) on Yhdysvaltojen kauppaministeriön alaisen virasto, jonka tehtävänä on edistää innovaatiota ja standardeja. NIST CSF-viitekehyksen luontiprosessi käynnistyi Yhdysvaltojen presidentin Barack Obaman säädöksestä vuonna 2014 (Cybersecurity Enhancement Act of 2014). Säädöksen tarkoituksena ja tavoitteena on parantaa Yhdysvaltojen kriittisen infrastruktuurin kyberturvallisuutta. NIST *Framework for Improving Critical Infrastructure Cybersecurity* versio 1.1 julkaistiin 16.4.2018, jolloin se korvasi vuoden 2014 versio 1.0:n. NIST kannustaa organisaatioita tarvittaessa muokkaamaan mallia tarpeidensa mukaan, jotta siitä saataisiin maksimaaliset hyödyt. CSF-kypsyysmalli perustuu organisaation itsearviointiin ja sen tarkoituksena on kustannustehokkaasti auttaa organisaatioita tunnistamaan, arvioimaan ja hallitsemaan kybertoimintaympäristöön liittyviä riskejä. (NIST 2018, i–iii, v.) Viitekehyksen ei ole tarkoitus toimia valmiina ja yleispätevänä mallina, joka toimii kaikille. Sen tarkoitus on auttaa organisaatiota kehittämään oma lähestymistapansa kyberturvallisuuteen, jolloin organisaatiolle ominaiset vaatimukset, uhkat, riskit, haavoittuvuudet ja sietokyky tulevat huomioitua mahdollisimman tehokkaasti. Viitekehys tähtää riskien vähentämiseen ja hallintaan. (NIST 2018, 2.) Viitekehys muodostuu kolmesta osa-alueesta: viitekehyksen ydin, toteutusasteet ja viitekehysprofiilit.

Viitekehysydin koostuu joukosta kyberturvallisuuden aktiviteettejä, toivottuja lopputuloksia ja sovellettavia referenssejä, jotka ovat yleisiä eri toimialoilla. Viitekehysydin ohjaa organisaatiota kehittämään omaa kyberturvallisuusprofiiliaan. Sen avulla voidaan priorisoida toimenpiteitä, riskitoleranssia ja resursseja. Ydin pitää sisällään viisi arvioitavaa toiminnallisuutta: tunnista (identify), suojaa (protect), havaitse (detect), vastaa (respond) ja palaudu (recover). Toiminnallisuudet jaetaan kategorioihin, alakategorioihin ja informaatioreferensseihin. Näiden tarkoituksena on auttaa organisaatiota saavuttamaan kyberturvallisuudelle asetetut tavoitteet. Tarkasteltaessa kaikkia viittä toiminnallisuutta yhdessä saadaan strategisen tason näkökulma organisaation kyberturvallisuusriskien hallintaan. (NIST 2018, 3.)

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Kuva 2. Viitekehysydin (alkuperäinen kuva: NIST: *An Introduction to the Components of the Framework*) (NIST 2019)

Toteutusasteet (tier) auttavat organisaatiota saavuttamaan kyberturvallisuustavoitteensa. Se tarjoaa organisaatiolle kontekstin, jonka avulla organisaatio näkee itsensä, omat riskinsä ja omat riskienhallintaprosessinsa. Organisaatio voidaan luokitella eri asteille (tier), jotka kertovat sen tilasta ja kehityksestä. (NIST 2018, 3–4.) Ensimmäisellä tasolla organisaation kyberturvallisuus on kehitysvaiheessa. Toisella tasolla organisaation kyberturvallisuus on muodostumassa ja vakiintumassa. Kolmannella tasolla organisaation kyberturvallisuussuunnitelma tai -strategia on määritetty ja hyväksytty. Viimeisellä tasolla yritys on toimeenpannut kyberturvallisuusstrategiansa, kehittää sitä jatkuvasti ja etsii aktiivisesti tietoa uusista uhkista pysyäkseen kehityksen edellä. Valitessaan astetta, tulee organisaatiossa tarkastella nykyisiä riskienhallintakäytäntöjä, uhkaympäristöä, laillisia ja säädöksellisiä vaatimuksia, liiketoiminnan tai toiminnan tavoitteita sekä organisaatiolliset rajoitteet. (NIST 2018, 8–10.)

Viitekehysprofiili kuvaa organisaation nykytilaa ja mahdollista tulevaa tavoitetilaa. Tällöin organisaatio kykenee tarkastelemaan näiden kahden tilan eroja sekä toimenpiteitä, joita pitää tehdä. Tarkoituksena on auttaa organisaatiota kyberturvallisuuden toimeenpanossa. Sen avulla voidaan järjestää ja priorisoida kyberturvallisuustoimenpiteitä. (NIST 2018, 4.)

Viitekehysydin on prosessi kyberturvallisuuden parantamiseksi. Ensimmäinen vaihe on *tunnistaa* organisaation omat toiminnot, prosessit ja tietojärjestelmät. Mitkä niistä ovat kriittisiä, mitä tietoa ne sisältävät ja mitkä vaativat suojausta. Kun tunnistus on toteutettu, voidaan sen perusteella tehdä *suojaus*toimenpiteitä. Kun suojaukset ovat kunnossa voidaan *havainnoida* toimintaa ja havaintojen perusteella tarvittaessa kehittää suojausta. Jos jotain tapahtuu, tulee siihen kyetä *vastaamaan*. Tämä tarkoittaa esimerkiksi toimintasuunnitelmaa, sisäistä ja ulkoista kommunikointisuunnitelmaa (kriisiviestintä) sekä muita toimenpiteitä, joihin on ryhdyttävä hyökkäyksen tapahduttua. *Palautuminen* pitää sisällään oppimisprosessin (lessons-learned). Sen tarkoituksena on varmistaa, että haavoittuvuus on korjattu, prosessit ovat toimintakuntoisia ja tapahtumasta on opittu. (NIST 2018, 7–8.)

Jokainen toiminnallisuus jaetaan kategorioihin, joiden tarkoituksena on tarkentaa toiminnallisuuksia. Nämä kategoriat jaetaan vielä alakategorioihin, jolloin toiminnallisuus tarkentuu entisestään. Esimerkiksi riskienhallinta voi olla *tunnistamisen* kategoria ja riskienhallinnan alakategoria saattaisi olla menetelmät, joilla sitä tehdään. *Informatiiviset referenssit* ovat parhaita käytäntöjä tai suosituksia, siitä miten kyseisten toiminnallisuuksien osalta kannattaisi toimia. (NIST 2018, 7.)

Viitekehystä on kritisoitu siitä, että se on käytännössä itsearviointi. Tämä tarkoittaa sitä, että se perustuu organisaation subjektiiviseen näkemykseen. Näin ollen tieto ei ole objektiivisesti vertailukelpoista. Viitekehyksen käyttöönotto perustuu vapaaehtoisuuteen, mutta vaatii huomattavia resursseja, jolloin yksityiset yritykset ja organisaatiot saattavat vältellä sitä. Toisaal-

ta hyökkäyksen haittavaikutukset saattavat olla huomattavasti suuremmat. Ennen kuin mitään on tapahtunut resurssein kohdentamista viitekehyksen mukaiseen toimintaan voi olla vaikea perustella. Useat asiantuntijat kuitenkin suosittelevat sen käyttämistä. Etuna viitekehyksessä on myös, että se tarjoaa organisaatioille yhteisen kielen, jolla keskustella ja vaihtaa tietoa kyberturvallisuudesta. (Brook 2018.) Tämä parantaa puolestaan tiedon saatavuutta.

4.2.2 Operatiivisen turvallisuuden mittarit

Hubbard & Seiersen (2016, 207) esittelevät oman näkemyksensä kypsyysmallista. Heidän mallinsa keskiössä on ennakoiva analytiikka. Periaatteena on, ettei organisaatio tarvitse merkittävää määrää tietoa tai kyvykkyyksiä päästäkseen alkuun. Organisaation valmiudet määrittyvät sen mukaan, kuinka kehittynyttä organisaation analytiikka on. Organisaatioiden ei myöskään tule rynnätä kehittyneiden menetelmien kimppuun, vaan aloittaa perusmenetelmistä. Perusmenetelmät auttavat ymmärtämään tarpeet, jolloin kyvykkyyksien kehittäminen on järkevää. Teknologia ja menetelmät saattavat tuoda liikaa häiriötekijöitä päätöksen tekoon, jolloin päätöksenteko hankaloituu. Mittaamisessa on lopulta kyse päätöksen teon tukemisesta.

Operatiivisen turvallisuuden mittarit -malli (Operational Security-Metrics Maturity Model) jaetaan neljään tasoon (Hubbard & Seiersen 2016, 207):

- hajanaisen tiedon analytiikka (Sparse Data Analytics – SDA)
- toiminnalliset turvallisuuden mittarit (Functional Security Metrics – FSM)
- turvallisuustietovarastot (Security Data Marts – SDM)
- ohjaileva turvallisuusanalytiikka (Prescriptive Security Analytics – PSA)

Hajanaisen tiedon analytiikka tarkoittaa sitä, ettei organisaatio tarvitse suuria määriä tietoa tehdäkseen ennakoivia päätöksiä. Organisaatiolla on usein enemmän tietoa kuin he luulevat ja he tarvitsevat vähemmän tietoa kuin uskovat. Yksinkertaisten menetelmien avulla, organisaatio kykenee tehostamaan riskienhallintaa huomattavasti vähäisellä tietomäärällä. Organisaatio pääsee alkuun pelkillä asiantuntijan arvioilla, joita voidaan täydentää ja päivittää uuden tiedon ilmaantuessa. SDA:n avulla organisaatio kykenee määrittämään tarvitsemansa investoinnit turvallisuuden kehittämiseen. (Hubbard & Seiersen 2016, 208)

Käytännössä Hubbard ja Seiersen esittävät tilasto- ja todennäköisyyslaskennan hyödyntämistä organisaation riskienhallinnassa. Nämä menetelmät eivät ole liian haastavia, sillä niitä voi toteuttaa esimerkiksi Excel-ohjelman avulla. Käytettäviä menetelmiä ovat muun muassa Monte Carlo -simulaatio, Bayesin metodi, beta-jakauma sekä todennäköisyyskalibrointi -koulutus.

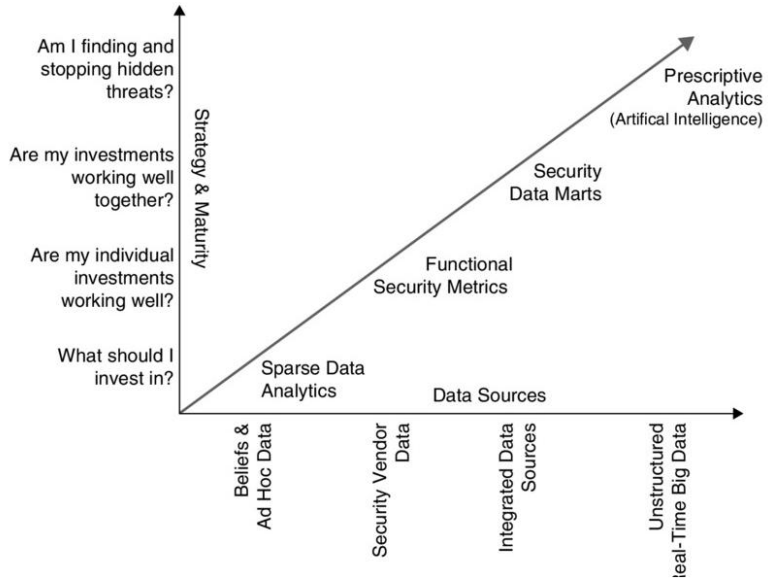
Toiminnallisten turvallisuuden mittareiden (FSM) tarkoituksena on selvittää hankittujen järjestelmien ja kyvykkyyksien vaikutus kyberturvallisuuteen. Tarkoituksena on optimoida tärkeimmät kyberturvallisuuden toiminnallisuudet. Toiminnallisuuksia voivat olla esimerkiksi virustorjunta, palomuuri, penetraatiotestaus, verkkoturvallisuusratkaisut ja turvallisuusarkkitehtuuri. FSM tähtää siihen, että kaikkien toiminta on konfiguroitua ja niiden kattavuudet ovat tiedossa. (Hubbard & Seiersen 2016, 208–209.)

Turvallisuustietovarastot (SDM) ovat tietokantoja, jotka tuottavat tietoa eri järjestelmistä riskienhallinnan tueksi. Tarkoituksena on tuottaa tietoa ohjelmien ja järjestelmien välisestä tehokkuudesta. Se vastaa kysymykseen: ”Toimivatko henkilöt, prosessit ja teknologia yhdessä tehokkaasti vähentääkseen riskiä eri osa-aluilla tai ovatko toiset kontrollit tehokkaampia kuin toiset”. Käytännössä tavoitteena on tarkastella miten hyvin käyttöönotetut järjestelmät, kyvykkyydet ja menetelmät vähentävät riskejä. Lisäksi tavoitteena on havaita päällekkäisyyksiä ja ylimäärää turvallisuusratkaisuissa. Tietovarastojen avulla voidaan myös selvittää, mikä on hyökkäysten havainnointiaika, mikä sen pitäisi olla ja kuinka paljon halutun tason saavuttaminen maksaa tai kuinka kauan hyökkäys on kestänyt, ennen kuin se on havaittu. Tämän kaltaista tietoa voidaan saada toiminnallisuuksista, kuten: (Hubbard & Seiersen 2016, 209–211.)

- virustorjunta
- whitelisting
- tiedostojen eheyden valvonta
- maineen varmistus
- haavoittuvuuksien hallinta

Ongelmana jäännösriskin arvioinnissa on se, että turvallisuusratkaisuissa ollaan hyökkääjää aina jäljessä. Tätä jäännösriksiä voi ja tulee kuitenkin mitata ja sitä kautta hallita. Tähän tarkoitukseen tietovarastot ovat käyttökelpoisia. (Hubbard & Seiersen 2016, 211.)

Ohjaileva turvallisuusanalytiikka (PSA) voidaan jakaa kolmeen kategoriaan: kuvaileva-, ennustava- ja ohjaileva-analytiikka (Hubbard & Seiersen 2016, 211). *Kuvaileva-analytiikka* on käytössä olevaa perusanalytiikkaa. Se pitää sisällään esimerkiksi summien ja keskiarvojen tarkastelun. *Ennustava-analytiikka* hyödyntää esimerkiksi koneoppimista (machine learning). Ilman tämän kaltaisia menetelmiä perinteiset turvallisuuden puolustautumisratkaisut ovat usein myöhässä. *Ohjaileva-analytiikka* hyödyntää data-analytiikan ja päätäntätieteiden elementtejä optimoitujen suosituksien tekemiseen. Parhaimmillaan pystytään tuottamaan tietoa reaaliaikaiseen päätöksentekoon tai tekemään päätöksiä itsenäisesti. Näin ollen lähestytään jo turvallisuusanalytiikan ja riskienhallinnan tekoälyä.



Kuva 3. Operationaalisen turvallisuuden mittaamisen malli (Hubbard & Seiersen 2016, 208)

Hubbardin ja Seiersenin malli lähtee liikkeelle perusteista, joilla luodaan pohjaa tehokkaammalle ja älykkäämmälle riskienhallinnalle. Alimmalla tasolla hyödynnetään päätöksentekoa tukevaa analytiikkaa ja mitä korkeammalle tasolle siirrytään, päätöksentekoanalytiikan rinnalle tuodaan tietotekniikan ja datan analysoinnin mahdollistamia menetelmiä.

4.3 Kyberturvallisuuden riskien mittaaminen

Turvallisuuden mittaaminen on haastavaa, sillä turvallisuus on abstrakti ja latentti käsite (Edgar & Manz 2017, 56). Sitä voidaan verrata esimerkiksi ihmisen älykkyyteen. Älykkyyden mittaamiseen on kuitenkin kehitetty älykkyystestejä, joiden avulla voidaan määrittää numeraalinen arvo tai indikaattori ihmisen älykkyydelle. Sama voidaan tehdä turvallisuuden osalta. Turvallisuuden mittaristolla usein tarkastellaan kustannuksia ja hyötyjä (Juvonen 2014, 24). Näitä voidaan arvioida esimerkiksi neljän indikaattorin avulla: kontrollit, haavoittuvuudet, estetyt hyökkäykset ja estetyt tappiot. Kontrollilla tarkoitetaan turvatoimenpiteitä, kuten esimerkiksi ovea, lukkoa, salasanaa, salausta tai palomuuria. Haavoittuvuuksilla tarkoitetaan järjestelmän ominaisuutta, joka tekee siitä turvallisuuden näkökulmasta heikon tai hyödynnettävän hyökkäyksessä. Haavoittuvuus järjestelmässä voisi olla esimerkiksi salaamattomana tallennetut salasanat. Estetyillä hyökkäyksillä tarkoitetaan niitä hyökkäyksiä, jotka toteutettiin, mutta havaittiin ajoissa ja estettiin. Estetyillä tappioilla tarkoitetaan arvoa, joka olisi menetetty, jos hyökkäys olisi onnistunut.

Riskit ovat epävarmuutta ja sitä voidaan arvioida subjektiivisesti tai objektiivisesti. Subjektiivinen arviointi perustuu siihen, miten henkilö tulkitsee informaatiota. Käytännössä samasta informaatiosta kaksi eri henkilöä voi tehdä kaksi eri johtopäätöstä. Objektiivisesti arvioidut riskit perustuvat matemaattiseen todennäköisyys- ja tilastolaskentaan. Näin ollen objektiivi-

sen arvioinnin perusteella henkilöiden tulisi aina päätyä samaan johtopäätökseen. (Karha ym. 2005, 73.) Yritystoiminnassa ja rahoitusmarkkinoilla pyritään usein maksimoimaan tuotot ja minimoimaan riskit. Kuitenkin usein tuoton maksimoiminen johtaa riskien kasvuun ja riskien minimointi tuottojen laskuun. (Karha ym. 2005, 78.)

Riskienhallinta on jatkuva prosessi, jossa tunnistetaan, arvioidaan ja vastataan riskeihin. Hallitakseen riskejä organisaation tulee ymmärtää niiden ilmentymistodennäköisyyksiä ja haittavaikutuksia. Näiden tietojen avulla organisaatio voi asettaa hyväksyttävän riskitason ja -toleranssin, toiminnan tavoitteiden saavuttamiseksi. Riskitoleranssin ymmärtäminen edesauttaa kyberturvallisuustoimenpiteiden priorisointia informoidulla päätöksenteolla. (NIST 2018, 4.)

ISO 31000 -standardin mukainen riskienhallintaprosessi lähtee liikkeelle toimintaympäristön määrittelystä, jossa käsitellään neljää osa-aluetta: liiketoimintaympäristö, organisaatio, riskienhallintaprosessi ja riskinottohalu. Riskienhallinnan osalta huomioidaan tarpeet ja resurssit. Riskinottohalulla tarkoitetaan kriteeristöä, jossa määritellään millaisia ja kuinka suuria riskejä voidaan hyväksyä. Standardin mukaan riskien arviointi koostuu kolmesta vaiheesta: riskien tunnistaminen, riskianalyysi ja riskien merkityksen arviointi. (Juvonen 2014, 17–19.) Riskien tunnistamiseen on käytössä useita eri menetelmiä. Juvonen (2014, 19) mainitsee näistä haavoittuvuusanalyysin, poikkeamatarkastelun sekä vikapuuanalyysin. ISO 31010 määrittelee useita riskienarvioinnin menetelmiä (ISO 2019b).

Riskianalyysi edellyttää riskien tunnistamista. Riskit voivat johtua kontrollien puutteesta, tiedon puutteesta tai ajan puutteesta. Riskianalyysiä pidetään riskienhallinnan merkittävimpänä prosessina. Analyysi lähtee siitä, että jokaiselle riskikohteelle määritellään suurin mahdollinen vahinko. Liitteessä 1 on esitetty kaksi tapaa kuvata riskienhallintaprosessia (kuva 11 ja 12).

Riskejä voidaan arvioida deterministisesti tai todennäköisyyksien mukaan. Deterministinen lähtökohta olettaa, että kaikki haavoittuvuudet ovat löydettävissä ja näin ollen priorisoitavissa. Todennäköisyyksien arviointiin perustuvien menetelmien käyttöä on perusteltu sillä, että usein hyökkäykset hyödyntävät *nolla-päivä* -haavoittuvuuksia, jolloin riskejä ei välttämättä voida ennakoida. (Pendleton ym. 2016, 62:13.)

4.3.1 Riskimatriisit

The Open Web Application Security Project on vuonna 2001 alkunsa saanut voittoa tavoittelematon järjestö, joka tuottaa artikkeleita, menetelmiä, dokumentteja ja työkaluja verkkotur-

vallisuuteen liittyen. Järjestön tavoitteena on tehdä sovellus- ja verkkoturvallisuudesta näkyvää, jotta yksilöt ja organisaatiot voivat tehdä informoituja päätöksiä. (OWASP 2019a.)

OWASP riskiluokitusmenetelmän tarkoituksena on arvioida riskien prioriteettia, jotta riskienhallinnan päätöksenteko helpottuisi. Ajatuksena on, että toimialalla olisi käytössä yksi standardoitu riskienluokittelun viitekehys. Menetelmässä kuitenkin tunnistetaan, että kaikki riskit ja haavoittuvuudet eivät ole kaikille organisaatioille yhtä merkittäviä. Näin ollen viitekehystä tulee käyttää sovelletusti siten, että se palvelee organisaation tarpeita tehokkaasti. Viitekehyksen kehityksessä on hyödynnetty useita tunnettuja menetelmiä, joista on pyritty luomaan ohjelmistonkehityksen käyttöön soveltuva mahdollisimman yksinkertainen, mutta tarpeeksi yksityiskohtainen viitekehys. OWASP:n mukaan $riski = todennäköisyys \times vaikuttavuus$. (OWASP 2019b; kts. myös Hayden 2010, 15–16.)

OWASP:n *kokonaisvaltainen riskinhallintamenetelmä* on jaettu kuuteen askeleeseen:

1. tunnista riskit
2. tekijät, jotka vaikuttavat todennäköisyyteen
3. tekijät, jotka vaikuttavat vaikuttavuuteen
4. riskin vakavuuden määritys
5. korjaustoimenpiteiden määritys
6. riskinluokitusmallin muokkaaminen

Riskien tunnistamiseen vaikuttavat uhkatoimijat (threat agents), hyökkäysmenetelmät, haavoittuvuudet ja onnistuneen hyökkäyksen vaikutukset liiketoimintaan. Riskien tunnistamisen jälkeen arvioidaan karkeasti, kuinka todennäköisesti tiettyjä haavoittuvuuksia voidaan käyttää hyväksi. Arviointi voidaan tehdä asteikolla *matala, keskitaso, korkea*. Todennäköisyyteen liittyy olennaisesti uhkatekijät. Tavoitteena on arvioida, kuinka todennäköisesti hyökkäys onnistuu mahdollisilta hyökkääjiltä. Uhkaa arvioidaan kertoimien avulla, jotka saavat arvon väliltä 0–9. Uhkatoimijoiden kertoimet muodostuvat taitotasosta, motiivista, mahdollisuudesta ja tekijöiden koosta. Haavoittuvuuskertoimet muodostuvat haavoittuvuuden löydettävyydestä, haavoittuvuuden hyödynnettävyydestä, haavoittuvuuden tunnettavuudesta ja tunkeutumisen havaitsemisesta. (OWASP 2019b.)

Vaikutuksen arviointi perustuu tekniseen vaikutukseen ja liiketoiminnalliseen vaikutukseen. Teknisen vaikutuksen kertoimet (0–9) muodostuvat: luotettavuuden menetyksestä, eheyden menetyksestä, saatavuuden menetyksestä ja jäljitettävyydestä. Liiketoiminnan vaikutukset muodostuvat: taloudellisesta menetyksestä, maineen menetyksestä, sääntöjen noudattamatta jättämisestä, yksityisyyden loukkauksista. (OWASP 2019b.)

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

Kuva 4. Todennäköisyyden määrittäminen (alkuperäinen kuva OWASP 2019b)

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

Kuva 5. Teknisen ja liiketoiminnallisen vaikuttavuuden määrittäminen (alkuperäinen kuva OWASP 2019b)

Riskin kokonaisvakavuus arvioidaan laskemalla todennäköisyyden keskiarvo (0–3 vähäinen, 3–6 keskiverto, 6–9 korkea) (alkuperäinen kuva OWASP 2019b).

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Kuva 6. Riskin kokonaisvakavuus (alkuperäinen kuva OWASP 2019b)

Korjaustoimenpiteiden määrityksen tulisi perustua arvioon riskien kokonaisvaikutuksista. Vakavimmat riskit tulisi huomioida ensin. On kuitenkin otettava huomioon, ettei kaikkia riskejä ole välttämättä järkevä korjata. Esimerkiksi mikäli toimenpide kustantaa 100 000 euroa ja haavoittuvuudesta koituvat tappiot ovat arvioilta 2 000 euroa vuodessa, jolloin menisi 50 vuotta saavuttaa hyöty. (OWASP 2019b.)

Riskiluokitusmallin muokkaaminen organisaation tarpeisiin sopivaksi on edellytys onnistuneelle riskienhallinnalle. Muokkaamista voidaan tehdä esimerkiksi kertoimien ominaisuuksien osalta. Esimerkiksi armeijan käyttöön suunnitellussa ohjelmistossa voidaan arvioida riskien vaikutuksia ihmishenkiin. Organisaatio voi myös muokata kertoimien painoarvoja tarpeidensa mukaisiksi. OWASP-menetelmän vahvuus on siinä, ettei se perustu vain yhteen matriisiin. Menetelmä hyödyntää useita matriiseja, joista saadulla yhteistuloksella on merkitystä. Ver-

kosta on myös saatavilla valmiita laskureita riskiarvon määrittämiseksi, jolloin kynnys menetelmän käyttöönotolle saattaa madaltua.

4.3.2 Tilastot ja todennäköisyydet

Hubbard & Seiersen (2016, 13–14, myös Miessler 2018; Abbadi 2006) esittää, että kyberturvallisuuden mittaaminen pitäisi perustua määrälliseen tietoon. Hayden ei hylkää mittaria vain sen takia, ettei se ole määrällinen. Hän toteaa, että kaikki empiriaan perustuvat mittarit, jotka vähentävät epävarmuutta ovat hyviä. Hän kuitenkin toteaa myös, että perinteiset tavat arvioida turvallisuutta on usein riittämättömiä ja saattavat johtaa harhaan. (Hayden 2010, 4 ja 6).

Turvallisuusriskejä kuvataan usein ilmenemistodennäköisyydellä ja vaikuttavuudella sekä näiden yhteisvaikutuksella. Mittaristo muodostuu nominaali- tai järjestysasteikoista. Arviot riskeistä saattavat perustua asiantuntijoiden intuitiiviseen ja subjektiiviseen arvaukseen. Pahimmassa tapauksessa tämän kaltainen toiminta saattaa johtaa epärealistiseen turvallisuuden tunteeseen tai liialliseen luottamuksen tunteeseen. Hubbardin & Seiersen (2016, 15) mukaan ei voida absoluuttisesti todeta, että tämä menetelmä edistäisi kyberturvallisuutta. Heidän mukaan sama voidaan esittää myös suhteellisen helposti matemaattisesti laskemalla tapahtumien todennäköisyyksiä sekä niiden vaikutusta menetettyihin tuloihin. Tällöin arvio ei perustu subjektiivisuuteen vaan tilastotieteeseen. Tämä ei tarkoita, että mitattavan kohteen tulisi olla määrällinen, sillä myös laadullista ilmiötä voidaan mitata määrällisesti (esim. turvallisuus). Hubbard & Seiersen (2016) esittääkin teoksessaan *How to Measure Anything in Cybersecurity risks*, että suurin yksittäinen kyberturvallisuuden riski on yleiset käytössä olevat epäpätevät riskinarviointityökalut (matriisit).

Hubbardin ja Seiersenin mukaan esimerkiksi järjestelmän tai ohjelman penetraatiotestauksessa ei ole kyse järjestelmän muuttamisesta vaan epävarmuuden vähentämisestä liittyen järjestelmän turvallisuuteen. *Todennäköisyys* ei ole vain datan perusteella suoritettu laskutoimitus vaan *epävarmuutta* kuvaava arvo. (Hubbard & Seiersen, 2016, 45).

Kyberturvallisuuden mittaamisessa merkittävää on tietää tarkalleen mitä kyberturvallisuudella tarkoitetaan ja mikä siinä on merkittävää organisaatiolle. Tulee siis kysyä tarpeeksi tarkkoja kysymyksiä. Jos ilmiö on organisaatiolle tärkeä, sitä voidaan havaita ja tarkkailla. Jos ilmiö on havaittavissa, niin se voidaan havaita määrissä. Jos ilmiö voidaan havaita määrissä, sitä voidaan myös mitata. Ymmärtääkseen mitä mitataan, tulee kysyä ”*miksi* mitataan”, eikä ”*mitä* mitataan”. Mittaamisen tulisi aina tukea päätöksentekoa ja edistää jotain. Kyberturvallisuutta mitataan, jotta kyetään paremmin kohdentamaan resursseja riskien minimoimiseksi. Ilmiön mittaaminen edellyttää sen selkeää määrittelyä ja ymmärtämistä. Kyberturvallisuus ei ole vain järjestettyjen koulutusten määrää tai uusien palomuurien määrää vaan näiden tulokses-

ta vähentynyttä riskiä. Näin ollen tulee ymmärtää myös mitä tarkoitetaan riskillä. Kun todetaan, että turvallisuus on parantunut, todellisuudessa tarkoitetaan, että riskit ovat pienentyneet. Kyberturvallisuuteen panostetaan nykypäivänä niin merkittäviä resursseja, että pienikin vähennys epävarmuudessa voi tuoda merkittäviä säästöjä. (Hubbard & Seiersen, 2016, 48–50; kts. myös Black ym. 2008, 2–4).

Monte Carlo -simulaatio käyttää tietokoneiden laskentatehoa laskeakseen ennalta asetetun määrän skenaarioita perustuen annettuihin arvoihin. Menetelmää on hyödynnetty muun muassa niin sanotussa Manhattan-projektissa, jonka tarkoituksena oli ydinpommin kehittäminen (Hayden 2010, 254). Riskien arvioinnissa simulaation vahvuus on siinä, ettei arvojen tarvitse olla tarkkoja, vaan ne voivat perustua vaihteluvälille. Lisäksi menetelmällä voidaan arvioida analytiikalle liian monimutkaisia riskejä (ISO 2019c, 74). Esimerkiksi simulaatio laskee eri skenaarioita riskille, jonka luottamusväli (confidence interval) on 90 %, todennäköisyys on 5 % ja vaikutus 10 000–50 000 euroa. Näitä skenaarioita voidaan laskea esimerkiksi miljoona kappaletta, jolloin jokaisen skenaarion tuloksista voidaan laskea keskiarvo. Monte Carlo -simulaation voi toteuttaa yksinkertaisesti esimerkiksi Excel taulukko-ohjelmalla. (Hubbard 2014, 125, 127–128.) Hubbard & Seiersen tarjoaa valmiit Excel-taulukot verkkosivuillaan. Monte Carlo simulaatiota on hyödynnetty usealla eri toimialalla (esim. rakennus-, IT-, vakuutus- ja rahoitusala) riskienhallinnassa ja arvioinnissa (Hubbard 2014, 140). Myös Hayden (2010, 248) suosittelee Monte Carlo -simulaation hyödyntämistä kyberriskien vaikuttavuuksien arviointiin. Lisäksi voidaan hyödyntää Poisson-prosessia. Poisson-prosessin avulla voidaan määrittää todennäköisyyksiä tuleville toisistaan riippumattomille tapahtumille perustuen jo sattuneisiin tapahtumiin. (Hayden 2010, 254.)

Kyberturvallisuuden osalta usein ajatellaan, ettei käytössä ole tarpeeksi dataa riskien matemaattiseen arviointiin. Tämä on kuitenkin harhaluulo. Usein käytössä on enemmän dataa kuin luullaan ja sitä tarvitaan vähemmän kuin kuvitellaan. (Hubbard & Seiersen 2016, 79; Hayden 2010, 6.) Hubbardin näkemyksen mukaan luottamusväliin ja tilastotieteeseen perustuva riskiarvio vähentää epävarmuutta tehokkaammin, kuin subjektiiviset ja nominaali- tai järjestysasteikkoihin perustuvat riskimatriisit. Tästä ei ole kuitenkaan tieteellistä näyttöä, mutta näiden näkemyksien tueksi Hubbard esittää muuta tukevaa tieteellistä tutkimusta (Hubbard & Seiersen 2016, 81.)

Simulaation tuloksia voidaan tukea vahinkokäyrällä (loss exceedance curve), jota voidaan pitää yhdenlaisena riskitoleranssikäyränä (risk tolerance curve). Riskitoleranssikäyrä esittää, kuinka paljon organisaatio kykenee sietämään riskiä. Päätöksenteon tukena käytetään myös kontrollin hyötyä kuvaavaa kaavaa:

$$Kontrollin\ hyöty\ = \frac{vähennys\ arvioiduissa\ menetyksissä}{kontrollin\ kustannukset} - 1$$

Arvioidut menetykset saadaan Monte Carlo -simulaation keskiarvosta.

Kyberturvallisuuden mittaamisessa on tilanteita, joissa asiantuntijoiden subjektiivista osaamista ei voida sivuuttaa, kuten esimerkiksi arviot riskien ilmentymistodennäköisyydestä ja vaikutuksista. Ongelmana on usein asiantuntijoiden liian positiiviset sekä epäjohdonmukaiset arviot. Asiantuntijoiden kykyä toteuttaa näitä subjektiivisia arvioita voidaan kuitenkin kehittää koulutuksella ja jatkuvalla palautteella. (Hubbard & Seiersen, 2016, 85–87.) Tätä kykyä puolestaan voidaan mitata objektiivisesti. Subjektiivisen arviointikyvyn kehittäminen parantaa matemaattistilastollisen menetelmän tarkkuutta. Koulutuksen tarkoituksena on kehittää kyberturvallisuusasiantuntijan kykyä arvioida todennäköisyyksiä. Asiantuntijat arvioivat esimerkiksi tapahtuman todennäköisyyden ja vaikuttavuuden. Hubbardin kokemusten perusteella tämän kaltaista koulutusta tarvitaan, koska ihmiset ovat usein yliluottavaisia arviointeihinsa. Lisäksi ihmiset pyrkivät luonnostaan välttelemään ääriarvoja. (Hubbard & Seiersen 2016, 156.) Arvioinnissa auttaa myös se, että riski jaetaan tarpeeksi pieniin ja yksityiskohtaisiin osiin. Tämän kaltainen jako voidaan tehdä esimerkiksi tietoturvasta tutun CIA-periaatteen (luottamus, eheys, saatavuus) mukaisesti. (Hubbard & Seiersen, 2016, 148).

Monimutkaisempien riskien arvioimisessa Bayesin ehdollisen todennäköisyyden menetelmä sopii myös kyberturvallisuuden arviointiin. Menetelmä hyödyntää tiedettyä tietoa ”ennen” (a priori) ja ”jälkeen” (a posteriori) tapahtuman, eikä muuta tietoa tarvita (ISO 2019c, 78). Bayesin menetelmä mahdollistaa ehtojen lisäämisen todennäköisyyslaskentaan. Kaava merkitään: P (A|B). Esimerkiksi voidaan todeta ”tapahtuman A todennäköisyys on B, kun C” tai ”palvelunestohyökkäyksen todennäköisyys on noussut 10 %, ottaen huomioon viimeaikaisen hyökkäyksen kilpailijayritystä vastaan”. Menetelmä mahdollistaa todennäköisyyksien tarkastelun myös käänteisesti. (Hubbard & Seiersen 2016, 170–174.) Beta-jakaumaa voidaan hyödyntää Bayesin menetelmässä. Beta-jakauman avulla voidaan laskea todennäköisyyksiä hyvin pienen havaintojoukon perusteella. Esimerkiksi mikä on riski massiiviselle tietomurrolle, joka on toistaiseksi tapahtunut vain muutamalle yritykselle. (Hubbard & Seiersen 2016, 205.) Näiden menetelmien perusteella voidaan laskea tilastotieteeseen perustuen todennäköisyyksiä esimerkiksi tietomurroille tai palvelunestohyökkäyksille, kun tarkkaa tietoa ei ole saatavilla. Menetelmien yhdisteleminen hankaloittaa hieman laskukaavoja, mutta kaikki on esitettävissä Excelillä ja esimerkki taulukot ovat saatavilla internetistä.

			Impact				
			Negligible	Minor	Moderate	Critical	Catastrophic
			<$10K	$10K to <$100K	$100K to <$1 Million	$1 Million to <$10 Million	≥$10 Million
Likelihood	Frequent	99%+	Medium	Medium	High	High	High
	Likely	>50%–99%	Medium	Medium	Medium	High	High
	Occasional	>25%–50%	Low	Medium	Medium	Medium	High
	Seldom	>1%–25%	Low	Low	Medium	Medium	Medium
	Improbable	≤1%	Low	Low	Low	Medium	Medium

Kuva 7. Riskimatriisi (alkuperäinen kuva Hubbard & Seiersen 2016, 110)

Hubbard & Seiersen (2016, 110) esittää riskimatriisien käyttöön liittyviä ongelmia esimerkkien kautta:

> Esimerkki 1. Kaksi riskiä ”Seldom” eli ”harvoin” todennäköisyysluokasta.
> Riski A: todennäköisyys 2 %, vaikutus 10 milj. dollaria.
> Riski B: todennäköisyys 20 %, vaikutus 100 milj. dollaria.

Riskimatriissa usein lasketaan vaikuttavuus painotetulla todennäköisyydellä. Tämä tarkoittaa sitä, että todennäköisyys kerrotaan vaikutuksella (A: 2 x 10, B: 20 x 100). Toisin sanoen, riskin B vaikuttavuus on satakertainen suhteessa riskiin A, mutta ne on silti luokiteltu matriisissa samaan kategoriaan.

> Esimerkki 2. Kaksi riskiä, joista toinen luokasta ”occasional” eli ”satunnainen” ja toinen ”likely” eli ”todennäköinen”.
> Riski C: todennäköisyys 50 %, vaikutus 9 milj. dollaria.
> Riski D: todennäköisyys 60 %, vaikutus 2 milj. dollaria.

Riskin C painotettu vaikuttavuus on 4,5 milj. dollaria ja riskin D vaikuttavuus 1,2 milj. dollaria. Kuitenkin matriisin perusteella riski C on luokiteltu korkeaksi (high) ja riski D keskitasoksi (medium).

4.3.3 Yhteenveto kyberriskien mittaamisesta

Hubbardin tutkimuksissa kohdeyrityksistä yli 60 % käytti riskimatriiseja ja yli 70 % ordinaaliasteikkoja riskiarvioinnissa. Vain hieman alle 15 % yrityksistä käytti Monte Carlo -simulaatiota tai Bayesin menetelmää. (Hubbard & Seiersen 2016, 104.)

Matriisiperusteisissa menetelmissä heikkoutena on, etteivät ne kykene tarjoamaan tarkkaa tietoa resurssien kohdentamisesta tiettyihin riskien kontrollointimenetelmiin subjektiivisuuden ja käytettyjen asteikkojen takia. (Hubbard & Seiersen 2016, 74; Hayden 2010, 10; Black ym. 2008, 3–4.) Minkä arvoista on laskea tietyn riskin tasoa *korkeasta keskitasoon*? Kannattaa-

ko käytössä olevilla resursseilla vähentää 10 matalaa riskiä vai yhtä keskitason riskiä (Hubbard & Seiersen, 2016, 74)? Tai onko todennäköistä, että riski tapahtuu vuoden vai kymmenen vuoden sisällä (Hubbard & Seiersen, 2016, 105)?

Matriisien vahvuus on siinä, että ne ovat yksinkertaisia. Niitä ei kuitenkaan tulisi käyttää päätöksentekoon, vaan ennemminkin turvallisuusasiantuntijoiden mielipiteen määrittämiseen johonkin tiettyyn riskiin liittyen. Haydenin mukaan matriisi on turvallisuusasiantuntijoille liian yksinkertainen. Asiantuntijoiden tulisi kyetä tarjoamaan tarkempaa ja valistuneempaa arviota riskeistä, kuin mihin matriiseilla kyetään. (Hayden 2010, 10.)

Matriiseja pidetään liian subjektiivisina (ISO 2019c, 85; Hubbard & Seiersen 2016, 15; Hayden 2010, 11). *Todennäköinen*, *vakava* tai *punainen* arvo matriisissa voi tarkoittaa eri henkilöille eri asioita. Tämän kaltaista asteikkoa kutsutaan *nominaaliasteikoksi*, joka tarkoittaa, ettei niitä voi määrällisesti verrata keskenään. (Hayden 2010, 12.) Matriiseja voidaan esittää myös *ordinaaliasteikolla* eli *järjestysasteikolla* (esim. 1. 2. ja 3.), joka tarkoittaa sitä, että arvojen välisiä eroja ei tarkkaan tiedetä (Hubbard & Seiersen 2016, 104; ISO 2019c, 85; kts. myös Black ym. 2008, 4). Tilastotieteisiin perustuvien menetelmien vahvuus on siinä, että ne tarjoavat enemmän objektiivista ja tieteeseen perustuvaa tietoa päätöksenteon tueksi. Todennäköisyyslaskenta saattaa tuntua hankalalta, mutta menetelmien käyttöön on useita valmiita työkaluja ja ohjeita.

Tietokantahaussa ei noussut esille tieteellisesti todistettua tietoa siitä, mikä menetelmä tukee päätöksentekoa parhaiten. Hubbard & Seierseen (2016) kuitenkin tuo esille, että tieteellistä tietoa on saatavilla siitä, että perinteiset riskimatriisit eivät johda parempiin päätöksiin. He myös esittävät teoriaa tukevaa tutkimusta kyberturvallisuuden ulkopuolelta siitä, että yksinkertainenkin algoritmi on parempi arvioimaan todennäköisyyksiä kuin asiantunteva ihminen. (Hubbard & Seierseen 2016, 81.) Heidän mukaansa myöskään ”parhaat käytännöt” eivät tarkoita sitä, että menetelmien käyttö olisi tieteellisesti todistettu parantavan päätöksenteon laatua. Ihmisen kyky tehdä arvioita ja ennusteita on usealla tutkimuksella osoitettu huonoksi. Hubbard & Seiersenin mukaan kyseessä on usein niin sanottu analyysilume. Tällä tarkoitetaan sitä, että uskotaan sokeasti yleisesti käytössä olevan menetelmän parantavan arviointia. Esimerkiksi lääketieteessä uuden lääkkeen oletetaan olevan lumelääke kunnes sen toimivuus on kyetty tieteellisesti todistamaan. Sama pätee kyberturvallisuudessa. (Hubbard & Seierseen 2016, 76–77.)

Matriisit ovat käyttökelpoisia, mutta ei niin kuin usein ensisijaisesti ajatellaan. Matriiseilla ei todellisuudessa mitata riskien tasoa, vaan asiantuntijoiden mielipiteitä riskeistä. Tämä on eri tavalla merkittävää tietoa. Esimerkiksi asiakastyytyväisyyskyselyt eivät todellisuudessa mittaa tuotteiden laatua, vaan asiakkaan mielipidettä tuotteesta. Hayden kuitenkin kritisoi mat-

riisien käytössä sitä, että niiden käyttöä perustellaan laadullisella mittaamisella, vaikka todellisuudessa riskimatriisit eivät ole laadullinen tapa mitata riskejä. ISO 31010 standardin mukaan riskimatriisit perustuvat määrälliseen asteikkoon (2019c, 85), mutta Hayden (2010) sekä Hubbard & Seiersen (2016) pitävät asteikkoja nominaalisena tai ordinaalisina, jolloin todellista määrällistä tietoa ei kyetä tuottamaan. Matriisit, joihin on yksinkertaisen *nominaaliasteikon* lisäksi lisätty lukuja kuvaamaan todennäköisyyksiä (esim. 90 % tai 0,25) tai vaikuttavuuksia (esim. alle 25 000 euroa tai yli 50 000 euroa) ovat edelleen samoja, mutta koristeltuja riskimatriiseja. (Hayden 2010, 11–12.) Ongelmana on myös se, että matriiseista puuttuu usein konteksti eli ajallinen rajaus, johon todennäköisyys ilmiön tapahtumisesta sidotaan (esim. seuraavan vuoden aikana) (Black ym. 2008, 4).

Aineistossa ei juuri noussut esille tilastollisten menetelmien heikkouksia suhteessa matriiseihin. Silti tilastolliset menetelmät vaikuttavat olevan selvästi matriiseja harvemmin käytössä yrityksissä ja organisaatioissa. Tästä voidaan tehdä kaksi päätelmää. Joko menetelmää ja sen etuja ei tunneta laajasti riittävän hyvin tai se ei tarjoa merkittävää parannusta arviointiin suhteessa yksinkertaisempiin menetelmiin. Tilastolliset menetelmät eivät kuitenkaan ole uusia, joten mikäli niistä olisi merkittävästi etua, se todennäköisesti tiedettäisiin ja ne olisivat laajemmin käytössä.

Tilastollisia menetelmiä kohtaan on esitetty jonkin verran kritiikkiä. Kritiikkiä on kohdistunut esimerkiksi siihen, ettei se kykene ottamaan kantaa kaikkiin riskeihin. (Hubbard & Seiersen 2016, 116.) Toisaalta ei kykene matriisitkaan. Lisäksi tilastollisten menetelmiä vältellään, koska luullaan, ettei niiden käyttöön ole saatavilla tarpeeksi tarkkaa dataa. Mikäli tarkkaa dataa olisi saatavilla, niin todennäköisyyksien tai riskimatriisien käyttöä ei lähtökohtaisestikaan tarvittaisi. Näin ollen voidaan todeta, että todennäköisyys- ja tilastoperusteista menetelmää käytetään juuri siksi, ettei tarkkaa dataa riskeistä ole saatavilla. Ongelma on myös siinä, että mikäli epätarkkaa dataa syötetään tilastotieteellisiin menetelmiin, niin se ei välttämättä tee ulos tulevasta datasta tieteellistä. Määrällisiä menetelmiä on kritisoitu myös siitä, ettei niitä voida hyödyntää, koska ilmiö on liian monimutkainen ja siihen vaikuttaa ihmisen käyttäytyminen. Samat ongelmat ja haasteet pätevät kuitenkin myös laadullisiin menetelmiin. Ilmiön kompleksisuus puolestaan on syy, minkä takia sitä ei tule arvioida ainoastaan subjektiivisesti. Aerodynamiikka ja ydinvoima ovat myös kompleksisia ilmiötä, eikä niihinkään kohdistuvia riskejä arvioida ainoastaan asiantuntijoiden subjektiivisilla näkemyksillä. (Hubbard & Seiersen 2016, 121.)

Monte Carlo -menetelmän heikkoudeksi on todettu, että simulaatioiden määrä vaatii huomattavaa laskentatehoa. Teknologian kehittyessä tämä ei kuitenkaan enää ole ongelma. Lisäksi monimutkaisten riskien mallintaminen saattaa olla haastavaa. Niiden esittäminen ymmärrettävästi päätöksentekijöille saattaa myös olla haastavaa. (ISO 2019c, 75) Bayesin menetel-

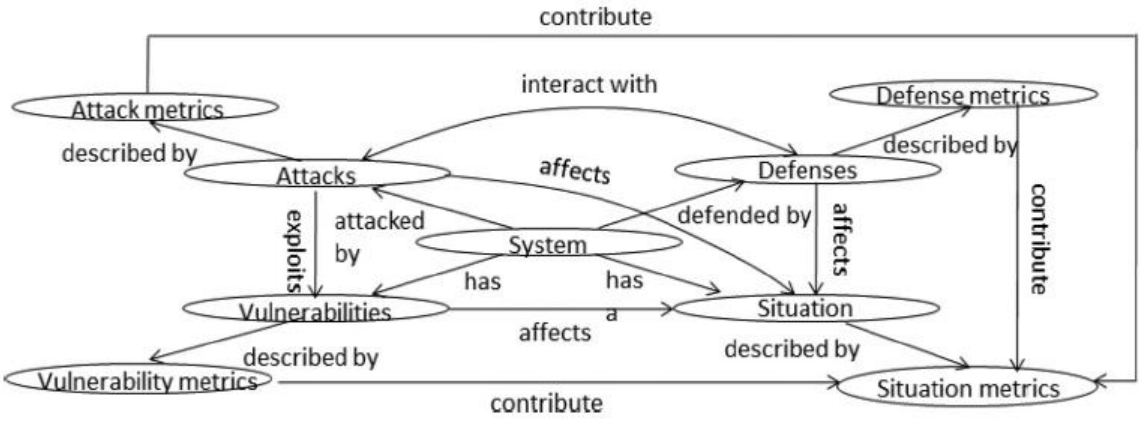
mää on kritisoitu myös liian monimutkaisena. Menetelmä vaatii useiden konditionaalien yhdistämistä, jotka usein myös perustuvat asiantuntijoiden arvioihin. (ISO 2019c, 78–79.) Kurittu (2019) suhtautuu hieman varovaisemmin kyberturvallisuuden tarkkaan mittaamiseen. Hänen mukaansa kyseessä ei ole tarkka tiede, jolloin tarkkojen malleja ja mittareita ei välttämättä voida kehittää. Päätöksenteon kannalta merkittävämpää on tarkastella trendejä ja muutossuuntia. (Kurittu 2019.)

4.4 Teknisen ja taktisen tason mittarit

Organisaatiossa voidaan hyödyntää useita erityyppisiä turvallisuuden mittareita. Näitä voivat olla esimerkiksi prosessiturvallisuus-, verkkoturvallisuus-, sovellusturvallisuus- tai henkilöturvallisuusmittarit. (Abbadi, 2006, 8.) Prosessiturvallisuus mittaa muun muassa sääntörikkomusten määrää, heikkojen salasanojen määrää sekä prosessien määrää, joille on tehty riskiarvio. Verkkoturvallisuus mittaa muun muassa estettyjen virusten määrää ja päivitysten määrää. Sovellusturvallisuus mittaa muun muassa hyökkäyspinta-alaa ja turvallisuuskerrosten määrää. Henkilöturvallisuus mittaa käyttäytymistä ja koulutusta. (Abbadi, 2006 9–15.) Abbadin mukaan yleisin tapa mitata kyberturvallisuuden tasoa on kuitenkin riskianalyysin avulla (2006, 17).

Pendlenton ym. (2016, 62:1) esittää, että turvallisuusmallinnusta toteutettaisiin neljän järjestelmäturvallisuuden mittarin perusteella. Mittarit perustuvat hyökkäyksen ja puolustuksen vuorovaikutuksiin. Näitä mittareita ovat järjestelmän haavoittuvuudet, puolustusteho, hyökkäyksen vakavuus sekä tilannetietoisuus. Mittaaminen perustuu siihen, että jokainen kategoria jaetaan alakategorioihin, jolloin päästään riittävän tarkasti mitattavalle tasolle. Haavoittuvuuksia voidaan mitata käyttäjien, käyttöliittymien tai ohjelmiston osalta. Käyttäjien haavoittuvuudet voidaan vielä jakaa kognitiivisiin taipumuksiin (esim. kalastusviestien avaaminen) ja rajoituksiin (esim. salasanojen pituus). (Pendlenton ym. 2016, 62:8). Käyttöliittymien haavoittuvuuksia voidaan arvioida hyökkäyspinta-alan perusteella, kuinka monella tavalla hyökkääjä voi päästä ohjelmistoon käsiksi. Tätä voidaan arvioida sisäänmeno- ja ulostuloväylien avulla. Mitä eri tapoja hyökkääjällä on syöttää dataa tai lähettää sitä ulos ohjelmistosta. Ohjelmiston haavoittuvuudet voidaan edelleen jakaa ajallisiin, yksittäisiin ja kollektiivisiin haavoittuvuuksiin. Ajallisissa haavoittuvuuksissa kriittinen tietoa on haavoittuvuuden kesto. Yksittäisten haavoittuvuuksien arviointi perustuu priorisointiin, jonka mukaan haavoittuvuuksia korjataan. Tätä voidaan tehdä pisteyttämällä yleisiä heikkouksia ja haavoittuvuuksia *Common Weakness Scoring System* (CWSS) ja *Common Vulnerability Scoring System* (CVSS) -menetelmillä. Usein hyökkäykset toteutetaan hyödyntäen useita eri haavoittuvuuksia. Kollektiivisia haavoittuvuuksia voidaan arvioida muun muassa Bayesin menetelmällä tai Hyökkäyspuumenetelmällä. (Pendlenton ym. 2016, 62:8–13; Black ym. 2008, 6)

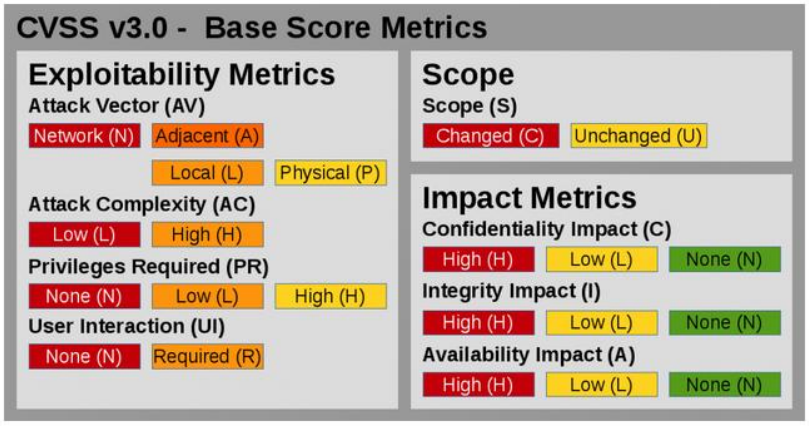
Puolustuskeinojen tehoa voidaan arvioida ennaltaehkäisevien, reaktiivisten ja proaktiivisten puolustusmenetelmien kautta. Ennaltaehkäiseviä menetelmiä ovat *mustat listat* (engl. black-list), *datan suoritusten ehkäisy* (engl. Data Execution Prevention, DEP), sekä *ohjausvirtaukset* (engl. Control-Flow Integrity, CFI). Reaktiivisiin menetelmiin kuuluvat tunkeutumisen havaitsemismenetelmät sekä virusten ja haittaohjelmien torjuntamenetelmät. Proaktiivisia menetelmiä ovat *osoiteavaruuden satunnaistus* (engl. Address Space Layout Randomization, ASLR, jonka tehtävänä on muuttaa datan sijaintia, jolloin myös haavoittuvuuksien sijainnit muuttuvat) sekä *liikkuva kohde puolustus* (engl. Moving Target Defense, MTD). Hyökkäyksien vakavuutta voidaan arvioida nolla-päivä-hyökkäyksien (elinaika ja uhrit), kohdennettujen hyökkäyksien, bottien (koko, kaistaleveys, tehokkuus, kestävyys), haittaohjelmien levinneisyyden (infektioaste) sekä puolustuksien väistötekniikoiden (esim. koneoppimista hyödyntävät hyökkäykset) avulla. (Pendlenton ym. 2016, 62:14–20.) Tilannetietoisuutta voidaan tarkastella turvallisuustilanteen, tapahtuneiden turvallisuusselkkauksien ja turvallisuusinvestointien kautta (Pendlenton ym. 2016, 62:20). Kaikki edellä mainitut kategoriat ovat jaettavissa vielä useampiin alakategorioihin, jolloin voidaan mitata tarpeeksi yksityiskohtaista tietoa. Pendlenton ym. (2016, 62:3) tutkimus on ainoa tietohaussa esiinnoussut tieteellinen tutkimus ilmiöstä.



Kuva 8. Järjestelmäturvallisuuden ontologia jaettuna neljään mitattavaan kategoriaan (alkuperäinen kuva Pendleton ym. 2016, 62:7)

Lähdeaineiston perusteella CVSS-menetelmää voidaan pitää merkittävänä, sillä se nousee esille useissa julkaisuissa (Black ym. 2008, 6; Pendleton ym. 2016, 62:11, Hubbard & Seiersen 2016, 14, Hayden 2010, 15). Menetelmä on NIST-yhteensopiva, maailmanlaajuinen ja valmistajasta riippumaton. Järjestelmää ylläpitää FIRST-yhteenliittymä (Forum of Incident Response and Security Teams), johon kuuluu muun muassa Kyberturvallisuuskeskus. Menetelmässä haavoittuvuuden vakavuudelle annetaan arvo mahdollisimman nopeasti haavoittuvuuden löytämisen jälkeen. Lukuarvon perusteella haavoittuvuuden vakavuutta ja riskiä voidaan arvioida. Lukuarvo annetaan yhden desimaalin tarkkuudella asteikolta 0,0–10,0. Pisteytyksessä ensin käytetään kuutta tekijää, mitkä kuuluvat *base*-mittaristoon: hyökkäystapa,

hyökkäyksen monimutkaisuus, tunnistautumisvaatimus, luottamuksellisuus, eheys, saatavuus. Lisäksi voidaan hyödyntää ajallisia ja ympäristöllisiä mittaristoja lopullisen CVSS-arvon laskemiseen. (Laurio 2014; FIRST 2019.) Menetelmää on kuitenkin kritisoitu siitä, että vaikka se tarjoaa tietoa eikä hyödynnä matriiseja, se perustuu ordinaalia- sekä nominaaliasteikkoon ja hyödyntää epäpätevää matematiikkaa (Hubbard & Seiersen 2016, 92; Hayden 2010, 15).



Kuva 9. SUSE esimerkki CVSS v3.0 mittaristosta (alkuperäinen kuva SUSE 2017)

Kyberturvallisuuden arvioinnissa voidaan hyödyntää myös penetraatiotestausta ja niin sanottuja Red Teameja (suom. punainen joukkue). Penetraatiotestauksen tarkoituksena on selvittää, voiko hyökkääjä saavuttaa tiettyjä tavoitteita kohdatessaan nykyiset turvallisuuden konfiguraatiot. Punaiset joukkueet on suunniteltu jatkuvasti ja tehokkaasti simuloimaan mahdollisia oikean maailman hyökkääjiä, jotta kyberturvallisuutta voidaan parantaa. (Miessler, 2019.) Suomessa esimerkiksi F-Secure tarjoaa Red Team testausta. Testin avulla organisaatio saa selville, havaitseeko turvallisuus- ja puolustusmenetelmät hyökkäyksen. Näin ollen saadun palautteen perusteella turvallisuusprosesseja voidaan kehittää. F-Securen Red Team vastuuhenkilön Tuomo Makkosen mukaan simuloitu hyökkäys onnistuu lähes joka kerta (Vänskä 2017).

IoT-laitteiden lisääntyessä turvallisuustyökalujen, kuten esimerkiksi Shodanin tai NMAP:n, merkitykset lisääntyvät. Shodanin avulla voidaan etsiä mitä tahansa internetiin kytkettyjä laitteita. Näin voidaan paikantaa ja korjata laitteita, joissa on tunnettuja haavoittuvuuksia (Miessler, 2018c). NMAP on yksi tunnetuimmista porttiskannereista, jonka avulla voidaan paikantaa avoimia portteja verkosta (Miessler, 2018b). Eri työkalujen hyödyntämisessä mittaamiseen on kuitenkin haasteensa. Esimerkiksi eri porttiskannerit käyttävät erilaisia algoritmejä, jolloin mittaamisen tulokset saattavat vaihdella, eivätkä ne ole keskenään verrattavia. Tästä syystä Black ym. (2008, 3) mukaan tulisi ennemmin keskittyä tavoitteiden saavuttamisen mittaamiseen kuin yksittäisten mittareiden määrittämiseen.

Miessler (2018a) mukaan parhaiten turvallisuutta kuvaa päivitettyjen järjestelmien prosentuaalinen osuus, turvallisuushallinnon alla olevien sovellusten prosentuaalinen osuus sekä ulospäin suuntautuvan valvotun ja suodatetun DNS-liikenteen prosentuaalinen osuus. (Miessler 2018a.)

Security Information and Event Management (SIEM) on kyber- ja tietoturvallisuuden analysointijärjestelmä, joka tarkkailee organisaation verkko- ja tietojärjestelmiä sekä hälyttää poikkeuksien ilmaantuessa. SIEM hyödyntää tapahtuma- ja lokitietoja valvonnassa ja tilastollisessa analysoinnissa. Analyyseistä on johdettavissa mitattuja tunnuslukuja, jotka kertovat organisaation kyberturvallisuuden tasosta. (Vesamäki 2016; Kinnunen 2017; Kurittu 2019.) Kurittun (2019) mukaan teknisen tason mittareita on kuitenkin tulkittava varoen. Esimerkiksi SIEM saattaa antaa kriittisiltä vaikuttavia hälytyksiä, vaikka todellinen uhka on huomattavasti pienempi

Kuvatut menetelmät ovat vain pieni osa kaikista menetelmistä ja työkaluista, joiden avulla voidaan saada tietoa yksittäisestä kyberturvallisuuden osasta. Näitä tietoja yhdistelemällä voidaan arvioida suurempaa kokonaisuutta. Tietoja voidaan hyödyntää myös riskienhallinnassa ja niiden avulla voidaan arvioida esimerkiksi riskien ilmentymisen todennäköisyyksiä.

5 ANALYYSI: KYBERTURVALLISUUDEN MITTARIT

Kyberturvallisuuden kenttä on kansainvälisesti tarkasteltuna ”villilänsi”. Siitä puuttuu sekä *de facto* että *de jure* pelisäännöt. Kyberturvallisuuden mittaaminen on korostunut 2010-luvulla, sillä turvallisuusratkaisuihin kohdennetaan yhä enemmän resursseja, mutta niiden toimintaan ja vaikuttavuuteen kiinnitetään usein liian vähän huomiota. Resurssien kohdistaminen oikeisiin ratkaisuihin tuottaa merkittäviä säästöjä. (Hayden 2010, xix; Hubbard & Seiersen, 2016, 74; Limnéll ym., 2014, 107.)

Turvallisuuteen liittyy olennaisesti riskit, uhkat ja haavoittuvuudet. Näin ollen kyberturvallisuudesta voidaan saada tieto tarkastelemalla näitä elementtejä. Tutkimusmenetelmät tuottivat lähdeaineistosta tulokseksi kyberturvallisuuden mittaamisen periaatteita eri tasoilla. Näitä tasoja ovat organisaation valmiudet ja kypsyys, organisaation toiminta, yksilön toiminta ja tekniset menetelmät. Organisaation valmiuksia ja kypsyyksiä voidaan arvioida kyberturvallisuuden kypsyysmallien avulla. Tätä tasoa kutsutaan tässä tutkimuksessa strategiseksi tasoksi. Strategisella tasolla korostuu uhkien tarkastelu. Organisaation kyberturvallisuuden toiminnoilla tarkoitetaan niitä toimintoja, joita toteutetaan strategisen tason tavoitteiden saavuttamiseksi. Tätä tasoa kutsutaan tässä tutkimuksessa toiminnalliseksi tasoksi. Toiminnallisella tasolla korostuu riskien tarkastelu. Alimmalla tasolla voidaan mitata yksilöiden kyberturvallisuusvalmiuksia ja teknisiä turvallisuusratkaisuja, joita ovat esimerkiksi tietoturvapoikkeamat, salasanojen vahvuudet ja puolustuksen kerrokset (Miessler 2019; Kurittu 2019). Tässä tutkimuksessa tätä tasoa kutsutaan tekniseksi ja taktiseksi tasoksi. Tällä tasolla korostuu haavoittuvuuksien tarkastelu. Yksilötaso osoittautui erittäin merkittäväksi, sillä lähdeaineiston perusteella kyberturvallisuus on perusteiden hallintaa ja suuren riskin organisaatiolle aiheuttaa sisäiset toimijat (Limnéll ym. 2014, 107; Nielssen 2017). Kurittun (2019) mukaan tämä on kuitenkin haasteellista, sillä yksilöiden välillä osaamistasot ovat erittäin suuria. Tieto- ja viestintäteknologian toimintaperiaatteita ei ymmärretä kovin syvällisesti ja monelle työntekijälle tietokoneiden käyttö on vain pakollinen paha. Limnéll ym. (2014, 14) on kuitenkin sitä mieltä, että kyberturvallisuus on kaksi kolmasosaa muuta kuin teknologiaa. Mittaamisessa kriittistä on ymmärtää riittävän tarkalla tasolla, mitä halutaan mitata ja mitä mittaamisella halutaan saavuttaa (Hayden 2010, xxiv; Miessler 2018a; Hubbard & Seiersen, 2016, 48 ja 148).

5.1 Strateginen taso - uhkat

Strategisen tason kyberturvallisuudella tarkoitetaan tässä tutkimuksessa sitä tasoa, joka edesauttaa tavoitteiden ja vision saavuttamista. Strategisen tason kyberturvallisuudella mahdollistetaan kybertoimintaympäristön tuomien mahdollisuuksien hyödyntäminen. Kypsyysmallien avulla voidaan tarkastella, millaiset edellytykset organisaatiolla tähän on. Kypsyysmalleista saatu informaatio tulisi kohdistaa operatiivisen tason kyberturvallisuuden paranta-

miseen. Esimerkiksi mikäli kypsyysmallista saatujen tulosten perusteella todetaan henkilöstön ohjeistus ja koulutus heikoksi, se konkretisoituu operatiivisella tasolla riskeinä.

Strategisella tasolla tarkastellaan organisaation turvallisuuskulttuuria, ohjeistuksia, koulutuksia sekä prosessien ja tietojärjestelmien turvallisuuden yleistä tasoa. Strategisen tason mittareiden tulisi liittyä läheisesti liiketoimintaprosesseihin (Limnéll ym. 2014, 188). Kyberriskit muuttuvat usein mielenkiitoiseksi vasta silloin, kun ne liittyvät oleellisesti organisaation liiketoimintaprosesseihin (Kurittu 2019). Kyberturvallisuusstrategia auttaa hahmottamaan muutostekijöitä ja käytännön toimenpiteitä tavoitteiden saavuttamiseksi. Mittareiden asettaminen on myös menetelmä viestiä organisaatiolle tärkeiksi koetuista asioista. Strategisella tasolla mittaamista vaikeuttavat ilmiöt, joita on hankala hahmottaa kuten esimerkiksi keskinäisriippuvuudet ja kerrannaisvaikutukset. Kyberturvallisuus on dynaamista, jolloin ilmiön muuttuessa myös mitattu tieto on vanhaa ja mittarit eivät tuota enää toivottua tietoa. Näin ollen mittareiden tulisi olla riittävän tarkkoja, mutta yleispäteviä sekä tarpeen tullen muokattavissa. Kyberturvallisuus on suurimmaksi osaksi muuta kuin teknologiaa, jolloin mittareidenkin tulisi mitata suurimmaksi osaksi muuta kuin teknologiaa. Yksi merkittävimmistä uhkista ovat käyttäjät itsessään, jolloin koulutuksella, ohjeistuksella ja valvonnalla voidaan vaikuttaa merkittävästi kyberturvallisuuden tasoon. Käyttäjien toimintaa ja osaamista voidaan mitata eri menetelmillä toiminnallisella tasolla.

Strateginen taso tuottaa ennen kaikkea tietoa kyberturvallisuuden hallinnosta. Tällä tasolla mitataan muun muassa lakeja, sääntöjä, määräyksiä, ohjeita, koulutusta, suunnittelua, turvallisuushenkilöstön määrää ja vaatimuksia, jatkuvuuden hallintasuunnitelmia sekä kriisiviestintä suunnitelmia. Strategisen tason mittaamisessa haasteena on se, että usein saatavilla olevat kypsyysmallit perustuvat itsearviointiin, jolloin ollen tulokset ovat subjektiivisia ja heikosti verrattavia (Black ym. 2008, 3). NIST CSF tarjoaa kuitenkin yleisesti käytössä olevan kypsyysmallin yrityksen valmiuksien tason määrittämiseksi. Viitekehyksen mukaisten tasojen vertailu organisaatioiden välillä tarjoaa puolestaan suuntaa-antavaa tietoa kokonaisvaltaisemmasta tasosta. Näin ollen Haydenin (2010, 7) mukainen periaate täyttyy, että mikä tahansa mittaaminen on parempi kuin ei mitään, mutta laadukkaimmillaan mittaaminen liittyy liiketoimintaprosesseihin. Vaikka CSF ei tarjoaisikaan tieteellisesti vedenpitävää tietoa kyberturvallisuuden tilasta, niin se pakottaa organisaation itsensä perehtymään omaan kyberturvallisuuteensa. Näin ollen organisaatio saa itse huomattavan määrän tietoa kyberturvallisuudesta.

5.2 Toiminnallinen taso - riskit

Liiketoiminnassa operatiivisella toiminnalla tarkoitetaan tuotteiden, materiaalien ja palveluiden tuottamista sekä jakelua (Juvonen 2014, 40). Tutkimusaineiston perusteella operatiivisella eli toiminnallisella tasolla kyberturvallisuutta voidaan mitata riskienhallinnan menetelmillä. Riskienhallintaa voidaan suorittaa eri menetelmillä ja valmiita viitekehyksiä menetelmien käyttöön on saatavilla useita. Aineiston perusteella asiantuntijat suosittelevat todennäköisyyslaskentaan ja tilastotieteisiin perustuvaa mallia, jolloin päätöksenteon tueksi on käytettävissä tieteellistä tietoa. (Miessler 2019; Hubbard & Seiersen 2016; Hayden 2010.) Valmiit viitekehykset hyödyntävät usein yksinkertaisempia matriiseihin perustuvia menetelmiä (OWASP 2019b; Juvonen 2014, 20–22).

Miesslerin näkökulmat kyberturvallisuuden mittaamiseen ovat hyvin käytännönläheisiä. Hän esittää, että organisaation tulee tarkastella tietyistä tapahtumista saatuja prosentuaalisia arvoja, kuten esimerkiksi turvallisuuspoikkeamien osuutta. (Miessler 2019.) Tämä antaa tietoa riskien todennäköisyydestä. Miessler ei kuitenkaan ota kantaa siihen, mikä on hyväksyttävä, hyvä tai huono riskitoleranssi.

Hubbard & Seiersen (2016) eivät puolestaan ota kantaa siihen, mitä tulisi mitata, vaan miten tulisi mitata. Oikeiden mittareiden asettaminen on onnistumisen edellytys. Mittaamisen tulisi aina perustua epävarmuuden vähentämiseen. Lisäksi mittaamista tulisi suorittaa riittävän tarkalla tasolla: ”devil is in the details” (Hubbard & Seiersen 2016, 27). Tähän perustuu myös Pendletonin (2016) tutkimus järjestelmäturvallisuudesta, jossa mitattavat kohteet (haavoittuvuudet, puolustus, hyökkäys, tilanne) jaetaan riittävän moneen alakategoriaan.

5.3 Tekninen ja taktinen taso - haavoittuvuudet

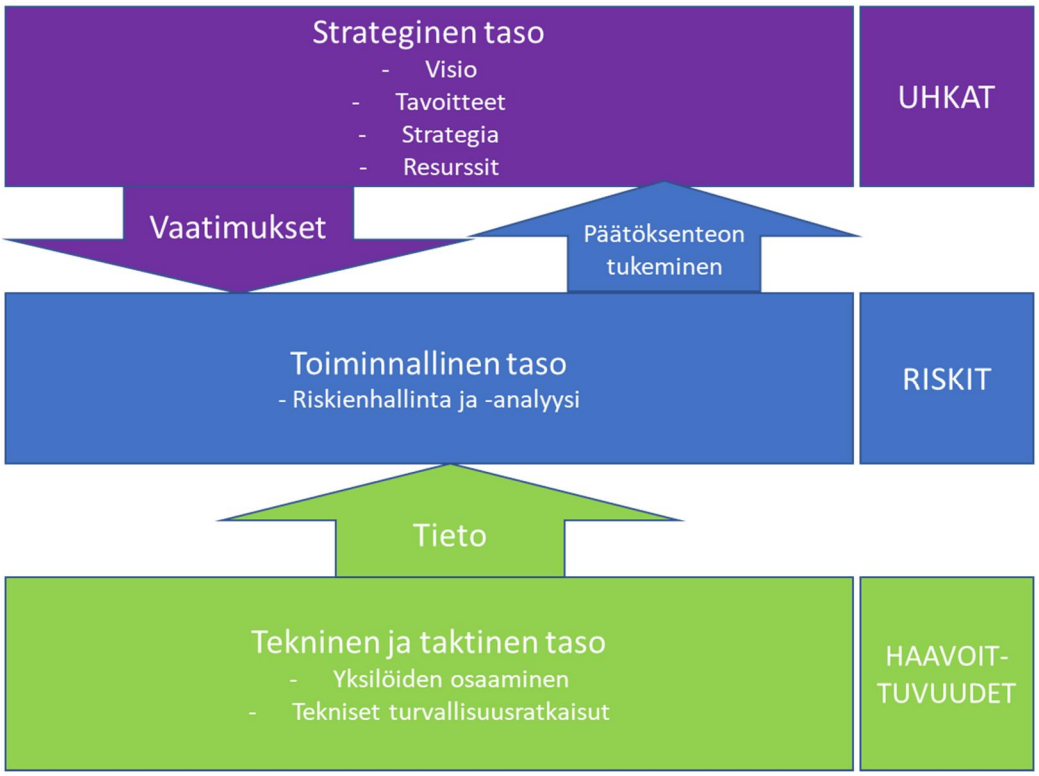
Tutkimusaineiston perusteella toiminnallisen tason alapuolelle voidaan vielä lisätä tekninen taso (kts. esim. Miessler 2019 ja Pendleton ym. 2016). Riskien mittaamisen ja analysoinnin tueksi keskeisiä mitattavia kohteita ovat ihmiset ja teknologia. Tässä tutkimuksessa teknisellä tasolla tarkoitetaan kaikkia niitä toiminnallisen tason toimenpiteitä, joihin liittyy teknologian hyödyntäminen tiedon keräämiseen. Tällä tarkoitetaan esimerkiksi penetraatiotestauksien tuloksia, tietoliikenteen seurantaa, tunnettuja haavoittuvuuksia, salasanojen vahvuuksia, mustia listoja, aktiivisen puolustuksen menetelmiä ja tietojärjestelmien päivityksiä. Työntekijöiden osaaminen, motivaatio ja toimintatavat kertovat myös paljon kyberturvallisuuden tasosta ja organisaatiokulttuurista. Teknisen ja taktisen tason mittarit eivät kuitenkaan yksistään kerro tarpeeksi organisaation kyberturvallisuuden kokonaisvaltaisesta tasosta. Niiden avulla saatetaan paljastaa haavoittuvuuksia tai niistä saatua tietoa voidaan hyödyntää riskien todennäköisyyksien arvioimisessa toiminnallisella tasolla.

Etenkin teknisistä järjestelmistä on saatavilla lukematon määrä dataa. Näin ollen on kehitetty myös useita menetelmiä tämän datan mittaamiseen (esim. CVSS, NMAP, Shodan. SIEM). (Kts. esim. Pendleton 2016.)

Vahvuutena tämän tason mittareissa on objektiivisuus. Saatava data voi olla esimerkiksi päivitettyjen järjestelmien prosenttiosuus tai salasanojen keskipituus. Ongelmana on kuitenkin muutos ja kehitys. Esimerkiksi kahdeksan merkkiä pitkä salasana voi tänään olla ”vahva”, mutta laskentatehon kehittyessä jo kahden vuoden päästä ”heikko”. Uusien päivitysten myötä saattaa ilmentyä uusia *nolla-päivä*-haavoittuvuuksia.

5.4 Analyysin yhteenveto

Strategisen tason tehtävänä on tuottaa vaatimuksia toiminnalliselle tasolle siitä, mitä riskejä ja kuinka paljon voidaan sietää? Teknisen ja taktisen tason tehtävänä on puolestaan tuottaa tietoa toiminnalliselle tasolle, minkä perusteella voidaan toteuttaa riskienhallintaa ja -analyysiä. Kuvassa 10 on havainnollistettu kyberturvallisuuden mittaamisen tasoja ja suhteita toisiinsa.



Kuva 10. Kyberturvallisuuden mittaamisen tasot ja suhteet.

Keskeinen ongelma kyberturvallisuuden mittaamisessa on ilmiön dynaamisuus. Miten voidaan tietää mittareiden perusteella, johtuvatko vuoden aikana lisääntyneet onnistuneet hyök-

käykset tekniikoiden kehittymisestä, parantuneesta hyökkäyksien havaitsemisesta ja tilastoinnista, onnistuneista tietojen kalastelusta vai koulutuksen puutteesta tai epäonnistumisesta. Ongelmana on myös ymmärtää mitkä mittarit korreloivat ilmiön kanssa parhaiten ja mille mittarille tulisi antaa suurin painoarvo. (Black ym. 2008, 4–5.)

Kokonaisvaltainen kyberturvallisuuden mittaaminen vaatii usean eri tason ja osa-alueen mittaamista. Mitattavat kohteet ja mittaamisen tavoitteet tulee olla tarkasti määritelty. Mitä yksityiskohtaisempaa asiaa halutaan mitata, sitä enemmän epävarmuutta tulokset vähentävät. Kyberturvallisuus nähdään organisaatioissa usein pakollisena ja tuottamattomana pahana eikä mahdollistajana. Tämä osaltaan korostaa laadukkaan tiedon merkitystä päätöksenteon tueksi. Laadukasta tietoa ei kuitenkaan ole saatavilla ilman resurssien kohdentamista kyberturvallisuuden mittareiden kehittämiseen. Kehittäminen tulisi aloittaa ylimmältä tasolta, jolloin organisaation johto saadaan sitoutettua kehitysprosessiin ja mittarit sidottua liiketoimintaprosesseihin. Strategiselta tasolta saadaan johdettua tavoitteet toiminnallisen tason mittareille, jolloin päätöksenteon tueksi voidaan tuottaa vain johdon tarvitsemaa tietoa. Teknisellä ja taktisella tasolla on huomattava merkitys organisaation kyberturvallisuuteen. Henkilöstön valmiuksien kehittäminen on kuitenkin haasteellista. Teknisistä ratkaisuista, menetelmistä ja järjestelmistä on saatavilla hyödyllistä tietoa kyberuhkien, -riskien sekä -haavoittuvuuksien trendeistä ja muutossuunnista.

6 JOHTOPÄÄTÖKSET

Tutkimustehtävänä oli selvittää, miten kyberturvallisuutta voidaan mitata. Tutkimuksen ensimmäisessä vaiheessa selvitettiin mitä on kyberturvallisuus ja miten siitä voidaan saada tietoa. Toisessa vaiheessa tutkittiin mitä olemassa olevia menetelmiä kyberturvallisuuden mittaamiseen on olemassa. Tutkimusaineiston perusteella ei voida luoda yhtä valmista mallia kyberturvallisuuden tason *de facto* määrittämiseksi, josta saatavat tulokset olisivat yleisesti verrannollisia toistensa kanssa. Mittaamista voidaan toteuttaa eri tasoilla ja sillä voidaan parhaimmillaan parantaa päätöksentekoa sekä vähentää epävarmuutta. Laadukkaaseen ja onnistuneeseen mittaamiseen on saatavilla tietoa, työkaluja ja valmiita menetelmiä.

Kyberturvallisuuden mittaaminen on tieteellisesti vähän tarkasteltu aihe. Limnéll ym. (2014, 188) teoksessa kyberturvallisuuden mittaamista käsiteltiin kahdella lauseella eikä tietokantahaussa aiheesta löytynyt merkittävästi tieteellisiä julkaisuja. Kyberturvallisuuden analysointi on laajasti vielä alkutekijöissä ja se perustuu enemmänkin tietoturvallisuuden arviointiin. Kyberturvallisuuden mittaamisessa haasteena on hahmottaa ero ”mitä voidaan mitata” ja ”mitä tulee mitata” välille (Pendleton ym. 2016, 62:23; Hayden 2010, xxiv; Hubbard & Seiersen 2016, 27–28). Usein mitattavaa asiaa ja mittaamisen tavoitteita ei ymmärretä riittävän hyvin, mikä heikentää mittaamisen tarkkuutta (Black ym. 2008, 3). Turvallisuus nähdään vain pakollisena pahana, joka ei tuota mitään, jolloin siihen ei haluta kohdentaa resursseja. Turvallisuus halutaan sisäänrakennettuna. Teknologisissa ratkaisuissa se nähdään myös ulkoistusmahdollisuutena. (Kurittu 2019, Limnéll ym. 2014, 14.)

Kansallista kypsyysmallia ollaan vasta ottamassa käyttöön, vaikka kansalliset riskiarviot ovat usean vuoden korostaneet kyberturvallisuuden kasvavaa merkitystä. Kansallista menetelmää tullaan hyödyntämään yhteiskunnan toimivuuden kannalta kriittisten yritysten valmiuksien arvioinnissa. Näin ollen mallin tulisi olla soveltuva minkä tahansa yrityksen käyttöön. Yhtenevät menetelmät tarjoavat mahdollisuuden vertailevaan tutkimukseen, mikä parantaa ilmiön kokonaisvaltaista tutkimusta ja kehittämistä.

Kyberturvallisuuden laatua tulisi analysoida yrityksen kaikilla tasoilla. Näin ollen saadaan luotettava kuva siitä, mitkä ovat yrityksen valmiudet selviytyä kybertoimintaympäristössä sekä mikä on yrityksen kyky kohdentaa resursseja riskien minimoimiseksi.

6.1 Tutkimuksen pätevyys ja luotettavuus

Tutkimuksen *reliaabelius* (luotettavuus) tarkoittaa tutkimuksen toistettavuutta. Tämä tarkoittaa kuinka hyvin toinen tutkija päätyisi samoihin tuloksiin käyttäen samoja menetelmiä ja aineistoa. Tämän tutkimuksen luotettavuutta on parannettu kuvaamalla tarkasti tietoaineiston

haku, lähdeaineisto, tutkimusmenetelmät ja tutkimusprosessi. Tutkimusprosessia on myös seurattu johdonmukaisesti läpi tutkimuksen. Tutkimuksen *validius* (pätevyys) tarkoittaa tutkimusmenetelmän kykyä mitata tutkittavaa aihetta ja ilmiötä. Pätevyyttä arvioitaessa tulee tarkastella, että onko esitetty selitys luotettava ja uskottava. Tässä tutkimuksessa uskottavuutta on parannettu kattavalla lähdeaineistolla ja siihen kohdistetulla kritiikillä. (Hirsjärvi 2002, 213.)

Tutkimuksen luotettavuutta olisi edelleen parantanut useamman tutkimusmenetelmän käyttö (triangulaatio) (Hirsjärvi 2002, 215). Esimerkiksi teemahaastattelut yritysten ja organisaation informaatioturvallisuudesta vastaaville henkilöille olisi saattanut tuoda käytännönläheistä tietoa *de facto* toimintatavoista yrityksissä.

Hubbard, Seiersen, Miessler ja Hayden ovat konsultteja, jotka yrittävät myydä tuotettaan. Tästä syystä heihin tulee suhtautua kriittisesti. Kaikilla on kuitenkin pitkä kokemus kyberturvallisuudesta ja riskienhallinnasta. Miessler esittää näkemyksiään verkkosivuillaan ja ne perustuvat täysin hänen omiin mielipiteisiinsä. Miesslerin uskottavuutta parantaa se, että häneen on viitattu muun muassa Lehto ym. (2018, 67) määritettäessä hyvien mittareiden ominaisuuksia julkaisussa *Kyberturvallisuuden strateginen johtaminen Suomessa*. Tässä tutkimuksessa yksi keskeisimmistä lähteistä on Hubbard & Seiersenin *How to Measure Anything in Cyber Security Risk,* joka ei ole tieteellinen teos. Laajempi tieteellinen lähdeaineisto olisi parantanut tutkimuksen luotettavuutta. Ongelmaksi muodostui tieteellisen tutkimuksen saatavuus. Myös useamman viitekehykset ja mallin vertaaminen olisi tuottanut laadukkaampaa tietoa, mutta tämän opinnäytetyön laajuudessa se ei ollut mahdollista.

6.2 Tutkimuksen onnistuminen ja hyödynnettävyys

Tämän tutkimuksen avulla yritykset ja organisaatiot voivat arvioida omia menetelmiään resurssien mahdollisimman tehokkaan kohdentamisen varmistamiseksi. Tämä tutkimus ei tarjoa valmista mallia, menetelmää tai mittaria kyberturvallisuustasojen arvioimiseksi. Tällä tutkimusaineistolla sitä ei välttämättä olisi mahdollista edes toteuttaa. Käytetty tutkimusaineisto puoltaa useassa kohtaa tilastollisia menetelmiä, mutta tässä tutkimuksessa ei kyetä tieteellisesti osoittamaan, mikä menetelmä on todellisuudessa käyttökelpoisin ja vähentää epävarmuutta tehokkaimmin. Tutkimuksessa on kuitenkin esitetty asiantuntijoiden näkemyksiä siitä, miksi toiset menetelmät vähentävät epävarmuutta tehokkaammin kuin toiset. Tutkimus tarjoaa tietoa siitä, mistä eri näkökulmista subjektiivista, muuttuvaa ja abstraktia kyberturvallisuuden käsitettä voidaan lähestyä ja miten siitä voidaan saada tietoa. Ennen kaikkea kyberturvallisuutta tulee arvioida kokonaisvaltaisesti ja mittaaminen tulee olla tavoitteellista sekä edistää päätöksentekoa.

Turvallisuuden tutkiminen vaatii aina tieteellisen paradigman ja näkökulman valitsemista. Alemman korkeakoulututkinnon tasoisessa opinnäytetyössä usein on tuottaa mahdollisimman käytännönläheistä tietoa hyviä tieteen käytäntöjä noudattaen. Tutkimusaineisto osoittaa, että mitä alemmalla ja yksityiskohtaisemmalla kyberturvallisuuden mittaamisen tasolla ilmiötä tarkastellaan, sitä konkreettisempaa ja käytännönläheisempää tietoa on saatavilla. Tässä tutkimuksessa keskityttiin tarkastelemaan toiminnallista tasoa. Edelleen käytännönläheisempää tietoa olisi ollut saatavilla, mikäli tutkimuksen fokus olisi ollut teknisellä ja taktisella tasolla. Tässä tapauksessa tutkimusta ei välttämättä voitaisi hyödyntää yhtä laaja-alaisesti, eikä se välttämättä kestäisi aikaa yhtä hyvin. Toinen tapa tuottaa käytännönläheisempiä tutkimustuloksia olisi ollut käyttää empiirisiä tutkimusmenetelmiä. Esimerkiksi yrityksille kohdennettu kyselytutkimus olisi saattanut tuottaa erittäin käytännönläheisiä tuloksia *de facto* kyberturvallisuuden arviointimenetelmistä. Tutkimuksen hyödynnettävyyden keskeisenä kysymyksenä onkin, että mikä on tutkimuksen arvo, jos kyberturvallisuuden käsite on jatkuvasti muuttuva? Tästä syystä riskienhallinnan menetelmät soveltuvat kyberturvallisuuden mittaamiseen varsin hyvin, sillä menetelmät pätevät yhä, vaikka siihen syötetyt arvot vanhenisivatkin.

6.3 Oppiminen

Tutkimusaiheen valinnassa keskeisenä motiivina oli ymmärtää, miten voidaan sanoa onko kyberturvallisuus hyvä vai huono. Alkuperäisenä tavoitteena oli löytää tai luoda yleispätevä teoria tai malli kyberturvallisuuden mittaamiselle, jota organisaatiot tai yritykset voisivat hyödyntää. Kirjallisuuskatsauksessa kuitenkin nopeasti selvisi, ettei se ollut realistinen tavoite. Käytettävät mallit riippuvat paljon muun muassa siitä mitä halutaan mitata ja millaisessa toimintaympäristössä. Sen sijaan tavoitteeksi asettui ymmärtää mitä eri menetelmiä kyberturvallisuuden mittaamiselle on.

Opinnäytetyön tekeminen opetti paljon tieteellisen tutkimuksen toteuttamisesta. Etenkin tiedon analysointi kehittyi tutkimuksen teon aikana. Analyysiosaaminen on varmasti hyödyllinen taito tulevaisuuden työtehtävissä. Keskeisin oppi ammattitaidon kehittymisen kannalta oli kuitenkin oppi kyberturvallisuudesta ja mittaamisen periaatteista. Kyberturvallisuus liittyy olennaisesti tietojenkäsittelyyn sekä liiketalouteen, jotka ovat tämän koulutusohjelman keskeisimmät teemat. Opinnäytetyön toteuttaminen vaati aikaisemman tiedon ja tutkinnon aikana opitun tiedon yhdistämistä sekä täysin uuden tiedon oppimista. Näin ollen voidaan todeta tutkimuksen edistäneet kokonaisvaltaisesti ammattitaitoa.

Minulla ei juuri ollut aikaisempaa osaamista tässä tutkimuksessa esitetyistä tilastotieteellisistä menetelmistä. Mielenkiintoista oli oppia hyödyntämään näitä menetelmiä riskiarvioinnissa. Ennakkoasenteeni oli, että ne ovat liian hankalia, jotta voisin niitä itse käyttää. Opin kuitenkin, että näiden menetelmien toteutus esimerkiksi Excel taulukko-ohjelmalla on kohtalaisen

yksinkertaista. Lisäksi saatavilla on useita käytännönläheisiä ohjeita menetelmien toteuttamiseen. Tätä osaamista tulen hyödyntämään tulevaisuudessa parantaakseni käsitystä niiden todellisesta käytettävyydestä.

Opinnäytetyön tekoon oli käytössä rajallinen aika, mikä pakotti aikataulun luomista, siinä pysymistä ja tehokasta työskentelyä. Mikäli aikaa olisi ollut enemmän käytössä, olisin todennäköisesti kyennyt analysoimaan laajemman lähdeaineistoa ja perehtymään eri yritysten toimita tapoihin syvemmin. Tämä olisi osaltaan parantanut tutkimuksen tieteellisyyttä ja lisätä käytännönläheisyyttä. Toisaalta jo nyt tutkimuksen lähdeaineisto on vaatimuksiin nähden suhteellisen laaja sekä riittävä tutkimuksen tavoitteiden saavuttamiseen. Lähdekritiikki oli paikoin haastavaa. Kuinka paljon voi antaa arvoa millekin lähteelle. Kyberturvallisuudesta yleisesti on kirjoitettu paljon, jolloin oleellisen aineiston löytäminen juuri tämän tutkimuksen kannalta korostuu. Tutkimuksen *itse korjaantuvuus* on hyvien tieteellisten käytäntöjen mukaista. Näin ollen tässä tutkimuksessa tehdyt virheet on korjattavissa tulevissa tutkimuksissa.

6.4 Jatkotutkintamahdollisuudet

Kyberturvallisuus on suhteellisen nuori ilmiö, joten jatkotutkimusmahdollisuuksia on useita. Etenkin tieteellistä tutkimusta tulisi tehdä, jotta mahdollisimman objektiivista tietoa ilmiöstä olisi helposti saatavilla. Objektiivisen tiedon kannalta merkittävää on tutkia myös mahdollisuuksia toteuttaa tieteellistä tutkimusta kyberilmiöstä.

Käytännönläheisintä tietoa kyberturvallisuudesta on saatavilla teknisellä ja taktisella tasolla. Näin ollen esimerkiksi toiminnallinen opinnäytetyö penetraatiotestauksen tai Red Team -menetelmien hyödynnettävyydestä eri organisaation kyberturvallisuuden teknisen ja taktisen tason mittaamiseen, tuottaisi mielenkiintoista ja käytännönläheistä tietoa näiden menetelmien hyödyistä.

Kybertoimintaympäristöä ei säädellä kansainvälisellä lailla. Näin ollen tästä näkökulmasta toteutettu tieteellinen tutkimus tuottaisi tietoa kybertoimintaympäristöstä, jota voitaisiin hyödyntää kansallisen tason ohjeistuksien ja säädösten luomiseen. Se saattaisi auttaa myös organisaatioita ja yrityksiä ymmärtämään kybertoimintaympäristön uhkia ja riskejä esimerkiksi liiketoiminnan näkökulmasta.

Lähdeaineistossa esiintyi ristiriitaa riskienhallintamenetelmien käytöstä. Tämän tutkimuksen lähdeaineistossa asiantuntijat korostivat tilastotieteellisiä menetelmiä laajasti käytettyjen riskimatriisien sijaan. Toisaalta empiria näyttää tukevat riskimatriiseja enemmän kuin tilastotieteellisiä menetelmiä. Tieteellinen tutkimus siitä, mitkä menetelmät vähentävät epävarmuutta parhaiten, edistäisi päätöksentekoa käytettävien menetelmien suhteen.

LÄHTEET

Abbadi, Z. 2016. Security Metrics What Can We Measure? Luettavissa: https://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf. Luettu: 29.3.2019

Black, P. E. & Scarfone, K., Souppaya, M. 2008. Cyber Security Metrics and Measures. National Institute of Standards and Technology, Gaithersburg, Maryland. PDF ladattavissa: https://www.researchgate.net/publication/237783252_Digital_Disaster_Cyber_Security_and_the_Copenhagen_School1.

Brook, C. 4.12.2018. Datainsider, artikkeli: What is the NIST Cybersecurity Framework? Luettavissa: https://digitalguardian.com/blog/what-nist-cybersecurity-framework. Luettu: 29.3.2019.

Chistopher, J. 1.11.2018. Artikkeli: The Cybersecurity Maturity Model: A Means To Measure And Improve Your Cybersecurity Program. Forbes. Luettavissa: https://www.forbes.com/sites/forbestechcouncil/2018/11/01/the-cybersecurity-maturity-model-a-means-to-measure-and-improve-your-cybersecurity-program/#7d882555680b. Luettu: 28.3.2019.

Cohen, F. 2011. Measuring Security. PDF ladattavissa: https://pdfs.semanticscholar.org/f48b/9a9db0c9d27f7767bbb469437ee7daccc110.pdf.

Edgar, T. & Manz, D. 2017. Research Methods for Cyber Security. Syngress, Cambridge, Yhdysvallat.

Eskola, S. 2008. Turvallisuus käsitteenä. Maanpuolustuskorkeakoulu, Strategian laitos Julkaisusarja 3, Strategian asiatietoa, No 10. PDF ladattavissa: https://www.doria.fi/bitstream/handle/10024/74107/StratL3_10.pdf?sequence=1&isAllowed=y.

Europol. 2019. Cybercrime. Luettavissa: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime. Luettu: 29.3.2019.

Fielder, A. & Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. 2016. Decision support approaches for cyber security investment. PDF ladattavissa: https://reader.elsevier.com/reader/sd/pii/S0167923616300239?token=07788A8D9FF91E4BC

6B78EE2C9645C788F68B19A0C3FF0B8C0EC0A2CD7F56EC11D3619859E4850DF5734E147668D7E9F.

Finna.fi. 2019. Tietokanta. Luettavissa: https://www.finna.fi/Content/organisations. Luettu: 19.3.2019.

FIRST. 2019. Common Vulnerability Scoring System v3.0: User Guide. Luettavissa: https://www.first.org/cvss/user-guide. Luettu: 18.4.2019.

Hammasten, H. 15.2.2017. Viisi ikuisuuskysymystä strategiasta ja mittareista: Aalto-yliopiston professori Teemu Malmi vastaa. Artikkeli. Luettavissa: https://www.aaltopro.fi/aalto-leaders-insight/2017/viisi-ikuisuuskysymysta-strategiasta-ja-mittareista. Luettu: 4.3.2019.

Harisalo, R. 2005. Riskit yhteiskunnassa ja markkinoilla: Itävaltalaisen teorian näkökulma. Teoksessa: Kuusela, Hannu & Ollikainen, Reijo (toim.). Riskit ja riskienhallinta. Tampere University Press, Tampere. PDF ladattavissa: https://tampub.uta.fi/bitstream/handle/10024/65418/riskit_ja_riskienhallinta_2005.pdf?sequence=1.

Hayden, L. 2010. IT-Security Metrics – Practical Framework for Measuring Security and Protecting Data. PDF ladattavissa: https://epdf.tips/it-security-metrics-a-practical-framework-for-measuring-security-protecting-data.html.

Hiltunen, A. 16.6.2017. Millainen on hyvä strategia. Helsingin kaupungin valtuuston seminaari. PDF ladattavissa: https://www.hel.fi/static/helsinki/kaupunkistrategia/valtuustoseminaari-0617/hiltunen.pdf.

Hubbard, D. 2014 (2007). How To Measure Anything – Finding the Value of “Intangibles” in Business (3rd edition). Wiley.

Hubbard, D. & Seiersen, R. 2016. How To Measure Anything In Cybersecurity Risk. Wiley.

Kinnunen, Y. 22.8.2017. SIEM-järjestelmä on organisaation kyberturvallisuuden hermokeskus. Insta, artikkeli. Luettavissa: https://www.insta.fi/medialle/tiedotteet-ja-artikkelit/insta-defsec/2017/08/siem-jarjestelma-on-organisaation-kyberturvallisuuden-hermokeskus.html. Luettu: 24.4.2019.

Institute of Risk Management. 2019. Cyber risk and risk management. Verkkosivut. Luettavissa: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/. Luettu: 29.3.2019.

ISO. 2019a. ISO/IEC 27000 family - Information security management systems. Luettavissa: https://www.iso.org/isoiec-27001-information-security.html. Luettu: 12.4.2019.

ISO. 2019b. ISO/IEC 31010. Luettavissa: https://www.iso.org/obp/ui/#iso:std:iec:31010:ed-1:v1:en. Luettu: 12.4.2019.

ISO. 2019c. ISO/IEC 31010 final draft. PDF ladattavissa: http://ehss.moe.gov.ir/getattachment/f7de1f2a-7559-49b5-8b97-c69b13fa17a9/31010-FDIS-(Risk-Assessment-Technics).

Jardine, E. 2017. Sometimes Three Rights Really Do Make a Wrong: Measuring Cybersecurity and Simpson's Paradox. PDF ladattavissa: https://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/07/WEIS_2017_paper_18.pdf.

Juvonen, M. & Koskensyrjä, M., Kuhanen, L., Ojala, V., Penttinen, A., Porvari, P., Talala, T. 2014. Yrityksen riskienhallinta. Finanssi- ja vakuutuskustannus Oy.

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylän ammattikorkeakoulun julkaisuja 234.

Kannus, K. 2017. Suomen valmistavan teollisuuden kyberturvallisuuden tulevaisuudennäkymiä. Diplomityö, Tampereen teknillinen yliopisto, tietotekniikan koulutusohjelma. PDF ladattavissa: https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/24932/Kannus.pdf?sequence=3&isAllowed=y.

Kaplan, R. & Norton, D. 2004. Strategiakartat – Aineettoman pääoman muuttaminen mitattaviksi tuloksiksi. Talentum, Helsinki.

Karha, H. & Kuusela, H., Kanto, A. 2005. Taloudellisen riskin hallinta. Teoksessa: Kuusela, Hannu & Ollikainen, Reijo (toim.): Riskit ja riskienhallinta. Tampere University Press, Tampere. PDF ladattavissa: https://tampub.uta.fi/bitstream/handle/10024/65418/riskit_ja_riskienhallinta_2005.pdf?sequence=1.

Keskuskauppakamari. 2016. Tietoturvaopas yrityksille. PDF ladattavissa: http://www.doaudit.fi/tietoturvaopas/.

Kurittu, A. 24.4.2019. Sähköposti kirjoittajalle. Kyberturvallisuuskeskus. Materiaali kirjoittajalla.

Kuusela, H. & Ollikainen, R. (toim.). 2005. Riskit ja riskienhallinta-ajattelu. Teoksessa: Riskit ja riskienhallinta. Tampere University Press, Tampere. PDF ladattavissa: https://tampub.uta.fi/bitstream/handle/10024/65418/riskit_ja_riskienhallinta_2005.pdf?sequence=1.

KvaliMOTV. 2019. Teoria ja tutkimus. Yhteiskuntatieteellinen tietoarkisto. Luettavissa: https://www.fsd.uta.fi/menetelmaopetus/kvali/L2_2.html. Luettu: 21.3.2019.

Kyberturvallisuuskeskus. 2018. Tietoturvan vuosi 2018. Traficom. PDF ladattavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf.

Laurio, J-M. 14.10.2014. Haavoittuvuuden vakavuuden luokittelu lähtee CVSS-arvosta. Nixu cybersecurity, verkkoartikkeli. Luettavissa: https://www.nixu.com/fi/blog/haavoittuvuuden-vakavuuden-luokittelu-lahtee-cvss-arvosta. Luettu: 18.4.2019.

Lehto, M. & Limnéll, J., Kokkomäki, T., Pöyhönen, J., Salminen, M. 2018. Kyberturvallisuuden strateginen johtaminen Suomessa. Luettavissa: https://tietokayttoon.fi/documents/10616/6354562/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf/efea3c33-3c74-4cf6-b237-d49b4f10ab83?version=1.0.

Limnéll, J. & Majewski, K., Salminen, M. 2014. Kyberturvallisuus. Docendo.

Miessler, D. 5.12.2018a. An Information Security Metrics Primer. Verkkoartikkeli. Luettavissa: https://danielmiessler.com/study/security-assessment-types/#audit. Luettu: 4.4.2019.

Miessler, D. 5.12.2018b. An NMAP Primer. Verkkoartikkeli. Luettavissa: https://danielmiessler.com/study/nmap/. Luettu: 18.4.2019.

Miessler, D. 5.12.2018c. A Shodan Tutorial and Primer. Verkkoartikkeli. Luettavissa: https://danielmiessler.com/study/shodan/. Luettu: 18.4.2019.

Miessler, D. 4.2.2019. Information Security Assessment Types. Verkkoartikkeli. Luettavissa: https://danielmiessler.com/study/security-assessment-types/#audit. Luettu: 4.4.2019.

MIT Technology Review. 2019. Six Cyber Threats to Really Worry About in 2018. Verkkoartikkeli. Luettavissa: https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/. Luettu: 29.3.2019.

Nilsen, R. 2017. Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges. PDF ladattavissa: https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2013&context=gscis_etd.

NIST. 16.4.2018. Framework for Improving
Critical Infrastructure Cybersecurity – versio 1.1. PDF ladattavissa:
https://www.nist.gov/cyberframework/framework.

NIST. 2019. An Introduction to the Components of the Framework. Verkkoartikkeli. Luettavissa: https://www.nist.gov/cyberframework/online-learning/components-framework. Luettu: 29.3.2019.

Ollila, K. 24.1.2013. Kyberstrategia paljastui pohjapaperiksi. TiVi, verkkoartikkeli. Luettavissa: https://www.tivi.fi/Uutiset/2013-01-24/Kyberstrategia-paljastui-pohjapaperiksi-3197981.html. Luettu: 4.3.2019.

Oulun yliopisto. 18.2.2019. Tieteellisiin julkaisuihin pohjautuva arviointi*:* Google Scholar*.* Luettavissa: http://libguides.oulu.fi/julkaisujenarviointi/GS. Luettu: 19.3.2019.

OWASP. 2019a. Verkkosivut. Luettavissa: https://www.owasp.org/index.php/Main_Page. Luettu: 1.4.2019.

OWASP. 2019b. OWASP Risk Rating Methodology. Verkkosivut. Luettavissa:
https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. Luettu: 1.4.2019.

Oxford dictionaries. 2019. Cyberthreat. Verkkosanakirja. Luettavissa:
https://en.oxforddictionaries.com/definition/cyberthreat. Luettu: 29.3.2019.

Pendleton M. & Garcia-Lebron, R., Cho, J-H., Xu, S. 2016. A Survey on Systems Security Metrics. ACM Comput. Surv. 49, 4, Article 62. PDF ladattavissa:
http://delivery.acm.org/10.1145/3010000/3005714/a62-

pendle-
ton.pdf?ip=192.130.252.29&id=3005714&acc=CHORUS&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E6D218144511F3437&__acm__=1555498684_d7dda8748a3fe513b8adcffef5b2c191.

Poliisi. 2019. Kyberrikollisuus. Luettavissa: https://www.poliisi.fi/rikokset/kyberrikollisuus. Luettu: 29.3.2019.

Puolustusministeriö. 2019. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Verkkosivut. Luettavissa: https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille. Luettu: 12.4.2019.

Rautio, P. 23.2.2015. Strategisten tavoitteiden toteutumisen mittaaminen. Metropolian ammattikorkeakoulu, Insinööri, Tuotantotalouden koulutusohjelma. PDF ladattavissa: https://www.theseus.fi/bitstream/handle/10024/89635/ONT2_Rautio_Pasi.pdf?sequence=1

Rousku, K. 2014. Kyberturvallisuus: Tietoturvaa kotona ja työpaikalla. Talentum.

Salminen, A. 2011. Mitä on kirjallisuuskatsaus–johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovellutuksiin. Vaasan yliopiston julkaisuja, opetusjulkaisuja 64, Vaasa. PDF ladattavissa: https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf.

Salo, U-M. 2015. Simsalabim, sisällönanalyysi ja koodaamisen haasteet. Teoksessa Umpikujasta oivallukseen: Refleksiivisyys empiirisessä tutkimuksessa. Aaltonen, S. & Högbacka, R. Tampere: Tampere University Press.

Sipilä, J. & Koivula, T. 2014. Kuinka strategiaa tutkitaan, 2. uudistettu painos. Maanpuolustuskorkeakoulu, Strategian laitos, julkaisusarja 2, tutkimusselosteita No 52, Helsinki.

Sisäministeriö. 3/2016. Suomen kansallinen riskiarvio 2015. PDF ladattavissa: https://www.kansalainen.fi/wp-content/uploads/riskiarvio.pdf

Sisäministeriön julkaisuja. 2019:5. Kansallinen riskiarvio 2018. PDF ladattavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161332/5_2019_Kansallinen%20riskiarvio.pdf

SUSE. 16.1.2017. SUSE will move to CVSS v3.0. Blogi-kirjoitus. Luettavissa: https://www.suse.com/c/suse-will-move-cvss-v3-0/. Luettu: 18.4.2019.

Theseus. 2019. Tietokanta. Luettavissa: https://www.theseus.fi/. Luettu: 19.3.2019.

Tieteen termipankki. 2019a. Filosofia:ontologia. Verkkosivut. Luettavissa: https://tieteentermipankki.fi/wiki/Filosofia:ontologia. Luettu: 21.3.2019

Tieteen termipankki. 2019b. Filosogia:epistomologia. Verkkosivut. Luettavissa: http://tieteentermipankki.fi/wiki/Filosofia:tietoteoria. Luettu: 21.3.2019

Tieteen termipankki. 2019c. Filosogia:metodologia. Verkkosivut. Luettavissa: http://tieteentermipankki.fi/wiki/Filosofia:metodologia. Luettu: 21.3.2019

Tieteen termipankki. 2019d. Paradigma. Verkkosivut. Luettavissa: http://tieteentermipankki.fi/wiki/Filosofia:paradigma. Luettu: 12.3.2019.

Tilastokeskus. 14.6.2002. Subjektiiviset vai objektiiviset mittarit. Verkkosivut. Luettavissa: https://www.stat.fi/tup/tietoaika/tilaajat/ta_06_02_melkas.html. Luettu: 4.3.2019.

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Tammi, Helsinki.

Ulkoministeriö. 2019. Kyberturvallisuus ja kybertoimintaympäristö. Verkkosivut. Luettavissa: https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto. Luettu: 10.4.2019.

Valtioneuvoston periaatepäätös. 2.11.2017 (VNp 2017). Yhteiskunnan turvallisuusstrategia 2017. Turvallisuuskomitea. PDF ladattavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf.

Valtioneuvoston periaatepäätös. 24.1.2013 (VNp 2013). Suomen kyberturvallisuusstrategia. Luettavissa: https://www.defmin.fi/files/2368/Suomen_kyberturvallisuusstrategia_ja_taustamuistio.pdf.

VAHTI. 2/2014. Tietoturvallisuuden arviointi -ohje. Valtiovarainministeriö. PDF ladattavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ce1ccede-8669-4166-b084-9cafbe6e1e60&groupId=10229.

VAHTI. 2/2016. Toiminnan jatkuvuuden hallinta. Valtiovarainministeriö. PDF ladattavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229.

Verschuuren, G. M. 2014. Excel simulations – Using Excel to Model Risk, Investments, Genetics, Growth, Gambilng and Monte Carlo Analysis. Holy Marco! Books.

Verizone. 2013. Data Breach Investigations Report 2013. PDF ladattavissa: http://www.eventtracker.com/eventtracker/media/eventtracker/files/collateral/verizon-data-breach-2013.pdf.

Verizone. 2018. Data Breach Investigations Report 2018. PDF ladattavissa: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.

Vesamäki, P. 15.3.2016. Vieraskynä: SIEM lokitiedon hyödyntämisessä. Traficom, verkkoartikkeli. Luettavissa: https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn201603151527.html . Luettu: 24.4.2019.

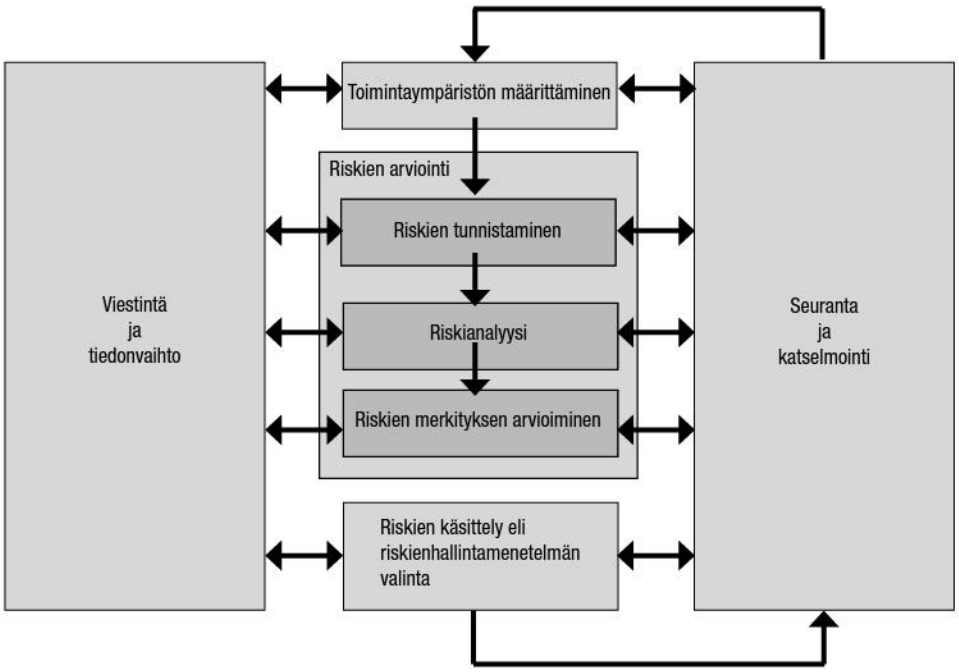
Vänskä, O. 30.8.2017. F-Securen Red Team murtautuu mihin tahansa suomalaiseen toimistoon – "Onnistumme käytännössä satavarmasti". Tekniikka ja talous, verkkoartikkeli. Luettavissa: https://www.tekniikkatalous.fi/tekniikka/f-securen-red-team-murtautuu-mihin-tahansa-suomalaiseen-toimistoon-onnistumme-kaytannossa-satavarmasti-6672403. Luettu: 2.5.2019.

Wang L. & Jajodia, S., Singhal, A. 2017. Network Security Metrics. Springer, Sveitsi.

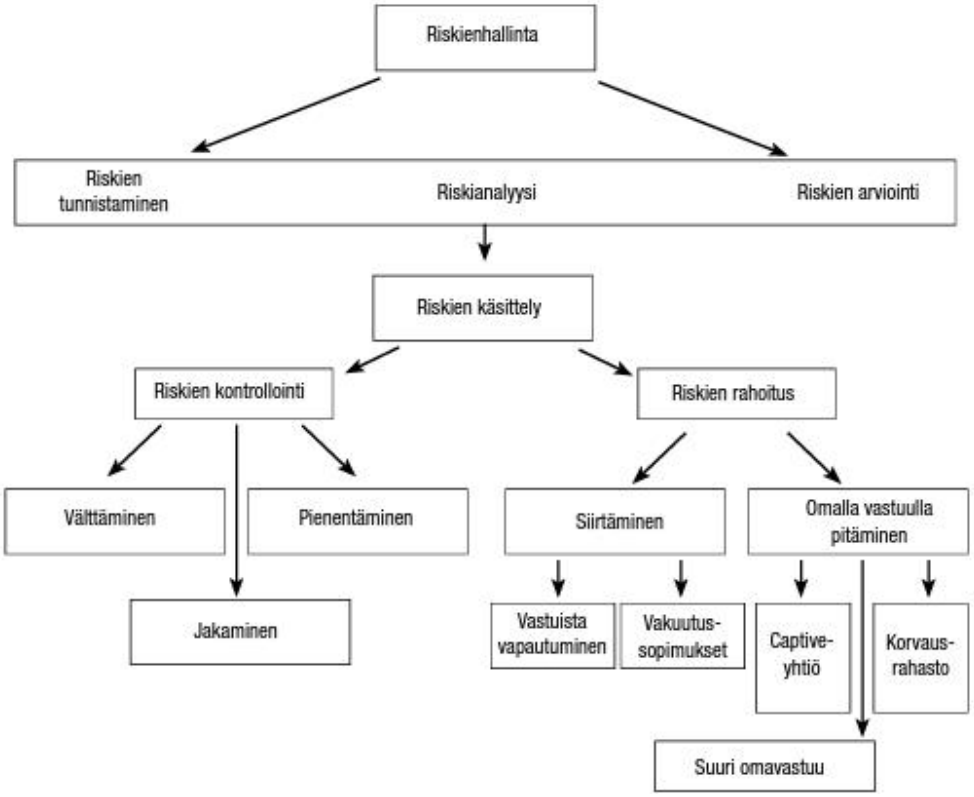
Ylisirniö, M. 2011. Strateginen mittaaminen. WSOY.

LIITTEET

Liite 1. Riskiehallintaprosessit



Kuva 11. ISO 31000 mukainen riskienhallintaprosessi (Juvonen 2014, 18).



Kuva 12. Riskienhallinnan prosessi Heilmannin mukaan (Juvonen 2014, 23).